No 2(99) 2025

eISSN 2544-7068

BEZPIECZNY BANK

SAFE BANK

BFG Bankowy Fundusz Gwarancyjny

SAFE BANK is a journal published by the Bank Guarantee Fund since 1997. It is devoted to issues of financial stability, with a particular emphasis on the banking system.

PUBLISHER

Bankowy Fundusz Gwarancyjny
ul. Ks. Ignacego Jana Skorupki 4
00-546 Warszawa

SECRETARY

Ewa Teleżyńska
Telephone: 22 583 08 78
e-mail: redakcja@bfg.pl

DOM WYDAWNICZY ELIPSA

Desktop publishing:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel. 22 635 03 01, e-mail: elipsa@elipsa.pl,
www.elipsa.pl

Contents

Jacek Jastrzębski*

A word from the Editors

The moment we – the Programme and Scientific Council, the Editorial Committee of the journal *Safe Bank*, and myself as the editor of this special volume – commend to the Readers a thematic issue dedicated to crypto-assets is, given the topic, nothing short of special.

From a global perspective, the fundamental reason is the new approach of the U.S. federal administration to crypto-assets, particularly crypto-currencies. We are witnessing efforts – both declared and reflected by tangible legislative actions – to open the financial market to crypto-assets, accompanied by efforts to stop the work on central bank digital currency (CBDC), sometimes presented as a kind of alternative to crypto-currencies. The openness of the U.S. administration to crypto-assets also translates into the strategies of global financial institutions with their principal place of business in the United States of America, where they generate a significant part of their revenue: some institutions which have so far expressed scepticism towards crypto-assets and towards the engagement of financial institutions in this area of trade are now changing their stance in the new regulatory environment.

In the European Union, a new regulation has come into effect – Regulation on markets in crypto-assets (MiCAR[1]), which aims to standardise and regulate the crypto-asset market, primarily to protect its participants.

From Poland's perspective, the proposal for a law aimed at adapting Polish law to MiCAR – including through the designation of a national authority competent to license and supervise crypto-asset service providers – is now a subject-matter

* The editor of Issue 2(99) 2025 of *Safe Bank* and the author of the introduction is dr hab. Jacek Jastrzębski, prof. UW, Chair of the Board of the Polish Financial Supervision Authority (PFSA). The views and opinions expressed in the text below are the views and opinions of the author and do not necessarily reflect the official position of the PFSA or of the Board of the PFSA. The author of each article published in this issue is individually responsible for the views they express.

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.

of parliamentary work. The proposal attracted a lot of interest from stakeholders already at the stage of the government's work, as reflected by numerous comments submitted during consultations and by the conclusions from consensus conferences.

At the same time, the Polish financial market shows clear interest in crypto-assets and related products, both on the part of clients (investors) and financial institutions. Studies among investors have shown that even up to approx. 3 million Polish citizens have had some experience with crypto-assets.[2] Even if the total amounts of the funds so engaged are not significant yet, the figure indicates that the society is highly interested in this type of assets. Financial institutions often claim that offering the possibility of acquiring crypto-assets or related products becomes necessary as this is something clients expect. Moreover, studies confirm that clients are interested in the option of gaining exposure to this category of assets through entities that enjoy special trust: in particular banks and investment firms.[3] All these factors demonstrate the great responsibility public institutions and financial institutions themselves have for handling the crypto-asset market, which in turn leads to the question about the regulatory and supervisory policies regarding that market. This is also a matter of whether the crypto-asset market is part of the financial market, in particular capital market – and the answer may turn out non-trivial or nuanced due to the diversity and a different regulatory status of crypto-assets. I shall go back to this matter further in the introduction.

The papers selected for this issue of *Safe Bank* guide the Readers through various aspects of the functioning and regulation of the crypto-asset market.

The first three texts provide a general framework for a discussion on the crypto-asset market by addressing topics such as: social groups interested in crypto-assets, the relations between the crypto-asset market and the financial market, and the general question about the banks' appetite to engage in operations related to crypto-assets.

Firstly, the Readers can acquaint themselves with the results of empirical studies relating to the profile of investors interested in the crypto-asset market. The authors who conducted the studies assessed a series of parameters regarding human behaviour and decision-making which may be typical of individuals interested in buying crypto-assets. The findings from this kind of research are potentially of paramount importance both to the supervisory policy in this respect and to risk management at financial institutions. Meanwhile, the description of characteristics of this group in terms of communication channels that can be useful in reaching the group becomes particularly relevant in the context of financial education as well as effective formulating and positioning of messages addressed to potential participants in the crypto-asset market.

[2] The image of Poles as (non-)investors [Pol. *(Nie)inwestycyjny obraz Polaków*]. Accenture's study on Polish retail investors, March 2024, https://jakinwestujapolacy.pl/raport.pdf, p. 22.

[3] Retail investor in Poland: self-portrait vs the industry's view (Pol. *Inwestor indywidualny w Polsce – autoportret vs spojrzenie branży*]. Report prepared by Accenture and University of Warsaw, March 2025, https://jakinwestujapolacy.pl/raport2025.pdf, p. 31.

The second text explores the relationship between the crypto-asset market and the financial market. From the perspective of the regulatory and supervisory policy, the key is to assess the occurrence of any risk of contagion between the crypto-asset market and the market of traditional financial assets – shares, bonds, and other financial instruments. Those reflections may provide insights about potential economic functions of crypto-assets, particularly in the context of a hypothesis – albeit treated with scepticism – regarding the hedging function of crypto-assets based on their unproven countercyclical function in contrast to stock markets or markets of other goods. However, an important conclusion from a regulatory and supervisory point of view is that crisis scenarios involve an increase in the correlation between the crypto-asset market and other markets, which may indicate the existence of the risk of spill-over of the crisis from the crypto-asset market to the financial or commodity markets. Consequently, not only do crypto-assets fail to play the role of a stabiliser for financial or commodity markets but, on the contrary, in a stress scenario the impulses from the crypto-asset market may adversely affect the functioning of the capital or commodity markets by initiating, for example, the outflow of capital. Such a finding is important as it leads to the conclusion that even if the crypto-asset market were to be institutionally independent from the capital market, the functioning of the crypto-asset market cannot protect the financial market against negative effects of crisis scenarios in the crypto-asset market. In other words, any crisis or shock in the crypto-asset market might not remain confined within the limits of this market but rather spill over to traditional capital or commodity markets. This shows the scale of responsibility associated with redirecting material streams of funds to the crypto-currency market, which may become a risk factor for the financial market, even if the institutional links – stemming from, for example, the participation of financial institutions in the crypto-currency market – were relatively small.

Systemic thoughts are also at the heart of the next article, which explores the engagement of banks in the crypto-asset market. The author discusses possible forms of such engagement, considering both business aspects – in particular the risks and benefits generated by this type of business – and the regulatory approach of the EU legislator to banks engaging in those forms of business. On one hand, such business may enrich banks' offer and, from their perspective, provide an additional stream of revenue; on the other hand, though, it may create a new channel of contagion and transfer of risk from the undoubtedly more volatile and riskier crypto-asset market to a sector traditionally seen as the most conservative in terms of risk management: the banking sector.

The three opening papers in this issue create a context for the analyses presented in the next five articles: four of them are dedicated to detailed legal reflections on how MiCAR regulates selected crypto-asset services, and one assesses the effectiveness of MiCAR provisions that are to prevent manipulation.

The articles presented in the first part of the issue focus on selected aspects of a general reflection on the crypto-asset market or their relation to the traditional financial market, while the next group of articles deals with a legal analysis of issues arising from the regulatory framework adopted in MiCAR.

There are several reasons underlying the legal discussion presented in this volume.

First of all, the EU legislator has decided that crypto-assets – including those other than financial instruments as defined in Article 4(1)(15) of MiFID II[4] – should fall under a regulation modelled on the regulation pertaining to the financial market, in particular the capital market. In several of its aspects, MiCAR refers to or is based on solutions provided for in regulations concerning the market in financial instruments, in particular MiFID II and MAR (e.g. to the extent related to inside information and manipulation).

At this point it should be emphasised that according to the assumptions of MiCAR, it does not apply to crypto-assets being financial instruments as defined in MiFID II (Article 2(4)(a) of MiCAR), which as such have already fallen within the scope of application of EU rules regarding financial instruments (cf. recital 3 of MiCAR). In other words, by decision of the European legislator, under MiCAR, rules modelled on and shaped similarly to the rules governing the financial market, in particular the capital market, have been applied to services related to objects (crypto-assets) other than financial instruments.

Such a solution has various implications. In the first place, it may raise questions about the adequacy of the implemented solutions in view of typical challenges witnessed in the market of crypto-assets other than financial instruments. The question about the effectiveness of solutions transferred to the crypto-asset market from the traditional financial instrument market may apply, i.a., to the rules on manipulation.

Furthermore, the adopted regulatory model creates an image of close affinity between the market in financial instruments and the market in crypto-assets other than financial instruments, which also has certain consequences, in particular it may lead to a scenario where the crypto-asset market would start to be regarded by the general public as a segment of the financial market. This thread may pose a particular challenge in the context of shaping the relevant supervisory and regulatory policies; I shall come back to it in the final part of the introduction.

Secondly, crypto-assets (as defined in Article 3(1)(5) of MiCAR) may turn out to be not only financial instruments as defined in MiFID II but also other objects falling – by virtue of EU law – under other sectoral regulations, in particular those pertaining to the financial market, e.g. funds as defined in the PSD2.[5] In this respect, the conflict-of-laws rule which draws a line between the scopes of application of MiCAR and PSD2 is not that clear as in relation to crypto-assets being financial

[4] 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, p. 349).

[5] 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, p. 35).

instruments: in fact, Article 2(4)(c) stipulates that MiCAR does not apply to crypto-assets being funds as defined in PSD2 (in this respect, PSD2 applies), unless such crypto-assets qualify as e-money tokens. The term 'e-money token' or an equivalent term 'electronic money token' (abbreviated to 'EMT') means a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency (Article 3(1)(7) of MiCAR). Even though under Article 2(4)(c) of MiCAR, the regulation does not apply to crypto-assets being funds but not EMT, the case of EMT compels an opposite conclusion: such crypto-assets fall under the scope of application of MiCAR. The question is, though, about the potential dual legal regime for EMT in a case where services related to EMT were to fall under both MiCAR and PSD2. This overlap of regulatory regimes for the crypto-asset market and the payment market has attracted interest not only from the market but also from EU institutions, which are taking actions to reduce the regulatory uncertainty and legal risk associated with a potential cumulative regime in regard to EMT. However, with the functional distinctions into more payment-related or more investment-related purposes of transactions, these matters are not entirely free from controversy. These topics are addressed in detail in two articles of this issue.

The closing paper of this issue addresses the topic of the qualification of digital goods – such as programmable central bank digital currency (PCBDC) in this case – seen from the perspective of the theory of money rather than any specific normative material. The author concludes that although the status of the CBDC as money seems to leave no doubt, the qualification of the programmable CBDC depends on the adopted theory of money. This may be one of the reasons why even the central banks engaged in the work on the CBDC are rather unforthcoming about the issuance of programmable money.

Now, having provided a brief overview of the topics explored in the articles published as part of this issue, I would like to go back to the topic of challenges stemming from MiCAR's general approach to regulatory framework for the markets in crypto-assets other than financial instruments – a framework modelled on the regulations concerning the financial market, in particular capital market. This also begs the question about the relation of the crypto-asset market to the financial market, and the role and tasks of the financial supervisor and the regulatory and supervisory policy.

The starting point here should be the original purpose of financial market and financial market regulation and supervision. It is about building confidence in the financial market as an infrastructure which allows conversion of savings into investments and lending activity. Confidence is built, on one hand, by establishing prudential regulation and supervision to ensure the solvency of financial institutions which are subject to such supervision and, on the other hand, by ensuring an appropriate level of protection of market participants: customers of financial institutions and investors in the capital market, in the form of conduct-of-business rules and information disclosure requirements. Traditionally, bank supervision consisted mainly in prudential supervision, while capital market supervision focused on:

(i) ensuring appropriate conduct-of-business rules governing the relations with clients of investment firms, (ii) enforcing information disclosure requirements, and (iii) preventing manipulation and misuse of information privilege. With time, the supervisory convergence is progressing, which is reflected by a greater focus on the conduct-of-business in the area of bank supervision (e.g. product governance) on one hand, and on components of prudential supervision of capital market entities on the other hand. In any case, however, building confidence – both using the tools of prudential supervision and conduct-of-business supervision – is not only an end in itself. With this confidence, the financial market can effectively serve as a mechanism of transforming savings into investments – be it equity, debt, or credit. This is why the State engages its public authority – expressed for instance in an established public supervision of the financial market – to ensure that the society has confidence in the financial market and its institutions so that potential can be created for the financial market to efficiently perform its organic function of providing financial intermediation and financing the investment needs of the economy. Another element is ensuring a safe and effective payment mechanism to reduce the costs of transactions between counterparties, thus making the exchange more efficient. This is also the reason why in the long-term the objectives of financial supervision – in Poland, defined in Article 2 of the Act on financial supervision[6] – have synergy with the efforts to promote the development of the financial market. The market develops properly only when individuals who – as depositors or investors in collective investment undertakings, or shareholders or bondholders who entrust their funds directly to specific issuers – entrust their funds to professional financial intermediaries, do it with a sense of confidence in the proper and fair functioning of the market and a sense that their funds are secure to the extent adequately correlated with the expected rate of return.

How relevant are these reflections in the context of crypto-assets? Since the 'crypto-assets' category treated as a whole is characterised by a high degree of inner diversification, it is worth taking a look at whether and how the crypto-asset market performs functions specific to the financial market and has the same organic features which have induced the State to assume the responsibility for establishing and enforcing financial regulations and for their functioning.[7] It is also interesting to refer to the legislative intentions expressed in the preamble to MiCAR.

Recital 2 of MiCAR reads as follows: *'Crypto-assets are digital representations of value or of rights that have the potential to bring significant benefits to market participants, including retail holders of crypto-assets. Representations of value include external, non-intrinsic value attributed to a crypto-asset by the parties concerned or by market participants, meaning the value is subjective and based only on the interest*

6 Act of 21 July 2006 on financial market supervision (Journal of Laws 2025, item 640).

7 Cf. The opening address: „Czy kryptoaktywa są elementem rynku finansowego?" *[Are crypto-assets an element of the financial market?]* and the related discussion held during the 28th Open Academic Session of the Commercial Law Chair of the Faculty of Law and Administration of the University of Warsaw on 7 April 202, https://kph.wpia.uw.edu.pl/nagranie-z-xxvii-opn-z-udzialem-dr-hab-jacka-jastrzebskiego-llm-berkeley-prof-uw/

of the purchaser of the crypto-asset. By streamlining capital-raising processes and enhancing competition, offers of crypto-assets could allow for an innovative and inclusive way of financing, including for small and medium-sized enterprises (SMEs). When used as a means of payment, crypto-assets can present opportunities in terms of cheaper, faster and more efficient payments, in particular on a cross-border basis, by limiting the number of intermediaries.'

The mutual relationship of the statements in that part of MiCAR may require further analysis.

On one hand, the text expressly admits that crypto-assets 'include external, non-intrinsic value attributed to a crypto-asset by the parties concerned or by market participants, meaning the value is subjective and based only on the interest of the purchaser of the crypto-asset', which seems to be a veiled recognition of a purely speculative nature of those instruments, whose valuation is not based on any fundamental value.

On the other hand, it is stated that crypto-assets may streamline the capital-raising process and constitute an innovative and inclusive way of financing, particularly for small and medium-sized enterprises (SMEs). Such an approach would mean that in a way, crypto-assets perform an organic function of the capital market and – as a method of raising capital for business projects – they would in fact represent a certain fundamental value, which in turn would not be consistent with the preceding sentence. One may also ask: do crypto-assets for capital-raising purposes not fall under other EU regulations, for example MiFID II, whose application, as already mentioned, excludes the application of MiCAR?

Finally, from the third perspective, crypto-assets may also be used as a means of payment; in that case also, as it seems, their inherent value cannot be denied. Their regulatory status – and whether they fall under PSD2 only or under both MiCAR and PSD2 if they are to be identified as EMT (which, after all, is a questionable point – and probably subject to further discussion) – has already been mentioned.

The conclusions from recital 2 of MiCAR are therefore ambiguous. On one hand, they point to a speculative nature of crypto-assets, which are deprived of any inherent value whatsoever. On the other hand, the examples mentioned – capital raising, the function of a means of payment – suggest that crypto-assets have an underlying value expressed, for instance, in the valuation of a business project to be so financed.

The above observations are somewhat in line with the assumptions regarding the scope of application of MiCAR. A declaration in this regard can be found in recital 9 of MiCAR, which stipulates that: '*Union legislative acts on financial services should be guided by the principles of 'same activities, same risks, same rules' and of technology neutrality. Therefore, crypto-assets that fall under existing Union legislative acts on financial services should remain regulated under the existing regulatory framework, regardless of the technology used for their issuance or their transfer, rather than this Regulation.*' That declaration is mirrored – as already mentioned – by the conflict-

of-laws rules laid down in Article 2(4) of MiCAR, which exclude the application of MiCAR to crypto-assets being financial instruments (point (a)) and funds, which exception does not apply to EMT (point (c)).

One should ask then: what is the real scope of application of MiCAR to crypto-assets used by business entities for capital-raising purposes (which, as it may appear, will be treated in most cases as financial instruments) or as a means of payment (which in many cases are to qualify as funds)? One may have an impression that such scope of application is to cover mainly the EMTs for which regulatory dualism of PSD2 and MiCAR may occur, and perhaps the crypto-assets that are to be used by businesses to obtain financing, other than financial instruments (if the market creates such a category). Yet, such an observation considerably affects the understanding of recital 2, as it may follow from it that the definition of the scope of application of MiCAR may exclude a material part of crypto-assets used for the purposes stated therein. At the same time, it is hardly conceivable that the MiCAR regulation should be considered as a regulation giving access to the European financial markets to cryptocurrencies (as a part of a broader category of crypto-assets).

In this context, one should also note recital 5 of MiCAR, under which: *'The absence of an overall Union framework for markets in crypto-assets can lead to a lack of user confidence in those assets, which could significantly hinder the development of a market in those assets and lead to missed opportunities in terms of innovative digital services, alternative payment instruments or new funding sources for Union companies.'* In general, funding sources for companies are regulated under EU regulations on the capital market, while payment instruments – in quite elaborate EU regulations on payment services. Now, a question arises: what is the area of crypto-assets – not regulated under other EU regulations on financial markets – for which the call for building '*user confidence in those assets*' remains valid?

I believe this will be the key question determining the future approach of regulators and supervisors as well as the further supervisory policy on the application of MiCAR.

Any new crypto-assets emerging in the market and falling under MiCAR which pursue the natural purposes of the financial market – in particular alternative payment instruments or new forms of business funding not regulated by other rules – should be seen from the regulatory perspective as manifestations of the development of the financial market. Building confidence in such assets should be treated as a catalyst for such development. This could apply, in particular, to such forms of tokenisation of assets related to running a business which would slip out of financial instrument market regulation and pave the way for new methods of financing business which perhaps would be more appealing to new generations of investors.

To any other extent, in particular to the extent in which crypto-assets falling under MiCAR do not perform any of the natural functions of the financial market, especially being a "*representation of value*" with no intrinsic value, such description of those assets should also be taken into account in the relevant regulatory and supervisory

policies. Customer protection could then become a goal in itself because the efforts to build confidence in such asset categories and to develop the market in question would no longer serve any other legitimate purpose (other than maybe fiscal revenue), as the market does not perform the functions which organically justified the engagement of the State in building such confidence.

The final answer to the question to what extent the crypto-asset market may provide new tools for the financial market to fulfil its own goals and to what extent it will respond to other kinds of needs will come from the economic and technological development. Meanwhile, the responsibility of regulators and supervisors, who have been or will be tasked with protecting the proper functioning of the market, is to keep track of this development and to adapt the regulatory and supervisory policies accordingly.

Problems and Opinions

DOI: 10.26354/bb.10.2.99.2025

Katarzyna Niewińska*
ORCID: 0000-0002-0902-7491
kniewinska@wz.uw.edu.p

Agnieszka Postuła*
ORCID: 0000-0001-9495-0733
apostula@wz.uw.edu.pl

Tomasz Rosiak*
ORCID: 0000-0001-8599-3862
tomasz.rosiak@uw.edu.pl

Paweł Wójcik*
ORCID: 0000-0003-1560-263X
pwojcik@wz.uw.edu.pl

Jacek Pasieczny*
ORCID: 0000-0002-9405-3861
jpasieczny@wz.uw.edu.pl

Who Invests in Cryptoassets? Demographics, Knowledge Sources, and Risk Perception in High-Risk Asset Markets

Abstract

The aim of this study is to identify behavioral and decision-making factors that determine interest in high-risk assets, with particular emphasis on cryptoassets. The analysis covers demographic variables (age, gender, education), prior investment experience, knowledge sources, and product comprehensibility. In February 2025, a two-stage CAWI survey was con-

* Katarzyna Niewińska, Agnieszka Postuła, Tomasz Rosiak, Paweł Wójcik, Jacek Pasieczny – University of Warsaw.

ducted: a random-quota poll (N = 3500) and a targeted study of investors and individuals interested in cryptoassets (N = 940). Regression and correlation analyses indicated that industry conferences and fintech events are significantly associated with investment interest, especially among older respondents and women. Gender differences were also observed in responses to webinars and online training. The results highlight the need to diversify financial education strategies. A limitation of the study is that all of the respondents came from a single country, which may restrict the generalizability of the results to populations in different cultural and social contexts. Furthermore, the data were collected over a relatively short period, which may limit the study's ability to capture dynamic changes in the phenomenon under investigation.

Keywords: cryptoassets, cryptocurrencies, behavioral finance, investment decision-making, financial literacy

JEL codes: G41, D14, A20

Introduction

Over the past decade, the cryptoasset market has evolved from a niche technological innovation into an integral part of the global financial system, with an estimated market capitalization of approximately USD 2.4 trillion. (CCAF 2024). A defining feature of cryptoassets is their exceptionally high price volatility (BIS 2023; Sergio & Wedemeier 2025), which is rarely observed in traditional stock markets and typically accompanies corrections or recessions. The scale of potential risks to retail investors is confirmed by a study of 128 regulatory authorities across 106 jurisdictions – 57% of respondents rated consumer risk in the cryptoasset segment as high (26%) or very high (31%). This is more than twice the level recorded for other areas of fintech, indicating serious threats that may lead to abrupt capital losses among individual investors (World Bank & CCAF 2022).

Existing literature suggests a discernible, though heterogeneous, profile of the cryptoasset investor. Hayashi & Routh (2025) found that cryptocurrency holders tend to exhibit higher risk tolerance, lower levels of objective financial literacy, and are more likely to come from socially disadvantaged groups. Other analyses based on transactional data indicate that while early adopters were typically from high-income brackets, today's investors span a wide range of income levels. Their investment decisions are driven by past gains, market volatility, and the desire to hedge against inflation (Aiello et al. 2023). Akana (2023) confirms this profile, highlighting the dominant role of speculative motives and curiosity.

However, the literature lacks studies that simultaneously consider demographic variables (particularly generational cohorts) and the knowledge acquisition channels used by investors. Most existing research has been conducted in the United States or Asia (Akana 2023; Hayashi & Routh 2025; Meyer et al. 2024; Sato 2024; Sharma et al. 2023). The present study aims to help fill this gap.

A structured questionnaire was administered to a randomly selected sample of 3,500 Polish residents. From this sample, 940 respondents who declared investment experience or interest in cryptoassets were selected for analysis. The study was conducted in February 2025.

The primary objective of this article is to identify behavioral patterns and decision-making factors that influence interest in high-risk assets, particularly cryptoassets. The analysis focuses on demographic variables (generational cohorts, gender) and the sources of financial knowledge used. In particular, the following research questions were posed: How does investor age (understood as generational cohort affiliation) influence the relationship between knowledge sources and interest in cryptoasset investments? To what extent does gender differentiate the strength of associations between forms of investment education and declared interest in the cryptoasset market? What role do social media play as a source of investment knowledge among the youngest investors, and are they a significant predictor of interest in cryptoassets?

The structure of the article is as follows: Section 2 presents a literature review on individual investor behavior in high-risk asset markets, with a focus on cryptoassets. Section 3 outlines the data sources and methodology. Section 4 presents the empirical findings, with particular emphasis on the relationship between demographic variables and information channels. The article concludes with a discussion of the results, practical implications, and recommendations for future research.

1. Literature Review

Many existing global studies have attempted to describe investors by analyzing them through the lens of generational cohorts. Their findings remain somewhat inconclusive. Behavioral theorists argue that the investment behavior of Generation Y significantly differs from that of earlier generations (Altaf & Jan 2023; Grinblatt & Keloharju 2009). Other analyses show that Generation Z's behavior closely mirrors that of Generation Y. A significant portion of this demographic group tends to invest primarily in cryptocurrencies and NFTs, driven by curiosity and fear of missing out – FOMO (CFA Institute 2022).A broader spectrum of investment intentions was explored by Altaf & Jan (2023), who confirmed the importance of FOMO as one of the investment drivers. They also pointed to other factors influencing investment decisions, such as socially responsible investing, overconfidence, and herd behavior.

Intergenerational studies conducted by Thomas et al. (2024) examined the investment behaviors of Generations X, Y, and Z in India. The results revealed that although there were no statistically significant differences in financial literacy across generations, Generation Z scored the highest on financial literacy tests. This underscores the importance of ongoing financial education initiatives targeting younger individuals. Additionally, the studies showed that risk tolerance decreases with age, with Generation Z showing the highest risk tolerance, followed by

Generations Y and X. This finding is supported by Bhuvaneswari & Mugesh (2023), who argue that age is significantly associated with risk appetite, meaning younger generations tend to favor more high-risk investment options. This aligns with research demonstrating that socioeconomic factors influence investment decisions through expected returns, perceived self-efficacy, and risk perception. However, risk perception does not directly affect millennials' decisions regarding equity investments (Ratnadi 2023).

Despite rapid technological advances, no statistically significant differences in technology dependence were observed across age cohorts, indicating that technology exerts a relatively uniform influence on investment behaviour regardless of age.

Gender constitutes another demographic lens through which to analyse investment behaviour. Nevertheless, empirical evidence remains mixed. Some studies find that gender exerts little influence on investment decision-making (Baruah & Parikh 2018; Senthil 2019). Others demonstrate that men display higher levels of self-confidence and a greater propensity toward risk-taking in investment decisions than women (Barber & Odean 2001; Bhandari & Deaves 2006; Kumar & Goyal 2015; Lutfi 2011). Psychological research corroborates these findings, indicating that men generally display greater overconfidence than women, especially in finance and investment contexts (Barber & Odean 2001).

Investment decisions may be influenced by a range of factors, including how information is presented (framing) (Barber & Odean 2001) the source of information on success probability (Hertwig et al. 2004), experience (Sekścińska 2015), and individual traits (Campbell et al. 2004). Risk-taking tendencies may also be explained using regulatory focus theory (Higgins 1998; Higgins et al. 2001). A promotion-oriented motivation system is associated with openness to riskier financial decisions and behaviors, while a prevention-oriented system is linked to risk avoidance. Given that investing may involve both relatively safe and aggressive financial instruments, it can fulfill both security and growth needs depending on the type of investment (Sekścińska et al. 2016).

One can hypothesize that crypto investors make decisions somewhat differently from those in traditional investment markets. Studies of cryptoasset investors show they tend to hold onto losing positions too long and exit winning investments too quickly (Ballis & Verousis 2022). This may stem from distinct information sources and learning processes specific to the cryptoasset market.

Both financial knowledge and interest in finance are generally associated with greater risk tolerance. However, individuals with financial knowledge – despite being more aware of cryptocurrencies – more often declare that they do not intend to hold them (Panos & Karkkainen 2019). At the same time, there is a positive correlation between crypto literacy and general financial knowledge. Better understanding of cryptocurrencies can lead to more informed financial decisions (Jones et al. 2024). Individuals with higher levels of subjective knowledge about cryptoassets more often seek professional advice and view it as complementary

to their own understanding of digital assets (Jones et al. 2024). This may help explain why awareness of risk and returns positively influences the intention to purchase cryptoassets (Chittineni 2022). A significant association exists between age and whether investors have ever attended a course or read a book on investing (Bhuvaneswari & Mugesh 2023). However, typical sources of knowledge about the cryptoasset market are the internet and social media. These not only influence the learning process but, as studies show, moods expressed on Facebook and Twitter can also affect financial decisions (Bollen et al. 2011; Siganos et al. 2014). This influence is not uniform across the investor community. Research shows that YouTube content affects the prices and trading volumes of low-cap cryptocurrencies (Moser & Brauneis 2023). This suggests that such content may reach and influence investors who could be categorized as occasional or novice participants.

Interestingly, there is no significant association between age and awareness of investment risk (Bhuvaneswari & Mugesh 2023), although – as previously indicated – generational groups differ in terms of risk tolerance. It can be assumed that the intentions guiding younger and older investors may vary significantly. Other demographic variables, such as gender, may also affect engagement in the cryptoasset market.

Financial knowledge can also play a pivotal role in investment decision-making. Drawing on a representative sample of U.S. residents (N = 6,000), Bannier et al. (2019) found that women possess lower levels of knowledge about the Bitcoin's features compared to men. The authors emphasise, however, that socio-demographic variables and personality traits explain only a small share of this gender gap. Instead, both objective and subjectively perceived financial knowledge constitute key determinants, accounting for roughly 40 per cent of the disparity in Bitcoin literacy.

Some studies indicate that crypto investors are predominantly young men with high self-reported risk tolerance (Hayashi & Routh 2025), who simultaneously exhibit a lack of objective financial knowledge (Mkrtchyan & Treiblmaier 2025). A study of business students (n=204) and professional financial advisors (n=174) found that male students chose riskier asset allocations than female students, providing evidence of gender differences in risk tolerance (Bollen & Posavac 2018). Confidence and access to information influence trading frequency. More frequent information exposure is associated with more frequent trading. However, overconfident investors tend to trade more often, sometimes excessively (Barber & Odean 2001), particularly when they believe they are using specialized information. Investors with lower confidence levels trade less frequently, especially when relying on bank advice (Abreu & Mendes 2012). Nevertheless, the literature lacks studies that combine demographics, investment experience, knowledge acquisition channels, and product comprehensibility in large, representative samples from Central and Eastern Europe.

As previously indicated, investor knowledge sources are diverse. Jones et al. (2024) showed that cryptocurrency holders are willing to learn from financial professionals (financial advisors). However, decisions are often shaped by a combination of

other factors, such as sentiment on social media. Research shows that sentiment on Facebook is positively associated with current stock returns (Siganos et al. 2014). Sentiment is also influenced by the activity of high-reach individuals online. An analysis of 4,607 videos and 7 crypto influencers, each with over 300,000 subscribers within one year, revealed that their messages impact the prices and trading volumes of low-cap cryptocurrencies (Moser & Brauneis 2023). At the same time, studies do not confirm that influencers are accurate in their market predictions. Numerous studies provide evidence that online discussion forums may be used by investors to promote or abandon sensitive stocks and manipulate the trading behavior of other investors (Agarwal et al. 2019; Sabherwal et al. 2011).

2. Research method

The findings presented in this article are part of a broader research project designed in accordance with the principles of theoretical, methodological, and researcher triangulation. The research process was divided into three main stages.

The first stage was an omnibus survey conducted in October 2024. This preliminary phase provided foundational insights into the population of investors interested in cryptoassets in Poland. The results of this stage informed the design of the research tools used in subsequent phases.

The second stage involved a qualitative study based on semi-structured interviews. The exploratory nature of this method allowed for a deeper understanding of respondents' motivations, experiences, and attitudes toward cryptoassets. Based on the collected empirical material, the following research hypotheses were formulated and subsequently tested:

Hypothesis 1 (H1): The strength of the relationship between the use of professional knowledge sources and interest in cryptoasset investment increases with the investor's age.

Hypothesis 2 (H2): Women exhibit a stronger association between participation in organized educational formats (e.g., webinars, fintech conferences) and interest in cryptoasset investment compared to men.

Hypothesis 3 (H3): Among members of Generation Z, informal sources of knowledge (e.g., social media, friends, influencers) are not significantly correlated with the level of interest in cryptoasset investment.

The third phase – the quantitative study – was conducted using the CAWI method (Computer Assisted Web Interview). Interviews were carried out via the ARIADNA online research panel between February 5 and 10, 2025. The sample selection process followed a two-stage procedure. In the first stage, a filtering question regarding investment experience or interest in cryptoassets was asked of respondents from a nationally representative random-quota sample of Polish residents aged 15 and older (N = 3500).

A total of 948 individuals who declared investment experience or interest in cryptoasset investment qualified for the main study. The demographic structure of this subsample was as follows: 48% women and 52% men; 10% aged 18–24, 18% aged 25–34, 21% aged 35–44, 17% aged 45–54, and 34% aged 55 and above. Regarding place of residence: 37% of respondents lived in rural areas, 32% in small or medium-sized towns, and 13% in cities with over 500,000 inhabitants.

3. Research Results and Discussion

Quantitative analysis revealed significant differences in the strength of associations between knowledge sources and interest in investing in cryptoassets. The study identified two key variables moderating these relationships: respondents' age and gender. Pearson correlation coefficient was used to analyze the connections between knowledge sources and interest in investing in cryptoassets. Before the analysis, it was checked whether the assumptions of normality of distributions, linearity and homoscedasticity of the analyzed variables were met. The results of the analyses and the sample size (N=948) allowed for the assumption of normality of distributions and other assumptions.

Table 1. Preferred Knowledge Sources by Age Cohort

	"Baby Boomers" (N = 55)	**"Generation X" (N = 122)**	**"Generation Y" (N = 163)**	**"Generation Z" (N = 83)**
Industry conferences	0.44*	0.48*	0.26*	0.09
Webinars or online training	0.35*	0.37*	0.17	0.19
Local community meetups	0.43*	0.35*	0.36*	-0.11
On-site workshops organized by crypto-sector companies	0.53*	0.35*	0.21	0.25
Fintech fairs and events	0.46*	0.42*	0.36*	-0.01
International conferences/forums on capital markets	0.35*	0.37*	0.33*	0.03
Conferences/meetings organized by regulators	0.44*	0,21	0.15	0.01
Academic events	0.29	0.35*	0.23*	0.02
Workplace-based thematic training	0.33	0.34*	0.17	0.05

* – statistically significant coefficient p <0,01

Source: own elaborations.

Table 1 presents correlation coefficients between interest in cryptoassets and specific knowledge sources across three generational cohorts. The highest correlation values are observed among Generation X respondents, particularly regarding participation in industry events (r = 0.482) and fintech conferences (r = 0.469). Professional financial advisors also appear as relevant sources for this group. In Generation Y, the strongest correlations are seen with webinars (r = 0.314) and industry events (r = 0.288). Generation Z exhibits generally lower correlation levels, which may suggest a different mode of information consumption – perhaps more fragmented and less oriented toward professional sources. The table also indicates that social media are not a strong predictor of investment interest, which challenges the often-repeated assumption about their dominant role among younger cohorts.

These findings are supported by the qualitative analysis. Younger investors, particularly those from Generation Z, tend to make investment decisions impulsively and under emotional influence (e.g., curiosity, FOMO), drawing information from informal sources such as social media, peers, online forums, or influencers. However, this does not imply a complete lack of critical thinking – some younger respondents voiced skepticism toward NFTs or so-called memecoins. Respondents from older age groups, who more frequently reported attending industry conferences and educational events, demonstrate a more structured decision-making style and a stronger need to verify sources. It is also important to consider that younger generations generally have lower incomes, which often translates into smaller, or even minimal, investment amounts. Spontaneous investment, not preceded by methodical information-seeking and analysis, may also be related to the relatively low value of such investments.

Table 2. Preferred Knowledge Sources by Gender

	Women (N= 232)	**Men (N=191)**
Industry conferences	0.40*	0.24
Webinars or online training	0.30	0.21
Local community meetups	0.28	0.31*
On-site workshops organized by crypto-sector companies	0.36*	0.26
Fintech fairs and events	0.40*	0.24
International conferences/forums on capital markets	0.39*	0.21
Conferences/meetings organized by regulators	0.26	0.11
Academic events	0.34*	0.10
Workplace-based thematic training	0.32*	0.16

* – statistically significant coefficient p <0,01

Source: own elaborations.

Table 2 shows the distribution of correlation coefficients by gender. Women exhibit stronger associations between interest in cryptoasset investment and participation in webinars (r = 0.387) as well as fintech events (r = 0.365), which may suggest a greater tendency to engage in organized forms of online education. Among men, traditional knowledge sources such as news portals and expert materials dominate, although the strength of these correlations is lower compared to women.

Qualitative data offer deeper insight into this interpretation. Women more frequently expressed the need to understand market mechanisms and to seek out sources that offer structured knowledge. Men, on the other hand, emphasized trust in intuition, personal or peer experience, and reliance on influencer analysis. Only a small number of female respondents mentioned consultations with professionals – possibly indicating more limited access or a lack of trust in financial advisors.

The observed differences can be interpreted in light of earlier literature. As shown by Bannier et al. (2019), women more often report lower confidence in financial investment contexts, which may lead them to seek structured knowledge. Meanwhile, the higher prevalence of men in self-directed knowledge acquisition channels may be associated with overconfidence and a tendency to act based on informal cues (Barber & Odean, 2001). Additionally, women statistically have higher levels of education than men, which may be linked to a stronger need for and ability to acquire and systematize knowledge.

Both the quantitative and qualitative findings point to the need for differentiated educational and communication strategies. Promoting investment education through industry events and fintech conferences may be particularly effective for Generation X and women. For Generation Z, more personalized and interactive formats that employ the language and communication environments familiar to younger individuals may be more successful. At the same time, it is crucial to strengthen critical thinking and risk awareness competencies – especially among those relying on social media and informal channels for information.

4. Conclusions

The study provides empirical evidence of differentiated investment patterns based on age, gender, and the use of financial knowledge sources. The findings confirm that interest in cryptoassets – as a class of high-risk assets – is not a homogeneous phenomenon and that its determinants depend on a variety of demographic and cognitive factors. In particular, the results confirm that individuals from Generation X and women show stronger associations between participation in educational events and investment interest, indicating greater responsiveness to professional knowledge distribution channels (H1, H2).

Additionally, the findings do not support the common assumption regarding the key role of social media as a source of investment knowledge among younger cohorts.

For Generation Z, these correlations were relatively weak, which may suggest that although young investors do use social media for information, it does not directly translate into their level of investment interest (H3).

From a theoretical perspective, the study expands our understanding of the role of information sources in decision-making processes related to high-risk investments and reveals the importance of intergenerational and gender differences. It contributes to the field of behavioral finance and financial education.

The practical implications primarily concern the design of effective educational programs and regulatory actions. The results indicate that educational campaigns should be better tailored to specific target groups – both in terms of format and content. Short, visual, and interactive formats may work well for Generation Z, while older cohorts and women are more responsive to industry events and structured training. From a public policy perspective, this implies the need to develop communication strategies that take into account not only knowledge levels but also learning styles.

