Luiss Guido Carli

Department of Economics and Finance

Crypto-Assets: Policy Evaluation in Frauds and Risks

Author:

Silvio De Simone

Supervisor:

Giacomo Morelli

Co-supervisor:

Paola Lucantoni

Academic Year 2024/2025

Contents

Chapter 1

Digital Currencies: Concepts and Challenges

1.1 Introduction

The crypto world is one of the fastest-growing sectors globally. During the last decade, according to data from CoinMarketCap, the overall market capitalization of cryptocurrencies increased from just under 4 billion euros in January 2015 to almost 3.5 trillion euros in January 2025, an amount approximately 875 times greater. In contexts such as this, where the expansion of a new sector occurs at an exceptionally rapid pace, it is expected that, although with inevitable delays, legislation will eventually adapt to the new challenges posed by such disruptive technology. Precisely during this period of regulatory uncertainty, fraudulent schemes and scams tend to proliferate, creating what has often been described as a "digital Wild West". The first chapter provides a general overview and specific details of the crypto-assets world and European legislation, while the second chapter focuses on the legal framework surrounding crypto-assets in Europe. Lastly, the third chapter focuses on the analysis of the Markets in Crypto Assets Regulation (MiCAR). It has been chosen as the object of the analysis due to its relevance in the European (and potentially global) landscape, its recency, and its completeness. MiCAR will also definitely impact future innovation in the European FinTech sector, although it is not a direct part of the quantitative analysis. It is also important to remember that the use of econometric tools and methodologies to analyze the effect of specific regulations is fundamental to creating the best possible legislation, and its importance grows with public interest in the market. According to Aerts et al. (2025), ”*The market capitalisation of crypto-assets has surged recently, fuelled by positive and broadening investor interest, including from traditional finance*” and their statement finds empirical confirmation from the data displayed in Figure 1.1. It is clear that in this environment of increasing interest, the efficiency of a regulation to protect both retail and institutional investors becomes very important. The ECB sources also confirm that there is increasing enthusiasm among both previous owners of crypto-assets (where, in 2024, over half of European households which already held crypto-assets, on average, planned to buy more in the next year) and households which did not yet own any crypto-asset (where, in 2024, about 10% of European households which did not own any crypto-asset, on average, planned to buy more in the next year). Lastly, MiCAR has the nice property, from an econometric point of view, of being directly applicable to issuers of crypto-assets, CASPs, and companies who intend to use them, while also having precise deadlines to let actors in the market adapt to the new normative context, allowing for a more precise analysis.

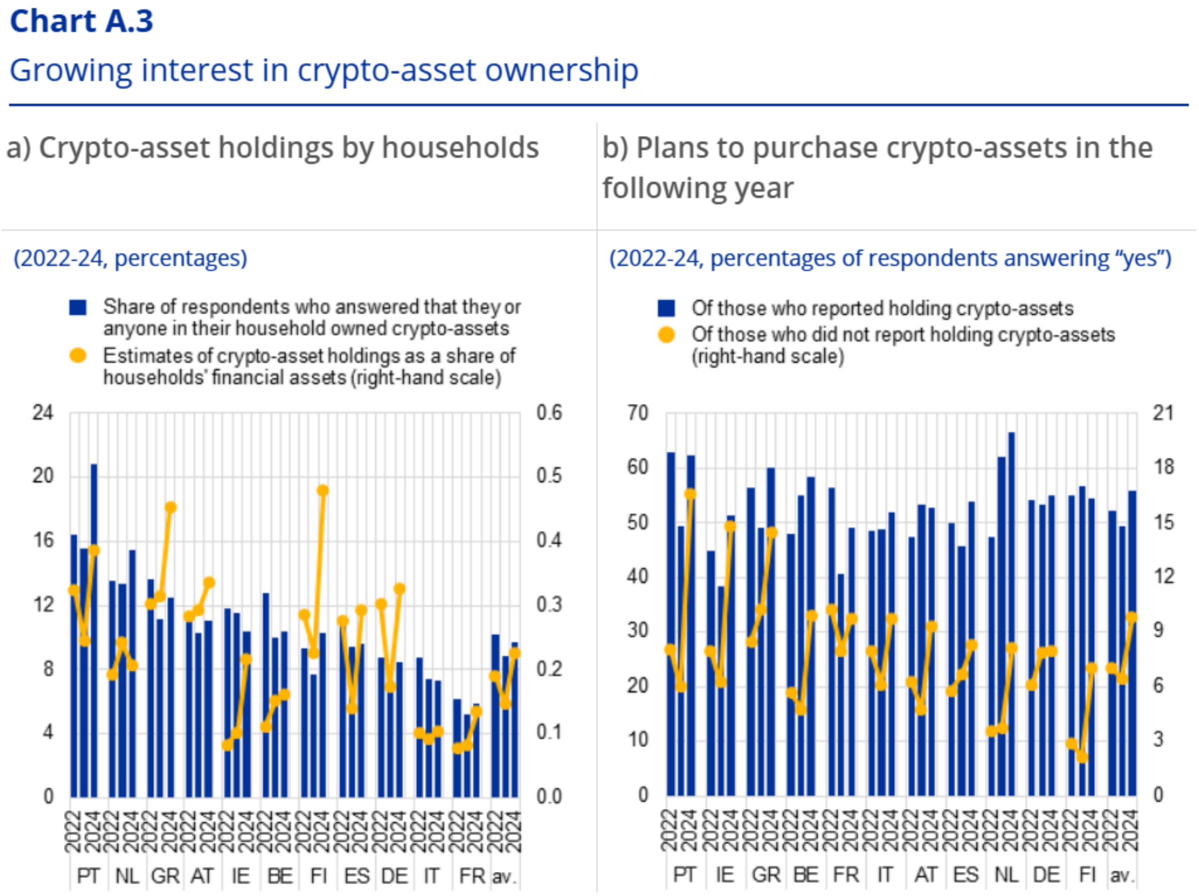


Figure 1.1 Interest in crypto-assets, Financial Stability Review ECB (2025)

1.1.1 Literature review

Since MiCAR was only approved in June 2023 and that title III and IV came into effect in June 2024, while titles I, II, V, VI and VII became applicable in December 2024, the literature on this kind of policy evaluation is lacking, in fact, from a quantitative point of view, no other piece of academic literature has been published regarding an evaluation of the regulation. There have, however, been qualitative studies on the matter, and also comparative analyses with other kinds of regulations. Dr. Iris M. Barsan, in the paper *Are MiCAR's Market Abuse Rules Useful?*(2024), critically analyzes the new legislation and compares it with the pre-existing Market Abuse Regulation (MAR). Specifically, the absence of some exemptions from the normative, which are instead present in MAR, makes MiCAR potentially stricter in the cases where it needs to be applied and redundant when regulatory uncertainties need to be seen "*through the lens of MAR*". The author argues that instead of "*serving as a pale copy of MAR*", the regulation would have been way more effective if it provided an extension to the existing legislative landscape, filling the normative void in blockchain and crypto-assets sectors, as is the case for transparency on smart-contract, miners, validators, and communication channels for blockchain actors. The strictness of MiCAR is also addressed by other authors such as *Lehmann* (2024) whose scope in the paper "*Gold Standard or Regulatory Poison for the Crypto Industry?*" is to understand wether MiCA is efficient at pursuing its objectives, potentially setting the base for the European legislation to spread globally and become the framework which other countries can build upon (namely the *gold standard*), or pose a threat to FinTech and crypto-assets innovation, isolating Europe from this industry in favor of more permissive countries. The answer to this question is that it will probably depend on how much crypto-assets will spread across Europe, if the enhanced transparency and security level will attract enough investors, without significantly slowing down the innovative process of this worldwide-connected industry, the regulation will be a success; otherwise, it will just end up poisoning its own growth. In the publication, the technology neutrality of MiCA is also challenged, assuming that it will need to constantly be updated in order to keep up with the new technological features implemented, which would be a significant burden for any regulator. *Asscheman* (2023) also analyzes MiCA, explaining the necessity of a comprehensive regulation in Europe, highlighting the risks of not regulating, and arguing that its success will depend on the "*Regulatory Convergence*" and cooperation among national and European authorities. Lastly, several master's theses that analyze MiCA from different points of view have been published on the matter, primarily supervised by Professor Andrea Minto from UniVe; however, these, being master's theses, have not been published by any scientific journal, hence they are just mentioned to acknowledge the existing field of studies.

1.1.2 Scope of the analysis

Due to the evident lack of literature in the policy evaluation of MiCA from a quantitative point of view, the analysis proposed in this thesis aims to take the first steps into this untouched field, producing initial pieces of evidence and sharing the methodology used and the data collected. In order to do so, two different metrics have been investigated. The research questions linked to the first metric, and therefore the first analysis, are "*how did the frauds in the cryptocurrency world evolve after MiCA? Did MiCA affect this evolution? If so, what is the scale of this effect?*". The research questions linked to the second metric, and analysis are "*how did the risks and volatility associated with cryptocurrencies evolve? Did MiCA affect this evolution? If so, what is the scale of this effect ?*". It is therefore the objective of this analysis to give an opinion on the effectiveness of MiCA in reducing the amount of fraud and the trust of investors in the crypto-assets market.

1.2 Crypto-assets, classifications and differences

Due to the innovative nature of the matter, there isn't yet a global definition for the term "Crypto-assets", both academic literature and institutions or authorities have tried to give their own definitions to the phenomenon, creating different classifications based on different approaches. In fact, some of these are made by classifying crypto-assets based on the underlying technological structure, while others try to separate them from an economic or legal perspective. Then, within these macro classifications, different authorities have slightly different views on the matter. For the scope of this thesis, crypto-assets will be classified from an economic point of view, using and citing both academic and institutional sources using the framework by Kochergin, D. (2022), shown in Figure 1.2, and implementing other definitions and study cases such as Zetzsche D, Woxholth J. (2025), Bieri et al. (2020), Kahya et al. (2021), or the "*Markets in Crypto-Assets Regulation*".

First and foremost, the European Commission states that "*A crypto-asset is a digital representation of value or a right that can be transferred or stored electronically using distributed ledger technology or similar technology*".This very broad definition includes various subdivisions and classifications. The first step to clarify the differences between crypto-assets, is the division between virtual currencies and digital tokens.

1.2.1 Virtual currencies

Virtual currencies can be defined as "*a digital expression of value (price), which can be bought and sold digitally and function as a means of exchange and/or a unit of account and/or a means of preserving value but does not have the legal status of money at the national level*" Kochergin, D. (2022). This category is also, although with some differences, known as payment tokens. On the other hand, digital tokens, are defined as "*digital assets that are issued by clearly identified issuers using distributed ledger technology (usually on the blockchain) and give to their owners' debt, equity, and dividend rights or access rights to the consumption of certain goods on the issuer's platform*" Kochergin, D. (2022). The clear difference between the two, visible from these definitions, stands in the scope of existence of these crypto-assets; virtual currency's scope is to be exchanged for goods and services, or to assess the value of goods and services, or to preserve purchasing power over time, sometimes all at the same time, they can essentially serve functions traditionally held by physical money, without the legal status. Digital tokens' scope is to transfer a right from the issuer to the owner. The differences in the given rights, as explained later in this section, create different types of digital tokens. Within the initial distinction between virtual currencies and digital tokens, further divisions are necessary. We begin by considering virtual currencies; these can be subsequently divided into cryptocurrencies, the most famous and oldest type of digital asset, and stablecoins, which, although originating in the second generation of crypto-assets, have recently become of interest for consumers, as well as financial institutions and regulators.

Cryptocurrencies are unique for several reasons; first and foremost, they are decentralized, meaning that there is no issuer for these, their supply is based on the underlying blockchain protocol, and can be capped, as is the case for Bitcoin. Another important factor is the way these assets form value; in this case, it is entirely driven by the mechanisms of supply and demand, and therefore the value stands in the trust that the public has in these assets and in their present and future ability to be exchanged for goods and services. For this aspect, cryptocurrencies are very similar to fiat currencies or commodities like oil and gold, with the clear difference that the latter also have an intrinsic use outside of finance and that their supply is limited by the amount available on our planet (for the time being), instead of a predefined mathematical algorithm. Lastly, obviously, there's the technological innovative aspect that these assets stand upon: the blockchain. Without delving into the technical aspects which would fall out of the scope of this thesis, this kind of distributed ledger technology allows two operators of a transaction to conduct exchanges remotely, in the absence of trust, and without an intermediary, while the algorithm confirms its authenticity on the network. Cryptocurrencies, therefore, have a series of characteristics that make them very appealing as means of payment; they reduce counterparty risk through the blockchain, and may lower transaction costs through their decentralized nature. However, not all cryptocurrencies are best suited as a means of payment. Bitcoin itself is arguably more appropriate as a reserve asset, while the second most well-known cryptocurrency, Ethereum, is particularly useful for the implementation of decentralized applications (DApps), whose code is written in self-executing programs called smart contracts on the blockchain. There is, however, one problem, which is deeply connected to the nature itself of these assets, their volatility. According to the study by Bakas D. et al. (2022), the main factors that affect the volatility of Bitcoin are Google Trends data for Bitcoin, total circulation, the S&P 500 index, and US consumer confidence. It is, however, worth mentioning that these are the variables deemed significant among the twenty-two that they analyzed, divided into five groups chosen according to previous literature on Bitcoin empirics: Bitcoin environment, market sentiment, financial markets, macroeconomic conditions, and policy and market uncertainty. Particular attention was given to US-specific variables.

