INSTITUTE FOR LAW AND REGULATION OF DIGITALISATION

MEDİPOL UNV-ANKARA ANKARA MEDİPOL ÜNİVERSİTESİ

Möslein / Polat (Eds.)

Investor Protection in Crypto-Asset Markets

Workshop Report

Virtual Workshop

10 October 2024

Organized as part of the project

"Protection of Investor and Consumer on Online Platforms"

Funded by the

Scientific and Technological Research Council of Türkiye

TÜBİTAK ARDEB

December 2024

About the Project

The workshop is organized within the scope of the project titled as "Protection of Investor and Consumer on Online Platforms" (Project No: 123K086). The project is led by Asst. Prof. Dr. Cemre Polat (Ankara Medipol University) under the supervision of Prof. Dr. Florian Möslein (the Philipps University of Marburg). The project team includes four other researchers: Salih Tayfun İnce (Ph.D. candidate at the Philipps University of Marburg), Elif Akıncı (Ph.D. candidate at Hacı Bayram Veli University), Aybüke Keskin (Ph.D. candidate at İstanbul University) and Ali Burak Kırkbaş (LL.M. candidate at Ankara University of Social Sciences). This two-year-project (September 2023 – September 2025) has received funding from the Scientific and Technological Research Council of Türkiye within the scope of 3501 – Career Development Program.

Table of Contents

Foreword

This report, born out of the workshop titled "Investor Protection in Crypto-Asset Markets", represents a collective effort to address some of the most pressing questions in this evolving domain. Jointly organized by the Philipps University of Marburg and Ankara Medipol University, the workshop convened experts from Türkiye, the European Union, and the United States to explore diverse regulatory frameworks and their implications for investor protection.

By facilitating a comparative analysis across different jurisdictions, the workshop hopefully contributed to advancing the understanding of investor protection in the context of crypto-assets. As crypto-assets continue to reshape the global financial landscape, their growing prevalence presented new challenges for both regulators and investors. Lawmakers have already acted in this respect. Especially the EU has showed an unusual speed to adopt MiCAR. As one of the world's largest crypto ecosystems, the US market offers valuable lessons. Türkiye, in particular, has emerged as one of the world's most active markets for crypto-assets. With an estimated 10 million users engaging in crypto trading, Türkiye ranks among the top in global adoption rates.

Alongside the rapid growth, there are substantial risks, as it is almost always the case. Market volatility, regulatory uncertainty, and the potential for fraud and security breaches all pose serious threats to investors. Notably, some scandals[1] underscored the need for stronger oversight and regulation to safeguard users and restore confidence in the market.

It is our hope that this report will contribute meaningfully to the ongoing discourse, inspiring further exploration and collaboration in shaping the future of this dynamic field.

Prof. Dr. Florian Möslein

Dr. Cemre Polat

[1] 'Thodex Cryptocurrency Boss Jailed for 11,196 Years in Türkiye for Fraud' (8 September 2023) <https://www.bbc.com/news/world-europe-66752785> accessed 17 November 2024.

Crypto-Asset Regulation in the European Union - Prof. Dr. Florian Möslein[2]

Reported by Aybüke Keskin

Prof. Dr. Florian Möslein discussed the evolving framework of crypto-asset regulation within the European Union, with a focus on the newly introduced Regulation on Markets in Crypto-Assets (MiCAR) [3]. He emphasized that investor protection is a key element not only for safeguarding individuals but also for enhancing market stability and confidence. Möslein, further compared MiCAR with other financial regulatory frameworks, such as Markets in Financial Instruments Directive (MiFID II)[4], the Prospectus Regulation[5] and the Market Abuse Regulation (MAR)[6], highlighting the complexities and overlaps between these regulations. He concluded by addressing how MiCAR balances the need for strong investor protection while ensuring the efficient functioning of the crypto-asset market.

Overview

The topic of investor protection within the EU has increasingly centered on the newly introduced MiCAR, which is now widely recognized across legal and financial sectors. However, considering that today's event specifically focuses on investor protection, the introduction will take an unconventional approach. Instead of delving directly into MiCAR itself, it will initially refer to an image that might seem unrelated to law, but one that many German corporate and capital markets lawyers often contemplate when addressing investor protection: an image rooted in physics, that is, communicating tubes, which some may recall from school-level physics.

---

[2] Florian Möslein is a professor of law at the Philipps University of Marburg, specializing in German civil law, German and European business law, and digitalization law. He holds an LL.M. from University College London and a Ph.D. from the University of Hamburg. He serves as co-director of the Institute for Law and Regulation of Digitalization and vice director of the Hessian Center for Responsible Digitality. His research includes corporate law, banking law, European law, and legal theory, with notable publications such as "Robots in the Boardroom: Artificial Intelligence and Corporate Law.

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

[4] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU

[5] Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the pu blic or admitted to trading on a regulated market, and repealing Directive 2003/71/EC

[6] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 200

It holds particular significance because it illustrates the foundational ideas articulated by Klaus Hopt, the founding father of German capital markets law, in his habilitation writing. In his seminal work[7], one of the Hopt's main argument was that investor protection in capital markets is not an aim in itself but it relates to the market stability. His analogy of communicating tubes highlights this relationship: if more water is added to the investor protection tube, the level of market stability simultaneously increases.

This insight leads to the conclusion that markets where investors are well-protected tend to enjoy greater trust and confidence from participants, which in turn results in increased stability and efficiency. Therefore, investor protection is not only about safeguarding individual investors —who may lack sufficient understanding or face particular vulnerabilities— but also about achieving broader objectives, such as ensuring the smooth functioning of capital markets.

This principle is not confined to traditional capital markets law but is also directly applicable to crypto market regulation. A closer examination of MiCAR reveals that investor protection is frequently mentioned in connection with market stability and

[7] Hopt KJ, *Der Kapitalanlegerschutz im Recht der Banken: gesellschafts-, bank- und börsenrechtliche Anforderungen an das Beratungs- und Verwaltungsverhalten der Kreditinstitute* (Beck 1975) (Partially at the same time: Munich, Univ., Habilation Writing, 1973, with the title: Hopt, Klaus J.: Anlegerschutz beim Wertpapiergeschäft der Kreditinstitute)

efficiency. The regulation's title itself underscores its dual focus: MiCAR is not merely about protecting individual investors but also about regulating the broader crypto-asset market to prevent systemic dysfunctions. However, a thorough review of MiCAR is essential to determine whether it provides a balanced approach or if it may be overly stringent in its attempt to protect investors.

In this context, it is helpful to compare the MiCAR with more traditional financial regulatory frameworks, such as the MiFID II, the Prospectus Regulation, and the MAR.

Outline of Regulatory Content

MiCAR is an extensive regulation that covers a broad range of crypto-assets. It begins with a general section that applies to most crypto-assets, followed by Title II, which outlines the specific rules applicable to the majority of crypto-assets. Titles III and IV focus on certain categories of tokens, namely asset-referenced tokens and e-money tokens. In addition, the regulation includes provisions concerning the prevention of market abuse (Title VI) as well as the administrative framework, competent authorities, and transitional rules.

Title 1: Subject matter, scope of application and definitions (Art. 1-3)
Title 2: Crypto assets other than asset-backed tokens or e-money tokens (Art. 4-15)
Title 3: Asset-referenced tokens (Art. 16-47)
Title 4: E-money tokens (Art. 48-58)
Title 5: Authorization and conditions for the exercise of the activity of a provider of crypto-asset services (Art. 59-85)
Title 6: Prevention and prohibition of market abuse in connection with crypto-assets (Art. 86-92)
Title 7: Competent authorities, the EBA and ESMA (Art. 93-139)
Title 8: Transitional and final provisions (Art. 140-149)

One critical consideration is the placement of the MiCAR in the broader framework of financial market law. MiCAR, in many respects, draws heavily from existing legislation, particularly traditional securities regulation and capital market legislation, though it is not a mere duplication. As it is similar but not identical, it is vital to have a clear line between crypto-assets regulation and the traditional financial market law. The key concept in this regard is the *financial instrument* since the MiCAR is designed to apply to tokens that do not qualify as financial instruments under the MiFID II. According to the MiCAR, tokens are subject to the regulation as long as they are not classified as financial instruments—a distinction that makes logical sense from a legislative standpoint, given that other tokens, those financial instrument tokens, are already regulated and subject to existing investor protection provisions under MiFID II. However, the boundary between these two regulatory frameworks is not as clear-cut as it may initially seem. It is because the MiFID II does not provide a precise, pan-European definition of financial instruments. Rather, it refers to its annex that lists various categories of financial instruments, including transferable securities, which are defined differently in various EU member states. It is a question of national law what is considered as a security. For example, in some jurisdictions, shares of limited companies are classified as transferable securities, while in others they are not. As a result, national law plays a critical role in this definition, which complicates the process of establishing a clear distinction between MiCAR and MiFID II. The referral to national law at this stage introduces considerable complexity, making it difficult to delineate precisely where the boundary between MiCAR and MiFID II lies. This challenge is further compounded by the overlap with other traditional securities regulations. For instance, the Prospectus Regulation also uses the term “securities”, and its definition is tied to the one found in MiFID II. As a result, the same issue arises with regard to the Prospectus Regulation: it applies to transferable securities as defined by MiFID II. Consequently, the dividing line between MiCAR and the Prospectus Regulation poses the same difficulties as the boundary between MiCAR and MiFID II.

Similarly, the same complication exists when considering the dividing line between MiCAR and MAR. MAR defines its scope by referencing financial instruments, which are, once again, understood in the same way as in MiFID II. This means that the problem previously outlined resurfaces here as well. In theory, crypto-asset law and capital markets law are intended to be two exclusive areas of regulation that should not overlap, according to the intentions of the European legislator. However, in practice, drawing a clear and definitive boundary between the two areas remains a significant challenge.