The main limitations of the study include its restricted geographical scope (Poland) and one-time measurement. Future research should expand the analysis to other Central and Eastern European countries and incorporate psychological variables such as perceived control, impulsivity, or motivational regulatory styles. Another limitation of the study was that the information collected was declarative in nature and may differ from the actual behaviour of the respondents.

A promising direction for future research is to examine how different educational channels foster an informed and responsible approach to investing. Integrating insights from psychology, sociology, and finance could substantially advance strategies that support individual investors and inform the design of more targeted regulations to protect their interests in high-risk markets.

Summary

This article addresses the topic of interest in cryptoassets as a form of high-risk investment by analyzing the impact of demographic factors and knowledge sources on investment decisions. The study, based on a representative sample of Polish residents (N = 3500) and a group of individuals declaring experience or interest in cryptoassets (N = 948), reveals the complexity of investor behavior. Quantitative findings demonstrate substantial variation in the correlations between knowledge sources and declared interest – both by age cohort and gender.

The strongest associations with investment interest were observed among Generation X and women participating in fintech events and webinars. Younger cohorts, particularly Generation Z, showed weaker correlations with traditional educational channels, suggesting a different dynamic of learning and decision-making. The results imply a need to differentiate educational and regulatory

strategies – not only in content but also in delivery format – to more effectively address the needs of diverse investor groups. This article contributes to the literature on behavioral finance and financial education in the context of high-risk markets.

Bibliography

Abreu M., & Mendes V. (2012). *Information, overconfidence and trading: Do the sources of information matter?* Journal of Economic Psychology, 33(4), 868–881. https://doi.org/10.1016/j.joep.2012.04.003

Agarwal S., Kumar S., & Goel U. (2019). *Stock market response to information diffusion through internet sources: A literature review*. International Journal of Information Management, 45, 118–131. https://doi.org/10.1016/j.ijinfomgt.2018.11.002

Aiello D., Baker S.R., Balyuk T., Di Maggio M., Johnson M.J., & Kotter J.D. (2023). *Who Invests in Crypto? Wealth, Financial Constraints, and Risk Attitudes* (31856).

Akana T. (2023). *Cryptocurrency ownership during a crypto winter: effects of a downturn on consumer attitudes to crypto*.

Altaf H., & Jan A. (2023). *Generational theory of behavioral biases in investment behavior*. Borsa Istanbul Review, *23*(4), 834–844. https://doi.org/10.1016/j.bir.2023.02.002

Ballis A., & Verousis T. (2022). Behavioural finance and cryptocurrencies. *Review of Behavioral Finance*, *14*(4), 545–562. https://doi.org/10.1108/RBF-11-2021-0256

Bannier C., Meyll T., Röder F., & Walter A. (2019). *The gender gap in 'Bitcoin literacy'*. Journal of Behavioral and Experimental Finance, 22, 129–134. https://doi.org/10.1016/j.jbef.2019.02.008

Barber B.M., & Odean T. (2001). *Boys will be Boys: Gender, Overconfidence, and Common Stock Investment*. The Quarterly Journal of Economics, 116(1), 261–292. https://doi.org/10.1162/003355301556400

Baruah M., & Parikh A.K. (2018). *Impact of Risk Tolerance and Demographic Factors on Financial Investment Decision*. GIS Business, 13(5), 31–40. https://doi.org/10.26643/gis.v13i5.3270

Bhandari G., & Deaves R. (2006). The Demographics of Overconfidence. *Journal of Behavioral Finance*, *7*(1), 5–11. https://doi.org/10.1207/s15427579jpfm0701_2

Bhuvaneswari M., & Mugesh J. (2023). *A Study on Investment Patterns Among X, Y and Z Generations*. International Journal of Advanced Research in Science, Communication and Technology, 3(10).

BIS (2023). *The crypto ecosystem: key elements and risks Report submitted to the G20 Finance Ministers and Central Bank Governors*.

Bollen Mao, H., & Zeng X. (2011). *Twitter mood predicts the stock market*. Journal of Computational Science, 2(1), 1–8. https://doi.org/10.1016/j.jocs.2010.12.007

Bollen & Posavac S. (2018). *Gender, risk tolerance, and false consensus in asset allocation recommendations*. Journal of Banking & Finance, 87, 304–317. https://doi.org/10.1016/j.jbankfin.2017.10.016

Campbell W.K., Goodie A.S., & Foster J.D. (2004). Narcissism, confidence, and risk attitude. Journal of Behavioral Decision Making, 17(4), 297–311. https://doi.org/10.1002/bdm.475

CCAF (2024). *The 2nd Global cryptoasset regulatory landscape study*.

CFA Institute. (2022). *Gen Z and investing: Social media, cryptocurrencies, and the metaverse*. https://rpc.cfainstitute.org/sites/default/files/-/media/documents/article/industry-research/Gen_Z_and_Investing.pdf

Chittineni J. (2022). *A Study on Cryptocurrency Investors' Purchase Intentions: Revisiting the Brand Personality Theory*. International Journal of Economics and Financial Issues, 12(4), 28–33. https://doi.org/10.32479/ijefi.13102

Grinblatt M., & Keloharju M. (2009). *Sensation Seeking, Overconfidence, and Trading Activity*. The Journal of Finance, 64(2), 549–578. https://doi.org/10.1111/j.1540-6261.2009.01443.x

Hayashi F., & Routh A. (2025). *Financial literacy, risk tolerance, and cryptocurrency ownership in the United States*. Journal of Behavioral and Experimental Finance, 46, 101060. https://doi.org/10.1016/j.jbef.2025.101060

Hertwig R., Barron G., Weber E.U., & Erev I. (2004). *Decisions from Experience and the Effect of Rare Events in Risky Choice*. Psychological Science, 15(8), 534–539. https://doi.org/10.1111/j.0956-7976.2004.00715.x

Higgins E.T. (1998). *Promotion and Prevention: Regulatory Focus as A Motivational Principle* (pp. 1–46). https://doi.org/10.1016/S0065-2601(08)60381-0

Higgins E.T., Friedman R.S., Harlow R.E., Idson L.C., Ayduk O.N., & Taylor A. (2001). *Achievement orientations from subjective histories of success: Promotion pride versus prevention pride*. European Journal of Social Psychology, 31(1), 3–23. https://doi.org/10.1002/ejsp.27

Jones M., Luu T. (Jack), & Samuel B. (2024). *The interdependence of financial literacy and crypto literacy*. Economics Letters, 239, 111737. https://doi.org/10.1016/j.econlet.2024.111737

Kumar S., & Goyal N. (2015). *Behavioural biases in investment decision making – a systematic literature review*. Qualitative Research in Financial Markets, 7(1), 88–108. https://doi.org/10.1108/QRFM-07-2014-0022

Lutfi L. (2011). *The Relationship Between Demographic Factors and Investment Decision in Surabaya*. Journal of Economics, Business, and Accountancy | Ventura, 13(3). https://doi.org/10.14414/jebav.v13i3.13

Meyer E.A., Welpe I.M., & Sandner P. (2024). *Testing the credibility of crypto influencers: An event study on Bitcoin*. Finance Research Letters, 60, 104864. https://doi.org/10.1016/j.frl.2023.104864

Mkrtchyan G., & Treiblmaier H. (2025). *Business Implications and Theoretical Integration of the Markets in Crypto-Assets (MiCA) Regulation*. FinTech, 4(2), 11. https://doi.org/10.3390/fintech4020011

Moser S., & Brauneis A. (2023). *Should you listen to crypto YouTubers?*, Finance Research Letters, 54, 103782. https://doi.org/10.1016/j.frl.2023.103782

Panos G.A., & Karkkainen T. (2019). *Financial Literacy and Attitudes to Cryptocurrencies*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3482083

Ratnadi N.M.D. (2023). *The Influence of Socio-Economic and Psychological Factors on Millennial Generation's Stock Investment Decisions*. Accounting Analysis Journal, 12(2), 123–133. https://doi.org/10.15294/aaj.v12i2.67039

Sabherwal S., Sarkar S.K., & Zhang Y. (2011). *Do Internet Stock Message Boards Influence Trading? Evidence from Heavily Discussed Stocks with No Fundamental News*. Journal of Business Finance & Accounting, 38(9–10), 1209–1237. https://doi.org/10.1111/j.1468-5957.2011.02258.x

Sato H. (2024). *Financial Innovation and Risk Management in Japan*. International Journal of Finance and Accounting, 9(2), 14–25. https://doi.org/10.47604/ijfa.2452

Sekścińska K. (2015). *People's Financial Choice Depends on their Previous Task Success or Failure*. Frontiers in Psychology, 6. https://doi.org/10.3389/fpsyg.2015.01730

Sekścińska K., Maison D.A., & Trzcińska A. (2016). *How People's Motivational System and Situational Motivation Influence Their Risky Financial Choices*. Frontiers in Psychology, 7. https://doi.org/10.3389/fpsyg.2016.01360

Senthil Dr.D. (2019). *Investment Insight: Demographics and Investment Preference among Retail Investors*. International Journal of Innovative Technology and Exploring Engineering, 8(9), 2974–2977. https://doi.org/10.35940/ijitee.I8715.078919

Sergio I., & Wedemeier J. (2025). *Global surge: exploring cryptocurrency adoption with evidence from spatial models*. Financial Innovation, 11(1), 96. https://doi.org/10.1186/s40854-025-00765-0

Sharma R., Mehta K., & Rana R. (2023). *Cryptocurrency Adoption Behaviour of Millennial Investors in India* (pp. 135–158). https://doi.org/10.4018/978-1-6684-8361-9.ch006

Siganos A., Vagenas-Nanos E., & Verwijmeren P. (2014). *Facebook's daily sentiment and international stock markets*. Journal of Economic Behavior & Organization, 107, 730–743. https://doi.org/10.1016/j.jebo.2014.06.004

Thomas R.M., Nair S., Benny M.J., & Almeida S.M. (2024). *Comparative Analysis of Investment Behaviour: Exploring Investment Patterns and Decision-Making between Generation X, Generation Y, and Generation Z*. Management Journal for Advanced Research, 4(2).

World Bank, & CCAF (2022). *The 3rd Global Fintech Regulator Survey*.

Safe Bank 2(99) 2025

DOI: 10.26354/bb.11.2.99.2025

Paweł Węgrzyn*
ORCID: 0000-0001-8963-2765
pwegrz@sgh.waw.pl

Marcin Glicz**
ORCID: 0000-0003-4128-0267
marcin.glicz@upsl.edu.pl

Agnieszka Butor-Keler***
ORCID: 0000-0002-2761-3144
abutor@sgh.waw.pl

Price volatility and regulatory risk of selected cryptocurrencies as a challenge for financial markets

Abstract

The aim of this article is to estimate and compare the price volatility risk of cryptocurrencies (BTC and ETH) and traditional financial assets using GARCH models, as well as to identify regulatory risk stemming from existing and proposed normative frameworks. The research hypothesis assumes that cryptocurrencies – particularly BTC and ETH – exhibit a higher level of risk compared to traditional financial instruments, due to their significant price volatility and insufficient regulatory frameworks. As a result, their potential as portfolio diversification assets may be limited, and their presence in financial markets may contribute to increased investment risk. The empirical analysis applies GARCH(1,1) econometric models to examine the conditional volatility of cryptocurrency prices and compare them with traditional financial assets such as the EUR/USD and USD/PLN currency pairs, as well as the S&P500 and WIG20 stock indices. The results confirm that BTC and ETH demonstrate significantly higher price volatility than conventional financial instruments. Moreover, the Value at Risk (VaR) measures for the analysed cryptocurrencies are substantially higher than those for traditio-

* Paweł Węgrzyn – PhD, Assistant Professor, Economic Geography Department, SGH Warsaw School of Economics.

** Marcin Glicz – Dr habil., LL.M., University Professor, Institute of Law and Administration, Pomeranian University in Słupsk.

*** Agnieszka Butor-Keler – PhD, Assistant Professor, Division of Digital Finance (FinTech), SGH Warsaw School of Economics.

The views expressed in this article are the personal views of the authors and do not represent the official position of the institution where they are employed.

nal assets. The study also includes a regulatory dimension, providing a normative analysis of legal acts relating to the crypto-asset market and assessing the role of such regulations in mitigating risk in financial markets.

Keywords: cryptocurrencies, price volatility, bitcoin, ether, GARCH

JEL codes: C58, G12, G18, K22

Introduction

1. The growing role of cryptocurrencies in financial markets

Cryptocurrencies, led by BTC and ETH, have gained a prominent place in global financial markets over the past decade or so. The dynamic growth in the popularity of these assets is the result of a combination of innovative blockchain technologies, growing social acceptance and the search for alternative forms of investment in the face of low interest rates and macroeconomic uncertainty (Corbet et al. 2019). The growing market capitalisation of cryptocurrencies, which has reached trillions of dollars in recent years, means that a potential collapse of this market could have cascading effects on other segments of the financial system, particularly in the context of institutional links between investors and regulated markets and the cryptocurrency sector (European Central Bank 2019; International Monetary Fund 2021). Such risks became apparent, for example, during the spectacular price declines of cryptocurrencies in 2018 and 2022. After reaching historic peaks in December 2017 and January 2018, when BTC reached USD 19 345 (16 December 2017) and ETH around USD 1 385 (13 January 2018), prices fell sharply. During the first quarter of 2018. BTC lost about 64% of its value and ETH saw a decline of about 94% from its peak to its low of 15 December 2018. The year 2022 brought another significant wave of declines in the cryptocurrency market. Bitcoin started the year at US 47 450 and ended the year at US 16 513, down 65.2%. Ether lost approximately 68.2% of its value over the same period.

In light of the high price volatility and the potential transmission of risk across markets, this study aims to estimate and compare the volatility risk associated with cryptocurrencies (BTC and ETH) and traditional financial assets using GARCH models, as well as to identify regulatory risk stemming from existing and proposed legal frameworks. According to the research hypothesis, cryptocurrencies, in particular BTC and ETH, exhibit a higher level of risk compared to traditional financial instruments due to their significant price volatility and insufficient regulatory framework. As a result, their potential as an investment portfolio diversification asset may be limited and their presence in financial markets may contribute to an increase in risk.

2. Price volatility risk of cryptocurrencies and portfolio diversification

Research on the links between the cryptocurrency market and traditional financial markets does not allow for definitive conclusions regarding the potentially stabilising or destabilising impact of cryptocurrencies arising from their price volatility risk. Bouri et al. (2017) used the DCC-GARCH model to investigate whether BTC can act as a hedge or safe haven against traditional assets (global equities, bonds, oil, gold, commodity index, US dollar). The results showed that BTC's advantage could be at best its low correlation with these assets under normal conditions, and a significant role as a strong safe haven was only observed in the case of extreme weekly declines in Asian stock markets (Bouri et al. 2017). In other words, except in exceptional crisis situations, BTC did not hedge risks in traditional markets, although it could serve as a portfolio diversification component (Ji et al. 2019; Liu and Tsyvinski 2018). The potential of cryptocurrencies to diversify an investment portfolio – due to their low level of correlation to other financial assets – was considered one of the determinants of their growing popularity. Similarly, Dyhrberg (2016), using GARCH models, found that BTC exhibited intermediate characteristics between gold and FIAT currencies. Her model demonstrated bitcoin's hedging properties similar to gold – BTC reacted asymmetrically to shocks, making it useful for risk management

Other work, however, suggests the limitations of cryptocurrencies as 'safe havens'. This is primarily supported by the risk of sudden losses associated with extreme price fluctuations, which could lead to negative consequences for individual investors and thus potential macro-financial consequences (Financial Stability Board 2018; Gandal et al. 2018). Also Klein et al. (2018) argue that the highly speculative nature of cryptocurrencies undermines their credibility as a stable hedging instrument, especially during periods of extreme market volatility. In other words, in situations of severe financial turbulence, cryptocurrencies do not provide as reliable value protection as traditional safe assets (e.g. gold or government bonds). The relatively low correlation of cryptocurrencies with traditional assets during calm periods means that adding a small exposure to cryptocurrencies may have so far had a stabilising effect on the portfolio through a diversification effect. However, with the evolution of the cryptocurrency market there is a growing interdependence and potential risk transmission channels. Canh et al. (2019) examined seven types of cryptocurrencies (bitcoin, litecoin, ripple, stellar, monero, dash, bytecoin) for coincident changes and structural breakthroughs using parameter stability tests, Granger causality tests and the DCC-MGARCH model. They showed that all of these cryptocurrencies experienced significant structural price changes, with shocks initially occurring in the smaller cryptocurrencies then spilling over to the larger ones (testing on data up to 2018). Furthermore, strong positive dynamic correlations and linkage of volatility within the cryptocurrency market were found (Canh et al. 2019). This means that a collapse in one cryptocurrency can easily translate into declines in others, a potentially destabilising mechanism within this market segment. It is important to note, however, that the cited studies focus primarily on the price-related aspects of cryptocurrencies, without addressing legal

risks associated with BTC and ETH. The authors of this study extend the scope of analysis to include this dimension, which is explored in greater detail in the section devoted to the regulatory risk of these two cryptocurrencies. Numerous studies investigate the transmission of volatility and shocks between cryptocurrencies and, for instance, equity or commodity markets.

Many studies have analysed the transmission of volatility and shocks between cryptocurrencies and, for example, the stock or commodity markets. Symitsi and Chalvatzis (2018) investigated the relationship of BTC with energy and technology stocks using a VAR-BEKK-AGARCH model on daily data up to 2017. They showed that price changes and volatility of BTC affect the share prices of these companies (one-way spillover effects). In addition, they identified bidirectional responses to inter-market shocks and time-varying correlations that are relevant for investment portfolio management. Another study using BEKK and DCC-MGARCH models (period January 2017 – May 2021) examined the integration of BTC with several of the world's largest equity markets. It was found that the average dynamic correlation between BTC and stock indices was low, confirming the short-term hedging potential of BTC (Sajeev and Afjal 2022). However, on deeper analysis, it appeared that negative shocks to the BTC market (sharp declines) translated more strongly into stock market reactions than positive shocks. In particular, crisis years (such as 2018 or 2022) saw more pronounced stock market reactions to cryptocurrency collapses than to cryptocurrency appreciation. This suggests an asymmetry in transmission – falls in cryptocurrencies may carry a destabilising effect on other financial markets to a greater extent than rises have a stabilising effect.

Recent work examining the COVID-19 pandemic period indicates that the relationship between cryptocurrencies and traditional assets can intensify during periods of extreme uncertainty. For example, a study on daily data from 2011 to mid-2022 (distinguishing the pre-pandemic sub-period and during the pandemic) used a combination of a DCC-GARCH model and neural networks to analyse the price volatility link between BTC, gold and six major global stock market indices. The results indicated a long-run volatility transmission between BTC and gold, as well as between BTC and stock markets (Ibrahim et al. 2024). Interestingly, short-term strong linkages emerged mainly during periods of stress – for example, during the 2020 market panic, significant short-term contagion occurred between BTC and the Chinese and Japanese stock markets. The study also highlighted that the high volatility of BTC poses a difficult-to-control threat to local equity markets (Ibrahim et al. 2024).

In summary, the literature points to the dual impact of cryptocurrencies on risk for financial markets. Under normal market conditions, cryptocurrencies (mainly including the most studied BTC) are characterised by relative independence from traditional assets, which implies stabilisation benefits through diversification. However, in crisis conditions, correlations can increase rapidly and shocks to the cryptocurrency market can spill over to other market segments, having a destabilising effect. As the cryptocurrency market has evolved, it has also seen an increase internal correlations within the segment since 2018, highlighting

systemic risk within the cryptocurrency market itself and limiting the – previously mentioned – opportunities to hedge risk by investing in different cryptocurrencies (Koutmos 2018; Smales 2021; Xu, Zhang, and Zhang 2021; Yi, Xu, and Wang 2018).

1. Data and research method

1.1. Data

This study of cryptocurrency price volatility stands out in terms of the length of the period analysed – it covers over nine years of daily data (2016-Q1 2025). In comparison, many other studies have used much shorter periods. For example, Sajeev and Afial (2022) analysed four years and one quarter (i.e. from March 2017 – to May 2015), Bouri et al. (2017) examined the period from the beginning of July 2011 to December 2015, i.e. approximately four and a half years. and Dyhrberg (2016) just under five years (from 19 June 2010 to 22 May 2015). The longer time series in this study allows for a more accurate assessment of the price volatility and risks associated with cryptocurrencies over the long term. The choice of this time range is dictated by both the availability of data and significant developments in the cryptocurrency market. The initial date of the study was set at 1 January 2016 since ETH was created in the second half of 2015 (7 August 2015). Starting the analysis at the beginning of 2016 made it possible to simultaneously analyse the two most important cryptocurrencies – BTC and ETH – from the early stage of the latter's development. The end date, 31 March 2025, was chosen to include the most recent period of analysis, thus allowing the most recent conclusions on price volatility and risk in the cryptocurrency market.

Table 1. Characteristics of the logarithmic rates of return of the variables studied

Date	BTC	ETH	EURUSD	USDPLN	SP500	WIG20
Observations	3377	3377	2389	2388	2323	2310
Mean	0.00155	0.00225	~0	~0	0.00044	0.000173
SD	0.03563	0.05148	0.00457	0.006529	0.011394	0.013893
Skewness	-0.34618	0.009135	-0.02486	0.287525	-0.84085	-0.65524
Kurtosis	8.960696	9.51671	4.89045	6.693409	19.168257	11.39759
ADF_pval	<0.001***	<0.001***	<0.001***	<0.001***	<0.001***	<0.001***

Significance levels:* p<0.05,** p<0.01,*** p<0.001.

Source: own elaboration.

Table 1 shows the statistical characteristics of the logarithmic returns for the six analysed variables. The data for BTC and ETH include 3377 daily observations, which is due to the fact that cryptocurrencies are traded 7 days a week, without weekend or holiday breaks. In contrast, traditional market assets – currency pairs (EUR/USD, USD/PLN) and stock indices (S&P500, WIG20) – have a lower number of observations (in the range from 2310 to 2389), as they are only traded on weekdays. The average daily returns for BTC (0.155%) and ETH (0.225%) are noticeably higher than for traditional assets, for which the values oscillate around zero. The standard deviations of the surveyed variables confirm the significantly higher volatility of cryptocurrencies – 3.56% for BTC and as much as 5.15% for ETH respectively – compared to the relatively low volatility for EUR/USD (0.46%), USD/PLN (0.65%) and the moderate volatility of stock indices (S&P500 – 1.14%, WIG20 – 1.39%). The skewness and kurtosis indices identify the asymmetry and leptokurticism of the distributions – all series show excess tails compared to a normal distribution, which justifies the use of GARCH models with Student's t-distribution. The highest kurtosis was observed for the S&P500 index (over 19), indicating an exceptionally strong concentration of large deviations from the mean. Importantly, the results of the ADF test for all the variables tested indicate the stationarity of the return series – for each of them, the p-value was less than 0.001, which allows us to reject the hypothesis of the presence of a unit root at the 0.1% significance level.

GARCH(1,1) models were estimated separately for each asset on the full available dataset, without artificially synchronising the quotation calendars. Only at the benchmarking stage were the series matched against a common portion of the dates, allowing the results to be correctly summarised without interfering with the structure of the original data. This approach allows both the full use of the information contained in the cryptocurrency data (including weekend data) and consistency in cross-sectional analyses and visualisations between asset classes.

1.2. Research method

Research dedicated to the volatility of cryptocurrencies has used various methods to capture the unique properties of volatility and to understand the interdependencies between these asset classes. By far the dominant approach has been GARCH models and their variations, attempting to assess the volatility of cryptocurrencies over time. This is because cryptocurrency prices are characterised by the occurrence of volatility clustering, i.e. periods of large price swings interspersed with periods of relative stability. GARCH models, are particularly effective in studying this type of volatility, as they consider the fact that current price volatility depends on the volatility observed in the past. In addition, as confirmed by Katsiampa's (2017) observations, cryptocurrency price series have distributions with a significant number of extreme observations (so-called fat tails). GARCH models deal well with such extremes as they assume conditional heteroscedasticity, allowing for a better representation of the dynamic features of the data (Bollerslev 1986). Price volatility

is, as defined by the Basel Committee, among the core components of market risk, understood as the risk of incurring losses as a result of adverse movements in the market price of financial instruments (Bank for International Settlements 2016) .

As noted by Fiszeder (2009, p. 88), one of the most widely used models from this family is GARCH(1,1), which is recommended in the literature as a starting point for modelling volatility in financial markets, including the cryptocurrency market, due to its simplicity and good predictive properties (Chu et al. 2017; Dyhrberg 2016; Katsiampa 2017). In general, already Bollerslev (1986) has shown that GARCH(1,1) effectively models conditional variance dynamics and provides stable and reliable short-term forecasts.

The full specification of the GARCH(1,1) model used includes two equations – the mean equation and the conditional variance equation:

1) Equation of the mean: $r_t = \mu + \varepsilon_t$
2) Variance equation: $\sigma_t^2 + \omega + \alpha\varepsilon_{t-1}^2 + \beta\sigma_{t-1}^2$

Where:

r_t – the asset's rate of return over time,
μ – a constant component in the average equation, reflecting the expected rate of return of the asset,
ε_t – prediction error (model residual), with $\varepsilon_t \mid \Omega_{t-1} \sim t(0, \sigma_t^2, \nu)$ having a Student's t-distribution with ν degrees of freedom,
σ_t^2 – conditional variance of returns,
$\omega > 0$ – constant variance component, representing the long-term level of variability,
$\alpha \geq 0$ – ARCH parameter measuring the immediate response of the variance to new information (recent price shocks),
$\beta \geq 0$ – GARCH parameter indicating the persistence of variation, i.e. the extent to which the current variance depends on previous values.

The choice of the GARCH(1,1) model is also justified by the fact that empirical studies of the cryptocurrency market have confirmed that time series of cryptocurrency prices are characterised by a significant number of extreme observations (Katsiampa 2017). In such situations, it is important to choose the conditional error distribution appropriately. The literature suggests that a Student's t-distribution may be more appropriate than a normal distribution as it better reflects the presence of fat tails in financial data (Cont 2001). The use of a Student's t-distribution improves the efficiency of value-at-risk (VaR) estimation and improves the accuracy of predicting extreme events (Kuester 2005). Katsiampa (2017) conducted a comparison of the effectiveness of different GARCH models for the bitcoin market, indicating that GARCH(1,1) with a t-Student distribution has the best fit and volatility prediction accuracy. Similarly, Chu et al. (2017) confirmed the dominant role of this GARCH variant when modelling cryptocurrency volatility, highlighting its superiority in capturing the dynamic features of the series.

Complementing the econometric modelling, the Value at Risk (VaR) measure was also used to examine the assessment of the level of risk. The calculated VaR answers the question: what is the potential maximum loss (assuming a significance level) that should not be exceeded over a given time horizon? Formally, assuming a significance level α (e.g. 5% or 1%) and a horizon of one day, then VaRα is the cut-off value such that with probability (1–α) the actual loss will not exceed this value. The study uses the historical method to estimate VaR, which involves collecting the historical daily returns of the asset under study over the relevant time window (i.e. from 2016 to the end of Q1 2025) and determining the quantile of order α from the empirical distribution thus obtained. The advantage of the historical method is that there are no assumptions about the distribution (e.g. normal) of returns. Real market data are used for the calculation. A disadvantage may be the lack of updating against current volatility (if volatility is increasing, historical data from a softer period may underestimate risk). Therefore, the study also calculated VaR parametrically based on a GARCH(1,1) model with a t-student distribution (McNeil et al. 2005, pp. 283–291). For this purpose, the average level of over the sample period reflecting the typical level of variability from the sample was used.

In addition to VaR, the Expected Shortfall (ES) is also presented**.** ES (1–α) estimates the average loss assuming that the loss has already exceeded the VaR threshold. Methodologically, the historical version counts the average of the worst α% of historical return observations.

The dogmatic method, commonly used in legal sciences, was also utilised as a research approach for conducting the analyses.

2. Empirical results and discussion

Table 2 summarises the key parameters of the GARCH(1,1) models with Student's t-distribution for the six assets analysed: two cryptocurrencies (BTC, ETH), two currency pairs (EUR/USD, USD/PLN) and two equity indices (S&P500, WIG20).

In the sample, cryptocurrencies (BTC, ETH) achieved a sum of α+β=0.999, which means that periods of high volatility in these markets are extremely persistent (very high volatility persistence). A comparable level is also found in the S&P500 index, where the α component (short-term shock response) is higher than in cryptocurrencies (0.166 vs 0.101–0.151). Despite this, BTC and ETH have significantly higher ω, i.e. the initial variance condition (they were the only assets in the table to reach significance for this parameter). This suggests a certain baseline level of volatility, noticeable even in the absence of market shocks.

One of the key factors influencing risk assessments is the so-called 'fat tails'. This is informed by the *shape* parameter showing how strongly the distribution of returns deviates from normal in terms of extreme events (for low levels of this parameter). A high *shape* level in the range 3.22–3.34 for cryptocurrencies indicates extremely fat

tails and therefore an increased frequency of extreme price fluctuations. Although the distribution of the S&P500 is also leptokurtic (shape 5.48) – to a noticeably lesser extent than for cryptocurrencies. The WIG20 index and the EUR/USD and USD/PLN currency pairs presented noticeably higher *shape* levels, suggesting that extreme volatility is statistically less likely than in the cryptocurrency market.

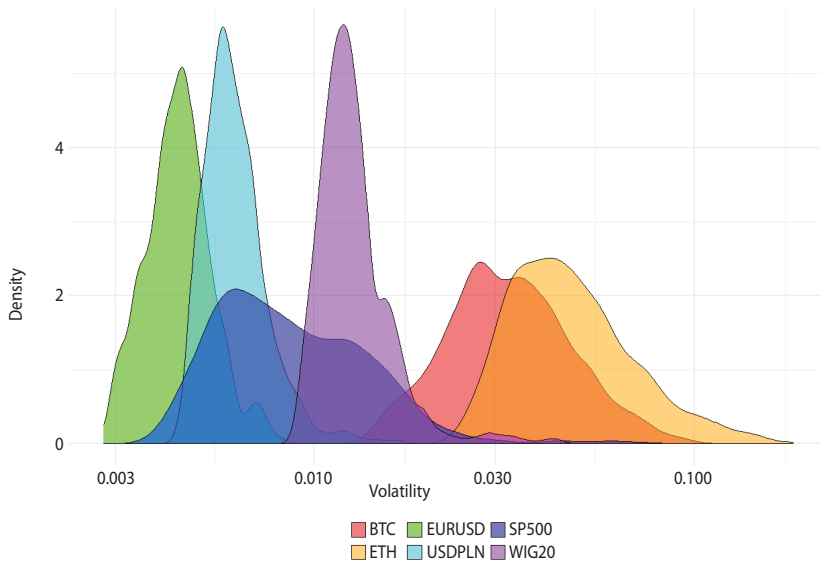
Table 2. Comparison of parameters of GARCH(1,1) models for the assets analysed

Asset	μ (constant in the average equation)	ω (initial condition of variance)	α (shock response)	β (persistence of variability)	Shape (thickness of tails)
BTC	0.00137***	0.00002**	0.10140***	0.89760***	3.22256***
ETH	0.00102	0.00008**	0.15136***	0.84764***	3.34473***
EUR/USD	-0.00003	~0	0.03425***	0.95922***	9.51623***
USD/PLN	-0.00009	~0	0.07170***	0.88958***	10.01976**
SP500	0.00094***	~0	0.16610***	0.83288***	5.47750***
WIG20	0.00029	~0	0.05633**	0.92011***	8.11741***

Significance levels:∗ p<0.05,∗∗ p<0.01,∗∗∗ p<0.001.

Source: own calculations based on data from the period under review.

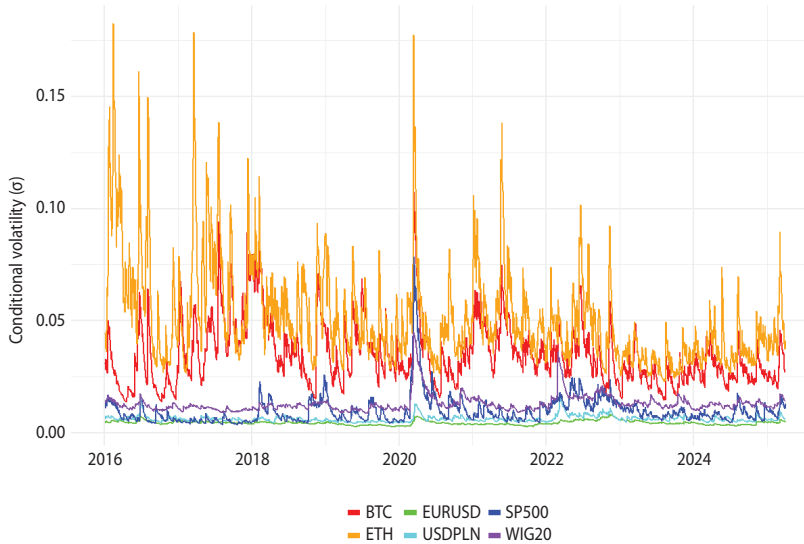
Figure 1. Comparison of volatility distributions of individual assets



Source: own compilation based on GARCH(1,1) model estimations.

The differences in the levels of occurrence of extreme volatility are evident in Figure 1, showing a comparison of the volatility distributions of all the assets studied. This graph shows that ETH and BTC regularly adopt higher volatility values (on a daily basis) than the other assets.

Figure 2. Comparison of the conditional volatility of selected financial assets



Source: own compilation based on GARCH(1,1) model estimations.

As can be seen from the data presented in Figure 2, episodes of extremely high volatility occur much more frequently for cryptocurrencies and reaches around 10–15% of the daily standard deviation, while the conditional volatility of the other assets studied oscillates within a few per cent (stock indices) or less (currency pairs) over the period studied. The results presented here indicate a significantly higher market risk in the cryptocurrency market than in traditional equity or currency markets.

In order to complement the conclusions obtained from the GARCH(1,1) model, a calculation was made of the VaR level, which is one of the key risk measures used in modern finance, as it quantifiably describes what loss – with a certain probability – will not be exceeded in a given time horizon. Calculations were carried out in a historical variant and a parametric variant based on conditional volatility from the GARCH(1,1) model.

Table 3. VaR and ES estimates (historical approach)

Assets	VaR(5%)	ES(5%)	VaR(1%)	ES(1%)
BTC	-5,55%	-8,80%	-10,87%	-13,92%
ETH	-7,41%	-11,91%	-14,92%	-19,81%
EURUSD	-0,73%	-0,97%	-1,06%	-1,45%
USDPLN	-1,00%	-1,38%	-1,61%	-2,04%
SP500	-1,74%	-2,82%	-3,33%	-4,84%
WIG20	-2,10%	-3,07%	-3,33%	-5,12%

Values in the table indicate logarithmic daily loss.

Source: own elaboration.

Table 4. VaR and ES estimates in parametric terms (GARCH(1,1))

Assets	VaR(5%)	ES(5%)	VaR(1%)	ES(1%)
BTC	-7,86%	-12,95%	-14,88%	-22,62%
ETH	-11,48%	-18,42%	-21,37%	-31,78%
EURUSD	-0,82%	-1,09%	-1,25%	-1,52%
USDPLN	-1,16%	-1,51%	-1,76%	-2,12%
SP500	-1,86%	-2,86%	-3,12%	-4,28%
WIG20	-2,41%	-3,32%	-3,76%	-4,72%

Values in the table indicate the logarithmic daily loss.

Source: own elaboration based on GARCH(1,1) model estimations.

The results obtained confirm that, during the period studied, cryptocurrencies (BTC and ETH) exhibited by far the highest risk, understood as the possibility of large daily declines in value. This is evidenced by both the VaR and ES values calculated using the historical approach (Table 3) and the results of parametric estimation based on the conditional volatility of the GARCH(1,1) model (Table 4).

In the historical approach, which uses an empirical distribution of returns, ETH achieves a VaR(5%) close to -7.41% and VaR(1%) is as high as -14.92%, suggesting a significant probability of losses of several per cent on a one-day basis. Similarly high risks are observed for BTC (-5.55% and -10.87% at the respective confidence levels). For currency pairs (EUR/USD, USD/PLN), VaR indications are noticeably lower, not exceeding a few per cent, which means that on most days losses of more than -1% or -2% are rare. The market situation of the indices (S&P500 and WIG20)

in terms of VaR measures (1.7–2.1% at the 5% level and up to around 3.3% at the 1% level) ranks indirectly between cryptocurrencies and currencies.

In contrast, parametric analysis (Table 4), in which VaR and ES levels are determined based on estimated conditional volatility from GARCH(1,1) models and Student's t-distribution, further highlights the increased vulnerability of cryptocurrencies to extreme price fluctuations. In particular, Ether (ETH), with a VaR(5%) of -11.48% and an ES(5%) of over -18%, shows the greatest sensitivity to sharp price movements. The differences between the historical and parametric method in percentage terms are small for the more stable markets (e.g. EUR/USD, USD/PLN), meaning that the realistically observed return distribution is close to what the GARCH model predicts. In the case of BTC and ETH, however, the inclusion of high volatility persistence and fat tails results in higher VaR and ES values than in the historical approach.

The potential for daily high negative returns in cryptocurrency markets carries the risk of rapid and steep capital losses, which, with high turnover and shallow markets, can lead to escalating crisis phenomena. In contrast, lower, relatively stable VaR parameters in the currency segment and on the main indices indicate a lower risk of deep declines in the short term.

At the same time, it is worth emphasising that the assessment of the impact of the cryptocurrency market on the risk to financial markets cannot be conducted solely from a quantitative perspective. The regulatory aspect is also important, especially in view of the growing number of crypto-related instruments (e.g. futures contracts, ETFs) and the potential interest in the cryptocurrency market by banking sector players and investment firms. To date, however, relatively few studies have been produced that combine the rigour of statistical and econometric methods with detailed regulatory analysis, making the issue of addressing the risks arising from the increased volatility of cryptocurrencies one that requires a new, interdisciplinary approach. This article therefore includes not only an examination of the price volatility of selected cryptocurrencies and its implications for risk in financial markets, but also conducts an analysis of regulatory risk factors in the context of the current regulatory framework.

