Raising the Bar: Assessing Historical Cryptocurrency Exchange Practices in Light of the EU's MiCA and DORA Regulation

Marilyne Ordekian, Ingolf Becker, Tyler Moore, Marie Vasek

[a] *University College London, Department of Computer Science, 169 Euston Rd., London, NW1 2AE, UK*
[b] *University College London, Department of Crime Science, 35 Tavistock Square, London, WC1H 9EZ, UK*
[c] *School of Cyber Studies, College of Engineering & Computer Science, 800 S Tucker Dr, Tulsa, 74114, OK, USA*
[d] *University College London, Department of Computer Science, 169 Euston Rd., London, NW1 2AE, UK*

Highlights

Raising the Bar: Assessing Historical Cryptocurrency Exchange Practices in Light of the EU's MiCA and DORA Regulation

Marilyne Ordekian, Ingolf Becker, Tyler Moore, Marie Vasek

- First, we conduct a doctrinal analysis on recent EU regulations, the Markets in Crypto-Assets Regulation (MiCA) and Digital Operational Resilience Act (DORA). We identify requirements for centralized cryptocurrency exchanges and systematically extract them and create a standard framework comprising 53 criteria.
- Second, we conduct the first comprehensive empirical study of self-regulation practices among all 75 fiat-dealing centralized cryptocurrency exchanges in Europe, analyzing 143 documents, including terms and conditions (T&Cs) and security policies. We compile a dataset of 371 hand-coded variables across 14 themes describing exchange practices.
- Third, we use the extracted legal standards to evaluate exchange practices, assessing their compliance posture with recent regulations. This

study provides a baseline to gauge the effectiveness of MiCA/DORA in the long term and track changes compared to the pre-regulation era. Additionally, it provides a tool to understand the areas currently lacking or that need more attention in industry practices.

- Fourth, we present evidence indicating that many exchanges face challenges in effectively self-regulating, fulfilling their custodial duties, maintaining robust security measures, and (may) use T&Cs to shift liability onto users. By documenting these practices and shortcomings, we provide regulators and the industry with actionable and tailored recommendations for improvements.

- Fifth, we provide a replicable methodology to investigate the self-regulation and governance of service providers and platforms in other emerging self-regulating.

- An earlier draft of this research has been communicated with the EU's European Securities and Markets Authority (ESMA) and European Banking Authority (EBA) in a closed meeting with the lead author. A final version has been requested by said authorities. Additionally, findings from this paper have been submitted as evidence for consultation calls in the UK. Particularly, consultation calls from the FCA and HM Treasury.

Raising the Bar: Assessing Historical Cryptocurrency Exchange Practices in Light of the EU's MiCA and DORA Regulation

Marilyne Ordekian, Ingolf Becker, Tyler Moore, Marie Vasek

[e] *University College London, Department of Computer Science, 169 Euston Rd., London, NW1 2AE, UK*
[f] *University College London, Department of Crime Science, 35 Tavistock Square, London, WC1H 9EZ, UK*
[g] *School of Cyber Studies, College of Engineering & Computer Science, 800 S Tucker Dr, Tulsa, 74114, OK, USA*
[h] *University College London, Department of Computer Science, 169 Euston Rd., London, NW1 2AE, UK*

Abstract

Centralized cryptocurrency exchanges have quickly become internal components of the digital finance ecosystem, mirroring traditional institutions by offering custody, investments, and transactional services. Despite their increasing prominence, the regulatory oversight has historically been fragmented and inadequate, leaving them largely relying on self-regulation. The resulting environment has been marked by exchange collapses, connections to criminal activities, cyberattacks, and poor operational security. High-profile failures, such as Mt. Gox and FTX, highlight the systemic risks and failure of internal governance models to properly mitigate or protect user funds from cascading risks or security breaches. In response, the European Union introduced the Markets in Crypto-Assets (MiCA) regulation and the Digital Operational Resilience Act (DORA), intending to standardize regulatory oversight and enhance user protection.

This paper presents the first comprehensive interdisciplinary analysis of centralized exchanges under the MiCA and DORA frameworks. Drawing on methods from both law and computer science, we systematically translate regulatory requirements into measurable compliance standards, and develop a novel doctrinal and empirical methodology to evaluate current self-regulatory practices of 75 centralized exchanges operating in Europe. Through a detailed analysis of 143 exchange legal documents, we identify

major compliance gaps and regulatory uncertainties. Our findings indicate significant shortcomings in exchange practices relating to asset custody, cybersecurity, and liability. This suggests that serious efforts are needed to change these practices and ensure their alignment with regulatory requirements. Our framework enables a systemic comparison between regulation and practice, and establishes a baseline for evaluating the effectiveness of regulatory measures. This approach can be replicated to study other self-regulating emerging sectors.

Keywords: cryptocurrency regulation, cryptocurrency exchange, MiCA, DORA, cybersecurity, mixed methods

1. Introduction

Centralized cryptocurrency exchanges[1] facilitate cryptocurrency transactions and custodial services, which significantly shapes the accessibility and usability of cryptocurrencies [1]. These exchanges have rapidly surged in popularity, emerging as the primary cryptocurrency service providers for regular users worldwide [2]. Centralized exchanges are increasingly mirroring traditional financial institutions by providing banking-like services such as payment, custody, and investment [3, 4, 5]; this has gained them the title of "crypto-banks" [6]. However, unlike their counterparts in traditional finance, exchanges have operated predominantly by self-regulating and internal governance measures [7, 8].

The inadequacies of self-regulation were apparent in major failures in the ecosystem that ended in infamous collapses, bankruptcies, and users losing their assets. This all began with the failure of Mt. Gox in 2014, then the largest Bitcoin exchange globally. The exchange's collapse, which is attributable to security breaches, internal mismanagement, and fraud [9, 10, 11], highlighted the risks inherent in the absence of robust regulatory oversight, especially with the ongoing decade-long bankruptcy case [12].

[1]The Markets in Crypto-Assets regulation adopts and defines the term Crypto-Asset Service Provider (CASP). In this paper, we interchangeably use the terms CASP and exchange to refer to centralized cryptocurrency exchanges. *See* art. 3(1)(15) MiCA: "crypto-asset service provider means a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with article 59." *See* art. 3(1)(16) MiCA for a detailed list of services and activities.

Subsequent collapses to Mt. Gox underlined the minimal progress accomplished in the field. The more recent dramatic failure of FTX in 2022 [13], indicates the continuous presence of vulnerabilities in exchanges' internal controls and operation practices [14, 15]. Particularly, in between Mt. Gox and FTX's failures, 40% of exchanges operating before 2022 subsequently failed [16]. These occurrences highlight an ongoing instability and immaturity in the ecosystem as a whole [17], which can pose many risks. Risks targeting users, for instance, can cause them to lose their assets without being able to get reimbursement. Whilst on a macro level, such risks can affect the market integrity of the entire sector.

These consistent vulnerabilities are explained, in part, through insights from the field of security economics [18]. Misaligned incentives, driven by information asymmetry and insufficient accountability mechanisms, can encourage exchanges to adopt risky business models, underinvest in cybersecurity [19], and potentially misuse client assets. Consequently, when a collapse occurs, customer face the consequences by losing their funds while platforms aim to shift liability. Such systemic issues can have major implications for customer protection, market integrity, and broader financial stability. A matter that emphasizes the urgent need for effective and comprehensive regulatory intervention.

Recognizing these risks and regulatory gaps, the EU introduced two leading regulatory instruments: Markets in Crypto-Assets (MiCA) regulation and the Digital Operational Resilience Act (DORA) [20, 21]. MiCA represents the world's first comprehensive and cryptocurrency-specific regulatory framework, which seeks to standardize the operations, supervision, and oversight of crypto-asset service providers (CASPs) across the EU. Simultaneously, DORA addresses cybersecurity standards by imposing uniform ICT [2] security requirements on financial institutions, including CASPs (DORA, art. 2(1)(f)), to enhance operational resilience and risk management practices across the sector [22].

Despite these leading regulatory initiatives, the effectiveness of MiCA and DORA remains uncertain, many EU countries are still in a transitional period [23]. Furthermore, the current inconsistent and opaque self-regulatory practices, which are overseen among exchanges and cryptocurrency service providers in general, further hinder this [24]. Without clear evidence de-

[2]Information and Communication Technology.

lineating existing Pre-MiCA/DORA exchange practices, as there exists no baseline of how centralized exchanges self-regulate, it is challenging to predict the extent and effectiveness of regulatory compliance. Ergo, a detailed understanding of the pre-regulation landscape is vital to evaluate the impact of these regulations, determine the extent of needed future amendments, and assess the compliance efforts expected of exchanges.

To bridge this major gap, this paper introduces a novel methodological framework combining legal analysis with empirical investigation. First, we systematically analyze and extract CASP-specific regulatory criteria from MiCA and DORA, translating these requirements into measurable compliance benchmarks. Second, we conduct a comprehensive empirical analysis by examining self-regulatory practices among 75 centralized cryptocurrency exchanges operating within Europe, systematically analyzing 143 legal documents, including terms and conditions (T&Cs) and security policies. Third, the practices identified through the empirical analysis are evaluated against the regulatory criteria extracted in the first step.

This paper addresses the critical need to understand and evaluate the existing operational and governance practices of centralized cryptocurrency exchanges in light of the EU's recently adopted regulatory framework. To this end, it develops a novel interdisciplinary methodology that synthesizes doctrinal analysis with empirical approaches grounded in computer science. The paper is structured as follows: Section 2 sets out the legal and technical background on centralized exchanges. Section 3 outlines the methodological approach. Section 4 presents the results of the empirical study and the evaluations with the extracted criteria. Section 5 discusses the implications of these findings and offers recommendations for regulators and the sector. Section 6 concludes.

2. Legal and Technical Background of Cryptocurrency Centralized Exchanges

The regulation and cybersecurity of cryptocurrency exchanges are closely interconnected, and present challenges at the intersection of legal frameworks and information security practices. As these platforms increasingly serve as new avenues for cryptocurrency custody, their operational failures, whether due to hacks, technical issues, or internal misconduct, raise questions about institutional design and legal accountability. The latest regulatory efforts (MiCA and DORA) in the EU, mark a significant step for formalizing the

regulatory frameworks around these actors in hopes of bringing more stability and trust in the market.

2.1. Cryptocurrency Exchanges and Custody Models

Centralized cryptocurrency exchanges are intermediaries that facilitate the buying, selling, and holding of cryptocurrencies through platforms operated by centralized entities. To deliver these services, exchanges take custody of their users' cryptocurrencies. Here, users deposit cryptocurrencies into wallets controlled by the exchange, hereby entrusting the exchange with exclusive control over the private keys [25]. Wallets are digital applications or devices designed to securely store, manage, and facilitate transactions of digital assets [24]. Wallets store private keys, which allow access and control over the cryptocurrencies found in the wallet [26]. Since exchanges retain control over the private keys, and thus, in principle, hold assets on behalf of users; this is referred to as the custodial wallet structure, as opposed to non/custodial or unhosted wallets, whereby users retain their own private keys [27].

