LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

CRYPTO-ASSETS MARKET ABUSE AND MARKET PARTICIPANTS - MARKETS IN CRYPTO-ASSETS REGULATION (MICA)

Ellen Helminen
University of Lapland
Faculty of Law
European Law
Master's Thesis
Supervisor: Markku Kiikeri
May 2025

University of Lapland

Faculty: Faculty of Law

Title of the Thesis: Crypto-Assets Market Abuse and Market Participants - Markets in Crypto-Assets Regulation (MiCA)

Author: Ellen Helminen

Degree Program: Master's Program in Law

Level: Master's thesis

Number of Pages: XVII + 80

Keywords: Crypto, Crypto-Asset, Cryptocurrency, Digital Asset, Stablecoin, Virtual Asset, DeFi, Decentralized Finance, Smart Contract, Distributed Ledger, DLT, Blockchain, Markets in Crypto-Assets, MiCA, Market Abuse, Inside Information, Insider Trading, Market Manipulation, Crypto-Asset Service Provider, CASP, Issuance of Crypto-Assets

Year: 2025

Abstract:

This thesis focuses on the Markets in Crypto-Assets Regulation (MiCA) from the perspective of market abuse and crypto-assets market participants. More specifically, this thesis examines the ways in which the crypto-assets market participants are regulated to to support innovation and promote greater use of crypto-assets and DLTs, as well as to ensure adequate consumer and investor protection and market integrity. The market participants are examined from the perspective of the market abuse provisions in MiCA. Another important objective of this thesis is to highlight the gaps and shortcomings in the market abuse provisions of MiCA.

The legal doctrinal method is applied to highlight how MiCA has achieved its objective of preventing market abuse and to identify any shortcomings or concerns in the legislation as it stands. MiCA seeks to prevent market abuse by regulating market access, activities of market participants, such as issuers of crypto-assets and crypto-asset service providers (CASPs), and by defining what constitutes abuse in the crypto-assets market. The market abuse provisions of MiCA are largely based on the Market Abuse Regulation (MAR), which was developed for traditional financial markets.

The findings demonstrate that the crypto-assets market has unique characteristics compared to traditional financial markets, such as 24-hour trading and global nature. Furthermore, the findings indicate that both market participants and abuse that occurs in the crypto-assets market have specific characteristics that require a deeper understanding of the market to regulate. Applying the insufficient rules mainly developed for traditional financial markets without modifications, combined with a lack of a truly crypto-assets market-specific regulatory framework, can ultimately lead to a decline in market integrity. This thesis concludes that MiCA as such is not sufficient for preventing and detecting abuse in the market, but rather a useful springboard a future regulation on crypto-assets.

Contents

References V
List of Abbreviations XV
1 Introduction 1
1.1 Background - Crypto-Assets Transforming the Financial Landscape 1
1.2 Scope, Objective and Research Questions 3
1.3 Structure and Methodology 5
1.4 Understanding Distributed Ledger Technology and Blockchains 6
1.5 General Terminology and Composition of the Crypto-Assets Market 9
2 An Overview of MiCA 15
2.1 Road to MiCA 15
2.1.1 Bitcoin and Other Crypto Dinosaurs 15
2.1.2 ICOs and Libra 16
2.1.3 Legislative Process 17
2.2 Scope of MiCA 19
2.2.1 Scope of Crypto-Assets 19
2.2.2 Scope of Issuers, Offerors and Persons Seeking Admission to Trading of Crypto-Assets 22
2.2.3 Scope of CASPs 25
2.2.4 Geographical Scope of MiCA 26
3 Responsibilities of Issuers, Offerors and Persons Seeking Admission to Trading of Crypto-Assets 30
3.1 Process for Initiating the Issuance, Offer or Admission to Trading 30
3.1.1 Application for Authorization and Supervisory Bodies 30
3.1.2 Crypto-Asset White Paper and Marketing Communications 32
3.1.3 Traditional Financial Institutions 34
3.2 Operational Requirements for Issuers of ARTs 35
3.2.1 Conduct of Business and Prudential Requirements 35
3.2.2 Significant ARTs 38
3.3 Operational Requirements for Issuers of EMTs 39
3.3.1 Conduct of Business and Prudential Requirements 39
3.3.2 Significant EMTs 41
3.4 Operational Requirements for Offerors and Persons Seeking Admission to Trading of Other Crypto-Assets 42

4 Rights and Responsibilities of CASPs 44
4.1 Identified Risks and Regulation Specific to CASPs 44
4.2 Authorization Process of CASPs 45
4.3 Conduct of Business and Prudential Requirements 47
5 Regulation of Market Abuse in MiCA 50
5.1 MiCA Provisions on Market Abuse in Relation to Other Legislation 50
5.2 Misuse of Inside Information and Insider Dealing 52
5.2.1 Definition of Inside Information 52
5.2.2 Prohibition on Insider Dealing and Definition of Insiders 54
5.2.3 Disclosure of Inside Information 57
5.2.4 Prohibition on Misuse of Order Information, and Front-Running 58
5.3 Prohibition of Market Manipulation 61
5.4 Traditional Types of Market Manipulation 62
5.4.1 Pump and Dump 62
5.4.2 Wash Trading 64
5.4.3 Spoofing and Layering 65
5.4.4 Stop-Loss Hunting and Whale Techniques 66
5.4.5 DDoS Attacks 67
5.5 Manipulative Activities Specific to the Crypto-Assets Market 68
5.5.1 Rug Pull Schemes and AMM Protocols 68
5.5.2 Flash Loan and Oracle Attacks 70
5.5.3 MEV Extraction 72
5.6 Prevention and Detection of Market Abuse 74
6 Concluding Remarks 78
Answer to the First Research Question 78
Answer to the Second Research Question 79

References

Literature

Agarwal, Sharad - Atando-Siu, Gilberto - Ordekian, Marilyne - Hutchings, Alice - Mariconti, Enrico - Vasek, Marie, *Short Paper: DeFi Deception - Uncovering the prevalence of rugpulls in cryptocurrency projects*, International Conference on Financial Cryptography and Data Security, 2023. (Agarwal et. al. 2023)

Alexander, Carol - Cumming, Douglas, *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation*, Wiley 2020. (Alexander - Cumming 2020)

Argelich-Comelles, Cristina, *Towards Proprietary Digital Assets Under European Soft Law in Governance and Control of Data and Digital Economy* in the European Single Market - Legal Framework for New Digital Assets, Identities and Data Spaces, (ed.) Pastor Sempere, Carmen, Law, Governance and Technology Series Vol. 71, p. 55-70, 2025. (Argelich-Comelles 2025)

Auer, Raphael - Haslhofer, Bernhard - Kitzler, Stefan - Saggese, Pietro - Victor, Friedhelm, *The Technology of Decentralized Finance (DeFi),* BIS Working Papers No. 1066 of Monetary and Economic Department of the Bank for International Settlements, 17 January 2023. (Auer et. al. 2023)

Bains, Parma, *Blockchain Consensus Mechanisms: A Primer For Supervisors*, International Monetary Fund Fintech Note 2022/003, 2022. (Bains 2022)

Baker, Colleen - Werbach, Kevin, *Blockchain in financial services* in Fintech - Law and Regulation, (ed.) Madir, Jelena, Edward Elgar Publishing Limited 2024. (Baker - Werbach 2024)

Barsan, Iris M., *Are MiCAR's Market Abuse Rules Useful? - A critical analysis of the market abuse rules under MiCAR*, 25 October 2024. [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5002239] (Retrieved 23 March 2025) (Barsan 2024)

Cernera, Federico - La Morgia, Massimo - Mei, Alessandro - Sassi, Francesco, *Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens* in Ethereum and in the Binance Smart Chain (BNB) in 32nd USENIX Security Symposium (USENIX Security 23), p. 3349-3366, 2023. (Cernera et. al 2023)

Chance, Don M, *Derivative Markets and Instruments* in Derivatives, (ed.) Pirie, Wendy L., p. 385-428, CFA Institute. Wiley 2017. (Chance 2017)

Chernoff, Alan - Jagtiani, Julapa, *Beneath the Crypto Currents - The Hidden Effect of Crypto "Whales*", Working Paper of Federal Reserve Bank of Philadelphia (WP 24-14), August 2024. (Chernoff - Jagtiani 2024)

Daian, Philip - Goldfeder, Steven - Kell, Tyler - Li, Yunqi - Zhao, Xueyuan - Bentov, Iddo - Breidenbach, Lorenz - Juels, Ari, *Flash Boys 2.0: Frontrunning in Decentralized exchanges, Miner Extractable Value, and Consensus Instability*, pp. 910-927, IEEE Symposium on Security and Privacy, Virtual IEEE, 2020. [https://ieeexplore.ieee.org/document/9152675] (Retrieved on 16 February 2025). (Daian et. al. 2020)

Da Silva Filho, Osny*, Doctrinal Methods in Civil Law Jurisdictions*, Research Methods in Contract Law and Scholarship, Elgar 2025. (Da Silva Filho 2025)

Daskalakis, Nikos - Georgitseas, Panagiotis, *An Introduction to Cryptocurrencis - The Crypto Market Ecosystem Contemporary Issues in Finance*, Routledge 2020. (Daskalakis - Georgitseas 2020)

Durston, Gregory J. - McKeon, Alisa, *The Little Book of Market Manipulation: An Essential guide to the Law*. Waterside Press 2020. (Durston - McKeon 2020)

Eigelshoven, Felix - Ullrich, André - Parry, Douglas, *Cryptocurrency Market Manipulation - A Systematic Literature Review*, International Conference on Information Systems (ICIS) 2021 Proceedings, 2021. (Eigelshoven - Ullrich - Parry 2021)

Feder, Amir - Gandal, Neil - Hamrick, J. T. - Moore, Tyler, *The impact of DDoS and other security shocks on Bitcoin currency exchanges - Evidence from Mt. Gox*, p. 137-144, Journal of Cybersecurity 3(2), 2017. (Feder et. al. 2017)

Goldberg, Dror, *Famous Myths of "Fiat Money"*, Journal of Money, Credit and Banking, Vol. 37. No. 5 p. 957–967, October 2005. (Goldberg 2005)

Hautamäki, Jon - Atallah, Max - Koskikare, Karri, *Virtuaalivaluutan tarjoaminen: käsikirja virtuaalivaluuttalain soveltamiseen,* Edita Publishing 2019. (Hautamäki - Atallah - Koskikare 2019)

Herrera, Lucia Alvarado, *PSD3 and the Regulation on Payment Services in the Context of Crypto Assets as a Means of Paymen*t in Governance and Control of Data and Digital Economy in the European Single Market - Legal Framework for New Digital Assets, Identities and Data Spaces, (ed.) Pastor Sempere, Carmen, Law, Governance and Technology Series Vol. 71, p. 373-394, 2025. (Herrera 2025)

Hirvonen, Ari, *Mitkä Metodit? Opas oikeustieteen metodologiaan*, Yleisen oikeustieteen julkaisuja 17, 2011. (Hirvonen 2011)

Ho, Annetta - Cazan, Cosmin - Schrumm, Andrew, *The Ecology of Automated Market Makers*, Bank of Canada and Ontario Securities Commission, Staff Discussion Paper 2024. (Ho - Cazan - Schrumm 2024)

Howell, Sabrina T. - Niessner, Marina - Yermack, David, *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales*, NBER Working Paper Series 24774, June 2018 (Revised September 2019). (Howell - Niessner - Yermack 2018)

Lambert, Thomas - Liebau, Daniel - Roosenboom, Peter, *Security Token offerings*, p. 299-325, forthcoming in Small Business Economics, 25 June 2021. (Lambert - Liebau - Roosenboom 2021)

Lee, Joseph - Schu, Lukas, *8. Market abuse in the crypto-assets market: same risks, same activities, and same regulatory outcomes?* in A Research Agenda for Financial Law and Regulation, p. 157–178, Edward Elgar Publishing 2025 (Lee - Schu 2025)

Li, Tao - Shin, Donghwa - Sun, Chuyi, Wang, Baolian, *The Dark Side of Decentralized Finance: Evidence from Meme Tokens*, 12 July 2023. [https://chuyi-sun.github.io/repo/papers/meme_token.pdf] (Retrieved 28 March 2025) (Li et. al. 2023)

Maume, Philip, *The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?*, p. 243-275, European Company and Financial Law Review (ECFR), 2023. (Maume 2023)

McDonald, Oonagh, *Cryptocurrencies: Money, Trust and Regulation*, Agenda Publishing 2021. (McDonald 2021)

McGauran, Katrin, *The impact of letterbox-type practices on labour rights and public revenue*, Discussion paper commissioned by the European Trade Union Confederation (ETUC), June 2016. (McGauran 2016)

McGurk, Brendan - Reichenbach, Stefan, *Financial Services Law and Distributed Ledger Technology*, Edward Elgar Publishing Limited 2024. (McGurk - Reichenbach 2024)

Mount, Michelle, *Bitcoin Off-chain Transactions: Their Invention and Use*, p. 685-698, Georgetown Law Technology Review 685, 2020. (Mount 2020)

Noertjahyana, A - Christopher, A - Abas, Z. A. - Yusoh, Z. I. M. - Setiawan, *A: Stop hunt detection using indicators and expert advisors in the forex market,* Journal of Physics: Conference Series Vol. 1502, 2020. (Noertjahyana et. al. 2020)

Padhye, Sahadeo - Sahu, Rajeev A. - Saraswat, Vishal, *Introduction to cryptography*, CRC Press, Taylor & Francis Group 2018. (Padhye - Sahu - Saraswat 2018)

Rehman, Muhammad Habib ur - Salah, Khaled - Damiani, Ernesto - Svetinovic, Davor, *Trust in Blockhain Cryptocurrency Ecosystem*, p. 1196-1212, IEEE Transactions on Engineering Management Challenges and Opportunities Vol. 67, Issue 4, 2020. (Rehman et. al. 2020)

Sanmarchi, Francesco - Toscano, Fabrizio - Fattorini, Mattia - Bucci, Andrea - Golinelli, Davide, *Distributed Solutions for a Reliable Data-Driven Transformation of Healthcare Management and Research*, Frontiers in Public Health, 7 July 2021. (Sanmarchi et. al. 2021)

Srokosz, Witold - Lenio, Pavel - Sobiecki, Grzegorz, *Blockchain Technology in Project Finance - A Legal and Practical Model for Financing Mega-Investments*, Routledge Open Business and Economics 2025. (Srokosz - Lenio - Sobiecki 2025)

Thakkar, Dev - Sabale, Suraj - Waghmare, Aayushka, *Exploring the Efficiency of Off-Chain vs. On-Chain Transactions in Blockchain Network*, International Journal of Scientific Research in Computer Science, Engineering and Information Technology Vol. 10 No. 3, May-June 2024. (Thakkar - Sabale - Waghmare 2024)

Then, Corey - Hill, Caroline - Anderson, David, *Unlocking Stablecoins: Exploring Opportunities and Risks,* The Bretton Woods Committee, February 2025. (Then - Hill - Anderson 2025)

Tovanich, Natkamon - Soulié, Nicolas - Heulot, Nicolas - Isenberg, Petra, *The evolution of mining pools and miners' behaviors in the Bitcoin blockchain*, IEEE Transactions on Network and Service Management, 2022. (Tovanich et. al. 2022)

Truchet, Marc, *Decentralized Finance (DeFi): opportunities, challenges and policy implications*, EUROFI Regulatory Update with input from Jeff Bandman, EUROFI Regulatory Update, February 2022. [https://www.eurofi.net/wp-content/uploads/2022/05/eurofi_decentralized-finance-defi_opportunities-challenges-and-policy-implications_paris_february-2022.pdf] (Retrieved 9 January 2025) (Truchet 2022)

Uzoma Ihugba, Bethel, *Introduction to Legal Research Method and Legal Writing*, Malthouse Press Ltd., 2020. (Uzoma Ihugba 2020)

Wang, Qianwen - Huang, Jiehua - Wang, Shen - Chen, Yibo - Zhang, Pan - He, Li, *A Comparative Study of Blockchain Consensus Algorithms*, Journal of Physics: Conference Series 1437, 2020. (Wang et. al. 2020)

Whitehouse-Levine, Miller - Kelleher, Lindsey, *Self-Hosted Wallets and the Future of Free Societies: A Guide for Policymakers*, Blockchain Association, November 2020. [https://theblockchainassociation.org/wp-content/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf] (Retrieved on 1.4.2025) (Whitehouse-Levine - Kelleher 2020)

Wu, Ke - Wheatley, Spencer - Sornette, Didier*, Classification of cryptocurrency coins and tokens by the dynamics of their market capitalizations*, Royal Society Open Science 5:180381, 5 September 2018. (Wu - Wheatley - Sornette 2018)

Xu, Jiahua - Paruch, Krzysztof - Cousaert, Simon - Feng, Yebo, *SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols*, ACM Computing Surveys, 2022. (Xu et. al. 2022)

Zaccaroni, Giovanni, *Decentralized Finance and EU Law: The Regulation on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology,* European Papers Vol. 7/2022, No. 2, p. 601-613, 2022. (Zaccaroni 2022)

Čuk, Tilen - Van Waeyenberge, Arnaud, *European legal framework for algorithmic and high frequency trading (Mifid 2 and MAR): A global approach to managing the risks of the modern trading paradigm*, pp. 146-153, European Journal of Risk Regulation Vol. 9, No. 1, March 2018. (Čuk - Van Waeyenberge 2018)

Official Sources (EU)

European Commission, COM(2020) 591 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU. 24 September 2020. (European Commission 2020)

European Commission Newsroom, The story of DigiCash and its eCash. 18 September 2019 [https://ec.europa.eu/newsroom/cef/items/658303/en] (Retrieved 13 March 2025) (European Commission Newsroom 2019)

European Banking Authority (EBA), Final Report on Draft Regulatory Technical Standards on information for application for authorisation to offer to the public and to seek admission to trading of asset-referenced tokens and Draft Implementing Technical Standards on standard forms, templates and procedures for the information to be included in the application, under Article 18(6) and (7) of Regulation (EU) 2023/1114. EBA/RTS/2024/03 and EBA/ITS/2024/03. 7 May 2024. (EBA 2024a)

European Banking Authority (EBA), Final report on the Draft Regulatory Standards to specify the procedure and timeframe to adjust the own funds requirements for issuers of significant asset-referenced tokens or of e-money tokens subject to such requirements. EBA/RTS/2024/09. 13 June 2024. (EBA 2024b)

European Banking Authority (EBA), Decision of the European Banking Authority EBA/DC/558 concerning the Procedure for the classification of asset-referenced tokens and e-money tokens as significant and the transfer of supervisory powers and reporting on those tokens following the classification as significant under MiCAR. 17 September 2024. (EBA 2024c)

European Banking Authority (EBA), Final report on Draft Regulatory Technical Standards on adjustment of own funds requirements and stress testing of issuers of asset-referenced tokens and of e-money tokens subject to such requirements. EBA/RTS/2024/08. 13 June 2024. (EBA 2024d)

European Banking Authority (EBA), Final Report on Draft Regulatory Technical Standards on the detailed content of information necessary to carry out the assessment of a proposed acquisition of qualifying holdings in issuers of asset-referenced tokens under Article 42(4) of Regulation (EU) 2023/1114. EBA/RTS/2024/04. 7 May 2024. (EBA 2024e)

European Banking Authority (EBA), Guidelines amending Guidelines EBA/GL/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('the ML/TF Risk Factors Guidelines') under Articles 19 and 18(4) of Directive (EU) 2015/849. EBA/GL/2024/01. 16 January 2024. (ML/TF Risk Factors Guidelines 2024)

European Banking Authority (EBA), Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation 8EU) 2023/1113 ('Travel Rule Guidelines'). EBA/GL/2024/11. 4 July 2024. (Travel Rule Guidelines 2024)

European Banking Authority (EBA) and European Securities and Markets Authority (ESMA), Joint Report on Recent developments in crypto-assets (Article 142 of MiCAR). ESMA75-453128700-1391 and EBA/Rep/2025/01. 13 January 2025. (EBA and ESMA Joint Report 2025)

European Data Protection Supervisor (EDPS), on Central Bank Digital Currency. TechDispatch Report 1/2023. [https://www.edps.europa.eu/system/files/2023-03/23-03-29_techdispatch_cbdc_en.pdf] (Retrieved 1 May 2025) (EDPS 2023)

European Parliamentary Research Service (EPRS), Market in crypto-assets (MiCA). Briefing on EU Legislation in Progress, 29 September 2023. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221] (Retrieved 15 March 2025) (EPRS 2023)

European Securities and Markets Authority (ESMA), Consultation Paper on the Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper. ESMA75-453128700-438. 5 October 2023. (ESMA 2023a)

European Securities and Markets Authority (ESMA), Consultation Paper on the Draft technical standards and guidelines specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience - third consultation paper. ESMA75-453128700-1002. 25 March 2023. (ESMA 2023b)

European Securities and Markets Authority (ESMA), Statement on ESMA clarifies timeline for MiCA and encourages market participants and NCAs to start preparing for the transition. ESMA74-449133380-441. 17 October 2023. (ESMA 2023c)

European Securities and Markets Authority (ESMA), Consultation Paper on the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments. ESMA75-453128700-52. 29 January 2024. (ESMA 2024a)

European Securities and Markets Authority (ESMA), Final Report on the Guidelines on reverse solicitation under the Markets in Crypto-Assets Regulation (MiCA). ESMA35-1872330276-1899. 17 December 2024. (ESMA 2024b)

European Securities and Markets Authority (ESMA), Final Report on the Guidelines specifying Union standards on the maintenance of systems and security access protocols for offerors and persons seeking admission to trading of crypto-assets other than asset referenced tokens and e-money tokens. ESMA75-223375936-6089. 17 December 2024. (ESMA 2024c)

European Securities and Markets Authority (ESMA), Final Report on the Draft technical standards specifying certain requirements in relation to the detection and prevention of market abuse under the Markets in Crypto Assets Regulation (MiCA). ESMA75-453128700-1278. 17 December 2024. (ESMA 2024d)

European Securities and Markets Authority (ESMA), Final Report on the Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments. ESMA75453128700-1323. 17 December 2024. (ESMA 2024e)

European Securities and Markets Authority (ESMA), Statement on MiCA Transitional Measures. ESMA75-453128700-1396, 17 December 2024. (ESMA 2024f)

European Securities and Markets Authority (ESMA), Supervisory Briefing on the Authorization of CASPs under MiCA. ESMA75-453128700-1263. 31 January 2025. (ESMA 2025a)

European Securities and Markets Authority (ESMA), Final Report on the Guidelines on supervisory practices for competent authorities to prevent and detect market abuse under the Markets in Crypto Assets Regulation (MiCA), 29 April 2025. (ESMA 2025b)

European Securities and Markets Authority (ESMA), Decentralized Finance in the EU: Developments and risks. ESMA TRV Risk Analysis. ESMA50-2085271018-3349. 11 October 2023. (TRV Risk Analysis 2023)

European Union Agency for Cybersecurity (ENISA), Threat Landscape: Finance Sector, January 2023 to June 2024. 21 February 2025. [https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf] (Retrieved 25 April 2025) (ENISA 2025)

Official Sources (Other)

Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), Guidance FIN-2013-G001 on Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, 18 March 2013. [https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf] (Retrieved 3 March 2025) (The U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) 2013)

U.S. Department of Justice, Former Employee of NFT Marketplace Sentenced To Prison in First-Ever Digital Asset Insider Trading Scheme, 22 August 2023. [https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-sentenced-prison-first-ever-digital-asset-insider] (Retrieved 30 April 2025) (U.S. Department of Justice (DOJ) 2023)

U.S. Department of Justice, Eighteen Individuals and Entities Charged in International Operation Targeting Widespread fraud and Manipulation in the Cryptocurrency Markets, 9 October 2024. [https://www.justice.gov/usao-ma/pr/eighteen-individuals-and-entities-charged-international-operation-targeting-widespread] (Retrieved 18 March 2025) (U.S. Department of Justice (DOJ) 2024a)

