Evaluating MiCA Framework via Industry Perceptions of Risks

ABDULKHAMID MUKHAMEDOV, TPM, TU Delft, Delft, Netherlands
VANESSA SIMÕES DE AZEVEDO, Independent Researcher, Amsterdam, Netherlands
MICHEL VAN EETEN, TPM, TU Delft, Delft, Netherlands
JOLIEN UBACHT, TPM, TU Delft, Delft, Netherlands
YURY ZHAUNIAROVICH, TPM, TU Delft, Delft, Netherlands

The growing economic value of blockchain-driven financial applications brings increasing risks. In recent years, EU regulators felt the urgent need to address the financial and security risks that digital currencies might pose if left unsupervised. In 2020, the European Commission proposed a draft regulation called Markets in Crypto-Assets (MiCA). It sets out the rules for the crypto-asset issuers and service providers located in the EU or serving EU clients. To date, there is no evaluation of the risks covered by the proposed regulations besides the Commission's own evaluation.

We conducted a study to identify the risk perceptions of different stakeholder groups in the market by interviewing 20 representatives of Crypto-Asset Service Providers, Crypto-Asset Issuers, Institutional Investors, and Legal Experts. We then compared the risks deemed relevant by the stakeholder groups with the risks covered in the MiCA framework. That allowed us to identify which risks and stakeholder groups' concerns are insufficiently covered by the current version of the MiCA framework. As a result, we show that Crypto-Asset Issuers' risks are the least addressed in the current MiCA version. Specifically, residual risks remain with regard to smart contracts, oracles, and transactions. These risks should be considered for upcoming amendments to the regulation.

CCS Concepts: • **Applied computing → Law**; • **Social and professional topics → Governmental regulations**; • **General and reference → Empirical studies;**

Additional Key Words and Phrases: Markets in crypto-assets, MiCA, regulation, risk analysis, decentralized finance

ACM Reference Format:
Abdulkhamid Mukhamedov, Vanessa Simões de Azevedo, Michel van Eeten, Jolien Ubacht, and Yury Zhauniarovich. 2026. Evaluating MiCA Framework via Industry Perceptions of Risks. *ACM J. Responsib. Comput.* 3, 1, Article 6 (January 2026), 27 pages. https://doi.org/10.1145/3785002

Authors' Contact Information: Abdulkhamid Mukhamedov, TPM, TU Delft, Delft, Netherlands; e-mail: abdulkhamid_mukhamedov@hotmail.com; Vanessa Simões de Azevedo, Independent Researcher, Amsterdam, Netherlands; e-mail: simoes.vanessa@outlook.com; Michel van Eeten, TPM, TU Delft, Delft, Netherlands; e-mail: M.J.G.vanEeten@tudelft.nl; Jolien Ubacht, TPM, TU Delft, Delft, Netherlands; e-mail: j.ubacht@tudelft.nl; Yury Zhauniarovich (corresponding author), TPM, TU Delft, Delft, Netherlands; e-mail: y.zhauniarovich@tudelft.nl.

ACM 2832-0565/2026/01-ART6
https://doi.org/10.1145/3785002

1 Introduction

In June 2019, Facebook revealed the news about Libra, a worldwide digital currency project built on the blockchain infrastructure [62]. This announcement attracted mixed responses among the public and regulators. While the advocates and supporters highlighted the benefits of the technological efficiency of Libra and the potential economic inclusivity it may bring, the critics voiced concerns about Libra's ability to destabilize the global [45] and national [66] financial systems. In 2019, Facebook had around 2.4 billion active monthly users, all of whom could be potential users of the Libra currency [12]. At several billion potential users, Libra's private money could pose a competitive risk to the financial sovereignty of entire countries and contribute to the denationalization of money by overcoming politics and the traditional credit system [51]. Moreover, Facebook was just the first mover, as in 2019, Telegram announced its decentralized cryptocurrency Gram [23], and Walmart attempted to patent its own stablecoin [65].

These developments called for an increase in oversight [12, 66]. Within just two weeks after the Libra's announcement, some of the major banks and regulators around the world, such as the Bank of England, US Federal Reserve and Bank of France, communicated that they would be closely inspecting Libra and introducing heavy regulations, while the **European Central Bank** (**ECB**) led a critical discussion on the evaluation of risks posed by digital currencies together with the **Group of Seven** (**G7**) states [105]. In the **European Union** (**EU**), governments struggled to apply the existing financial regulations, mainly the **Markets in Financial Instruments Directive II** (**MiFID**) [38], to crypto-markets, due to the lack of clarity about what falls under the definition of financial instruments and about how market integrity rules would apply in crypto-markets. Hence, in 2020, the **European Commission** (**EC**) published the first draft of the **Markets in Crypto-Assets Framework** (**MiCA**) [36], which, for the first time, outlined rules and standards for crypto-markets and their participants. The new framework aimed to solve identified issues by directly targeting crypto-assets, such as stablecoins, and introducing integrity rules specific to markets dealing with crypto-assets and services. Implemented in 2023 and anticipated to fully come into effect on December 30, 2024, MiCA is the first attempt to introduce stability, legal clarity, and enhanced market integrity into the newly emerging crypto-markets.

Several attempts were made to evaluate the MiCA framework draft from different perspectives: from an environmental perspective [101], from the compliance and alignment perspective with the previous regulations [104], from the implementation and enforceability viewpoints [13], and from the national systems perspective [17, 72, 78]. Additionally, several recent studies investigated the perspectives of stakeholders on the challenges and risks of blockchain, but they were either focused on specific topics, such as sustainability and supply chains [22], blockchain adoption [63], or scoped around the general aspects of technology rather than its use in financial applications [83]. However, to the best of our knowledge, none of the prior studies, besides the EC's own evaluation [35], have empirically analyzed how MiCA relates to what the industry players perceive as important risks. In this study, we close this gap by answering three research questions:

RQ1: *What risks are seen as the most relevant by industry stakeholders?*
RQ2: *What risks are covered by the MiCA framework?*
RQ3: *What residual risks remain, and whose interests do they mostly affect?*

To answer these questions, we interviewed 20 experts representing different groups of industry stakeholders, namely, ***Crypto-Asset Service Providers (CASP)***, ***Crypto-Asset Issuers (CI)***, ***Institutional Investors (II)***, and ***Legal Experts (LE)***. We asked the respondents to assess the relevance of 18 risks derived from the **World Economic Forum** (**WEF**) "Decentralized Finance Policy-Maker Toolkit" [31] document. We also conducted a content analysis of MiCA to assess the

extent of the risks being covered by the framework and integrated the results with the findings from the interview study, drawing actionable conclusions.

Our analysis shows that risks raised by CASPs are covered the most in the current version of the MiCA framework, while risks raised by CIs are covered the least. This might reflect unequal participation or representation during the development of the regulation or a stronger lobbying position of IIs. At the same time, according to Rodríguez Bolívar et al. [83], the development of an effective regulation related to blockchain and distributed ledger technologies requires balanced involvement of diverse stakeholders. We also find that *Smart contract*, *Oracle*, and *Transaction* risks are not covered by the MiCa framework yet deemed important by stakeholders. We conclude that these risks need to be prioritized for inclusion in future amendments. Ellul et al. [34] also support this conclusion, noting that regulations of blockchain, distributed ledger, and smart contracts technologies should move beyond mainly financial control and incorporate also technological assurances.

In summary, our study offers a unique insight into how well MiCA addresses the risks identified by industry players. It critically examines the regulation and highlights the current relevance of these risks. Additionally, it provides actionable recommendations and outlines key areas for future regulatory focus that should be incorporated into the regulation through an iterative process [83].

2 Background

2.1 MiCA Framework

In 2020, the EC published the first draft of the MiCA framework 2020/0265 (COD) [36], an element of the Digital Finance Package and Digital Finance Strategy. The framework aims at installing appropriate levels of consumer and investor protection and market integrity, ensuring financial stability, while supporting innovation and promoting the development of crypto-assets. *It introduces the rules on issuance, trading, and provision of other financial services on blockchain that do not qualify under the judicial scope of electronic money, financial instruments, or deposits under the existing laws of MiFID* [36]. When enforced as planned in 2024, MiCA will establish a single licensing regime allowing issuers and service providers of crypto-assets to operate freely across every EU Member State. Companies both inside and outside the union will be under the scope of MiCA regulation as long as they serve EU clients. Companies would also have a choice to operate under the specific member national law, avoiding getting the common EU license [36].

The MiCA framework [36] consists of *nine* sections, referred to as *Titles*. *Title I* sets down the focus and the scope of the regulation in general and presents the definitions, while other titles focus on the regulatory requirements for specific types of crypto-assets and participants. To refer to blockchains, MiCA uses the synonymous term ***Distributed Ledger Technology (DLT)***, while cryptocurrencies or digital currencies are referred to as *crypto-assets*. MiCA makes a distinction between *issuers* and *service providers* of crypto-assets: issuers offer the assets to the public, and service providers perform services and functions with regard to crypto-assets. Issuers and service providers may be decentralized (so-called *Decentralized Autonomous Organizations* or DAOs), i.e., be governed by a distributed code-based contract. There are no distinctions between the levels of centralization defined in the framework. At the moment of conducting this research, the topics of **Decentralized Autonomous Organizations (DAOs)** and **Non-Fungible Tokens (NFTs)** were omitted by the regulators and not mentioned in the text of the initial MiCA proposal. However, the first amendment A09-0052/1 [94] acknowledged that certain crypto-assets might be issued by a DAO as opposed to a legal entity. In that case, as long as such assets satisfy MiCA's requirements and do not compromise financial stability, market integrity rules, and investor protection, the EU trading platforms are permitted to admit them. Regarding NFTs, MiCA states it does not apply to crypto-assets that are unique and non-fungible, including digital art and collectibles. Nevertheless,

the text underlines that the issuance of a crypto-asset in a large series or collection makes it qualify as a fungible asset, despite having a potentially unique identifier representing the asset. In short, the MiCA framework calls for a substance-over-form approach where the nature of an asset should be determined by competent authorities, regardless of what the issuer states it to be.

Once the MiCA framework comes into the force, the stakeholder groups, namely, *CI*, *CASP*, *II*, *LE*, *Private Investors* and *Users*, are expected to comply with the regulation within the defined timeline. We excluded the latter two groups from consideration because their representatives were unlikely to be familiar with the regulation, upcoming at the time of conducting this research. Moreover, we also excluded *Policy Makers* from the consideration because they are not subjects of the MiCA framework enforcement. Thus, within this work, we study only the former four groups of stakeholders: CI, CASP, II, and LE.

2.2 WEF's Risk Framework

The WEF [2] is an independent international non-governmental organization funded by its member companies committed to improving the state of the world by involving political, business, cultural, academic, and other leaders in developing and setting global, regional, and local agendas. As a response to the rapid growth of the DeFi ecosystem in 2018–2020, the WEF developed "Decentralized Finance Policy-Maker Toolkit" [31] that covers risks and policy approaches for this area. We decided to utilize the 17 risks identified in this document to evaluate what risks are covered, not covered, or partially covered by the MiCA framework. These risks have been collected as a result of extensive industry collaboration and input from experts across various entities involved in digital assets.

Additionally, after consulting with the field experts and doing a pilot study, we have decided to add an additional risk, ***Regulation Risk***, which is not mentioned in the WEF toolkit [31]. Researchers in the field of DeFi regulation have highlighted that the current retroactive policy approach could have disastrous effects on the industry and be even counter-productive in addressing the **Anti-Money Laundering** (**AML**) and **Combating the Financing of Terrorism** (**CFT**) concerns [85]. For instance, experts say that the Indian Finance Bill 2022, introducing 30% tax on crypto profits (including holdings) and 1% additional tax on every crypto transaction, will have a detrimental effect on the industry in the country [76].

Thus, we have got 18 risks in total. Table 1 lists the risks and provides their short description, while below we elaborate on each risk and provide the examples of its execution.

