

Financial Law Review

No. 38 (2)/2025

UNIVERSITY OF GDAŃSK • MASARYK UNIVERSITY • PAVEL JOZEF ŠAFÁRIK UNIVERSITY
<http://www.ejournals.eu/FLR>

LADISLAV HRABČÁK*

MICA REGULATORY FRAMEWORK AND CYBERSECURITY: NEW HORIZONS OF CONSUMER PROTECTION IN SLOVAKIA¹

Abstract

With the growing popularity of crypto-assets, the number of cyber threats posing a significant risk to consumers is also increasing. Given this dynamic, it is essential to establish a robust institutional and legal framework to protect them. This article discusses new horizons in consumer protection against cyber attacks in the context of the MiCA (Markets in Crypto-Assets Regulation) and its application at the national level. The aim of this article is to identify cyber threats in crypto-asset markets and assess the new legal framework and institutional basis for protection against cyber attacks at the EU and Slovak levels. In examining this issue, we have established the following hypothesis: The new European MiCA regulation, in conjunction with the supervisory activities of the National Bank of Slovakia and other authorities, provides consumer protection against cyber threats in crypto-asset markets. The new

* The author is assistant professor at the Department of Financial Law, Tax Law and Economy, Faculty of Law, Pavol Jozef Šafárik University in Košice in the Slovak Republic. In his publications he focuses mainly on the relationship between law and modern technologies, as well as on tax evasion and the possibilities of their prevention.
Contact email: ladislav.hrabcak@upjs.sk, ORCID: 0000-0002-4670-3399.

¹ The article is the output of research activities within the project Cybersecurity Competence Center at Pavol Jozef Šafárik University in Košice (KC KB UPJŠ), project code: 17R05-04-V01-00007. This work was supported also by the Slovak Research and Development Agency under the Contract no. APVV-23-0158 and it is a partial output of the project VEGA no. 01/0698/25 „Development fee as a tool for the development of municipalities and cities in the Slovak Republic“.

legislation contains several measures that have the potential to contribute to consumer protection in crypto-asset markets. However, there are certain shortcomings that should be addressed in the future to improve and strengthen this specific type of protection. The analysis and synthesis methods were primarily used to address this issue, supplemented by historical and comparative methods.

Key words: MiCA, crypto-assets, cybersecurity, consumer

JEL Classification: K24

1. Introduction

The current digital age is characterized by constant growth in technological innovation, but at the same time faces an unprecedented increase in cyber threats. These threats are no longer just a theoretical risk, but pose a real danger to global financial systems, critical infrastructure, and, last but not least, consumers. The dynamically developing crypto-asset markets have proven to be a particularly vulnerable sector that attracts the attention of cyber attackers. Despite their innovative potential and growing popularity, these digital assets are often the target of sophisticated attacks, leading to significant financial losses for investors and undermining confidence in the entire sector.

In response to these risks, Regulation (EU) No 2023/ 1114 on markets in crypto-assets (hereinafter also referred to as “MiCA”) was adopted at the European Union (hereinafter also referred to as “EU”) level, with the aim of creating a uniform and secure legal framework for markets in crypto-assets. This regulation represents a groundbreaking legislative act, the main objective of which is to establish a uniform and comprehensive legal framework for markets in crypto-assets. Until its adoption, there was no comprehensive legal regulation in the EU [Bočánek 2021: 37–53], which led to market fragmentation and considerable legal uncertainty for both service providers and investors.

The MiCA Regulation aims not only to protect consumers and investors from fraud and manipulation, but also to promote financial stability and prevent money laundering and terrorist financing. It introduces strict rules for crypto-asset issuers, such as transparency requirements, the obligation to publish whitepapers, and ensuring the proper functioning of their services. At the same time, it sets licensing conditions for crypto asset service providers, which should significantly increase their credibility and accountability.

In this way, the EU is seeking to ensure that the growing crypto-asset market operates in a regulated and predictable environment, thereby minimizing cyber risks and strengthening confidence in the entire sector.

The issue of crypto-assets, as well as other phenomena² brought about by the industrial (digital) revolution 4.0 [Popovič, Sábo 2022: 1–16], is one of the current topics in financial law [Babčák, Cakoci, Štrkolec 2017: 98–102] and other legal disciplines. This is also confirmed by the increasing number of publications devoted to this issue [e.g. Kačaljak, Katkovčín 2021: 195–205]. Although there is a relatively extensive body of literature devoted to the phenomenon of crypto assets [e.g., Wolf 2017, Tumpel, Kofler 2019: 177–188, Srokosz 2021: 54–63, Štrkolec 2022: 99–115, and others], we have identified a lack of publications focusing on the identification of cyber threats in the crypto-asset market and new European measures addressing them.³ We also perceive a relatively low level of interest among the scientific community in examining the role and position of national and European supervisory authorities in the crypto-asset market, which we believe will change in the near future.

