Compliance, ethics & sustainability

An international journal with a European focus

JAARGANG 25 - SEPTEMBER 2025 4

Paulien Makkinga, Pauline Wijma, Peter-Jan Engelen and Arend Koper
Editorial

Peter Engering, Leon Kort, Paulien Kraaijeveld and Yorrick Zaat
From inadequate oversight to effective regulation?

Nikolai de Koning and Julia van der Grint
Enforcement under MiCAR – Challenges and uncertainties

Meredith Fitzpatrick, Thomas Hyun and Loretta Rice
The Only Constant is Change: State of Crypto Regulations Across the Globe

Jeroen Boogaard
'Met de digitale euro kan Europa onafhankelijk blijven'

Dominik Lynen
Banking crypto clients: better monitoring through adoption

Delaney Diederik
Choice Architecture and Financial Health on Crypto-Asset Service Platforms
Assessing the Effectiveness of EU Regulation in Protecting Investors

Edgar Karssing
Uit de boekenkast van de bedrijfsethiek (95)

DEN HOLLANDER

Uitgeverij Den Hollander BV
Postbus 325 7400 AH Deventer
tel.: 0570 - 751 225
e-mail: info@denhollander.info
www.uitgeverijdenhollander.nl

Abonnementsprijs
Zie:https://denhollander.info/

Nieuwe abonnementen
Abonnementen kunnen via onze website worden afgesloten en gaan in op een door u gekozen datum. De looptijd bedraagt 12 maanden.
Wanneer de ingangsdatum niet aansluit op een reeds lopend abonnement bij Den Hollander, wordt het nieuwe abonnement gekoppeld aan de looptijd van het bestaande abonnement. In dat geval wordt het tarief voor de resterende periode van het lopende jaar naar rato berekend, op voorwaarde dat het abonnement ook voor het volgende jaar wordt voortgezet.
Op alle abonnementen zijn onze algemene voorwaarden van toepassing.

Beëindiging abonnement
Opzegging van abonnementen kan uitsluitend via uw account en dient uiterlijk één maand vóór het einde van het lopende abonnementsjaar te gebeuren.
Bij te late opzegging wordt het abonnement automatisch met één jaar verlengd.

Adreswijziging
Adreswijzigingen dienen zo snel mogelijk te worden doorgevoerd in uw account via onze website.

Citeerwijze
CE&S 2025, nr. 4

DEN HOLLANDER
UITGEVERIJ

COMPLIANCE, ETHICS & SUSTAINABILITY

Journal

JAARGANG 25 - SEPTEMBER 2025 - NUMMER 4

123 *mr. drs. P. Makkinga, P. Wijma MSc, prof. mr. dr. P.J. Engelen and A. Koper LLM*
Editorial

124 *P. Engering, L. Kort, P. Kraaijeveld and mr. Y.B.A. Zaat*
From inadequate oversight to effective regulation?

133 *mr. N. de Koning and mr. drs. J.J. van der Grint*
Enforcement under MiCAR – Challenges and uncertainties

140 *M.M. Fitzpatrick, T. Hyun and L. Rice*
The Only Constant is Change: State of Crypto Regulations Across the Globe

148 *J. Boogaard*
'Met de digitale euro kan Europa onafhankelijk blijven'

151 *D. Lynen*
Banking crypto clients: better monitoring through adoption

158 *D.M. Diederik LL.M.*
Choice Architecture and Financial Health on Crypto-Asset Service Platforms
Assessing the Effectiveness of EU Regulation in Protecting Investors

166 *prof. dr. E. Karssing*
Uit de boekenkast van de bedrijfsethiek (95)

Editorial

mr. drs. P. Makkinga, P. Wijma MSc, prof. mr. dr. P.J. Engelen and A. Koper LLM

In 2022, the CE&S Journal published a widely-read edition on Virtual Assets. The fourth edition of 2025 provides an update on some of the topics covered in 2022. Furthermore, this edition also investigates new regulatory requirements and marketing practices, as virtual assets continue to be a hot topic, particularly with the rapid development of stablecoins this year. The hegemony of dollar-denominated stablecoins remains strong and will be given a new impetus by the recently adopted GENIUS Act in the US. However, alternatives are being developed by a multitude of mature financial institutions, encouraged by the regulatory clarity provided by the EU's Markets in Crypto-Assets Regulation (MiCAR). This new regulation introduced MiFID-II-like rules for Crypto Asset Service Providers (CASPs), the implementation of which will be subject to regulatory scrutiny. We are delighted that various legal and compliance experts in the field of virtual assets have contributed their thoughts and insights to this edition.

The article that *Peter Engering* en *Leon Kort* published in 2022 on the regulatory oversight of crypto assets was one of the most popular. In this edition, both authors, together with *Paulien Kraaijeveld* and *Yorrick Zaat*, provide an equally informative update on some of the regulatory developments since 2022. The article also describes the remaining challenges and risks, and provides recommendations for moving forward.

Zooming in on the application of MiCAR, *Nikolai de Koning* and *Julia van der Grint*'s article examines how the law has been implemented in the Netherlands, including the transfer of authority from the DNB to the AFM. Providing a crucial examination of MiCAR's enforcement, the article goes beyond the text of the law to explore how its credibility and the level of trust it commands from market participants will be determined by its real-world application.

In the article “The Only Constant is Change: State of Crypto Regulations Across the Globe” by *Meredith Fitzpatrick, Thomas Hyun*, and *Loretta Rice* focus on five jurisdictions that are embracing regulatory postures on cryptocurrency in pursuit of becoming the dominant hub for institutional cryptocurrency adoption. Is this the start of a race to attract the capital, talent, and infrastructure that define tomorrow's financial system?

Another interesting development, albeit one moving at a more reserved pace, is the digital euro project. Could we soon see a government-issued digital euro as an alternative to stablecoins offered by private companies? *Jeroen Boogaard* had the opportunity to ask *Menno Broos*, project manager digital euro at the Dutch regulator DNB, a wide range of questions.

The article by *Dominik Lynen* explores the growing integration of crypto assets in the financial system and the challenges and opportunities this presents for banks. The article outlines various levels of crypto adoption for banks - from minimal involvement to full-fledged integration - and discusses the integrity risks associated with each level. *Dominik Lynen* not only provides an overview of the arguments in favour of a more positive approach but also discusses the various ways in which banks can engage with the new technology and the tools for managing associated risks.

Delaney Diederik's article delves into how European Union regulations aim to protect investors from manipulative practices on crypto-asset service platforms. It explores the influence of cognitive biases on investor behavior and assesses the effectiveness of key EU frameworks like MiCAR, UCPD, and MiFID II in ensuring transparency and fairness, and whether there is still room for improvement.

It was not long ago that cryptocurrency was considered the jester of the financial industry, challenging the traditional financial industry to be better, quicker and cheaper. The importance of someone challenging the status quo is analysed in a contribution by *Edgar Karssing*. In his recurring column, he dives into the different apparitions of the jester (in Dutch “hofnar"), and all the different ways this personage can provide an organization and its leadership with some healthy testing.

We hope you find this issue insightful and engaging.

Paulien Makkinga, Pauline Wijma, Peter-Jan Engelen & Arend Koper

From inadequate oversight to effective regulation?

P. Engering, L. Kort, P. Kraaijeveld and mr. Y.B.A. Zaat[1]

Regulatory oversight of the crypto industry has made significant steps towards greater clarity and enforcement since we published our article in 2022.[2] Governments and regulatory bodies worldwide have made efforts to address the risks associated with crypto, including money laundering, sanction evasion, terrorist financing, fraud, and market manipulation, by introducing EU wide regulatory frameworks like MiCAR, DORA and stronger AML rules. In addition, financial regulators have built expertise and experience in the crypto sector necessary to have discussion with crypto parties across the board. Despite these steps forward, fundamental challenges remain. The global regulatory environment is marked by fragmentation, with disparate approaches across jurisdictions creating a complex and often inconsistent compliance landscape. Moreover, the rapid pace of innovation within the crypto ecosystem continues to outpace regulatory frameworks, leaving gaps in investor protection. The inherent borderless nature of crypto further complicates enforcement efforts, making it difficult for regulators to effectively monitor and control illicit activities. Investor protection remains a pressing concern, as many retail investors are exposed to highly volatile markets and sophisticated products that may not be fully understood or regulated yet.

In July 2025, Mark Nuvelstijn, former Chief Executive Officer and co-founder of Dutch crypto exchange Bitvavo, resigned following media reports linking him to insider trading and breaches of anti-money laundering rules. His departure came just weeks after Bitvavo received its Market in Crypto-Asset Regulation (Regulation (EU) 2023/1114, MiCAR) license and shortly after Nuvelstijn passed the suitability assessment of the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, the AFM).[3, 4] The timing raised questions: how could such serious concerns emerge so soon after two key regulatory milestones had been met? This illustrates a deeper problem. In 2022, we published an article examining the regulatory position of crypto-assets within the Dutch financial oversight landscape. Central to that piece was a critical question: *Who acts as the gatekeeper in the cryptocurrency domain?*

Our analysis at the time revealed that crypto's rapid technological advancement was outpacing the legal and supervisory infrastructure meant to govern it. Banks and payment service providers were increasingly confronted with crypto-related transactions, but lacked the tools, expertise, and legal clarity to monitor them effectively. Meanwhile, Crypto-Asset Service Providers (CASPs) largely operated outside the bounds of traditional financial regulation. The duty-of-care framework did not apply to clients of CASPs, leaving investors exposed to high risks without sufficient warnings and creating uncertainty about responsibility in cases of fraud-related losses. The result? Ambiguity, fragmentation, and above all, room for abuse by bad actors.

We observed that regulators have maintained a passive approach, primarily due to the lack of a strong legal framework. Crypto supervision drifted between the Anti-Money Laundering and Counter-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*, Wwft) and the Dutch Financial Markets Supervision Act (*Wet op het financieel toezicht*, Wft), without clear regulatory anchors. Registration obligations were weakly enforced, and neither prudential nor conduct supervision by the Dutch Central Bank (*De Nederlandsche Bank*, DNB) or the AFM was adequately in place. Fundamental questions, such as whether cryptocurrencies qualify as financial instruments or payment methods, remained unresolved.

This absence of a unified approach to crypto-related financial economic crime risks and the ambiguity related to the responsibilities between banks, crypto companies, and supervisory authorities, limited the ability to trace or disrupt illicit financial activities.

The limited crypto expertise within financial institutions wasn't helping in this area. Employees had minimal access to relevant tools or specialized training, and crypto was often dismissed as "too complex" or "too risky."

1. Peter Engering, Leon Kort, Paulien Kraaijeveld and Yorrick Zaat, Compliance Champs B.V. More information on compliancechamps.com
2. Engering, P., & Kort, L. J. H. (2022). *Vingerwijzen, bijten zonder tanden en gebrek aan verantwoordelijkheidsgevoel: Falend toezicht en regelgeving in een cryptowereld vol risico.* Tijdschrift voor Compliance, jaargang 22.
3. Silicon Canals. (2025, July 4). *Bitvavo CEO Mark Nuvelstijn steps down permanently following insider trading, AML allegations.* siliconcanals.com/bitvavo-mark-nuvelstijn-steps-down-permanently/
4. Bitvavo. (2025, July 4). *Mark Nuvelstijn steps down as CEO of Bitvavo.* https://bitvavo.com/fr/blog/mark-nuvelstijn-steps-down-as-ceo

This raises the core question of this article: *Has enhanced supervision been effective and reduced crypto-related risks?*

Recent data confirms that crypto-related crime is not reducing. In 2024, illicit actors received an estimated $40.9 billion in crypto, a figure projected to exceed $51 billion as more crypto wallet addresses are identified.[5] This represents approximately 0.14% of all on-chain volume. The accuracy of reported figures remains subject to debate. While Chainalysis is widely cited as a leading source, questions persist regarding the completeness and reliability of its data. This uncertainty is further compounded by the well-known criminological concept called the *'dark number of crime'*, the volume of unreported or undetected criminal activity beyond the reach of current monitoring tools.[6] Theft rose to $2.2 billion (a 21% year-on-year increase), while investment scams generated up to $12.4 billion, driven in part by a 40% surge in pig-butchering schemes.[7] Notably, stablecoins now account for 63% of laundering volume, overtaking Bitcoin as the primary medium for illicit finance.[8] Recent articles have also indicated that Supervisory bodies such as AFM and the Financial Stability Board (FSB) are worried about the financial stability risks that crypto brings.[9, 10,]

These developments underscore a critical tension: while regulatory frameworks have matured, financial crime risks remain active and highly adaptive.

1. Development in supervision and regulation since 2022

Since 2022, the regulation of crypto-assets has undergone a significant transformation. These developments reflect regulatory efforts to guide innovation, protect consumers, and safeguard financial integrity. Considering the increasing adoption of crypto-assets and the growing role of crypto services, regulators worldwide have taken major steps to strengthen legal frameworks.

The following paragraphs highlight key laws and initiatives introduced since 2022. In this article we focus on the developments in European regulations.

1.1. European developments

The most important pillar of the new European framework is MiCAR.[11] Applicable from 30 December 2024, MiCAR creates a uniform framework for crypto-assets in the European Union (EU). It sets out requirements for transparency, disclosure, licensing, and supervision of CASPs. In addition to MiCAR, CASPs also need to implement the Travel Rule, expanding obligations to provide sender/receiver information in crypto transactions.[12, 13,] Unlike most European jurisdictions, which generally allow an 18-month transition period, the AFM has set a significantly shorter six-month window, meaning that CASPs previously registered with DNB had to obtain an AFM license by 30 June 2025 to continue operating at full scope. Entities not previously subject to DNB registration, but now falling under MiCAR, had to be licensed by 30 December 2024.

These differing transition periods have created an uneven playing field across the EU. Whilst MiCAR aims to harmonise regulation, some jurisdictions offer a smoother path to licensing, potentially undermining uniformity. An example being Malta, whose MiCAR licensing process has been scrutinised by the European Securities and Markets Authority (ESMA). ESMA highlighted several shortfalls and proposed a set of recommendations for Malta's Financial Services Authority (MFSA), including the need for the MFSA to assess material issues that were either still pending at the date of the authorisation or that have not been adequately considered at the authorisation stage.[14,15,]

Another big regulatory milestone is the Digital Operational Resilience Act (Regulation (EU) 2022/2554, DORA).[16] DORA focuses on strengthening the digital

5. Chainalysis. (2025, January 15). *2025 Crypto Crime Trends: Illicit volumes portend record year*. https://www.chainalysis.com.
6. Coleman, C., & Maynihan, J. (1996). *Understanding crime data: Haunted by the dark figure*. Open University Press.
7. Reuters. (2025, February 14). *Crypto scams likely set new record in 2024 helped by AI, Chainalysis says*. https://www.reuters.com/technology/crypto-scams-likely-set-new-record-2024-helped-by-ai-chainalysis-says-2025-02-14/ (accessed July 4, 2025). Pig butchering will be further discussed in paragraph 3.4 of this article.
8. CoinLedger. (2025, June 9). *Crypto crime report: 2025 statistics & trends*. https://coinledger.io/research/crypto-crime-report (accessed July 4, 2025).
9. Autoriteit Financiële Markten (AFM). (2025, January). *AFM Trend Monitor 2025: Supervisory priorities and financial stability risks*. www.afm.nl/en/over-de-afm/verslaglegging/trendzicht (accessed July 4, 2025).
10. Financial Stability Board. (2024, December). *2024 Annual Report*. Available at: www.fsb.org (accessed July 4, 2025).
11. European Parliament & Council. (2023). *Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto assets*. Official Journal of the European Union.
12. 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.
13. European Banking Authority, *EBA issues Travel Rule guidance to tackle money laundering and terrorist financing in transfers of funds and crypto-assets*, available at: https://www.eba.europa.eu.
14. Cointelegraph. (2024, July 22). *Malta's MiCA licensing comes under scrutiny from EU regulator*. https://cointelegraph.com/news/mica-regulator-alarm-malta-crypto-licensing-process
15. European Securities and Markets Authority. (2025, July 10). *Peer review report: Executive summary. Fast-track peer review on a CASP authorisation and supervision in Malta* (ESMA42-2004696504-8164). https://www.esma.europa.eu/sites/default/files/2025-07/ESMA42-2004696504-8164_Fast-track_peer_review_on_a_CASP_authorisation_and_supervision_in_Malta.pdf
16. Regulation(EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

operational resilience of financial entities, including CASPs. It harmonizes ICT risk management rules within the EU. In the Netherlands, CASPs must integrate these requirements as part of their MiCAR application.[17, 18,]

Finally, the EU Anti-Money Laundering (AML) package introduces a new Anti-Money Laundering Authority (AMLA) and strengthens rules for CASPs, closing regulatory gaps and supporting uniformity across the EU.[19]

Regulatory developments in the crypto space are not limited to the EU. Other regions around the world are also actively (re-)shaping their frameworks. Clearer frameworks signal that the market is maturing, which in turn encourages greater institutional involvement.[20]

1.2. Developments related to financial supervisors

The ESMA was assigned a coordinating and supervisory role in implementing MiCAR in the EU.[21, 22,] In the Netherlands, the AFM is the main supervisory authority for most crypto parties.[23] Supervisory bodies have made substantial investments in recent years in building knowledge, creating specialized units, and forming interdisciplinary teams.[24]

In the Netherlands, both the AFM and DNB have established dedicated expert groups focused on CASPs. These financial regulators are involved in European working groups, developing technical standards and guidelines for the implementation of MiCAR.

At the European level, supervisory expertise has also deepened. In preparation for the rollout of MiCAR and the revised Travel Rule, ESMA and European Banking Authority (EBA) have published comprehensive consultation papers reflecting technical and legal analyses of the crypto market.[25, 26]

A global trend is developing where regulators worldwide are rapidly professionalizing in the crypto domain and international cooperation is increasing.[27,28] This evolution is important for achieving effective, proportionate, and future-proof oversight of the crypto market.

These regulatory developments, coupled with the growing expertise of supervisors, are laying the foundation for a more structured and accountable crypto market. However, regulation does not operate in isolation. Its effectiveness will ultimately be measured by how well it performs in practice – across jurisdictions, markets, and technologies. While international coordination is improving, fragmented supervision and differing legal standards continue to create opportunities for regulatory arbitrage.

2. Is the enhanced supervision effective?

2.1. Identified risks before 2022

The key risks identified in 2022 are grouped into four categories: fragmentated regulation, insufficient AML controls, technological opacity, and institutional unpreparedness. Each has seen partial, though uneven, progress.

Compared to 2022, the EU has achieved a great reduction in fragmentation with the recent regulatory developments. The adoption of MiCAR and the revised Transfer of Funds Regulation (Travel Rule) has introduced a harmonised framework for licensing and transparency, directly addressing the regulatory ambiguity.[29, 30,] However, enforcement gaps persist both beyond and within the EU. Within the EU, variations in the implementation of MiCAR, particularly regarding grandfathering periods and licensing procedures have so far prevented the establishment of a true level playing field across all EU Member States.

17. License application form: AFM, website *"CASP licence"*, available at: https://www.afm.nl/en/sector/cryptopartijen/vereisten-en-vergunningen/casp-vergunning (accessed July 8, 2025).
18. KPMG Netherlands, *"DORA implementation for MiCAR application proves a daunting challenge for CASPs"*, published July 2024, available at KPMG.nl (accessed July8, 2025)
19. The EU AML package, includes:
20. Catenaa. (2025, March 23). *Coinbase study: 75% of institutional investors to increase crypto exposure in 2025.* https://investors.catenaa.com/news/coinbase-study-75-of-institutional-investors-to-increase-crypto-exposure-in-2025.
21. CMS 2023 *Overview of Competent Authorities under MiCAR ; available at https://cms-lawnow.com/*
22. European Securities and Markets Authority (ESMA). (2024). *Opinion to support the convergent application of MiCA.* https://www.esma.europa.eu/
23. AFM supervises most crypto services- like CASPs-, Electronic Money Tokens (EMTs) an Asset-Referenced Tokens (ARTs)-often referred to as stablecoins- fall under the supervision of DNB.
24. Osborne Clarke. (2024, July 25). MiCAR: first experiences with Dutch AFM licence application process. Retrieved from www.osborneclarke.com/insights/micar first experiences dutch afm licence application process.
25. European Securities and Markets Authority (ESMA). n.d. *Markets in Crypto-Assets Regulation (MiCA).* Accessed July 13, 2025. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mic
26. European Anti-Money Laundering Authority. (2025, July 15). *AMLA expects high standards against financial crime in crypto sector.* EU AMLA. Retrieved from https://www.amla.europa.eu/resources/news-articles/amla-expects-high-standards-against-financial-crime-crypto-sector_en
27. Financial Stability Board. (2023). *FSB global regulatory framework for crypto-asset activities.* https://www.fsb.org/
28. Zetzsche, D. A., Arner, D. W., Buckley, R. P., & Börner, C. (2020). *The Market in Crypto-Asset Regulation (MiCA) and the EU digital finance strategy.* https://papers.ssrn.com
29. European Parliament & Council. (2023). *Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto assets.* Official Journal of the European Union, L150/40.
30. Regulation (EU) 2023/1113 on information accompanying transfers of funds and crypto-assets [2023] OJ L150/1.

Secondly, the AML vulnerabilities remain substantial. Peer-to-peer transactions, crypto cards, and privacy-enhancing tools are still largely evading oversight. Centralized exchanges and crypto ATMs run by licensed CASPs face tougher rules under MiCAR, but non-compliant or unregistered providers still create loopholes at the margins of the ecosystem.

Institutional competence has improved but remains uneven. Supervisory bodies like DNB and AFM have established dedicated crypto teams, and the ESMA has issued technical standards to enhance regulatory clarity. Yet technological capacity varies significantly across jurisdictions, and Decentralized Finance (DeFi) protocols, governed by autonomous code, still escape meaningful oversight. Within financial institutions, it is our observation that there is an increase in knowledge and awareness regarding crypto, with some banks now having dedicated transaction monitoring and Customer Due Diligence (CDD) crypto teams.

2.2. Rising systematic risks

At the same time, the increasing convergence of traditional finance and the crypto sector is resulting into new systemic risks. Where crypto-assets were once viewed as a detached, alternative asset class, the lines between the two domains have blurred significantly. A growing number of banks, asset managers, and institutional investors are gaining exposure to crypto, creating stronger interdependencies.[31]

One notable example is the Spanish bank BBVA, which in June 2021 became the first major European bank to offer Bitcoin trading and custody services via its Swiss subsidiary.[32] According to a 2023 PwC report, more than half of global asset managers have direct or indirect exposure to digital assets.[33] One example closer to home is neobank bunq, who enables its clients to invest in the crypto-asset market since April 2025. Bunq's crypto service is supported through the infrastructure of Kraken, a large CASP who has secured a license under MiCAR from the Central Bank of Ireland (CBI) and has passported to the Netherlands.[34, 35,]

This trend increases the risk of contagion. Events in the crypto space, such as sharp price drops, cybersecurity breaches, or the collapse of major exchanges, can directly impact traditional financial institutions and their clients. The collapse of FTX in November 2022 clearly illustrated this, affecting over nine million clients globally and causing losses for various traditional funds.[36] In times of market stress, crypto-related volatility and liquidity shocks can quickly spill over into broader financial markets.

In a July 2023 statement, the FSB warned that deepening integration between crypto-assets and traditional finance significantly increases the potential for systemic disruptions.[37] During the Financial Stability Conference in June 2025, the FSB highlighted this again by stating that growing risks from the crypto sector and its growing ties to traditional finance may soon reach a tipping point.[38]

At the same time, there is growing recognition that regulatory absence amplifies these risks. A harmonised supervisory framework, such as MiCAR is a good next step in safeguarding financial stability in an environment where digital and traditional finance are becoming increasingly intertwined.

2.3. Regulatory arbitrage

By mid-2025, a growing number of CASPs have obtained full MiCAR licences, enabling them to operate across the EU under the passporting regime.[39] Notable examples include Bitvavo (licensed in the Netherlands) and Coinbase (licensed in Luxembourg), alongside Kraken (licensed in Ireland), OKX and Crypto.com (both licensed in Malta), and Bybit (licensed in Austria).[40] The speed and jurisdictions in which most of the crypto firms obtained their licenses in our opinion demonstrate that compliance is not merely a regulatory hurdle, but a prerequisite for sustainable growth and a competitive advantage in building institutional partnerships.

MiCAR is considered a leading global framework, but its details are complex. This imposes practical challenges to navigate during the licensing process. At the same time, other jurisdictions have po-

31. Brasser, P. (2025, August 1). *Crypto wordt een systeemrisico, tot afgrijzen van toezichthouders.* Het Financieele Dagblad. https://fd.nl/financiele-markten/1563919/crypto-wordt-een-systeemrisico-tot-afgrijzen-van-toezichthouders
32. BBVA, *BBVA launches the first bitcoin trading and custody service for private banking clients in Switzerland*, press release, 18 June 2021, available at: https://www.bbva.com.
33. PwC, *Global Crypto Hedge Fund Report 2023*, May 2023, available at: https://www.pwc.com.
34. bunq. "bunq Brings Crypto Investing to Its Secure Banking App." *bunq Newsroom*, April 29, 2025. https://press.bunq.com/249420-bunq-brings-crypto-investing-to-its-secure-banking-app
35. Kraken. (2024, April 18). *Kraken receives MiCA license from Central Bank of Ireland*. Kraken Blog. https://blog.kraken.com/news/mica-license-central-bank-of-ireland
36. Financial Times, *FTX had more than 9 million users, liquidators reveal*, 19 December 2022; see also: US Bankruptcy Court for the District of Delaware, *FTX Trading Ltd. Chapter 11 filing*.
37. Financial Stability Board (FSB), *Crypto-asset activities: Global regulatory framework*, 17 July 2023, available at: https://www.fsb.org.
38. Cointelegraph. 2025. "FSB Warns Crypto Tipping Point with TradFi." *Cointelegraph*, July 10. https://cointelegraph.com/news/fsb-warns-crypto-tipping-point-tradfi
39. See, for instance, the interim MiCA Register made available by the ESMA, see: www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.
40. Cryptopolitan, 'CEX CASPs Thrive in EU 6 Months Into MiCA Regulations' (2 July 2025) https://www.cryptopolitan.com/cex-casps-thrive-eu-6m-into-mica-regulations/# accessed 4 July 2025.

sitioned themselves as crypto-friendly. The United Arab Emirates (UAE), for example, built a crypto-friendly regulatory and tax regime while Switzerland established a 'Crypto Valley' in Zug.[41, 42,]

Ironically, while the EU aims to protect consumers and stabilize markets, it may be undermining its own strategic autonomy. CASPs are deciding to be headquartered and licensed outside the EU, limiting the EU's influence on the crypto market.

Even within the EU's supposedly harmonised framework, implementation varies notably from country to country. Starting with the transitional period that differs between 6 and 18 months.[43] Companies are actively choosing to base themselves in Member States where the interpretation and implementation of EU rules are more favorable. If enforcement differs among jurisdictions within the EU, the harmonisation intended by MiCAR may not be fully achieved.

2.4. Progress or the same old problems?

On February 21, 2025, centralized exchange Bybit suffered a catastrophic cyberattack resulting in the theft of approximately $1.46 billion in crypto-assets; the largest crypto heist on record. The Bybit hack was promptly linked to Lazarus Group, a North Korean state-sponsored cybercriminal collective. The scale, speed and sophistication of the laundering operation following the breach raise urgent questions about security standards, compliance frameworks, and the effectiveness of regulatory initiates, such as DORA. This Bybit hack reflects a wider trend of repeated fraud, collapse, and regulatory lapses in crypto. While frameworks have advanced since 2022, vulnerabilities, poor governance, weak transparency, and poor investor protection persist in both centralised and decentralized contexts.

High-profile bankruptcies remain common. The fallout from FTX's 2022 collapse triggered insolvencies at Alameda Research, Celsius Network, and Genesis Global.[44, 45,] More recently, Terraform Labs filed for bankruptcy in 2024 following a $40 billion investor loss, settling SEC fraud charges for $4.47 billion.[46] Meanwhile, Celsius founder Alex Mashinsky was sentenced to 12 years in prison for securities fraud, and Terraform's Do Kwon faces similar charges.[47, 48,] Civil litigation involving Gemini, Genesis, and Digital Currency Group over alleged fraud exceeding $1 billion underscores the scale and continuity of misconduct.[49]

Although incidents as significant as the collapse of FTX have been less frequent in 2024 and 2025, fundamental vulnerabilities persist. Without stronger governance and enforcement, sophisticated attacks and mismanagement will persist despite regulatory advances.

3. Remaining risks under new regime

Regulators have addressed some structural risks since 2022, yet the crypto ecosystem continues to develop, bringing new challenges such as DeFi growth, and Artificial Intelligence (AI) integration. These developments are reshaping the risk landscape and testing the limits of existing oversight models. The following sections examine how these dynamics create new compliance and enforcement dilemmas that often exceed traditional regulatory approaches.

3.1. Impact on innovation

As crypto regulation strengthens, does it drive innovation or stifle it? On the one hand, frameworks like the MiCAR offer legal certainty and higher standards for consumer protection, market integrity, and risk management. This clarity attracts institutional investors and moves crypto beyond speculation. In addition, jurisdictions such as Singapore, the UAE, and the EU increasingly align on shared principles, supporting secure cross-border activity and legitimacy.

On the other hand, rigorous licensing, disclosure and Know Your Customer (KYC) requirements impose high costs, disproportionately affecting early-stage or smaller firms.