1. Market Risk. A risk of increase or decrease of the value of a position or portfolio that occurs due to fluctuations in market prices [50]. This risk is a very general financial risk that can occur in trading any assets where factors such as interest rates, commodity prices, and interest rates can affect the market [41]. The importance of this risk is mainly posed by challenges related to comparing digital tokens to fiat currencies or real-life assets that may cause significant price fluctuations, often driven purely by traders' trust and expectations related to the digital tokens. For instance, a lawsuit against Elon Musk was filed in June 2022, accusing him of the intentional pumping of the Dogecoin price of more than 36,000% in two years. Price volatilities in crypto-markets pose significant threats to investors and the financial eco-systems that are built incorporating crypto-assets and services. In the previous years, there were signs of a bear market, where the total value of cryptocurrencies plummeted from 800 billion USD in 2017 to 100 billion USD in 2019, considerably wiping out wealth and assets possessed by investors and crypto-asset owners [106].

2. Counterparty Risk. A risk of a counterparties' failure to fulfill their end of a financial obligation, which can also involve credit or settlement risks. According to Fantazzini and Zimin [41], credit risk in the scope of cryptocurrencies is "the gains and losses on the value of a position of a cryptocurrency that is abandoned and considered dead according to professional and/or academic criteria, but

Table 1. Descriptions of the Risks

ID	Risk	Risk Description
1	**Market**	A risk of increase or decrease of the value of a position or portfolio that occurs due to fluctuations in market prices.
2	**Counterparty**	A risk of a counterparties' failure to fulfill their end of a financial obligation, which can also involve credit or settlement risks.
3	**Liquidity**	A risk of incurring insufficient funds or assets to support the value of a financial asset.
4	**Transaction**	A technical risk of failing or dysfunctional Layer1 blockchain network, potentially causing double-spending, overly expensive transactions and insufficient throughput, which ultimately affects the application layer.
5	**Smart Contract**	A smart contract is an agreement defined in the form of software code stored in a blockchain that is executed based on a predefined set of factors and events.
6	**Miner**	A risk of market manipulation by miners who order and execute transactions by enabling certain parties to profit faster than others.
7	**Oracle**	A risk of manipulated on-chain prices or data due to oracles providing unsafe or inauthentic data, which are selected based on developers' best knowledge.
8	**Routine Maintenance and Upgrades**	A risk related to the challenging implementation of routine maintenance and upgrades as some platforms and activities cannot be shut down, fixed, and relaunched in the same way as traditional servers.
9	**Forks**	A risk associated with the creation or existence of blockchain forks with an altered or similar set of parameters of the original service.
10	**Key Management**	A risk associated with a loss of cryptographic keys.
11	**Governance Mechanisms**	A risk of abuse of governance voting mechanisms through bribery, concentrated token control, and aggressive acquisition of tokens to gain influence over the system.
12	**Redress of Disputes**	A risk associated with the lack of clarity on how to resolve a conflict that has occurred on a decentralized platform using a centralized judicial system.
13	**Fraud and Market Manipulation**	A risk associated with malicious behavior of actors in the DeFi spaces intended to misinform and scam users.
14	**Financial Crime**	A risk associated with criminal activity such as money laundering, terrorism financing, and evasion of financial sanctions.
15	**Regulatory Evasion**	A risk of failure to comply with the regulatory standards of traditional financial services.
16	**Dynamic Interactions**	A risk of DeFi's use of cross-border, unlimited user interaction, leading to unprecedented emergent risks, as well as new interaction risks, as a consequence of the interoperability between traditional and decentralized finance.
17	**Flash Crashes or Price Cascades**	A risk of significant loss of assets due to price cascades that cannot be stopped or frozen in a traditional manner.
18	**Regulation**	A risk of creating additional barriers to innovation and technology development due to the introduction of new regulations.

which can be potentially revived and revamped." The criticality of credit risk in DeFi is largely posed by volatility that can generate under-collateralization. Moreover, the anonymous nature of DeFi creates challenging processes to determine whether a party can be trusted with a credit loan. Settlement risk is the failure to receive expected assets as a result of fraud, misinformation, uneducated investment choices, and inability to understand the smart contract that oversees the completion of payments [31]. For instance, in March 2022 a hacker exploited the flawed design of a pay-to-earn crypto game named Axie Infinity to steal 625 million USD. The users were only reimbursed for a third of their losses [6].

3. Liquidity Risk. A risk of incurring insufficient funds or assets to support the value of a financial asset. Liquidity risk can be faced by both users and issuers of a crypto-asset. If there is a lack of liquidity for a user, the trading position can be forcefully liquidated, resulting in a loss of funds and assets. For a CASP, a lack of liquidity can result in an inability to support the transactions on the trading platform, severely affecting its operational performance. This risk is very similar to the one of traditional finance liquidity risk, yet it is more critical in dealing with crypto-assets due to

their notorious volatility. For instance, in March 2023, the price of USDC stablecoin (which should remain at 1 USD) fell to 0.87 USD because a part of its reserves was in the collapsed Silicon Valley Bank.

4. Transaction Risk. A technical risk caused by a failing or dysfunctional Layer 1 blockchain network, potentially causing double-spending, overly expensive transactions and insufficient throughput, which then ultimately affects the application layer. Transaction risks can be caused by a malicious attack on the network, for instance, a double spending[1] or spam[2] attacks [10]. One of the most famous examples of this risk execution is the CryptoKitties game. Due to its popularity, this app was responsible for 20% of all computations on the Ethereum platform and caused network congestion, which forced the developers of the game to double the fee of each transaction [4]. Another indicative example is the hack of the MakerDAO platform [15]. The hacker managed to clog Ethereum Mempool so that the bids in the MakerDAO collateral auctions from other participants did not get minted into the blockchain blocks, i.e., did not get executed. This allowed the hacker to participate in these auctions, in some cases solely, and buy ETH tokens at a very low price, sometimes even reaching 0 USD. The total gain of the attacker is estimated at 8.3 million USD.

5. Smart Contract Risk. A smart contract is an agreement defined in the form of software code stored in a blockchain that is executed based on a predefined set of factors and events [87]. Like all software, smart contracts can have potential vulnerabilities that may result in programming errors, flaws, and misintended executions. Even though distributed ledgers are not susceptible to single-point-of-failure attacks, the novel nature of the said technology presents opportunities for malicious behavior. For instance, in August 2021, the Poly Network was hacked, and around 610 million USD in different cryptocurrencies were transferred to the attackers' wallets [5]. Luckily, the hacker returned all the stolen funds. Another case occurred in 2022, when an Ethereum liquidity provider XCarnival suffered a loss of 4 million USD after a malicious attack exploiting a smart contract vulnerability. The attack resulted in a paid ransom of 1.8 million USD by XCarnival, while no legal charges have been filed against the hacker in exchange for the return of the stolen funds [73].

6. Miner Risk. A risk of market manipulation by miners who order and execute transactions by enabling certain parties to profit faster than others. In blockchain systems, miners are individuals who are paid a fee for processing transactions and creating blocks. Since miners can rearrange transactions, they possess an advantage over non-miners when it comes to token offerings and arbitrage trades [90]. For instance, MEV (Miner Extractable Value) bots create and exploit arbitrage opportunities via front-running attacks. In September 2022, a MEV bot earned more than 1 million USD by exploiting only one transaction [40].

7. Oracle Risk. A risk of manipulated on-chain prices or data due to oracles providing unsafe or inauthentic data, which are selected based on developers' best knowledge [33]. Due to the absent interoperability of blockchains with the real world, the so-called oracles play a significant role as the main interface between the two realms. By definition, *oracles* are external third-party centralized entities that report data to a blockchain, which a smart contract relies on to execute its protocols. If Oracle data is compromised, users may be at risk of observing manipulated on-chain prices. For instance, in February 2020, an attacker managed to take a profit of 2,378 ETH by pumping the price of the sUSD token at Kyber, which is the price oracle for bZx, and selling at bZx 943,837 sUSD bought at the other platform, namely Synthetic Depot [75].

[1]Double spending attack occurs if the same single token is spent more than once.
[2]Spam attack can be defined as a malicious action that utilizes network inefficiencies and weaknesses to reduce its transaction speed and delay block generations.

8. Routine Maintenance and Upgrades Risk. A risk related to the challenging implementation of routine maintenance and upgrades, as some platforms and activities cannot be shut down, fixed, and relaunched in the same way as traditional servers. For instance, after the launch of the Solana blockchain [93] in March 2020, the platform has experienced several outages. Due to the outage in June 2022, the price of Solana cryptocurrency dropped by 12% [64].

9. Forks Risk. A risk associated with the creation or existence of blockchain forks with an altered or similar set of parameters of the original service. One of the most famous cases of this risk execution was witnessed in September 2020, when an anonymous developer Chef Nomi created a fork of a well-known DEX Uniswap [1] and launched SushiSwap (SUSHI). The fork was almost identical to Uniswap, but a portion of the transaction fees was converted into SUSHI tokens and distributed among all holders of SUSHI tokens. Moreover, initial participants were able to get SUSHI tokens only if they deposited Uniswap's tokens, which could be swapped for the underlying **liquidity pool** (**LP**) assets. As a result, Uniswap's liquidity was drained to SushiSwap. This event is known as the first "vampire mining" in the DeFi space [95].

10. Key Management Risk. A risk associated with a loss of cryptographic keys. Key management is highly important in DeFi, and the loss of keys can result in users and service providers permanently losing access to their assets and services. For instance, it is estimated [26] that Satoshi Nakamoto, the anonymous creator of Bitcoin, mined around 1.1 million BTCs in 2009, which is equal to around 20 billion USD at the current price. Since then, this early fund has not been touched, creating speculations if the key to it is still available. Another example of this risk is the hack of the Vulcan Forged blockchain game studio, during which the attackers got access to 96 private keys, allowing them to drain assets from the corresponding wallets.[3]

11. Governance Mechanisms Risk. A risk of abuse of governance voting mechanisms through bribery, concentrated token control, and aggressive acquisition of tokens to gain influence over the system. In certain blockchains, token owners have the ability to vote on a range of issues, which can vary from minor parameter adjustments to a complete overhaul of the governance mechanism [44]. Once certain actors own a substantial amount of network tokens, they can abuse the system, making this a severe risk in the crypto markets. For instance, a DeFi project Beanstalk lost its reserves worth 182 million USD due to a governance attack [91]. An attacker took a flash loan, acquired enough Beanstalk tokens, passed a malicious proposal to the network and seized the platform's funds.

12. Redress of Disputes Risk. A lack of clarity on how to resolve a conflict that has occurred on a decentralized platform using a centralized judicial system. Individuals seeking redress resulting from a software failure, market manipulation or misinformation may not be able to receive effective juridic support. Correcting and relaunching a smart contract is often impossible or is highly challenging; thus, any alteration requirements or procedures similar to traditional contracts may simply not be an option. For instance, the Ethereum foundation was even forced to make a hard fork of its blockchain to return the investments stolen as a result of "The DAO" attack [29].

13. Financial Crime Risk. A risk associated with criminal activity, such as money laundering, terrorism financing, and evasion of financial sanctions. Since users are anonymous and the prevention of transactions, in general, is impossible, AML and CFT monitoring is difficult to establish. Not surprisingly, hackers often exploit cryptocurrencies for their illicit activities [100]. For instance, a recent report [58] claims that attackers linked to North Korea managed to steal more than 1.7 billion USD only in 2022.

[3] https://rekt.news/vulcan-forged-rekt/

14. Fraud and Market Manipulation Risk. A risk associated with the malicious behavior of actors in the DeFi spaces intended to misinform and scam users. A recent systemic literature review [98] reports that the most represented fraud cases are **Initial Coin Offering** (**ICO**) scams [96], Ponzi schemes [14], phishing [24], mining malware [27], pumps and dumps [59], and wallet scams [67].

15. Regulatory Evasion Risk. A risk of failure to comply with the regulatory standards of traditional financial services. Since many DeFi services are by nature similar to traditional banking services (investing, borrowing, lending, insurance, etc.), they may still need to comply with the traditional regulations and not be exempted from it simply due to performing these services using alternative technology such as blockchain. This creates regulatory tensions and the risks of accidental or purposeful failure to comply with existing financial services regulations. One prominent example of regulatory evasion is the Ooki DAO. This decentralized platform provides its users, including U.S. persons, the facilities to trade crypto derivatives products. According to US laws, in this case the platform must be registered and conduct **Know-Your-Customer** (**KYC**) checks, which have not been performed to date [71].