Based on the above, we have set ourselves the goal of this article to identify cyber threats in crypto-asset markets and assess the new legal framework and institutional basis for protection against cyber attacks at the EU and Slovak Republic level, while verifying the established hypothesis: The new European MiCA regulation, in conjunction with the supervisory activities of the National Bank of Slovakia and other authorities, provides consumer protection against cyber threats in crypto-asset markets.

A combination of several scientific methods was used to achieve the above-stated goal of this article and to verify the hypothesis. In the first phase of the research, the analysis and synthesis of existing literature and legislation was key, enabling the identification and systematic classification of the main cyber threats in crypto-asset markets and the measures to eliminate them. Subsequently, a comparative method was applied, comparing the new

² In addition to crypto assets, other “digital phenomena” include digital services (Simić 2021: 194–214) and the sharing economy (Cakoci, Červená 2021: 37–43; Vartašová, Červená, Olexová 2022: 433–440).

³ The author Jurkowska-Zeidler, A. (2016) in her monograph “The architecture of the European financial market: Legal foundations” maps the legislative development of the European financial market. The monograph covers several crises but was written before the adoption of MiCA. However, it is also possible to build further research on this relatively new area.

MiCA regulation with the legal frameworks and regulatory practices that were in place in the EU and Slovakia prior to its adoption. This method allowed us to assess the scope and quality of the changes that MiCA brings in the area of consumer protection. An important part of the research was also the historical method, which was applied to examine the development of legislation and cyber risks in the crypto-asset sector, helping to understand the context and need for the adoption of the MiCA regulation.

2. Cyber risks for consumers in the crypto-asset market

In recent years, crypto-assets have become widely accessible to the general public, not just to tech-savvy individuals. It is therefore no surprise that there has been an enormous increase in various crypto projects, as well as an increase in the value of traded capital on the crypto-asset market, etc. Directly proportional to this trend is the increase in the number of various fraudulent activities to which individuals are exposed on the crypto-asset market.

Cyber threats are particularly prevalent in the crypto-asset market because transactions are virtually irreversible and, once lost, it is almost impossible to recover these assets or their equivalent in cash corresponding to their value at the time of the transaction, for various reasons.

Very common fraudulent practices in the crypto-asset market, and therefore not only in the digital space, include:

- **phishing:** This is the most common method of attack, in which perpetrators attempt to obtain the login details of the person concerned or the so-called “seed phrase” (a series of words for wallet recovery). To this end, various fake emails, SMS messages, or websites are used that pretend to be legitimate crypto asset service providers (e.g., exchanges or crypto asset wallets). Once the identification data has been entered, the attackers immediately transfer the crypto-assets to their accounts, thereby removing them from the owner’s control. The anonymity of the attackers and the anonymity of the transactions lead to losses that in many cases are not compensated due to the impossibility of tracing the attacker. Phishing is an illegal activity that occurs throughout the financial sector [Streiber, Pöhn 2025: 239–251].
- **malware and viruses:** This is another cyber threat/danger that can be encountered in the crypto-asset market [Darmawansyah, Djunaedi,

Kristiawanto 2023: 2393–2401]. This threat consists of attackers installing malicious software on a device (usually a computer or mobile phone) that can record keystrokes, take screenshots, or directly access a crypto wallet when its owner is logged in. In this regard, IT recommendations include following safe browsing practices and avoiding unknown and untrustworthy websites [Cryptocurrencies and Security: How to Protect Your Investments]. Up-to-date antivirus software also plays a very important role in protecting individuals and can significantly contribute to consumer protection.

- **vulnerabilities of crypto exchanges and crypto wallets:** Although reputable crypto exchanges and crypto wallets are protected, there is always a risk that their systems may be attacked by third parties [Kirobo 2025: 580–590]. An interesting solution in this regard is the use of so-called hardware wallets, which are becoming increasingly popular among “investors.” This type of wallet allows investors’ private keys to be stored offline and is therefore rightly considered the most secure form of storage.
- **unsecured network:** Trading crypto-assets on an unsecured network poses a major cyber threat from the consumer’s perspective. Although the blockchain technology itself, which is the basis for crypto-assets such as Bitcoin [Bitcoin: A Peer-to-Peer Electronic Cash System], is inherently very secure, the weakest link is always the user and the way they access their accounts and wallets. When conducting transactions with crypto-assets on a public Wi-Fi network, users expose themselves to the risk that attackers can intercept data using specialized software. When conducting crypto-assets transactions on a public Wi-Fi network, users expose themselves to the risk that attackers may use specialized software to intercept data and gain access to their accounts. It is therefore always necessary to use a secure, preferably private, network.