The custody models used by exchanges vary significantly, ranging from explicit custodial arrangements, where exchanges clearly outline fiduciary duties and segregation of user assets, to tacit or undefined custodial relationships, crating ambiguity and legal uncertainty regarding asset ownership, control, and rights in the event of a security breach or insolvency [28]. Custodial wallets offer convenience as, in principle, they are user-friendly and integrated with instant fiat payment channels and trading. However, they necessitate users to place trust in the service provider as a custodian [27]. This contrasts with the original design of Bitcoin, which was intended to eliminate intermediaries [29].

History has shown that this trust might not always be granted, as the collapse or misconduct by exchanges can lead to catastrophic losses of user assets, as seen in infamous incidents from the Mt. Gox failure in 2014, to the more recent incident of FTX in 2022 [11, 30]. A key aspect of exchange custody is using wallet architectures to balance security and accessibility. In principle, exchanges state they operate a tiered system of "cold" and "hot" wallets to hold and store cryptocurrencies. Cold wallets store private keys entirely offline, be it, for example, on air-gapped computers or hardware devices; therefore, they are more secure and less vulnerable to cyberattacks [26]. Hot wallets, in contrast, are internet-connected wallets, enabling fast withdrawals, deposits, and trading by providing the exchange with rapid access

to funds. This real-time quick availability comes with the cost of higher security risk exposure, as hot wallets are a much easier target for malicious actors and are easier to breach [26]. Again, in principle, most exchanges state that they keep the majority of user assets in cold storage for safety, while keeping a smaller amount in hot wallets for operational and liquidity requirements.

Consequently, from a governance perspective, this custodial architecture raises normative questions about accountability and trust. Here, users must trust that the exchange will not misappropriate custodial assets and properly secure wallets. Unfortunately, this has not been the case in many instances, considering the many misconducts and security incidents exchanges in the ecosystem continue to encounter [31, 32].

2.2. Cryptocurrency Exchange (In)security

Centralized exchanges remain the most popular intermediaries for cryptocurrency operations as they process the most transactions [2, 33]. In 2024, exchanges had $\$18.83t$ in spot trading volume [34]. However, throughout the years, their popularity has also turned them into prime targets for bad actors, even the largest exchanges have been compromised [31, 32, 16, 11]. In 2024 alone, security breaches targeting exchanges resulted in losses exceeding $\$2.2b$ [35]. These incidents highlight the persistent vulnerabilities in their security system [19].

Not all breaches lead to collapses or direct financial loss, some compromise personal information of users. To comply with anti-money laundering and countering terrorism regulations, exchanges implement Know Your Customer procedures. This requires users to submit personal data such as government identification, address, contact details, etc, for verification. While they are intended to enhance compliance, such data pools are lucrative targets for attackers, and enable threats like phishing, social engineering, and wrench attacks [36, 37]. Coinbase recently suffered a major breach involving insider collusion, which resulted in user data compromise [38].

Beyond security breaches, organizational mismanagement and fraud have also precipitated collapses. The infamous downfall of Mt. Gox in 2014, which handled over 70% of global bitcoin transactions at the time, was attributed to a combination of alleged internal fraudulent practices and security breaches [39]. More recently, FTX's 2022 bankruptcy resulted from risky financial investments and misappropriation of customer funds [40]. This triggered a cascading liquidity crisis, including the collapse of other exchanges, and

exposed the risk of contagion spreading to other exchanges and the broader financial system [41, 42].

These collapses illustrate an important paradox: while exchanges position themselves as trustworthy custodians akin to traditional financial institutions, many still operate without equivalent regulatory oversight or safeguards [3]. The recurring collapses not only erode public trust but also highlight the need for robust legislative initiatives, such as the Markets in Crypto-Assets Regulation (MiCAR), to ensure transparency, accountability, and user protection.

2.3. Legislative Background: MiCA and DORA

Since Bitcoin was introduced in 2008, regulators have grappled with how to regulate the technology. As bitcoin and subsequent emerging cryptocurrencies had been built on new decentralized technology – the blockchain – this posed an unprecedented challenge to regulators globally, as there was no specific party against whom regulation could be enforced [7, 43]. This changed with the introduction of exchanges, which acted as a central intermediary that regulators could finally target. In the past few years, a few jurisdictions, such as Malta and the Emirate of Dubai in the UAE, took the initiative to regulate cryptocurrency service providers on a national level [44, 45]. However, on a geographical level, the EU was the first to propose a comprehensive piece of legislation in the world, by adopting the Digital Financial Package [46]. The latter comprised three pillars: 1) the Markets in Crypto-Assets (MiCA) regulation, which is tailored for cryptocurrency activities and service providers, 2) the Digital Operations Resilience Act (DORA), which offers specific provisions related to cybersecurity, and 3) the Distributed Ledger Technology (DLT) Pilot Regime, which is intended to boost the usage of DLT infrastructure and support innovation in the financial sector. In this paper, we focus on MiCA and DORA.

MiCA. The EU's Markets in Crypto-Asset (MiCA) regulation establishes, under Title V, the first comprehensive regulatory framework for crypto-asset service providers (CASPs), also referred to as centralized exchanges. MiCA's Title V, which took effect at the end of 2024, treats CASPs as fiduciary organizations, mandating a licensing procedure, adherence to strict governance and risk management standards, and strict custodial protocols. MiCA has several goals, including: (i) professionalizing the industry by ensuring a baseline level of competency and reducing the risk of bad actors entering the space, (ii) enhancing consumer protection through transparency

and disclosure obligations, which allows users to have better information about CASPs' practices and associated risks, and (iii) promoting financial stability by allowing only legitimate businesses to provide services and by enforcing mandates to manage operational risks.

DORA. MiCA integrates a distinct piece of legislation, the Digital Operations Resilience Act (DORA), in its provisions.[3] This ensures that exchanges are also subject to the requirements stipulated by DORA. DORA, which came into force at the beginning of 2025, aims to strengthen the cybersecurity posture of the European financial sector. This is by focusing on the operational resilience of financial entities against ICT (Information and Communication Technology) risk. It mandates the creation of robust ICT risk management frameworks that include identifying and assessing potential vulnerabilities, implementing safeguarding measures, and conducting regular resiliency testing. These requirements ensure entities, including exchanges, have the necessary infrastructure and protocols to maintain organizational continuity and safeguard user funds during incidents.

2.4. Terms and Conditions as a Data Source

Terms and conditions (T&Cs) constitute this study's primary empirical data source. T&Cs are publicly available documents outlining rules governing online service providers and regulating their relationship with users. T&Cs include provisions on the terms of use, rights/obligations, prohibited activities, and information on how service providers manage risk, protect their interests, and limit their liabilities [47]. T&Cs are long documents written by lawyers, full of legalese, and often include ambiguous and generalized language. T&Cs belong to a category of contracts known as "Contracts of Adhesion," which are unilaterally drafted and imposed by one party on a "take it or leave it" basis [48]. Hence, users cannot negotiate,[4] as they can either accept the terms to use the service or refrain from using it.

Researchers have observed limited comprehension and understanding of T&Cs among users [49, 50, 51, 52, 53, 54], leaving them uninformed of the full implications of the agreement [55]. Users often agree to these contracts without reading them [56, 57] or realizing their legally binding nature [48], which could create adverse consequences. The EU recognizes this imbalance

[3] *See*, MiCA art. 68.

[4] In this current study, none of the exchanges included in the dataset offered corporations or entities separate terms, or the right to negotiate some clauses.

with the Unfair Contract Terms Directive, which aims to protect consumers against unfair terms they have not negotiated, especially those that cause a significant imbalance in rights/obligations to the detriment of the consumer [58, 59]. However, it is worth noting that not all potentially unfair terms are automatically rendered void, as the directive is implemented with a varying enforcement level at the national level [59]. In this paper, we do not address the validity of the terms and conditions of exchanges under EU or any national law, but rather survey and analyze their provisions.

3. Methodology

This study investigates the current self-regulatory and compliance practices of centralized cryptocurrency exchanges operating in Europe, evaluated against the requirements of MiCA and DORA regulations.

For that purpose, we conduct two interlinked studies. First, we create a novel methodological approach for systematically translating regulatory provisions (here, MiCA and DORA) into specific compliance standards (§3.1). This translation utilizes expertise from both legal and technical scholarship to make sense of the regulations and the underlying technology in a nuanced yet discretized manner. The resulting framework, which includes 76 criteria, offers a structured basis for mapping current practices and identifying areas for regulatory and industry improvements.

In the second study, we apply this framework in a large-scale empirical assessment of the sector. We follow an iterative and qualitative coding process to analyze 143 legal documents, including terms and conditions, security policies, and supplementary disclosures, for 75 centralized exchanges operating in Europe (§3.2).

To our knowledge, this is the first study to both construct a compliance framework directly from EU cryptocurrency relevant legislation and evaluate the industry's self-regulatory practices against it. In doing so, this offers a tailored empirical account of how exchanges operationalize legal obligations and where regulatory and compliance gaps exist.

3.1. Study 1: Systematic Creation of Compliance Standards

MiCA and DORA introduce a new regulatory paradigm for exchanges (crypto-assets service providers) in the EU. As leading frameworks, their practical impact on industry participants, especially centralized exchanges,

remains largely untested. The absence of empirical baseline data for pre-MiCA/DORA compliance practices poses a significant challenge to regulators, scholars, and industry stakeholders looking to evaluate the effectiveness interpretability and enforceability of these regulatory instruments.

To address this gap, we create a structured methodology to systematically translate legal requirements into an operationalizable compliance framework. This is important not only to evaluate current exchange practices, but also to create a reusable and scalable framework for future regulatory evaluations, including for other emerging self-regulatory industries. Our approach proceeds in four phases:

1. **Doctrinal analysis** of MiCA and DORA provisions, focusing on custodial duties, operational resilience and security, liability, and security breach disclosure requirements.
2. **Criteria extraction**, whereby 53 core requirements and compliance standards were identified directly from legislative text through an iterative legal-technical reading and analyzing process.
3. **Practice-based extension**, in which we add 23 additional criteria from observing both the terms and conditions used by exchanges, and the expertise of the authors (including law, cybersecurity, and computer science academics). These capture potential regulatory blind spots.
4. **Chronological reclassification taxonomy**, which organizes the criteria thematically, as legal requirements are not always presented in a format conducive to industry alignments or technical implementation. This reclassification is for both analytical and practical purposes: it enhances clarity for comparative analysis and reflects the functional requirements relevant to service provider governance.

The resulting framework consists of 76 compliance criteria divided into four categorical groups: institutional legitimacy (§4.1), operational risk management (§4.2), liability (§4.3), incident management and disclosure (§4.4). This framework allows a structured comparison between regulations and industry implementation. Moreover, it also enables a bottom-up evaluation of whether and how industry practices align with, diverge from, or await regulatory mandates. These standards are outlined in the results section, whereby each standard is stated before the subsequent empirical results.

	Codes	Range	Median
Institutional Legitimacy	9	[0, 8]	4
Operational Risk Management	22	[0, 12]	1
Exchange Liability	11	[0, 8]	5
Incident Management & Disclosure	42	[0, 23]	12

Table 1: Number of codes within our thematic categories and range/median number of codes within that category that a single exchange implemented.

3.2. Study 2: Empirical Analysis of Cryptocurrency Exchanges' Terms and Conditions

We conduct an empirical analysis of the T&Cs, security policies, and supplementary legal documents for 75 exchanges representing all fiat-dealing centralized exchanges operating in Europe. In the subsequent subsections, we explain the selection criteria of exchanges (§3.2.1), and the data collection and analysis process (§3.2.2).

