Safe Bank 2(99) 2025

DOI: 10.26354/bb.14.2.99.2025

Szymon Ciach*
ORCID: 0000-0002-2240-7640
szymon.ciach@osborneclarke.com

Kamil Prokopowicz**
ORCID: 0000-0002-1519-2733
kamil.prokopowicz@osborneclarke.com

Selected issues related to crypto-asset custody services in light of MiCAR

Abstract

One of the crypto-assets services that has been regulated by the European Union Regulation 2023/1114 on markets in crypto-assets (MiCAR) is the service of providing custody and administration of crypto-assets on behalf of clients. The aim of the article is to discuss the key issues related to the provision of this service, with particular emphasis on the regulatory requirements that the EU legislator has imposed on crypto-asset service providers (CASPs) to ensure a high level of client protection, as well as the stability and integrity of crypto-asset markets. According to the authors, despite the shortcomings of the EU solutions adopted in MiCAR, the regulatory direction taken by the EU legislator should be considered appropriate. The final assessment of the achievement of the objectives behind the establishment of MiCAR regulations in this area will, however, depend on future market trends, supervisory activities, and the actions of national legislative bodies of EU member states.

Keywords: crypto-asset custody, blockchain, DLT, CASP, MiCAR

JEL codes: K22, K23, K24

* Szymon Ciach – attorney-at-law, Counsel at Osborne Clarke law firm.
** Kamil Prokopowicz – trainee attorney-at-law, Associate at Osborne Clarke law firm.

Introduction

Introduction to MiCAR. One of the two main subjects of the Regulation of the European Union (hereinafter: "**EU**") 2023/1114 of 31 May 2023 on markets in crypto-assets (hereinafter: "**MiCAR**")[1], in addition to the requirements for the offer to the public and admission to trading on a trading platform of crypto-assets, are the requirements for crypto-asset service providers (hereinafter: "**CASPs**").

The requirements for CASPs are contained in particular in the provisions of Title V of MiCAR, entitled: *authorisation and operating conditions for crypto-asset service providers*. In Article 3(1)(16) of MiCAR, the EU legislator defined 'crypto-asset service' by citing a closed catalogue of such services. In the first instance (in Article 3(1)(16)(a) of MiCAR), it pointed in this regard to *providing custody and administration of crypto-assets on behalf of clients*. The counterparts of this service within the area of traditional finance (the so-called TradFi) are, for example, safekeeping and administration of financial instruments for the account of clients, which is an ancillary service under MiFID[2], and safekeeping and administration in relation to units of collective investment undertakings, which is a non-core service under UCITSD[3] and AIFMD[4].

Prior regulation. In seeking the origins of the distinction and regulation in EU law of the crypto-assets custody services, it should be noted that MiCAR is historically the first comprehensive regulation on the provision of crypto-asset services enacted at EU level. Prior to 30 December 2024, i.e., the date of application of MiCAR's provisions on the requirements for CASPs, the provision of crypto-asset services was generally regulated only by selected EU Member State legislators. Prior to 30 December 2024, the EU legislature only residually regulated the provision of crypto-asset services (and exclusively virtual currencies) through AML/CFT legislation. Indeed, by 10 January 2020, EU Member States had to implement into their national legal orders the provisions of the so-called AML V Directive[5] enacted on 30 May 2018, which included in the catalogue of so-called obliged entities:

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, OJ L 150, 9.6.2023, pp. 40–205.

2 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, OJ L 173, 12.6.2014, pp. 349–496.

3 Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS), OJ L 302, 17.11.2009, pp. 32–96.

4 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, OJ L 174, 1.7.2011, pp. 1–73.

5 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, pp. 43–74.

(1) providers engaged in exchange services between virtual currencies and fiat currencies, and (2) custodian wallet providers.

Service characteristics. The placement by the EU legislator of crypto-assets custody and administration services at the forefront of the catalogue of crypto-asset services set out in Article 3(1)(16) of MiCAR appears to be not coincidental. In market practice, the provision of such a service essentially involves ensuring that crypto-assets held on behalf of a client will be available to that client, including not becoming subject to theft or being lost for any other reason. Failure to fulfil this assurance will most often result in significant harm to the interests of the user, given that the execution of a transaction using a means of access to a crypto-asset is difficult to trace and is usually irreversible, just as the loss of that such means is also irreversible. A user entrusting a provider with control of a crypto-asset must therefore act on the basis of a strong bond of trust linking them to the provider, the breach of which may in turn undermine trust in the crypto-asset market as a whole. In the past, such undermining of trust has materialised on a large scale, in the case of the collapse of exchanges such as FTX, which had active control over their clients' crypto-assets (Arner, Zetzsche, Buckley, Kirkwood 2023).