In addition to the above-mentioned threats, others may also arise in the crypto-asset market. All risks were exacerbated by the fact that the crypto-asset market was unregulated for a long time, which led to many uncertainties. However, the situation is changing with the arrival of new European legislation. Prior to the adoption of MiCA regulation, the legal regulation of the crypto-asset market was characterized by several problems:

- **insufficient consumer protection:** In the past, investors in crypto-assets were not protected by the same rules as consumers in the traditional financial market (e.g., mechanisms for protecting deposits or other investments). This is naturally due to the fact that crypto-assets are outside the supervision of states and their central banks. Therefore, it cannot be expected that consumer protection will be at the same level as traditional financial market instruments in the future. However, with the adoption of new legislation at EU level, at least some degree of protection should be ensured by subjecting the crypto-asset market to legal regulation (see below).
- **fraudulent schemes:** Since the crypto-asset market was unregulated, a number of fraudulent projects, known as “rug pulls,” emerged. The essence of these projects is that developers terminate the crypto project and flee with investors’ funds. The MiCA regulation should also address such situations, as one of its ambitious goals is to reduce the number of such cases by introducing several obligations (e.g., the obligation to publish whitepapers).
- **existence of unregulated entities:** Although the MiCA Regulation has been adopted, there are still entities operating on the market that are not authorized to provide crypto-asset services. This is because crypto-asset service providers were given an additional period to obtain all the necessary documents required for the licensing process. It is important to note that it is essential to use only verified and licensed platforms. National institutions will maintain a register of such entities, which can greatly assist in verifying the legitimacy of a particular crypto asset service provider.

In the following text, we will attempt to clarify the impact that MiCA regulation will have on consumer protection, what we see as the benefits of the new legislation in the area of consumer protection, and we will focus in particular on the role of supervisory authorities within the consumer protection system in the crypto-asset market.

3. MiCA regulation and its impact on consumer protection

As mentioned several times in this article, the MiCA regulation represents a fundamental shift in the financial and legal regulation of the crypto-asset market within the EU. Until its entry into force, the crypto-asset market was

characterized by considerable legal uncertainty and fragmented regulation, which had a direct negative impact on the level of consumer protection in this area. The MiCA regulation introduces a comprehensive and harmonized legal framework that significantly strengthens the protection of investors in these digital assets in several respects, namely:

1. increased transparency and information requirements for crypto-asset issuers,
2. regulation of the status of crypto-asset service providers (hereinafter also referred to as “CASP”) and introduction of supervision,
3. regulation of stablecoins,⁴ and
4. preventive measures against market abuse in the crypto asset market.

In order to provide a comprehensive overview of the impact of MiCA regulation, we will systematically analyse the key mechanisms that the regulation introduces to protect consumers. In our opinion, these four main areas represent the fundamental pillars of the new legislation and the protection of individuals in the crypto-asset market.

3.1. Increased transparency and information requirements for crypto-asset issuers

One of the most significant contributions of the MiCA regulation is the introduction of strict transparency requirements and information obligations for issuers of crypto-assets. In this context, we believe it is necessary to mention the so-called whitepaper. This document must be approved by the competent authority of the EU Member State and must contain clear, accurate, and non-misleading information about the crypto-asset, as well as information about any risks, the rights and obligations of the issuer, and the technology (e.g., blockchain) on which it is based [Whitepaper according to MiCA regulation].

We believe that this obligation under MiCA regulations significantly reduces the risk of information asymmetry, which was typical of the unregulated crypto-asset market. Under the new legislation, consumers gain access to standardized and verifiable data on specific digital assets, enabling them to make investment decisions. If an issuer violates these obligations

⁴ Stablecoins are a type of crypto asset whose value is supposed to be relatively stable and is tied to a currency in the true sense of the word (e.g., USD) or a commodity (e.g., gold).

and provides false or misleading information in the whitepaper, they are liable for such a violation under MiCA and face the associated legal consequences, thereby increasing consumer protection, which is receiving increased attention at the EU level [Vojčík 2012: 386–395].

3.2. Regulation of the status of CASP and introduction of supervision

Another key benefit of MiCA regulation is that this legal act introduces a licensing regime for all entities wishing to provide crypto-asset services in the EU (e.g., crypto-asset exchanges, advisory services, etc.). In order to obtain a license, these entities must meet relatively strict conditions, which we will not discuss in detail here due to the breadth of the issue [Hrabčák, Štrkolec 2024: 27–45].