3. Regulatory risk of cryptocurrencies BTC and ETH

3.1. Introductory remarks

Regulatory risk, understood as an element of the broader category of legal risk, occupies an important place in the analysis of risks associated with cryptocurrencies. Regulatory risk is related not only to changes in the legal environment, but also includes situations where there is a lack of relevant regulations or their application is a source of interpretation problems The source of risk in this aspect is also the jurisdictional diversity, which includes different rules for carrying out transactions,

recording and settling them in the laws of different countries, as well as the potential vindication of claims (Kuźniak 2008). In order to identify regulatory risks, a normative analysis of cryptocurrencies should be carried out using the research methods of legal science. The scope of the analysis should include the juridical nature of cryptocurrencies and the legal relations of trading. The scope of analysis determined in this way directs the structure of considerations to the issues of the essence of cryptocurrencies and the normative layer, i.e. the legal solutions currently in force in this area will complement the previously conducted economic analysis with a regulatory aspect. The research method used in this layer of the study is the dogmatic-legal method consisting in the analysis of selected legal regulations. The subject of the analysis is therefore the content of the law in force as well as its interpretation conducted in doctrine and jurisprudence on the subject of assessing the regulation of cryptocurrencies, with particular emphasis on BTC and ETH. The aim of applying this method is to establish what norms are in force in the legal system what the practice of applying these norms looks like and to formulate conclusions through the prism of regulatory risk to market security. The analyses assume that the complexity of legal relations in the field of cryptocurrencies requires the application of regulatory methods belonging to different branches of law.

3.2. Regulatory issues regarding the concept of cryptocurrency

The analysis of the issue of the legal essence of cryptocurrencies such as BTC and ETH involves an intertwining of two closely related issues: the concept and its juridical nature. These issues are characterised by a rather high complexity due to their treatment as a phenomenon of the nature of digital technology, the economic sphere and also the legal sphere (Michna 2018, p. 4). However, characteristic of the cryptocurrency plane is the occurrence of regulatory deficits already at the conceptual level, which constitute a significant source of regulatory risk The reason for this state of affairs is the difficulty in the unambiguous qualification of the cryptocurrency creation process, but also the diversity of functions performed by them, including considering them in the context of money (Marshal 2019, p. 110). An additional source of difficulty in defining the concept and juridical nature of BTC and ETH is their association with a network (Bitcoin and Ethereum, respectively) that is not itself the subject of rights and obligations (Wnęk 2023, p. 37). Cryptocurrencies in legal literature are also conceptually juxtaposed with virtual currencies and digital currencies as money in virtual form (Skorupka, Urbanowicz-Sobczak, and Zawłocki 2024:856). At this point, it should be noted that the Polish legislator has not explicitly defined cryptocurrency but has formulated a legal definition of virtual currency. A relevant regulation in this regard is contained in Article 2(2)(26) of the Act of 1 March 2018 on the prevention of money laundering and terrorist financing (2018). However, this definition is not universal and was formulated for the purposes of this particular law.

Although they are a means of exchange and perform a thesesurisation function, they nevertheless lack the legal tender attribute necessary to be considered as money. By contrast, BTC and ETH can be considered private money, which is not issued by a specific entity, but created/issued (*mining*) by the network itself. Cryptocurrencies such as BTC and ETH undoubtedly perform the function of a measure of value other than money under civil law (Zacharzewski 2014, p. 1133) .

An unambiguous definition of cryptocurrencies is also not contained in the Regulation of the European Parliament and of the Council (EU) 2023/1114 of 31 May 2023 (hereinafter: MiCA Regulation) on cryptocurrency markets. The EU legislator has admittedly introduced a definition of the term 'crypto-asset', which is a digital representation of a value or right that can be transferred and stored in electronic form using distributed ledger technology or similar technology. This definition is broad and includes cryptocurrencies in the form of BTC and ETH (ESMA 2024, p. 17). The Regulation provides for three categories of assets: asset-linked tokens (so-called ARTs), e-money tokens (so-called EMTs) and cryptocurrencies other than asset-linked tokens and e-money tokens, including utility tokens. Due to the nature of BTC and ETH, in particular related to the lack of central issuer attribution, these cryptocurrencies will not be subject to the issuance obligations contained in the MICA such as apply to EMTs, ARTs or utility tokens. However, this does not mean that the trading and storage of these cryptocurrencies will not be regulated. In this aspect, the provisions of the MICA regulation related to *Crypto Asset service Providers* (CASPs) will apply. Indeed, CASP providers may provide crypto-related services by, inter alia, storing cryptoassets, operating trading platforms and managing cryptocurrency wallets on behalf of and for third parties.

It should be emphasised that the formulation of legal definitions in legal science may be fraught with risks in terms of the effectiveness and practicality of such regulation. As noted aptly in the doctrine, an overly detailed definition entails the risk that only a slight change in the algorithm or the way it functions would lead to the exclusion of a specific definition from the scope of the legal definition and thus from the scope of regulation. A general definition, on the other hand, could lead to a situation in which other virtual currencies, which should not be included in this definition (Mazur 2024, p. 205), would also have to be qualified as cryptocurrencies. In addition, new concepts are emerging to create further cryptocurrency systems based on a model similar to Bitcoin or Ethereum (Behan 2022, p. 241). However, the lack of definition of the concept of cryptocurrency in the legal sciences does not preclude the description of its exemplary characteristics (relationship to crypto technology, ease of transfer, anonymity of use and the possibility of de-anonymisation, convertibility, interchangeability, irreversibility, security, but also the manner of issuance and linkage to other values and the indication that their value is not guaranteed, their acceptance is an expression of the community's trust in the concept itself and they are stored by a decentralised distributed database system (Behan 2022, p. 242).

3.3. Directions for classifying cryptocurrencies at the regulatory level

Despite the identified definitional problems of cryptocurrencies under private law, they are the subject of legal relations of circulation. This is because freedom of contract allows parties to create legal relations in which cryptocurrency is an object of performance and may even perform a function analogous to money. Under criminal law, cryptocurrency is not treated as money, another legal tender, a document or a financial instrument. It is also not treated as a property right or an asset, nevertheless it may constitute the object of a prohibited act (Blazowska 2024, p. 153).

In civil law, the treatment of BTC and ETH as things and consequently their inclusion in the rules of legal transactions is problematic. Also other theoretical civil law concepts qualifying cryptocurrency as a property right, debt, work or financial instrument are not without doubts (Szewczyk 2018, p. 243; Wnęk 2023, pp. 55–64; Zacharzewski 2014, p. 1133). A broader discussion of the doubts relating to the jurisprudential nature of cryptocurrencies is beyond the scope of this paper, so it should be limited to stating that there is no uniform position in the legal doctrine on the jurisprudential nature of cryptocurrencies. This state of affairs fosters a multiplicity of conceptual categories and further contributes to ambiguity by making interpretation difficult.

The rulings of the judicature also do not provide a clear answer regarding the legal qualification of cryptocurrencies. All the more so as they relate to a fragment of cryptocurrency trading, which are fiscal issues. The Supreme Administrative Court, in a judgment of 12 July 2022, II FSK 3094/19, held that cryptocurrencies do not have a materialised form and are not managed by any central institution or central system, as they exist as a certain numerical value recorded in a computer system. Instead, trading in cryptocurrencies, in the court's view, is an intermediary service, where the seller acts as an intermediary between the persons making changes to the register of the bitcoin system (the so-called miners) and the person for whose benefit the change in the register is made (i.e. the 'buyer'). In another judgment of 6 March 2018, II FSK 488/16, the Supreme Administrative Court held that bitcoin in the practice of civil law relations is a type of property and in a judgment of 4 August 2022, II FSK 3150/19, it referred to the issue of possession of BTC stating that it is the possession of a cryptographic key allowing a given user to make an entry in the public register operating within the bitcoin network. On the other hand, the issues of the creation of a cryptocurrency are addressed by the judgment of the Supreme Administrative Court of 2 September 2021, II FSK 651/21, in which the court held that the process of digging a cryptocurrency is similar to the process of creating a thing or a work that is the subject of copyright. In the case of cryptocurrencies, the effect of 'digging' is to obtain a property right that did not previously exist. The case law on the qualification of cryptocurrencies is therefore not clear-cut and does not always remain consistent with the pronouncements of the doctrine of law This is an important factor generating increased regulatory risk, which may negatively affect the security of the financial market.

3.4. Regulatory risk and financial market security

Financial market security is one of the main objectives of the legislator's interference with the free functioning of trading mechanisms. This interference, in the case of the crypto-asset market, does not cover the entire market, but focuses on selected areas of its functioning, creating organisational and functional bases for trading so as to ensure a high level of their integrity. The modalities of impact take the form of different regulatory models, which either restrict access to participate in trading or regulate specific behaviours (prohibition model), or impose additional obligations on market participants related to the functioning of trading, exchange and storage platforms (organisational model). As highlighted by the EU legislator in recital 4 of the MiCA Regulation, the lack of rules in this regard exposes holders of these cryptocurrencies to risks and may cause a significant threat to market integrity. Although investments in cryptocurrencies do not fall under the prohibition model, i.e. in simpler terms they are not prohibited, they nevertheless entail far-reaching risks stemming also from the lack of legal certainty, which for the security of market trading is fundamental. BTC and ETH are not regulated at a level that makes it possible to clearly define their juridical nature, even though they are included in the broad legal category of crypto-assets. The value of both cryptocurrencies essentially refers to how much the purchaser is able to pay for them and whether they accept them as a means of performance. In addition, the link to technology makes it difficult to set boundaries to protect participants in the trading of these assets.

Regulatory certainty is an important prerequisite for the safe operation of trading. These regulations should allow for effective redress and ensure that investors are adequately protected. In this respect, a particularly high regulatory risk is revealed in its jurisdictional aspect related to the functional sphere of crypto-asset trading, i.e. the execution of transactions. The rules that are applied in one country do not necessarily apply in another (Kuźniak 2008, p. 94). In legal sciences, attention is drawn to the difficulties in determining the law governing the relations of international trading in the digital space, which lead to the formulation of the concept of a separate quasi-legal system for the sphere of digital trading, the so-called *lex crypotografica* system based on the assumption of "*code is law*" (Świerczyński 2024, p. 171). These concepts certainly only increase regulatory risk in the context of market security. This is because they create solutions that compete with traditional trade regulation instruments.

In concluding remarks on regulatory risk, it is worth noting that the lack of applicable regulations for cryptocurrencies and their price volatility were explicitly indicated in the judgment of the Supreme Administrative Court of 11 October 2023, II GSK 883/20 as their features in the context of the subject of investment. The analysis of the normative plane of cryptocurrencies therefore leads to the conclusion that the current state of regulation of BTC and ETH is a source of regulatory risk. Additional sources of this risk are the lack of a central entity issuing cryptocurrencies (for the cryptocurrencies analysed in the paper, i.e. BTC and ETH), their functioning in IT networks outside the market understood as a place of concentration of the supply and demand side, and the jurisdictional risk resulting from the lack of unambiguously

clear criteria to indicate the law applicable to the qualification and trading of cryptocurrencies The evolution of the market of cryptocurrencies requires in-depth legal research into the essence of this category of cryptocurrencies not only in the domestic dimension, but also at the level of international law.

Summary and conclusions

Cryptocurrencies, as one of the most dynamically developing forms of digital assets in the financial sector in recent years, have repeatedly demonstrated their capacity to generate significant risks for financial markets. The analyses presented in this paper, covering both traditional volatility measures and the estimation of GARCH(1,1) models with Student's t-distribution, as well as computed values of Value at Risk (VaR) and Expected Shortfall (ES), clearly show that the cryptocurrencies examined (BTC and ETH) are characterised by high volatility metrics and a susceptibility to sharp daily losses. In the historical approach, ETH exhibited VaR(1%) figures reaching several percentage points, while under the parametric approach – additionally accounting for fat-tailed return distributions – the forecasted extreme losses (ES) were even higher, exceeding -30%. Similarly elevated risk exposure of BTC confirms that both major cryptocurrencies distinctly differ from traditional financial instruments such as currency pairs (EUR/USD, USD/PLN) and stock indices (S&P500, WIG20), for which analogous VaR and ES measures are much lower.

The results obtained thus support the hypothesis that cryptocurrencies – especially in their current phase of development and with current, often ambiguous regulations – have a destabilising rather than stabilising function in financial markets, thus contributing to an increase in risk. Of key importance here is the coupling of price and regulatory risk, which undermines the predictability of market processes and decisions and, given the technological aspect of the cryptocurrencies analysed (BTC, ETH) and their international nature, makes it difficult to adopt a uniform and consistent legal framework. In the authors' opinion, with the current legal status and development dynamics of the selected cryptocurrencies, i.e. BTC and ETH, as well as in the light of the market risk analysis conducted, they should be seen as speculative instruments rather than stable assets in investment portfolios. Their high price volatility, cross-border and decentralised nature, as well as their complex legal nature exacerbated by the lack of uniformity of legal qualification in trading, hinder their effective inclusion in a single regulatory framework in the future and, for non-professional investors, represent a particular source of risk that may become the subject of numerous legal claims in the future.

It should be noted that during periods of high trading volume and low liquidity, even relatively small shifts in investor sentiment can trigger a series of sharp price swings. Although, under normal market conditions, BTC or ETH may offer some diversification benefits (due to its low correlation with the returns of traditional financial assets). Numerous studies indicate that the aforementioned stabilising effect disappears in moments of crisis. GARCH models suggest that a collapse in the cryptocurrency

market can easily propagate through volatility channels and increasing correlations between cryptoassets and equity markets and other financial market segments. If such a collapse occurs during macroeconomic stress, the rapidly increasing volatility of cryptocurrencies can accelerate capital outflows, amplifying volatility in other markets.

In addition, the analysed GARCH(1,1) models with Student's t-distribution showed that cryptocurrencies have a higher probability of extreme events, which are not accounted for by simple normal distribution assumptions. Moreover, the results showed that periods of high volatility persist for exceptionally long periods of time. These issues have obvious implications for regulatory policy and monitoring of market phenomena. The high unpredictability of cryptocurrency prices requires special attention from regulators – not only because of possible losses for individual investors – but above all because of potential feedbacks between this segment and traditional financial market segments. Furthermore, due to the peculiarities of BTC and ETH, the provisions of the MICA Regulation will only be applicable to a limited extent, thus not providing sufficient protection for investors in this market.

In conclusion, the conducted research confirms that – with the current state of development and regulatory risks – the cryptocurrency market does not fulfil a stabilising function, representing a significant source of risk, which increases especially during periods of unexpected external shocks. Thus, the further development of the cryptocurrency market will require not only the refinement and harmonisation of regulatory solutions, in order to mitigate regulatory risks, but also the continuation of research into volatility, correlation structure and the identification of potential directions of financial capital flows, in order to effectively mitigate and manage risks in financial markets.

Bibliography

Bank for International Settlements (2016). *Minimum Capital Requirements for Market Risk*. Basel Committee on Banking Supervision.

Behan A. (2022). *Virtual currencies as objects of crime*. Issue I, legal status as of 31 December 2021. Krakow: Krakow Institute of Criminal Law Foundation.

Błażowska A. (2024). *Cryptocurrencies in Polish Criminal Law*. Legal Monographs. Warsaw: Wydawnictwo C. H. Beck.

Bollerslev T. (1986). *Generalized Autoregressive Conditional Heteroskedasticity*. Journal of Econometrics, 31(3), 307–327. doi:10.1016/0304-4076(86)90063-1

Bouri E., Molnár P., Azzi G., Roubaud D., Hagfors L.I. (2017). *On the Hedge and Safe Haven Properties of Bitcoin: Is It Really More than a Diversifier?* Finance Research Letters, 20, 192–198. doi:10.1016/j.frl.2016.09.025

Canh N.P., Wongchoti U.,. Thanh S.D, Thong N.T. (2019). *Systematic Risk in Cryptocurrency Market: Evidence from DCC-MGARCH Model*. Finance Research Letters, 29, 90–100. doi:10.1016/j.frl.2019.03.011

Chu J., Chan S., Nadarajah S., Osterrieder J. (2017). *GARCH Modelling of Cryptocurrencies*. Journal of Risk and Financial Management, 10(4), 17. doi:10.3390/jrfm10040017

Cont R. (2001). *Empirical Properties of Asset Returns: Stylized Facts and Statistical Issues*. Quantitative Finance, 1(2), 223–236. doi:10.1080/713665670

Corbet S., Lucey B., Urquhart A., Yarovaya L. (2019). *Cryptocurrencies as a Financial Asset: A Systematic Analysis*. International Review of Financial Analysis, 62, 182–199. doi:10.1016/j.irfa.2018.09.003

Dyhrberg A.H. (2016). *Bitcoin, Gold and the Dollar – A GARCH Volatility Analysis*. Finance Research Letters, 16, 85–92. doi:10.1016/j.frl.2015.10.008

ESMA (2024). *Consultation Paper on the Draft Guidelines on the Conditions and Criteria for the Qualification of Crypto-Assets as Financial Instruments*.

European Central Bank (2019). *Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures*, Occasional Paper Series (223).

Financial Stability Board (2018). *Crypto-Asset Market. Potential Channels for Future Financial Stability Implications*.

Fiszeder P. (2009). *GARCH class models in empirical financial research*. Habilitation dissertation / Nicolaus Copernicus University. Torun: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.

Gandal N., Hamrick J., Moore T., Oberman T. (2018). *Price Manipulation in the Bitcoin Ecosystem*, Journal of Monetary Economics, 95, 86–96. doi:10.1016/j.jmoneco.2017.12.004

Ibrahim B.A., Elamer A.A., Alasker T.H., Mohamed M.A., Abdou H.A. (2024), *Volatility Contagion between Cryptocurrencies, Gold and Stock Markets Pre-and-during COVID-19: Evidence Using DCC-GARCH and Cascade-Correlation Network*, Financial Innovation, 10(1), 104. doi:10.1186/s40854-023-00605-z

International Monetary Fund. (2021). *COVID-19, Crypto, and Climate: Navigating Chellenging Transitions*. Global Financial Stability Report. Washington, DC.

Ji Q., Bouri E., C.K.M. Lau, Roubaud D. (2019). *Dynamic Connectedness and Integration in Cryptocurrency Markets*, International Review of Financial Analysis, 63, 257–272. doi:10.1016/j.irfa.2018.12.002

Katsiampa P. (2017). *Volatility Estimation for Bitcoin: A Comparison of GARCH Models*, Economics Letters, 158, 3–6. doi:10.1016/j.econlet.2017.06.023

Klein T., Pham Thu H., Walther T. (2018). *Bitcoin Is Not the New Gold – A Comparison of Volatility, Correlation, and Portfolio Performance*'. International Review of Financial Analysis, 59, 105–116. doi:10.1016/j.irfa.2018.07.010

Koutmos D. (2018). *Return and Volatility Spillovers among Cryptocurrencies*, Economics Letters, 173, 122–127. doi:10.1016/j.econlet.2018.10.004

Kuester K. (2005). *Value-at-Risk Prediction: A Comparison of Alternative Strategies*, Journal of Financial Econometrics, 4(1), 53–89. doi:10.1093/jjfinec/nbj002

Kuźniak K. (2008). *Zarządzanie Ryzykiem Prawnym w Przedsiębiorstwie*, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, Finanse, Bankowość, Rachunkowość, 6(1196).

Liu Y., Tsyvinski A. (2018). *Risks and Returns of Cryptocurrency*. w24877. Cambridge, MA: National Bureau of Economic Research. doi:10.3386/w24877

Marszałek P. (2019). *Cryptocurrencies – Concept, Features, Controversies*. BAS Studies, 1(57), 105–125. doi:10.31268/StudiaBAS.2019.06

Mazur Ł. (2024). 'Cryptocurrencies as a means of contractual redemption'. In *Law of electronic contracts: outline of the system*, *Legal Monographs*, edited by J. Gołaczyński. Warsaw: Wydawnictwo C. H. Beck.

McNeil A., Frey R., Embrechts P. (2005). *Quantitative Risk Management: Concepts, Techniques, and Tools*, Vol. 101.

Michna M. (2018). *Bitcoin As an Object of Civil Law Relationships*. Legal Monographs. Warsaw: C.H. Beck Publishing House.

Sajeev K.C., Afjal M. (2022), *Contagion Effect of Cryptocurrency on the Securities Market: A Study of Bitcoin Volatility Using Diagonal BEKK and DCC GARCH Models*, SN Business & Economics, 2(6), 57. doi:10.1007/s43546-022-00219-0

Skorupka J., Urbanowicz-Sobczak K., Zawłocki R. (2024). *Crimes Against Property and Economic*. 3rd edition, edited by R. Zawłocki. System Prawa Karnego / Editor-in-Chief Lech K. Paprzycki, Andrzej Marek. Warsaw: Wydawnictwo C. H. Beck : published in cooperation with the Institute of Legal Sciences of the Polish Academy of Sciences.

Smales L.A. (2021). *Volatility Spillovers among Cryptocurrencies*, Journal of Risk and Financial Management, 14(10), 493. doi:10.3390/jrfm14100493

Świerczyński M.. (2024). *Breakthrough information technologies in private international law*. Legal status as of 30.11.2023. Legal Monographs. Warsaw: Wydawnictwo C. H. Beck.

Symitsi E., Chalvatzis K.J. (2018. *Return, Volatility and Shock Spillovers of Bitcoin with Energy and Technology Companies*, Economics Letters, 170, 127–130. doi:10.1016/j.econlet.2018.06.012

Szewczyk J. (2018). *On the Civil Law Aspects of Bitcoin*. Monitor Prawniczy, (5), 243–251.

Law of 1 March 2018 on the prevention of money laundering and financing of terrorism. 2018.

Wnęk M. (2023). *The Legal Nature of Cryptocurrency*. Legal Monographs. Warsaw: Wydawnictwo C. H. Beck.

Xu, Q., Zhang Y., Zhang Z. (2021). *Tail-Risk Spillovers in Cryptocurrency Markets*, Finance Research Letters, 38, 101453. doi:10.1016/j.frl.2020.101453

Yi S., Xu Z., Wang G.-J. (2018). *Volatility Connectedness in the Cryptocurrency Market: Is Bitcoin a Dominant Cryptocurrency?*, International Review of Financial Analysis, 60, 98–114. doi:10.1016/j.irfa.2018.08.012

Zacharzewski K. (2014). *Bitcoin as a Subject of Private Law Relationships*. Monitor Prawniczy, (21), 1132–39.

DOI: 10.26354/bb.12.2.99.2025

M. Konrad Borowicz*
ORCID: 0000-0001-5088-106X
M.K.Borowicz@tilburguniversity.edu

What Crypto Risks Can Bank Take (in the EU)?

Abstract

This article examines the types of crypto-asset risks that EU banks can prudently take under the transitional regulatory regime introduced by Article 501d of CRR3 and supplemented by the EBA's draft regulatory technical standards (RTS). The analysis is grounded in the evolving EU legal framework, particularly MiCAR and CRR3, and considers how banks may engage with crypto-assets through custody, payments and trading, and issuance. It also reviews industry responses to the draft RTS and highlights key accounting challenges, especially the tension between fair value and cost models under IFRS. It concludes that while crypto offers strategic and technological opportunities for banks – particularly in custody and tokenized finance – their ability to scale such activities remains heavily constrained by prudential rules and regulatory uncertainty.

Keywords: crypto-assets, crypto custody, Capital Requirements Regulation (CRR3), Markets in Crypto Assets Regulation (MiCAR), prudential regulation, stablecoins, Basel framework

JEL codes: G21, G28, G32, O33, M41

Introduction

Banks – traditionally conservative and heavily regulated entities – are increasingly pressed to determine if and how they should participate in the crypto-asset market. But what crypto risks can banks take? This question has taken on particular relevance as regulators develop new rules to govern banks' crypto exposures. The Basel Committee for Banking Supervision (BCBS) has developed a comprehensive standard for the prudential treatment of crypto-asset exposures (BCBS 2022). In the European Union, regulators have responded with a transitional prudential regime for crypto-assets in banks, included in the latest banking regulation reforms. Notably, Regulation (EU)

* M. Konrad Borowicz – Assistant Professor, Tilburg Institute for Law, Technology and Society, Tilburg University.

2024/1623 (the Capital Requirements Regulation's "quick fix" often dubbed CRR3) introduced Article 501d, which sets out transitional provisions on the prudential treatment of crypto-asset exposures. Article 501d became applicable on 9 July 2024, meaning that from that date EU banks are subject to specific capital requirements and limits for any crypto-asset exposures they hold. This was ahead of most other CRR3 measures (which entered into force on 1 January 2025) and reflects EU regulators' desire to immediately constrain bank crypto-risk pending a full framework.

Article 501d tasks the European Banking Authority (EBA) with developing regulatory technical standards (RTS) on how banks should calculate and aggregate their crypto exposures during this transitional period. In response, on 8 January 2025 the EBA published a draft RTS on the calculation and aggregation of crypto exposure values. This draft RTS, which until recently was at the consultation stage – comments were open until 8 April 2025 – specifies detailed methodologies for categorizing crypto-assets, applying risk weights, recognizing hedges, and computing exposure values across risk types. The final version is expected to be submitted to the European Commission by 10 July 2025. Once submitted, the Commission is anticipated to adopt the RTS as a regulation, which will supplement and give technical effect to the broader requirements set out in Article 501d of CRR3.

In parallel, and adding some complexity to the regulatory landscape, the European Commission is expected – pursuant to recital 59 of CRR3 – to propose a separate legislative act by 30 June 2025 to implement the 2024 version of the BCBS standard for the prudential treatment of crypto-asset exposures. While this forthcoming proposal is likely to align with the EBA's draft RTS, its precise scope remains unknown as of May 2025. The analysis that follows is based on the draft RTS, which, although not yet adopted, offer useful insight into how a bank's risk function – illustrated here using the example of SAFE Bank – should interpret and apply prudential rules for crypto-assets during the transitional period. Throughout this article, I examine the rationale behind these rules, assess industry feedback on the draft RTS, and explore related considerations such as accounting treatment, all of which inform how banks weigh decisions to engage with crypto-asset exposures in the EU.

1. How do banks engage with crypto-assets, and why would they want to?

1.1. Modes of bank crypto-asset engagement

In EU law, the Markets in Crypto Assets Regulation (MiCAR) defines the range of possible crypto-asset engagements, which it defines as "crypto-asset services."[1] These can be categorized into: (1) custody, (2) payment and trading services,[2]

1 Article 3(1)(16).

2 These range from transmission of order on behalf of clients, through exchange of crypto-assets for funds or other crypto-assets, transfer services, to execution of orders on behalf of clients and operation of trading platforms.

(3) issuance and (4) portfolio management and advisory services. For the discussion, I will disregard (4) as it does not trigger any prudential requirements, which are the core focus of this article. Under Article 59, to perform any and all of crypto-asset services, a person must either be an authorized crypto-asset service provider or a credit institution (or another licensed provider of financial services). MiCAR thus allows credit institutions (refer to hereinafter, for simplicity, as banks) to provide these services but only if, in line with Article 60, they notify their competent authority in advance and ensures full compliance with MiCAR's conduct, prudential, and organizational requirements.

1.2. Custody

In this model, the bank acts as a custodian of crypto-assets on behalf of its clients, similar to how a traditional custody bank safeguards stocks or bonds for asset managers (Chan et al. 2007).[3] The bank does not own the crypto-assets but provides secure storage and related services, presumable leveraging specialized digital vaults or third-party custody solutions to manage and protect the private keys controlling access to these assets. When structured correctly, the crypto-assets remain the legal property of the clients (Low and Teo 2017), and the bank functions purely as a service provider – even though, as Zetzsche and Nikolakopoulou (2025) have shown, the terms of custody agreements vary enormously.

For example, if SAFE Bank's corporate client deposits 10 BTC, the Bitcoin would typically be recorded off the bank's balance sheet as a client asset. The bank might reflect this through a custodial liability or off-balance-sheet disclosure[4], depending on jurisdictional accounting practices.[5] Critically, the bank does not assume market risk from the price volatility of the crypto-asset; any gains or losses accrue solely to the client. However, the bank does take on *operational risk* – particularly cybersecurity and key management risks – and could face legal exposure if it fails to safeguard the assets appropriately. Under CRR3, the operational risk associated

[3] An alternative to the custodial model is the non-custodial or self-custody model, in which the client – not the bank – retains exclusive control over the private key and thus maintains full control over their crypto-assets. This model falls outside the scope of the regulations analyzed, as it does not constitute a service provided by a financial institution and does not generate any balance-sheet exposures or capital requirements for the bank.

[4] Staff Accounting Bulleting (SAB) 121, issued in 2022 in the U.S., required crypto custody assets to be on the balance sheet with a liability. 17 CFR Part 211. Interestingly, shortly thereafter it was rescinded through SAB 122. As Krause (2025) notes, this shift was driven by factors such as the adoption of Fair Value Accounting and the Trump administration's pro-crypto stance.

[5] Basel III requires banks to report crypto-assets held under custody within Template CAE1, providing a clear view of the volume and nature of crypto-assets for which the bank acts as custodian (Basel Committee on Banking Supervision 2024). Although these assets are off-balance-sheet, banks are still expected to disclose them in aggregate form in the narrative accompanying the CAE1 template, reinforcing transparency around the scale and scope of custodial crypto activities.

with such services my trigger Pillar 2 add-ons, if supervisors assess the bank's control framework as insufficiently mature.

The custody model also encompasses reserve assets deposited at a bank by issuers of a crypto assets, the value of which is backed by such reserve assets, such as e-money tokens (EMTs referencing the value of a single currency) or asset-referenced tokens (ARTs – a stablecoin that is not an EMT, for example, because it purports to maintain a stable value by referencing multiple currencies rather than a single currency.). MiCAR requires the issuers of such crypto assets to deposit reserve assets either with banks or investment firms authorized to provide the ancillary service of "safekeeping and administration of financial instruments for the account of clients." While such custody services fall outside of the definition of crypto-asset services under MiCAR, they can have an impact on the bank's prudential obligations. Like crypto custody, market and credit risk for the bank are limited, as the reserve assets are not held on the bank's own account, and any fluctuations in value or credit events are borne by the issuer or token holders. However, operational risk remains material – the bank must ensure the safekeeping, segregation, and availability of reserve assets at all times, particularly under stress scenarios.

Crucially, because these deposits are intended to be available on demand to support token redemptions, they may also introduce liquidity risk for the custodian bank. When assessing the liquidity risk profile of deposits received from stablecoin issuers, regulators and banks must consider both the behavioral characteristics of these deposits and the operational role they serve. Under the liquidity coverage ratio (LCR) framework, there may be grounds to classify such deposits similarly to those from other financial institutions, given the nature of the depositor and the potential volatility of the balances (Coste 2024). Specifically, deposits from stablecoin issuers – used to back the issuance of EMTs or ARTs – could be characterized either as: (i) operational deposits from financial institutions, where the deposit supports clearing, custody, or cash management services provided by the bank, or (ii) non-operational deposits from financial institutions, which are generally assumed to be more volatile and subject to higher outflow rates under the LCR (Coste 2024).

The appropriate classification depends on the underlying contractual arrangements and the degree of operational integration between the issuer and the bank. For example, if the reserve account is used solely for regulatory segregation without supporting additional operational services, it may be more appropriate to treat it as non-operational, attracting a higher assumed outflow rate. Conversely, if the bank is providing broader transactional services to the stablecoin issuer, an operational deposit classification may be justified – potentially resulting in a lower outflow rate for LCR purposes.

In either case, the key consideration for risk and treasury teams is that these deposits are potentially unstable, especially during periods of market stress or redemption pressure. Supervisors may therefore expect banks to hold high-quality liquid assets against these liabilities and demonstrate that they have adequate liquidity buffers to accommodate sudden outflows linked to stablecoin redemptions.

1.3. Payment and trading services

Banks may take incremental steps toward the intermediation of crypto-asset transactions, starting with services that most closely resemble traditional payment activities. Among these, the most accessible initial offerings are likely to be the exchange of crypto-assets for funds or other crypto-assets, and the transfer of crypto-assets on behalf of clients. These functions – permitted under MiCAR – are operationally comparable to fiat currency conversion and payment initiation. They can be structured in ways that limit the bank's direct exposure to crypto-assets, particularly where transactions are client-driven and settled on a delivery-versus-payment basis.

As banks gain confidence and build internal capabilities, a natural progression is to expand into the reception and transmission of client trading orders,[6] and ultimately, the execution of those orders. In the reception and transmission model, the bank forwards a client's instruction to a third-party trading venue – such as a MiCAR-registered crypto exchange or broker – without executing the trade itself. This is a relatively low-risk, off-balance-sheet service that avoids proprietary exposure and is therefore considered a conservative entry point for banks exploring crypto-asset markets under MiCAR.

However, once a bank begins offering exchange, transfer, or execution services, it may start to incur on-balance-sheet exposures, depending on how those services are delivered. For example, if SAFE Bank facilitates the exchange of crypto-assets for euros or transfers tokens on behalf of clients using its own wallet infrastructure, it may temporarily hold either fiat or crypto-assets during the settlement process. Similarly, if the bank uses its own liquidity to fulfill an execution order – such as pre-funding a trade or facilitating internal matching – these positions may qualify as exposures under CRR3, with corresponding capital requirements.

Where these exposures are short-term and linked to client facilitation or market-making, they are generally booked in the trading book and must be capitalized under the revised market risk framework,[7] as adapted for crypto-assets. If the exposures are held longer-term – such as for settlement or reserve management purposes – they may fall into the banking book, attracting capital charges under the credit risk framework.[8] In either case, the regulatory expectation is clear: as banks

[6] MICAR, Article 3(1)(9)(g). In 2024, Deutsche Bank has been reported to expand its partnership with Austrian fintech unicorn and cryptocurrency exchange Bitpanda, granting the bank's clients the ability to deposit or withdraw their fiat currencies from Bitpanda through Deutsche Bank accounts (Montager 2024).

[7] Banks must also calculate the counterparty credit risk charge for over-the-counter (OTC) derivatives, repo-style and other transactions booked in the trading book, separate from the capital requirement for market risk. Basel Framework, CRE55, available at https://www.bis.org/basel_framework/chapter/CRE/55.htm.

[8] To mitigate risk and regulatory burden, banks will often seek to structure these services so that settlement occurs on a delivery-versus-payment (DvP) basis, with pre-funded accounts or trusted intermediaries reducing or eliminating counterparty credit exposure. When structured in this way, and if the bank does not retain inventory or take principal risk, the resulting exposures may be minimal or temporary, and the associated capital requirements correspondingly low.

expand their crypto service offerings beyond pure intermediation, they must assess how each activity impacts their prudential metrics and ensure that the relevant capital, liquidity, and risk governance requirements are fully integrated into their operational model.

1.4. Issuance

MiCAR also allows banks to issue crypto-assets, specifically either EMT (Article 48(1)(a)) or ART (Article 16(1)(b)). If a bank – such as SAFE Bank – were to issue either an EMT or an ART, it would assume the role of guarantor of the token's value, much like an e-money institution issuing e-money in exchange for the receipt of funds. In this context, it is important to note that MiCAR requires issuers of EMTs and ARTs to fully back (cover) the value of issued tokens with reserve assets on a 1:1 basis, explicitly ruling out the possibility of employing a fractional reserve model. The reserve assets backing the tokens – held on balance sheet but legally segregated – must be capitalized according to their risk weights under CRR3. For example, cash held at a central bank would receive a 0% risk weight, while deposits with commercial banks or non-sovereign bonds may attract higher charges.

Furthermore, these reserve assets contribute to the leverage ratio exposure measure and may affect the bank's LCR and Net Stable Funding Ratio (NSFR), especially given the EMT's and ART's redeemable-on-demand nature. Crucially, the issuance of such tokens does not trigger *new* capital, LCR or NSFR requirements as SAFE bank to the extent reserve assets comprise an existing pool of SAFE Bank's assets. When the issuer of an EMT or an ART is a bank, as Coste (2024) notes, the bank has no change in the total amount of assets it holds, only a change in the structure of its liabilities.

Beyond these Pillar 1 considerations, supervisors may also assess Pillar 2 capital requirements, particularly where EMT or ART issuance introduces material operational, liquidity, or reputational risk. For example, the bank must ensure that it can meet large-scale redemptions under stress. To that end, MiCA requires banks to develop robust redemption and recovery plans, for EMT, under Article 55 and, for ART Article 46 (recovery) and 47 (redemption), outlining how reserves would be liquidated and token holders made whole in the event of market disruption or insolvency. The EBA has issued accompanying guidelines (2024/13) on orderly redemption planning, essentially requiring banks to prepare a "stablecoin living will" to protect token holders and preserve financial stability.

Banks can also issue tokenized securities – for instance, a digital bond issued as a blockchain-native token rather than through a traditional securities depository. From a prudential standpoint, the key consideration is that the tokenized form does not alter the underlying economic characteristics of the instrument. As long as the token represents a traditional financial instrument (e.g., a debt security issued under standard legal terms), its treatment under CRR/CRD remains the same as its conventional equivalent.

Each of these three modes crypto-asset engagements can entail different on-balance-sheet exposures. Pure custody might keep crypto off the balance sheet but requires disclosure; trading and settlement on behalf of client will put some assets on balance sheet; token issuance does not create any new assets on the balance sheet but acceptance of reserve assets on deposit creates new liabilities. The EBA's draft RTS and CRR3 Article 501d are primarily concerned with *exposures* – i.e., where the bank itself is at risk from crypto-asset value changes or counterparty defaults. In our scenario, SAFE Bank's relevant exposures would include any crypto-assets it owns under the trading or banking book (like the BTC inventory), any credit exposures to counterparties in crypto trades on behalf of clients, and reserve assets for the stablecoins it has accepted on deposit.

1.5. Business case for banks: opportunities vs. risks

Why would SAFE Bank even consider getting into such a complicated and risk-fraught business as crypto services? First, there is growing demand from certain client segments – high-net-worth individuals, institutional investors, corporates dealing with blockchain projects – for custody and banking services related to crypto. Banks fear that if they do not offer these services, clients will turn to alternative providers (such as fintech companies or foreign banks). For example, SAFE Bank's wealth management clients might already be buying Bitcoin through crypto exchanges; by offering an in-house custody solution, SAFE could keep those assets within its ecosystem, earning fees and deepening the client relationship.

Second, crypto services can be fee-driven. Custody can generate safekeeping fees; trading services earn commissions or spreads; tokenization could lead to investment banking fees. If the crypto market grows, this could be a new stream of non-interest income. Some banks also see the possibility of market-making in crypto or offering crypto-structured products to clients, which come with trading profits and arrangement fees.

Third, beyond immediate revenue, banks have a strategic interest in blockchain and digital assets. Many in the industry believe that finance is gradually tokenizing – e.g., securities and even currencies might largely operate on distributed ledgers in the future. Being involved early allows a bank to build expertise and technology. For instance, by mastering how to custody crypto, SAFE Bank also builds capability to custody future central bank digital currencies (CBDCs) or tokenized stocks. There's a first-mover advantage argument: a bank that successfully integrates crypto could become a leader in the next generation of financial services, whereas those that abstain entirely might struggle if and when digital assets become mainstream.

Finally, some banks are exploring crypto (particularly stablecoins or blockchain networks) to improve payment and settlement efficiency. International payments using a well-designed stablecoin or blockchain can be faster and cheaper than legacy correspondent banking. A bank might not necessarily take on significant

crypto holdings to use these benefits – it could simply use the technology – but in practice to use, say, a USD stablecoin, the bank has to hold some of that stablecoin and interact with its issuer. The business case here is operational improvement and potentially offering near real-time cross-border payments as a product.