3.2.1. Selection of Exchanges

An exhaustive register of all centralized exchanges operating across Europe is currently lacking. MiCA provides a transitional "grandfathering" period permitting already registered platforms to continue operating for a short time while they seek a license. However, the grace period ranges from one country to another; for instance, it is 18 months in France, whilst 6 months in the Netherlands [23].

As an official comprehensive registry is still lacking, we resort to two cryptocurrency exchange aggregator websites to identify exchanges: CoinMarketCap and CoinGecko [60, 61]. As we will demonstrate in 4.1, some exchanges do not publicize an accurate operating location, and others offer services in some European countries despite only being registered abroad. This practice makes it difficult to map out all exchanges operating *de facto* in Europe. As a proxy, we consider exchanges accepting at least one European fiat[5] currency.[6]

[5]The potential for additional legal scrutiny when interacting with the heavily regulated traditional financial system is considered.

[6]In total, 47 currencies were considered. The website from which the list of European currencies was taken was Wikipedia, "List of currencies in Europe". *See* `https://en.`

Following this step, 138 exchanges are identified. A set of inclusion and exclusion criteria detailed in Table A.7 is applied, resulting in a final dataset of 75 exchanges. From these 75 exchanges, 143 documents and pages are extracted. Table A.7 outlines this process.

These selection criteria introduce some limitations, in particular, the focus on fiat dealing exchanges. However, as not all exchanges listed on CoinMarketCap and CoinGecko are legitimate businesses, we hypothesize that the focus on fiat-dealing exchanges can exclude some of the obvious fraudulent exchanges.

3.2.2. Data Collection and Analysis

We access and obtain the publicly available (public domain) T&Cs, security policies, and other relevant information pages (Table A.7). We archive these documents on `archive.org`. While the documents we collect and analyze are from 11/2022, we note that most exchanges do not update their terms for extended periods or only do so to include new offerings like staking or NFTs, or for AML-CFT (anti-money laundering and countering the finance of terrorism) regulation compliance, which are outside of the scope of this project. Our focus remains on generally applicable T&Cs and security-related information.

Towards this end, we conduct a multi-stage manual analysis using thematic analysis [62]. In the first stage, we conduct a pilot study involving three coders. Each coder identifies and extracts from three exchanges selected at random, passages per the themes described in §3.1. Following multiple rounds of discussion and identifying areas of relevance, a draft codebook is generated. Our goal was to identify provisions relating to the compliance standard extracted from MiCA/DORA. Therefore, the next step involves the three coders finding and separating from all exchange T&Cs, excerpts that explicitly discussed these criteria.

After this stage, one of the authors, who is a law and cybersecurity academic, worked inductively to identify and classify texts accordingly. This required interpretation and a thorough manual inspection to precisely convey normative provisions, as they are not uniformly written across documents nor not they always expressly communicated. This process was iterative, and the documents were re-coded as the coder advanced into the dataset, and the

`wikipedia.org/wiki/List_of_currencies_in_Europe`

language of the codebook was honed. A final codebook is generated with 371 codes across 14 themes describing exchange practices. The codebook is then used to analyze and annotate the passages previously extracted. Out of this comprehensive dataset, we use 163 codes across 23 sub-themes in this study. Table A.8 shows a rough outline of this. Table 1 summarizes the process of consolidating themes. The latter Table also shows the range and median number of codes within a single category. As seen, the range starts with zero with all the major four categories, meaning that in all of them, some exchanges did not tick these requirements.

Throughout the data collection and analysis period, a few exchanges collapsed or closed for multiple reasons, including interconnectedness to FTX's bankruptcy. We recorded collapses for a period of 15 months following FTX's collapse, and outlined in the results and relevant tables the practices of those that collapsed. Specific causes for exchange closures are outlined in Table 2. Furthermore, a few exchanges had obtained pre-MiCA local licenses to operate as VASPs,[7] which are noted as well. This is with the aim of showing whether having a license had any influence on practices.

Experienced Changes	# Exchanges
Closed	8
Collapsed following FTX	3
Liquidation/Bankruptcy	4
Fraud allegations	2
Rebranded	3
Acquired	1
Unspecified (service ended)	3

Table 2: Exchange changes over the period of 15 months, starting with 75 exchanges.

4. Results

4.1. Institutional Legitimacy of Cryptocurrency Exchanges

MiCA establishes a set of baseline requirements for institutional obligations for CASPs, including foundational conditions, and making available

[7]Virtual Asset Service Provider.

Institutional Legitimacy								
Checked Practice	**MiCA/DORA Reference**	**Required?**	**Exchanges**		**Licensed**		**Collapsed**	
			#	%	#	%	#	%
Basic Requirements								
Identifiable Legal Person	59(1)	✓	38	50.7	15	83.3	7	70
Unidentifiable Legal Person	59(1)	✗	26	34.7	2	11.1	2	20
Detailed Physical Address - Stated	59(2), 62(2)	✓	43	57.3	16	88.9	6	60
Broad Physical Location - Stated	59(2), 62(2)	✗	17	22.7	3	16.7	3	30
Contact Information - Stated	62(2)	✓	54	72	12	66.7	9	90
Applicable Law - Stated	70(4)(a), 75(1)(g)	✓	66	88	17	94.4	9	90
Licensing								
Licensed as Exchange	59(1)(a), 62(1)	✓	18	24	17	94.4	1	10
Licensed as Exchange - Multiple	–	(✓)	5	6.7	5	27.8	0	0
Security Certificate - Stated	Recital(81), 68(7), 68(8)	✓	7	9.3	3	16.7	2	20

Table 3: Institutional legitimacy practices of 75 centralized cryptocurrency exchanges in Europe compared to MiCA regulation requirements. ✓: required practice. (✓): best practice not explicitly outlined. (✗): best practice contradicted and not explicitly outlined. ✗: practice is explicitly contradicted.

terms and conditions governing their relationship with their users (MiCA, arts 70(9), 75(1)).

Legal Personality and Registration. Cryptocurrency exchanges must be constituted as legal persons, distinct from natural persons(MiCA, art. 59(1)), and registered in the commercial registry of an EU member state. Consequently, individuals acting alone may not apply for a CASP authorization. Furthermore, when applying for a CASP license, service providers must also provide verifiable contact information, including a valid e-mail address and telephone number (MiCA, art. 62(2)).

In the exchanges surveyed, whilst most claim to operate as legitimate businesses as legal persons, only 37 of 75 offer documentary evidence to identify them. Eleven exchanges do not provide a corporate or business name. Of the 37 that do offer registry information, ten could not be verified in the relevant national registries when checked by our team. This may suggest potentially false disclosure by service providers about their legal personality.

This lack of verifiable identity raises concerns regarding the legitimacy of some platforms, particularly considering the low barrier to setting up fraudulent exchange websites and the immense financial harm users may incur as a result [63]. Recently, the ecosystem is witnessing the proliferation of sophisticated hybrid investment fraud, where fraudsters build trust with victims over time to exploit them financially through fake cryptocurrency exchanges and investment platforms [64, 65]. These schemes have led to significant losses, with reports showing that hybrid investment fraud schemes accounted for 33.2% of total cryptocurrency scam revenue, generating $\$9.9bn$ in 2024 [35]. Consequently, without identifiable legal personalities, exchanges may inadvertently become conduits for such fraudulent activities, or this may be an indication of hidden illegitimate activities.

Detailed Physical Address. MiCA mandates exchanges to maintain a physical office within at least one EU member state. General location descriptors, such as a P.O. box or a city name, are not sufficient to meet this standard (MiCA, arts. 59(2), 62(2)). Of the examined exchanges, over one-third of the exchanges fail to provide a detailed physical address or contact information. The absence of such transparency may reflect attempts to avoid regulatory oversight, frustrate user complaints, obfuscate the identity of the service provider, or even may be a practice of a fraudulent exchange.

Offering Transparent Agreement to Users. Having T&Cs alone is not enough. T&Cs must also include specific details to transparently inform users. This involves exchanges explaining the scope of their services, and the rights and responsibilities of parties involved in the contract (MiCA, arts. 70(4), 75(1)).

In the examined dataset, not all exchanges provide T&Cs. Those that do often lack standardization, suitable up-to-date terms, or essential clauses such as the applicable law. We further notice a lack of uniformity in these terms across exchanges with significant discrepancies in length (2 to 70 pages), quality (spelling/grammar mistakes), and content among the examined provisions.

Many exchanges fail to demonstrate being in line with the latest legal requirements by not updating their terms. In our dataset, only about half (41) provide a revision date indicating when terms were last updated. When provided, revisions are often two or more years old. Additionally, only one exchange provided a previous version of its terms, although no summary of changes to the contract is given. The latter practice hinders users from staying informed and updated about newly changed provisions.

4.1.1. Licensing

CASP Authorization Requirements. MiCA introduces a mandatory licensing regime for exchanges, requiring all entities providing crypto-asset services to obtain a formal authorization from competent authorities (MiCA, arts. 59(1), 62(1)).

Although a few pre-MiCA national licensing regimes existed, such as the Maltese Virtual Financial Assets Act, our findings show that only a quarter of exchanges (18) hold such a license already, with five holding multiple licenses. This suggests that the majority of exchanges are now required to undergo the licensing process under MiCA. Moreover, as of 2024, about 55% of global cryptocurrency trading volume is handled by exchanges holding at least an EU pre-MiCA license [66]. This suggests that almost half of trading still flows through exchanges lacking EU authorization. Table 3 indicates that pre-MiCA licensed exchanges in our dataset are already demonstrably more compliant with foundational institutional requirements, such as legal personality, etc. Major players in the ecosystem have begun pursuing regulatory approval, but many are unlicensed pending MiCA's full enforcement. For example, in 2023, Binance faced enforcement setbacks in the EU as it withdrew from the Netherlands after failing to obtain a Dutch license from the central bank [67].

Cybersecurity Certification. To ensure operational resilience, exchanges should establish internal controls, risk management procedures, and secure ICT systems that safeguard the confidentiality, integrity, and availability of the service. CASPs may demonstrate such compliance with internationally recognized security certifications (MiCA recital 81, arts. 68(7), 68(8)).

The number of exchanges demonstrating cybersecurity hygiene by obtaining security certifications was quite low. We identify seven exchanges demonstrating formal certifications, such as ISO 27001, PCI DSS, or SOC, this is despite widespread claims of security compliance. Such security certifications, though not directly mandated by law, are increasingly regarded as a best practice, which signals to regulators and users that an exchange's systems and data are safeguarded to serious and (externally) audited standards. The focus on operational resilience is perhaps an express reaction to the ecosystem's infamous record of operational lapses and security breaches. High-profile failures have shown that rigorous security and risk measures are as important as legal compliance in maintaining market confidence. Per MiCA's framework and complementary legislation like DORA, the EU is

attempting to import the presidential robustness of traditional finance to forestall CASP failures.