All requirements set out in the MiCA regulation aim to create a trustworthy and transparent environment that eliminates fraudulent projects and other illegal activities described above. Thanks to the granting of a license and constant supervision by the relevant national authorities (in the Slovak Republic, this is the National Bank of Slovakia), consumers are protected against CASP failure and unfair practices. We will discuss the issue of supervision, as an essential component of individual protection in the crypto-asset market, in more detail in the next section of this article.

3.3. Regulation of stablecoins

The MiCA regulation pays particular attention to stablecoins, which pose a potential systemic risk to financial stability. Although these types of crypto-assets should maintain a stable value, as their name suggests, recent events related to the TerraUSD/LUNA stablecoin have convinced us that the opposite is true [To Sue Firm Behind Failed Terra Stablecoin, Terraform Labs].

It is therefore not surprising that European regulators have also focused their attention on regulating this type of crypto-asset with a declared stable value. For this reason, under the MiCA regulation, stablecoin issuers have a number of obligations, the most notable of which are:

- **maintain sufficient reserves:** From a value preservation perspective, we consider this requirement to be essential. In accordance with the MiCA regulation, reserves must be held in safe and liquid assets,

separate from the issuer's assets. This ensures that stablecoin holders can convert their tokens into fiat currency at any time.

- **meet governance and transparency requirements:** Issuers must have robust governance mechanisms in place and regularly publish audits of their reserves, eliminating the risk of situations such as the one described above involving the TerraUSD stablecoin.

In our opinion, this relatively strict regulation increases confidence in stablecoins as a more stable form of these digital assets and protects consumers from their sudden devaluation.

3.4. Preventive measures against market abuse in crypto-assets

In addition to the above-mentioned impacts of the MiCA regulation, rules are also being introduced to prevent and punish market abuse [Saenz 2025: 285–305], which are inspired by the regulation of traditional financial markets. These include, in particular, a ban on insider trading, unauthorized disclosure of confidential information, and market manipulation [European crypto-assets regulation (MiCA)]. These measures aim to contribute to the integrity of the crypto-assets market and ensure that the trading environment is fair and transparent for all participants, including retail investors (especially consumers). MiCA thus complements existing EU legislation, which pursues a very similar purpose. Taken together, European legislation can have a synergistic effect and contribute to the elimination of various unfair practices occurring in the crypto-asset market.

4. The role of supervisory authorities in consumer protection under MiCA

One of the fundamental changes that will come with the adoption of MiCA regulation is the role of supervisory authorities in consumer protection in the crypto-asset market. Of course, it is necessary to emphasize that crypto-assets have not been and will never be under the complete supervision of state institutions, but the introduction of several obligations for crypto-asset issuers or CASPs also requires supervision and an adequate sanction mechanism in case of non-compliance.

Central banks will play a major role in the implementation of supervision and enforcement of compliance, which naturally follows from their position within the institutional framework. In the Slovak Republic, this is the National

Bank of Slovakia. However, in addition to central banks, other supervisory authorities will also play a complementary but no less important role. In the following text, we will attempt to clarify their position and how they contribute to consumer protection in the crypto-asset market. The adoption of MiCA should bring about a qualitative change, but as we will point out, the applicability of some rules may be more than just problematic.

4.1. The National Bank of Slovakia and consumer protection in the crypto-asset market

The National Bank of Slovakia (hereinafter referred to as “NBS”), which is an independent central bank, plays an irreplaceable role in consumer protection in the crypto-asset market. The existence of the NBS is directly provided for by the Constitution of the Slovak Republic No. 460/1992 Coll. as amended (hereinafter referred to as the “Constitution of the Slovak Republic”), while its status is specified in Act No. 566/1992 Coll. on the National Bank of Slovakia, as amended (hereinafter referred to as the “the NBS act”)⁵.

Until MiCA was adopted, lawmakers left the NBS Act unchanged, without any amendments prompted by the boom in crypto-assets, and did not make any major changes. There are several reasons for this approach, but primarily because crypto-assets are not issued by the state, are decentralized, and have other specific characteristics compared to currencies in the true sense of the word. However, time has shown us that this approach was not correct and that it was very important to adopt certain measures, which could have prevented many frauds. The desired change only came with the adoption of the MiCA regulation.

As already outlined, the new European legislation envisages entrusting certain competences in the area of crypto-asset markets to national financial authorities, thereby respecting the existing structure of national financial authorities in EU Member States [Babčák, Čakoci, Štrkolec 2017: 103–104]. As far as the Slovak Republic is concerned, many tasks will be performed by the NBS, which is a natural outcome of the historical development and position of this authority within the hierarchy of national financial authorities.

⁵ The importance of this national financial authority is further enhanced by the fact that the Constitution of the Slovak Republic also regulates its internal organizational structure (in terms of its highest governing body, which is the Bank Board), which is regulated and governed in more detail by the NBS act.

