Capital Markets Law Journal, 2024, **19**, 207–229
https://doi.org/10.1093/cmlj/kmae010
Advance access publication 12 June 2024
Article

OXFORD

Crypto custody

Dirk Zetzsche, Julia Sinnig and Areti Nikolakopoulou*

*Dirk Zetzsche, Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Department of Law, Faculty of Law, Economics and Finance, University of Luxembourg, and Co-Lead, FinTech National Centre of Excellence, Luxembourg. Julia Sinnig, Postdoctoral Researcher, ADA Chair in Financial Law (Inclusive Finance), University of Luxembourg, Luxembourg. Areti Nikolakopoulou, PhD Researcher, ADA Chair in Financial Law (Inclusive Finance), University of Luxembourg, Luxembourg. This research was funded in whole, or in part, by the Luxembourg National Research Fund (FNR), grant reference NCER22/IS/16570468/NCER-FT.

Key points

- This article discusses the EU's approach to regulating crypto custody services under the Market in Crypto-assets (MiCA) Regulation against the background of asset diversions and misappropriations observed throughout the Crypto Winter.
- It seeks to identify whether MiCA meets its legislative objectives and whether it provides a sufficiently solid foundation for the future of the emerging crypto industry.
- We find that MiCA's focus is on what we have called herein 'institutional resilience', ensuring that the custodian is soundly organized and governed and must not reuse clients' assets on their own accounts.
- At the same time, MiCA lacks strength on 'asset resilience' (ie providing safeguards for cases where the custodian, third parties, the token-issuer or DeFi application, as the case may be, encounter difficulties).

1. Introduction

This article discusses the EU's approach to regulating crypto custody under the Markets in Crypto-assets (MiCA)[1] Regulation. To ensure financial stability, an adequate degree of investor protection, market fairness and integrity in places where gaps in the traditional EU financial regulation have been identified,[2] MiCA subjects crypto-asset service providers (CASPs) to both licensing and financial supervision if they provide certain crypto-asset services specified in Article 3(1)(16) MiCA. The provision of custody and administration of crypto-assets on behalf of clients is one such crypto-asset service.[3]

Custody is one means of providing safekeeping and is the main function of investment fund depositaries.[4] Under established investment fund regulation, custody requires registration 'in a financial instruments account opened in the depositary's books' or physical delivery to the depositary.[5] The AIFMD[6] limits the holding in custody to financial instruments, whereas for other

[1] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA) [2023] OJ L150/40.
[2] MiCA, recs 1, 2 and 4.
[3] For an empirical analysis of the current crypto custody practice, cf Dirk Zetzsche and Areti Nikolakopoulou, 'Crypto Custody and Crypto Wallets—An Empirical Assessment' (2024), Working Paper <www.ssrn.com/abstract=4769396> accessed 25 April 2024.
[4] Sebastiaan Hooghiemstra, 'Depositary Regulation' in Dirk Zetzsche (ed), *The Alternative Investment Fund Managers Directive* [hereinafter: *AIFMD*] (3rd edn, Kluwer 2020) 460.
[5] AIFMD, art 21(8)(a)(i).
[6] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (AIFMD) [2011], OJ L174/1.

Accepted: 26 April 2024

assets, ownership verification and record-keeping is required.[7] The widespread insecurity about the qualification of crypto-assets as financial instruments or not[8]—prior to MiCA—also impacted on what custody and safekeeping of crypto-assets was deemed to entail; this, in turn, may have contributed to token-holders' losses in a period known as the Crypto Winter,[9] with billions of Euros in asset value lost in less than two years.[10] These losses have undermined the token-holders' trust in crypto, threatening to halt the growth of crypto and investments in distributed ledger technology (DLT) at large,[11] not even two years after enthusiastic predictions of a golden crypto future.[12] Even today, when Bitcoin as most prominent digital asset experiences an upturn in the Spring of 2024, most large-volume crypto-assets (such as Ether, Tether, USCD) trade below their record highs of 2023. In this article, we seek to identify where MiCA furthers legal certainty in this regard, as well as the robustness of the crypto custody system at large, and whether MiCA provides a sufficiently solid foundation for the future of the emerging crypto industry.

First, we discuss the context of crypto custody against the background of the Crypto Winter, the current market needs and the international proposals to regulate crypto in Section 2. We then highlight the scope of MiCA's custody rules, as well as the general requirements applicable to all CASPs, and those affecting crypto custodians in particular in Section 3. Thereafter, Section 4 issues policy considerations, and Section 5 concludes.

2. The case for regulating crypto custody

Large-scale asset misappropriations

Starting in the second half of 2021, a series of operational shortcomings, malfunctions and asset diversions of major crypto projects became apparent, with losses often in the hundred millions of US Dollars.[13] Following the Terra-Luna stablecoin algorithms' collapse in May 2022 that wiped out US$50 billion in just three days,[14] the crypto industry experienced large-scale turmoil, sparking a string of bankruptcies of prominent crypto firms such as Three Arrows Capital, Voyager Digital and Celsius Network, culminating in FTX's failure, which has been referred to as the 'Lehman moment'[15] for the crypto industry. What is now dubbed the 'Crypto Winter of 2022–2023'[16] severely undermined investors' trust in the crypto industry, triggered asset price deterioration, and several spillover effects into traditional finance. Eventually, this event pushed crypto up policymakers' agendas.

The role of crypto custodians

Crypto custodians have played and continue to play a pivotal role in crypto malfunctions. Crypto custody, so far, has usually taken the form of 'hot' collective custody, meaning that the wallet provider stores all of their clients' private keys together in wallets that are permanently online and linked to the distributed ledger. These (sort of) 'omnibus wallets' are significantly vulnerable to internet attacks and security breaches.[17]

[7] AIFMD, art 21(8).
[8] cf Hooghiemstra (n 4) 465–466.
[9] Douglas Arner and others, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022–2023' (2024) Computer & Security Review, available as (2023) UNSW Law Research Paper no. 23–31, 19, 6ff. <https://ssrn.com/abstract=4372516> accessed 25 April 2024; Dirk Zetzsche and others, 'Remaining Regulatory Challenges in Digital Finance and Crypto-Assets after MiCA' (2023) Study for the European Parliament, 33ff. <https://ssrn.com/abstract=4487516> accessed 25 April 2024.
[10] ibid.
[11] LHoFT, PWC and ALFI, 'Crypto-assets Management Survey 2nd edition' (Report, May 2023) <app_data-import-alfi-crypto-assets-management-survey-2023.pdf> accessed 25 April 2024.
[12] PwC, Elwood and AIMA, '4th Annual Global Crypto Hedge Fund Report 2022' (Report, June 2022) 3. <https://www.pwc.com/gx/en/financial-services/pdf/4th-annual-global-crypto-hedge-fund-report-june-2022.pdf> accessed 25 April 2024.
[13] cf Arner and others (n 9) 6ff; Zetzsche and others (n 9) 33ff.
[14] CoinMarketCap, 'Historical Data for TerraClassicUSD' (*CoinMarketCap*) <https://coinmarketcap.com/currencies/terrausd/historical-data/> accessed 25 April 2024.
[15] Zetzsche and others (n 9) 38.
[16] ibid 33ff.
[17] ibid 46–47.

In this environment, six deficiencies contributed to token-holders losing trust in crypto:

1) Crypto custodians were unable to prevent the loss of private keys administered by them relating to their clients' assets;[18]
2) Crypto custodians applied custody policies insufficient to address cyber-risks, misrepresentations, theft and fraud from the inside and the outside;[19]
3) Crypto custodians mixed custody business with risk-exposed activities of crypto exchanges, brokers, investments and lending on the same balance sheet.[20] Multi-functional CASPs providing custody in relation to their other crypto-asset services mimicked the financial conglomerate model of TradFi, yet neglected to implement the same safeguards, information barriers and internal controls. In turn, conflicts of interest became widespread throughout the industry and counterparty risks from other types of businesses undermined the crypto custodians' own stability;[21]
4) Crypto custodians commingled numerous clients' assets with their own assets in a way that neither their clients' assets nor their own were identifiable as such. This was, for instance, the case for 'collective' hot (online) wallets where multiple clients' assets—and usually the custodian's own assets—are commingled;[22]
5) Crypto custodians executed deficient bookkeeping, asset earmarking, internal controls, and business continuity practices so that in hindsight transactions on behalf of clients could not be distinguished from those in the custodian entity's own name;[23] and
6) Crypto custodians reused client assets for proprietary trading on their own or a related entity's account. In particular, large losses from proprietary trading were covered with clients' custodial assets.[24] Still today, more than one year after the Crypto Winter ended, in their terms and conditions, many custodians entitle themselves to reuse the entrusted assets for their own investment or business purposes.[25]

News about these deficiencies hit crypto markets hard at a time when signs of market concentration were emerging. When some of the new systemically important crypto intermediaries (SICIs)[26] were failing, with risks to token-holders, market stability and market integrity of systemic dimensions, clients initiated massive sell-offs akin to bank runs[27] common to TradFi. These sell-offs revealed previously unknown interconnections and spillover effects[28] into TradFi markets, further undermining the stability of crypto custodians.

The many bankruptcies of crypto custodians occurring in the vicinity of these events[29] further revealed that when token-holders depended on their custodians the most, prominent custodians

[18] *Inter alia* Gareth Jenkinson, 'CoinEx hack: Compromised Private Keys Led to $70M Theft' (*Cointelegraph*, 19 September 2023) <https://cointelegraph.com/news/coinex-compromised-private-keys-behind-70-million-hack> accessed 25 April 2024; Sidhartha Shukla, 'Crypto Exchange HTX Hit by $258 Million Outflow After Hack' (*Bloomberg*, 11 December 2023) <https://www.bloomberg.com/news/articles/2023-12-10/justin-sun-linked-crypto-exchange-htx-sees-258-million-outflow-after-hack> accessed 25 April 2024.

[19] Reuters, 'Exclusive: Behind FTX's Fall, Battling Billionaires and A Failed Bid to Save Crypto' (*Reuters*, 11 November 2022) <https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto 2022-11-10/> accessed 25 April 2024.

[20] ibid.

[21] SEC, 'SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao' (*SEC*, 5 June 2023) <https://www.sec.gov/news/press-release/2023-101> accessed 25 April 2024.

[22] For an overview of the crypto-asset segregation and commingling practices on-chain as well as off-chain, cf Zetzsche and Nikolakopoulou (n 3).

[23] Khadim Shubba, Joshua Oliver and Sujeet Indap, 'New FTX chief Says Crypto Group's Lack of Control Worse than Enron' (*Financial Times*, 18 November 2022) <https://www.ft.com/content/7e81ed85-8849-4070-a4e4-450195df08d7> accessed 25 April 2024.

[24] ibid; Oliver Knight, 'Lender Babel Finance Lost $280M Trading Customer Funds: Report' (*Coindesk*, 29 July 2022) <https://www.coindesk.com/business/2022/07/29/babel-finance-lost-280m-trading-customer-funds-report/> accessed 25 April 2024.

[25] On the practice of reuse, cf Zetzsche and Nikolakopoulou (n 3).

[26] Arner and others (n 9) 15–16.

[27] Jannik Woxholth and others, 'Competing Claims to Crypto assets' (2024) 28 Uniform Law Review 226, 5ff.