To address this volatility issue in 2014, the first stablecoins emerged, notably in BitUSD and Tether. Stablecoins are defined by Kahya et al. (2021) as "*A digital token on a blockchain that is designed to minimize price volatility with respect to a stable fiat currency or asset.*" and have similar characteristics to cryptocurrencies, although with some notable differences. "*they are issued by identified issuers on the blockchain in the form of circulating digital monetary obligations or certificates of deposit, [...] they maintain the stability of the exchange rate by pegging to the basic low-volatility monetary or commodity security or through the use of algorithmic* *technologies*", and "*they can be used as a means of exchange and/or a means of payment, as well as savings funds from individuals besides the issuer*" (Kochergin, D. 2022). If the classification of crypto-assets in general can differ among authors and institutions, academics seem to be aligned on classification of stablecoins, dividing them into three categories: fiat or asset backed, crypto-collateralized and algorithmic stablecoins. The first kind is that which is pegged to an underlying asset, usually held by a private bank, which ensures that each coin is backed one-to-one by that asset. Examples of this are Tether, which is pegged to the USD, or Diem, previously known as Libra, whose project initially intended, with the support of Meta (then Facebook), for the stablecoin to be pegged to and backed by a basket of fiat currencies, namely USD, EUR, GBP, and JPY; the project ended up being revised and modified due to regulatory and political pressures, particularly regarding monetary policy and competition with fiat currencies, and was then sold to Silvergate Capital, which later filed for bankruptcy protection on september 18, 2024. The second kind, crypto-collateralized stablecoins, are usually either pegged to a single cryptocurrency or token, or a basket of them. One would argue that using such volatile assets as collateral would make the stablecoin not so stable; that's why "*The core component is over-collateralizing the backing cryptocurrencies so that their volatilities have minimal impact on the stablecoin's price*"(Kahya et al. 2021). Of course, in case of very steep changes in the collateral's price, the stability would be compromised, no matter the amount of cryptocurrency buffer used. Diversifying the collateral is a great way to limit this effect; that's why using a basket of cryptocurrencies to anchor the price of the stablecoin is usually a better option. A clear example of this is MakerDAO (DAI). It initially only accepted Ethereum as collateral for its minting, but later also expanded to include other cryptocurrencies such as USD coin (USDC) and Wrapped Bitcoin (WBTC). The way these are created is also noteworthy; the user deposits the cryptos as collateral into a vault to lock them in, and can then mint DAI up to a certain amount established by the collateralization ratio, which depends on the type of collateral used. This works like a debt position, and is also used as such, for example to exploit the financial lever, or to gather liquidity. To get the blocked collateral back, the user then has to repay the minted DAIs (which will be burned) plus a stability fee. Whenever the price of the collateral falls below a certain threshold, the position can be automatically liquidated by selling the collateral, to cover both the debt and the fee. In this scenario, the stability fee acts as an interest rate. When the price rises above the target of one USD, the fee lowers, incentivizing the minting of DAIs, and the amount of coins in circulation, effectively raising supply and reducing their price. The opposite happens when the price gets too low. Another stability tool is the DSR (DAI savings rate), which represents the interest rate paid to users who lock their DAIs into MakerDAO smart-contracts; whenever the price rises above the target, the DSR can be lowered, reducing the incentive to deposit DAIs in smart-contracts and potentially increasing the amount of coins in circulation, lowering their price. The opposite also holds true. In this regard, companies like MakerDAO act similarly to central banks, with the objective of keeping the stablecoin's value fixed and fostering the community's development, just as central banks aim to keep money stable and foster economic development. The third and final kind of stablecoin, algorithmic stablecoins, is based on the idea that it's possible to fix the value of the coin without pegging it to any asset. In these cases, an algorithm automatically performs some operations to try to anchor its price, such as expanding or shrinking the supply, or by giving market incentives. This kind of stablecoin has, however, proven not to be very effective in reaching its stability objective; some experiments have been done in this matter, although not very successfully. The Terra-Luna case, where, at the time of the collapse, around 45 billion dollars of market cap were burned in a week (Bloomberg, 2022), is an example. From these distinctions and categories, several positive and negative aspects of each type of stablecoin emerge. Most notably, there's a tradeoff between decentralization and stability; fully decentralized projects like the algorithmic stablecoins tend to lose stability in the long term, while the somewhat decentralized crypto-backed stablecoins must over-collateralize their value to maintain price stability. Lastly, fiat-backed stablecoins need a central authority to hold and manage the underlying money reserves.

1.2.2 Digital Tokens

On the other side of the classification of crypto-assets there are digital tokens, Kochergin, D. (2022) defines them as "*Digital assets that are issued by clearly identified issuers using distributed ledger technology (usually on the blockchain) and give to their owners' debt, equity, and dividend rights or access rights to the consumption of certain goods on the issuer's platform*". The clear difference with Virtual currencies stands therefore in the transfer of economic or access rights from the issuer to the user. These are then subdivided into investment tokens and utility tokens. Investment tokens grant economic rights, usually in the form of dividends, interest, or ownership. They are commonly used to raise capital for start-ups and other companies that face difficulties in raising funds in traditional markets, such as venture capital. The mechanism through which these firms emit investment tokens is called ICO or ITO which stands for initial coin offering or initial token offering. In this case the company issues new tokens accepting cryptocurrencies as payment for those. In the case of the IEO, initial exchange offering, an exchange platform acts as an intermediary in the process. This process has its own advantages and disadvantages, the most obvious drawback being that the exchange platform represents an extra cost for the company; this is however offset by the fact that an IEO attracts a greater number of investors, due to the higher level of trust provided by the exchange platform and the wider reach of the offering. The trust that an exchange platform provides is crucial in a market where, in addition to the intrinsic risk that investing in many start-up companies embeds, the risk of scams is very high. According to Grobys, K et. al (2022) "*The evidence presented in this paper infers that 56.80% of all launched ICOs were subject to fraud, corresponding to 65.80% of the overall market capitalization. Specifically, from the total of USD 15.38 billion raised by the 1014 ICOs, USD 10.12 billion were lost due to scams*". Investment tokens can also give their owners voting rights in relevant matters, such as the distribution of dividends. Another phenomenon that is expanding with the creation of investment tokens is the ”tokenization” of traditional assets, where instead of creating new assets to raise capital, the tokens are used to digitalize previously existing assets through blockchain technology. This applies to both financial and non-financial assets, and interestingly enough, also to illiquid assets such as real estate or art. Utility tokens, on the other hand, instead of granting economic rights, provide access to products or services supplied by the issuer, as stated in Article 3 of the Markets in Crypto Assets Regulation (MiCAR) (Regulation (EU) 2023/1114). These are therefore used to finance the development of goods and services, and can grant the owners voting rights in the direction that the updates will pursue. The fact that these tokens’ main objective is to raise capital does not mean that they cannot be traded on exchange platforms for other digital assets or even fiat currencies.

Investment tokens and utility tokens have, from a theoretical point of view, a very clear distinction in the rights owed to the investor. There are, however, practical cases where the classification is not as defined, for example, digital tokens that grant both types of rights, or that can be used as payment tokens on the issuer’s infrastructure. The literature has therefore created a new subtype: hybrid tokens, which can have characteristics of both investment and utility tokens. A type of hybrid token is the decentralized finance ecosystem token (DeFi) which can have both governance and financial characteristics, giving the owner the right to vote on the development of the protocol of the blockchain platform. Some of them also establish a credit position or derive from other digital assets. Lastly, NFTs (Non-Fungible Tokens) are issued with the objective of granting, fixing, or declaring unique rights. Their non-fungibility, meaning that no other crypto-asset will be able to replace them, is granted by the blockchain. These NFTs possess a series of unique properties, including incompatibility with other platforms, indivisibility into smaller units, indestructibility, meaning that they cannot be destroyed or replicated, and verifiability, as the blockchain stores data about the current and all previous owners of the token (Kochergin, D. 2022).

1.2.3 National virtual assets and CBDCs

To complete the overview on crypto-assets, it is also mandatory to mention two important items in the landscape: national virtual assets and CBDC. Although they are not crypto-assets per se, as they are emitted by central authorities such as central banks and state institutions, they share some similarities and are still considered digital assets. National virtual assets are issued by state authorities, typically in periods of economic turmoil and with the objective of accessing alternative forms of financing, eluding sanctions; they are recognized by the state and usually backed by real assets. It is the case of the Petro, issued by the Venezuelan government in february 2018, in order to bypass the US sanctions and access financing. Its characteristics were at the time very innovative in the matter, it was completely pre-mined, which means that the total supply of ”petromonedas” was decided at launch and there was no way to create new coins after the initial issuance, and, in an effort to keep its value stable (given the hyperinflation that Venezuela was experiencing) its value was pegged to the oil reserves of Venezuela, meaning that it would have been equivalent to one barrel of oil. Many economists and journalists have criticized the initiative for its design, the contradictory statements of President Maduro on the matter, and the shady aspects of its development, particularly regarding its main creator, Gabriel Jiménez, who ultimately fled the country and became a political refugee in the US. Central bank digital currencies on the other hand are issued by central banks and attract significantly more interest. In fact, in the study ”*Advancing in tandem – results of the 2024 BIS survey on central bank digital currencies and crypto* by Illes et al. (2025), a survey was conducted among 93 central bank authorities, of these, 85 of them (91%) were exploring a kind of CBDCs or both. According to Auer et al. (2023), CBDCs can be either meant for wholesale or retail use; in the first case, they would only be utilized in transactions between financial institutions, and in the latter, they would also be expanded to the general public. They can also differ vastly in design, underlying infrastructure, and, for retail CBDCs, the access methodology for the public. First and foremost, regarding their design, they can be direct, meaning that the central bank directly controls the infrastructure (which will be discussed soon) and offers retail services, they can be hybrid, where the intermediaries offer retail services and keep the records of all the transactions, but at the same time the central bank also keeps the same record and operates a backup infrastructure to be used if needed. Lastly they can be intermediated, where the only difference with hybrid CBDCs stands in the fact that the central bank maintains only a wholesale ledger. In all of these cases, the CBDC represents a direct claim on the central bank. With regards to their underlying infrastructure, it can be either based on a traditional centralized database or on permissioned variants of DLT where operators can decide who is admitted to the network. Lastly, the technical aspects linked to the access to the CBDC are based either on personal accounts complete with identification protocols or on digital tokens, which do not require identification to be used and grant a greater level of anonymity, just like normal cash, this would obviously be more appealing for unbanked individuals, but it would also expose the digital currency to illegal activities. The same paper from Auer et al. (2023) also conducts a statistical study on the correlation between the degree of development of a CBDC and various key variables, including mobile phone use, internet use, innovation score, government effectiveness, and GDP per capita. Their results show that CBDC projects are more likely to start where there is a greater use of mobile phones, innovation capacity, financial development, and the size of the informal economy.

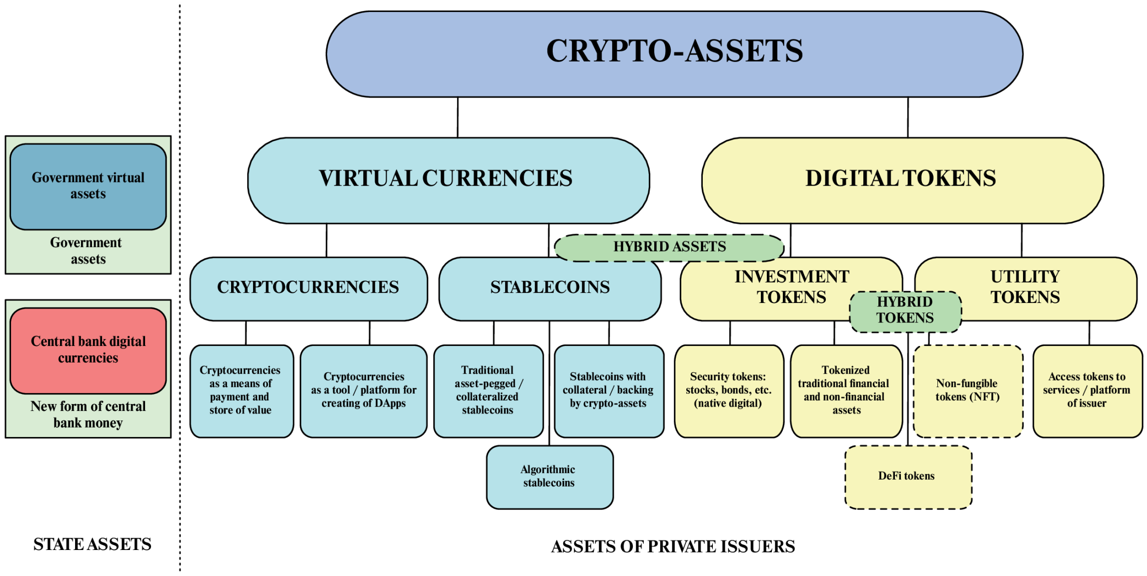

CRYPTO-ASSETS
VIRTUAL CURRENCIES
DIGITAL TOKENS
Government virtual assets
Government assets
Central bank digital currencies
New form of central bank money
STATE ASSETS
CRYPTOCURRENCIES
STABLECOINS
HYBRID ASSETS
INVESTMENT TOKENS
UTILITY TOKENS
HYBRID TOKENS
Cryptocurrencies as a means of payment and store of value
Cryptocurrencies as a tool / platform for creating of DApps
Traditional asset-pegged / collateralized stablecoins
Stablecoins with collateral / backing by crypto-assets
Algorithmic stablecoins
Security tokens: stocks, bonds, etc. (native digital)
Tokenized traditional financial and non-financial assets
Non-fungible tokens (NFT)
Access tokens to services / platform of issuer
DeFi tokens
ASSETS OF PRIVATE ISSUERS

Figure 1.2 Classification of Crypto-Assets, Kochergin (2022).