Member States had to respond to the adoption of the MiCA regulation by adopting an adequate national legislative framework, even though the provisions of the regulation, as a legal act, are, taking into account Article 288 of the Treaty on the Functioning of the EU, directly applicable and enforceable in all EU Member States without the need for further transposition. In the Slovak Republic, Act No. 248/2024 Coll. on certain obligations and rights in the field of crypto-assets and on amendments to certain acts (hereinafter also referred to as the “MiCA Act”) was adopted. In the post-MiCA era, the position of the NBS in the area of consumer protection in crypto-asset markets has changed fundamentally. The MiCA Act contains a relatively wide range of tools for the NBS, and for the purposes of this article, we will focus in more detail on selected ones.

As mentioned above, the NBS performs a number of activities that can be categorized into several areas for academic purposes, specifically:

- **regulatory and advisory activities:** In this context, it is necessary to begin by quoting Article 56(1), second sentence, of the Constitution of the Slovak Republic: “The National Bank of Slovakia may, within the limits of its competence, issue generally binding legal regulations if it is authorized to do so by law.” The MiCA Act contains several provisions authorizing the NBS to issue generally binding legal regulations, in particular:
 - authorization for the NBS to determine the criteria for assessing the professional knowledge of natural persons as CASPs (§ 4(3)),
 - the NBS’s power to determine the templates, structure, scope, content, form, breakdown, deadlines, method, procedure, and place of submission of reports, statements, and other documents of obligated persons (§ 5), etc.

In addition, the NBS may participate in the preparation of draft laws and submit them to the Government of the Slovak Republic. However, it should be added that the central bank itself does not have the right of legislative initiative. Another important power of the NBS is the preparation of opinions on draft laws for government deliberation and the performance of an advisory function towards the Government of the Slovak Republic within the scope of its competence (among other things) in the area of crypto-assets.

- **decision-making activity:** Decision-making is an important activity of the NBS, which has been strengthened by MiCA regulation

and extended to the area of crypto-assets. Following the adoption of MiCA, services related to crypto-assets are licensed activities, with the authority to issue licenses for the provision of crypto-asset services falling within the remit of the NBS. As part of this process, the central bank will assess whether the conditions for providing crypto-asset services have been met [Hrabčák, Štrkolec 2024: 27–45]. Related to this is the fact that the NBS is authorized to decide on the imposition or non-imposition of sanctions on obligated persons in the field of crypto-asset markets, which, in our opinion, significantly strengthens consumer protection in crypto-asset markets.

- **supervisory activity:** Supervision by the NBS is also a key element of consumer protection in the crypto-asset market. The new MiCA regulation imposes a number of obligations on certain persons (CASP or crypto-asset issuers). The central bank will thus supervise whether the supervised entities comply with regulatory requirements (e.g., compliance with minimum requirements for own funds, compliance with prescribed requirements for company management and control, ensuring the security of clients' funds and crypto-assets, etc.), but also whether supervised entities fulfil their obligations under other legal acts⁶. As we will point out below, mutual assistance and cooperation with other supervisory authorities at European or national level will be important in this regard.
- **information activity:** The NBS informs consumers and the wider public about the safe use of crypto-assets and how to recognize crypto fraud⁷. We view this educational approach very positively. The NBS also provides information at the level of individual state authorities in the field of crypto assets. Equally important is the provision of information to supranational (European) authorities, as we will further highlight below.

In our opinion, the NBS's activities, which we have attempted to clarify above, will undoubtedly contribute to the protection of individuals in the crypto area. For now, it remains to be seen how effective these measures will be. One of the problems we see is the possible differences between national

⁶ An example of this is whether supervised entities fulfil their obligations under DORA regulations or also supervision in the AML area (which complements law enforcement authorities).

⁷ The NBS publishes this information in a relatively comprehensive form on its website www.nbs.sk.

legal regulations adopted for the effective implementation of the measures introduced by the MiCA regulation, which will likely lead to different conditions for entrepreneurs in this area. Paradoxically, this situation may lead to greater or lesser conflicts with the principles on which the EU's single internal market is built. In addition, the actual enforceability of the rules on the exchange of information, assistance and cooperation between EU Member States, but especially the rules on assistance and cooperation with non-EU Member States (Article 107 MiCA), remains controversial.

4.2. The roles of other supervisory authorities in the crypto-asset market

Supervision of the crypto-asset market by the relevant authorities is key to ensuring stability and consumer protection in the digital financial environment. Although the NBS has the primary role in Slovakia, the effectiveness of this supervision depends on cooperation with other authorities at European and national level. Together, these authorities form a comprehensive system that regulates the crypto-asset market in accordance with the MiCA Regulation and relevant national legislation.