The latter is best illustrated by MiCAR's capital re-

41. Peak, Bradley. 2025. "5 Countries Where Crypto Is (Surprisingly) Tax Free in 2025." *Cointelegraph*, July 11. Accessed July 13, 2025. https://www.cointelegraph.com/news/countries-where-crypto-is-tax-free
42. Crypto Valley Association. n.d. "Welcome to Crypto Valley – Blockchain's New Home in Switzerland." Accessed July 13, 2025. cryptovalley.swiss/welcome-crypto-valley-blockchains-new-home-switzerland/
43. European Securities and Markets Authority (ESMA), *List of MiCA Grandfathering Periods (Art. 143(3))*, December 2024. Available at: https://www.esma.europa.eu/sites/default/files/2024-12/List_of_MiCA_grandfathering_periods_art._143_3.pdf)
44. ConsumerNotice, *Crypto Bankruptcies: Companies That Filed & Tips for Investors* Crypto Bankruptcies: Companies That Filed & Tips for Investors accessed 4 July 2025
45. Reuters, 'Valuing crypto in the bankruptcy multiverse' (13 April 2023) Valuing crypto in the bankruptcy multiverse | Reuters accessed 4 July 2025.
46. Reuters, 'Terraform Labs approved for bankruptcy wind-down after US SEC settlement' (19 September 2024) https://www.reuters.com/technology/terraform-labs-approved-bankruptcy-wind-down-after-us-sec-settlement-2024-09-19/ accessed 4 July 2025.
47. The Verge, 'Celsius founder Alex Mashinsky sentenced to 12 years in prison' (8 May 2025) Celsius Founder Alex Mashinsky Sentenced to 12 Years in Prison | WIRED accessed 4 July 2025.
48. Financial Times, 'Former Terraform Labs founder Do Kwon faces fraud charges in US' (2 January 2025)Subscribe to read accessed 4 July 2025.
49. Axios, 'Gemini, Genesis and DCG hit with civil fraud suit in continuing crypto saga' (20 October 2023) Crypto Groups Gemini, Genesis, and DCG Sued for \protect \TU\textdollar1.1 Billion 'Fraud' | WIRED accessed 4 July 2025.

quirements, which may be manageable for major players in the market, but they risk entry barriers for smaller innovators or early-stage innovators. Many argue this restricts innovative experimentation and favours well-capitalised incumbents. Others raise the question whether we are undermining our competitive position- both within and beyond the EU.

Technologies like DeFi, stablecoins, and AI -driven tools develop faster than regulation, leaving new use cases constrained by outdated rules.

Ultimately, the impact of regulation depends not on its existence, but on its clarity, adaptability, and operational nuance. Clear, adaptable rules foster innovation; unclear regimes push entrepreneurs to less transparent channels.

3.2. Growing DeFi

DeFi refers to a fast-evolving ecosystem of financial services, like lending, trading, and investing, built on blockchains and operated without traditional intermediaries like banks. Instead, DeFi relies on smart contracts: self-executing code that facilitates peer-to-peer transactions with enhanced efficiency and reduced costs. Its potential lies in expanding global access to financial services, particularly for those excluded from conventional banking systems.

DeFi poses significant oversight and compliance challenges. DeFi's decentralized nature, often governed by pseudonymous developers or decentralized autonomous organizations (DAOs), limits traditional supervision and complicates core compliance objectives such as KYC, transaction monitoring, and accountability.[50] This lack of clear responsibility is one of the reasons the EU has not included DeFi within MiCAR.

Regulators are exploring innovative approaches to DeFi oversight, including the EU's 2025 pilot on "embedded supervision," which leverages automated data collection and real-time monitoring built into blockchain protocols.[51] Meanwhile, industry efforts like identity attestations, blacklisting tools, and analytics integrations are emerging,[52] with some platforms implementing tiered access based on user verification.[53] These technological solutions alone are not enough; a coordinated global response and adaptive, risk-based regulatory models are required to ensure effective oversight while supporting innovation in the DeFi space.

3.3. AI and crypto

The crypto sector has witnessed an increase in AI-generated phishing schemes and social engineering attacks. These range from fake wallets and imitation platforms to personalized phishing messages created in multiple languages. According to Chainalysis (2025), approximately 60% of all deposits to fraudulent wallets this year were linked to AI-powered scams.[54] AI significantly enhances the sophistication and scalability of fraud. Current financial regulations still largely assume human intent and accountability, but AI systems can evolve based on patterns, including those derived from prior manipulative activity. Without an updated regulatory paradigm, AI is not merely a neutral tool, but it becomes a multiplier of existing systemic risks. Authorities such as the ESMA and DNB have been investigating the role of AI in financial markets. [55, 56] In June 2024, the EU adopted the Artificial Intelligence Act, the world's first rules on AI.[57]

As AI continues to reshape the financial landscape, its integration into the crypto sector introduces both powerful tools and unprecedented risks. While AI holds promise in enhancing market surveillance and detecting suspicious activity, it simultaneously creates new angles for manipulation and fraud, threats that current regulatory frameworks are ill-equipped to address.

3.4. Elevated money-laundering and sanction risk

In addition to the developments in AI and DeFi, there are also different scams and tools that still pose an increased risk to money laundering and sanction evasion. A clear example is the Automated Teller Machines (ATMs)- machines that allow cash purchases or sales of crypto-assets. They pose not only a significant money-laundering risk but also acute sanctions-evasion vulnerabilities. In Poland, there are over 280 of these machines in operation, with most located near borders with jurisdictions such as Belarus and Russia. At such crossings, a person can convert cash into crypto at a local ATM, carry the crypto on a mobile wallet or voucher across the border, and liquidate it- circumventing traditional financial channels subject to sanction screening.[58]

50. Zetzsche, D. A., et al. (2022). Regulating DeFi: The case for a functional approach. Stanford Journal of Blockchain Law & Policy.
51. Blockworks. (2024). *EU plans pilot project on DeFi supervision this year*, available at: https://www.blockworks.co.
52. Elliptic. (2023). *DeFi: Risk, Regulation and the Rise of DeCrime*, available at https://www.elliptic.co.
53. Merkle Science. (2023). *How DeFi platforms can overcome compliance challenges*, available at: https://www.merklescience.com.
54. Chainalysis, *AI-Powered Crypto Scams: How Artificial Intelligence is Being Used for Fraud*, available at: https://www.chainalysis.com.
55. European Securities and Markets Authority (ESMA), *AI in Financial Markets*, 2024.
56. DNB, *AI en toezicht: position paper*, 2023.
57. European Parliament. (2023, June 1). EU AI Act: First regulation on artificial intelligence. www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
58. Financial Action Task Force. (2023). *Targeted update on implementation of the FATF standards on virtual assets and VASPs.* FATF. https://www.fatf-gafi.org

Under MiCAR, crypto ATM providers must obtain a license to continue to operate in the EU. It remains to be seen how this will be enforced.

A growing but less visible threat is the "pig-butchering" scam, where victims are groomed through romance or investment schemes to transfer large sums to fraudulent platforms or individuals posing as loved ones. The term refers to "fatting up" victims with trust before financially exploiting them.[59] Existing regulatory tools are insufficient: AFM guidance on fake platforms is limited, and international coordination remains weak.[60] The Global Anti-Scam Alliance (GASA) urges standardised cross-border protocols and stronger retail-investor protections, but implementation lags.

The well-known pump and dump schemes also remain widespread in crypto and are classified as high-risk by the AFM.[61] The mechanism follows a standard procedure: the organizer selects a specific crypto-asset and platform, then buys a large amount of that crypto-asset. Through social media, mainly groups on platforms like Telegram, they announce the day of the pump and dump, without immediately revealing the crypto-asset's name. It is disclosed shortly before the pump begins. Once the pump starts, participants buy the crypto-asset en masse, causing a sharp price increase. The organizer then sells (dumps) at the peak, earning huge profits. The price drops as a result, leaving other participants with heavily devalued or worthless tokens.[62]

MiCAR explicitly bans organizing or participating in pump-and-dump schemes.[63] The AFM is warning investors about this, but acknowledges complete eradication is unlikely.[64] Monitoring promotional activity, enforcing disclosure rules, and educating consumers are essential steps to reduce the risks these unregulated voices pose to market integrity and retail investor protection.

A study by Wijzer in Geldzaken indicates that one in three young crypto investors who followed "finfluencers" advice later faced financial hardship.[65] The AFM warns that finfluencing often blurs the line between information and marketing. Posts may conceal conflicts or interests, such as undisclosed payments for promoting certain crypto-assets, or omit crucial risk disclosure required under financial law.[66] According to the AFM, misleading or incomplete recommendations can encourage impulsive trading behaviour and contribute to pump-and-dump schemes or participation in unlicensed platforms.

4. The way forward for crypto oversight

4.1. What works from the current framework?

The preceding risks underscore a critical tension: while regulatory frameworks like MiCAR have significantly improved oversight of traditional crypto services, they are still not fully equipped to address the changing complexity of the ecosystem. The EU's legal clarity is increasing as MiCAR aims to unify licensing requirements, improve consumer protection, and set standards for stablecoin issuance.[67] Supervisors such as ESMA and the AFM have strengthened their technical capacity, improving monitoring of market integrity and operational resilience.[68]

However, the current regulatory framework is relatively narrow, MiCAR does not fully apply to DeFi protocols or permissionless platforms, where systemic risks like Maximal Extractable Value (MEV)[69], front-running, and programmable settlement vulnerabilities persist unchecked.[70] These limitations are compounded by enforcement asymmetries. Despite growing institutional adoption and technical enforcement tools, the current architecture still struggles to govern the borderless, code-based logic of decentralised systems.

This has led to growing calls for an expanded and more agile successor framework, often referred to as "MiCAR 2 or MiCAR 1.1." Supervisory authorities like ESMA have flagged uneven licensing and supervision practices across EU Member States, recommending that future iterations of MiCAR embed more uniform technical and operational standards. A potential successor must therefore prioritise regulatory coverage of DeFi, stronger supervisory coor-

59. NOS, *Zorgen over nieuwe datingfraude "pig butchering": 'Ik voelde me zo dom', 2024, available at: https://nos.nl.*
60. AFM, *Waarschuwingen beleggingsfraude en cryptovaluta, 2023.*
61. AFM, *Pump-en-dump waarschuwingsbericht, September 2024, available at: https://www.afm.nl.*
62. Crypto Insiders, *Crypto's pump-en-dumpen is vanaf december officieel verboden in Nederland, 2024, available at: https://www.crypto-insiders.nl.*
63. See Title VI (specifically art. 91) of the *Markets in Crypto Assets Regulation (MiCAR).* Regulation (EU) No. 2023/1114. *Official Journal of the European Union*, L150/40.
64. AFM, *Pump-en-dump waarschuwingsbericht, September 2024, available at: https://www.afm.nl.*
65. NOS. (2024, May 7). *Veel jongeren verliezen geld door tips van 'finfluencers'*. Retrieved from https://nos.nl/artikel/2559546
66. Autoriteit Financiële Markten (AFM). (n.d.). *Finfluencing. Available at: https://www.afm.nl.*
67. European Union. (2023). *Markets in Crypto Assets Regulation (MiCAR).* Regulation (EU) No. 2023/1114. *Official Journal of the European Union*, L150/40.
68. *AFM Trend Monitor 2025: Supervisory priorities and financial stability risks.* www.afm.nl/en/over-de-afm/verslaglegging/trendzicht (accessed July 4, 2025).
69. MEV (Maximal Extractable Value) refers to the profit that can be made by reordering, inserting, or censoring transactions within a block, typically by miners or validators.
70. ESMA. (2025). *Maximal Extractable Value: Implications for Crypto Market Integrity* (ESMA50 481369926 29744). Retrieved July 4, 2025, from https://www.esma.europa.eu/sites/default/files/2025-07/ESMA50-481369926-29744_Maximal_Extractable_Value_Implications_for_crypto_markets.pdf

dination, and mechanisms for international alignment to close the gaps left by the current regime.

4.2. Balancing innovation and investor protection

Building on the regulatory gaps identified in MiCAR's current form, the next step for policymakers is to recalibrate oversight in a way that encourage innovation while preserving market integrity. One promising approach is principled-based regulation: setting high-level objectives such as transparency and investor protection, while allowing flexibility in how firms meet them.[71] This model has gained traction in recent discussions within the European policy circles, where rigid prescriptive rules are seen as ill-suited to fast changing technologies.[72] At the same time, regulators must modernise enforcement by integrating Supervisory Technology (SupTech) and Regulatory Technology (RegTech) to monitor decentralised systems, cross-chain transactions, and high-frequency trading practices.[73] Risk-based disclosures tailored to product complexity and user sophistication can further strengthen investor protection without suppressing experimentation. Global coordination is also crucial: as the FSB recommends, applying a "same activity, same risk, same regulation" principle across jurisdictions can prevent regulatory arbitrage and maintain consistent standards.[74] If aligned with international bodies such as IOSCO and FATF, this approach could offer a scalable template for balancing innovation with systemic safeguards.

4.3. Future of crypto and oversight beyond 2025

With the recent regulatory frameworks into place, the foundation is being laid for a more structured and resilient regulatory crypto landscape.

The next phase of crypto regulatory oversight is expected to focus on four priorities. First, cross-border coordination will be essential in addressing the current patchwork of regulations that often leads to uncertainty and regulatory arbitrage. A more harmonised global approach will help ensure consistent enforcement standards and reduce compliance burdens for international actors.

Secondly, DeFi governance will take centre stage, as regulators explore how decentralised protocols can align with legal and compliance requirements without compromising their foundational principles of autonomy and transparency. Finding regulatory models that respect decentralization while ensuring accountability will be a key challenge.

Thirdly, technological supervision will gain prominence, with authorities increasingly leveraging tools such as blockchain analytics, machine learning, and real-time monitoring systems to detect illicit activity and assess systemic risk.

Lastly, as the crypto market matures and adoption accelerates, the lines between decentralized technologies and legacy finance are becoming increasingly blurred. Major financial institutions are offering crypto-asset custody, tokenized securities, and blockchain-based settlement solutions. At the same time, decentralised protocols are exploring partnerships with banks, payment providers, and fintech platforms to expand access and usability. This convergence presents both opportunities and challenges, demanding thoughtful oversight to ensure stability, interoperability, and trust.

Together, these priorities reflect a shift towards smarter, more adaptive regulation that seeks to safeguard the financial system without hindering innovation.

Looking ahead, the most effective regulatory environments will be those that are not only clear and forward-looking but also adaptable to change. A future-proof regulatory framework will require ongoing dialogue between regulators, technologists, and market participants, ensuring that the crypto ecosystem can scale responsibly while maintaining financial integrity and consumer trust.

5. Conclusion

Since 2022, regulatory oversight of the crypto industry has made significant steps toward greater clarity and more robust enforcement measures. Governments and regulatory bodies worldwide have taken steps to address the risks associated with crypto, including money laundering, terrorism financing, sanction evasion, fraud, and market manipulation, by introducing enhanced regulatory frameworks like MiCAR and DORA. In addition, financial regulators have grown expertise and experience in the crypto sector necessary to have in-depth discussion with crypto parties across the board.

However, despite these advances, fundamental challenges remain. The global regulatory environment

71. Goyal, A., & Yadav, A. (2024). *Regulatory Approaches to Cryptocurrency: Balancing Investor Protection, Market Stability, and Innovation*. Atlantis Press. Retrieved from https://www.atlantis-press.com/article/126004224.pdf
72. Axios. (2025, July 10). *Senators discuss broad principles for crypto regulation*. Retrieved from https://www.axios.com/2025/07/10/crypto-senate-legislation-regulation-clarity
73. Bank for International Settlements. (2022). *Crypto, tokens and DeFi: navigating the regulatory landscape*. Financial Stability Institute Insights No. 49. Retrieved from https://www.bis.org/fsi/publ/insights49.pdf
74. Financial Stability Board. (2023, July). *High-level Recommendations for the Regulation, Supervision and Oversight of Crypto Asset Activities and Markets*. Retrieved from https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/

is marked by fragmentation, with disparate approaches across jurisdictions creating a complex and often inconsistent compliance landscape. This patchwork of rules not only complicates operations for global crypto enterprises but also encourages regulatory arbitrage, where actors gravitate toward more permissive regimes. Moreover, the rapid pace of innovation within the crypto ecosystem, particularly in DeFi, and the use of AI, continues to outpace regulatory frameworks. This causes uncertainty and leaves gaps in investor protection. Many retail investors are exposed to highly volatile markets and sophisticated products that may not be fully understood or regulated yet. The inherent borderless nature of crypto further complicates enforcement efforts, making it difficult for regulators to effectively monitor and control illicit activities.

While regulatory oversight in the crypto sector has become more effective and structured, it remains a work in progress. Addressing the enduring challenges of global coordination, innovation-driven regulatory gaps, and consumer protection will be essential to move to a mature, resilient crypto ecosystem.

Enforcement under MiCAR – Challenges and uncertainties

mr. N. de Koning and mr. drs. J.J. van der Grint[1]

Following the expiration of the transitional period in June 2025, the Markets in Crypto-Assets Regulation (MiCAR) is now fully effective in the Netherlands. This means that crypto-asset service providers (CASPs) operating in the Netherlands, such as trading platforms and custodians, are required to obtain a licence from the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, the AFM). Obtaining the licence is only the beginning: upon authorisation, a CASP must comply with prudential, organisational and conduct-of-business requirements on an ongoing basis.[2]

MiCAR represents the first comprehensive EU-wide framework for crypto-assets. It seeks to harmonise what had previously been a fragmented landscape of national registration regimes introduced under the Fifth Anti-Money Laundering Directive (5AMLD).[3] By moving beyond money-laundering prevention to encompass investor protection, market integrity and financial stability, MiCAR fundamentally alters the regulatory position of (among others) CASPs in the EU.

Taken together, MiCAR introduces a comprehensive set of rules that CASPs must comply with. Many market participants have made significant efforts in recent months to obtain a licence and to comply with the on-going requirements set out in MiCAR. Certain other market parties have either started the licensing process rather late or have opted not to pursue a MiCAR licence at all.

Whether licensed or not, CASPs are now subject to active supervision. Responsibility for enforcement in the Netherlands lies with the AFM, in coordination with European supervisory authorities at an EU level. This marks an important transition from the Dutch Central Bank (*De Nederlandsche Bank*, DNB), which supervised crypto service providers under the AMLD5 registration regime, to the AFM, which is tasked with enforcing a much broader set of rules.

The effective application of MiCAR will depend not only on entities' compliance but also on the supervisory approach adopted. Enforcement is the true test of MiCAR, as it will determine whether the ambitious objectives of harmonisation and investor protection are realised in practice. Questions remain over how supervisory authorities will interpret MiCAR's scope, how strictly they will use their new powers, and how cross-border and third-country cases will be handled.

This article explores the key challenges and legal uncertainties surrounding the enforcement of MiCAR by the AFM, with a particular focus on CASPs. Section 2 examines DNB's enforcement practice under the former registration regime. Section 3 outlines the AFM's supervisory and enforcement toolkit under MiCAR. Sections 4 to 6 analyse specific challenges relating to cross-sector, cross-border and third-country enforcement. The article concludes by reflecting on the uncertainties that remain and what can be expected in the next phase of supervisory practice.

1. Enforcement by DNB prior to MiCAR

Prior to MiCAR, crypto service providers were subject to a registration regime under 5AMLD. DNB actively took strong enforcement action against unregistered crypto service providers. The regulator targeted illegal crypto service provision in the Netherlands through targeted enforcement efforts, including administrative fines and orders subject to penalty. DNB imposed and published multi-million euro fines and orders subject to large penalties on several major crypto trading platforms that it considered to be active in the Dutch market without the required registration. DNB applied a broad interpretation of when crypto services counted as being provided "in the Netherlands." This expansive reading was widely regarded as a strict approach to the registration requirement.

The registration regime and the associated legal concepts were significantly shaped through these enforcement decisions and the related case law. It remains to be seen how this practice will carry over under MiCAR. A recurring point of contention between DNB and affected parties was whether their crypto services were being provided "in the Netherlands". DNB seems to have developed a set of stan-

1. Nikolai de Koning and Julia van der Grint both work as lawyers at law firm Norton Rose Fulbright LLP in Amsterdam, the Netherlands.
2. Title V MiCAR.
3. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ 2018 L 156/43.

dard indicators to establish that a provider was directing its business at the Dutch market.[4] These included, among other things, offering an app in the Dutch app stores, providing referral or affiliate programmes in the Netherlands, making information available in Dutch, or offering the domestic payment method iDEAL.[5]

MiCAR requires a licence where crypto-asset services are provided "in the Union".[6] MiCAR itself does not define when these services are deemed to be provided within the European Union (EU) or within a particular EU Member State. It is therefore conceivable that the AFM will, in practice, be guided by the indicators used by DNB, as these were rooted in European case law.[7] At the same time, the scope of MiCAR cannot be equated with the registration regime under the Act on the prevention of money laundering and terrorism financing (*Wet ter voorkoming van witwassen en financiering van terrorisme*, Wwft). Whereas DNB categorically rejected reliance on reverse solicitation[8] under the Wwft (or 5AMLD), MiCAR expressly recognises such a regime, albeit a very narrow one.

The strict approach taken by DNB has already been subject to judicial scrutiny. In several cases, crypto service providers contested DNB's interpretation of what constituted offering services "in the Netherlands". The courts were called upon to review whether DNB's indicators, such as Dutch-language websites and the availability of iDEAL, sufficed to demonstrate market targeting. While courts generally accepted DNB's broad interpretation, the litigation underscored that enforcement decisions in this field are not immune from legal challenge and that courts play an important role in defining the boundaries of supervisory authority.[9]

Another question is whether prior enforcement action under the registration regime must be considered when determining sanctions under MiCAR, either as recidivism or as an aggravating factor. Under Dutch law, recidivism exists if, at the time of the new infringement, less than five years have elapsed since an administrative fine was imposed on the same offender for the same offence. In that case, the fine must be doubled. The key issue is therefore whether a breach of the registration requirement and a subsequent breach of the MiCAR licensing obligation constitute "the same offence". One could argue that both regimes concern market access obligations and that repeated non-compliance should be treated as recidivism. On the other hand, they arise under (entirely) different legal frameworks. The registration regime under the Wwft was exclusively aimed at money laundering prevention, while MiCAR establishes a comprehensive framework addressing investor protection, market integrity and financial stability.[10] The range of regulated activities under MiCAR is also significantly broader. For that reason, it would require particularly convincing justification for a supervisory authority to classify such breaches as "the same offence".

It is also noteworthy that DNB's enforcement style under the Wwft contrasted with approaches taken in other EU Member States. Whereas some jurisdictions adopted a relatively light-touch interpretation of the AMLD5 registration requirement, the Netherlands quickly developed a reputation for rigorous enforcement. In the first months of MiCAR's application, the AFM has likewise already shown itself to be attentive to compliance, including by contacting firms in relation to possible or alleged breaches. The supervisory culture established by DNB may influence expectations for MiCAR enforcement, but the transition to AFM supervision marks a shift in emphasis. Early practice suggests that the AFM has so far taken a more balanced and pragmatic approach, focusing on dialogue with market participants during the licensing process rather than on deterrence through enforcement. Whether this cooperative stance will persist once MiCAR ages, or whether the AFM will ultimately adopt a more assertive enforcement style akin to DNB's, remains an open question.

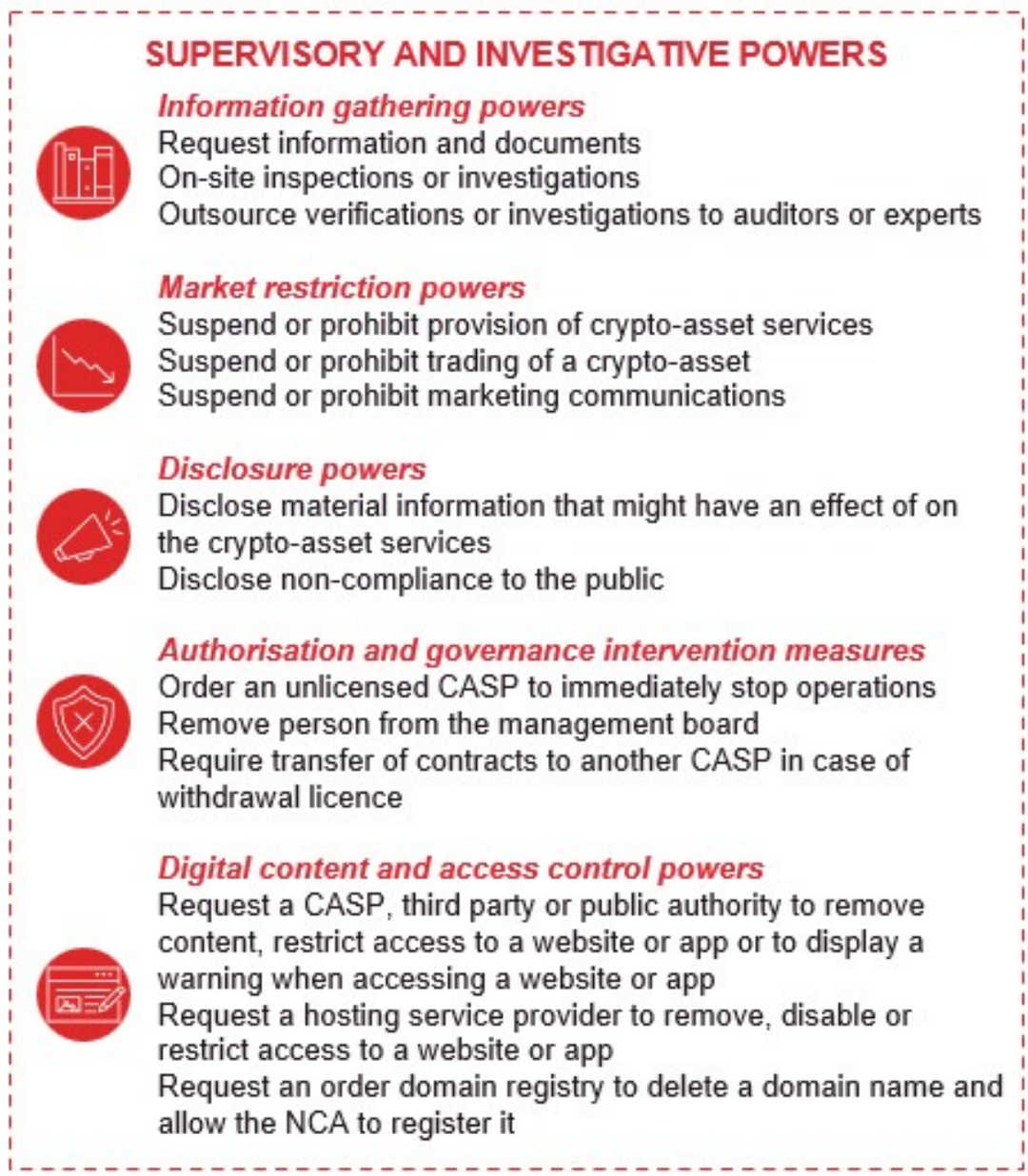
In any case, when considering whether to impose an administrative fine under MiCAR, the AFM is likely to take into account whether the offender has previously been reprimanded by DNB for a breach of the registration regime. Such a history could be invoked to demonstrate a pattern of disregard for regulatory obligations and to argue for a higher sanction. However, this assessment must be made carefully, case

4. This can be inferred from the enforcement measures published by DNB on its website, specifically under the section "Enforcement measures" in the news archive, where decisions against crypto service providers are made publicly available.
5. Please be referred to the enforcement decisions published on DNB's website.
6. Article 59 MiCAR.
7. CJEU 7 december 2010, ECLI:EU:C:2010:740 (*Pammer & Alpenhof*).
8. In several published enforcement measures, DNB has argued, drawing on the legislative history of the Wwft and the judgement of the Court of Justice of the European Union's in *Pammer v Reederei Karl Schlüter GmbH & Co KG* and *Hotel Alpenhof GesmbH v Heller* (Joined Cases C-585/08 and C-144/09, EU:C:2010:740), that the Dutch legislator did not envisage any scope for reverse solicitation under the criterion "in or from the Netherlands," and on that basis it has categorically rejected reliance on reverse solicitation under the Wwft (implementing 5AMLD). At the same time, DNB's reasoning is open to criticism. In practice, DNB acknowledges that the mere servicing of Dutch clients, without any active targeting of the Dutch market, does not suffice to establish an offering "in or from the Netherlands." In our view, the legislative history likewise does not explicitly rule out any form of reverse solicitation, leaving at least some conceptual room for such a defence in defined circumstances.
9. For example: Rotterdam District Court 10 March 2024, ECLI:NL:RBROT:2024:2110.
10. CASPs will remain subject to Wwft/AMLR obligations in parallel with MiCAR. However, this parallel applicability does not necessarily mean that infringements under both regimes should be regarded as "the same offence", given their distinct objectives and scope.

by case, and with adequate reasoning. In that context, the conduct of the offender remains highly relevant: where the provider has taken serious steps to comply and to prevent recurrence, such efforts should be recognised as significant mitigating factors. This balanced approach aligns with Dutch administrative enforcement practice, which requires proportionality between the sanction imposed, the seriousness of the infringement, and the conduct of the offender.

2. MiCAR supervision and enforcement toolkit

A fine is only one of the instruments available to the AFM if it concludes that a CASP is not acting in compliance with MiCAR. The regulation establishes a broad supervisory and enforcement toolkit, combining investigative powers, remedial measures and punitive sanctions. When deploying these powers, the AFM must assess which instrument is most effective and proportionate in achieving the supervisory objective at hand.

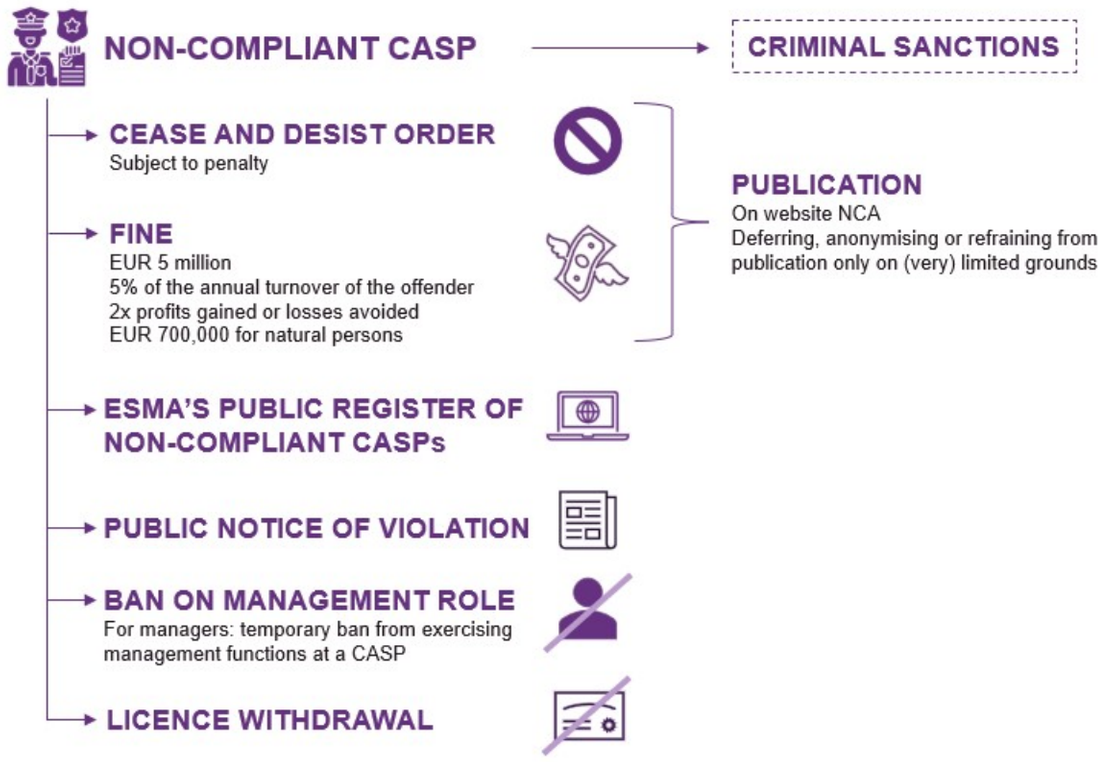


MiCAR supervision toolkit

Several of the supervisory and investigative powers mirror those already available to the AFM under the Act on Financial Supervision (*Wet op het financieel toezicht*, AFS) and general administrative law. However, MiCAR also introduces a number of new and far-reaching powers.