4.2. Operational Risk Management

Operational Risk Management

Checked Practice	MiCA/DORA Reference	Required?	Exchanges		Licensed		Collapsed	
			#	%	#	%	#	%
Security Measures								
Penetration Testing	24, 25(1)		4	5.3	2	11.1	1	10
Bug Bounty	25(1)	✓	5	6.7	6	33.3	2	20
Anomaly Detection	10, 17, 25	✓	9	12	3	16.7	1	10
DDoS Countermeasures	8, 10, 11, 17	✓	5	6.7	1	5.6	2	20
Past Compromises	13	✓	2	2.7	1	5.6	0	0
Audit	5(2), 6(6)	✓	10	13.3	2	11.1	1	10
Personnel Background Check	62(3)(a), 68(1)	✓	3	4	1	5.6	0	0
In Office Security Policy	9(4)	✓	4	5.3	0	0	0	0
Access Control	6(2), 9(4)	✓	9	12	1	5.6	2	20
Wallet Custody Policies								
Fund Segregation	70(1), 70(3), 75(7)	✓	15	20	8	44.4	1	10
Omnibus Account	70(1), 70(3), 75(7)	(✗)	10	13.3	5	27.8	2	20
Hot and Cold Wallets	75(1), 75(3)	✓	27	36	6	33.3	5	50
Portion Stored Offline Stated	75(1), 75(3)	✓	11	14.7	3	16.7	2	20
Securing Wallets								
Wallet (cold) - Air gapped	75(1), 75(3), 70(1)	✓	2	2.7	1	5.6	0	0
Wallet - Multisignature	75(1), 75(3), 70(1)	✓	9	12	1	5.6	2	20
Wallet (cold) - Encryption (any)	75(1), 75(3), 70(1)	✓	11	14.7	2	11.1	2	20
Wallet - Processor Protection (HSM)	75(1), 75(3), 70(1)	✓	4	5.3	0	0	1	10
Wallet - Offsite Geographically Distributed	75(1), 75(3), 70(1)	✓	8	10.7	2	11.1	0	0
Wallet - Multiparty Computation (MPC)	75(1), 75(3), 70(1)	✓	4	5.3	1	5.6	1	10
Delay Transactions	–	(✓)	9	12	2	11.1	4	40
Remote Backup Keys	68(7),11, 12	✓	3	4	0	0	0	0
Insurance/Compensation - Limited	67(4), 67(5), 67(6)	✓	8	10.7	4	22.2	1	10
Insurance/Compensation - Unavailable	67(4), 67(5), 67(6)	✗	5	6.7	1	5.6	1	10

Table 4: Operational risk management practices.

In recent years, high-profile exchange breaches have resulted in the loss of billions of dollars [35, 68]. These incidents highlight the necessity for tailored and robust risk management. While general cybersecurity principles apply across the financial system, exchanges present a unique exception as custodians for wallet-based custodians, facing additional heightened operational and security threats. This subsection examines 23 risk management standards and practices to provide insights into the current state of operational resilience. Table 4 outlines the assessed standards and practices.

4.2.1. Security Measures

MiCA classifies CASPs as fiduciaries, considering them in a position of trust and confidence with corresponding obligations to safekeep user assets and act in their best interest (MiCA, art. 66.1). This fiduciary role entails the implementation of comprehensive custodial and operational risk frameworks, per MiCA and DORA provisions.

Digital Security Measures. DORA requires financial institutions, including exchanges, to establish: 1. digital operational resilience testing program which necessitates *penetration testing* (DORA, arts. 24, 25), 2. assessment criteria for ICT systems, potentially through *bug bounty* programs (DORA, art. 25), 3. *anomaly detection* systems (DORA, arts. 10, 17, 25), 4. dedicated plans to identify, prevent, and contain ICT risks and incidents, such as *DDoS countermeasures* (DORA, arts. 8, 10, 11, 17), 5. periodic *audit* plans (DORA, arts. 5(2), 6(6)), and 6. procedures to review and learn from past compromises (DORA, art. 13).

Despite these expectations, only a minority of exchanges adopt measures against external threats, and most were not explained. For example, nine exchanges state using anomaly detection, and four mention penetration testing. This comes as a surprise, as these are standard practices. Thirty-one exchanges have bug bounty programs, which indicates the growing interest in preemptive threat detection. Nevertheless, transparency is limited among those outsourcing and relying on third parties, particularly among newer exchanges that rely heavily on cloud-based infrastructure [69].

Physical Security Measures. DORA also requires ICT risk management frameworks to include physical security. This includes in-office security policies like restrictions to physical or logical access to information (DORA, art. 9(4)), and role-based access control (DORA, arts. 6(2), 9(4)). MiCA further requires that exchange members of the exchange management body possess

a good reputation, experience, and no criminal record (MiCA, arts. 62(3), 68(1)).

Adoption of basic internal controls is inconsistent. Only four detail in-office security practices like monitoring employee actions, encrypting hard drives, and enabling screen locking. Nine describe access control systems with logged and permission entry, while three conduct employee background checks. Similarly, 10 report conducting audits, with only three doing so periodically, this is despite audits being important for maintaining operational integrity, precision, and accountability. These practices are concerning given the persistent risk of insider threats. Multiple major platform failures, including Mt. Gox, FTX, and BitGrail, were linked to internal misconduct, resulting in losses of about $170 million in user funds [70]. More recently, Coinbase announced that the hack, which led to attackers gaining access to customer personal data, was facilitated by some insiders [38].

4.2.2. Wallet Custody Policies

Under MiCA, custodial CASPs, (i.e., exchanges that hold their clients' currency for them) must adopt formal custody policies and conclude agreements with users outlining the scope of their custodial responsibilities and duties (MiCA, art. 75.(1)). These requirements show regulatory concerns following a series of high-profile collapses, in which inadequate fund segregation practices were exposed. Such practices include exchanges not separating their assets from those of their users. For instance, after Mt. Gox's collapse, Japanese regulators required strict segregation of user assets [71]. Other alarming practices include fund misappropriation, e.g., FTX had misappropriated billions of its clients' funds, reportedly utilizing them for proprietary trading [72]. To this end, custody and wallet security practices are discussed below.

Fund Segregation. MiCA mandates exchanges to segregate their own funds (both cryptocurrency and fiat) from those of their clients, and also clearly distinguish and document the means of access (MoA) to these assets (MiCA, arts. 70(1), 70(3), 75(7)).

Our findings show that custodial practices are not appropriately outlined, which exposes users to unnecessary risks. Only 14 exchanges state that they segregate their funds from user assets, while 61 give no clear disclosure on their governance policies or custody arrangements.

Such a lack of transparency is very problematic [73, 25], as it affects users'

asset vulnerability negatively and their proprietary rights, particularly in cases of insolvency, whereby users' assets might become part of the exchange's estate, or users (creditors) lose order priority [28].

On the other hand, MiCA does not specifically prohibit *omnibus accounts*. Omnibus accounts are used to combine and hold all users' cryptocurrencies collectively, i.e., pooled without segregation. Our data indicates that none of the exchanges affirm to segregate user funds from each other, but ten openly report using omnibus accounts. The usage of omnibus accounts is controversial, as some would consider the failure to separate user funds individually increases systemic exposure, single points of failure, mixes users' entitlements, and exposes them to shared risks such as insolvency and cyberattacks. See more in §5.

Hot and Cold Wallet Management. MiCA mandates that the custody policy establishes internal rules and procedures for safekeeping or controlling the user assets or their means of access (MiCA, art. 75(1), 75(3)). As MiCA's provisions here are broad, per best practices set in the industry, the custody policy must demonstrate the methods of storing keys, whether in cold (offline) storage, hot (online) storage, or both. This also includes being transparent about cryptocurrency allocations between these wallets; for example, disclosing the portion of funds stored in hot and/or cold wallets.Best practices suggest a hybrid structure of custody, where hot wallets are used to facilitate real-time and day-to-day trading, and cold wallets serve to secure the majority of reserves. This allows exchanges to run their business while limiting their risk of security issues associated with hot wallets.

Yet, wallet management disclosures are minimal across most investigated exchanges. Only 28 report using the hot/cold wallet combination. Of these 28, 12 provide details on the distribution of funds across these different wallet types. However, 47 exchanges fail to disclose any wallet management strategies with their wallets, and 63 provide no clarity on fund distribution. Why is this important to clearly disclose? Before its collapse, FTX had never disclosed its fund distribution across wallets, though it repeatedly reassured users of using the ideal hot/cold wallet combination. During its bankruptcy proceedings, it was revealed that it had stored the majority of customer funds in hot wallets, exposing them to security threats [74].

4.2.3. Wallet Security

The technical measures and safeguards implemented by exchanges to protect wallets are essential to their resilience against potential security breaches. The configuration and strength of these controls directly determine the success of an attack, the exchange's susceptibility to breaches, the magnitude of potential loss, and the feasibility of recovery.

Wallet Safeguarding. To safeguard users' funds, exchanges must establish internal controls and operational procedures that secure cryptocurrencies, their means of access, and wallets (MiCA, arts. 70(1), 75(1), 75(3); DORA, art. 9). However, MiCA/DORA stop short of describing specific security measures, which leaves discretion to the exchanges.

As a result, wallet security policies largely vary across exchanges, which limits and complicates standardization and comparability. While many exchanges affirm that user assets are securely stored, only a minority provide useful details. Among those that do, two report using air-gapped wallets, nine implement multi-signature with cold wallets, and four combine multi-signature along with technical processor protection, including a hardware security module (HSM). A subset further decentralizes some risks by storing cold wallet keys or means of access off-site and geographically distributed. Given this variability and the importance these systems play in safeguarding user assets, standardizing practices for secure wallets is warranted to protect user assets consistently. See more on wallet security in §5.

Delay and Recovery. Operational continuity and recovery from security incidents are also vital in stopping and addressing disruptions and security incidents. MiCA and DORA require exchanges to have a timely recovery plan (MiCA, art. 68(7); DORA, arts. 5, 11, 12). Within the cryptocurrency ecosystem, exchanges have adapted traditional cybersecurity methods to fit their infrastructure. These adapted traditional methods include delay and recovery mechanisms. For instance, nine exchange state they may delay transactions to comply with internal security protocols, or to allow internal verification when transferring funds in and out of cold storage. Four report using remote private key backups. Technically, these practices present inherent trade-offs. While backing up keys may enhance asset safety and resiliency, and facilitate recovery when necessary, it also expands exchanges' attack surface. For this reason, although these practices are disclosed in some of the investigated exchanges, they are best interpreted cautiously, especially

since regulatory frameworks have not yet articulated clear standards around these risk/benefit measures.

4.3. Exchange Liability Under Differing Circumstances

This subsection examines how exchanges allocate liability in their terms, with a focus on liability disclaimers, and the rare circumstances in which liability is expressly accepted. While some limitations in liability may be justified, especially in the face of specific threats or market volatility, for instance, many cases reveal more intricate approaches, including those related to service performance, cybercrime/theft of funds, breaches, and unauthorized access. A specific contentious area of concern is force majeure clauses, as some exchanges invoke unavoidable and unforeseeable events to disclaim liability for certain events like breaches, even in cases that may be reasonably anticipated. This section examines 11 standards and practices relating to liability clauses, which are summarized in table 5.