Instruments of Financial Market Law

In order to compare traditional capital markets regulation with the regulation of crypto-assets, one must examine the core instruments of investor protection in each framework. One of the most important instruments is the disclosure requirement, which applies whenever financial instruments or crypto-assets are issued. Under MiCAR, this disclosure takes the form of a white paper, which serves a similar function to the prospectus in traditional securities markets. White paper bears a strong resemblance to the prospectus. Both documents require issuers to disclose key information to potential investors. The content, definitions, and exceptions required under MiCAR’s white paper provisions closely mirror those found in the Prospectus Regulation.[8] Furthermore, the content is in large parts similar. However,

[8] For example, please compare art. 6 MiCAR and art. 6 Prospectus Regulation.

there are notable differences between these two regimes, particularly at the enforcement level. The most important difference is that under MiCAR, the white paper does not require approval by a supervisory authority, whereas a prospectus must be formally approved before securities can be offered to the public.[9] This lack of a formal approval requirement under MiCAR may seem like a development because it reduces the administrative burden and allows for greater flexibility in the crypto-asset market.

The liability for misleading or incomplete information in the white paper is, at its core, addressed within the framework of MiCAR. Moreover, there is an additional external liability imposed on board members of companies issuing crypto-assets,[10] which is a notable departure from traditional capital market regulation. In fact, this shift presents a political challenge, as liability has historically been viewed as a matter within the purview of national law, rather than EU law. However, under the new crypto-asset market regulation, liability is now governed at the European level. While the regulation mandates the existence of issuer liability, the specific details are delegated to individual member states. Nevertheless, the principal assumption is enshrined in MiCAR.

From the perspective of investor protection, it is essential to consider the standard—essentially the yardstick—by which misleading information is assessed. The question arises as to what type of investor is envisioned when evaluating whether the information is correct or wrongful, as this determination is closely tied to the expertise and sophistication of the reader. In traditional capital markets law, the expected level of understanding has typically been quite high, though this standard has varied across different member states. While under MiCAR the principle of liability is codified at the European level, the regulation does not explicitly define the level of understanding that should be presumed for investors when determining whether information is misleading. This introduces a degree of ambiguity, as it is unclear whether MiCAR imposes a uniform standard across the EU or leaves this determination to national authorities.

The rules of conduct governing the behaviour of market participants represent another key instrument of investor protection. MiCAR imposes rules of conduct on market participants. These rules, which govern how issuers and intermediaries must behave, are in some respects stricter than those found in MiFID II. For example, indicating a degree of harmonization between the two frameworks, MiCAR's Article 40 is closely aligned with MiFID II's Article 24, which lays out the rules of conduct for traditional financial markets. However, MiCAR extends these

[9] Please see art. 2(r) Prospectus Regulation.
[10] Art. 15, 26 and 52 MiCAR.

rules of conduct beyond intermediaries, applying them more comprehensively to issuers as well. In traditional capital markets law, issuers are generally subject to fewer conduct rules, which primarily apply to intermediaries such as brokers or dealers. MiCAR, in contrast, imposes stricter obligations on both issuers and intermediaries, which may contribute to a higher overall level of investor protection.

Prohibitions of Abuse

MiCAR also includes prohibitions against insider trading[11] and market manipulation,[12] which mirror the prohibitions found in MAR.[13] The similarities between the two regulatory regimes are striking. Both MiCAR and the MAR define insider information[14] in much the same way, and the prohibitions themselves are largely identical in scope. Similarly, the entities subject to these prohibitions—whether they are individuals or companies—are the same under both regulatory frameworks. However, there is a significant difference between the two frameworks: MiCAR does not include certain exemptions—known as safe harbors—that are present in traditional regulations. These safe harbors,[15] which provide protection for specific activities by exempting them from the prohibitions on insider trading and market manipulation, are not included in MiCAR. In traditional markets, these exemptions make it clear that certain activities are not subject to regulation, providing a level of legal certainty for market participants. MiCAR, by eliminating these safe harbors, imposes a stricter regulatory framework, which may make compliance more challenging for crypto-asset market participants.

What is particularly surprising is the reasoning provided by the EU legislator for this stricter regime. The legislator argues that by removing these exemptions, the rules governing market abuse in MiCAR have been streamlined and simplified, ostensibly making them easier to understand and comply with. However, in practice, the removal of safe harbors makes it more difficult for market participants to navigate the regulatory landscape, as they are no longer certain whether certain activities are exempt from regulation. Thus, in certain respects, MiCAR imposes a stricter regulatory regime for participants in the crypto-asset market than traditional market abuse law.

[11] Art. 89 MiCAR.
[12] Art. 91 MiCAR.
[13] Art. 8 and 12 MAR.
[14] Please see art. 87 MiCAR and art. 7 MAR.
[15] Art. 5 MAR.

Instruments of Consumer Law

The final point to be addressed, and arguably the most significant in terms of investor protection, is the integration of consumer law instruments to the MiCAR. This is an entirely new development in the context of capital markets regulation. Traditional capital markets law does not explicitly address the concept of consumer protection, nor does it incorporate the legal instruments typically associated with consumer law. MiCAR, however, introduces a very distinctive consumer law mechanism in the form of the right of withdrawal, which is found in Article 13 of the regulation. This right is like the withdrawal rights established in consumer law for distance contracts[16] or certain types of credit contracts. [17]

Applying this right of withdrawal to a market as dynamic as the crypto-asset market is a somewhat novel and untested concept. There is considerable debate among European legal scholars about how this right will function in practice. The details of its implementation remain unclear, and it is uncertain how effective this consumer protection instrument will be in a market that operates at the speed and scale of modern digital asset trading.

In conclusion, the introduction of consumer protection instruments like the right of withdrawal raises important questions about the relationship between investor protection and market stability. Returning to the earlier analogy of communicating tubes, it is worth questioning whether raising the level of investor protection, as MiCAR aims to do, will necessarily lead to greater market stability. In physics, there is another theory that shows that it is possible for the levels in different tubes to vary, even if they are interconnected. Similarly, while MiCAR may increase investor protection, it is not guaranteed that this will translate into a corresponding improvement in the stability of crypto markets.

[16] Art. 9 Consumer Rights Directive.
[17] Art. 26 Directive on Consumer Credit Agreements.

Recent Developments in the Regulation of the U.S. Crypto-Asset Markets - Anja von Rosenstiel, LL.M. [18]

Reported by Aybüke Keskin

Anja von Rosenstiel addressed recent developments in the regulation of the U.S. crypto-asset markets, highlighting key areas such as investor protection, the role of the SEC, and the classification of crypto-assets as securities. She emphasized the complex regulatory landscape in the U.S., marked by jurisdictional overlaps among various agencies. The "Howey Test" and its application to crypto-assets were discussed, along with significant litigation involving major exchanges like Coinbase and Binance. Additional topics included the liability of software developers, stablecoins regulation, and the ongoing regulatory "turf war" between the SEC and CFTC.

Overview

The regulation of crypto-assets across jurisdictions presents several challenges, many of which resonate with those discussed in the European context. Listening to Professor Möslein's presentation, it is evident that some of the issues encountered in the EU are mirrored in the U.S., albeit with varying legal and regulatory responses. The complexity of this transnational technology necessitates a global dialogue to address these common challenges effectively. The discussion will proceed with recent developments in U.S. crypto-asset regulation.

The key areas of focus in the U.S. crypto-asset market today concern investor protection, securities law, the liability of platform providers and developers, and consumer protection. During a comprehensive conference on this subject in NYC, an interesting debate emerged regarding the relative significance of the upcoming U.S. elections versus the enforcement of MiCAR in shaping the future of the U.S. crypto market. Although opinions were divided, many participants agreed that the outcome of the U.S. election would have a more profound impact on the market than MiCAR's implementation. However, further commentary on U.S. politics will be refrained from to focus on U.S. court rulings. For example, a recent U.S. court ruling legalized the opening of a prediction market for election outcomes. Offshore platforms, such as PredictIt[19], which offered such a prediction market in the aforementioned case, have already accumulated over one billion dollars in deposits for predictions related to the U.S. election, illustrating the growing influence of decentralized prediction

[18] Anja von Rosenstiel is a mediator and attorney practicing in Germany and Boston, with expertise in banking law, capital markets, FinTech, and DeFi. She is counsel at a leading law firm, advising on regulatory compliance and international private law for digital assets. A graduate of Boston University's LL.M. program, she has published extensively on mediation and blockchain law, and she regularly participates in the International Chamber of Commerce's Annual Mediation Competition.

[19] https://www.predictit.org

markets. Nonetheless, I will now turn to the more pressing regulatory concerns—primarily the role of the Securities and Exchange Commission (SEC).

The predominant question regulators are grappling within the U.S. is whether a crypto asset qualifies as a financial instrument or falls outside the scope of securities regulation. This classification determines which regulatory body has jurisdiction over the asset. Unlike Germany, where regulatory oversight is more centralized, the U.S. regulatory landscape can be likened to an "alphabet soup" of regulators. Each regulator covers different aspects of the financial market, leading to considerable jurisdictional overlap and, at times, regulatory turf wars.

Securities Market, the SEC, and Enforcement Actions

To begin with, let us focus on the SEC and its role in the regulation of the securities market. Recently, Hester Peirce, a notable member of the SEC, colloquially referred to as the "crypto mom" due to her dissenting opinions within the commission, shed light on two pivotal issues facing the U.S. crypto-asset market: (1) the legality of token launches in the U.S. and (2) the regulation of financial services offered through open-source software. In the initial coin offering (ICO) era, regulatory issues primarily revolved around token sales, which closely resembled traditional financial instruments. Today, however, the market has evolved. The SEC has shifted its focus to the secondary market, particularly the spot market for crypto assets, and is now embroiled in litigation with major exchanges, including Coinbase, Binance, Kraken, and Bittrex.

As gatekeepers, exchanges play a crucial role in determining whether a crypto-asset qualifies as a security. Based on this determination, they are required to register as a market participant in the securities market, specifically as a national exchange. Should a crypto-asset be deemed a security, it is required to register it with the SEC prior to its sale. Therefore, they are responsible for ensuring that the primary offer and sale of securities is registered with the SEC. This classification lies at the heart of ongoing litigation, as many of these assets are categorized as "investment contracts"—a type of security in U.S. federal law. What is particularly fascinating is how well-known the term "investment contract" has become worldwide, despite its origins in U.S. case law. The classification stems from the Howey Test, derived from a Supreme Court decision[20], which has become an almost universally recognized standard.