Examples include the power to prohibit the provision of crypto-asset services to specific clients, to restrict or prohibit marketing communications, and to require the transfer of existing agreements to an-

other CASP.[11] A particularly notable innovation is the power to impose obligations directly on third parties such as hosting service providers and domain name registries. These may be required to remove content from an online interface (such as an app or website), restrict or block access, display warnings, deactivate an online service, or even arrange for a domain name to be deleted.[12] These measures underline the focus of MiCAR on effective digital enforcement.



MiCAR enforcement toolkit

PRODUCT INTERVENTION

WHAT?

ESMA and/or the NCAs may prohibit or restrict:

- marketing, distribution or sale of certain crypto-assets; or
- a type of activity or practice related to crypto-assets.

WHEN?

In case of:

- significant investor protection concern;
- threat to orderly functioning and integrity of markets; or
- threat to the stability of the financial system

TEMPORARY – ESMA

PERMANENT – NCAs

MiCAR product intervention

Once the AFM has established, with or without the use of these supervisory powers, that a CASP is in breach of MiCAR, for example by offering crypto-asset services without authorisation, it can impose a wide range of measures. These include administrative fines, orders subject to periodic penalty payments, and temporary bans on managers from exercising functions in a CASP.[13] In cases of serious infringements, in particular those jeopardising investor protection, client interests or market integrity, the AFM may even withdraw a CASP's licence.[14] Other measures are aimed at reputational deterrence: information on sanctions may be published, and ESMA is tasked with maintaining a central register of entities providing crypto-asset services in the EU without the required licence.[15]

With regard to publication of sanctions, Article 114(1) MiCAR establishes transparency as the default rule. National competent authorities (NCAs) must publish without undue delay any decision imposing an administrative penalty or other enforcement measure, including information on the type and nature of the infringement and the identity of the person concerned. At the same time, Article 114(2) MiCAR allows NCAs to defer publication, to publish anonymously, or to refrain from publication altogether, where disclosure would be disproportionate, would jeopardise the stability of financial markets or the integrity of an ongoing investigation, or, in the case

11. Article 1:77n AFS.
12. Article 94 (1) (aa) MiCAR and Article 1:77n (u) AFS.
13. Article 111 MiCAR; Article 1:87 AFS; Annex 36 to the Decree EU regulations AFS (*Besluit EU-verordeningen Wft*).
14. Article 64 (1) (g) MiCAR.
15. Article 110 MiCAR.

of a natural person, would cause disproportionate damage. The framework therefore combines a presumption of full disclosure with a limited possibility to restrict publication in exceptional circumstances.

MiCAR further prescribes a list of factors that NCAs must take into account when determining the appropriate enforcement measure or the level of an administrative fine.[16] These largely correspond with the criteria already embedded in the enforcement policy of the AFM and DNB, as well as the AFM's fine assessment policy.[17] Particular weight is attached to the conduct of the offender, the degree of cooperation with the investigation, and whether voluntary steps have been taken to remedy the breach and prevent recurrence. Where such mitigating factors are present, the AFM may opt for a less intrusive measure or apply a reduction in the fine. Conversely, obstructive behaviour or repeated violations may justify the application of the most severe sanctions.

3. Cross-sector enforcement

Traditional financial undertakings may also provide crypto-asset services under MiCAR, provided they complete the appropriate notification procedure laid down in MiCAR.[18] This possibility is available to investment firms authorised under the revised Markets in Financial Instruments Directive (Directive (EU) 2014/65, MiFID II), credit institutions authorised under the Capital Requirements Directive (Directive (EU) 2013/36), and electronic money institutions under the Electronic Money Directive (Directive 2009/110/EC). For example, an investment firm authorised to provide investment services in relation to financial instruments under MiFID II may, following such notification, also provide equivalent services in relation to crypto-assets under MiCAR.

The decisive factor for determining the applicable regulatory framework is whether the instrument qualifies as a crypto-asset under MiCAR or as a financial instrument under MiFID II.[19] This classification is not always straightforward. MiCAR defines "crypto-asset" broadly in Article 3(1)(5) MiCAR, excluding financial instruments, deposits and e-money. MiFID II, in turn, defines "financial instruments" in Article 4(1)(15) and Annex I, Section C . The boundary between the two regimes is particularly difficult to draw in the case of asset-referenced tokens or utility tokens with investment-like features.

To promote consistent application, ESMA has consulted on draft guidelines setting out conditions and criteria for the classification of crypto-assets as financial instruments.[20] The primary responsibility for ensuring a correct classification lies with the issuer or the person seeking admission to trading.[21] Nevertheless, NCAs retain the power to review and, if necessary, challenge such classification, and may reach a different conclusion.[22]

A failure to correctly classify an instrument may have far-reaching consequences. If an asset presented as a crypto-asset is subsequently deemed a financial instrument, a CASP without a MiFID II licence would be providing investment services without the required authorisation. Conversely, if an investment firm applies MiCAR requirements to an instrument that should be treated as a financial instrument under MiFID II, the stricter MiFID II standards may be circumvented. Even where an investment firm has completed the MiCAR notification procedure, an incorrect classification can result in the wrong regulatory framework being applied.

Although MiFID II and MiCAR contain a number of overlapping requirements, there are material differences in scope and emphasis. Misclassification not only exposes undertakings to enforcement risk but may also deprive clients of the full protection of the correct framework. In such circumstances, the AFM may impose enforcement measures ranging from administrative fines to orders subject to periodic penalty payments, or even withdrawal of authorisation in serious cases.

A further complication arises where the same conduct breaches obligations under both MiFID II and MiCAR. In principle, this constitutes two distinct breaches, which would allow the AFM to impose two fines. In practice, however, the AFM tends to adopt a pragmatic approach: where the obligations are substantially identical and breached by the same conduct, the AFM usually imposes a single fine. This approach is consistent with existing enforcement policy and aims to avoid disproportionate outcomes.

4. Cross-border enforcement

CASPs generally operate across borders, serving clients in multiple EU Member States simultaneously. This cross-border reality requires close cooperation between NCAs and a clear coordination role for the European supervisory authorities to ensure coherent and effective enforcement of MiCAR throughout the EU.

MiCAR imposes a general duty on NCAs to cooperate with each other, as well as with ESMA and EBA, and to provide one another with assistance and information necessary for supervision, investigation and

16. Article 112 MiCAR.
17. The enforcement policy of the AFM and DNB (*Het handhavingsbeleid van de AFM en DNB*) and Fine assessment policy AFM (*Boetetoemetingsbeleid AFM*).
18. Article 60 MiCAR.
19. Article 2 (4) (a) MiCAR.
20. ESMA, Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments, 19 March 2025.
21. Recital 14 MiCAR.
22. Recital 14 MiCAR; ESMA Final report on the guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments, 17 December 2024.

enforcement.[23] To support this framework, ESMA, in close cooperation with EBA, is mandated to prepare draft regulatory technical standards specifying the information to be exchanged between NCAs, and draft implementing technical standards establishing standard forms, templates and procedures for that exchange.[24] In addition, ESMA must develop draft implementing technical standards establishing standard forms, templates and procedures for cooperation and information exchange between NCAs and ESMA/EBA.[25]

Where a host Member State has clear and demonstrable grounds for suspecting that a CASP established in another EU Member State is acting in breach of MiCAR, it must notify the home NCA and ESMA without delay, and where the matter concerns asset-referenced or e-money tokens, also the EBA.[26] If the home NCA does not take the necessary action, the host NCA may, after informing the home NCA, ESMA and, where relevant, EBA, adopt precautionary measures to protect local clients.[27] Disagreements between home and host NCAs may ultimately be referred to ESMA, or to EBA where asset-referenced tokens or e-money tokens are concerned.[28]

MiCAR also provides for product-intervention powers. NCAs may prohibit or restrict the marketing, distribution or sale of certain crypto-assets, practices or activities where this is necessary to address significant investor-protection or financial-stability concerns.[29]. These national measures must be notified in advance to other NCAs, ESMA and, where applicable, EBA, and are subject to an opinion procedure coordinated by ESMA or EBA. ESMA itself may impose temporary EU-wide intervention measures, while EBA may do so in respect of asset-referenced and e-money tokens.[30]

Transparency plays a further role in cross-border enforcement. ESMA must maintain a public register of authorised CASPs and white papers[31], as well as a public list of entities providing services in breach of the authorisation or reverse-solicitation rules.[32] NCAs are obliged to publish decisions imposing administrative measures or penalties, subject to the proportionality safeguards of Article 114(2) and (3) MiCAR, and to report annually to ESMA and EBA on the sanctions imposed. ESMA, in turn, must maintain a central non-public database of sanctions and measures to support supervisory convergence[33], a function broadly comparable to the coordination achieved through the Anti-money laundering and countering the financing of terrorism (AML/CFT) supervisory colleges under AMLD5 (and reinforced under the forthcoming AML Regulation[34]).

The division of responsibilities is therefore clear. Day-to-day enforcement remains with the NCA of the EU Member State in which the CASP is established. ESMA coordinates information exchange, promotes supervisory convergence, and may impose temporary EU-wide product measures where necessary, while also ensuring transparency through the registers. EBA's remit is narrower, being focused on significant issuers of asset-referenced and e-money tokens.[35] In practical terms, enforcement in the Netherlands will continue to rest with the AFM, but its actions will form part of a broader European framework designed to secure consistent supervision through cooperation, coordination and transparency.

5. Enforcement against third-country crypto parties

MiCAR also has important implications for crypto-asset entities established outside the EU. As a rule, third-country CASPs may not provide crypto-asset services within the EU without obtaining authorisation. The only exception is the reverse-solicitation regime laid down in Article 61 MiCAR. This exemption is deliberately very narrow and applies only where services are provided exclusively at the initiative of the client. ESMA's guidelines on reverse solicitation make it clear that the exemption is exceptional, time-limited and cannot be used as a structural market-entry strategy.[36]

The enforcement of MiCAR against non-compliant third-country crypto parties is not straightforward. Where a foreign CASP targets Dutch clients without authorisation, for example via Dutch-language websites, EU-targeted campaigns or use of local payment methods, the AFM may intervene domestically. Among other things, MiCAR empowers NCAs to require the removal or restriction of access to online interfaces, to direct hosting providers to remove or disable access, and to order deletion and re-assignment of domain names.[37] These powers are particularly relevant where the provider itself is outside EU jurisdiction and cannot be reached directly.

In practice, however, the effectiveness of such measures is limited. Online platforms and hosting ser-

23. Articles 95 and 96 MiCAR.
24. Article 95(10) and (11) MiCAR.
25. Article 96(3) MiCAR.
26. Article 102(1) MiCAR.
27. Article 102(2) MiCAR.
28. Article 102(3) MiCAR.
29. Article 105(1) and (2) MiCAR.
30. Article 103 and 104 MiCAR.
31. Article 109 MiCAR.
32. Article 110 MiCAR.
33. Article 115 MiCAR.
34. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
35. Articles 117–119 and 122–134 MiCAR.
36. Guidelines on situations in which a third-country firm is deemed to solicit clients established or situated in the EU and the supervision practices to detect and prevent circumvention of the reverse-solicitation exemption under the Markets in Crypto-Assets Regulation (MiCAR) (ESMA35-1872330276-2030, 6 February 2025).
37. Article 94(aa) MiCAR.

vices may be located outside the EU as well, complicating enforcement of blocking or removal orders. Even where measures are technically possible, they may be circumvented through mirror websites, VPNs or relocation of domains to jurisdictions beyond EU reach. Likewise, restricting access to payment channels requires cooperation from banks and payment institutions, which may be hesitant to act in the absence of clear regulatory guidance or binding orders. Public warnings are a valuable tool to alert clients, but in our experience their deterrent effect is often modest against firms determined to target the EU market.

Alongside these domestic tools, MiCAR does provide for cooperation with non-EU supervisors.[38] However, such cooperation depends on the willingness and capacity of third-country supervisory to act, which cannot (always) be assumed. The AFM's practical enforcement strategy against third-country providers will therefore have to rely on a combination of gatekeeper intervention, reputational measures and client awareness, rather than direct sanctions against the offenders themselves.

6. Conclusion

MiCAR has fundamentally changed the regulatory position of CASPs in the Netherlands and across the EU. The earlier registration regime under the Wwft has given way to a harmonised licensing framework that extends well beyond anti-money laundering and covers prudential, organisational and conduct requirements. Supervision now rests with the AFM, supported at EU level by ESMA and EBA.

The main questions now lie in application. MiCAR leaves scope for interpretation on points such as when services are deemed to be provided "in the Union", how previous breaches under the Wwft should weigh in sanctioning, and how proportionality should be ensured in practice. These are matters that will be clarified not by the text of MiCAR, but by supervisory and judicial practice.

For CASPs, obtaining a licence is only the starting point. The real challenge is ongoing compliance in an environment where supervisory expectations are still developing. The AFM has already shown that it is attentive to possible breaches, but the extent to which enforcement will mirror DNB's earlier strictness remains uncertain. Much will depend on how the first cases are dealt with, and whether they manage to combine effective deterrence with legal certainty and proportionality.

Looking ahead, the first wave of enforcement will play a decisive role in setting the boundaries of MiCAR in practice. Early decisions by the AFM and other NCAs will provide guidance on territorial scope, classification questions and the use of new supervisory tools. At the same time, coordination through ESMA and EBA will be essential to avoid divergent practices across EU Member States. The way in which these early uncertainties are resolved will determine not only the credibility of MiCAR, but also the level of trust that market participants and clients can place in the new framework.

38. Article 107 MiCAR.

The Only Constant is Change: State of Crypto Regulations Across the Globe

M.M. Fitzpatrick, T. Hyun and L. Rice[1]

Key jurisdictions across the globe are changing their regulatory postures on cryptocurrency to better balance innovation and oversight and attract major industry players to their shores.
The US has reversed course under President Trump's second term, introducing pro-crypto policies, clearer regulatory boundaries, and new laws like the GENIUS Act and CLARITY Act, focusing on stablecoins and market clarity. Meanwhile, the UK adopts a consultative approach via the FCA, focusing on stablecoins and custody through industry feedback. The EU, already implementing MiCAR, offers a unified regulatory framework, though transition challenges persist, particularly for stablecoin compliance. Singapore leads in Asia with a licensing regime under the MAS, strong AML controls, and stablecoin regulations supporting responsible innovation and asset tokenization. The UAE offers a layered regulatory model via free zones like ADGM and DIFC, with Dubai's VARA and Abu Dhabi's FSRA tailoring rules for both innovation and institutional-grade oversight.
For firms, success in this complex landscape depends on understanding jurisdictional differences, participating in regulatory consultations, and maintaining agile, well-resourced compliance programs. Adapting to evolving rules is crucial not only to minimize risk but also to capture strategic opportunities in the rapidly maturing crypto ecosystem.

1. Introduction – Change is in the air

The world's major financial centres are changing their regulatory postures on cryptocurrency in pursuit of becoming the dominant hub for institutional cryptocurrency adoption, as crypto intersects more meaningfully with traditional finance (TradFi). With the rise of fiat currency-backed stablecoins[2], the familiarity of regulation and real-world value is drawing more TradFi institutions. The stakes are clear: jurisdictions that provide regulatory clarity first will attract the capital, talent, and infrastructure that define tomorrow's financial system.

For business leaders and compliance professionals, this changing regulatory landscape offers both opportunity and complexity. Companies can weigh jurisdictional differences for strategic advantage, whether choosing where to launch crypto products or structure their operations.

We focus this article on five jurisdictions that are embracing this change: the US and EU as the world's largest financial markets, the UK leveraging its historical role as a global financial hub, Singapore as a leading innovator in blockchain and digital assets and the financial centre of Asia, and the UAE as the gateway between East and West. We outline key developments in each country's approach, how they balance innovation with security, and considerations for regulated institutions and compliance professionals navigating the global patchwork of regulations.[3]

2. US – Drastic shift towards a pro-crypto policy agenda

In the six months following President Donald Trump's second inauguration, major changes to regulatory guidance, enforcement priorities, and proposed regulations clearly signal the US's intent to be a global leader in digital assets and attract lawful market participants.

Two days into his second term, President Trump confirmed a dramatic shift in the approach to digital asset regulation by signing an Executive Order aimed at ending "regulatory overreach" in the crypto sector and establishing the US as "the world capital of crypto".[4,5] The Executive Order gave agencies 60 days to review existing regulations and recommend whether they should be rescinded or modified, effectively rebooting US crypto policy. Regulators were directed to provide clear jurisdictional boundaries, safeguard open access to public blockchain

1. Meredith Fitzpatrick and Thomas Hyun are Directors and Loretta Rice is a Senior Associate with Forensic Risk Alliance. All three specialize in cryptocurrency investigations and compliance.
2. A stablecoin is a type of cryptocurrency designed to maintain a steady value, typically by having its value pegged to a commodity or underlying asset, like the US dollar.
3. As regulatory guidelines in this industry are evolving rapidly, this article is current as of 21 July 2025.
4. www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-executive-order-to-establish-united-states-leadership-in-digital-financial-technology/
5. www.independent.co.uk/news/world/americas/us-politics/trump-cryptocurrency-world-liberty-financial-b2608885.html

networks, and promote the growth of lawful, dollar-backed stablecoins. However, these policy shifts and reversals only offer real business opportunities, if accompanied by the right compliance controls.

a. Policy reversals with caveats

While the momentum in the US towards updated regulations are positive for businesses and financial institutions seeking to engage with digital assets, they must continue adhering to existing financial regulatory obligations and risk and compliance practices. Federal priorities may have changed, but they still have the power to prosecute violations of law.

In parallel with the White House's broader crypto strategy, the Securities and Exchange Commission (SEC) has signalled a major shift in its regulatory and enforcement approach compared to its approach under President Biden. In January 2025, the SEC announced a new task force responsible for delivering clear regulatory lines, developing realistic paths to registration, and deploying enforcement resources more judiciously, pivoting away from its previously cautious and enforcement-heavy stance on digital assets. [6] As demonstrated by dismissals of civil enforcement actions or cases against crypto market participants such as Kraken,[7] Coinbase,[8] and Robinhood,[9,10] these measures have signalled a pivot away from enforcement actions under the Trump administration. However, the SEC has committed to continue to regulate fraud and enforce securities laws, while balancing a commercially grounded posture that acknowledges the unique features of blockchain technology.

Similarly, the Department of Justice (DOJ) has shifted its enforcement priorities, effectively ending its prior approach of "regulation by prosecution".[11] On 7 April 2025, Deputy Attorney General Todd Blanche issued a memorandum stating that the DOJ will "focus on prosecuting individuals who victimize digital asset investors, or those who use digital assets in furtherance of criminal offenses such as terrorism, narcotics and human trafficking, organized crime, hacking, and cartel and gang financing".[12] This aligns the DOJ's enforcement approach with recent Executive Orders and focuses on protecting individual and private-sector interests rather than targeting digital asset platforms, such as cryptocurrency exchanges, for inadvertent violations of regulation or acts by its end users.

US banking regulators have also loosened prior regulatory guidance for its supervised institutions. The Office of the Comptroller of the Currency (OCC),[13] Federal Deposit Insurance Corporation (FDIC),[14] and the Federal Reserve Board (FRB)[15] all withdrew prior guidance which previously required financial institutions to either notify or receive a non-objection prior to engaging in digital asset-related activities. These policy reversals offer new opportunities for TradFi to directly compete with technology-oriented disruptors who have historically offered digital asset capabilities from exchange services to tokenized offerings[16], including stablecoin issuance.

b. Classifying digital assets and clarifying regulatory oversight

US regulators have long debated the definition of digital assets, their classification under securities and commodities law, and how digital assets and institutions engaging digital assets should be supervised. With proposed legislation actively under review by both chambers of the US Congress, more clarity is on the horizon. Despite this evolving landscape, firms must remain vigilant and review how their digital assets will be classified under existing law. This includes the need to enhance programme and control measures aligned to anti-fraud and anti-money laundering (AML) requirements, and prepare for new registration and supervision requirements based on the classification of the firm's digital asset portfolio.

A new proposal named the Digital Asset Market Clarity (CLARITY) Act of 2025, which was introduced in the US House of Representatives by the Committees on Financial Services and Agriculture on 29 May 2025, is a recent attempt to clarify regulatory oversight over digital assets, delineate roles between US regulatory agencies, and classify certain digital assets.[17] The CLARITY Act divides oversight of digital assets between the SEC and the Commodity Futures Trading Commission (CFTC) and determines whether a digital asset falls under securities or commodities law.

More importantly for compliance professionals, under the CLARITY Act, both the SEC's and CFTC's anti-fraud and anti-market manipulation authority will be enforced in addition to the application of the Bank Secrecy Act and its related AML requirements for those defined as 'financial institutions' (e.g., digital commodity brokers and dealers).[18] On 17 July

6. www.sec.gov/newsroom/press-releases/2025-30
7. www.sec.gov/enforcement-litigation/litigation-releases/lr-26278
8. www.sec.gov/newsroom/press-releases/2025-47
9. newsroom.aboutrobinhood.com/sec-closes-investigation-into-robinhood-crypto-with-no-action/
10. www.reuters.com/legal/us-sec-closes-investigation-into-robinhood-with-no-action-2025-02-24/
11. www.justice.gov/dag/media/1395781/dl?inline
12. www.justice.gov/dag/media/1395781/dl?inline
13. www.occ.treas.gov/news-issuances/news-releases/2025/nr-occ-2025-16.html
14. www.fdic.gov/news/press-releases/2025/fdic-clarifies-process-banks-engage-crypto-related-activities
15. www.federalreserve.gov/newsevents/pressreleases/bcreg20250424a.htm
16. A tokenized offering refers to the issuance of ownership of an asset into a digital token on the blockchain.
17. financialservices.house.gov/uploadedfiles/052925_clarity_act.pdf
18. financialservices.house.gov/uploadedfiles/2025-05-29_-_sbs_-_clarity_act_of_2025_-_final.pdf

2025, the CLARITY Act was passed by the US House of Representatives.[19] If passed by the US Senate and signed into law, the bill would establish the US's first dedicated market structure for digital assets, shifting from regulation by piecemeal oversight toward a forward-looking, rule-based clarity, and greater transparency on asset classification and the respective rules of the SEC and the CFTC.

c. Stablecoins at the centre of new legislation

Institutional demand, emerging payment use cases, and TradFi's entry to the market have made stablecoins a priority for US lawmakers and the Trump administration. On 18 July 2025, President Trump signed into law the Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act, establishing a new regulatory framework for digital assets, specifically "payment stablecoins".[20] Under the GENIUS Act, stablecoin issuers seeking to operate in the US or market participants providing payment stablecoins to any persons in the US, will be required to comply with this new federal regulatory framework focused on transparency, consumer protection, and licensing and supervisory requirements, including those related to US AML laws.

The GENIUS Act defines a "payment stablecoin" and provides clarification that payment stablecoins are not to be considered securities or commodities—removing them from SEC and CFTC jurisdiction. The GENIUS Act also requires payment stablecoins to be issued by a "permitted payment stablecoin issuer", which may include subsidiaries of insured depository institutions, institutions approved by the OCC to issue payment stablecoins (e.g., non-bank entities), or smaller issuers chartered under a state payment stablecoin regulator. Payment stablecoin issuers are also subject to the Bank Secrecy Act and its related AML requirements applicable for financial institutions. After 3 years, restrictions would also apply for those operating secondary markets, as "digital asset service providers" (e.g., cryptocurrency exchanges) would be prohibited in offering or selling certain stablecoins, unless issued by a permitted payment stablecoin issuer. Additional requirements include mandatory one-to-one reserve backing, reserve composition limitations, prohibition of interest or yield-bearing payment stablecoins, and robust transparency and disclosure requirements.[21]
The GENIUS Act is expected to take effect in late 2026 once federal regulators issue its final implementing regulations. The US will then be able to effectively compete with other jurisdictions which have already established and advanced stablecoin frameworks, including the EU, UAE, and Singapore. The GENIUS Act therefore levels the playing field by fostering innovation while prioritizing consumer safeguards, reducing systemic risk, and establishing clearer oversight over stablecoin issuers operating in the US.

3. UK – Policymaking through industry engagement and consultation

Rather than fast-tracking legislation, the FCA is opting for a collaborative approach-engaging industry stakeholders within the private sector through these discussion papers. The Cryptoassets Roadmap outlines the various regulatory discussion papers and consultations the FCA plans to release throughout 2025, with final policy statements due to be published in 2026.[22] UK cryptoasset firms should actively participate in this consultative effort which provides an opportunity to provide feedback, shape future regulation, and have foresight into the FCA's priorities. For compliance programmes, these are opportunities to educate regulators on how to better align regulatory requirements to mitigate appropriate risks, while balancing operational limitations and efficiency considerations as a result of new policies.

As with other jurisdictions, stablecoins are a key focus for the UK's financial regulatory authorities. In response to prior proposals, the His Majesty's (HM) Treasury issued draft legislation in April 2025 which defines qualifying cryptoassets and qualifying stablecoins and brings newly regulated activities, including the issuance of qualifying stablecoins in the UK and safeguarding qualifying cryptoassets under the scope of the FCA. In May 2025, the FCA also published two consultation papers outlining proposed rules for the issuance of stablecoins and the custody of cryptoassets in coordination with the Bank of England.[23,24] The proposals mandate that stablecoin issuers maintain full reserve backing, ensuring each token is supported by equivalent assets. Additionally, firms providing custody services must implement robust systems to safeguard client assets and ensure their accessibility, segregating all client assets from the firm's own assets, held under non-statutory trusts.

19. financialservices.house.gov/news/documentsingle.aspx?DocumentID=410816
20. www.whitehouse.gov/briefings-statements/2025/07/the-president-signed-into-law-s-1582/
21. www.govinfo.gov/content/pkg/BILLS-119s1582es/pdf/BILLS-119s1582es.pdf
22. www.fca.org.uk/publication/documents/crypto-roadmap.pdf
    In accordance with the roadmap, the FCA has published several policy statements, discussion papers and consultations over the years, including "Financial Promotion Rules for Cryptoassets" in June 2023 and its discussion paper FCA's DP24/4: "Regulating cryptoassets: Admissions & Disclosures and Market Abuse Regime for Cryptoassets", published 16 December 2024, aimed "to help inform the development of a balanced regime that addresses market risks without stifling growth."
23. www.fca.org.uk/publication/consultation/cp25-14.pdf
24. www.fca.org.uk/publication/consultation/cp25-15.pdf

4. EU – MiCAR's remaining challenges post-implementation

The EU's Markets in Crypto-Assets Regulation (MiCAR) – which took full effect on 30 December 2024 – was the West's first comprehensive approach to regulating digital assets, including stablecoins. However, certain challenges remain from the issuance of compliant stablecoins to operational challenges during transitional periods. Notably, stablecoin issuers must consider whether to uplift programmes to adhere with MiCAR to operate in the EU or face market exit.

MiCAR introduces a uniform framework for crypto-asset issuers (CAIs) and crypto-asset service providers (CASPs). CAIs and CASPs across all 27 EU Member States are expected to complete their transition to the new MiCAR framework by July 2026, as MiCAR replaces the fragmented national regimes with a harmonized rulebook that enforces robust standards on transparency, governance, and AML.
MiCAR categorizes crypto-assets into three types: Asset-Referenced Tokens (ARTs), E-Money Tokens (EMTs), and other crypto-assets like Bitcoin or utility tokens.[25] The regulation introduces strict requirements for stablecoin issuers, including mandatory authorisation for CASPs, transparent white papers for issuers, and a ban on anonymous token offerings.[26] Reserve requirements under MiCAR are stringent; stablecoins must maintain a 1:1 reserve ratio,[27] with up to 60% of reserves held in bank deposits for significant issuers.[28,29]

a. Transitional period challenges

Under Article 143(3) of MiCAR, Member States can shorten the standard 18-month transitional period (January 2025 to July 2026) allowing a fragmented rollout. The "grandfathering" clause allows pre-existing crypto service providers to continue operating under local rules until they receive or are denied MiCAR authorisation, or until July 2026. While countries like France, Italy, and Spain are using the full period, others, such as Germany, the Netherlands, and Sweden, have opted for shorter 12-month transitions to sooner align with MiCAR.[30] These differences reflect each country's regulatory maturity, market readiness, and policy priorities. For example, Germany already requires Federal Financial Supervisory Authority (BaFin) licensing for crypto custody, creating dual compliance during the transition.[31] In addition to obligations under existing EU anti-money laundering directives, this provides added complexities for crypto operators as they attempt to comply with existing national requirements while seeking MiCAR authorisation across various transitional periods as defined by each Member State.

