The Risks and Regulation of Decentralized Finance

A Recommendation to Policy Makers

MSc Graduation Project

Abdulkhamid Mukhamedov

Delft University of Technology

TU Delft

The Risks and Regulation of Decentralized Finance

A Recommendation to Policy Makers

A Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of
Master of Science
and
to be publicly defended on August 30th, 2022

by

Abdulkhamid Mukhamedov

Engineering & Policy Analysis
Spec: Emerging Technology-Based Innovation & Entrepreneurship
Faculty of Technology, Policy and Management

Chair: Prof. Dr. Michel van Eeten
First Supervisor: Dr. Jolien Ubacht
First Advisor: Dr. Yury Zhauniarovich
Second Advisor: Dr. Sélinde van Engelenburg
EY Supervisor: Vanessa Simões de Azevedo
Project Duration: March, 2022 - August, 2022
Faculty: Technology, Policy and Management, Delft

Cover: Jeremy Bezanger, Unsplash

TU Delft

Preface

For someone who is very interested in technological trends and socio-political problems, writing this thesis on the risks and regulation of Decentralized Finance has been a highly rewarding experience. Since 2017, I have been closely following the crypto space and observing the emergence of peer-to-peer financial systems all around the globe. In December 2021, I attended the three-day Blockchance conference in Hamburg where I listened to dozens of industry leaders present the latest developments and discuss the latest trends in the blockchain industry. As various tech CEOs, developers and start-up founders were discussing the crazy innovations and novel products they are working on, I could not help but think about the societal implications of these creations. Play-to-earn gaming, digital sovereign identities, create-to-earn open-source social media platforms, decentralized gambling, blockchain-based cities, economies and virtual realities were just some of the mind-breaking conversations that took place at this conference. While it may at first sound unrealistic, there are thousands of people with very extensive resources working every day to make these things a reality. With mostly just the private sector being present during the conference (besides the government of El Salvador who famously adopted Bitcoin as a legal tender) there was no discussion about regulation or policy, or about any risks of the presented technologies as a matter of fact. Unfortunately, there were no speakers or identifiable visitors from the European Commission, or any other European government, indicating that there are still many bridges to be built in this industry. If effective regulation is to be introduced to this space to create a safe and fair environment for everybody, there must be many more points of contact between the creators and the regulators, especially at conferences of this scale.

The academic work on regulation of crypto-markets is just taking off and I am very glad to have written one of the few academic reports about the MiCA framework, and the first one focusing on the risks and industry perceptions. This would not have been possible without the close supervision and support of my graduation committee. Firstly, I would like to thank Michel van Eeten for chairing this committee and helping me navigate through this research, and Jolien Ubacht for giving me valuable advice and encouragement throughout the process. Moreover, I would like to thank my advisor Yury Zhauniarovich for close cooperation, technical help, advice and efforts in finding interviewees for the research. Also, I would like to thank my second advisor, Sélinde van Engelenburg, for advising me on the direction of my research and brainstorming with me during the challenges in the initial phases of my work. Furthermore, I would like to extend my gratitude to EY Netherlands for providing me with the resources and necessary support to conduct this research, especially to Vanessa Simões de Azevedo for close mentorship, encouragement, feedback and advice throughout the process, and Rudrani Djawalapersad for encouraging me to pursue this topic. I would like to also thank all my colleagues at EY for the great internship and valuable help during the project. Furthermore, I am very thankful to the content contributors listed on the following page for their input and knowledge contributions that helped realize this research. Last but not least, I would like to thank my dear family and friends for the invaluable support system they provided me with during this time.