U.S. Department of Justice , Man Convicted for USD 110M Cryptocurrency Scheme, 18 April 2024. [https://www.justice.gov/archives/opa/pr/man-convicted-110m-cryptocurrency-scheme] (Retrieved 14 February 2025) (U.S. Department of Justice (DOJ) 2024b)

U.S. Department of Justice, Founder of Cryptocurrency Financial Services Firm "Gotbit" Extradited to the United States to Face Charges of Market Manipulation and Fraud Conspiracy, 26 February 2025. [https://www.justice.gov/usao-ma/pr/founder-cryptocurrency-financial-services-firm-gotbit-extradited-united-states-face] (Retrieved 18 March 2025) (U.S. Department of Justice (DOJ) 2025)

U.S. Securities and Exchange Commission (SEC), SEC v. Avraham Eisenberg [https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-13.pdf] (Retrieved 2 February 2025) (The U.S. Securities and Exchange Commission (SEC) 2023)

U.S. Securities and Exchange Commission (SEC), Report of Investigation No. 81207, 25 July 2017 [https://www.sec.gov/files/litigation/investreport/34-81207.pdf] (Retrieved 11 January 2025) (The U.S. Securities and Exchange Commission (SEC) 2017)

U.S. Congress, H.R.4763 - Financial innovation and Technoloy for the 21st Century Act. 118th Congress (2023-2024). [https://www.congress.gov/bill/118th-congress/house-bill/4763/text?s=1&r=1&q=%7B%22search%22%3A%5B%22Financial+Innovation+and+Technology+for+the+21st+Century+Act.%22%5D%7D] (Retrieved 12 April 2025) (FIT21 Act)

Financial Conduct Authority (FCA), Discussion Paper on distributed ledger technology DP 17/3, April 2017. (FCA 2017)

Financial Conduct Authority (FCA), Crypto: The basics. 17 February 2023 (Last updated 10 May 2024). [https://www.fca.org.uk/investsmart/crypto-basics] (Retrieved 9 May 2025) (FCA 2023)

G7 Working Group on Stablecoins, Investigating the impact of global stablecoins, October 2019. [https://www.bis.org/cpmi/publ/d187.pdf] (Retrieved 29 March 2025) (G7 Working Group on Stablecoins 2019)

Emerging Markets Committee of the International Organization of Securities Commissions (IOSCO), Insider Trading: How Jurisdictions Regulate It, Report, March 2003. (IOSCO 2003)

Legislation (EU)

Regulations

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (DLT Pilot Regime)

Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (MAR)

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA)

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA)

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Revised TFR)

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (DMA)

Directives

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 (MiFID II)

Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation (DAC8)

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)

Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on the 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)

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and

repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (4AMLD)

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (6AMLD)

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (CRD)

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) (recast) (UCITS Directive)

Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive) (Market Abuse Directive, MAD II)

Preparatory works

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) (Proposal for MiCA)

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 (Proposal for PSD3)

Online Sources

Adler, David, Silk Road: The Dark Side of Cryptocurrency, Fordham Journal of Corporate and Financial Law, 21 February 2018 [https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/] (Retrieved 29 March 2025) (Adler 2018)

Chainalysis, The 2025 Crypto Crime Report: The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation, February 2025. [https://www.antiriciclaggiocompliance.it/app/uploads/2025/03/The-2025-Crypto-Crime-Report-Chainalysis.pdf] (Retrieved 23 April 2025) (Chainalysis 2025)

Copeland, Tim, Jaredfromsubway.eth's MEV bot rakes in millions of dollars in three months, 10 May 2023. [https://www.theblock.co/post/230218/jaredfromsubway-mev-bot] (Retrieved 13 February 2025) (Copeland 2023)

Dougherty, Carter - Huang, Grace, Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss, Bloomberg.com, 28 February 2014 [https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy] (Retrieved 9 May 2025) (Dougherty - Huang 2014)

An Introduction to Libra. White Paper From the Libra Association Members, 18.6.2019 [https://www.allcryptowhitepapers.com/wp-content/uploads/2019/06/LibraWhitePaper_en_US.pdf] (Retrieved 6 April 2025) (Libra Association 2019)

Lightning Network White Paper, 14 January 2016. [https://lightning.network/lightning-network-paper.pdf] (Retrieved 15 May 2025) (Lightning Network 2016)

McGee, Suzanne, Cryptoverse: Next wave of US crypto ETFs already in the pipeline, Reuters.com, 10 January 2025. [https://www.reuters.com/technology/cryptoverse-next-wave-us-crypto-etfs-already-pipeline-2025-01-10/] (Retrieved 30 February 2025) (McGee 2025)

Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. [https://bitcoin.org/bitcoin.pdf] (Retrieved 27 April 2025) (Nakamoto 2008)

Stock Market Holidays and Trading Hours, Nasdaq Trading Schedule [https://www.nasdaq.com/market-activity/stock-market-holiday-schedule] (Retrieved 13 May 2025) (Nasdaq Trading Schedule)

Pinkerton, Julie, The History of Bitcoin. Edited by Aaron Davis, U.S. News & World Report, 18 February 2025. [https://money.usnews.com/investing/articles/the-history-of-bitcoin] (Retrieved 21 May 2025) (Pinkerton 2025)

Program on International Financial Systems, A Review of Cryptoasset Market Structure and Regulation in the United States. February 2023. [https://www.pifsinternational.org/wp-content/uploads/2023/01/PIFS-Cryptoasset-Market-Structure-and-Regulation-in-the-U.S.-02.01.23.pdf] (Retrieved 17 March 2025) (Program on International Financial Systems 2023)

Solana Foundation, 9-14 Network Outage Initial Overview, 20 September 2021, [https://solana.com/fi/news/9-14-network-outage-initial-overview] (Retrieved 10 April 2025) (Solana Foundation 2021)

List of Abbreviations

AMM	automatic market maker
ART	asset-referenced token
CASP	crypto-asset service provider
CBDC	central bank digital currency
CEX	centralized exchange
Commission	European Commission
Council	Council of the European Union
CRD	Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC
DAC8	Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation
dApp	decentralized application
DDoS	distributed denial-of-service
DeFi	decentralized finance
DEX	decentralized exchange
DFS	Digital Finance Strategy (EU)
DLT	distributed ledger technology
DMA	Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
EBA	European Banking Authority
ECB	European Central Bank

EMD2	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
EMI	electronic money institution
EMT	electronic money token, e-money token
ENISA	European Union Agency for Cybersecurity
ESMA	European Securities and Markets Authority
ETF	exchange-traded fund
EU	European Union
GSC	global stablecoin
ICO	initial coin offering
ICT	information and communications technology
OJEU	Official Journal of the EU
MAD II	Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive)
MAR	Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC
MEV	miner extractable value
MiCA	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
MiFID II	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
NFT	non-fungible token
PPAET	person professionally arranging or executing transactions
Parliament	European Parliament
PoS	Proof-of-Stake

PoW	Proof-of-Work
PSD2	Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on the 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
PSD3	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
P2P	peer-to-peer
RTS	regulatory technical standards
STOR	suspicious transaction or order report
TFR (Revised)	Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849
UCITS Directive	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) (recast)
U.S.	United States
4AMLD	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC
6AMLD	Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2 019/1937, and amending and repealing Directive (EU) 2015/849

1 Introduction

1.1 Background - Crypto-Assets Transforming the Financial Landscape

In the global digital financial markets, the introduction of new forms of currency - so-called 'crypto-assets' - has fundamentally changed the way we understand the nature of money. Crypto-assets are purely digital assets whose balances are recorded in a ledger analogous to a bank account system with the main difference being that the ledger is operated by decentralized publicly available network.[1] In recent years, crypto-assets have become increasingly mainstream. Reasons for the rise of crypto include the advantages of using such assets over fiat money[2], such as enhanced security, adaptability, decentralization, faster transaction speed and lower costs. Traditional financial transfers, which once required days and potentially numerous intermediaries to complete, can now be completed and finalized instantly at virtually no cost. Bitcoin, the first decentralized cryptocurrency released in 2009, has led the rise of crypto-assets.[3] The success of Bitcoin has also paved the way for other crypto-assets, allowing thousands of new coins and tokens to enter the market while sparking debate on the role of central banks and the future of global trade. The crypto-assets market has rapidly expanded over the past years reflecting the increasing public acceptance of digital assets and the growing recognition among investors and institutional players. The increasing importance of regulating the crypto sector continues to rise as digital assets evolve deeper into mainstream and global use.

The European Union (EU) was at the forefront in setting technical standards and broader guidelines for the regulation of crypto-assets market. In September 2020, the European Commission (Commission) released its Digital Finance Strategy (DFS) [4], with the aim of unleashing European innovation and creating opportunities to develop better financial

[1] Srokosz - Lenio - Sobiecki 2025, p. 48.
[2] Most coin and paper currencies used throughout the world are fiat money. This includes the U.S. dollar, the British pound and the euro. Fiat money, a government-issued currency is an object that is not backed by any commodity, has no intrinsic value and is not convertible into anything. Such currencies have value only as a result of voluntary collective consensus on the value of the currency as a medium of exchange. See, Goldberg 2005, p. 957. The EU has also defined the concept of fiat currency in a similar way in point 4(b)(10) of Annex I of Directive 2023/2226/EU on administrative cooperation in direct taxation (DAC8).
[3] Pinkerton 2025.
[4] European Commission 2020.

products. In the package, the Commission unveiled a proposal for a legislative framework on crypto-assets. In under three years of time, the European Parliament (Parliament) approved the act, and the Regulation on Markets in Crypto-Assets (EU) 2023/1114, called both 'MiCA' and 'MiCAR' for short, entered into force in June 2023. In this thesis, the terms MiCA or the Regulation are used to refer to the EU legislation on markets in crypto-assets. The initial deadline for full entry into application of MiCA was 30 December 2024, but in reality, the implementation is scheduled to take place in stages, with the transition ending by 1 July 2026. MiCA provided the necessary legal definitions for a number of terms used in the crypto sector that had not been defined in existing legislation. The Regulation defined, for example, the concept of a crypto-asset. According to Article 3(1)(8) of MiCA, crypto-asset is a digital representation of a value or of a right that is able to be transferred or stored electronically using distributed ledger technology like blockchains or other similar technology. The objective of MiCA was to control financial risk and harmonize the crypto sector in the EU, while also ensuring innovation and competition,[5] by regulating the characteristics and use of certain crypto-assets, as well as the operation of the market and its participants.

As the crypto-assets market matures and expands, so does the potential for misuse, criminal activity and related risks. The development of MiCA was strongly motivated by the objective to provide a comprehensive regulatory framework to control and eradicate market abuse and financial crime.[6] The nature of the crypto-assets market as a completely new and unique domain gives rise to both traditional and previously unseen industry-specific risks and challenges. The decentralized character of crypto-assets, the high volatility and lack of trust in the market, as well as the opportunities for money laundering and crime created by the novel technologies, provide fertile ground for manipulation and abuse. As a result, MiCA introduced a legal framework for crypto-assets market abuse based on the corresponding provisions of the Market Abuse Regulation 2014/596/EU (MAR), which addresses market abuse in traditional financial markets. Abuse regulated by MiCA and MAR share many common features, as will be demonstrated in this thesis, as traditional financial markets and crypto-assets market are rapidly becoming more and more integrated. To address market abuse and ensure investor protection in the crypto-assets market, MiCA seeks to define the scope of abuse and to closely regulate market

[5] Recital 6 MiCA Regulation.
[6] Recital 4 MiCA Regulation.

access, the activities and obligations of market participants, as well as the prevention and detection of market abuse. By setting guidelines that simultaneously protect the market and its participants, but also support innovation, the much-needed comprehensive European regulation on crypto-assets could improve the ability of the market to expand, but also increase the credibility of the sector in the eyes of individuals, large institutions and even governments.

1.2 Scope, Objective and Research Questions

For as long as crypto-assets have existed, their unregulated market has been a playground for scammers and schemers seeking to exploit the market to defraud funds from the uninitiated. The most famous scams in the market date back to at least 2014, when Mt. Gox crypto exchange platform filed for bankruptcy after losing USD 480 million worth of Bitcoins to hackers.[7] Crime and abuse in the crypto-assets market has been particularly easy to perpetrate due to the lack of comprehensive regulation, but also because the market allows for pseudo-anonymity and easy access for novice users. These features reflect the nature of the distributed ledger technologies (DLTs) that underlie the crypto-assets market, the characteristics and operation of which will be discussed in more detail later in this thesis. The novelty of the technologies used in the crypto-assets market also contributes to the possibility for criminals and fraudsters to exploit gaps in the systems, as was the case with Mt. Gox. Silk Road, the first online black market, is also a familiar case for many who have followed the early days of crypto-assets and related crime. Silk Road was discovered and operated by Ross Ulbricht between 2011 and 2013, during which time a wider online market for illegal goods and services was also created.[8] With regard to crypto-assets, the case is significant, as Bitcoin was chosen as a primary means of payment in the market due to its poor traceability and easy availability, which also contributed to the rise in value and recognition of the asset. Silk Road and the global coverage of the case is one of the reasons why many people still associate crypto-assets solely with crime to this day.

MiCA addresses market abuse by regulating market access and activities of market participants as well as by setting limits on what constitutes market abuse. For the purpose of

[7] Dougherty - Huang 2014.
[8] Adler 2018.

this thesis, it is appropriate to combine the examination of the regulation of market participants and market abuse in MiCA, given the close link between the two. The objective of this thesis is to explore the ways in which MiCA seeks to regulate the prevention and detection of market abuse, while also taking into account the unique nature of the crypto-assets market. At the same time, the intention is to identify any shortcomings or concerns with the Regulation in its current form in relation to market abuse.

To achieve the objective of this thesis, the following two research questions are set:

1. How does the regulation of market participants in MiCA reflect its regulatory objective of preventing market abuse?
2. Is the existing MiCA regulatory framework for market abuse sufficient, when considering the specific characteristics of the crypto-assets market and abusive practices that occur in the sector?

While market abuse is not uncommon in modern crypto-assets market, there have so far been no such cases in the EU where MiCA would have become applicable. The most recent significant cases involving crypto-assets market abuse have been pursued in the United States (U.S.)[9] This is due to the fact that existing legislation in the U.S. has been extended to cover most cryptocurrencies, although no comprehensive legislation specific to the crypto-assets market yet exists.[10] The author understands that the lack of European case law may make it more difficult to conduct research of this nature, but notes that due to the global nature of the crypto-assets market, the abusive practices are consistent across the world. As a result, it is possible to carry out the research by assessing, for example, cases pursued in the U.S. from the perspective of MiCA. Such a perspective is also possible as a result of the fact that this thesis aims to point out gaps and shortcomings in the content of MiCA in relation to the regulation of market abuse, rather than to assess the application of its provisions in different situations.

The secondary purpose of this thesis is to give the reader a comprehensible overview of the crypto-assets market. The novelty of the market, and the related technologies and regulation adds to the fascination of the topic, but also creates challenges for a focused

[9] For case examples, see U.S. Department of Justice (DOJ) 2024a and U.S. Department of Justice (DOJ) 2025.
[10] However, the U.S. House of Representatives passed a major crypto legislation, the Financial Innovation and Technology for the 21st Century Act (FIT21), in 2024, to close gaps and tackle the shortcomings of current legislation. FIT21 has not yet been enforced. For more information, see Fit21 Act.

treatment of the subject. In order to approach the research questions, some general fundamentals of the crypto-assets market need to be introduced. These elements, such as Decentralized Finance (DeFi), DLTs and related technologies, will be covered in the following sections as clearly and concisely as possible and in a way that gives the reader a general idea of how the crypto-assets market works before focusing on its regulation. Understanding the underlying technology of the crypto-assets market is important for the topic of this thesis, as in many cases of abuse occurring in digital markets, it is the technology and its characteristics that play a major role. However, in order to narrow the scope, some aspects of the crypto-assets market have also been excluded from the scope of the assessment. Such issues include, for example, further examination of possible purposes or ways of use of the crypto-assets, such as crypto-assets as a means of payment, and criminal activity, such as money laundering and terrorist financing, which may have links to the crypto sector.

1.3 Structure and Methodology

Historically, legal doctrine has been the dominant method of legal research within civil law jurisdictions.[11] Doctrinal research is based mainly on legal doctrine which refers to the interpretation of legal text or a series of facts based on legal principles.[12] Legal doctrinal method examines what constitutes existing legislation and the significance of the material found in different legal sources, such as law, legislative documents and judicial decisions.[13] In addition to the existing legislation, the legal doctrinal method weighs and harmonizes legal principles, which also always requires interpretation of legal norms.[14] This thesis will approach the research questions outlined above using the legal doctrinal method. The legal doctrinal method is applied to analyze how MiCA has achieved its objective of preventing market abuse and to identify any shortcomings or concerns in the legislation as it stands. In this context, to support a comprehensive coverage of the topic, other EU legal instruments covering crypto-assets will also be discussed where appropriate. Alongside legislation, this thesis discusses a number of reports and guidelines issued to complement MiCA by EU institutions, such as the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA). Other sources used are

[11] Da Silva Filho 2025, p. Abstract.
[12] Uzoma Ihugba 2020, p. 6.
[13] Hirvonen 2011, p. 23.
[14] Ibid, p. 24.

mainly literature and various articles, as well as some news reports and publications by the U.S. government agencies in relation to cases of market abuse.

This thesis is divided in such a way that the reader is first given a general overview of the structure of the crypto-assets market and its underlying technologies in the following sections of Chapter 1. This is followed in Chapter 2 by a presentation of MiCA and its origins. The introduction of the origins of MiCA begins from the creation of the crypto-assets market and leads to the presentation of the legislative process. Subsequently, the scope of MiCA is addressed. In this context, the different crypto-assets and market participants that fall under the scope of MiCA will be presented together with the geographical scope of the Regulation. Chapters 3 and 4 cover the operation of market participants, separating the examination on requirements and obligations imposed on issuers, offerors and persons seeking admission to trading of crypto-assets and crypto-asset service providers. The penultimate chapter introduces the market abuse provisions of MiCA by distinguishing between misuse of inside information, insider dealing and market manipulation. For each type of abuse covered by MiCA, not only the legislation and its shortcomings, but also the related behavior in the crypto-assets market is examined. Chapter 5 also highlights the specific characteristics of abuse occurring in the crypto-assets market. In the final chapter, Chapter 6, a summary of the key findings of this thesis is presented, which are then used to answer the research questions set out in Chapter 1.2.

1.4 Understanding Distributed Ledger Technology and Blockchains

Distributed ledger is defined in Article 3(2) of MiCA as a repository of information that keeps records of transactions and that is shared and synchronized among a set of DLT network nodes using a consensus mechanism. In distributed ledgers, a transaction is not validated by a central authority, such as banks in traditional financial transactions, but by other network users, also called 'nodes', without any specific entity having to control the process. Article 3(4) of MiCA defines node as a device or process that is a part of a network and that holds a complete or partial replica of records of all transactions on a distributed ledger. More clearly, nodes can be described as a distributed ledger moderator system that maintains and builds the network infrastructure. DLTs, on the other hand, are the technologies that allow for the operation and use of distributed ledgers and as noted, the technologies behind crypto-assets. DLTs are described as a set of technological solutions that enables a single, sequenced, standardized and cryptographically-secured record

of activity, to be safely distributed to, and acted upon by, a network of varied participants.[15] These technologies operate on decentralized and distributed ledgers which can be used for a range of purposes, including the creation and exchange of value of, for example, financial products and services, and for recording and verifying transactions.[16] Distributed ledgers are not a new concept in technology. DLTs have been used for decades in industries where the need for collecting and using data is vital. However, since the launch of crypto-assets, the development and use of these systems has grown considerably even in industries such as healthcare or finance.[17]

MiCA does not directly impose any obligations on the characteristics and operation of DLTs and blockchains.[18] However, at the same time as the need to regulate crypto-assets market in Europe arose, so did the need to regulate DLTs. Hence, the EU initiated a pilot regime explicitly including DLTs in its proposed DFS alongside MiCA and the Digital Operational Resilience Act (EU) 2022/2554 (DORA) in 2020. On 23 March 2023, a Regulation on a Pilot Regime for Market Infrastructures Based on DLTs (EU) 2022/858 became applicable, which pointed out that the existing EU financial services legislation was not designed with DLTs and crypto-assets in mind.[19] The aim of the Pilot Regime is to allow for development of crypto-assets that qualify as financial instruments and for the development of DLTs, while at the same time preserving high level of investor protection, market integrity, financial stability and transparency, and avoiding regulatory arbitrage and loopholes.[20] These factors were taken into account by addressing types and definitions of market infrastructures, scope of financial instruments under the regime, obligations imposed on different market infrastructures and cooperation between ESMA and DLT market infrastructures.[21] Such a regime was established to allow regulators and target groups to evaluate the functioning of the new rules over a fixed timeframe. The Pilot Regime is still ongoing, so its effectiveness remains to be seen.

Blockchain on the other hand is a type of DLT where records are collated into 'blocks' and linked using a cryptographic signature.[22] Cryptography refers to the study of secure

[15] FCA 2017, p. 10.
[16] McGurk - Reichenbach 2024, p. 13-14.
[17] See, for example Sanmarchi et. al. 2021.
[18] Recital 6 MiCA Regulation "The Union framework for markets in crypto-assets should not regulate the underlying technology."
[19] Recital 4 DLT Pilot Regime.
[20] Recital 6 DLT Pilot Regime.
[21] Zaccaroni 2022, p. 605.
[22] FCA 2017, p. 12-13.

designs required to protect sensitive communication.[23] In blockchains, each block is a collection of individual transactions, which are verified and added to the chain as a unit, hence the term Blockchain.[24] Blockchains are perhaps the best known and most widely used amongst all DLTs. When it comes to crypto-assets, blockchain is the system that allows the *peer-to-peer* (P2P) transfer of money without intermediaries. One major positive argument in favor of crypto is the role of blockchains as a base of crypto-assets in particular. Blockchains are digital platforms that use cryptographic methods to store information, which cannot be falsified or reversed, and where the entire history of the transactions among the users of the network is recorded, validated, stored and publicly available for everyone.[25] This allows for the transfer of funds in a reliable and transparent way. The blockchain of Bitcoin, for example, holds a record, available for anyone to see, of all Bitcoin transactions since its launch in 2009. The pioneering technology of blockchains also increases the speed of transfers and reduces the costs by eliminating the need for human intervention. However, blockchains too have their weaknesses, such as the unstoppable nature of a distributed network running on multiple servers as well as the environmental impacts of high energy consumption. Also, in terms of market abuse and crime, the nature of blockchains allows, for example, easy access and anonymity, and thus poor traceability of transactions as was proven in the Silk Road case.

Consensus mechanisms are a critical component of blockchains, alongside cryptography and DLTs. Consensus mechanisms are mathematical algorithms that allow thousands of nodes scattered around the world to reach a decentralized consensus on blockchain transactions and block creation.[26] Consensus mechanisms also include an incentive mechanism to promote the effective operation of the blockchain system. While the number of different consensus mechanisms is wide, to limit the scope of the coverage, two of the most commonly used protocols in public blockchains are presented below. The best-known consensus mechanism in the world is no doubt the *Proof-of-Work* (PoW) developed by Satoshi Nakamoto and used, for example in Bitcoin blockchain. PoW involves nodes solving complicated asymmetrical mathematical puzzles to produce new blocks in

[23] Cryptographic study focuses on the means and methods of data conversation in secure forms with the aim of protecting access to the data, preventing its modification, guaranteeing its authenticity and ensuring that it cannot be repudiated by the generator. See, Padhye - Sahu - Saraswat 2018, p. 2.
[24] Baker - Werbach 2024, p. 218.
[25] Daskalakis - Georgitseas 2020, p. 9-10.
[26] Wang et. al. 2020, p. 1.

a process known as 'mining'.[27] These nodes involved in transaction validation, also known as *miners*, compete to solve these mathematical puzzles, as the first to succeed is rewarded with compensation in the form of transaction processing fees. Generally speaking, any person can set up their computer to mine, for example, Bitcoin, and thus also act as a node in the network. *Proof-of-Stake* (PoS) is another consensus mechanism, where an algorithm randomly selects 'validators' for block creation based on the amount of the crypto-asset the holders contribute to a stake.[28] Crypto staking refers to the process of immobilizing crypto-assets to support the operation of the PoS mechanism or other similar consensus mechanisms in exchange for the granting of validator privileges that can generate block rewards.[29] PoS is used in networks such as Ethereum. Validators are incentivized by rewarding them with crypto-assets, usually with the same one deposited for staking, for successful transaction validation. Any person who has ownership of such crypto-asset and stakes it is likely to act as a validator on the blockchain. Crypto-assets based on PoS mechanisms can be placed in staking by average users on most crypto exchange platforms.