This reinforces, especially in a transitional environment, firms with well-designed compliance programmes that show good faith efforts to mitigate risk are essential to meet the current national requirements and satisfy new, EU-wide standards under MiCAR. Routine evaluation and testing of AML programmes by independent parties can also strengthen a company's AML posture to ensure alignment with AML directives, evolving regulatory requirements, and expectations before, during, and after MiCAR authorisation processes.

b. Impact of non-compliant ARTs and EMTs

The implementation of MiCAR's rules for ARTs and EMTs, effective from 30 June 2024, has already begun transforming Europe's stablecoin landscape. The shift intensified when the EBA and the ESMA issued coordinated public guidance clarifying how non-compliant stablecoins are to be treated under the regulation. The EBA emphasized that issuers of ARTs and EMTs must be fully authorised under MiCAR to continue operating in the EU, [32] while ESMA instructed CASPs, in a January 2025 statement, [33] to halt trading and promotion of non-compliant stablecoins by the end of January, with temporary "sell-only" access allowed through Q1 2025, allowing users to liquidate existing positions.
In response, major exchanges including Coinbase, Kraken, Binance and OKX began delisting non-compliant stablecoins, including Tether (USDT).[34] Stablecoin issuer Tether confirmed that the company would not seek MiCAR registration, citing concerns over reserve requirements to be held with EU banks.[35] However, Circle, the issuer for USDC, has secured an EU e-money license, and is positioning itself as a MiCAR-compliant alternative to gain

25. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114
26. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114
27. www.eba.europa.eu/sites/default/files/2024-06/3f3557fa-deb0-4765-add9-51666791e12c/Final%20report_draft%20RTS%20to%20specify%20the%20minimum%20content%20of%20liquidity%20management%20policy%20Article%2045%207.pdf
28. www.eba.europa.eu/sites/default/files/2024-06/580db2f3-8370-4927-baa3-0f995722b417/Final%20report_draft%20RTS%20further%20specifying%20the%20liquidity%20requirements%20Article%2036%204.pdf
29. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX
30. www.esma.europa.eu/sites/default/files/2024-12/List_of_MiCA_grandfathering_periods_art._143_3.pdf
31. www.bafin.de/EN/Aufsicht/MiCAR/MiCAR_node_en.html
32. www.eba.europa.eu/sites/default/files/2024-07/7dcd9ce9-96e3-4c5c-8d86-39d7784d1f03/EBA%20statement%20on%20Application%20of%20MiCAR%20to%20ARTs%20and%20EMTs.pdf
33. www.esma.europa.eu/sites/default/files/2025-01/ESMA75-223375936-6099_Statement_on_stablecoins.pdf
34. https://www.bloomberg.com/news/articles/2024-10-04/coinbase-to-delist-non-compliant-stablecoins-in-eu-in-december, https://www.bloomberg.com/news/articles/2024-03-18/crypto-exchange-okx-to-pull-tether-trading-pairs-in-europe, www.theblock.co/post/344182/binance-delist-tether-other-non-mica-compliant-stablecoins support.kraken.com/articles/stablecoin-offerings-for-eea-clients
35. https://cointelegraph.com/news/tether-ceo-defends-decision-to-skip-mi-ca-registration-for-usdt

ground among institutional users and platforms seeking legal clarity and institutional grade stability.[36]

Crypto firms willing to seek MiCAR-compliant status should first prioritize its understanding of the potential risks associated with new crypto-related offerings, including those associated with non-compliant ARTs and EMTs. Through risk assessment processes, CAIs and CASPs can effectively assess the risks tied to new and existing offerings, including the issuance, listing and delisting of tokens, and to remediate any potential MiCAR-related regulatory and compliance gaps. This is critical for stablecoin issuers as more TradFi institutions, who are well-versed with the risk management processes, begin to compete for stablecoin market share. These developments mark a new chapter for stablecoins in the EU-one defined not only by compliance, but by consolidation around those players willing and able to operate within MiCAR's clear but demanding framework.

5. Singapore – Asia's innovation and financial capital prioritizing onshore adoption and supervision

Singapore is amongst Asia's leading crypto hubs, with the Monetary Authority of Singapore (MAS) adopting a risk-based, innovation friendly approach towards crypto asset regulation. Through phased rules under the Payment Services Act 2019 (PSA) and the Financial Services and Markets Act 2022 (FSMA), MAS has tightened customer protections, addressed money laundering and terrorism financing risks, and promoted adoption and institutional tokenisation. For exchanges, stablecoin issuers, or traditional finance firms seeking to innovate with asset tokenization use cases in Singapore, the MAS has proven to a be first mover in digital assets regulation through established licensing frameworks with strict enforcement of stated requirements.

a. Regulating digital finance within and outside of Singapore

The PSA, which came into effect in January 2020, created a framework for MAS to regulate the fast-moving nature of digital payment technologies, including cryptocurrencies. The PSA not only defined cryptocurrencies under the term 'Digital Payment Token' (DPT) but instituted a licensing regime for cryptocurrency exchanges providing DPT services in Singapore. Under the PSA, MAS has approved 34 institutions offering Digital Payment Token (DPT) services to date, including for major exchanges like Coinbase and Crypto.com.[37]

FSMA, enacted in April 2022, complements existing requirements within the PSA (including other existing regulation such as the Securities and Futures Act 2001 (SFA)) and seeks to address a gap in the current regulatory framework by creating a new licensing requirement for entities established in Singapore but providing services associated with DPTs or digital representations of capital markets products as defined under the SFA to customers outside of Singapore. Therefore, the FSMA effectively expands MAS' territorial reach over Digital Token Service Providers (DTSPs) offering services outside of Singapore.

On 30 May 2025, MAS announced that firms offering crypto services to overseas clients must register and hold a license under the FSMA by 30 June 2025 or cease operations, with no transition period. [38] This has prompted major platforms, including Bitget and Bybit to consider relocating to more accommodating jurisdictions, such as Hong Kong and Dubai.[39] MAS clarified that "money laundering risks are higher in such business models and if their substantive regulated activity is outside of Singapore, MAS is unable to effectively supervise such persons".[40] Given these risks, the MAS will issue a DTSP license only in "extremely limited circumstances".[41]

Firms offering DPTs, DTSPs and those establishing operations in Singapore should understand the MAS' regulatory reach related to offshore activities, its high bar towards licensing, and MAS' general hesitation towards certain business activities outside of Singapore. More importantly, given MAS' focus on money laundering risks, especially in a cross-border context, these considerations should be thoroughly addressed from risk identification to its inclusion within internal controls to demonstrate the firm's ability to mitigate and manage potential activities and engagement with its customers, both locally in Singapore and in other jurisdictions the institution may serve.

b. Responsible innovation through asset tokenization and interoperability

Singapore is also actively promoting institutional adoption of tokenised finance through Project Guardian. MAS has, under this project, convened over "40 financial institutions, industry associations and international policymakers across seven jurisdictions to carry out industry trials on the use of

36. www.circle.com/pressroom/circle-is-first-global-stablecoin-issuer-to-comply-with-mica-eus-landmark-crypto-law
37. eservices.mas.gov.sg/fid/institution?sector=Payments\&category=Major%20Payment%20Institution\&activity=Digital%20Payment%20Token%20Service
38. www.mas.gov.sg/news/media-releases/2025/mas-clarifies-regulatory-regime-for-digital-token-service-providers
39. www.bloomberg.com/news/articles/2025-06-11/singapore-order-leads-unlicensed-crypto-exchanges-to-weigh-exit
40. www.mas.gov.sg/news/media-releases/2025/mas-clarifies-regulatory-regime-for-digital-token-service-providers
41. www.mas.gov.sg/-/media/response-to-feedback-received-from-dtsp-cp.pdf

asset tokenisation in capital markets".[42] MAS noted that these efforts reflect a growing interest in tokenisation and Singapore's commitment to scaling tokenised capital markets through industry-wide coordination. MAS has also developed the Global Layer One (GL1) platform, which aims to develop "an ecosystem of compatible market infrastructures" using a shared DLT ledger across regulated financial institutions, led by a core group of banks which includes Bank of New York Mellon, Citi, J.P. Morgan, MUFG and Societe Generale-FORGE.[43,44]

c. Advancing stablecoin regulations ahead of its peers

On 15 August 2023, MAS finalised its stablecoin regulatory framework, which apply to single-currency stablecoins (SCS) pegged to the Singapore Dollar or any G10 currency and issued in Singapore, making it amongst the first jurisdictions to have such rules.[45] To qualify as "MAS-regulated stablecoins," issuers must meet strict requirements on value stability, capital adequacy, redemption rights, and disclosure. Only those meeting the full criteria may label their products accordingly, with penalties imposed for misrepresentation. As MAS explained, "MAS' stablecoin regulatory framework aims to facilitate the use of stablecoins as a credible digital medium of exchange, and as a bridge between the fiat and digital asset ecosystems".[46]

Global stablecoin issuers, especially those with a significant presence in Singapore, should consider a multi-license strategy to ensure compliance in MAS' stablecoin framework and to ensure interoperability. Issuers should evaluate existing programmes for areas to harmonize globally while appending certain elements related to satisfy local requirements. For example, Paxos issues USD-denominated stablecoins through its approval by the New York State Department of Financial Services (NYDFS) and has received in-principle approval in November 2023 from MAS to issue stablecoins that comply with Singapore's framework.[47,48]

6. UAE – An agile framework for regulating onshore and across financial free zones

The UAE has adopted a slightly different playbook, positioning itself as a jurisdiction for crypto innovation. Confidence in the UAE's regulatory framework has strengthened of recent years, particularly following the UAE's removal from Financial Action Task Force or FATF's "gray list" in February 2024.[49] The growing list of newly licensed firms in the UAE demonstrates its popularity as an international base for crypto institutions. As a first mover in crypto asset regulation, those vying for an opportunity to operate in the UAE will have to navigate through a sophisticated regulatory framework based on specifications from regional regulators, particularly in Dubai and Abu Dhabi.

The UAE has five virtual asset regulators, the Securities and Commodities Authority (SCA), the UAE Central Bank (CBUAE), Dubai Financial Services Authority (DFSA), Financial Services Regulatory Authority (FSRA), and Dubai Virtual Assets Regulatory Authority (VARA). Its regulatory framework is layered and nuanced, with federal laws, emirate-level laws and free-zone regulations all operating simultaneously. The UAE also has two financial free zones, Abu Dhabi Global Market (ADGM) and Dubai International Financial Centre (DIFC), operating under English common law,[50,51] each with their regulators: FSRA for ADGM and DFSA for DIFC.[52] Virtual asset activities conducted onshore (i.e., outside ADGM and DIFC) are regulated primarily by the SCA and the UAE Central Bank.[53]

Depending on its service offerings and capabilities, firms must weigh whether to be regulated through VARA, FSRA, or through a combination of local regulatory regimes. This creates a complex web of licensing and supervisory requirements, based on the applicable regulatory framework. Firms must be able to establish, maintain and evidence sufficient risk and compliance programmes, including through audits and inspections post-licensure, to ensure adherence to stated rulebooks and to align to the evolving expectations of sophisticated local regulators such as VARA.

a. Dubai's VARA: An evolving rulebook for regulated VASPs

VARA, established in February 2022, is the world's first independent regulator dedicated solely to virtual assets.[54] VARA has already licensed multiple Virtual Asset Service Providers (VASPs), including

42. www.mas.gov.sg/news/media-releases/2024/mas-announces-plans-to-support-commercialisation-of-asset-tokenisation
43. www.mas.gov.sg/news/media-releases/2023/mas-partners-financial-industry-to-expand-asset-tokenisation-initiatives
44. www.mas.gov.sg/news/media-releases/2024/mas-expands-industry-collaboration-to-scale-asset-tokenisation-for-financial-services
45. www.cnbc.com/2023/08/15/singapore-among-worlds-first-to-agree-stablecoin-crypto-regulation.html
46. www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework
47. www.mas.gov.sg/news/speeches/2023/shaping-the-financial-ecosystem-of-the-future
48. www.dfs.ny.gov/reports_and_publications/press_releases/pr1909051
49. www.reuters.com/world/africa/fatf-financial-crime-watchdog-removes-uae-gibraltar-grey-list-2024-02-23/
50. www.adgm.com/adgm-courts/english-common-law
51. www.difc.com/whats-on/news/difc-announces-enactment-of-amendments-to-difc-law-on-application-of-civil-and-commercial-laws
52. www.adgm.com/media/announcements/sca-dfsa-and-adgms-fsra-reach-agreement-on-licensing-and-promoting-investment-funds
53. www.adgm.com/media/announcements/sca-dfsa-and-adgms-fsra-reach-agreement-on-licensing-and-promoting-investment-funds
54. www.vara.ae/en/about-vara/#'s%20first%20independent,framework%20to%20

Binance FZE, Laser Digital Middle East FZE, OKX Middle East Fintech FZE, and Crypto.com.
On 19 May 2025, VARA issued a Version 2.0 of its activity-based rulebooks.[55] The revised framework enhances oversight across eight core virtual asset activities, including advisory, brokerage, custody, exchange, lending and borrowing, management, transfer and settlement, and issuance services. Key updates include stricter controls around margin trading and token distribution services, and clarifications for collateral wallet arrangements.

On 31 August 2024, the Dubai VARA also issued the "Regulations on the Marketing of Virtual Assets and Related Activities 2024" to establish a comprehensive framework governing the promotion of virtual assets within Dubai, effective from 1 October 2024, and carrying significant penalties of up to AED 10 million per violation.[56] The new framework introduces detailed compliance obligations for all entities-domestic or foreign-that advertise virtual assets or related services in or targeting the UAE; these obligations apply regardless of whether the entity is licensed by VARA. The new rules also strictly prohibit marketing or conducting virtual asset activities involving "Anonymity-Enhanced Cryptocurrencies" (commonly known as privacy coins) – i.e. assets that obscure transaction ownership and lack traceability mechanisms.

b. Abu Dhabi: Institutional focus within the ADGM

ADGM, the finance-focused free zone of the emirate of Abu Dhabi, has regulated crypto asset activities since June 2018.[57] Most recently updated in June 2025, the Guidance on the Regulation of Virtual Assets Activities in ADGM provides a comprehensive and risk-sensitive approach to regulating digital assets.[58]

The FSRA requires any entity wishing to conduct virtual asset activities within ADGM to obtain a Financial Services Permission (FSP), be subject to AML and counter terrorism financing (CTF) requirements, taking advice from FATF recommendations in its approach to risk-based principles like customer risk assessment and customer due diligence. Only individually approved "Accepted Virtual Assets"[59] may be used, subject to seven key factors: maturity, security, traceability, exchange connectivity, type of distributed ledger, innovation, and practical application. Virtual asset exchanges operating as Multilateral Trading Facilities (MTFs) must implement market surveillance and transaction recording mechanisms, bringing regulatory oversight on par with conventional financial markets.

The FSRA also introduced a new regulatory framework for the issuance of fiat-referenced tokens (FRTs) that came into effect on 5 December 2024.[60] The framework makes FRT (e.g., fiat-backed stablecoins) issuance a distinct Regulated Activity within ADGM's financial services regulatory regime.

In December 2024, Zodia Markets, backed by TradFi giants Standard Chartered, received regulatory approval to operate as a virtual asset brokerage in Abu Dhabi.[61] This expansion reflects the FSRA's strategy of anchoring its digital asset ecosystem around institutional grade players and aligns with ADGM's broader commitment to establish itself as a regional hub for compliant and regulated virtual asset activity.

7. Conclusion

In this geopolitical contest for digital asset leadership, a government's success will hinge on its ability to strike the balance between enabling growth and innovation while safeguarding consumer trust. For compliance officers, the competitive landscape demands active monitoring and strategic positioning. The US policy reversal creates immediate opportunities, but legislative processes remain unpredictable. While the UK aligns on its final policy considerations, the EU's MiCAR framework, despite implementation challenges, provides a comprehensive rulebook and is already reshaping global stablecoin markets. Meanwhile, Singapore and the UAE have established themselves as innovation-friendly alternatives with proven licensing pathways.

For firms willing to venture into and/or expand their crypto reach, we suggest three immediate priorities: First, assess your company's specific ambitions in these core markets and whether the opportunities presented can be effectively managed by existing processes or require significant uplift. The current environment poses constant pressure on compliance organisations to keep pace with product and business ambitions. Compliance officers should thoroughly understand the risks of any new opportunity and whether additional capabilities, internal controls or resources may be required. Second, engage actively in consultations were possible – especially in the UK and US – if not to influence outcomes, then to stay on top of the regulatory debate. Third, once operational, regularly review, test and enhance compliance programmes in the con-

55. www.vara.ae/en/news/vara-issues-updated-activity-rulebooks-to-strengthen-market-integrity-and-risk-oversight/
56. rulebooks.vara.ae/sites/default/files/en_net_file_store/VARA_EN_419_VER1.pdf
57. www.adgm.com/media/announcements/adgm-launches-crypto-asset-regulatory-framework
58. adgmen.thomsonreuters.com/sites/default/files/net_file_store/Guidance_-_Regulation_of_Virtual_Asset_Activities_in_ADGM(VER07.100625
59. adgmen.thomsonreuters.com/sites/default/files/net_file_store/Guidance_-_Regulation_of_Virtual_Asset_Activities_in_ADGM(VER07.100625
60. www.adgm.com/media/announcements/fsra-introduces-a-regulatory-framework-to-support-the-issuance-of-fiat-referenced-tokens-in-adgm
61. www.adgm.com/media/announcements/zodia-markets-granted-financial-services-permission-by-adgm-strengthening-middle-east-presence

text of evolving regulations to maintain your regulatory and reputational standing. Regulated firms and their compliance programmes must be responsive to different requirements, especially those operating across multiple jurisdictions. These measures will not only minimize the institution's risk exposure but help risk and compliance programmes scale and remain compliant in the face of emerging regulatory changes.

‘Met de digitale euro kan Europa onafhankelijk blijven’

J. Boogaard

Niet alle Nederlandse banken zijn enthousiast over de komst van de digitale euro gezien de vereiste investeringen in hun IT-systemen. Maar op de lange termijn werkt de digitale euro in hun voordeel: de banken krijgen een alternatief betaalmiddel in handen en kunnen zo de afhankelijkheid van Amerikaanse spelers verminderen.

Dat zegt Menno Broos, projectleider digitale euro bij De Nederlandsche Bank (DNB) in een gesprek met Compliance, Ethics & Sustainability Journal. Samen met collega’s van de Europese Centrale Bank (ECB) werkt hij al geruime tijd aan de ontwikkeling van de digitale euro. Het moment waarop we met de nieuwe munt kunnen betalen is nog onbekend, want de Europese politiek moet zich hier nog over buigen, maar een veelgehoorde datum is 2029 of 2030, zegt Broos. Dat betekent dat de Nederlandse banken en ook het bedrijfsleven zich langzamerhand moeten gaan voorbereiden op de komst van de digitale euro.

Wat zijn de belangrijkste redenen voor de introductie van een digitale euro?

‘Allereerst speelt het afnemende gebruik van contant geld een grote rol. Deze trend wordt versterkt door de groei van e-commerce en het toenemende gebruik van digitale betaalmiddelen. Cash is publiek geld, uitgegeven door de centrale bank. Omdat die rol afneemt, denken centrale banken wereldwijd na over de digitalisering van hun diensten en de introductie van een Central Bank Digital Currency voor het brede publiek, een zogeheten retail CBDC. Met de digitale euro willen we op de lange termijn garanderen dat publiek geld beschikbaar blijft binnen de economie. Dat is voor ons de belangrijkste drijfveer. Daarnaast speelt strategische autonomie een cruciale rol. Op dit moment is Europa in het betalingsverkeer sterk afhankelijk van een paar grote Amerikaanse partijen, zoals Visa en Mastercard. Deze bedrijven beheren niet alleen het creditcardverkeer, maar ook een groot deel van de pinbetalingen. Bovendien zien we dat technologiebedrijven als Apple en Google zich steeds meer bemoeien met het betalingsverkeer, onder andere via digitale betaalpassen op smartphones. Dat gezegd hebbende: niet de hele betaalinfrastructuur is in buitenlandse handen. Bankoverschrijvingen verlopen bijvoorbeeld nog altijd via Europese netwerken. De kwetsbaarheid van Europa zit vooral in het domein van pin- en creditcardbetalingen, en juist daar willen we met de digitale euro meer onafhankelijkheid creëren.’

In hoeverre vormen de bitcoin en stablecoins een bedreiging voor de euro?

‘De discussie over de digitale euro kwam in een stroomversnelling toen Facebook zijn plannen aankondigde voor een eigen digitale munt, de Libra. Zulke initiatieven brengen het risico met zich mee dat het merendeel van de betalingen niet langer in euro’s plaatsvindt, maar in alternatieve valuta. Voor de ECB is dat een zorgwekkende ontwikkeling. Als de euro niet langer het prijsanker is binnen de eurozone, verliest de centrale bank grip op het monetaire systeem. Hoewel Facebook zijn plannen uiteindelijk niet heeft doorgezet, is de dreiging niet verdwenen. We zien een sterke opkomst van cryptovaluta en met name van stablecoins, zoals de US dollar-gekoppelde varianten, die wereldwijd steeds meer terrein winnen. Het betalingsverkeer is voortdurend in beweging, en het is lastig te voorspellen welke initiatieven dominant worden. Het is denkbaar dat ook bedrijven als X, het voormalige Twitter, in de toekomst een digitale munt lanceren. Tegen deze ontwikkelingen moet Europa zich kunnen wapenen. De digitale euro is een belangrijk instrument om die monetaire soevereiniteit te behouden en een robuust Europees alternatief te bieden in een snel veranderend betaalecosysteem.’

Het gevaar dreigt dat burgers in crisissituaties massaal geld overhevelen van bankrekeningen naar digitale euro’s. Dat kan leiden tot bankinstabiliteit. Hoe gaan jullie hiermee om?

‘Voor centrale banken is financiële stabiliteit één van onze doelstellingen, naast het bevorderen van de goede werking van het betalingsverkeer. We gaan niet de ene doelstelling opgeven voor de andere. Om de stabiliteit te waarborgen, en het risico van een ‘bankrun’ te verminderen, zullen er holdinglimieten voor de digitale euro zijn. Consumenten kunnen dan tot een bepaald bedrag geld aanhouden in hun digitale portemonnee. De limiet is nog niet vastgesteld, maar bedragen van €3000 worden genoemd. De relatief lage holdinglimiet brengt met zich mee dat de digitale euro geen oppotmiddel wordt, maar een betaalmiddel. We willen de digitale euro zoveel mogelijk op cash laten lijken en daarom zullen we ook geen rente op de digitale euro vergoeden. Voor cash geldt er weliswaar geen holdinglimiet, zolang je het

maar aangeeft bij de Belastingdienst, maar er zijn uiteraard fysieke barrières om veel geld op te potten. Doordat het betalingssysteem zo snel verandert, kunnen risico's voor de stabiliteit van het bankwezen overigens ook uit een heel andere hoek komen. Denk bijvoorbeeld aan instant payments[1]. De mogelijke invloed van de digitale euro op de stabiliteit is relatief beperkt en we moeten ons dan ook niet blindstaren op die holdinglimiet.'

Is de digitale euro een alternatief voor cryptocurrencies?

'De bitcoin en sommige stablecoins worden ook ingezet voor speculatie, transacties tussen cryptowallets, cross-border overschrijvingen en waarschijnlijk ook voor malafide overboekingen. Voor deze zaken is de digitale euro geen alternatief. De digitale euro is de natuurlijke opvolger van cash, die naast cash komt te staan, en die je kan gebruiken als betaalmiddel in webwinkels via een app. Gelijktijdig met de voorbereidingen voor de finale versie van de Verordening Digitale Euro bereidt de Europese Commissie wetgeving voor om cash in omloop te houden. Daar zijn wij een groot voorstander van, want contant geld heeft een belangrijke rol als betaalmiddel, vooral voor specifieke groepen in de samenleving.'

Hoe garanderen jullie de privacy van gebruikers van de digitale euro?

'De privacy van gebruikers van de digitale euro waarborgen we door als centrale bank zo weinig mogelijk persoonlijke gegevens in te kunnen zien. De ECB mag alleen de informatie inzien die noodzakelijk is voor het uitvoeren van een transactie. De persoonsgegevens zijn niet opgeslagen in onze database maar zijn fysiek ergens anders, zodat wij geen directe toegang hebben. Dit is vergelijkbaar met de huidige overboekingen tussen bankrekeningen, waarbij wij betalingen ook niet kunnen koppelen aan een persoon. De banken kunnen deze koppeling overigens wel maken. Er komt zowel een online als een offline digitale euro. Die laatste staat op je telefoon. Boek je offline geld over naar een winkel of persoon, dan ziet de ECB dat überhaupt niet. Overigens komt in de wetgeving te staan dat de digitale euro niet programmeerbaar mag zijn, zodat de overheid of ECB niet kan bepalen wat er met de digitale euro wordt gekocht. Ook dat is een extra waarborg voor de bescherming van privacy van de gebruikers.'

Banken moeten grote bedragen gaan investeren in technologie om de digitale euro te ondersteunen en aan wet- en regelgeving te voldoen. Hoe kijkt DNB hier tegenaan?

'We zijn hierover al in gesprek met banken, want het is duidelijk dat de invoering van de digitale euro aanpassingen aan hun IT-systemen vraagt. Banken zijn hierin terughoudend, mede vanwege de benodigde investeringen en de capaciteit die ze moeten vrijmaken. Ze stellen zich de vraag of de digitale euro wel noodzakelijk is. Daarop wijzen wij hen op twee belangrijke argumenten. Ten eerste is het vanuit maatschappelijk oogpunt essentieel om weerbaar te zijn en meerdere betaalopties beschikbaar te houden. Dat is niet per se efficiënt, net zoals dat het in stand houden van contant geld kosten met zich meebrengt. Maar iemand moet die maatschappelijke kosten dragen. Ten tweede zijn Nederlandse banken momenteel sterk afhankelijk van een klein aantal dominante Amerikaanse spelers in het betalingsverkeer. Deze partijen verdienen goed aan hun monopoliepositie. Op de lange termijn is het daarom strategisch voordelig voor banken om een Europees alternatief in handen te hebben. Ook voor henzelf is minder afhankelijkheid uiteindelijk gunstig.'

'De benodigde investeringen richten zich vooral op eenmalige aanpassingen aan het settlement-systeem voor digitale eurotransacties. Wij doen er alles aan om de extra lasten – bovenop reguliere uitgaven aan het betalingsverkeer – zo beperkt mogelijk te houden. Onze visie: als een bank in staat is om een creditcard aan klanten aan te bieden, dan moet het ook mogelijk zijn om zonder veel extra inspanning de digitale euro te integreren. Zodra de wetgeving is vastgesteld en er duidelijkheid is over de tijdslijn, verwachten we dat de investeringen vanzelf op gang komen. Wij zullen banken hierin actief ondersteunen. De offline digitale euro wordt als een losstaand product ontwikkeld en door ons 'turn-key' opgeleverd. Banken kunnen deze oplossing eenvoudig integreren in hun eigen apps – als dat überhaupt nodig is, want de ECB ontwikkelt ook een eigen app voor de digitale euro.'

Hoe worden de risico's van de digitale euro met betrekking tot Anti-Money Laundering (AML) en Counter-Terrorism Financing (CTR) gemitigeerd?

'Ook hierover voeren we een continue dialoog met de banken en wetgever. Vooralsnog gaan we ervan uit dat voor digitale eurotransacties dezelfde normen gaan gelden als voor het gewone digitale betalingsverkeer. Banken zullen transacties risicogebaseerd moeten monitoren om witwassen en terrorismefinanciering te voorkomen. Waarschijnlijk is monitoring voor offline-bedragen niet nodig, ook omdat dit technisch nog niet mogelijk is. Voor compliance-managers is het afwachten van de wetgever gaat doen. De Europese privacy waakhond zal zich met name nog gaan buigen over de offline digitale euro. Daarbij zal een afweging worden gemaakt tussen de risico-acceptatie door overheden en het gebruikersgemak. Als DNB volgen wij deze discussie vanaf de zijlijn, maar met veel interesse.'

Nigeria is een van de vier landen met een retail CBDC. De zogeheten eNaira werd in oktober 2021 gelanceerd en wordt vooralsnog niet veel gebruikt, met een adoptiegraad van circa 6%. Bij welke adoptiegraad is de digitale euro volgens jullie succesvol?

'In Nigeria is de adoptiegraad inderdaad laag, maar het land heeft ook een ander betaalsysteem dan wij hebben. Veel Nigerianen hebben geen smartphone maar doen hun digitale betalingen via hun gewone mobiele telefoon. In Europa zal de adoptiegraad van

1. Betalingen binnen 10 seconden

de digitale euro per land aanzienlijk verschillen, afhankelijk van de nationale betaalgewoontes en het gebruik van contant geld. In Nederland gebruiken we bijvoorbeeld iDeal voor e-commerce transacties, terwijl de Duitsers met Paypal of credit cards online betalen. We hebben geen concrete adoptiegraad voor ogen, maar hopen dat veel Nederlanders de digitale euro gaan gebruiken. Als ongeveer de helft van de bevolking een digitale euro-portemonnee downloadt, dan zou dat een mooi resultaat zijn. Een adoptiegraad van 50% dus. Het aandeel in het daadwerkelijke betalingsverkeer mag wel wat lager om het toch als een succes aan te merken.'

Wat betekent het verbod voor overheden en bedrijven om digitale euro's aan te houden?

'Het doel van de digitale euro is niet om een oppotmiddel te worden. Daarom is de huidige visie dat ook bedrijven en overheden geen digitale euro's mogen aanhouden. Digitale euro's die bij winkels binnenkomen, worden automatisch of aan het eind van de dag overgeboekt naar hun zakelijke bankrekening. Anders dan contant geld, blijven ze dus niet in de 'kassalade' liggen. Dat is voor ondernemers ook praktisch, want zo behouden zij de liquiditeit die ze nodig hebben voor hun dagelijkse uitgaven op hun bankrekening. Bedrijven zullen de digitale euro moeten accepteren, met mogelijke uitzonderingen voor kleinere handelaren zoals marktlieden. Het is aan ons om ervoor te zorgen dat de invoering hiervan zo weinig mogelijk kosten met zich meebrengt. Zo hoeven winkeliers niet te investeren in extra betaalterminals. De digitale euro kan via dezelfde infrastructuur worden geaccepteerd die ze nu al gebruiken voor betalingen met bijvoorbeeld Visa en Mastercard.'

Komt de ECB ook met een 'wholesale CBDC' die door financiële instellingen wordt gebruikt?

'De ECB is inderdaad ook druk bezig met de ontwikkeling van een wholesale digitale euro. Daarbij onderzoeken we mogelijkheden om de huidige betalingssystemen voor banken via distributed ledger technology, of DLT, toegankelijk te maken. Het gaat dan simpel gezegd om de ontwikkeling van een door de ECB uitgegeven stablecoin die banken kunnen gebruiken om grote betalingen af te wikkelen. Er is zoveel innovatie, dat de retail CBDC in de toekomst vermoedelijk ook met DLT verder ontwikkeld zal worden. Maar voorlopig blijft onze grote uitdaging om de retail CBDC bij de klant te brengen en de techniek is een relatief simpel onderdeel daarvan.'