16. Dynamic Interactions Risk. A risk of DeFi's use of cross-border, unlimited user interaction that may lead to unprecedented emergent risks, as well as new interaction risks, as a consequence of the interoperability between traditional and decentralized finance. This risk does not exist in traditional finance and is still largely unexplored, as it is not clear how large-scale DeFi adoption will impact the global financial system. However, a recent example of the Silvergate bank collapse due to the FTX currency exchange bankruptcy [82] confirms the relevance of this risk.

17. Flash Crashes or Price Cascades Risk. A risk of significant loss of assets due to price cascades that cannot be stopped or frozen in a traditional manner. When the number of liquidations dramatically increases in a short period of time, the extreme decrease in asset price results in large losses for the investors. In traditional finance, brokers are able to freeze transactions to prevent this from happening, but such strategies are not suitable for blockchain systems governed by smart contracts. For instance, an exploitation of the Harvest Finance DeFi platform in October 2020 [102] resulted in a 65% drop of its token price in less than one hour.

18. Regulation Risk. A risk of creating additional barriers to innovation and technology development due to the introduction of new regulations. Researchers in the field of DeFi regulation have highlighted that the current retroactive policy approach could have disastrous effects on the industry and be even counter-productive in addressing the AML and CFT concerns [85]. For instance, experts say that the Indian Finance Bill 2022, introducing 30% tax on crypto profits (including holdings) and 1% additional tax on every crypto transaction, will have a detrimental effect on the industry in the country [76]. Another more recent example of this risk execution is the adoption of the Data Act by the European Parliament [9]. According to this legislation, smart contract developers must perform a conformity assessment of their developed contracts to the essential requirements listed in the bill, potentially hindering innovation and technology development in this area. Finally, the upcoming enforcement of the MiCA regulation has already resulted in spurring the talks about delisting the noncompliant tokens from cryptocurrency exchanges [86].

3 Methodology

3.1 Identifying Relevant Risks

To answer **RQ1**, i.e., *"What risks are seen as the most relevant by industry stakeholders?"*, we decided to collect the opinions of the stakeholder group representatives. While surveying a large number of representatives across different stakeholder groups could offer a more accurate estimation of the most relevant perceived risks, the absence of a widely accepted list of risks specific to the crypto-assets markets, combined with the need for clarification and explanation of the risk

definitions provided in the "Decentralized Finance Policy-Maker Toolkit" [31], led us to opt for an interview-based study instead.

3.2 Recruiting Experts for Interviews

However, recruiting the right respondents—insiders who have the required knowledge and can provide valuable insights—proved to be difficult. First, people working in the blockchain industry are often privacy-savvy. They often hide behind pseudonyms, and it is very hard to persuade them to participate in an interview that is recorded. Second, the blockchain industry is relatively new, so the pool of people with sufficient expertise was smaller than in other well-established areas. Third, up to now, a lot of professionals have been ignoring the legal aspects of the blockchain industry because they believe in distributed smart-contract-based governance. Furthermore, at the time of the study, regulations for the crypto industry were still in their early stages of development, and many professionals were not yet familiar with them. Despite these constraints, to ensure the quality of the obtained data, we set up additional requirements for the respondents to become selected for this study. They must:

(1) have prior or current professional involvement in crypto-assets and services provisioning;
(2) have at least two years of professional experience in the crypto-asset and services industry;
(3) be employed by an EU organization or by a non-EU company that plans to serve or serves EU clients (thus, falling within the MiCA regulatory scope);
(4) be well-familiar with MiCA (for legal firm employees) or with general crypto regulatory practices in the EU (for the private sector);
(5) have an understanding and showcase awareness of risks their employer perceives.

We utilized several strategies to find candidates. First, an open invitation was posted on LinkedIn and widely promoted by the research group. The post called upon experts working in the crypto-markets and employed by either a legal firm, a CI, a CASP, or an institutional investment company that participates in the crypto-markets or develops an entry strategy. Second, the research team reached out to their networks and sent out personal invitations to industry experts from every category described above. In total, more than 170 personal invitations were sent out. The response rate among these experts was notably low. Most commonly, experts declined due to time constraints and heavy professional commitments. Nevertheless, from the responses obtained by utilizing both of these strategies, we selected 20 interviewees who passed our selection criteria. Table 2 describes the participants, reporting the data about their group, background and whether their company is based in the European Union (EU-based). Note that no two interviewees were employed by the same entity at the time of the study. Although detailed backgrounds cannot be disclosed for privacy reasons, the sample includes experts from technical, regulatory, and risk-focused roles, working in firms of varying sizes. Additionally, the selected interviewees form a diverse sample consisting of professionals located in Italy, the USA, the Netherlands, Germany, Belgium, Switzerland, Norway, India, and Spain.

According to Hennink and Kaiser [52], opinion saturation is achieved within the range of 9–17 interviews for homogeneous groups, which is smaller than our total sample size. However, given that our total sample size consisted of diverse experts, our group can be argued to be heterogeneous. Hagaman and Wutich [48], performing a multi-cultural study on water issues in four sites, revealed that reaching metathematic data saturation required 20–40 interviews. While we acknowledge that our sample size is at the low end of this spectrum due to the sensitivity and complexity of interview objective, we tried to minimize the impact on the validity of our results by considering the factors described by Rahimi and Khatooni [79] to increase saturation. First, by avoiding random sampling and targeting industry experts mostly from selective reputable firms or DeFi projects with at least

Table 2. List of Interviewees

ID	Group	Background	EU-based
1	LE	Legal Expert	Yes
2	LE	Legal Expert	Yes
3	CI	Employee at a Crypto-Asset Issuer Firm	No
4	CASP	Employee at a Crypto-Asset Service Provider Firm	Yes
5	CASP	Employee at a Crypto-Asset Service Provider Firm	Yes
6	II	Employee at an Institutional Investment Firm	Yes
7	II	Employee an Institutional Investment Firm	Yes
8	CI	Ex-Employee at a Crypto-Asset Issuer Firm	Yes
9	CASP	Employee at a Crypto-Asset Service Provider Firm	Yes
10	II	Employee at an Institutional Investment Firm	No
11	LE	Legal Expert	No
12	LE	Legal Expert	Yes
13	CASP	Employee at a Crypto-Asset Service Provider Firm	No
14	CASP	Employee at a Crypto-Asset Service Provider Firm	Yes
15	LE	Legal Expert	Yes
16	LE	Legal Expert	No
17	CASP	Employee at a Crypto-Asset Service Provider Firm	Yes
18	LE	Legal Expert	Yes
19	LE	Legal Expert	Yes
20	CI	Ex-Employee at a Crypto-Asset Issuer Firm	No

two years of direct professional experience in crypto markets, we aimed to maximize the depth and quality of information. Second, by setting the data collection time per interview to an average of one hour, we enabled nuanced insight gathering and discussions, while avoiding information overload and interviewee fatigue. Third, by employing a combined data-gathering approach of open questions followed by a guided closed risk ranking exercise, we further enhanced the richness of the obtained data.

It is important to note that the aim of the study was not to achieve comprehensive representation of all stakeholder perspectives for statistical generalization, but rather to derive broadly applicable insights. According to Guest, Bunce, and Johnson [47], as few as six interviews can be sufficient to identify basic metathematic elements in homogeneous groups. Our LE and CASP groups, comprising 8 and 6 participants respectively, met this criterion. Recruiting participants for the remaining two groups proved more challenging, particularly for the CI group. Nevertheless, we successfully identified 3 representatives for this group, matching the number recruited by the EC during the public consultation phase [35], despite the extensive resources available to them. We also note that, thanks to the focused experience of the representatives from these two groups, during the third interviews with IIs and CIs we already noted repetition of core themes due to the depth of responses from the first two. However, we recognize that our findings may exhibit some variations when applied to a different group of experts.

3.3 Interview Setup

The interviews with the experts were held online as one-on-one video calls, lasting for approximately one hour. The interview consisted of two parts. During the first part, the interviewees were asked open-ended questions about their awareness and reception of the MiCA and the DeFi regulation in general. During the second part, the interviewees scrutinized the risks individually. They were

presented with a list of 18 risks described in Section 2.2 and tasked to go through it with the interviewer, indicating whether they perceived a risk as relevant in their line of work. This approach allowed the respondents to understand each risk, asking the interviewer for any clarifications if required. Note that the number of risks that can be selected as relevant was not limited.

For all interviewees and each stakeholder group individually, we calculated the percentage of participants who considered each risk relevant. If more than two-thirds of participants deemed a risk relevant, we classified its relevance as *High*; if fewer than one-third considered it relevant, we marked it as *Low*. The relevance of the risks falling between these thresholds was categorized as *Medium*.

Ethics. This study was discussed with the university's IRB and got a clearance to conduct it. Before the start of each interview, participants were briefed about the data collection process and signed a consent form. The respondents were assured anonymity to encourage them to feel safe and free to voice their opinions. We explained that non-anonymized data would not be shared with anyone besides the researchers participating in this study. We report aggregated results and do not provide details about the demographics of the interviewees since, given the small size of the dataset and the uniqueness of some of the experts, this data could enable the de-anonymization of the participants.

3.4 Identifying Risks Covered in MiCA

To answer **RQ2**, i.e., *"What risks are covered by the MiCA framework?"*, we performed the content analysis of the entire MiCA framework to identify the risks covered by the framework and understand to what extent they are addressed by the regulation. To complete this task, we adopted the Summative Content Analysis methodology described by Hsieh and Shannon [55]. The methodology is used in qualitative research to analyze and interpret the content of texts, documents, and other forms of communication. It aims to identify patterns and themes within the textual data, gain insights, and draw conclusions based on those insights. The objective of the content analysis is to classify the risks according to the extent of their coverage in the MiCA framework. We selected three categories of risk coverage: *Addressed*, *Partially Addressed*, and *Not Addressed*. A risk is considered as *Addressed* by the MiCA framework if it is directly mentioned, elaborately explained, and addressed by an article or chapter that is designed to minimize the said risk. In case risks are indirectly mentioned by the framework, briefly explained, and only partially addressed in a limited manner and/or for specific cases, they are considered as *Partially Addressed*. Finally, risks are considered *Not Addressed* if they are not directly mentioned, defined, or reflected by a MiCA article or chapter.

To bootstrap the content analysis, for each risk, we assigned a list of keywords consisting of the risk name itself and any synonymous or relevant terms that could aid in locating the risk in the text. We applied a keyword search to the MiCA framework and got a set of articles mentioning the corresponding risk. Then, we carefully reviewed the content of these articles, finding justifications for putting the risk into a particular category. Note that keyword search was used to kick off the content analysis, providing the starting point for further scrutiny. If additional pertinent articles were uncovered during the subsequent investigation, they were included in the list as well. Table 3 elaborates on how we executed the content analysis.

Let us consider the "Fraud and market manipulation" risk as an illustrative example. For this risk, we selected the following set of keywords: fraud, manipulation, scam, insider, false, dishonest, misleading, misinformation, dealing, bribery, and abuse. A search using these keywords, followed by a closer examination of the text, identified four relevant articles: 77, 78, 79, and 80. We carefully analyzed those articles and provided justifications to assign the risk to the *Addressed* category.