The EU and its leaders are fully aware that cyber threats know no borders and have therefore created a unified legislative framework and equipped the existing institutional framework with additional powers to ensure the protection of individuals in the crypto-asset market. The European institutional framework includes, in particular, the European Banking Authority (hereinafter also referred to as "EBA"), the European Securities and Markets Authority (hereinafter also referred to as "ESMA") and, finally, the European Insurance and Occupational Pensions Authority (hereinafter also referred to as "EIOPA").

The EBA specializes in the regulation and supervision of asset-referenced tokens (referred to as ARTs) and electronic money tokens (also known by the abbreviated term EMTs). The EBA even issued an official statement on July 5, 2024, addressed to consumers [EBA statement]. As the popularity of stablecoins grows, it is essential that they be strictly regulated, which is changing to some extent with MiCA regulation (see above). The role of the EBA, as the supervisory authority at EU level, is to ensure that issuers of these tokens meet strict requirements for governance, capital, liquidity, and reserves, which serve as a guarantee for token holders. In the event of a systemic failure of stablecoins, financial stability could be

disrupted, as the amount of capital contained in these assets is relatively high and significant. Therefore, EBA supervision of these tokens is crucial. In addition, the EBA is also tasked with developing regulatory technical standards and guidelines to ensure a harmonized approach to crypto-assets regulation across the EU⁸. It works closely with national supervisory authorities to ensure consistent implementation and enforcement of MiCA rules, which, as we have already mentioned, is quite crucial.

ESMA has broader powers in the area of market supervision and can be said to complement the EBA's activities in this area. This European authority is responsible for CASPs, especially when they operate across EU Member States. ESMA also issues opinions on current developments in the crypto-assets market. Among recent and very important opinions, we can mention the one from July 15, 2025, which concerned the provision of unregulated CASP services [Avoiding Misperceptions: Guidance for Crypto-Asset Service Providers Offering Unregulated Services]⁹. Its main task is to coordinate the activities of national authorities (in the Slovak Republic, this is the NBS, as already mentioned) to ensure the uniform application of the MiCA regulation in all Member States. ESMA also sets technical standards and guidelines (for whitepapers, CASPs, etc.), thereby increasing the transparency, credibility, and security of the entire market. This also shows how ESMA complements similar activities carried out by the EBA. ESMA also focuses on preventing and punishing market abuse, such as manipulation and insider trading.

Furthermore, EIOPA's involvement in the supervision of the crypto-asset market is limited, but in our view it plays an important role in assessing the risks that crypto-assets pose to the insurance and pension sector, and therefore this authority cannot be overlooked in the context of assessing the activities of other supervisory authorities at EU level. This body also monitors how volatility and cyber threats could affect assets managed by insurance companies and pension funds, and this is where we see a fundamental overlap with the area of crypto-assets.

⁸ The NBS has already adopted several methodological guidelines in response to the EBA guidelines at the European level. An overview of the EBA guidelines adopted by the NBS is published on the central bank's website, which we consider very positive in terms of transparency and predictability of public authorities' actions in this area.

⁹ It should be noted that, in addition to regulated services in the field of crypto assets, there are still activities that fall outside the legal and regulatory framework. This is a certain weakness of the current regulation, which we believe will be remedied in the near future.

As can be seen, each of the European authorities listed above fulfils a specific role to ensure comprehensive protection across the EU financial system, including in the context of new digital technologies, such as crypto-assets. All three authorities, collectively referred to as the European Supervisory Authorities, work together to make the regulatory framework in the EU as effective as possible, which also applies to MiCA regulations.

Cooperation between these European authorities and national supervisory institutions, such as the NBS in Slovakia, is fundamental to the successful implementation of the MiCA regulation. Their joint efforts ensure that the same rules are followed in the crypto-asset market and that consumers are protected regardless of the Member State in which they are established. For these reasons, the hypothesis set out in the introduction to this article has been confirmed. A European solution to this issue has been long overdue. We believe that this comprehensive and coordinated approach is essential to manage the dynamic cyber risks in this sector and to promote individuals' trust in the entire crypto-asset ecosystem. The same applies to the organizational and legal basis of supervisory authorities, consisting of a structure of national authorities supplemented by European supervisory authorities that will harmonize procedures within EU member states.