Banking crypto clients: better monitoring through adoption

D. Lynen[1]

The accelerating mainstream adoption of crypto assets presents both opportunities and significant integrity risks for banks. With more than 30 million users in the EU and over 40 trillion US dollar in associated trading volume per year, crypto assets are becoming an integral part of the financial system, supported by evolving international regulatory frameworks. Traditional, passive approaches by banks, such as offboarding crypto clients, are no longer practical nor commercially viable.
Instead, banks should develop a clear vision and risk appetite around crypto, tailored to their client portfolios and strategic goals, balancing the need to manage risks like money laundering, terrorism financing, and sanctions evasion with the potential benefits of crypto integration. While the level of adoption is by no means a one-size-fits-all endeavour, the case is made that adopting a crypto strategy leads to better control and mitigation of crypto-related risks.
The article will first set out an approach on crypto adoption by traditional financial institutions and the various levels that can be worked towards, before elaborating on some of the most significant integrity risks related to crypto and discussing how monitoring of crypto clients differs from traditional monitoring and what is needed to do so effectively.

1. Mainstream adoption

The market for crypto or virtual assets has grown rapidly in the Netherlands over the last few years. In the Netherlands, over two million individuals possess crypto assets. [2] In the European Union ("EU"), somewhere upwards of 30 million citizens hold crypto assets[3], generating an annual trading volume of 40.5 billion US dollar.[4] Be it out of curiosity, as a short-term investment, to transfer funds (internationally) or to HODL[5] – crypto is here to stay. Moreover, the rise of stablecoins has provided an extra boost to mainstream adoption, as it provides an every-day use case (payments and remittances) for the masses, due to its currency-pegged constant value.[6]

Think tanks and legislators globally advanced the market through regulatory frameworks, from Financial Action Task Force ("FATF") Standards to the EU's AML Directives[7] (since 2020), the "Travel Rule"[8] (since end of 2024) and the Markets in Crypto Assets Regulation ("MiCAR")[9] (which requires crypto-asset service providers, or "CASPs" for short, to operate under a license as of 30 June 2025), as well as the US GENIUS Act[10] on stablecoin regulation (signed into law on July 18 2025), which in turn leads to more trust and mainstream adoption.
Hereinafter, it will be discussed how traditional financial institutions should move from a passive approach regarding crypto assets to a level of adoption that reflects regulatory developments, mainstream acceptance and their own client portfolio. Subsequently, crypto-related integrity risks are being elaborated on, as well as the approach to monitoring that is needed to mitigate these risks effectively.

1. Dominik Lynen, Senior Manager at Deloitte Forensic & Financial Crime. This article reflects the own views of the author and it is not representing the views of Deloitte.
2. The latest market research by Multiscope dates from 2023. 'Cryptovaluta Monitor', *Multiscope* 2023, https://www.multiscope.nl/diensten/marktcijfers/cryptovaluta-monitor.html. Other publications of 2024 already mention 2.5 million. 'Cijfers over het crypto gebruik in Nederland in 2024', *Het Ondernemersbelang* 19 March 2024, https://www.ondernemersbelang.nl/nieuws/cijfers-over-het-crypto-gebruik-in-nederland-in-2024/.
3. The ECB estimates that around 9.7% of households own some form of crypto assets, while a survey by Gemini suggests higher adoption rates, at least for some countries. 'EU central bank sees crypto adoption growth', *Ledger Insights* 28 May 2025, https://www.ledgerinsights.com/eu-central-bank-sees-crypto-adoption-growth-raises-stability-concerns/.
4. Based on a projection over 2024. 'Which countries trade crypto the most? A Comprehensive Analysis', *CoinWire* 2024, https://coinwirez.com/crypto-trading-report-2024/.
5. Originally a spelling mistake of "hold", the term "HODL" has become synonymous with a long-term investment strategy in crypto assets (now jokingly standing for "Hold On for Dear Life").
6. Stablecoins have a global supply of more than 200 billion USD, with a transfer volume of 27.6 trillion USD in 2024, more than Visa and MasterCard combined. 'Stablecoin surge: Here's why reserve-backed cryptocurrencies are on the rise', *World Economic Forum* 3 June 2025, https://www.weforum.org/stories/2025/03/stablecoins-cryptocurrency-on-rise-financial-systems/
7. Which will be mostly replaced by the EU Anti-Money Laundering Regulation (2024/1624/EU), applicable as of 10 July 2027.
8. EU Transfer of Funds Regulation (2023/1113/EU).
9. EU Markets in Crypto-assets Regulation (2023/1114/EU).
10. Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, S. 1582, 119th Cong. (2025).

2. Passive approach by traditional financial institutions

In terms of Customer Due Diligence, while many traditional financial institutions have long taken a passive approach towards (clients with) crypto assets – *e.g.*, rejecting/offboarding them or treating crypto assets like a cash variant (in terms of financial crime) – such a course is no longer feasible given the maturity of the market and the ever-growing mainstream adoption. It is simply unrealistic, commercially reckless and unnecessarily costly, to treat millions of clients as a high risk, or even have them offboarded, simply for owning a certain, now regulated, asset class.

Instead, banks are encouraged to develop a strategic vision for engaging with cryptocurrency. This vision should guide the way for all subsequent decisions on the topic, serving internal stakeholders – from senior management to first-line employees. To do so, banks must have a deep understanding of the workings and risks of crypto transactions, analyse their client portfolio, and choose a level of adoption that matches their portfolio, strategic ambitions and appetite for risk. The risk appetite should be concise and specify thresholds and limits, so as to avoid ambiguity later on. Only once these factors are given, a bank should move forward to embedding its vision in policies, procedures and operations – finding a balance between completely avoiding crypto, with the awareness that zero risk is practically unattainable, and blindly following the hype. Consequently, this translates into the integrity risk analysis (in the Netherlands well-known as the Systematic Integrity Risk Analysis, or SIRA for short, laid down in article 2b of the Dutch AML Act, *Wet ter voorkoming van Witwassen en financiering van terrorisme*), which likewise requires a deep understanding of and granular approach to crypto-related integrity risks, so as to be effective.

3. Client portfolio and levels of adoption

a. Client portfolio

One of the first steps that guides the approach, is performing an analysis on the client portfolio. It should provide insights into, *inter alia*, the number of clients involved with crypto assets, volume and frequency of crypto transactions, CASPs being used[11] and, distilled from that, types of behaviour.

One can differentiate between four types of client behaviour around crypto assets, ranging from very little to significant exposure to the blockchain:

1. Closed-loop: clients send money from their bank accounts to a CASP and subsequently only buy and sell on that CASP's platform. The crypto assets never leave the platform onto the blockchain (or at least not directly by the client), as trades are matched internally on the platform. The inherit risk of such activity is relatively low.
2. Incoming from chain: crypto transfers are made from (self-hosted[12]) wallets to CASP platforms, then converted and transferred as fiat currency to a bank account. This poses an increased risk, as the source of the funds is not immediately clear.
3. Outgoing to chain: Fiat currency is sent to CASP platforms, whereafter crypto assets are bought and sent to (self-hosted) wallets on the blockchain. The unclear transaction purpose increases risk.
4. Full open-loop: clients are frequently transacting between the blockchain, CASP platforms and banks. These are often advanced users with deeper knowledge of the blockchain and its capabilities. The risk increases as a result of frequent and often complex interactions with the blockchain.

While the majority of clients holding crypto assets may fall within the first category, only trading on a CASP platform and (almost) never interacting with the blockchain directly, banks still must analyse – and keep updated – their client portfolio to ensure that the right risk-based approach is maintained. The extent to which this can be achieved without relying exclusively on information from CASPs is influenced by how banks choose to integrate and participate in the crypto ecosystem.

b. Level of adoption

There are generally three levels of crypto adoption, aside from the option to not participate at all, ranging from (1) a very limited adoption by simply allowing clients to use the bank as a "ramp" to and from CASPs, to (2) providing basic crypto-related services to clients, such as a custodial wallet, to (3) far-fledged adoption, by operating – for example – a platform for buying and selling crypto assets (thus, becoming a CASP), deeply integrated with its regular banking services.

While more far-fledged adoption may sound like a daunting task and undoubtedly requires significant resources upfront, the ability to effectively monitor crypto clients and mitigate crypto-related risks actually increases along with the adoption level, limiting risk exposure and costs down the line (next to having a commercial potential, which is outside of the scope of this article).

11. The CASPs being used can be a significant risk factor and the range of CASPs (and their risks) is broad. From differences in licensing regimes within the EU, to unlicensed CASPs operating de facto illegally within the EU (but still holding a license in a third country), to unregulated CASPs from high-risk or non-cooperative jurisdictions – increasing the risk of serious AML and CFT deficiencies (and thus exposure for the bank).
12. Wallets that are not part of a CASP platform, custodian, etc.

Avoid all crypto

Clients will bank elsewhere if their interaction with crypto assets is severely hampered by the bank. Either the bank loses clients completely or it is only involved at the very end of the financial flow, meaning that there is no visible link to the crypto assets anymore. One could argue that this is an effective risk mitigation strategy, but it is terribly inconvenient for clients, and time has shown repeatedly that looking away is not a particularly advantageous strategy. It also complicates evidencing the source of funds of the clients.

The ramp stage

The "ramp" stage is where most banks that do not fully avoid crypto stand at the moment. Clients may use their bank accounts (via various payment channels) to move funds from and to CASPs, a simple fiat exchange to and from crypto assets (*e.g.*, using a Rabobank account to buy Bitcoin via iDeal at Bitvavo). The bank can only monitor transactions between the client and the CASP of choice. In this scenario, banks could make a risk assessment about the CASPs involved – analysing the reputation, licensing, percentage of tainted transactions, etc. – which may give a very high-level picture of potential client behaviour. Additionally, clients may be asked to send an overview of their transactions at the CASPs, but the challenge is then to verify that information, as statements can currently be easily manipulated (and there is no standardised format to have it automated). Standardisation and collaboration with CASPs would therefore be highly recommended, for example through an API where the client explicitly consents to the sharing of information, although not always realistic. Moreover, looking at blockchain analytics is often not possible at this stage, as simple buy/sell transactions at a CASP often do not end up on the blockchain at all (as also described above under "closed-loop"), making asking for wallet addresses not the first choice either. In case clients do interact with the blockchain through the CASP platform, blockchain analytics can make sense in this scenario and provide insights into source of funds and transaction purposes (see the "incoming from chain", "outgoing to chain" and "full open-loop" types of behaviour above). However, this can only be detected through a prior analysis of the transaction overview (again, keeping in mind that verifying that information is challenging and that there is no certainty that all wallets of the client are being covered).

Basic on-chain services (e.g., custodial wallets)

Moving towards the next level of adoption and starting to offer basic services that "touch" the blockchain, such as custodial services, unlocks the potential to effectively leverage blockchain analytics, by monitoring the activity from and to a custodial wallet (for example), and therewith track the (historical) transactions of clients across the blockchain. The client's behaviour at CASPs is generally not visible, however, as the crypto assets often end up in a collective "hot wallet" of the CASP (and the transactions at the CASP often don't take place on the blockchain, as mentioned before). Nevertheless, it adds an important angle to the profile of the client: a verified wallet, and thus the opportunity to link all past and future transactions with this wallet to a single person, (slowly) building up a crypto client profile. For illustration purposes, such a service / level of adoption could be an add-on to a bank's existing custody or wealth management offerings.

Note that custodial services require a license under MiCAR[13], but there is a simplified "top up" regime for certain financial entities, allowing them to provide crypto asset services via a notification procedure instead of having to obtain an authorisation.[14]

Full-fledged adoption

The final stage of adoption is a full-fledged crypto solution that seamlessly interacts with the main banking services, offering clients a frictionless way to buy, sell and transfer crypto assets.

Transitioning to fully integrated crypto services takes significant time and resources, even though "as-a-service" solutions are available. It does, however, allow significant oversight over the crypto activities of one's clients. The bank monitors the traditional transactions, the ramping to/from crypto and any transactions between various crypto assets on its own platform and the blockchain, allowing it to assess behaviour, volumes, risks, etc. all within its own environment. If implemented well, a client might not even need another CASP anymore. Naturally, a client may still decide to utilise other CASPs, and keep banking services and crypto services strictly separated, but ease of use and a frictionless ecosystem should not be underestimated as factors in this regard, especially not when looking at mainstream adoption. Currently, fully integrated solutions can be found (perhaps unsurprisingly) at neobanks such as Revolut and bunq.

Such full-fledged solutions will consist of one or more of the 10 service categories that require a license under MiCAR[15], but – as mentioned in the previous paragraph – there is a simplified regime for certain financial entities. Specifically, credit institutions (all 10) and investment firms (8 out of 10) may provide many crypto asset services via the notification procedure.[16]

13. Article 3 (1)(16) MiCAR defines the 10 types of crypto asset services that fall within the scope of the licensing regime, which are (in short) (a) custody and administration, (b) trading platforms, (c) exchanges of crypto assets for funds, (d) exchanges of crypto assets for crypto assets, (e) execution of orders, (f) placing, (g) reception and transmission of orders, (h) advice, (i) portfolio management and (j) transfer services.
14. Article 60 MiCAR lays down the types of crypto asset services that may be provided by different financial entities, such as credit institutions, investment firms and electronic money institutions.
15. Article 3(1)(16) MiCAR.
16. Article 60(1) and (3) MiCAR.

4. Crypto-related integrity risks[17]

While the impact and mitigation possibilities of crypto-related integrity risks can be significantly influenced by the actual client portfolio and (desired) level of adoption,– the main types of risks related to crypto assets stay largely unchanged. Hereinafter, a high-level overview of these types is provided, based on known activity, historical volumes and emerging trends. Naturally, this is a non-exhaustive list and risks materialise differently for every regulated entity. Furthermore, not all of these integrity risks are particularly new per se, but often have to be adapted to relevant scenarios and/or may require a different approach to mitigation in the context of crypto.

a. "Old-school" money laundering

One of the most obvious risks concerning crypto currencies is money laundering through the general pattern of placement, layering and integration – using the blockchain technology to legitimise criminal revenues. In this scenario, criminals have accumulated funds in traditional fiat currency and move it onto the blockchain to hide the criminal nature. The weak spot lies with the "ramp", the CASP that is used to exchange fiat currency for crypto assets and vice versa. While significant regulatory efforts have been made (*e.g.*, the aforementioned FATF standards, MiCAR, Travel Rule), many jurisdictions have not yet implemented strong supervision and enforcement of CASPs. Therefore, it is still possible to find a CASP that will onboard a person (acting in bad faith) and accept their inaccurate declaration regarding the source of funds. Once that hurdle is cleared, the crypto assets can be easily moved around internationally and sent to a variety of wallets (the pseudonymous addresses used to send and receive transactions), CASPs and decentralised services (such as decentralised exchanges, bridges and mixers)[18] – obscuring their origins. The use of high-risk CASPs, decentralised services, or the use of privacy coins[19] are all red flags that should be monitored.

b. Creation of crypto assets, coin offerings and token sales

A method of money laundering that is somewhat unique to crypto assets is the creation of a new crypto asset (token) by criminals.

Creating a crypto asset is a matter of minutes, as networks such as Ethereum or Solana provide a sophisticated way to create a new token on their existing and widely available infrastructure. Tokens are created through smart contracts on the network of choice (*e.g.*, Ethereum). They are basically boilerplate contracts written in code, documenting details such as the token's name and ticker symbol, and there are websites that let anyone "fill in" such smart contract without any technical knowledge – not much different from common legal template websites. Execution of the smart contract works by signing and broadcasting it to the blockchain, just like any crypto asset transaction.[20] As long as the code is technically correct and the initial transaction fee is paid, the token is ready for use.

After the crypto asset is created, the criminals will create attention around it so as to increase its value and at some point sell their holdings. While traditionally this behaviour has been seen in "pump and dump" fraud schemes, it is being used increasingly as a modus operandi for money laundering. The original illicit funds can be used to hire programmers, create attention (through ads, bots, etc.) and manipulate the crypto asset. There may not always be a visible link between the original illicit funds and the profits from a seemingly successful crypto asset launch, providing criminals with a solid background story at first sight, when they want to exchange the crypto asset for fiat currency. Thus, profits from significant value increases, especially from newly-launched crypto assets, should be seen as a potential red flag for further investigation.

c. Underground banking

The concept of underground banking is not new, but crypto assets and their underlying infrastructure have made easier to operate, due to its decentralised nature, pseudonymity and borderless operation. Criminals move funds through underground

17. Due to the focus of this article on monitoring (CDD and TM) of banks' clients with crypto assets, the scope of the risks is limited to CDD and TM as well – often labelled as "integrity risk".
18. These are all forms of smart contracts running on the blockchain. A decentralized exchange is a peer-to-peer marketplace where transactions take place directly on the blockchain, without any middleman, through a set of smart contracts that manage liquidity, prices, etc. Decentralised exchanges are not regulated, like their centralized counterparts (i.e., CASPs). Bridges are tools that let one transfer a certain crypto asset from one blockchain to another. For example, a Solana coin can be sent to the Ethereum blockchain through a bridge. The original coin is locked in a smart contract on the Solana blockchain and a Solana token is then issued on the Ethereum blockchain. It is a popular way to increase interoperability between blockchains, but at the same time it can make tracing assets more difficult. Mixers are services that receive transactions from various users and pool them together, before sending them out to the actual beneficiaries. By pooling/mixing the funds and sending them out from this "shared wallet", it becomes increasingly (with more users) unclear which sender belongs to which beneficiary (*e.g.*, time delays are used to mix up the order of transactions). An (in)famous example is Tornado Cash, whose developers have been arrested and convicted (one in the Netherlands).
19. Privacy coin is the definition for a crypto asset with privacy-enhancing features, obscuring traceability. Monero, Zcash and Dash are three of the most prominent ones, using concepts like stealth (one-time) addresses and ring signatures.
20. Cointelegraph has a concise guide to creating a simple token, which is highly recommended so as to try it hands-on and understand the concept better. G. Kaur, 'How to create your first cryptocurrency token: A beginner's guide', *Cointelegraph* 9 July 2025, https://cointelegraph.com/learn/articles/a-step-by-step-beginners-guide-to-creating-your-first-cryptocurrency-token.

bankers, by providing the illicit (cash) funds to the banker, who in turn settles with the underground banker of the receiving party. The illicit funds are never actually wired – the settlement takes place through crypto asset transactions. Underground banking with crypto assets generally falls into two categories. One purely uses the blockchain network as infrastructure, possibly even on a separately created blockchain, to have a reliable, anonymous underground banking ledger – a sole bookkeeping operation, essentially. The other one utilises widely available blockchains and their crypto assets, operating a vast number of wallets, and using decentralised services and loosely regulated CASPs to not only settle in crypto assets, but also to be able to eventually launder and exchange them (using, for example, old-fashioned shell companies). Such underground banking operations are also highly intertwined with cybercrime operators, who are looking for ways to cash out on illegally acquired crypto assets.

d. Cybercrime

Cybercrime has surged over the past decade and there is no end in sight, with generative Artificial Intelligence ("AI") accelerating the trend even further.[21] While cybercrime is to a certain extent a form of fraud, the distinction made here is that cybercrime either has an IT system as a target or involves sophisticated use of IT systems (as means). Forms of cybercrime that are closely intertwined with crypto assets are hacking [22], ransomware and social engineering targeted to acquire crypto assets, with "pig butchering" romance scams emerging as one of the most prominent types. [23] As investigators and crypto compliance experts become better at detecting crypto-related cybercrime early and blocking cash outs to fiat, criminals are also changing their tactics. Instead of attempting fast exchanges from crypto assets to fiat currency, cyber criminals turn to the aforementioned underground crypto bankers, who may provide cash and have complex structures at their disposal, being it on the blockchain or in a more traditional sense with shell companies and trade-based money laundering schemes. The convergence of underground banking and cybercrime is an emerging trend that could take centre stage in the years to come, with both crypto adoption and cybercrime on the rise.[24]

e. Terrorism financing

Terrorism financing is a key concern given blockchain's characteristics. Contrary to typical money laundering, terrorism financing may often involve many payments/donations from a vast number of people, who are willingly or unwillingly contribute to the terrorists' cause. The blockchain makes such donations easy due to its accessibility, international character and perceived anonymity.[25] Terrorist groups can create a wallet in a matter of seconds and instantly share a QR code with its followers, where donations can be received from anywhere in the world. No onboarding procedure, no geographical restrictions. Sympathisers often perceive a donation via crypto assets as an anonymous way to contribute, but that only holds up as long as a wallet cannot be linked to a person.

f. Sanctions evasion

The use of crypto assets to evade sanctions, particularly by countries like North Korea and Russia, has been widely discussed. The US and EU now sanction crypto, targeting both digital wallets and their owners. These wallets can be flagged and extensively monitored in blockchain analytics tooling, so that not only the sanctioned person is in view, but every wallet transacting with it. In terms of modus operandi, sanctions evasion often follows a similar route as more traditional money laundering, exploiting the global, pseudonymous nature of blockchains: finding CASPs with looser controls/oversight, using a vast amount of wallets, and utilising decentralised services such as bridges, mixers and privacy coins to obscure the transaction flow.

All of these risks can significantly impact the financial system and society, so effective mitigation is crucial. While these risks in a traditional context can be mitigated through established strategies, crypto demands and enables new mitigation techniques through blockchain monitoring. The chosen level of adoption largely determines how much monitoring is possible (because of the increased interaction between client and blockchain) and, thus, how well these risks can be mitigated (as previously

21. The volume of cybercrime in 2015 was around 3 trillion USD, while the expectation for 2025 is 10.5 trillion USD. 'How AI-driven fraud challenges the global economy – and ways to combat it', *World Economic Forum* 16 January 2025, https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/.
22. Accumulating to 2.2 billion US dollar in 2024. 'Category deep-dive: $2.2 billion was stolen in crypto-related hacks in 2024', *TRM Labs* 17 March 2025, https://www.trmlabs.com/resources/blog/category-deep-dive-2-2-billion-was-stolen-in-crypto-related-hacks-in-2024.
23. Pig butchering is a sophisticated investment scam, where fraudsters build a relationship with victims over time, gaining their trust, before ultimately defrauding them. The term pig butchering is a methaphor for they in which scammers "fatten up" victims before "slaughtering" them financially. This form of cybercrime has seen a massive uptick in recent years, with massive forced-labour camps in South-East Asia targeting citizens globally. A. McCready & A. Mendelson, 'Exclusive: Inside the Chinese-Run Crime Hubs of Myanmar that Are Conning the World: "We Can Kill You Here"', *South China Morning Post* 22 July 2023, https://pulitzercenter.org/stories/exclusive-inside-chinese-run-crime-hubs-myanmar-are-conning-world-we-can-kill-you-here.
24. Interesting read on an underground banking operation that was closely linked to cybercrime. 'How cryptocurrency is used to move billions of RMB in and out of China', *ThinkChina* 28 February 2025, https://www.thinkchina.sg/economy/how-cryptocurrency-used-move-billions-rmb-and-out-china.
25. 'Crowdfunding for Terrorism Financing', *FATF* October 2023, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

mentioned in paragraph 3(b)).

5. Conventional monitoring

Traditionally, client monitoring has been separated into two processes: customer due diligence on one hand and transaction monitoring on the other.[26] Customer due diligence is initially being performed at client acceptance, typically consisting of identification & verification, PEP and sanction screening, and client profiling questions on, *inter alia*, source of funds and source of wealth. Clients are subsequently given a risk score and reviewed at certain intervals according to their risk score/classification (*e.g.*, annually, bi-annually or every five years). No apparent risk means limited client monitoring.

Transaction monitoring, on the other hand, is a more "dynamic" process, which might provide more timely insights into client behaviour.

In recent years, there has been a shift away from the rather static approach to customer due diligence, not in the least due to regulatory pressure[27], and towards ongoing due diligence, in which certain data points of the client are monitored to trigger customer due diligence. Such data points often relate to personal details of the client, a PEP designation, a possible sanction hit or outcomes of a transaction monitoring investigation. When one of these data points changes, an event driven review is carried out. Periodic customer due diligence is then only needed when no event-driven review has taken place during the defined interval. A positive trend, which leads to a convergence of customer due diligence and transaction monitoring (to some extent), providing a more integrated picture of clients and their behaviour.[28] It is also a mindset necessary for effective monitoring of crypto clients, as the line between customer due diligence and transaction monitoring is per definition blurred and those two processes highly intertwined.

6. Monitoring crypto: risk attribution at arbitrary moments

The main difference between traditional monitoring and monitoring in the crypto space, is that all historical transactions on the blockchain are visible and traceable to a wallet, not only the transactions a client carries out with his or her bank. Banks analyse their clients' transactions and may take action based on that limited view. Conventionally, only the FIU may have a more comprehensive and bank-overarching view of a person's unusual transactions, and only in case they have been reported by multiple financial institutions. On the blockchain, on the contrary, it is possible to investigate all transactions ever carried out, and such investigations are being conducted constantly by regulated entities' crypto analysts, law enforcement agencies and blockchain intelligence companies. As a result of these ever-ongoing investigations and the domino effect along the transaction history, transactions, wallets and consequently clients may only be classified as risky at a later point in time.

To illustrate, person A receives crypto assets in his wallet from person B's wallet on 1 January. Person A moves these crypto assets to a CASP platform and exchanges them for fiat currency. Person A subsequently transfers the fiat currency to his bank account. So far, neither the CASP nor the bank has identified these transactions as risky and they are executed. On 1 March, the US Office of Foreign Assets Control ("OFAC") publishes a list of wallets that are being sanctioned[29], as they are linked to malicious cyber activity. One of the sanctioned wallets is from person C, who frequently transacts with the wallet from person B where the crypto assets of the transaction on 1 January originate from. Thus, through this indirect but clearly visible link, the transaction of 1 January is retrospectively "tainted" and person A might have some relation to the malicious cyber activity. While that original transaction cannot be undone, the involved entities should act on such a designation and potentially investigate (the association of) the client.

Given the full transparency of all transactions on the blockchain, a situation as the one above can quickly become very complex, when the steps/wallets between a client's wallet and a "malicious" wallet increase (*e.g.*, a connection between A and C via B, versus a connection between A and C via B, D and E successively). The extent of the investigation – such as how many wallets deep one will look and how significant the transactions must be - should be determined by regulated entities in accordance with their risk appetite and integrity risk analysis. The risk designations of wallets and transactions range from malicious cyber activity to narcotics trafficking, WMD proliferation, terrorism, transnational organised crime and human rights abuses – and these are just some of the designations used by OFAC.[30] The EU has sanctioned wallets as part of its Rus-

26. For readability purposes, name and transaction screening are not mentioned explicitly, but are touched upon later.
27. A prominent case being the fine for Volksbank N.V. for serious shortcomings in its anti-money laundering controls. 'Fine for de Volksbank N.V. for deficient anti-money laundering controls', *De Nederlandsche Bank* 30 January 2025, https://www.dnb.nl/en/general-news/enforcement-measures-2025/fine-for-de-volksbank-n-v-for-deficient-anti-money-laundering-controls/.
28. This requires, at some point, a shift in the distinction between CDD and TM analysts, but that is a different discussion.
29. OFAC sanctions wallet addresses as part of its well-known SDN list, as explained in OFAC's FAQ. 'Questions on Virtual Currency', *US Office of Foreign Assets Control*, https://ofac.treasury.gov/faqs/topic/1626.
30. OFAC FAQ, question 561. 'Questions on Virtual Currency', *US Office of Foreign Assets Control*, https://ofac.treasury.gov/faqs/topic/1626.

sia sanction packages.[31] And blockchain intelligence providers, such as Chainalysis, Elliptic or TRM Labs have their own designations as well, for example on suspected scams, darknet markets or ransomware.[32]

While the transparency of the blockchain is a great advantage when it comes to monitoring clients and their transactions for money laundering, terrorism financing and other illicit activity, the above shows that it also adds a new layer of complexity. Knowing the client population and its characteristics, as well as deeply understanding the workings of and risks around crypto assets is essential for traditional financial institutions.

7. Conclusion: embracing crypto with clarity and confidence

The rapid mainstream adoption of crypto assets is no longer a question of "if", but "how", and banks stand at a crossroad. Avoiding the shift towards crypto assets is not viable anymore, nor commercially prudent. Instead, banks should embrace a forward-looking vision that recognises crypto assets as an integral part of the evolving financial system. This requires a deep understanding of the integrity risks involved, ranging from more traditional money laundering to sophisticated underground banking, cybercrime and terrorism financing. Setting a clear, well-defined risk appetite, aligned with its vision, is essential. It enables banks to navigate between careful consideration and missed opportunity, and to establish practical thresholds that guide decision-making and operational execution.

Adopting crypto-related services is by no means a one-size-fits-all endeavour. Banks should carefully assess their client portfolios and choose an adoption level that matches their strategic ambitions and risk tolerance – from simply acting as a ramp for CASPs, to providing full-fledged, integrated crypto services. Nevertheless, the technology and momentum are there to step up, and move beyond hesitation and passive approaches. Now is the time to adopt a crypto level of adoption and, with it, a comprehensive (integrity) risk framework – one that balances innovation with integrity, protecting not only the bank, but the broader financial system. In doing so, crypto will be more than just another obligation, enabling banks to position themselves as trusted, responsible stewards in a new era of financial services.

31. Notably, it sanctioned the Russian CASP Garantex in its 16th sanction package. '16th package of sanctions on Russia's war of aggression against Ukraine: EU lists additional 48 individuals and 35 entities', *Council of the European Union* 24 February 2025, https://www.consilium.europa.eu/en/press/press-releases/2025/02/24/16th-package-of-sanctions-on-russia-s-war-of-aggression-against-ukraine-eu-lists-additional-48-individuals-and-35-entities/.

32. A question that is often asked and completely valid, is if one can blindly trust the designation of such intelligence providers and may block transactions/accounts based on these designations. They are neither regulatory bodies, nor law enforcement agencies. I would argue for a differentiated approach, whereby the quality of the providers and the impact on clients is monitored periodically, but that could fuel a whole separate article.

Choice Architecture and Financial Health on Crypto-Asset Service Platforms

Assessing the Effectiveness of EU Regulation in Protecting Investors

D.M. Diederik LL.M.[1]

This article examines the extent to which European Union (EU) regulations protect investors from manipulative choice architecture practices on crypto-asset service platforms (CASPs). The article begins by establishing a foundation in behavioural finance, highlighting how cognitive biases such as familiarity, overconfidence, anchoring and social norming shape investor behaviour. It further demonstrates how these biases can be exploited through choice architecture techniques used by CASPs. Key EU frameworks such as Markets in Crypto-Assets Regulation (MiCAR), Unfair Commercial Practices Directive (UCPD) and the Markets in Financial Instruments Directive II (MiFID II) were assessed for their effectiveness in safeguarding investors. While these regulations establish a solid foundation for achieving transparency, fairness and risk disclosure vis-à-vis retail investors, MiCAR currently lacks extensive judicial interpretation, limiting clarity on enforcement to date. Furthermore, the *Collingridge Dilemma*[2] complicates the regulatory process because intervening too early may stifle innovation, whereas intervening too late reduces the ability to effectively address risks. The article concludes that EU regulations provide an essential baseline for investor protection against harmful choice architecture on CASPs, but their effectiveness ultimately depends on evolving legal interpretations, strong enforcement and closer collaboration between regulators, central banks and CASPs. Effective oversight must strike a balance between protecting investors and fostering innovation in the digital financial sector.