Abdulkhamid Mukhamedov
Tashkent, August 2022

Content Contributors

We would like to extend our gratitude for the content contributors who helped realize this project by sharing their knowledge, resources and expertise:

Andrea Berutto, Founder and Consultant at Karuna Ethical Blockchain Advisory
Andrea Pantaleo, Lead Lawyer at DLA Piper
Baris Yakali, Founder and CEO at BEY Trading
Bernard Kaplanian, Founder and CEO Cryptocurrency Consulting Munich
David Kurze, Sales Project Manager at BörseGo AG
Dimitriy Remerov, Product Manager at Unslashed Finance
Eric Groothedde, Digital Assets Strategy Lead at ING
Jesse Baas, Senior Bot Creator Retention Specialist at BOTS
Jim Rusagara, EMEIA Financial Services Regulation and Public Policy Manager at EY
Jürg Baltensperger, Managing Director at JayBee AG
Lasse Meholm, CEO and Head Consultant at Finansit
Mikel Ayala, Chief Growth Officer at Atani
Simon Polrot, President at European Crypto Initiative
Timothee Bissessar, Manager Digital Assets at EY
Willem Röell, Lawyer at De Roos Advocaten
Willem-Jan Smits, Lawyer and Co-Founder at Watson Law

Disclaimer: The text presented in this report does not reflect the views and opinions of the content contributors and companies listed on this page, but solely of the main author.

Abstract

In the past several years, financial applications of the blockchain technology experienced significant growth, development and adoption among the public and institutional investors. With the rise of stablecoins and major events such as the announcement of Facebook's own cryptocurrency Libra in 2019, the EU regulators felt the urgent need to address the digital currencies that may pose financial and security risks if left unsupervised. In 2020, the European Commission introduced the Markets in Crypto-Assets (MiCA) framework to regulate the crypto-asset issuers and service providers located in the EU or serving EU clients from abroad. One of the regulation's objectives is to address the risks of the crypto-markets while leveraging its benefits, yet there has been no evaluation of the proposed regulation besides the Commission's own impact assessment.

Thus, this research offers an evaluation of the MiCA framework by adopting World Economic Forum's DeFi Whitepaper risk framework and interviews with the industry experts to generate both qualitative and quantitative data that is used to construct policy considerations for future amendments. By conducting interviews with 8 legal experts, the study provides insights into the strengths and weaknesses of the MiCA framework, while the interviews with 2 respondents from crypto-asset issuer entities, 6 from crypto-asset service providers entities and 3 from institutional investors entities provided further insights into the perceptions of the industry participants on the EU crypto regulation. Moreover, the study presents the risk perceptions of each respondent groups as during the interview rounds the participants were presented 18 risks of DeFi and were asked to select the most 5 critical risks perceived by them. This information is used to reveal what risks are perceived by each group. Lastly, the study presents a content analysis to assess the extent to which the 18 risks ranked by the interviewees are addressed in the MiCA framework. In summary, the results of the study suggest many points of improvement to the MiCA framework with respect to definitions, scoping, classifications and the regulatory approach. Moreover, the results suggest that the policy makers should focus on the unaddressed risks in the future amendments and policies, most importantly on technical and operational risks that have been left out from the framework.

Contents

Nomenclature

Abbreviation	Definition
AML	Anti-Money Laundering
BTC	Bitcoin
CASP	Crypto-Asset Service Provider
CBDC	Central Bank Digital Currency
CeFi	Centralized Finance
CFT	Countering Financing of Terrorism
DAO	Decentralized Autonomous Organizations
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DLT	Distributed Ledger Technology
DORA	Digitial Operational Resilience Act
EBA	European Banking Authority
EPA	Engineering and Policy Analysis
EC	European Commission
ESMA	European Securities Market Authority
ETH	Ethereum
EU	European Union
FinTech	Financial Technology
FSCS	Financial Services Compensation Scheme
G7	The Group of Seven
GDP	Gross Domestic Product
MiCA	Markets in Crypto-Assets
MiFID	Markets in Financial Instruments Directive
NFT	Non-Fungible Tokens
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
POS	Proof-of-Stake
POW	Proof-of-Work
WEF	World Economic Forum

1

Introduction

In June 2019, Facebook revealed the news about the so-called Libra Association, a worldwide digital currency project built on the blockchain infrastructure created by the social media conglomerate itself. As stated by its association, the goal of the Libra currency was to provide *"a simple global currency and financial infrastructure that empowers billions of people"* (The Libra Association, 2019). Libra was meant to be a stablecoin, meaning it would be a cryptocurrency which maintains its value by being pegged to a number of currencies, and was planned to be backed by a real asset reserve (referred to as Libra Reserve in the whitepaper). The Libra Association, an independent centralized institution, would be the governing body of the peer-to-peer electronic currency system upon its intended 2020 launch.