Objectives of the article. The purpose of this paper is to descrbie MiCAR's provisions on the service of providing custody and administration of crypto-assets on behalf of clients, pointing out potential problems of interpretation and weaknesses of this Regulation from the point of view of fulfilling the objective of protecting the user's economic interests. Further considerations are carried out in relation to three specific issues, which include: (1) the scope of crypto-assets custody and administration services, and (2) the public and (3) private law requirements for their provision set out in MiCAR. The attribution of specific activities to the service in question is an important practical issue, on which depends the identification of the scope of entities obliged to comply with the selected MiCAR requirements, as well as the scope of permissible public law supervision by the competent supervisory authorities. Nonetheless, it is the effectiveness of the identified public and private law requirements that determines whether the regulation envisaged in MiCAR will in fact fulfil its objectives, protecting the user from the surrounding risks and thereby enhancing the security and stability of the crypto-asset markets.

1. Scope of the service of providing custody and administration of crypto-assets on behalf of clients

Definition of service. According to Article 3(1)(17) of MiCAR, 'providing 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*. According to the aforementioned definition, the service will therefore be provided where a CASP exercises (1) safekeeping or (2) controlling over (a) a crypto-asset or (b) the means

of access to a crypto-asset. In turn, in recital 83 of MiCAR, the EU legislator specified that the service in question may include *the holding of crypto-assets belonging to clients or the means of access to such crypto-assets.*

Definition of crypto-asset. In order to define the scope of crypto-assets custody and administration services, the definition of 'crypto-asset' in Article 3(1)(5) of MiCAR is relevant. According to this provision, '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* (hereinafter: "**DLT**") *or similar technology.*

The definition of 'crypto-asset' consists of two essential elements, i.e. an indication of the economic-legal nature of a crypto-asset, as a digital record reflecting a value or right, and an indication of its technological nature, narrowing the concept to digital records existing in DLT or similar technology. In this context, the reference to the *representation of value*, should be understood as the ability of an asset to be traded as a result of the existence of a demand for such an asset (Völkel 2023). This makes it possible to include within the scope of the definition of a crypto-asset those tokens whose value results strictly from the ratio of demand and supply, and whose issuance is not based on any assurances by the entity putting the tokens into circulation. An example of this type of crypto-asset is Bitcoin, the ownership of which does not involve any contractually defined obligations to its creators. On the other hand, tokens can be used as a vehicle for declarations of will, related, for example, to the granting of contractually defined rights to each token holder. Examples of this type of crypto-assets are utility tokens, the possession of which usually entitles the holder to use the functionality of digital services[6] . The provision of crypto-assets custody and administration services can refer to both the first and the second type of crypto-asset described above, to which the definition in MiCAR refers.

In view of the broad definition of a 'crypto-asset', the provision of crypto-assets custody and administration services is therefore generally not dependent on the type of crypto-asset and may include all types of crypto-assets, including both asset-referenced tokens (hereinafter: "**ART**"), e-money tokens (hereinafter: "**EMT**"), as well as other crypto-assets, including utility tokens. It may also include both crypto-assets representing value (e.g. Bitcoin) and crypto-assets representing rights (e.g. ART tokens, EMT tokens or utility tokens). Furthermore, the provision of crypto-assets custody and administration services may also apply to crypto-assets that will not be subject to MiCAR's public offering provisions due to the fact that they do not have an identifiable issuer. Indeed, Recital 22 to MiCAR mentioning such crypto-assets does not exclude the application of MiCAR Title V to them. The MiCAR requirements regarding the crypto-assets custody will not apply to crypto-assets that are unique and not fungible with other crypto-assets (NFT – Non-Fungible Tokens). Such crypto-assets have been generally excluded from the scope of MiCAR (Article 2(3) of MiCAR). Furthermore, the discussed requirements will not apply

[6] See tokens representing virtual properties in the Decentraland platform.

to other groups of crypto-assets listed in Article 2(4) of MiCAR (including financial instruments, deposits, insurance products).

Data storage in the DLT. On the technological side, it should be noted that an essential feature of the DLT is the dispersion of data processing. This means that copies of the databases containing the digital records that constitute crypto-assets are duplicated and located in the memory of the computers (nodes) that make up the DLT. In the case of public, open and globally distributed DLT, it is not possible to identify one specific data storage entity or one specific location. The identification of such entities and locations is possible in the case of private, closed DLT, which is maintained by a specific group of entities. In both cases, however, this is irrelevant to the crypto-assets custody and administration services, which should not be related to the actual processing of data (storage) within the DLT, but to the economic aspect of such services, related to safekeeping or controlling of crypto-asset or the means of access to a crypto-asset.