1. Introduction

The COVID-19 pandemic significantly accelerated the adoption of digital technologies across both the public and private industries worldwide.[3] The financial industry was no exception, experiencing rapid digital transformation that introduced both new innovations, opportunities, but also regulatory challenges. The rapid growth of decentralised finance (DeFi) coincided with the height of the pandemic, further accelerating the digital transformation of the financial industry.[4] As the use of CASPs and other digital financial tools expanded, the need for enhanced public and regulatory policy became increasingly evident to ensure investor protection and financial market integrity.[5]

In recent years, investors have increasingly turned to online platforms and advanced digital tools, such as online trading platforms and robo-advisors, to manage their financial decisions. Often influenced and supported by social media figures known as "finfluencers".[6-7] Overall, such tools not only facilitate transactions but also provide access to adver-

1. Delaney Diederik began his career at Promontory Financial Group, an IBM company, where he advised European financial institutions on risk, regulation and technology. He joined ABN AMRO Bank in 2023 as an Advisor on Compliance Risk Policies & Methodologies. The author wrote this article in a personal capacity.
2. The risks of new technologies often emerge only after they are widely adopted, making it challenging to mitigate their potential impacts in advance.
3. IMF, "How Pandemic Accelerated Digital Transformation in Advanced Economies" (*IMF*, March 21, 2023) <www.imf.org/en/Blogs/Articles/2023/03/21/how-pandemic-accelerated-digital-transformation-in-advanced-economies>.
4. Youcef Maouchi, Lanouar Charfeddine and Ghassen El Montasser, "Understanding Digital Bubbles amidst the COVID-19 Pandemic: Evidence from DeFi and NFTs" (2021) 47 Finance Research Letters 102584 <www.sciencedirect.com/science/article/pii/S1544612321005341>.
5. Chainalysis Team, "The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) Region Leads the World in Terms of Global Cryptocurrency Adoption" (*Chainalysis*, October 1, 2024) <www.chainalysis.com/blog/2024-global-crypto-adoption-index/>.
6. ESMA, "Discussion Paper On MiFID II Investor Protection Topics Linked to Digitalisation" (2023) 7 <https://www.esma.europa.eu/sites/default/files/2023-12/ESMA35-43-3682_Discussion_Paper_on_MiFID_II_investor_protection_topics_linked_to_digitalisation.pdf>.
7. European Securities and Markets Authority (ESMA), "Call for Advice to the European Securities and Markets Authority (ESMA) Regarding Certain Aspects Relating to Retail Investor Protection" (2022) 2 <https://www.esma.europa.eu/sites/default/files/library/call_for_advice_to_esma_re-

tising, recommendations and advice, pushing investors to make certain decisions when buying or selling financial products and services. These shifts underscore the growing importance of technology in shaping the financial industry. Furthermore, the design and choice architecture of such platforms play a pivotal role in influencing investor behaviour. These platforms incorporate specific architectures, such as incentives or default settings, which subtly guide user decisions.[8] The design elements of these platforms can significantly shape how investors perceive their options, evaluate risks and ultimately make choices.[9]

Last year, the European Securities and Markets Authority (ESMA) published a paper addressing investor protection issues related to digitalisation, highlighting a range of emerging risks in this evolving landscape.[10] In their February–March 2025 newsletter, this authority once again underscored the risks associated with investing on platforms that leverage, *e.g.* AI to influence or pressure investors. Scientific literature has highlighted the rise of harmful choice architecture on such CASPs, which exploits behavioural biases as a central component of its design.[11] Investors were frequently persuaded to invest in crypto-assets without a clear understanding of the significant risks associated with these investments.[12] In addition, low entry barriers, conveyed trust, social media and the spread of misleading and false information were often used to manipulate consumers into investing in eventually worthless crypto-assets.[13] In this context, frameworks such as MiFID II, Chapter II section 2 and the UCPD Chapter II include provisions ensuring consumer protections in relation to investing or influencing economic behaviours.[14-15] Given the rapid technological advancements, it is essential to assess whether these existing frameworks remain effective and relevant to date. Or whether it requires updates and adjustments to effectively address the challenges and risks posed by unfair practices on some CASPs, manipulative choice architecture and the role of finfluencers.[16]

The main regulation relevant to this article is MiCAR, adopted in 2023.[17] MiCAR seeks to create a harmonised regulatory framework for the issuance, trading and management of crypto assets across EU Member States. MiCAR aims to mitigate risks associated with crypto assets, such as market manipulation, promoting consumer protection and financial stability. MiCAR, the UCPD and MiFID II form the regulatory framework examined in this article, which explores whether the existing legislation sufficiently addresses the evolving intersection of technology, consumer protection and financial market integrity.

2. Behavioural Finance

2.1. Investor decision-making process and psychological biases

Before delving into the concept of choice architecture, it is essential to first establish a foundation in investor decision-making processes and the cognitive biases that can influence individuals even before they commit to an investment. According to Josef Bergt's book on Decentralised Finance Unmasked, behavioural finance examines how psychological factors and systematic biases shape financial decisions, often leading investors away from purely rational choices.[18]

The study of behavioural finance diverges from traditional finance, which assumes individuals always act rationally, by integrating human error into its models, acknowledging that financial market participants often exhibit irrational behaviours influenced by cognitive biases and emotional responses.[19] Individuals do not always act in a purely rational and economic manner, as suggested by the *homo economicus model*. Instead, they rely on heuristics, which are also mental shortcuts and make decisions based on, for example, preferences, beliefs and their ability to process information, particularly when faced with information overload.

In short, behavioural finance provides valuable in-

garding_certain_aspects_relating_to_retail_investor_-protection.pdf>.

8. Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008) 83-100.
9. Nicole Neuss and Verena Zielke, "Nudging the Private Investor - A Systematic Literature Review" (*AIS Electronic Library (AISeL)*) 3 <https://aisel.aisnet.org/pacis2022/270/>.
10. ESMA, "Discussion Paper On MiFID II Investor Protection Topics Linked to Digitalisation" (2023) <https://www.esma.europa.eu/sites/default/files/2023-12/ESMA35-43-3682_Discussion_Paper_on_MiFID_II_investor_protection_topics_linked_to_digitalisation.pdf>.
11. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 161-162.
12. ESMA, "Opening Statement by Steffen Kern, Head of Risk Analysis and Chief Economist, European Securities and Markets Authority (ESMA)" (2022) 4 <https://www.esma.europa.eu/sites/default/files/library/public_statement_to_econ_sk.pdf>.
13. AFM, "AFM Warns against Crypto Pump-and-Dump Schemes" (*©2022 AFM*) <https://www.afm.nl/en/sector/actueel/2024/september/pump-en-dump>.
14. *"Directive - 2014/65 - EN - Mifid Ii - EUR-Lex" <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065>.*
15. *"Directive - 2005/29 - EN - EUR-LEx"* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029>.
16. ESMA, "Public Statement on the Use of Artificial Intelligence (AI) in the Provision of Retail Investment Services" (European Securities and Markets Authority 2024), 4-7, ESMA35-335435667–5924 <https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924__Public_Statement_on_-AI_and_investment_services.pdf>
17. *"Regulation - 2023/1114 - EN - EUR-LEX"* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R1114>.
18. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 48.
19. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 38.

sights into the actual behaviour of investors, recognising the significant influence of cognitive and emotional biases on investment decisions. Understanding these biases offers a more realistic perspective on financial markets and investor actions, moving beyond the assumptions of rationality in traditional finance theories.[20-21] Below are a few cognitive biases relevant to this article.

2.2. Representativeness and familiarity biases

Two cognitive biases significantly influence financial decision-making. Representativeness bias leads investors to judge investments based on superficial similarities or stereotypes, such as equating strong earnings and rapid growth with sound investment quality, which can result in overvalued assets.[22] Familiarity bias causes investors to favour well-known or popular companies, often ignoring potentially better opportunities. Familiarity bias is also referred to as the *momentum effect.* This bias drives choices based on recognition or personal affinity rather than fundamental analysis or strategy, potentially increasing investment risk.[23]

2.3. Cognitive dissonance and overconfidence bias

Cognitive dissonance leads investors to distort memories of past investments, rationalising poor choices as successes and reinforcing biased decision-making.[24] Overconfidence bias arises when investors overestimate their knowledge due to abundant market information, leading to excessive risk-taking, underestimation of uncertainty and overly optimistic forecasts. This effect is amplified by optimism bias, where new information is interpreted as confirming existing beliefs.[25]

2.4. Law of small numbers

Investors often identify patterns in limited or random data and use them to predict future market movements. This overgeneralisation from small samples of data can lead to decisions based on incomplete or misleading information.[26]

2.5. Anchoring and attachment biases

Anchoring occurs when investors fixate on reference points, such as past stock prices or all-time highs, shaping unrealistic expectations, especially in volatile markets like crypto. Attachment bias reflects emotional ties to investments, causing investors to ignore negative signals and hold onto risky positions, often resulting in poor decision-making.[27]

2.6. Social norming

Social interactions heavily influence investment behaviour, often leading to herding and informational cascades where individuals follow others instead of independent analysis. The internet and social media amplify this effect by spreading both insights and misinformation, reinforcing social norming and making popular opinions appear credible. In crypto markets, where traditional financial fundamentals are often absent, valuations are particularly driven by sentiment, online discourse and fear of missing out (FOMO), leaving investors highly susceptible to volatility and impulsive decisions.[28-29]

Investment decisions often vary, as they can be influenced by a range of different parameters. While CASPs can leverage these insights to offer more tailored and effective investment guidance, they may also exploit these cognitive biases to influence investor behaviour for their own benefit. While these biases can be exploited in every business-consumer relationship, the following paragraphs introduce their forms, explore their application and analyse their impact on investor decision-making within CASPs.

3. Choice Architecture

3.1. Different Forms of Choice Architecture

If you directly influence the choices other people make, you are a choice architect – according to Thaler and

20. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 41.
21. Roberto Arturo Agudelo Aguirre and Alberto Antonio Agudelo Aguirre, "Behavioral Finance: Evolution from the Classical Theory and Remarks" (2023), 38, 452-453, Journal of Economic Surveys <onlinelibrary-wiley-com.ezproxy.leidenuniv.nl/doi/epdf/10.1111/joes.12593>.
22. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 41.
23. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 42.
24. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 42.
25. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 43.
26. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 44.
27. Gurdgiev C and O'Loughlin D, "Herding and Anchoring in Cryptocurrency Markets: Investor Reaction to Fear and Uncertainty" (2020), 2. 25 Journal of Behavioral and Experimental Finance 100271<https://www.sciencedirect.com/science/article/abs/pii/S2214635019301534>
28. Josef Bergt, *Decentralized Finance Unmasked* (Nomos 2023) 47-48.
29. AFM, "Observing Online Investment Platforms An Exploratory Study into Guiding Investor Behaviour" (2023) 12 <https://www.afm.nl/~/profmedia/files/publicaties/2023/report-observing-online-investment-platforms.pdf>

Sunstein.[30] Thaler introduced the term choice architecture to describe how principles from behavioural economics can be strategically applied to guide decision-making, shaping choices without altering their objective values. In the context of choice architecture, it is essential to recognise that its influence can be both beneficial and harmful. Introducing small nudges in the decision-making process can serve as a valuable tool to ensure individuals are fully aware of their choices, avoid expected errors and prompt them to reflect more carefully before acting. In many cases, a well-designed nudge can guide individuals towards better financial decisions. However, this article will primarily explore the potential downsides of choice architecture, investigating how certain design strategies on CASPs may influence investor behaviour in ways that could contribute to less optimal financial decision-making.

In 2024, the Dutch Authority of Financial Markets (AFM) published an explanatory study examining the choice architecture used by CASPs. The study analysed how these platforms use choice architecture to influence investor behaviour and identified several key risks.[31] The following paragraph explores how CASPs apply choice architecture and critically examines the associated risks.

3.2. Choice Architecture on CASPs

3.2.1. Easy access to platforms

CASPs design registration to be fast and user-friendly, exposing users to ads that stress profitability, passive income and security, thereby fostering *overconfidence* and a false sense of safety. This positive framing, reinforced by identity checks, lowers scepticism and encourages investment. According to the AFM's study, one platform even promotes the possibility of generating passive income by *"putting crypto to work"*, further enticing new investors. The German Federal Financial Supervisory Authority (BaFin) also warns about this common technique of promoting *"fast money"*.[32] Furthermore, platforms use *referral programs* with financial incentives (15–20% of fees) and pre-generated links, which, combined with social norming, build trust through friend recommendations. These design choices amplify engagement and can push users to invest more frequently and riskier than intended.[33]

3.2.2. Forms of user manipulation during engagement

Investors are guided by vague filters such as *"trending"* or *"popularity"* filters, reinforcing familiarity bias, while default deposit settings (€1,000-2,500) normalise high investments.[34] News sections and push notifications blur the line between information and promotion, shaping decisions through attention bias. Platform design further drives impulsive trading: buy buttons are more prominent than sell, placed for effortless access and highlighted with high-contrast visuals to create urgency. Though some platforms issue warnings or feedback prompts, research shows these are often ignored.[35] Finally, CASPs actively promote *staking* and *lending*, sometimes as default options, encouraging participation without sufficient risk awareness, an especially serious concern for investors who may lack financial literacy.[36]

3.2.3. The role of finfluencers

While social media and the role of finfluencers specifically may not constitute a choice architecture on their own, they play a significant role in the broader investor decision-making process, particularly through social norming (see paragraph 2.6). It is also important to acknowledge the growing influence of this trend in shaping investor behaviour. Research by Krause suggests that this phenomenon has significant downsides, as the potential for biased or inaccurate information can mislead retail and inexperienced investors, leaving them vulnerable to misinformation and, ultimately, leading to financial losses.[37] His study evidence that such influencers often lack formal financial training to understand the associated risks. By using their social media platforms, they target a diverse audience, particularly younger investors who often have lower levels of financial literacy and understanding of risks. High-profile figures have shown the power of social

30. Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008) 83.
31. AFM, "Risks in the Choice Environment of Crypto Apps" (2024) <www.afm.nl/~/profmedia/files/rapporten/2024/verkenning-cryptodienstverleners-en.pdf>.
32. BaFin, "Investment Tips on Social Media: Caution Is Paramount" (BaFin 2022) <www.bafin.de/EN/Verbraucher/Finanzbetrug/Anlagebetrug/Social_Media/social_media_artikel_en.html>.
33. Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008) 97-100.
34. Jon M Jachimowicz and others, "When and Why Defaults Influence Decisions: A Meta-Analysis of Default Effects" (2019) 174-175 Behavioural Public Policy 159-161 <www.cambridge.org/core/journals/behavioural-public-policy/article/when-and-why-defaults-influence-decisions-a-metaanalysis-of-default-effects/67AF6972CFB52698A60B6BD94B70C2C0>.
35. Australian Securities and Investments Commission (ASIC) and Dutch Authority for the Financial Markets (AFM), "Disclosure: Why It Shouldn't Be the Default" (ASIC AFM 2019), 45-48, Report REP 632 <https://download.asic.gov.au/media/5303322/rep632-published-14-october-2019.pdf>
36. European Banking Authority (EBA) and European Securities and Markets Authority (ESMA), "Crypto-Lending: Recent Developments in Crypto-Assets" (2025) report <www.esma.europa.eu/sites/default/files/2025-01/EBA-ESMA_crypto_lending_and_staking.pdf>.
37. David Krause, "The Impact of Financial Influencers on Crypto Markets: Systemic Risks and Regulatory Challenges" (2025) 2-3 Elsevier Inc <papers.ssrn.com/sol3/papers.cfm?abstract_id=5144847>.

media to move crypto markets. In 2021, Elon Musk's posts caused volatility in Dogecoin's price, while in February 2025, Dave Portnoy and Argentinian President Javier Milei were linked to a $LIBRA pump-and-dump scheme that misled investors and caused heavy losses.[38]

3.2.4. Encouraging user retention and engagement

Both within and outside the platform, investors are continuously prompted to act through news updates and push notifications, even when the platform is closed. Push notifications often end with activating texts such as *"view"*, *"discover"* or *"trade now"*. Some notifications also present temporary promotions and prize contents.[39] These frequent notifications are particularly effective in the crypto market, which operates 24/7, unlike traditional stock markets with fixed trading hours. Finally, on all CASPs analysed by the AFM, investors can monitor real-time price fluctuations and access historical trends filtered by different timeframes, such as daily, weekly, monthly, or even hourly data. Filtering options allow users to sort crypto assets by absolute price or percentage change. Percentage changes are prominently displayed using visual cues, such as green for positive returns and red for negative returns, often supplemented by directional arrows to enhance trend recognition. Prior research in investment behaviour indicates that past returns and indications of positive returns are key factors in financial decision-making.[40] This aligns with the concept of anchoring, as discussed in paragraph 2.5. The following paragraph will introduce the relevant EU regulatory framework.

4. EU Regulatory Framework

4.1. Relevant provisions of MiCAR

MiCAR represents the EU's first comprehensive legal framework dedicated specifically to crypto assets. It was designed in response to the sector's rapid growth and the recurring challenges of fraud, market manipulation, pump-and-dump schemes, misleading advertising and inadequate investor protection.[41] It applies to CASPs and sets obligations to ensure transparency, fairness and suitability. Key provisions relevant to this article include Article 6, requiring clear, non-misleading white papers; Articles 7 and 29, mandating fair marketing communications. Recital 24 provides additional context on the dissemination of information, emphasising that advertising messages and marketing materials for crypto assets, including those shared via new channels like social media platforms, must be fair, clear and not misleading. Article 66, obliging CASPs to act honestly, fairly and professionally. The French Financial Supervisory Authority, the Autorité Des Marchés Financiers (AMF), links Article 66 to the obligation of *"good conduct"* by CASPs.[42] And finally, Article 81, requiring MiFID II-like suitability assessments[43] for clients, particularly relevant for robo-advice on CASPs. Guidelines issued by ESMA provide further interpretation of Article 81.[44] When offering advice on crypto-assets, CASPs are required to collect sufficient information to assess a client's ability to understand the nature and risks of the crypto-assets or services being advised. MiCAR builds on MiFID II and the UCPD, reinforcing investor protection, proper disclosure and responsible conduct, including adherence to existing consumer protection laws.

A clear understanding of the roles and responsibilities under MiFID II and MiCAR is crucial, as both serve as key pillars within the EU's financial regulatory landscape. These frameworks are intended to function alongside each other and can often apply concurrently, although in specific instances, one may override the other. Due to their interconnected nature, ESMA has issued supplementary guidance to help determine when crypto assets fall within the definition of financial instruments.[45] While the scope and definitions help determine which regulatory framework applies, the underlying concept of investment advice and suitability remains mostly consistent across both regimes, see Articles 60 and 81 of MiCAR and Articles 24-25 of MiFID II.

38. David Krause, "The Impact of Financial Influencers on Crypto Markets: Systemic Risks and Regulatory Challenges" (2025) 4-8 Elsevier Inc <papers.ssrn.com/sol3/papers.cfm?abstract_id=5144847>.
39. AFM, "Risks in the Choice Environment of Crypto Apps" (2024) <www.afm.nl/~/profmedia/files/rapporten/2024/verkenning-cryptodienstverleners-en.pdf>.
40. Josef Bergt, Decentralized Finance Unmasked (Nomos 2023) 45.
41. *"Regulation - 2023/1114 - EN - EUR-LEX"* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R1114>.
42. AMF, "The European Regulation Markets in Crypto-Assets (MiCA)" (*AMF*, March 19, 2025) <www.amf-france.org/en/news-publications/depth/mica#MiCA_requirements_for_CASPs>.
43. When providing investment advice or portfolio management, the service provider must assess the client's knowledge, experience, financial situation, and risk tolerance to ensure recommendations are suitable, in line with Article 25 of the MiFID II.
44. ESMA, "Guidelines on Certain Aspects of the Suitability Requirements and Format of the Periodic Statement for Portfolio Management Activities under MICA" (European Securities and Markets Authority 2025) ESMA35-1872330276–2031 <https://www.esma.europa.eu/sites/default/files/2025-03/ESMA35-1872330276-2031_-Guidelines_on_suitability_and_periodic_statement_-MiCA.pdf>
45. ESMA, "Guidelines on the Conditions and Criteria for the Qualification of Crypto-Assets as Financial Instruments" (European Securities and Markets Authority 2025) ESMA75453128700-1323 <https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323_-Guidelines_on_the_conditions_and_criteria_for_the_-qualification_of_CAs_as_FIs.pdf>

4.2. Relevant provisions of UCPD

The UCPD aims to uphold a high level of consumer protection by harmonising the rules on unfair commercial practices across the EU. Articles 5–9 define unfair, misleading and aggressive practices, including false claims, omissions of essential information, harassment, undue influence and exploitation of vulnerabilities. In 2022, the *Modernisation Directive* updated the UCPD for digital contexts, adding prohibitions such as fake reviews or misrepresented endorsements, reflecting emerging online risks. The European Commission (EC) also clarified that compensated social media content creators, finfluencers, are considered traders under the UCPD and must provide fair, clear, and non-misleading communications. Together, these provisions aim to protect consumers from manipulative practices, including harmful choice architecture in online environments, while ensuring transparency and accountability.

Paragraph 2 explored how behavioural finance can be manipulated during the investment decision-making process. Paragraph 3 examined how CASPs apply choice architecture and critically assessed the associated risks. Building on this foundation, the following section connects these parts to relevant EU regulatory frameworks explained in this paragraph. It draws on a regulatory study by the AFM, which investigates how CASPs advertise and disclose information under MiCAR, and incorporates insights from the Centre on Regulation in Europe (CERRE), which is one of Europe's leading think tanks in Brussels.

5. An analysis of the EU Regulatory Framework

5.1. MiCAR

In January 2025, the AFM published a study on CASPs, examining their advertising and information disclosure practices. Examining such practices of CASPs directly relates to their use of choice architecture, as these elements shape how information is presented to and perceived by investors and can potentially influence their decision-making behaviour. The study referred to the similar MiCAR Articles as in paragraph 4 of this article and emphasised that CASPs can use this study as a practical tool to meet the requirements set out in MiCAR. The AFM has raised concerns that unfair, unclear or misleading communications and advertisements could compromise investors' ability to make well-informed investment decisions.[46]

The AFM observed that many CASPs' advertisements did not adequately inform investors of the risks associated with investing in crypto assets, despite MiCAR mandating such disclosures and information.[47] While some CASPs provided a reasonably balanced presentation of potential risks and benefits, others failed to do so effectively. Important to note, even when risk warnings were included, they were often placed alongside promotional content, potentially steering consumers toward a more favourable impression and undermining the impact of the actual risk warning. CERRE, calls these instances of placing actual content next to advertising content *"disguised ads"*, which is considered a harmful choice architecture and the advertising content might be perceived as content.[48] Furthermore, AFM articulated that only stating that investing in crypto assets may be risky is not enough; the authority explains that the CASPs need to make clear what the relevant risk is, for example, that the consumer could lose their investment. MiCAR emphasises that clear and accurate information disclosure is essential to safeguarding consumer interests and ensuring that individuals are adequately informed when engaging with CASPs. According to CERRE, withholding or obscuring important information, such as hidden costs or potential losses like the risk of losing one's investment, constitutes a harmful form of choice architecture known as *"sneaking"*.[49]

Finally, the AFM observed that some CASPs' advertisements displayed historical returns based on unrepresentative, overly short time periods. The authority emphasised that when presenting historical or actual returns, these should reflect a representative timeframe to avoid misleading consumers. Here, the CASPs make use of the representativeness bias as described in paragraph 2.2, as they connect certain investments directly to returns. In other words, when investing, you get a direct return. Connecting certain actions and or choices directly to an incentive is also a form of choice architecture, as explained by Thaler and Sunstein.[50]

In conclusion, MiCAR imposes clear transparency obligations on CASPs to ensure that consumers are adequately informed about risks, pricing, costs and fees. It mandates that such information be prominently disclosed on their websites or platforms (Article 66(4)) and requires that all disclosures must be fair, clear, and not misleading (Article 66(2)) – also obligations of *"good conduct"*. The AFM's findings,

46. AFM, "Study into Advertisements and Information Disclosure on Costs by CASPs: Analysis | Report" (The Dutch Authority for the Financial Markets 2025) <https://www.afm.nl/~/profmedia/files/rapporten/2025/study-advertisement-information-casp-en.pdf>
47. AFM, "Study into Advertisements and Information Disclosure on Costs by CASPs: Analysis | Report" (The Dutch Authority for the Financial Markets 2025) <https://www.afm.nl/~/profmedia/files/rapporten/2025/study-advertisement-information-casp-en.pdf>
48. CERRE, "Harmful Online Choice Architecture - CERRE" (*CERRE*, May 28, 2024), 10-11 <cerre.eu/publications/harmful-online-choice-architecture/>.
49. CERRE, "Harmful Online Choice Architecture - CERRE" (*CERRE*, May 28, 2024), 10-11 <cerre.eu/publications/harmful-online-choice-architecture/>.
50. Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008) 83.

combined with this research's focus on behavioural biases and their connection to theories of harmful choice architecture, situated within the EU regulatory framework, underscore instances of non-compliance with MiCAR in this context.

5.2. UCDP

As MiCAR acknowledges and reinforces the continued relevance of the UCPD within the broader regulatory framework for crypto assets, the following paragraphs critically analyse the interaction between these two instruments. It explores the extent to which the UCPD complements MiCAR in addressing unfair commercial practices and enhancing consumer protection, particularly in the context of digital environments and evaluates the continued effectiveness of the UCPD in today's digital landscape. Although the UCPD does not explicitly refer to harmful online choice architecture in its Articles or recitals, the CERRE argues that the Directive's broad, principle-based provisions are sufficiently flexible to encompass and address most forms of such practices.[51] This interpretation is supported by guidance from the Netherlands Authority for Consumers and Markets (ACM).[52] They clarify that consumer protection law, such as the UCPD, provides a framework that permits traders to influence consumer decision-making, as long as this influence remains within lawful and ethical boundaries. As this framework is technologically neutral, it applies consistently across all channels of interaction, whether in physical retail environments, websites or platforms. As a result, CASPs must ensure that their business-to-consumer relationships are fair, transparent and not misleading across all platforms. This is particularly relevant in light of the findings in paragraph 3.2 of this article, which details how some CASPs utilise harmful choice architecture. This article has also linked these practices to behavioural biases. The analysis identifies several potentially problematic design features, such as ease of access to trading interfaces, manipulative interaction patterns, the influence of social media and finfluencers and mechanisms aimed at encouraging user retention and repeated engagement.

While regulatory and academic consensus, including from the AFM, ACM and CERRE, suggests that the UCPD does extend to harmful elements of online choice architecture, there is also broad agreement that significant improvements are needed. In October 2024, the EC conducted a Digital Fairness fitness check of EU consumer protection law, reviewing several Directives, including the UCPD. A key focus of this evaluation was whether existing legal frameworks are adequate to regulate harmful digital practices, given current fragmentation, inconsistencies and the risk of ineffectiveness or unintended negative consequences. This initiative, which is currently subject to a call for evidence running until October this year, may ultimately culminate in a new legislative proposal, referred to as the Digital Fairness Act. Further commentary written in the European Parliamentary paper from January 2025, focused on *Regulating Dark Patterns in the EU: Towards Digital Fairness*, also supports the need for more robust, harmonised consumer protections in digital contexts.[53] The paper underscored that dark patterns take advantage of consumer behaviour bias, while EU consumer legislation assumes that consumers are rational economic actors.

MiCAR establishes a comprehensive regulatory framework for CASPs, embedding essential principles of so-called *"good conduct"*, fairness, transparency and the prevention of misleading practices.[54] By explicitly acknowledging the continued applicability of the UCPD, MiCAR seeks to strengthen consumer protection within the crypto-asset industry. However, in the absence of current judicial interpretation or case law, the practical application and boundaries of these obligations remain uncertain to date. While regulatory guidelines and existing studies provide some direction, additional legal clarity and consistency may emerge through future enforcement actions and jurisprudence. These developments will help define how requirements under MiCAR interact with the UCPD and inform practical application, and indicate whether judicial and regulatory authorities drawn on MiFID II practices when interpreting MiCAR. According to Article 140 of MiCAR, by June 30, 2027, the EC, after consulting the European Banking Authority (EBA) and ESMA, must submit a report to the European Parliament and the Council on how MiCAR has been applied. This report may be accompanied by a legislative proposal if needed. An interim report was also required by June 30, 2025, with the same possibility of proposing legislation. Both reports must include an assessment of fraudulent marketing communications and scams involving crypto assets, particularly those occurring through social media networks. This interim reporting process will offer valuable insights into how supervisory authorities detect and address such fraudulent activities, guiding the development of future regulatory and enforcement frameworks in relation to harmful choice architecture on CASPs.

51. CERRE, "Harmful Online Choice Architecture - CERRE" (*CERRE*, May 28, 2024), 18 <cerre.eu/publications/harmful-online-choice-architecture/>.
52. Netherlands Authority for Consumers & Markets, "Protection of the Online Consumer: Boundaries of Online Persuasion" (2021), 6-7 <https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf>
53. European Parliament, Car P, Filippo Cassetti, and Members' Research Service, "Regulating Dark Patterns in the EU: Towards Digital Fairness" (European Union 2025) report PE 767.191 <https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA(2025)767191_EN.pdf>
54. AMF, "The European Regulation Markets in Crypto-Assets (MiCA)" (*AMF*, March 19, 2025) <www.amf-france.org/en/news-publications/depth/mica#MiCA_requirements_for_CASPs>.

5.3. Regulate or innovate?

While the EU regulatory framework examined in this article may provide adequate legal protections, it remains difficult to accurately predict the future impact of emerging technologies.[55] This challenge is closely related to the *Collenridge Dilemma*, which highlights the tension between the need to regulate technologies early, when potential risks and benefits are still uncertain and the difficulty of anticipating all the consequences of those technologies once they become widely adopted.[56]

There are instances where choice architecture may evolve, where additional layers or features may be introduced that fall outside the scope of existing protections. This raises concerns about the extent to which current safeguards can effectively address future risks that are not yet fully understood. To address this dilemma, it is recommended to apply the *precautionary principle*. This is a strategy that advocates for proactive (regulatory) action in the face of uncertainty. This principle is particularly relevant with crypto-assets and, for example, with AI-driven robo-advice. By prioritising caution, the precautionary principle allows regulators to introduce safeguards early, thereby preventing harm to investors and market integrity before such consequences materialise.[57]

6. Conclusion

The article has examined the intersection of behavioural finance, choice architecture and digital investment platforms, with a particular focus on CASPs in the EU. The article highlights how psychological biases influence investor decision-making and how CASPs leverage choice architecture to enhance user engagement and, in some cases, to further commercial interests at the expense of investor (financial) well-being. The integration of social media dynamics and finfluencers' activities further amplifies these risks, underscoring the need for comprehensive oversight.