Investment Contracts and the Howey Test

The Howey Test sets forth the criteria for identifying an investment contract: (1) an investment of money, (2) in a common enterprise, (3) with an expectation of profit

[20] SEC v. W.J. Howey Co. 328 U.S. 293 (1946).

of the purchaser, (4) derived from the managerial efforts of others. Though the test itself appears straightforward, it is underpinned by 80 years of complex case law, resulting in considerable regulatory confusion. As it stands, the hot-button issue in the U.S. concerns the secondary market for crypto securities on exchanges. The courts are divided on whether a contractual relationship is necessary between the original issuer of the token and the secondary market purchaser to establish an investment contract. Even within a single district, such as the Southern District of New York, different courts have issued conflicting rulings on this matter.

While some courts maintain that the totality of circumstances of the economic reality should be considered—without differentiating between primary and secondary sales—others argue that secondary market purchasers often lack the necessary context, thereby complicating the classification of these transactions. Amidst this legal uncertainty, exchanges as gatekeepers remain responsible for registering tokens that qualify as securities.

The free distribution of tokens, such as airdrops, has also come under scrutiny. The SEC argues that these transactions represent an investment of money, particularly when tokens are promoted through private social media channels. Such alleged promotion of the SEC considers already consideration. Overall, courts have largely agreed with this expansive SEC interpretation of the Howey Test criteria, e.g. investment under the Howey Test. In order to understand whether a crypto asset constitutes a security, one must consider not the asset itself but how it is utilized in the respective token's eco-system. In the aforementioned staking example, when participants risk their assets to support network operations, this constitutes an investment of money. The SEC has asserted that staking services offered by exchanges like Coinbase meet the criteria for an investment contract, as the profits derived from staking depend on the efforts of others – in this case, the network validators.

Payment Stablecoins Sold as Securities?

A key legal issue is whether certain assets, such as payment stablecoins, involve a common enterprise—a central requirement under the Howey Test. According to the SEC, when investors pool their assets, the resulting shared profits or losses constitute communality to qualify as common enterprise. This has been confirmed in cases involving staking, where pooled assets are collectively staked, creating an investment structure subject to securities regulation. Moreover, validation-as-service-providers like Coinbase, are considered to contribute the managerial efforts necessary for profits by offering specialized knowledge and software to the user, further cementing its claim that staking services qualify as investment contracts.

In summary, the classification of crypto-assets as securities continues to be a source of significant regulatory uncertainty. Classification of these assets also affects the outcome of the question of whether the SEC or another regulator holds the primary jurisdiction over the market. Whether the SEC or another regulator holds primary jurisdiction over the market depends on how these assets are categorized. This in turn affect another open question of whether the crypto-asset market is all about investor protection or as Prof. Möslein noted, there might be consumer protection aspects to consider as well which is the purpose of the Commodity Exchange Act. Depending on the subject matter jurisdiction, different disclosure duties apply. Moving forward, this area is expected to remain highly contentious as regulators and market participants strive to clarify these definitions.

Prosecution of Software Developers for Bad Acts of Third Parties

Another critical issue in the U.S. regulatory landscape is whether software developers can be held liable for the bad acts of third parties who misuse their platforms. This debate in the U.S. extends beyond civil liability, and unlike the MiCAR enters the realm of criminal liability as well. In cases where developers violate money transmitter regulations, anti-money laundering laws, or sanctions laws, they may face criminal charges.

The key question is whether a software provider or developer should be classified as a financial institution, thereby subjecting them to financial regulations. At what point does the provision of software or access to it constitute a transfer of funds or a financial transaction? Furthermore, if a developer provides access to open-source software, such as a permissionless blockchain like Bitcoin or Ethereum, should they be held accountable for how that software is used? This debate, which pits liability against the right to privacy, remains one of the most hotly contested issues in U.S. crypto law.

Bank Secrecy Act: Anti-Money Laundering and Counter-Terrorist Financing for Money Service Businesses

The Bank Secrecy Act (BSA) governs the transfer of cryptocurrency, which is enforced by the Financial Crimes Enforcement Network (FinCEN). FinCEN provides clear guidance[21] to help crypto developers understand when their software crosses the line into the realm of financial undertakings, requiring compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations.

[21] Department of the Treasury Financial Crimes Enforcement Network, Guidance (FIN-2013-G001), Application of FinCEN's Regulations to Person Administering, Exchaning, or Using Virtual Currencies, 18 March 2013; FinCEN Guidance (FIN-2019-G001), Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 9 May 2019.

One prominent case is that of Tornado Cash, a platform accused of providing a mixing service on the Ethereum blockchain to obscure the path of transactions. The developers of Tornado Cash have argued in a criminal case that they merely provided the user interface for the software and did not control or participate in the financial transactions conducted on the platform. A recent court ruling supported this argument, noting that Tornado Cash does not exert independent control over users' transactions, but that is not the only criterion.[22] The court also emphasized that the developers should have exercised constructive knowledge—the expectation that they could foresee potential misuse of their software.

This issue arises from wallet regulation or guidance. The software service in question closely resembles a mixer or tumbler service, which is classified as a money service business (MSB). Moreover, there is an accusation that providing access to this software constitutes a violation of sanctions law.

In response, the software developers argue that they had no contact with the third parties involved, nor were they aware of entities like the so-called Lazarus Group, a North Korean bad actor. They question how they can be held responsible. However, the court ruled otherwise, stating that specific knowledge is not required for liability to arise. The developers should have known or had "constructive knowledge" that their software could be abused. This is considered sufficient for liability.

Consequently, the question of money laundering and sanctions violations is shifting upstream to the design level. In the U.S., the design of software code is generally protected under the First Amendment as a form of free speech. However, the court now asserts that this case is not about the act of writing code itself, but rather about the use of that code's functionality for private gain. Since Tornado Cash issued a token and built an ecosystem around it, there was a beneficial interest involved. As a result, the court ruled that privacy is not at stake in this case; it is about liability.

Primary Jurisdiction over Crypto-Assets: Turf War between the CFTC and the SEC

The issue of regulatory jurisdiction over crypto-assets in the United States remains contentious, with a clear delineation of authority between the SEC and the CFTC yet to be established by law. The situation has given rise to what can be best described as a regulatory "turf war" between these two agencies. This jurisdictional dispute centers on the question of which body should regulate the crypto-asset spot market, a matter that is currently the subject of substantial litigation.

The secondary market for crypto-assets is a key area of regulatory contention. The SEC's primary mandate is investor protection, whereas the CFTC has a broader

[22] United States of America v. Roman Storm, Roman Semenov, 23 Cr. 0430, 12-05-2023.

remit, with a particular emphasis on consumer protection. Under the Commodity Exchange Act, the CFTC grants a greater degree of self-regulation to the market, allowing for a system of self-certification. This contrasts sharply with the SEC, which requires market participants to formally register with the commission and undergo its approval processes, subjecting them to a much higher level of regulatory scrutiny. This fundamental difference in regulatory philosophy has fuelled the debate over which agency is better suited to oversee the burgeoning crypto-asset market.

In Congress, this issue has sparked a broader philosophical debate regarding the balance between market autonomy and government oversight. The central question is whether regulatory responsibility should rest with a government agency—which would maintain strict control over the market—or with the market itself, which would operate under a self-regulatory framework. The resolution of this debate will have far-reaching implications for the regulatory architecture governing crypto-assets in the U.S., especially for the regulation of decentralized financial productes.

The turf war between the SEC and CFTC also revolves around the classification of crypto-assets. A significant point of contention was the determination of whether Ethereum should be classified as a security or a commodity. This issue has largely been resolved with the approval of Exchange-Traded Funds (ETFs) that include Ethereum as the underlying asset. Moreover, the SEC has suspended its investigation into Ethereum and its related ecosystem, including ConsenSys, a major provider of wallet services such as MetaMask. However, other classification issues remain unresolved, particularly with respect to stablecoins.

The SEC recently initiated enforcement actions against Terraform Labs and Binance, asserting that even stand-alone payment stablecoins fall under the Howey Test. According to the SEC, these stablecoins are deeply integrated into their respective ecosystems, and the profits generated from the sale of these stablecoins are reinvested into the ecosystem, thereby fulfilling the conditions of the Howey Test.

Conversely, the CFTC has maintained that stand-alone payment stablecoins are commodities, not securities. The CFTC's argument is that these stablecoins are primarily used as a medium of exchange or a store of value, rather than as speculative investments. They are bought for consumption, and therefore, the CFTC asserts that stablecoins fall under its jurisdiction as commodities. However, the CFTC has also acknowledged that there exists a regulatory gap with respect to the oversight of stablecoins, further complicating the regulatory landscape.

In conclusion, the U.S. regulatory framework for crypto-assets remains in flux, with infrastructure being another critical topic of debate. Although the EU's MiCAR framework is often admired for its relative clarity, significant regulatory uncertainty persists in the U.S.. As highlighted by Prof. Möslein, even under MiCAR, unresolved issues remain. Nonetheless, the U.S. continues to grapple with key regulatory challenges, such as the launch of tokens, the regulation of decentralized finance (DeFi), platform liability, and user privacy. It may be argued that these topics will be central to forthcoming legislative efforts in the U.S. Congress, as policymakers seek to address the complexities of regulating the crypto-asset market in a comprehensive manner.

Q&A Session I

1. *What are the views of the panelists on the international investment protection of cryptocurrencies? Furthermore, could the panelists provide insights on the limitations of the definition of crypto-assets?*

Ata Türkfiliz: Firstly, I would like to inquire about the panelists' views on the international investment protection of cryptocurrencies. Cryptocurrencies can be considered as assets, but do they meet the requirement of contributing to the development of the host state? Secondly, I would be grateful if the panelists could provide insights on the limitations of the definition of crypto-assets.

Anja von Rosenstiel: From a U.S. law perspective, I must refer to the well-known Morrison decision of the U.S. Supreme Court, which limited investor protection to the U.S. market. This decision is now being challenged in the Binance case, where the scope of U.S. jurisdiction is under scrutiny, but it is basically limited to the U.S. market, to the U.S. jurisdiction. The key criterion for determining U.S. jurisdiction is whether the transaction took place within the U.S. market. The SEC has also taken the position that, when services in the U.S. are used to purchase securities, the transaction falls within U.S. jurisdiction. This expansive interpretation of U.S. market involvement was particularly evident in the Tezos enforcement action, where the SEC argued that transactions on the Ethereum network, because most nodes are based in the U.S., implicate U.S. jurisdiction. Therefore, if you have an Ethereum transaction, this already involves the U.S. market. This is a very expansive interpretation of this Morrison Decision, and this again, is litigated right now on the appeals level in the Binance Decision. Hence, while this interpretation is still under litigation, it highlights the SEC's broader approach to defining personal jurisdiction in the context of crypto-assets.