Safekeeping or controlling. In market practice, crypto-assets custody and administration services follow two leading models, which are reflected in their definition. Firstly, safekeeping and controlling of crypto-assets can take place by transferring the crypto-asset from the holder's (or possibly another person's) distributed ledger address or account to the CASP's distributed ledger address or account. In such a situation, the crypto-asset comes under the direct authority of the CASP, which has complete control over it. The CASP's obligation to keep a register of positions corresponding to each client's rights to crypt-assets (see Article 75(2) of MiCAR) then takes on particular practical significance. This is because clients' crypto-assets may be held in one or more distributed ledger address or account controlled by the CASP, and the CASP must be able to determine the amount of its clients' positions. Secondly, safekeeping or controlling may be exercised over the means of access to the crypto-assets. In this case, the crypto-assets are not transferred, but remain tied to the holder's distributed ledger address or account. In turn, the holder provides the CASP with a means of access to crypto-assets, most often in the form of a cryptographic private key associated with an address or account on the DLT.

The EU legislator in the MiCAR legislation has not defined the difference between safekeeping and controlling. The common meaning of these terms indicates that safekeeping should be referred primarily to the holding of crypto-assets associated with their transfer to CASP or the holding of means of access to the crypto-assets themselves. This would be indicated in particular by the word 'safekeeping', which refers to protection against harm or loss ('Safekeeping', n.d.). The essence of control, on the other hand, is to have decision-making power, to have sovereignty over the crypto-asset (e.g. transferring, exercising associated powers).

Concept of control. For comparative purposes, it may be pointed out that, according to *the Principles of Digital Assets and Private Law* (hereinafter: "**PDAPL**") adopted by the International Institute for the Unification of Private Law (UNIDROIT 2023), a custodian maintains a crypto-asset for a client if that custodian has control over

the crypto-asset or entrusts such a control to a sub-custodian (UNIDROIT 2023, 68–69). Unlike MiCAR, the PDAPL defines the concept of 'control' by assuming that it is exercised when one has the ability to obtain substantially all the benefits from the crypto-asset or to prevent others from obtaining such benefits, and when one has the exclusive ability to transfer such ability to another person (UNIDROIT 2023, 51–52). In this context, it has been noted that the notion of 'control' exercised over a crypto-asset is equivalent to the notion of 'possession' of a movable asset operating in private law. Indeed, both concepts refer to an authority of a factual nature that can be exercised separately from the fact of possession of proprietary rights (UNIDROIT 52–54). There is no fundamental obstacle to an identical understanding of 'control' as referred to in Article 3(1)(17) of MiCAR.

Scope of control. As rightly noted in recital 83 of MiCAR, control over a crypto-asset may take on a partial or full nature, depending on whether the CASP's entry into it constitutes an impediment to the parallel exercise of control by the client. The transfer of a crypto-asset to an address or account on a distributed ledger, controlled solely by CASP, will involve a complete transfer of control. The provision of the means of access to a crypto-asset to the CASP does not, however, preclude the CASP's client from retaining access to the crypto-asset, for which it is sufficient to retain the means of access on any other physical or digital medium. In such a situation, only partial control on the part of the CASP will occur.

Non-custodial wallets. Recital 83 of MiCAR *in fine* makes it clear that *hardware or software providers of non-custodial wallets should not fall within the scope of this Regulation.* Non-custodial (or self-custodial) wallets primarily take the form of hardware (e.g., a flash drive preloaded with software[7]) or software (e.g., in the form of a mobile application, a web browser add-on[8]) that facilitate the management of means of access to crypto-assets. Wallets of this type allow interaction with decentralised finance protocols, either through their own interfaces or by connecting the wallet to other applications. Their key feature is that, unlike custodial wallets, they give users exclusive control over their means of access to crypto-assets, and it is users' responsibility to secure these means. Providers of this type of wallet do not take possession of either the crypto-assets themselves through their transfer or the means of access to the crypto-assets. Loss of the means of access by the user usually results in permanent loss of access to a crypto-assets (European Banking Authority, 2025, p. 13). Such a situation could occur, for example, if a flash drive storing private keys is destroyed.