Exchange Liability

Checked Practice	**MiCA/DORA Reference**	**Required?**	**Exchanges**		**Licensed**		**Collapsed**	
			#	%	#	%	#	%
Disclaiming Liability								
Reasonable Efforts to Operate/Maintain Service	Recital(81), 68(7), 9, 11, 12	✓	15	20	5	27.8	0	0
Not Liable - Service Performance	Recital(83), 75(8)	✗	71	94.7	14	77.8	10	100
Not Liable - Cybercrime	Recital(83), 75(8)	✗	58	77.3	14	77.8	9	90
Not Liable - Data Breach/Data Loss	Recital(83), 75(8), 18, 50, 51, 52	✗	40	53.3	7	38.9	7	70
Force Majeure - Security Breaches	Recital(83), 75(8), 18, 50, 51, 52	✗	13	17.3	1	5.6	3	30
Not Liable - Unauthorised Access	Recital(83), 75(8), 6	✗	29	38.7	9	50	6	60
User Liable - Any Activity	Recital(83), 75(8)	✗	37	49.3	9	50	5	50
Accepting Liability								
Accept Liability - Conditional	Recital(83), 75(8)	✓	39	52	13	72.2	5	50
Accept Liability - Theft, if Exch Negligent	Recital(83), 75(8)	✓	7	9.3	5	27.8	0	0
Accept Liability - Loss of MoA Control, if Exch Negligent	Recital(83), 75(8)	✓	11	14.7	3	16.7	1	10
Conditional Refund Granted - Unauthorised Transactions	Recital(83), 75(8)	✓	1	1.3	1	5.6	0	0

Table 5: Liability provisions under differing circumstances as stated in CASPs' T&Cs.

4.3.1. Disclaiming Liability

Per MiCA provisions, exchanges are held liable for the loss of their users' funds or the corresponding means of access when such incidents are *attributable to* the exchange (i.e., within their control) (MiCA, art. 75(8)). Exchange liability is capped at the market value of the cryptocurrencies listed at the time of the incident (MiCA, recital 83). Exchanges are expected to employ "all reasonable" efforts to ensure service performance continuity, including the implementation of resilient and secure ICT systems, along with measures to protect the confidentiality, integrity, and availability of data.

Yet, what qualifies as "all reasonable" efforts, or what falls within the exchanges' "control" or is "attributed" to them, remains undefined, which leaves significant room for interpretation (MiCA, recital 81, art. 68(7); DORA, arts. 9, 11, 12). This ambiguity can enable exchanges to contractually disclaim liability, with a direct conflict with MiCA. In fact, our findings indicate that many exchanges assert that they adopt *reasonable* and *necessary measures* in service operation and maintenance, thereby positioning any failures as outside of their control. Example of clauses here include statements like *"Security is at the heart of everything we do"* or *"the Website is supported by appropriate security measures based on* ***current standards****"* or *"(exchange) will take every* ***reasonable measure*** *to secure funds stored in a (exchange) Wallet,* ***but cannot guarantee complete security****."*

Disclaimers and statements like these can obscure the gap between claims and actual implementation. In reality, past incidents have shown that many exchanges fail to uphold safeguards they reference, and in fact, some have invoked these provisions in litigation as a legal shield against liability [75]. The increase in cybersecurity incidents, coupled with failures to safeguard user funds, has led to a surge in lawsuits against exchanges [75, 76, 77, 78]. Such practices can be seen in our dataset, where many exchanges disclaimed and shifted liability to users. Selected examples pf these clauses are analyzed below:

Service Performance: . Exchanges are required to ensure the continuity and regularity of their services, including availability and performance (MiCA, art. 68(7)). MiCA considers exchanges liable for the loss of users' cryptocurrencies and means of access due to malfunctions, or system failures, or any form of operational failure, whether caused by software or hardware issues (MiCA, recital 83, art. 75(8)).

Despite these expectations, in current practices, nearly all exchanges (71)

include liability clauses on performance issues, be it operations, service reliability, or availability. Specifically, they disclaim liability for damages or losses resulting from service delays, failures, or interruptions. Commonly, exchanges interrupt service for a short, necessary period for emergent maintenance. However, some exchanges invoke such clauses broadly, without providing a clear duration or limitation, or scope. Such practices can open the door to potential exploitation. In particular, some fraudulent exchanges have staged exit scams by masking them as maintenance interruptions [79]. One extreme example includes an exchange in our dataset that has remained offline for over 17 months while citing maintenance on its website.

Cybercrime and Theft of Funds. Under MiCA, exchanges will become liable for losses caused to users due to any form of cybercrime, including cyber attacks targeting user funds, which result in their theft (MiCA, recital 83, art. 75(8)). At present, most exchanges (59) disclaim liability for damages or losses resulting from events like DDoS attacks or fund theft due to hacking. Additionally, they do not guarantee safety from malware (including viruses, worms, trojan horses, or "malicious interface") on their platforms. For instance:

> "(...) the user is aware that [...] the possibility [exists of someone] taking control over the User's device or in any other way [...] take over the User's account [...] which, may result, among other things, **in the theft of the User's funds—the User bears sole responsibility [...] and cannot make any claims against [exchange] on this account."**

Given exchanges' high susceptibility to cyber attacks, this can indicate a lack of commitment to platform security and suggest a lack of confidence in their security measures as custodians.

Moreover, exchanges do not guarantee the safety and integrity of their services. One exchange states:

> **"The Platform does not guarantee [...] security of the services** [...] the Platform shall not be held responsible to the Users or any third party[...]: (3) where the Platform services are **interrupted or delayed due to such factors as hacker attacks."**

These disclaimers stand in tension with requirements enshrined in MiCA, which raised questions about the fairness and enforceability of such terms, especially when users lack the bargaining power to evaluate the security and reliability of the service. More on this see §5.

Breach User Data. Under MiCA, exchanges will be liable for data loss or security breaches targeting their systems; these include events that lead to the loss of users' means of access, such as the private keys. Such events subject exchanges to penalties (MiCA, recital 83, art. 75(8); DORA, arts. 18, 50, 51, 52). However, over half of the exchanges (40) examined in the dataset currently disclaim liability for user data breaches or loss/damage to data, while the remaining 35 exchanges do not explicitly address this. This liability shift, not only raises huge concerns regarding user data privacy, but also contradicts article 82 of the GDPR, which grants users the right to compensation for data protection infringements [80].

Force Majeure. As with any user agreement, the terms and conditions of exchanges also include force majeure clauses. While these clauses mostly included typical events, like acts of God, wars, strikes, etc., our dataset also includes 13 exchanges that consider cyber attacks to constitute force majeure. Consequently, they absolve themselves from performing their duty without relevant consequences if the event occurs.

For context, MiCA considers cyber attacks to be events attributable to the exchange (MiCA, art. 75(8)), as explained above. Therefore, we can conclude that cyber attacks constitute foreseeable and avoidable events, rather than a force majeure event, which would have relieved exchanges from fulfilling their contractual obligations. Whilst this clause is not prevalent, its presence sets a dangerous precedent. In an attack-prone space [31, 32], the elements constituting a force majeure are lacking. Cyber attacks are not unforeseeable for exchanges; they are a significant and expected risk. While cyber attacks may not always be avoidable, defensive measures are required. Classifying cyber attacks as force majeure can discourage and excuse exchanges from prioritizing the security of the platform.

Liability for Unauthorized Access. Per DORA provisions, exchanges are expected to have procedures in place against unauthorized access risks. Concurrently, per the liability provisions set in MiCA, exchanges are liable for user losses following an ICT incident, including those leading to unauthorized access to a user's account (DORA, art. 6; MiCA, recital 83, art. 75(8)).

In a rare finding, one exchange explicitly assumes liability for unauthorized access and offers refunds under specific conditions, this is compared to 44 that disclaim liability. The remaining exchanges either consider the user liable for all activities regardless (37) or absolve liability depending on when the user reports the incident (15).

Unauthorized access is an indicator of porous operations. Notably, 41 out of 44 exchanges that disclaim liability for unauthorized access also disclaim liability for service performance. Therefore, these exchanges, aware of poor service performance, deny responsibility for any resulting consequential damages, such as unauthorized access caused by their failure to maintain reliable service.

Users Liable for Compensation. Not only do most exchanges disclaim their liability, but some exchanges will demand compensation from users. We find 3 exchanges to hold their users liable for up to $2 million for any breach of terms, determined solely at the exchange's discretion. An example clause states: *"Shall you breach this Agreement or any applicable law or administrative regulation,* ***you shall pay to us at least Two million US dollars in compensation*** *and bear all the expenses in connection with such breach (including attorney's fees, amongst others)."* Considering users often ignore T&Cs, do not fully understand them, nor have negotiating power [57, 81], this might be regarded as an unfair clause per the EU's Unfair Contract Terms Directive. Per the directive, this situation might be considered to be imposing a significant imbalance on the users' detriment, which can consequently be ground for considering the clause as unfair.

4.3.2. Accepting Liability

Only a minority claim to accept liability. However, this acceptance is not absolute and is highly conditioned to an extent that might make it impossible for a user to even challenge and win.

For instance, a minority accepts some liability during security incidents, particularly when attributed to their negligence, fraud, or fault, such as fund theft (7) or loss of user account control (11). Yet, users face challenges in proving such negligence, fraud, or fault due to limited means and access to evidence. Another 40 exchanges accept liability under general and vague conditions like "gross" breach of terms. However, exchanges' failure to address the burden of proof implies that users bear this burden from their perspective, which again poses significant challenges.

4.4. Results: Incident Management and Disclosure

This section examines how CASPs address platform abuse and security breaches. It considers the types of user conduct prohibited in their terms (EX Ante), the enforcement measures CASPs may take in response to violations (Ex Post), and the extent to which they notify users and disclose information following security breaches (which can result from platform abuse). Table 6 details the relevant practices.

4.4.1. Ex Ante Conduct Restrictions

Exchanges are often exploited by bad actors engaged in financial, organized, and cybercrime. The way in which an exchange governs and monitors its platform is central to ensuring user safety. MiCA requires CASPs to implement effective systems to deter and prevent activities like market abuse (MiCA, recital 81, art. 76(7)), money laundering and terrorist financing (MiCA, recital 77, art. 64(1)), and fraud (MiCA, art. 75(3)).

Our findings show that exchanges attempt to enforce control by prohibiting certain user activities; however, their vague rules and broad discretionary powers contribute to uncertainty for users.

Computer Crime. Exchange systems are frequent targets for malicious actors. Seventy-three exchanges prohibit acts threatening the confidentiality, integrity, or availability of their system, e.g. acts causing malfunction. Malicious attacks are explicitly prohibited by 31 exchanges, with some specifying forms like DDoS or malware. Furthermore, 33 exchanges prohibit conduct against users, which includes unauthorized access to, or facilitation of access to, user accounts.

Organized and Financial Crime. Exchanges are often exploited for organized and financial crime. In line with MiCA requirements, exchanges are required to adopt measures to prevent such misuse. Among the exchanges surveyed, 52 prohibit money laundering, 41 prohibit terrorist financing, and 45 prohibit fraud.

Despite these formal prohibitions, there is a disconnect between written terms and their actual effective enforcement. An example highlighting this gap is the world's largest exchange Binance. The exchange was found in violation of U.S. money laundering laws, which resulted in a record ($4.3*bn*) penalty and a short jail sentence for its CEO [82]. Furthermore, in 2022, Chainalysis reported that half of the $24*bn* in illicit transactions they identified were laundered through centralized exchanges [83].

Incident Management and Disclosure.