Florian Möslein: Thank you for your question, which indeed touches upon a very complex issue. While I am not an expert in international investment law, an answer can be provided based on a closely related area of law, namely European primary law and its fundamental freedoms, which share significant overlap with international investment law. These fundamental freedoms include the freedom of establishment, among others. The free movement of capital within the EU may offer a useful analogy. This freedom is the only one of the EU's fundamental freedoms that applies not only within the Union but also to third countries.

The key issue, however, is whether crypto-assets qualify as capital under EU law. Surprisingly, this question has not been widely debated in the literature, nor has it been addressed by the European Court of Justice (ECJ). Nevertheless, it may become increasingly relevant, particularly considering MiCAR, as it is a matter of primary law that could take precedence over secondary legislation. Therefore, this question is central, but it is difficult to provide a clear answer because it is unclear whether we should rely on national laws and their definitions, or on secondary legislation. Resolving this issue would allow us to establish an independent concept of capital or assets at a higher regulatory level.

2. *Do investors in crypto-assets qualify as consumers for the purposes of consumer protection law?*

Müge Çetin: I would like to hear our speakers' thoughts on a particular topic. There are differing opinions regarding the protection of investors as consumers in certain capital market activities. What are their views on such protections in the context of the crypto asset markets?

Florian Möslein: Thank you for raising this interesting point. The classification of investors in crypto-assets as consumers is indeed a matter of debate. Traditionally, investment activities have not been seen as typical consumer activities. When we think of consumer protection, we generally consider the purchase of goods or services for personal use, or perhaps obtaining credit, but investment has not traditionally fallen within this realm.

That being said, it may be necessary to distinguish between different types of tokens. Pure investment tokens are likely not representative of typical consumer activities, whereas purchasing a utility token, for example, aligns more closely with traditional consumer behavior. Hence, while an individual investing in crypto assets may be considered a consumer, this designation is not guaranteed. Although this may be a vague answer, it reflects the current understanding of the issue.

Anja von Rosenstiel: This is a great question, and one that is highly relevant in the U.S. market as well. For example, the CFTC has brought enforcement actions focusing on consumer protection aspects, such as in the Mango Markets case, where price manipulation of governance tokens was a central issue. The CFTC took the position that protecting consumers from market manipulation should be a regulatory priority, while the SEC later brought a separate enforcement action focusing on the issuance of their governance tokens, asserting that the Mango Markets DAO was not a true decentralized autonomous organization, but rather an entity controlled by a few token holders. The SEC intervened by defining them as brokers to protect investors, effectively establishing this type of intermediary to prevent conflicts of interest.

If an intermediary steps in, the conflict of interest can be avoided. This creates a conflation of consumer protection and investor protection aspects. In the U.S., the regulatory framework is somewhat flexible and not rigidly defined by primary statutory law, resulting in the involvement of two agencies. From the perspective of organizations like the Mango DAO, this uncertainty is concerning, as they may not know what to be vigilant about. Is the focus here on consumer protection, or is it solely about securities market investor protection?

In addition, recent rule-making efforts by the SEC have included changes to the definition of a dealer. For instance, in the case of liquidity pools, the SEC may consider liquidity providers as investors since they pool their assets and receive fees for providing liquidity, which constitutes an investment contract. These liquidity providers also utilize the liquidity pool and its automated market makers. Arbitrageurs and others may transact against them, often resulting in losses for the liquidity providers when using these automated market makers. This creates a tension between user and consumer protection aspects and the role of investors and investor protection. It is a complex issue that ultimately depends on one's perspective.

3. *Does MiCAR art. 75(8) impose strict liability on crypto-asset service providers for investor losses, or is it fault-based liability?*

Furkan Güven Taştan: My question pertains to MiCAR art. 75(8), which imposes liability on crypto-asset service providers for clients' losses. Is this liability based on fault, or can it be classified as strict liability? Many argue that it is not fault-based due to the absence of a fault-based framework. I would appreciate your thoughts on this distinction.

Florian Möslein: A very specific and again very excellent question. MiCAR art. 75(8) does indeed introduce a liability regime for crypto-asset service providers, though it leaves certain aspects open to interpretation. Specifically, the regulation does not explicitly clarify whether this liability is fault-based or constitutes strict liability. The fact that the European legislator does not specify this does not mean it is not addressed by other legislators. The real question is whether this differentiation should be made at the European level or left to national authorities. In other words, do national legislators have the discretion to determine whether liability is fault-based or follows a strict liability framework?

Many argue that European law mandates strict liability, requiring national legislators to transpose it into national law in that form. However, this is not entirely clear to me; it remains an open question. I am inclined to believe that the European legislator leaves this issue unresolved, allowing national lawmakers to decide, though I hold this view tentatively.

4. *Will the lack of a clearly defined fault standard in MiCAR create problems of application across different EU member states?*

Deniz Baytemur Köksal: Building on the previous question, do you think the lack of a clearly defined fault standard in MiCAR will create application problems across different member states? For example, in the context of prospectus liability, we know that Italy applies a fault-based system, whereas other countries take different approaches. Hence, do you think this will cause application problem within the countries?

Florian Möslein: This is indeed a critical question, and one that will likely present challenges in the coming years. The lack of precedent regarding EU-based liability provisions is a central issue. This is the first time that a liability regime has been incorporated into a European regulation rather than a directive, meaning that it does not require transposition by national lawmakers. This is a relatively new phenomenon, and the European lawmaker has taken only one step instead of two. While the principle is outlined in MiCAR, it is not clearly defined. As a result, European legislation exists, but only to a certain extent. This raises important questions about whether, and to what extent, European law prescribes specific aspects of liability. These concerns go beyond the fault-based versus strict liability distinction and extend to the civil procedure framework for enforcing liability. It is an issue that will likely keep us engaged for the coming years.

5. *Should the enforcement of MiCAR be carried out by a central European authority, or is it better left to national regulators?*

Cemre Polat: I have a question regarding the enforcement of MiCAR. Given its broad scope and the novelty of certain provisions, do you think it is appropriate that national regulators are responsible for its enforcement, or would it be preferable for a centralized authority at the EU level to handle enforcement? I think both the subject matter is quite suitable for that. Moreover, you mentioned that, for the first time, MiCAR introduces a civil liability provision in a regulation. However, in the side of the administrative law, enforcement is still left to national regulators. Do you believe it would be more effective for enforcement to be centralized at the EU level, given the wide scope and regulatory nature of MiCAR?

Florian Möslein: In an ideal scenario, the enforcement of MiCAR at the European level might indeed be beneficial, as it could provide greater consistency and uniformity in the application of the regulation. However, past experiences with securities regulation and banking law have shown that there is considerable reluctance among EU member states to cede regulatory authority to centralized European bodies. Even within the European Banking Union, where regulation is arguably more stringent, there is no uniform European authority. Instead, institutions like the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) serve more as coordinating bodies rather than full-scale authorities. Even in the highly regulated area of banking law, there is no single European supervisory authority. Therefore, it may be difficult to argue for the establishment of one in the field of crypto-assets.

While this is not directly related to the issue of liability, as it involves civil enforcement rather than public enforcement, you are correct that greater centralization could point in that direction. However, I would still be cautious about recommending a European regulator, given the limited experience with such a framework in this area so far.

Anja von Rosenstiel: Florian, you mentioned civil liability and other forms of enforcement. In U.S. securities law, private parties can bring lawsuits against issuers. Similarly, MiCAR introduces Whitepaper liability, which is something the U.S. has extensive experience through private enforcement or litigation of securities issues. If this approach is adopted in other jurisdictions, I just wanted to highlight that the U.S. has a long tradition in this area, and I am keen to see how it develops in the EU.

Crypto-Asset Regulation in Turkish Capital Market Law - Dr. Cemre Polat[23]

Reported by Elif Akıncı

The second half of the session began with a focus on examining regulatory developments in Turkish law. Polat provided an in-depth discussion of the recent developments in the regulation of crypto-assets under the Turkish capital market law. She started by addressing the recent amendments made to the Turkish Capital Markets Act (CMA), which have been amended as to incorporate new provisions regarding crypto-assets.[24] Unlike the European Union's approach of having a separate legal instrument for crypto assets, Turkish legislator has chosen to integrate these provisions into the existing CMA. The law is enforced by the Capital Markets Board of Türkiye (CMB), which have been granted extensive powers to issue guidance and enact secondary legislation.

Scope

Polat outlined that, instead of including numerous detailed provisions, the act empowers the CMB to direct the market by enacting further rules through delegated legislation. The presentation began by detailing the **territorial scope** of the regulations. CMA applies to all crypto asset service providers (CASPs) established in Türkiye, as well as foreign entities providing services to individuals residing in Türkiye. The assessment of whether a company is providing services to Turkish residents is based on certain criteria, which include the use of the Turkish language, having a workplace in Türkiye, and promotion or marketing activities within Türkiye.[25] Additional criteria may be designated by the CMB, if necessary. She noted that while Türkiye has linguistic similarities with other Turkic-speaking countries such as Azerbaijan and Uzbekistan, there are clear and recognisable differences between them. However, she highlighted the special case of the Turkish Republic of Northern Cyprus, where the official form of Turkish used is identical to that of Türkiye. When the website of a CASP is available for use in Turkish, a statement such as "Turkish (Turkish Republic of Northern Cyprus)" -an example seen recently- should not be sufficient to escape the scrutiny of the CMB, unless there is a geo-blocking for residents in Türkiye.

As to the **material scope** of application, CMA applies to capital market instruments which are "securities and derivative instruments as well as other capital market

[23] Asst. Prof. Dr. Cemre Polat has graduated from Koç University and received her LL.M degree from UCL. After receiving her Ph.D. title from Bilkent University with her dissertation "Autonomous Systems in the Law of Extra-Contractual Liability" she started to work as an assistant professor at Ankara Medipol University School of Law, Department of Civil Law.

[24] Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun (7518), Official Journal: 2 July 2024, 32590.