[28] Bank for International Settlements, 'Financial Stability Risks from Cryptoassets in Emerging Market Economies' (2023) BIS Policy Papers 138, 7–18, 21–22 <https://www.bis.org/publ/bppdf/bispap138.pdf> accessed 25 April 2024; Roshan Iyer and Adina Popescu, 'New Evidence on Spillovers Between Crypto Assets and Financial Markets' (2023) IMF Working Papers 2023/213, 22ff <https://www.imf.org/en/Publications/WP/Issues/2023/09/30/New-Evidence-on-Spillovers-Between-Crypto-Assets-and-Financial-Markets-539476> accessed 25 April 2024.

[29] Zetzsche and others (n 9) 36ff.

could not deliver on their promise of safeguarding their clients' assets.[30] The insolvency proceedings made it transparent that proper asset segregation, business continuity and recovery approaches, as well as other good custody practices, were lacking throughout the industry. Clients were left entirely unprotected, while the patchy, yet emerging crypto property and insolvency laws in most jurisdictions[31] did little to further private protection for the token-holders themselves.

All in all, these instances prompt the question of whether the term 'custodian' would be the right term for this type of crypto service, since, after all, very little was held 'in custody' or safeguarded at all.

International proposals to regulate crypto custodians

In light of all these incidents, the crypto custodians have already become the focal point of international policymakers, resulting in partly overlapping policy proposals as displayed (cf Table 1).

According to policy recommendations of the FSB,[32] the IMF[33] and the IOSCO[34] addressing crypto custody, the custodians shall safeguard the entrusted assets and their clients' rights against loss and misuse especially in the event of insolvency, and they shall provide proper controls, as well as operational, cyber-resilience and risk-minimizing custody policies. They must also keep correct and up-to-date records establishing their clients' holdings. Furthermore, they shall segregate the entrusted crypto-assets from their own proprietary assets, while title transfer arrangements and reuse of clients' assets shall be permitted only with the client's prior express consent and extensive *ex ante* disclosures. When the safekeeping is outsourced, they shall implement similar safeguards and additional risk management and inform the clients accordingly.

Moreover, the custodian shall provide transparency regarding *inter alia* the rights and obligations stemming from the custodial agreement, safeguarding arrangements, any outsourcing, any use of omnibus accounts, the respective reuse of clients' assets, as well as all other related risks.

In addition, the multi-functional CASPs also offering custody shall identify, disclose and manage any conflicts of interest, and shall be subject to a mandatory separation of functions or even disaggregation of business lines. The IMF and the IOSCO set requirements on the safekeeping and segregation of clients' funds; on top of that, custodians must have additional own funds or participate in guarantee schemes to compensate the clients in the event of asset loss or theft, or insurance of the assets. The IMF further recommends the adoption of an effective wind-down plan, while the IOSCO suggests proper and frequent on-chain and off-chain reconciliations.

The crypto market today

In the aftermath of these events, crypto inevitably pushed its way onto the agenda of regulators and supervisory authorities in multiple jurisdictions. In addition to the recent 25-year sentence of Sam Bankman Fried, former CEO of FTX,[35] regulators launched a series of enforcement

[30] ibid.

[31] cf Woxholth and others (n 27) 7–19.

[32] Financial Stability Board, 'Global Regulatory Framework for Crypto-Asset Activities' (17 July 2023) FSB Policy Papers. <https://www.fsb.org/wp-content/uploads/P170723-1.pdf> accessed 25 April 2024; Financial Stability Board, 'High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final report' (17 July 2023) FSB Policy Papers <https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/> accessed 25 April 2024 [referred to in Table 1 as 'FSB (2023)'].

[33] International Monetary Fund, 'Elements of Effective Policies for Crypto Assets' (February 2023) IMF Policy Papers <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092> accessed 25 April 2024 (referred to in Table 1 as 'IMF (2023)'); Parma Bains and others, 'Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets' (September 2022) Fintech Notes 2022/007 <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715> accessed 25 April 2024 (referred to in Table 1 as 'IMF (2022)').

[34] International Organization Of Securities Commissions, 'Final Report, Policy Recommendations for Crypto and Digital Asset Markets' (November 2023) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf> accessed 25 April 2024 [referred to in Table 1 as 'IOSCO (2023)'].

[35] Luc Cohen and Jody Godoy, 'Bankman-Fried Sentenced to 25 Years for Multi-Billion Dollar FTX Fraud' (*Reuters*, 28 March 2024) <https://www.reuters.com/technology/sam-bankman-fried-be-sentenced-multi-billion-dollar-ftx-fraud-2024-03-28/> accessed 25 April 2024.

Table 1. International recommendations on crypto custody (and MiCA implementation)

Regulatory requirement for crypto custodians	*Recommended by*	*MiCA provisions*
Transparency and disclosures on the rights and obligations of the custodial agreement, the custodian's safeguarding arrangements, reuse, outsourcing, etc.	Recommendations 1, 5, 6, 7 FSB (2023); Element 5 IMF (2023); pp 22–24 IMF (2022); Recommendations 12, 13, 14, 18 IOSCO (2023)	Article 75(1), (9)
Conflicts of interest and risk management, and separation for multi-functional CASPs also offering custody	Recommendations 4, 5, 8, 9 FSB (2023); Element 5 and Annex III IMF (2023); pp 23–24 IMF (2022); Recommendations 2, 3, 17 IOSCO (2023)	Article 72
Asset segregation and protection of clients from default of custodian/ reuse of assets and/or title transfer arrangements only with the client's explicit prior consent and disclosure	Recommendation 5, 7 FSB (2023); Element 5 IMF (2023); Table 1 and p 23 IMF (2022); pp 22–23 IMF (2022); Recommendations 12, 13, 14 IOSCO (2023)	Articles 70(1), 75(7)
Operational resilience and proper risk-minimizing custody policy	Recommendations 5, 7, 8 FSB (2023); Element 5 IMF (2023); pp 22–23 IMF (2022); Recommendations 12, 14, 17 IOSCO (2023)	Articles 68, 75(3)
Safekeeping of clients' assets	Recommendation 5 FSB (2023); Element 5 IMF (2023); Table 1 and pp 22–23 IMF (2022); Recommendations 14, 16 IOSCO (2023)	Article 70(1)
Safekeeping of clients' funds	Element 5 IMF (2023); Table 1 and pp 22–23 IMF (2022); Recommendation 16 IOSCO (2023)	Article 70(2)–(5)
Record-keeping establishing clients' rights and positions	Recommendation 5 FSB (2023); Table 1 and p 23 IMF (2022); Recommendation 12 IOSCO (2023)	Article 75(2)
Outsourcing: similar safeguards, additional risk management and information of the client	Recommendations 5, 7 FSB (2023); Element 5 IMF (2023); pp 23–24 IMF (2022); Recommendation 14 IOSCO (2023)	Article 73, 75(9)
Insurance of custodied assets/ custodian's guarantee	Element 5 IMF (2023); p 23 IMF (2022); Recommendation 15 IOSCO (2023)	Article 67(4), (6)
Reconciliation processes	Recommendation 15 IOSCO (2023)	–
Effective wind-down plan	Element 5 IMF (2023); p 24 IMF (2022)	Article 74

cases and lawsuits against the largest crypto companies, most notably Coinbase[36] and Binance.[37]

Even today, when Bitcoin as the most prominent digital asset experiences an upturn in the Spring of 2024 (which effects unique to Bitcoin may help explain[38]), most large-volume crypto-assets (such as Ether, Tether, USCD) trade below their record highs of 2023 or, in the case of

[36] Bob Van Voris, 'SEC Suit against Coinbase Can Go Forward, Judge Rules', (*Bloomberg*, 27 March 2024) <https://www.bloomberg.com/news/articles/2024-03-27/sec-suit-against-coinbase-can-go-forward-judge-rules> accessed 25 April 2024.

[37] Chris Prentice and Hannah Lang, 'Binance, SEC Face Off over Regulator's Crypto Oversight', (*Reuters*, 22 January 2024) <https://www.reuters.com/legal/binance-kicks-off-oral-arguments-push-end-sec-lawsuit-2024-01-22/> accessed 25 April 2024; Turner Wright, 'What to expect at Changpeng Zhao's sentencing on April 30' (*Cointelegraph*, 15 April 2024) <https://cointelegraph.com/news/changpeng-zhao-sentencing-binance> accessed 25 April 2024.

[38] One notable price effect may stem from 'bitcoin halving'. For an overview of how the bitcoin halving creates scarcity and increases the demand and thus the price of Bitcoin, cf Luke Conway, 'What Is Bitcoin Halving? Definition, How It Works, Why It Matters' (*Investopedia*, 15 April 2024). < https://www.investopedia.com/bitcoin-halving-4843769> accessed 25 April 2024.

stablecoins like Tether and USCD, below par. All in all institutional investors remain reluctant to invest large-scale amounts in crypto, but increasingly engage on an experimental level. In turn, institutional services like crypto ETFs,[39] stablecoin by global payment service provider Paypal,[40] exchange-traded products drawing on Bitcoin, and TradFi-based crypto-asset and custody solutions[41] have emerged. The ongoing institutionalization of crypto makes the need for a proper regulatory framework even more apparent.

3. MiCA's rules on crypto custodians

The bespoke rules for CASPs in Title V MiCA cover the crypto-asset services defined in a long list in Article 3(1)(16) MiCA. One of these services is the 'provision of custody and administration of crypto-assets on behalf of clients' (cf Article 3(1)(16)(a) MiCA). While this list is far from complete (for instance, it does not cover crypto-lending and crypto-staking expressly[42]), MiCA does not require that any activity is the provider's main or exclusive activity. For MiCA's custody rules to apply, it is sufficient that the CASP offers—amongst others—custody and administration services for crypto-assets on behalf of clients.

For these services, any CASP needs an authorization subject to Title V Chapter 1 MiCA, which may either be specific to a crypto-asset service, or an expansion of an existing license as, for example, a credit institution, an e-money institution, a payment service provider, MiFID investment firm, or investment fund manager.[43] On top of that, Title V Chapter 2 MiCA provides for general rules applicable to all CASPs, while Title V Chapter 3 MiCA stipulates rules for certain regulated activities. After explaining the scope of Title V MiCA in the custody context, below we discuss the most important operating requirements.

Scope of MiCA's custodian rules

Article 4(3) MiCA exempts a number of token types from the whitepaper duties laid down in Title II MiCA.[44] Article 4(5) MiCA provides the analogous exemption with regard to crypto-asset services in relation to these token types; in all of these cases, the CASP is exempted from Title V MiCA.

Issues of delineation emerge in relation to three aspects: the application of acts of the EU financial law acquis other than MiCA; the extent to which MiCA applies to fully decentralized applications; and MiCA's definition of 'custody'.

Distinction from other EU financial laws

MiCA is a gap-filling exercise focusing on crypto-assets.[45] It does not apply where financial services are already regulated (cf Article 2(4) MiCA). In turn, MiCA's rules do not apply where a digital asset qualifies as a financial instrument or a structured deposit, to name only two of several examples. In light of the former, MiCA's scope is limited to EMTs,[46] ARTs[47] and 'other crypto-assets' within the scope of MiCA that do not qualify as EMTs and ARTs.[48]

Note that MiCA's list of exemptions does not mention collective portfolio management. In turn, for investment funds sometimes only the rules for funds investing in financial instruments

[39] BlackRock, Fidelity and VanEck have gained the US SEC's approval for Bitcoin exchange-traded funds; cf Paul Katzeff, 'SEC Approves New Bitcoin ETFs: What It Means For Investors' (*Forbes*, 11 January 2024). < https://www.forbes.com/advisor/investing/cryptocurrency/sec-approves-new-bitcoin-etfs/> accessed 25 April 2024.