The safest type of non-custodial wallets are considered to be hardware wallets, which are cold wallets. Unlike software wallets, which are most often hot wallets, they are not accessible online, making them more resistant to external cyber-attacks. An example of using a hardware wallet involves connecting it to an external device used for preparing transactions, activating it, and entering a password

7 E.g. a product of the Ledger or Trezor brand.
8 E.g. a product from the Metamask brand.

to secure access to the wallet. Since these types of wallets do not have an active network connection, signing transactions must always be preceded by physical access to them. They also do not operate autonomously, meaning that conducting transactions requires cooperation with another device preparing the transaction. Due to all the above reasons, hardware wallets are most commonly used for storing larger amounts of crypto-assets over a long-term horizon.

Other non-custodial services. The considerations set out above do not provide clarification with regard to whether the provision of crypto-assets custody and administration services will occur in cases where CASP does not exercise safekeeping or controlling of the crypto-asset or the means of access to the crypto-asset, but only performs other activities that could possibly fall within the notion of 'administration' of crypto-assets not further defined in MiCAR. Indeed, the exemption described above, which is included in recital 83 of MiCAR *in fine,* refers only to non-custodian wallets and not to other non-custodian services. In our view, there is no strong reason to believe that any other ancillary services unrelated to the exercise of control over crypto-assets, while not constituting other regulated services within the meaning of MiCAR, should be subject to the Regulation. In particular, it should be noted that the provision of services related to non-custodial wallets may also involve certain risks to the user's crypto-asset (e.g. related to the failure of the device or software provided by the provider). The purpose of regulating of crypto-assets custody and administration services is therefore not for the legislator to mitigate all existing risks in the market, but only those of the most serious individual or systemic nature.

Administration involving safekeeping or controlling. The problem identified above will not be relevant for services that can be considered to consist of 'administration' of crypto-assets, and include safekeeping or controlling activities. Rather, such services should be subject to the requirements of MiCAR and the public law supervision exercised to comply with the provisions of that regulation, as being closely related to the exercise of control over the crypto-asset. The literature indicates that such 'administration' services may include those related to the recognition of any direct benefits to the client arising from the possession of crypto-assets. This could refer, in particular, to airdrops, deciding on forks proposals (i.e. on splitting blockchain history into separate paths), voting on smart contracts or staking protocols (Ossio, Nixon, Yates 2023, p. 14). As a caveat, however, the indicated enumeration is controversial insofar as, in the case of discretionary decision-making activities by CASPs in relation to controlled crypto-assets, it may be legitimate to qualify such activities also as a crypto-asset portfolio management service, i.e. a separate service regulated through MiCAR. However, an analysis of the indicated problem is beyond the scope of this paper.

To summarise the above considerations, in our view, a prerequisite for a particular service to qualify as a service for providing custody and administration of crypto-assets on behalf of clients is, at the very least, that the CASP takes control of the client's crypto-asset or means of accessing the client's crypto-asset. The purpose

of doing so is irrelevant, in that it may only include ensuring that the client's crypto-asset or means of access to the crypto-asset is not stolen or otherwise lost. Alternatively, the provision of the service in question may be operationally linked to the provision of other crypto-asset services, including in particular the provision of crypto-asset transfer services or crypto-asset portfolio management. In contrast, the provision of the service in question will not occur where control of a crypto-asset is exercised by the CASP on its own behalf and not that of its client. This may be the case, in particular, for contracts corresponding to loan agreements or collateral agreements concluded with the client, from which the CASP will directly benefit.

2. Public regulatory requirements

Regulation of the service. In general, the provision of custody and administration of crypto-assets services requires: (1) obtaining an authorisation under the procedure described in Articles 62–63 of MiCAR or alternatively (2) fulfilling the notification obligation under the procedure described in Article 60 of MiCAR. Only selected financial entities, which are credit institutions (Article 60(1) of MiCAR), central securities depositories (Article 60(2) MiCAR), investment firms (Article 60(3) of MiCAR) and electronic money institutions (Article 60(4) of MiCAR), are entitled to provide the service in question without authorisation, subject to the fulfillment of the notification obligation. However, in relation to electronic money institutions, Article 60(4) of MiCAR stipulates that the service in question can only be provided in relation to EMTs. *A contrario*, for the other three types of financial institutions, the service in question can be provided regardless of the type of crypto-asset in custody or administration.