Checked Practice	MiCA/DORA Reference	Required?	Exchanges		Licensed		Collapsed	
			#	%	#	%	#	%
Ex Ante Conduct Restrictions								
Allow Account Access Control to 3^{rd} Party – Prohibit	–	(✓)	38	50.7	10	55.6	3	30
Account Only Used by User	–	(✓)	23	30.7	4	22.2	3	30
User Must Notify Exch Unauthorized Access	–	(✓)	57	76	11	61.1	10	100
Help/Gain Unauthorized Access - Prohibited	5, 6	✓	33	44	6	33.3	4	40
Violate Exch Computers - Prohibited	5, 6	✓	35	46.7	7	38.9	8	80
Scraping Website - Prohibited	5, 6	✓	17	22.7	4	22.2	3	30
Fraud - Prohibited	75.3	✓	45	60	16	88.9	6	60
Market Abuse - Prohibited	Recital(81), 76(7)	✓	34	45.3	7	38.9	5	50
Terrorist Financing - Prohibited	Recital(77), 64(1)	✓	41	54.7	10	55.6	5	50
Money Laundering - Prohibited	Recital(77), 64(1)	✓	52	69.3	12	66.7	6	60
Cryptocurrency Mixers - Prohibited	–	(✓)	3	4	1	5.6	0	0
Underground Markets - Prohibited	–	(✓)	3	4	1	5.6	0	0
Damaging Exchange's Interest - Prohibited	–	(✓)	47	62.7	11	61.1	6	60
Any Illegal Activity - Prohibited	–	(✓)	62	82.7	13	72.2	10	100
Ex Post Enforcement Measures: Direct Responses								
Account Control - Security Concern	68(7),11, 12	✓	24	32	5	27.8	4	40
Discontinue/Suspend Platform - Security Breach	68(7),11, 12	✓	7	9.33	1	5.6	0	0
Account Control - Platform Malfunction	68(7),11, 12	✓	8	10.7	1	5.6	2	20
Account Control - ToS/Law Violation	–	(✓)	59	78.7	12	66.7	9	90
Transaction Control - ToS/Law Violation	–	(✓)	48	64	13	72.2	4	40
Service Use Control - ToS/Law Violation	–	(✓)	44	58.7	9	50	9	90
Withhold Funds	–	(✓)	15	20	4	22.2	2	20
Ex Post Enforcement Measures: Indirect Responses								
Warn All	–	(✓)	3	4	0	0	1	10
Warn Violators	–	(✓)	2	2.67	0	0	1	10
Publish Violations	94(3)	✓	5	6.67	1	5.6	0	0
Delete Violations	94(3)	✓	15	20	3	16.7	3	30
Ex Post Engagement with Public Authorities								
Notify Authorities	–	(✓)	26	34.7	5	27.8	4	40
Response - Share Information	94(1), 94(3)	✓	37	49.3	7	38.9	6	60
Response - Freeze/Sequestrate Funds	94(1), 94(3)	✓	10	13.3	2	11.1	0	0
Response - Action on Account	94	✓	39	52	14	77.8	6	60
Will Not Inform of Cooperation	–	(✓)	14	18.7	3	16.7	1	10
Will Inform - Unless Prevented by Law	–	(✓)	4	5.33	2	11.1	0	0
Will Inform - Unless Security Reasons	–	(✓)	2	2.67	0	0	0	0
Best Security Measures	Recital(13),(45)	✓	41	54.7	11	61.1	4	40
Adhere to Standards and Laws	Recital(6)	✓	11	14.7	4	22.2	2	20
Ex Post Cyber Incident Notification								
Will Notify - Account Security Risk	14, 17, 19	✓	9	12	3	16.7	0	0
May Notify - Account Security Risk	–	(✓)	1	1.33	0	0	0	0
Will Notify - Platform Security Risk	14, 17, 19	✓	4	5.33	1	5.6	1	10
May Notify - Platform Security Risk	–	(✓)	2	2.67	0	0	0	0
Notify Public Channels	14, 17	✓	2	2.67	1	5.6	1	10
Notify Privately	14, 17	✓	4	5.33	4	22.2	0	0
Will Notify - Account Control - Security Reasons	19	✓	2	2.67	2	11.1	0	0
May Notify - Account Control - Security Reasons	–	(✓)	1	1.33	0	0	0	0

Table 6: Ex Ante/ex post incident management and disclosure practices.

These issues highlight that exchange exploitation may arise not only from users, but also from some exchanges themselves, whether through direct involvement, negligence, or facilitation. As an example, the BTCEX from our dataset, lacking a legal name and address, closed after the data collection period due to fraud allegations, this is despite its terms banning users from engaging in fraudulent activities [84]: *"11.1.6 you must not use the Website [...] in any way which is unlawful, illegal, fraudulent or harmful, or in connection with any unlawful, illegal, fraudulent or harmful purpose of activity."*

To this end, prohibiting certain activities on paper without corresponding enforcement renders such provisions moot. This highlights the necessity of exchanges to actively monitor their platforms and demonstrate a clear commitment to controlling this environment and sanctioning violators.

4.4.2. Ex Post Enforcement Measures: Responses to Terms Violations

It is unclear when CASPs are required to report illegal activity on their platforms. However, given a long history of facilitating criminal activity [63], we inspect the T&Cs for stated policies of countering abuse. Exchanges prioritize internal methods of control to respond to user violations over security incident response. However, they lack clear boundaries for violations. This grants discretionary power but creates uncertainty and potential unfairness for users who might be uninformed of true platform expectations. We outline primary and subsidiary response methods adopted internally and unilaterally by exchanges in the following situations:

Direct Enforcement Measures. Neither MiCA nor DORA provide detailed guidance on internal enforcement mechanisms, though they both implicitly require exchanges to address actions to maintain service integrity. In practice, exchanges employ a range of unilateral measures in response to a law breach or T&C violation. Our analysis shows that 59 exchanges reserve the right to suspend user accounts, 48 to control transactions, 44 to restrict service usage, and 15 to withhold users' funds. Such discretionary enforcement of terms raises concerns over contractual and procedural fairness, especially that in many cases, users are not given an explanation for these decisions or even the right to appeal.

Indirect Enforcement Measures. MiCA does cover subsidiary or indirect enforcement measures when user violations are observed, such as publishing or removing the recorded violations (MiCA, art. 94(3)). A small group of

exchanges implements these indirect responses, including the deletion (15) or publication (5) of violations.

However, we notice an absence of defined standards with both direct and indirect measures, which continues to pose risks. For instance, some fully terminate or indefinitely suspend an account upon unauthorized suspicions: *"we may temporarily or indefinitely freeze your account in the following cases: i. We detect unauthorized access to your account."* Yet, this is without clarifying whether "indefinitely" implies permanent or prolonged suspension. While full transparency may not be appropriate in every instance, for example, in cases involving fraudulent actors, it remains vital for protecting users from arbitrary enforcement of unclear terms and external harms.

Engagement with Public Authorities. Under MiCA, competent authorities have investigative powers to work with and enforce actions on CASPs. These include requesting information and documents, temporarily suspending services, and ordering the freezing or sequestration of funds (MiCA, arts. 94(1), 94(3)). Exchanges are expected to cooperate with such requests, with one-third of exchanges stating they will notify authorities of any law-violating or illegal activities. Around half of the exchanges state they will share user information upon request, and a similar proportion will comply with requests to freeze transactions. Finally, a minority acknowledge cooperation involving the transfer of user funds.

Current forms of collaboration with authorities could create severe consequences for users, particularly where allegations of abuse are mistaken or unsubstantiated. Such enforcement may result in the loss of funds or compromise user privacy. This, in consequence, affects the custodial relationship. For example, the terms of a surveyed exchange states: *"If in our sole discretion we believe that You are in breach of the above representation and undertaking, we may discretionarily or in coordination with local law enforcement authorities seize, restrict or close-out Your Account(s), fiat currency and digital assets."* In many cases, users are neither informed of these measures nor provided with avenues for remedy or appeal, regardless of fault. Most exchanges do not provide any clarification on this matter, which suggests users may not be informed when accounts are suspended or information is shared with authorities. Table 6 presents further detailed insights.

4.5. Ex Post Cyber Incident Notification

Following a significant ICT event (malicious or accidental) that affects users' interests, CASPs must inform impacted users and disclose the measures implemented in response (DORA art. 19(3)). CASPs must also maintain ICT response and recovery plans (MiCA, art. 68(7); DORA, arts. 11, 12), maintaining a timely response in the event of operational or security disruptions. Below, we outline when and how exchanges disclose breaches:

Breach Disclosure. DORA imposes obligations for crisis communication (DORA arts. 14, 17, 19), to ensure the responsible and prompt disclosure of events. In the conducted survey, terms discussed disclosure in two cases, first to affected users where individual accounts have been compromised, and second, broader platform-level compromises communicated to users, stakeholders, and media. Nine exchanges commit to notifying users of individual account breaches, while only four commit to disclosing broader security incidents; two more state they *may* do so.

Following an incident, exchanges must respond and take reactive measures such as temporary account suspension. However, only three exchanges commit to notifying affected users of such enforcement measures. Notably, the majority of exchange terms do not clarify whether users *will* or *may* be notified of such actions.

Notification Method. DORA requires CASPs to communicate (at least) major ICT incidents or client vulnerabilities via direct and public channels (DORA arts. 14,17). In the surveyed exchanges, four specify direct methods (e.g. email), while two provide for public announcements (e.g., social media).

Notification to Authorities. Additionally, DORA requires exchanges to report major ICT-related incidents to competent authorities. However, reporting of cyber threats is voluntary (DORA art. 1(a)).

The current examined exchange terms do not reflect this obligation. None of the surveyed exchanges explicitly commits to reporting to competent authorities, despite the growing importance of this mandate under the new regulatory regime.

5. Recommendations

This study offers a timely interdisciplinary analysis of centralized cryptocurrency exchanges, evaluated against the requirements set by MiCA and

DORA. Our findings reveal a substantial gap between existing self-regulatory practices and the new regulatory frameworks. Exchanges display varied adherence to fundamental practices, primarily in the management of assets and wallets, cybersecurity, and liability allocation. The lack of transparency regarding custodial arrangements and operational resilience strategies, not only exposes users and their assets to risks, but also undermines the objectives of regulatory interventions.

Furthermore, the extensive and widespread prevalence of liability disclaimers, often coupled with suboptimal operational practices, raises major concerns. Particularly, exchanges frequently use these disclaimers as legal shields to shift the burden onto users. These practices directly conflict with the principles of fairness and accountability articulated within MiCA. Although article 75(8) of MiCA stipulates liability provisions in the event of security incidents, the language is widely open to interpretation, and consequently, potential exploitation by exchanges.[8]

Lastly, our analysis indicates substantial weaknesses in incident response and disclosure protocols. Current noted practices often leave users uninformed about security breaches or operational disruptions, which amplifies market instability and user vulnerability.

Based on the issues detailed throughout this paper, we recommend that the following concerns be urgently addressed by EU regulators and exchanges.

5.1. Standardizing Corporate Wallet Management and Safety

Reliance on hot wallets, which are internet-connected wallets, exposes cryptocurrencies to significant cybersecurity threats, as hot wallets are inherently vulnerable to cyberattacks and unauthorized access.[9] To establish a good practice, regulations should mandate the use of a hybrid wallet combination of hot and cold storage solutions. Additionally, regulatory guidelines should impose a minimum threshold for the proportion of cryptocurrencies maintained in cold storage. This ensures a more secure and resilient custodial environment.