[40] Paypal, PayPal Stablecoin, US Dollar Cryptocurrency. <https://www.paypal.com/us/digital-wallet/manage-money/crypto/pyusd> accessed 25 April 2024.

[41] For instance, Fidelity Digital Assets currently offers Bitcoin and Ether custody and trading on their own platform, cf Fidelity Digital Assets. <https://www.fidelitydigitalassets.com/trading-custody> accessed 25 April 2024.

[42] Zetzsche and others (n 9) 52–69.

[43] MiCA, art 59(1)(b).

[44] Pursuant to MiCA, art 4(3), these include crypto-assets offered for free; rewards for validation, utility tokens and tokens in limited networks of merchants.

[45] MiCA, art 3(1)(5): crypto-asset 'means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology'. For a detailed discussion of MiCA's scope, see Dirk Zetzsche and Jannik Woxholth, *EU Regulation of Crypto-assets* (Cambridge University Press 2024), ch 3 (forthcoming).

[46] MiCA, art 3(1)(7).

[47] ibid art 3(1)(6).

[48] ibid art 4(1).

apply,[49] sometimes only the rules for alternative investment funds apply[50] and sometimes MiCA's rules on top of the rules on alternative investment funds apply. Notably, under EU financial law, the custody of assets on behalf of alternative investment funds is subject to particular rules specified in Article 21 AIFMD.[51] We focus in this article on MiCA's custody rules only[52] and touch upon the relationship with other intermediary types only in passing.

Fully decentralized applications as CASPs?

For some crypto-assets, in particular Bitcoin, it is difficult to identify a single token issuer. Pursuant to Recital 22, '[w]here crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of [MiCA]. Crypto-asset service providers providing services in respect of such crypto-assets should, however, be covered by' MiCA. Recital 22 therefore clarifies that CASPs must comply with Title V MiCA even where Titles II, III and IV MiCA do not apply. We welcome this clarification as, with regard to crypto custodians, it renders the difficult decision as to what constitutes 'partly' decentralized applications in contrast to 'fully decentralized applications' unnecessary. This means that for tokens issued by partly and fully decentralized applications, the CASP rules apply if a crypto-asset service is being provided.

Beyond the qualification and degree of centralization of the token issuer, whether Title V applies to *fully decentralized custody providers* requires further consideration. From the outset, the answer seems to be in the affirmative, as Title V is activity-based. Yet, the definition of a CASP in Article 3(1)(15) MiCA states that 'crypto-asset service provider' means '*a legal person or other undertaking* whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis' (emphasis added). This notion is confirmed by the (non-binding) Recital 22 that excludes from the scope of MiCA the provision of crypto-asset services in a fully decentralized manner without any intermediary.

On that basis, fully decentralized applications challenge the CASP definition on two grounds. First, the requirement of a 'legal person' or 'undertaking' could be missing. Second, given that smart contracts perform services, we could question whether the service is provided by a person and/or on a professional basis. MiCA does not define 'undertaking' but the general understanding as 'a task or project, especially one that is important and/or difficult,' similar to a venture,[53] would cover decentralized crypto projects.[54] Regarding the second element, namely the question of whether or not the service is provided by smart contracts or natural persons, we argue that this is not a criterion of relevance for MiCA's scope (ie MiCA applies regardless of whether the service is performed by code or humans and that service provision by smart contracts is one of the characteristic features of the crypto industry).[55] Yet, national competent authorities (NCAs) have a hard time identifying someone to comply with the regulation if the service is provided by an application that is entirely dispersed, with multiple unrelated parties contributing, and with Bitcoin nodes functioning as the archetype. For that reason, we hold that whenever *someone* controls an application, be it by legal or factual means, that 'someone' is the CASP for the purposes of Title V MiCA.[56] Second, the term 'on a professional basis' singles out mere hobby projects. In EU financial law, generally, 'professional basis' materializes if the service is provided on a permanent basis and the provider (ie platform) looks out for clients by way of

[49] Directive 2009/65/EC of the European Parliament and of the Council of 13 July on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (recast) (UCITSD) [2009] OJ L 302/32.
[50] AIFMD.
[51] For details on fund custody on behalf of alternative investment funds, see Hooghiemstra (n 4) 441ff.
[52] For a detailed analysis of the intersection between MiCA and investment fund law, see Dirk Zetzsche, Filippo Annunziata and Julia Sinnig, 'Digital Assets, MiCA and EU Investment Fund Law' (2024) EBOR, forthcoming. <https://ssrn.com/abstract=4637019> accessed 25 April 2024.
[53] 'Undertaking, noun' (*OALD Online*, OUP 2022) <https://www.oxfordlearnersdictionaries.com/definition/english/undertaking?q=undertaking> accessed 25 April 2024.
[54] This understanding is confirmed by MiFID which uses the same term for other regulated activities in regard to financial instruments.
[55] Dirk Zetzsche, Douglas Arner and Ross Buckley, 'Decentralized Finance (DeFi)' (2020) 6 Journal of Financial Regulation 172, 181.
[56] For a detailed analysis, see Zetzsche and Woxholth (n 45) ch 7 (forthcoming).

client-oriented communication.[57] This requirement is fulfilled by many crypto custody solutions.

Control over cryptographic keys as a core criterion of 'custody'

Article 3(1)(17) MiCA states that the provision of 'custody and administration of crypto-assets on behalf of clients' means 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.

Two issues arise from this legislative text. First, MiCA clarifies that crypto-assets *can* be held in custody, a matter that was widely discussed prior to MiCA.[58] Second, given that a crypto-asset is intangible, and its existence depends on recognition by the nodes in the DLT, it defines that custody 'means the safekeeping or controlling … of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys.'[59] The former is supplemented by Recital 83, stating that the custody agreement shall 'specify, inter alia, the nature of the service provided, which could include the holding of crypto-assets belonging to clients *or* the means of access to such crypto-assets, in which case the client might keep control of the crypto-assets in custody. Alternatively, the crypto-assets or the means of access to them could be transferred to the full control of the crypto-asset service provider.' (Italics added by authors).

We wonder what 'holding' of a crypto-asset means for an asset class where the existence of the crypto-asset depends on the processing of the same code by multiple nodes, hence the token itself is potentially stored on multiple servers simultaneously, and only the access key preserved to the holder of crypto-asset. This shifts the attention from safeguarding to the second feature mentioned in Article 3(1)(17) MiCA: control of the means of access to such crypto-assets.

In simple terms, control over their clients' private keys means control of the crypto-assets assigned to those keys.[60] Each user has, typically, a pair or pairs of private–public keys consisting of a private (secret) key from which a public (openly disclosed) key is mathematically derived. The public key is functionally equivalent to a bank account number that 'identifies' it to other users, so the account can receive or send funds, while the private key is the functional equivalent of the PIN code or the signature in a bank cheque that enables the holder to control and spend the bank account balance. Meanwhile, a crypto wallet is a digital tool that stores these keys.[61]

However, MiCA does not specify exactly what 'control' over the keys entails. This is an important feature when it comes to defining which wallet providers fall under the definition of Article 3(1)(17) MiCA, thereby delineating providers offering custodial wallet services from those offering a so-called self- or non-custodial wallet outside of MiCA's scope.[62] This distinction is crucial given that practice has developed a full spectrum of custodial, non-custodial and middle-ground wallet solutions.[63]

On one side of the spectrum are custodial solutions where *clients do not have direct access* to either the crypto-assets or private keys. The custodian generates fresh public–private key pairs (or wallets) for the crypto-assets they accept to hold in custody. The safekeeping and recovery of the keys and assets here are tied to the custodian.[64]

[57] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (MiFID) [2014] OJ L173/349, rec 12 and 30.

[58] cf Woxholth and others (n 27) 7–19; Zetzsche, Annunziata and Sinnig (n 52) 24 (in press).

[59] MiCA, art 3(1)(17).

[60] For an overview, cf Carol Goforth and Yuliya Guseva, *Regulation of Cryptoassets, American Casebook Series* (2nd edn, West Academic Publishing 2022) 760–781, 790; Primavera De Filippi and Aaron Wright, *Blockchain and the Law: the Rule of Code* (Harvard University Press 2018) 14–16, 20–29; Stephen Small, 'Bitcoin: The Napster of Currency' (2015) 37 Houston Journal of International Law 581, 588ff; Philipp Maume, Lena Maute and Mathias Fromberger, *The Law of Crypto Assets* (Bloomsbury 2022) 6–10; Wulf Kaal and Hayley Howe, 'Custody of Digital Assets' (2023) 63 Jurimetrics 169.

[61] De Filippi and Wright (n 60) 21; Small (n 60) 588–89; Maume, Maute and Fromberger (n 60) 10; Matthias Haentjens, Tycho de Graaf and/Ilya Kokorin 'The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them' (2020) 2020 Singapore Journal of Legal Studies 526, 531–34.

[62] MiCA, rec 83 *in fine*.

[63] Examples of custodial wallet providers include CEFFU, Coinbase Custody, Taurus, BitGo, Seba Bank; non-custodial wallet providers include Trezor, Atomic Wallet, MetaMask; middle-ground solutions include Ledger Recover, Zengo wallet, Casa 2-of-3 multisig wallet.

[64] For custodial wallet providers' examples, cf n 63.

On the other side of the spectrum are custody solutions where *only the client has possession of the keys* (so-called self-custody). For these cases, MiCA's recitals clarify that the service provider is outside the definition of custody, and thus does not provide a crypto-asset service under MiCA.[65]

The users will generate and control their own key pairs to hold crypto-assets. This usually happens via a hierarchical deterministic wallet[66] with a seed encoded as mnemonic,[67] where the seed is the master key, randomly generated during the wallet initialization by the user, and the latter needs to back it up.[68] If the user loses access to their wallet and the seed, their assets are utterly lost.[69]

For that reason, middle-ground custody solutions share control over the keys in some way between the user and the wallet provider. Where self-custody is defined by the users' exclusive key control, these cases are borderline and need to be assessed according to the way in which control over the key is exercised.

This results in a taxonomy of middle-ground custody solutions as follows:

1) Wallet providers with middle-ground solutions that assign control of the keys to the client, while the master key is backed up by the wallet provider, belong to the first group of custodial solutions, where control resides eventually with the custodians. For example, in the case of Ledger Recover,[70] the wallet splits the user's seed into three fragments, which are sent to three entities for backup purposes. The keys may be generated by the user at the wallet initialization phase, so that they 'never leave the wallet device'; in fact, the keys may also be regenerated from these backups when necessary. In these cases, the wallet assigns *some* control of the keys to its users, yet the control is not exclusive, so the wallet provider has the capacity to access (and thus potentially control) the keys, while the users (need to) trust that the wallet provider will not abuse that power.[71]
2) The second group of middle-ground solutions, where control resides with the client to a large extent, includes cases of multi-signature[72] ('multisig') wallets, key sharing,[73] or similar technologies. These technologies create multiple keys or key shares which can be held by different persons, while a minimum threshold of these keys or key shares is required to perform any transaction regarding x crypto-assets.[74] In our case, the wallet provider and the client hold different keys or key shares over the same assets. We consider a situation where neither the key(s) or key share(s) held by the client, nor the key(s) or key share(s) held by the service provider are sufficient to initiate a transaction. Therefore, for any transaction to

[65] MiCA, rec 83 *in fine*.