[25] CMA art. 99/A para.1.

instruments designated in this context by the Board, including investment contracts."[26] Material scope of new provisions, on the other hand is the "crypto-assets which are intangible assets that can be created and stored electronically using distributed ledger technology (DLT) or a similar technology, distributed over digital networks and can express value or rights."[27] This definition covers crypto-assets that provide rights specific to capital market instruments (i) and also those that do not provide such rights (ii). It should be noted that the while the CMA provides a definition of crypto-assets, it does not regulate the assets themselves in detail. Instead, it focuses on regulating crypto-asset service providers (CASPs) which brings us to the **personal scope** of the CMA. CASPs are defined as "platform operators, crypto-asset custody service providers and other entities designated in the regulations to be enacted on the basis of this Act to provide services in relation to crypto-assets, including the initial sale or distribution of crypto-assets."[28] A CASP is a legal subject and CASPs are required to verify the client's identity which implies that De-Fi is left out of the scope of CMA and subject to general provisions.

Crypto-Assets in the CMA

The presentation further explained that the act divides crypto assets into two categories. The first category is crypto-assets that represent capital market instruments and traded on a platform. In principle, capital market instruments shall be issued in a dematerialised form in the electronic environment and the records shall be monitored by the Central Registry Agency (CRA).[29] The novelty introduced by new provisions is that capital market instruments may be issued in the form of crypto assets, with records monitored by CASPs instead of the CRA.[30]

The second category includes crypto assets that are traded on a platform but do not represent any capital market instruments such as asset-referenced tokens or e-money tokens. Although there are no specific provisions regulating this category, the Board has the power to create secondary legislation to cover their distribution and sale. So, the new provisions of CMA do not regulate what MiCAR regulates; but rather it gives the power to the CMB to issue secondary legislation. The CMB is entitled to [not shall] determine principles for the sale or distribution of crypto assets, other than crypto assets that provide rights specific to capital market instruments, created through the development of distributed ledger technology or a similar technological infrastructure, whose value cannot be separated from this technology, on platforms without being subject to the provisions of the Law on

[26] CMA art. 3, para. 1, (ş).
[27] CMA art. 3, para. 1 (bb).
[28] CMA art. 3, para. 1 (cc).
[29] CMA art. 13.
[30] CMA art. 13, para. 1.

capital market instruments.[31] In the preamble, it is stated that an opportunity is given to the CMB to regulate such crypto-assets.

	Crypto-assets that are capital market instruments	Crypto-assets that are not capital market instruments
Crypto-assets that are traded on a platform	Such assets and CASPs for such assets are subject to the Act.	Such assets are not subject to the Act, however the Board is entitled to designate applicable rules. CASPs for such assets **are** subject to the Act!
Crypto-assets that are not traded on a platform (peer-to-peer)	Not possible.	Not subject to the Capital Markets Act and the Board is not expected to designate applicable rules not to hinder the development of the market (see, the Preamble)

Regarding cyrpto-assets that are not traded on a platform and that do not qualify as a capital market instrument, resolution of the CMB dated 19.09.2024 should be noted here. The CMB made a warning stating that "In peer-to-peer (P2P) digital marketplaces that enable the direct buying, selling, and exchanging of crypto-assets among users, engaging in transactions in one's own name but on behalf of others on a regular basis, as part of a commercial or professional activity, may be considered unauthorized crypto-asset service provision [which is a criminal offence] under Article 99/A of the Law. Those engaging in such activities must cease their operations by November 8, 2024." [32]

Requirement for CASPs

CASPs are required to obtain license from the CMB to commence providing service. [33] Principles and procedures are not stated in CMA, rather it confers power on the CMG to enact secondary legislation. CASPs are obliged to make the necessary arrangements, to take the necessary precautions and to establish the necessary internal control departments and systems for the safe management of their systems. Shareholders, board members, and authorized representatives of a CASP must meet certain conditions similar to those applicable to the shareholders in an investment firm, such as not being bankrupt; not being sentenced for certain crimes; having necessary financial strength; honesty and reputation.[34] Regarding prospectus or white paper, CMA does not include any specific provision regarding crypto-assets. Regarding the first category of crypto-assets those that represent a capital market

[31] CMA art. 35/B para. 6.
[32] Resolution of the CMB, Date: 19.09.2024, No: 1484.
[33] CMA art. 35/B.
[34] CMA art. 35/B.

instrument, general prospectus requirement is applicable to the issuer.[35] As noted before regarding the second category of crypto-assets those that do not represent a capital market instrument but traded on a platform, there is no specific provision in CMA. However, the CMB has the power to regulate them in a secondary legislation. Accordingly, there is no white paper requirement in CMA as to this category.

Legal Relationship between CASPs and Clients

The contract between CASPs and their clients are subject to written form requirement. Written form requirement, besides being a validity condition of the contract, is a must for an authorized service provision. Written form requirement may be fulfilled remotely via communication tools, or through any method that the CMB deems equivalent to a written form, using an information or electronic communication device that allows for customer identity verification.[36]

The contract is not necessarily a distance contract within the context of consumer protection law. When it is so -which is only possible when the client is a customer- the right to withdrawal under consumer protection law is applicable.

Regarding rules applicable to such contracts (about the fee and costs, termination of the contract, etc) again the CMB is entitled to designate them in a secondary legislation.

CMA expressly states that prices on platforms are determined freely. The limit is market disruptive actions:

> Prices on platforms are determined freely. Except for transactions involving crypto-assets deemed by the Board to be widely traded in foreign markets and whose prices are also formed in such markets, the provisions of Article 104 of this Law shall apply to actions and transactions on platforms that cannot be reasonably and economically justified and that disrupt the reliability, transparency, and stability of operations on the platforms. Platforms must establish order and transaction principles to ensure that transactions are conducted reliably, transparently, efficiently, stably, fairly, honestly, and competitively, and to detect, prevent, and avoid the recurrence of market-disruptive actions and transactions. They are required to set up the necessary monitoring systems within their organizations and take all preventive measures. Platforms are also obliged to detect market-disruptive actions and transactions carried out within their systems, take the necessary measures, including restricting, suspending, or closing the accounts involved in such actions and transactions, and report their findings to the Board in a documented format.[37]

[35] CMA art. 4 *et seq.*
[36] CMA art. 35/C, para. 1.
[37] CMA art. 35/C, para. 3.

Obligations of CASPs towards Clients

The principle is that cash and crypto-assets belonging to clients should be kept in clients' own wallets.[38] In order to minimize security risks, the Act requires the CASPs to keep records of the wallets and accounts through which their client transfer crypto assets in a secure, accessible and traceable manner. The integrity, accuracy, and confidentiality of all transaction records are ensured.[39]

In cases where clients do not prefer to keep crypto assets in their own wallets; it must be submitted by banks authorized by the CMB and approved by Banking Regulation and Supervision Agency or by other institutions authorized by the CMB to provide crypto asset custody services.

Conclusion

The overarching aim is to regulate Crypto-Asset Service Providers (CASPs), emphasizing that the nature of the crypto-asset itself is not decisive in applying these regulations. This framework introduces a "capital market order" approach, encompassing assets that may not necessarily qualify as capital market instruments, including the imposition of criminal offenses prescribed for capital markets. This broadens investor protection to individuals who might not typically be considered investors. Peer-to-peer (P2P) transactions remain outside the scope of these regulations and are governed by general legal provisions, reflecting no intent to interfere with decentralized environments. Moving forward, specific rules issued by the CMB addressing other crypto-assets traded on platforms -those that are regulated in MiCAR- may emerge in the near future. Similarly, regulations concerning P2P crypto-asset transactions could be introduced through separate legal instruments, though this development is expected to take place over a longer time frame.

[38] CMA art. 35/C, para. 6.
[39] CMA art. 35/C, para. 5.

The Liability of Crypto Asset Service Providers – Assoc. Prof. Dr. Pınar Çağlayan Aksoy[40]

Reported by Aybüke Keskin

Pınar Çağlayan Aksoy discussed the rapid evolution of the crypto-assets ecosystem, emphasizing the need for global awareness in advising clients and shaping regulatory frameworks. She explained that Türkiye's initial regulatory steps in 2021, including the Central Bank's ban on crypto payments and MASAK's AML/KYC requirements, were initially seen as restrictive, but recent developments, such as the Thodex Fraud Case and Türkiye's placement on the FATF gray list, have underscored the need for robust investor protection. In 2024, the Capital Markets Act amendments introduced a regulatory framework with licensing requirements similar to those for banks, alongside strict liability provisions for crypto-asset service providers, treating their activities as "abnormally dangerous" due to potential harm from cyber-attacks or operational failures. Aksoy described extensive liability measures, including civil, tortious, and criminal liabilities, applying to both the providers and individual members of crypto-asset services. While she expressed optimism that this framework would enhance investor protection, Aksoy also voiced concerns that evolving regulatory demands from the Capital Markets Board (CMB) could deter crypto projects from operating in Türkiye, as they may seek more stable regulatory environments abroad.

Overview

It is undoubtedly challenging to keep pace with the rapid developments in the crypto-assets ecosystem. Each day brings new technical or legal developments, making it difficult to fully grasp all aspects of the field without specialized expertise. As is widely known, crypto-assets operate on a global scale, which further adds to the complexity. Thus, it is essential for lawyers, particularly when advising clients or conducting research, to be aware of international practices. Understanding what other jurisdictions are implementing can enable us to propose more effective solutions or critically assess the frameworks we already have. This holistic perspective is vital, and Assoc. Prof. Dr. Pınar Çağlayan Aksoy is hopeful that it will lead to productive future collaborations.

Early Regulatory Steps in Türkiye

After listening to Cemre Polat's presentation, you are now familiar with the developments that have taken place in Türkiye, beginning in early July. Since approximately 2018, there have been discussions about enacting a crypto-assets

---

[40] Assoc. Prof. Dr. Pınar Çağlayan Aksoy received her LL.B, LL.M. and Ph.D. degrees from Ankara University. She became an associate professor with her habiliatation thesis titled "Smart Contracts: Formation and Validity Conditions" She is currently working in the civil law department of Bilkent University Faculty of Law.

regulation in Türkiye. However, it was not until 2021 that any tangible regulatory steps were taken, and even then, the regulations introduced were not particularly in favour of the crypto-asset ecosystem. Specifically, in 2021, the Central Bank of Türkiye enacted a new regulation. It banned crypto-asset payments from being made without recourse to the bank, and the payments were completely banned.[41] This restriction was perceived as a negative impact for the Turkish market.