5. Conclusion

In this article, we have attempted to systematically analyse cyber risks in the crypto-asset market and assess the new legal and institutional framework for consumer protection in the crypto-asset market at the EU level and specifically in the Slovak Republic. This corresponds to the objective of the article set out in its introduction. In our research, we identified several cyber threats to consumers (individuals) that are very widespread in practice, such as phishing, malware, and the vulnerability of individual platforms. We also assessed how the new MiCA regulation addresses these risks through a number of measures it introduces, but above all through rules on increased transparency, the introduction of a relatively strict licensing regime for CASPs, the regulation of stablecoins, and finally the establishment of rules against market abuse.

An analysis of the adopted rules and the creation of an institutional framework led us to conclude that the hypothesis – that the new European MiCA regulation, in conjunction with the supervisory activities of the National Bank

of Slovakia and other authorities, provides consumer protection against cyber threats in crypto-asset markets – was confirmed with certain reservations, which we have attempted to outline and describe, along with the specific reasons for our concerns and reservations.

Although MiCA and related European or national regulations do not provide absolute protection, as no regulation can completely eliminate the risks associated with the decentralized nature of crypto-assets, they significantly strengthen consumer legal protection and reduce legal uncertainty in the market. It should be added that full supervision and regulation is not desirable, as crypto-assets are not issued by states or supranational organizations.

Measures such as the introduction of supervision of CASPs, mandatory disclosure of whitepapers, and regulation of stablecoins create a safer and more predictable environment for all stakeholders in the crypto-asset market, which we view very positively. National authorities such as the NBS, which has been granted extensive supervisory powers over crypto-asset issuers and CASPs, also play an important role in this process. In addition, synergy with other European authorities, such as ESMA and EBA, should ensure the most comprehensive and harmonized approach by the competent authorities of EU Member States.

In conclusion, the new legislation represents a significant qualitative step forward, but for it to be fully effective, it will be necessary to enforce the rules effectively and consistently at the national level and to cooperate internationally, especially with authorities from non-EU member states, which may be problematic, but at this point it is impossible to draw premature conclusions on this issue. Only practice will show to what extent it will be possible to translate theoretical assumptions into a real reduction in cyber risks in the crypto-asset market for consumers, who are highly vulnerable without adequate legislative and institutional support.

References

Babčák, V., Čakoci, K., Štrkolec, M. Finančné právo na Slovensku [Financial law in Slovakia]. Bratislava: EPOS, 2017

Bočánek, M.: First draft of crypto-asset regulation (MiCA) with the European Union and potential implementation, *Financial Law Review*, nr 22 [2], 2021, DOI: <https://doi.org/10.4467/22996834FLR.21.011.13979>

Čakoci, K., Červená, K., Výzvy a perspektíva zdaňovania v prostredí zdieľanej ekonomiky [Challenges and perspectives of taxation in the sharing economy environment] (in:) Szakács, A. et al. (eds.): Bratislavské právnické fórum 2021: Aktuálne výzvy pre finančné právo : zborník príspevkov z medzinárodnej vedeckej online konferencie [Bratislava Legal Forum 2021: Current challenges for financial law], Bratislava: Univerzita Komenského v Bratislave, 2021

Darmawansyah, A., Djunaedi, D., Kristiawanto, K.: Legal Protection of Cryptocurrency Users Against Cybercrime Attacks, *Journal of Social Research*, nr 2 [7], 2023, DOI: <https://doi.org/10.55324/josr.v2i7.1256>

Hrabčák, L., Štrkolec, M.: EU Regulation of the Crypto-Assets Market, *Bialystok Legal Studies*, nr. 1 [29], 2024, DOI: <https://doi.org/10.15290/bsp.2024.29.01.02>

Jurkowska-Zeidler, A. The architecture of the European financial market: Legal foundations. Gdańsk: Gdańsk University Press, 2016

Kačaljak, M., Katkovič, M., Kryptoaktíva ako finančné účty [Cryptoassets as financial accounts] (in:) Štrkolec, M., et al. (eds.): IV. Slovensko-České dni daňového práva: Zdaňovanie virtuálnych platidiel a digitálnych služieb – COVID-19 a iné aktuálne výzvy pre daňové právo. Recenzovaný zborník vedeckých prác. [IV. Slovak-Czech Tax Law Days: Taxation of Virtual Currencies and Digital Services – COVID-19 and Other Current Challenges for Tax Law. Peer-reviewed Proceedings of Scientific Papers], Košice: ŠafárikPress, 2021

Kirobo, A.: Security Vulnerabilities of Cryptocurrency Wallets – A Systematic Review, *FUOYE Journal of Engineering and Technology*, nr 9 [4], 2025, DOI: <https://doi.org/10.4314/fuoyejet.v9i4.4>

Popovič, A., Sábo, J.: Taxation of Robots an AI – Problem of Definition, *Financial Law Review*, nr 1 [25], 2022, DOI: <https://doi.org/10.4467/22996834FLR.22.001.15651>