[66] Cryptopedia Staff, 'What Are HD Crypto Wallets?' (*Gemini Cryptopedia*,10 March 2022) <HD Crypto Wallets: What Are They? | Gemini> accessed 25 April 2024, stating that 'A hierarchical-deterministic (HD) wallet generates a new key pair from a master key pair for each crypto transaction to enhance privacy and security. Its hierarchical structure resembles that of a tree, with the master key "determining" the key pairs that follow it in the hierarchy … The vast majority of wallets are hierarchically deterministic.'

[67] The wallet is deterministic because the same seed-master key will always produce the same sequence of keys even when imported to new wallets. The seed is a recovery mechanism. The mnemonic supports information retention or retrieval of the access data to the crypto-asset (the 'keys'). Andreas Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* (2nd edn, O'Reilly Media 2017) ch 5.

[68] For non-custodial wallet providers' examples, cf (n 63).

[69] Vitalik Buterin, 'Why we Need Wide Adoption of Social Recovery Wallets' (*Vitalik*, 11 January 2021) <https://vitalik.ca/general/2021/01/11/recovery.html> accessed 25 April 2024.

[70] Ledger, 'Announcing the Ledger Recover Cryptographic Protocol White Paper' (*Ledger*, 21 June 2023) <https://www.ledger.com/blog/announcing-the-ledger-recover-cryptographic-protocol-white-paper> accessed 25 April 2024.

[71] 'Technically speaking, it is and always has been possible to write firmware that facilitates key extraction. You have always trusted Ledger not to deploy such firmware whether you knew it or not.' Source: Tom Blackstone, 'Ledger clarifies how its firmware works after deleted-tweet controversy' (*Cointelegraph*, 10 May 2023) <https://cointelegraph.com/news/ledger-clarifies-how-its-firmware-works-after-deleted-tweet-controversy> accessed 25 April 2024.

[72] Antonopoulos (n 67) ch 7.

[73] Amos Beimel, 'Secret-sharing Schemes: A Survey' (International Conference on Coding and Cryptology, Quingdao, May–June 2011) 2–3. <https://www.researchgate.net/profile/Amos-Beimel/publication/220776045_Secret-Sharing_Schemes_A_Survey/links/09e41513f14a20f236000000/Secret-Sharing-Schemes-A-Survey.pdf> accessed 25 April 2024; Jean-Philippe Aumasson, Adrian Hamelink and Omer Shlomovits, 'A Survey of ECDSA Threshold Signing' (*Cryptology ePrint Archive*, 2020) 1–7. <https://eprint.iacr.org/2020/1390.pdf> accessed 25 April 2024.

[74] In simple words, depending on the wallet set-up and technology, we encounter wallets with multiple keys or key shares where neither the wallet provider nor the client holds alone the necessary threshold of keys or key shares to initiate a transaction and they need to coordinate (see category 2 of our Taxonomy and example Zengo Wallet), or where the client holds alone the necessary threshold to initiate a transaction (see category 3 of our Taxonomy and example Casa 2-of-3 multisig wallet).

take place, the collaboration and 'co-approval' of the wallet provider *and* the client are necessary. One example of this is the Zengo[75] wallet.

3) Regarding the third middle-ground group, these encompass cases of multisig wallets, key sharing and similar technologies where the client *alone* holds the minimum threshold of keys or key shares necessary to perform a transaction on their own. The wallet provider holds some key(s) or key share(s) that alone are not sufficient for any transaction and does not have access to clients' key(s) or key share(s). Thus, the wallet provider's key(s) or key share(s) shall be mainly held for backup purposes in case the clients lose some of their key(s) or key share(s).[76]

We draw the line here based on the risks clients are facing that rely on the custody solution: where clients face the risk that the means of access could be stolen or obtained by way of 'inside jobs' by parties or persons not entitled to the assets, the typical custodial risks addressed by Title V MiCA do exist. In these cases, MiCA rules (should) apply. In turn, we hold that MiCA applies to the first group of middle-ground custody solutions where all relevant access data (ie where all keys are mere datasets) can be obtained from the service providers' staff, servers and algorithms, but not to the second or third middle-ground categories since here no conduct on the side of the wallet provider or its staff *alone* is sufficient to obtain control over the assets.

In short, whenever the service provider can present a single point of failure that leads to a potential loss of assets, MiCA applies. By contrast, *truly* shared control, where no-one can ever act without the user's consent, is not 'control' for the purposes of Article 3(1)(17) MiCA.

Authorization

Licensing principle

For CASPs that do not hold a relevant license under EU financial law, Articles 59, 61ff. MiCA foresee a fully-fledged authorization requirement.[77] This authorization is of relevance for new service providers that want to serve AIFMs as delegates with regard to order transmission and reception, portfolio management and advice.[78]

Fund managers, e-money and credit institutions, and MiFID firms (as well as other licensed intermediaries) can gain the right to provide crypto-asset services by way of notification to their respective NCA.[79] These entities need to deliver the information relevant for expanding the authorization specified in Article 60(9) MiCA[80] 40 days prior to the commencement of the service to their NCA.[81] To avoid repetitive documentation and double reviews, the CASPs that

[75] Zengo, 'User Agreement' (*Zengo*, 3 October 2023). <https://zengo.com/user-agreement/> accessed 25 April 2024, as follows: 'Zengo uses distributed security, by which our servers hold a key share ("Server Share") to sign transactions, while the other share is on the User's mobile device ("Device Share"). Only when both Shares interact, a Transaction can take place. This means that Zengo is unable to access Users' Assets without their volition and consent.'

[76] An example is Casa 2-of-3 multisig wallet with two hardware keys. cf Nick Neuman, 'Choosing your 3-key Vault Setup' (*Casa*) <https://support.keys.casa/hc/en-us/articles/360045419111-Choosing-Your-Basic-Multisig-Setup> accessed 25 April 2024, as follows: 'Two hardware keys, preferably by different manufacturers (Ledger, Trezor, Coldcard, etc), One Casa Recovery Key (held by Casa for emergencies in case something happens to one of the other keys)'; Casa, 'Casa Terms and Conditions' <https://casa.io/terms-of-service> accessed 25 April 2024, as follows: 'You acknowledge and agree that if you choose to authorize Casa to control a cryptographic key created by you through the Services (a "Recovery Key"), (i) Casa will have sole and exclusive control over such Recovery Key; … You further acknowledge that the Services may require the transmission of multiple cryptographic keys to an Exchange in order to access your digital or virtual currency or assets, and that the Recovery Key alone may therefore be insufficient for such access without at least one (1) or more Private Keys …'.

[77] cf ESMA, 'Consultation Paper on Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA)' ESMA74-449133380-425, 12–29, 76–109 discussing the content of the templates for the application for authorization of the CASPs. For an analysis, cf Zetzsche and Woxholth (n 45) ch 7 (forthcoming).

[78] AIFMD, arts 20(1) and 6(4)(b).

[79] cf, for instance, MiCA, art 60(5) for UCITS and AIFMs with regard to order transmission and reception, portfolio management and advice.

[80] Intermediaries holding a license under EU financial law must submit to the NCA, *inter alia*, a bespoke programme of operations (including types of crypto-assets and marketing countries), disclosures on internal controls, AML/CTF measures and risk assessments, the business continuity plan, the ICT systems and security arrangements in technical and non-technical language, the procedure for the segregation of clients' crypto-assets and funds, the custody and administration policy, whether the crypto-asset service relates to asset-referenced tokens, e-money tokens or other crypto-assets. See further on the notification process ESMA74-449133380-425, 9–11, 54–75.

[81] The NCA then has 20 days to require in one step additional information when the notification is incomplete, and set a new deadline not exceeding 20 days which delays the expiration of the 40-day period. Further requests do not extend the deadline.

hold a license under EU financial law do not need to submit any information that they have already delivered as part of their previous licensing process if that information is identical, but they must state that this is the case in their notification.[82]

EU passport

CASPs that receive authorization are allowed to provide crypto-asset services throughout the Union, either through the right of establishment, including through a branch, or through the freedom to provide services.[83] CASPs that provide crypto-asset services on a cross-border basis shall not be required to have a physical presence in the territory of a host Member State.

General and operating requirements

Title V MiCA mainly regulates the relationships between CASPs and clients (and in some cases, issuers of crypto-assets) and thus applies a regulatory perspective similar to that afforded to investment firms. Title V Chapter 2 MiCA stipulates *general* operating conditions applicable to all CASPs. The most important of these requirements for crypto custodians include[84] the fiduciary duties (Articles 66 and 72 MiCA), delegations and outsourcing (Article 73 MiCA) and asset recovery and business continuity (Article 74 MiCA).

Fiduciary duties (Articles 66 and 72 MiCA)

Equivalent to similar provisions in EU financial law,[85] Article 66(1) MiCA establishes that CASPs are fiduciaries: CASPs 'shall act honestly, fairly and professionally in accordance with the best interests of their clients and prospective clients.' This provision underpins a number of requirements on fairness, transparency and management of conflicts of interest, which follow the principle that clients' interests shall be paramount, unless the clients have been informed and have provided their explicit consent to being treated in a disadvantageous manner.

The fiduciary duties have, on the one hand, a harmonizing effect that aligns the position of CASPs with other off-balance-sheet intermediaries in the field of finance. MiCA clarifies beyond doubt that CASPs must not use clients' assets on their own accounts. On the other hand, it establishes limits to crypto business models resulting in value transfers from clients to the CASPs, as were frequent at the height of the Crypto Winter (cf at Part II).

Outsourcing (Article 73 MiCA)

Article 73 MiCA on outsourcing is modelled on Article 16(5) MiFID and Article 20 AIFMD and the respective implementing legislation.[86] The former's purpose is to ensure the effectiveness of the authorization requirements and financial supervision even where the authorized CASPs rely on other, potentially not authorized, service providers.

CASPs 'that outsource services or activities to third parties for the performance of operational functions shall take all reasonable steps to avoid additional operational risk.[87] They shall remain fully responsible for discharging all of their obligations pursuant to' Title V MiCA. CASPs

[82] cf MiCA, art 60(9).

[83] MiCA, art 65.

[84] We do not discuss herein the prudential requirements (MiCA, art 67) and the provisions on governance and complaints handling (MiCa, arts 68, 69, 71). On the governance arrangements for the continuity and regularity in the performance of services as well as the record-keeping obligations for all CASPs, cf ESMA, 'Consultation Paper on Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper' ESMA75-453128700-438, 16–25, 37–54, 102–215. For an overview, see Zetzsche and Woxholth (n 45) ch 7 (forthcoming). On safekeeping of crypto-assets and client funds subject to MiCA art 70, cf 'Safekeeping and custody' section.

[85] MiFID, art 24, UCITSD, art 25, AIFMD, art 21(10).

[86] Commission Directive 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organizational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive [2006] OJ L241/26, arts 13–15; Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision [2013] OJ L083/1.