Subsequently, other regulatory measures were introduced. The Financial Crimes Investigation Board (MASAK), namely the other "financial watchdog," implemented changes to strengthen anti-money laundering (AML) and Know Your Customer (KYC) requirements. However, understanding how to protect investors in this ecosystem requires an understanding of the objectives of the CMB when enacting these new regulations in Türkiye.

The Impact of High-Profile Incidents and Global Developments

From 2021 to 2024 various events and developments necessitated action from lawmakers, leading the CMB to introduce new regulatory principles. In Türkiye, one of the most notable events was the Thodex Crypto-Currency Exchange Fraud in 2021, where the exchange defrauded investors, with the CEO absconding with over $2 billion. Last year, a lengthy prison sentence was imposed in connection with this scandal. The Thodex case[42] serves as a prominent example within Türkiye, underscoring the critical importance of investor protection.

Furthermore, a series of global crypto-related failures occurred, which, while not unique to Türkiye, were closely monitored due to the high level of interest in crypto-assets among Turkish citizens. According to recent statistics, Türkiye has approximately 10 million active crypto users. A report prepared by Paribu,[43] one of Türkiye's largest crypto-currency exchanges, on crypto-currency awareness and perception reflects the increasing interest of the Turkish public, and, as Professor Möslein noted earlier, the need for investor protection has grown significantly. Establishing secure protective mechanisms for investors is essential to fostering a healthy market environment.

Türkiye also faced in 2021 the issue of being on the Financial Action Task Force (FATF) "grey list."[44] Exiting this list has become crucial, as I often highlight in my

[41] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik (Regulation o the Prohibition of the Use of Crypto-Assets as Payment), Official Journal: 16 April 2021, 31456.
[42] 'Thodex Cryptocurrency Boss Jailed for 11,196 Years in Türkiye for Fraud' (n 1).
[43] 'Kripto Para Bilinirlik ve Algı Araştırması' (PARİBU 2024).
[44] Türkiye has recently been removed from the grey list. Huseyin Hayatsever and Daren Butler, 'Türkiye Removed from FATF Money Laundering Grey List in Boost to Standing' *Reuters* (28 June

presentations. In the early years of crypto-asset projects, operating in a regulatory grey area was sometimes viewed as advantageous. However, after 2021, particularly in the wake of the COVID-19 Pandemic and as numerous countries worldwide, including several U.S. states, jurisdictions adopting MiCAR, and others, began introducing comprehensive legislation, the regulatory greyness in Türkiye has increasingly become a disadvantage.

Remaining on the FATF grey list, coupled with a lack of regulatory stability, has deterred investors from entering the Turkish market. Numerous tokenization projects and other crypto-related ventures that originated in Türkiye were ultimately forced to establish themselves abroad, where they found more definitive regulatory environments and greater clarity in legal frameworks.

2024 Capital Markets Act Amendments: A New Regulatory Framework

Finally, on June 22, 2024, a draft of new legislation was released in Türkiye, though it has yet to come into force. Coinciding with this, BtcTurk, one of Türkiye's largest crypto exchanges, experienced a cyber-attack.[45] The official statement from BtcTurk indicated that their team detected a cyber-attack on their platform on June 22, which resulted in unauthorized withdrawals. Fortunately, only the balances held in hot wallets of ten crypto-currencies were affected, while the cold wallets, where most assets are securely stored, remained unaffected. Nevertheless, this incident led to a temporary suspension of services, underscoring the importance of investor protection in the Turkish crypto ecosystem.

In outlining these developments in Türkiye from 2021 onward, my aim has been to provide a comprehensive view of the regulatory landscape and challenges we face. To summarize the key events: the prohibition of crypto-asset payments introduced in 2021 remains in effect, as Capital Markets Act (CMA) was amended without altering this prohibition. That same year, MASAK introduced enhanced AML (Anti-Money Laundering) and KYC (Know Your Customer) obligations.[46] Then, on July 2, 2024, amendments were made to CMA introducing a framework law comprising 19

2024) <https://www.reuters.com/world/middle-east/simsek-indicates-that-Türkiye-removed-fatf-watchdogs-grey-list-2024-06-28/> accessed 6 November 2024.

[45] Bloomberght, 'BtcTurk siber saldırıya uğradı' (*Bloomberght*) <https://www.bloomberght.com/btcturk-siber-saldiriya-ugradi-2355135> accessed 18 November 2024.

[46] 'Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklere İlişkin Temel Esaslar [Basic Principles Regarding the Obligations on Prevention of Laundering Proceeds of Crime and Financing of Terrorism for Crypto Asset Service Providers]' (MASAK 2021) <https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf>.

articles.[47] While there are certain aspects that can be revised in the legislation, these amendments constitute an important step towards investor protection and strengthening the Turkish crypto ecosystem.

While the amendments introduced a sound framework, it quickly became clear that secondary legislation was necessary to implement these changes effectively. Following the publication of the amended CMA in the Official Gazette on July 2, 2024, the CMB issued a series of announcements or principal decisions outlining additional requirements for existing platforms. These requirements included providing specific information to the Board and, for platforms that opted to cease operations, notifying the Board and initiating winding-up procedures.

At the same time, new entrants to the market were also required to meet specific criteria. The CMB essentially sought to gain a comprehensive understanding of the Turkish crypto ecosystem, examining the operational structures of crypto-asset service providers. This process continued with an announcement on August 2024, in which the CMB published a list of operational and non-operational companies. This list is updated every day. Therefore, it is not a definitive list. While inclusion on this list does not constitute a license to operate, it reflects the status of these companies and signals that they may need to apply for a license to engage in market activities, depending on the CMB's requirements.

On August 2024, the Capital Markets Board issued another decision[48] outlining conditions for establishing platforms and criteria for partners and directors. This decision aims to create a more investor-friendly environment, ensuring that partners and directors are trustworthy and that platforms are built according to a roadmap set forth by the legislator.

The CMB issued another principle decision on September 2024,[49] which introduced additional investor protection measures. Among these is the requirement that client assets be kept separate from those of crypto-asset service providers. In the case of breach of performance or in the case of seizure, client assets must remain untouchable. Furthermore, client cash must be stored in banks, over which platforms do not have control. Cash transfers are limited to authorized entities. This measure addresses a persistent concern of the CMB, as they seek to ensure a secure custody environment. Although further detailed regulations are needed to clarify the relationships among crypto-asset service providers, custody service providers, and clients, the current framework mandates that if platforms store client-owned

[47] Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun (7518), Official Journal: 2 July 2024, 32590.
[48] Principal Decision of the CMB, Date: 08.08.2024, No.: 42/1259.
[49] Principal Decision of the CMB, Date: 19/09/2024, No: 1484.

crypto-assets, they must do so securely, with technical standards to be determined by TÜBİTAK.

Receiving orders via social media is prohibited. As of November 8, 2024, platforms are obliged to record all customer orders in a non-falsifiable manner. Platforms are prohibited from engaging in activities similar to foreign exchange bureaus and must provide clients with adequate disclosure to ensure they make informed decisions. Furthermore, peer-to-peer (P2P) trading is restricted, and platforms must ensure that advertisements and promotions are objective, accurate, and cannot promise fixed returns or direct users to specific crypto-assets.

As of today, this is the regulatory landscape and crypto-asset ecosystem in Türkiye. Moreover, as of October 2, 2024, foreign crypto-asset service providers were required either to set up an office in Türkiye or to cease their advertisement and activities directed to Turkish users.

In summary, these new rules primarily seek to prevent unlicensed crypto-asset service activities. Listing and delisting standards will be overseen by TÜBİTAK, which is the scientific research agency. They are working diligently to prepare detailed regulations.

The custody of crypto-assets will be overseen by banks and other institutions regulated by the Banking Regulatory Authority. Furthermore, there is guidance on NFT platforms, which will not be subject to these regulations, while stablecoins will fall under electronic money regulations.

As mentioned, the new rules introduce specific regulations concerning advertising and promotions. Regarding contracts with customers, Dr. Cemre Polat previously discussed safeguarding users' crypto-assets and ensuring their protection. The state will monitor the flow of crypto-assets to prevent money laundering and terrorism financing.

Civil and Criminal Liability for Service Providers

Moving to the primary topic, Çağlayan Aksoy discussed the liability of crypto-asset providers. The lawmaker frequently references terms like "liable" or "responsible" in the legal text. This is to say, these terms appear quite extensively. To begin with, it is essential to note that civil and criminal liability apply to illegal actions and investor losses within the crypto-asset market.

The first relevant provision is found in Article 35/B. Rather than reciting the article in full, the critical elements concerning liability will be highlighted. The CMB is empowered to establish regulatory procedures, issue special and general decisions, and enforce measures and sanctions concerning crypto-assets with attributes similar to capital markets instruments. This article also addresses crypto-assets that may not function as securities but instead may be utility tokens or payment tokens. Importantly, the lawmaker states that, during these transactions, real persons and legal entities who sign information documents prepared and disclosed according to CMB standards are jointly and severally liable for damages arising from incorrect, misleading, or incomplete information within these documents.[50]

As seen, this liability framework is extensive, covering not only the content of the information provided but also extending to all parties responsible for the information. Specifically, real and legal persons signing all kinds of information documents are accountable for any false or misleading information provided to the CMB. Regular updates on company structure, operational workflows, and underlying technology must be submitted to the Board, and any inaccuracies in this data can result in liability for misrepresentation.

Cemre Polat talked about contracts between crypto-asset service providers and their customers. These contracts may be executed electronically or in written form, but it is essential to emphasize that any contractual terms aiming to limit or exclude liability of crypto-asset service providers to their customers are deemed invalid.[51] The regulation does not specify the nature of the liability (whether intentional, gross negligence, or slight negligence), but it broadly excludes any limitation of liability.

To fully understand this provision, one should consider what the Turkish Code of Obligations (TCO) states regarding limitation or exemption from liability. Under Turkish law, similar to Swiss law, parties may exempt themselves from liability for slight negligence, provided that the agreement is valid and legally enforceable.[52] However, if the contract is carried out with the permission granted by the law or authorized authorities and is for the performance of a profession or art requiring expertise, it is absolutely null and void, which means that in the cases where the permission is granted by a designated authority, just like in the case of crypto-asset

[50] CMA Art. 35/B para. 6: "(6) Real persons and legal entities signing all kinds of information documents prepared and announced in a manner to be determined by the Board during these transactions are jointly and severally liable for the losses arising from incorrect, misleading or incomplete information contained in these documents."