While the EU regulatory framework, including MiCAR, UCPD, the Modernisation Directive and MiFID II lays a solid foundation for investor protection against harmful choice architecture on CASPs, several challenges remain. Limited judicial interpretation, potential uneven enforcement of MiCAR across Member States and the rapid evolution of crypto assets may hinder the practical effectiveness of these regulation(s). Additionally, the *Collingridge Dilemma* illustrates the inherent difficulty in anticipating the societal impacts of emerging technologies, complicating regulatory responses.

The findings of this article suggest that, although current regulations promote transparency, fairness and suitability in CASPs, important gaps remain in protecting investors from misleading practices and manipulative choice architectures. Addressing these challenges requires not only effective enforcement and ongoing regulatory adaptation but also a stronger emphasis on investor education to enhance resilience against evolving risks. Equally crucial is collaboration between regulators, such as central banks, CASPs and financial institutions, to ensure that innovation in digital finance develops within a framework that safeguards trust and market integrity.

55. Marianna Capasso, "Responsible Social Robotics and the Dilemma of Control" (2023) 15 International Journal of Social Robotics 1981 <link.springer.com/article/10.1007/s12369-023-01049-2>.
56. Marianna Capasso, "Responsible Social Robotics and the Dilemma of Control" (2023) 15 International Journal of Social Robotics 1981 <link.springer.com/article/10.1007/s12369-023-01049-2>.
57. European Parliament, Didier Bourguignon and European Parliamentary Research Service, "The Precautionary Principle" (2015) report PE 573.876 <www.europarl.europa.eu/RegData/etudes/IDAN/2015/573876/EPRS_IDA(2015>.

Uit de boekenkast van de bedrijfsethiek (95)

prof. dr. E. Karssing[1]

In de bedrijfsethiek is een groot aantal boeken en artikelen verschenen waarin op praktische wijze prangende vraagstukken worden behandeld en concrete aanbevelingen worden gedaan voor het bevorderen van de ethiek en integriteit van organisaties en hun medewerkers. Niet iedereen weet deze publicaties te vinden of heeft tijd ze te lezen. Daarom kijkt Edgar Karssing geregeld voor het *Compliance, Ethics & Sustainability Journal* in de boekenkast van de bedrijfsethiek en bespreekt hij een artikel of boek. Deze bijdragen zijn geen recensies, maar een samenvatting van de belangrijkste conclusies en aanbevelingen van de auteur(s), die hij zal confronteren met zijn eigen observaties als onderzoeker, trainer en adviseur op het gebied van ethiek en integriteit.

In dit nummer bespreek ik de hofnar als bewaker van de (morele) werkelijkheid.

1. Inleiding

Wie houdt de koning een spiegel voor, zodat hij niet aan hoogmoed ten onder gaat? Wie zorgt ervoor dat de koningin met beide voeten op de grond blijft staan? Wie trekt er aan de bel bij dreigend machtsmisbruik? Dat was van oudsher de hofnar. Een wijze dwaas met een lange geschiedenis in vele landen en culturen – van China tot India, van Turkije tot Frankrijk en Engeland – zoals Beatrice Otto laat zien in haar boek *Fools are everywhere. The court jester around the world,* een overzichtsstudie naar wel en wee van de hofnar.[2] De hofnar is bij uitstek degene die de koning de waarheid vertelt, zegt wat anderen denken maar niet durven te zeggen, met een vleugje humor om de pijn te verzachten. Alleen, de koning is tegenwoordig vooral folklore en heeft nog nauwelijks macht. Daarmee dreigt de teloorgang van nut en noodzaak van de hofnar. Otto heeft jaren na de publicatie van haar boek een artikel geschreven met een fascinerende vraag in de titel: *The court jester is universal . . . but is he still relevant?*[3] Jazeker, schreef managementdenker Manfred Kets de Vries 25 jaar eerder in het artikel *The organizational fool. Balancing a leader's hubris.*[4] En dan niet letterlijk als nar aan het koninklijk hof – Willem Alexander, of in de tijd van het artikel: Beatrix, kan gerust zijn – maar bij het management. De CEO is immers de hedendaagse koning of koningin en de overige leden van de Raad van Bestuur of het managementteam de hofhouding. Net als vroeger is de taak van de hofnar om als waarheidszegger en bewaker van de werkelijkheid ('guardian of reality') misstappen te voorkomen. Of, zoals Kets de Vries in onvertaalbaar Engels paradoxaal formuleert, de 'fool prevents the pursuit of foolish actions'.[5] Otto geeft een positief antwoord op haar eigen vraag en formuleert zelfs een personeelsadvertentie voor een hofnar in organisaties; ze benoemt de primaire verantwoordelijkheden en de benodigde competenties. Daarmee krijgen we meer beeld bij de vrolijke joker. Maar tien jaar na de personeelsadvertentie is veel meer materiaal beschikbaar om de rol van de hofnar in te kleuren. Zo heb ik in mijn boekenkast liefst vijf Nederlandstalige boekjes staan die geheel en alleen hierover gaan.

Twee van deze boekjes zijn van de hand van Marco Raad die al jaren werkzaam is als 'hedendaagse hofnar' of ook wel 'ambteNar'.[6] In zijn boekje *De hedendaagse hofnar* benoemt Raad met de ondertitel een belangrijke rol van de hofnar: een spiegel van de waarheid. Oftewel: tegenspraak bieden. Een spiegel met een kwinkslag, geen nar zonder humor. Daarom hanteert Raad als zijn narrenmotto een uitspraak van zijn 11-jarige dochter: 'Geloof nooit de woorden van de Hofnar, maar denk er over na'.[7] Raad is zelf hofnar en in zijn boekjes geeft hij allerlei voorbeelden van wat hij zoal doet, waarbij hij in het boekje *De alledaagse AmbteNar* specifiek kijkt naar zijn avonturen in overheidsorganisaties. Op basis van zijn ervaringen onderscheidt Raad vier rollen die hij koppelt aan de plan-do-check-act-cirkel van Deming: de rationele hofnar (plan), de praktische hofnar (do), de reflectieve hofnar (check) en de creatieve hofnar (act). Op die manier kan de hofnar verschillende soorten problemen aanpakken. De rationele hofnar komt bijvoorbeeld in actie als plannen weinig doordacht zijn, als er sprake is van tunnelvisie. En de creatieve

1. Edgar Karssing is als hoogleraar Filosofie, Beroepsethiek en Integriteitsmanagement verbonden aan Nyenrode Business Universiteit. De auteur dankt Olga Crapels, Wim Lieve en Birgit Snijder-Kuipers voor hun commentaar op het concept van deze bijdrage. Voor reacties en suggesties: e.karssing@nyenrode.nl
2. B. Otto (2001). *Fools are everywhere. The court jester around the world*. University of Chicago Press.
3. B. Otto (2015). 'The court jester is universal... but is he still relevant?'. *Management and Organization Review*, 11(3), 559-573.
4. M. Kets de Vries (1990). 'The organizational fool. Balancing a leader's hubris'. *Human Relations*, 43(8), 751-770.
5. Kets de Vries (1990), ibid.: 757.
6. M. Raad (2008). *De hedendaagse hofnar. Een spiegel van de waarheid*. Uw Hofnar; M. Raad (2024). *De alledaagse AmbteNar. Bespiegelingen uit de praktijk.* Uw Hofnar.
7. Raad (2008), ibid.: 9.

hofnar bij gebrek aan vernieuwing, bij te weinig initiatieven en ideeën: hij laat de organisatie bruisen.

De drie andere boeken zijn geschreven door Juri Hoedemakers, die van de herwaardering van de hofnar in de huidige maatschappij zijn missie heeft gemaakt, er een prijswinnende scriptie over heeft geschreven, hier ook promotieonderzoek naar doet, zichzelf Profnar noemt (afkorting van 'professioneel hofnar'; ja, narren spelen graag met woorden), een hofnarmethode heeft ontwikkeld, opleidingen tot hofnar aanbiedt en een narrengilde heeft opgericht.[8] Zijn eerste klus als hofnar was bij AFAS Software. In Hoedemakers' *Handboek hofnar* schrijft de AFAS-CEO Bas van der Veldt het voorwoord waarin hij aangeeft wat de hofnarren AFAS hebben opgeleverd:

– 'De mensen binnen de organisatie trekken meer hun mond open.
– Het management weet veel beter wat er speelt in het bedrijf.
– Er worden betere beslissingen genomen.
– Medewerkers zijn voelbaar gelukkiger'.[9]

Waar Raad vier rollen voor hofnarren benoemt, maakt Hoedemakers onderscheid tussen maar liefst 16 rollen, zoals entertainer, spion, criticus, zondebok, vertrouweling en flapuit. Net als Raad geeft Hoedemakers ook heel veel voorbeelden hoe hofnargedrag eruit kan zien en beschrijft hij oefeningen om je in de vereiste vaardigheden te bekwamen.

Wat ga ik in deze boekenkast doen? Ik neem de vijf boeken en nog wat andere literatuur als houvast om te snappen wat een hofnar is en doet en waarom we een hofnar zouden willen werven. De nadruk ligt daarbij op de trilogie van Hoedemakers. In paragraaf 2 bespreek ik de belangrijkste rollen en functies van de hofnar. Je zou een hofnar als een geïnstitutionaliseerde functie kunnen zien, maar we kunnen allemaal hofnargedrag vertonen. Dit is het onderwerp van paragraaf 3: wat is hofnargedrag, hoe kunnen we het oefenen, en wat zijn voorwaarden waaronder dit gedrag ook effectief kan zijn? In de slotparagraaf bespreek ik wat dit betekent voor compliance & ethics professionals: Mogen zij ook hofnar zijn? Kunnen zij ook hofnargedrag vertonen?

2. Hofnar: rollen en functies

Het is geen toeval dat ik deze 'boekenkast' schrijf na mijn tweeluik over macht en machtsmisbruik. Ik had daarin macht heel neutraal neergezet als de mogelijkheid om iets voor elkaar te krijgen: er is niks mis met machtsGEbruik. Maar zeker wel met machtsMISbruik. En ik besprak de machtsparadox die aangeeft dat het hebben van macht zomaar tot machtsmisbruik kan leiden doordat macht corrumpeert, bijvoorbeeld doordat je nauwelijks nog corrigerende negatieve gevolgen ondervindt van eventueel wangedrag. Omdat het in mijn aard zit niet alleen over problemen na te denken, maar ook meteen over praktische oplossingen, kwam de hofnar bijna als vanzelf in beeld als waarheidszegger tegen machthebbers. Het zou mooi zijn als het zo werkt: de nar houdt bij dreigend grensoverschrijdend gedrag de koning met een kwinkslag een spiegel voor waardoor deze machthebber schrikt en afziet van machtsmisbruik. En ze leefden nog lang en gelukkig. Maar dat geloof ik dus niet: ik heb nu allemaal hele nare machtsmisbruikers voor ogen en kan me niet voorstellen dat die zich laten corrigeren door de fratsen van de hofnar; ik vrees vooral voor de gezondheid van onze vrolijke dwaas. Een paradoxale uitdaging: 'the masters most likely to benefit from the jester role are those less likely to welcome the jester's messages'.[10] Mijn conclusie: een hofnar kan pas effectief zijn indien de koning(in) bereid is om te reflecteren, om te leren, om zichzelf te ontwikkelen.

Wat mij bijzonder aanspreekt in de aanpak van Hoedemakers is dat hij zijn pleidooi voor het revitaliseren van de hofnar begint met nut en noodzaak van reflectie. Mensen zijn feilbare wezens; ook managers, ook de leiders van organisaties, zijn mensen. En met hun mens-zijn komen alle menselijke, o zo menselijke tekortkomingen.[11] Mensen maken fouten. Wat helpt, is reflecteren. Hoedemakers geeft aan dat structureel reflecteren veel voordelen heeft: 'Door reflectie vergroot je je beroepsbekwaamheid, kun je de behoeften van jouw mensen en doelgroepen beter vervullen, betere ethische en morele afwegingen maken, wensdenken tegengaan en jezelf als instrument inzetten om anderen te helpen. En als kers op de taart kun je je kernkwaliteiten gaan benutten en krijg je (nog) meer zelfvertrouwen'.[12] Kortom, door te reflecteren kun je werken aan een betere versie van jezelf. En aan een betere versie van de organisatie. Reflecteren betekent letterlijk het terugkaatsen van een beeld; je kunt ook zeggen: spiegelen. Het grote probleem van reflecteren in je eentje is dat je jouw eigen blinde vlekken niet ziet. Per definitie, want daarom is het een blinde vlek. En dan is het fijn dat er een hofnar is die jou de spiegel voorhoudt en daarmee jou op jouw blinde vlekken wijst. Een hofnar is op die manier een belangrijke hulpbron bij reflecteren.

Als gezegd, Hoedemakers onderscheidt liefst 16 rollen die een hofnar zou kunnen spelen. Hij werkt ze in zijn boeken stuk voor stuk uit als afzonderlijke rollen, al geeft hij ook meteen aan dat ze in de praktijk door elkaar heen kunnen lopen en dat de hof-

8. J. Hoedemakers (2021). *Gezocht: Hofnar. Reflectie voor leiders en leidinggevenden*. Haystack; J. Hoedemakers (2023). *Handboek hofnar. Doorbreek machtspatronen en wensdenken door je organisatie een spiegel voor te houden*. Lev.; J. Hoedemakers en L. Nijgh (2023). *Reflecteren met de hofnar*. Boom.
9. Hoedemakers (2023), ibid.: 11.
10. S. Clegg et al. (2022). 'Speaking truth to power: The academic as jester stimulating management learning'. *Management Learning*, 53(3), 547-565: 551; vgl. M. Kets de Vries (2018). *Trump: A tragi-comedy*. INSEAD Working Paper No. 2018/22/EFE.
11. Hoedemakers (2023), ibid.: 18.
12. Hoedemakers (2023), ibid.: 23.

nar soms heel snel tussen verschillende rollen moet schakelen.[13] Ik vind 16 teveel om te kunnen onthouden, daarom beperk ik me hieronder tot de rollen waarvan ik vermoed dat ze het meest functioneel zijn als hulpmiddel bij reflectie.[14] Daarbij neem ik steeds twee rollen als duo, rollen die Hoedemakers dus expliciet uit elkaar trekt.

- De entertainer en satiricus
- De vertrouweling en vriend
- De coach en adviseur
- De criticus en flapuit

De entertainer en satiricus

Een hofnar moet natuurlijk in de eerste plaats de koning(in) amuseren. 'Het entertainment van de hofnar was zeer divers. Het kon bestaan uit muziek maken, zingen, dansen, lachen, grappen maken, gekke bewegingen maken, sonates en ballades zingen, honen en bektrekken, dwergworstelen, imiteren, boeren en scheten laten, omkeringen, scheelkijken, poëzie opvoeren, jongleren, dichten, poppenshows opvoeren, magische trucs tonen, boogschieten en mesgooien'.[15] Maar het gaat niet alleen om entertainment, dan kun je net zo goed een clown of een goochelaar inhuren. Uiteindelijk is de humor, het vermaak, altijd slechts een hulpmiddel om de koning(in) een spiegel voor te houden.[16] Satire is komische overdrijving, je ziet het vaak in spotprenten en cabaret. Hoedemakers legt uit hoe satire iets heel anders is dan sarcasme. Sarcasme bespot en veracht, bijvoorbeeld als belediging verpakt als compliment, en doet mensen pijn. Satire is echter een vorm van constructieve kritiek met humor die mensen laat lachen maar dus tegelijkertijd wel wijst op dwalingen en zwakheden.[17]

Oefening spotprent

'De essentie van een spotprent is out of the box kunnen denken, situaties op een andere manier kunnen benaderen, vaak op basis van karikatuur, oftewel: komische overdrijving'.
-Maak een karikatuur van jouw organisatie (huidige situatie).
- Licht je karikatuur toe in twee minuten.[18]

De vertrouweling en vriend

Een hofnar is loyaal, hij heeft geen eigen agenda, geen ambities, en is daardoor geen bedreiging voor de koning(in). Dat maakt de hofnar bijzonder geschikt als klankbord. De koning(in) kan erop vertrouwen dat de hofnar niet (ver)oordeelt en geen misbruik maakt van informatie die (nog) geheim moet blijven. De hofnar als vertrouweling is als een soort dagboek waaraan je alles kan vertellen zonder dat je wordt uitgelachen of jouw intiemste gedachten worden doorverteld. Hoedemakers beschreef deze rol in zijn scriptie, vanuit de theorie, en vreesde dat het in de praktijk knap lastig zou zijn om als profnar die vertrouweling te worden: 'Het tegenovergestelde bleek waar te zijn. In werkelijkheid krijg ik een hoop inside-information van mensen: over scheidingen, affaires, vreemdgaan, sollicitaties, zelfs zelfdodingsgedachten ... Als vertrouweling heb je een uitdagende en verantwoordelijke rol, en man, soms brengt het flink wat ethische vraagstukken met zich mee'.[19] Dat kan ik me voorstellen. En dat roept meteen de vraag op in welke mate compliance & ethics professionals een hofnar kunnen zijn. Daar kom ik in de slotparagraaf op terug. De door Hoedemakers geïnterviewde zorgbestuurders hadden niet echt behoefte aan een hofnar als beste vriend. Dat komt wellicht door de associaties die dit woord oproept. Wat mij betreft liggen vertrouweling en vriend heel dicht bij elkaar, zeker als je ziet dat Hoedemakers in zijn uitwerking aangeeft dat de koning(in) bij de hofnar zichzelf kan zijn, politieke correctheid even kan laten zijn voor wat het is en zich niet bedreigd hoeft te voelen. Tevens, een belangrijk kenmerk van een goede vriend is dat hij het beste met je voor heeft. En dat is een wezenskernmerk van de hofnar: positieve intenties staan voorop, de hofnar wil de ander helpen door op een leuke manier die ander iets te leren.[20] De hofnar werkt altijd in het belang van de koning(in). Als een echte vriend.

De coach en adviseur

De hofnar is er ter lering ende vermaak. Daarom springen deze twee rollen bij de hofnar als hulpmiddel bij reflectie er meteen bovenuit. Als coach is de hofnar een spiegel, een spiegel die zelf niks weet maar de koning(in) laat 'zien', waar hij of zij dan zelf iets mee moet doen. De hofnar als coach leert je dus eigenlijk niks nieuws: 'Een hofnar laat je iets zien en of jij daarvan wilt leren, dat is uiteindelijk aan jou. Al is het eigenlijk wel de bedoeling, of vooral verstandig voor jezelf, dat je er wat mee doet. Maar van de hofnar moet niks'.[21] De hofnar helpt als coach bij nadenken en betere beslissingen nemen, maar de mening van de wijze dwaas zelf is niet interessant. De hofnar kan natuurlijk wel degelijk ook advies geven. En omdat de hofnar geheel belangeloos is – geen eigen agenda heeft – hoeft de koning(in) niet bang te zijn voor dubbele bodems of politieke spelletjes. Maar... er is natuurlijk een maar... Hoedemakers herhaalt in eigen woorden het narrenmotto van Raad: 'Geloof nooit de woorden van de Hofnar, maar denk er over na'.[22] Oftewel, je moet als koning(in) het advies niet klakkeloos overnemen, maar er wel over nadenken. Overigens, een belangrijke eigenschap van

13. Hoedemakers (2023), ibid.: 24.
14. Voor zijn scriptieonderzoek heeft Hoedemakers 20 zorgbestuurders geïnterviewd over de manier waarop zij hun reflectief vermogen versterken en welke rol hofnarren daarbij zouden kunnen spelen. De antwoorden die zij gaven op de specifieke behoefte aan de 16 verschillende rollen heb ik hierbij meegenomen – ik had de vraag eerst ook aan mezelf gesteld en kwam tot min of meer dezelfde uitkomst. Om deze scriptie te downloaden: thesis.eur.nl/pub/54074/Juri-Hoedemakers.pdf
15. Hoedemakers (2021), ibid.: 68.
16. Otto (2015), ibid.: 567.
17. Hoedemakers (2023), ibid.: 101.
19. Hoedemakers (2023), ibid.: 72-73.
20. Hoedemakers (2021), ibid.: 168.
21. Hoedemakers (2023), ibid.: 169.
22. Hoedemakers (2023), ibid.: 56.

een hofnar is dat hij met iedereen op de werkvloer communiceert (en wellicht ook nog met mensen buiten de organisatie). Dat betekent dat hij de wijsheid van de werkvloer in zijn adviezen meeneemt: 'Als de hofnar advies geeft, doet hij dat niet voor zichzelf, zoals de gemiddelde organisatieadviseur doet, maar namens alle medewerkers … De hofnar zorgt ervoor dat ook degenen die zich normaal gesproken minder snel uitspreken een stem krijgen … Dit is van groot belang voor een baas die een leider wil zijn voor iedereen'.[23]

De criticus en flapuit

De hofnar als criticus corrigeert en bekritiseert de koning(in); oftewel, als in de inleiding aangegeven, zegt wat anderen denken maar niet durven te zeggen, met een vleugje humor om de pijn te verzachten. Dit belichaamt het meest de hofnar als waarheidszegger. Daarvoor kan de hofnar zijn gehele gereedschapskist inzetten, van woordspelingen tot sonates en ballades zingen en honen en bektrekken. In de volgende paragraaf bespreek ik verschillende vormen van hofnargedrag. Zo kan de hofnar als flapuit met zijn hart op de tong zeggen wat hij denkt. Omdat soms choqueren de enige manier is om mensen bewust te maken van hun gedrag.[24] Hoedemakers geeft wel aan dat je ook de flapuit-rol met wijsheid moet invullen: 'Onthoud dat het belangrijk is om respectvol te zijn en de gevoelens van anderen in acht te nemen. Het doel is niet om jezelf volledig te censureren, maar om je bewust te zijn van de impact van je woorden en om meer controle te hebben over je impulsieve reacties'.[25]

Denk eerst na voordat je er iets uitflapt
'Voordat je iets zegt, neem je een moment om na te denken over de gevolgen van je woorden. Vraag jezelf af of je opmerking gepast is, of die anderen kan kwetsen of ongemakkelijk kan maken, en of het nodig is om te zeggen wat je in gedachten hebt'.[26]

Hiermee heb ik acht van de 16 rollen die Hoedemakers uitwerkt kort beschreven. Ze zijn allemaal ondersteunend aan de reflectie van de koning(in). De overige rollen vind ik op hun beurt ondersteunend aan deze acht rollen of nevenschikkend aan de primaire functie van helpen bij reflectie. Bij ondersteunend horen de hofnar als spion, de hofnar als waarnemer (vanuit helicopterview observeren wat er aan de hand is) en de hofnar als allesweter (met iedereen praten en overal vragen stellen) waardoor de hofnar meer inzicht heeft in het reilen en zeilen van de organisatie en daardoor beter kan spiegelen, beter advies en kritiek kan geven. Nevenschikkend zijn de hofnar als zondebok (iemand die je de schuld kunt geven voor zaken die zijn misgegaan), de hofnar als onderhandelaar (als zaakwaarnemer van de koning), de hofnar als sfeerbewaarder (tussen koning(in) en hofhouding), de hofnar als buffer tussen koningin en volk en de hofnar als statussymbool (hoe meer hofnarren, hoe belangrijker de koning(in)).

3. Hofnargedrag

'"Maar het oor van vorsten verafschuwt de waarheid", zal men zeggen, "en ze gaan wijzen uit de weg precies omdat ze bang zijn dat er eentje te vrij wordt en iets durft te zeggen dat meer waar dan aangenaam is." Inderdaad, vorsten verfoeien de waarheid, maar toch pakt dat voor mijn gekken heel goed uit, want hun waarheden en zelfs hun openlijke beledigingen worden met plezier aangehoord. Daardoor wekt dezelfde uitspraak die een halsmisdrijf zou zijn als hij uit de mond van een wijze kwam ongelooflijk veel plezier op als hij van een zot komt. De waarheid heeft namelijk een soort authentiek vermogen om te plezieren, zolang er niets krenkends bij zit. Maar dat vermogen hebben de goden alleen aan gekken verleend'.[27]

Aldus Erasmus in zijn *Lof der Zotheid*. Dit boek als hoogtepunt van hofnargedrag mag natuurlijk niet ontbreken in een bespreking van de hofnar. Erasmus (±1466-1536), de grote humanist waarnaar de universiteit in Rotterdam is genoemd, verschuilt zich in zijn maatschappijkritiek achter de godin Zotheid. Zij houdt een lofrede op zichzelf. Door deze literaire 'truc' kon Erasmus legitiem ongemakkelijke waarheden benoemen, een zot heeft immers een mandaat om met humor pijnlijke dwaasheden te verwoorden. In het citaat vertelt de godin waarom hofnarren een belangrijke functie hebben. Erasmus is zelf geen hofnar, maar maakt wel gebruik van hofnargedrag. En dat kunnen we allemaal. Ook wie niet de ambitie heeft om hofnar te worden, kan gebruik maken van hofnargedrag. Door kennis te nemen van de gereedschapskist van de hofnar en door oefening je te bekwamen in de methoden en technieken van de hofnar, zoals 'humor, mensenkennis, feedback geven, verhalen vertellen, de juiste vragen stellen, creativiteit, enthousiasme en vooral heel veel lef'.[28] Het goede nieuws is dat Raad en Hoedemakers niet alleen rollen en functies van de hofnar beschrijven, maar ook heel veel oefeningen meegeven waarmee je zelf aan de slag kunt. In het *Handboek hofnar* staan bijvoorbeeld oefeningen om actief luisteren en samenvatten te trainen, of empathie tonen. Er zijn oefeningen hoe je een positieve sfeer kunt creëren en behouden en hoe je goed kunt kijken. Of hoe je satirische stukken kunt schrijven en hoe je een leven lang kunt blijven leren (met liefst tien verschillende oefeningen).

Ga goed kijken: wat zie je nu echt?
'Hoe kun je oordeelloos kijken? Oefen daar eens mee. Door echt te omschrijven wat je ziet, zonder daar een oordeel aan te hangen. Dus op het moment dat iemand met de armen over elkaar gaat zitten, vraag je niet "waarom sluit je je nu af?"

23. Hoedemakers (2023), ibid.: 57.
24. Hoedemakers (2023), ibid.: 163.
25. Hoedemakers (2023), ibid.: 165.
27. Erasmus, geciteerd in Hoedemakers en Nijgh (2023), ibid.: 90.
28. G. Vergouw (2015). 'De hofnar'. in: *Het dodo-effect. Over gedragsverandering in organisaties.* Boom/Nelissen: 26.

of "waarom heb je nu opeens een gesloten houding?", maar benoem je het eens gewoon zonder in te vullen. Vraag: "Waarom ga je nu met je armen over elkaar zitten?" Probeer dit eens en zie hoe verrassend de antwoorden kunnen zijn. Benoem wat je ziet en niet wat je dénkt te zien'.[29]

Hoedemakers heeft reeds in zijn eerste boek, G*ezocht: hofnar*, de managementboekversie van zijn scriptie, de hofnar uitdrukkelijk gekoppeld aan nut en noodzaak van reflectie en de rol die een hofnar – of hofnargedrag – hierbij zou kunnen spelen. Hij maakt onderscheid tussen twee manieren van reflecteren: actief en passief. Bij actieve reflectie doe je het helemaal zelf, alleen. Goed geschikt voor mensen die zich bewust zijn van hun blinde vlekken. Bij passieve reflectie maak je gebruik van een derde, bijvoorbeeld een hofnar. Dit is beter geschikt voor de mensen die hun blinde vlekken nog niet hebben ontdekt, waarschijnlijk de meeste mensen... Hoedemakers heeft op basis van bestaande reflectiemodellen eigen modellen gemaakt. Voor actieve reflectie is dit de Koningscirkel, voor passieve reflectie de Hofnarcirkel. Bij deze laatste is expliciet ruimte ingebouwd voor feedback vragen aan een derde, waarbij overigens ook het hele proces met een derde kan worden doorlopen. Hoedemakers nieuwste boek, *Reflecteren met de hofnar*, geschreven samen met Lida Nijgh, is een prettige verdieping en verbreding en geeft verdere praktische uitwerking van die reflectiemodellen en met name de daarbij passende vaardigheden. 'Hofnarren' wordt een werkwoord, het boek is geen handboek voor de hofnar, maar een lesboek voor hofnargedrag. Doelgroep is het hoger onderwijs, waar reflecteren steeds meer aandacht krijgt. Vaak tot verdriet van studenten, die helemaal gek worden van al die verplichte reflectieopdrachten die hen weinig brengen.[30] Of vooral aanzet tot rumineren, tot piekeren, waarbij je blijft hangen in nutteloze denkprocessen.[31] Dan kun je ermee stoppen – want het levert weinig op – of je kunt de manier van reflecteren verbeteren. Met de hofnarmethode wordt een nieuwe manier van reflecteren geïntroduceerd die wél aantrekkelijk is om mee aan de slag te gaan. Het boek is geschreven met heel veel voorbeelden en kleine oefeningen, er is een 'online leeromgeving' met nog veel meer oefeningen, testjes en video's met achtergrondmateriaal. Wat mij betreft ook zeer geschikt voor leren op de werkvloer. Bij reflecteren hebben we de ogen van de ander nodig.[32] De grote vraag wordt dan: wie is jouw hofnar, wie zijn jouw hofnarren? En voor wie mag jij een hofnar zijn?