Chapter 2

Legal Framework

2.1 First steps

The European regulatory framework for cryptocurrencies, culminating in the recent MiCA Regulation, is still evolving and has been shaped gradually over more than a decade. The first formal recognition of this sector occurred in October 2012, when the European Central Bank published the so-called "Virtual Currency Schemes" report. In this document, we also see one of the first formal definitions of the phenomenon; in fact, the ECB defined "Virtual Currencies" as *"a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*".Another important aspect highlighted in this paper is the many types of "virtual currencies" that were available at the time. These classifications would later prove very useful for both institutions and academia to assess the evolution of digital currencies. In particular, the ECB divided "currency schemes" into three types based on their degree of openness and exchangeability with physical currencies and goods or services. Type 1 referred to closed schemes, typically used in online video games. Type 2 schemes usually had a conversion rate allowing real money to be exchanged for virtual currency, which could then be used to purchase primarily virtual goods. Finally, type 3 schemes had both buy and sell exchange rates, making them the most open systems to the real economy, as they could—and often still can—be used to purchase both digital and real goods and services. Additionally, this first study by the ECB emphasizes that the issuers of these new currencies are not traditional financial actors, such as central banks, but rather private companies, making the existing financial laws and regulations inapplicable. This is particularly relevant in the first case study of the document, the Bitcoin case, where both the money supply and the clearing of transactions are directly managed by community members, and its price is uniquely determined by the laws of supply and demand. Bitcoin can become problematic as it may serve as an alternative means of exchange for drug trafficking and money laundering, due to the high degree of privacy embedded in such operations. The ECB also outlines a series of risks and challenges associated with virtual currency schemes, closely linked to the central banks' traditional goals of monetary stability and economic growth. In particular, type 3 virtual currency schemes, being the most open to the real economy, are also the most threatening for it. First and foremost, the ECB states that they ”*do not pose a risk to price stability provided that money creation continues to stay at a low level*” and that although they are very volatile, they ”*cannot jeopardize financial stability*” due to ”*their limited connection to real economy, their low volume traded and lack of wide user acceptance*”. They then warn public authorities of the legal uncertainty sorrounding the sector and the lack of close monitoring of these phenomena. Lastly, they assess the reputational risk for central banks, as potential incidents and frauds with wide press coverage could be seen as a result of central banking authorities' negligence in the matter, given the shared characteristics between these currencies and traditional ones, which fall under central banks' responsibilities. To summarize, this initial study acknowledges both the opportunities and the risks that these schemes entail, but also states that these do not affect those who are not users of said schemes. In February 2015, the ECB published another study on the matter, titled "*Virtual Currency Schemes: A Further Analysis*", in which its previous assessments and identified risks were updated with new data. First and foremost, it was noted that some e-commerce platforms had announced their intention to start accepting Bitcoin as a means of payment, although the overall acceptance of virtual currency schemes still did not appear to be widespread. Moreover, this new report highlighted certain aspects regarding the anonymous nature of VCS: "*VCS present several drawbacks and disadvantages for users, i.e. lack of transparency, clarity and continuity; high dependency on IT and on networks; anonymity of the actors involved; and high volatility.*" Other risks connected to the intrinsic nature of VCS were also mentioned, such as "*counterparty risk, (...) exchange risk (...) and the risk of investment fraud.*" Overall, the prior belief that these emerging virtual currencies posed a low systemic risk was confirmed, as well as the recognition of potential opportunities in terms of financial innovation. The first official legislative step about cryptoassets was, however, the recommendations from the European Banking Authority to bring virtual currency-to-fiat exchanges and providers of virtual currency custodian wallet services into the scope of the Anti-Money Laundering Directive (Zetzsche & Woxholth, 2025)

2.2 Cryptocurrencies in AMLDs

The AMLDs (Anti-Money Laundering Directives) are measures adopted by the European Union to counter activities such as money laundering and the financing of terrorism. In this process, directives have gradually evolved, becoming more complete while adapting to changes in the financial system and the rise of new technologies. During the period of legal uncertainty surrounding cryptocurrencies and crypto-assets in general, the EU established some rules and guidelines for member states to update their legislation. The first direct reference to the sector in AMLDs occurred in AMLD5. This directive, approved in May 2018 and implemented in January 2020, ”*represented a significant step in the regulation of crypto-assets by bringing cryptocurrency exchanges and custodian wallet providers under the scope of EU AML laws. As* *a result, crypto exchanges and wallet providers were included on the list of 'obliged' entities, meaning that they were required to perform customer due diligence checks, ongoing monitoring, and suspicious activity reporting.*" (Jones Day, 2025). The inclusion of these market actors in the AMLD context became relevant as the directives were updated, namely, on 31 May 2024, with the approval of the so-called AML package, including AMLR, AMLD6, TFR, and the creation of the AMLA, among others. In fact, when AMLD6 was approved, the updated provisions and clarifications of responsibilities also affected the wallet providers and crypto exchange platforms. With the introduction of the AMLR, the European regulation whose objective is to harmonize member states' laws, the so-called CASPs (Crypto Asset Service Providers) were explicitly included in the regulation. These entities became officially subject to customer simplified or enhanced due diligence, based on the risk profile, suspicious transaction reporting and retention of records for at least five years. They were also required to comply with the "travel rule" as specified in TFR, which requires information of the source of the asset and its beneficiary to travel with the transaction and be stored by both parties of this transaction. Lastly, the regulation 2024/1620 established the AMLA (Anti-Money Laundering Authority), equipping it with supervisory and investigative powers to ensure compliance with AML (Zetzsche & Woxholth, 2025)

2.3 Harmonization and clarity

In this complex regulatory landscape, where national laws, European regulations and directives — not always directly applicable — and guidance from institutions such as the ECB all coexisted, the European Commission decided to launch the *EU FinTech Action Plan* on 8 March 2018 to put an end to regulatory confusion. Through this plan, the Commission tasked the European financial supervisory authorities, namely the EBA, ESMA, and EIOPA, with providing clarity on whether previous financial regulation was applicable to crypto-assets, as well as guidelines for future drafts and regulations concerning the sector. On 9 January 2019, reports from both the EBA and ESMA were published, highlighting the risks that crypto-assets posed in terms of market integrity, consumer protection, and operational resilience. ESMA also noted that, since the world of crypto-assets was becoming ever more diverse, many of them would neither qualify as financial instruments nor as e-money, effectively falling outside European jurisdiction and creating a legal void. These reports formed the basis upon which MiCAR and the PilotR would later be built. At the same time, EIOPA was not asked to publish a report but instead to examine whether insurance companies and pension funds were exposed to crypto-assets. With the guidance received from the ESA's reports, and the knowledge matured with the inclusion of cryptoassets in the AMLD5, the European Commission, on 24 September 2020, announced the adoption of the Digital Finance Package, which includes, among other things, the Digital Finance Strategy (DFS 2020). In particular, the DFS 2020 presented three legislative proposals, namely MICA, PilotR, and DORA, all of which had different areas of interest but shared the same scope: to fill in the legal gaps in the European regulatory system. In fact, MICA focused on creating a new financial regulatory framework. DORA's main focus was the protection from cyberattacks and general digital resilience. Lastly, PilotR's main objective was to enhance the development and innovation in the DLT market infrastructures.

2.4 MiCAR

The Markets in Crypto-Assets Regulation (MiCAR) is the latest and most important piece of legislation added to the European regulatory landscape in the matter of crypto-assets. It not only fills the normative void left by technological and financial innovations but also dictates clarity in the scopes of each regulatory fragment. In this matter it often takes advantage of the existence of previous directives and regulations, such as the Markets in Financial Instruments Directive (MiFID) and the Prospectus Regulation (PR), in order to create a sort of continuity between the existing financial legislation and MiCAR. Its development stages are shown in Figure 2.1 from ESMA.

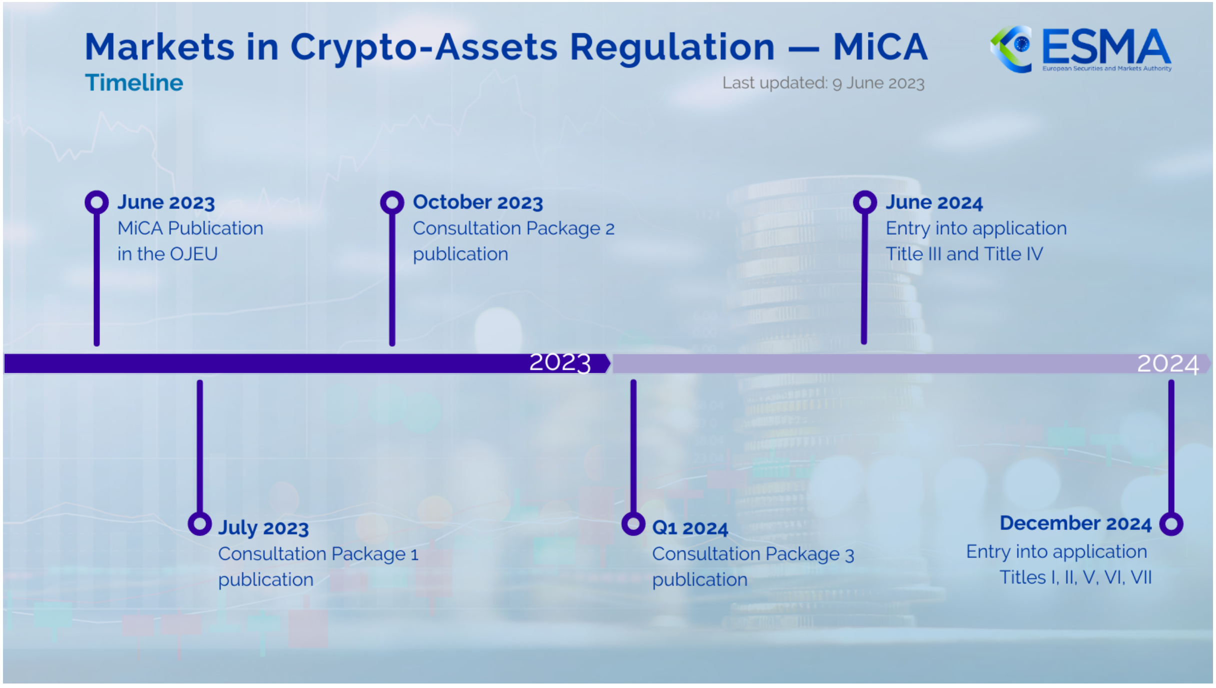

Markets in Crypto-Assets Regulation — MiCA
Timeline
Last updated: 9 June 2023
ESMA
European Securities and Markets Authority
June 2023
MiCA Publication in the OJEU
July 2023
Consultation Package 1 publication
October 2023
Consultation Package 2 publication
2023
Q1 2024
Consultation Package 3 publication
June 2024
Entry into application Title III and Title IV
December 2024
Entry into application Titles I, II, V, VI, VII
2024

Figure 2.1 MiCA implementation timeline, ESMA (2023).

First and foremost, MiCAR provides a series of definitions of crypto-assets, Distributed Ledger Technology(DLT), and Crypto-Asset Service Providers (CASPs). These are intentionally designed to be as future-proof as possible, as having stricter definitions could bring new actors or types of services, crypto assets and intermediaries, to fall out of the new regulation's scope. Article 2(1) of Regulation (EU) 2023/1114 states: "*This Regulation applies to natural and legal* *persons and certain other undertakings that are engaged in the issuance, offer to the public and admission to trading of crypto-assets or that provide services related to crypto-assets in the Union.*" There are, however, some notable exceptions. Most importantly, it does not cover *directly* crypto-assets with no identifiable issuer, as is the case for those that are completely decentralized. This is because there is no single legal person upon whom the burden of the legislation could fall, and be responsible for its compliance. This means that important crypto-assets, such as Bitcoin fall outside MiCAR's scope. One might argue that the relevance of these fully decentralized currencies in the market makes the regulation less effective. However, this is not the case, as even if the assets themselves cannot be subject to MiCAR, the operations and operators connected to these definitely are. The other exemptions from the normative are: NFTs and assets covered by other financial laws (Article 2(4)) except for EMTs (Electronic Money Tokens), which fall under both MiCAR and the Electronic Money Directive (EMD). CBDCs are also out of the regulation's scope, this is because public authorities are exempted (and therefore also their issued currencies), as are those entities which only provide crypto-related services to other companies in the same group and liquidators of insolvency procedures. The regulation specifies each type of financial instrument that is not included in its scope. However it also envisions a series of measures in order to avoid confusion for future and existing assets: the ESMA is required to create guidelines on the classification of crypto-assets, which have already been published, and national competent authorities can request an opinion to ESAs for the classification matter, these in turn will make an annual report to clarify common misconceptions among NCAs, also, when the white paper (also known as prospectus for other assets) is notified to the national authority, if the crypto-asset is deemed to fall out of MiCAR's scope, an explanation which follows ESA's guidelines (which have been published in december 2024) should be added to the documentation. It is clear that, apart from these, every crypto-asset offered to the European public or intended for trading in the EU must comply with the European regulatory regime, irrespective of its origin.