1.5 General Terminology and Composition of the Crypto-Assets Market

Besides DLTs, the structure of the crypto-assets market and its various components must also be introduced before moving on to the topic of the research questions. However, before going into the composition of the market, it is important to distinguish between a few related terms that are often used interchangeably in the context of crypto, such as terms of digital assets and crypto-assets. Digital asset is an umbrella term that covers all assets that exist in a digital format and can be stored, transferred and controlled electronically. Such definition covers, for example digital music and art or even virtual real estate. Cryptocurrencies, which also fall under both categories of digital and crypto-assets, refer to private virtual currencies that use cryptographic encryption algorithms, meaning not all crypto-assets are cryptocurrencies.[30] The concept of cryptocurrency must also be distinguished from that of a public digital currency which is often used in the same context. The very term digital currency is used more to refer to a fiat currency such as euro or the

[27] Bains 2022, p. 8.
[28] Ibid, p. 10.
[29] EBA and ESMA Joint Report 2025, p. 43.
[30] Hautamäki - Atallah - Koskikare 2019, p. 8.

US dollar issued by central banks and that is converted into electronic form, rather than cryptocurrencies. However, there is also a specific term for such a currency, a central bank digital currency (CBDC).[31] A difference must also be drawn between cryptocurrency coins and tokens, as they have different functions, but the terms are often used interchangeably in the crypto sector. Coins, such as Bitcoin, are primarily used as a means of payment and operate on their own independent network, whereas tokens are based on existing coin networks and can serve multiple different purposes.[32]

The introduction to the structure of the crypto-assets market can be divided in several of ways. However, for the purpose of this thesis, the overview is appropriate to divide into three main components: crypto-assets, decentralized finance (DeFi) and crypto-asset service providers (CASPs). The overview begins with a closer look at crypto-assets, which are understandably the most important component of the market. Crypto-assets have a myriad of uses, such as a store of value, a medium of exchange, an indicator of ownership and identity, and a way of tokenizing various real-life tangible objects. Crypto-assets have also been linked to traditional financial market, as different stocks and funds deriving value from the crypto-assets are on the rise. In the case of Bitcoin, for example, the first wave of U.S. Bitcoin ETFs attracted USD 65 billion in 2024, raising the value of the coin from USD 43,000 to over USD 100,000.[33]

Given the wide range of use cases for crypto-assets, projects have taken varying approaches early on to develop the technologies and underlying blockchains in different directions. The blockchains on which Bitcoin and Ether (Ethereum), for example, are based on were intended to be decentralized, whereas other crypto-assets designed for completely different purposes might reside in blockchains where the majority control of nodes is inherently in the hands of one or more interconnected entities.[34] Thus, not all blockchains and crypto-assets are equally decentralized, nor are they intended to be. Whether the purpose of the project is to create tokens or coins is also relevant, as the creation of a coin requires the creation of an entire blockchain, while the creation of tokens is relatively easy. In addition to creating a token or coin, crypto-assets can typically be acquired by participating in the mining or validation of transactions as discussed be-

[31] EDPS 2023, p. 2.
[32] Wu - Wheatley - Sornette 2018, p. 2.
[33] McGee 2025.
[34] Program on International Financial Systems 2023, p. 4.

fore, receiving them directly from another holder, investing directly in initial coin offerings (ICOs) or purchasing through a crypto exchange.[35] ICOs will be discussed further later in the thesis.

Crypto-assets can be categorized into *stablecoins* and crypto-assets that are not tied to any intrinsically valuable asset. Stablecoins were created to solve the extreme volatility and lack of trust in the crypto-assets market by tying the value of crypto-assets to more stable real-world assets, such as gold, fiat currencies or oil. Such crypto-assets are needed for enabling transition from traditional applications of assets to those that take place on blockchains, as decentralized finance cannot support fiat currencies that are not available *on-chain*.[36] On-chain refers to transactions initiated, recorded and validated within the specific blockchain, whereas 'off-chain' transactions would refer to transactions taking place outside of the primary blockchain network.[37] An example of an off-chain transaction is, for example in relation to executing an off-chain Bitcoin transaction, carrying out a completely decentralized P2P transaction using an alternative blockchain to Bitcoin, such as the Lightning Network[38]. When transactions are made off-chain, the blockchain information regarding the ownership of the crypto-assets in question is not updated.[39] The term off-chain may also be used to refer to all data that is not stored in the blockchain. The nature of stablecoins makes them essential to crypto-assets market. The value of outstanding stablecoins has grown over the last four years from total circulation of USD 4 billion in 2020 to more than USD 200 billion in early 2025.[40] Crypto-assets backed by more traditional investments increase confidence in price stability and thus the market, allowing larger adoption and reducing the perception of speculative nature of crypto.

Although the term stablecoin is not once used in the Articles of MiCA, crypto-assets which are by nature falling into the category of stablecoins are divided into two types in its legal provisions: asset-referenced tokens (ARTs) and electronic money tokens or e-money tokens (EMTs). The term stablecoin is mentioned only once in MiCA in its recitals, referring specifically to algorithmic stablecoins that aim to maintain stable value against official currencies or other assets through protocols that allow for the supply of

---

[35] Alexander - Cumming 2020, p. 208.
[36] Then - Hill - Anderson 2025, p. 1.
[37] Thakkar - Sabale - Waghmare 2024, p. 40-41.
[38] The Lightning Network was built on the blockchain of Bitcoin to ease the transaction burden on the Bitcoin Network. For more information, see, Lightning Network 2016.
[39] Mount 2020, p. 688.
[40] Then - Hill - Anderson 2025, p. 1.

such assets to increase or decrease in response to changes in demand, rather than against a reserve of assets.[41] Algorithmic stablecoins fall under the regulation of either ARTs or EMTs, depending on their characteristics, regardless of the mechanism used to stabilize the value. On the other hand, algorithmic crypto-assets whose value is not stabilized in the same way as stablecoins, are regulated under the third unspecified category of crypto-assets. The division of stablecoins, definitions of ARTs and EMTs and the general scope of MiCA in relation to different crypto-assets will be discussed in Chapter 2.2.1 of this thesis. In addition to algorithmic stablecoins, the category of stablecoins can be divided into two main types based on how they work: collateralized and crypto-collateralized.[42] Collateralized stablecoins are linked to assets with strong intrinsic value like fiat currencies, precious metals or commodities, while crypto-collateralized stablecoins are backed by other crypto-assets. For clarity, the term stablecoin will be used in the remainder of this thesis to refer to all ARTs, EMTs and algorithmic stablecoins covered by MiCA.

As for crypto-assets whose value is not tied to a more stable asset, several exist, including cryptocurrencies, crypto-related funds, such as mutual funds, exchange-traded funds (ETFs), and a variety of tokens. Cryptocurrencies are virtual currencies, available as both coins and tokens, that use cryptography to operate in a distributed, decentralized and secure environment.[43] Cryptocurrencies are the best-known type of crypto-assets, the most famous one being Bitcoin. Cryptocurrencies have no intrinsic value, instead their value is mainly based on supply and demand in the market. As the name of cryptocurrencies implies, they are treated as currencies, for example, as a store of value or as a medium of exchange. The category of tokens, on the other hand, includes utility tokens, security tokens, non-fungible tokens and a number of others used for various purposes beyond currency. Utility tokens, such as Ether (Ethereum) and XRP (Ripple) may be also used as a means of payment, although their main purpose is to grant access to a community-based ecosystem by giving the holders a consumptive right on a product or service.[44] In turn, security tokens are digital representations of an investment product, recorded on a distributed ledger.[45] Security tokens may represent investment products or fractions of them such as companies or real estate which are held for investment purposes. Finally, *non-fungible tokens* (NFTs) represent ownership of a unique and individualized digital asset,

[41] Recital 41 MiCA Regulation.
[42] McDonald 2021, p. 49.
[43] Daskalakis - Georgitseas 2020, p. 24.
[44] Lambert - Liebau - Roosenboom 2021, p. 7.
[45] Ibid, p. 5.

which is therefore not fungible and whose transfer is subject to the legal regime of specific obligations by means of a certificate to the token holder as the owner.[46] Such tokens can also be used to prove the identity of the token holder, to tokenize the transfer of ownership with traceability of the transaction, and to prove the ownership of virtual objects in video games and online platforms, such as tokenized avatars, virtual land, or in-game digital assets.[47]

The second component of the crypto-assets market, *decentralized finance* or *DeFi*, is a new financial paradigm that leverages DLTs to offer services common in traditional financial markets such as lending, investing, or exchange of crypto-assets without having to rely on a traditional centralized intermediary.[48] DeFi is a very broad concept that refers to the whole decentralized financial system based on DLTs, which includes, for example, crypto-assets based on blockchains. DeFi consists of financial protocols - implemented as *smart contracts* - running on a network of computers automatically managing financial transactions.[49] Smart contracts are programs that enable the automatization of financial transactions without intermediaries. The programs contain pre-defined terms that allow transfers to take place when the specified conditions are met. The Monetary and Economic Department of the Bank for International Settlements has defined the term for the financial protocols used in DeFi. Such DeFi protocols provide one or more financial services to economic agents.[50] Financial services based on DLTs are composed of advanced DeFi protocols, which contain multiple smart contracts. DeFi protocols allow more sophisticated financial services to be built enabling for example, lending, borrowing and trading of crypto-assets. Such complex services include, amongst others, crypto trading platforms. In relation to crypto-asset services, MiCA specifically excludes fully and truly decentralized models from its scope, which also includes exclusion of such DeFi protocols.[51] An example of such a model could be a fully decentralized trading platform running solely on smart contracts over DLTs, such as a specific blockchain. However, the conditions for full and complete decentralization are rarely met, which is an issue that is further discussed in the context of the scope of CASPs.

---

[46] Argelich-Comelles 2025, p. 57.
[47] Ibid, p. 57.
[48] Auer et. al. 2023, p. Abstract.
[49] Ibid, p. 3.
[50] Ibid, p. 11.
[51] Recital 22 MiCA Regulation.

The last segment of the crypto-assets market are financial service providers, or when it comes to the crypto sector, *crypto-asset service providers*, also known as CASPs. CASPs are organizations or legal persons that provide, for example, crypto wallets for holding the assets or exchange and trading services. Article 3(1)(15) of MiCA defines crypto-asset service provider as a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in the EU. According to Article 3(1)(16) of MiCA, crypto-asset services include providing custody and administration, operating a trading platform, exchange of crypto-assets, execution of orders, placing of crypto-assets, reception and transmission of orders, providing advice or portfolio management and providing transfer services. Since the entry into force of MiCA, CASPs cannot operate in the EU without an official authorization or outside strict operational guidelines. Through this legislative approach, legislators have sought to prevent market abuse and ensure a level playing field for all persons wishing to engage in providing crypto-asset services in the EU. While CASPs are an important structural part of the digital crypto-assets market when acting, for example, as an operator of a trading platform, they also act as participants in the market. Other relevant participants in the crypto-assets market include issuers, offerors and persons seeking admission to trading of crypto-assets, miners and validators, and financial institutions. All of these entities will be discussed in more detail in this thesis.

2 An Overview of MiCA

2.1 Road to MiCA

2.1.1 Bitcoin and Other Crypto Dinosaurs

When considering how the first comprehensive regulation covering the crypto-assets market came about, the review should start with the first cryptocurrency, Bitcoin. Crypto-assets were initially introduced to the wider public during the 2008 Global Financial Crisis when an anonymous entity known as Satoshi Nakamoto published a paper, "Bitcoin: The Peer-to-Peer Electronic Cash System". In the document, Satoshi Nakamoto recognized the need for an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.[52] At the same time, Nakamoto introduced the term chain of blocks, which later turned into the word blockchain. Before Bitcoin, other cryptocurrencies had been introduced, but Nakamoto was the first to successfully implement a virtual currency and the underlying blockchain. Back in the 1990s, cryptographer David Chaum was the first to attempt to develop a decentralized and cryptographic digital money. Chaum and his company DigiCash created the first fully electronic money called eCash in 1993, but the idea eventually ran into too many problems and led to his bankruptcy.[53] However, many elements of his work were later to play a key role in the development of digital currencies.

The aim of Bitcoin was to allow online payments without the intervention of financial institutions. In addition to the trust-based model of electronic financial transactions, Nakamoto saw weaknesses in the global payment system, such as the non-reversible nature and cost of the payments.[54] The Bitcoin network launched in 2009, giving the public access to the decentralized digital currency. For the people, Bitcoin was this "new" form of money, that could not be monitored by banks or governments. As the first ever cryptocurrency, Bitcoin continues to dominate the landscape to this day, although it did not take long for alternatives, such as Litecoin (2011), Dogecoin (2013) and XRP (2013) to enter the market. These so-called 'altcoins', a term used to refer to all alternative crypto-

[52] Nakamoto 2008, p.1.
[53] European Commission Newsroom 2019.
[54] Nakamoto 2008, p.1.

currencies other than Bitcoin, are still in circulation at present. The second largest cryptocurrency today, Ether and its blockchain Ethereum were launched in 2015. Since the birth of Bitcoin, the number of cryptocurrencies has grown exponentially. The Financial Conduct Authority of the United Kingdom has estimated that there were more than 20 000 different crypto-assets at the beginning of 2023, although a large number of them are lying idle.[55] Over time, the crypto-assets market grew to such an extent, both in terms of users and value, that it could no longer be ignored by regulators. For example, in the U.S., the first regulatory guidelines regarding crypto-assets were issued in 2013.[56]

2.1.2 ICOs and Libra

In the EU, the regulatory landscape for crypto-assets was highly fragmented only a few years ago. Some Member States had already adopted a certain level of regulation covering the crypto-assets market in the absence of a uniform EU legislation.[57] The critical need for a unified regulatory framework was recognized, as the rapid growth and future prospects of the crypto-assets market were highlighted. In particular, a sudden surge in the number of initial coin offerings (ICOs) in 2017 and early 2018 attracted the attention of both Member State and European regulators.[58] ICOs are mechanisms used to raise capital for new innovative projects in blockchains to, for example, cover operational costs.[59] A company or a group in charge of the project creates ICO tokens which are sold directly to the public on a global scale, easily and without transaction costs. Such method of fundraising allows vast sums of money to be raised extremely fast, even in a matter of hours. ICOs involve three parties: business startups or projects using the blockchain technology, prospective investors and ICO providers, which are centralized platforms offering the process to take place.[60] ICOs turned out to be a great way for raising funds. In the end of 2017, the value raised through ICOs for the period of October and November reached USD 3.78 billion taking over the value of venture capital funding of USD 1.88 billion in the same timeframe.[61] The U.S. legislators closely followed the explosive growth of the

[55] FCA 2023.
[56] The U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), 2013.
[57] For example, France adopted the Law on Business Growth and Transformation (PACTE Act) (Act No. 2019-486 of 22 May 2019) in 2019 establishing regulatory framework for digital asset service providers (DASPs) and ICOs. The German Banking Act (Kreditwesengesetz, KWG) incorporated crypto-assets and custody business at the beginning of 2020 and the German Electronic Securities Act (Gesetz über elektronische Wertpapiere, eWpG) has allowed for the issuance of crypto securities since 2021.
[58] Howell - Niessner - Yermack 2018, p. 1.
[59] Daskalakis - Georgitseas 2020, p. 55.
[60] Ibid, p. 55.
[61] Ibid, p. 57 (Figure 5.2).

trend and eventually decided to establish strict regulatory framework around such offerings, while also complicating the process of creating new coins.[62] This also contributed to the eventual decline in the popularity and use of ICOs. In the EU, it was only MiCA that established comprehensive legislation on ICOs by introducing general rules on the issuance of crypto-assets.

Alongside the surge in popularity of ICOs, the regulatory attention was turned to stablecoins and the possible introduction of regulation regarding them. The introduction of Libra in 2019, the stablecoin of Facebook, pressured lawmakers to establish proper regulation on such crypto-assets. Libra was supposed to be a blockchain-based global stablecoin and a financial system that would have been backed by multiple assets instead of one.[63] Libra payment system would have enabled private transactions on the blockchain for billions of users. As expected, Libra was faced with a lot of resistance and criticism from both central banks and regulators across the world. The G7 Working Group on Stablecoins, established by the G7 countries to evaluate the Libra project, published a report on the impact of global stablecoins in October 2019, which painted a bleak picture of the future of Libra. In the report the group also defined the concept of global stablecoins.[64] According to the report, global stablecoins (GSCs) are initiatives built on existing large and cross-border customer base which may have the potential to scale rapidly to achieve a global or other substantial footprint. As the idea of Facebook GSC ran into opposition from the public, the company was forced to shut down and sell the project. While the attempt to introduce stablecoins to the masses was premature with Libra, the resulting demand for regulatory development played a role in the creation of MiCA.

2.1.3 Legislative Process

Despite the failure of the Libra project to take off, EU legislators had now realized that the absence of an overall Union framework would leave holders of crypto-assets exposed to risks and pose significant challenges to market integrity, including market abuse and financial crime.[65] While it was recognized that the rapidly growing unregulated crypto-assets market posed a threat to central banks and the traditional financial system, it also

[62] The U.S. Securities and Exchange Commission deemed crypto-assets offered through ICOs to mainly fall into the category of securities and stated that issuers of such securities must register offers and sales unless a valid exemption applies. See further, The U.S. Securities and Exchange Commission (SEC) 2017.
[63] Libra Association 2019, p. 3.
[64] G7 Working Group on Stablecoins 2019, p. 2.
[65] Recital 4 MiCA Regulation.

became clear that the lack of a relevant legislative framework could ultimately lead to a deficit in user confidence.[66] This in turn could hinder the development of the market and lead to missed opportunities in terms of innovative digital services, alternative payment instruments or new funding sources for Union companies. In addition, it was found that the legal uncertainty and regulatory fragmentation could have negative impact on the prospects of European crypto-asset operators in international markets. As a result of these concerns, the objective of MiCA was to create a robust and transparent legal framework to support innovation and promote greater use of crypto-assets and DLTs, to ensure adequate consumer and investor protection and market integrity, and to enhance financial stability.[67] In addition, one of the main purposes of MiCA was to fill the regulatory gap in the crypto-assets market by regulating all crypto-assets that fell outside the scope of other EU legislation.[68] Most of the crypto-assets and market participants had not been regulated in any way prior, apart from some general rules on money laundering and terrorist financing. However, as will become apparent later in this thesis, this objective of creating a legal framework covering all crypto-assets has fallen somewhat short, as the impact of MiCA only applies to crypto-assets defined in its legal provisions.

When MiCA was approved by the Parliament on 20 April 2023, it became the most advanced legal framework covering crypto-assets on a global scale. MiCA was signed into law on 31 May 2023, published in the Official Journal of the EU (OJEU) and soon enforced on 29 June 2023. As an EU regulation, MiCA is fully binding and immediately applicable among the Member States. However, due to the fragmented nature of national European legislations on crypto-assets, a staged approach to regulatory implementation was adopted. On 30 June 2024, the provisions set for ARTs and EMTs became applicable and finally, on 30 December 2024, the main body of MiCA, including the provisions on CASPs, came into effect. The staged approach also includes additional time for already existing CASPs to transition from compliance with the current regulatory framework to compliance with MiCA. Article 143(3) of MiCA states that CASPs that provided their services in accordance with applicable law before 30 December 2024, may continue to do so until 1 July 2026 or until they are granted or refused a regulatory authorization to

[66] Recital 5 MiCA Regulation.
[67] EPRS 2023, p. 2.
[68] Recital 16 MiCA Regulation "The terms 'crypto-assets' and 'distributed ledger technology' should therefore be defined as widely as possible to capture all types of crypto-assets that currently fall outside the scope of Union legislative acts on financial services."

operate, whichever is sooner. The so-called 'grandfathering period' allows CASPs to continue their crypto-asset services as they were until the end of June 2026. Member States had the opportunity to not apply the transitional period for CASPs or to reduce its duration in view of fostering financial stability and investor protection.[69] This has resulted in CASPs having different transitional times in different Member States, making the application of MiCA even more demanding. Therefore, ESMA warned the holders of crypto-assets and the clients of CASPs that they may not benefit from full rights and protections afforded to them under MiCA until as late as 1 July 2026.[70] Similarly, the scope for monitoring and, if necessary, intervening in the activities of beneficiaries of the grandfathering period will be narrower until July 2026. When the transitional period ends, CASPs operating under EU legislation must be fully MiCA compliant and legally authorized.

2.2 Scope of MiCA

2.2.1 Scope of Crypto-Assets

The general definition of crypto-assets provided by MiCA was introduced at the beginning of the presentation. MiCA identifies three categories of crypto-assets: *asset-referenced tokens* (ARTs), *e-money tokens* (EMTs), and all the others that do not fall into either of these categories whilst also not qualifying as, for example, financial instruments.[71] Crypto-assets that qualify as financial instruments are fully regulated under the Markets in Financial Instruments Directive II (2014/65/EU) (MiFID II). Article 3(1)(7) of MiCA defines EMTs as a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency. The price of an EMT is therefore always tied to a more stable asset, such as the euro or the US dollar. Again, according to Article 3(1)(6) of MiCA, ARTs are all tokens except EMTs, which purport to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies. The purpose of ARTs is to maintain a stable value by linking the value of the crypto-asset to either one asset or a pool of assets, which may consist of, for example, one or more official currencies, crypto-assets or commodities. As for the third and final group of crypto-assets, the legislators have deliberately left the precise definition of the category open in order to accommodate the wide range of crypto-assets that fall

[69] ESMA 2024f, p. 1.
[70] ESMA 2023c, p. 2.
[71] Recital 18 MiCA Regulation.

outside the definitions of ARTs and EMTs. MiCA refers to this category more generally as crypto-assets other than ARTs and EMTs.[72] Utility tokens are the only crypto-asset defined in MiCA besides the two types of stablecoins. Article 3(1)(9) of MiCA defines utility tokens as crypto-assets whose only intention is to provide access to a good or a service supplied by its issuer. Since utility tokens are the only crypto-asset defined in MiCA that fall into to the third unspecified group of crypto-assets, it remains unclear as to what other crypto-assets belong in this category.

Given that MiCA was only intended to regulate assets that fall outside or in between the scope of other legislation, it explicitly excludes many crypto-assets already regulated in the EU from its scope. Crypto-assets that fall under existing Union legislative acts on financial services will remain regulated under the existing regulatory framework, regardless of the technology used for their issuance or their transfer.[73] Accordingly, crypto-assets that qualify as financial instruments under MiFID II are explicitly excluded from the scope of the Regulation under Article 2(4)(2) of MiCA. For example, security tokens with features of transferable financial instruments are fully regulated under MiFID II. The distinction between the different characteristics of crypto-assets regulated by MiCA and the financial instruments covered by MiFID II appears to pose challenges. Due to MiFID II being an EU directive, whereas MiCA is a directly applicable legal instrument, potential difficulties in application were considered likely in the future. Consequently, ESMA published guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments to facilitate the distinction, as there is no commonly agreed application of the definition of 'financial instrument' in the EU.[74] In addition, crypto-assets that qualify as deposits or funds, with the exception of such funds qualifying as EMTs, as well as various securitization positions and insurance, social security or pension products and schemes are excluded from the scope of the Regulation under Article 2(4)(b)-(j) of MiCA.