TradFi equivalents. The aforementioned MiCAR provisions expressly stipulate that the equivalents of custody and administration of crypto-assets services are: (1) in relation to central securities depositories, the service of maintaining or operating securities accounts in relation to the settlement service, as referred to in Section B(3) of the Annex to the CSDR[9] , and (2) in relation to investment firms, safekeeping and administration of financial instruments for the account of clients, as referred to in Section B(1) of Annex I to MiFID. In our view, the consequence of these provisions is that the provision of custody and administration of crypto-assets services by the above-mentioned entities requires compliance not only with the requirements listed in MiCAR, but also with the requirements provided for indicated equivalent services in the CSDR and MiFID. In the case of CSDs, the requirements for the provision of banking-type ancillary services are described in Title IV of the CSDR and primarily include an authorisation requirement. Also,

[9] Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories, amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, OJ L 257, 28.8.2014, pp. 1–72.

according to Article 6 of MiFID, the authorisation granted to an investment firm should specify the scope of ancillary services.

Exception to authorisation/notification. Pursuant to Article 4(5) of MiCAR, the provision of custody and administration of crypto-assets services without obtaining authorisation or fulfilling the notification obligation is only possible if the public offering of the crypto-asset in question, other than ART and EMT, is subject to an exemption under Article 4(3) of MiCAR. However, this does not apply to such crypto-assets which have already been subject to a public offering or admitted to trading on a trading platform at any time in the past. Article 4(3) of MiCAR contains a catalogue of four cases exempting the obligation of a public offering, which include: offering a crypto-asset for free, offering a crypto-asset as a reward for distributed ledger maintenance or transaction validation, offering a utility token providing access to an existing good or service or offering crypto-assets recognised only in a limited network of merchants. By contrast, the exemption from authorisation or notification requirements does not apply in the case of providing this service in relation to crypto-assets other than ART and EMT, to which simplified public offerings apply in the cases set out in Article 4(2) of MiCAR.

Distinction of requirements. Providers wishing to provide custody and administration of crypto-assets services must comply with the MiCAR's (1) general requirements, i.e. applicable irrespective of the type of crypto-asset service provided, and (2) specific requirements, the fulfilment of which is linked solely to the fact of providing the service in question. The most important requirements of a specific nature are contained in Articles 70(1) and 75 of MiCAR. These requirements apply uniformly to both the financial entities listed in Article 60 of MiCAR and the other entities that must be authorised. This means that, in the intention of the EU legislator, the user of the service in question should be guaranteed the same minimum standard of protection, regardless of whether the CASP offering the service is at the same time another financial institution listed in MiCAR. However, given the fact that credit institutions are simultaneously subject to other prudential regulations of a specific nature, including operational risk management or resolution, it is these that will provide users with the highest standard of market protection. Indeed, compliance with these regulations will in practice also affect crypto activities.

Safeguard mechanisms. Pursuant to Article 70(1) of MiCAR, it is a fundamental obligation of CASPs to put in place mechanisms to safeguard ownership rights of clients in relation to crypto-assets, in particular in the event of CASP's insolvency, and to prevent the use of client's crypto-assets for the CASP's own account. Such mechanisms should be described in the custody policy referred to in Article 75(3) of MiCAR. In doing so, it should be recognised that, in accordance with Article 75(3) of MiCAR, the indicated policy should take into account all relevant risks, both external and internal, including, for example, the risks of fraud, cyber-security or negligence identified by the EU legislator. The measures adopted by the CASP to mitigate the risks identified may, in principle, be of a different nature and include primarily measures relating to the internal organisation of the CASP's activities as well as measures of a technological

nature. In light of Article 70(1) of MiCAR, the use of entrusted crypto-assets by CASP for its own benefit is absolutely excluded. The acquisition of financial instruments for investment purposes with such crypto-actives is therefore also prohibited, regardless of the degree of risk or liquidity of such instruments.

Risk mitigants. While the selection of appropriate mitigants should depend on the individual level of risks identified by the CASP, MiCAR provides for specific measures that CASPs providing custody and administration of crypto-assets on behalf of clients must consider in their operations. These measures boil down to the segregation of crypto-assets held on behalf of clients and the means to access them, from their own crypto-assets, at three levels, i.e. operational, technological and legal (Kokorin 2023, pp. 15–16). Operational segregation boils down to the obligation in Article 75(2) of MiCAR to keep open on behalf of each client a register of positions corresponding to each client's rights to crypto-assets. This register should record, as soon as possible, all operations arising from CASP client instructions. Technological segregation, on the other hand, boils down to the obligation to hold crypto-assets in separate accounts (Article 75(7), first subparagraph, of MiCAR). Finally, the CASP should also segregate crypto-assets legally, in accordance with the applicable law, so that creditors of the CASP cannot satisfy their claims from crypto-assets held on behalf of clients, in particular in the event of insolvency (Article 75(7), second subparagraph, of MiCAR).