Hoedemakers en Nijgh geven aan dat 'hofnarren' als werkwoord veel beter klinkt dan 'reflecteren'?[33] Daar ben ik het mee eens. Ze geven ook aan wat nodig is om succesvol te hofnarren, zoals:

– Benoem dat je de hofnar mag spelen, hiermee wordt officieel uitgesproken dat je de ander mag helpen.
– Zorg voor voldoende onafhankelijkheid, de hofnar mag geen belang bij de te bespreken casus hebben.
– Zorg voor een vertrouwde sfeer waarin alles gezegd mag worden zonder dat jullie daarbij boos worden op elkaar.
– Neem geen blad voor de mond. Zeg gewoon wat er in je opkomt, dat is ook je rol en daarbij moet je je niet inhouden.
– Een compliment is ook feedback. De hofnar is er niet alleen om kritiek te geven, ook positieve feedback draagt bij aan zelfinzicht.
– En, cruciaal, zorg dat jullie allebei weten dat alles wordt gezegd en geroepen met positieve intenties en om ervan te leren, hoe hard sommige zaken ook zullen klinken.[34]

We zeggen het niet om je te pesten

'Vroeger zeiden mijn ouders altijd: "We zeggen het niet om je te pesten, maar voor je eigen bestwil." En ik verplicht me om aan dat zinnetje te denken als iemand onaangenaam tegen mij doet. Ik ga altijd op zoek naar de les die diegene mij probeert te geven. Als je die intentie hebt – en ik geef toe dat het bij mij een jaar of tien heeft geduurd voordat ik dat kon – word je bijna nooit meer boos'.[35]

Belangrijk bij reflecteren – bij hofnarren als werkwoord – is je blik verbreden door vanuit verschillende brillen naar een kwestie te kijken. Hiervoor kun je heel goed de 16 rollen van de hofnar gebruiken. In het boek *Reflecteren met de hofnar* hebben Hoedemakers en Nijgh steeds een vraag per rol geformuleerd die een net andere zienswijze biedt om de situatie te doorgronden.

1. *Entertainer*: Hoe kun je de situatie grappig benaderen?
2. *Satiricus*: Hoe kun je de spot drijven met de situatie?
3. *Vertrouweling*: Hoe zorg je voor voldoende vertrouwen?
4. *Beste vriend*: Wat zou je zeggen binnen een intieme relatie?
5. *Coach*: Hoe kun je coachen richting een goed resultaat?
6. *Adviseur*: Wat zou jij als adviseur zeggen?
7. *Criticus*: Wat zou je zeggen als je heel kritisch bent?
8. *Flapuit*: Wat zou je zeggen zonder van te voren na te denken?
9. *Spion*: Welke zaken kun je blootleggen door middel van spionage?
10. *Waarnemer*: Wat zie je als je in een helikopter erboven gaat hangen?
11. *Allesweter*: In hoeverre hebben we alle informatie die we moeten hebben?
12. *Zondebok*: Wat kan er allemaal misgaan?

30. Zie ook T. Luken (2011). 'Zin en onzin van reflectie'. *Supervisie en coaching*, 28(4), 153-166.
31. Hoedemakers en Nijgh (2023), ibid.: 64.
32. Hoedemakers en Nijgh (2023), ibid.: 60.
33. Hoedemakers en Nijgh (2023), ibid.: 111.
34. Hoedemakers en Nijgh (2023), ibid.: 122-123.

13. *Onderhandelaar*: Tussen wie moet er onderhandeld worden?
14. *Sfeerbewaarder*: Hoe kun je de sfeer leuk houden?
15. *Buffer*: Waar zijn de partijen waartussen bemiddeld moet worden?
16. *Statussymbool*: Voor welke uitkomst zouden wij een trofee ontvangen?[36]

Volgens de auteurs kun je met het zestien-verschillende-kanten-principe iedere situatie aan.[37]

Complimentenwisselbeker
Iedere week krijgt een medewerker (digitaal) de wisselbeker toegespeeld. Wie? Dat is geheim! De medewerker met de beker geeft de hele week complimenten aan de overige collega's. Het valt natuurlijk op als alleen degene met de beker complimenten geeft. Het is daarom wel zo handig als andere collega's ook af en toe een compliment uitdelen, om het spannend te maken. Aan het einde van de week is het de bedoeling dat alle collega's raden wie de complimentenwisselbeker in bezit heeft. Degene die het raadt, mag de wisselbeker in het geheim aan de volgende overhandigen.[38]

4. Tot slot

Vergouw noemt de hofnar de verpersoonlijking van de tegenspraak: 'Hierdoor is hij uitstekend geschikt om tegenwicht te bieden aan (aankomende) zonnekoningen, groepsdenken en conformisme'.[39] Hoedemakers haalt geregeld woorden van Otto aan: de hofnar is een 'outsider on the inside' die kan zeggen 'what no insider can get away with'.[40] Oftewel, de hofnar biedt het perspectief van een buitenstaander, terwijl hij binnen is.[41] En dat is fijn voor de koning(in), die zo vaak vooral wordt omringd door ja-knikkers die niet echt kritisch meedenken, waardoor de koning(in) kan gaan geloven in de eigen onfeilbaarheid. Door de hofnar 'werd het overpeinzend vermogen van de koning vergroot, aangezien de hofnar hem aanleiding gaf om zaken vanuit een andere gezichtshoek te beschouwen, zijn eigen beslissingen in twijfel te trekken en oorbaar te zijn voor andere wegen. Deze raadgevingen haalden de koning uit zijn ingesloten wereld en toonden hem dat er ook andere benaderingen mogelijk waren'.[42] De koning(in) vandaag de dag is folklore, maar we kunnen op de werkvloer allemaal een hofnar gebruiken, en zeker het management. In een enquête bij *i4talent* gaven medewerkers aan dat door het aanstellen van een hofnar onder andere de volgende veranderingen merkbaar zijn in de organisatie: het waarom wordt meer uitgelegd, men komt nu zelf met onderbouwde voorstellen, er is meer verbinding gemaakt (tussen mensen en afdelingen), er is een positieve sfeer, er is meer openheid, er is meer een team-gevoel, duidelijkheid zorgt voor meer onderlinge rust.[43]

Hoeveel hofnarren kan een organisatie aan?

Vergouw geeft aan dat het eigenlijk een slecht signaal is dat een hofnar nodig is om de top te bereiken, omdat het aangeeft dat blijkbaar niemand nog de nek durft uit te steken: 'Een hofnar is een teken dat tegenspraak en andere meningen nauwelijks meer worden geduld'.[44] Ik snap wat hij bedoelt. Maar, zonder al te somber te zijn, we leven helaas niet in een ideale wereld, dus organisaties waarin iedereen overal altijd alles kan zeggen zullen er niet veel zijn. De manier waarop Raad en Hoedemakers invulling geven aan de hofnar spreekt mij aan: ze krijgen een natuurlijke plek bij het reflecteren door feilbare mensen, mensen met blinde vlekken die ook wel eens een denkfoutje maken. Wij allemaal dus. Dan kun je maar beter narren om je heen verzamelen dan ja-knikkers. En als het aanstellen van een hofnar te ver gaat, dan toch zeker collega's uitnodigen tot hofnargedrag. Interessant is om nog eens verder na te denken over hoeveel hofnarren een organisatie aankan. Vergouw meent dat teveel hofnarren leidt tot chaos: 'Anders denken en afwijkend gedrag zijn wenselijk, maar een teveel ervan leidt tot anarchie en chaos. Er is binnen organisaties slechts beperkt ruimte voor hofnarren en andersdenkenden'.[45] Ik vermoed dat hetzelfde geldt voor hofnargedrag.

Het mandaat van de hofnar

Het geheim van de hofnar of van 'officieel' hofnargedrag is dat de feedbackgever een expliciet mandaat heeft om als waarheidszegger een spiegel op te houden. En dat is hard nodig, want mensen houden er niet van om kritiek te krijgen of slecht nieuws te vertellen. 'We willen koste wat het kost gezichtsverlies voorkomen, voor onszelf én voor de ander. We willen empathisch overkomen en de goede relatie in stand houden. En dat betekent dat we liever onze mond houden en niet zo snel feedback geven. De hofnarmethode helpt om deze terughoudend los te laten. Als je in de schoenen van de hofnar stapt, dan stap je in een rol. Die rol geeft je de ruimte en veiligheid om te zeggen wat je wilt. Daar hebben jullie immers afspraken over gemaakt. Je kunt je dus letterlijk verschuilen achter de rol van de hofnar'.[46] Kun je dan echt alles zeggen? Nee, zoals eerder aangegeven, het tweede geheim van het succes van de hofnar is dat de hofnar altijd en alleen werkt in het belang van de 'koning(in)', hem/haar/hen probeert verder te helpen. Zolang dat de grondhouding van de hofnar of hofnar-partner is, en de koning(in) dat weet, dan

36. Hoedemakers en Nijgh (2023), ibid.: 124. In de verschillende boeken zijn er accentverschillen in de benaming van de 16 rollen. Ik heb hier en hierboven steeds de benaming gekozen die mij het meeste aanspreekt, ik heb de volgorde van de 16 vragen aangepast aan de volgorde waarin ik hierboven de 16 rollen heb besproken.
37. Hoedemakers en Nijgh (2023), ibid.: 123.
39. Vergouw (2015), ibid.: 32.
40. Otto (2015), ibid.: 568.
41. Hoedemakers (2023), ibid.: 78.
42. Hoedemakers (2023), ibid.: 64.
43. Hoedemakers en Nijgh (2023), ibid.: 148.
44. Vergouw (2015), ibid.: 32.
45. Vergouw (2015), ibid.: 32.
46. Hoedemakers en Nijgh (2023), ibid.: 126.

mag het knetteren, maar altijd vol liefde gericht op het werken aan een betere versie van jezelf en de organisatie.

De houdbaarheid van de hofnar

Hoedemakers geeft aan dat een hofnar een beperkte houdbaarheid heeft.[47] Dat geldt voor een officieel aangestelde hofnar, maar dat geldt ook voor de hofnar-partner die jou ondersteunt bij jouw persoonlijke reflectie. De frisse blik verdwijnt… waardoor de hofnar niet meer alert is op afwijkende zaken. De hofnar wordt bedrijfsblind, steeds meer een 'insider on the inside'. Ook moet je oppassen voor sleur. 'Voorkom dat reflecteren (met je hofnar) een verplicht nummer wordt. Als je altijd op hetzelfde moment, op dezelfde plaats en op dezelfde manier reflecteert dan ontstaat er een routine en dat komt je reflectie niet ten goede. Zorg voor afwisseling'.[48]

Compliance & ethics professionals als hofnar

In de vorige paragraaf stelde ik de vragen: wie is jouw hofnar, wie zijn jouw hofnarren? En voor wie mag jij een hofnar zijn? Dat roept vervolgvragen op die reeds waren aangekondigd: Mogen compliance & ethics professionals ook hofnar zijn? Kunnen zij ook hofnargedrag vertonen? Natuurlijk kunnen compliance & ethics professionals ook hofnargedrag vertonen. Het kan ze wellicht zelfs effectiever maken. Ik ken helaas geen onderzoek hiernaar, maar er is wel onderzoek gedaan naar hofnargedrag van HR professionals. En in *AuditMagazine* is aandacht besteed aan de auditor als hofnar. Dit betreft staffuncties die verwant zijn aan compliance & ethics. Ik bespreek de verschillende artikelen als inspiratiebron.

HR als moderne hofnarren

Anna Sender en Hannah Mormann beschrijven de resultaten van hun onderzoek in een artikel met een titel die leest als de samenvatting: *It takes a fool to remain sane: how and when HR executives use jesting techniques to trickle up paradoxical tensions.*[49] Net als compliance & ethics professionals hebben HR-managers te maken met spanningsvelden ('paradoxical tensions') tussen bijvoorbeeld sociale en zakelijke belangen (zoals bij HR het welzijn van medewerkers versus aandeelhouderswaarde). In gesprek met het topmanagement moeten HR-managers deze spanningsvelden bespreekbaar maken. Maar HR staat in de gemiddelde organisatie niet bovenaan in de pikorde, dus hoe zorg je ervoor dat je voldoende aandacht krijgt? Sender en Mormann hebben dit onderzocht in interviews door de hofnar als uitgangspunt te nemen: maken HR-managers gebruik van hofnargedrag en is dit effectief? Dat levert tweemaal een 'ja' op, en vele voorbeelden hoe HR-managers met humor en een kwinkslag belangrijke zaken bespreekbaar maken.

Auditors als moderne hofnarren

Een andere aan compliance & ethics professionals verwante beroepsbeoefenaar is de auditor. In 2022 schreef Marianne Boerman in *AuditMagazine* een mooi artikel over de hofnar, met een warm pleidooi voor hofnargedrag door auditors: 'Een nar is iemand die op zo'n manier zegt dat je naar de hel kunt lopen dat je je verheugt op het reisje. Door de joker in te zetten wordt de auditor iemand die moedig en oneerbiedig kan, mag en moet zeggen wat hij wil. Ook tegen de heersende opvattingen in. Iemand die simpele maar doordringende vragen vol humor stelt en die een confronterende spiegel voorhoudt zodat de leider (of in ons geval de auditee) zichzelf niet al te serieus neemt. Tegenspraak geven en spiegelen van de werkelijkheid wordt dragelijk door humor'.[50]

In 2024 had *AuditMagazine* zelfs een special over de hofnar.[51] In verschillende interviews en artikelen werd de vraag gesteld of een auditor een hofnar kan zijn. Bij lezing krijg ik een positief gevoel over de compliance & ethics professional als hofnar. Maar het is natuurlijk vooral belangrijk dat compliance & ethics professionals zichzelf hier senang bij voelen. Daarom nodig ik de verschillende afdelingen waar ze werkzaam zijn uit om eens met elkaar te bespreken: in hoeverre kunnen en willen wij hofnar zijn, in welke mate willen en kunnen we hofnargedrag laten zien? Hoe draagt dat bij aan onze effectiviteit? Als voer voor het gesprek geef ik een aantal citaten als een kort overzicht van antwoorden, van onder andere de ons nu bekende Hoedemakers en Raad; bij *AuditMagazine* mocht ook ChatGPT een artikel schrijven en zijn er drie auditors geïnterviewd:

- 'De hofnaraanpak maakt het mogelijk om auditbevindingen op een manier te presenteren die het management echt helpt, waardoor ze deze bevindingen beter accepteren en sneller implementeren. Uiteindelijk leidt dat tot een effectievere organisatie, en dat is uiteraard het doel'.[52]
- 'Ik denk dat beiden het vak uitoefenen om de organisatie beter te maken door kritische vragen te stellen en door de organisatie een spiegel voor te houden. Alleen is mijn gevoel dat een internal auditor meer op de inhoud zit. Een hofnar zit iets meer op de zaken eromheen, de verpakking, de cultuur. De internal auditor is echt intern, die kent de organisatie en denkt in de kleuren van het bedrijf. Een hofnar is toch meer een outsider on the inside'.[53]

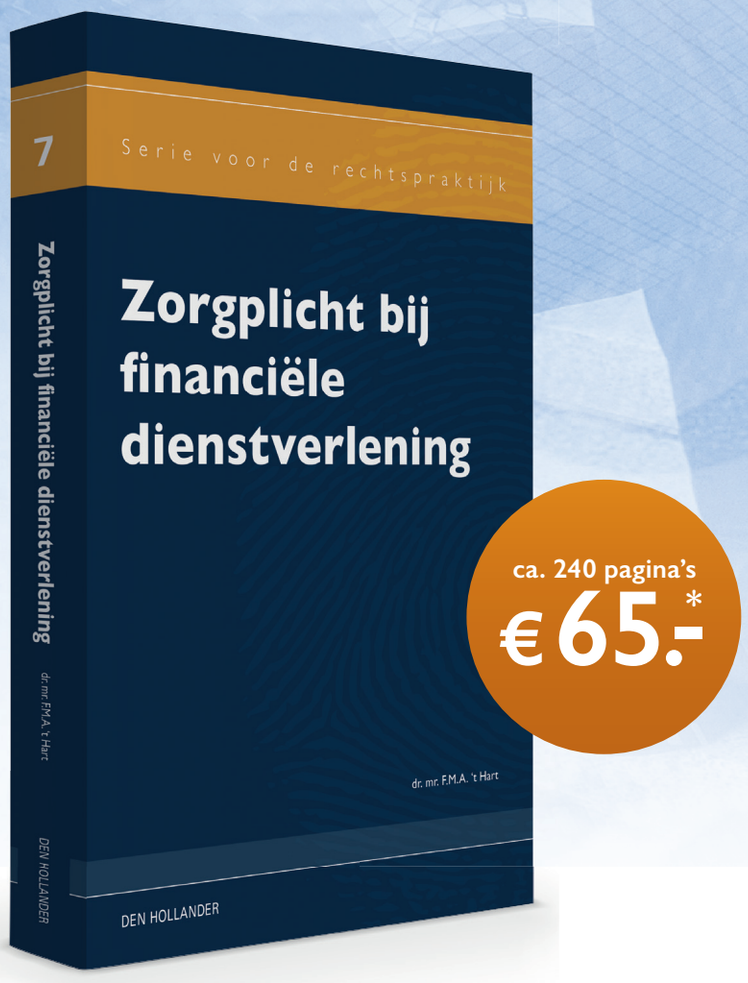
47. Hoedemakers en Nijgh (2023), ibid.: 133-134.
48. Hoedemakers en Nijgh (2023), ibid.: 134.
49. Sender, A., & Mormann, H. (2025). 'It takes a fool to remain sane: how and when HR executives use jesting techniques to trickle up paradoxical tensions'. *Journal of Management Inquiry*, 34(2), 186-202. Ik kwam op dit artikel door een kort hofnarliteratuuroverzicht: S. Peij, R. Renes, en P. Bezemer (2024). 'Bijblijven. Heeft u al een chief clown officer?', *Goed Bestuur &Toezicht*, 4, 52-55.
50. auditmagazine.nl/artikelen/auditor-zet-de-joker-in/
51. Zoek op auditmagazine.nl op 'hofnar'.
52. Interview met Roland Gelauff, voormalig hoofd Internal Audit en nu head of Finance van AkzoNobel. auditmagazine.nl/interviews/waarom-roland-gelauff-zichzelf-liever-hofnar-dan-politieagent-noemt/
53. Interview met Hoedemakers. auditmagazine.nl/interviews/de-hofnar-terug-van-weggeweest/

– 'Een internal auditor kan volgens mij best iets van de hofnar overnemen in het werk, zoals de boodschap verpakken op een manier die het gewenste effect geeft. Of dat nu met een grap, een provocatie of in een andere creatieve vorm gebeurt, het kan allemaal helpen de boodschap goed over te brengen'.[54]
– 'De hedendaagse internal auditor begrijpt dat het opbouwen van relaties en het communiceren met empathie en begrip net zo belangrijk zijn als de cijfers en bevindingen zelf. Het vermogen om op een constructieve manier kritiek te leveren, helpt bij het implementeren van veranderingen en het verbeteren van processen'.[55]
– 'De vraag is of een hofnar in een moderne wereld nog wel een plek heeft. Want een auditor is een zorgvuldig opererend mens die werkt met normenkaders, controlewerkprogramma's, oordelenstelsels en formele rapportages. Een hofnar is volgens mij per definitie out of the box. Je kunt dus de vraag stellen of een auditor en een hofnar niet per definitie zaken zijn die tegengesteld zijn aan elkaar. Wat een auditor natuurlijk wel moet doen, is daar waar het nodig is out-of-the-box denken, opereren en oordelen. Dus ad hoc inspelen op een situatie. Hofnargedrag past niet van nature bij een auditor, maar kan de toegevoegde waarde van de auditor aanzienlijk vergroten'.[56]
– 'De afgelopen tien jaar heb ik gezien dat de traditionele auditor zich niet altijd prettig voelt bij wat een rol als hofnar van ze vraagt. Als je het hebt over "de auditor van nu", verandert het verhaal. Deze moderne auditor voelt zich vaak comfortabeler in de rol van een gelijkwaardige gesprekspartner met wie bestuurders constructieve gesprekken kunnen voeren. Dergelijke auditors zijn beter in staat om de rol van hofnar op zich te nemen. Daarentegen voelt een meer traditionele auditor, die gewend is aan de structuur en formele aanpak die inherent is aan ons vak, zich mogelijk minder op zijn gemak in deze rol met de bijbehorende interventies'.[57]

Ter afsluiting

In zijn boekje *De alledaagse ambteNar* geeft Raad 16 narrenregels. De laatste is voor iedereen wijs, maar zeker ook voor narren: kijk zelf ook in de spiegel. Maar de allermooiste vind ik nummer 13, zo mooi dat ik er deze 'boekenkast' mee afrond: 'Leef je eerst in en daarna pas uit. Dan komt je kritische advies goed aan'.[58]

54. Interview met Raad. auditmagazine.nl/interviews/humor-eerlijkheid-lef-en-doen/
55. Antwoord van ChatGPT. auditmagazine.nl/columns/de-hofnar-en-de-internal-auditor/
56. Interview met Dirk Willem Huizinga, CAE bij de Volksbank. auditmagazine.nl/interviews/out-of-the-box-gestructureerd/
57. Interview met Erwin Engels, hoofd Internal Audit bij de Tilburg University. auditmagazine.nl/interviews/met-gestrekt-been-objectief-blijven/
58. Raad (2024), ibid.: 44.



ca. 240 pagina's

€ 65.-*

In dit boek treft u een bundeling van publicaties en annotaties die betrekking hebben op de zorgplicht die op financiële ondernemingen rust. Deze zorgplicht bepaalt in toenemende mate het verdienmodel van financiële ondernemingen nu de zorgplicht steeds verdergaande eisen stelt aan de (kwaliteit) van de dienstverlening aan (zowel particuliere als zakelijke) klanten.

Deze zorgplicht komt in vier fasen naar voren. Iedere fase wordt in deze uitgave beschreven.

De eerste fase bestaat uit de productontwikkelingsfase. Dit is wellicht de meest cruciale fase aangezien in deze fase de productenkenmerken, wijze van distributie en de wijze waarop het product aan het publiek wordt gepresenteerd, wordt bepaald.

De tweede fase ziet op de distributie van het financieel product. De distributie dient aan te sluiten op de aard en complexiteit van het product en de doelgroep waarvoor het product is bestemd.

De derde fase ziet op de communicatie met de klant zowel in de precontractuele fase als gedurende de looptijd (de zogenaamde nazorg).

De vierde en laatste fase betreft de wijze waarop toezichthouders de naleving van de publiekrechtelijke gedragsregels (informeel) handhaven. Daarbij is van belang dat toezichthouders in de praktijk verlangen dat financiële ondernemingen bepaald gedrag tonen dat door hen als wenselijk wordt beschouwd maar niet per definitie wettelijk voorgeschreven is. Ook daarmee dienen financiële ondernemingen rekening te houden.

Dit boek beoogt niet een uitputtend maar wel een breed en opiniërend beeld te geven van de ontwikkeling van de zorgplicht en actuele thema's op dat gebied.

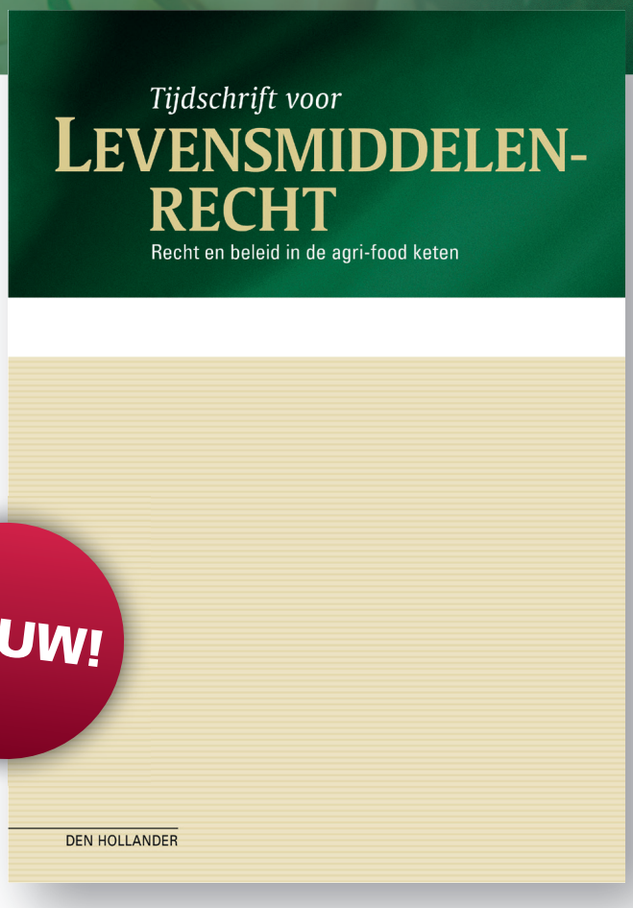
Redactie:
Dr. mr. F.M.A 't Hart

* De genoemde prijs is exclusief btw, exclusief verzendkosten en onder voorbehoud van wijzigingen.
ISBN: 978-90-77847-114
Bestellen via de website https://denhollander.info.

DEN HOLLANDER

Postbus 325 | 7400 AH Deventer | T 0570 - 75 12 25
info@denhollander.info | **https://denhollander.info**

Tijdschrift voor Levensmiddelenrecht



Het Tijdschrift voor Levensmiddelenrecht (TvL) is een onmisbaar tijdschrift voor professionals die op de hoogte willen blijven van belangrijke ontwikkelingen op dit rechtsgebied en zich willen bekwamen in hoe recht en beleid inwerken op de agri-food keten.

Het tijdschrift is een belangrijke bron van informatie voor degenen die zich bezighouden met regulatory affairs binnen de voedselindustrie, beleidsmakers en toezichthouders of consultants, advocaten, rechterlijkemacht en wetenschap.

NIEUW!

Een greep uit de onderwerpen die in TvL aan de orde komen:

- Marktordeningsrecht en mededingingsrecht gericht op de (beleids)praktijk,
- Voedselzekerheid en -veiligheid,
- Handel in levensmiddelen en veiligheidsstandaarden op nationaal en mondiaal niveau,
- Controle en handhaving door de overheid,
- Hoe bevoegdheden van de toezichthouders zich verhouden tot de verantwoordelijkheden van de levensmiddelenexploitant,
- Europese integratie en nationale regelgeving,
- De juridische positie van levensmiddelenproducenten en -exploitanten,
- Etikettering, claims, novel foods en duurzaamheid, toelating van pesticiden, diergeneesmiddelen en marktordening. Maar ook vraagstukken over begrenzing, zoals het onderscheid tussen levens- en geneesmiddelen en de praktische betekenis van het voorzorgsbeginsel,
- Duurzaamheid en de Green Deal,
- Levensmiddelenrecht in de praktijk en welke lessen die daaruit kunnen worden getrokken,
- Voedselveiligheidscrises en de (juridische) gevolgen daarvan.

Zie voor abonnement mogelijkheden: https://denhollander.info/

Het Tijdschrift inclusief archief is eveneens digitaal te raadplegen via content integrators Legal Intelligence en Rechtsorde BV.

Abonnement
U kunt zich abonneren via de website:
https://denhollander.info/

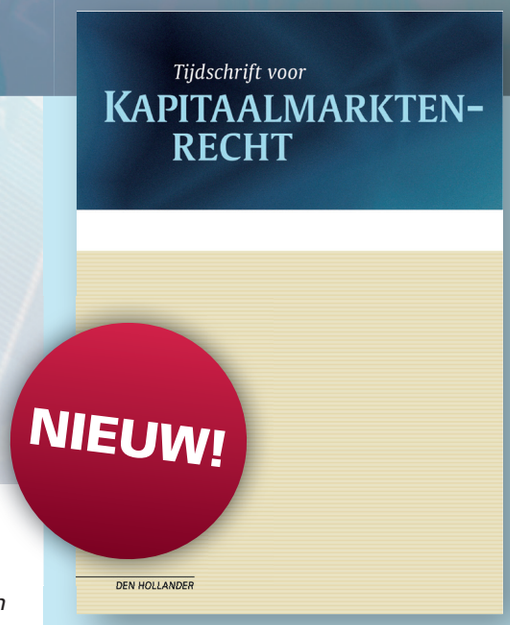
DEN HOLLANDER

Boomkampsweg 1 • 7245 WC Laren • info@denhollander.info • www.denhollander.info

Tijdschrift voor Kapitaalmarktenrecht

Het Tijdschrift voor Kapitaalmarktenrecht (KMR) bevat voor de rechtspraktijk relevante artikelen, annotaties en korte opiniërende columns.

KMR richt zich als eerste Nederlandse tijdschrift uitsluitend op kapitaalmarktenrecht:
(i) publiekrechtelijke regulering van kapitaalmarkten (financieel toezichtrecht); en
(ii) civielrechtelijke onderwerpen met betrekking tot kapitaalmarkten



Voor wie

- Bedrijfsjuristen (met name bij beursgenoteerde ondernemingen)
- Wetgevingsjuristen
- Advocatuur
- Financiële instellingen waaronder:
  - *Banken*
  - *Beleggingsondernemingen*
  - *Handelsplatformen*
  - *Beleggingsanalisten*
  - *Credit Rating Agencies*
  - *ESG Rating Providers*
  - *Benchmark Administrators*
  - *Proxy Advisers*
  - *Clearinginstellingen & CCP's*
  - *Custodians*
- Toezichthouders
- (Register-) Accountants
- Universiteiten

Inhoud

Het focusgebied van KMR valt uiteen in de volgende hoofd- en subcategorieën:

- Algemeen
  - *Kapitaalmarktunie*
  - *Economische ratio & doelstellingen toezichtregels*
  - *Regelgeving- en toezichtstructuur*
  - *Transactietypen (zoals aandelen-emissies, obligatie-emissies, beursgang, securitisations)*
  - *Financiële instrumenten*
  - *Duurzaamheid (ESG)*
  - *Digitalisering*
- Openbaarmaking informatie
  - *Prospectus*
  - *Periodieke publicatieverplichtingen*
  - *Openbaarmaking voorwetenschap*
  - *Melding zeggenschap*
- Handel & afwikkeling
  - *Handelsplatformen*
  - *Handelsregels (inclusief transparantieregels en handelsverplichtingen)*
  - *Short Selling*
  - *Algoritmische handel & HFT*
  - *Clearing & Settlement*
- Markmisbruik
  - Handel met voorwetenschap
  - Marktmanipulatie
- Tussenpersonen & gatekeepers
  - *Beleggingsondernemingen*
  - *Beleggingsanalisten*
  - *Credit Rating Agencies*
  - *ESG Rating Providers*
  - *Benchmark Administrators*
  - *Proxy Advisers*
  - *Clearinginstellingen & CCP's*
  - *Custodians*
- Civielrechtelijke aspecten
  - *Contractuele en vennootschappelijke aspecten financiële instrumenten*
  - *Administratie & bewaring effecten*
  - *Giraal effectenverkeer*
  - *Aansprakelijkheidsvraagstukken*
  - *Civielrechtelijke gevolgen overtreding toezichtrecht*

Meer informatie: https://denhollander.info/kapitaalmarktenrecht

DEN HOLLANDER

info@denhollander.info • www.denhollander.info