Table 3. Content Analysis Methodology to Estimate Risk Coverage

	Risk Coverage		
	Addressed	**Partially Addressed**	**Not Addressed**
Explanation	The risk is directly addressed by rules, guidelines or procedures in the framework	The risk is indirectly or partially addressed by rules, guidelines or procedures in the framework	The risk is not addressed in the framework
Indicators	The risk is directly mentioned, elaborately explained and addressed by an article or chapter that is designed to minimize the said risk	The risk is indirectly mentioned, briefly explained and partially addressed by an article or chapter that is designed to minimize the said risk, yet in a limited manner and only for specific cases	The risk is not directly mentioned anywhere in the framework
	Examples		
Risk	Fraud and market manipulation	Key Management	Smart Contract
Keywords	Fraud, manipulation, scam, insider, false, dishonest, misleading, misinformation, dealing, bribery, abuse	Keys, cryptographic keys, access, custody, key management, storing, reserve management	Smart contract, contract, protocol, mechanism terms, conditions, rules
Relevant Articles	Art. 77: Disclosure of inside information Art. 78: Prohibition of insider dealing Art. 79: Prohibition of unlawful disclosure of inside information Art. 80: Prohibition of market manipulation	Art. 33: Custody of reserve assets	Not Found
Justification	- Presence of clear definitions of the risk and incidents - Articles relating to a broad range of situations and nuances related to fraud and market manipulation - Possibility of goal operationalization direct enforcement of rules, guidelines and procedures	- No clear definitions of access keys, key management or "security access protocols" as mentioned in MiCA - Only relevant for CIs and CASPs with registered companies and liable individuals, decentralized projects are not addressed	- No definition or mention of smart contracts

Table 4. Identifying Residual Risk Level

		Risk Coverage		
		Addressed	**Partially Addressed**	**Not Addressed**
Risk Relevance	**High**	*Medium*	*Medium*	*High*
	Medium	*Medium*	*Medium*	*Medium*
	Low	*Low*	*Medium*	*Medium*

3.5 Identifying the Residual Risks

To answer **RQ3**, i.e., *"What residual risks remain, and whose interests do they mostly affect?"*, we combined the results of the previous RQs analysis, applying the qualitative risk assessment methodology with the classical two-factor measure of risk [80]. Table 4, adapted from NIST risk assessment guidelines [84], is used to determine the *Residual Risk*, which could have three levels: *High*, *Medium*, or *Low*. In order to find the residual risk level, one should select the corresponding *Risk Relevance* level (see Section 3.1) as the row index and the *Risk Coverage* level (see Section 3.4) as the column index, and take the corresponding cell value.

Similarly to how risk practitioners determine post-treatment risk levels to define risk acceptance strategy [77], in our approach, we consider MiCA regulations as treatments against defined risks presented in Table 1 to perform a high-level assessment and gain an understanding of the extent to which MiCA can be argued to address risks of the crypto markets. This approach allows us to assess the residual risk level both across all interviewees and within each stakeholder group individually.

In this study, we use the former to identify risks with high residual values that correspond to those that should be prioritized in future amendments to the MiCA framework. The latter is used to identify which group's risks are the least prioritized.

4 Findings

For this study, we interviewed 20 participants in the period of June-September, 2022. Out of 20 interviewees, 8 represent *LE*, 6 – *CASP*, 3 – *CI*, and 3 – *II* group (see Table 2). The majority of them (14) represent EU-based companies. At the time of the interviews, 2 interviewees were ex-workers of their companies.

In general, when the participants were asked about their views and thoughts on the MiCA framework as an open-ended question, many stated that there was a need for the regulation of crypto-assets and services. It would introduce legal clarity for the industry players and open more opportunities for II to participate in the market, which is generally perceived as a positive trend in the adoption of crypto-assets: *"Overall, I am positive about MiCA because it sets out clear boundaries for such an important topic as e-money tokens, asset-referenced tokens that are covered under the umbrella term of stablecoins, and these are very important in the picture of the overall market"* (Legal Expert, EU-based firm). According to the same interviewee, MiCA represents a *"significant step forward"* in providing clarity for stablecoins, establishing rules to prevent market manipulation, and defining custody requirements for CASPs and issuers. These measures are expected to encourage greater adoption of digital assets by consumers: *"I think the more we end up regulating [crypto-assets and services], the more things stabilize, the more it starts becoming attractive for the masses. I think eventually that's gonna be a good thing"* (Ex-Employee, CI Firm). Additionally, according to Legal Expert from a non-EU-based company, introducing the framework would have a positive effect not only on consumer's confidence, but also on II: *"I think it's a good thing for all involved because the moment you have clarity in framework, it puts every everyone at ease. This is especially important for institutional investors, because as you know, especially the big banks are heavily regulated and they can't just trade in anything and so the moment that there's an actual legal framework for them to rely on, it's a lot easier for them to step into the market and actually trade in crypto, hold assets for clients."* This opinion is also echoed by Employee of a CASP: *"I feel that in general, policies and regulations are important to bring the cryptocurrency market to the next level because without these regulations and policies, the really big players, like the traditional financial banks and companies, cannot really go to dive into it without these policies and regulations. So I feel that that it's a good thing that these things are happening."*

4.1 Risk Relevance

Table 5 reports the risk relevance for each stakeholder group individually (columns *CASP*, *CI*, *II,* and *LE*) and all participants (*All* column) together. Each cell shows the percent of interviewees deemed the risk as relevant and the corresponding risk relevance level in parenthesis. The value in the *# Unsure* column shows the number of interviewees who were unsure if the risk is relevant (*N/A* values in raw data). In our analysis, we did not take them into consideration. In the last row, we report the *Krippendorff's alpha* values [61] that show inter-rater agreement for each stakeholder group and all interviewees in the bottom right cell, which we have calculated using the `fast-krippendorff` Python library [21]. According to Klaus Krippendorff [61], Krippendorff's alpha equal to 1 indicates perfect agreement among raters. A value exceeding 0.8 signifies a satisfactory level of agreement, while values falling between 0.67 and 0.8 are typically considered to draw tentative conclusions. A level of 0 suggests no agreement among raters beyond what would be expected by chance alone. Conversely, levels below 0 indicate a systematic disagreement among raters. Note that these levels are indicative when raters use the same text as a reference, which

Table 5. Risk Relevance: Percent of Interviewees and the Corresponding Level in Parenthesis (*H* - High, *M* - Medium, *L* - Low)

ID	Risk	# Unsure	Stakeholder Group				All
			CASP	CI	II	LE	
1	**Market**	0	100 (H)	67 (M)	67 (M)	88 (H)	85 (H)
2	**Counterparty**	0	67 (M)	33 (L)	67 (M)	88 (H)	70 (H)
3	**Liquidity**	0	100 (H)	67 (M)	100 (H)	88 (H)	90 (H)
4	**Transaction**	0	67 (M)	100 (H)	67 (M)	88 (H)	80 (H)
5	**Smart contract**	0	67 (M)	100 (H)	100 (H)	75 (H)	80 (H)
6	**Miner**	1	50 (M)	67 (M)	67 (M)	62 (M)	60 (M)
7	**Oracle**	1	67 (M)	100 (H)	100 (H)	62 (M)	75 (H)
8	**Routine maintenance and upgrades**	3	100 (H)	100 (H)	0 (L)	50 (M)	65 (M)
9	**Forks**	0	50 (M)	100 (H)	33 (L)	50 (M)	55 (M)
10	**Key management**	0	100 (H)	100 (H)	100 (H)	88 (H)	95 (H)
11	**Governance mechanisms**	0	67 (M)	100 (H)	67 (M)	88 (H)	80 (H)
12	**Redress of disputes**	0	83 (H)	100 (H)	67 (M)	62 (M)	75 (H)
13	**Financial crime**	0	67 (M)	67 (M)	100 (H)	100 (H)	85 (H)
14	**Fraud and market manipulation**	0	100 (H)	67 (M)	100 (H)	100 (H)	95 (H)
15	**Regulatory evasion**	0	83 (H)	67 (M)	100 (H)	75 (H)	80 (H)
16	**Dynamic interactions**	2	83 (H)	67 (M)	33 (L)	62 (M)	65 (M)
17	**Flash crashes or price cascades**	0	100 (H)	100 (H)	67 (M)	88 (H)	90 (H)
18	**Regulation**	0	83 (H)	100 (H)	100 (H)	62 (M)	80 (H)
Krippendorff's alpha			0.03	-0.05	0.12	0.00	0.02

is not our case. However, they still can be used to draw conclusions about which group provides more consistent answers.

As shown in Table 5, the most relevant risks identified by the majority of the participants are: *Key management* (95% or 19 out of 20 interviewees), *Fraud and market manipulation* (95%), *Liquidity* (90%), and *Flash crashes or price cascades* (90%). Almost all participants identified *Key management* as a relevant risk. Indeed, this risk is one of the most related to the crypto industry because the ownership of a crypto-asset is typically proven with a cryptographic key. Thus, losing a key means that all the corresponding funds are lost. For example, in early 2019, a Canadian exchange QuadrigaCX was plugged off due to extreme monetary damages valued at over $200 million incurred by 76,319 users as a result of its founder's passing, the sole person who possessed the cryptographic keys to the platform's offline reserves. The company filed for bankruptcy; investors' and clients' losses could not be recovered [32]. It is also clear why *Fraud and market manipulation* is perceived by almost all participants. Given the anonymous and pseudo-anonymous nature of cryptocurrencies and the absence of regulations, it is hard to attribute the individuals who manipulate the market and convict them: *"Also, for market manipulation, that is so important having clear rules in such a market where pump-and-dumps and manipulation techniques, in general, are very, very common"* (Legal Expert, EU-based firm).

Some prominent differences emerge if the data is analyzed for each stakeholder group separately. For the LE group, the most relevant risks are *Financial crime* and *Fraud and market manipulation.* At the present moment, LE face these issues most often in their professional activities. *Liquidity*, *Smart contract*, *Oracle*, *Key management*, *Financial crime*, *Fraud and market manipulation*, *Regulatory Evasion* and *Regulation* risks are among the most relevant for the IIs. These risks may greatly influence the market value of crypto-assets, so they directly affect this stakeholder group. For instance, while IIs recognize the necessity of regulations, they also emphasize that these should not hinder innovation and development: *"Certainly we need regulation. If we want to take this niche,*

isolated, DeFi world and expose it to more traditional finance entities, there needs to be regulation that will actually spur growth into this segment of the market. Without it we are stuck to retail, and it's been important until now, but to keep going we need to allow regulation, regulation that doesn't hamper innovation. It needs to just put all of this into some sort of a legal framework, but without being too restrictive, which is also something that that it's worrying. Right now the space is kind of like the Wild West because of the lack of regulation" (Employee Institutional Investment, non-EU-based firm).

Besides examining which risks are considered the most relevant, it is also interesting to analyze which are the less relevant ones. For instance, as shown in Table 5, *Forks* (55%) and *Miner* risk (60%) are considered less relevant. Whereas the impact of these risks is quite high, the probability of their execution is quite low. Moreover, in the case of forks, individuals usually can choose which fork to adopt. Interestingly, none of the II identified *Routine maintenance and upgrades* as a relevant risk for them. At the same time, if these activities are executed poorly, this may considerably influence the value of the corresponding cryptocurrency [64] and affect investments.

By analyzing the number of participants who were unsure whether a risk was applicable to their work (*# Unsure*), we can identify which risks were the most challenging for participants to understand. We assume that if interviewees do not fully comprehend the risk description, they cannot accurately determine its applicability to their work. Overall, the number of such risks is low—only four risks have non-zero values in this column: *Routine maintenance and upgrades* (3), *Dynamic interactions* (2), *Miner* (1), and *Oracle* (1). Among these, *Routine maintenance and upgrades* ranks the highest. Two out of three participants, who have not fully comprehended the risk, represent the II group, suggesting that it is particularly unclear to representatives of this stakeholder group.

Analyzing Krippendorff's alpha values, it is also possible to draw interesting conclusions. First, as we can see, the inter-rater agreement values for all stakeholder groups are close to 0. This means that the interviewees, even within the same stakeholder group, perceive different risks in their work. The respondents from the CI group even tend to disagree with each other. That may suggest that this group should be split into several sub-groups with higher agreement. Second, the highest inter-rater agreement is achieved in the II group. Indeed, this group has a long history of analyzing risks and, in general, perceives them likewise. Note that the obtained values cannot be directly compared with reference levels because of the broad area and the subjectivity of each participant's experience.