Furthermore, improper key management and governance practices can result in total loss of access to cryptocurrencies. As an example, the users of the exchange QuadrigaCX lost their funds due to the CEO's death, having

[8] *See* §4.3
[9] *See* §2.1.

been the sole possessor of the private keys [85]. Additionally, prior academic work and incidents demonstrated how susceptible exchanges are to hacks and theft, this is due to their porous security measures in safeguarding wallets [19, 32, 16, 11]. To avoid a single point of failure and enhance the overall resilience and trustworthiness of exchanges, regulatory frameworks should require robust internal control standards for secure wallet management. Practices can include multi-signature access protocols or clear key recovery mechanisms.

5.2. Standardizing Incident Disclosure Practices

Delayed or insufficient disclosure of security breaches by exchanges creates great uncertainty among their users. This lack of up-to-date transparency can lead to speculation about potential fraudulent activities, such as exit scams, and also the exploitation by cybercriminals who target anxious users through hybrid investment fraud or phishing attacks under the guise of assisting with fund recovery or access recovery [86, 64].

In such situations, regulators are recommended to impose clear and prompt incident disclosure requirements on exchanges following any security breach. For instance, mandatory notification to users, combined with transparent communication protocols, could mitigate market uncertainty; this can also reduce users' susceptibility to phishing attacks and enhance their confidence in the exchange.

5.3. Careful Consideration of Omnibus Accounts

MiCA only mandates exchanges to segregate users' funds from the exchange's proprietary assets, but does not require exchanges to segregate individual user accounts from one another, as they are kept in omnibus accounts. Therefore, as discussed in §4.2.2, the widespread use of omnibus accounts poses significant risks as it exposes users collectively to potential losses in the event of security incidents and insolvency. Consequently, the permissibility of omnibus accounts might be something to be reconsidered by regulators.

5.4. Clarity on MiCA's Definition of "Liability" Due to Security Incidents

Under MiCA regulation, exchanges are liable for the loss of funds or means of access due to incidents attributable to them, yet the definition of

an "incident" is ambiguous (MiCA, art. 75(8)).[10] This creates opportunities for exchanges to evade liability by categorizing incidents, including security breaches, as incidents not under their control, hence not attributed to them. Consequently, regulators are recommended to clarify the definition and scope of "incident" within MiCA. Moreover, guidelines must restrict the conditions under which exchanges may invoke exemptions such as force majeure for security incidents. This ensures that liability for asset loss remains effective, and exchanges are responsible for custodial duties in case of security incidents.

5.5. Limiting the Discretionary Power of Exchanges

Exchanges currently possess broad and excessive discretionary power in enforcing their rules on users, allowing them to freeze, seize, or terminate accounts without clear justification or effective routes for challenge. Not communicating with users about specific consequences of violating terms leaves users vulnerable to arbitrary or unjustified actions. Consequently, it is recommended that regulators establish standardized enforcement procedures that limit exchanges' discretionary powers and require transparent and timely communication about the enforcement of their T&Cs. This also includes ensuring users have the right to challenge unwarranted decisions.

6. Conclusion

This paper presented the first comprehensive legal and empirical analysis of centralized cryptocurrency exchanges operating in Europe, assessing their self-regulatory practices against the requirements stated in the EU's recent MiCA and DORA. By systematically extracting compliance benchmarks from these regulations and analyzing the terms and conditions, security policies, and custodial practices of 75 exchanges, this study, not only proposed a new interdisciplinary methodology that can be leveraged by other research studying emerging self-regulatory technologies, but also mapped current industry practices and highlighted major caps in regulatory alignment.

The study indicates that despite public assurances of robust and secure governance, exchanges' actual operational practices fall short of the regulatory standards recently enacted by the EU. In particular, having weak cybersecurity resilience, inadequate asset segregation, using liability disclaimers

[10] *See* §4.3

as legal shields and as an approach to neglect security measures, and finally, ambiguous contractual terms. Such practices leave users exposed to substantial risk. These discrepancies suggest that the industry's prolonged self-regulatory mechanisms alone are not sufficient, which will necessitate extensive work from both regulatory and industry actors to come fully into compliance.

Future efforts should also prioritize bringing standardization to the industry. Particularly, more detailed and enforceable security measures regarding wallet management are needed, as well as reconsidering liability provisions in case of security breaches, as current practices will shift liability on users, which will affect the overall custodial relationship basis.

Finally, this work also aims to enhance the accessibility of legal documents by presenting legal information in a more user-friendly and comprehensive format. By doing so, it assists individuals to make more informed decisions regarding their legal rights and obligations. This accessibility also provides researchers in adjacent disciplines, such as computer science, public policy, and economics, the ability to investigate further issues in the field, mandating interdisciplinary investigations and solutions.

References

[1] I. H. Chiu, Regulating the Crypto Economy, Hart Publishing, 2021.

[2] Chainalysis, Cryptocurrency exchanges in 2021: A competitive landscape analysis (2021).
URL https://go.chainalysis.com/2021-crypto-exchange-landscape-report.html

[3] Coinbase, Can crypto really replace your bank account? (2025).
URL https://www.coinbase.com/en-gb/learn/crypto-basics/can-crypto-really-replace-your-bank

[4] R. Anderson, I. Shumailov, M. Ahmed, A. Rietmann, Bitcoin redux, Workshop on the Economics of Information Security (2018).
URL https://weis2021.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_38.pdf

[5] H. Nabilou, The dark side of licensing cryptocurrency exchanges as payment institutions, Law and Financial Markets Review 14 (1) (2020) 39–47.

[6] A. Tripathi, A. Choudhary, S. K. Arora, G. Arora, G. Shakya, B. Rajwanshi, Crypto bank: Cryptocurrency wallet based on blockchain, in: International Conference on Recent Trends in Image Processing and Pattern Recognition, Springer, 2023, pp. 223–236.

[7] M. Ordekian, I. Becker, M. Vasek, Shaping cryptocurrency gatekeepers with a regulatory 'trial and error', in: Financial Cryptography and Data Security: FC 2023 Workshops, The 4th Workshop on Coordination of Decentralized Finance, CoDecFin, Croatia, Springer Nature Switzerland, Cham, 2023, pp. 113–132.

[8] A. Ferreira, P. Sandner, Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure, Computer Law & Security Review 43 (2021) 105632.

[9] C. Decker, R. Wattenhofer, Bitcoin transaction malleability and Mt-Gox, in: 19th European Symposium on Research in Computer Security, Springer, 2014, pp. 313–326.

[10] M. Vasek, M. Thornton, T. Moore, Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem, in: Bitcoin Workshop, Springer, 2014, pp. 57–71.

[11] A. Feder, N. Gandal, J. Hamrick, T. Moore, The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox, Journal of Cybersecurity 3 (2) (2017) 137–144.

[12] M. Haentjens, T. De Graaf, I. Kokorin, The failed hopes of disintermediation: Crypto-custodian insolvency, legal risks and howto avoid them, Singapore Journal of Legal Studies (2020) 526–563.

[13] D. Z. Morris, 8 days in november: What led to ftx's sudden collapse (2022).
URL `https://www.coindesk.com/layer2/2022/11/09/8-days-in-november-what-led-to-ftxs-sudden-collapse/`

[14] I. Kokorin, The anatomy of crypto failures and investor protection under micar, Capital Markets Law Journal 18 (4) (2023) 500–525.

[15] C. Wronka, Crypto-asset activities and markets in the european union: issues, challenges and considerations for regulation, supervision and oversight, Journal of Banking Regulation 25 (1) (2024) 84–93.

[16] A. Mukherjee, T. Moore, Cryptocurrency exchange closure revisited (again), in: 2022 APWG Symposium on Electronic Crime Research (eCrime), IEEE, 2022, pp. 1–8. doi:10.1109/eCrime57793.2022.10142141.

[17] D. W. Arner, T. Ratna, S. Animashaun, J. Bedi, N. Mishra, Centralization in decentralized finance: Systemic risk in the crypto ecosystem and crypto's future as a regulated industray, Law and Contemporary Problems 87 (2) (2025) 185–210.

[18] R. Anderson, T. Moore, The economics of information security, Science 314 (5799) (2006) 610–613.

[19] P. McCorry, M. Möser, S. T. Ali, Why preventing a cryptocurrency exchange heist isn't good enough, in: Security Protocols Workshop, Springer, 2018, pp. 225–233.

[20] European Union, Regulation (EU) 2023/1114 of the european parliament and of the council of 31 may 2023 on markets in crypto-assets, and amending regulations (EU) no 1093/2010 and (EU) no 1095/2010 and directives 2013/36/EU and (EU) 2019/1937. OJ L 150/40 (2023).

[21] European Union, Regulation (EU) 2022/2554 of the european parliament and of the council of 14 december 2022 on digital operational resilience for the financial sector and amending regulations (EC) no 1060/2009, (EU) no 648/2012, (EU) no 600/2014, (EU) no 909/2014 and (EU) 2016/1011. OJ L 333/1 (2022).

[22] D. Clausmeier, Regulation of the european parliament and the council on digital operational resilience for the financial sector (dora), International Cybersecurity Law Review 4 (1) (2023) 79–90.

[23] ESMA, List of grandfathering periods decided by member states under article 143 of regulation (EU) 2023/1114 Markets in Crypto-Assets Regulation (MiCA) (2024).
URL https://www.esma.europa.eu/sites/default/files/2024-12/List_of_MiCA_grandfathering_periods_art._143_3.pdf

[24] T. Barbereau, B. Bodó, Beyond financial regulation of crypto-asset wallet software: In search of secondary liability, Computer Law & Security Review 49 (2023) 105829.

[25] A. J. Levitin, Not your keys, not your coins: Unpriced credit risk in cryptocurrency, Texas Law Review 101 (2022).

[26] S. Houy, P. Schmid, A. Bartel, Security aspects of cryptocurrency wallets—a systematic literature review, ACM Computing Surveys 56 (1) (2023) 1–31.

[27] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten, Sok: Research perspectives and challenges for bitcoin and cryptocurrencies, in: 2015 IEEE symposium on security and privacy, IEEE, 2015, pp. 104–121.

[28] M. Ordekian, I. Chiu, Asset vulnerability for customers of crypto-exchanges: In need of a regulatory solution and the limitations of mica, forthcoming (2025]).

[29] S. Nakamoto, Bitcoin whitepaper (2008).
URL `https://bitcoin.org/bitcoin.pdf`

[30] D. Vidal-Tomás, A. Briola, T. Aste, Ftx's downfall and binance's consolidation: The fragility of centralised digital finance, Physica A: Statistical Mechanics and Its Applications 625 (2023) 129044.

[31] T. Moore, N. Christin, Beware the middleman: Empirical analysis of Bitcoin-exchange risk, in: Financial Cryptography and Data Security, Springer, 2013, pp. 25–33.

[32] T. Moore, N. Christin, J. Szurdi, Revisiting the risks of bitcoin currency exchange closure, ACM Transactions on Internet Technology 18 (4) (2018) 50:1–50:18.

[33] E. Musa, Record breaking $11.3 trillion high for spot and derivatives trading on centralized crypto exchanges (2025).
URL `https://news.bitcoin.com/record-breaking-11-3-trillion-high-for-spot-and-`

[34] S. P. Lee, Crypto trading volumes reached $18.83t in 2024, still below 2021's $25.21t peak (2025).