Most of the different types of NFTs presented earlier in this thesis are excluded from the primary scope of MiCA due to their nature and purpose. Article 2(3) of MiCA states that the Regulation does not apply to crypto-assets that are unique and not fungible with other crypto-assets. Although, there is no common definition of what constitutes as a 'unique

[72] Ibid.
[73] Recital 9 MiCA Regulation.
[74] ESMA 2024e, pp. 4.

and non-fungible' crypto-asset, MiCA emphasizes the concept of substance over form approach.[75] The uniqueness and non-fungibility limits the utility of NFTs and excludes them from the regulatory framework of MiCA. In particular, individual NFTs regarding art or collectables often fall into this category. However, if an NFT contains sufficient features of, for example, a utility token, it will fall under the scope of MiCA. Crypto-assets falling under several legal classifications may be called as 'hybrid tokens'.[76] Similarly, when an NFT is part of a collection or series, the tokens fall under the scope of MiCA if they are interchangeable. Where tokens are part of a larger collection, individual unique NFTs can be traded with the tokens from the same group. However, even this is not self-evident, as ESMA also considers the size of the collection to have an impact on the definition of the nature of an NFT.[77] In this context, it is also important to note that MiCA recognizes NFTs that are divisible or subdivided into fractions and thus potentially part of a broader group as falling within the scope of its legislation.[78]

In addition to the already mentioned crypto-assets, MiCA recitals provide a number of other assets not covered by its regulatory scope. Firstly, digital assets that are non-transferable, that are only accepted by their issuer or offeror and that are technically impossible to transfer to other holders are excluded from the scope of MiCA.[79] An example of such an asset is loyalty schemes, where loyalty points can only be exchanged for benefits with the issuer or offeror of those points. Similarly, all crypto-assets with no identifiable issuer are deemed outside the scope of MiCA.[80] The legislative approach to this matter is understandable, as any regulatory measures would have no addressee, and the issuer is untraceable, but it is noteworthy that the exclusion of such assets could still allow unknown issuers to circumvent the MiCA requirements imposed for the issuance. Nevertheless, CASPs that provide services in respect of crypto-assets whose issuer is not identifiable are still covered by the Regulation. In addition to the above, MiCA does not address the lending and borrowing of crypto-assets, leaving this to be regulated by Member States at national level.[81] However, according to a survey conducted by EBA and ESMA in early 2025, only five responding authorities, representing four Member States, indicated that

[75] Ibid, p. 20.
[76] Ibid, p. 22.
[77] Ibid, p. 21.
[78] Recital 11 MiCA Regulation.
[79] Recital 17 MiCA Regulation.
[80] Recital 22 MiCA Regulation.
[81] Recital 94 MiCA Regulation.

lending or borrowing of crypto-assets is regulated to some extent in their jurisdiction.[82] This is particularly problematic because of the presence of 'flash loans' in the crypto-assets market, which are examined in the context of market manipulation in this thesis. Lastly, digital assets issued by central banks when acting in their capacity as monetary authority are also excluded from the scope of MiCA.[83] These digital assets include CBDCs, including possible future digital euro issued by the European Central Bank (ECB), and crypto-assets issued by other public authorities, such as central, regional and local administrations. MiCA also excludes all related digital services provided by central banks acting in their monetary authority capacity or other public authorities from its regulatory scope.

2.2.2 Scope of Issuers, Offerors and Persons Seeking Admission to Trading of Crypto-Assets

As is evident from the scope of crypto-assets discussed above, a great deal of responsibility is placed on the crypto-assets market participants to identify the type of asset they operate with, and therefore the relevant legislation. Consequently, MiCA regulates issuers, offerors and persons seeking admission to trading of crypto-assets to facilitate the supervision and control of the potential for abuse. Issuers of crypto-assets are entities that issue crypto-assets and thus have control over their creation.[84] Offerors of crypto-assets are defined in Article 3(13) of MiCA as entities who are either natural or legal persons or other undertakings, or issuers, who offer crypto-assets to the public. Article 3(12) of MiCA broadly defines an offer to the public as any communication that provides the potential holders with sufficient information about the terms of the offer and the crypto-assets being offered to allow an informed investment decision. From the perspective of MiCA, issuers and offerors are often the same entity, as the issuer is likely to be the person who initiates the project, issues the crypto and offers it to the public.[85] However, the offeror of crypto-assets could as well be a third party. Admission to trading refers to all admissions of crypto-assets to trading on a trading platform of crypto-assets.[86] As the legal treatment of different crypto-assets varies, this thesis is structured to examine the regulation of different market participants separately for each crypto-asset category. The

[82] EBA and ESMA Joint Report 2025, p. 48.
[83] Recital 13 MiCA Regulation.
[84] Recital 20 MiCA Regulation.
[85] Barsan 2024, p. 13.
[86] Recital 23 MiCA Regulation.

scope of issuers, offerors and persons seeking admission to trading of ARTs is more stringent compared to other crypto-assets as the legislators noted that the nature of such assets could pose increased risks in the future in terms of protection of holders and market integrity.[87] Failures of issuers of ARTs were seen to possibly lead to a large-scale redemption and trigger a fire-sale of their reserve assets as well as deposit withdrawal, potentially causing significant market disruptions and systemic risks in the broader financial system.[88]

The following conditions for the issue, offer and admission to trading of ARTs are laid down in Article 16 of MiCA. Firstly, Article 16(1) of MiCA limits the scope for the offer or admission to trading of an ART to the issuer of that specific ART, who is either a legal person or other undertaking established in the EU and authorized by the competent authority or, alternatively, a credit institution. Credit institutions, such as banks authorized under other legislation, must operate within the limits set by MiCA when engaging in the issuance of ARTs. Pursuant to the same provision, other persons than those mentioned above may also offer or seek admission to trading of an ART with the written consent of the issuer of the asset. The important factor to recognize in this context is that only an operator established in the EU may issue, offer or seek admission to trading of an ART within the Union. By limiting these activities to where supervision is feasible, the possibilities to address the risks associated with the increased use of stablecoins will be improved. As for other undertakings, the issuance of ARTs is only permitted provided that their legal status ensures an equivalent level of protection of the interests of third parties to that provided by legal persons, and if they are subject to a sufficiently prudent level of supervision corresponding to their legal form.[89] However, under Article 16(2) of MiCA, the conditions on the scope of issuers, offerors and persons seeking admission to trading of ARTs do not apply if the offer of an ART is targeted purely towards, and can only be held by, qualified investors or if the value of the asset never exceeds EUR 5 million over a period of 12 months.

The scope for issuers, offerors and persons seeking admission to trading of EMTs is even more limited and is provided for in Article 48 of MiCA. Solely issuers of EMTs, who are

[87] See Recital 40 MiCA Regulation, also Recital 5 MiCA Regulation
[88] EBA 2024d, p. 7 (Point 11.)
[89] EBA 2024a, p. 6.

also either authorized credit institutions or electronic money institutions (EMIs), may under Article 48(1) of MiCA offer and seek admission to trading of such assets. The operation of EMIs in the EU is subject to the Electronic Money Directive 2009/110/EC (EMD2) and the Revised Payment Services Directive 2015/2366/EU (PSD2). EMIs are defined in Article 2(1) of EMD2 as legal persons that have been granted authorization to issue electronic money. Additionally, electronic money is defined in Article 2(2) of EMD2 as a monetary value stored in electronic form, represented by a claim on the issuer, issued on receipt of funds for the purpose of making payment transactions and accepted by a natural or legal person other than the electronic money issuer. EMTs are considered to be electronic money under Article 48(2) of MiCA. Similar to ARTs, other persons may offer or seek admission to trading of EMTs with the written consent of the issuer. As a further clarification, when referring to issuers of ARTs or EMTs, this thesis simultaneously refers to offerors and persons seeking admission to trading of such assets, as they are the same entity.

As for the third undefined group of crypto-assets, both offerors and persons seeking admission to trading of such assets must be legal entities.[90] Thus, the criteria for those only involved in the last category of crypto-assets are seemingly less stringent. An even more permissive environment is created in Article 4(3) of MiCA for specific offerings of such crypto-assets. It follows that in such situations where the crypto-asset other than ART or EMT is offered for free or automatically created as a reward for the maintenance of the DLT or the validation of transactions, none of the rules for the third crypto-asset category of MiCA apply. Such offerings are therefore completely outside the scope of MiCA. The same applies where the offer concerns a utility token that provides access to an existing good or service, or where the holder of the crypto-asset has the right to only use it in exchange for goods and services from a limited network of merchants who have contractual arrangements with the offeror. However, a crypto-asset is not considered to be offered for free within the meaning of the exemption if the buyers are required to provide personal data in return or if the offeror receives fees, commissions, or other benefits from the prospective holders. In addition, according to Article 4(4) of MiCA, the exemption does not apply if the offeror later intends to seek admission to trading of the asset.

[90] See Article 4(1)(a) of MiCA with regard to offers to the public of crypto-assets other than ARTs and EMTs, and Article 5(1)(a) of MiCA with regard to admission to trading of such assets.

2.2.3 Scope of CASPs

In addition to the market participants referred to above, MiCA regulates entities providing crypto-asset services in the EU. The following scope of CASPs is specified in Article 59 of MiCA. First, under Article 59(1), the entities providing crypto-asset services must be either legal persons or other undertakings that have been authorized as CASPs. In order to enable effective supervision, and to eliminate the possibility of evading or circumventing the rules established in MiCA, services related to crypto-assets should only be provided by authorized CASPs that have a registered office in the Member State in which they carry out substantive business activities, including the provision of crypto-asset services.[91] In addition, such CASPs must be effectively domiciled in the EU, and at least one of the directors must be resident in the territory of Member States. To underline these rules, persons other than authorized CASPs are prohibited in Article 59(5) of MiCA from using a name, or a corporate name, issue market communications or undertake any other process suggesting or creating confusion on it being an authorized CASP. The provisions of MiCA in this respect are very strict, and under these market conditions it might be difficult for third country operators to offer crypto-related services in the EU. Such an approach could ultimately reduce the attractiveness of the crypto-assets market in this respect, and at the same time undermine the competitiveness of Europe vis-à-vis the rest of the world. However, limiting market access is important for market integrity, user protection and the prevention of market abuse and crime. Apart from authorized CASPs, Article 59(1) of MiCA also states that crypto-asset services may be provided by credit institutions, central securities depositories, investment firms, market operators, EMIs, UCITS management companies[92], or alternative investment fund managers.

With regard to the scope of CASPs, challenges arise in situations where services related to crypto-assets are provided partly in a decentralized manner. MiCA applies to all crypto-asset services and activities, including when part of such activities or services is performed in a decentralized manner.[93] As stated before in relation to DeFi protocols, functions carried out in a fully and truly decentralized manner without any intermediary are excluded from the scope of MiCA. In this context, situations where determining the exact

[91] Recital 74 MiCA Regulation.
[92] According to Article 1(1) of the UCITS Directive 2009/65/EC, UCITS refers to undertakings for collective investment in transferable securities. Pursuant to Article 2(1)(b) of the same Directive, UCITS management company refers to companies in the business of management of UCITS in the form of common funds or of investment companies.
[93] Recital 22 MiCA Regulation.

moment a DeFi protocol is considered fully decentralized and vice versa, when it inadvertently falls under the category of CASPs regulated by MiCA are particularly difficult. The use of automated smart contracts as well as the decentralized nature of the operation and governance of the platform are the two main features that distinguish DeFi from centralized blockchain systems.[94] MiCA fails to define the limits for sufficient decentralization in relation to these features, which may result in DeFi protocols being subject to the Regulation, and thus having to operate under stringent rules imposed on CASPs. The existence of the problem has also been recognized by ESMA. ESMA considers that an assessment of each system should be made on case-by-case basis considering the features of the system.[95] It is likely that in the near future, DeFi protocols and their operation will be subjected to a more comprehensive legislation and this regulatory gap will be addressed.

2.2.4 Geographical Scope of MiCA

The provisions of MiCA do not set a precise geographical limit to its regulatory scope. The Regulation, under Article 2(1) of MiCA, applies to all natural and legal persons and certain other undertakings that are engaged in the issuance, offer to the public and admission to trading of crypto-assets or that provide services related to crypto-assets in the Union. The wording of the provision extends the scope of MiCA beyond the Member States and will have far-reaching implications for all third-country operators wishing to engage in crypto-asset-related activities within the EU. However, such a broad geographical scope can pose problems both in terms of applicability and enforceability. Future problems may arise especially due to the wide geographical scope of the rules on market abuse in the Regulation defined in Article 86 of MiCA to a similar extent. The extensive scope of the market abuse rules covers all acts carried out by any person concerning crypto-assets that are admitted to trading or in respect of which a request for admission to trading has been made, regardless of whether such activities take place on a trading platform or not, or in Member States or third countries. Under such scope, any activity related to crypto-assets admitted to trading, or for which a request for admission has been submitted, falls within the scope of MiCA regardless of the country in which the operator is established or where the activities occurred.

[94] Truchet 2022, p. 69.
[95] ESMA 2023a, p. 29.

The scope of the market abuse provisions in MiCA thus defined should be critically examined, as an overly broad definition could pose problems of international jurisdiction and enforcement. For example, in a situation where crypto-assets market abuse occurs outside the Member States and the possible link to the EU is not clear, the chances of holding offenders liable under MiCA are low. However, it is worth noting that the original proposal of the Commission for crypto-assets market regulation had different wording in this context. Article 76 of the proposal, which precedes the current Article 86 on the regulatory scope of crypto market abuse provisions in MiCA, states that it is applied to crypto-assets admitted to trading, or for which a request for admission to trading has been made, on a trading platform for crypto-assets operated by an authorized crypto-asset service provider.[96] An authorized CASP in this context refers to an entity providing services related to crypto-assets within the EU in accordance with MiCA. Had the draft of the final article remained unchanged, the geographical scope of the market abuse provisions in MiCA would have been limited to EU operators. Such a significant change in wording reflects the intention to extend the scope of the market abuse provisions beyond crypto-assets admitted to trading in the EU. This may be due to the fact that a large number of CASPs are located outside the Union, and the opportunity to protect victims of crime on foreign exchange platforms, and to hold the perpetrators accountable, was sought. However, the purpose of the legislative approach will only be revealed once the opportunity for Member States to apply the relevant provisions of MiCA arises.

As regards the geographical limits for operation between the Member States, MiCA provides so-called 'passporting rights' for those entitled to operate within the EU. Passporting allows different crypto-assets market participants to operate freely throughout the EU, once they meet the conditions laid down in MiCA.[97] As outlined in relation to the scope of CASPs, authorization and a registered office within the Union are requirements for providing crypto-assets services in the EU. Authorized CASPs may provide crypto-asset services anywhere in the EU under Article 59(7) of MiCA, either through the right of establishment, for example through branches, or through the freedom to provide services.

[96] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending directive (EU) 201971937 COM(2020) 593 final 2020/0265(COD)

[97] See Article 16(3) of MiCA for the conditions on the operation in the EU in relation to issuers of ARTs, Article 51(13) of MiCA in relation to issuers of EMTs and Article 11(1) of MiCA in relation to offerors and persons seeking admission to trading of crypto-assets other than ARTs and EMTs. These conditions will be discussed in more detail later in this thesis.

Therefore, authorized CASPs are also not required to have physical presence in all Member States in which they operate when providing cross-border services within the Union. In this context, it is important to highlight that MiCA provides for one exception to the requirements for CASPs. However, third country firms have been given the possibility to circumvent the requirements in MiCA under the 'principle of reverse solicitation'. The principle of reverse solicitation applies in situations where services related to the crypto-assets market are provided at the exclusive initiative of the client.[98] According to Article 61(1) of MiCA, when a client either established or situated in the EU contacts a third-country firm for a crypto-asset service or activity by their own initiative, the requirement for authorization shall not apply to the provision of that service in question including the relationship between the parties related to the provision of that service or activity. As a result, when a customer initiates contact with a crypto platform or its representatives located in a third country, the company is not obliged to comply with the rules imposed on CASPs by MiCA.

The rationale for the principle of reverse solicitation rests on the idea that clients established or situated in the EU should not be excluded from using third-country firms if they choose to do so without previously having been solicited by such firms.[99] However, in a situation where a third-country firm solicits clients or prospective clients in the Union or promotes or advertises crypto-asset services or activities in the Union, its services should not be deemed to be crypto-asset services provided on the own initiative of the client.[100] In such a situation, the third-country service provider must apply for authorization as a CASP. In addition, Article 61(2) of MiCA also states that the own exclusive initiative of a client shall not entitle a third-country firm to market new types of crypto-asset services to that client. Third-country firms may, however, additionally offer to a client crypto-assets or related services of the same type as the one originally requested by the client without being in breach of the authorization requirements in MiCA.[101] The approach taken with MiCA to allow unauthorized third-country firms to provide crypto-asset services raises concerns as it also enables circumvention of MiCA. By exploiting this principle, third country service providers may be able to sidestep the market abuse rules imposed by the Regulation, if enforcement is not possible due to the location of the offender.

[98] ESMA 2024b, p. 5.
[99] Ibid, p. 6.
[100] Recital 75 MiCA Regulation.
[101] ESMA 2024b, p. 6.

However, ESMA has published guidelines on reverse solicitation, aiming to prevent and detect misuse and efforts to exploit or circumvent the exemption principle. In the guidelines, ESMA stated that genuine reverse solicitation situations should be understood as very limited and very narrowly framed.[102]

[102] Ibid, p. 7.

3 Responsibilities of Issuers, Offerors and Persons Seeking Admission to Trading of Crypto-Assets

3.1 Process for Initiating the Issuance, Offer or Admission to Trading

3.1.1 Application for Authorization and Supervisory Bodies

Competent authorities play an important role in the crypto-assets market. Competent authority is defined in Article 93(1) of MiCA as one or more authorities designated by a Member State with supervisory responsibility for the crypto-assets market. The responsibilities of competent authorities include supervision of the issuance, offer to the public and admission to trading of crypto-assets as well as the supervision of the activities of CASPs. The supervisory and investigative powers of competent authorities are listed in Article 94 of MiCA. Such powers include, for example, the power to suspend or prohibit the provision of crypto-asset services and the offer to the public or an admission to trading of crypto-assets, and to investigate infringements of the rules on market abuse.[103] Competent authorities also have the possibility under Article 111 of MiCA to impose penalties on issuers, offerors and persons seeking admission to trading of all crypto-assets, as well as on CASPs. In addition to the competent authorities, higher supervisory powers have been granted to either EBA or ESMA, depending on the type of crypto-assets under consideration.[104] The competent authorities are obliged to cooperate with EBA and ESMA, whose role is mainly to advice on the application of the Regulation, but the latter also have the possibility to intervene temporarily in specific market activities under Articles 103 and 104 of MiCA. However, the right of intervention of EBA or ESMA only applies to situations where the competent authority has not yet adequately done so. Lastly, in order to limit the scope of this thesis, additional obligations imposed on competent authorities, EBA and ESMA, for example in relation to their operational requirements or cooperation with each other or with third countries, will not be discussed in more detail.[105]

Under MiCA, there are two types of preliminary requirements for issuers, offerors and persons seeking admission to trading in the crypto-assets market, depending on the type

[103] Recital 98 MiCA Regulation.
[104] This division is further discussed in the context of significant ARTs and EMTs. For CASPs, ESMA has been given the primary higher supervisory powers in MiCA with regard to both standard and significant operators.
[105] For further information, the rights and obligations of competent authorities, EBA and ESMA are laid down under Title VII of MiCA.

of the crypto-asset they are involved with. These requirements include obtaining an authorization and the preparation and publication of a crypto-asset white paper. *A crypto-asset white paper* is a document providing the investors with the necessary technical aspects and other important information of a cryptocurrency or a blockchain project.[106] For issuers, offerors and persons seeking admission to trading of crypto-assets, the obligation to seek authorization applies solely to issuers of ARTs, as stated with regard to the scope of such entities. In relation to EMTs, MiCA requires issuers of such crypto-assets to be authorized but does not regulate the process as the authorization of credit institutions and EMIs is already covered by other EU legislation.[107] Issuers, offerors or persons seeking admission to trading of crypto-assets that fall into the third undefined category are not subject to similar authorization requirement. Given that MiCA limits the scope of authorization to issuers of ARTs, all references to issuers in this context refer only to such entities. Additionally, in order to narrow the subject, the scope of this thesis is only limited to the authorization process established by MiCA. By requiring authorization for operation from issuers of ARTs and EMTs, the competent authorities have the possibility to govern the overall issuance of such crypto-assets in the EU. In the case of ICOs, for example, it was found that such a restriction was necessary. Restricting the issuance of crypto-assets is also important in terms of market abuse, as there exists a high number of scams related to new tokens and coins in the crypto-assets market. Different types of market abuse will be further discussed in Chapter 5. of this thesis.

The application for authorization together with the crypto-asset white paper is submitted to the competent authorities of the Member State where the issuer is established, who may either approve or reject the application.[108] Article 21 of MiCA sets precise limits on when an application for authorization can be refused. Such grounds could be, for example, where there are objective and demonstrable grounds that the management body or its members fail to meet the criteria set out for them in the Regulation. The competent authorities must also refuse an authorization under Article 21(4) of MiCA if the ECB or another relevant central bank gives a negative opinion on risks posed to the smooth operation of payment systems, monetary policy transmission, or monetary sovereignty. The

[106] See, Recital 25 MiCA Regulation. The preparation and publication of the crypto-asset white paper is discussed in more detail in the next section.
[107] The authorization of credit institutions in the EU is covered by the Capital Requirements Directive 2013/36/EU (CRD), see Article 8(1) of CRD. In relation to the authorization of EMIs, see Article 1(1)(b) and Article 5 of PSD2.
[108] EBA 2024a, p. 6.

withdrawal of an authorization already granted is also possible in the specific situations provided for in Article 24 of MiCA. For example, the authorization must be withdrawn if the activity of the issuer poses a serious threat to market integrity, financial stability, smooth operation of payment systems, or poses serious risks in relation of money laundering and terrorist financing. This very possibility leaves the competent authorities with a lot of discretion to determine when the actions of the issuer may have negative consequences on the market or possibly create opportunities for market abuse or crime. Here too, the opinion of the ECB or other central bank is relevant, and a negative assessment may under Article 24(3) of MiCA lead to a limitation on the amount of crypto-assets to be issued or an imposition of a minimum denomination amount of the ART, or even to a withdrawal of authorization.

3.1.2 Crypto-Asset White Paper and Marketing Communications

Historically, white papers were fully promotional documents which provided explanations about the crypto-asset and its goals, but MiCA defined their status as regulated mandatory information in the EU.[109] Entities involved in the issuance, offering and admission to trading of crypto-assets must publish a crypto-asset white paper to inform potential retail holders of the characteristics, functions and risks of the crypto-asset in question. For ARTs and EMTs, this entity is the issuer, while for crypto-assets falling into the third undefined category, the responsibility for the preparation and publication of the white paper lies with the offeror or the person seeking admission to trading of such an asset. MiCA regulates the submission and content of the white paper separately for each category of crypto-assets falling within its scope. The content requirements for the crypto-asset white paper are largely equivalent for all crypto-assets, but more specific in relation to ARTs and EMTs.[110] In general, white papers should contain general, fair, clear and non-misleading information on the issuer, offeror or person seeking admission to trading, the project, the offer or admission to trading, the rights and obligations, the underlying technology and the associated risks.[111] The document must also provide further information on the reserve of the assets, where applicable, and the climate and other environmental impacts of the mechanisms that enable the use of the crypto-asset.