[87] According to ESMA's initial proposal, the CASPs shall keep detailed records on the outsourcing agreements and the outsourced services and activities, cf ESMA75-453128700-438, 162, 171–172; the CASPs seeking authorization or the notifying entities shall disclose to the Competent Authority their outsourcing policy and in particular the function or person responsible for outsourcing, the resources (human and technical) allocated to the control of the outsourced functions, services or activities and the related risk assessment, cf ESMA74-449133380-425, 58, 81.

engaged in outsourcing need to ensure that the outsourcing does not: (1) result in the delegation of their responsibility; (2) alter the relationship between them and their clients, nor their obligations towards their clients; and (3) alter the conditions for their authorization. Again, events during the Crypto Winter account for the introduction of such rules: many CASPs were inexperienced in financial services, and incapable of handling the operational risks of their DeFi applications and the entities relating to them. These outsourcing rules ensure that the institutional robustness of the licensing principle cannot be circumvented by way of delegation.

The core question relating to Article 73 MiCA is establishing when a service relied on is a *third party* (from MiCA's perspective)[88] and when that third party performs *operational functions*. Where custody as a crypto-asset service is concerned, to qualify as a delegate, that third party must provide material parts of custody services.[89] Given the core of custody is control of the means of access, examples of operational functions include the external storage of private keys, the involvement in the new generation of lost keys or key shares, or the reliance on a sub-custodian with bridges in place to connect to crypto-assets other than those that the custodian can access through their own bridges. Software developer firms are often engaged in code development, hosting and crisis management (in response to cyber-attacks or malfunctions); where these services come with temporary access to, or storage of, the private keys, these firms act as delegates of the CASP, and are consequently indirectly subject to regulation; in the case of sub-custody arrangements, they are subject to direct regulation as a CASP if the firm is located in the EU/EEA.[90] We account for that assessment in the same vein as we classified custody solutions in general (cf at III1.c): whenever the service provider can present a single point of failure that leads to a potential loss of assets, MiCA applies.

Burial plan (Article 74 MiCA)

Article 74 MiCA requires CASPs offering custody the setting up of a burial plan, which is a 'plan that is appropriate to support an orderly wind-down of their activities under applicable national law, including the continuity or recovery of any critical activities performed by those service providers. That plan shall demonstrate the ability of crypto-asset service providers to carry out an orderly wind-down without causing undue economic harm to their clients.' To be effective, the plan needs to be aligned with national insolvency law.[91] The fact that crypto insolvency law is, so far, not harmonized in the EU,[92] undermines the effectiveness of burial plans in protecting clients' assets.[93]

Safekeeping and custody

While Article 75 MICA provides for specific rules on crypto custody, one part of custody, namely the safekeeping of crypto-assets, forms the heading of Article 70 MiCA and is allocated within the general rules applicable to all CASPs.

Custody as qualified safekeeping (Article 70(1) MiCA)

While not all CASPs provide safekeeping in relation to crypto-assets, as they can also safekeep 'funds' (ie cash equivalents) to facilitate payments, in cases where custody *with regard to crypto-assets* is provided, Articles 70(1) and 75 MiCA apply in tandem. MiCA regulates crypto custody then as a qualified form of safekeeping under Article 70(1) MiCA, similar to Article 21(8)

[88] According to ESMA's initial proposal, permissionless DLTs shall be considered a form of 'common good' resource, whereas the use of a permissioned DLT operated by a commercial enterprise will likely be based on contracts available for 'white-labelled' blockchain products, in which case it can be considered as a 'third-party provider'. cf ESMA75-453128700-438, 19. Such a qualification encourages outsourcing to applications the provider cannot control nor monitor, in particular when seen together with privileges ESMA foresees on liability in these cases.

[89] For details, see Zetzsche and Woxholth (n 45) ch 7 (forthcoming).

[90] According to their qualification as CASP laid out in MiCA, art 62(1).

[91] MiCA, art 74: CASPs 'shall have in place a plan that is appropriate to support an orderly wind-down of their activities under applicable national law'.

[92] While the new Proposal for a Directive of the European Parliament and of the Council harmonising certain aspects of insolvency law, COM/2022/702 final, aspires to provide certain degree of harmonization amongst the Member States' insolvency laws, there are serious doubts as to whether the Directive applies in relation to crypto-assets, therefore the problem of non-harmonization remains.

[93] See the discussion on the repercussions of this lacking harmonization at Section 4.

AIFMD that regulates custody as a qualified type of safekeeping for financial instruments on behalf of alternative investment funds.

Within the scope of Article 70(1) MiCA are then not only crypto custodians, but potentially also crypto portfolio managers, crypto exchanges and crypto-lending and crypto-staking services that, albeit not within the scope of MiCA for their main service, hold clients' assets as an ancillary service.

Analogous to Article 16(8) and (9) MiFID, these CASPs 'shall make adequate arrangements to safeguard the ownership rights of clients, especially in the event of the [CASP's] insolvency, and to prevent the use of clients' crypto-assets for their own account.' The first requirement depends on what is necessary to protect the holders of crypto-assets under the insolvency laws applicable in the event of the DeFi application's insolvency or going out of business.[94] The second requirement responds to the widespread abuses where crypto intermediaries (eg FTX Exchange) were treating clients' assets as their own, for instance to cover up losses suffered from risky crypto investments in other parts of their crypto empire (eg Alameda, FTX's investment subsidiary[95]) or to back-up crypto-lending arrangements in which clients' assets are pooled and then transferred to third-party creditors.[96]

Custody contract, policy and procedures under Article 75 MiCA

Article 75 MiCA on custody services requires that CASPs must reside within the European single market,[97] and enter into an agreement with clients in which the contractual details are meticulously prescribed.[98]

The most important stipulations here relate to the parties' identities (which may be difficult to ascertain in cases of fully decentralized systems), the custody policy, a description of the CASP's security systems, the fees, costs and charges to be paid by the client, and the applicable law.[99]

The custody policy must contain procedures aimed at ensuring the safekeeping or control of the means of access to the crypto-assets.[100] This rule responds to the frequent incidents of private keys administered by custodians being misappropriated.[101] Furthermore, clients' rights to crypto-assets as well as any movement, modification, or creation in positions shall be registered in the name of each client,[102] while the client is entitled to receive information on the register entries.[103] This rule shall provide for transparent handling of the exercise of clients' rights.

Moreover, CASPs are obliged to provide procedures necessary for the return of crypto-assets to clients[104] as well as (an operational) segregation of the client's assets from the CASP's assets on the distributed ledger.[105] This shall ensure, for instance, that in the event of the CASP's insolvency, the client's assets remain unimpaired.

Notably, Article 75(4) MiCA establishes a private law provision mandating substitution: changes to the DLT and other events possibly impacting clients' rights shall establish the clients' right 'to any crypto-assets or any rights newly created on the basis and to the extent of the client's positions at the time of the occurrence of that change or event.'[106] While these provisions are meant to protect the custodian's clients, they also subject CASPs to liability risks for events taking place on the DLT which the CASPs may or may not be able to influence; note that a CASP may have no governance right in relation to the token's creation or modification by way

[94] Under most insolvency laws, only persons and entities can become insolvent, and it is uncertain whether DeFi applications qualify as one of the former.
[95] Arner and others (n 9) 8–10.
[96] cf Zetzsche and others (9) 30.
[97] cf MiCA, art 59(2). Where already licensed financial intermediaries provide crypto-asset services pursuant to MiCA, art 60, the authorization requirements of the CRD, MiFID, UCITSD, AIFMD and other pieces of legislation also require that the registered seat and headquarter is located within the EEA.
[98] MiCA, art 75(1). Unlike AIFMD, art 21(2), MiCA, art 75(1) does not require this agreement to be written.
[99] MiCA, art 75(1)(a) to (g).
[100] MiCA, art 75(3).
[101] For an overview of the incidents in Crypto Winter, see Zetzsche and others (n 9) 24.
[102] MiCA, art 75(2) and (4). An equivalent monitoring of an AIF's cashflows and assets held in custody, with the objective of ensuring investor protection, is foreseen by AIFMD, art 21(7) and (8).
[103] MiCA, art 75(5).
[104] ibid art 75(6).
[105] ibid art 75(7). An equivalent asset segregation and registration of an AIF's assets is foreseen by AIFMD art 21(8)(a)(ii).
[106] ibid art 75(4) subpara 2.

of the DLT. If the DLT does not allocate the right, or a particle thereof, to the respective token, it may never come within the custodian's reach.

Custodian's liability

This shifts the focus of attention onto the custodian's liabilities. MiCA introduces a broad rule in Article 75(8) MiCA: the custodian is liable for losing their clients' assets. This rule stands in contrast to the terms and conditions of most crypto custody providers so far that either exclude liability[107] or cap liability up to the total amount of fees charged to clients, constituting a fraction of their clients' losses.[108] The statutory liability is all the more important since liability is not preconditioned on any culpability or fault on the side of the custodian nor their staff.

A closer look reveals, however, that the liability of CASPs is **limited in three respects**. First, the CASP is liable for the loss of crypto-assets or the means of access to these assets only. MiCA does not foresee any other damage that the clients may suffer such as the loss of opportunity or reputational damage.[109] Second, liability is limited to situations attributable to, and under the control of, the CASPs.[110] Third, liability is capped at the market value of the lost crypto-asset at the time the loss occurred. Regardless, Article 75(8) MiCA may function as a game-changer in an environment characterized by a lack of accountability and resilience.

As to what constitutes a loss depends on the interpretation of the substitution rule[111] and the obligation to facilitate their clients' rights more generally: if the custodian decides not to extend custody to any crypto-assets created on the ledger to which their clients would be entitled, the question of whether the clients duly authorized the custodian to forego any claim on the new asset will determine whether (a part of) the assets were, in fact, lost (rather than ceded, voluntarily given up, donated, or something else). The same question of compliant conduct is of relevance when the consensus mechanism and other elements of the underlying DLT generate rewards, benefits or other passive income elements relating to crypto-assets and the custodian refrains from assigning these to their clients; these could be seen as a part of the crypto-asset or a loss stemming from a right separate from the crypto-asset. In this context, Article 66 MiCA, establishing fiduciary duties and the obligation to act in their clients' best interests, will provide a guideline in the absence of express contractual stipulations and client orders.

Even more important to determine is what constitutes an incident that is attributable to the custodian, given that liability is excluded where the loss is not attributable thereto. An attributable incident is any event that occurs in the realm of the custodian's operations that the latter controls or may control. Here, the core matter is what the law assumes the custodian has to control (ie how the custodian must be organized and what resources they must spend on securing such control). This may be derived from Recital 83 MiCA, clarifying that the custodian shall be liable for an ICT-related incident, including an incident resulting from a cyber-attack, theft, or any malfunction.

Therefore, liability under Article 75(8) MiCA results from an exercise of separating attributable from non-attributable incidents. In this regard, it is noteworthy that ESMA interprets Recital 83 MiCA to mean that CASPs using permissionless DLT infrastructure that they do not control or manage (ie no contractual arrangement exists) are exempted from this liability.[112] While this clearly sets incentive to outsource to permissionless rather than the permissioned DLT

[107] For instance CEFFU, 'Ceffu Terms of Use' <https://www.ceffu.com/legal/terms> accessed 25 April 2024, as follows: 'The Custodian assumes no liability for any loss or damage arising from the use of the Account and/or Services by you or any third party with or without your authorization.' Gemini, 'User Agreement' <https://www.gemini.com/legal/user-agreement#section-reasonable-care> accessed 25 April 2024, as follows: 'You further agree that neither we nor any Gemini Service Provider can be held responsible for any … "System Failure" (defined as a failure of any computer hardware or software used by Gemini, a Gemini Service Provider, or any telecommunications lines or devices used by Gemini or a Gemini Service Provider) … provided that we or the relevant Gemini Service Provider (as applicable) used commercially reasonable efforts to prevent or limit such …'. Bitcoin Suisse AG, 'General Terms and Conditions' <https://files.bitcoinsuisse.com/assets/pdf/20220927_General%20Terms%20and%20Conditions_EN.pd> accessed 25 April 2024, as follows: 'Specifically, BTCS shall not be liable for damages …, to the extent permitted by law, if such damages: … occur due to circumstances, both within and outside of BTCS' control, that cause the Services to become unavailable, including routine maintenance.'