4.2 Risks Coverage in the MiCA Framework

During our analysis of which risks are addressed in the MiCA framework (see Section 3.4), we identified 7 risks that are *Addressed*, 5 as *Partially Addressed*, and 6 as *Not Addressed* (see Table 6 for details). The MiCA framework has a clear incline toward making the market more stable and protecting consumers and investors by addressing the risks directly connected with market manipulation and market governance: *"Regulation of crypto and DeFi is still quite limited in my opinion. MiCA, from what I understand, tried to address some of the scams in crypto: rug pulls, pump-and-dumps, those type of projects, which is nice, but I believe that's only the surface of it and there is a still a long way to go until we have full regulations"* (Employee, EU-based CASP).

Despite the fact that MiCA seems to be focused on addressing regulatory evasion, several experts during the interviews highlighted that effectiveness of its enforcement mechanisms may not be sufficient due to the borderless nature of decentralized finance, arguing that stronger global coordination is needed to achieve regulatory objectives: *"It's definitely possible to regulate DeFi. The trouble is that this is a global market. If we, in Europe, have a regulation and the service provider in the Bahamas or Fiji or any of those tax havens, then it's a trouble because people can use them anyway.*

Table 6. Risk Coverage

Addressed	Partially Addressed	Not Addressed
1. Market	1. Counterparty	1. Transaction
2. Liquidity	2. Key management	2. Smart contract
3. Governance mechanisms	3. Dynamic interactions	3. Miner
4. Redress of disputes	4. Flash crashes or price cascades	4. Oracle
5. Financial crime	5. Regulation	5. Routine maintenance and upgrades
6. Fraud and market manipulation		6. Forks
7. Regulatory evasion		

But if the compensation scheme is there, if you are fooled as a user and a part of the scam is based out of the Bahamas, you don't get that compensation. This is the reason that regulation should be global. It should be all over the world, absolutely, 100% all over the world" (Employee, EU-based CASP).

Furthermore, regulatory evasion remains a real risk in the post-MiCA world, as even experienced LE struggle with interpreting MiCA definitions, which can also pose an additional risk of unregulated activities that otherwise should be supervised due to the ambiguous nature of their applicability to MiCA: *"It's still very difficult. Especially for the hybrids, it's just very difficult. You'll have clear case, a project, DeFi project or crypto assets, that you can just put in the box and that's it. You're done. But you'll find that a large part of the market is going to be in that gray zone where you're gonna have to discuss and have clarification as to do we fall into this definition?"* (Legal Expert, Non-EU firm). Additionally, in the words of another of another legal expert from an EU-based firm, despite announced outscoping of NFTs, an actual deep dive into different NFT projects invites uncertainty: *"For example NFTs, they might fall under the financial regulation, they might fall under the MiCA regulation or they might not be regulated at all, and sometimes it's hard to distinguish or to assess with 100% confidence that you're in one of the three scenarios, so that's the hardest part of our job."*

In the meantime, the majority of technical risks, such as *Transaction*, *Smart contract*, *Oracle*, and *Miner*, are not addressed in the current version, although their execution may affect the market integrity considerably. We assume that the explanation of this is that MiCA tries to establish a general framework, while concrete use cases, e.g., related to the technical risks, will be covered in accompanying documents, such as the **Digital Operational Resilience Act** (**DORA**).

4.3 Residual Risks

Table 7 presents the results of the qualitative assessment methodology described in Section 3.5, which was used to identify the residual risk levels across all participants. Several key insights can be drawn from this table. First, none of the risks got a low residual risk level (green cell). However, from a rational standpoint, this outcome is anticipated. In practice, there is little justification for mitigating risks within a regulatory framework that stakeholders do not perceive as relevant. Moreover, the regulation is still new and would be improved with the time: *"I think it's the first iteration of the text and with regards to the scope and the obligations, I think most of the industry participants don't consider the text to be perfect, far from it."* (Legal Expert, EU-based company). Second, majority of the risks have medium residual level. Third, there are several risks that stand out by having a high residual risk level that according to our analysis should be prioritized for consideration by the decision-makers in future amendments to the regulation. As presented in Table 7, three risks with the high residual level are: *Transaction*, *Smart contract*, and *Oracle*. Our analysis shows that risks need to be carefully examined and covered in the future MiCA amendments. Let us consider them in details.

Among those, *Smart contract* risk is probably the most important. The "smart contracts" concept is very popular in the crypto world. Although Ethereum is considered the first smart contract platform,

Table 7. Residual Risks for All Participants

All		Risk Coverage		
		Addressed	Partially Addressed	Not Addressed
Risk Relevance	High	1. Market 3. Liquidity 11. Governance mechanisms 12. Redress of disputes 13. Financial crime 14. Fraud and market manipulation 15. Regulatory evasion	2. Counterparty 10. Key management 17. Flash crashes or price cascades 18. Regulation	4. Transaction 5. Smart contract 7. Oracle
	Medium		16. Dynamic interactions	6. Miner 8. Routine maintenance and upgrades 9. Forks
	Low			

almost all blockchains[4] have facilities enabling developers to create and run smart contracts. Even Bitcoin has an embedded interpreter,[5] which allows one to deploy and run rudimentary smart contracts. Considering the widespread adoption of this concept, it might be anticipated that all related risks would receive comprehensive coverage in the regulations, but this is not the case with the MiCA framework.

The legal status of smart contracts mostly remains ambiguous. Consequently, the legal standing of DAOs, governed by smart contracts, also lacks clarity [28] in general:[6] *"It is my understanding that MiCA is really made with centralization in mind and centralized exchanges, issuers of stablecoins, etc., that's the starting point of this framework, and it does not really fit the framework of Decentralized Finance"* (Legal Expert, EU-based firm). Since DAOs are governed by code, there is often no identifiable legal entity (individual or organization) associated with them. This situation presents challenges when it comes to enforcing legal actions [54], even for straightforward matters such as sending a legal notice (as illustrated by the Ooki DAO case [71]) or performing customer or transaction checks: *"If it comes to KYC and AML type of regulations, then there's a long, long way to go for DeFi to implement all of those, because as it currently stands, it's relatively impossible to do. For example, on Ethereum you have UniSwap, and doing KYC on every single wallet and try to find out where the money is coming from, try to find out if this person is a fraud or if he launders money is in my opinion very impossible to do right now with the current structure."* (Employee, CASP). At the same time, DAOs already manage substantial amounts of assets, and in the future, these numbers are expected to grow further. For instance, Uniswap, a Decentralized cryptocurrency EXchange (DEX), currently manages the assets whose total value (*Total Value Locked* or TVL) is about 6 billion USD[7] and, at the peak, it was 10 billion USD. The first amendment to the MiCA framework, introduced after the completion of this research, offers greater clarity regarding the EU's stance on the DAO case (refer to Section 2.1). Its introduction essentially validates the observations done in our study regarding the most important risks.

Also, it is not evident who can regulate smart contracts and how to do this. Recently, the European Parliament has adopted legislation under the Data Act [9] that ensures fair access to and use of industrial data, which in Article 30 lists essential requirements regarding smart contracts for data sharing. According to this act, which is applicable per 2025, companies must arrange the same level of "protection and legal certainty as any other contracts generated through different

[4]Besides primarily designed for payment and asset exchange like Ripple or Stellar.
[5]Smart contracts for Bitcoin is written in a non-Turing-complete language called Script (https://en.bitcoin.it/wiki/Script).
[6]For instance, the state Wyoming, USA, recognizes DAOs as legal entities [89]. Still, on the country level, their status is not defined yet.
[7]https://defillama.com/protocol/uniswap

means," including the aptitude for trade secrets protection, data archiving, and interruption and termination of any transaction (kill-switch functionality [57]). Evidently, the inclusion of the kill-switch requirement appeared to supply legal facilities to suspend the operation of services deemed shady, e.g., Tornado Cash [70]. Although the bill has already been adopted, its implementation raises many tough questions, including technical feasibility, e.g., to the best of our knowledge, the interruption of transactions is not technically possible on modern distributed public blockchain platforms.

Like all software, smart contracts are susceptible to vulnerabilities and bugs, which can lead to errors or incorrect execution. A notable example is the Poly Network hack, which resulted in losses totaling 610 million USD across various cryptocurrencies [5]. Fortunately, the hacker returned all the withdrawn assets, and the users did not incur any damage. Considering the substantial rewards and anonymity inherent to crypto platforms, attacks on smart contracts are becoming more frequent. Consequently, these attacks have inflicted substantial losses on users and undermined investor trust. The legal responsibility for such events, the mechanisms for resolving these issues, and the allocation of responsibility for losses remain unclear. This problem becomes even more complex if the losses are caused by associated parties or smart contracts. For instance, in July 2022, several liquidity providers for the Uniswap DEX were phished out and lost about $7 million [103]. At the time, this amount constituted only approximately 0.15% of the Uniswap **Total Value Locked** (**TVL**), but this led to a 5% decrease in the price of the native UNI token. Bridges are also common targets of these attacks. Three out of ten most profitable attacks belong to this category: BNB[8] (around $586M of losses), Solana's Wormhole[9] (around $326M of losses) and Nomad[10] (about $190M of losses) bridges.

The associated smart contracts, such as oracles, can also cause such losses. Over the past few years, attacks on oracles have gained significant traction, as evidenced by notable incidents [16, 75]. Furthermore, these attacks often yield substantial returns. For instance, in February 2023, an oracle breach enabled attackers to manipulate the price of the AllianceBlock token [16], resulting in the theft of tokens estimated at $120 million. Consequently, it comes as no surprise why *Oracle* risk is in the list of risks with high residual level.

For businesses, including those utilizing blockchain technology, it is imperative that the infrastructure supporting their operations remains consistently functional. When infrastructure providers fail to meet this requirement, they not only lose customers but also incur financial losses. While major public blockchain networks, such as the Ethereum or Bitcoin networks have been maintaining high operational stability without significant disruptions, outages in other blockchain networks still occasionally occur. For instance, in June 2022, Solana experienced a 12% price drop as a result of a platform outage [64]. Hence, it comes as no surprise that the *Transaction* risk, although executed quite rarely, is also among the most critical risks to address.

Table 8 presents the results of the residual risk assessment for each stakeholder group individually. As shown in the table, the risks of the CASP group are the most comprehensively addressed within the MiCA framework. Only one risk, namely, *Routine maintenance and upgrades*, remains at a high residual risk level, while the others are assessed as medium. The criticality of this risk to the CASP group is unsurprising, as blockchain functionality is fundamental to their operations—without an operational blockchain, CASPs are unable to provide their services.

Two groups, namely, LE and II, have two risks with high residual risk level. For LE, these are *Transaction* and *Smart contract*. Both these risks stem from highly technical aspects of blockchain

[8] https://rekt.news/bnb-bridge-rekt/
[9] https://rekt.news/wormhole-rekt/
[10] https://rekt.news/nomad-rekt/

Table 8. Residual Risks for Individual Stakeholder Groups

CASP		Risk Coverage		
		Addressed	**Partially Addressed**	**Not Addressed**
Risk Relevance	**High**	1. Market 3. Liquidity 12. Redress of disputes 14. Fraud and market manipulation 15. Regulatory evasion	10. Key management 16. Dynamic interactions 17. Flash crashes or price cascades 18. Regulation	8. Routine maintenance and upgrades
	Medium	11. Governance mechanisms 13. Financial crime	2. Counterparty	4. Transaction 5. Smart contract 6. Miner 7. Oracle 9. Forks
	Low			

CI		Risk Coverage		
		Addressed	**Partially Addressed**	**Not Addressed**
Risk Relevance	**High**	11. Governance mechanisms 12. Redress of disputes	10. Key management 17. Flash crashes or price cascades 18. Regulation	4. Transaction 5. Smart contract 7. Oracle 8. Routine maintenance and upgrades 9. Forks
	Medium	1. Market 3. Liquidity 13. Financial crime 14. Fraud and market manipulation 15. Regulatory evasion	16. Dynamic interactions	6. Miner
	Low		2. Counterparty	

II		Risk Coverage		
		Addressed	**Partially Addressed**	**Not Addressed**
Risk Relevance	**High**	3. Liquidity 13. Financial crime 14. Fraud and market manipulation 15. Regulatory evasion	10. Key management 18. Regulation	5. Smart contract 7. Oracle
	Medium	1. Market 11. Governance mechanisms 12. Redress of disputes	2. Counterparty 17. Flash crashes or price cascades	4. Transaction 6. Miner
	Low		16. Dynamic interactions	9. Forks

LE		Risk Coverage		
		Addressed	**Partially Addressed**	**Not Addressed**
Risk Relevance	**High**	1. Market 3. Liquidity 11. Governance mechanisms 13. Financial crime 14. Fraud and market manipulation 15. Regulatory evasion	2. Counterparty 10. Key management 17. Flash crashes or price cascades	4. Transaction 5. Smart contract
	Medium	12. Redress of disputes	16. Dynamic interactions 18. Regulation	6. Miner 7. Oracle 8. Routine maintenance and upgrades 9. Forks
	Low			

systems. Thus, LE may perceive them as particularly challenging to address through regulatory mechanisms due to their dynamic and evolving nature. Indeed, failures in blockchain networks (e.g., double-spending, expensive transactions, or throughput issues) directly affect trust, a cornerstone for financial and legal systems. Such issues can create disputes regarding liability and compliance, increasing the legal burden. Vulnerabilities in smart contracts (e.g., bugs, malicious exploits, or unintentional misexecutions) can lead to irreversible losses or unintended outcomes. Resolving these issues may involve complicated legal processes, especially since smart contracts often operate autonomously and lack standardized safeguards.