---

[109] ESMA 2023a, pp. 56.
[110] With regard to the specific content and form requirements of a crypto-asset white paper in relation to each crypto-asset group, see Article 19 of MiCA for ARTs, Article 51 for EMTs and Article 6 for the third undefined group of crypto-assets.
[111] Recital 24 MiCA Regulation.

In relation to ARTs, the crypto-asset white paper draft is submitted as an attachment to the application for authorization, where its content and format are reviewed by the competent authorities. Issuers of EMTs, as well as offerors and persons seeking admission to trading of crypto-assets other than ARTs and EMTs must publish a crypto-asset white paper on their own initiative and to notify it to the competent authorities.[112] All entities required by MiCA to prepare a crypto-asset white paper must also modify the document in situations where there are significant changes to their organization or operations that occur after the authorization or the publication of the white paper.[113] This requirement for modification includes notification to the competent authorities of such circumstances and of the modified crypto-asset white paper. As regards for the issuers of ARTs, the modified white paper must be approved by the competent authorities in accordance with Article 25(2) of MiCA, as it is a condition for the authorization. In addition to the publication of a crypto-asset white paper, offerors and persons seeking admission to trading of crypto-assets other than ARTs and EMTs are obliged to publish marketing communications, such as advertising messages and marketing material.[114] The obligation stipulates that marketing communications must also be submitted to the competent authorities on request under Article 8(2) of MiCA. Such marketing communications are required to be fair, clear and non-misleading, and also consistent with the information provided in the crypto-asset white paper.[115] Issuers of ARTs and EMTs are not subject to the same obligation to prepare marketing communications. However, they are required to provide any marketing communications to the competent authorities upon request if such documents have been prepared.[116]

An exemption from the requirement to publish both a crypto-asset white paper and marketing communications has been granted for certain small offers of crypto-assets other than ARTs and EMTs. According to Article 4(2) of MiCA, such offers to the public include offers to fewer than 150 natural or legal persons per Member State, offers where the total cost of the offer over a 12-month period does not exceed EUR 1 million, and

---

[112] On the obligation to publish and notify a crypto-asset white paper, see Articles 4(1)(b)-(d) and 5(1)(b)-(d) of MiCA in relation to offerors and persons seeking admission to trading of crypto-assets other than ARTs and EMTs. For issuers of EMTs, see Article 48(1)(b) of MiCA.
[113] On the modification of a crypto-asset white paper in relation to each crypto-asset group, see Article 25 of MiCA for ARTs, Article 51 for EMTs and Article 12 for the third undefined group of crypto-assets.
[114] On the obligation to publish marketing communications, see Articles 4(1)(e)-(f) and 5(1)(e)-(f) of MiCA in relation to offerors and persons seeking admission to trading of crypto-assets other than ARTs and EMTs.
[115] Recital 24 MiCA Regulation.
[116] On the requirement to provide marketing communications on request, see Article 29(5) of MiCA for issuers of ARTs and Article 53(5) of MiCA for issuers of EMTs.

offers where the crypto-assets are addressed only to, and may be held exclusively by, qualified investors. However, this exemption does not apply if the offeror also intends to seek admission to trading of such crypto-asset. Furthermore, if the crypto-asset white paper is voluntarily drafted despite the exemption, other relevant requirements apply under Article 4(8) of MiCA. Issuers, offerors or persons seeking admission to trading of all crypto-assets are liable of any incomplete or misleading information in the white paper or in the modified version thereof, if losses are incurred as a result of this breach.[117] The rule on the liability for the information provided in the white paper is non-contractual and any conflicting provisions drafted contrary will not apply.[118]

3.1.3 Traditional Financial Institutions

MiCA facilitates and creates opportunities for traditional financial operators to smoothly expand their operations into the crypto-assets market. As previously mentioned, credit institutions are not obligated to seek for authorization under MiCA when conducting in the issuance of ARTs. However, the legislators concluded that credit institutions should be subject to all other conditions and requirements applicable to the issuance of ARTs, except the requirements in relation to authorization, own funds and the approval procedure of qualifying shareholders.[119] Therefore, credit institutions must also prepare and submit a crypto-asset white paper to the competent authority in accordance with MiCA when participating in the issue of ARTs. Credit institutions and EMIs shall also, when involved in the issuance of EMTs, draw up a crypto-asset white paper and notify it to the competent authority.[120] It is worth noting, however, that the legislation concerning EMIs may be subject to change or modification in the near future, as the Commission has issued a draft of the Third Payments Services Directive (PSD3) in June 2023. The draft aims to clarify the definition of providers of EMTs, which would result in the disappearance of EMIs and their definition transforming into payment institutions providing electronic money services.[121] At the same time, a new category of services, 'electronic money services', would be created, including, for example, the issuance of electronic money. As one might expect, such modifications may pose challenges in the future, since MiCA does

[117] On liability for the information given in a crypto-asset white paper, see Article 26 of MiCA for ARTs, Article 52 of MiCA for EMTs and Article 15 of MiCA for the third undefined group of crypto-assets.
[118] Maume 2023, p. 264.
[119] Recital 44 MiCA Regulation.
[120] Recital 66 MiCA Regulation.
[121] Herrera 2025, p. 378.

not recognize the new definitions. If PSD3 were to come into force in such a form, possible regulatory overlaps between MiCA and the regulation of electronic payment services could also increase concerning the issuance of EMTs and the provision of related services. However, as PSD3 is still in a draft form, it is still vulnerable to changes and will not be applicable for a long time. It should also be noted that PSD2 and the draft PSD3 only apply to EMTs, not ARTs or other crypto-assets.

As this thesis will not revisit in more detail the exemptions granted to traditional financial institutions entering the crypto-assets market, in this context it is also appropriate to briefly highlight the separate rules set in MiCA for investment firms or other similar entities aiming to provide services related to crypto-assets. Article 60 of MiCA allows traditional financial institutions such as investment firms, UCITS management companies and alternative investment funds to smoothly extend their services to crypto-assets. The crypto-asset services provided must be comparable to those investment services and activities the investment firm is authorized to propose. The Article 60 of MiCA also specifies how the traditional financial services will correlate with the crypto-related services to meet this requirement and what information must be provided to the competent authorities. The information to be submitted to the competent authority is very similar in content and requirements to that required of banks and EMIs involved in the issuance of ARTs or EMTs.

3.2 Operational Requirements for Issuers of ARTs

3.2.1 Conduct of Business and Prudential Requirements

Having previously covered the scope and the authorization process for issuers of ARTs in MiCA, the following paragraphs focus on the operational requirements for such entities when conducting business in the crypto-assets market. Different obligations and requirements are laid down for issuers of different crypto-assets to improve market integrity, protect retail holders and reduce the potential for abuse. Provisions in this respect are set out in MiCA for each crypto-assets category separately, considering their specific characteristics. As stated before, since ARTs could be widely adopted and thus pose increased risks, the related legislation is deliberately more stringent compared to EMTs and other crypto-assets.[122] The issuers of ARTs have a general obligation, according to Article 27

[122] Recital 40 MiCA Regulation.

of MiCA, to act honestly, fairly and professionally in the best interests of the holders and to treat them equally with some exceptions allowed, such as those specifically mentioned in the white paper or marketing communications. Article 34(2) and (4) of MiCA also imposes strict requirements for members of the management body and shareholders, emphasizing, for example, their level of personal competence, good repute and lack of criminal record.

A reporting obligation to the competent authorities has been imposed on issuers of ARTs in Article 22(1) of MiCA. The obligation consists of a requirement to provide quarterly reports to the competent authority on the status of the ART if its circulating value exceeds EUR 100 million. The required information includes, for example, the current number of holders, the value of the issued ART, the size of reserve assets, as well as the average number and total value of daily transactions. The data received is then monitored and controlled by the competent authorities, and it follows that additional restrictions may be imposed on issuers of ARTs under Article 23(1) of MiCA when the estimated quarterly average number and average total value of daily transactions is above 1 million transactions and EUR 200 million. The issuer of such asset shall in these circumstances stop issuing the ART and within 40 days of crossing the threshold, submit a plan to the competent authority to ensure that the activities remain within the set limits in the future. The issuer may only continue to issue the ART when the evidence is clear that the activity is occurring within the thresholds. The same information obligation may also be imposed on issuers of ARTs with a lower circulating value under Article 22(2) of MiCA.

Issuers of ARTs are at all times required to maintain a reserve of assets in accordance with Article 36(1) of MiCA to ensure their solvency in relation to their liability to holders. The reserve of assets should be used for the benefit of the holders of the ARTs when the issuer is not able to fulfil its obligations towards the holders, such as in insolvency situations.[123] This follows from the requirement in Article 39(1) of MiCA whereby holders of ARTs are at all times entitled to redemption and that issuers of such assets must establish, maintain and implement a recovery and redemption plan in this regard. For these reasons the reserve of assets should also be composed and managed in a way that market and currency risks are covered, including clear and explicit procedures to ensure that the reserve is completely separate from the funds of the issuer, that the reserve assets are not

[123] Recital 54 MiCA Regulation.

encumbered or pledged as collateral, and that the issuer of the ARTs has prompt access to the assets.[124] In addition to having a reserve of assets, issuers of ARTs are also required by Article 35(1) of MiCA to hold a certain amount of own funds. Issuers of ARTs should always have own funds equal to either an amount of EUR 350 000, 2 % of the average amount of the reserve assets or a quarter of the fixed overheads of the preceding year, whichever total is the highest. However, the competent authority may increase this requirement by up to 20 % under Article 35(3), if the risks associated with the activity or the nature of the undertaking are deemed to be higher. An assessment of this will be carried out on the basis of a regular stress testing.[125]

A wide range of requirements regarding disclosure and use of information has also been set out for issuers of ARTs. These requirements can be broken down into those concerning holders, internal measures and information to be provided to the competent authority. Issuers of ARTs have, in addition to the information provided in the white paper, an ongoing obligation to inform holders about the asset under Article 30(1) of MiCA. The content of this information obligation includes, in particular, timely information on the number of ARTs in circulation and the value and composition of the reserve assets.[126] Concerning the intra-organizational flow of information, the issuers of ARTs are required under Article 32(1) of MiCA to put in place systems to prevent, detect and disclose potential conflicts of interest. However, the obligation is limited to relationships between the issuer of the ART, and the shareholders and members, entities with a qualifying holding in the issuer, members of the management body, employees, holders of ARTs and any third parties related to the reserve or distribution of assets. As regards to the information to be provided to the competent authority, issuers of ARTs have an additional obligation under Article 33 of MiCA to provide the supervisory body with all information on changes concerning the management body of the issuer.

Finally, MiCA aims to protect the holders and integrity of the crypto-assets market by regulating acquisitions of issuers of ARTs in Article 41 of MiCA. Article 41(1) states that any natural or legal person seeking to acquire or increase a qualifying holding in an issuer of an ART must notify the competent authority of such an act. A qualifying holding is defined to occur when the proportion reaches or exceeds 20 %, 30 % or 50 % of the voting

[124] Recital 55 MiCA Regulation.
[125] EBA 2024d, p. 11-12.
[126] Recital 48 MiCA Regulation.

rights or of the capital held, or when the issuer of the ART would either cease to be or become a subsidiary of that person. The same applies under Article 41(2) of MiCA where a person seeking to dispose of a qualifying holding of any size in an issuer of an ART or where the proportion of voting rights or capital held by that person would, as a result of the disposal, fall below 10 %, 20 %, 30 % or 50 %, or so that the issuer of an ART would cease to be a subsidiary of that person. The competent authority, after receiving the notification, evaluates the proposed acquisition on the basis of the criteria set out in Article 42(1) of MiCA. However, it is stated in Article 42(2) of MiCA that the competent authority may oppose the proposed acquisition only when there are reasonable grounds for doing do based on the criteria or when the information provided has been identified as incomplete or incorrect.

3.2.2 Significant ARTs

Issuers of ARTs are primarily supervised by the competent authorities and ESMA. However, if the crypto-asset issued is defined as "significant", the supervisory role will fall to EBA. Both ARTs and EMTs are deemed as significant when they meet, or are likely to meet, certain criteria, including a large customer base, high market capitalization or large number of transactions.[127] The criteria for defining ARTs as significant are laid down in Article 43(1) of MiCA. The definition is met, when the number of the holders is more than 10 million, when the value of the asset in circulation, its market capitalization or the size of the asset reserve held by the issuer is higher than EUR 5 trillion or, when the average number and aggregate value of transactions per day is higher than 2,5 million transactions and EUR 500 million. Issuers that are providers of a core platform services designated as gatekeepers also meet the criteria for an issuer of significant ART.[128] In addition, the existence of a potentially significant ART may also be assessed through its international significance or whether the asset or its issuers are interconnected with the financial system. Lastly, the criteria are also met if the operator has issued at least one additional ART or EMT and provides at least one crypto-asset service. According to Article 43(2) of MiCA, EBA shall classify an ART as significant when at least three of the above criteria are met. Each year, EBA will assess and determine whether ARTs deemed

[127] Recital 59 MiCA Regulation.
[128] According to Article 3(1) of the Digital Markets Act (EU) 2022/1925 (DMA), an undertaking shall be designated as a gatekeeper if it has a significant impact on the internal market, provides a core platform service which is an important gateway for business users to reach end users and enjoys an entrenched and durable position or it is foreseeable that it will enjoy such a position in the near future.

as significant continue to meet the criteria set by the Regulation.[129] Article 44 of MiCA also allows for a voluntary application for designation of an ART as significant, provided that the criteria are met, in which case EBA will take a decision on the basis of an application.

Significant ARTs were perceived as risks in terms of financial stability, monetary policy transmission and monetary sovereignty, if used improperly or negligently.[130] As a result, the most relevant aspect of defining ARTs as significant is the additional requirements imposed on such crypto-assets and their issuers in Article 45 of MiCA. For example, issuers of significant ARTs are obligated under Article 45(1) of MiCA to adopt and maintain a strict remuneration policy promoting a sound and effective risk management. In addition, such entities are also required under Article 45(3) and (4) of MiCA to continuously assess and monitor the required level of liquidity of the crypto-asset and therefore establish and maintain a liquidity management policies and procedures, including regular liquidity stress testing. On this basis, EBA may impose stricter requirements to improve the liquidity of the ART and to protect holders and ensure market integrity. As regards the requirement for own funds held by issuers of ARTs defined as significant, the level for the average amount held is set at 3% of the reserve assets instead of 2% compared to issuers of standard ARTs.[131] In its draft regulatory technical standards, EBA has set a time limit of up to six months for the competent authority to grant permission for issuers of significant ARTs to meet this requirement.[132]

3.3 Operational Requirements for Issuers of EMTs

3.3.1 Conduct of Business and Prudential Requirements

Given that the issuers of EMTs were already subject to strict regulation due to their nature, MiCA refers to other legislation for general operational requirements in relation to the rules imposed on issuers of such crypto-assets. According to Article 48(3) of MiCA, the provisions of EMD2 concerning requirements for the taking up, pursuit and prudential supervision of the business of EMIs, as well as the issuance and redeemability of e-money are binding as regards the issuance of EMTs. MiCA mainly lays down rules, partly as

[129] EBA 2024c, p. 2.
[130] Recital 59 MiCA Regulation.
[131] Ibid, p. 5 (Point 4.)
[132] EBA 2024b, p. 8.

recognized exception to provisions of EMD2, regarding issuance and redeemability, investment of funds received in exchange of EMTs, as well as the requirement for recovery and redemption plan. However, there are also similar legal provisions between MiCA and EMD2, such as the prohibition of granting interest. As defined in Article 2(1) of EMD2, the definition of EMIs includes all legal persons authorized to issue electronic money, including credit institutions. Therefore, when referring to the provisions of EMD2 in this section, reference is made to both EMIs and credit institutions eligible to issue ARTs under MiCA.

Similar to the requirements imposed on issuers of ARTs in MiCA, EMD2 sets out rules on issuers of EMTs in relation to own funds of the issuer and protection of holders. Article 4 of EMD2 sets a limit of EUR 350 000 for the initial capital that an EMI must hold when applying for authorization under EMD2. As per Article 5(1) of EMD2, the amount of the own funds may not fall below the above amount or below the thresholds otherwise calculated in accordance with EMD2, whichever is higher. The calculation methods for the minimum amount of funds held may vary depending on whether the EMI offers services other than the issuance of EMTs. However, under Article 5(2) and (3) of EMD2, this requirement shall amount to at least 2 % of the average outstanding electronic money with regard to activities concerning the issuance of EMTs, and similarly to ARTs, the competent authority has the possibility to assess the adequacy of the funds. EMD2 imposes general requirements for EMIs on safeguarding the funds received in exchange for EMTs, but MiCA takes this requirement even further by restricting the investment of such funds in its Article 54. As regards the issuance and redeemability of EMTs, Article 49(1) of MiCA provides that the relevant provisions of EMD2 shall prevail over those of MiCA.

Issuers of EMTs are also subject to many obligations in relation to disclosure of information. According to Article 3(2) of EMD2, EMIs are, for example, required to inform the competent authorities in advance of any material changes in measures taken for safeguarding of funds received in exchange for the electronic money issued. As regards the sale or purchase of a qualifying holding, the general prudential rules of EMD2 indicate that the issuers of EMTs are subject to essentially the same reporting and information obligations to the competent authority as issuers of ARTs. However, EMD2 provides the competent authority with more robust tools to prevent such action if necessary. Article 3(3) of EMD2 states that if the impact of the proposed acquisition of an EMT issuer would be detrimental to the operator or if there has been a breach of disclosure obligations, the

competent authority could take other appropriate measures to bring such a situation to an end. Such measures may include injunctions, administrative sanctions or suspension of the exercise of voting rights attached to the shares in question. If the acquisition of a qualifying holding is carried out over the objection of the competent authority, measures may include suspension of the voting rights of the acquirer, nullity of votes cast or the possibility to have the votes annulled.

3.3.2 Significant EMTs

Separate rules and requirements have also been established for EMTs identified as significant under MiCA. In this respect, the requirements set out in MiCA for significant ARTs also apply to EMTs when at least three of the criteria, earlier introduced in this thesis in relation to significant ARTs, are met. However, Article 56(7) of MiCA provides an exception to this rule that also deviates from the rules set out for significant ARTs. The provision states that the supervisory responsibilities shall not be transferred to EBA in relation to issuers of significant EMTs whose official currency is other than the euro, if at least 80 % of the number of holders of such assets and the volume of transactions is concentrated in a Member State where the issuer is primarily established. In this case, the competent authority of the Member State must provide EBA with annual information on any entities operating in relation to such exemption. The assessment process for significant EMTs is also similar to that set out in MiCA for significant ARTs, where EBA will reassess the categorization of the asset annually.[133]

In MiCA, certain provisions concerning standard ARTs have also been extended to cover issuance of significant EMTs under Article 58 of MiCA, such as requirements to have a reserve of assets and to conduct regular liquidity and operational stress testing. In addition, the requirement purely limited to significant ARTs, whereby the average amount held in reserve should consist of 3 % of reserve assets instead of 2 %, may be extended to apply to significant EMTs. The competent authority has also been given the power to extend the requirements imposed on significant EMTs to EMIs issuing regular EMTs, where this is necessary to manage risks. Finally, similar requirements to the requirements imposed on ARTs have been imposed on EMTs denominated in currencies other than official currencies of Member States. Such requirements include more stringent reporting obligations, restrictions on the issuance of tokens used widely as a means of exchange,

[133] EBA 2024c, p. 1 (Point 1.)

and limiting or controlling the amount of the tokens issued when the potential for risks is perceived to have risen.

3.4 Operational Requirements for Offerors and Persons Seeking Admission to Trading of Other Crypto-Assets

The third undefined category of crypto-assets, which includes utility tokens, is regulated by MiCA distinctly from ARTs and EMTs. For example, the rules set out for significant crypto-assets do not apply to this category while the obligation for robust marketing communications, as outlined previously, plays a greater role. The third category is more broadly regulated, as it covers a wide range of different types of assets. Article 14(1) of MiCA sets out general operational requirements for both offerors and persons seeking admission to trading of crypto-assets other than ARTs and EMTs. Such legal persons are obligated to act honestly, fairly and professionally and to communicate with holders, and prospective ones, fairly, clearly and not in a misleading manner. Offerors and persons seeking admission to trading are also required to identify, prevent, manage and disclose any possible conflicts of interest under the provision and to maintain all of their systems and security access protocols in conformity with the appropriate Union standards. ESMA has issued guidance to clarify the definition of 'systems' as well as 'appropriate Union standards'. According to ESMA, the term systems should be interpreted narrowly regarding the guidelines and is used mainly to refer to information and communications technology (ICT).[134] Additionally, offerors and persons seeking admission to trading of other crypto-assets than ARTs and EMTs are required under Article 14(2) of MiCA to act in the best interests of the holders and to treat them equally, apart from exceptions indicated in advance in the crypto-asset white paper or marketing communications.

Article 10 of MiCA imposes requirements on offerors in relation to the funds collected to safeguard the interests of holders in the course of the offering. Offerors setting a time limit on their offer are required by Article 10(3) of MiCA to have effective arrangements in place to protect the holders' funds or assets raised during the offering. Where no time limit has been set for the offer, such issuers are required to act under the same obligation in accordance with Article 10(4) of MiCA until the holders' right of withdrawal has expired. The retail holders have the right to withdraw from their agreement to purchase

[134] ESMA 2024c, p. 7.

crypto-assets other than ARTs or EMTs, under Article 13(1) of MiCA, without any fees or costs and without having to justify themselves. The right of withdrawal is valid for 14 days from the date of the agreement. Naturally, the offeror is then obliged by Article 13(2) of MiCA to reimburse all payments and charges already received without undue delay and in any event no later than 14 days upon being informed of the withdrawal decision. However, the right of withdrawal does not apply to situations where the crypto-assets have been admitted to trading prior to their purchase by the retail holder because, in such cases the price of the assets depends on the fluctuations of the market.[135] The same applies in situations where the subscription period has ended in relation to offers where the time limit has been set. In the event of cancellation of the issuance of a crypto-asset that is not an ART or EMT, the responsible operators are obliged under Article 14(3) of MiCA to return the funds collected from the holders within 25 days.

Offerors of crypto-assets other than ARTs and EMTs are also subject to additional requirements relating to the disclosure of information concerning the time limit for the offer. If a deadline for the offering has been set by the issuer, the operator is required by Article 10(1) of MiCA to publish the result of the offer on its website within 20 days of the end of the subscription period. Similarly, where no time limit has been set, the offeror is obliged under Article 10(2) of MiCA to publish on its website the number of units of the crypto-asset in circulation on an ongoing basis, at least monthly. However, as an exemption from the reporting requirements, Article 11(2) of MiCA states that the offerors and persons seeking admission to trading of crypto-assets falling within the scope of the third undefined category that have published a white paper, or a modified one, are not subject to any further information requirements with regard to the offer or admission to trading of that specific asset. Compared to the extensive disclosure requirements imposed on issuers of ARTs and EMTs, the difference is significant and highlights the regulatory divergence between different crypto-asset categories. In general, the issuance and offering of assets falling under the third undefined category may be considered to be more difficult to supervise than the same activities related to ARTs and EMTs.

[135] Recital 37 MiCA Regulation.