[108] For the widespread practice of liability caps, cf Zetzsche and Nikolakopoulou (n 3).

[109] Since MiCA is silent regarding other losses, the fallback is the applicable national law liability regime.

[110] MiCA, art 75(8). The equivalent provision is AIFMD art 21(12) and UCITSD art 24 (1).

[111] ibid. art 75(4).

[112] cf Arner and others (n 9) 8–10.

applications, ESMA tries to remedy this shortcoming by proposing obligations in the event of a disruption involving a permissionless DLT, for instance, to communicate the disruption to the client along with the associated risks and their own liability exclusion for such events and finally, to act in the best interest of the clients. Further, CASPs should remain liable for any losses related to their own smart contracts, such as hacks or exploits, regardless of whether they are deployed on a permissionless or a permissioned DLT.[113] Tables 2 and 3 provide an overview of attributable and non-attributable incidents derived from MiCA's requirements for crypto custodians.

4. Policy considerations

Analysing the strengths and weaknesses of the MiCA crypto custody framework in turn, we first set out our analytical perspective section, before focusing on institutional resilience section and asset resilience section.

Analytical perspective

For the remainder of the article, we assume two different starting points for the analysis of MiCA's crypto custody framework.

We dub the first perspective 'institutional resilience'. Here, we ask whether MiCA ensures that the crypto custodians are soundly organized, and whether that misconduct stemming from events inside the intermediaries is adequately addressed. We thus focus on the operational risk inherent to crypto custody.

The second perspective is called herein 'asset resilience'. Under that term, we review the extent to which the existence or value of the crypto-asset is secured by way of regulation in the event of malfunctions, distress and the insolvency of the custodian, the token-issuer, the DeFi application or any third party, as the case might be. Accordingly, we focus on the overall embedding of MiCA into the legal system.

Institutional resilience

The 'institutional resilience' perspective measures MiCA's robustness in light of the many deficiencies inherent in the custodian's setup and conduct in the context of the Crypto Winter. From this perspective, MiCA is seen as a crisis mitigant by enhancing custodians' resilience.

MiCA ensures that the custodian is a duly authorized[114] fiduciary,[115] soundly organized and governed, subject to prudential requirements, conflicts of interest and operational risk management.[116] Custodians shall segregate[117] their own assets from their clients' assets and avoid the reuse of the latter for their own account.[118] The transparency obligations regarding clients' holdings[119] as well as the liability regime of the custodian[120] pursue the same objective.

However, even where the authorization and operating conditions are robust, the overall resilience desired may not be achieved where service providers have the ability to avoid, or take steps to circumvent, MiCA's authorization and operating conditions.[121]

We see three entry points here through which to undermine institutional resilience: MiCA's scope, liability provisions and outsourcing rules.

Scope

The effectiveness of any MiCA rule is limited by its scope: what is outside of the rules is not addressed by them effectively. We argue herein that limitations on fully decentralized

[113] cf ESMA75-453128700-438, 19, 21, 22.
[114] MiCA, title V ch 1.
[115] MiCA, arts 66 and 72.
[116] MiCA, title V ch 2.
[117] MiCA, arts 75(7) and 70(3).
[118] MiCA, art 70.
[119] MiCA, art 75(1)–(3) and (5).
[120] MiCA, art 75(8) and (6).
[121] We have seen several examples indicating that when the regulation of a jurisdiction on crypto-asset service providers becomes strict, crypto firms choose to seek license/registration in other jurisdictions to circumvent them. For instance, cf William Langley and Chan Ho-him, 'Hong Kong digital assets exchange warns over viability of city's new crypto rules' *Financial Times* (12 April 2024). <https://www.ft.com/content/41651975-4eca-4d6f-8ca2-d17aaf175a2f> accessed 25 April 2024.

Table 2. Attributable events

Incidents resulting in crypto-asset loss	Reasoning
Loss of private key(s)	Articles 3(1)(17); 75(3), (6), (8)
Wallet vulnerability due to insufficiently random generation of the private keys	Articles 3(1)(17); 75(3), (6), (8); Recital 83
Malfunction of the CASP's cybersecurity mechanisms where the attacker impersonates as client	Articles 3(1)(17); 75(3), (6), (8); Recital 83
The attacker disables the 2F authentication system of the custodial CEX and extracts assets from clients' accounts	Articles 3(1)(17); 75(3), (6), (8); Recital 83
System failure of any hardware or software used by the CASP, a service provider of the CASP, or of telecommunications lines or devices used by the CASP or its service provider	Articles 3(1)(17); 75(3), (6), (8); Recital 83
The client cannot obtain a new right substituting for their existing rights because the CASP decides not to support the material operating change of the underlying protocols (eg forks or airdrops)	Articles 75(4), (5), (8)
Loss of the client's assets held in omnibus wallet addresses on the blockchain due to the insolvency of another client whose assets were commingled in the same wallet and the CASP cannot demonstrate properly segregated records and registers	Articles 70(1); 75(2), (8)
Loss of the client's assets because they were held in collective wallet addresses on the blockchain with the custodian's own assets even if the CASP can demonstrate properly segregated records and registers	Articles 70(1); 75(7), (8)
Loss of the client's assets because of use by the CASP for their own account even if the client has signed the terms and conditions enabling such a possibility	Articles 70(1); 75(8); Recital 83
The CASP also providing a transfer service did not forward assets in a way that allowed for the crypto-asset being taken into custody	Articles 70(1); 82

applications, the definition of regulated activities as such, and self-custody may undermine the effectiveness of MiCA's custody rules.

Fully decentralized applications?

We discussed in the 'Fully decentralized applications as CASPs' section that MiCA covers fully decentralized applications only to the extent that they qualify as an 'undertaking'. If regulators construe the definition of 'undertakings' broadly, this will oblige many decentralized applications to introduce governance arrangements as required by Title V MiCA. One may argue this goes against the intention of MiCA which excludes from its scope undertakings that provide crypto-asset services in a fully decentralized manner without any intermediary, thus any identifiable person or entity for enforcement purposes.[122] Practically speaking, regulators may have difficulties when it comes to identifying persons responsible for the application, and to enforce orders in a broadly international environment.[123] By contrast, where regulators construe the definition of 'undertakings' narrowly, more applications remain untouched by MiCA's requirements, to the detriment of institutional resilience.

Custodial versus non-custodial applications?

We have further laid out in the 'Control over crypto-graphic keys as a core criterion of "custody"' section that the scope of MiCA's custody rules in Article 3(1)(17) MiCA rests on a delineation of custodial from non-custodial wallets. The same mechanics laid out in the previous section also apply to this delineation: institutional resilience increases when more DeFi applications are within the scope of MiCA, and decreases when more wallet solutions remain

[122] MiCA, rec 22.
[123] See Zetzsche, Arner and Buckley (n 55) 172–203.

Table 3. Non-attributable events

Incidents resulting in crypto-asset loss	Reasoning
Malfunction of a DeFi algorithm not controlled by the CASP (eg the attacker uses flash loans to buy governance tokens and exploits a token-issuer so the client loses the respective tokens)	Article 75(8) subparagraph 2
Unpredictable governance decisions in decentralized arrangements not controlled by the CASP (cf ESMA75-453128700-438, p 18.)	Article 75(8) subparagraph 2
Client gives away password or the private key or seed phrase because they shared it with others or lost their paper backups	Article 75(8) subparagraph 2
System failure of the client's mobile phone where the wallet is installed	Article 75(8) subparagraph 2
The CASP cannot obtain right substituting for existing rights of client, although the CASP exercised due care in facilitating clients' rights, due to technical malfunctions in the DeFi code	Article 66; 72; 75(4), (5), (8) subparagraph 2
The client cannot obtain a new right substituting for their existing rights because the CASP reserved the discretion to decide to support or not any material operating changes of the underlying protocols (eg forks or airdrops) in the signed terms and conditions, and the CASP exercised due care in assisting the client with any appropriate administrative actions such as enabling the withdrawal or transfer of crypto-assets (where applicable)	Article 66; 72; 75(4), (5), (8) subparagraph 2
The CASP did not receive assets from a separate asset transfer service	Article 75(8) subparagraph 2
The loss of the client's assets occurs due to the client instructing the CASP to send them to a wrong blockchain address	Article 75(8) subparagraph 2

unregulated. This is all the more important having already noted a trend towards non-custodial solutions since the introduction of MiCA and its intention to regulate more centralized crypto solutions were announced.[124]

Restrictions on regulated activities

Finally, institutional resilience is potentially at risk due to the definition of crypto-asset services. Services such as crypto-lending and crypto-staking are potentially out of scope, because they do not provide regulated crypto-asset services (for instance, custody or transfer services).[125]

Often, multi-function CASPs combine custody with risk-taking activities such as proprietary trading. How MiCA deals with these services besides conflict rules[126] is somewhat unclear: even the 'Significant CASPs' subject to bespoke rules under Title V Chapter 5 MiCA become significant due to the number of clients only.[127] The provision of multiple services as a characteristic of multi-function CASPs would have been a better criterion for determining complexity.

In these cases, the regulatory coverage of side services, like transfer and custody, will dictate institutional resilience.[128] Here, the first battle line will lie between the *taking* of crypto-assets *into custody* on behalf of clients as an ancillary service to crypto-lending and crypto-staking, in contrast to the *transfer* of crypto-assets *to others* (clients and non-clients) in the interest of

[124] Zetzsche and others (n 9) 16.
[125] MiCA, arts 70 and 82, respectively.
[126] MiCA, art 72. In the context of conflicts of interest management, ESMA proposes remuneration policies, procedures and practices of the CASPs. cf ESMA74-449133380-425, 37–38, 123–135.
[127] ibid art 85.
[128] The French regulator, for instance, has clarified that crypto-lending and -staking may constitute, depending on the agreed Terms and Conditions, crypto-asset services or payment services and in each case the respective legislation should apply. cf AMF, 'Position—Recommendation AMF—Questions and answers relating to the regime for crypto-asset service providers' DOC-2020-07, 34.

clients; note that the transfer of crypto-assets is a regulated activity different from custody, to which Article 75 MiCA does not apply, yet MiCA contains few details about what it entails.[129]

Second, where custody is one, potentially initial, element of the service, a battle will inevitably be fought over the extent to which the consent of clients allows for treatment different than that provided for under Article 75 MiCA. However, where reuse hinges on the client's consent, what implicit limits exist with regard to the reuse? Is there any compensation to be offered to clients, as a precondition for a valid consent? What are the legal requirements for a valid consent to the reuse?

The answers to these questions will determine how effectively MiCA ensures institutional resilience.