However, against these potential upsides, the profitability of banks' crypto ventures remains highly uncertain and likely low in the short term. Several reasons contribute to this skepticism. First, as I will detail in the next section, the prudential treatment of crypto exposures can be punitive. Compliance costs are also significant – banks need robust anti-money laundering (AML) controls for crypto transactions, monitoring systems for blockchain activity, new IT infrastructure, and training for staff. All these investments may not be justified by the small scale of revenues from an emerging market[9].

Second, it's not guaranteed that mainstream bank clients will flock to bank-provided crypto services at prices that make it profitable. Many crypto enthusiasts prefer self-custody or using specialized crypto firms. On the flip side, risk-averse bank clients might not be interested in crypto at all. So banks could find either low uptake or that they are competing against crypto-native companies with lower cost structures.

Third, offering crypto services exposes banks to risks that can lead directly to financial loss – for example, a cyber breach resulting in theft of crypto-assets might cost the bank money (either directly if its own assets are stolen or via liability to clients). Unlike traditional assets where infrastructures and legal frameworks are well-established (e.g., theft of stocks from a custodian is extremely rare and usually insured), crypto is a newer domain. Banks may need to spend heavily on technology and insurance to mitigate these risks, further cutting into any profits.

Finally, the evolving regulatory landscape itself is a risk. Banks could invest in setting up a crypto trading desk only to find regulations tighten further, or conversely invest in capabilities that become redundant if regulation shifts in favor of a different model (for example, if central bank digital currencies reduce the need for private stablecoins).

In conclusion, while banks do have plausible reasons to engage with crypto – client demand, new business lines, staying future-proof – the actual profitability of such ventures is highly uncertain and likely low under current conditions. As we move to the next sections, which detail the regulatory capital requirements, it will become even clearer why only a very measured exposure to crypto may be feasible. In the case of SAFE Bank, suppose the bank's strategy team forecast €5 million in

[9] With respect to EMT issuance, adherence to MiCAR's rules on full reserve backing and redemption rights means the bank is converting some of its funding into a narrow, ring-fenced structure: it raises funds via stablecoin issuance and must hold those funds in cash and high-grade bonds. This could be viable for offering new digital payment instruments to clients or for on-chain settlement use cases, but it limits the bank's ability to use those funds for lending. From a profitability standpoint, an issuing bank might earn a small return on the reserve assets (e.g. interest on bonds) but cannot pay interest to stablecoin holders, meaning the business model resembles a utility (like a payments service) rather than a traditional spread-lending approach.

annual fees from a new crypto service. The risk team would weigh that against the potential capital charge: if SAFE needs to allocate, say, €50 million of capital to back the exposures and operational risks, and hold perhaps another few million for operational risk, the return on that capital might be quite unattractive. Moreover, if a single incident or market crash could wipe out several years' worth of fees, the risk/reward calculus might suggest that the bank *cannot take* much crypto risk at all without endangering its safety and soundness standards.

2. Prudential treatment of crypto under CRR3

With an understanding of why a bank might limit its crypto activities, we now turn to the crux of the regulatory constraints: the prudential rules that determine how crypto exposures are treated for capital and risk management purposes. The European Union has moved swiftly to impose an interim regime via CRR3's Article 501d, acknowledging in recital 59 that a fully fleshed-out framework will take a few more years to implement. In this section, I explain the transitional prudential framework in place from 2024 onward, focusing on, first, the categories of crypto exposures defined in Article 501d(2) and, second, the specific capital requirements (risk weights and limits) attached to each.

2.1. Categories of crypto-asset exposures under Article 501d(2)

Article 501d(2) CRR3 breaks down crypto-asset exposures into three main categories, aligned largely with the types of crypto-assets defined in MiCAR: (1) tokenized traditional assets, (2) asset-referenced tokens and (3) other crypto-assets.

2.2. Tokenized traditional assets (Article 501d(2)(a))

These are crypto-assets that represent traditional assets. In simpler terms, if an asset exists on a blockchain but its value is derived from or backed by a non-crypto asset (e.g. a share, a bond, a commodity, or a *single* fiat currency), it falls under this category, provided it doesn't depend on other crypto-assets for value. This includes things like security tokens (digital representations of stocks or bonds) and EMTs. The regulatory logic here is that the risk of these exposures should mirror the risk of the traditional asset they represent. For example, if SAFE Bank holds a token that represents a sovereign bond, the primary risk is that (credit) of the issuer, not something fundamentally new.

2.3. Asset-referenced tokens (Article 501d(2)(b))

ARTs under MiCAR are essentially stablecoins or similar tokens that maintain a stable value by referencing a pool of assets, which can include fiat currencies, or commodities. Examples: a stablecoin backed by a mixture of cash and government bonds, or a token pegged to gold (with physical gold in reserve). The prudential treatment for banks' exposures to such ARTs is meant to be less strict than for completely unbacked crypto, but (as we'll see) still significantly more conservative than treating them like the actual underlying assets.

2.4. Other crypto assets (Article 501d(2)(c))

This is the catch-all category. It includes all crypto-assets that are *not* covered by (a) or (b). In essence, this means cryptocurrencies with no intrinsic backing (like Bitcoin, Ether, etc.), utility tokens, and any exotic crypto assets, as well as any asset-referenced tokens or EMTs or ARTs that *fail* certain criteria (e.g., perhaps an EMT issued by a non-compliant firm, or an ART that references crypto instead of traditional assets). As noted, even some tokens that would otherwise be (a) or (b) drop into (c) if they depend on crypto for value or are non-compliant. The EU regulators clearly view this category as the riskiest, since it captures volatile, speculative assets.

2.5. Capital requirements and exposure limits in the transitional regime

Under Article 501d's transitional provisions (effective July 2024 onwards), the classification described above directly translates into capital charges and quantitative constraints for banks.

2.6. Tokenized traditional assets (Article 501d(2)(a))

As mentioned, these are treated as exposures to the underlying assets. If the underlying is a cash claim or a traditional security, existing CRR2 rules for credit, market, and counterparty risk apply. In practice, if SAFE holds a tokenized government bond within its trading or banking book, the risk weight is the same as if SAFE held the actual bond (so if it's a high-quality sovereign, likely a 0% or low risk weight).

A similar treatment would apply to an EMT issued by a AAA-rated bank. In this case, holding the EMT is economically equivalent to holding a deposit balance with the issuer, fully redeemable at par in fiat currency. If the EMT meets all MiCA classification criteria – including full reserve backing, legal redemption rights, and transparency – the bank's exposure to the token could be treated as a deposit

with a AAA-rated bank, likely attracting a 20% or lower risk weight, depending on maturity.

However, the bank must also consider whether the holding introduces market or counterparty risk, depending on how the tokenized asset is structured and used. If the token is held in the trading book and is subject to fair value fluctuations, it may give rise to market risk under the trading book rules – especially if it is actively traded or valued mark-to-market. This would typically apply to tokenized securities whose prices vary in response to interest rates, credit spreads, or liquidity factors, even if the underlying asset is conventional.

In addition, counterparty credit risk may arise if the tokenized asset involves contractual settlement with a third party, such as through smart contracts or when exposures are cleared or margined via an intermediary. For example, if the token is held through a bilateral or centrally cleared structure involving deferred settlement or collateralized margining, then the bank must calculate exposure-at-default under the standard counterparty credit risk rules, as it would for any other OTC financial instrument.

2.7. Asset-referenced tokens (Article 501d(2)(b))

According to Article 2 of the EBA draft RTS, exposures to such ARTs (assuming the issuer complies with MiCAR, etc.) should be given a 250% risk weight for credit risk. This applies to banking book exposures (like if held as an investment or loan equivalent) and also informs the default treatment for trading book if not otherwise specified. Notably, as Häring, Ruof, and Blemus (2025) pointed out, the draft RTS ignores paragraphs 60.32 and 60.33 of the Basel framework, which allowed banks to *look through* to the backing assets to determine capital. For instance, if an ART was 100% backed by multi-currency deposit balances kept at a AAA-rated bank, depending on the specific terms of the custody arrangement, the risk should be akin to a deposit balance with that institution (low risk weight). EU, in transitional 501d, did not adopt that nuanced approach, arguably *overweighting* the risk of ARTs.

The draft RTS indicates in recital 25 that for market risk on ARTs, until the EU implements the new Fundamental Review of the Trading Book approach, banks should use the existing simplified standardized approach for market risk.

2.8. Other crypto assets (Article 501d(2)(c))

This is where the strictest rules apply. There are two key components: (i) a 1250% risk weight for credit risk (and by extension, a similar capital charge for other risk types if not otherwise covered), and (ii) an aggregate exposure limit of 1% of Tier 1 capital for all such exposures combined. What does 1250% risk weight mean in practice? It is effectively the maximum risk weight under CRR3 – it corresponds to

a capital requirement equal to the exposure value. In other words, *if using an 8% minimum ratio*, for every €100 of a category (c) exposure, SAFE Bank must hold €100 of capital because (100 × 12.5) × 0.08=100. This is akin to treating the exposure as if it were deducted from capital. The logic is that such crypto-assets are so volatile and potentially capable of total loss that the bank should not be leveraged against them at all – every euro exposure should be backed by a euro of capital, ensuring the bank could theoretically absorb a total wipeout.

For market risk, the draft RTS Article 3(4) allows a "Risk-Types Approach" for some of these point (c) exposures, but only if they meet certain criteria. If those criteria are not met, 1250% applies. The second component, the 1% Tier 1 limit, is crucial. Article 501d(3) of CRR3 (and mirrored in Basel's standard) says that a bank's total exposure to these "other crypto-assets" must not exceed 1% of its Tier 1 capital, and they shall be calculated on a net basis as specified by EBA.

To connect this to the overarching question – *what crypto risks can banks take?* – the answer from this regulatory section appears to be, not too surprisingly: only very limited and heavily capitalized risks. Under these [transitional] rules, a bank can engage with crypto in forms that mimic traditional assets (tokenized bonds, EMTs etc.) without extra capital, but that's not really new risk. For anything else (ARTs, other crypto-assets), the bank can take on some exposure but must equity-fund it and cannot let it grow beyond a trivial slice of its balance sheet (1% of Tier 1 is typically far less than 1% of assets; e.g., if Tier 1 ratio is 15%, 1% of Tier 1 is 0.15% of assets – a tiny slice). This essentially limits banks to a toe-hold in crypto to serve niche client needs primarily in the area of custody and, perhaps, payments.

The next part of the article will consider the reactions from the industry to these requirements and proposals – gleaned from the 2025 consultation responses.

3. Industry response to the EBA's draft RTS

This section offers a focused review of the responses submitted during the EBA's public consultation, which concluded in April 2025, with particular attention to how the broader industry – rather than the banking sector specifically – has responded to the draft proposals. With the notable exceptions of Fédération Bancaire Française (FBF), Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken (BDVR) and the European Association of Co-Operative Banks (EACB), none of the major national banking federations, pan-European banking associations, or individual banks submitted comments on the draft RTS. This absence may reflect limited engagement or capacity, or perhaps a strategic disengagement, particularly as some in the banking sector view crypto-assets – especially stablecoins – as a competitive threat to core banking services. In contrast, responses came primarily from crypto firms, trading venues, and market infrastructure providers. These are stakeholders more directly exposed to crypto markets and therefore more immediately affected by regulatory design.

Despite this, the feedback provides useful insight into how the industry – particularly market-facing participants – interprets the EBA's draft. Most respondents welcomed the EBA's effort to clarify and operationalize the Basel crypto-asset framework in the EU and broadly supported the goal of harmonization with international standards. However, the tone of the feedback was largely critical of specific features of the draft RTS, in particular the proposed 1% aggregate exposure limit. Industry associations – including the Association for Financial Markets in Europe (AFME) (AFME 2025, 1) – noted that the cap could unintentionally stifle low-risk, regulated activities, such as payments. Several respondents suggested that the 1% limit should be recalibrated over time, or at least include exemptions for low-risk and fully collateralized exposures, particularly where banks are not bearing underlying crypto price risk.

A related concern was the EBA's failure to explicitly permit netting of long and short crypto-asset positions when calculating exposures toward the aggregate limit. Respondents noted that Article 501d(5) of the CRR mandates the EBA to specify how to aggregate exposures, yet the draft RTS was silent on whether hedged positions could be offset. (AFME 2025, 2) emphasized that net exposures, not gross, should count toward the 1% Tier 1 capital limit. Without the ability to offset long and short positions, particularly those entered into for risk management purposes, the exposure metric becomes overly conservative and inconsistent with market risk principles applied elsewhere in the CRR framework.

Another area of concern was the treatment of client clearing exposures. In this context, client clearing refers to a service where the bank facilitates the clearing and settlement of crypto-asset derivative transactions on behalf of its clients – similar to providing execution, transfer, or post-trade services – but does not itself take a directional position in the underlying crypto-assets. The bank's role is limited to ensuring the client's trade is properly processed and risk-managed, often backed by initial and variation margin as well as participation in a default fund, which collectively mitigate the bank's exposure to client defaults. and Futures Industry Associations (FIA) (FIA 2025, 1–3) emphasized that, because the economic risk resides with the client and is already covered under the counterparty credit risk and large exposure frameworks, including these exposures in the crypto limit would amount to regulatory double-counting and unnecessarily constrain central clearing activities.

Finally, where the EBA offered policy options, industry respondents clearly preferred approaches that align with existing CRR frameworks over bespoke crypto-specific treatments. For example, the draft RTS proposed two alternatives for assigning risk weights to crypto derivative counterparties: either apply a flat 250% risk weight, or apply the standard risk weight of the counterparty, as used in the general CCR framework. Respondents – including FBF, BDVR, AFME and EACB – overwhelmingly favored the latter, arguing that it is more risk-sensitive and consistent with the principle of regulatory neutrality – i.e., same risk, same treatment. FBF and others emphasized that the 250% flat rate has no basis in the

Basel framework, and its inclusion would introduce unjustified conservatism and divergence from international norms. In general, the desire for full alignment with the Basel standard – and against EU-specific overlays – was a recurring theme across submissions.

4. Crypto valuation and accounting challenges

A bank's risk assessment is only as good as its measurement of exposures, and that in turn relies heavily on both accounting values and fair value determinations (Barth, Hodder, and Stubben 2008). Accurate exposure measurement ensures that risk managers have a clear picture of a bank's financial vulnerabilities, enabling them to allocate capital appropriately and maintain effective internal controls. However, crypto-assets present significant challenges in this context because they do not fit neatly into traditional accounting categories (Sterley 2019). There is currently no specific International Financial Reporting Standard (IFRS) fully tailored to crypto-assets. In practice, most standard-setters have concluded that cryptocurrencies (and similar digital assets) do not qualify as cash or cash equivalents, financial instruments, or inventory (except in certain cases for brokers) (Parrondo 2023). Consequently, under IFRS, in line with the 2019 decision of IFRS Interpretation Committee, the default treatment for crypto-assets has been to classify them as intangible assets (IFRS-IC, Holdings of cryptocurrencies 2019).

Under IFRS-IAS 38, banks have two models available for measuring intangible assets such as crypto-assets: the cost model and the revaluation model (IFRS – IAS 38 Intangible Assets 2025). With the cost model, crypto-assets are recorded at their initial acquisition cost and are subsequently carried at that value, less any impairment losses. This approach is conservative; even if market prices for crypto-assets fluctuate significantly, the balance sheet value remains unchanged until a decline is recognized through impairment. For example, if a bank acquires 10 Bitcoins at a given price, that historical cost will continue to represent the asset's value until a market downturn triggers an impairment loss. While this provides stability, it may result in a disconnect between the recorded value and the asset's current market risk.

Alternatively, the revaluation model allows banks to carry intangible assets at a revalued amount, provided an active market exists for those assets. Under this model, IFRS requires the use of IFRS 13 Fair Value Measurement to determine the current market value of crypto-assets. An active market is one in which there is sufficient trading frequency, liquidity, and observable price data (Palea and Maino 2013). When an active market is present, crypto-assets can be periodically revalued so that their carrying amounts on the balance sheet reflect current market conditions. This approach leads to greater transparency by more accurately mirroring the true economic risk of the crypto-assets. However, it also introduces earnings volatility and requires the bank to exercise significant judgment in determining whether

an active market exists for each cryptocurrency, as this decision may vary from one digital asset to another.

Under the draft RTS Article 1, MiCAR-compliant crypto-assets are included within the scope of the prudent valuation rules. This means that, for regulatory capital purposes, banks must apply additional valuation adjustments to such assets. Whether a bank uses the cost model or the revaluation model, these prudent valuation adjustments help ensure that the risk weightings assigned to crypto-assets are appropriate given their current market risk. The cost model tends to understate the dynamic market risk because it does not reflect real-time changes, forcing banks to rely on internal mark-to-market systems to supplement their risk assessments. The revaluation model, by contrast, allows banks to incorporate current market data directly, albeit at the cost of increased volatility in reported earnings.

Incidentally, the issue of prudential valuation rules was one of the features of the draft RTS that received considerable pushback from the industry. The view of respondents – including FBF, AFME and EACB – was that, at least with respect to EMTs and ART, the rules for exposures are sufficiently prudent and an additional margin of conservatism, such as the prudent valuation adjustment, seems excessive.

Conclusion

This article answered the question what crypto risks banks can take in the EU. Under the transitional framework, banks can take only carefully circumscribed and well-capitalized crypto risks. In the EU, this reflects a deliberate regulatory choice: crypto-assets – particularly unbacked or highly volatile ones – are treated as high-risk exposures subject to stringent capital, liquidity, and operational constraints. The rules under CRR3 and the EBA's draft RTS impose 1250% risk weights on most unbacked crypto-assets and a 1% Tier 1 capital cap on total exposure, effectively limiting banks to only minor positions – if any – unless those positions are hedged, fully collateralized, or supported by offsetting controls. From an internal risk perspective, crypto is allowed, but only in tiny, contained, and fully buffered quantities. The rationale is clear: any bank activity involving volatile crypto-assets must be ring-fenced, risk-mitigated, and subject to real-time oversight.

From a bank's perspective, the strategic value of such tightly controlled activity lies not in short-term profit, but in preparing for future opportunities. For now, most banks are treating crypto as an experimental domain – offering client custody or facilitating access while keeping proprietary exposure negligible. Yet the regulatory framework is evolving in anticipation of more institutional involvement. The design of CRR3, along with MiCA's treatment of stablecoins, assumes that banks will eventually play a larger role in issuing and handling tokenized assets, particularly those that resemble traditional financial instruments. The most promising near-term opportunity lies in tokenized traditional assets – such as digital bonds, tokenized deposits, or syndicated loans on private blockchains – which can be

treated under CRR3 as their conventional equivalents. These assets offer the benefits of DLT (efficiency, programmability, faster settlement) without exposing the bank to new types of market risk.

In contrast, stablecoins represent a middle ground: familiar in function but novel in structure. MiCA opens the door for banks to issue EMTs and ARTs, provided they meet strict backing and redemption requirements. For credit institutions, the existing CRR/CRD capital framework applies, but supervisors may still impose additional Pillar 2 capital buffers to reflect liquidity and operational risks. While the capital cost may be lower than for unbacked crypto-assets, issuing a stablecoin or accepting in custody reserve assets from another stablecoin issuer still requires careful reserve management, redemption planning, and technological oversight. Still, this category may prove strategically important in the long run – particularly if stablecoins become widely used in payments, settlement, or wholesale finance.

While the EU moves forward with implementing the Basel crypto-asset framework through MiCA and CRR3, it is worth noting that regulatory developments in the United States are progressing along a different but parallel path. U.S. banking regulators – primarily the Federal Reserve, OCC, and FDIC – have taken a cautious, supervisory-led approach to crypto-asset exposures, emphasizing safety and soundness over formal rulemaking. Notably, there is no finalized prudential framework for crypto-assets equivalent to the EU's RTS under Article 501d CRR. However, U.S. authorities have issued a series of policy statements, interpretive guidance, and supervisory procedures, including the Federal Reserve's supervisory nonobjection process for banks engaging in crypto activities.

As global regulators continue to converge around the Basel Committee's standards, the divergence in implementation timelines and methods – particularly between the EU and the U.S. – may create regulatory fragmentation, posing challenges for internationally active banks and financial institutions more generally. Respondents to the EBA consultation on the draft RTS – such as Deutsche Börse Group (2025) – highlighted the risk of regulatory fragmentation. While this underscores the value of ongoing cross-jurisdictional dialogue and coordination, the prospect of achieving a truly globally coherent approach to crypto prudential regulation may be increasingly unrealistic in today's fractured geopolitical landscape. In such an environment, regulatory divergence may prove more likely than convergence, challenging efforts to maintain consistency across major financial jurisdictions.

Bibliography

AFME (2025). "AFME Response to EBA CP RTS on the Calculation and Aggregation of Crypto Exposure." (May 1, 2025).

Barth M.E., Hodder L.D., Stubben S.R. (2008). *Fair Value Accounting for Liabilities and Own Credit Risk*, The Accounting Review, 83(3), 629–664. doi:10.2308/accr.2008.83.3.629

Basel Committee for Banking Supervision (2022). *Prudential Treatment of Cryptoasset Exposures*. https://www.bis.org/bcbs/publ/d545.htm (April 15, 2025).

Basel Committee on Banking Supervision (2024). "Disclosure of Cryptoasset Exposures."

Chan D., Fontan F., Rosati S., Russo D. (2007). "The Securities Custody Industry".

Coste C.-E. (2024). *Toss a Stablecoin to Your Banker – Stablecoins' Impact on Banks' Balance Sheets and Prudential Ratios*. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op353~11120d3428.en.pdf (May 1, 2025).

Deutsche Börse Group (2025). *Response to Consultation on Regulatory Technical Standards on the Calculation and Aggregation of Crypto Exposure Values* (May 1, 2025).

FIA (2025). *FIA Response to EBA CP on Bank Exposures to Crypto Assets* (May 1, 2025).

Häring W., Ruof C., Blemus S. (2025). "CRR III – Prudential Treatment of Crypto Exposures." *White & Case LLP | Insight Alert*. https://www.whitecase.com/insight-alert/crr-iii-prudential-treatment-crypto-exposures (May 1, 2025).

"IFRS – Holdings of Cryptocurrencies" (2019).

"IFRS – IAS 38 Intangible Assets." 2025. https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/ (May 1, 2025).

Krause D. (2025). *The Repeal of SAB 121: A Turning Point in Cryptocurrency Regulation and Accounting*. doi:10.2139/ssrn.5115080

Low K.F.K., Teo E.G.S. (2017). *Bitcoins and Other Cryptocurrencies as Property?*, Law, Innovation and Technology, vol. 9, issue 2. https://www.tandfonline.com/doi/abs/10.1080/17579961.2017.1377915 (April 15, 2025).

Montager D. (2024). *Banks Explore Crypto Partnerships in New Trend*. The Banker. https://www.thebanker.com/content/82871244-634a-5646-9d7e-09360e5a799b (April 15, 2025).

Palea V., Maino R. (2013). *Private Equity Fair Value Measurement: A Critical Perspective on IFRS 13*, Australian Accounting Review, 23(3), 264–278. doi:10.1111/auar.12018

Parrondo L. (2023). *Cryptoassets: Definitions and Accounting Treatment under the Current International Financial Reporting Standards Framework*, Intelligent Systems in Accounting, Finance and Management, 30(4), 208–227. doi:10.1002/isaf.1543

Sterley A. (2019). *Cryptoassets: Accounting for an Emerging Asset*, The CPA Journal; New York 89(6), 6–7.

Zetzsche D., Nikolakopoulou A. (2025). *Crypto Custody: An Empirical Assessment*, Journal of Financial Regulation: fjaf004. doi:10.1093/jfr/fjaf004

Safe Bank 2(99) 2025

DOI: 10.26354/bb.13.2.99.2025

Adrian Rycerski*
ORCID: 0000-0002-4673-0450
arycerski@swps.edu.pl

Protection of Clients Receiving Advice on Crypto-Assets (MiCAR) – Comparative Remarks in the Context of the MiFID II Regulatory Package

Abstract

Crypto-assets are the subject of considerable controversy, both in terms of their valuation (valuation methods) and the numerous risks they pose to investors. The crypto-asset market is unfortunately known for speculation, high price volatility, manipulation, and sophisticated marketing techniques. Providing advice under such conditions therefore entails significant and multifaceted risk. For this reason, the service of crypto-asset advisory may and should attract attention – particularly in relation to the mechanisms for protecting clients using this service and the potential civil liability of entities providing it.

The Regulation on Markets in Crypto-Assets (MiCAR) introduces a legal framework for the provision of crypto-asset advisory services. As a rule, the provision of this service requires authorization from the Polish Financial Supervision Authority (KNF), after first convincing the supervisory authority that the legal requirements – especially those aimed at client protection – are met. These requirements, along with the specific nature of the advisory subject (i.e., crypto-assets), call for deeper reflection on the proposed, expected, theoretical, and practical dimensions of this service.

However, in order to have a meaningful and informed discussion about crypto-asset advisory services, it is necessary to compare this service with investment advisory services as defined in Directive 2014/65/EU (MiFID II). Investment advice under MiFID II has a long-standing tradition – one that not only should, but must, be drawn upon. This comparison will help illustrate the specific nature of crypto-asset advisory and lead to the identification of the key obligations associated with its provision. Highlighting the key issues in crypto-asset advisory should help us understand what lies ahead for financial market participants in just a few months.

* Adrian Rycerski – PhD, Assistant Professor at SWPS University, an advocate, Certified Cryptoasset Anti-Financial Crime Specialist (ACAMS), Certificate of Advisor in MTF holder (no. 18/2015).

Keywords: advice, cryptoassets, MiCAR, MiFID II

JEL codes: K22

Introduction

Regulation 2023/1114 on markets in crypto-assets (hereinafter: 'MiCAR')[1] created a legal framework for, among other things, the service of providing advice on crypto-assets. Ever since the date of application of MiCAR, the provision of that service has been subject to authorisation by the competent supervisory authority[2] granted after a prior demonstration of compliance with a number of requirements, including organisational, regulatory and personnel ones, all with the aim of ensuring that clients are adequately protected. These requirements and the complex, and sometimes even controversial, specificity of the subject matter of providing advice (on crypto-currency) prompt a deeper reflection on the postulated, expected, theoretical and practical dimensions of this service. This article discusses the provisions of MiCAR relating to providing advice on crypto-assets by comparing them with the MiFID II[3] regulatory package, which has been in force for several years now and which foresees the service of investment advice. It is therefore necessary to compare both types of services on the basis of MiCAR and MiFID II[4], whereby the provisions of the latter have been implemented into the Polish legal system and are found in FITA[5]. The provision of investment advice as defined in MiFID II already has a long-standing tradition, of which it is worthwhile, if not imperative, to take advantage. This will allow an overview of the specificity of crypto-asset advice and lead to an indication of the key responsibilities involved in its provision.

1. MiFID II Regulatory Package as a source of inspiration for the European legislator

The MiFID II regulatory package comprises: MiFID II Directive, as a legislative act of EU law, and a number of delegated and implementing acts within the meaning of Articles 290–291 of TFUE[6], i.e. primarily the Commission Delegated Regulation

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 as amended) ('MiCAR').

2 With certain exceptions specified in Article 59 of MiCAR and Article 143(3) of MiCAR.

3 The term 'the MiFID II regulatory package' shall mean the provisions of MiFID II (see footnote 5 below), together with the non-legislative (implementing and delegated) acts to that Directive and the provisions of Polish law that implemented those provisions of EU law.

4 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 as amended) ('MiFID II').

5 Financial Instrument Trading Act of 29 July 2005 (Official Journal of Laws of the Republic of Poland Dz.U.2024.722, as amended) ('FITA').

6 Treaty on the Functioning of the European Union of 25 March 1957 (*Official Journal of Laws of the Republic of Poland* Dz.U. of 2004 No. 90, item 864).

(EU) 2017/565[7], which sets out the rules of conduct for investment firms with regard to, *inter alia*, the provision of service of investment advice and defines that service (Article 9 of Regulation 2017/565). Guidelines and recommendations from supervisory authorities[8] also play a vital role here.

MiFID II established a legal framework setting out the operating conditions for the provision of investment advice, i.e. advice concerning also financial instruments[9]. The MiFID II regulatory package, therefore, focuses on activities that relate to financial instruments and, consequently, their occurrence in the given de facto state is a necessary and sufficient condition for the application of this legal framework. Furthermore, the precedence of the legal framework for financial instruments is also confirmed by Article 2(4)(a) of MiCAR.

MiFID II sets out organisational requirements for the performance by investment firms of investment services (brokerage services, in the country nomenclature), requirements and conditions of the functioning of the financial instrument trading venue, data reporting services providers; reporting requirements in respect of transactions in financial instruments; position limits and position management controls in commodity derivatives; transparency requirements in respect of transactions in financial instruments.

2. Investment advice

The definition of investment advice, at the level of the EU legislative act, is found in Article 4(1)(4) of MiFID II and states that it is the provision of personal recommendations to a client, either upon its request or at the initiative of the investment firm, in respect of one or more transactions relating to financial instruments[10].

This definition is complemented by Article 9 of Regulation 2017/565, which provides that a 'personal recommendation' shall be considered a recommendation that is made to a person in his capacity as an investor or potential investor, or in his capacity as an agent for an investor or potential investor. That recommendation shall be presented as suitable for that person, or shall be based on a consideration of the circumstances of that person, and shall constitute a recommendation to take one of the following sets of steps: (i) to buy, sell, subscribe for, exchange, redeem, hold

[7] Commission Delegated Regulation of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (OJ L 87, 31.3.2017, pp. 1–83 as amended).

[8] Cf. G. Włodarczyk, *Obowiązki firm inwestycyjnych i banków w systemie MiFID II. Stanowiska i wytyczne organów nadzoru*, Warsaw 2022, in particular Chapter VI.1-4, Chapter VII.2–3. 9–11.

[9] Defined in Article 4(1)(15) of MiFID II by reference to Section C of Annex I.

[10] Cf. T. Sójka, *Umowa o doradztwo inwestycyjne w obrocie instrumentami finansowymi – zagadnienia podstawowe*, Przegląd Prawa Handlowego, No. 4/2014, pp. 39–45; W. Kapica, T. Sójka in: T. Sójka (ed.), *Obrót instrumentami finansowymi. Komentarz*, Warsaw 2022, pp. 494–497; G. Włodarczyk, *Obowiązki…*, p. 111 et seq.

or underwrite a particular financial instrument; (ii) to exercise or not to exercise any right conferred by a particular financial instrument to buy, sell, subscribe for, exchange, or redeem a financial instrument. A recommendation shall not be considered a personal recommendation if it is issued exclusively to the public.

The Polish legislator referred to the construction of investment advice in Article 76(1) of FITA, indicating that it consists in the preparation, on the initiative of the investment firm or at the request of the client, and the provision to the client, as defined in Article 9 of Regulation 2017/565, in a written, oral or other form, in particular an electronic one, meeting the requirement of a durable medium, of a recommendation, prepared on the basis of the client's needs and situation and concerning the purchase or sale of one or more financial instruments, or the performance of another activity producing equivalent effects, the subject matter of which are financial instruments, or a recommendation concerning refraining from the performance of such an activity.

The provision of a service that fulfils the aforementioned criteria constitutes the performance of a brokerage activity (Article 69(2)(5) of FITA), in principle requiring a brokerage authorisation[11].

There are two regulations clarifying the statutory requirements that are relevant from the perspective of the provision of brokerage services. These are: the Regulation of the Minister of Finance of 24 September 2024 on detailed technical and organisational conditions for investment firms, state banks conducting brokerage activities, banks referred to in Article 70 (2) of the Financial Instrument Trading Act, and custodian banks[12] and the Regulation of the Minister of Finance of 12 November 2024 on the procedure and conditions for the conduct of investment firms, state banks conducting brokerage activities, banks referred to in Article 70(2) of the Financial Instrument Trading Act, and custodian banks[13]. As for the investment advice, of particular relevance is §145 of the latter regulation, which sets out the obligations regarding the report to be provided to the client.

3. Advice on crypto-assets

According to Article 3(1)(24) of MiCAR, 'providing advice on crypto-assets' means offering, giving or agreeing to give personalised recommendations to a client, either at the client's request or on the initiative of the crypto-asset service provider providing the advice, in respect of one or more transactions relating to crypto-assets, or the use of crypto-asset services.

It might seem that – as with most other crypto-asset services that show similarities to brokerage activities – providing advice on crypto-assets covers the same elements

[11] Cf. exception concerning e.g. banks carrying out brokerage activities pursuant to Article 70(2) of FITA. Such activities do not constitute brokerage activities (Article 70(3) of FITA).

[12] *Official Journal of Laws of the Republic of Poland* Dz.U.2024.1423.

[13] *Official Journal of Laws of the Republic of Poland* Dz.U.2024.1735.

as the performance of the service of investment advice. However, even a cursory reading of the above definition allows a conclusion that the scope of advice on crypto advice is broader and does not include only a personal recommendation concerning a transaction relating to crypto-assets, but also the ' use of crypto-asset services'. This is also confirmed by the English language version of Article 3(1)(24) of MiCAR.

The foregoing means that a service of advice on crypto-assets can take two forms. The first form consists in the provision of a personalised recommendation in respect of one or more transactions relating to crypto-assets. In that case, the client asks the crypto-asset service provider ('CASP') for a personal recommendation on the 'transaction'. The second form consists in giving a personal recommendation on the use of crypto-asset services. In that case, the client, in turn, requests CASP for a recommendation in respect of the crypto-asset services. These can be any of the services listed in Article 3(1)(16) of MiCAR. It should be assumed that, as a result of the provision of this variant of the service of advice on crypto-assets, the client may receive a recommendation to refrain from using such services, to use a specifically indicated service, e.g. custody and administration of crypto-assets on behalf of the client, portfolio management on crypto-assets and, perhaps surprisingly, also provision of advice on crypto-assets (in the first variant). As regards the variant of provision of advice on crypto-assets, of decisive significance shall be the intention of the client, who may be determined to acquire crypto-assets on his own and wants a recommendation on which digital assets to choose (if any, given his individual situation) or may be considering various options for 'entering' the market of crypto-assets but need assistance in making the choice (e.g. acquisition by the client himself vs. portfolio management of crypto-assets, custody of crypto-assets by the client himself vs. custodial services and administration). In contrast, it should be strongly emphasised that the advice on crypto-assets in variant two, is not, as it were, a prelude to the provision of all other services, as long as the client takes the initiative to use a specific crypto-asset service (e.g. portfolio management of crypto-assets). In that case, the legal framework provided for the specific crypto-asset service should be applied.

In the context of providing advice on crypto-assets, of significance becomes the question of how detailed a personalised recommendation is to be. As regards investment advice, it is assumed that its criteria are not satisfied by '(...) a recommendation concerning only a certain category of financial instruments, e.g. Polish government bonds in general, Polish corporate bonds, or shares of companies of a certain region[14]. Even more so, a recommendation indicating the advantage of investing in one class of financial instruments (e.g. shares) over another class of financial instruments (e.g. government bonds) is not investment advice'[15]. However, the proviso that '(...) a recommendation concerning shares included in a specific stock market index (e.g. WIG 20) will be investment advice'[16] will be reasonable. In case of crypto-assets, the equivalent of a stock market index grouping issuers of

[14] T. Sójka, *Umowa o doradztwo...*, p. 42 et seq.
[15] *Ibidem.*
[16] Ibidem, pp. 42–43.

financial instruments may be classes (types) of crypto-assets representing common characteristics and performing the same functions, where the differences between the selection of a particular digital asset are not of conclusive significance. The client will be able to make a decision based on the recommendation of crypto-assets of a certain type, function and applications, because he will conclude that each digital asset included in the given group is suitable for him. In that case, it seems that a recommendation under the crypto-asset advice service may identify certain categories of crypto-assets[17].

4. Instruments for the protection of clients using the advice on crypto-assets

4.1. Introductory remarks

Providing advice on crypto-assets requires authorisation by the competent supervisory authority (Article 59 of MiCAR). In Article 59(1) of MiCAR, the legislator referred to two categories of entities and, although it used the word 'authorisation' for both, there is no authorisation procedure in the case of the entities referred to in paragraph 1(b) (Article 60 of MiCAR), while there is one in the case of the entities referred to in paragraph 1(a) (Article 63 of MiCAR). This fact is confirmed by Article 59(1) of MiCAR, according to which the right to provide crypto-asset services '(...) shall be revoked upon the withdrawal of the relevant authorisation that enabled the respective entity to provide the crypto-asset services without being required to obtain an authorisation pursuant to Article 59'.

The conditions to be met while providing that service are laid down mainly in Article 81 of MiCAR, but also in the provisions of Chapter 2 in Title V of MiCAR ('Obligations for all crypto-asset service providers'), applicable to all crypto-asset service providers, in particular Article 66 of MiCAR establishing an obligation to act honestly, fairly and professionally in accordance with the best interests of the clients. These provisions correspond to the obligations provided in FITA with regard to entities providing brokerage services, including the investment advice service.

Of paramount importance are the final ESMA guidelines clarifying some of MiCAR's requirements concerning the investor protection[18]. ESMA explicitly states in the Guidelines that the basis for the formulation of the same were ESMA Guidelines on MiFID II suitability assessment ('ESMA has taken the ESMA Guidelines on certain aspects of the MiFID II suitability requirements (...) as a basis for the draft guidelines')[19]. This is made following a reasonable assumption that the suitability

[17] Cf. the following comments in paragraph 5.5. concerning. the 'sufficient range' of crypto-assets taken into consideration when providing the advice on crypto-assets.

[18] Final Report – Guidelines specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) on investor protection – third package, 17 December 2024 (ESMA35-1872330276-1936) ('Guidelines').

[19] Guidelines, p. 7, nb. 7.

assessment of investment advice and the suitability assessment of advice on crypto-asset are based on the same principles and are very similar to each other[20]. Clients should therefore benefit from the same level of protection whether they invest in financial instruments (MiFID II regulatory package) or in crypto-assets that are not financial instruments (MiCAR)[21]. The vast majority of respondents agreed at the Guidelines consultation stage with ESMA's approach to ensuring consistency between the guidelines on the suitability assessment in accordance with the MiFID II regulatory package and the Guidelines (MiCAR)[22]. However, it should be emphasised that the legal framework set by the MiFID II regulatory package and the legal framework set by MiCAR are not identical, as can be seen, for example, in the categorisation of clients, which is one of the main elements of the protection regime for investors taking advantage of brokerage services, but which is absent from the protection regime for investors using the crypto-asset services. As is rightly pointed out by ESMA, although MiCAR does not provide for such an obligation, there is nothing to prevent crypto-asset service providers from having their own, internal rules regarding the client categorisation, provided that they can always ensure compliance with MiCAR suitability requirements[23].