4 Rights and Responsibilities of CASPs

4.1 Identified Risks and Regulation Specific to CASPs

Since the EU legislators identified a lot of risks and possibilities of misuse regarding CASPs, their operation is strictly regulated in MiCA, starting from the authorization process to the ongoing obligation to monitor and notify authorities of suspected and discovered cases of market abuse. According to a supervisory briefing issued by ESMA on 31 January 2025 after the full entry into force of MiCA, there are no low-risk CASPs.[136] This conclusion is justified by ESMA by the fact that CASPs often deal directly with retail investors and also have a limited track record on regulatory compliance and supervision. In addition, the novelty of the crypto sector itself poses risks to the integrity of the operations of CASPs and creates challenges for their monitoring and supervision. ESMA points out in its supervisory briefing that the idea of the non-existence of low-risk CASPs creates an environment where only a scrutinized approach is possible in the assessment of authorization applications for which the circumstances seem to suggest the need for enhanced vigilance.[137] ESMA also stated that the money laundering and terrorist financing risks presented by CASPs are generally high.[138] CASPs are exposed to these risks, in particular due to the specific features in their business structure, the cross-border nature of the activities, the possibility of profound anonymity of the parties involved, and the technology used. The issue and risks of outsourcing arrangements were also discussed in the supervisory briefing. In this context, the delegation of functions or services to the extent that the CASP would become a letter-box entity was forbidden.[139]

In relation to the identified risks associated with CASPs, other relevant legislation and policy guidelines have also been deemed necessary. For example, in December 2023, the Regulation on Information Accompanying Transfers of Funds and Certain Crypto-Assets (EU) 2023/1113 (TFR) came into effect revising the earlier regulation on the matter and extending its scope to the transfer of specific crypto-assets. In addition, the revised TFR

[136] ESMA 2025a, p. 6.
[137] Ibid, p. 6.
[138] Ibid, p. 6.
[139] Ibid, p. 14. Letter-box entities are legal entities established on paper in any EU jurisdiction without or with a minimal link to economic material activities carried out in that jurisdiction but just enough to enable legal standards that apply in the country of legal residence. See, McGauran 2016, p. 9.

amended the Directive on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (EU) 2015/849 (4th Anti-Money Laundering Directive, 4AMLD) by subjecting CASPs authorized by MiCA to the same requirements and supervision as other traditional credit or financial institutions.[140] To further extend the supervision of CASPs, Article 38(3) of the revised TFR obligated EBA to issue guidelines on risk variables and factors to consider by CASPs when entering into business relationships or carrying out transactions in crypto-assets. The revised TFR also introduced new rules for 4AMLD in its Article 19b regarding due diligence requirements for CASPs in high-risk money laundering and terrorist financing situations and when engaging in relationships with third country operators authorizing EBA to address these issues as well. As a result, on 16 January 2024, EBA released an amended version of its guidelines on money laundering and terrorist financing risk factors ('The ML/TF Risk Factors Guidelines'), in which the scope of the guidelines was presumably extended to include CASPs.[141] Article 36 of the revised TFR also requires EBA to draw up guidelines on issues such as missing or incomplete information on the payer, payee, originator or beneficiary. Accordingly, on 4 July 2024, EBA published guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers ('Travel Rule Guidelines').[142] Directive 4AMLD has been subsequently amended and repealed, with the current directive being the 6th Anti-Money Laundering Directive (6AMLD) (EU) 2024/1640.

4.2 Authorization Process of CASPs

As discussed before, all operators providing crypto-related services within the EU are required to apply for authorization as CASPs under MiCA. The process for authorization provided for in Article 63 of MiCA follows a very similar pattern to that set out for issuers of ARTs in MiCA, with some exceptions. One notable exception to the authorization process for issuers of ARTs is that in relation to CASPs, the competent authorities are required to carry out far more consultation and investigation work before taking a final decision on the application. Before granting or refusing an authorization, the competent authorities are obliged under Article 63(5) of MiCA to consult the competent authorities of any other Member State to which the applicant CASP has relevant connections. In

[140] Travel Rule Guidelines 2024, p. 4.
[141] ML/TF Risk Factors Guidelines 2024, p. 11.
[142] Travel Rule Guidelines 2024

accordance with Article 63(6) of MiCA, the competent authorities also have to verify with other Member States whether the applicant CASP has been subjected to investigation relating to money laundering or terrorist financing and to ensure that applicant CASPs with links to high-risk third countries comply with the legislation of the Member States in which they operate. Article 9(1) of the 6AMLD defines high-risk third countries as third-country jurisdictions with strategic deficiencies in their national regimes on anti-money laundering and countering the financing of terrorism that pose significant threats to the financial system of the EU. In addition, competent authorities are required to cooperate and communicate more closely with ESMA during the authorization process particularly in relation to CASPs identified as significant. According to Article 85(1) of MiCA, a CASP is considered significant if it has at least 15 million active users in the EU within one calendar year.

As regards the grounds for refusing authorization, the competent authorities must, in accordance with the Article 63(8) of MiCA, reject an application if their supervisory obligations are prevented from being effectively fulfilled due to the close links of the applicant CASP to one or more natural or legal persons whose activities are subject to the to the regulatory regime of a third country. In situations where close links exist between the applicant CASP and other natural or legal persons, the competent authorities may only grant authorization by Article 63(7) of MiCA when the arrangement is not an obstacle to the effective fulfilment of supervisory obligations. The competent authorities are also obligated under Article 63(10) of MiCA to refuse authorization where the management body of the applicant CASP poses risks to the entity, its customers or the integrity of the market, or otherwise exposes the operator to a serious risk of money laundering or terrorist financing, and where the applicant CASP itself or persons involved in its activities, such as board members or shareholders, do not meet the criteria set for them in MiCA. Furthermore, if the outsourced activities of a CASP are at a level that raises concerns for the supervision, the application should be rejected.[143]

Under Article 59(4) of MiCA, authorized CASPs must continue to meet the criteria for authorization at all times. The authorization may be withdrawn in whole or in part, under the grounds set out in Article 64(1) and (2) of MiCA, if a CASP no longer meets the criteria and has not taken the corrective action requested by the competent authority

[143] ESMA 2025a, p. 8.

within the timeframe set. However, some activities and entities are fully exempt from the obligation to apply for authorization as a CASP. According to Article 4(5) of MICA, an authorization is not required for the provision of custody, administration or transfer services for crypto-assets that fall within the third undefined category of crypto-assets, the provision of which is exempt under already discussed Article 4(3) of MiCA. This exemption does not apply in situations where another offer of the same crypto-asset is made, and that offer does not benefit from the exemption, or where the crypto-asset offered is admitted to a trading platform. In addition to such activities, EMIs should be able to provide custody services of EMTs issued by them, without a prior authorization.[144] Natural or legal persons allowed to distribute EMTs under EMD2 should also be exempt from the requirement to seek authorization to provide crypto-asset services for the activity of the placing of crypto-assets.[145] For both entities, this derogation is due to an effort to prevent regulatory overlap.

4.3 Conduct of Business and Prudential Requirements

As authorized operators, CASPs have a comparable obligation to issuers of ARTs to act honestly, fairly and professionally in the best interests of the clients and to provide them with all the necessary information in a fair, clear and non-misleading manner laid down in Article 66(1) and (2) of MiCA. Article 68 of MiCA imposes similar requirements on CASPs as on issuers of ARTs regarding the character, competence and lack of criminal record of persons profoundly involved with the business, such as board members and shareholders. The same applies to proposed acquisitions, whose legal treatment for CASPs mirrors that for issuers of ARTs.[146] In general, the level of regulation on CASPs and issuers of ARTs is very consistent. This is probably due to the fact that the aim of MiCA was to provide proportionate treatment for market participants, thereby giving raise to equal opportunities in respect of market entry and development of the market.[147] However, CASPs are not subject to as stringent disclosure requirements as issuers of ARTs. The disclosure requirements imposed on CASPs by Articles 66 and 69 of MiCA mainly relate to changes in the governing body, informing customers about the risks of

[144] Recital 91 MiCA Regulation.
[145] Recital 92 MiCA Regulation.
[146] EBA 2024e, p. 6.
[147] Recital 6 MiCA Regulation.

crypto-assets transactions, and providing specific information on the website of the service provider.

Prudential requirements imposed on CASPs are primarily aimed at safeguarding client assets. To achieve adequate protection of customers' funds, CASPs are required under Article 67(1) of MiCA to always have prudential safeguards in place. The provision states that such safeguards should consist of an amount equal to the permanent minimum capital, which according to Annex IV of MiCA is either EUR 50 000, 125 000 or 150 000 depending on the types of services provided, or an amount equal to one quarter of the fixed overheads of the previous year, whichever higher. According to Article 67(4) of MiCA, the prudential safeguards required may consist of own funds or an insurance policy covering the territories of the EU where the services are provided, or an equivalent guarantee, or a combination of the two. In addition, to ensure compliance with MiCA, CASPs are obliged to establish various internal policies, systems and procedures for safeguarding clients' funds and crypto-assets, as well as solid risk management and secure ICT systems.[148]

As mentioned earlier, one of the risk factors associated with CASPs is the outsourcing of services and activities to third parties and also grounds for rejecting an application for authorization. In an attempt to manage related risks, Article 73(1) of MiCA places all responsibility for outsourced services and activities on CASPs themselves and emphasizes the need to ensure compliance with all other obligations laid down for such entities. For example, CASPs must under Article 73(2) and (3) of MiCA have a comprehensive policy on their outsourcing, as well as written contracts with all third parties. Additionally, CASPs and third parties are required to make all necessary information available for authorities to assess the compliance of the outsourced activities in accordance with Article 73(4) of MiCA. ESMA has also taken a position on the outsourcing of CASPs, especially in terms of key functions and outsourcing to third countries. For such functions as internal control, risk assessment and IT control, ESMA considered that while outsourcing parts of these duties is possible, this should not jeopardize regulated entities' activities, effec-

[148] ESMA 2025a, p. 12–13.

tive supervision by competent authorities or compliance with money laundering legislation.[149] In this respect, the supervisory briefing also highlights the restriction on the outsourcing of anti-money laundering activities. Overall responsibility for this, as well as for other important activities, should always remain with CASPs. On outsourcing outside the EU, ESMA will require competent authorities to determine on a case-by-case basis whether the activities are carried out in accordance with the requirements set out in MiCA.[150]

While the level of regulation on CASPs is generally comparable to the regulatory standards placed on issuers of ARTs, MiCA also sets out specific requirements for each main type of crypto-asset service separately. This follows the recognition amongst legislators of the need to regulate crypto-asset services adequately, reflecting the specific risks and challenges associated with each type of activity.[151] These requirements are covered in Chapter 3 of Title V of MiCA, but it is not appropriate to go into their full content in detail in this thesis. However, a few important points are of relevance. In terms of liability, CASPs providing custody and administration of crypto-assets are liable to their clients for any losses resulting from an incident related to ICT, including cyber-attack, theft or malfunctions.[152] In this context, however, hardware or software providers of 'self-hosted' or 'non-custodial' wallets have been excluded from the scope of MiCA, affecting the area covered by the Regulation as a whole. Self-hosted and non-custodial wallets refer to wallets that are controlled by the owner of the assets as opposed to a hosted wallet, where a third party is responsible for the management, custody, security and use of the crypto-assets on behalf of the owner.[153] Another important matter is the obligation for CASPs operating a trading platform to prevent and report market abuse. Article 76(8) of MiCA requires such CASPs to inform competent authorities whenever they might identify cases of market abuse or attempted abuse occurring on or through their trading systems. CASPs operating a crypto trading platform should also have a transparent fee structure for the services provided to avoid the placing of orders that could contribute to market abuse or disorderly trading conditions.[154]

---

[149] Ibid, p. 14–16.
[150] Ibid, p. 14–16.
[151] Recital 83 MiCA Regulation.
[152] Ibid.
[153] Whitehouse-Levine - Kelleher 2020, p. 5-6.
[154] Recital 84 MiCA Regulation

5 Regulation of Market Abuse in MiCA

5.1 MiCA Provisions on Market Abuse in Relation to Other Legislation

The content of MiCA was heavily influenced by other existing legislation when it was enacted. Consequently, MiCA incorporates many existing terms and concepts, such as financial instruments defined in MiFID II and EMIs defined in EMD2, which contributes to a deeper understanding of the crypto sector and allows for a better adaptation to the scale of traditional finance. Using existing legislation as a basis for regulation of crypto-assets is objectively reasonable. However, integrating existing terms and concepts into a completely new area of finance without modification could also create challenges and contradictions if these are not fully compatible with the crypto sector as such. In addition to terms and concepts, MiCA incorporates almost directly equivalent provisions from other legislation on various aspects. One such example is Article 61 of MiCA on the principle of reverse solicitation, the content of which is very much in line with Article 42 of MiFID II. In general, MiFID II served as a basis for many of the provisions in MiCA for a reason, as the sectors of traditional financial instruments and crypto-assets are becoming increasingly integrated.

The provisions on market abuse in MiCA, which cover issues such as insider dealing, unlawful disclosure of inside information and market manipulation, are largely based on the corresponding provisions of MAR. However, MiCA contains only seven provisions on market abuse, compared to 39 related provisions of MAR. Legislators, when drafting MiCA, recognized that as the issuers of crypto-assets and CASPs are predominantly composed of small or medium-sized enterprises, it would be disproportionate to apply all of the provisions of MAR to them.[155] In order to increase user confidence and market integrity in the crypto-assets market, for MiCA, it was considered necessary to introduce new and market-specific provisions on market abuse. Nevertheless, the final market abuse provisions of the Regulation ended up being a reduced version of those in MAR, as can be gathered from their number. The scope of the market abuse provisions of MiCA also differs from MAR. As previously mentioned with regard to the geographical scope of MiCA, the market abuse provisions of the Regulation cover all crypto-assets that have been admitted to trading or for which an application to do so has been made. MAR, on

[155] Recital 95 MiCA Regulation

the other hand, also takes into account the potential impact of assets for which this is not the case.[156] Thus, the scope of the market abuse provisions of MiCA, even in its broadest sense, leaves a gap that may allow for crypto-assets admitted to trading to be manipulated by those not regulated due to the limitation. In addition, MiCA does not provide for criminal sanctions for breaches of its market abuse rules, unlike MAR together with the Directive on Criminal Sanctions for Market abuse 2014/57(EU (Market Abuse Directive, MAD II), leaving the matter to individual Member States to regulate, while also widening the regulatory gap between the markets. Despite these deficiencies, many of the exemptions to the market abuse provisions of MAR were excluded from MiCA, ultimately leading to a generally stricter regime in the crypto-assets market. These omissions, as well as other shortcomings in the market abuse provisions of MiCA, are examined in more detail in the following sections.

The new regulatory framework for market abuse in the crypto-assets market did not sufficiently consider the complexity and specificities of the sector compared to traditional financial markets. In particular, the previously discussed concerns about the broad geographical scope of MiCA and its market abuse provisions could pose problems for market safety and the exercise of enforcement powers in the future. Along with the absence of focus on the global and decentralized nature of the sector, MiCA also failed to address issues such as the significance of the unique opening hours of the crypto-assets market. The competent authorities will not have the same possibilities to monitor a global 24-hour market when compared to a geographically and temporally limited market, which is the case for most of the traditional financial markets.[157] Insufficient and unclear regulation, combined with a lack of a truly crypto-assets market-specific regulatory framework, can ultimately lead to a decline in market integrity. Nonetheless, it should also be noted that the market abuse provisions of MiCA are likely to be assessed and applied in the context of MAR due to their interconnection. However, this in itself does not remedy the inadequacy of MiCA, and such future perspective also raises the question of whether specific market abuse legislation is really necessary for crypto-assets, if it is, due to its shortcomings, to be interpreted in the light of another legislation.

---

[156] See, Recital 10 and Article 2(1)(d) of MAR Regulation

[157] For example, the U.S. Stock Market is primarily open from 9:30 am to 4:00 pm Eastern Time (ET), Monday through Friday. See, Nasdaq Trading Schedule. Other major stock exchanges are, for example London Stock Exchange and Hong Kong Stock Exchange.

As for the potential overlaps between MiCA and MAR, some problems may also arise in the future with regard to the regulation of derivatives. Derivatives are financial contracts that derive their performance from the performance of an underlying asset.[158] Derivatives qualifying as financial instruments, as defined in MiFID II, and whose underlying asset is a crypto-asset, are subject to MAR when traded on a regulated market, multilateral trading facility or organized trading facility.[159] However, crypto-assets falling within the scope of MiCA that are an underlying asset to those derivatives are subject to its market abuse provisions.[160] A distinction can be made on this basis between crypto-assets that serve as an underlying asset for derivatives, and crypto-assets that can potentially be classified as derivatives as such. In relation to the scope of MiCA, the latter group is particularly interesting, and especially with regard to ARTs. As noted earlier in the thesis, the value of ARTs is derived from one or more assets, such as official currencies, crypto-assets or commodities, in a similar way to derivative contracts. ARTs could therefore in principle be considered as crypto-derivatives and fall under the scope of MAR provided that the derivative would fall under one of the categories of derivatives qualifying as financial instruments listed in Annex I Section C, points (4)-(10) of MiFID II. In such derivative contracts as defined in the above provision of MiFID II, the parties exchange cash payments based on the difference between the contract price and market value of the underlying asset.[161] Cash in this context would refer to currency, bearer-negotiable instruments, commodities used as highly liquid stores of value and prepaid cards. Whether assets with similar rights to derivatives, but which would be settled in ARTs, EMTs or other crypto-assets rather than cash, fall under the category of derivatives listed in MiFID II is unclear. Another problem with this approach is that MiFID II is a directive and not a directly applicable EU regulation. Contradictions may arise if the Member States apply either MiCA or MAR on a case-by-case basis, depending on how MIFID II is interpreted.

5.2 Misuse of Inside Information and Insider Dealing

5.2.1 Definition of Inside Information

The definition of inside information is provided in Article 87 of MiCA. With regards to the misuse of inside information, it was noted during the enactment of MiCA that the

[158] Chance 2017, p. 2.
[159] Recital 97 MiCA Regulation.
[160] Ibid.
[161] ESMA 2024a, p. 16.

legal certainty of crypto-assets market participants should be enhanced by defining two elements essential to the specification of inside information, namely the precise nature of that information and its potential impact on crypto-asset prices.[162] Information is considered precise under Article 87(2) of MiCA if it indicates existing or foreseeable set of circumstances or a past or foreseeable event. However, such information has to be specific enough to draw conclusions about the potential impact of that set of circumstances or event on crypto-assets prices. The definition of precise information can also include details of future circumstances or events in relation to a protracted process, as well as intermediate steps of that process. According to Article 87(4) of MiCA, information has a significant effect on the prices of crypto-assets if it is of such a nature that a reasonable holder of the asset would be likely to use it as a part of the basis for investment decisions. Both of these elements should also be considered in preventing market abuse in the context of crypto-assets markets and their functioning, considering, for example, the use of social media, the use of smart contracts for order execution and the concentration of mining pools.[163] For example, concentration of 'mining pools' can be seen as a risk in relation to both insider dealing and market manipulation. Mining pools are collectives of miners who combine computational resources in order to obtain more stable and predictable income.[164] The concentration of mining pools is significant, as miners have a big impact on the functioning of blockchains. The significance of miners, as well as social media and the use of smart contracts for order execution, will be further discussed later in this thesis.

It is provided in Article 87(1)(a) of MiCA that inside information for the purposes of the Regulation consists of precise, not publicly disclosed, information on one or more issuers, offerors or persons seeking admission to trading or on one or more crypto-assets, and which, if made public, would likely have significant effect on the prices of those assets or of the related assets. The provision is very similar to the corresponding provision in Article 7(1)(a) of MAR. However, the MAR definition of inside information is limited to information on issuers and financial instruments, whereas MiCA also includes information on offerors and persons seeking admission to trading. This indicates that the definition of inside information in MiCA is broader than that of MAR. It is added in Article 87(1)(b) of MiCA that in the case of persons executing orders for crypto-assets on behalf

[162] Recital 96 MiCA Regulation.
[163] Ibid.
[164] Tovanich et. al. 2022, p. 1.

of clients, insider information can also mean any precise and significant information provided by a client with regard to pending orders

The relevance of inside information for market abuse reasons at the above scale and for all the entities mentioned is debatable. For example, in traditional financial markets the information on the issuer is of importance as the value of the asset being issued is often linked to the value of its issuer, such as is the case with shares.[165] However, this is not always the case in the crypto-assets market, as the value of stablecoins, for example, is tied to fiat currencies or other assets and possibly secured by the reserve of the issuer. In the case of utility tokens, the issuer plays a more prominent role if, for example, the crypto-asset offers rights to certain future services or the opportunity to participate in the project. With regard to crypto-assets belonging in the third undefined category, it should also be recalled that the issuer, offeror and person seeking admission to trading of such an asset may in principle all be different entities. In such a situation, for the offeror or the person seeking admission to trading of such an asset who is not also the issuer, especially the requirement under Article 88 of MiCA to disclose inside information, to be addressed later in this thesis, may be overly burdensome. In the context of such an offer, where the offeror can only influence the terms of the offer, or an admission to trading, where the price of the crypto-asset is mainly determined by supply and demand, inside information about the offeror itself or the person seeking admission to trading does not appear to have a significant impact on the price of the asset.[166] The same would apply in such a situation to members of management or shareholders of the entity, for example. Nevertheless, it seems that the wording on the scope of MiCA on this issue may oblige offerors and persons seeking admission to trading of such assets to disclose information about their business to the public even after the related activities.

5.2.2 Prohibition on Insider Dealing and Definition of Insiders

The prohibition on insider dealing has been extended to the crypto-assets market in line with the traditional financial markets. In the crypto-assets market, insider dealing can lead to rapid price rises and falls, causing ordinary investors and traders to lose their funds. In comparison to traditional financial markets, insider dealing in crypto-assets mainly occurs in the context of currency launches, listings or delistings at exchanges and can result in

[165] Barsan 2024, p. 14.

[166] Ibid, p. 14.

manipulation of the prices.[167] The employees of these exchanges may profit from such events by opening early trading positions. The prohibition of insider dealing is provided in Article 89(2) of MiCA stating that no person shall engage, or attempt to engage, in insider dealing or use inside information relating to crypto-assets, whether for their own account or for the account of a third party.

Insider dealing is, according to Article 89(1) of MiCA, deemed to occur when a person possesses inside information and uses it by acquiring or disposing, directly or indirectly, of crypto-assets to which that information relates, either for their own account or for the account of a third party. The use of inside information in relation to a crypto-asset by withdrawing or modifying an already placed order or submitting, modifying or withdrawing a bid by a person on their own behalf or on behalf of a third party, is also considered insider dealing under the provision. In line with Article 8(2) of MAR, Article 89(3) of MiCA explicitly prohibits persons in possession of inside information from recommending to another person the acquisition or disposal of such crypto-assets to which the information relates or the cancellation or amendment of an order in respect of those assets. In such situations, insider dealing occurs if the person making the recommendation or inducement knows or should have known that it is based on inside information. In the case of a legal person, the liability for the acts considered as insider dealing is attributed to the natural person responsible.

Definitions of insiders generally distinguish between two categories: primary and secondary insiders.[168] The definition of primary insiders generally includes members of management and the supervisory or administrative bodies of the issuer and is sometimes expanded to include employees, service providers and large shareholders. A secondary insider is someone who receives inside information from someone else, for example due to a special relationship with a person in possession of inside information, also known as a 'tippee', or due to special circumstances, such as overhearing a conversation or accidentally discovering confidential documents.[169] A division between primary and secondary insiders is also incorporated in MiCA. The list of primary insiders is set out in MiCA 89(5) and includes persons possessing inside information by virtue of being members of the administrative, management or supervisory bodies of an issuer, offeror or the person

[167] Rehman et. al. 2020, p. 9.
[168] IOSCO 2003, p. 7.
[169] Ibid, p. 9.

seeking admission to trading of crypto-assets. The list also includes shareholders as primary insiders. In addition, primary insiders are those who have access to inside information through their professional role or its connection to the underlying DLT or similar technologies. The increased access to inside information by those involved in DLT is a unique feature of the crypto-assets market and listing such persons as a primary insider differs from the content of MAR. Lastly, in line with Article 8(4)(d) of MAR, persons who obtain inside information through being involved in criminal activities are listed as primary insiders. Under MiCA, secondary insider is any other person who possesses inside information if that person knows or should have known the nature of the information, although the definition has not been specifically disclosed in the Regulation.