The following section will analyze the legal ”innovations” that MiCAR introduced. It is important to note that one of MiCAR's objectives is to implement a form of protection for investors, while avoiding the freeze effect that over-regulation and bureaucracy could have on the sector's innovative power. In this context, MiCAR introduces a series of requirements and obligations regarding the publication of a cryptoasset's white paper, which is very similar in many aspects to the prospectus introduced by the PR (Regulation (EU) 2017/1129), but arguably less complex. To avoid any confusion, the prospectus only applies to transferable securities that fall under MiFID's scope. These kinds of assets, as previously stated, are not covered by MiCAR. Inside the regulation, a differentiation is made between some types of crypto-assets, namely ARTs and EMTs. This is because Asset Referenced Tokens (ARTs) and Electronic Money Tokens (EMTs), which are two kinds of stablecoins, the first pegged to a basket of assets and the second to a single fiat currency, as described in the first chapter, are designed to keep the asset volatility as low as possible, making them less risky than other crypto-assets. The regulator, therefore, asks for a greater level of transparency and control for these supposedly safer assets. In fact, while for most of them the white paper simply needs to be notified to the competent national authority, ARTs need the white paper to be pre-approved. At the same time, EMTs have to redact a white paper just like any other crypto-asset, despite their similarities with e-money (PayPal accounts and prepaid cards are considered a form of e-money), for which no prospectus is even required, as they follow the EMD2. There also are cases where the white paper is not required at all in the MiCAR, in fact, according to Article 4(2) Regulation (EU) 2023/1114, this is the case for assets different from ARTs and EMTs which are offered to fewer than 150 natural or legal persons per member state, the offer does not exceed one million euros or it is only addressed to qualified investors which are the only ones able to hold them. When the white paper is required, the obligation to publish it lies with the legal person that offers the crypto-asset or the person seeking admission to trading. With regards to the content of the white paper Zetzsche & Woxholth (2025) argue that ”*As a general principle, the prospectus must contain the information necessary for an investor to make an informed investment decision*” and make some specifications such as: ”*information about the issuer, offeror, person seeking admission to trading, operator of the trading platform, any guarantor, and/or any other person engaged in drawing up the prospectus [...] the cryptoassets, the underlying technology and investment risks specific to the cryptoasset in question*” also all cryptoassets’ white paper except EMTs must state that they might lose their value and become illiquid. It is clear that in this context, the white paper is a handy tool for both retail and qualified investors to have greater transparency, which should lead to more informed decisions and a reduction in fraud schemes, which will be the focus of the third chapter. Particularly important for retail investors, is the mandatory presence in the whitepaper of a summary that provides all the key information, making its acquisition easier and faster. Marketing communications and advertisement in terms of crypto assets is also regulated, just like the whitepaper they have to be published online on the website of the issuer, member states authorities may exercise control over them, and, under article 7, should be clearly identifiable as such, the information is fair, clear, not misleading and consistent with the white paper the publication of which must be communicated in the advertisement, the rules for ARTs and EMTs again, are stricter, in fact their marketing statements also need to specify that owners of these assets have the right to trade their ARTs or EMTs for the underlying assets or fiat currency used as collateral. Another important element introduced by MiCAR is the regulation and definition of CASPs and their activities. Under article 3(15) of Regulation (EU) 2023/1114, Crypto Assets Service Providers (CASPs) are defined as ”*a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto asset services in accordance with Article 59*”. Legal entities who wish to operate as a CASP require an entirely new license unless they already have one under EU financial law, in that case they only require an extension on the existing license. They also must comply with fiduciary requirements such as honesty, fairness, and professionalism in accordance with their client's best interests, while disclosing their costs and fees and warning of any potential risk, their management members must "*possess the appropriate knowledge, skills and experience*" and, with key shareholders also must be "*of sufficiently good repute*" under article 68. Conflicts of interest are also addressed by the MiCAR, which states that CASPs must implement policies to identify, prevent, manage, and disclose them. They also need to follow certain requirements in terms of capital (which again, are stricter for issuers of EMTs and ARTs) and technological robustness, in addition to dealing with complaints fairly and consistently and keeping records of transactions. All of these measures should clearly have an impact on the amount of fraud in the crypto world, since there is a responsibility of both issuers of crypto-assets and CASPs, certain services are also further regulated, as is the case for trading platforms which "*shall prevent the admission to trading of crypto-assets that have an inbuilt anonymisation function unless the holders of those crypto-assets and their transaction history can be identified by the crypto-asset service providers operating a trading platform for crypto-assets*" under article 76(3). The European regulator is not however blind to the fact that laws themselves don't change the underlying fraudulent behaviors, an efficient supervision and enforcement system is also needed for them to be effective, it is however complicated to match both the national interests in keeping their sovereignty in matters as important as financial supervision, and the common interest to preserve the Union's financial stability and bolster cooperation among national authorities. In order to try and reconcile these values, MiCA is designed in such a way that competences are divided among national and Union institutions, using the pre-existing infrastructure for the supervision of the financial market as a framework. By default, the supervisory responsibility is given to national competent authorities with their own supervisory and investigative powers, in addition to "product intervention", which is the power to prohibit or restrict the diffusion of specific crypto-assets or practices; there are, however, some exceptions to this, and situations where cooperation between them and EBA is required. First and foremost, for ARTs and EMTs which are deemed "significant" the supervisory function is completely shifted to the EBA, due to their greater potential to pose a systemic risk, then, the EBA and ESMA are also tasked, within their respective areas of competence, to coordinate activities of different NCAs and have the same powers of national authorities in the matter of product intervention, to be used when they don't do so. It is clear however that due to the lack of enforcement powers of the EBA within any member state, and sufficient staff across Europe, it is logistically difficult for the institution to carry out on site investigations by themselves, for this reason "*the competent authority of the Member State concerned shall afford them the necessary assistance*" as per Article 124(8) MiCA. Supervision and enforcement matters are therefore also taken into account by the regulation, uniting the fragmented legislative landscape and filling the gaps within it.

Chapter 3
MiCAR policy evaluation

3.1 Overview

To best evaluate the effectiveness of the implementation and entry into force of the policy, two different analyses were made. The first analysis focuses on the amount of fraud committed in the crypto-assets world, analyzing pre-existing trends and investigating the possible effects that MiCA has had with respect to fraud. Although the amount of literature in terms of MiCA policy evaluation is minimal, the data science and computer science fields of study have created an extensive literature in terms of fraud detection in cryptocurrencies, this is both due to the larger time that has passed since the first frauds appeared, and the greater importance that crypto-assets have in the computer science field, with respect to the law or econometrics ones. The technological details that describe the phenomenon fall out of the scope of the analysis; however, it is important to mention, as will be relevant later, that the collection of data in terms of fraud in crypto-assets has developed to facilitate fraud detection, and that more and more sophisticated tools are used to detect and potentially prevent fraud from occurring. This is the case for the detection algorithm developed by Ou et al. (2023) which uses a machine learning technique called Random Forest, where a series of decision trees are aggregated in order to make a classification choice on the dataset, predicting wether a given website is fraudulent based on a series of features linked to its domain, its ranking, the used text etc. This method was revealed to be much more attractive than the ones previously used (97% of accuracy and 98% of precision against 55% accuracy and precision of the Tencent Security algorithm). The second analysis focuses on the prices registered by crypto-assets with a small capitalization. It looks for a potential causal link between MiCA and the volatility of returns in the market. This approach was chosen since the introduction of MiCA, and the regulation efforts that come with it, are expected to be relevant with regard to one of the most important characteristics that crypto-assets intrinsically have: volatility and associated risk. The underlying idea is that the market would react to the regulation and the higher level of transparency that CASPs and issuers need to provide, reducing the risk perceived by market operators and the overall volatility of returns in the sector.

3.2 Frauds analysis

3.2.1 Data collection

For this first analysis, three different datasets were used, as it will also be stated in the section about the limits of the analysis, the availability of data regarding fraud is minimal, with valuable datasets on the matter only being published very recently, and those who get published lack a clear separation by regions. The first group of data is "*Value of cryptocurrency theft worldwide from Q1 2021 to Q1 2025*"; this dataset, published on March 31, 2025, contains quarterly data from 2021 to the first quarter of 2025. Its publisher, Immunefi, is, as stated on their website "*the leading bug bounty and security services platform for Web3 which protects over $100 billion in users' funds*" and their report "*regularly assesses the volume of crypto funds lost by the community due to hacks and scams by year and by quarter*". The retrieved data is in million USD and will be the primary interest for the first analysis. The second group of data is "*Total value of losses due to card fraud worldwide*, this dataset was published on December 31, 2024, and contains yearly data from 2014 to 2023 and reliable predictions for the years 2024, 2026, and 2028. It has been published by Statista, which cites The Nilson Report as the source, which, "*in its 54th year of publication, is the most respected source of news and analysis of the global card and mobile payment industry*" according to *The Nilson Report*. Data is retrieved in billion USD and will be used as a sort of control for the main dataset. Lastly, the third group of data is "*Total number of Visa credit card transactions processed for payments worldwide*", published on July 29, 2025, and divided into quarterly data, from Q1 2008 up to Q1 2025. Data is once again published by Statista, which cites Visa Inc. as their source. The dataset describes the number of transactions of Visa credit cards worldwide in millions. It will be used to obtain accurate estimates of quarterly data for the period Q1 2021 to Q1 2025 for credit card fraud. Clearly, all data from groups 2 and 3 are worldwide retrieved, although they are also available for other regions. This is due to the fact that the objective of these groups is to create a reliable control for the main group, the crypto frauds; they therefore need to be comparable in both the measuring unit and the region of relevance to avoid population incomparability and non-independence of observations. The methodology section will explain how the retrieved data are used to create a new dataset and then compared. It is important to address the fact that, for group 2, the observations for the years 2024 and 2026, which will be used to estimate quarterly data of credit card frauds up to Q1 2025, are estimates themselves. These estimates are, however, consistent with data that have been collected so far. For example, the growth value of payments processed on Visa credit cards worldwide has been stable relative to the past in 2025, and it has also been the case for the number of Visa credit card transactions. One last piece of evidence for the robustness of these estimates stands in the *Value of damage caused by credit card fraud in Japan* which, although being only a regional subsection, is in perfect line with the global estimates, as shown in Figure 3.1

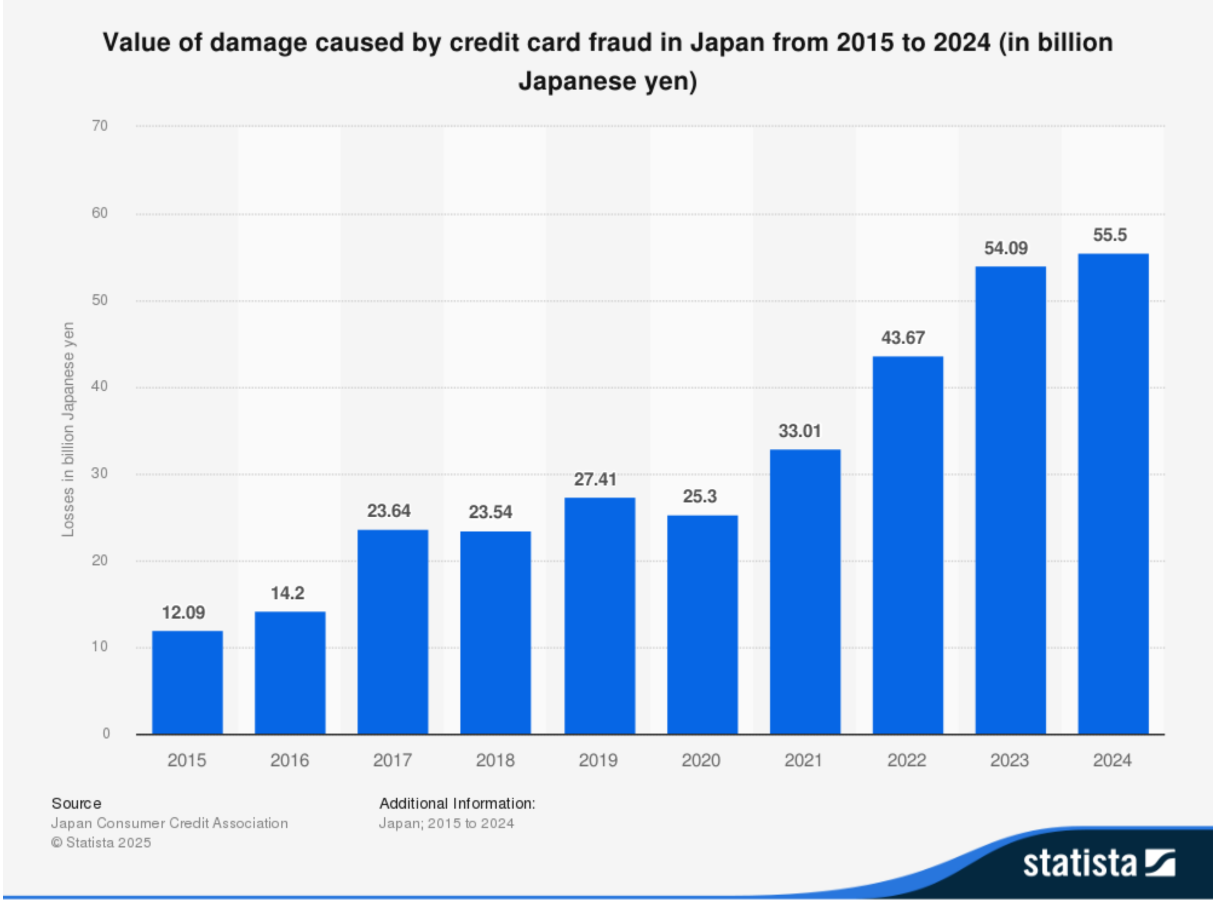


Figure 3.1 Value of damage caused by credit card fraud in Japan from 2015 to 2024 (in billion Japanese yen), Japan Consumer Credit Association & statista, 2025