For the II group, the risks with high residual levels are *Smart contract* and *Oracle*. II typically handle large volumes of capital, making them particularly vulnerable to issues in smart contracts and oracles. Indeed, programming errors, vulnerabilities, or misexecutions in smart contracts could result in substantial financial losses, so as smart contracts often automate transactions with high cumulative value with the limited possibility of human intervention during and after their execution. II often rely on external data (e.g., asset prices, interest rates) for decision-making and automated trades, therefore, compromised or inaccurate oracle data can directly lead to financial miscalculations or losses.

At the same time, the CI group stands out—5 risks, namely, *Transaction*, *Smart contract*, *Oracle*, *Routine maintenance and upgrades*, and *Forks*, have a high residual risk level. During our interviews with the CI experts, we frequently observed them as advocates of algocracy, favoring "code over talks" while approaching traditional regulatory mechanisms with skepticism [83]. Moreover, over the last decade, a limited amount of crypto-regulation documents existed, but this has not prevented the industry's rapid development. Therefore, the CI group may simply not recognize the importance of being involved in developing traditional regulations. That does not necessarily mean, however, that they do not want to collaborate or be consulted with in regulatory processes: *"There may be a possibility that the regulators may take a certain decision, but they may not be aware of all the intricacies and the challenges these systems post. So the primary stakeholders would be the users and the builders, and they should definitely have a say"* (Employee, Non-EU-based CI Firm). Additionally, an interviewee who was an ex-employee of an EU-based firm believed that technical knowledge possessed by the blockchain market players was key to effective regulation: *"As long as financial bodies have a better grasp of what is happening on blockchain networks, if they have a better idea of what tools to use to analyze transaction data, and if they work a little bit more with the people that create it, I think there is a much higher chance for them to weed out financial crime."* Nevertheless, their concerns are less reflected in the current version of the MiCA framework. The MiCA initiative webpage [35] provides some details on how the framework was discussed. Although it does not report all the details about the respondents, it supports our observation. For instance, after the analysis of the public consultation document results [35], we found out that only 3 out of 197 respondents identified themselves as belonging to the CI group. Our results also show that this group's opinions are highly underrepresented. Thus, our analysis suggests adding more experts from this group to future stakeholder consultations.

5 Discussions and Limitations

In this work, we have independently evaluated whether, what, and whose risks associated with the new crypto-asset market are covered in the MiCA framework. One of the objectives of this framework is to define clearly "the regulatory treatment of all cryptoassets that are not covered by existing financial services legislation" [36]. In this work, we show that there is still room for improvement in achieving this objective because risks specific to crypto-asset market and deemed important by the stakeholders, such as smart contract, oracle, and transaction, are not covered yet.

The obtained findings depend on the results of the expert interviewees and the assessment of the risk coverage in the MiCA framework. While we put significant effort into finding and interviewing 20 experts, it is always possible to increase the representativeness of the results by recruiting more participants.

We utilized the May 2022 version of the MiCA proposal for our study, the latest available during the start of our research. A review of the later versions reveals minimal impact on the relevance of our results. It retains the existing risk coverage and does not introduce new risks. Notably, some amendments indirectly validate our findings, such as the clarification of the EU's stance on the DAO case in the first amendment A09-0052/1 [94]. It is worth mentioning that Article 140 in the latest version [56] outlines future research directions. According to it, the EC will have to report to the EP and the Council within 48 months after MiCA's implementation on various topics, including a more in-depth investigation of the DeFi space where no identifiable CI or service providers can be found, a description of the classification of crypto-assets, and an assessment of the need for a novel white paper approval mechanism for crypto-assets falling outside the scope of asset-referenced and e-money tokens. Additionally, the EC will examine fraudulent activities, hacks, and the connections between crypto-assets and ransomware and cyberattacks. Consequently, we anticipate that some of the technical risks currently absent in MiCA may be addressed in forthcoming regulations once the research and reporting phases are completed.

Moreover, we acknowledge that the WEF framework [31] used in this study may be unexhaustive in its coverage of crypto-assets and services risks. For example, we incorporated an additional risk that the WEF list did not encompass, "regulation risk", as it is critical for understanding its perception by the participants, given the regulatory focus of this work. This inclusion was essential to gauge the participants' perceptions, aligning with the regulatory focus of our research. Moreover, some risks could be difficult for some participants to perceive. The rows with the non-zero number of unsure interviewees in Table 5 implicitly indicate those risks. Nevertheless, this article predominantly relied on the WEF list due to its comprehensive nature, addressing the concerns of all stakeholders in the crypto market, as opposed to the narrower focus often found in existing studies on risks associated with crypto-assets and services.

While we acknowledge that the coverage of every risk of each stakeholder group may be outside the scope, the MiCA framework is positioned as a part of the comprehensive regulations, and, thus, it should address concerns as much as possible: "This proposal is part of the Digital Finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks" [36]. Our work may help improve the regulation further by suggesting what risks should first be mitigated.

6 Related Work

Among the most significant challenges for blockchain, and hence DeFi adoption, is security [25, 39] and government regulation [81]. Before MiCA, there have been numerous studies explaining the urgent need for blockchain regulations [30], mostly to facilitate adoption in tightly regulated industries, such as banking [69]. ING Bank, in its 2022 white paper on DeFi [68], discusses the need for regulation and favorable policy that is likely to accelerate adoption among financial institutions, specifically legislation clarifying liability in case of a faulty DeFi protocol. A 2021 paper [88] called for regulator action, stating that while illicit activity permitted by the pseudonymity of blockchain-based systems has caused concerns among regulators, they should find reasonable solutions for a careful risk-based approach that does not pose barriers to innovation. Similarly, other recent studies that delved into the topic have called for regulatory attention not only on blockchain aspects related to regulatory risk, but also those related to technical risks [18, 19].

Some academics expressed criticism towards regulators' reactive policies, inability to properly understand blockchain technology and implement a proactive policy-making approach [3]. As a result, DeFi industry stakeholders faced long legal uncertainties when considering the adoption of blockchain for financial applications [46].

Recent literature offers numerous studies that have provided an analysis or commentary on the MiCA regulation from different perspectives. Some published a more general analysis of the regulation [8], but most focused on more specific topics, such as potential challenges in implementing regulations and balancing them with evolving markets [104], categorization of various types of services and importance of definitions [53], crypto-asset subcategories [97], disclosure requirements for smaller entities and regulatory burdens [42]. Others have provided a more scoped analysis, such as the impact on **Initial Coin Offerings (ICOs)** [74], impact on legal certainty and adoption [99], effect on illicit transactions [11], and global harmonization [20]. Additionally, researchers have explored the challenges related to regulation of stablecoins under MiCA [49], licensing requirements [7], and analysis of investor protection under MiCA [60].

The negative aspects of MiCA have emerged as a significant theme in related research. For instance, the EC carried out its own framework impact assessment [37]. The analysis claimed that more mature cryptocurrency issuers may face costs of up to $87K USD to comply with white-paper requirements and up to $28M in one-off compliance costs. To add, a study of the EU regulations of crypto-assets and services showed that MiCA may pose significant strains on the novel blockchain ecosystem by applying strong prescriptive policies compared to more general approaches [43].

There are several publications analyzing perspectives of various stakeholders on MiCA regulation. The 2021 report by the MiCA Taskforce of the **International Association for Trusted Blockchain Applications (INATBA)** provides insights from survey and stakeholder engagement sessions which revealed the market's excitement for regulatory clarity, but also its concerns about stifled innovation and proportionality [92]. Another study adopting a legal-sociological approach that examined materials to assess the views of market stakeholders has found that while institutional stakeholders agreed that MiCA would benefit consumer trust, FinTech companies expressed proportionality concerns due to burdening compliance costs [99].

The perspectives of market stakeholders on blockchain regulation have been explored in the literature outside MiCA as well. For example, [83] explored the views of developers, regulators, investors, and end-users on the benefits and challenges of regulatory initiatives, concluding that while financial regulators and government decision makers see regulatory challenges in financial markets, developers are more interested in security, operational resilience, and risk management. The conflicting areas of interests and priorities highlight the stark need for a multi-stakeholder regulatory approach and representation of all stakeholder views. Ellul et al. [34] explored the need for regulatory frameworks beyond the financial aspects and presented a technology regulatory framework. The authors argue that technology flaws can lead to large financial losses and call for technology assurance processes for critical and high-risk applications.

7 Conclusion

The MiCA framework, initially drafted in 2020 and entered into full force on December 30, 2024, represents the EC's pioneering effort to establish regulatory guidelines for the crypto industry. Given its cross-border regulatory scope, the innovative nature of the sector, and its potentially significant impact on stakeholders, it is clear why the framework gained substantial attention both from academia and industry.

In this work, we contribute to the analysis of the framework by offering a novel perspective on which stakeholder groups' opinions are underrepresented and what risks should be prioritized in future amendments. To construct this perspective, we conducted interviews with 20 experts

representing diverse stakeholder groups and conducted a thorough examination of the MiCA framework to determine what risks it currently covers. Our findings reveal that the opinions of CI are the least addressed, that is indicated by the number of their high-level risks in the current framework version. Moreover, our analysis highlights the need to prioritize smart contract, oracle, and transaction risks for consideration in future framework amendments. These findings affirm that the current framework requires refinement and highlight specific areas for improvement, which, as suggested by relevant studies, should be addressed through an iterative development process.

References

[1] [n. d.]. Uniswap Protocol. Retrieved from https://uniswap.org. Accessed: 2023-05-24.

[2] [n. d.]. World Economic Forum. Retrieved from https://www.weforum.org/. Accessed: 2023-05-24.

[3] Omar Ali, Mustafa Ally, Peter Clutterbuck, and Yogesh Dwivedi. 2020. The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management* 54 (2020), 102199. DOI: https://doi.org/10.1016/j.ijinfomgt.2020.102199

[4] Alyssa Hertig (CoinDesk). 2017. Loveable Digital Kittens Are Clogging Ethereum's Blockchain. Retrieved from https://www.coindesk.com/markets/2017/12/04/loveable-digital-kittens-are-clogging-ethereums-blockchain/. Accessed: 2023-05-24.

[5] Alyssa Hertig (CoinDesk). 2021. Cross-Chain DeFi Site Poly Network Hacked; Hundreds of Millions Potentially Lost. Retrieved from https://www.coindesk.com/markets/2021/08/10/cross-chain-defi-site-poly-network-hacked-hundreds-of-millions-potentially-lost/. Accessed: 2023-05-24.

[6] Amrita Khalid (Engadget). 2022. 'Axie Infinity' is back open for business following $625 million hack. Retrieved from https://www.engadget.com/axie-infinity-nft-game-restarts-ronin-blockchain-213023936.html. Accessed: 2023-05-24.