4.2. Suitability assessment for the needs of providing the advice on crypto-assets

The primary obligation of crypto-asset advice service providers is to conduct a suitability assessment, i.e. to assess whether the crypto-asset services or crypto-assets are suitable for their clients or prospective clients, taking into consideration their knowledge and experience in investing in crypto-assets, their investment objectives, including risk tolerance, and their financial situation including their ability to bear losses (Article 81(1) of MiCAR). For the purposes of the suitability assessment, crypto-asset service providers providing advice on crypto-assets obtain from their clients or prospective clients the necessary information regarding their knowledge of, and experience in, investing, including in crypto-assets, their investment objectives, including risk tolerance, their financial situation including their ability to bear losses, and their basic understanding of the risks involved in purchasing crypto-assets, so as to enable crypto-asset service providers to recommend to clients or prospective clients whether or not the crypto-assets are suitable for them and, in particular, are in accordance with their risk tolerance and ability to bear losses (Article 81(8) of MiCAR).

Suitability assessments for the needs of providing investment advice and advice on crypto-assets are very similar to each other, as confirmed by the Guidelines. First and foremost, the suitability assessment is a prerequisite for providing the advice on

[20] *Ibidem.*
[21] Guidelines, p. 7, nb. 8.
[22] Guidelines, p. 9, nb. 21.
[23] Guidelines, p. 13, nb. 41.

crypto-assets. It should be assumed that no response from the client or potential client results in the inability to provide the advice both in variant one and in variant two, the latter consisting in providing a personal recommendation of crypto-asset services (cf. comments above concerning the structure of the crypto-asset advice service).

Where clients do not provide the information required for the suitability assessment, or where crypto-asset service providers providing advice on crypto-assets consider that the crypto-asset services or crypto-assets are not suitable for their clients, the service providers do not recommend such crypto-asset services or crypto-assets, nor begin the provision of portfolio management of such crypto-assets. (Article 81(11) of MiCAR). An analogous regulation is contained in Article 83g of FITA.

Common features of suitability assessments for investment advice and advice on crypto-assets undoubtedly include: avoidance of such a formulation of the assessment questionnaire which may lead to a self-assessment of the client or potential client[24], adjustment of the level of details and the scope of questions to the situation of certain persons ('Crypto-asset service providers should also take into account the nature of the client'), for example older people[25], avoidance of introduction of yes/no answers into the questionnaire[26], emphasising the relevance of the suitability assessment and its importance for the service provided[27], the obligation to put in place mechanisms to catch discrepancies in answers[28], and the approach to carrying out suitability assessments of legal persons and organisational units referred to in Article 33^1 of the Civil Code[29]. and natural persons represented by an attorney-in-fact[30].

The suitability assessment for the needs of providing advice on crypto-assets also generates new problems. First of all, the crypto-asset service provider should ensure that the suitability assessment also includes an analysis of the client's knowledge of technological aspects and risks involved, including the Distributed Ledger Technology (DLT)[31]. An extremely interesting theme is the assessment in terms of the ESG (environmental, social, governance) factors, which is not a mandatory element in case of markets in crypto-assets , which distinguishes this legal framework from the MiFID II regulatory package (cf. Article 54(2)(a) and (5) of Regulation 2017/565). Nevertheless, in the Guidelines, ESMA, despite emphasising several times the absence of any such obligation ('while not mandatory', 'though they are not required') has identified this element of assessment as a good practice, highlighting its beneficial impact on clients who may be interested in crypto-assets

[24] Guidelines, p. 58, nb. 48.
[25] Guidelines, p. 57, nb. 43.
[26] Guidelines, p. 59, nb. 49.
[27] Guidelines, p. 49, nb. 13–14.
[28] Guidelines, p. 60, nb. 54.
[29] the Act of 23 April 1964 – the Civil Code (consolidated text in the *Official Journal of the Republic of Poland* Dz.U.2024.1061) ('the Civil Code').
[30] Guidelines, p. 62, nb. 64.
[31] Guidelines, p. 11, nb. 31–32 and pp. 54–55, nb. 34.

more consistent with the ESG factors[32]. This aspect can be problematic since, on the one hand, there is an emphasise of no obligation to analyse the ESG factor-related issues, while, on the other hand, it is incumbent on the crypto-asset service provider to obtain the information necessary to assess the client's individual situation, including, for example, his investment objectives, which may be co-determined by the ESG factors.

The purpose of the suitability assessment is to enable the crypto-asset service providers to '… recommend to clients or prospective clients whether or not the crypto-assets are suitable for them and, in particular, are in accordance with their risk tolerance and ability to bear losses.' (Article 81(8) *in fine* of MiCAR). It would appear that this purpose has been limited solely to assessing the suitability of crypto-assets ('whether or not crypto-assets are suitable for them'), and thus to the exclusion of 'crypto-asset services'. However, the phrase 'whether or not crypto-assets are suitable for them' should be understood as inclusive of the crypto asset services. This conclusion is confirmed by Article 81(8) of MiCAR read in conjunction with Article 81(1) and (11) of MiCAR, which refer to both the suitability of crypto-assets themselves and the crypto-asset services. In Article 81(11) of MiCAR, the EU legislator has explicitly indicated that if clients do not provide the information required pursuant to paragraph 8, or if crypto-asset service providers consider that 'the crypto-asset services or crypto-assets' are not suitable for their clients, they shall not recommend such crypto-asset services or crypto-assets, nor begin the provision of portfolio management of such crypto-assets.

Crypto-asset service providers providing advice on crypto-assets (and also the portfolio management of crypto-assets) shall establish, maintain and implement policies and procedures to enable them to collect and assess all information necessary to conduct the suitability assessment for each client and shall take all reasonable steps to ensure that the information collected about their clients or prospective clients is reliable (Article 81(10) of MiCAR). A review of the suitability assessment for each client must be carried out at least every two years (Article 81(12) of MiCAR)[33]. The frequency of verification of information obtained from clients should take into account the client's risk profile and the crypto-assets that are the subject matter of the recommendation[34]. This means that it will generally be inappropriate to set the same frequency of verification for all customers.

4.3. Reporting obligation to clients

Once the suitability assessment or its review has been performed, crypto-asset service providers providing advice on crypto-assets is obliged to draw up and provide clients with (in an electronic form) a 'report on suitability' (Article 81(13) MiCAR)

[32] Guidelines, pp. 11–12, nb. 33–34.
[33] Guidelines, p. 61, nb. 59.
[34] Guidelines, p. 61, nb. 58.

specifying the advice given and how that advice meets the preferences, objectives and other characteristics of clients. That report shall, as a minimum: (i) include an updated information on the assessment; and (ii) provide an outline of the advice given. The report should make clear that the advice is based on the client's knowledge and experience in investing in crypto-assets, the client's investment objectives, risk tolerance, financial situation and ability to bear losses.

4.4. Advice on crypto-assets provided on an independent and dependent basis

Under Directive 2009/39 (MiFID I)[35] one of the biggest problems related to the protection of non-professional investors was the lack of independence of the advisor providing personalised recommendations[36]. The MiFID II regulatory package therefore emphasises the issue of independent and dependent provision of investment advice, including so-called incentives. The relevant provisions on these issues, in relation to investment advice, are thus to be found in Article 24(4) and (7) of MiFID II and then, as a result of their implementation, in Article 83c(5) to (6) of FITA. In turn, Article 76(2) of FITA determines that an investment firm may provide investment advice on a dependent or independent basis. It is therefore not surprising that the EU legislator applied a similar solution in MiCAR.

The obligations concerning the provision of advice on crypto-asset on an independent and dependent basis may be divided into general ones, irrespective of the manner in which the service is provided (on an independent or dependent basis), and specific ones, which update when the service is provided on an independent basis.

Article 81(2) of MiCAR imposes an obligation on crypto-asset service providers providing advice on crypto-assets to inform, in good time before providing advice on crypto-assets, the prospective clients whether the advice is: (i) provided on an independent basis; (ii) based on a broad or on a more restricted analysis of different crypto-assets, including whether the advice is limited to crypto-assets issued or offered by entities having close links with the crypto-asset service provider or any other legal or economic relationships, such as contractual relationships, that risk impairing the independence of the advice provided. The implementation of this obligation is an instrument for the protection of investors, as it increases their awareness of conflicts of interest and the range of crypto-assets that will be taken into account when making a personalised recommendation. This provision replicates the provisions of Article 24(4)(a)(i)–(ii).

[35] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ L 145, 30.4.2004, pp. 1–44).

[36] T. Sójka in: T. Sójka (ed.), Cywilnoprawna ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym, Warsaw 2016, p. 218; N. Moloney, EU Securities and Financial Markets Regulation, Oxford 2014, p. 802 et seq.

In turn, Article 81(3) of MiCAR sets out the rules for the provision of advice on crypto-assets when provided on an independent basis. The provision of this service on an independent basis, i.e. in the manner that is most beneficial for clients, entails certain obligations, including regarding the 'thoroughness' of the analysis carried out by the crypto-asset service providers providing advice on crypto-assets and a ban on the acceptance of the so-called inducements. This provision replicates the content of Article 24(7) of MiFID II.

The wording of Article 81(2)(b) and (3)(a) of MiCAR prejudges that, in the case of service provision on an independent basis, the client may not obtain, in fulfilment of the obligation referred to in paragraph (2)(a), information with content other than indicating that the provision of advice on crypto-assets is not limited to the crypto-assets indicated therein. This follows directly from paragraph 3(a), according to which, in the case of advice provided on an independent basis, the service provider must not be limited to crypto-assets issued or provided by: (i) that same crypto-asset service provider; (ii) entities having close links with that same crypto-asset service provider; or (iii) other entities with which that same crypto-asset service provider has such close legal or economic relationships, such as contractual relationships, as to pose a risk of impairing the independent basis of the advice provided. The provision of advice on crypto-assets on an independent basis may not occur be accompanied by information provided to the prospective client under Article 81(2)(b) of MiCAR that the advice is limited to crypto-assets issued or provided by entities having close links with the crypto-asset service provider.

As per Article 81(3)(a) of MiCAR, when the service is provided on an independent basis, the analysis of crypto-assets may include those issued or provided by entities with close links to the same provider. Indeed, the provision stipulates that the analysis must not be limited to the crypto-assets, so, consequently, they must not be the only crypto-assets taken into consideration when providing advice. One should, nevertheless, unambiguously opt for a situation when such crypto-assets constitute a significant minority since in each case they undermine the protection of clients using the crypto-asset advice. This also follows from the obligation to assess the 'sufficient range' of crypto-assets available on the market, which must be 'sufficiently diverse', and the general obligation to exercise due care with regard the interests of the client (Article 66 of MiCAR). In this case, it is possible to make an alternative reference to Article 53(1) of Regulation 2017/565, which sets out elements of the financial instrument selection process to assess and compare a sufficient range of financial instruments available on the market.

4.5. Problems of creating obligations with the use of vague concepts – 'sufficient range' and 'sufficiently diverse' range of crypto-assets

Both MiCAR and MiFID II use the terms: 'sufficient range' and 'sufficiently diverse' – in relation to the assets analysed (crypt-assets and financial instruments, respectively). These are elements that seem to generate the highest risk on the

service providers providing investment advice and advice on crypto-assets, due to their vague character. One cannot rule out that clients will question the range and diversity of crypto-assets taken into consideration when providing crypto-asset advice, especially as crypto-assets are to a larger extent more cross-border and at the same time subject to fewer access barriers. It is therefore the responsibility of the service providers to structure, and then document, their crypto-asset selection and analysis processes in such a way as to be able to demonstrate that the analysis was sufficiently thorough, while maintaining an appropriate level of rationality. On the one hand, a service provider providing advice on crypto-assets does not need to assess all crypto-assets available on the market, but, on the other hand, one cannot exclude a situation in which the assessment is made taking into consideration only a few classes (types) of crypto-assets representing specific characteristics, replicated by other crypto-assets, thus acting as a kind of representative of the given 'type', i.e. a broader group of digital assets with the same characteristics.

4.6. Inducements

Another prerequisite for the provision of advice on crypto-assets on an independent basis is the ban on the use of inducements (Article 81(3)(b)). A crypto-asset service provider may not accept and retain fees, commissions or any monetary or non-monetary benefits paid or provided by any third party or a person acting on behalf of a third party in relation to the provision of the service to clients. This provision has its counterpart, albeit slightly modified, in Article 83d of FITA. It should be pointed out that, for example, the exception provided for in Article 83d(1)(3) of FITA differs from the one provided in the second paragraph of Article 81(3) of MiCAR, since MiCAR exceptionally allows in this respect the acceptance only of non-monetary benefits, while Article 83d(1)(3) of FITA allows, under certain conditions, the acceptance of both non-monetary and monetary benefits. This discrepancy is interesting since Article 24(7)(b) of MiFID II uses the same working that was used in MiCAR, both in the Polish and in the English version ('*Minor non-monetary benefits*'). This means that on the basis of Article 81(3) of MiCAR the ban on the acceptance of monetary benefits is definitive and there are no exceptions to it. However, it must be assumed that the exceptions set out in Article 83d(1)(1) and (2) of FITA, which have no counterpart in Article 81(3) of MiCAR, would be redundant. The ban on acceptance of inducements may not be understood as prohibiting the acceptance of benefits, for example, from a person acting on behalf of a client (let alone from the client himself). An analogous assessment should be applied with regard to the performance of a monetary benefit by a third party (Article 356 § 2 of the Civil Code). Consequently, it should be considered acceptable for a provider of advice on crypto-assets provided on an independent basis to accept a monetary benefit from any person, as long as it is the main or ancillary benefit resulting from the primary contractual relationship between the provider and the client. Furthermore, it is exclusively prohibited to 'accept and retain' (*shall not accept and retain*) inducements but it is not prohibited to 'transfer' the same, as was set out in Article 83d of FITA.

5. Civil liability of service providers providing advice on crypto-assets

The same rules of civil liability that apply to the provision of investment advice apply of course to the provision of advice on crypto-assets[37]. A service provider may be held liable for an improper performance of the agreement on the provision of advice on crypto-assets under Article 471 et seq. of the Civil Code. However, it should be emphasised that the crypto-asset service provider is not a guarantor of the client's financial success and, consequently, not every damage to the client's assets incurred in connection with the implementation of a recommendation will lead to his civil liability[38]. Therefore, the service providers should not be perceived as entities that in any way, through their status, raise expectations concerning investments in crypto-assets, or enhance the credibility of such investments, or even of the crypto-assets themselves. The crypto-asset advice service provider must, however, ensure that its operations comply with the obligations imposed on it by the EU legislator and which to a certain extent have been outlined in this article. In this respect, it will be crucial to at least establish appropriate rules and criteria regarding suitability assessment to ensure that crypto-assets, that in many cases are highly speculative, should not be recommended to people who are not ready for the risks associated with them. It seems that an analysis of crypto-assets, including the problem of 'sufficient range' and 'sufficiently diverse' range will constitute a particular difficulty and, at the same time, a threat to the crypto-asset advice service providers, which results from the fact that as regards these, still new, digital assets, we do not have at hand such proven methods of analysis as those available in case of the market in financial instruments. Interestingly, the existence of a fundamental value of crypto-assets is also often questioned, while it is that method of analysis that is considered the most scientific and giving greater certainty as to market predictions[39]. It would appears that for at least some crypto-assets, the behavioural analysis will be of crucial significance[40].

Summary

The provision of advice on crypto-assets is essentially very similar to the provision of investment advice. This fact should not come as a surprise as it was the legal framework for the investment advice that provided a source of inspiration for the EU legislator when creating MiCAR. The provision of advice on crypto-assets also demonstrates certain, quite significant, differences, which poses additional

37 Cf. T. Sójka, in: T. Sójka (ed.), *Cywilnoprawna ochrona…*, pp. 221–225.

38 Cf. *ibidem*, p. 221.

39 See a review of literature on valuation methods, including fundamental analysis in: A. Rycerski, *Test racjonalnego inwestora w unijnym prawie rynku kapitałowego*, Warsaw 2022, pp. 87–105.

40 Cf. A. Szyszka, *Finanse behawioralne. Nowe podejście do inwestowania na rynku kapitałowym*, Poznan University of Economics and Business, Poznań 2009.

challenges in both the practical and theoretical spheres. The obligations associated with the provision of these services, in the market in financial instruments and the market in crypto-assets, are formulated so as to ensure the protection of clients, including those most exposed to the risks associated with a participation in these markets – non-professional clients. Of key importance is the suitability assessment, which, if inadequately designed, may not serve its purpose. The crypto-asset service providers are charged with a difficult task, On the one hand, in order to address the market expectations they must update their service offering by opening up to crypto-assets, while, on the other hand, the crypto-assets (with some exceptions) are extremely difficult to fit into a rational analytical and investment framework, which is, after all, the basis for the preparation of a personalised recommendation. The civil liability of service providers providing advice on crypto-assets, if any, may not, however, be derived from the failure of the crypto-asset investment itself. The guarantees of such a provider are limited to the application of organisational and procedural safeguards that protect clients from distortions in the process of preparing a personalised recommendation or from mismatches between crypto-assets and crypto-asset services and the individual needs of clients.

Bibliography

Kapica W., Sójka T. (2022). In: T. Sójka (ed.), *Obrót instrumentami finansowymi. Komentarz*, Warszawa.

Moloney N. (2014). *EU Securities and Financial Markets Regulation*, Oxford.

Regulation (MiCA) on investor protection – third package, 17 December 2024 (ESMA35-1872330276-1936).

Rycerski A. (2022). *Test racjonalnego inwestora w unijnym prawie rynku kapitałowego*, Warszawa.

Sójka T. (2016). In: T. Sójka (ed.), *Cywilnoprawna ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym*, Warszawa.

Sójka T. (2014). *Umowa o doradztwo inwestycyjne w obrocie instrumentami finansowymi – zagadnienia podstawowe*, Przegląd Prawa Handlowego, nr 4.

Szyszka A. (2009). *Finanse behawioralne. Nowe podejście do inwestowania na rynku kapitałowym*, Uniwersytet Ekonomiczny w Poznaniu, Poznań.

Włodarczyk G. (2022). *Obowiązki firm inwestycyjnych i banków w systemie MiFID II. Stanowiska i wytyczne organów nadzoru*, Warszawa.

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.

Safe Bank 2(99) 2025

DOI: 10.26354/bb.15.2.99.2025

Konrad Stolarski*
ORCID: 0000-0002-1390-3300
konrad.stolarski@ftl.pl

The area of interplay of crypto-asset and payment services in EU law

Abstract

Due to the (un)expected delays of the Polish government in the work of adapting national law to the EU MiCA Regulation[1] , despite the fact that this act is already fully applicable throughout the European Union as of December 30, 2024, in mid-2025 it is still not possible to make a reliable legal or business assessment of the first months of functioning of the EU and Polish market in the new regulatory framework of crypto-asset services. However, it should be emphasized that the scale of complexity of legal issues impacted by the emergence of MiCAR in the EU financial market goes far beyond the strictly local – e.g. Polish specifics. One can even conclude that at the level of EU legislative work, it was either underestimated or not fully noticed, how widely the MiCAR regulation will affect the „traditional" financial market. The purpose of this article is to indicate precisely such an example of regulatory interplay at the EU level, where crypto-asset laws affect the payment service regulations, both those already in force as well as pending adoption, i.e. respectively (i) the PSD2[2] and EMD2[3] directives, and (ii) the PSR[4] regulation and the PSD3[5] directive, which are currently at the final stage of the EU legislative process.

* Konrad Stolarski – doctor of laws and attorney at law, partner at ftl law firm and Board Member of the European Payment Institutions Federation (EPIF).

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) 2019/19377 (hereafter, I use the terms "**MiCA Regulation**" or "**MiCAR**" interchangeably).

2 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 ("**PSD2**").

3 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC ("**EMD2**").

4 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010 ("**PSR**"), COM/2023/367 final.

5 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC ("**PSD3**"), COM/2023/366 final.

Keywords: MiCA, MiCAR, PSD2, PSD3, crypto, emoney, payments, FINTECH, PAYTECH, EBA, EU

JEL codes: E42, G20, G28, G29, K23, K24, K29, L59

Introductory remarks

June 30th, 2025 marks the second anniversary of MiCAR becoming applicable[6] in the European Union. It is therefore possible to make the first assessment of how it has affected the EU financial market. Unfortunately however, this assessment still needs to be based more on analytical and doctrinal achievements than on market practice. This is because, despite the fact that MiCAR is an EU regulation directly and fully applicable throughout the EU, not all member states have complied with their Treaty obligations and have still not adopted national legislation enabling its provisions to be fully applied in practice by service providers[7] . As a result of the lack of national crypto-services laws aligned with MiCAR, suppliers in such countries are not only unable to apply for the relevant MiCAR authorizations[8] but are not even sure of the transitional period during which they will be able to operate under the existing rules. What is also obvious is that they are thus put at a market disadvantage in comparison to their competitors in other member states where relevant legislation has already been enacted and licenses have been issued. Such competitors are in the meantime free to offer their services across borders – including in Poland – using the so-called European single passport under Article 65 of MiCAR. As of May 20, 2025, the „empirical" study area across the EU is therefore set out only by 16 electronic money token („**EMT**") and 27 crypto-asset service ("**CASP**") licenses [9]. As it will demonstrated below, this state of affairs is contributed to not only by the tardiness of national legislators and supervisors from individual member states, but above all by the far-reaching legislative imperfection of the MiCA Regulation itself, which failed to fully recognizes how it's scope intersects with other legislation of the EU financial market. This is above all demonstrated by the unfortunate clash of this regulation with the EU's payment services and electronic money laws.

6 It should be added here, for the sake of precision, that this date applies only to the provisions of Titles III and IV of MiCAR, which apply from June 30, 2024, while the rest of MiCAR applies from December 30, 2024.

7 Among the examples of the most blatant violations of EU law in this regard are Poland, Belgium and Portugal, which, as of May 20, 2025, had not even yet referred national laws aligning national laws with MiCAR for parliamentary work.

8 On the subject of MiCAR licenses and the public law aspects of doing business in cryptocurrencies, see more extensively Stolarski, 2023.

9 https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica#InterimMiCARegister, accessed 20.5.2025.

1. Electronic money – definitions and interpretations of the term

The definition of electronic money in EU member states is based on Article 2(2) of the EMD2. Due to the legal instrument of harmonization of the law in this area (directive), there are some differences in the content of the definition of electronic money transposed across national law in EU member states[10]. Much further reaching are however differences in the understanding of the term 'electronic money". It is in particular necessary to point to the Polish approach to electronic money, shaped largely by the position of the Polish Financial Supervision Authority („**KNF**") of 10.7.2015 regarding the issuance of prepaid cards (Polish Financial Supervision Authority 2015), and the alternative concept, where user's funds held by a provider beyond the so-called D+1 period qualify as electronic money[11]. The latter position was presented in particular by the United Kingdom and the Republic of Lithuania (for more on this see Stolarski 2023, p. 63). Much has nevertheless changed in this regard as a result of the judgment of the Court of Justice of the EU („**CJEU**") of February 22, 2024 (Court of Justice of the European Union, 2024), which ultimately found the UK and Lithuanian approaches to be incorrect, stating that the activity of a payment institution to receive funds from a payment service user, where such funds are not immediately accompanied by a payment order and therefore remain available in the payment account maintained by the institution within the meaning of Art. 4(12) of the PSD2, constitutes a payment service provided by that payment institution within the meaning of Article 4(3) of the PSD2, and not an electronic money issuance transaction within the meaning of Article 2(2) of the EMD2.

The direction indicated by the CJEU in the context of interpreting what e-money is, now is also followed by EU legislative bodies and institutions. In the course of work on the revision of the PSD2 directive, the European Commission also proposed in article 3.50 of the PSR to maintain the definition of e-money essentially coinciding with that known to date from EMD2, i.e. as: *electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on the receipt of funds for the purpose of making payment transactions and which is accepted by other natural or legal persons than the issuer* (European Commission 2023a). Thus, compared to the existing definition from EMD2, the only wording changes are cosmetic. The key change is nevertheless is the that of the legal instrument in which the definition is contained. The legal successors to PSD2 will be both the PSR Regulation and the accompanying PSD3 (European Commission 2023b), and the legal definitions of key terms will be found in both legal acts. The mere inclusion of them in the EU regulation means that with the adoption of the PSR, these definitions will become part of the legal system of each EU member state and will thus be directly applicable. With the adoption of PSD3, the EMD2 will moreover be repealed and electronic money institutions as such will disappear from the EU

[10] Cf. in this regard, in particular, the definition of electronic money in Article 2(21s) of the Payment Services Act of 19.8.2011 (Journal of Laws of 2022, item 2360, as amended; hereinafter: "**PSA**").

[11] That is, within the deadlines set forth in Article 87.2 of PSD2 and Article 54 of the PSA.

legal order. Electronic money on the other hand will be issued in the EU as a matter of principle exclusively by banks (credit institutions) and payment institutions.

Interestingly, however, even the introduction of a uniform definition of e-money will not necessarily automatically remove all interpretive doubts around the concept of e-money. On January 17, 2025, in response to an inquiry from an entity whose application for a license to provide services as an electronic money institution has been refused by one of the EU national supervisory authorities, the European Banking Authority ("**EBA**") once again had to provide its interpretation of the term "e-money" (European Banking Authority 2025). In the context of the definition of e-money, the EBA clarified that the phrase "*accepted by other natural or legal persons than the issuer*" means that the payee (e.g., a *merchant*) must become the holder of the e-money and enter into a direct contract with the issuer. It is not sufficient (as suggested by the inquirer) for the recipient to accept payments made by customers using cards linked to e-money, without having such an agreement. It should be assumed that **this is precisely the understanding of the concept of e-money that will operate in the legal market after the adoption of the PSD3 and PSR package**.

2. MiCAR and '*stablecoins*'

The area of common regulations of MiCAR and EU payment/e-money law is primarily set out by the regulations on so-called "stable cryptocurrencies" (*stablecoins*). This term itself has been in fairly common use and in circulation for years, but as such does not reflect any specific legal or specialist terminological framework. It has been however mainly commercialized by promoters of particular cryptocurrencies (Financial Action Task Force 2021). In practice, despite the name of such cryptocurrencies, their main characteristic is not so much their actual "stability," but simply their *pegging* (*pegging*) to some other metric, potentially stabilizing their value. Depending on what kind of value point of reference we are dealing with, the level of such "stabilization" can vary. There are currently numerous projects which aspire to the title of "stable cryptocurrency." In addition to pegging to official currencies, other convertible goods/assets (such as gold or oil), cryptocurrencies, there are also cases where the pegging is provided solely by an internal algorithm, which decides on the level of issuance of a given cryptocurrency in a given moment, depending on the market demand for it (Martínez Nadal 2025, p. 178). Despite the lack of a legal definition of the term "stable cryptocurrency" in MiCAR itself[12], it is indeed reasonable to assume that two types of such crypto-assets are the subject of regulation in this legal act, i.e.: asset referenced tokens („**ART**") and electronic money tokens ("**EMT**")[13]. And it is the latter category of crypto-assets that marks

[12] The term, moreover, appears only in paragraph 41 of the MiCAR preamble.

[13] As for the qualification of ART and EMT as stable cryptocurrencies, there is generally consensus in the doctrine. So in particular: Mosoń, 2024, p. 67; Tomczak, 2023, footnote 62; and Bilski, 2022, p. 101.

the interface between EU payments and crypto-assets regulations. In view of the above, the remainder of this paper focuses exclusively on this particular „stable crypto-asset."

3. Electronic money versus electronic money token (EMT)

Article 3.1.7) of MiCAR defines an e-money token (e-money token) as type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency. This definition is further supplemented by Article 48.2 of MiCAR, which explicitly stipulates that e-money tokens shall be deemed to be electronic money. Despite such an unambiguous wording of the provision, during public consultation of the draft Polish law on market of crypto assets (Ministry of Finance 2024), some industry organizations questioned this dependence. In particular, they argued that the parallel functioning of the definition of e-money in Article 2.21a of the PSA and the definition of EMT in Article 3.1.7 of the MiCAR would lead to an "overlap of two legal regimes" (Ministry of Finance 2024a, paragraphs 9, 12, 23), and advocated treating e-money and EMT as two separate product categories (Ministry of Finance 2024a, paragraphs 9, 23, 34). These demands were correctly rejected by the Ministry of Finance as directly contradicting MiCAR. Indeed, it should be emphasized that **with the adoption of the MiCA regulation, a new category of e-money emerged on the market, which takes the form of token**. It thus functions alongside the long-known and already widespread forms of "server" e-money (where the payment instrument held by the user is used to connect to the server and authorize the deduction of monetary values to the payer and subsequently assign them to the payee) and "card" e-money (i.e. stored on a card, where a transaction with such an instrument is accompanied by the deduction of records or pulses directly on such a card). Indeed, EMT is therefore the only category of electronic money that currently has its own autonomous definition in a separate legal act. The comments pointing to potential definitional dualism in this regard, arising from the fact that the definition of EMT in the directly applicable MiCA regulation currently operates in parallel with the definition of electronic money in the PSA, implementing EMD2 in this regard, should be considered inaccurate. Theoretically it is of course conceivable that the Polish legislator in national law would introduce a definition of e-money that would contradict EMD2 and the definition of EMT from MiCAR. Such a situation would however constitute both a violation of the EMD2 directive, which by virtue of its article 16 is a full harmonization directive, and article 4(3) of the Treaty on European Union, which defines the so-called principle of loyal cooperation in EU law[14] . Any doubts in this regard will however be removed with the adoption of the PSR, as a result of which the „EU definition" of electronic money, like the definition

[14] According to this principle, Member States shall not only adopt all appropriate measures to ensure the implementation of their obligations under EU law, but shall also refrain from any action that could jeopardize the achievement of the Union's objectives, including those set forth in secondary legislation, such as EU directives and regulations.

of EMT, will already be included in the content of the EU regulation and, through the above, will have a direct effect and be directly applicable in all member states – including Poland[15]. As also rightly noted by M. Michna (Michna 2024), Article 49 of MiCAR furthermore introduces dedicated *lex specialis* rules for the issuance and redemption of EMTs in relation to EMD2, which makes it all the more clear that there is no conflict between these legal acts, as well as between MiCAR and the national laws implementing them (the opinion on lack of such a collision between EMD2 and MiCAR is also supported by Alcorta 2025, p. 149).

4. Common area of EU crypto market and payments/electronic money laws

It by no means can be stated that the issue of a potential conflict or "overlap" between the scope of MiCAR regulations and the already existing EU payment services law regulations evaded the notice of EU lawmakers entirely. Already in 2014, the EBA pointed out that virtual currencies – a concept with a slightly broader scope of meaning than cryptocurrencies – despite the fact that resemble products that already fall within the scope of EMD2, should be distinguished from electronic money, which, unlike virtual currency, is a digital representation of fiat currency (European Banking Authority 2014, p. 6). *A contrario*, if anything were to change such a position with regard to virtual currency (cryptocurrency), it would be its association with fiat currency, which is, after all, precisely the characteristic of EMTs. Also, during the public consultations preceding the adoption of MiCAR, EU legislators also considered regulating the trading with "stable cryptocurrencies" in the EMD2 (European Commission 2020a, p. 9)[16] as the so-called Option 2. Moreover, in the text of impact assessment the accompanying MiCAR, the European Commission explicitly pointed out the key and seemingly quite obvious fact that in case a provider offers such services as the transfer of „stable cryptocurrencies," then this service could fall under PSD2, and if **"stable cryptocurrencies" were considered electronic money, then services involving their transfer would have to be considered payment services** (European Commission 2020b, p. 54). The fact that some cryptoasset services may overlap with payment services from PSD2 is also pointed out in paragraph 90 of the MiCAR recitals. For the above reason, it is difficult to understand how it is possible that we came to a such far-reaching legal and regulatory uncertainty in the EU that CASP currently finds itself, when wishing to provide certain crypto-asset services that include EMT.

[15] The progressive phenomena of the choice of regulations as instruments of legal harmonization in the area of regulation of new areas of the EU financial sector in recent years is also highlighted by me in relation to crowdfunding activities (Dlugosz, Stolarski 2024, para. 5.1)

[16] This was eventually abandoned due to, among other things, consumer protection concerns and the inability of EMD2 to address the issue of systemic entities, which global "stable cryptocurrencies" could potentially become (European Commission 2020a, p. 9).

5. Crypto services vs EMTs

As demonstrated above, Article 48(2) of MiCAR unambiguously dispels, doubts about the legal status of EMTs, explicitly recognizing them as a category of electronic money. However, the EU legislator's contentions to the above provision alone completely ignores a number of secondary, practical implications for CASPs wishing to provide crypto-asset services relating to EMTs. Note in particular two of the crypto services, viz:

(i) providing custody and administration of crypto-assets on behalf of clients (service under Article 3.16.a of MiCAR); and
(ii) Providing cryptoasset transfer services on behalf of clients (service from MiCAR Article 3.16.j).

It can be assumed that, in a certain simplification, these services are, in terms of cryptoassets, the "equivalent" of the services of maintaining an electronic money payment account (wallet) and providing electronic money transfers from such an account. However, in the context of the comments made above on MiCAR defining EMTs as e-money**,** this means that **to the extent that a CASP would manage its client's EMT wallet or provide EMT transfers from such a wallet, those services would simultaneously constitute the provision of electronic money payment services.** This applies to both "on-chain" transactions (i.e., carried out directly on blockchain technology, with the recording of the operation in a distributed ledger (DLT), without the involvement of traditional banking infrastructure) and "off-chain" transactions (involving the transfer of the value of electronic money outside the blockchain – e.g., through an accounting entry in the system of the issuer or service provider, without recording the transaction itself in a distributed ledger (DLT)). In order to perform either service, the current state of the law therefore requires the status of a credit institution[17], electronic money institution or a payment institution[18]. There is no provision of MiCAR or other EU financial market legislation that exempts CASPs from being authorized to operate as any of these institutions.

MiCAR regulations seem to take notice of this provision only partially. Yes, MiCAR does provide, in Article 60, a simplified route to obtain the right to offer crypto services for credit institutions (paragraph 1) and electronic money institutions (paragraph 4), if they submit the information and documents indicated in Article 60 paragraph 7 of MiCAR to the competent supervisory authority 40 days prior to the start of such services (for more on this, see Stolarski 2023 p. 66). These provisions, however, provide a short route only for these two categories of providers and leave out CASPs themselves[19]. Thus, in order to provide EMT crypto services in the EU independently, one must now apply for two independent authorizations, i.e. –

[17] That is, in the Polish case, a bank or a cooperative savings and loan association (SKOK).
[18] In doing so, I am deliberately omitting cases of services where the provision of such services is excluded from the scope of the EMD regulations, such as under Article 1, paragraphs 4–5 of EMD2.
[19] And – something that is already completely incomprehensible and will be elaborated on below – payment institutions.

a CASP authorization and – at a minimum – an e-money institution authorization. MiCAR provisions, for completely incomprehensible reasons, fail to note how great of an organizational, financial and regulatory challenge such a situation entails for CASPs. **Neither MiCAR, PSD2 or EMD2 provide any simplification for CASPs in the process of applying for any of the above licenses.**

In the current state of the affairs, the only viable alternative for CASPs obtaining and holding "dual authorization" is to take up and operate EMT services in cooperation with a credit, e-money or payment institution in the so-called *white label* model[20]. It will be however highly problematic (though not impossible) to create a regulatory model of cooperation with the provider in such a case, if he himself does not have CASP authorization. This is because, in part, such a service would be provided by the CASP in its own name, and in part in the name and on behalf of the cooperating e-money service provider. This would contribute to high complexity of the construction of the service, both in business and legal-regulatory terms. This state is is also completely contrary to the principles and objectives of the EU financial market and the single European passport.

Issues signalized above were rather quickly recognized by the largest crypto service providers present on the market, who, without waiting for the situation to develop, decided to apply in parallel for both CASP and electronic money services authorization[21] . Through this they gained a market advantage over competitors who did not decide or weren't able to do so. The approach of the aforementioned providers is however highly expensive and for this reason alone, will not be available to every contender, what in consequence will negatively affect the market development and the commercial offer for users in the EU. The European Commission made an attempt to solve this problem by applying on December 6, 2024 (European Commission, 2024) to the EBA and the European Securities and Markets Authority („**ESMA**") to assess the risk of double regulation of CASP's EMT transfer activities resulting from the simultaneous application of MiCAR and PSD2. Pointing to Article 9c of Regulation (EU) 1093/2010 of the European Parliament and of the Council of November 24, 2010 establishing the European Banking Authority, the Commission suggested that the EBA consider issuing a so-called "no-action letter" or taking other actions to limit the enforcement of PSD2 rules against such services. The Commission distinguished here between the use of EMTs as (i) *means of payment* or the subject of a P2P payment transaction, and (ii) situations in which EMTs would be used for investment purposes, where a CASP intermediates the exchange of EMTs for cash or other cryptocurrency. Only in the latter case, the Commission argues that the obligation to obtain dual authorization and meet dual requirements under both MiCAR and PSD2 may constitute an excessive regulatory burden, requiring EBA intervention under Article 9c of Regulation (EU) No. 1093/2010.

[20] On *white label* financial services, see Grabowski, 2021, among others.

[21] This is the case for Circle and Coinbase, among others, which already hold both CASP and e-money institution licenses – https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica#InterimMiCARegister , accessed 20.05.2025.

It is however controversial whether EMT transfers made solely for investment purposes between portfolios of the same client should be treated as payment transactions at all.

In its letter to the EBA and ESMA, the Commission furthermore did not notice a number of other significant problems arising from the current overlapping regulation of payments and EMT cryptoassets.

First of the omissions of the Commission is issue of the providers' requirement as regards EMT transfer timing. As a consequence of the qualification of EMT as electronic money the so called "D+1 rule| will apply to it, requiring that the date on which the payee's payment account is credited with the amount of the payment transaction be no later than the business day on which the payee's payment service provider's account is credited with the amount of the payment transaction. Furthermore, the amount of the payment transaction as a matter of principle should be made available to the payee immediately after the amount is credited to the payee's payment service provider's account. In case of EMT "*on-chain*" transfers it is meanwhile necessary to perform an operation on the network, which, depending on the consensus method used on the blockchain (and the cost of performing the transaction), can often take longer than D+1. The time and rules for performing a given operation and achieving consensus on the blockchain may also no longer be subject to modification due to the already adopted (and blockchain inscribed) network rules and principles.

Another major challenge in the context of EMTs is strong customer authentication ("**SCA**"), as mentioned in Article 97 of the PSD2. The obligation to apply SCA both in case of initiating an EMT transfer and accessing the wallet where the CASP holds client EMTs. There is no doubt that the SCA principles were developed without consideration of how they could potentially be applied on decentralized networks such as a blockchain. Since virtually all of the wallets on which CASPs hold EMTs for their customers will be online, EU open banking rules will also apply to each of them the obligation to provide dedicated access interfaces to such wallets under Commission Delegated Regulation 2018/389[22]. TPPs (*third party providers*) offering account information services or payment initiation services should – at least in theory – also be able to offer their services in relation to such. It is clear that neither TPPs nor the EU open banking system is currently prepared to integrate such services with respect to EMTs.

The dual authorization regime for activities involving EMTs also implies the doubling and parallel application of MiCAR (Article 67) and PSD2 (Article 10) prudential requirements, including those setting capital requirements for crypto activities and payment services. In the latter case, in the most disadvantageous configuration, a cryptocurrency service provider for EMT will be required to simultaneously hold

[22] Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open communication standards.