3.2.2 Methodology

The first step in the analysis process was to identify a robust way to obtain quarterly data, from Q1 2021 to Q1 2025, in millions of dollars of credit card fraud. Obviously, having annual data and dividing it equally among the four quarters assumes that each quarter had the same amount of fraud, which does not account for the increase in fraud during festivities (potential seasonality component), and also would create significant discontinuities between the fourth quarter of one year and the first quarter of the next one. The dataset containing the amount of transactions conducted on Visa credit cards was used to obtain more accurate quarterly data. To do so, the amount of transactions of each quarter in a year was summed up, creating a ”yearly amount of transactions”. The amount of transactions of each quarter was then divided by the corresponding yearly total, creating a new variable, different for every quarter, which will be called ”Ratio”. This new variable is then multiplied by the corresponding yearly amount of credit card fraud for every quarter to create a dataset with the quarterly amount of fraud. The observation for Q1 2025, has been calculated the same way, however, since the yearly frauds for 2025 are currently yet to be observed and published, the fraud amount has been calculated as the corresponding amount of the previous year (2024), times 1.052, which is square ratio between frauds in 2024 and 2026, or, in other words, the yearly estimated frauds growth, on the other hand, the ratio variable for Q1 2025 has been chosen as the mean ratio for the first semesters from year 2008 to 2025. Lastly, the dataset for credit card fraud amounts has been converted from billion dollars to millions for comparability. Figure 3.2 displays the two datasets of crypto fraud and credit card fraud.

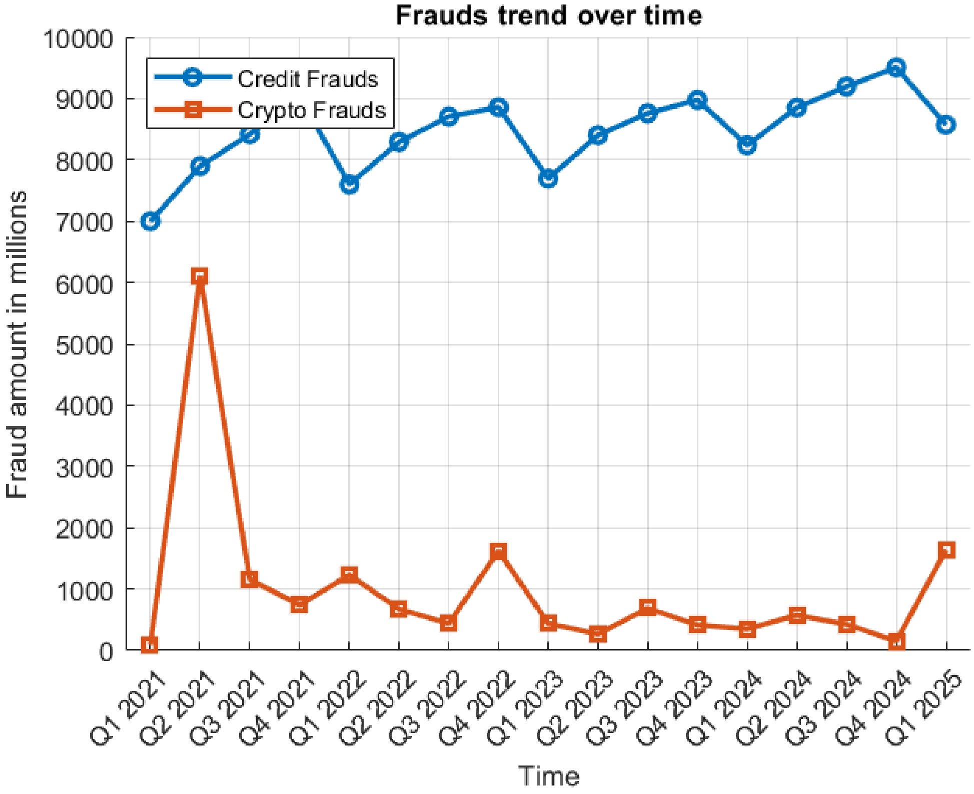


Figure 3.2 Frauds trend over time, Author's elaboration

From the figure, it is clear that a seasonality component, which was expected due to the nature of credit card frauds and transactions, is present; therefore, the series is deseasonalized by creating an OLS regression with dummy variables for quarters 2,3, and 4, as Q1 is used as the baseline to avoid multicollinearity in the dummies. Then the seasonality estimate is calculated through simple OLS formulas. The final value for deseasonalized frauds is calculated as the difference between frauds and seasonality - mean seasonality. This ensures that the deseasonalized series has the same overall level as the original one, ensuring that only the seasonality component is removed, keeping the average level of frauds constant. All the formulas and the deseasonalized graph are subsequently shown

$$\text{frauds}_t = \beta_0 + \beta_2 D_{Q2,t} + \beta_3 D_{Q3,t} + \beta_4 D_{Q4,t} + \varepsilon_t, \tag{3.1}$$

$$\widehat{\text{seasonality}}_t = \widehat{\beta}_0 + \widehat{\beta}_2 D_{Q2,t} + \widehat{\beta}_3 D_{Q3,t} + \widehat{\beta}_4 D_{Q4,t}, \tag{3.2}$$

$$\text{frauds}_t^{\text{deseasonalized}} = \text{frauds}_t - \left(\widehat{\text{seasonality}}_t - \overline{\widehat{\text{seasonality}}}\right), \tag{3.3}$$

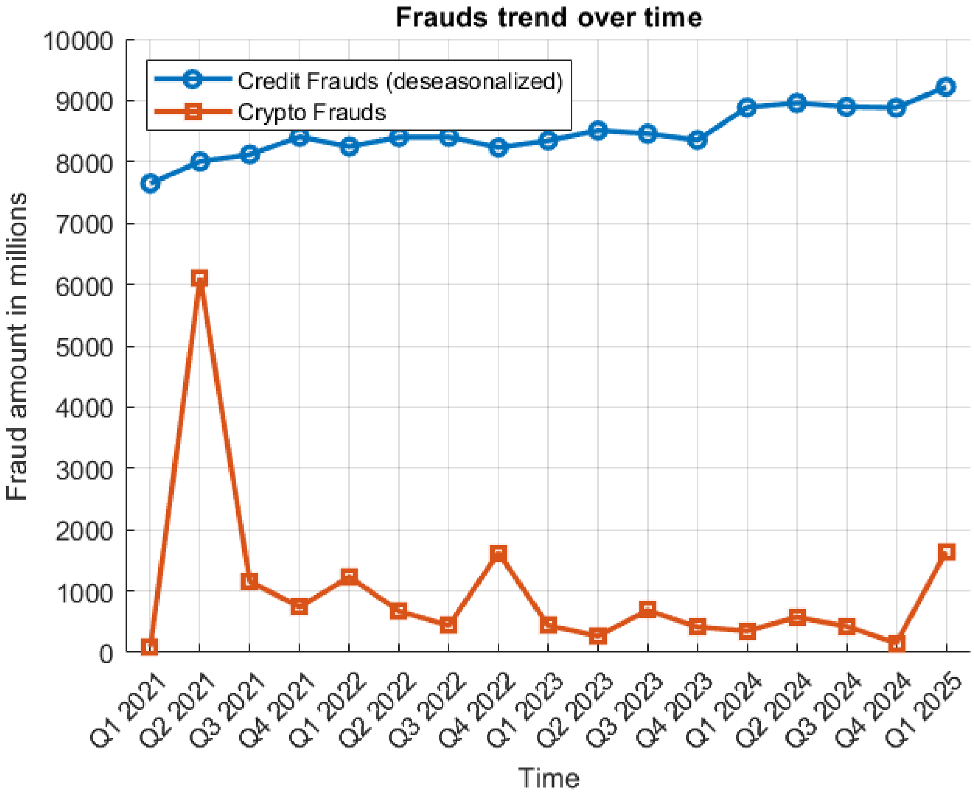


Figure 3.3 Frauds deseasonalized trend over time, Author's elaboration

It has to be noted that, as also stated by the original authors of the crypto frauds dataset (immunefi), the frauds in Q2 2021 are significantly distorted due to 2 outstanding frauds cases regarding Africrypt, which accounted for a loss of 3.5 billion USD, and Thodex, for a loss of 2 billion USD, the frauds in Q1 2025 are also skewed due to an outlier, the 1.5 billion USD fraud to Bybit, while, for Q4 2022, the observations were not classified as outliers, as the spike in frauds is not given by a single break but from multiple losses of different amounts, notably the frauds to FTX and BNB chain of around 500 million USD, among others, like the one which damaged Mango Markets, which accounted for around 100 million USD, of which 67 million were recovered. To account for the presence of these outliers, the subsequent analysis was conducted using data from Q3 2021 onwards, and the data for Q1 2025 was adjusted by removing the outlier. The next step in the analysis was to examine the logarithmic variation across quarters of both credit card fraud and crypto fraud. This approach was chosen over a normal percentage variation due to the logarithm's robustness in handling very volatile data, which is characteristic of crypto frauds. Also, the logarithm is symmetric to both increases and decreases in the data and provides additive changes over time, upgrading the overall interpretability of the results. Lastly, two difference-in-differences approaches were used in an attempt to claim causality. However, results should be interpreted with caution, as certain assumptions are needed in order to do so. The chosen cutoff dates were Q2 2023, as the MiCA was published in June 2023, and Q2 2024, as in June 2024, title III and IV entered into application. A third analysis with Q4 2024 as the cutoff date, when titles I, II, V, VI, and VII entered into application, would have been an interesting and easily implemented research, but, due to the lack of data, as noted in the section about the limits of the analysis, it was not possible to pursue. The difference in differences formulas used are shown next, where T1 refers to the cutoff date of Q2 2023 (3.4), and T2 refers to the cutoff date of Q2 2024 (3.5).

$$\text{DiD}_{T1} = \left(\overline{\text{Crypto}}_{\text{post},T1} - \overline{\text{Crypto}}_{\text{pre},T1}\right) - \left(\overline{\text{Credit}}_{\text{post},T1} - \overline{\text{Credit}}_{\text{pre},T1}\right) \tag{3.4}$$

$$\text{DiD}_{T2} = \left(\overline{\text{Crypto}}_{\text{post},T2} - \overline{\text{Crypto}}_{\text{pre},T2}\right) - \left(\overline{\text{Credit}}_{\text{post},T2} - \overline{\text{Credit}}_{\text{pre},T2}\right) \tag{3.5}$$

The characteristics of the used model need the validity of the parallel trends assumption, which will be discussed both in the results and limits of the analysis sections; however, to better show these results, an explorative analysis with a simplified interrupted time series was pursued, comparing the frauds in cryptos before and after the cutoff date, as shown in (3.6)

$$\Delta_{\text{Crypto},T2} = \overline{\text{Crypto}}_{\text{post},T2} - \overline{\text{Crypto}}_{\text{pre},T2} \tag{3.6}$$