[7] Filippo Annunziata. 2023. The licensing rules in MiCA. *Fintech Regulation and the Licensing Principle, Edited by Dário Moura Vicente Diogo Pereira Duarte Catarina Granadeiro, Centro de Investigaçao de direito privado, European Banking Institute, Frankfurt* (2023). Available at SSRN: https://ssrn.com/abstract=4346795

[8] Filippo Annunziata. 2023. An overview of the markets in crypto-assets regulation (MiCAR). *European Banking Institute Working Paper Series no. 158.* Available at SSRN: https://ssrn.com/abstract=4660379 or http://dx.doi.org/10.2139/ssrn.4660379

[9] Assad Jafri (CryptoSlate). 2023. EU passes Data Act including smart contract regulation. Retrieved from https://cryptoslate.com/eu-passes-data-act-including-smart-contract-regulation/. Accessed: 2023-05-24.

[10] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, and A. Sarwar. 2020. Blockchain attacks analysis and a model to solve double spending attack. *International Journal of Machine Learning and Computing* 10, 2 (2020), 352–357.

[11] Vladlena Benson, Bogdan Adamyk, Anitha Chinnaswamy, and Oksana Adamyk. 2024. Harmonising cryptocurrency regulation in europe: Opportunities for preventing illicit transactions. *European Journal of Law and Economics* 57, 1 (2024), 37–61.

[12] Nicola Bilotta and Fabrizio Botti. 2018. *Libra and the Others: The Future of Digital Money.* Technical Report. Istituto Affari Internazionali (IAI). Retrievedfromhttp://www.jstor.org/stable/resrep19691

[13] Marek Bočánek. 2021. First draft of crypto-asset regulation (MiCA) with the european union and potential implementation. *Financial Law Review* 22, 2 (2021), 37–53.

[14] Yazan Boshmaf, Charitha Elvitigala, Husam Al Jawaheri, Primal Wijesekera, and Mashael Al Sabah. 2020. Investigating MMM ponzi scheme on bitcoin. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20).* 519–530. DOI: https://doi.org/10.1145/3320269.3384719

[15] Brady Dale (CoinDesk). 2020. Mempool Manipulation Enabled Theft of $8M in MakerDAO Collateral on Black Thursday: Report. Retrieved from https://www.coindesk.com/tech/2020/07/22/mempool-manipulation-enabled-theft-of-8m-in-makerdao-collateral-on-black-thursday-report/. Accessed: 2023-05-24.

[16] Brayden Lindrea (CoinTelegraph). 2023. BonqDAO protocol suffers $120M loss after oracle hack). Retrieved from https://cointelegraph.com/news/bonqdao-protocol-suffers-120m-loss-after-oracle-hack. Accessed: 2023-05-24.

[17] Marco Cappai. 2023. The role of private and public regulation in the case study of crypto-assets: The italian move towards participatory regulation. *Computer Law and Security Review* 49 (2023), 105831. DOI: https://doi.org/10.1016/j.clsr.2023.105831

[18] Agostino Capponi, Garud Iyengar, and Jay Sethuraman. 2023. Decentralized finance: Protocols, risks, and governance. *Foundations and Trends® in Privacy and Security* 5, 3 (2023), 144–188. Available at SSRN: https://ssrn.com/abstract=4651020 or http://dx.doi.org/10.2139/ssrn.4651020

[19] Francesca Carapella, Edward Dumas, Jacob Gerszten, Nathan Swem, and Larry D. Wall. 2022. Decentralized finance (DeFi): Transformative potential and associated risks (October 02, 2022). FRB Atlanta Policy Hub Paper No. 2022-14, https://doi.org/10.29338/ph2022-14. Available at SSRN: https://ssrn.com/abstract=5191051 or http://dx.doi.org/10.2139/ssrn.5191051

[20] Cristina Carata and William J Knottenbelt. 2024. Towards a harmonized global regulation: An analysis of the MiCA regulation and its implications for the european crypto-asset market. In *Proceedings of the 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 288–289.

[21] Santiago Castro. 2017. Fast Krippendorff: Fast computation of Krippendorff's alpha agreement measure. Retrieved October 13, 2024 from https://github.com/pln-fing-udelar/fast-krippendorff

[22] Atanu Chaudhuri, Manjot Singh Bhatia, Yasanur Kayikci, Kiran J. Fernandes, and Samuel Fosso-Wamba. 2023. Improving social sustainability and reducing supply chain risks through blockchain implementation: Role of outcome and behavioural mechanisms. *Ann Oper Res* 327 (2023). 401–433. https://doi.org/10.1007/s10479-021-04307-6

[23] Monica Chin. 2020. Telegram shuts down its cryptocurrency operation. Retrieved from https://www.theverge.com/2020/5/12/21256407/telegram-cryptocurrency-shutdown-sec-gram. Accessed: 2023-05-24.

[24] Shahan Ahmed Chowdhury. 2024. GitHub spam is getting out of hand! Retrieved from https://dev.to/codewithshahan/github-spam-is-getting-out-of-hand-1cai. Accessed: 2024-10-11.

[25] Mauro Conti, E. Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys and Tutorials* 20, 4 (2018), 3416–3452. DOI: https://doi.org/10.1109/COMST.2018.2842460

[26] Daniel Phillips (Decrypt). 2021. How many Bitcoin does its inventor Satoshi Nakamoto still own? Retrieved from https://decrypt.co/34810/how-many-bitcoin-does-its-inventor-satoshi-nakamoto-still-own. Accessed: 2023-05-24.

[27] Stanislav Dashevskyi, Yury Zhauniarovich, Olga Gadyatskaya, Aleksandr Pilgun, and Hamza Ouhssain. 2020. Dissecting android cryptocurrency miners. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY'20)*. DOI: https://doi.org/10.1145/3374664.3375724

[28] David Kappos, Evan Norris, Daniel Barabander (CoinDesk). 2022. More than Just the Ooki DAO: Lessons for Web3 Companies About Control After bZx Retrieved from https://www.coindesk.com/layer2/2022/10/31/more-than-just-the-ooki-dao-lessons-for-web3-companies-about-control-after-bzx/. Accessed: 2023-05-24.

[29] David Siegel (CoinDesk). 2023. Understanding The DAO Attack. Retrieved from https://www.coindesk.com/learn/understanding-the-dao-attack/. Accessed: 2023-05-24.

[30] Primavera De Filippi. 2014. Bitcoin: A regulatory nightmare to a libertarian dream. *Internet Policy Review* 3, 2 (2014).

[31] Deshmukh, Sumedha and Warren, Sheila and Werbach, Kevin (World Economic Forum). 2021. Decentralized Finance (DeFi) Policy-Maker Toolkit. Retrieved from http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf. Accessed: 2023-05-24.

[32] Doug Alexander (Bloomberg). February, 2019. Crypto CEO Dies Holding Only Passwords That Can Unlock Millions in Customer Coins. Retrieved from https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem. Accessed: 2023-05-24.

[33] Alexander Egberts. 2017. *The oracle problem-an analysis of how blockchain oracles undermine the advantages of decentralized ledger systems*. Master's thesis. EBS Business School.

[34] Joshua Ellul, Jonathan Galea, Max Ganado, Stephen Mccarthy, and Gordon J Pace. 2020. Regulating blockchain, DLT and smart contracts: A technology regulator's perspective. In *Proceedings of the Era Forum*. Springer, 209–220.

[35] European Commission. [n. d.]. EU regulatory framework for crypto-assets. Retrieved from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12089-Financial-services-EU-regulatory-framework-for-crypto-assets_en. Accessed: 2023-05-24.

[36] European Commission. 2020. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF. Accessed: 2023-05-24.

[37] European Commission. 2020. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0380&from=EN. Accessed: 2023-05-24.

[38] European Securities and Market Authority. [n. d.]. MIFID II. Retrieved from https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir. Accessed: 2023-05-24.

[39] Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, 436–454.

[40] Ezra Reguerra (Cointelegraph). 2022. MEV bot earns $1M but loses everything to a hacker an hour later. Retrieved from https://cointelegraph.com/news/mev-bot-earns-1m-but-loses-everything-to-a-hacker-an-hour-later. Accessed: 2023-05-24.

[41] Dean Fantazzini and Stephan Zimin. 2020. A multivariate approach for the simultaneous modelling of market risk and credit risk for cryptocurrencies. *Journal of Industrial and Business Economics* 47, 1 (2020), 19–69.
[42] Guido Ferrarini and Paolo Giudici. 2021. Digital offerings and mandatory disclosure: A market-based critique of MiCA. *European Corporate Governance Institute-Law Working Paper* 605 (2021). Available at SSRN: https://ssrn.com/abstract=3914768 or http://dx.doi.org/10.2139/ssrn.3914768
[43] Agata Ferreira and Philipp Sandner. 2021. Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law and Security Review* 43 (2021), 105632.
[44] Garimidi, Pranav and Kominers, Scott Duke and Roughgarden, Tim (a16zcrypto). 2022. DAO governance attacks, and how to avoid them. Retrieved from https://a16zcrypto.com/content/article/dao-governance-attacks-and-how-to-avoid-them/. Accessed: 2023-05-24.
[45] Jonas Groß, Bernhard Herz, and Jonathan Schiller. 2019. *Libra - Concept and Policy Implications*. Wirtschaftswissenschaftliche Diskussionspapiere 02-19. Universität Bayreuth. Retrieved from http://hdl.handle.net/10419/205241
[46] Andres Guadamuz and Christopher Marsden. 2015. Blockchains and bitcoin: Regulatory responses to cryptocurrencies. *First Monday* 20, 12-7 (2015).
[47] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field Methods* 18, 1 (2006), 59–82.
[48] Ashley K Hagaman and Amber Wutich. 2017. How many interviews are enough to identify metathemes in multisited and cross-cultural research? Another perspective on guest, bunce, and johnson's (2006) landmark study. *Field Methods* 29, 1 (2017), 23–41.
[49] Patrick Hansen and Helmut Bauer. 2024. MiCA's significance regime for stablecoins-a sledgehammer to crack a nut? Available at SSRN: https://ssrn.com/abstract=4699043
[50] Philipp Hartmann. 2010. Interaction of market and credit risk. *Journal of Banking and Finance* 34, 4 (2010), 697–702.
[51] Friedrich A. von (Friedrich August) Hayek. 1990. *Denationalisation of Money: The Argument Refined* (3rd ed.). Institute of Economic Affairs.
[52] Monique Hennink and Bonnie N. Kaiser. 2022. Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science and Medicine* 292 (2022), 114523. DOI: https://doi.org/10.1016/j.socscimed.2021.114523
[53] Martin Hobza. 2021. Crypto-asset services under the draft MiCA regulation. In *Proceedings of the Challenges of Law in Business and Finance*. Societatea de Stiinte Juridice si Administrative, 13–21.
[54] Alex Richardson (The Daily Hodl). 2023. Judge Overseeing SEC's Coinbase Lawsuit Dismisses Class Action Against Uniswap. Retrieved from https://dailyhodl.com/2023/08/30/judge-overseeing-secs-coinbase-lawsuit-dismisses-class-action-against-uniswap/. Accessed: 2023-09-07.
[55] Hsiu-Fang Hsieh and Sarah E. Shannon. 2005. Three approaches to qualitative content analysis. *Qualitative Health Research* 15, 9 (2005), 1277–1288.
[56] Irene Tinagli (European Commission). 2023. Amendment A9-0052/002-002 for the Markets in Crypto-assets (MiCA) proposal. Retrieved from https://www.europarl.europa.eu/doceo/document/A-9-2022-0052-AM-002-002_EN.pdf. Accessed: 2023-05-26.
[57] Jack Schickler (CoinDesk). 2023. EU Parliament Passes Bill Requiring Smart Contracts to Include Kill Switch. Retrieved from https://www.coindesk.com/policy/2023/03/14/eu-parliament-passes-bill-requiring-smart-contracts-to-include-kill-switch/. Accessed: 2023-05-24.
[58] Kelly Ng (BBC News). 2023. Crypto theft: North Korea-linked hackers stole $1.7b in 2022. Retrieved from https://www.bbc.com/news/world-asia-64494094. Accessed: 2023-05-24.
[59] Kevin Helms (Bitcoin.com News). 2024. FBI Creates Crypto Token to Expose Fraud — Seizes $25M in Cryptocurrency, Charges 18. Retrieved from https://news.bitcoin.com/fbi-creates-crypto-token-to-expose-fraud-seizes-25m-in-cryptocurrency-charges-18/. Accessed: 2024-10-11.
[60] Ilya Kokorin. 2023. The anatomy of crypto failures and investor protection under MiCAR. *Capital Markets Law Journal* 18, 4 (2023), 500–525.
[61] Klaus Krippendorff. 2019. *Content Analysis: An Introduction to Its Methodology*. Sage Publications. DOI: https://doi.org/10.4135/9781071878781
[62] Libra Association. 2019. An Introduction to Libra: White Paper. Retrieved from https://sls.gmu.edu/pfrt/wp-content/uploads/sites/54/2020/02/LibraWhitePaper_en_US-Rev0723.pdf. Accessed: 2023-05-24.
[63] Ji Liu, Zheng Xu, Yanmei Zhang, Wei Dai, Hao Wu, and Shiping Chen. 2022. Digging into primary financial market: The issues of primary financial market issuance and investigations from the perspective of blockchain. *Frontiers in Blockchain* 5 (2022). Frontiers Media SA. DOI: 10.3389/fbloc.2022.908912
[64] MacKenzie Sigalos (CNBC). 2022. Solana suffered its second outage in a month, sending price plunging. Retrieved from https://www.cnbc.com/2022/06/01/solana-suffered-its-second-outage-in-a-month-sending-price-plunging.html. Accessed: 2023-05-24.