(i) capital of €150,000 under Article 67.1.a of MiCAR and Annex IV of MiCAR, and (ii) initial capital of €350,000 under Article 4 of EMD2.

The above are just some examples of the extremely burdensome "dual" requirements of payment services law applicable to the crypto market, which have not been given sufficient thought during the MICAR legislative process.

6. Awaiting PSD3/PSR in the context of EMTs – EBA Opinion and the General Approach of the Council of the EU

As indicated above, the legal situation for suppliers wishing to engage in crypto activities involving EMTs is highly complicated under current regulations. Unfortunately constructed regulations impose on such entities disproportionately burdensome and costly regulatory and legal requirements. Unfortunately, the PSD3 and PSR regulations intended as the legal successors of the PSD2 and the EMD2 in their original wording presented by the Commissions – not only failed to provide solutions to these problems, but actually created further problems themselves.

For this reason, the entire crypto-asset market was awaiting, with considerable impatience but also hope, the EBA's response to the "non-action letter" proposed by the European Commission. Although the EBA promptly expressed a favorable stance on the proposal (European Banking Authority 2024), its response, in the form of an opinion on the interplay between Directive (EU) 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens was published as late as 10 June 2025 (European Banking Authority, 2025b). Moreover, the substance of the opinion largely consists of *pro futuro* recommendations addressed to EU legislative bodies in the context of PSD3 and PSR. Any resolution of the identified regulatory problems will therefore materialize no sooner than within the next 2–3 years (after the PSR and PSD3 become applicable).

In its opinion, the EBA indeed does confirm that while crypto-asset exchange services into fiat currency (Art. 3.16(c) of MiCAR) and exchanges of crypto-assets for other crypto-assets (Art. 3.16(d) of MiCAR) do not qualify as payment services, providing custody and administration of crypto-assets on behalf of clients (Art. 3.16(a) of MiCAR) and transfers of crypto-assets on behalf of clients (Art. 3.16(j) of MiCAR), in relation to EMTs, do constitute payment services (European Banking Authority 2025b, p. 8). This means that a CASP intending to provide such services in relation to EMTs must have a valid legal basis to do so under both MiCAR and PSD2 regimes. In practice, this means the provider must meet the capital and own funds requirements set out in both acts (European Banking Authority 2025b, p. 12, para. 25) and undergo a complex licensing procedure before one of the EU member state regulatory authorities. **The only material simplification proposed by the EBA for the market is "advising" member state regulatory authorities to grant applicants a transition period until 1 March 2026 before the authorisation needs to be held**

(European Banking Authority, 2025b, p. 2). The EBA also recommends that, during this transitional period, supervisory authorities should not prioritize enforcement of certain PSD2 requirements vis-à-vis CASPs – particularly those concerning safeguarding, information duties, consumer protection, or open banking (European Banking Authority 2025b, p. 2). Within the context of PSD2 licensing procedures, EBA further advises that member state regulators, to the greatest extent possible, rely on the information previously submitted by the CASP during its application under the MiCAR framework (European Banking Authority 2025b, p. 10). It should be however taken into account what the current practice across the EU regarding the duration of licensing proceedings under PSD2 is, as well as the fact that in some countries, such as Poland, Portugal, or Belgium there is still no national crypto legislation at all. It is therefore impossible in such members state to apply for a CASP authorisation, let alone hold it. In such context the simplification measures currently proposed by the EBA in its opinion should be assessed critically as clearly insufficient.

Both the Commission as well as the EBA on the other hand still fail to notice the PSD3/PSR unjustifiably ignoring the fact that under the payment services law currently in force, it's not only credit institutions and electronic money institutions that can provide payment services in the field of electronic money. Payment institutions can as well. This possibility is granted by virtue of article 8 of the EMD2, according to which member states may allow payment institutions to issue electronic money, provided that they have been authorized to do so in accordance with the requirements of the directive. In Polish law, this provision is implemented in Article 73a of the PSA, which allows a national payment institution ("**NPI**") with an initial capital of not less than the equivalent of EUR 125,000 to issue electronic money. Such authorization is at the same time limited exclusively to the territory of Poland and limited to the equivalent of 5 million euros per month[23] . Thus, already having authorization to issue e-money, additional authorization to provide crypto-asset services would enable an NPI to provide such EMT services unhindered. By leaving payment institutions completely out of scope of the MiCAR, at present such providers, unlike credit institutions and e-money institutions, do not have any „simplified" path to obtaining the authority to provide cryptoasset services. Meanwhile, any payment institution wishing to provide payment services, firstly has to undergo a complicated procedure before a member state financial supervisory authority and is obliged to meet strict prudential and regulatory requirements, which do not differ significantly from those for electronic money institutions[24] . In spite of this, the status of a payment institution is, for the time being, *de facto* aligned with any other provider which does not hold any financial services authorization at the time of applying for a CASP. **Thus, in order to provide any crypto services**

[23] In order to start providing electronic money services, a NPI is required to simultaneously notify the KNF in advance and submit an application for the registration of information on issuing electronic money along with an update of its program of activities. Each of these requirements is subject to evaluation by the KNF on a case-by-case basis.

[24] Although, of course, there are some differences here – if only in terms of the increased requirement in relation to the amount of initial capital. Cf. Article 4 of EMD2.

(i.e., not just EMT), a payment institution must go through the entire, standard authorization process. The above should be assessed critically.

When publishing the drafts of the PSD3 and the PSR in June 2023, the European Commission failed to use such opportunity to correct the collision fields between them and the MiCA regulation in the process. And this is despite the fact that at that time MiCAR was already in force in the EU legal system. This is quite puzzling, since one of the Commission's major legislative proposals under the new EU payment services legislation is the final merger of the EMD2 and PSD2, and the consequent annihilation od electronic money institution as separate entities. With the adoption of the PSD3 and PSR, payment institutions will thus become the only non-bank (i.e., non-credit institution) payment service provider authorized to provide e-money services. In spite of this, the Commission has not chosen to reflect the above decision in the content of other EU legislation which, when referring to electronic money institutions at times granti them dedicated benefits (simplifications) arising from holding an e-money institution status alone (as is the case with MiCAR, among others). **Meanwhile, there is nothing to prevent the amendment of MiCAR through the PSD3 and PSR by granting payment institutions all the benefits currently applicable to electronic money institutions.** An alternative solution could also be to grant the existing payment institutions the status of electronic money institutions. If maintaining the catalog of payment services that a particular payment institution is authorized to provide at the moment, such amendment would only be a change in nomenclature. In turn, it would unequivocally contribute to solving many of the problems described in this article, which should be considered one of the basic areas of *de lege farenda* demands. Unfortunately neither of them have to date been raised at any stage of the PSD3 and PSR legislative process.

A somewhat more optimistic conclusion may be drawn from the updated drafts of the PSR (European Commission, 2025a) and PSD3 (European Commission 2025b), published on 18 June 2025 as the so-called *General Approach*, which will serve as the basis for trilogue negotiations between the European Commission, the European Parliament, and the Council of the EU. The amendments to Article 3 of PSD3 include dedicated provisions concerning applicants for payment licenses who have previously obtained authorization under the MiCAR regime. If applied favorably in the future, these provisions could indeed shorten the time required for such entities to obtain a payment license necessary to carry out their core activities in the crypto-asset space. However, as noted above, a realistic assessment of the impact of these changes will still require at least another 2–3 years.

Summary

A cross-analysis of EU laws on payment services and cryptoassets (both in force and pending entry) unfortunately does not give the best testimony as to the legislative quality of EU lawmaking in this area. Despite having the human resources of Europe's leading lawmakers and specialists, the EU legislator is increasingly becoming

a "victim" of the incredible pace of technological progress in the financial market. Each time a piece of EU legislation is added, it requires an increasingly complex and elaborate analysis of its impact on other existing and drafted legislation. On the other hand, EU authorities and policymakers are under increasing pressure of complaints on the "over-regulation of the EU economy" (Dumont 2023). Through this, the EU is in threat of losing competitiveness vis-à-vis, among others, the United States of America and the People's Republic of China, both in terms of scientific research (Rodríguez-Navarro 2024) and new technology economy, what has been particularly highlighted recently in the context of artificial intelligence (Prenga 2024; Chun, Wittm, Elkins 2024). As regards the regulation of artificial intelligence, it can furthermore be argued that the situation is similar to crypto-actives, as in both cases the EU laws were the first comprehensive attempts to regulate their subject matter.

A systemic analysis EU policies and lawmaking lays beyond the scope of this paper. Despite criticisms of the current state of affairs in the crypto-assets and payment services interface, it is however premature to conclude that the EU approach will not work in the long run. In particular, it should be borne in mind that, at least since the adoption of MiCAR and the publication of the PSD3 and PSR drafts, awareness of existing regulatory shortcomings has definitely increased in the EU. Particularly in the course of work in the Council of the EU during the Polish Presidency, there was a ively discussion on how PSD3 and PSR should correct many of the imperfections of MiCAR raised in this article and the member states themselves submitted unofficial proposals for solutions in this regard to the Council of the EU, in the form of so-called "non-papers"[25]. It should therefore be expected that the upcoming PSR and PSD3 trilogues of the Council, the European Parliament and the European Commission, will bring positive developments.

Bibliography

Alcorta J.G. (2025). *Regulating Stablecoins in the European Union. Asset-Referenced Tokens and E-Money Tokens*. In: C. Pastor Sempere (eds), *Governance and Control of Data and Digital Economy in the European Single Market*. Law, Governance and Technology Series, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-031-74889-9_7

Bilski A. (2022). *A new legal framework for cryptoassets in the European Union*. In: R. Bieda, Z. Okon (eds.), *Meta-world: legal and technical aspects of disruptive technologies*, Warsaw.

Chun J., Wittm C.S., Elkins K. (2024). *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US*. Cornell University Computers and Society.

[25] The term "non-paper" in the EU context refers to informal documents used in the decision-making and legislative process, mainly for the purpose of discussing the proposals for solutions presented in their content. Although they have no official status and are not officially published, they play an important role in shaping policies and positions and are exchanged between EU bodies and member states.

Court of Justice of the EU (2024). Judgment of February 22, 2024 in Case C-661/22, ABC Projektai UAB v. Lietuvos bankas. ECLI:EU:C:2024:138.

Dlugosz Z., Stolarski K. (2024). *Commentary to Article 12 of Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7.10.2020 on European providers of crowdfunding services for business ventures and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937*. In: J. Dybiński (ed.), *Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7.10.2020 on European providers of crowdfunding services for business ventures and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937*. Commentary, Warsaw.

Dumont B. (2023). *On a Search for a Regulation Reduction Act (RRA)*. European Journal of Risk Regulation, 14(2), 355–370.

European Banking Authority (2014). *EBA Opinion on 'Virtual Currencies' (EBA/Op/2014/08)*, https://www.eba.europa.eu/regulation-and-policy/consumer-protection.

European Banking Authority (2014). *EBA response to Mr. Berrigan on the interdependence between MiCA and PSD2*, December 10.

European Banking Authority (2025a). *Single Rulebook Q&A 2022_6336: Definition of electronic money*, https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2022_6336

European Banking Authority (2025b). *Opinion of the European Banking Authority on the interplay between Directive (EU) 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens.*

European Commission (2020a). *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937*, COM(2020) 593 final, 2020/0265 (COD), Brussels, 24 September.

European Commission (2020b). *Commission Staff Working Document – Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937*, SWD(2020) 380 final, Brussels, 24 September.

European Commission (2023a). *Proposal for a Regulation of the European Parliament and of the Council on payment and electronic money services in the internal market and amending Regulation (EU) No 1093/2010 (COM(2023) 367 final)*.

European Commission (2023b). *Proposal for a Directive of the European Parliament and of the Council on payment and electronic money services in the internal market, amending Directives 2009/110/EC, 2013/36/EU and (EU) 2015/2366 and repealing Directive 2015/2366/EU (COM(2023) 366 final).*

European Commission (2024). *Letter to EBA and ESMA on the relationship between MiCA and PSD2*, Ref. Ares(2024)8440645 – 06/12/2024.

European Commission (2025a), *Payment Services Regulation (PSR) – Mandate for negotiations with the European Parliament,* June 13th 2025, 10268/25, https://data.consilium.europa.eu/doc/document/ST-10268-2025-INIT/en/pdf

European Commission (2025b). *Dyrektywa w sprawie usług płatniczych (PSR) – Mandat do negocjacji z Parlamentem Europejskim*, June 13th 2025, 10176/25, https://data.consilium.europa.eu/doc/document/ST-10176-2025-INIT/en/pdf

Financial Action Task Force (2021). *Updated Guidance for a risk-based approach: Virtual assets and virtual asset service provider*, Paris**.**

Financial Supervision Commission (2015). *Position on the issuance of so-called prepaid cards by banks*, https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf

Grabowski M. (2021). *Legal Aspects of "White-Label" Banking in the European, Polish and German Law*. Journal of Risk and Financial Management, 14(6), 280.

Martínez Nadal A. (2025). *Stablecoins in the MiCA Regulation*. In: C. Pastor Sempere (ed.), *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces*, Springer Suiza, pp. 177–198.

Michna M. (2024). *E-money tokens as a new form of electronic money*, Monitor Prawa Bankowego, 10, 77–88.

Ministry of Finance (2024). *Crypto market bill. Project number UC2. Office of the Prime Minister*, https://www.gov.pl/web/premier/projekt-ustawy-o-kryptoaktywach

Ministry of Finance (2024a). Statement of comments (all comments submitted for consultation, consensus and opinion), April 18, 2024, https://legislacja.gov.pl/docs//2/12382311/13040393/13040396/dokument664311.rtf

Mosoń K. (2024). *Introduction to stablecoins in MiCA*, Monitor Prawa Bankowego, 11, 65–75.

Prenga K. (2024). *AI regulation in the EU, the US and China: An NLP quantitative and qualitative lexical analysis of the official documents*. Journal of Ethics and Legal Technologies, 6(2).

Rodríguez-Navarro A. (2024). *Countries pushing the boundaries of knowledge: the USA's dominance, China's rise, and the EU's stagnation*. Quality & Quantity, 26.12.2024.

Stolarski K. (2023). *The impact of MiCA on the regulatory and legal conditions of doing business with crypto-actives in Poland and the EU*. Monitor Prawniczy, No. 9, 62–66.

Tomczak T. (2023). *The substantive scope of the MiCA Regulation.* Allerhand Law Review 2023, vol. 6, no. 1 (11), item. 4.

Safe Bank 2(99) 2025

DOI: 10.26354/bb.16.2.99.2025

Rafał Włoczka*
ORCID: 0009-0000-7729-5036
rafal.wloczka@gmail.com

The problem of the legal qualification of selected crypto-asset services in light of MiCAR

Abstract

The article examines the possible legal qualification for providing custody and administration of crypto-assets and providing transfer services for crypto-assets on behalf of clients, concerning e-money tokens within the meaning of Regulation (EU) 2023/1114 of the European Parliament and of the Council on Markets in crypto-assets, as payment services within the meaning of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market.

The article examines whether the specified services fall within the scope of the payment services, and analyses the potential implications of this. The study uses a legal-dogmatic approach based on the interpretation of legal acts, case law, and the domestic and foreign academia.

The results show that the recognition of these services as payment services would entail dual regulatory requirements – for both crypto asset providers and payment service providers. This issue is crucial for the stability of the financial market and the effectiveness of the supervision of its participants.

Keywords: MiCAR, PSD2, crypto-asset services, payment services, CASPs

JEL codes: K22, K23, G28

Introduction

This article examines the legal qualification of the services of providing custody and administration of crypto-assets on behalf of clients (Article 3(1)(16)(a) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of

* Rafał Włoczka – Lawyer specializing in financial regulations; extramural PhD student at the Faculty of Law and Administration of the Jagiellonian University in Cracow.

31 May 2023 on crypto-asset markets)[1] and the provision of transfer services for crypto-assets on behalf of clients (Article 3(1)(16)(j) of MiCAR), the subject of which may be e-money tokens.[2]

The concept of crypto-assets under MiCAR is not homogeneous. It includes asset-referenced tokens (Article 3(1)(6) of MiCAR), EMTs (Article 3(1)(7) of MiCAR), and crypto-assets other than asset-referenced tokens or EMTs (Article 4 *et seq.* of MiCAR). Although the determination of the meaning and scope of the subject matter of crypto-assets has been subject to significant changes during the legislative phase of MiCAR (see Tomczak 2023, *passim*; Tomczak 2022, *passim*), and these issues may evoke interpretative challenges (Korus 2024, *passim*), this article is only concerned with EMT-related services.

It should first be noted that the provision of crypto-asset services is regulated by MiCAR. At the same time, in recognising the possibility of a potential double qualification of crypto-assets or crypto-asset-related services as being subject to both MiCAR and other EU financial services legislation, the EU legislator has introduced corresponding conflict of law rules.

Under Article 2(4) of MiCAR, crypto-asset-specific rules do not apply to those crypto-assets that are covered by other EU regulations on the functioning of the financial market. This assumption is based on the regulatory paradigm of the EU financial services market, i.e. "same activity, same risk, same rules" (recital 9 of MiCAR). According to this approach, if a given right or service (including crypto-assets) falls under a different legal regime in the financial services area, it should be covered by the relevant rules, regardless of any technological aspects.

However, the indicated catalogue of exemptions from MiCAR treats crypto-assets as qualifying as "funds" specifically. Under Article 2(4)(c) of MiCAR, the regulation does not apply to crypto-assets that qualify as funds unless they qualify as EMTs. The exception provided for EMTs from MiCAR's general exemption means that the provisions of MiCAR apply to EMTs. At the same time, there is no conflict of laws rule that excludes the application of other regulations to this type of crypto-asset. Consequently, it must be assumed that EMTs may be subject to both MiCAR and the payment services-specific regulation. This article focuses on analysing this thesis and its legal implications.

[1] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on crypto-asset markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ EU. L. 2023, No. 150, p. 40, as amended; hereinafter: MiCAR).

[2] Hereinafter as: EMT.

1. EMT – crypto-asset or electronic money?

Under Article 3(1)(7) of MiCAR, EMTs are a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency. Article 48(2) of MiCAR further provides that EMTs are considered electronic money. Treatment of EMTs directly as "electronic money" is also confirmed *expressis verbis* in recital 66 of MiCAR. This approach is also confirmed by the draft PSR[3] which equates EMTs with electronic money. Recital 29 of the draft PSR indicates that the payment services rules should unambiguously specify the situations in which the regime applicable to payment services will not apply to EMT-related activities. This allows one to assume that if the EU legislator had intended to exclude the application of the rules applicable to payment services to transactions involving EMTs, it would have done so explicitly. However, at the current stage of legislative work on the draft PSR, there are no provisions exempting its application to transfer services for crypto-assets, and crypto-asset custody and administration services on behalf of clients.

Given the above, there is a strong case to be made that the provision of some type of crypto-asset services, involving the use of EMTs, results in these activities being simultaneously subject to the regulatory regime applicable to payment services.

2. Does storing and administering crypto-assets mean operating a payment account?

Deciding whether the activity of storing and administering crypto-assets can be classified as a payment account activity first requires defining and identifying the design features of the instrument.

Under Article 4(12) of the PSD2[4], a payment account means an account held in the name of one or more payment service users which is used to execute payment transactions. This definition is faithfully reproduced in Article 2(25) of the Payment Services Act[5]. Importantly, the mere operation of a payment account does not constitute a payment service (see Article 3(1)(1–8) of the PSA and Annex I to the PSD2). Nevertheless, due to the functionally inseparable link between the payment account and certain payment services, the operation of a payment account is considered to be an ancillary service arising from the payment services contract (Czech 2021, p. 27).

[3] Position of the European Parliament adopted at first reading on 23 April 2024 with a view to the adoption of Regulation (EU) 2024/... of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (accessed on 20.05.2025: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0298_EN.html; hereinafter: draft PSR).

[4] 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, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC (OJ EU. L. 2015 No 337, p. 35 as amended; hereinafter: PSD2).

[5] Hereinafter as: PSA.

The concept of a payment account has three essential elements: firstly, it must have the characteristics inherent in accounts, i.e. it must allow certain values (in this case, funds) to be recorded; secondly, it must allow payment transactions to be performed; and thirdly, it must be held for one or more users.

Firstly, a payment account must have a bookkeeping function to record funds correctly. The view of the bookkeeping component of payment accounts is confirmed by doctrine which points out that a payment account "*is an accounting device maintained by the payment service provider, used to record receivables between the parties to the legal relationship: payment service provider and user*" (Czech 2021, p. 23; Iwański 2025, thesis 11). The record-keeping nature of a payment account allows for the disclosure of the amount of claims between the account holder and the payment service provider[6] maintaining the payment account (Czech 2019, p. 49). The indicated feature is essential for the economic purpose of payment accounts, i.e. to enable the execution of payment transactions. This is because it makes it possible to keep records and to make appropriate settlements of the funds held in the accounts (so with regard to bank accounts: Janiak 2022, Nb 1).

Secondly, the payment account must be used to perform payment transactions. The payment account agreement should specify the types of services provided in connection with the account; this may include services related to payment transactions (Czech 2021, p. 30). At this point, however, attention should be drawn to the incorrect positions expressed in legal doctrine which indicate that the performance of payment transactions should be the "predominant purpose" or a purpose at least equivalent to the other functions of the account for it to qualify as a payment account (cf. Czech 2021, p. 30). Such reasoning seems to go too far. While, by their nature, payment accounts should primarily perform payment functions, the qualification of an account as a payment account should be determined by the scope of functionalities associated with it (similarly, see Blocher 2019, p. 30). Neither the PSA nor the PSD2 provide any basis to introduce a subjective criterion of the 'predominant nature' of the assumed purpose of using the account for its proper classification. This is confirmed by the jurisprudence of the Court of Justice of the European Union[7] which indicates that, to assess the "payment" nature of an account, it is necessary to establish whether the account enables the execution of payment transactions. There are even positions in doctrine attributing an overriding character to this attribute. According to this approach, the concept of a payment account should be understood functionally as "*an account (including a bank account) that serves (has the function of) performing payment transactions*" (Blocher 2019, p. 71). The very possibility of performing payment transactions from an account, regardless of its economic purpose, renders it a payment account.

This assertion is also confirmed by the positions expressed by the European Commission. Indeed, it indicates that all accounts may qualify as payment accounts

6 Hereinafter as: PSP.
7 Hereinafter as: CJEU.

if they are not covered by the exemption arising from the PSD2, if they allow payment transactions to be made, and even if these transactions are not made to or from third parties in relation to the account holder.[8] The European Commission's position was taken into account and confirmed by the Polish legislator during legislative work on the draft PSA.[9]

Thirdly, the payment account must be maintained by the PSP in favour of the user. Against this background, M. Blocher rightly points out that a payment account can only be one to which the characteristic of "externality" can be attributed, resulting from the obligatory relationship between the PSP and the user-account holder (Blocher, 2019, p. 73). This thesis is well demonstrated if the wording of Article 2(25) PSA is read along with Article 4(12) PSD2, where it is indicated that a payment account is *an account held in the name of one or more payment service users* (French: *un compte qui est détenu au nom d'un ou de plusieurs utilisateurs de services de paiement*). Notwithstanding the academic differences concerning the meaning of the possibility to attribute an account to a specific holder (cf. in this respect, i.a. Rogoń 2012, pp. 44–45; Blocher 2019, pp. 73–74; Czech 2021, pp. 28–29), the operation of a payment account is a service provided by the PSP to its holder (i.e. an entity other than the PSP). Thus, the PSP acts in this relationship in an intermediary role, enabling payment transactions using the account. This is confirmed by the fact that technical accounts, internal accounts, *loro*/*nostro* accounts, accounts opened by banks to service credit commitments, and other similar accounts do not constitute payment accounts under the PSA (Byrski, Zalcewicz, Bajor 2021, Article 2(25)).

In view of the above, a funds accounting and record-keeping system that allows the execution of payment transactions and that is operated for the benefit of a user (entity) who acts in a different role to the entity operating that system should be considered a payment account. Thus, it should be considered whether the provision of the custody and administration of EMTs on behalf of customers can be considered the operation of a payment account within the meaning of the regime applicable to payment services.

Under Article 3(1)(17) of MiCAR, the service defined therein should be understood as safekeeping or controlling, on behalf of clients, crypto-assets or the means of access to such crypto-assets where applicable in the form of private cryptographic keys (French: *la garde ou le contrôle, pour le compte de clients, de crypto-actifs ou des moyens d'accès à ces crypto-actifs, le cas échéant sous la forme de clés cryptographiques privées*).

Crypto-asset service providers[10] providing crypto custody and administration on behalf of clients should establish and implement a custody policy. The provision of such services must have a contractual basis. The contract should clarify the nature

[8] European Commission staff paper, *Your questions on PSD. Payment Services Directive 2007/64/EC. Questions and answers*, answers to questions 25, 31, 150, 187 and 262 (accessed on 20.05.2025: https://finance.ec.europa.eu/system/files/2023-06/110222-faq-transposition-psd_en.pdf).

[9] Uzasadnienie rządowego projektu ustawy z 17 maja 2011 r. o usługach płatniczych, Druk Sejmowy VI kadencji, Druk nr 4217.

[10] Hereinafter as: CASP.

of the service provided. This may include the custody of crypto-assets belonging to clients or the disposition of means of access to those crypto-assets, in which case, the client retains control over the stored crypto-assets. The crypto-assets or the means of access to them can also be transferred under the full control of a CASP. These entities, when storing or having the means to access crypto-assets belonging to clients, should ensure that these crypto-assets are not used for their own purposes (MiCAR, recital 83).

The contract between the CASP and the client for the provision and administration of the crypto-asset custody service by the CASP on behalf of the client must set out the parties' obligations and rights and the CASP's responsibilities (Article 75(1) of MiCAR). This agreement must include, i.a. a description of the nature of the service to be provided and the policy for the custody of crypto-assets by the CASP concerned (Article 75(1)(b)–(c) of MiCAR).

CASPs providing the service of custody and administering crypto-assets on behalf of clients are required to keep a register, open in the name of each client, in which a record would be kept of the positions corresponding to each client's rights in crypto-assets. In this register, CASPs are obliged to register all operations arising from their clients' instructions as soon as possible (Article 75(2) of MiCAR). In addition to its accounting and record-keeping function, this arrangement is intended to ensure the transparency of CASPs' activities vis-à-vis their clients (Zetzsche, Sinnig, Nikolakopoulou 2024, p. 219). The safekeeping and administration of clients' crypto-assets itself should be done in accordance with the CASP's internal policies and rules and procedures adopted to ensure custody or control of crypto-assets or the means to access them (Article 75(3) in conjunction with Article 70(1) of MiCAR)

Analysis of the indicated rules makes it possible to conclude that a CASP providing custody and administration of clients' crypto-assets does not become their owner, but only has custody of these assets (records the legal and factual status on the part of the authorised client and has custody of clients' crypto-assets). This interpretation is consistent with the nature of crypto-assets which constitute a *sui generis* property right (Article 3(1)(5) of MiCAR). I believe that, consequently, the "account" of crypto-assets should be ascribed the characteristics of a proprietary account (proprietary account) as found in the case of financial instruments[11] (Chłopecki 2016, p. 9). Indeed, cryptocurrencies are a specific category of property rights that can be traded. Furthermore, as stated above, CASPs are obliged to record all transactions resulting from their clients' instructions as soon as possible (Article 75(2) sentence 2 MiCAR). In my opinion, this obligation corresponds to the constitutive nature of the entry in the crypto "account". Indeed, I see no reason to treat crypto-assets, including EMTs, differently from other types of tokenised rights (see, in this regard, Wosiak 2023, *passim*; Włoczka 2022, pp. 78–81), or financial instruments which are also subject to registration in proprietary accounts (Sójka, Godlewski 2022, thesis 2; Michalski 2023, Nb 19). This view would make it possible

[11] Act of 29 July 2005 on trading in financial instruments (Journal of Laws 2024, item 722, as amended).

to distinguish crypto-assets from funds held in payment accounts (e.g. bank accounts) which constitute the account holder's claim on the PSP[12] (on the nature of the account holder's claim on the bank, see e.g. Gołaczyński 2023, Nb 16; Bączyk 2020, Nb 106).

Of course, this difference does not make it clear that the service of providing custody and administering crypto-assets on behalf of clients cannot constitute the activity of maintaining a payment account under the payment services regime. Even if one accepts as correct the understanding of the so-called crypto-asset accounts as proprietary accounts, this does not affect their legal qualification under MiCAR and the PSD2. The domestic understanding of the nature of the contractual relationship arising from a bank account agreement, including payment accounts and securities accounts (and in this case, crypto-assets), cannot affect the interpretation of EU law. Neither MiCAR nor the PSD2 define the normative nature of the accounts or the effects of making entries in these accounts.

With this in mind, it should be pointed out that there are important similarities between payment accounts and crypto-asset custody and administration services. Firstly, in both cases, there is a contractual basis for the CASP or PSP to provide the service to the client. Secondly, the custody and administration of crypto-assets on behalf of clients includes, *verba legis*, the maintenance of an open register of items corresponding to the rights of each client, and therefore, the service includes a record-keeping and accounting component. Thirdly, the custody and administration of crypto-assets on behalf of clients does not preclude the same CASP from being able to provide the service of transferring those crypto-assets. This means that, at least in theory (and usually also in practice), the service of storing crypto-assets will be functionally linked to the ability to dispose of them.

Thus, in my view, it is possible to consider the service of providing custody and administering EMTs on behalf of the client as an activity that qualifies as the operation of a payment account. This qualification will depend on the specific circumstances of the contractual relationship between the CASP and the client but, in principle, there are no normative differences that would support a separate qualification of this type of activity. This means that the qualification of the maintenance of so-called crypto-asset accounts on behalf of clients by a CASP as a payment account is not excluded.

3. Transfer of crypto-assets or payment transaction?

To determine whether an EMT transfer service qualifies as a payment transaction, it is first necessary to define the defining features of both activities. Bearing in mind the findings above on the nature of the crypto-asset custody and administration

[12] See on the nature of the obligation relationship arising from the bank account agreement: judgment of the Appellate Court in Szczecin of 6 March 2015, I ACa 40/15, LEX No. 1770856.

service, the EMT transfer service may entail the need for a CASP to be authorised to provide payment services.

Article 4(5) of the PSD2 defines the term "payment transaction" as an action initiated by the payer, on behalf of the payer or by the payee, involving the deposit, transfer, or withdrawal of funds, irrespective of the underlying obligations between the payer and the payee. This concept refers to the overall and single action between payer and payee, and not only to the individual relationships of the payer and payee with its own PSP.[13] A similar, but not identical, implementation of this definition can be found under Article 2(29) of the PSA.

With this in mind, it can be pointed out that the concept of a payment transaction must consist of the fact that their object is funds (e.g. EMTs – *author's note*) that are transferred by means of a closed catalogue of settlement activities, and that these activities are carried out on the user's initiative, i.e. the payer or the payee (Czech 2023, p. 59). On the other hand, the execution of payment transactions must have a basis in an agreement between the PSP and the customer (Article 4(21) PSD2) or in an individual payment transaction agreement (Article 44(1) PSD2).

Payment transactions can be categorised, depending on the entity initiating them, as "initiated by the payer", transactions "initiated by the payee", and transactions "initiated through the payee" (Byrski, Zalcewicz, Bajor 2021, Article 2(25); Grabowski 2020, Nb 59). However, payment transactions themselves can be divided into direct debits (Article 3(1)(2)(a) PSA), payment transactions using a payment card, or similar instrument (Article 3(1)(2)(b) PSA) and credit transfers (Article 3(1)(2)(c) PSA). Within the scope of this article, special attention should be paid to credit transfer services as this represents the most emblematic type of money transfer.

Under Article 3(4) of the PSA, credit transfer means a payment service for crediting a payee's payment account, where a payment transaction from the payer's payment account is made by the PSP maintaining the payer's payment account based on an instruction given by the payer. Under this service, the payer gives a payment instruction (order) to the PSP maintaining the payment account and the transaction itself is made using (debited) funds held on the payment account. However, the PSP is responsible to the payer for causing the payee's payment account to be credited (Iwański 2025a, thesis 18). The definition of a credit transfer referred to in Article 3(4) of the PSA is indeed similar to the definition of a credit transfer referred to in Article 63c of the Banking Law.[14] Thus, to some extent, it is permissible to use an auxiliary interpretation of this concept with reference to the national banking law acquis (with the proviso, however, that the interpretation of PSA through the prism of banking law can only be done in an auxiliary manner – the PSA, being an implementation of PSD2, is characterised by a kind of autonomy of the conceptual grid, aiming to ensure the effectiveness of European law). This allows for an easier grasp of the concept of 'crediting the account' of the payee as a result of a credit transfer. It denotes an entry

[13] CJEU judgment of 21 March 2019, C-245/18, Tecnoservice Int. Srl, ECLI:EU:C:2019:242, paragraph 26.
[14] Banking Law Act of 29 August 1997 (Journal of Laws 2024, item 1646, as amended).

that indicates an increase in the amount of the debt owed by the PSP maintaining the payee's payment account to the holder of that account as a result of the receipt of a certain amount of funds (Pisulinski 2025, Nb 2).

Thus, the payment service referred to in Article 3(1)(2)(c) PSA in conjunction with Article 3(4) PSA is the transfer of funds from the account holder's account to the payee, initiated by the payer, the execution of which is the PSP's responsibility. The proper execution of the transfer order, on the other hand, is to "add" funds to the payee's account, i.e. to increase the debt of the PSP maintaining the payee's account towards the payee.

Under Article 3(1)(26) of MiCAR, the provision of transfer services for crypto-assets on behalf of clients means the provision, on behalf of a natural or legal person, of transfer services for crypto-assets from one address or account on a distributed ledger to another. The conceptual scope of this service should include the activities of intermediary entities that provide the transfer of crypto-assets on behalf of a client from one address or account on a distributed ledger to another. Thus, the scope of this service does not include, for example, validators, nodes or so-called miners, that may be part of the process of validating transactions and updating the state of the distributed ledger (MiCAR, Recital 93).

The provision of a crypto-asset transfer service must be based on a contractual node between the CASP and the client which must set out the parties' obligations and responsibilities. The mandatory elements of this contract are described in Article 82(1)(a) to (e) of MiCAR. In accordance with the disposition of Article 82(2) of MiCAR, on 26 February 2025 the European Securities and Markets Authority[15] has published guidelines for CASPs providing transfer services for crypto-assets on behalf of clients with regard to procedures and policies, including client rights, in the context of transfer services for crypto-assets.[16]

Under the Guidelines, CASPs are required to provide information to the client regarding, i.a. a description of the form and procedure to initiate or consent to a crypto-asset transfer and to withdraw an instruction or consent, including a specification of the information that the client must provide to properly initiate or execute a crypto-asset transfer (including the method of authentication), and the conditions under which the CASP may reject a crypto-asset transfer instruction. This information must specify the means and timeframe by which the client must notify the CASP of any unauthorised or incorrectly initiated or executed crypto-asset transfers, as well as the CASP's liability, including its maximum amount, for unauthorised or incorrectly initiated or executed transfers (Guidelines, paragraph 12).

The above makes it possible to reconstruct at least the following characteristics that are relevant for the provision of a crypto-asset transfer service on behalf of clients.

[15] Hereinafter as: ESMA.

[16] ESMA, on rules and procedures, including customer rights, in the context of crypto-asset transfer services under the Crypto-assets Markets Regulation (MiCA) with regard to investor protection, ESMA35-1872330276-2032, 26 February 2025 (hereinafter: Guidelines).

Firstly, the service in this area is performed by the CASP which, being in the role of an intermediary, acts on behalf of the client to transfer crypto-assets. There is, in my view, no sufficient normative basis to conclude that the scope of the CASP's activities in this area is reduced to merely technically enabling the transfer of crypto-assets from one account to another. In particular, MiCAR does not contain a legal standard that would convincingly and unequivocally indicate what kind of activity undertaken by a CASP makes the service merely "technically enabling" the transfer, as opposed to the activity undertaken by a PSP (cf. Minto 2024, p. 371, to the contrary but without extensive argumentation).[17] Thus, the role of a CASP providing transfer services for crypto-assets is structurally similar to that of a PSP performing payment transactions.

Secondly, the provision of this service must be based on an agreement setting out the rights and obligations of the parties in relation to the transfer of crypto-assets. It is worth noting that the contract referred to in Article 82 of MiCAR could qualify as a "framework contract" within the meaning of the PSD2, i.e. a payment service contract covering the future execution of individual and subsequent payment transactions (Herrera 2025, p. 391).

Thirdly, the CASP is responsible for due performance (although the extent and amount of this responsibility may depend on the internal policies and procedures adopted, in accordance with para. 25 of the Guidelines), i.e. the transfer of crypto-assets involving the crediting of the transferred value (by overwriting blocks in *blockchain* technology) to the transfer recipient's account. However, it is worth noting that a CASP's liability for unauthorised crypto-asset transfers has not been shaped as strictly as a PSP's liability for unauthorised payment transactions.

The construction of the transfer services for crypto-assets as presented in this way corresponds, in its design, to the constitutive features of a payment transaction including, in particular, a funds transfer order.

Summarising the issue of the EMT transfer service on behalf of clients, I believe that it may qualify as a service for the execution of payment transactions including, in particular, a credit transfer service, subject to the regulation inherent in payment services. This is prejudiced by the structural identity (or the very far-reaching normative proximity of the two activities) demonstrated above. In addition, it is important that the EU legislator has not introduced a normative exemption that would unambiguously indicate the exclusive jurisdiction of a specific legal regime over these operations. On the contrary, recitals 90 and 93 of the MiCAR Regulation unequivocally indicate the recognition of the phenomenon of the overlapping of these regulations and the acceptance of the full consequences resulting from such a situation. On the contrary, in analogous cases, e.g. the transfer of monetary values related to the handling of assets arising from securities, including dividends, distribution of income,

[17] However, it should be borne in mind that in the case of crypto-asset services, which would really only amount to the provision of a distributed finance infrastructure within which *peer-to-peer* transfers could take place, this reasoning could be considered correct.

or distribution of other profits, the EU legislator has provided for the application of only the regime applicable to payment services (Article 3(h) PSD2).

This means that for transfer services for crypto-assets on behalf of a client which are provided directly by a CASP that accepts a transfer order from a client and acts to execute it, there is a structural identity between the concept of a payment transaction and this service. Thus, when EMTs are the subject of such a transfer – there is a duality of legal regimes applicable to this situation – MiCAR and the regime are applicable to payment services.

4. Do crypto-asset service providers have to be payment service providers? Conclusions.

Given the legal analysis set out above, I believe that, in the case of EMT transfer services and the custody and administration of EMTs on behalf of clients, it is possible to conclude that these activities constitute payment services. Consequently, it would be necessary for a CASP to obtain a specific authorisation to provide such services.