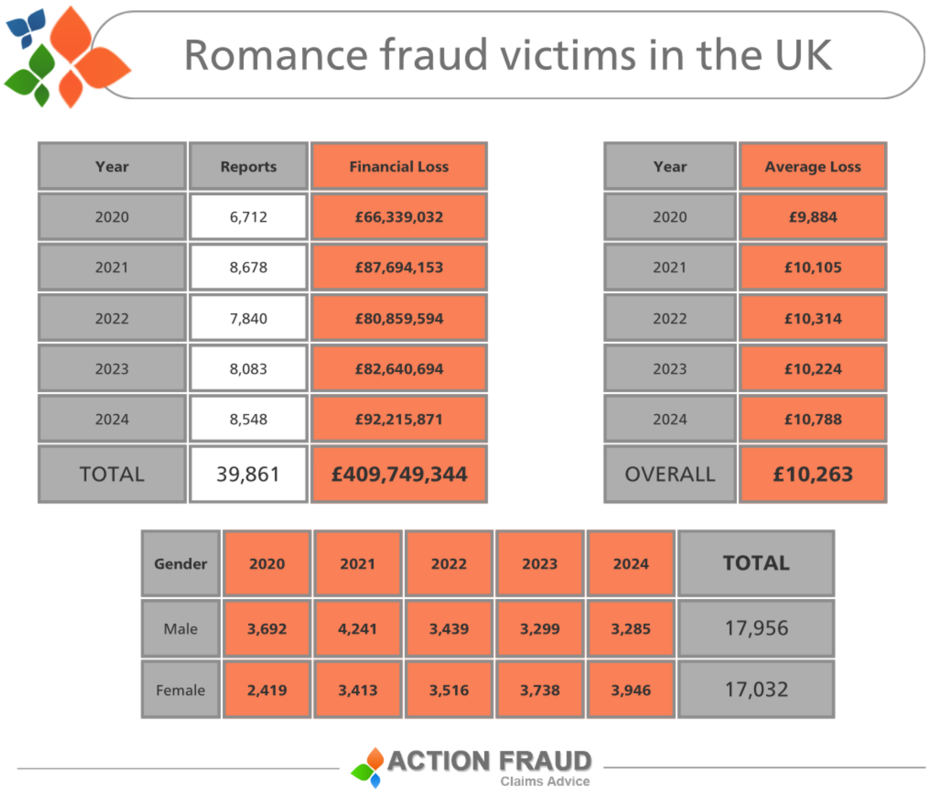
3.2.3 Results

This first analysis yields some interesting results, most notably in Table 3.1, where all calculated logarithmic differences are reported. These approximate the percentage change in fraud from one quarter to another for both cryptos and credit cards. Although the approximation is not as accurate for very volatile measures, as is the case for the crypto frauds, it shows interesting results. As it can be clearly seen, there is a considerable difference in volatility among these two variables; the quarterly log-variation for crypto frauds takes values that often surpass 0.5 in absolute value, while the variation in credit card frauds rarely exceeds 0.02. This indicates that crypto frauds are way more volatile than credit card frauds, as it was also noticed from figure 3.3, there is however, despite this significant volatility, a pretty stable trend in the decrease of crypto frauds, the average log-variation is of -0.13 meaning that crypto frauds decrease by approximately 13% per quarter of the considered period (Q3 2021 to Q1 2025) while credit card frauds have an average log variation of 0.009, meaning that credit card frauds have on average a quarterly increase of around 0.9% over the whole series. Given these differences in volatility and trends, it is clear that making a difference-in-differences analysis could be considered questionable since the parallel trends assumption, which assumes that the treated and control groups have similar trends before the cutoff date, may not strictly hold. However, due to the fact that the credit card frauds in the control group have been relatively stable on average, the difference-in-differences analysis and the simplified interrupted time series yield numerically similar results, thereby creating still informative results.

Time	Crypto_log_diff	Credit_log_diff
Q4 2021	-0.444	0.035
Q1 2022	0.508	-0.019
Q2 2022	-0.606	0.018
Q3 2022	-0.425	0.000
Q4 2022	1.307	-0.020
Q1 2023	-1.309	0.013
Q2 2023	-0.499	0.019
Q3 2023	0.949	-0.006
Q4 2023	-0.504	-0.012
Q1 2024	-0.173	0.061
Q2 2024	0.497	0.008
Q3 2024	-0.300	-0.007
Q4 2024	-1.035	-0.001
Q1 2025	0.155	0.037

Table 3.1: Quarterly log changes in crypto and credit card frauds. Author's elaboration

Specifically, for the DiDT2, the estimated value is -0.33, meaning that, if the crypto frauds had followed the same trend of credit card frauds, the average log-difference, for the quarters from Q3 2024 to Q1 2025, would have been 0.33 log-variation units lower than expected. The difference between the value of frauds post and pre-cutoff date yields a result of -0.32, meaning that, compared to the trend observed from Q3 2021 to Q2 2024, the deviation in crypto frauds for the subsequent quarters amounts to approximately -0.32 log-variation units. Both analyses therefore indicate that there has been a substantial decline in crypto frauds following the entry into application of Titles III and IV of MiCA. Clearly, this decline in crypto fraud can potentially be attributed to the MiCA; however, to claim this, we need to imply causality between the two events, which was one of the secondary objectives of this initial analysis. The causality claim needs to be argued; in fact, due to the lack of data to make extra controls and check for external shocks, there could be a number of reasons why this is violated, which will be discussed in-depth in the section about the limits of the analysis. There are, however, also a number of reasons that support the causality. First and foremost, the used control, credit card frauds, did not report any shock, in fact, its observations were remarkably stable during the considered period, so one can exclude any shock which would have also affected the amount of frauds for credit cards, for example, if a new kind of technology or innovation in the frauds sector was to be discovered or become more widespread, the amount of frauds in credit cards would have increased reflecting this new practice, at the same time any innovation in the fraud detection and prevention sector would have had an impact on the control group, decreasing the growth or inverting the growing trend in credit card frauds. This assumes that crypto frauds would have followed their previous trend realistically. Then, the fact that MiCA targets crypto-assets specifically, and that the reduction in frauds strictly coincides with the entry into application of titles III and IV, makes the assumption even more believable, reducing the chance that this reduction comes from endogenous variables. The only globally known events that could have impacted the amount of crypto fraud during the considered period are AI-driven scams and pig butchering, as cited by *Chainalysis* (2025). Both of these events would only increase the amount of scams; the causal results could therefore only differ numerically, increasing the estimated causal effect that MiCA had on the amount of fraud. Also, these cannot really be considered shocks, as frauds plausibly increase slowly over a long process rather than overnight. Then, specifically for AI driven fraud schemes, these very plausibly would also affect credit card frauds, therefore including this event in the control group, while pig butchering schemes, which is the type of fraud where the victim is convinced to make increasingly bigger payments or investments, cannot be controlled with credit card frauds, in this case another kind of fraud which is a result of ”social engineering” can be used as a control, romance scams.



Romance fraud victims in the UK

Year	Reports	Financial Loss
2020	6,712	£66,339,032
2021	8,678	£87,694,153
2022	7,840	£80,859,594
2023	8,083	£82,640,694
2024	8,548	£92,215,871
TOTAL	39,861	£409,749,344

Year	Average Loss
2020	£9,884
2021	£10,105
2022	£10,314
2023	£10,224
2024	£10,788
OVERALL	£10,263

Gender	2020	2021	2022	2023	2024	TOTAL
Male	3,692	4,241	3,439	3,299	3,285	17,956
Female	2,419	3,413	3,516	3,738	3,946	17,032

ACTION FRAUD
Claims Advice

Figure 3.4 Romance Frauds, Action Fraud (2025)

Pig butchering is, in fact, one of the most common types of fraud conducted through dating apps and in general in romance. According to collected data, the amount of fraud in the UK peaked in 2021 and has been steadily increasing throughout the considered period, as shown in Figure 3.4. The amount has not yet reached the previous peak; however, the total financial loss has already exceeded the amount registered in 2021. An increase in the growth of fraud in the matter has been registered, from 2022 to 2023, the fraud increased by 3.1%, while the increase was of 5.8% for the 2023 to 2024 period. This increase is, however, deemed not significant enough to alter the study in cryptocurrencies, since pig butchering is just one of the many types of scams regarding cryptos, and due to the limited proportion of the growth. It is then concluded from this analysis that the decrease in crypto fraud can realistically be attributed to the MiCA intervention in the sector, although with some limitations, which will be further discussed in the appropriate section.

3.3 Volatility analysis

3.3.1 Data collection

For this second analysis, two different datasets were used, both of which are composed of the prices of indices, namely the NASDAQ index and the S&P Cryptocurrency BDM Ex-LargeCap Index. Both of these indices are based in the US market and therefore the trading prices are expressed in USD. The reason for the choice of using US markets rather than European ones, for which the effect of MiCA could be easier to highlight, is both to stay consistent with the previous analysis and because the US market is arguably the most important in the crypto-assets sector. At the same time, as it is also the case for the previous analysis, US and worldwide assets are also heavily impacted by the MiCA, as it will be further discussed in the section about the limits of the analysis. The NASDAQ composite index is a stock exchange formed by over 3000 stocks which heavily weights companies in the IT sector, with a high level of innovation, which is a direct effect of the competitiveness of the sector and its intrinsic characteristic of being often driven by disruptive types of innovations. It was chosen as the control for the analysis because MiCA has a limited effect on the listed companies, as it focuses on regulating crypto-assets, which have a deep connection with IT, but whose companies have limited exposure to them. It therefore makes for an excellent proxy for an innovative financial market that is not affected by the examined Regulation. The other dataset, which will be called S&P crypto for linearity of speech, is, as stated in the factsheet of the index, "*Designed to track the constituents of the S&P Cryptocurrency BDM Index, excluding constituents of the S&P Cryptocurrency LargeCap Index*". There are some peculiarities relevant to this particular index that made it so that this was chosen as the data set for the treated group. First and foremost the BDM which stands for "Broad Digital Market", this means that a lot of different types of crypto-assets are included in this listing, including investment and utility tokens among with cryptocurrencies, with the exception of stablecoins, these were chosen to be excluded from the analysis due to the fact that many of these, as illustrated in the first chapter of the thesis, are pegged to an underlying asset, usually fiat currencies or very liquid assets, but sometimes also baskets of these kind of assets or cryptocurrencies. This characteristic makes it so that their value is artificially kept stable, and could hinder the effect of MiCA estimated from the analysis. Secondly the Ex-LargeCap characteristic of the index, which means that crypto-assets with a large capitalization are excluded from this dataset, is chosen because it represents the performance of the crypto sector beyond the largest and most capitalized crypto-assets (such as Bitcoin and Ethereum), whose performance is also influenced by coin-specific factors such as mining halving, and other macroeconomic effects which we want to exclude. Since a significant weight is given to these assets in other indices, the search for a causal link between the MiCA and volatility in returns could be hindered. The S&P crypto taken as a data set, therefore, has more components than similar, but more standard, indices. It should therefore better represent the true exploding market of crypto-assets, low capitalized crypto-assets also have a higher dependency from CASPs making them more directly impacted by the regulation, and their higher level of risk makes normative stability and transparency more important. Both datasets are composed of daily observations that represent the time span from June 2020 to May 2025.

3.3.2 Methodology

The first step in the analysis, was to manipulate the retrieved data in order to check some properties of the time series. The prices of both indices where transformed in returns, to do so the price2ret matlab function was used, which is a very simple function expressed in equation 3.7.

$$r_t = \frac{P_t - P_{t-1}}{P_{t-1}} \tag{3.7}$$

These returns are then plotted separately in Figure 3.5. To make the graphs comparable, different scales were used, and this highlights the difference in magnitude of volatility between the two groups. The presence of a widespread financial phenomenon known as ”volatility clustering” is also evident. This phenomenon describes the tendency in periods of high volatility to be followed by other periods of high volatility, and conversely, the tendency in times of low volatility to be followed by other periods of low volatility. This phenomenon cannot be ignored because it essentially tells us that volatility is history-dependent. Failing to take into account this characteristic can make the whole analysis less robust and potentially yield misleading results. Another important characteristic that these graphs have in common, which will become more evident with the analysis of squared returns, is that periods of high or low volatility are common between the two indices.

To further investigate these characteristics, one of two essentially equivalent routes can be taken; in this analysis, it was chosen to look at squared returns. However, absolute returns could also be used with the same purpose, this is due to the fact that, to make the volatility clustering more evident, one can only plot its positive values (therefore squaring or applying the absolute value) to show the serial dependence in conditional variance which, due to the balance between positive and negative values of standard returns, which are approximately distributed as a white noise, would not be shown in the correlation graph. Once again, the two graphs have different scales to make them easily comparable. There is, however, a significant difference in the squared