Legal segregation of crypto-assets. In our view, the requirement in MiCAR to legally segregate client crypto-assets from CASP crypto-assets represents a flaw in MiCAR's regulation of custody and administration of crypto-assets services. Addressing the disposition of Article 75(7) of MiCAR exclusively to CASP raises doubts as to whether the obligation of EU Member States to adopt such public law provisions, in particular with regard to the applicable enforcement procedures, which would exclude the possibility of enforcement of claims against CASP from crypto-assets held on behalf of its clients, can be derived from this provision. Such doubts, on the other hand, do not exist in principle at least in the case of Article 10(1)(a) *in fine* of PSD2[10], which refers to the rules on the protection of users' funds applicable to payment service providers. In our view, if it is at all possible to enforce crypto-assets under the domestic law in a given country (particularly given the possibility of different arrangements in relation to the private law nature of such assets), such provisions should be provided for in the national order in accordance with MiCAR. Otherwise, CASP will not in fact have sufficient means to protect crypto-assets from claims by CASP creditors, and segregation at the legal level will only be illusory.

Outsourcing. The final relevant regulatory requirement for CASPs in relation to the provision of custody and administration of crypto-assets services is the specific outsourcing rules provided for in Article 75(9) of MiCAR. According to the indicated

[10] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, pp. 35–127.

provision, the use of other crypto-asset service providers for the service in question may only take place if such insourcers have CASP status obtained under the authorisation or notification procedure provided for in MiCAR. In our opinion, the indicated requirement only refers to situations where there is a transfer of safekeeping or controlling activities in regard to a crypto-asset or a mean of access to it to another entity, which in such a case may be referred to by the term 'sub-custodian'. Indeed, it does not seem reasonable to extend this requirement to providers of services or activities for the purpose of performing operational functions under Article 73 of MiCAR, given that Article of 75(9) MiCAR mentions crypto-asset service providers narrowly. In order to apply the enhanced outsourcing requirements, the activities performed by such an insourcer for CASPs must therefore qualify as the provision of custody and administration of crypto-assets services within the meaning adopted in MiCAR.

3. Private law requirements for the user agreement

General requirements. One of the overarching objectives of MiCAR is to increase the level of protection for holders of crypto-assets. Given the existing and heterogeneous market practice, a number of private law standards have been introduced into MiCAR. In particular, Article 66 of MiCAR, which applies to all CASPs, introduces rules requiring CASPs to act honestly, fairly and professionally in accordance with the best interests of their clients and prospective clients (paragraph 1), as well as an obligation to provide fair, clear and not misleading information to their clients (paragraph 2). According to Article 66(4) of MiCAR, each CASP is obliged to make its policies on prices, costs and charges publicly available by posting them in a prominent place on its website. Consequently, it must be assumed that contracts for the custody and administration of crypto-assets services will, at least in part of their provisions, be adhesion contracts.

The private-law nature of crypto-assets. The question of the private law qualification of crypto-assets is still pending in MiCAR and its detailed discussion is beyond the scope of this paper. It is worth noting, however, that under Article 70(1) of MiCAR, an obligation has been established for CASPs that hold crypto-assets or means of access to such crypto-assets on behalf of clients to put in place appropriate mechanisms to, inter alia, secure 'ownership rights of clients'. However, in light of this provision, as well as the regulation as a whole, it appears that the EU legislator avoids introducing an explicit proposal as to the resolution of the private law status of crypto-assets. The matter therefore needs to be resolved at the level of national law.

Similarly, it should remain within the purview of national legislative and judicial bodies to determine whether and to what extent national regulations concerning the bailment agreement should apply to services providing the custody and administration of crypto-assets on behalf of clients, insofar as they are not inconsistent with MiCAR provisions. In Polish private law (Article 835 and subsequent articles of the Act of 23 April 1964, Civil Code), the bailment agreement of movable items, although it

also assumes the custodian's obligation to safekeeping the movable item, does not apply to items designated as to their kind that have not been individualised when being handed over[11]. The characteristic of tokens other than NFTs, however, is that they are fully fungible and not further individualised. Despite this, the prohibition on disposing of the transferred crypto-assets brings the contract for the custody of crypto-assets closer to a classic bailment agreement, rather than the irregular deposit contract inherent in things designated as to their kind.