[51] CMA art. 35/C para. 1: "(1) Any contractual terms that eliminate or limit the liability of crypto asset service providers to their customers are invalid."

[52] TCO art. 115: "(1) A prior agreement that the debtor will not be liable for the debtor's gross negligence is absolutely null and void.
(2) Any prior agreement of the debtor with the creditor that the debtor will not be liable for any debt arising from the service contract is absolutely null and void.
(3) If a service, profession or art requiring expertise can only be carried out with the permission granted by law or by the competent authorities, any prior agreement that the debtor shall not be liable for slight negligence shall be null and void."

service providers, any clauses seeking to exempt liability are absolutely null and void.

In the case of crypto-asset service providers, this aligns with standard contract terms. Often, a service provider may include terms exempting themselves from liability due to negligence. However, under the TCO art. 115(3), when an activity is legally permitted by an authorized body, exemption from liability is not permitted. This provision has implications for standard contract terms, as it negates the need to scrutinize such terms for incorporation, interpretation, and content.

Turning to tort liability and contractual liability, Article 99/B addresses damages resulting from illegal activities by crypto-asset service providers and their failure to fulfil cash payments or crypto-asset delivery obligations. This provision is important in two respects.[53] Firstly, service providers are liable for damages caused by illegal activities. Secondly, if damages arise due to the inability of a provider to fulfil financial or delivery obligations and the crypto-asset service provider (CASP) as an entity cannot compensate these damages, CASP members themselves may be personally liable for any damages attributed to them. Notably, the law does not specify "director" or "board member" but uses the term "member of a CASP", thus broadening the scope of potential liability.

An additional provision pertains to the tort liability of crypto-asset service providers, addressing losses arising from acts such as the operation of information systems, all kinds of cyber-attacks, information security violations, or any behaviour of the personnel, within the scope of the TCO art. 71.[54] This article concerns strict

[53] CMA Art. 99/B para. 4: "(4) Crypto asset service providers are liable under Article 71 of the Law No. 6098 for crypto asset losses arising from the operation of information systems, all kinds of cyber-attacks, acts such as information security breaches or any behaviour of the personnel. In the event that the losses cannot be compensated from the crypto asset service providers or it is clearly evident that they cannot be compensated, the members of the crypto asset service providers shall be liable to the extent that the losses can be attributed to them according to their faults and the requirements of the situation, and the provisions of Article 110/B of this Law shall apply in relation to personal liability. Losses arising from interruptions in the services provided without the fault of the crypto asset service providers, in cases where orders cannot be transmitted or transactions/transfers cannot be made for a temporary period and similar situations are not considered within the scope of this paragraph."

[54] TCO art. 71: "(1) In the event of damage arising from the operation of an enterprise that poses a significant danger, the owner and, if any, the operator are jointly and severally liable for this damage.
(2) An enterprise shall be considered to be dangerous if, in view of its nature or the materials, tools or forces used in its operation, it is capable of causing frequent or serious damage even if all due care is exercised by a person skilled in the art. In particular, if any law provides for a special hazard liability for enterprises that pose similar hazards, this enterprise shall also be deemed to be an enterprise that poses a significant danger.
(3) The special liability provisions foreseen for a particular case of danger are reserved.

liability for dangerous activities, a category now extended to certain crypto-asset services.

The law stipulates that if the losses cannot be compensated from the service providers, or if it is evident they cannot be compensated, the employees of the CASP are liable to the extent that the losses can be attributed to them. In such cases, personal liability for CASP employees will apply according to the nature of the fault, the requirements of the situation, and relevant provisions in the Capital Markets Law shall apply regarding personal liability. There is, however, a limited exception: damages arising from service interruptions not due to default, such as temporary order transmission failures, fall outside this liability framework.

When examining these provisions alongside those in the TCO, we observe that, similar to German and Swiss law, tort liability in Turkish law is divided into fault-based liability and strict liability. Art. 49 and subsequent articles of the Code discuss fault-based liability, which requires an act or omission, fault, unlawfulness, causation, and damage. Strict liability, by contrast, arises from the control that a person has over another person or thing.

One can further distinguish between ordinary strict liability and strict liability for dangerous activities. Here, art. 71 applies, which involves liability for activities considered abnormally dangerous. In Turkish law, there is similar strict liability in cases involving traffic accidents or nuclear facilities, reflecting activities with high risk. In this regulation, the Capital Markets Board classifies crypto-asset services as abnormally dangerous due to the severity of potential damage. While cyber-attacks and operational failures may not occur frequently, when they do, they can result in significant harm, hence the heightened caution from Turkish lawmakers. Hence, they have enacted huge amount of responsibility both on CASPs and their employees. CASP employees may also be held personally liable for the losses that occur on the investors.

In addition to civil liability, there are also criminal liability provisions. These apply to the unauthorized provision of crypto-asset services, embezzlement of money, and other actions by board members and officers of CASPs. Article 110B specifies that the chairman and board members, real person partners who have legally or de facto management or control of a CASP who engage in activities deemed embezzlement may face direct bankruptcy proceedings initiated by the Board. Thus, an extensive

(4) Even if such activity of an enterprise that poses a significant danger is permitted by the legal order, the injured parties may demand compensation for the damages caused by the activity of this enterprise.)

array of responsibilities has been imposed on crypto-asset service providers and their employees, encompassing both civil and criminal liability.

Finally, Çağlayan Aksoy addressed strict liability and offered her view that this approach may not be the most suitable method for regulating crypto-assets. She then discussed criminal liability to conclude her presentation. Over the past three years, from 2021 to 2024, there have been numerous drafts of this legislation. Notably, the strict liability provision was only introduced in the final stages of its enactment.

She believes that this strict liability provision was introduced at the last minute. Consequently, it may not be entirely appropriate to classify all crypto-asset service provision activities as abnormally dangerous. It would be inaccurate to assert that all activities undertaken by crypto-asset service providers inherently pose a significant or grave risk. This provision should therefore be carefully reconsidered.

The second key issue pertains to whether crypto-asset service providers should be regarded as financial institutions in terms of investor protection. It appears that Turkish lawmaker is deliberately avoiding subjecting crypto-asset service providers to the exact same regulatory framework as financial institutions or banks. Nevertheless, these providers are subject to licensing requirements, similar to banks, e-money institutions, and factoring companies. In some respects, however, the lawmaker has imposed even more stringent obligations on crypto-asset service providers, particularly on directors and board members, than what the Banking Law establishes in Türkiye. Both in terms of criminal and civil liability, the law imposes a considerable level of responsibility on crypto-asset service providers. These measures have clearly been enacted with the goal of protecting investors and fostering a legally accountable, well-regulated crypto-asset ecosystem in Türkiye.

Potential Chilling Effects and Future Outlook

In her concluding remarks, she noted that, without introducing additional conditions as outlined in the Banking Law, more stringent conditions have been defined here. This suggests that lawmakers perceive the crypto-asset market as a sector of high risk with regard to investor protection. In banking law, responsibility typically falls on executive partners, inspectors, or members of the board; however, in the case of crypto-asset service providers, all members may be held accountable, personal liability is also established.

Looking to the future of Türkiye's crypto-asset market, she is cautiously optimistic. Since the law was introduced and came into force in early July, there has been a sense of optimism in terms of having a regulatory framework that can now provide clear guidance and investor protection. This framework offers a certain level of assurance, creating an environment where investors can feel confident in the legal protections available to them.

However, as the CMB issues new announcements and principal decisions, it has become apparent that the regulatory story will not end here. Assoc. Prof. Dr. Çağlayan Aksoy shares the concern of colleagues who fear a potential chilling effect on the market. Projects that are unable to anticipate future regulatory requirements may find the conditions increasingly challenging, potentially leading some crypto-asset service providers to consider relocating outside of Türkiye to establish operations in jurisdictions with a more predictable regulatory environment.

Q&A Session II

1. *What is the regulatory stance on peer-to-peer transactions and self-custodial wallets in Türkiye?*

Anja von Rosenstiel asked about the regulatory emphasis on service providers in Türkiye. She sought clarification on whether peer-to-peer transactions through service providers are prohibited, and in particular asked about the role of self-hosted, self-custodial wallets and whether they are excluded from the regulatory framework in Türkiye.

Dr. von Rosenstiel also drew comparisons with regulatory approaches in the United States, noting the significant focus on intermediaries and service providers there. She referred to recent efforts by the U.S. Securities and Exchange Commission (SEC) to redefine what constitutes an exchange. This includes a draft rule change that proposes to include communication protocols as one of the non-discretionary methods to facilitate trading, effectively broadening the definition to encompass what would be considered a multi-trading facility (MTF) in Europe. She concluded her question by inquiring whether there are any initiatives in Türkiye to similarly expand the scope of service providers into new regulatory territories.

Cemre Polat clarified that peer-to-peer transactions are not prohibited under the current framework. She explained that such transactions are entirely free and governed by general provisions, such as contract law. However, she cautioned that individuals engaging in peer-to-peer transactions as a regular commercial activity on behalf of others would deem as unauthorized service provision.[55]

Pınar Çağlayan Aksoy echoed Polat's comments and provided further insights. She noted that non-custodial wallets are also used in Türkiye, highlighting ongoing debates about the limitations placed on peer-to-peer transactions. The key issue, according to Çağlayan Aksoy, revolves around enforcement—how the authorities would monitor and control these transactions. This question remains unresolved and continues to be a topic of discussion outside the regulatory sphere.

She also responded to the second part of von Rosenstiel's question concerning the regulatory approaches of the SEC and the Capital Markets Board. Çağlayan Aksoy emphasized that, unlike other jurisdictions such as the UK, where scholars are often consulted during the law-making process, the Capital Markets Board in Türkiye has not fully adopted this multilateral approach. While initial efforts were made to gather opinions, the process ultimately lacked transparency, leaving scholars and other stakeholders with limited insight into the Board's plans.

[55] Please see page 24.

Çağlayan Aksoy went on to outline the steps taken by the Board since July. The first step involved mapping out the ecosystem by identifying existing crypto asset service providers and understanding their operations. Subsequently, the Board outlined new obligations for platforms and their members. The regulatory focus then shifted to foreign crypto asset service providers, and this phase has since been completed. Looking ahead, the November deadline will be crucial for the Turkish crypto asset market, as the Board is expected to introduce further clarifications and details regarding specific types of crypto assets. Çağlayan Aksoy speculated that while the Board has not yet explicitly defined these categories in the law, it is likely to consider more specific regulations in the future.