Notable difference between provisions on insider dealing of MiCA and MAR is that MiCA does not include a legitimate behavior clause similar to Article 9 of MAR in relation to both insider dealing and unlawful disclosure of inside information, exempting persons acting in conformity with the rules established. This suggests that the related provisions on the use of inside information set out in MiCA are broader in scope and that activities that would be permitted in traditional financial markets are not necessarily permitted in the crypto-assets market. In addition, the corresponding requirements to draw up a list of insiders under Article 18 of MAR or to disclose managers' transactions under Article 19 of MAR have been completely omitted from MiCA. The omission of these requirements is highly questionable, as they are also intended to enhance the detectability of insider dealing and misuse of inside information. Moreover, given that the legislative approach of MiCA was clearly intended to broaden the scope of misuse of inside information and insider trading compared to traditional financial markets, it is surprising that supervision of such activities has not been facilitated by solutions similar to MAR.

An interesting case in terms of the scope of MiCA and its provisions related to insider trading is that of Nathaniel Chastain, a case pursued in the United States. Chastain was sentenced to three months in prison for committing insider trading in NFTs in 2023.[170] While working at OpenSea, a large NFT marketplace, Chastain was responsible for selecting NFTs to be promoted on the homepage of the company, which constituted confidential information prior to publication due to the price implications of the release. From June to September 2021, Chastain used this confidential business information from

[170] U.S. Department of Justice (DOJ) 2023

OpenSea to buy the NFTs about to be presented right before the launch in order to later sell them at profit. To conceal his actions, Chastain used anonymous digital currencies, such as Ether, and accounts for the purchases and sales on OpenSea. The case of Chastain shows that NFTs are not as harmless as they seem. Despite their varying technical nature, all NFTs can be misused as any other crypto-asset. Therefore, it is also relevant to look at the case from the perspective of MiCA, since the Regulation excludes most NFTs from its scope. The insider trading in the case involved information on several different NFTs to be released for promotion, which all presumably had different characteristics, as most NFTs have unique features. In such a single case of insider trading, it is thus possible that some of the NFTs traded would fall within the scope of MiCA, for example being part of a larger collection or series, but some would not, resulting in different NFTs being subject to different rules. However, with regard to the broad scope of insiders discussed in the previous section, employees who have such information of admission to trading of crypto-assets and who are able to take advantage of such knowledge will always be insiders without exceptions, as the intention to request admission is in itself inside information.[171]

5.2.3 Disclosure of Inside Information

Prohibition on the unlawful disclosure of inside information is laid down in Article 90 of MiCA, while at the same time an obligation to properly disclose inside information to the public is imposed in Article 88 of MiCA. According to Article 90(1) of MiCA, person in possession of inside information must not unlawfully disclose such knowledge to another person, unless acting in the ordinary course of their employment, occupation or duties. As a result, disclosure of inside information is allowed, as long as it is done within the limits of normal responsibilities of employment, occupation or duties. The conditions for unlawful disclosure of inside information are also met under Article 90(3) of MiCA where a person in possession of inside information attempts to influence another person to use it and where the person disclosing the suggestion or inducement knows or should have known that it was based on such information.

Issuers, offerors and persons seeking admission to trading are obligated under Article 88(1) of MiCA to disclose all inside information that directly concerns them to the public as soon as practicable and in a manner that permits prompt access and complete, accurate

[171] Barsan 2024, p. 15.

and timely assessment by the public. Furthermore, it is added that the disclosure of such inside information must not be combined with the marketing of the activities. The obligation further requires issuers, offerors and persons seeking admission to trading to publish and maintain on their website all inside information disclosed to the public for at least five years. Similarly to Article 17 of MAR, issuers, offerors and persons seeking admission to trading may, according to Article 88(2) of MiCA, postpone the disclosure of inside information to the public under their own responsibility provided that all the conditions laid down for doing so in the provision are met. Public disclosure of inside information may be delayed, if an immediate disclosure is likely to prejudice the legitimate interests of the issuers, offerors or persons seeking admission to trading, if such delay of disclosure is not likely to mislead the public and if the confidentiality of the information is ensured.

5.2.4 Prohibition on Misuse of Order Information, and Front-Running

Front-running is a practice in which the service provider who receives a large buy or sell order from a client holds acting on it until after personally executing an order for the same asset for their own account.[172] Later when the request of the client is executed, there is a rise or fall in the price of the asset creating an instant profit for the service provider. Front-running thus refers to, for example, when a service provider, such as a broker, uses the information it receives from a client to its own advantage. Front-running is often used in connection with the terms back-running and sandwich attacks. Back-running is a similar technique to front-running except that the person seeks to have their transaction executed immediately after a pending transaction rather than before it.[173] Sandwich attacks on the other hand refer to the combination of front-running and back-running. Because there is no single party playing the role of a broker in decentralized systems, the opportunity for front-running, back-running and sandwich attacks arises for operators with an advantageous position in the underlying infrastructure, such as CASPs.[174]

In an attempt to prevent front-running, Article 87(1)(b) of MiCA extends the definition of inside information to information of a precise nature relating to the pending orders of the client. However, in the provision, this extension is set out to apply only to persons executing orders for crypto-assets on behalf of clients. Article 78(2) of MiCA also includes a direct requirement for CASPs executing orders to prevent its employees from

[172] Alexander - Cumming 2020, p. 57-58.
[173] TRV Risk Analysis 2023, p. 15.
[174] Daian et. al. 2020, p. 912.

misusing any information relating to client orders. The same obligation is imposed in Article 80(3) of MiCA on CASPs receiving and transmitting orders for crypto-assets on behalf of clients. It is also important to mention that MiCA does not explicitly prohibit the misuse of order information with respect to CASPs other than previously mentioned. For example, CASPs operating trading platforms may come into contact with the same information as CASPs executing, receiving and transmitting client orders. Such a legislative approach may cause problems of interpretation in the future, but it is nevertheless clear that all CASPs are also subject to the general underlying principles and rules of conduct set out in MiCA.

Although MiCA clearly prohibits the misuse of order information falling under the category of inside information as regards the CASPs mentioned, the matter is not entirely unambiguous in relation to public information. Articles 87(1)(b) and 80(3) of MiCA prohibit the same CASPs as previously mentioned from misusing any information relating to pending client orders. However, since this requirement is not limited to the misuse of order data defined as inside information but to any information relating to client orders, it remains unanswered whether certain CASPs are acting in breach of MiCA when using public blockchain data available to everyone. The use of public blockchain data also raises questions at a general level for market participants other than CASPs. For example, it is unclear whether the use of publicly available data can even fall within the definition of insider dealing in relation to individuals, such as members of management, who would otherwise be subject to insider dealing regulation, or whether the activity in question is merely market manipulation.

It is also important to note that front-running based on public market information, such as breaking news, is not only legal, but serves as a basis for a multi-billion dollar high-frequency trading economy, as automated market bots compete to profit from information at extremely high speed.[175] Similar to traditional finance, high-frequency trading bots are constantly scanning the blockchain for arbitrage opportunities and gaining an advantage over retail investors by building faster connections to access the public blockchain data.[176] The success of many of the manipulation techniques typical to the crypto-assets market, such as rug pulls discussed later in this thesis, may be due to the use of these trading

[175] Ibid, p. 912.
[176] Ho - Cazan - Schrumm 2024, p. 33.

bots.[177] Both MiFID II and MAR cover algorithmic and high-frequency trading, and Article 12(2)(c) of MAR, for example, defines algorithmic trading and high-frequency trading strategies as market manipulation if they have negative impact on the functioning of the trading platform or other users.[178] However, MiCA does not offer a similar direct answer, leaving open the question of the legality of the behavior. The 24/7 opening hours of the crypto-assets market and the possibility of anonymity created by decentralized platforms can pose problems in relation to high-frequency trading, as well as the resulting lack of possibilities to intervene in manipulative activities in a market of this nature. In relation to activities covered by MiFID II and MAR, the firm and venue should be able to either stop an algorithm with a kill function or stop overall trading when noticing unusual trading activity.[179] On decentralized exchange platforms, the use of a similar "kill switch" is not possible in a similar way, as they operate on multiple servers without a centralized control layer that would be able to perform this function. However, the possibility of order information being misused in this way indicates precisely to the use of smart contracts for order execution, a concern that the legislators raised as an important aspect of market abuse when drafting MiCA.[180]

Some blockchain technologies are more prone to front-running than others. As a result of such vulnerabilities, even ordinary users can exploit public blockchain data to pursue their own interests. In particular, decentralized applications such as Ethereum are highly vulnerable to front-running due to the 'gas fees', or simply 'gas', required for every transaction.[181] Gas fees refer to the transaction processing fees charged to compensate and incentivize the validators or miners of the blockchain network. Every participant monitoring the 'mempool', which again stands for the list of transactions waiting to be processed by miners or validators and eventually included in a block, can potentially front-run unconfirmed transactions by sending an adaptative transaction with a higher amount of gas.[182] In particular, trading bots are often programmed to read public blockchain data quickly and execute an order before ordinary users. Miners and validators are also able to exploit this feature to manipulate the market and raise higher gas fees. This phenomenon

[177] Cernera et. al 2023, p. 3359.
[178] Article 17 of MiFID II and Article 12(2)(c) of MAR.
[179] Čuk - Van Waeyenberge 2018, Chapter II.2.
[180] Recital 96 MiCA Regulation.
[181] TRV Risk Analysis 2023, p. 15.
[182] Ibid, p. 15.

is as *miner or maximal extractable value* (MEV)[183] and will be discussed in more detail later in the thesis in the context of manipulation techniques specific to the crypto-assets market.

5.3 Prohibition of Market Manipulation

The provisions of market manipulation in MiCA are very similar in substance to Article 12 of MAR but have been adapted to better reflect the crypto-assets market. The prohibition of market manipulation is set out in Article 91(1) of MiCA and states that no person shall engage or attempt to engage in market manipulation. All forms of market manipulation that are directly prohibited by MiCA are listed below, as they will be referred to later when reviewing different examples of market manipulation. Market manipulation within the meaning of the Regulation is defined in Article 91(2)(a) of MiCA as entering into transaction, giving an order to trade or other conduct which gives, or is likely to give, false or misleading signals as to the supply, demand or price of crypto-assets or secures, or is likely to secure, the price of one or more crypto-assets at an abnormal or artificial level, unless carried out for legitimate reasons. The scope or definition of legitimate reasons has not been defined in MiCA, leaving the interpretation unclear. In addition, Article 91(2)(b) of MiCA defines market manipulation as entering into a transaction, placing an order or any other act or conduct that affects or is likely to affect the price of one or more crypto-assets, using a fictional device or any other form of deceit or contrivance. The dissemination of false or misleading information in the media or otherwise about the supply, demand or price of one or more crypto-assets, or which secures or is likely to secure the price of one or more crypto-assets at an abnormal or artificial level, shall also be considered market manipulation under Article 91(2)(c) of MiCA, if the person engaging in such activity knew or should have known the nature of the information.

In addition to the above, according to Article 91(3)(a) of MiCA, market manipulation constitutes securing a dominant position in the supply or demand of crypto-assets that directly or indirectly results, or is likely to result, in the fixing of purchase or sale prices or creates, or is likely to create, other unfair trading conditions. The definition of market manipulation under Article 91(3)(b) of MiCA also includes placing, cancelling and modifying orders on a trading platform with the aim of interfering or delaying the operation of the platform and making it difficult for others to identify genuine orders on the trading

[183] Ibid, p. 15.

platform, including placing orders resulting in the disruption of the normal functioning, giving false or misleading signals about the supply, demand or price of a crypto-asset, in particular by placing orders to initiate or exacerbate a trend, or engaging in any activities likely to have such an effect. In such cases, it is also a condition that the activity or behavior gives or is likely to give false or misleading signals about the supply, demand or price of crypto-assets, or secures or is likely to secure the price of one or more crypto-assets at an abnormal or artificial level. Finally, using the media to manipulate prices by expressing an opinion on a crypto-asset while having previously taken positions on such asset and not having simultaneously disclosed that conflict of interest to the public is considered market manipulation under Article 91(3)(c) of MiCA. This includes the use of both traditional and electronic media as a tool for manipulation.

Although the above-mentioned list of activities considered as manipulative is included in MiCA, it does not contain a list of exempt market practices as in Article 13 of MAR. While MiCA generally excludes all legitimate activities from the definition of market manipulation, no further clarification on what constitutes as legitimate activity is provided. As a result, the scope of market abuse provisions in MiCA is much broader than that of MAR, making it more stringent. In addition, MiCA does not include exemption for buy-back and stabilization programmes as does Article 5 of MAR. Similar to strategies employed in the traditional financial markets, these programmes are used in the crypto-assets market for asset stabilization.[184] The lack of precise definition of legitimate reasons or behaviors increases legal uncertainty and complicates the ability of market participants to engage certain activities that may or may not fall under the definition of market manipulation in MiCA.

5.4 Traditional Types of Market Manipulation

5.4.1 Pump and Dump

The majority of the most common forms of abusive behaviors occurring in traditional financial markets are the same as those found in crypto-assets market.[185] The objective of the following section is to identify and introduce few of the most common forms of market manipulation in the financial sector and the ways in which they occur in the crypto-

[184] Lee - Schu 2025, p. 177.
[185] ESMA 2024d, p. 7.

assets market. The first method of market manipulation to be considered is well-known in traditional finance and is called 'pump and dump'. Pump and dump scheme is an approach which involves an entity accumulating a large amount of a target asset, typically one with low market capitalization and low unit price, and subsequently promoting its purchase as an opportunity for substantial future return.[186] The purpose of the promotional activities is to create significant buying demand, which drives up the price (i.e. the "pump"). As the promotion continues, and while others are still trying to enter, the initial position is completely unwound for a substantial profit, halting the promotion and crashing the price (i.e. the "dump"), often causing significant losses to those slow to react. Pump and dump schemes are a form of market manipulation, which can be performed in a number of different ways. The manipulation carried out with this method generally falls within the prohibitions under Article 91(2) of MiCA but may also be prohibited under inside information provisions of MiCA if the circumstances indicate that such information has been used.

In the crypto-assets market, pump and dump schemes often manifest themselves in a way that is distinct from traditional financial markets. Within crypto-assets market, trading groups are formed on social media platforms where low market capitalization crypto-assets are selected and advertised by administrators.[187] The parties involved in pump and dump schemes often meet each other on social media, for example on WhatsApp, X or Telegram, where misleading information is also spread. False and misleading information is widely used in the crypto-assets market, where rumors and hype have a strong influence, to affect peoples' emotions. There is also no common EU regulatory framework regarding the marketing of crypto-assets, which may contribute to facilitating the spread of misinformation. When MiCA was enacted, the impact of social media in the crypto sector was recognized as a risk factor, and especially in the case of market abuse, was called for to be taken into account.[188] Another distinct feature of a typical crypto-assets market pump and dump scheme is that it takes place in a short period of time, even within minutes.[189] In this case, pump and dump is implemented by members of such trading groups engaging in intensive purchasing, causing the price of the crypto-asset to rise, with

[186] Alexander - Cumming 2020, p. 215.
[187] Ibid, p. 215.
[188] Recital 96 MiCA Regulation
[189] Alexander - Cumming 2020, p. 215.

the members often being aware of what is occurring and in spite of that willing to participate in the belief that they can sell to others at a higher price.

5.4.2 Wash Trading

The next method of market manipulation under examination, also well-known in traditional financial markets, is called wash trading. Wash trading is a manipulation technique based on trades being executed, and it is prohibited under Article 91(2)(a) of MiCA. Wash trades are defined as entering into arrangements for the sale or purchase of a financial instrument where there is no chance of beneficial interest or market risk.[190] This could mean a person trading with themselves or, alternatively, with another party at a pre-agreed deal and price. With wash trading, the aim is to artificially increase the number of executed trades and thus the volume, while misleadingly raising the price of the crypto-asset in question. By amplifying the activity data accessible to other investors, for example by using bots, wash trades can make an asset appear more liquid or valuable than it truly is. In the year 2024, according to a crypto compliance data and services provider Chainalysis, suspected wash trading on selected blockchains Ethereum, BNB and Base could account for up to USD 2.57 billion in trading volume.[191] Even the crypto exchanges themselves may use wash trading as a way to inflate their traded volumes on purpose to attract new users and crypto-asset issuers.[192] However, in the crypto-assets market, compared to traditional financial markets, the main problem in terms of wash trading is the possibility of greater anonymity amongst the operating entities, since the identity of the owners of the accounts from and to which the transactions are made remains unknown.[193] As a result, a single user can easily operate multiple accounts, especially when the creation of accounts is often completely free of charge.

In the United States, the first-ever criminal charges for market manipulation in the crypto sector, which took the form of wash trading and pump and dump schemes, were brought in October 2024. Eighteen different individuals working at four major crypto companies, known as 'market makers', were charged with conducting wash trades to create the impression of high trading activity to attract new investors and raise the price of certain tokens, only to eventually sell the assets and dump the price.[194] Market makers, as the

[190] Ibid, p. 282.
[191] Chainalysis 2025, p. 46.
[192] TRV Risk Analysis 2023, p. 14.
[193] Ibid, p. 14.
[194] U.S. Department of Justice (DOJ) 2024a

name implies, are large entities such as brokers, hedge funds and banks with the large market shares that "create" markets by providing liquidity on both the buy and sell sides and by influencing market price movements.[195] This case shows not only how young the related global case law on crypto-assets market is, but also how widespread and large-scale the abuse has already become. The largest of the companies involved in the market abuse, Saitama, at one point had a multi-billion-dollar market value.[196] In addition, more than USD 25 million in crypto-assets was seized in the case, and several trading bots responsible for millions of dollars' worth of wash trades in around 60 different cryptocurrencies were disabled. The use of bots leveraging smart contracts to influence the price of crypto-assets, which has been highlighted in the context of front-running, is in itself a concerning phenomenon, but even more so when such technologies are used by market makers and crypto-asset providers themselves. Consequently, those wanting to invest in the market need to be particularly careful not only about the types of crypto-assets they choose, but also about their investment plan, so as not to be exposed to price fluctuations that may be deliberately intended to influence investors. The impact of MiCA on the problem remains to be seen, however, as the reality is that a large part of the crypto-assets market, and therefore the major players, are located outside the EU.

5.4.3 Spoofing and Layering

Spoofing is a method of market manipulation that occurs when an entity tricks the market into thinking that there is more demand to buy or sell a particular financial product that is truly the case.[197] This can occur by placing orders for a large number of the same product with no intention of having the orders filled. Therefore, spoofing is manipulation based on placing orders with the intention of driving up the price and finally allowing the original entity to cancel the orders placed and dispose of the holding at a higher price than would otherwise be possible. This also gives the public the impression of a highly liquid and healthy market. Layering is also a market manipulation technique very familiar to traditional financial markets and is considered to be a form of spoofing. Layering is the process of placing large orders on one side of an electronic order book, which are lists of current orders, often at prices unlikely to attract counter-orders, but which move the price according to supply and demand, without any real intention of executing the orders.[198]

---

[195] Noertjahyana et. al. 2020, p. 2.
[196] U.S. Department of Justice (DOJ) 2024a
[197] Durston - McKeon 2020, p. 36.
[198] Ibid, p. 36.

This is then followed by the execution of a usually much smaller trade on the opposite side of the order book taking advantage of the movement and by the cancellation of the large initial order. Spoofing and layering are both prohibited under Article 91(2) of MiCA. Although the literature investigating spoofing occurring in any financial markets is relatively scarce, it has been found that many of the financial assets targeted share certain common attributes, such as higher return volatility, lower market capitalizations, and lower price levels.[199] All of these features are very common amongst crypto-assets, making them more likely to be subject to spoofing.

5.4.4 Stop-Loss Hunting and Whale Techniques

Stop-loss and take-profit are orders commonly placed by clients in the foreign exchange market (Forex, FX), instructing the bank to buy or sell a specific amount of currency at a specific price.[200] Stop-loss and take profit-orders can be left in place for a longer period of time, for example overnight or until cancellation, allowing the client to relax in the knowledge that any loss is limited or profit is guaranteed should the market reach a certain level. These orders can also be used to monitor the market. Order books of exchanges can provide valuable information about the balance between supply and demand in the market, as well as indications in relation to the sensitivity of the market to specific prices.[201] Stop-loss hunting or stop hunting occurs when market makers or crypto 'whales' push market prices to touch a certain price level with the aim of triggering the highest number of stop-losses from ordinary traders.[202] After reaching a level flooded with stop-losses, the market price usually reverses quickly, resulting in ordinary traders reacting too late to price movements.

Crypto whales and market makers are both terms used to describe major players in the crypto-assets market with huge amounts of wealth, although they are not exactly synonymous. Whales differ from market makers in the sense that not all crypto whales are market makers. Whales are large investors seeking to monetize the market, for example, by creating supply shortage of certain crypto-assets by holding them for long periods of time and by causing large price fluctuations and volatility in the market.[203] As for stop-

[199] Alexander - Cumming 2020, p. 21.
[200] Ibid, p. 190.
[201] Ibid, p. 190.
[202] Noertjahyana et. al. 2020, p. 2.
[203] Chernoff - Jagtiani 2024, p. 2.

loss hunting in the crypto-assets market, crypto whales holding huge amounts of a particular cryptocurrency artificially increase liquidity by selling massive amounts of their holdings, thus creating a spiral of sell orders that allows them to eventually buy the asset back at lower price. In addition to stop-loss hunting, whales may also use other techniques, such as spoofing and pump and dump schemes, to manipulate the market to their advantage by artificially creating volatility and asset price fluctuation. Naturally, the mere fact that a market participant sells or buys a large amount of crypto-assets does not directly make the activity market manipulation. However, if the apparent purpose of the activity is price manipulation, such whale techniques are prohibited under MiCA.

5.4.5 DDoS Attacks

A distributed denial-of-service (DDoS) attack refers to an illegal attempt to disable the service provided by a website or network by repeatedly sending a high volume of service requests.[204] The attacks are organized by a linked collection of "zombie computers", known as a Botnet, which is remotely controlled by an underlying attacker.[205] Often the individual zombies, or Bots, are malware-infected machines whose owners are completely unaware of their participation in an attack. Typical targets of DDoS attacks include the servers of e-commerce or news websites, banks and government websites. DDoS attacks in traditional financial and crypto-assets markets are very similar, although the attacks against the latter may be motivated by different reasons. DDoS attacks may be motivated, for example, by the fact that attacks on currency exchanges have the potential to be economically profitable for the perpetrators, while preventing others from buying or selling creates an unfair financial advantage for the attacker at the expense of ordinary participants.[206] The general form of the strategy used in cryptocurrency markets can be divided into three phases: initial sell order, sustained DDoS attack and position accumulation.[207] First, the attacker places a large sell order on the exchange right before the DDoS attack commences. Next, the attacker launches the DDoS attack that prevents others from participating in new trading. During the attack, the large sell order is filled, creating downward pressure as buying volume decreases. In the absence of new buy orders, the price continues to fall to fill the large sell order, causing a further downward spiral as stop-loss positions begin to trigger. Eventually, the attacker stops the DDoS attack and is able to

[204] Eigelshoven - Ullrich - Parry 2021, p. 10.
[205] Alexander - Cumming 2020, p. 220.
[206] Feder et. al. 2017, p. 137.
[207] Alexander - Cumming 2020, p. 221.

buy a large position at a low price. In the light of the above, it is thus clear that DDoS attacks can be a very lucrative technique of market manipulation.