The problem described in this article has been recognised directly by the EU legislator. Indeed, it explicitly considered that, i.a. a crypto-asset transfer service may overlap in scope with payment services (MiCAR, recitals 90, 93). The EU legislator seems to take the position that crypto-asset services qualifying simultaneously as payment services require both relevant authorisations. This is prejudiced by recital 93 to MiCAR, stating that: "*in such cases, the transfers [i.e. the qualification of a crypto-actives transfer service as a payment service – author's note] should be carried out by an entity authorised to provide payment services in accordance with this Directive*". Currently, the problem of the confluence of the two standards has been recognised by the European Commission which has asked the European Banking Authority[18] to develop potential legislative suggestions in this area.[19] In response to this call, the EBA has published an opinion on the interplay between the PSD2 and MiCAR regimes[20]. The EBA submits that due to the qualification of EMTs as e-money – the problem of the application of the dual legal regime to certain services provided by CASPs needs to be regulated at the level of EU law. Leaving this issue without

[18] Hereinafter as: EBA.

[19] EC, Directorate General for Financial Stability, Financial Services and Capital Markets Union, Letter to EBA and ESMA entitled "Subject: Interplay between MiCA and PSD2 – Possible "no action letter" by the EBA", Brussels 5.12.2024 (accessed 20.05.2025: https://www.eba.europa.eu/sites/default/files/2024-12/3225040c-5f3d-410f-9156-f06a43231938/Letter%20to%20EBA%20and%20ESMA%20on%20the%20interplay%20between%20MiCA%20and%20PSD2.pdf).

[20] European Banking Authority, Opinion on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens, 10.6.20205, EBA/Op/2025/08 (accessed on 7.07.2025: https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-bcba0a28dbe7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf).

legislative intervention may lead to undesirable consequences from the standpoint of an EU financial sector regulatory policy[21].

I believe that the the EU legislative, while regulating these issue, should adopt a position clarifying that no authorisation as a PSP is necessary for CASPs providing the services analysed. The following arguments may be in favour of such interpretation of EU law. Firstly, following the argument derived from the principle of rationality of the legislator, it should be considered that MiCAR is a complete normative regulation. Thus, the performance of activities regulated under the MiCAR regime, which require authorisation to operate as a CASP, should not require an additional authorisation to carry out other regulated activities. This argument is underscored by the fact that the EU legislator has nowhere explicitly indicated in MiCAR that such a necessity exists. Secondly, an applicant for authorisation as a CASP must specify the scope of its intended activities in its application (Article 62(2)(d) of MiCAR). These services, on the other hand, are specifically regulated in MiCAR and in the delegated acts and guidelines of supervisory authorities adopted under MiCAR. These solutions are incompatible with MiCAR (e.g. with regard to the use of strong authentication for payment transactions or in the area of liability for unauthorised payment transactions). Thus, the application of both the requirements under the PSD2 regime (and, in the future, the draft PSR) and MiCAR to services with EMTs as their object would raise significant difficulties.

In view of the above, I believe that a desirable legislative solution would be for the draft PSR to prejudge the issue under consideration by establishing a standard excluding the scope of application of the payment services regime to crypto-asset services having EMTs as their object.

Notwithstanding the above, it should also be pointed out that, from a purely practical point of view, many CASPs will be able to require authorisation to provide payment services – not only because of their EMT-enabled services, but also because they transact and hold client funds (Minto 2024, p. 373). This has also been recognised by the EU legislator which has indicated that CASPs may themselves provide payment services linked to the crypto-asset service they offer if they hold the relevant authorisation issued under the regime applicable to payment services (Article 70(4) of MiCAR).

Bibliography

Bączyk M. (2020). *Rozdział 20. Umowy bankowe w polskim systemie prawnym*. In: M. Stec (ed.), *Prawo umów handlowych. System Prawa Handlowego. Tom 5C*, ed. 1, Warszawa.

Blocher M. (2019). *Cechy konstrukcyjne rachunku płatniczego. Glosa do wyroku TS z dnia 4 października 2018 r., C-191/17*, Europejski Przegląd Sądowy, No. 6.

[21] *Ibidem*, p. 3.

Blocher M. (2019). *Podstawowy rachunek płatniczy i umowa podstawowego rachunku płatniczego*, Warszawa, not published.

Byrski J., Zalcewicz A., Bajor B. (2021). In: J. Byrski (ed.), A. Zalcewicz (ed.), *Ustawa o usługach płatniczych. Komentarz*, ed. 2, Warszawa, commentary to Article 2 pkt 25.

Chłopecki A. (2016). *(Niektóre) paradoksy prawa papierów wartościowych*, Przegląd Prawa Handlowego, No. 9.

Czech T. (2021). *Pojęcie rachunku płatniczego*, Monitor Prawa Bankowego, No. 7–8.

Czech T. (2023). *Transakcja płatnicza*, Monitor Prawa Bankowego, No. 10.

Czech T. (2019). *Wpis na rachunek płatniczy*, Monitor Prawa Bankowego, No. 10.

Dokument służb Komisji Europejskiej, *Your questions on PSD. Payment Services Directive 2007/64/EC. Questions and answers* (accessed on 20.05.2025 r.: https://finance.ec.europa.eu/system/files/2023-06/110222-faq-transposition-psd_en.pdf).

EC, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, letter addressed to the EBA and ESMA (2024). Entitled "Subject: Interplay between MiCA and PSD2 – Possible 'no action letter' by the EBA", Brussels 5 December 2024.

European Banking Authority (2025). *Opinion on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens*, 10.6.20205, EBA/Op/2025/08.

ESMA Guidelines (2025). Guidelines on transfer services for crypto-assets under MiCA, ESMA35-1872330276-2032, 26 February 2025.

Gołaczyński J. (2023). In: E. Gniewek (ed.), P. Machnikowski (ed.), *Kodeks cywilny. Komentarz*, ed. 11, Warszawa, commentary to Article 725.

Grabowski M. (2020). In: M. Grabowski, *Ustawa o usługach płatniczych. Komentarz*, ed. 2, Warszawa, commentary to Article 2.

Herrera L.A. (2025). *PSD3 and the Regulation on Payment Services in the Context of Crypto Assets as a Means of Payment*. In: C.P. Sempere (ed.), *Governance and Control of Data and Digital Economy in the European Single Market. Legal Framework for New Digital Assets, Identities and Data Spaces*, Vol. 71.

Iwański W. (2025). In: K. Osajda (series ed.), J. Dybiński (volume ed.), *Ustawa o usługach płatniczych. Komentarz*, ed. 5, Warszawa, commentary to Article 2.

Iwański W. (2025a). In: K. Osajda (series ed.), J. Dybiński (ed. volume), *Ustawa o usługach płatniczych. Komentarz*, ed. 5, Warszawa, commentary to Article 3.

Janiak A. (2022). In: M. Gutowski (ed.), *Kodeks cywilny. Tom III. Komentarz. Art. 627–1088*, ed. 3, Warszawa, commentary to Article 725.

Judgment of the Appellate Court in Szczecin of 6 March 2015, I ACa 40/15, LEX No. 1770856.

Judgment of the Supreme Court of 8 December 2010, V CSK 163/10, OSNC-ZD 2011, No. 2, position: 48.

Judgement of the CJEU of 21 March 2019, C-245/18, *Tecnoservice Int. Srl*, ECLI:EU:C:2019:242

Judgement of the CJEU of 4 October 2018, C-191/17, *Bundeskammer für Arbeiter und Angestellte v. ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG*, ECLI:EU:C:2018:809.

Korus K. (2012). *Pojęcie usługi płatniczej w ustawie o usługach płatniczych*, Monitor Prawa Bankowego, No. 7–8.

Korus K. (2024). *Zakres przedmiotowy pojęcia kryptoaktywa w Rozporządzeniu MiCA*, Monitor Prawa Bankowego, No. 7–8.

Michalski M. (2023). In: M. Wierzbowski (ed.), L. Sobolewski (ed.), P. Wajda (ed.), *Ustawa o obrocie instrumentami finansowymi. Komentarz*, ed. 4, Warszawa, commentary to Article 7.

Minto A. (2024). *E-money tokens and coordination issues between Market in Crypto-assets Regulation (MiCAR) and the payment services legislation (PSD2)*, Capital Markets Law Journal, Vol. 19, No. 4.

Pisuliński J. (2025). In: P. Machnikowski (ed.), *Prawo bankowe. Komentarz*, ed. 1, Warszawa, commentary to Article 63c.

Pyzioł W., Walaszek-Pyzioł A. (2012). *Pozycja prawna banku jako wykonawcy usług transferu środków pieniężnych*, Przegląd Prawa Handlowego, No. 3.

Rogoń D. (2012). *Usługi płatnicze powiązane z kredytem na przykładzie umowy o konsumencką kartę kredytową*, Monitor Prawa Bankowego, No. 7–8.

Sójka T., Godlewski M. (2022). In: T. Sójka (ed.), *Obrót instrumentami finansowymi. Komentarz*, Warszawa, commentary to Article 7.

Uzasadnienie rządowego projektu ustawy z 17 maja 2011 r. o usługach płatniczych, Druk Sejmowy VI kadencji, Druk No. 4217.

Włoczka R. (2022). *Pojęcie papieru wartościowego wobec zjawiska tokenizacji*, Kraków, not published.

Wosiak K. (2023). *Depozyt papierów wartościowych w technologii rozproszonego rejestru (DLT) a „własność" papierów wartościowych*, Monitor Prawa Bankowego, No. 11.

Zetzsche D., Sinnig J., Nikolakopoulou A. (2024). *Crypto custody*, Capital Markets Law Journal, tom 19, nr 3.

Safe Bank 2(99) 2025

DOI: 10.26354/bb.17.2.99.2025

Mikołaj Górny*
ORCID: 0000-0003-1363-2077

Critical assessment of regulatory options to prevent abuse on the crypto-asset market

Abstract

The aim of Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA) is, inter alia, to ensure market integrity and protect investors from market abuse, such as manipulation and insider trading. The provisions of Title VI of MiCA form the foundation of the EU regime for counteracting abuse in the crypto-asset market, defining key concepts and regulatory obligations. The article attempts to assess the adequacy, effectiveness, and proportionality of anti-abuse mechanisms in light of the specific nature of the market in question. A formal-dogmatic research method was applied, consisting of an analysis of the legal text in the context of academic literature and the guidelines of international institutions. The results of the study indicate that although the regulation includes provisions prohibiting abuse in the crypto-asset market, significant concerns may arise due to the lack of direct reference to abuses involving derivatives not traded on an organised market, as well as the omission of detailed rules on investment recommendations. The absence of a duty to report managerial transactions on the crypto-assets market can, in turn, be considered a proportionate solution.

Keywords: MiCA, MAR, cryptoassets, market abuse, inside information, market manipulation, investment recommendations, managerial transactions

JEL codes: K22 (Business and Securities Law), K42 (Illegal Behavior and the Enforcement of Law)

Introduction

Modern financial markets play a fundamental role in the economy, enabling effective interaction between the demand and supply of money and the transfer of risk. They serve both private and public interests, allowing cash to flow from surplus entities that dispose of savings to deficit entities that obtain funds necessary for further

* Mikołaj Górny – graduate of the Jagiellonian University in Krakow.

operations (Blicharz et al. 2021, p. 15). Through the free formation of the price of traded securities, the financial market allocates available resources, moving capital to where it is most useful.

As „renouncing current consumption in favor of future uncertain benefits" (Jajuga 2011, p. 15), each investment activity is undertaken under conditions of risk and lack of full access to information. The essence of risk is the possibility of not achieving the expected effect, or more broadly, achieving an effect other than intended (Czerwińska, Jajuga 2016, p. 28).

In this light, institutions and legal regulations on combating abuse in the financial market are essential for the effective development of the market (Woźniak 2023, nb. 1) and for the protection of investor confidence. Investors allocating their financial resources and taking risks have the right to expect to be engaged in a , *level playing field*', in which the success or failure of an investment depends on individual skills, the right decisions and the prevailing economic environment, rather than on the fraudulent actions of other market participants.

A key condition for the smooth functioning of the market is to ensure transparency and equality in access to information. Information asymmetry, resulting from unequal access to knowledge by market participants, is an important source of distortion of price-setting mechanisms (Commission 1977; Explanatory Memorandum 11B). Information relevant to investment decisions should be publicly available, reliable, understandable, precise and timely reported. Their absence, illegibility, misinterpretation or deliberate distortion can lead to artificial price formation, which undermines the market's ability to allocate resources efficiently and threatens the public interest.

What is more, permanent information asymmetry may lead to the disappearance of reliable turnover and the phenomenon of "*race to the bottom*". As George Akerlof (Akerlof 1970) aptly noted, under conditions of asymmetry, " *dishonest dealings tend to drive honest dealings out of the market*," leading to its erosion. Reliable entities may be discouraged from entering a market where financing is more expensive, as investors demand a discount in response to the uncertainty surrounding the information provided.

The broad recognition of the validity of the above principles, namely information transparency, investor protection, the "level playing field," and the pursuit of market efficiency and integrity, entails an obligation for public authorities to implement legal regulations aimed at preventing market abuse, including insider trading, the unlawful disclosure of inside information, and market manipulation (MAR, Recital 7).

With regard to crypto-assets markets, the relevant provisions are contained in Title VI of MiCA. The provisions of this title define inside information (MiCA, Article 87) and prohibit its use (MiCA, Article 89) and unlawful disclosure (MiCA, Article 90), define and prohibit market manipulation (MiCA, Article 91), require immediate, non-discriminatory disclosure of inside information directly relating to the issuer of crypto-assets (MiCA, Article 88) and oblige crypto-asset professionals to prevent, detect and report cases of abuse (MiCA, Article 92).

1. Characteristics of the crypto-asset market

Crypto-assets are a relatively young group of financial assets whose spectrum of applications is not yet fully developed (MiCA, recital 1). In the light of Article 3(1)(5) of MiCA, a 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. MiCA refers only to such assets, with significant exceptions to its scope, as the regulation does not specifically apply to crypto-assets that are financial instruments (MiCA, Article 2(4)(a)) or *non-fungible tokens (*NFTs) (MiCA, Article 2(3)).

The history of crypto-assets begins in 2008, when a person or group of persons under the pseudonym Satoshi Nakamoto published an article titled *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto 2008), which was the theoretical basis for the issuance of the first cryptocurrency – Bitcoin.

Bitcoin debuted as a digital asset that enables *peer-to-peer* transactions based on *distributed ledger technology* (DLT), without the intermediation of a central clearing institution. In the Bitcoin architecture, the trusted third party has been replaced by a *proof of work* mechanism, in which "nodes", i.e. computing devices connected to the system, validate individual transactions, which make up blocks that make up a chain (Nakamoto 2008, p. 3).

This requires public access to information about all transactions in the history of the blockchain, with the anonymity of users being cryptographically secured through the use of public and private key mechanisms. Anyone can see that someone is transferring a certain amount to someone else, but without knowing the identity of the public key holder, it is impossible to link that transaction to a specific person (Nakamoto 2008, p. 6).

Since Bitcoin's inception, thousands of other crypto-assets have debuted on the market. While there is no central issuer for the original cryptocurrency, a large proportion of other crypto-assets are issued by a specific entity, often used to fund its business activities, through a process called ICO (*initial coin offering*), in which the issued crypto-assets are exchanged for investors' cash (Delivorias 2021, p. 3).

Bitcoin units do not have any objectively measurable *intrinsic value*. For this reason, the current price of this currency is determined solely on the basis of expectations about its future price (Berentsen, Schär 2018, p. 7), resulting in significant fluctuations in the exchange rate and high volatility. Similar considerations can also be made for many other crypto-assets, which are subject to sudden and extreme price fluctuations and are speculative in nature, as their price is often based solely on consumer demand (ESAs 2022, p. 2). This feature differentiates crypto-assets, in particular, from units of fiat currency, whose value is protected by monetary authorities (see NBPU, Article 3(1)).

Given the above circumstances, it is important to point out significant regulatory challenges related to the crypto-asset market, in particular in the area of anti-abuse.

The innovative nature of these instruments, their potential anonymity, the frequent lack of methodologically well-established valuation mechanisms, markedly limited intervention of public authorities and high price volatility imply an increased risk of abuse. The above factors impose on the legislator the obligation to develop adequate and – most notably, proportionate – normative solutions.

2. Reception of MAR legal institutions

An in-depth, critical analysis of the provisions contained in Title VI of MiCA requires prior reference to the typology of regulatory instruments used to prevent market abuse developed in the EU legal system, in particular as developed on the basis of MAR. The starting point for such a list should be the observation that the EU legislator, in formulating the MiCA framework, consciously and systemically referred to many years of legislative experience collected in the course of MARs application (Rycerski 2025, p. 33). This is indicated by the obvious linguistic similarity of individual formulations and their similar structure.

The impact of the legislative acquis to date is noticeable even at the initial stage of comparative analysis, in particular within the normative solutions relating to the definition of basic concepts (e.g. confidential information, market manipulation), disclosure obligations and the principles of transparency of market participants. As ESMA points out, referring in turn to the similarities between MiCA and MIFID II, similar concepts should be interpreted in a consistent manner (ESMA 2025). The linguistic similarity between MiCA and MAR is therefore the first important argument for the application of a similar set of criteria to the assessment and interpretation of both regulations, in accordance with the principle prohibiting homonymous interpretation.

Secondly, it should be noted that both the financial instruments market and the crypto-asset market, although structurally and technologically different, perform partially similar functions in terms of capital mobilization and support for investment activities. This functional parallel is highlighted by the EU legislator itself in recital 2 of the MiCA preamble, pointing out that crypto-asset markets play an increasingly important role in financing the economy, including, most notably, SMEs. As a consequence, the *ratio legis* of the regulations contained in MAR and MiCA turns out to be convergent – both legal acts aim to ensure market integrity and an adequate level of investor protection, taking full account of the specifics of the crypto-asset market described above.

It should be emphasized that the explicitly stated objective of anti-market abuse regulation, both in the context of financial instruments and crypto-assets, is to prevent market participants from exploiting information asymmetry, irrespective of the financial tools or structures employed to do so. The essence of market abuse lies in the violation of the principles of fair trading for the purpose of rapidly obtaining above-average profits (Dybiński 2016, pp. 1331–1332), while the agent or instrument involved serves merely as a vehicle for the underlying economic intent.

Regardless of the means used to commit abuse, the ethical justification for its prohibition remains right – abusive transactions, in particular in the form of *insider dealing*, are perceived as "*immoral, unscrupulous, unfair, and vicious attack on the market and investors* " (Macey 1999, p. 269), and This view, which is almost universally[1] accepted in both legal literature and practice, remains decades ahead of contemporary classifications of financial instruments and their technological implementation.

Therefore, also from a teleological perspective, it is justified and methodologically justified to refer to the achievements developed on the basis of MAR, when interpreting and applying the provisions of MiCA. The transposition of this content not only supports the interpretation process, but also promotes the systemic coherence of EU financial markets law, in line with the principle of technology neutrality, which obliges the legislator to treat ICT equally and create conditions for their fair competition (see IDPRZP, Article 3(19)). In the context of financial market law, technological neutrality should imply that regulatory instruments are tailored to the socio-economic nature of the activity, irrespective of the underlying technology employed.

EU legislative acts on financial services should be guided by the principle of '*same activities, same risks, same rules'*, as confirmed by recital 9 of the MiCA. From the systemic point of view, MiCA and MAR should therefore constitute, cumulatively, a complete regulation, aimed at preventing market abuse regardless of the technology used for the transfer of capital or risk and regardless of the technical or organizational conditions in which the transfer takes place. However, one cannot disregard the specific characteristics of the crypto-assets market, which, due to its relatively early stage of development and high degree of dynamism, constitutes an environment inherently suitable for investors with an elevated risk tolerance and expectations of above-average returns. In this context, excessive regulatory intervention may pose a threat comparable in its adverse effects to that arising from an insufficient level of regulation.

3. The principles of proportionality, equality and consistency of the legal system

As part of the assessment of the MiCA regulations, considered in light of the existing EU acquis on market abuse and the relevant academic literature, it is essential to examine the application of the principle of proportionality. Given that the entities subject to the new regulatory regime – such as issuers of crypto-assets or crypto-asset service providers – are often micro, small and medium-sized enterprises, the implementation of solutions similar to those adopted in the financial instruments sector could lead to an excessive regulatory burden (MiCA, recital 95).

[1] See. discussed by Macey 1999; opposing views.

In this context, there is a significant tension between, on the one hand, the need to ensure *a level playing field* and coherent and effective mechanisms to prevent market abuse, and, on the other hand, the need to implement a *bespoke regulatory framework* that will not hamper the development of this still emerging market. This requires particular attention in view of the stated objective of MiCA by the EU legislator to promote innovation, growth and job creation (MiCA, recital 1).

Excessive regulatory complexity and overregulation are among the key barriers to investment and development in the European Union (European Commission 2024, p. 18). Excessive regulatory burdens may, in addition to effectively suppressing sound economic initiative, at the same time create an environment conducive to corruption and the development of activities in the shadow economy (OECD 2011, p. 20), which is a particularly significant threat in the context of distributed ledger technology and the anonymity of transactions.

The waiver of the application of some of the principles described in the MAR to the crypto-asset market should therefore be based on the principle of proportionality. This does not mean that the MiCA regulatory framework is arbitrary – proportionality and market development must not violate the principles of technological neutrality, a level playing field, as well as the necessary investor protection mechanisms and market integrity, as described above.

It becomes necessary to define precisely how the principle of proportionality is to be understood in this context. It should be noted that this principle is explicitly expressed in the primary law of the European Union. Indeed, as stated in Article 5(4) of the Treaty on European Union, '*Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties*'.

The principle of proportionality, as a fundamental legal norm, is grounded in the premise that state authorities, when exercising their conferred powers, must refrain from imposing excessive limitations on the exercise of individuals' fundamental rights and freedoms (Lipniewicz 2015, p. 91). This implies that regulations must be designed to achieve their intended objectives while imposing the least possible burden on entities, and that the obligations imposed should be proportionate to the level of risk generated, that is itself a function of the size and nature of the activity in question.

At the same time, the adopted regulations should ensure a level playing field for entities exposed to comparable risks, irrespective of their legal status (Szpringer, Kasiewicz, Kurkliński 2013, p. 2). Therefore, alongside proportionality, consistency within the legal system is essential, understood as the requirement to avoid unwarranted discrepancies in the treatment of identical or legally comparable situations (Szczucki 2021, Art. 6, nb. 2). The same legal interests as regards the merits should not be treated differently by the legal system due to legally irrelevant criteria. The principle of equality before the law requires the prohibition of unjustified or arbitrary distinctions in legal treatment (Garlicki, Zubik 2016, art. 32, nb. 13).

In other words, the coherence of the legal system requires that legal loopholes cannot be exploited to circumvent the rules and benefit from unfair practices. In this context, a legal loophole refers to a regulatory gap that can reasonably be understood as unintended by the legislator (Supreme Court 2001). It should be noted that the assessment of whether we are dealing with a legally neutral issue or a loophole in the law depends on the knowledge of positive law and the axiological and teleological assumptions of the legislator.

Applying the above considerations to the market abuse law, it should be stated that the departure from the rules known from MAR under MiCA should be based on the principle of proportionality, i.e. it should be justified, generally speaking, by comparing the socio-economic costs of introducing the regulation to the benefits for market integrity and investor protection resulting from it. At the same time, the regulation may not be contrary to the principles of equality of legal entities in the substantive sense and the coherence of the legal system.

In the above context, three selected issues will be considered in turn – the material scope of MiCA and MAR, with particular emphasis on derivatives based on crypto-assets, the abandonment of the regulation of investment recommendations relating to crypto-assets, and the abandonment of the obligation to report transactions of persons performing supervisory functions (PDMR) within the structure of crypto-asset issuers.

4. Subject matter of MiCA and MAR

As previously indicated, MiCA applies exclusively to crypto-assets that do not qualify as financial instruments within the meaning of MIFID II. As a rule, only such value carriers fall within the scope of this regulation, and Title VI of MiCA does not provide any exception to this principle. They relate only to activities relating to crypto-assets admitted to trading or for which an application for admission to trading has been submitted (MiCA, Article 86(1)). Although the regulation covers transactions, orders and behaviours relating to crypto-assets regardless of whether they take place on a trading platform (MiCA, Article 86(2)), it does not, in principle and explicitly, cover financial instruments.

This interpretation is supported by recital 97 of the MiCA, according to which derivatives that qualify as financial instruments under MIFID II and whose underlying asset is a crypto-asset are subject to MAR when traded on a regulated market, MTF or OTF. On the other hand, crypto-assets within the scope of MICA, which are the underlying assets of those derivatives, should be subject to MiCA's market abuse rules. It is clear from the recital that financial instruments within the meaning of MIFID II are subject to the provisions of the MAR on the terms set out therein and are not subject to the MiCA regulation.

Pursuant to Article 2 of MAR, the material scope of this regulation has been indicated by reference to the concept of financial instruments and the place or admission to trading of them. MAR covers financial instruments that are traded on a regulated market, MTFs or OTFs, and in the case of the first two platforms – also instruments that are the subject of an application for admission to trading. MAR does not differentiate financial instruments by their type – its scope includes equity, debt and derivative instruments (Dybiński 2016, 1339). With respect to derivatives, MAR also applies when the security (e.g. CFD or CDS) is based on an underlying instrument that is the subject of organised trading or is subject to an application for admission to such trading (Article 2(1)(d) of MAR).

Therefore, it is reasonable to emphasize that a derivative instrument traded over the counter (i.e. an OTC instrument) does not fall within the scope of MAR unless it is linked to clearly defined underlying assets. These, in turn, in order to be considered for admission to trading on a regulated market, MTF or OTF, must meet the definition of financial instruments within the meaning of MIFID II (see MIFID II, Article 4(1)(21)–(23)).

5. OTC derivatives

Derivatives not traded on a regulated market, in an MTF or an OTF, the underlying of which are crypto-assets that are not financial instruments, are therefore not subject to MAR. Such a conclusion can be drawn from Article 2 of the MAR and follows, *a contrario*, from the wording of recital 97 of the MiCA.

To fully grasp the systemic and practical relevance of this thesis, it is necessary to return to the provisions of MiCA, with a narrowed focus on abuses involving the use of inside information. The prohibition of such conduct in the crypto-asset market is set out in Article 89(1) of MiCA. However, the scope of this provision is determined by the subject matter of the regulation set out in Article 2, as well as by the subject matter of its Title VI defined in Article 86. Consequently, this prohibition does not extend to conduct or instruments that fall outside the scope of MiCA.

A literal interpretation of Article 89(1) of the MiCA leads to an unequivocal conclusion that the submission, modification or cancellation of orders relating to financial instruments (including OTC derivatives) does not fall within the scope of this provision either. It only refers to the "acquisition" or "disposal", "direct" or "indirect" – of crypto-assets. Cancellation or modification of orders also applies only to these assets. Activities involving financial instruments, even if their underlying is a crypto-asset, are not covered by MiCA regulations.

On the basis of the above considerations, it should be concluded that investment behaviour related to OTC derivatives with crypto-assets as an underlying is not covered by either MiCA or MAR.

An entity holding inside information on crypto-assets may, without violating applicable regulations, enter into a transaction on OTC derivatives (e.g. open a position in a CFD contract), obtaining a profit resulting from the information asymmetry in relation to the other party to the transaction and, more broadly, other market participants. With regard to financial instruments, this situation is described in Recital 10, sentence 3 of MAR, according to which: " *Examples of where such instruments can be used for market abuse include inside information relating to a share or bond, which can be used to buy a derivative of that share or bond, or an index the value of which depends on that share or bond".*

From the perspective of the *ratio legis* underpinning European financial market law, such a situation is unacceptable. The purpose of market abuse regulations is to ensure equality among all market participants, to eliminate information asymmetry, and to safeguard market integrity against practices whereby privileged access to information results in unfair, above-average gains. In the scenario at hand, an entity possessing inside information may knowingly exploit its privileged position to derive economic benefit.

Moreover, the literature on the basis of MAR indicates that the purpose of Article 2(1)(d) of this regulation is to counteract circumvention of the provisions (Mucha 2023, Article 2, nb. 15). The scope of application of this regulation is defined in the doctrine as "*broad, watertight and covering essentially all fields of possible market abuse*" (Stokłosa 2021, art. 2, nb. 2). In this context, it cannot be assumed that the lack of application of analogous rules in the crypto-asset market is justified in any way. From an economic point of view, there is an obvious analogy between profiting from abuse in this market and in the financial instruments market.

In particular, it must be emphasized that the exclusion of OTC derivatives – whose underlying asset is a crypto-asset – from the scope of the market abuse prohibition cannot be justified by reference to the principle of proportionality set out in Recital 95 of MiCA. Such an omission constitutes a direct violation of the principles of legal equality and systemic coherence.

The prohibition of insider trading is explicitly enshrined in the text of MiCA and, as such, does not represent a norm that is disproportionate to the specific characteristics of the crypto-assets market. Extending this prohibition to include OTC derivatives merely reinforces and complements the existing framework, rather than establishing a new legal construct, imposing an additional obligation, or introducing a more onerous requirement. On this basis alone, invoking the principle of proportionality to justify the exclusion of such instruments cannot be sustained.

Moreover, it should be emphasized that entities providing services related to OTC derivatives are required to hold the status of an investment firm (MIFID II, Article 5). As professional market participants, investment firms are obliged to implement technical and organisational measures for the detection and prevention of market abuse, as stipulated in Article 16 of MAR. Similarly, Article 92 of MiCA imposes analogous obligations on persons who professionally execute or facilitate

transactions involving crypto-assets. Accordingly, there is no basis for asserting that the absence of sanctions for the type of abuse in question reflects a legitimate application of the principle of proportionality.

In this context, the violation of the principle of equality lies in permitting insiders in the crypto-asset market to exploit inside information by taking positions in OTC derivatives. In contrast, entities engaging directly in transactions involving the underlying crypto-assets, thereby producing a comparable economic effect, are subject to legal sanctions. This unequal treatment is further evident when comparing insiders possessing information about crypto-assets with those holding inside information related to financial instruments, who are clearly subject to stricter regulatory constraints.

The nature of derivative instruments implies that the profit gained by an insider typically corresponds to a loss incurred by the counterparty to the transaction. In the case of many commonly used instruments, such as contracts for difference (CFDs), the counterparty is often the investment firm issuing the instrument, operating under the market maker model (KNF 2023). Lacking access to inside information, the investment firm permits the insider to enter into a transaction at a market price that appears appropriate at the time, but is in fact misaligned in light of the undisclosed information. This creates a clear information asymmetry, ultimately resulting in a financial loss for the investment firm once the information becomes public and the insider closes the position.

If the company hedges its exposure or uses other forms of execution of orders relating to OTC derivatives (e.g. *straight-through-processing*, STP), only the loss-incurring entity may change, but in each case the insider's profit must mean the loss of another market participant. This undermines the integrity of the legal system and poses a threat to the integrity and protection of investors for the financial market.

6. Lack of regulation of investment recommendations

Title VI of the MiCA Regulation does not provide for a separate regulation on investment recommendations in relation to crypto-assets, analogous to that contained in Article 20 of the MAR and the implementing regulations set out in RTS 2016/958. As a consequence, the publication of investment recommendations for crypto-assets is not subject to formal requirements, such as the obligation to disclose conflicts of interest, or substantive requirements, such as the general requirement to maintain the objectivity of the recommendations.

In light of MAR and RTS 2016/958, these obligations are justified by the information asymmetry faced by investors in the capital market, which creates a potential risk of abuse in the area of investment recommendations (Weber 2023, Article 20, nb. 4 and the literature cited therein). An investor relying on a recommendation does not have access to information about the circumstances of its author, and therefore

cannot properly assess their credibility or potential conflicts of interest. Owing to the authority or public recognition of the person issuing the recommendation, the investor may make decisions that they would not have otherwise made, potentially including the acceptance of a higher level of risk. For this reason, authors of recommendations are required to ensure their objectivity, clarity, and precision (RTS 2016/958, Recital 1).

In the context of crypto-assets, particular attention is paid to the role of social media in the dissemination of investment recommendations. This role is significantly more prominent than in the case of traditional financial instruments, which creates additional risks of abuse (ESMA 2025b, p. 6). Market practice concerning financial instruments has already demonstrated the need to issue a separate warning directed at entities publishing recommendations on social media (ESMA 2024), which confirms the significance of the problem in this area as well. However, the absence of equivalent requirements in MiCA makes it impossible to effectively address undesirable phenomena, such as non-transparent recommendations.

In the empirical literature, particular attention is given to the use of automated accounts (bots) in the dissemination of manipulative investment recommendations, especially as a component of *pump and dump* schemes (Nizzoli 2020). These accounts, often created *en masse* on social media platforms such as X and Telegram, are designed to artificially amplify investor interest and create the illusion of widespread popularity surrounding a given crypto-asset project.

The absence of specific requirements governing the content of investment recommendations – such as the obligation to disclose the identity of the author (RTS 2016/958, Article 2(1)) or the duty to distinguish facts from opinions and to indicate sources of information (RTS 2016/958, Article 3(1)) – significantly hampers efforts to prevent the dissemination of unreliable recommendations. In light of these existing rules applicable to financial instruments, the use of fictitious accounts to distribute purportedly authored recommendations misleads recipients regarding the identity of the author and may constitute unlawful conduct.

The only, albeit narrowly defined, limitation on the freedom to issue investment recommendations concerning crypto-assets is set out in Article 91(2)(c) of MiCA, supplemented by the example provided in Article 91(3)(c). These provisions address the dissemination of false or misleading signals regarding crypto-assets, including the publication of opinions in mass media following the acquisition of a position in those assets and profiting from the recommendation's impact without adequately disclosing a conflict of interest. It can be assumed that the normative scope of these regulations is generally confined to the most egregious forms of abuse – namely, deliberate falsehoods or manipulative conduct concerning crypto-assets.

In particular, the example set out in Article 91(3)(c) of MiCA does not encompass situations where a recommendation is made by a person acting on behalf of the asset holder but who does not personally hold a position in the crypto-asset concerned. This marks a key distinction from Article 20 of MAR, which adopts

a broader regulatory approach – the disclosure of a conflict of interest constitutes a positive obligation, irrespective of the legal or factual basis of the relationship. Where the entity issuing a recommendation concerning a crypto-asset is neither the issuer nor subject to specific obligations to shape the marketing message (see, for example, MiCA Article 7(1)(b)), a recommendation that does not fall under the prohibition in Article 91(2)(c) – i.e., it does not convey false or misleading signals – remains beyond the reach of regulatory scrutiny.

Given the difficulties identified in the literature with regard to determining the intrinsic value of many crypto-assets – which often fail to generate any predictable stream of cash flows – there is a significant risk that conduct highly problematic from the standpoint of investor protection and market integrity may fall outside the scope of market manipulation as defined in Article 91(2)(c) of MiCA. Extreme opinions expressed about crypto-assets, including those disseminated through automated means such as bots, will not be subject to sanctions unless they are demonstrably false or misleading. In light of the subjective and speculative nature of these assets – whose value is determined solely by supply and demand – there may be serious challenges in effectively operationalizing the relevant provision.

To conclude, the absence of comprehensive regulation regarding positive obligations related to investment recommendations for crypto-assets warrants critical assessment. The principle of proportionality cannot be invoked in this context – the provisions of Article 20 of MAR, together with RTS 2016/958, which apply to all investment recommendations (regardless of whether they are issued by professionals within the meaning of Article 3(1)(34)(i) of MAR), provide adequate and proportionate solutions. On the one hand, they offer effective safeguards against the widespread dissemination of unreliable recommendations via social media; on the other, they avoid imposing excessive administrative burdens on market participants. The absence of analogous provisions in MiCA is therefore unjustified.

7. Absence of Regulation on the Disclosure of Managerial Transactions

In the area of financial instrument trading, the obligation to report managerial transactions is governed by Article 19 of MAR. This provision applies to two categories of persons: those discharging managerial responsibilities within the issuer's structure and persons closely associated with them (MAR, Article 19(1)). These individuals are required to report transactions involving the issuer's shares or debt instruments, as well as, in particular, investments in other financial instruments that result in a comparable economic exposure (see RTS 2016/522, Article 10(2)).

The *ratio legis* of Article 19 of MAR is to ensure transparency in the activities of persons performing managerial functions. This provision serves as a preventive tool against market abuse, particularly insider trading (MAR, Recital 58). At the same

time, disclosed managerial transactions constitute a valuable source of information for market participants, offering insight into how the issuer's situation is perceived by its management. In this context, Article 19 functions as a mechanism for reducing information asymmetry (Kalss et al. 2021, p. 348). The aim of the regulation is to enable investors to make independent assessments of the significance of such transactions – particularly as to whether they may be interpreted as buy or sell signals.

In the context of the crypto-asset market, there are analogous grounds for introducing regulations governing the transactions of individuals holding managerial positions within the structures of crypto-asset issuers. Such individuals may possess inside information, and a reporting obligation could function as a form of social oversight over managerial activity. At the same time, this would align with the principles of transparency and accountability – values that constitute a kind of *idée fixe* within communities centered around distributed ledger technology.

This issue is particularly important given the widespread occurrence of *pump and dump* manipulation in the crypto-asset market, in which individuals holding key functions within the issuer's structure may be involved. The literature highlights that the anonymity characteristic of this market heightens investor vulnerability to such forms of abuse (Mirtaheri et al. 2021, p. 607). It can therefore be *prima facie* assumed that increased transparency in managerial transactions could help mitigate such practices. In particular, a sudden sell-off of crypto-assets by the issuer's executives may be perceived by market participants as a warning signal, suggesting that those with privileged information consider the asset to be overvalued and anticipate the onset of a "dump" phase.

On the other hand, it should be acknowledged that classic *pump and dump* schemes orchestrated via social media are often unrelated to any actions taken by the issuer of the crypto-asset. These schemes typically involve the artificial promotion of a selected asset by a coordinated group of individuals (Mirtaheri et al. 2021, p. 607), whose sole aim is to trigger a short-term, abrupt price movement, without any intention of pursuing a sustained strategy or long-term involvement with the asset. Notably, a common practice involves the organizer of the "pump" creating a group in an encrypted messaging application and notifying participants of the impending operation, initially without even revealing which asset the campaign targets (Constantino 2022, p. 3).

Attention should also be drawn to the temporal dimension of disclosure – specifically, the interval between the execution of a transaction and its public announcement. Under MAR, there is a considerable delay between these two events. The person subject to the reporting obligation must notify both the issuer and the competent authority without delay, but no later than three business days following the transaction (MAR, Article 19(1)). The issuer, in turn, has two additional business days from the date of receipt of the notification to make the information public (MAR, Article 19(3)). This mechanism – effectively a compromise between reducing information asymmetry and avoiding excessive administrative burdens – is

justifiable within the financial instruments market. However, it may be inadequate in the context of the crypto-asset market, which is marked by high volatility and rapid trading dynamics. In such a setting, disclosure received five business days after the transaction may lose its practical relevance. At the same time, significantly shortening this period could risk breaching the principle of proportionality by imposing unduly burdensome obligations on crypto-asset issuers.