Liability as a barrier to entry?

Another reason potentially undermining institutional resilience stems from the liability provisions of Article 75(8) MiCA: where serious and well-financed intermediaries must fear liability, they may decide to opt-out of the market.[130] Given that the crypto market is small, in relative terms, staying out of crypto is one of several options financial intermediaries have when deciding upon their crypto strategy. While entirely opting-out is unlikely in the long run, as intermediaries risk missing opportunities, a viable and already observed strategy is to establish lowly financed subsidiaries, while taking the main balance sheet outside the scope of liability rules.[131] To the extent that most large intermediaries refrain from crypto, and do not stand ready to entertain the existence of crypto-assets, the crypto market will remain small, in relative terms, and abstention from crypto, by and large, *remains* a viable option.

In this context, it is noteworthy that MiCA does not require a bank-like capitalization of custodians; hence, crypto custodians may be thinly capitalized entities under MiCA.[132] Where custodians put up the minimum capital only, it is foreseeable that the losses may easily accumulate to an amount where the custodian's capital is insufficient to compensate clients for losses. To this extent, liability is a double-edged sword. While potentially assisting crypto clients and investors, it may also shun the robust, well-governed and well-financed intermediaries the crypto markets so direly need.[133] In the absence of well-financed intermediaries that can compensate token-holders in the event of losses, liability rules are of little benefit in practice.

To demonstrate the importance of our argument, we need to take into account the use by custodians, and especially exchange-linked wallet providers, of 'hot storage' of private keys of multiple clients. These storage tools are constantly connected to the internet, to ensure time and cost

[129] MiCA does not provide any substantive provisions besides MiCA, art 82. The focus is on definitions. See MiCA, art 3(1)(26) ('providing transfer services for crypto-assets on behalf of clients' means providing services of transfer, on behalf of a natural or legal person, of crypto-assets from one distributed ledger address or account to another); MiCA rec 93 ('Such transfer service should not include the validators, nodes or miners that might be part of confirming a transaction and updating the state of the underlying distributed ledger. Many crypto-asset service providers also offer some kind of transfer service for crypto-assets as part of, for example, the service of providing custody and administration of crypto-assets on behalf of clients, exchange of crypto-assets for funds or other crypto-assets, or execution of orders for crypto-assets on behalf of clients. Depending on the precise features of the services associated to the transfer of e-money tokens, such services could fall under the definition of payment services in Directive (EU) 2015/2366. In such cases, those transfers should be provided by an entity authorised to provide such payment services in accordance with that Directive.').

[130] cf Zetzsche, Annunziata and Sinnig (n 52), 37–38.

[131] In similar vein, see on the criticism of the 2022 US SEC staff accounting bulletin (SAB) on accounting for custodied crypto-assets because the proposed inclusion of the custodied crypto-assets on the balance sheet of banks acts as a major deterrent for banks to engage in any crypto custody services. cf Celisa Morin and Will Atherton, 'A SAB state of affairs: SEC guidance deters U.S. financial institutions from providing crypto-asset custody' (ReedSmith, 25 July 2023) <https://www.reedsmith.com/en/perspectives/2023/07/a-sab-state-sec-guidance-us-financial-institutions-crypto-asset-custody> accessed 25 April 2024 and Bill Flook, 'Resolution Nixing SEC Crypto Accounting Guidance Clears House Committee' (*Thomson Reuters*, 1 March 2024) <https://tax.thomsonreuters.com/news/resolution-nixing-sec-crypto-accounting-guidance-clears-house-committee/> accessed 25 April 2024.

[132] MiCA, art 67 and Annex IV require that custodians have a regulatory capital of EUR 125,000 plus a quarter of the fixed overhead costs of the preceding year. For instance, where there fixed overhead costs amount to EUR 3 million (which we estimate is a reasonable amount for a fairly large CASP with 20 to 30 employees) the overall regulatory capital available will sum up to EUR 875,000. In the absence of additional banking business, these custodians will hardly be able to cover large losses of token holders.

[133] We also see some spill-over effects: where custodians depend on custodial networks the prevalence of many small and thinly capitalized crypto custodians paired with liability rules will mute the readiness of the well-financed (traditional or DeFi-only) custodians to enter the market.

efficiency.[134] These hot wallets have been referred to as 'an attractive 'honey pot' for hackers' and are more vulnerable than the cold (offline) key storage methods.[135]

Outsourcing?

Another factor that could undermine institutional resilience results from the outsourcing rules under Article 73 MiCA. As CASP rules apply to EU entities only[136] even though many crypto intermediaries reside outside of the EU,[137] outsourcing to non-EU entities potentially weakens the institutional resilience provided by MiCA.[138] Indeed, Article 73 provides that the CASP engaging in the outsourcing shall remain fully responsible for discharging all of their obligations pursuant to' Title V MiCA. The outsourcing does not: (1) result in the delegation of their responsibility; (2) alter the relationship between them and their clients, nor their obligations towards their clients; and (3) alter the conditions for their authorization. However, none of the above obligations concern directly the third-party sub-custodian who actually controls the assets/keys, since the latter (third party) is not subject to MiCA as long as it is not located within the EU/EEA. While the EU CASP, due to low levels of mandatory regulatory capital under MiCA,[139] will be unable to cover all or most of the holders' losses even if it is held liable for violating its duties (such as the prohibition to alter relationships and obligations) when outsourcing to non-EU crypto service providers.

Furthermore, even when MiCA applies, that is, in the case of EU/EEA-based third-party sub-custodians, several issues related to the outsourcing of the safekeeping duties are not sufficiently addressed by MiCA. For instance, in TradFi, in cases of outsourcing of the safekeeping function, it is established that the client's assets shall be segregated from the custodian's proprietary assets, from the third-party's proprietary assets, as well as from assets belonging to other clients of the third party.[140] We do not find the same to be the case in MiCA. This is not fundamentally changed by the fact that the CASP needs to hold certain records on, and store all communication with, the sub-custodian[141] and make provision for the sub-custodian's insolvency in its business continuity plan.[142] While MiCA requires segregation of the client's assets from the custodian's proprietary assets,[143] it lacks bespoke rules on outsourcing crypto custody similar to EU investment fund law mentioned herein.

In addition, with regard to asset segregation by the sub-custodian, MiCA is ambiguous as to the following: First, whether it requires on-chain segregation (ie with separate blockchain addresses), or whether off-chain suffices (ie probably by means of a segregated record-keeping system).[144] Second, whether the custodian can rely on the records of the sub-custodian, who

[134] Zetzsche and others (n 9) 46–47.
[135] cf Bains and others (n 33) 22.
[136] MiCA, art 2(1).
[137] For a geographical breakdown of the prominent crypto custodians cf Zetzsche and Nikolakopoulou (n 3).
[138] Idem for the possibility of non-protection of the clients' assets in case of insolvency when the safekeeping has been delegated to third parties. Several contractual clauses in the researched Terms and Conditions have mentioned the fact that the third-parties (sub-)custodians reside in third-country jurisdictions where the local legislation applies as a factor that undermines the protection of the custodied assets in case of insolvency, indicating possible deterioration of the clients' position when outsourcing to several jurisdictions lacking the EEA's legal safeguards takes place.
[139] art 67 and Annex IV MiCA sets the mandatory capital of CASPs providing crypto custody at EUR 125,000 plus a quarter of the annual fixed costs.
[140] AIFMD, art 11(d), UCITS, art 22a(3), Commission Delegated Regulation (EU) 2018/1618 of 12 July 2018 amending Delegated Regulation (EU) No 231/2013 as regards safe-keeping duties of depositaries [2018] OJ L271/1, rec 2, Commission Delegated Directive (EU) 2017/593 of 7 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to safeguarding of financial instruments and funds belonging to clients, product governance obligations and the rules applicable to the provision or reception of fees, commissions or any monetary or non-monetary benefits [2016] OJ L87/500, art 2(1)(d).
[141] According to ESMA's consultation paper, the CASP shall keep records from the third-party CASP evidencing the positions of the clients and shall keep records of the communications evidencing that the CASP complied with MiCA, art 75(9) subpara 2, when the CASP uses other CASPs for safekeeping or controlling the crypto-assets or the means of access. cf ESMA75-453128700-438, 171–172.
[142] According to ESMA, the business continuity plan of the CASP shall take into account the potential impact of the insolvency or other failures of third-party service providers, death of a key person and, where relevant, political risks in the service provider's jurisdiction. cf ESMA74-449133380-425, 86.
[143] MiCA, art 75(7).
[144] For an overview of the asset segregation and commingling practices on-chain as well as off-chain, cf Zetzsche and Nikolakopoulou (n 3).

actually controls the assets/keys, in order to fulfil its own recordkeeping obligation.[145] Third, MiCA does not foresee safeguards for the sub-custodian's insolvency—and thus does not address a crypto-industry-wide problem: the fact that a CASP holds information on the sub-custodian's account[146] does not assure that the assets are segregated in the sub-custodian's insolvency, nor that the CASP has legal standing in legal and insolvency proceedings relating to the sub-custodian's assets. Since the latter point is one of asset resilience, we further address it in that context in the next section.

Asset resilience

While, despite minor deficiencies, MiCA clearly strengthens institutional resilience, we are less convinced that MiCA provides the necessary framework with respect to asset resilience (ie a framework that ensures the existence of the assets when there are operating changes on the distributed ledger (eg forks, airdrops), when the token-issuer or DeFi application experience difficulties, or finally, when the crypto custodian, or third-parties such as the custodian's other clients, are bankrupt or close to bankruptcy).

While MiCA addresses the distress and malfunction of the token-issuer only in the context of ARTs and EMTs in its Titles III and IV, it does address the changes (eg airdrops, forks, or similar events) on the underlying distributed ledger for all types of crypto-assets in two ways: MiCA provides for the 'substitution rule' of Article 75(4)[147] and therefore the custodian's obligation to facilitate the exercise of the clients' rights resulting from such events, in conjunction with the custodian's fiduciary duty and its disclosure obligations vis-à-vis the client.[148]

Finally, to deal with the case that the custodian, sub-custodians or third parties find themselves in difficulties, malfunctions or misconducts affecting the clients' crypto-assets, Articles 70 and 75 MiCA provide *inter alia* for: the custodian's obligation to safekeep the assets and rights according to a proper custody policy, especially in the event of the custodian's insolvency; the obligation to keep detailed records for each client; the obligation to segregate clients' assets from the custodian's own assets; the prohibition of asset reuse for the custodian's own account; and the liability of the latter for asset losses.

Analysing the effectiveness of asset resilience requires (a) some context regarding the private law on crypto-assets followed by (b) a short examination of the potential of financial regulation to ensure asset resilience. On that basis, we summarize our concerns on asset resilience after the adoption of MiCA.

Roots in the EU legislative process: private law basis in doubt

Due to the nature of DLT, the existence of the asset relies on the recognition by and the functioning of other nodes. In this multi-party context, the effectiveness of legal protection depends on the nature and extent of the rights that the client has over the crypto-assets held in custody, under the applicable private law.