In the crypto-assets market, strong anonymity allows DDoS attacks to be carried out more easily.[208] Another factor that can expose systems to attacks is their lack of security and sophistication of the technologies. However, the requirements imposed by MiCA regarding the maintenance of protective systems and mechanisms for CASPs operating in the EU have improved this aspect. Even so, it is alarming that, for example, the European Union Agency for Cybersecurity (ENISA), has recently published research in stating that DDoS attacks are the biggest cyber threat affecting the EU in 2025, accounting for up to 46% of all threats detected during the monitoring period.[209] Within the crypto-assets market, DDoS attacks can target the blockchain network itself or the exchange platforms on which crypto-assets are traded. DDoS attacks against blockchain networks can cause delays in transactions and increase gas fees as users race to get their payments through. For example, on 14 September 2021, the Solana network was down for 17 hours due to a denial-of-service attack.[210] During the attack, bots were creating transactions which flooded the network and caused many validators to crash forcing the network to slow down and eventually stall. In addition, attackers may manipulate the market as described above, or even blackmail the service provider to cease the attack. When exchange platforms are targeted by DDoS attacks, users may be prevented from executing transactions and accessing their funds. Such scenarios decrease users' trust in service providers and market integrity.

5.5 Manipulative Activities Specific to the Crypto-Assets Market

5.5.1 Rug Pull Schemes and AMM Protocols

As noted before, the manipulation techniques occurring in crypto-assets market are in many ways very similar to those used in traditional financial markets. Although the ways of manipulation are very much alike, crypto-assets market is also characterized by its own unique techniques. 'Rug pulling' is one such relatively new method of manipulation. Rug pull schemes belong to the group of exit scams, i.e. scams in which the project developers abandon the project and run away with investors' funds, but which take place in DeFi

[208] Ibid, p. 221.
[209] ENISA 2025, p. 10. (Figure 5.)
[210] Solana Foundation 2021.

solutions instead of real life and often relate to new crypto projects.[211] As for the crypto-assets market and its rapid growth, the emergence of DeFi prompted investors to transition from more controlled centralized exchanges (CEXs), such as Coinbase, to decentralized exchanges (DEXs). DEXs are decentralized applications (dApps) for trading that run on-chain powered by smart contracts without the involvement of third parties.[212]

In DEXs, the fully decentralized nature of activities allows for anonymity and a higher level of security, but also for low costs for users and almost non-existent oversight. DEXs are ideally suited for rug pulls as the *automated market maker* (AMM) protocols often used in such exchanges allow new trading pairs to be created and traded by other users, while in CEXs the platform creates the pairs.[213] Rather than matching the buy and sell sides, as in traditional order-book-based exchanges, AMMs use a *peer-to-pool* method where a digital pool of assets, known as a 'liquidity pool', contributed by liquidity providers acts as a single counterparty for each transaction.[214] As a result, users have access to immediate liquidity without having to find a counterparty, whereas liquidity providers profit from the supply of assets through exchange fees charged to users. In peer-to-pool method, the price of an asset is determined algorithmically through a so-called 'conservation function', allowing the price to move only along predefined trajectories.[215]

In the crypto-assets market, rug pull schemes can be implemented, for example, by creating one or more new tokens with no intrinsic value and enticing other users of the DEX to exchange it for another valuable crypto-asset. One method is to create a coin with the same name as an existing one to attract attention and to trick users into accidentally buying the wrong crypto-asset.[216] The scammers may also reach out to several prominent people who create false hype around the project to attract other potential buyers and raise the price of the token. In such cases, the "rugged" buyers are often unable to later swap the scam token back for another crypto-asset with value. Attackers may also use wash trading to attract more investors.[217] In such cases, the creator of the pool of scam tokens tries to create the impression that the liquidity pool is active, by faking the trading volume by repeatedly buying and selling tokens. Rug pulls are a very recent problem, but a big

[211] Agarwal et. al. 2023, p 1.
[212] Cernera et. al 2023, p. 3349.
[213] Ibid, p. 3349.
[214] Xu et. al. 2022, p. 1.
[215] Ibid, p. 1.
[216] Ibid, p. 21.
[217] Cernera et. al 2023, p. 3355.

one. DeFi protocols have seen USD 211.9 million stolen via scam and rug pull schemes, with at least 20 instances of scams mainly consisting of rug pulls, between 2020 and October 2024.[218] In the case of meme tokens, which are crypto-assets that combine internet memes, trends or other humorous characteristics and investments, 62 % of the investors have become victims of rug pull scams.[219] Provisions on issuers of crypto-assets in MiCA are particularly relevant in limiting the opportunities for rug pull schemes. Requirements for issuers of crypto-assets laid down in MiCA, such as legal form, publication of the crypto-asset white paper and marketing communications, combined with other operational requirements, could assist in preventing rug pull schemes in the future, as just anyone can no longer issue tokens. However, as has been highlighted in this thesis, it is also possible to circumvent these requirements, as well as the provisions of MiCA on market abuse.

5.5.2 Flash Loan and Oracle Attacks

Flash loans, where the term 'flash' refers to the rapid execution speed of the transactions, are uncollateralized loans where both the borrowing and repayment happen in one single block on the blockchain.[220] The *atomicity* of blockchains, a feature that allows multiple transactions to be processed collectively in a single block or alternatively fail collectively, allows flash loans to be uncollateralized and at the same time protects the lender.[221] These types of loans provide DeFi users the opportunity to access crypto-assets without collateral, potentially in connection with complex trading strategies, such as arbitrage, collateral swaps, or refinancing.[222] This allows users to benefit from temporary price differences between DeFi protocols or to restructure positions in a single transaction. However, according to a recent report published by EBA and ESMA on the developments in crypto-assets, flash loans have also consistently been used as a source for various hacks and attacks against DeFi protocols.[223] As with other manipulation techniques specific to the crypto-assets market, the use of flash loans for this purpose is easy due to their accessibility, poor traceability and lack of cost. The report indicated that approximately 20 % of value theft occurring in DeFi include the use of flash loan attacks, with the primary type of attack being smart contract exploitation. Smart contract exploitation includes using,

[218] EBA and ESMA Joint Report 2025, p. 22.
[219] Li et. al. 2023, p. 18.
[220] TRV Risk Analysis 2023, p. 7.
[221] Ibid, p. 7.
[222] EBA and ESMA Joint Report 2025, p. 69.
[223] Ibid, p. 69.

for example, reentrancy techniques, exploitation of diverse math, logic errors related to swaps, incentive rewards or donation functions. This type of manipulation aims to shift supply and demand in the market, often for less liquid crypto-assets.

According to the report, the second most common attacks exploiting flash loans are mainly carried out through price manipulation, in particular by exploiting price information provided by oracles.[224] Oracles are used to allow smart contracts to access relevant external or off-chain data through queries.[225] The role of oracles is therefore to bring external information, such as information on asset prices, into the blockchain to be incorporated into the DeFi transaction flow, thus enabling the execution of smart contracts. There are four main types of oracles: price, event, randomness and cross-chain oracles.[226] Price oracles are used to feed real-time information of all types of assets into smart contracts, while event oracles provide information on real-world events, randomness oracles provide a source of randomness to lottery or gaming systems, and cross-chain oracles facilitate data transfer. The nature of external data extraction means that oracles are also vulnerable to manipulation of their data sources, as well as technological problems with regard to the smooth flow of information and possible system crashes.

One example of the combination of flash loans and oracle manipulation to perform price manipulation in the crypto-assets market is the case of Mango Markets, a decentralized crypto exchange. The perpetrator Avraham Eisenberg was convicted for engaging in a scheme to fraudulently obtain approximately USD 110 million worth of cryptocurrency from Mango Markets and its customers by artificially manipulating the price of certain perpetual futures contracts.[227] Perpetual futures are innovative products introduced with DeFi that, unlike traditional futures, have no expiry date.[228] This allows perpetual futures to be held indefinitely without the need to roll over contracts as they approach expiration. In the case, Eisenberg using different accounts on Mango Markets, sold and bought perpetual future contracts on approximately 488 million MNGO tokens, and later executed a series of large purchases of the low-traded tokens at progressively higher prices, artificially increasing their price on exchanges using price oracles.[229] The large increase in the

[224] EBA and ESMA Joint Report 2025, p. 69.
[225] TRV Risk Analysis 2023, p. 7.
[226] Ibid, p. 68.
[227] See, U.S. Department of Justice (DOJ) 2024b
[228] TRV Risk Analysis 2023, p. 7.
[229] The U.S. Securities and Exchange Commission (SEC) 2023

value of the holding allowed Eisenberg to use the virtually worthless position as collateral to borrow and eventually raise over a hundred million dollars in crypto-assets. Once Eisenberg stopped manipulating the price of the MNGO token, a significant decline in the prices of MNGO and MNGO perpetual futures subsequently occurred. From the perspective of crypto-assets market in the EU, the case is interesting as MiCA does not regulate lending or borrowing of crypto-assets. Thus, flash loan attacks may not fall within the scope of MiCA, but it will be interesting to see what the future application will be in situations where oracle and loan manipulation techniques are combined.

5.5.3 MEV Extraction

Miners and validators were previously discussed in the context of consensus mechanisms and insider trading. Both of these entities are an integral part of DeFi and hold considerable power over the composition of blockchains. As mentioned earlier in the thesis, MEV refers to the maximum value that miners, or validators in some blockchains, are able to obtain by manipulating transactions. The nature of blockchains allows for decentralized and competitive processing of transactions. Users of blockchains are able to accelerate and influence the place of their transactions in the processing queue by increasing the amount of gas fees they are willing to pay. These gas fees are paid to miners and validators as compensation for the work they do. MEV extraction is based in the fact that in most blockchains there are no restrictions on the exact order of transactions within a block.[230] The technique has existed since the emergence of blockchains but became popular in 2020 with the growth of DeFi and the development of trading bots designed to exploit the inefficiencies of DEX protocols. The benefits of MEV extraction include facilitating price discovery, creating more efficient markets across centralized and DEX platforms, as well as enabling arbitrage, and faster transaction execution.[231]

Given that miners and validators have the discretion to include or exclude transactions from blocks, it has been observed that MEV extraction can also be abused by prioritizing transactions at the expense of other users.[232] Crypto-assets market participants seeking to profit from MEV extraction are sometimes just individuals using a single algorithm or trading bot, but who can accumulate substantial profits in a short period of time.[233] For

[230] EBA and ESMA Joint Report 2025, p. 27.
[231] ESMA 2024d, p. 9.
[232] Xu et. al. 2022, p. 19.
[233] EBA and ESMA Joint Report 2025, p. 32.

example, in 2023, a bot used to exploit MEV extraction made millions in proceeds in just three months through arbitrage and sandwich attacks.[234] Such bots are similar to trading bots used in front-running, efficiently analyzing mempool data and implementing targeted strategies to maximize profits from MEV extraction by offering miners and validators higher gas fees. MEV extraction bots may use legitimate methods, such as arbitrage or front-running based on public blockchain information, but they can also be used illegally to manipulate prices of crypto-assets. MEV bots and arbitragers can also share characteristics with wash trading, as they buy and sell the same token pairs in very short time intervals.[235] However, this activity is typically not aimed at increasing volume, but rather than at exploiting arbitrage opportunities.

MiCA does not explicitly mention or prohibit MEV extraction or the use of MEV bots. In its consultation paper on the prevention and detection of market abuse, ESMA initially proposed that MEV extraction should be considered as market abuse, and stated that the activity would fall under the reporting obligation of persons professionally arranging or executing transactions, which is discussed next in this thesis.[236] However, after receiving responses to the consultation, and when a significant number of respondents were of the opinion that miners and validators should be excluded from this obligation, ESMA also accepted this approach.[237] ESMA also added that miners and validators would still be held liable if they act in breach of market abuse provisions of MiCA. The rationale of for excluding miners and validators from the reporting obligation was, for example, that such an approach might encourage such entities to leave or avoid establishing in the EU, complicating the supervision of EU CASPs as they might outsource services to these entities and push innovation abroad. Fourteen respondents had also objected to the mechanical presumption of MEV extraction activities as market abuse proposed in the consultation paper, since its primary purpose is to compensate good actors for the work performed.[238] These respondents argued that whilst some types of MEV extraction activities are inherently abusive, such as sandwich attacks or using inside information from private mempools, other types are a legitimate practice that facilitate arbitrage between decentralized exchanges or identify opportunities to realize DeFi positions. EBA and ESMA have acknowledged that MEV extraction activities are widespread in DeFi, and therefore the

[234] Copeland 2023.
[235] Chainalysis 2025, p. 40.
[236] ESMA 2023b, p. 10, paragraph 19.
[237] ESMA 2024d, p. 11-12.
[238] Ibid, p. 34.

negative externalities need to be further examined.[239] It is likely that cases related to MEV extraction will be examined on a case-by-case basis in the future, but if abuses occur, EBA and ESMA may change their approach.

5.6 Prevention and Detection of Market Abuse

Persons professionally arranging or executing transactions (PPAETs) are required by Article 92 of MiCA to put in place effective arrangements, systems and procedures to prevent and detect market abuse. PPAETs are then obliged to report to the competent authority, without delay, any reasonable suspicion or risk of possible market abuse. The competent authorities receiving a suspicious transaction or order report (STOR) are responsible for transmitting such information to the competent authorities of the possible trading platforms concerned. The definition for PPAETs is not provided in MiCA but can be found in MAR. Article 3(1)(28) of MAR defines PPAETs as persons professionally engaged in the reception and transmission of orders for, or in the execution of transactions in, financial instruments, in line with the purposes of traditional financial markets. However, MiCA contains no reference to this article of MAR, leaving the definition of PPAETs in the crypto-assets market completely unspecified. ESMA has defined STOR as the report on suspicious orders or transactions, including any cancellation or modification thereof, and other aspects of the functioning of the DLT where circumstances might exist indicating that market abuse has been committed, is being committed or is likely to be committed.[240] STOR is only intended to report orders, transactions and other DLT-related matters and should not be used in relation to other types of fraud such as scams, payment fraud or account takeover that not do not have an identifiable link to market abuse.[241] Article 16 of MAR on prevention and detection of market abuse in traditional financial markets was used as a basis for Article 92 in MiCA, and the provisions share many common features.

ESMA was given a mandate in Article 92(2) of MiCA to develop draft regulatory technical standards (RTS) to further specify the details concerning the measures to be taken under the above-mentioned provision. In December 2024, ESMA issued its draft RTS specifying certain requirements in relation to the detection and prevention of market

[239] EBA and ESMA Joint Report 2025, p. 2.
[240] ESMA 2024d, p. 54.
[241] Ibid, p. 7.

abuse under MiCA. As the scope of PPAETs is not defined in MiCA, ESMA briefly addressed the matter in the report submitted with the draft RTS. According to ESMA, the definition of PPAETs for the purpose of Article 92 of MiCA covers CASPs that operate a trading platform or provide services related to crypto-assets, such as receiving or transmitting orders on behalf of clients, portfolio management and the exchange of crypto-assets for funds or other crypto-assets.[242] Furthermore, the definition of PPAETS also covers persons dealing on their own account in crypto-assets on a professional basis or as a part of their business activity. ESMA stated in its final report on the draft RTS that a person having a staff or structure dedicated to systematic trading on their own account, such as a trading desk, indicates that the person falls within the definition of a PPAET.[243] Despite this analysis, ESMA concluded that the definition of PPAETs should not be specified in the RTS in order to maintain a broad scope and to allow for supervisory experience to be used to further define the category in the future.[244] Therefore, it is still unclear at present who is responsible for monitoring and preventing market abuse.

As regards the requirement for PPAETs to put in place effective arrangements, systems and procedures to prevent and detect market abuse, ESMA expressed its views on the level, quality and methods required in its final report accompanying the draft RTS. The draft requires PPAETs to establish arrangements, systems and procedures that ensure an effective and ongoing monitoring of transactions, orders, and other aspects related to the DLT and allow for the reporting of STORs to the relevant competent authority.[245] ESMA stressed that the systems, arrangements and procedures developed should be proportionate and appropriate to comply with the STOR regime, taking into account the size, nature and scale of the business conducted by PPAETs, and updated regularly. The draft RTS also establish certain required technical capabilities for the operation of PPAETs, including a software capable of preventing market abuse in real-time and operating in an algorithmic trading environment.[246] However, one of the key elements set out in the draft RTS to prevent market abuse is the requirement for a certain level of human interaction. While

[242] Ibid, p. 6.
[243] Ibid, p. 6.
[244] Ibid, p. 13.
[245] Ibid, p. 7.
[246] Ibid, p. 8.

the software may be able to prevent market abuse in real time, an appropriate level of human analysis is always required to further ensure market safety.[247]

As for the extent of these systems, arrangements and procedures, the full range of trading activities undertaken by PPAETs should be covered and the monitoring of every transaction and order should be enabled, whether occurring on or off of a trading venue.[248] ESMA complemented the latter requirement by specifying that the monitoring should encompass off-chain transactions, such as transactions between a crypto-assets trading platform and its users, as this is where most of the trading takes place.[249] As regards on-chain transactions, PPAETs should monitor on-chain transactions falling under their business activity but not beyond that. Such situation arises, for example, where a PPAET is directly involved in the on-chain transaction, for instance as a sender or recipient. Partial outsourcing of the mechanisms required by the draft RTS is allowed for PPAETs, as long as the responsibility for preventing market abuse remains with the operating entities.

ESMA was also given a mandate under Article 92(3) of MiCA to issue guidelines on supervisory practices for competent authorities to prevent and detect market abuse before the end of June 2025, if not already addressed in the RTS. ESMA issued its final report on the topic on 29 April 2025 and called on competent authorities to develop and maintain a good understanding of, and a risk-based forward-looking approach on the risks posed by CASPs and issuers directly supervised, as well as other persons, such as traders, miners and relevant persons active on social media, whose activities may constitute market abuse.[250] In this context, ESMA refers in particular to acts such as order book manipulation, MEV extraction and dissemination of false or misleading information. Competent authorities were also encouraged to include in their supervisory activities manipulative practices that stem from the specific technology behind blockchains or the ways in which crypto-assets are offered or evaluated.[251] For the latter, ESMA mentioned, as an example, the manipulation of the supply of tokens, likely referring to activities such as the promotion of new crypto-assets for the purposes of pump and dump schemes or rug pulls, and, in relation to stablecoins, in particular ARTs, the assessment of the backing assets. In

[247] Ibid, p. 8.
[248] Ibid, p. 8.
[249] Ibid, p. 15.
[250] ESMA 2025b, p. 15.
[251] Ibid, p. 16.

addition, competent authorities were urged to monitor social media to cover risky information posted on crypto-assets, and to take into account the persons in possession of inside information, in particular employees of CASPs aware of the decision to list a new token, or miners and validators who engage in front-running or influence the flow of validated transactions.[252]

[252] Ibid, p. 16.

6 Concluding Remarks

Answer to the First Research Question

MiCA seeks to improve market integrity and investor protection by imposing regulatory obligations on market participants to prevent market abuse in the crypto-asset sector. However, while the efforts to regulate the crypto-asset market participants in terms of market abuse are evident, many of the provisions concerning market abuse in MiCA are either ambiguous, overbroad or insufficient. In line with the objective, MiCA introduces a framework for the issuance, offering, and admission to trading of crypto-assets, and establishes authorization and conduct requirements for CASPs. Specifically, MiCA imposes differentiated obligations based on the classification of the crypto-assets. Issuers of EMTs and ARTs are subject to more stringent regulation, including mandatory authorization, transparency, and disclosure requirements. Certain CASPs, such as those operating trading platforms, are further subject to specific obligations laid down in MiCA aimed at detecting and preventing market abuse, including, inter alia, robust trading systems, transparent fee structures, and mandatory reporting. While MiCA establishes a general obligation in Article 92 of MiCA for persons professionally arranging or executing transactions to prevent and detect market abuse, the ambiguity surrounding the personal and material scope of these obligations, particularly for persons not expressly included within the regulated entities, undermines their practical enforceability.

In general, when examining the regulatory solutions made regarding the market participants, seems that the legislators lacked a thorough understanding of the functioning of the crypto-assets market and what kind of behavior is common in practice. Furthermore, MiCA did not really succeed in achieving its objective of facilitating the operation of small and medium-sized enterprises by establishing tailored, market-specific rules on abuse within the crypto-asset sector either. The scope of market abuse provisions of MiCA has been extended in the absence of explicit exemptions or definitions of legitimate market behavior, thereby introducing legal uncertainty. In addition, MiCA extends the concept of insider trading and the misuse of inside information beyond the parameters established under MAR but fails to provide supervisory authorities with corresponding enforcement tools. The lack of precise definitions and supervisory mechanisms impedes effective implementation and enforcement, particularly in cross-border contexts involving third-country entities operating under reverse solicitation. The regulatory gaps in the

regulation concerning market participants are particularly challenging for entities that are already active in traditional financial markets and are now seeking to enter the crypto-assets space, as activities that are either clearly permitted or prohibited under MAR are often ambiguous under MiCA, creating confusion and risk. Despite these shortcomings, both ESMA and EBA will continue to monitor market developments and provide further guidance. However, while such guidance is beneficial, it does not remove the general problematic nature of MiCA.

Answer to the Second Research Question

The current regulatory framework established by MiCA proves inadequate when assessed against the unique features and abusive practices that exist in the crypto-asset sector. While MiCA purports to provide a comprehensive framework for market abuse in the crypto-assets market, its substantive provisions often fall short due to being overly broad, excessively vague, or insufficiently responsive to specific risk factors inherent in the market. The legislative intent behind MiCA appears to have been driven by the inherent tension between preventing market abuse and preserving room for innovation. This conflict manifests in a framework that lacks clear provisions in a number of critical areas, such as the impact of social media, the exploitation of smart contracts for manipulative order execution, and the concentration of power within mining pools, each of which presents demonstrable risks. MiCA does not give specific rules on regulating such matters, even though their impact was recognized by the legislators. Furthermore, the exclusion of miners and validators from the direct regulatory scope of MiCA represents a significant oversight, particularly in the context of practices such as MEV extraction and high-frequency trading facilitated through automated trading bots. The absence of definitions or tailored obligations for such strategies leave substantial regulatory gaps, especially when such techniques can amplify volatility or distort price formation. This omission is further exacerbated by the global and decentralized nature of the crypto-asset market, where a significant portion of activity originates outside the EU, thereby reducing the practical reach of the enforcement mechanisms of MiCA.

The challenges posed by DeFi infrastructures, including AMMs, DEXs, and self-hosted or non-custodial wallets, highlight the limits of the regulatory scope of MiCA. While the Regulation imposes certain obligations on centralized CASPs, it excludes most decentral-

ized technologies from its scope, thereby allowing for continued anonymity, lack of oversight, and exposure to abuse techniques such as rug pulls or wash trading. The DLT Pilot Regime may offer an insight on the legislation of such novel technologies, but until a comprehensive regulatory approach is adopted for DeFi, the ability of MiCA to address abuse remains fundamentally constrained. In addition, MiCA does not resolve critical questions of liability in decentralized environments. Where code errors in autonomous systems lead to investor loss without any malicious intent behind the activity, the Regulation provides no clear redress or apportionment of liability, leaving a gap that undermines investor protection. Given the limited added value of MiCA compared to MAR, and in particular the failure to take into account the 24-hour trading and global reach of crypto-assets market, a more nuanced and robust framework is required.

Lastly, and despite all these shortcomings, MiCA represents an important foundational effort in regulating crypto-assets. While there is no one big problem with MiCA, and the Regulation has achieved many of its objectives, the accumulation of smaller gaps and shortcomings takes away from the relevance of its provisions and makes it difficult for those in the market to operate. All these flaws also render the Regulation inadequate for the full prevention of market abuse in the crypto-assets market. However, allowing the monitoring of the progress of developing markets is important and in the case of MiCA, the challenging market conditions will increase the level of commitment required from legislators. It is still debatable whether it was necessary to enact such a flawed framework only to allow the EU to be the first player to regulate the market more comprehensively, or whether it would have been more sensible to extend the provisions of MAR to crypto-assets while a high-quality legislation on the market is being developed. Nevertheless, it is possible, that issues now fully or partially excluded from the scope of the Regulation, such as DeFi protocols, lending and borrowing of crypto-assets, miners and validators, self-hosted and non-custodial wallets, as well as NFTs may be fully addressed in the near future in a possible MiCA II Regulation.