Entering into a contract with the user. Further specific private law standards for provision of custody and administration of crypto-assets services can be found in Article of 75 MiCAR, which is exclusively dedicated to CASPs providing such a service. According to Article 75(1) of MiCAR, the CASP is obliged to enter into a contract with the client, which implies at least the obligation to make the content of the contract available for acceptance by the client. This provision also establishes minimum requirements for the content of the contract – the CASP is obliged to indicate, among other things, its identity, the client's authentication system, fees and applicable law.

Creation or modification of client rights. A regulation specific to the crypto-assets market is Article 75(4) of MiCAR, which establishes the obligation of CASPs towards the facilitation of the exercise of rights attached to to crypto-assets. Any event that may create or modify client rights is to be immediately recorded in the client position register. By contrast, the next paragraph of this provision regulates so-called forks[12] of distributed ledger and similar events at the DLT level. The assumption is made that the client is entitled to any newly created crypto-assets or rights based on and within the scope of the client's position at the time of the event. This is a dispositive provision, meaning that the parties may contractually exclude such client entitlement.

CASP's liability. Article 75(8) of MiCAR regulates the liability of CASPs to their clients. CASPs that provide custody and administration of crypto-assets services are liable to their clients for the loss of crypto-assets or means of access to crypto-assets as a result of an incident attributable to them. The EU legislator has clarified that incidents not attributable to the CASP include any event for which the CASP demonstrates that it occurred independently of the provision of the service in question or independently of the CASP's operations, such as a problem inherent in the operation of a distributed ledger over which the CASP has no control. This has not been explicitly prejudged, while this regulation of liability seems to suggest a reversed burden of proof on the CASP. Indeed, in a situation of loss of crypto-assets or loss of means of access to crypto-assets held and administered by CASP, the client

[11] Therefore, the bailment agreement does not apply to money that has not been placed in an envelope or money box (Gudowski 2017, p. 448).

[12] The word 'fork' refers to the 'forking' of a DLT, for example, a decision by part of the community maintaining the DLT to upload an update and continue recording transactions in a new version of the registry, while the old version is still maintained by another part of the community. Included in MiCAR as "changes to the underlying crypto-asset distributed registry technologies or any other event that may give rise to or alter client rights."

may have limited evidentiary options. In addition, CASP's liability is limited to the market value of the lost crypto-assets at the time the loss occurred.

While the MiCAR does not define the term 'incident' as mentioned above, some clarification is provided here by recital 83 of MiCAR, indicating that CASPs should be liable for all losses resulting from information and communication technology (ICT) incidents, including those caused by cyber-attacks, theft or any failure.

In our view, Article 75(8) of MiCAR is intended to prejudge the often contentious nature of CASP's liability for damages caused by incidents, including cyber-attacks. Clauses excluding CASP's liability to the extent indicated above will be invalid, due to their contradiction with MiCAR provisions. On the other hand, the above provision does not exclude the possibility of CASP being held liable on other legal grounds, including as a result of non-performance or improper performance of an obligation or on the basis of a tort. However, with regard to liability for incidents in the scope outlined above, CASP is entitled to rely on Article 75(8) of MiCAR as *lex specialis*, concerning in particular the prerequisites and amount of its liability for such incidents.

Summary

The scope of entities entitled to provide custody and administration of crypto-assets services is limited by the MiCAR provisions. It only allows the provision of such a service by authorised entities or by certain financial entities providing adequate services outside the crypto market, once they have complied with their notification obligation to the competent supervisory authority. Further requirements under MiCAR generally apply uniformly, regardless of the type of CASP.

The material scope of the service under consideration is the issue that may cause the most practical problems, due to the terminological inconsistency between the recitals and the definition of the service in MiCAR, as well as the lack of explanation of the wording used in the definition. These issues will therefore be subject to further elaboration through literature, positions of competent authorities and case law. The most important conclusion is that the service in question may cover all types and categories of crypto-actives as defined in MiCAR, with the exception of crypto-assets that are generally excluded from the scope of application of this Regulation. However, it will mainly exclude from its scope non-custodian wallet services and situations where the CASP exercises safekeeping or controlling of the crypto-asset on its own behalf and not on behalf of a client. Furthermore, the service in question cannot be provided if the CASP does not exercise effective control over the client's crypto-asset or means of access to the client's crypto-asset also in the case of any service other than the provision of non-custodial wallets.