Where MiCA requires crypto custodians to safeguard the ownership rights of their clients in the event of the custodian's insolvency[149] and where it provides for a solid burial plan for their activities,[150] it could be argued that it substitutes for the lack of harmonized property and insolvency laws for crypto-assets by imposing an 'obligation of result', leaving Member States wide discretion on the means of achieving these results. However, the obligation to safeguard the ownership rights is undermined when it is not certain, from a private law perspective, that the clients actually *have* ownership rights over the custodied crypto-assets and whether their nature is contractual or proprietary;[151] after all the holders' enforcement position is uncertain and a risk/costs consideration will prevent them to take legal action. In turn, public enforcement bodies (including courts) have little to enforce. Given the widespread legal uncertainties regarding

[145] For issues stemming from that reliance with regard to investment fund depositaries, see Isabelle Riassetto, 'La ségrégation des instruments financiers et le dépositaire d'OPC' (2018) 5 Revue de Droit Bancaire et Financier 25.
[146] cf (n 140).
[147] cf 'Custody contract, policy and procedures under Article 75 MiCA' section.
[148] cf MiCA, arts 66, 72, 75(2), (7) and (5).
[149] MiCA, arts 70(1) and 75(7).
[150] MiCA, art 74.
[151] On the clients' entitlements to crypto-assets according to the Terms and Conditions of the prominent crypto custodians. cf Zetzsche and Nikolakopoulou (n 3).

ownership and property rights in digital assets,[152] it will be interesting to see how CASPs acting for clients in several jurisdictions meet the above-stated requirements on a case-by-case basis. In particular, the lack of a harmonized legal framework and overall ambiguity encourages the existing custodians to provide in their terms and conditions that the client has only an unsecured contractual claim regarding the entrusted crypto-assets, and/or provide for title transfer arrangements.[153]

Financial regulation as a mitigant of underdeveloped private law

To some extent, the product regulation for ARTs and EMTs in Titles III and IV MiCA substitutes for this private law gap with respect to crypto. Issuers of ARTs and EMTs are subject to licensing, custodial and prudential requirements—including redemption and recovery plans—for ART[154] and EMT[155] issuers. On top of that, issuers are required to wind down their activities when business continuity is at risk.[156] This ensures asset resilience even where private law is largely absent. Necessarily, the setup and operational effectiveness of these burial plans require significant resources on the side of the issuer and the supervisory agency. This explains why Title II MiCA on other crypto-assets refrains from similar rules—and therefore why token-holders of other assets remain largely unprotected.

Asset protection in the case of failures and malfunctions of the custodian or third party

Finally, while MiCA defines the rights and obligations of the custodian and their clients in the event of the custodian's own failures or malfunctions, these rules provide little asset protection vis-à-vis third parties, such as the custodian's other clients, counterparties and malicious actors.

Asset safekeeping and segregation

As for the protection of assets in the case of malpractices or failures of the custodian's other clients, MiCA only clarifies the obligation to segregate clients' assets from the custodian's own assets 'operationally' (ie on the DLT using separate blockchain addresses)[157] and 'legally'[158] (ie probably by means of a segregated record-keeping system).[159] This counters the custodian's practice of using, for time and cost reasons, common blockchain wallet addresses commingling the assets of multiple clients with their own proprietary assets. However, MiCA does not require segregation on a client-by-client basis on the DLT. This allows for the use of omnibus wallets (ie common blockchain addresses to which multiple clients' crypto-assets are pooled). Here, the protection of crypto clients lacks the rigidity of TradFi,[160] where the use of omnibus wallets is permitted when the safekeeping is delegated and under strict segregation requirements. In turn, crypto clients remain exposed not only to the elevated risk of cyber-attacks,[161] but also to risks stemming from the insolvency of the *other* clients of the custodian, whose assets are pooled

[152] cf Woxholth and others (n 27) 7–19; Ignacio Tirado and Louise Gullifer, 'Proprietary rights and digital assets: a "modest proposal" from a Transnational Law perspective' (2024) 87(2) Law and Contemporary Problems, forthcoming. For an argument that streamlining of crypto insolvency laws is a priority, cf Zetzsche and others (n 9) 91.

[153] The obligation of the custodian to protect the ownership rights of the client may be circumvented if the clients have no ownership over the assets, while the custodian or any third party appears as the owner. cf Foris DAX Limited, 'Exchange Terms and Conditions' <https://crypto.com/exchange/document/tnc> accessed 25 April 2024, as follows: 'Subject to clause 5.4 [Custodial arrangements for jurisdictions and clients for which certain special safekeeping rules apply] … you grant Crypto.com and/or its Affiliates (as applicable) the rights to all On-Exchange Assets … b) your rights in relation to any On-Exchange Assets are limited to a contractual obligation for Crypto.com to provide an equivalent amount and type of On-Exchange Assets.'. BitMEX, 'BitMEX HK Risk Disclosure' <https://www.bitmex.com/bitmex-hk-risk-disclosure> accessed 25 April 2024, as follows: '… you do not have any proprietary claim in respect of any digital assets transferred to the Company or any Account balance.'

[154] MiCA, title III chs 2, 3 and 6.

[155] MiCA, title IV ch 1.

[156] See MiCA, title III ch 6 and art 55. For a detailed analysis, see Zetzsche and Woxholth (n 45) ch 6 (forthcoming).

[157] According to proposals by ESMA, the CASP needs to ensure that the clients have separate wallet addresses from the CASP's own wallet address. However, with regard to the segregation of the clients' assets, the CASP only needs to disclose how they segregate clients' crypto-assets. cf ESMA74-449133380-425, 60, 91.

[158] MiCA, arts 70(1), 75(2), (4), (5) and ESMA (in its initial proposal) require CASPs to keep records that the CASPs can distinguish crypto-assets held for one client from crypto-assets held for other clients and from their own assets. cf ESMA75-453128700-438, 161–62, 170–72.

[159] For an overview of the crypto-asset segregation and commingling practices on-chain as well as off-chain, cf Zetzsche and Nikolakopoulou (n 3).

[160] cf AIFMD art 21(8) and (11), Commission Delegated Regulation 2018/1618, rec 2, UCITSD, arts 22(5) and 22a, Commission Delegated Directive (EU) 2017/593, art 2.

[161] Malicious actors usually attack omnibus wallets to take advantage of multiple clients' assets.

inside the same omnibus wallet.[162] Note that token-holders have no information about these other clients, and thus have no means of protecting themselves by pulling out early, or issuing orders of injunction. This information asymmetry adds to legal uncertainties regarding the nature of the token-holders' rights in the crypto omnibus account.

As for the protection of assets in the case of malpractices or failures of any sub-custodian, MiCA does not provide for granular provisions addressing the segregation obligation that the sub-custodian shall assume and the protection of the custodied assets in case of insolvency of the sub-custodian (see 'Restrictions on regulated activities' section).

Reuse and title transfer arrangements

Furthermore, as for the protection of assets in the case of malpractices or failures of the custodian or third parties such as the custodian's counterparties, Article 70(1) MiCA prohibits the reuse of clients' assets for the custodian's own account and Recital 83 MiCA requires that the clients' assets shall be unencumbered.

However, the absolute prohibition and the narrow wording of these provisions leave room for circumventions. In light of common practices that combine various types of asset reuse[163] with the lack of specifications regarding an intermediary's function as custodian, liquidity provider or counterparty,[164] we find that MiCA's rules lack granularity on the legal requirements for asset reuse. Meanwhile, TradFi sets an appropriate level of desirable protection, with one of the main safeguards being that title transfer arrangements are permitted only when the custodian discloses *ex ante* all relevant information and risks to the client and obtains their express prior consent.[165]

Oversight control and representation against third parties

Finally, the custodian is not mandated to represent their clients' interests vis-à-vis any third parties (for instance, by performing oversight or monitoring of other CASPs' conduct), nor do they have express legal standing to represent the clients and their interests in legal proceedings vis-à-vis third parties under MiCA. While the mandate to represent clients could be derived from the custodian's fiduciary duty, without standing any legal action is laden with risks.

While one could argue that standing would follow from the custodian's registration on behalf of their clients on the distributed ledger, this would be at odds with models of true segregation on the ledger[166] (cf 'Asset safekeeping and segregation' section); and even where standing is given, the uncertainty in crypto private law renders the taking of legal action on behalf of clients risky. Here, MiCA lacks the clarity and simplicity of TradFi regulation: depositaries of investment funds do represent their clients' interests by exercising oversight,[167] and also have, under most laws, legal standing in proceedings as ancillary competence to custody, where claims against the fund manager are concerned.[168] Given that the financial regulation provisions on investment funds have long substituted for uncertainties surrounding the private law of collective investment schemes in a cross-border context,[169] TradFi depositary regulation provides a useful blueprint for crypto custody, which MiCA neglected to implement.

[162] On omnibus accounts transparency requirements, see Recommendation 14 in International Organization of Securities Commissions (n 34).

[163] For instance, many custodians claim in their Terms and Conditions that they don't reuse the clients' assets for their own account but merely all of the custodians have a security interest, lien, right to set-off or title transfer arrangements in place to cover any (present or future) outstanding claims they have against their clients, which seems to be at odds with the absolute obligation to keep the clients' assets unencumbered as per MiCA Recital 83. For further analysis, cf Zetzsche and Nikolakopoulou (n 3).

[164] Arner and others (n 9) 24–25.

[165] Eg. MiFID, art 16(8) to (10), Commission Delegated Directive (EU) 2017/593, arts 5 and 6. On title transfer arrangements regarding crypto-assets cf International Organization of Securities Commissions (n 34); Financial Stability Board (n 32).

[166] For instance, when each client's assets have their own blockchain wallet address.

[167] UCITSD, art 22(3) and (4) and AIFMD, art 21(7) and (9).

[168] Dirk Zetzsche, 'Aktivlegitimation gemäß §§ 78, 89 KAGB im Investment-Drei- und -Viereck', in Matthias Casper, Lars Klöhn, Wulf-Henning Roth and Christian Schmies (eds), *Festschrift für Johannes Köndgen* (RWS 2016) 677–700.

[169] See Dirk Zetzsche, 'Das grenzüberschreitende Investmentdreieck', in Dirk Zetzsche and Matthias Lehmann (eds), *Grenzüberschreitende Finanzdienstleistungen* (Mohr Siebeck 2018).

5. Conclusion

MiCA's rules on custody are novel and provide a benchmark for non-EU jurisdictions seeking to regulate crypto.

In this regard, MiCA's focus is on what we have called herein 'institutional resilience', ensuring that the custodian is soundly organized and governed and must not reuse clients' assets on their own accounts. Under MiCA's CASP rules, all crypto custodians are fiduciaries, and subject to governance, conflicts of interest, asset segregation and operational risk requirements. The provisions on the custodian's liability also heighten the custodian's propensity to safeguard clients' assets.

At the same time, MiCA lacks strength on 'asset resilience' (ie providing safeguards for cases where the custodian, third parties, the token-issuer, or DeFi application, as the case may be, encounter difficulties). This deficiency is partly due to the nature of DLT, where the existence of the asset relies on the recognition by and the functioning of other nodes, and partly due to the fact that MiCA does not regulate private law, and the insolvency proceedings regarding crypto-assets in particular. To some extent, the product regulations for ARTs and EMTs compensate for this gap, but holders of other crypto-assets are left unprotected. In this regard, MiCA, in terms of protection, trails behind TradFi regulation where depositaries play a much stronger role in ensuring asset resilience, through express powers that allow for oversight of other service providers, and representation of clients' interests in legal proceedings against third parties.

Capital Markets Law Journal, 2024, 19, 207–229
https://doi.org/10.1093/cmlj/kmae010
Article