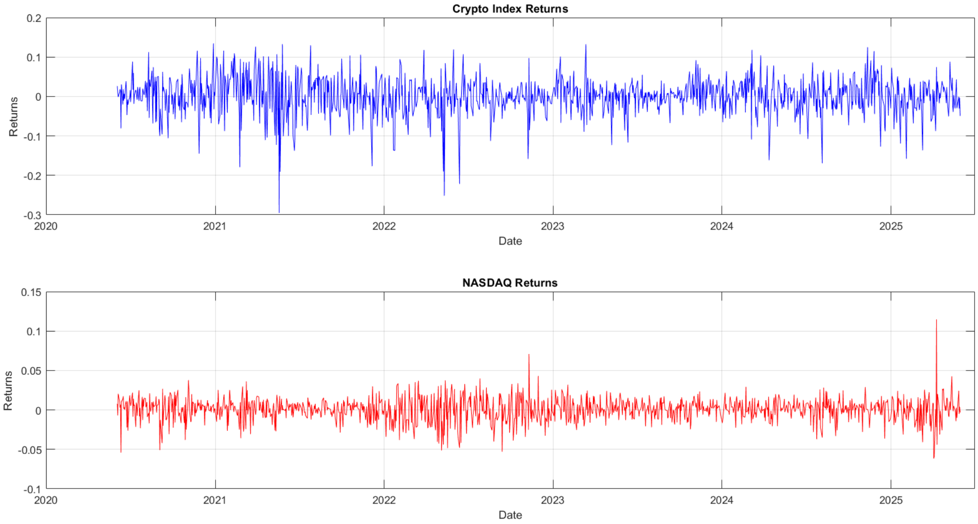


Figure 3.5 Crypto and NASDAQ returns, Author's elaboration

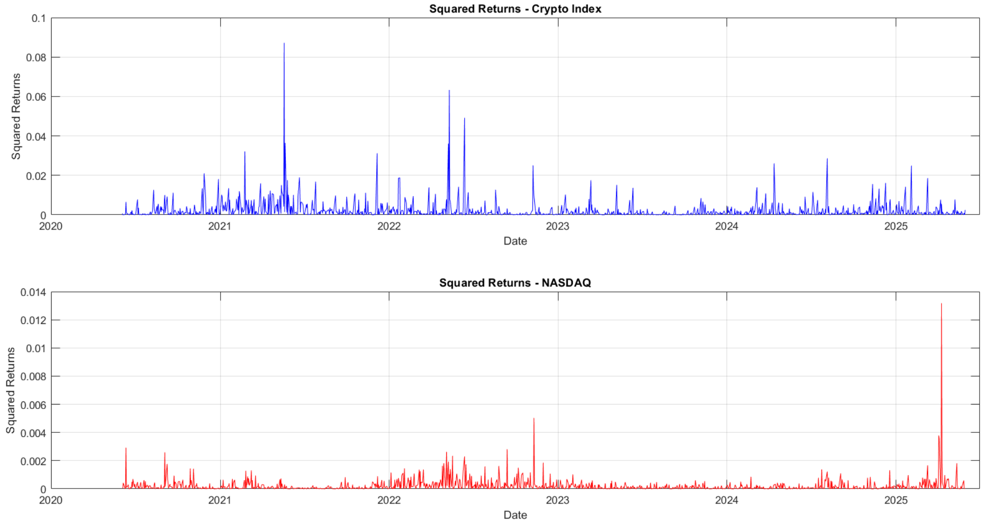


Figure 3.6 Crypto and NASDAQ squared returns, Author's elaboration

returns of the crypto index, which are clearly greater in amount than those of the NASDAQ, as expected. What can be clearly seen from Figure 3.6 is that times of volatility clustering coincide between the two indices, with a small exception for the late 2020 to late 2021 period, where the NASDAQ was still in a transition state from the pandemic shock, while the crypto index thrived due to the hype that crypto-assets had during that period. In order to further check the volatility clustering hypothesis, the autocorrelation functions of the crypto and NASDAQ indices are plotted in Figure 3.7. Both autocorrelograms of squared returns show a clear serial dependence. Despite autocorrelation being significant up to lag 5, it was chosen to model the conditional variance with a GARCH(1,1) model for both datasets, as it is the standard for much research done in the financial econometrics field. Estimates of conditional variance and standard

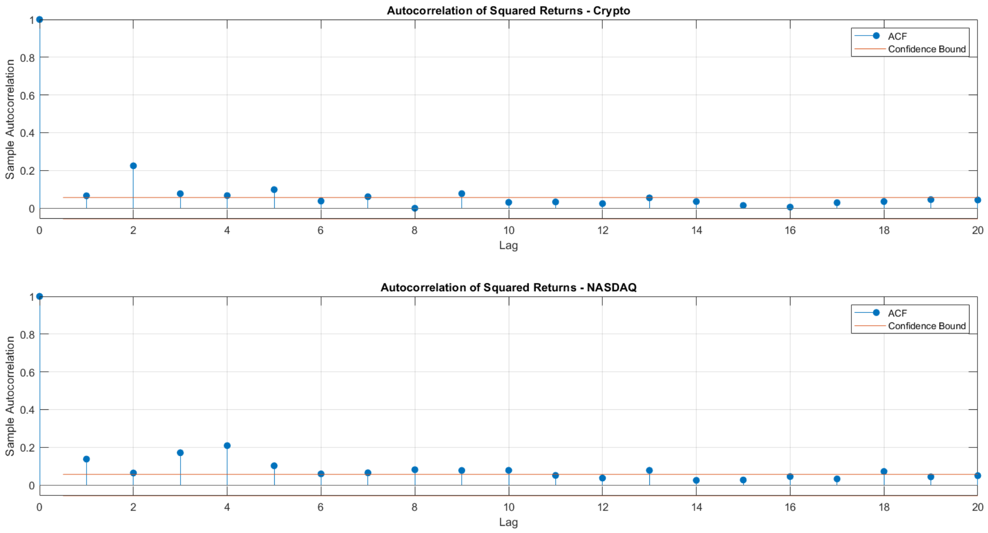


Figure 3.7 Crypto and NASDAQ squared returns ACFs, Author's elaboration

deviation were generated using the model. These estimates were then utilized to calculate the average volatility before and after the cutoff dates. In this specific case, for reasons explained in the results section, the three chosen cutoff dates were 20/04/2023, 30/06/2024, and 30/12/2024. Lastly, these averages were used to calculate the log difference between post and pre-cutoff dates for both indices' returns, and create three final difference-in-differences values for the three cutoff dates using crypto as the treated group and NASDAQ as the control group. The diff-in-diff framework is not usually employed to compare relative changes over time of the estimated conditional volatility; this approach, however, provides a simple way to quantify the effects of MiCA on the perceived risks in the financial crypto market.

3.3.3 Results

The results of the analysis, which are shown in Table 3.2, need to be carefully interpreted. First and foremost, the three cutoff dates were chosen so that results could be divided among different stages of MiCA. As it can be clearly seen, the estimated reduction in volatility of the crypto index at the time of adoption is mainly driven by a general reduction in uncertainty in the financial market, which is captured by the NASDAQ volatility. Therefore, the effect that MiCA had on the variation in volatility in the crypto index, when it was adopted, is very low. This result is to be expected as market operators need time to adapt to the regulation and create technological and legal infrastructure to comply; therefore, the effect is not yet so evident. One can definitely argue that the ”legal uncertainty” associated with many new pieces of legislation, which increases volatility when regulations are adopted, does not apply to MiCA. This again is to be expected, as one of the primary purposes of the regulation was to reduce legal uncertainty and unify different frameworks, while making clear distinctions in definitions and roles of institutions.

Table 3.2: Analysis results, Author's elaboration

Cutoff	LogChangeCrypto	LogChangeNasdaq	DiD
2023-04-20 Adoption MiCA	-0.178	-0.162	-0.016
2024-06-30 Title III and IV (ARTs/EMTs)	-0.035	0.098	-0.133
2024-12-30 Full enter into force of MiCA (CASPs included)	-0.042	0.293	-0.335

It seems that this objective was generally centered by the regulators, as the perceived riskiness of the market not only did not increase with the adoption of MiCA, but slightly declined. Then, the second cutoff date marks the entry into application of Titles III and IV. Here, it seems that the variation of the average volatility in the crypto index was slightly negative, and the variation was a lot smaller relative to the previous cutoff date. However, the true difference can be seen with respect to the NASDAQ index. In fact, this very small (but still relevant) decline in perceived riskiness of the crypto index is surrounded by an environment of increased volatility, as shown by the control group. Therefore, although the market was experiencing a period of turmoil, the perceived risk in the crypto sector, during the considered period, slightly declined, while the perceived risk declined noticeably with respect to the rest of the market. Lastly, the last cutoff date marks the entry into application of the full MiCA text; the results are similar in general direction to those of the previous cutoff date, but they differ in size. The variation of the average volatility in the crypto index continued to decline in an environment of even greater uncertainty. It needs to be noted that these results are differences between logarithms of averages, therefore, due to logarithmic properties, they can be interpreted as the logarithm of the ratio of averages, but not directly as percentage changes, especially for values which are larger, as it is the case for the last cutoff date, where the conversion of the DiD yields an approximate reduction of 28.6 % in volatility. This analysis has the excellent property of being simple to interpret; more complex models, in such a complex environment, could create a black box that makes results less clear. These more complex models have the advantage of being more robust, as they can utilize a greater number of controls and statistical properties. Also, making further checks and hypothesis tests, which are not really possible with this framework, as it will also be noted in the section about the limits of the analysis. To increase the robustness of these results, the same analysis has been repeated, with the exact cutoff dates, using only data relative to the observations of the previous and subsequent month. This is because the results might be skewed due to external significant shocks that altered the volatility of either indices, attributing this external change to the MiCA. A clear example of external shock is the tariffs that the USA imposed on imports, and their multiple announcements and reversals, altering the dynamics of international supply chains and hurting the general market stability of both indices. The drawback is that having fewer observations makes the analysis overall more exposed to outliers and does not account for medium to long-term effects of the regulation, which are captured instead by the comprehensive analysis. These results somewhat confirm the previous analysis in a smaller size, and are shown in Table 3.3. Of great interest are the results regarding the second cutoff date; here, from month to month, the variation of the average volatility of the crypto index increased, despite the long-term effect being negative. The fact that the overall diff in diff stays negative, despite this change, reflects the fact that it was a period of particular turmoil for the market overall, but the MiCAR still had a positive result, reducing the average volatility by around 4%. The previous remarks regarding the effect of MiCA around the third cutoff date also hold, making the analysis more robust, since the analyzed period is smaller. The main difference stands in the size of the estimated effect, the fact that the new DiD for the third cutoff has a value of -0.259 in log variation, or approximately -22.8 %. This difference of approximately 5.8% is explained by a smaller volatility variation in the NASDAQ, which is consistent with the absence of observations relative to the tariffs, as previously explained, despite a larger reduction in crypto volatility.

Table 3.3: DiD results using a 1-month window before and after each cutoff, Author's elaboration

Cutoff	**LogChangeCrypto**	**LogChangeNasdaq**	**DiD**
2023-04-20 Adoption MiCA	-0.101	-0.120	0.019
2024-06-30 Title III and IV (ARTs/EMTs)	0.120	0.162	-0.042
2024-12-30 Full enter into force of MiCA (CASPs included)	-0.093	0.166	-0.259

The results are therefore consistent among the two analyses, it's clear that, after the implementation of the last titles of MiCA, the average volatility declined both in the short and medium/long term. This in itself is a valuable result and serves as an explorative analysis for the build-up of future literature, as, at the time of writing, it does not exist. The claim of causality, even if the data and the used models seem to support it, has to be taken with caution, due to the limitations and assumptions involved. Further research in the matter might shed light upon this question, testing these results with more controls, and possibly over a longer horizon, since not even a year has passed since the last cutoff date. This and other limitations are discussed in the next section.

3.4 Limits of the analysis

In my opinion, it is essential for every thesis and academic publication to include a section acknowledging potential problems and limitations. It is important so that future literature can build upon the existing one by correcting potential mistakes, including new techniques and exploring new ideas. The final objective is to create enough scientific evidence to have an impact on more practical matters, as it is the purpose of this analysis on the MiCA regulation, or just to find the answers to unanswered questions. In order to reach this objective, critical thinking is required, and the process is vastly more efficient when it begins with those who know the work best: the authors of their own work. The first problem that was found stems from the availability of fraud data; in fact, as it was already previously stated, the literature with regards to frauds and crypto-assets mainly stems from the studies in computer science with regards to the sector of fraud detection. The collected data, as is usually the case, was also developed in this direction. There are many datasets available with information regarding crypto frauds which contain a series of variables which are very useful when the objective is to create an algorithm which predicts wether a given crypto-asset or website is fraudulent or clean, but are of no use, in my view, for an economic analysis on the effect of any event on the amount or total value of frauds conducted in a selected time period. The dataset used in the first analysis was not chosen due to its specific characteristics, as it was instead the case for the second analysis; it was chosen as the only available dataset that displayed the value of fraud in cryptocurrencies over time, with observations updated so that they could be relevant for the event study. After the analysis was completed and the current thesis was in its final stages, a new dataset, which shares similar problems with the one used in the analysis, was released (on September 4, 2025). This new dataset, published by the Federal Trade Commission, displays quarterly data for fraud from Q1 2020 to Q2 2025, differentiated for the type of payment methods in the US (Federal Trade Commission. (2025). A new potential study in the matter could utilize this dataset to identify discrepancies between fraud in cryptocurrency payments and other payment methods, thereby enabling a more accurate policy evaluation of MiCA with a greater number of controls. A problem that this new dataset does not address is its lack of Europe-centricity; it is based on the US, whereas the study's dataset includes worldwide fraud. This is not a significant issue, as crypto-assets and CASPs seeking to operate in the European market must comply with European legislation, regardless of their ”origin”. It is clear that in an intrinsically global market, as is the case for the cryptocurrency one, a new set of rules and needed documentation, for example, the white-paper/prospectus, will have a global effect, as all investors worldwide will be able to access that newly published documentation, regardless of their country's legislation. If Europe-centric data was in the matter was published, it could be possible to replicate this analysis to check the effect of MiCA on the frauds in Europe (which is presumably what matters for the European regulator) rather than in the world, but, it is argued that this change in data would not matter as much due to the nature of the regulation and the weight that European investors carry in financial markets. Another point to be made is that, since the regulation lastly entered into effect from December 2024, not enough time has passed to estimate any long-term effects of the full entry, just the anticipation effect from the approval in June 2023 and the entry into effect of titles III and IV in June 2024. In the future, when more data will be retrieved and published, it will be possible to introduce a third cutoff date (as it has been done for the second analysis, due to data being available), which tracks the entry into force of other titles from MiCAR. The last limit that was found for the first analysis is the parallel trends assumption for the diff in diff, as it was already explained, to counter this problem a second study was done, where instead of assuming that crypto frauds would have followed credit card frauds, which might be far fetched due to their previous history, it is instead assumed that they would follow their previous trend, which is supported by the fact that credit card frauds were very stable in the considered period, the two results almost coincide due to the aforementioned stability. Overall, the analysis can be considered robust in the context of exploring this mostly untouched sector. The causality claim is, as is the case for most studies, realistic, although it rests on these assumptions, which are both reasonable and justified with facts and data. With regards to the second analysis, the same argument of geographically different data is used as per the first analysis, in this case, both indices capture US based data, but the effect of MiCA on global volatility is still important, as crypto-assets relevant in the EU mostly also operate in the US market, and a general reduction in perceived risk from European investors can easily spread among international investors, therefore capturing the effect nonetheless. Once again, capturing the effect on European specific markets would be in the best interest of the European Regulator, therefore, a future analysis with different data could be helpful for policy-making. Although it is true, as shown by the graphs, that volatility clustering periods mostly coincide between NASDAQ and the crypto index, the parallel trends assumption, although realistic, might be violated, making the causal inference less robust. An analysis with further controls could be done, using, for example, certain commodities to check for macroeconomic shocks, or different indices, and this could improve the robustness of the causal inference. Lastly, the GARCH (1,1) model is a standard in the industry and was therefore chosen to model estimated volatility due to the volatility clustering characteristic of financial markets. Both GARCH models used for the indices however, assume normal standard errors which, although very convenient, might not be respected, and one could decide, especially for the crypto index, to use a t-student distribution of standard errors, which is also a standard for the financial industry and could better capture the ”*fat tails*” of the distribution. Overall, the second analysis nicely serves the purpose of investigating the volatility in the ex-large-cap crypto market in the periods that follow and precede the MiCA regulation.