On a positive note, MiCAR introduces a number of important public law obligations for CASPs providing the service under analysis. The obligations regarding the operational, technological and legal segregation of clients' crypto-assets, the practical

application of which may, however, raise questions, should be regarded as particularly important. Above all, ensuring adequate protection of clients vis-à-vis CASP creditors, particularly in the event of CASP bankruptcy or restructuring, requires a legislative initiative of the relevant EU Member States in order to be effective. In the private law sphere, the MiCAR, on the other hand, introduces minimum requirements regarding the very obligation to conclude, as well as the content of, a CASP's contract with the recipient of the custody and administration of crypto-assets services. MiCAR also establishes minimum information obligations and regulates in a limited way the liability of the CASP towards the client.

The multiplicity of obligations imposed on CASPs in MiCAR, which are inspired by similar solutions already in place under TradFi, in juxtaposition with the broad subject-matter scope of the service in question, suggests that this regulation will safeguard the interests of users at least at a basic level. The fact that the requirements for CASP are subject to a detailed examination as part of the authorisation and notification procedure deserves a positive assessment. As part of these, an applicant for CASP status must provide comprehensive evidence of compliance with both private and public law obligations under MiCAR, in particular by providing a description of custody and administration policy, as well as a description of the procedure for the segregation of clients' crypto-assets, as required by the relevant Delegated Regulations 2025/303[13] and 2025/305[14]. Ultimately, however, it is the practice of application of the MiCAR regulations, including supervisory practice, that will determine whether the mechanisms provided for in MiCAR will prove to be effective and contribute significantly to reducing the number of market abuse or other incidents affecting the interests of clients.

Bibliography

"Safekeeping" (n.d.) Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/safekeeping (accessed 10.05.2025).

Arner D., Zetzsche D., Buckley R., Kirkwood J. (2023). *The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022–2023*, University of Hong Kong Faculty of Law Research Paper, 2023/19.

Commission Delegated Regulation (EU) 2025/303 of 31 October 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included by certain financial

[13] Commission Delegated Regulation (EU) 2025/303 of 31 October 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included by certain financial entities in the notification of their intention to provide crypto-asset services, OJ L, 2025/303, 20.2.2025.

[14] Commission Delegated Regulation (EU) 2025/305 of 31 October 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in an application for authorisation as a crypto-asset service provider, OJ L, 2025/305, 31.3.2025.

entities in the notification of their intention to provide crypto-asset services, OJ L, 2025/303, 20.2.2025.

Commission Delegated Regulation (EU) 2025/305 of 31 October 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in an application for authorisation as a crypto-asset service provider, OJ L, 2025/305, 31.3.2025.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, pp. 35–127.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, pp. 43–74.

Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS), OJ L 302, 17.11.2009, pp. 32–96.

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, OJ L 174, 1.7.2011, pp. 1–73.

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, OJ L 173, 12.6.2014, pp. 349–496.

European Banking Authority (2025), Joint Report, Recent developments in crypto-assets (Article 142 of MiCAR), https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1391_Joint_Report_on_recent_developments_in_crypto-assets__Art_142_MiCA_.pdf (accessed 10.05.2025).

Gudowski J. (2017). 'Art. 835', in: T. Bielska-Sobkowicz, H. Ciepła, P. Drapała, M. Sychowicz, R. Trzaskowski, T. Wiśniewski, C. Żuławska, J. Gudowski (eds.), *Kodeks cywilny. Komentarz. Tom V. Zobowiązania. Część szczegółowa*, wyd II, Warszawa: Wolters Kluwer, p. 448.

Kokorin I. (2023). *The Anatomy of Crypto Failures and Investor Protection Under MiCAR*, Forthcoming in the Capital Markets Law Journal, pp. 15–16.

Ossio D., Nixon L., Yates M. (2023). *Custody of Cryptoassets: Moving Towards Industry Best Practice*, https://financialmarketstoolkit.cliffordchance.com/en/financial-markets-resources/resources-by-type/guides/custody-of-cryptoassets--moving-towards-industry-best-practice--.html (accessed 10.05.2025).

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, OJ L 150, 9.6.2023, pp. 40–205.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on cryptocurrency markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, OJ L 150, 9.6.2023, pp. 40–205.

Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories, amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, OJ L 257, 28.8.2014, pp. 1–72.

UNIDROIT (International Institute for the Unification of Private Law) (2023), *Principles On Digital Assets And Private Law*, International Institute for the Unification of Private Law, https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf (accessed 10.05.2025).

The Act of 23 April 1964, Civil Code (consolidated text: Journal of Laws of 2024, item 1061, as amended).

Völkel O. (2023). *MiCAR versus MiFID – Wann ist ein vermögenswertreferenzierter Token kein Finanzinstrument?*, "Zeitschrift für Finanzmarktrecht", p. 6.