Moreover, in the crypto-asset market, the signaling function is often performed by analytical tools that enable the monitoring of individual participants' holdings – an outcome made possible by the transparent and decentralized nature of distributed ledger technology. In this context, public keys assigned to individual wallets serve as identifiers. By analyzing the transaction history associated with a given key, it is possible to estimate the value of the assets held and, consequently, to identify market participants of significant influence (commonly referred to as "whales") whose investment decisions can have a measurable impact on market dynamics (Chernoff, Jagtiani 2024, p. 3). These entities may have no formal relationship with the issuer of a particular crypto-asset. Nonetheless, the observation of their investment activity carries an important signaling function for other market participants.

With respect to transactions conducted outside the main register of a given crypto-asset (i.e. off-chain transactions), such as those recorded in the internal books of custody service providers, MiCA imposes an obligation to implement mechanisms for the prevention, detection, and reporting of market abuse – specifically through the STOR (Suspicious Transactions and Orders Reporting) procedure (MiCA, Article 92(1)). While these obligations do not substitute for the traditional signaling function associated with the reporting of managerial transactions, they serve as an important complementary tool in the prevention of insider trading and market manipulation.

To conclude, imposing obligations on crypto-asset issuers and their management analogous to those set out in Article 19 of the MAR Regulation appears disproportionate. While such instruments may serve a specific signaling and preventive function, their effectiveness in light of the unique characteristics of the crypto-asset market is subject to legitimate doubt. These regulatory objectives could be pursued through alternative, less burdensome measures – an especially important consideration given that issuers of crypto-assets are often SMEs.

Summary

Title VI of MiCA constitutes a regulation of fundamental importance for establishing a stable and transparent legal framework governing the functioning of the crypto-asset market. Undoubtedly, the introduction of prohibitions on insider trading, the unlawful disclosure of inside information, and measures to counter market manipulation represent essential steps toward safeguarding investor interests and upholding market integrity.

While it is reasonable to acknowledge that not all mechanisms provided under MAR should be automatically extended to the crypto-asset market – given the distinct structure, dynamics, and composition of crypto-assets – it must be strongly emphasized that the omission of certain key areas significantly undermines the effectiveness of the adopted regulatory model. In particular, the absence of regulation concerning the OTC derivatives market based on crypto-assets appears to be an unacceptable oversight in light of the objectives pursued by anti-market abuse legislation.

An equally significant shortcoming is the absence of detailed regulations governing investment recommendations related to crypto-assets – an area which, as market practice demonstrates, can be exploited as a tool for manipulation, particularly within social media environments.

For these reasons, it should be concluded that although Title VI of MiCA represents a significant step toward establishing the legal legitimacy of the crypto-asset market, its selective and fragmented approach to specific market segments and communication practices risks undermining the effectiveness of the overall regulatory regime. A consistent and comprehensive implementation of anti-abuse objectives will require future revision and expansion of the framework – particularly in areas most susceptible to abuse.

It is necessary to bear in mind the risks associated with the potential overregulation of this nascent market, a concern explicitly acknowledged in selected recitals of MiCA. The adoption of an excessively restrictive approach, in particular through the full application of comprehensive normative frameworks analogous to those applicable to financial instruments (MIFID II, MAR) is unjustified. Regardless of the final shape of the regulatory framework, particular importance should be attached to investor education and to ensuring that investors are fully aware of the scale of risks they may face. While investors should retain the right to undertake risk, such a right must be preceded by reliable and adequate warnings regarding the potential threats involved.

Bibliography

Akerlof G.A. (1970). *The Market for „Lemons": Quality Uncertainty and the Market Mechanism*. The Quarterly Journal of Economics, 84(3), 488–500. doi: 10.2307/1879431 (accessed 17.05.2025).

Berentsen A., Schär F. (2018). *A Short Introduction to the World of Cryptocurrencies*. Federal Reserve Bank of St. Louis Review, 100(1), 1–16. doi:10.20955/r.2018.1-16.

Blicharz G., Oręziak B., Wielec M. et al. (2021). *Rynek finansowy: Zapobieganie przyczynom przestępczości*. In: M. Wielec, B. Oręziak, G. Blicharz (eds.), Warszawa: Instytut Wymiaru Sprawiedliwości, [online] https://iws.gov.pl/wp-content/uploads/2021/07/Rynek-finansowy_DRUK.pdf (accessed 17.05.2025).

Chernoff A., Jagtiani J. (2024). *Beneath the Crypto Currents: The Hidden Effect of Crypto "Whales"*. Philadelphia: Federal Reserve Bank of Philadelphia, Working Paper 24–14, [online] https://www.philadelphiafed.org/-/media/frbp/assets/working-papers/2024/wp24-14.pdf (accessed 17.05.2025).

Constantino J. (2022). *Why are cryptocurrencies vulnerable to pump-and-dump schemes in Europe?*, Amsterdam Law Forum, 14, p. 8, [online] https://doi.org/10.37974/ALF.444 (accessed 17.05.2025).

Czerwińska T., Jajuga K. (2016). *Ryzyko instytucji finansowych: Współczesne trendy i wyzwania*. Warszawa: C.H. Beck.

Delivorias A. (2021). *Understanding initial coin offerings: A new means of raising funds based on blockchain*. Briefing. Luksemburg: Europejskie Centrum Wydawnicze Parlamentu Europejskiego. PE 696.167 – Lipiec 2021. [pdf] European Parliamentary Research Service (EPRS), https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI(2021)696167_EN.pdf (accessed 17.05.2025).

Dybiński J. (2016). *Rozdział 25. Ochrona przed nadużyciami na rynku instrumentów finansowych*. In: M. Stec (ed.), *Prawo instrumentów finansowych. System Prawa Handlowego. Tom 4*. Warszawa: C.H. Beck.

Komisja Europejska (2024). *The future of European competitiveness: A competitiveness strategy for Europe. Part A*. Luksemburg: Urząd Publikacji Unii Europejskiej, [online] https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en (accessed 17.05.2025).

ESAs (2022). Europejskie Urzędy Nadzoru (EBA, ESMA i EIOPA), *Wspólne ostrzeżenie dla konsumentów dotyczące ryzyk związanych z kryptoaktywami*. [pdf] ESA 2022 15, 17 marca 2022. Paryż: Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA), https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf (accessed 17.05.2025).

ESMA (2024). Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA), *Ostrzeżenie dla osób publikujących rekomendacje inwestycyjne w mediach społecznościowych*. [pdf] ESMA, numer dokumentu: ESMA74-1103241886-912, 6 lutego 2024, https://www.esma.europa.eu/sites/default/files/2024-02/ESMA74-1103241886-912_Warnings_on_Social_Media_and_Investment_Recommendations.pdf (accessed 17.05.2025).

ESMA (2025a). Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA), *ESMA_QA_2463 – Do "copy trading services" (also referred as "auto trading services") related to crypto-assets fall within the scope of portfolio management or any other crypto-asset services as listed in Article 3(1)(16) of MiCA?* [online] https://www.esma.europa.eu/publications-data/questions-answers/2463 (accessed 17.05.2025).

ESMA (2025b). Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA), *Raport końcowy: Wytyczne dotyczące praktyk nadzorczych organów krajowych w zakresie zapobiegania i wykrywania nadużyć rynkowych zgodnie z rozporządzeniem MiCA*. [pdf] ESMA, numer dokumentu: ESMA75-453128700-1408, 29 kwietnia 2025. Dostępne na: https://www.esma.europa.eu/sites/default/files/2025-04/ESMA75-453128700-1408_Final_Report_MiCA_Guidelines_on_prevention_and_detection_of_market_abuse.pdf (accessed 17.05.2025).

Garlicki L., Zubik M. (eds.) (2016). *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II*. Wyd. 2. Warszawa: Wydawnictwo Sejmowe.

IDPRZP – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2024 r. poz. 1557).

Jajuga K., Jajuga T. (2011). *Inwestycje: Instrumenty finansowe, aktywa niefinansowe, ryzyko finansowe, inżynieria finansowa*. Wyd. 1. Warszawa: Wydawnictwo Naukowe PWN.

Kalss S., Oppitz M., Torggler U., Winner M. (eds.) (2021). *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 596/2014*. Elgar Commentaries in Financial Law. Cheltenham–Northampton: Edward Elgar Publishing, https://doi.org/10.4337/9781800882249 (accessed 17.05.2025).

Komisja (1977). *Zalecenie Komisji z dnia 25 lipca 1977 r. dotyczące europejskiego kodeksu postępowania w zakresie transakcji papierami wartościowymi zbywalnymi (77/534/EWG)*. *Dziennik Urzędowy Wspólnot Europejskich*, L 212, 20.8.1977, pp. 37–43, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A31977H0534 (accessed 17.05.2025).

KNF (2023). Komisja Nadzoru Finansowego, *Czym się charakteryzuje broker działający w modelu Market Maker?* [online] Dostępne na: https://www.knf.gov.pl/dla_rynku/forex/pytania_i_odpowiedzi (accessed 17.05.2025).

Lipniewicz R. (2015). *Zasada proporcjonalności a podatkowe ograniczenia swobód rynku wewnętrznego Unii Europejskiej*. Ruch Prawniczy, Ekonomiczny i Socjologiczny, 77(4), pp. 93–103. [online] Dostępne na: https://pressto.amu.edu.pl/index.php/rpeis/article/view/4276/4345 (accessed 17.05.2025).

Macey J.R. (1999). *Securities Trading: A Contractual Perspective*. Case Western Reserve Law Review, 50(2), pp. 269–283, https://scholarlycommons.law.case.edu/caselrev/vol50/iss2/10 (accessed 17.05.2025).

MAR, Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE (Dz.U. L 173 z 12.6.2014, s. 1–61).

MiCA, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.U. L 150 z 9.6.2023, pp. 40–205).

MIFID II, Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, pp. 349–496).

Mirtaheri M., Abu-El-Haija S., Morstatter F., Ver Steeg G., Galstyan A. (2021). *Identifying and analyzing cryptocurrency manipulations in social media*. IEEE Transactions on Computational Social Systems, 8(3), pp. 607–617, [online] https://doi.org/10.1109/TCSS.2021.3059286 (accessed 17.05.2025).

Mucha A. (2023). Artykuł 2 Rozporządzenia nr 596/2014. In: J. Dybiński (ed.), *Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE. Komentarz*. Wyd. 1. Warszawa: C.H. Beck.

Nakamoto S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online] https://bitcoin.org/bitcoin.pdf (accessed 17.05.2025).

NBPU – ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz.U. z 2022 r. poz. 2025).

Nizzoli L., Tardelli S., Avvenuti M., Cresci S., Tesconi M., Ferrara E. (2020). *Charting the Landscape of Online Cryptocurrency Manipulation*. *IEEE Access*, PP, p. 1–1, [online] https://doi.org/10.1109/ACCESS.2020.3003370 (accessed 17.05.2025).

OECD (2011). *Administrative Simplification in Poland: Making Policies Perform, Cutting Red Tape*. Paris: OECD Publishing. [online] https://doi.org/10.1787/9789264097261-en (accessed 17.05.2025).

RTS (2016/522). Rozporządzenie delegowane Komisji (UE) 2016/522 z dnia 17 grudnia 2015 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 w kwestiach dotyczących wyłączenia niektórych organów publicznych i banków centralnych państw trzecich, okoliczności wskazujących na manipulację na rynku, progów powodujących powstanie obowiązku podania informacji do wiadomości publicznej, właściwych organów do celów powiadomień o opóźnieniach, zgody na obrót w okresach zamkniętych oraz rodzajów transakcji wykonywanych przez osoby pełniące obowiązki zarządcze podlegających obowiązkowi powiadomienia (Dz.U. L 88 z 5.4.2016, pp. 1–18).

RTS (2016/958). Rozporządzenie delegowane Komisji (UE) 2016/958 z dnia 9 marca 2016 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 w odniesieniu do regulacyjnych standardów technicznych dotyczących środków technicznych do celów obiektywnej prezentacji rekomendacji inwestycyjnych lub innych informacji rekomendujących lub sugerujących strategię inwestycyjną oraz ujawniania interesów partykularnych lub wskazań konfliktów interesów (Dz.U. L 160 z 17.6.2016, pp. 15–22).

Rycerski A. (2025). *Definicja informacji poufnej na rynku kryptoaktywów oraz rynku instrumentów finansowych*. Przegląd Ustawodawstwa Gospodarczego, 78(1), pp. 32–39, [online] https://doi.org/10.33226/0137-5490.2025.1.5 (dostęp 17.05.2025).

Sąd Najwyższy (2001). Postanowienie Sądu Najwyższego z dnia 25.05.2001 r., WA 15/01, OSNKW 2001, nr 9–10, poz. 81.

Stokłosa A. (2021). Artykuł 2 Rozporządzenia MAR. In: S. Syp, A. Stokłosa (eds.), *MAR. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie nadużyć na rynku. Komentarz*. Wyd. 2. Warszawa: Wolters Kluwer Polska.

Szczucki K. (2021). *Ustawa o Sądzie Najwyższym. Komentarz*. Wyd. 2. Warszawa: Wolters Kluwer Polska.

Szpringer W., Kasiewicz S., Kurkliński L. (2013). *Zasada proporcjonalności a polski sektor bankowy. Uwarunkowania, narzędzia, szanse, zagrożenia*. Warszawa: ALTERUM – Ośrodek Badań i Analiz Systemu Finansowego, Zakład Warszawskiego Instytutu Bankowości, [online] http://alterum.pl/uploaded/Tresc_raportu_-_Zasada_proporcjonalnosci_a_polski_sektor.pdf (dostęp 17.05.2025).

Weber A.M. (2023). *Artykuł 20 Rozporządzenia nr 596/2014*. In: J. Dybiński (ed.), *Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku […] Komentarz*. Wyd. 1. Warszawa: C.H. Beck.

Woźniak R. (2023). *Artykuł 1 Rozporządzenia nr 596/2014*. In: J. Dybiński (ed.), *Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE. Komentarz*. Wyd. 1. Warszawa: C.H. Beck.

Safe Bank 2(99) 2025

DOI: 10.26354/bb.18.2.99.2025

Łukasz Hardt*
ORCID: 0000-0001-6542-5833
lhardt@wne.uw.edu.pl

Is Programmable Central Bank Digital Currency (PCBDC) Money? Some Remarks from the Ontology of Money Perspective

Abstract

The goal of this paper is to investigate whether programmable central bank digital currency (PCBDC) qualifies as money under different ontological theories of money. This study shows that according to the state theory, it qualifies as money, under the institutional theory, it has the potential to be money, and from the perspective of the credit theory, it is money but with important caveats. This paper refers to current debates regarding CBDCs, and by using the perspective offered by various ontological theories of money it sheds a new light on these issues.

Keywords: Programmable central bank digital currency (PCBDC), digital money and finance, ontology and philosophy of money

JEL codes: E42, E51, B52

Introduction

What is money? Does money have intrinsic value? What is the essence of money? Where does money come from? What makes money persist while in use? Does money simply exist because people believe it does? Is it necessary for something to be backed by state authority to be qualified as money? These questions concern the ontology of money.

The above questions are definitely not new, they have been asked by philosophers and economists for centuries. In particular, it was Aristotle who proposed the so-called commodity theory of money which treats money as a commodity serving as a medium of exchange, a unit of account, and a store of value. In order to perform

* Łukasz Hardt – University of Warsaw, and Advisor to the Chair of the KNF Board.

these functions, a commodity qualified as money should be easy to store and transport as well as to be measured and divided to facilitate calculations. Also, it should be difficult to destroy.

A different theory of money is the one seeing money as a social construction, namely a credit relation (see, e.g., Ingham 2004). Here money represents a claim on goods or services. In other words, every unit of money is a record of a debt. For a credit relation to serve as money, it should be sufficiently credible and the credit should be transferable, namely acceptable by others as payment for trade. There is a general agreement that the most creditworthy issuer of credit money is the state[1].

In recent years, due to technical progress, new forms of money have emerged, e.g., electronic money, cryptocurrencies, and central bank digital currencies (CBDCs). This has attracted the attention of economists, who question whether these can be classified as money (e.g., Passinsky 2020). A special case is programmable CBDC (PCBDC), which incorporates built-in rules (code) that govern its use, for instance, limiting spending to certain goods, imposing expiration dates, or adjusting interest automatically. The goal of this paper is to investigate whether PCBDC qualifies as money under different ontological theories of money. Such a question is not only theoretically worth asking, but also has important practical consequences. In this context, reference can be made to various legal disputes regarding whether Bitcoin is money and correspondingly to different positions in court rulings (see, e.g*., SEC v. Shav*ers 2013, or *United States v. Ulbricht* 2014). It is easily imaginable that the very same issue can be raised in hypothetical legal and court proceedings regarding PCBDC.

The question we are asking here is very up-to-date. Various central banks around the globe are preparing their CBDCs. For instance, the European Commission states in the following way the reasons for introducing the digital euro:

> "In the euro area, the establishment of a retail CBDC – the digital euro – is necessary to supplement cash and adapt the official forms of the currency to technological developments, so that the euro can be used as a single currency, in a uniform and effective manner across the euro area" (COM(2023) 369 final).

However, in the very same document there is a clear statement that CBDC to be issued by the European Central Bank under no circumstances will take the form of a programmable CBDC, i.e., "The digital euro would not be programmable money and could therefore not be used to limits its spending to or direct it at specific goods or services: as a digital form of the single currency, it should be fully fungible" (ibid.). Very recently, various representatives of the ECB have called for a swift introduction of the digital euro, also due to rising risks of geopolitical fragmentation and a need for the European Union to maintain control over its monetary and financial system – a diplomatically framed argument for reducing reliance on US-based payment providers (Lane 2025).

[1] For more insights regarding general ontological theories of money, see, e.g., de Bruin et al. (2023).

A more open approach towards programmability of their CBDC is presented by the Chinese authorities. Although digital yuan (e-CNY) is not par excellence programmable, it has specific functions easing its use in programmable payments, namely smart-contract and conditional-payment features. Moreover, in 2023, the People's Bank of China conducted a pilot study in Chengdu, distributing e-CNYs that were programmed to allow payments for public transport only. Some representatives of the Chinese financial authorities are openly suggesting adding a programmable dimension to the e-CNY in the future[2]. The situation is quite the opposite in the United States, where President Donald Trump, in his Executive Order of January 23, 2025, prohibited any actions aimed at creating a digital dollar.

This paper proceeds as follows. Section 2 presents various theories referring to the ontologies of money. Next, Section 3, discusses in detail characteristics of PCBDC. Then, in Section 4, it is answered which ontological views on money allow PCBDC to be qualified as money. Conclusions follow.

1. Disentangling different ontological theories of money

In the above introductory remarks, we referred to two important traditions in the ontology of money. Since the commodity theory of money is of little use nowadays, as most money is fiat money, we should primarily refer to various theories treating money as a specific institution. An insightful instantiation of such a view is a perspective offered by J. Searle in *The Construction of Social Reality* (1995) where money is an institutional fact or, in other words, a kind of a commonly shared belief:

> "in order that the concept 'money' apply to the stuff in my pocket, it has to be the sort of thing that people think is money. If everybody stops believing it is money, it ceases to function as money, and eventually ceases to be money" (32).

And next he adds: "Most money is now in the form of magnetic traces on computer disks. It does not matter what the form is as long as it can function as money" (34–35). So, here we have a definition of money in terms of its function (what money does) rather than of its structure (what money is made of). Such definitions are typical of institutions, and the primary task of institutions is to facilitate exchange. So, here we have money-as-an-institution ideal, as Guala (2020) nicely explains: "To say 'X is money' is a shorthand for a complex list of possible actions for the proper use of object X, which is regulated by money-as-an-institution. Actions such as purchasing, borrowing, saving, betting, inheriting, and so forth" (275). On a more metaphysically rich understanding, money consists of "deontic power to buy, pay, and close debts" (Searle 2017, 1463), granting individuals "the ability to buy and sell and the ability

[2] See, e.g., a 2023 statement by Mr. Lu Lei, deputy administrator of the State Administration of Foreign Exchange, as reported by Reuters (https://www.reuters.com/markets/currencies/china-fx-regulator-says-cbdc-features-could-improve-monetary-policy-2023-10-13/).

to incur and pay debts" (Searle 2017, 1466)[3]. Everyday statements such as "the purchasing power of money" can be framed in this way.

Stating that money is an important institution easing market exchange means that it reduces transaction costs what should motivate individuals to use money. However, once it ceases to perform this function, it is no longer money. For instance, if a given currency is subject to hyperinflation, people are more willing to use different currencies, and thus the malfunctioning currency starts to lose its status as money. In this context, Hindirks (2024, 20) states that "bills and coins are artifacts that can but need not be money. What ultimately matters for being money is not whether an entity is accepted as such, but whether it performs its functions". One reservation is in order here: something can be partially money, meaning it does not fulfill all the functions that money should have[4]. Or, in other words, it has the potential to become a widely used form of money, but it has not yet fully achieved this status due to volatility, limited acceptance, and regulatory concerns. Some cryptocurrencies (probably) have such a status, at least for now.

Let us come back to the just disregarded commodity theory of money, and let us have a closer look at what *commodity* can mean. Historically, as we have mentioned earlier, it was a particular commodity, for instance, a cow, a barrel of oil, or a golden coin. In modern monetary systems such a theory is generally claimed to be untenable, however, what if we introduce the idea of a universal commodity, namely an abstract commodity which is exchangeable for all others? For instance, in Walras' moneyless economic model, the numeraire represents the pre-existing value of a randomly selected commodity, serving as the reference standard of value against which the exchange rates between commodities are calculated. But this randomly selected commodity can be a kind of an abstract commodity being introduced *artificially* to serve as money. There is a long tradition in economics to treat this commodity as a kind of lubricate that facilitates market exchange as Hume once famously said: "Money is not, properly speaking, one of the objects of commerce, but only an instrument. It is none of the wheels of trade: it is the oil which renders the motion of the wheels smooth and easy" (Hume 1792). In modern interpretation, "As opposed to the *commodity* cigarette, the *monetary* cigarette in any cigarette *standard* would be an *abstract* cigarette" (Ingham 2004, 25). We will use these terms later in describing PCBDCs. For now, let us just describe such a view on what money is as the abstract-commodity theory of money.

What is common to all the above-discussed theories of money is that money, whether treated as a commodity or as an institution, emerges spontaneously from human interactions. It is only after evolutionarily emerged that it is backed by state authority, though state intervention cannot be considered a condition sine qua non for the persistence of money in market exchange. In such a perspective, "Money is

[3] For more insights regarding Searl's views on money, see, e.g., Hindriks (2024).

[4] Some authors debating these issues introduce a distinction between the nominal essence of money and its real essence, however, referring to such debates is beyond the scope of this paper (more philosophically oriented readers are advised to look into, for instance, Mäki (2020)).

not a medium that emerges from exchange. It is rather a means for accounting for and settling debts, the most important of which are tax debts" (ibid., 47). So, here we have the state theory of money with its central claim that it is impossible to understand money "without the idea of the state" (Knapp 1973, vii–viii). Here, the state is not primarily issuing money rather it is accepting what can be qualified as money, namely a means to pay taxes.

An interesting *example* of this theory *in practice* was the proposal of the former Italian government in 2018 to allow Italian citizens to pay their taxes with Italian government bonds. If this were to happen, then according to this theory, these bonds would become a form of money. This proposal was met with clear criticism from M. Draghi, the then-governor of the ECB, saying: "They are either money, and then they are illegal, or they are debt, and then that stock goes up […]. It is either money or debt, and I do not think there is a third possibility" (2019). In this sense, if a given government were to accept, for instance, Bitcoin as payment for taxes, then Bitcoin would be considered money[5].

Let us return to our considerations on the ontology of money. The state theory of money described above can be understood as a view in which money is exogenously created, namely through the state's act of accepting something as a means of paying taxes. On the other hand, however, we have endogenous money theories where "first, loans make deposits, second, deposits make reserves, and third, money demand induces money supply" (Wray 1990, 73–74). Proponents of exogenous money theory recognize that the banking system generates credit money, but maintain that the central bank retains control over this process through its ability to issue high-powered base money as reserves for the system. Nevertheless, in all these theories money is a kind of credit relation.

Now, on a more sociological front, money is seen as a symbolic medium of communication and interaction. Also, especially in the Weberian tradition, money is not a neutral veil but "a weapon in this struggle [for economic existence], and prices are expressions of this struggle; they are instruments in this struggle only as estimated quantifications of relative chances in this struggle" (Weber 1978, 108). However, money *qua* weapon is not a very useful concept to be employed in answering the central question of our paper. But still, it underlines the very fact that what is accepted as money has important redistributive consequences. Being in the field of sociology, it is worth turning to Simmel's *The Philosophy of Money*, which is however more focused on what money does to society rather than on what money is. Nevertheless, he criticised the commodity theory of money and states that "money

[5] For instance, in an official statement from 2014 the US Internal Revenue Service (IRS) announced that it would treat virtual currencies not as currency for federal tax purposes: "The IRS is aware that 'virtual currency' may be used to pay for goods or services, or held for investment. Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like 'real' currency […] is customarily used and accepted as a medium of exchange in the country of issuance – but it does not have legal tender status in any jurisdiction" (IRS Notice 2014-21). It was confirmed more recently in IRS Notice 2023-34.

is only a claim upon society" (1978, 177). So, for him, the very existence of money results from individuals' beliefs that something is money, and such a belief system is a kind of a "social-psychological quasi-religious faith" (ibid., 178). In other words, money is a cultural fact. Once money *exists* in individuals' minds as a shared mental model, it can then be represented symbolically. It is insightfully, and metaphorically, described in Y. Harari's *Sapiens*:

> "[...] money is also the apogee of human tolerance. Money is more open-minded than language, state laws, cultural codes, religious beliefs and social habits. Money is the only trust system created by humans that can bridge almost any cultural gap, and that does not discriminate on the basis of religion, gender, race, age or sexual orientation. Thanks to money, even people who don't know each other and don't trust each other can nevertheless cooperate effectively" (2015, 177).

So, money is here conceptualised as a trust system. It is similar to view money as an institution enabling human cooperation.

What we have done above legitimizes us to claim that the dominant ontological theories of money locate money in collective agreement, credit relationships, and state law, rather than in innate properties of objects. Most functionalists traditions, on the other hand, define money, including its existence, by its roles and functions. What needs to be added here, however, is that the intrinsic properties (functions) of money, such as its power to enable the purchase of goods, can be offset by external conditions, such as a legal system that prohibits the use of a given form of money. A necessary condition for money's proprieties (functions) to be actualised is that money must be used. Also, what should be now clear is that a given *X* can be money under, say, functionalist ontological theory of money, but at the same time not according to state theory if *X* is not legally backed by the state. Although studying this is definitely beyond the scope of this paper, it is unlikely that *X*, accepted as money by a given state authority, can persist in the long term if it is stripped of the typical functions of money, namely a medium of exchange, a unit of account, and a store of value.

In what follows, we will discuss the key characteristics of CBDCs, especially those with programmable features. Next, we will return to various ontological theories of money to examine under which theories a PCBDC qualifies as money.

2. Central bank digital currencies with programmable features

We now have examples of central banks that have introduced their own digital currencies, albeit with caution and various limitations, e.g., the digital yuan issued by the People's Bank of China. Several other major central banks, including the ECB, are now on the verge of doing the same. Although the idea of expanding access to digital central bank liabilities dates back at least to Tobin (1985), recent developments in the area were stimulated by advancements in financial-sector technologies, new competitors entering payment and intermediation markets, a noticeable drop in

cash usage in some countries, and growing focus on privately issued digital tokens (BIS 2018, 3).

There is still an ongoing debate concerning how to best define central bank digital currencies, especially on how to distinguish CBDCs from other forms of electronic money, including reserves. Here are some definitions:

> "[...] a CBDC is a digital form of central bank money that is different from balances in traditional reserve or settlement accounts" (ibid., 4).
>
> "digital euro denotes a liability of the Eurosystem recorded in digital form as a complement to cash and central bank deposits" (ECB 2020, 6).
>
> "digital euro means the digital form of the single currency available to natural and legal persons" (COM(2023) 369 final).
>
> "Central Bank Digital Currencies (CBDCs) are digital representations of sovereign currency that is issued by a jurisdiction's monetary authority and appears on the liability side of the monetary authority's balance sheet" (OECD 2023, 5).

All of these definitions share the idea that CBDC is a form of central bank money that is digital, universally accessible, issued by the central bank, and implemented either as tokens or through accounts. However, CBDCs can vary based on who is permitted to use them and their underlying technology. The main distinction lies between retail and wholesale CBDCs. A retail CBDC functions like cash or a bank deposit and is open to households and businesses for daily transactions. In contrast, a wholesale CBDC is limited to financial institutions and is designed for high-value interbank payments and settlements. While both types represent liabilities of the central bank, wholesale CBDCs simply convert existing central bank reserves into digital form, whereas retail CBDCs broaden access to central bank money to the general public.

Another important classification is account-based vs. token-based (a bearer instrument). A token-based CBDC resembles digital cash: transfers are peer-to-peer and verifying a payment involves checking the token's authenticity. A general-purpose token CBDC would be accessible to anyone (a retail digital currency), whereas a wholesale token CBDC would be restricted for interbank settlements. By contrast, an account-based CBDC would require users to have digital accounts with the central bank. In this model, the central bank opens accounts for individuals or businesses and records balances and transactions, with identity verification on each account holder. Account-based CBDCs function like today's electronic bank deposits, but held at the central bank.

A bearer-form CBDC would operate beyond the immediate oversight of the central bank and its regulated intermediaries, which means that things like caps on how much one can hold, limits on the size of cross-border transfers, and restrictions on who can use it would have to be built into and enforced by the payment device itself (ECB 2020).

Now, let us focus on programmable CBDCs. Here again we have various definitions, for instance, ECB (2024) defines it as "a digital form of money used for a predefined purpose, like a voucher, with limitations on where, when or with whom people

can use it". Similarly, Lee (2021) in a FED Note of June 23, 2021, states that "Two natural components of the definition [of the programmable CBDC] are a digital form of money and a mechanism for specifying the automated behavior of that money through a computer program (this mechanism is termed 'programmability')". In other words, programmability requires an inseparable link between the currency's ledger and executable logic. Importantly, some analysts distinguish programmable payments (where the payment system can enforce logic) from programmable money (where the currency itself has embedded restrictions) (IMF 2023). In either case, programmability relies on technologies like smart contracts or APIs to trigger actions when conditions are met. Meanwhile, some central banks emphasize that adding programmable features should not compromise money's fundamental qualities. In fact, institutions like the ECB and the Bank of England have made it clear they are not to introduce fully programmable CBDCs.

Nevertheless, as a recent survey by BIS confirms, 62% of central banks in advanced economies and 39% in the emerging ones consider introducing wholesale CBDCs that allow for programmable payments (BIS 2024). Interestingly, however, less than 15% central banks in advanced economies study the possibility of introducing programmable money in the form of PCBDC (app. 25% in emerging countries). Here, programmable CBDC is understood as "a coherent product that encapsulates both the storage of digital value and programmability of that value" (ibid.). Debating technical complexities of doing it is beyond the scope of this paper.

For the sake of simplicity in what follows, we are to understand PCBDC as a digital form of money with an inseparable programmable dimension allowing for imposing such restrictions as paying only for certain goods, imposing expiration dates, or adjusting interest automatically.

3. Programmable CBDCs as seen from various ontological theories of money perspective

Let us start from the functionalist ontological view on money. Here, a programmable CBDC can be qualified as money only if it performs crucial functions of money, namely a medium of exchange, a unit of account, and a store of value. The programmable nature of PCBDCs may make performing these functions difficult, if not impossible. For instance, if currency units are encoded with spending restrictions or expiration, their fungibility is constrained, potentially undermining their general acceptability, and thus making PCBDCs special-purpose tokens. Also, programmability could hinder the store of value role if one adds an expiration date to PCBDC. Lastly, PCBDC can perform the role of a unit of account if prices and contracts refer to that currency. Therefore, under the functionalist view PCBDC can hardly be treated as money.

On the other hand, if we treat money as an institution (a shared belief) facilitating exchange then PCBDC can potentially qualify as money. This is so, when people think a given PCBDS is money. Its moneyhood rests on collective recognition. To program

a CBDC is to layer additional institutional rules onto what is already an institutional construct. However, once programmability takes the extreme form of an algorithm whose logic of action is largely hidden from the possessor of money, such a PCBDC may lose its status as money, since it ceases to be collectively recognized. In general, the programmability of CBDC can be seen as a factor undermining trust, so once a given central bank decides to issue such a CBDC, it should be very careful in communicating its programmable functions to the public.

In the state theory of money, it is the state that grants the status of money to a given instrument. So, once the state declares that PCBDC is money then it is so. In particular, when the state allows individuals to pay taxes using PCBDC, such acceptance gives PCBDC the status of money. Synonymous name of the here-referred-to theory is chartalism, a term originally coined by Knapp based on the Latin word *charta* which "bears the sense of ticket or token" (1924, 32), and next, "Chartality rests on a certain relation to the laws" (34). So, for instance, the future moneyhood of digital euro in the chartalism sense would be derived from the now proposed regulation of the European Parliament and of the Council on the establishment of the digital euro (COM(2023) 369 final). However, its Article 24 prohibiting the introduction of programmable euro immediately strips it of the status of money under the state theory of money

Last but not least, let us look at the PCBDC from the perspective offered by the credit theory of money. Here, PCBDC is a digital ledger of central bank liabilities: each electronic unit is a claim on the central bank (or government). Once such a claim is allowed, then its representation, a PCBDC, is money in the credit theory sense. It should be added however that the majority of credit theories are preoccupied mostly with interpersonal debts (I owe you something) rather than with only impersonal *state* debt claims (a state owes you something). And here we have a challenge since, say, a PCBDC allowing only for paying public transport tickets can hardly be considered someone's debt. Not to mention a programmable PCBDC with an expiration date which would be highly unusual for a credit relation. The credit theorist might say that PCBDC *functions* like money but is not literally credit in the same way a bank ledger is. So, the PCBDC is more aligned with the state's credit than with personalized debt-credit, and hence it only partially satisfies credit-theory criteria.

In sum, the PCBDC can be money at least under some ontological theories of money, for instance, the state one. In other cases, programmability introduces significant uncertainty about whether a given PCBDC qualifies as money. It should also be emphasized that, in practical terms, the answer to this central question must be determined on a case-by-case basis, as it depends on the specific type of programmability involved.

Conclusions

Whether a programmable central bank digital currency qualifies as money depends on the ontological theory of money applied. Under the state theory it is money, however, under the institutional theory it only could be money, and in the credit theory sense it is money but with caveats. This presents a different situation from that of a standard CBDC, which – at least from an ontological perspective – leaves no illusions about its monetary status[6]. Therefore, it is legitimate that the vast majority of central banks considering the introduction of CBDCs have made it clear that they do not intend to introduce programmable CBDCs.

But still, many questions remain. For instance, especially in legal documents regarding CBDCs there is a clear distinction between programmable payments using CBDCs and programmable CBDCs as such. Whether such a distinction is possible to be applied in practice is rather unclear given fast developments in blockchain technology (see, e.g., Lee 2021). Also, many important issues emerge while debating whether it would be easier to add a programmable dimension to token-based or account-based CBDC. We leave those questions for further studies, since this paper should be treated mostly as an invitation for interdisciplinary studies regarding the status of programmable central bank digital currencies.

Bibliography

BIS (2018). *Central Bank Digital Currencies*, Paper by the BIS Committee on Payments and Market Infrastructures, March 2018.

BIS (2024). *Embracing Diversity, Advancing Together – Results of the 2023 BIS Survey on Central Bank Digital Currencies and Crypto*, BIS Papers, no 147.

de Bruin B., Herzog L., O'Neill M., Sandberg J. (2023). *Philosophy of Money and Finance*. In: E. Zalta, U. Nodelman (eds.), *The Stanford Encyclopedia of Philosophy* (Spring 2023 Edition), https://plato.stanford.edu/archives/spr2023/entries/money-finance/.

Draghi M. (2019). Speech during Press Conference, June 6, 2019, https://www.reuters.com/article/us-ecb-policy-italy/italy-needs-credible-mid-term-plan-for-reducing-debt-ecbs-draghi-idUSKCN1T71U4/ (accessed: 15.05.2025).

ECB (2020). *Report on a Digital Euro*, ECB, Frankfurt.

ECB (2024). *FAQs on a Digital Euro*, https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html (accessed: 15.05.2025).

Geoffrey I. (2004). *The Nature of Money*, Polity Press, Cambridge.

[6] We set aside questions related to the impact of CBDC introduction on the monetary transmission mechanism and cross-border payments, as these issues are not central from the perspective of the ontology of money.

Guala F. (2020). *Money as an Institution and Money as an Object*, Journal of Social Ontology, vol. 6(2), 265–279.

Harari Y. (2015). *Sapiens: A Brief History of Humankind*, Harper Collins Publishers, London.

Hindriks F. (2024). *The Social Ontology of Money*. In: J. Sandberg, L. Warenski (eds.), *The Philosophy of Money and Finance*, Oxford University Press, Oxford, 15–31.

Hume D. (1792). Published as: 'David Hume: Of Money (1752)'. In: E.W. Fuller (ed.), *A Source Book on Early Monetary Thought*, Edward Elgar Publishing, Cheltenham, 260–266.

IMF (2023). *How Should Central Banks Explore Central Bank Digital Currency? A Dynamic Decision-Making Framework*, Fintech Notes, no 2023/008.

Ingham, G. (2004). *The Nature of Money*, Cambridge: Polity Press.

Knapp G. (1973). *The State Theory of Money*, Augustus M. Kelly, New York.

Lane P. (2025). *The Digital Euro: Maintaining the Autonomy of the Monetary System*, Keynote speech by Philip R. Lane, Member of the Executive Board of the ECB, University College Cork Economics Society Conference 2025, https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250320_1~41c9459722.en.html (accessed: 15.05.2025).

Lee A. (2021). *What is Programmable Money?*, FEDs Notes, June 23, 2021.

Mäki U. (2020). *Reflections on the Ontology of Money*, Journal of Social Ontology, vol. 6(2), 245–263.

OECD (2023). *Central Bank Digital Currencies (CBDCs) and Democratic Values*, OECD Business and Finance Policy Papers, no. 31.

Passinsky A. (2020). *Should Bitcoin be Classified as Money?*, Journal of Social Ontology, vol. 6(2), 281–292.

Searle J. (1995). *The Construction of Social Reality*, Simon and Schuster, New York.

Searle J. (2017). *Money: Ontology and Deception*, Cambridge Journal of Economics, vol. 41(5), 1453–1470.

Simmel G. (1978). *The Philosophy of Money*, Routledge, London.

Tobin J. (1985). *Financial Innovation and Deregulation in Perspective*, Bank of Japan Monetary and Economic Studies, vol. 3(2), 19–29.

Weber M. (1978). *Economy and Society: An Outline of Interpretive Sociology*, University of California Press, Oakland CA.

Wray L. (1990). *Money and Credit in Capitalist Economies*, Edward Elgar, Aldershot.