[65] Marie Huillet (Cointelegraph). 2019. Walmart Is Trying to Patent Its Own 'Libra' Like Digital Currency. Retrieved from https://cointelegraph.com/news/walmart-is-trying-to-patent-its-own-libra-like-digital-currency. Accessed: 2023-05-24.
[66] Edoardo D. Martino. 2024. Monetary sovereignty in the digital era. The law and macroeconomics of digital private money. *Computer Law and Security Review* 52 (2024), 105909. DOI: https://doi.org/10.1016/j.clsr.2023.105909
[67] Matthew Elmas (SmartCompany). 2020. Musk, Bezos, Gates and Buffet accounts hacked in Twitter Bitcoin scam. Retrieved from https://www.smartcompany.com.au/industries/information-technology/twitter-hack-obama/. Accessed: 2024-10-11.
[68] Meegan, X and Koens, T (ING). 2021. Lessons Learned from Decentralised Finance (DeFi). Retrieved from https://www.ingwb.com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi_white_paper_v2.0.pdf. Accessed: 2023-05-24.
[69] Quoc Khanh Nguyen. 2016. Blockchain-a financial technology for future sustainable development. In *International Conference on Green Technology and Sustainable Development*. IEEE, 51–54.
[70] Nikhilesh De (CoinDesk). 2022. Crypto-Mixing Service Tornado Cash Blacklisted by US Treasury. Retrieved from https://www.coindesk.com/policy/2022/08/08/crypto-mixing-service-tornado-cash-blacklisted-by-us-treasury/. Accessed: 2023-05-24.
[71] Nikhilesh De (CoinDesk). 2023. CFTC Calls for Default Judgment Against Ooki DAO in Ongoing Lawsuit. Retrieved from https://www.coindesk.com/policy/2023/01/12/cftc-calls-for-default-judgement-against-ooki-dao-in-ongoing-lawsuit/. Accessed: 2023-05-24.
[72] Marko S. Novakovic. 2021. The reform of the crypto licenses system in estonia and the regulation on markets in crypto assets proposal. *Strani Pravni Zivot* 2021, 4 (2021), 687.
[73] Oliver Knight (CoinDesk). 2022. Ethereum Lending Protocol XCarnival Hit With $3.8M Exploit, Recovers 50%. Retrieved from https://www.coindesk.com/business/2022/06/27/ethereum-lending-protocol-xcarnival-hit-with-38m-exploit-recovers-50/. Accessed: 2023-05-24.
[74] Francesco Paolo Patti. 2024. The european MICA regulation: A new era for initial coin offerings. *Georgetown Journal of International Law, Forthcoming, Bocconi Legal Studies Research Paper* 4810910 (2024).
[75] Peckshield. 2020. bZx Hack II Full Disclosure (With Detailed Profit Analysis). Retrieved from https://peckshield.medium.com/bzx-hack-ii-full-disclosure-with-detailed-profit-analysis-8126eecc1360. Accessed: 2023-05-24.
[76] Prashant Jha (CoinDesk). 2022. 30% crypto tax becomes law in India following Finance Bill approval. Retrieved from https://cointelegraph.com/news/30-crypto-tax-becomes-law-in-india-following-finance-bill-approval. Accessed: 2023-05-24.
[77] Arief Prabawa Putra and Benfano Soewito. 2023. Integrated methodology for information security risk management using ISO 27005: 2018 and NIST SP 800-30 for insurance sector. *International Journal of Advanced Computer Science and Applications* 14, 4 (2023).
[78] Lener Raffaele. 2022. Cryptocurrencies and crypto-assets in the italian and EU perspective. *Vestnik of Saint Petersburg University. Law* 13, 1 (2022), 219–229.
[79] Sara Rahimi and Marzieh Khatooni. 2024. Saturation in qualitative research: An evolutionary concept analysis. *International Journal of Nursing Studies Advances* 6 (2024), 100174. DOI: https://doi.org/10.1016/j.ijnsa.2024.100174
[80] Atle Refsdal, Bjørnar Solhaug, Ketil Stølen, Atle Refsdal, Bjørnar Solhaug, and Ketil Stølen. 2015. *Cyber-risk Management*. Springer.
[81] Fergal Reid and Martin Harrigan. 2013. An analysis of anonymity in the bitcoin system. In *Proceedings of the Security and Privacy in Social Networks*. Springer, 197–223.
[82] Rita Liao (TechCrunch). 2023. Crypto-friendly bank Silvergate to wind down after FTX blow-up. Retrieved from https://techcrunch.com/2023/03/08/crypto-friendly-bank-silvergate-to-wind-down-after-ftx-blow-up/. Accessed: 2023-05-24.
[83] Manuel Pedro Rodríguez Bolívar, Hans Jochen Scholl, and Roman Pomeshchikov. 2021. Stakeholders' perspectives on benefits and challenges in blockchain regulatory frameworks. In *Blockchain and the Public Sector. Public Administration and Information Technology*, C. G. Reddick, M. P. Rodríguez-Bolívar, and H. J. Scholl (Eds.). Vol 36. Springer, Cham. https://doi.org/10.1007/978-3-030-55746-1_1
[84] Joint Task Force Transformation Initiative. 2012. Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[85] Mikkaela Salamatin. 2021. Balancing innovation and protection: Understanding the landscape for DeFi regulation. Available at SSRN: https://ssrn.com/abstract=3918656 or http://dx.doi.org/10.2139/ssrn.3918656
[86] Savannah Fortis (CoinTelegraph). 2024. Coinbase to delist noncompliant stablecoins under EU MiCA rules. Retrieved from https://cointelegraph.com/news/coinbase-delist-non-compliant-stablecoins-mica. Accessed: 2024-10-11.
[87] Alexander Savelyev. 2017. Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information and Communications Technology Law* 26, 2 (2017), 116–134. DOI: https://doi.org/10.1080/13600834.2017.1301036

[88] Fabian Schär. 2021. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review* (2021). Available at SSRN: https://ssrn.com/abstract=3843844 or http://dx.doi.org/10.20955/r.103.153-74
[89] Sean Dickens (Yahoo!Finance). 2021. Wyoming becomes first US state to legally recognise DAO. Retrieved from https://www.cnbc.com/2022/06/01/solana-suffered-its-second-outage-in-a-month-sending-price-plunging.html. Accessed: 2023-05-24.
[90] Shevchenko, Andrey (Cointelegraph). 2020. Researcher suggests miners are manipulating Ethereum blocks to exploit DeFi. Retrieved from https://cointelegraph.com/news/researcher-suggests-miners-are-manipulating-ethereum-blocks-to-exploit-defi. Accessed: 2023-05-24.
[91] Sidhartha Shukla (Bloomberg). 2022. DeFi Project Beanstalk Loses $182 Million in Flash Loan Attack. Retrieved from https://www.bloomberg.com/news/articles/2022-04-18/defi-project-beanstalk-loses-182-million-in-flash-loan-attack. Accessed: 2023-05-24.
[92] Ivona Skultetyova, Luz Parrondo-Tort, Konstantinos Stylianou, Filippo Zatti, Josina Rodrigues, et al. 2021. Blockchain Ecosystem's Response to MiCA Regulation Proposal. Retrieved from https://flore.unifi.it/retrieve/e398c381-0c11-179a-e053-3705fe0a4cff/2021-02-Blockchain-Ecosystems-Response-to-MiCA-Regulation-Proposal-Final.pdf. Accessed: 2024-11-27.
[93] Solana. [n. d.]. Solana | Web3 Infrastructure for Everyone. Retrieved from https://solana.com. Accessed: 2023-05-24.
[94] Stefan Berger (European Commission). 2023. Amendment A9-0052/001-001 for the Markets in Crypto-assets (MiCA) proposal. Retrieved from https://www.europarl.europa.eu/doceo/document/A-9-2022-0052-AM-001-001_EN.pdf. Accessed: 2023-05-26.
[95] The Defiant. 2020. SushiSwap's Vampire Scheme: Hours Away and With $1.3B at Stake. Retrieved from https://thedefiant.io/sushiswaps-vampire-scheme-hours-away-and-with-1-3b-at-stake. Accessed: 2023-05-24.
[96] The United States Department of Justice. 2022. BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme. Retrieved from https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme. Accessed: 2023-05-24.
[97] Tomasz Tomczak. 2022. Crypto-assets and crypto-assets' subcategories under MiCA regulation. *Capital Markets Law Journal* 17, 3 (2022), 365–382.
[98] Arianna Trozze, Josh Kamps, Eray Arda Akartuna, Florian J. Hetzel, Bennett Kleinberg, Toby Davies, and Shane D. Johnson. 2022. Cryptocurrencies and future financial crime. *Crime Science* 11, 1 (2022), 1–35.
[99] Tina van der Linden and Tina Shirazi. 2023. Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation* 9, 1 (2023), 22.
[100] Rolf van Wegberg, Jan-Jaap Oerlemans, and Oskar van Deventer. 2018. Bitcoin money laundering: Mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime* 25, 2 (2018), 419–435.
[101] Emanuel Wanat. 2021. Are crypto-assets green enough?–An analysis of draft EU regulation on markets in crypto assets from the perspective of the european green deal. *OER Osteuropa Recht* 67, 2 (2021), 237–250.
[102] William Foxley (CoinDesk). 2020. Harvest Finance: $24M Attack Triggers $570M 'Bank Run' in Latest DeFi Exploit. Retrieved from https://www.coindesk.com/tech/2020/10/26/harvest-finance-24m-attack-triggers-570m-bank-run-in-latest-defi-exploit/. Accessed: 2023-05-24.
[103] Yusoff Kim (Yahoo!Finance). 2022. Uniswap Users Were Hacked For $7 Million - Who's Next? Retrieved from https://chaindebrief.com/uniswap-users-hacked-for-7-million/. Accessed: 2023-05-24.
[104] Dirk A. Zetzsche, Filippo Annunziata, Douglas W. Arner, and Ross P. Buckley. 2021. The markets in crypto-assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal* 16, 2 (2021), 203–225.
[105] Dirk A. Zetzsche, Ross P. Buckley, and Douglas W. Arner. 2021. Regulating libra. *Oxford Journal of Legal Studies* 41, 1 (2021), 80–113.
[106] Yuanyuan Zhang, Stephen Chan, Jeffrey Chu, and Hana Sulieman. 2020. On the market efficiency and liquidity of high-frequency cryptocurrencies in a bull and bear market. *Journal of Risk and Financial Management* 13, 1 (2020), 8.

Received 5 May 2024; revised 29 August 2025; accepted 25 November 2025