URL https://www.coingecko.com/research/publications/largest-centralized-crypto-exchanges

[35] Chainalysis, The chainalysis 2025 crypto crime report (2025).
URL https://go.chainalysis.com/2025-Crypto-Crime-Report.html

[36] Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan, Phishing attacks: A recent comprehensive study and a new anatomy, Frontiers in Computer Science 3 (2021) 563060.

[37] M. Ordekian, G. Atondo-Siu, A. Hutchings, M. Vasek, Investigating wrench attacks: Physical attacks targeting cryptocurrency users, in: 6th Conference on Advances in Financial Technologies (AFT 2024), Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024, pp. 24–1.

[38] Coinbase, Protecting our customers - standing up to extortionists (2025).
URL https://www.coinbase.com/en-gb/blog/protecting-our-customers-standing-up-to-extortionists

[39] N. Gandal, J. Hamrick, T. Oberman, T. Moore, Price manipulation in the bitcoin ecosystem, Journal of Monetary Economics 95 (2018) 86–96.

[40] D. W. Arner, D. A. Zetzsche, R. P. Buckley, J. M. Kirkwood, The financialisation of crypto: Designing an international regulatory consensus, Computer Law & Security Review 53 (2024) 105970.

[41] E. Akyildirim, T. Conlon, S. Corbet, J. W. Goodell, Understanding the ftx exchange collapse: A dynamic connectedness approach, Finance Research Letters 53 (2023) 103643.

[42] E. Bouri, E. Kamal, H. Kinateder, Ftx collapse and systemic risk spillovers from ftx token to major cryptocurrencies, Finance Research Letters 56 (2023) 104099.

[43] P. De Filippi, Bitcoin: a regulatory nightmare to a libertarian dream, Internet Policy Review 3 (2) (2014).

[44] Malta, Virtual Financial Assets Act (Nov. 2018).
URL https://legislation.mt/eli/cap/590/eng/pdf

[45] UAE, Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (Feb. 2022).
URL https://rulebooks.vara.ae/rulebook/law-no-4-2022-regulating-virtual-assets-emirate-dubai

[46] M. Cappai, The role of private and public regulation in the case study of crypto-assets: The italian move towards participatory regulation, Computer Law & Security Review 49 (2023) 105831.

[47] J. B. Earp, A. I. Antón, L. Aiman-Smith, W. H. Stufflebeam, Examining internet privacy policies within the context of user privacy values, IEEE Transactions on Engineering Management 52 (2) (2005) 227–237.

[48] N. S. Kim, Wrap contracts: Foundations and ramifications, Oxford University Press, 2013.

[49] A. I. Antón, J. B. Earp, Q. He, W. Stufflebeam, D. Bolchini, C. Jensen, Financial privacy policies and the need for standardization, IEEE Security & Privacy 2 (2) (2004) 36–45.

[50] C. Jensen, C. Potts, Privacy policies as decision-making tools: an evaluation of online privacy notices, in: Proceedings of the SIGCHI conference on Human Factors in Computing Systems, 2004, pp. 471–478.

[51] M. W. Vail, J. B. Earp, A. I. Antón, An empirical study of consumer perceptions and comprehension of web site privacy policies, IEEE Transactions on Engineering Management 55 (3) (2008) 442–454.

[52] T. Ermakova, A. Baumann, B. Fabian, H. Krasnova, Privacy policies and users' trust: does readability matter?, in: Americas Conference on Information Systems (AMCIS), 2014.
URL https://core.ac.uk/download/pdf/301361898.pdf

[53] J. J. Prichard, M. B. Hayden, Assessing the readability of freeware end-user licensing agreements, Issues in Information Systems 9 (2) (2008) 452–459.
URL https://iacis.org/iis/2008/S2008_1071.pdf

[54] A. M. McDonald, L. F. Cranor, The cost of reading privacy policies, I/S: A Journal of Law and Policy for the Information Society 4 (2008) 543.

[55] A. M. McDonald, R. W. Reeder, P. G. Kelley, L. F. Cranor, A comparative study of online privacy policies and formats, in: Privacy Enhancing Technologies, Springer, 2009, pp. 37–55.

[56] D. B. Meinert, D. K. Peterson, J. R. Criswell, M. D. Crossland, Privacy policy statements and consumer willingness to provide personal information, Journal of Electronic Commerce in Organizations (JECO) 4 (1) (2006).

[57] N. Steinfeld, "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment, Computers in human behavior 55 (2016) 992–1000.

[58] European Union, Council directive 93/13/eec of 5 april 1993 on unfair terms in consumer contracts. OJ L 95/29 (1993).

[59] H. Schulte-Nölke, The objectives of directive 93/13/eec on unfair contract terms: An overview after 30 years of case law, European Review of Private Law 32 (3) (2024).

[60] Coinmarketcap (2023). [link].
URL `https://coinmarketcap.com/`

[61] CoinGecko (2023). [link].
URL `https://www.coingecko.com/en/`

[62] J. Fereday, E. Muir-Cochrane, Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development, International journal of qualitative methods 5 (1) (2006) 80–92.

[63] Chainalysis, The chainalysis 2024 crypto crime report (2024).
URL `https://go.chainalysis.com/crypto-crime-2024.html`

[64] M. Ordekian, A. Papasavva, E. Mariconti, M. Vasek, A sinister fattening: Dissecting the tales of pig butchering and other cryptocurrency scams, in: 2024 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2024, pp. 136–148.

[65] M.-H. Maras, E. R. Ives, Deconstructing a form of hybrid investment fraud: Examining 'pig butchering' in the united states, Journal of Economic Criminology 5 (2024) 100066.

[66] ESMA, Crypto assets: Market structures and EU relevance (2024).
URL https://www.esma.europa.eu/sites/default/files/2024-04/ESMA50-524821-3153_risk_article_crypto_assets_market_structures_and_eu_relevance.pdf

[67] BBC, Binance exits netherlands and faces france probe (2023).
URL https://www.bbc.co.uk/news/business-65935263

[68] K. Oosthoek, C. Doerr, From hodl to heist: Analysis of cyber security threats to bitcoin exchanges, in: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2020, pp. 1–9.

[69] L. Ankne, What's so different about cryptocurrency exchanges? (2019).
URL https://www.forbes.com/sites/leslieankney/2019/01/04/whats-so-different-about-cryptocurrency-exchanges/

[70] H. Partz, Bitgrail's founder contributed to $150m loss, Italian authorities allege (2020).
URL https://cointelegraph.com/news/bitgrail-s-founder-contributed-to-150m-loss-italian-authorities-allege

[71] T. Nagase, T. Tanaka, T. Fukui, Blockchain & cryptocurrency laws and regulations 2023 japan (2023).
URL https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/japan

[72] P. Tortorelli, K. Rooney, Sam Bankman-Fried's Alameda quietly used FTX customer funds for trading, say sources (2022).
URL https://www.cnbc.com/2022/11/13/sam-bankman-frieds-alameda-quietly-used-ftx-customer-funds-without-raising-al
html

[73] United States Commodity Futures Trading Commission, CFTC obtains $12.7 billion judgment against FTX and Alameda (2024).
URL https://www.cftc.gov/PressRoom/PressReleases/8938-24

[74] D. D. United States Bankruptcy Court, First interim report of John J. Ray III to the independent directors on control failures at the FTX exchanges (2023).
URL https://www.courtlistener.com/docket/65748821/1242/1/ftx-trading-ltd/

[75] M. A. Yahya, N. Pecharsky, Crypto-Litigation: An empirical overview for 2020-present, SMU Science & Technology Law Review 25 (2022) 195.

[76] S. Witley, Crypto hack lawsuits rise as theft victims try untested claims (2023).
URL https://news.bloomberglaw.com/privacy-and-data-security/crypto-hack-lawsuits-rise-as-theft-victims-try-unte

[77] T. Meshel, M. A. Yahya, Crypto dispute resolution: an empirical study, University of Illinois Journal of Law, Technology and Policy (2021) 187.

[78] F. Ghodoosi, Crypto litigation: An empirical view, Yale Journal on Regulation 40 (2022) 87–100.
URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4288024

[79] J. A. Lanz, Exit scam? Bitcoin exchange BitForex shutters after $57m mysteriously withdrawn (2024).
URL https://decrypt.co/219012/exit-scam-bitforex-shutters-after-57-million-wi

[80] E. O'Dell, Compensation for breach of the general data protection regulation, Dublin University Law Journal 40 (2017) 97.

[81] A. Kitkowska, J. Högberg, E. Wästlund, Online terms and conditions: Improving user engagement, awareness, and satisfaction through ui design, in: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, 2022, pp. 1–22.

[82] United States Department of Justice, Binance and CEO plead guilty to federal charges in $4b resolution (2023).
URL https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

[83] Chainalysis, The chainalysis 2023 crypto crime report (2023).
URL https://go.chainalysis.com/2023-crypto-crime-report.html

[84] Coinotag News, Crypto exchange btcex shuts down amidst fraud allegations: What's next? (2023).
URL https://coinmarketcap.com/community/articles/6494588dface9415894625cb/

[85] N. De, 'Request for Exhumation': QuadrigaCX creditors ask for proof that cotten is dead (2019).
URL https://www.coindesk.com/markets/2019/12/13/request-for-exhumation-quadrigacx-creditors-ask-for-proof-that-cotten-is-dead

[86] A. Khatri, Defi100 claims website hack after allegations of exit scam (2021).
URL https://cryptodaily.co.uk/2021/05/defi100-scam-update

Appendix A.

Exchange Selection	Total
Initial exchange dataset	138
Duplicates	8
Not in English	14
Exchange is dead or inaccessible	8
Non-European currencies	18
Non-fiat dealing exchange	11
Decentralized exchange	2
No terms and conditions	5
Included set of exchanges	75
Analyzed exchange documents and information webpages	143
Terms and conditions documents	75
Security policy documents (and webpages)	28
License documents (and webpages)	10
General legal information webpages	20
Law enforcement dedicated page	10

Table A.7: Exchange dataset selection criteria and a description of used documents.

	Initial Codebook	Final Codebook
Categories	14	4
Subcategories	60	23
Codes	371	163

Table A.8: Initial vs. final state of the codebook.

Appendix B. List of Exchanges Considered

AAX
B2BX
Biconomy
Binance
Binance TR
BIT.TEAM
Bitay
Bitci
BITEXBOOK
Bitexen
Bitfinex
bitFlyer
Bitget
BitGlobal
Bitinka.com
BitMart
Bitonic
Bitpanda Pro
Bitrue
Bitstamp
Bittylicious
Bitubu Exchange
Bitvavo
Blockchain.com
BTC-Alpha
BTCEX
BtcTurk PRO
BTSE
BTX
CEX.IO
Coinbase Exchange
CoinCasso
CoinCorner
Coinfalcon
CoinJar Exchange
CoinMate
Coinmetro
Coinsbit
Coinstore
CoinW
Cryptology
Cryptonex
Currency.com
DigiFinex
Emirex
eToro
ExMarkets
EXMO
FTX EU
Gate.io
Globitex
HitBTC
Huobi Global
Kanga
KickEX
Kraken
KuCoin
Kuna
Latoken
Liquid
LiteBit
Luno
Lykke
MEXC Global
Okcoin
OKX
Paymium
Polyx
Purcow
The Rock Trading
Tokpie
WhiteBIT
XT.COM
ZBX
Zonda