Saenz, E. M., Regulating Market Abuse in Crypto Assets (in:) Sempere, P. C. (eds.): Governance and Control of Data and Digital Economy in the European Single Market, Springer, 2025

Simić, S.: Regulation and Taxation of Digital Services in Accordance with the Initiatives of the European Union, *Financial Law Review*, nr 4 [24], 2021, DOI: <https://doi.org/10.4467/22996834FLR.21.040.15407>

Srokosz, W.: Prawna regulacja kryptoaktywów, tokenów płatniczych oraz pieniądza elektronicznego w UE [Legal regulation of cryptoassets, payment tokens and electronic money in the EU], *Monitor Prawa Bankowego*, nr 9, 2021

Streiber, R., Pöhm, D.: Legal and ethical considerations when conducting phishing experiments in Germany, *International Cybersecurity Law Review*, nr 6 [3], 2025, DOI: <https://doi.org/10.1365/s43439-025-00148-2>

Štrkolec, M.: Virtuálne meny (právna podstata, regulačný rámec a zdaňovanie) [Virtual Currencies (Legal Nature, Regulatory Framework, and Taxation)], *Acta Universitatis Carolinae Iuridica*, nr 4 [68], 2022, DOI: <https://doi.org/10.14712/23366478.2022.49>

Tumpel, M., Kofler, J.: Tax treatment of digital currencies (in:) Haslehner, W. et al. (eds.): *Tax and the digital economy: Challenges and proposal for reform*, Alpehn aan den Rijn: Wolters Kluwer, 2019

Vartašová, A., Červená, K., Olexová, C., *Taxation of Accommodation Services Provided in the Framework of the Collaborative Economy in the Slovak Republic* (in:) *Proceedings of the 5th International Conference on Tourism Research*, Porto: Academic Conferences International Limiter, 2022

Vojčík, P. et al. *Občianske právo hmotné [Civil substantive law]*. Martin: Aleš Čeněk, 2012

Legal Acts

Treaty on the Functioning of the EU (EUR-Lex, OJ C 202, as amended)

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 (EUR-Lex, PE/54/2022/REV/1, as amended)

Constitution of the Slovak Republic No. 460/1992 Coll. as amended (SLOV-LEX, as amended)

Act No. 248/2024 Coll. on certain obligations and rights in the field of crypto assets and on amendments to certain acts (SLOV-LEX, as amended)

Act No. 566/1992 Coll. on the National Bank of Slovakia, as amended (SLOV-LEX, as amended)

Internet Resources

EBA statement

Available at: <https://www.eba.europa.eu/sites/default/files/2024-07/7dcd9ce9-96e3-4c5c-8d86-39d7784d1f03/EBA%20statement%20on%20Application%20of%20MiCAR%20to%20ARTs%20and%20EMTs.pdf>, accessed: 23th August 2025

Avoiding Misperceptions: Guidance for Crypto-Asset Service Providers Offering Unregulated Services

Available at: https://www.esma.europa.eu/sites/default/files/2025-07/ESMA35-1872330276-2329_-_MiCA_Statement_Access_to_Unregulated_Activities.pdf, accessed: 23th August 2025

Wolf, K.: Náš postoj ke kryptoměnám? Nepomáhat, nechránit, neškodit, nevodit za ruku [Our stance on cryptocurrencies? Not to help, not to protect, not to harm, not to lead by the hand]

Available at: www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/Nas-postoj-ke-kryptomenam-Nepomahat-nechranit-neskodit-nevodit-za-ruku/, accessed: 19th August 2025

Havlíčková, B.: Whitepaper podle nařízení MiCA [Whitepaper according to MiCA regulation]

Available at: <https://www.epravo.cz/top/clanky/whitepaper-podle-narizeni-mi-ca-115942.html>, accessed: 19th August 2025

Nariadenie o európskych kryptoaktívach [European crypto-assets regulation (MiCA)]

Available at: <https://eur-lex.europa.eu/SK/legal-content/summary/european-crypto-assets-regulation-mica.html>, accessed: 19th August 2025

Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System

Available at: <https://bitcoin.org/bitcoin.pdf>, accessed: 13th August 2025

Kovár, Ľ.: Kryptomeny a bezpečnosť: Ako chrániť svoje investície [Cryptocurrencies and Security: How to Protect Your Investments]

Available at: <https://kryptomagazin.sk/kryptomeny-a-bezpecnost-ako-chranit-svoje-investicie/3/>, accessed: 19th August 2025

Taylor, S.: SEC To Sue Firm Behind Failed Terra Stablecoin, Terraform Labs

Available at: <https://bitcoinist.com/sec-sue-terraform-labs/>, accessed: 19th August 2025