3.5 Conclusions

Two analyses were made to explore the most recent developments in the crypto world. The first analysis focused on the total value of frauds, and clearly shows that over time, frauds have been on a steady decline, although with some bumps on the road, which are attributed to single big scams, rather than a sum of multiple small frauds. If crypto frauds, after the entry into effect of titles III and IV of MiCA, had followed the same trend of credit card frauds, the average log-difference, for the quarters from Q3 2024 to Q1 2025, would have been 0.33 log variation units lower than expected, while if they had followed their previous trend from Q3 2021 to Q2 2024 they would have been 0.32 log-variation units lower than expected. There is no way to be sure that either of these two assumptions would hold, as explicitly described in the section about the limits of the analysis, but they both have their points of strength and weakness. They both represent realistic scenarios supported by data and facts, as reported in the appropriate sections. However, the estimate may lack precision due to the limited availability of data and the model's controls. This is precisely why further analysis in the matter is needed, and more importantly, just as a European harmonized data collection system for fraud is needed, given that the data is already collected by local authorities when scams are reported. The technological infrastructure is already in use for many other data-driven sectors; therefore, an investigation into the feasibility of a harmonized European dataset could be very useful, not only for this particular policy evaluation, but also for evaluating and updating future harmonizing efforts. Such progress would allow more robust analyses to be made, with more precise estimates of their true effects, ultimately strengthening the scientific evidence upon which future regulatory decisions could be made.

The second analysis, rather than focusing on fraud, focused on the perceived risk and volatility variation in the crypto-assets market. It shows the evolution of volatility, estimated with a GARCH(1,1) model to account for volatility clustering, and then captures the variation in average estimated volatility at multiple cutoff dates. Most notably, the last cutoff date, the full entry into force of MiCA, shows a significant reduction of the average volatility relative to the control group: the NASDAQ index. This result is confirmed by replicating the same analysis, using only data that accounts for the previous and following months to the cutoff date, to prevent extra shocks from skewing the results, although with a reduced estimated effect. Here, once again, some simplifying assumptions were made in order to reach these results, and the limits are driven by the absence of previous econometric analysis in the matter. The important discovery that stems from these results, which needs to be highlighted, is that reducing the legal uncertainty in the market, with an effort in the harmonization process among different legislative attempts, both from state members and European previous directives and regulations, seems to have a positive effect on concrete matters, such as perceived risks and value of frauds. Future research could investigate various econometric evaluations of different policies to uncover aspects unknown to regulators, such as whether directives or regulations are more effective, considering their respective strengths and drawbacks.

Summary

In the financial world, crypto-assets are becoming more and more relevant every day. New cryptocurrencies are born every day, digital tokens provide services in a way that has never been possible before, and most central banks are either investigating or testing CBDCs. In this evolving landscape, the European jurisdiction tries to keep up by promoting the publication of technology neutral legislation, harmonizing member state laws and previous European directives, and supporting a legal and safe environment where innovation can thrive without potentially harming the stability of financial markets. In this thesis, these aspects of the financial world are discussed in the first chapter, where a taxonomy of crypto-assets is developed starting from the basic structure made by Kochergin (2022) and re-elaborating it, adding new definitions, examples, and updating it with new aspects from more specific studies on narrower types of crypto-assets to offer a new, comprehensive and updated classification. A second chapter on the legal framework has been developed, detailing the evolution of the regulatory landscape in Europe up to the most recent legislation, MiCA, produced by European regulators. For a comprehensive and accurate description of the main characteristics of the regulation, the original text of MiCAR itself was used, published on EUR-Lex (Regulation 2023/1114, 2023), while the book from Zetzsche & Woxholth (2025), among others, was used to have a more academic point of view on the matter as well as clarification from a legal textbook. The third chapter is instead based on the author's statistics and econometric analysis; the first of the two describes the evolution of fraud in cryptocurrency worldwide and finds a substantial reduction in the average variation of fraud after the introduction of MiCA. A claim of causality is then developed with a Diff-in-Diff approach, although with some limits, which are thoroughly described in a subsequent section about the limits of the analysis. The second analysis focuses instead on the perceived risks from the market in the cryptocurrency sector, estimating conditional variance with a GARCH(1,1) model and analyzing the evolution of volatility in the US market, finding a significant reduction in the average relative conditional volatility after the event. Once again, a claim of causality is then developed with a Diff-in-Diff approach, with its own challenges and limits, which have been discussed. Overall, further analysis on the matter is needed, particularly when new data becomes available and possibly when additional data is published to enhance the analysis. It is clear that in sectors so complicated, technologically advanced, and interconnected as is the case for cryptos, guarding the safety of the financial markets, while avoiding over-regulation and the subsequent strangling of innovation, is a complex challenge

even for the most informed regulators. However, the only way to make this challenge easier is to continue creating scientific evidence and update the legal landscape accordingly. This thesis makes a step in the right direction, where decisions are based on the innovative collaboration of data analysis and human ideas, hopefully creating the best possible regulations for a better society.

Bibliography

[1] Zetzsche D, Woxholth J. *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation*. Cambridge University Press; (2025).

[2] European Central Bank. *Virtual Currency Schemes*. Frankfurt am Main: European Central Bank; (2012).

[3] European Central Bank. *Virtual Currency Schemes: A Further Analysis*. Frankfurt am Main: European Central Bank; (2015).

[4] Benson, V., Adamyk, B., Chinnaswamy, A. et al. *Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions*. Eur J Law Econ 57, 37–61 (2024).

[5] European Union. *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. Official Journal of the European Union (2018).

[6] Chainalysis. *Crypto Crime Report 2025*. Chainalysis Inc.; (2025).

[7] Kochergin, D. *Crypto-Assets: Economic Nature, Classification and Regulation of Turnover*. International Organisations Research Journal, 17(3) (2022).

[8] Ankenbrand, T., Bieri, D., Cortivo, R., Höhener, J., & Hardjono, T. *Proposal for a Comprehensive (Crypto) Asset Taxonomy*. arXiv preprint arXiv:2007.11877 (2020).

[9] Bakas, D., Magkonis, G., Oh, E.Y. *What drives volatility in Bitcoin market?* Finance Research Letters, 50, 103237 (2022).

[10] Kahya, A., Krishnamachari, B., Yun, S. *Reducing the Volatility of Cryptocurrencies – A Survey of Stablecoins*. arXiv preprint arXiv:2103.01340 (2021).

[11] Grobys, K., King, T., & Sapkota, N. *A Fractal View on Losses Attributable to Scams in the Market for Initial Coin Offerings*. Journal of Risk and Financial Management, 15(12), 579 (2022).

[12] Auer, R., Cornelli, G., Frost, J. *Rise of the Central Bank Digital Currencies*. International Journal of Central Banking, 19(4), 185–214 (2023).

[13] Illes, A., Kosse, A., Wierts, P. *Advancing in tandem – results of the 2024 BIS survey on central bank digital currencies and crypto*. BIS Papers No. 159, Bank for International Settlements (2025).

[14] Aslan, A., Şensoy, A., Akdeniz, L. *Determinants of ICO success and post-ICO performance*. Borsa Istanbul Review, 23(1), 217–239 (2023).

[15] Caccia, E., Tapking, J., Vlassopoulos, T. *Central bank digital currency and monetary policy implementation*. ECB Occasional Paper No. 345 (2024).

[16] European Securities and Markets Authority (ESMA). *Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments*. ESMA Document ESMA75453128700-1323, Paris (2025).

[17] European Banking Authority (EBA), European Securities and Markets Authority (ESMA), & European Insurance and Occupational Pensions Authority (EIOPA). *Joint ESA Final Report on Art 97 Guidelines MiCAR*. JC 2024 28, Paris (2024).

[18] European Union. *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 public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC*. Official Journal of the European Union (2017).

[19] European Union. *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*. Official Journal of the European Union (2023).

[20] Aerts, S., Born, A., Gati, Z., Kochanska, U., Lambert, C., Reinhold, E., & van der Kraaij, A. *Just another crypto boom? Mind the blind spots*. Financial Stability Review, Issue 1, 86–97. European Central Bank (2025).

[21] Barsan, I. M. *Are MiCAR's Market Abuse Rules Useful? A critical analysis of the market abuse rules under MiCAR*. SSRN Electronic Journal (2024).

[22] Lehmann, M. *MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?* European Banking Institute Working Paper Series No. 160 (2024).

[23] Asscheman, A. *Crypto-assets under MiCAR: a deep dive into risks, solutions, and regulatory convergence*. ERA Forum, vol. 24, no. 4, pp. 489–500 (2023).

[24] Ou, H., Guo, Y., Huang, C., Zhao, Z., Guo, W., Fang, Y., & Huang, C. *No Pie in the Sky: The Digital Currency Fraud Website Detection*. In *International Conference on Digital Forensics and Cyber Crime*, pp. 176–193 (2023).

[25] Immunefi; Immuni Software Pte. *Value of cryptocurrency theft worldwide from Q1 2021 to Q1 2025 (in million U.S. dollars) [Data set]*. In Statista. Published March 31, 2025.

[26] Statista. *Total value of losses due to card fraud worldwide — split between the United States and rest of the world — from 2014 to 2023, with forecasts on the total size of fraud for 2024, 2026, and 2028 (in billion U.S. dollars) [Data set]*. In Statista. Published December 31, 2024.

[27] Statista. *Total number of Visa credit card transactions processed for payments worldwide from 1st quarter 2008 to 1st quarter 2025 [Data set]*. In Statista. Published July 29, 2025.

[28] Statista. *Value of payments processed (TPV – Total Payment Volume) of Visa issued credit cards worldwide from 1st quarter 2008 to 2nd quarter 2025 [Data set]*. In Statista. Published July 29, 2025.

[29] Japan Consumer Credit Association. *Value of damage caused by credit card fraud in Japan from 2015 to 2024 (in billion Japanese yen) [Graph]*. In Statista. Published March 7, 2025.

[30] S&P Dow Jones Indices. *S&P Cryptocurrency BDM Ex-LargeCap Index [Data set]* (2025)

[31] NASDAQ. *NASDAQ Composite Index Historical Data [Data set] (2025).*

[32] Federal Trade Commission. *Value of fraud loss in the United States from 1st quarter 2020 to 2nd quarter 2025, by payment method (in million U.S. dollars) [Graph]*. In Statista. (2025)

Sitography

- CoinMarketCap. (2025). *Cryptocurrency market capitalization charts*. Retrieved from https://coinmarketcap.com

- Reuters. (2025). *Bitcoin hits fresh record as Fed easing bets add to tailwinds*. Retrieved from https://www.reuters.com/

- Jones Day. (2025). *Crypto Assets, CASPS, and AML/CFT Compliance: The New European Regulatory Landscape Under MiCA and AMLR*. Retrieved from https://www.jonesday.com

- Cointelegraph. (2020). *What Is the EU's Fifth Anti-Money Laundering Directive (AMLD5)?*. Retrieved from https://cointelegraph.com

- Bloomberg. (2022). *Terra's $45 Billion Face Plant Creates Crowd of Crypto Losers*. Retrieved from https://www.bloomberg.com

- Action Fraud. (2025). *Our research and statistics on romance fraud*. Retrieved from https://www.actionfraud.org.uk/

- New York Times. (2025). *Trump Tariff Timeline*. Retrieved from https://www.nytimes.com/