2*. How can regulatory bodies address criminal liability in the crypto sector and foster international cooperation?*

Malik Feriani addressed the challenges posed by the decentralized and borderless nature of crypto assets, particularly concerning the establishment of effective international cooperation and legal frameworks. He inquired how regulatory bodies could address criminal liability associated with activities such as money laundering, terrorist financing, and market manipulation within the crypto asset sector. His question sought insight into potential strategies for harmonizing regulations across jurisdictions to tackle these global issues effectively.

Pınar Çağlayan Aksoy acknowledged the complexities of addressing criminal liability in the context of crypto assets, noting that her expertise lies in private law rather than criminal law. Nevertheless, she provided non-expert observations on the issue, emphasizing that the challenge is not limited to criminal liability but extends to civil liability as well. She highlighted the difficulty in determining applicable laws and jurisdictions when dealing with decentralized structures like Mangadao and other international entities. The complexity of pinpointing which country's laws should apply and which courts have jurisdiction over disputes adds to the legal challenges in this area.

Çağlayan Aksoy stressed that a key element in establishing effective international cooperation and legal frameworks is raising awareness. There is a need to enhance understanding across different jurisdictions regarding what constitutes a cryptocurrency and a crypto asset, as these definitions and perceptions vary globally. She suggested that international cooperation projects could be a way forward, focusing on educational initiatives that target both the general public and legal professionals.

In terms of criminal liability, Çağlayan Aksoy mentioned that organisations such as Financial Action Task Force (FATF) have been attempting to set standards regarding the regulation of financial instruments. However, she pointed out that these standards are not legally binding, which limits their effectiveness. Çağlayan Aksoy concluded by suggesting that an international convention could be a functional approach, but reiterated that her comments were based on general observations rather than expertise in criminal law.

3. *Is it appropriate to address civil liability in a legislative instrument which mainly pertains to supervision law?*

Florian Möslein expressed his thoughts on the concept of crypto trading being classified as an "abnormally dangerous activity," noting that this characterization was both intriguing and somewhat alarming. He then shifted to his main question, focusing on the regulatory approach to liability within the realm of crypto markets.

He pointed out that most discussions about crypto regulation tend to fall under supervision law, which is a branch of public law concerned with the oversight of crypto markets. Drawing a parallel to the European regulatory landscape, where the issue of liability often involves questions of jurisdictional competence between the EU and national states, Möslein questioned whether a similar situation exists in Türkiye. Specifically, he asked Çağlayan Aksoy if it is appropriate to regulate civil liability the framework of a supervisory law, or whether this responsibility should rather rest with the civil courts, which are typically tasked with determining the level of liability.

Pınar Çağlayan Aksoy began by providing historical context, explaining the usual stance within Turkish law. She noted that the Turkish Code of Obligations was amended in 2011, and until then, it was largely identical to the Swiss Code of Obligations. However, there was an initiative, particularly influenced by a bill in Switzerland (the "Antwerp Bill"), which aimed to reform tort law. Although this bill was suspended in Switzerland, Turkish lawyers had already drawn some elements from it, while omitting others.

Çağlayan Aksoy elaborated that the Swiss bill included the concept of liability for extremely dangerous events, but it also specified a "characteristic risk" as a necessary condition for imposing strict liability. This element of characteristic risk was not incorporated into the Turkish Code of Obligations. As a result, activities that do not inherently carry a characteristic risk might still be subject to strict liability under Turkish law. She illustrated this with a common example in Türkiye: if a person walks through the garden of a dangerous facility and trips, the incident might still be covered under strict liability because the element of characteristic risk is not required.

Çağlayan Aksoy further clarified that, traditionally, strict liability in Türkiye has been reserved for specific activities designated by law, such as nuclear facilities, genetic experiments, and highway traffic. Its own set of regulations governs each of these areas. She agreed with Möslein's observation, noting that it is unusual to introduce strict liability within the Capital Markets Act. This piece of legislation, which she described as a "patchwork act," has undergone numerous amendments, with crypto asset provisions now integrated, along with various principal decisions and announcements by the Capital Markets Board.

Çağlayan Aksoy concluded by stating that while the Board might have intended to introduce strict liability, this approach diverges from traditional legal practices in Türkiye. Historically, strict liability has been confined to separate, activity-specific laws, making its inclusion in the Capital Markets Act a departure from the norm. She emphasized that this is unorthodox, even within the context of Turkish legal standards.

4. How are crypto assets classified under Turkish civil law?

Florian Möslein raised a question regarding the classification of crypto assets under Turkish civil law. He asked Polat how these assets are defined: specifically, whether they are treated as property or as assets, despite their intangible nature. He emphasized that this issue had not been previously addressed during the discussion but deemed it a crucial question, expressing surprise that public lawmakers have not shown significant interest in clarifying this legal classification.

Cemre Polat began by referring to the article by Çağlayan Aksoy.[56] Addressing the legal nature of crypto assets under Turkish law, Polat noted that there is no definition of a movable property in the Turkish Civil Code. However, she pointed out that the element of tangibility is included in almost all definitions found in the literature. Polat argued for a more flexible approach, suggesting that the law should adapt to include new developments and evolving needs. Even if crypto assets are not directly classified as property, it is still possible to apply relevant rules through analogy, a method permitted by the Civil Code. She explained that, for example, natural resources and electricity are not directly categorized as property but are governed by rules related to movable property. Such an approach will also align with the recommendations of the UNIDROIT[57] which state that legal classification does not matter as long as it is allowed to have ownership and security rights over

[56] Pınar Çağlayan Aksoy, 'The Applicability of Property Law Rules for Crypto Assets: Considerations from Civil Law and Common Law Perspectives' (2023) 15 Law, Innovation and Technology 185.
[57] 'UNIDROIT Principles on Digital Assets and Private Law' (International Institute for the Unification of Private Law 2023) <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>.

such assets. The key is to enable legal structures that facilitate ownership, create security interests, and make it possible to use these assets for loans and other financial operations.

Additional Comments

Furthermore, Polat provided insights into the broader implications within the CMA. She spoke about the Customs Union Agreement between the European Union and Türkiye and noted ongoing yet politically complex negotiations between the EU and Türkiye. According to Polat, while Turkish law often mirrors EU legislation, there is a "silent political agreement" where compliance is prioritized only when it affects trade, such as in the case of product security, but not necessarily product liability.

Regarding crypto assets, Polat observed that MiFID II and MiCAR have extraterritorial effects, but the EU does not enforce alignment in Türkiye, giving Türkiye greater regulatory freedom within the CMA. She remarked that the provisions in the act reflect a strategy akin to the UK's approach, focusing less on binding regulatory rules and more on empowering regulatory authorities and encouraging collaboration between public bodies. However, when it comes to liability, she noted that the approach remains distinctly Turkish. Dr. Polat pointed out that, when faced with complex situations, Turkish lawmakers tend to implement straightforward, stringent solutions.

She illustrated this with an example related to online platforms. Recently, the Turkish legislature completely prohibited self-preferencing practices, where platform operators sell their own goods on their platforms. Citing the case of a well-known platform, Polat explained that the operator had to create a separate venue to sell its own products. She suggested that the strict liability rules in the CMA may stem from similar motivations, particularly following the Thodex scandal in 2021, which was a significant event that led to harsh regulatory responses. Dr. Polat concluded by stating that, in her view, these measures, though severe, are not surprising.

Çağlayan Aksoy added her perspective on the classification of crypto assets, acknowledging that the issue remains controversial in Turkey. She observed that the approach depends on whether one follows the more traditional Swiss path or adopts more modern perspectives.

Florian Möslein summarized the key insights from the discussion, emphasizing two main points. Firstly, he expressed that it was both fascinating and reassuring to see that, despite differences across jurisdictions, there are shared challenges and topics of concern in the realm of crypto regulation. This commonality suggests that similar issues are being addressed worldwide, providing a basis for comparative analysis.

Secondly, he highlighted the inherently political nature of crypto law. He referred to the earlier example regarding the adoption, or lack thereof, of European legal standards, which demonstrated that political considerations play a significant role in shaping crypto regulations. According to Prof. Dr. Möslein, it is crucial to keep these political dimensions in mind when attempting to understand the legal frameworks governing crypto assets.

Möslein proceeded the query: "As a lawyer working in Turkey, I would like to ask Pınar Çağlayan Aksoy's opinion on competent courts for disputes between crypto asset service providers and investors, since I think it will affect the liability rulings, especially for consumer courts and commercial courts. What is your answer to this?"

Çağlayan Aksoy addressed the question by emphasizing the importance of definitions in legal classification. She explained that if crypto assets can be granted the status of property, it would simplify handling issues across various legal fields, including inheritance, contract law, and private international law. However, she pointed out that while the Turkish government has recently defined what a crypto asset is, they have yet to clearly establish its legal character, unlike jurisdictions like Germany. This lack of a defined legal character contributes to the ongoing confusion regarding crypto assets in Turkey.

Çağlayan Aksoy noted that while there is no specific legislation concerning property law and crypto assets, Turkish courts have made rulings recognizing crypto assets as part of digital inheritance. She mentioned a 2021 decision by a higher court in Antalya, which allowed crypto assets to be passed on to heirs, provided the service platform retains the private keys. This practice has been implemented in Turkey, though it remains largely based on court decisions rather than explicit legislation.

She also highlighted a related issue: whether crypto users are considered consumers under Turkish law. This topic has been widely debated, as it directly impacts the application of consumer protection laws. Çağlayan Aksoy stressed that there appears to be a gap in how different laws interact, such as electronic commerce regulations and obligations for NFT platforms. She argued that lawmakers should have established clear guidelines on whether crypto platforms fall under consumer protection or platform obligations, but this has yet to happen.

In concluding her answer, Çağlayan Aksoy provided her perspective on which courts should handle disputes between crypto asset service providers and investors. She opined that, based on current practices, the competent court would likely be the commercial court rather than the consumer courts. This is because users are generally engaging in these transactions as part of investment activities rather than as consumers. Nevertheless, she acknowledged the need for a definitive ruling to clarify this legal ambiguity.