Naturally, this announcement attracted mixed responses among the public and regulators. While the advocates and supporters highlighted the benefits of the technological efficiency of Libra and potential economic inclusivity it may bring, the critics voiced concerns about Libra's ability to destabilize the global financial system (Groß et al., 2019). In 2019, Facebook had around 2.4 billion active monthly users, all of whom could be the potential users of the Libra currency (Bilotta & Botti, 2019). At that time, the company already had significant experience in providing financial services and constructed relationships with financial institutions due to its provision of payment services on Facebook Messenger. At several billion potential users, Libra's private money could pose a competitive risk to the financial sovereignty of entire countries and contribute to the denationalization of money by overcoming politics and the traditional credit system (Friedrich, 1983). Considering Libra's potential of rapidly reaching a disruptive scale, regulators and politicians around the globe did not hesitate to call for monitoring and regulatory action (Bilotta & Botti, 2019).

Within just two weeks of Libra's announcement, some of the major banks and regulators around the world, such as the Bank of England, US Federal Reserve and Bank of France, communicated that they would be closely inspecting Libra and introducing heavy regulations, while The European Central Bank (ECB) led a critical discussion on the evaluation of risks posed by digital currencies together with the Group of Seven (G7) states (Zetzsche et al., 2021). In 2020, the European Commission published the first draft of the Markets in Crypto-Assets Framework (MiCA) 2020/0265 (COD), which for the first time outlined rules and standards for crypto-markets and its participants (European Commission, 2020a). On the second page of the document, in the section *Context of the Proposal*, subsection *Reasons for and objectives of the proposal*, MiCA makes a statement about the risks coming with the rise of digital currencies launched by the private sector:

"A relatively new subset of crypto-assets – the so-called 'stablecoins' – has recently emerged and attracted the attention of both the public and regulators around the world. While the crypto-asset market remains modest in size and does not currently pose a threat to financial stability, this may change with the advent of 'global stablecoins', which seek wider adoption by incorporating features aimed at stabilising their value and by exploiting the network effects stemming from the firms promoting these assets."

While Libra is not explicitly mentioned in the MiCA framework, it is clear from this quote that the EU regulators' concerns over digital stablecoins stem from the attempts of the Big Tech and other private corporations to enter the financial markets. The reason for policy-makers' concerns is not just Facebook, as in 2019 Telegram announced its decentralized cryptocurrency Gram (Chin, 2020) and Walmart attempted to patent its stablecoin Walmart's Units (Huillet, 2019). While these digital currencies never saw actually the light of day, other stablecoins such as USD Tether, USD Coin, Binance USD and dozens of others have a market capitalization of over 150 billion USD as of August 2022, a dramatic increase from 3 billion in 2019 (CoinGecko, 2022). At such growth rate, it becomes clear why the regulators are concerned with market integrity, governance policies, reserve management. Unfortunately, the existing financial regulations in the European Union, mainly Markets in Financial Instruments Directive II (MiFID II, Directive 2014/65/EU) were challenging to apply to crypto-markets due to lack of clarity with respect to what falls under the definition of financial instruments and how market integrity rules would apply in crypto-markets (European Commission, 2020a). Thus, the MiCA framework aims to solve the issue by directly targeting crypto-assets such as stablecoins (referred to as asset-referenced tokens and e-money tokens in the framework) and introducing market integrity rules specific to markets dealing in crypto-assets and -services.

This report aims to construct advice for the EU policy makers on the Markets in Crypto-Assets framework by carrying out a policy evaluation focused on risks and industry perceptions. The evaluation of MiCA is performed by conducting interviews with 19 industry experts from various backgrounds and expertise to understand the shortcomings of the current policy and regulatory approach, as well as to assess whether MiCA addresses the risks of crypto-assets and -services perceived by the stakeholders. Thus, the main research question answered in this study is *"What are the policy considerations that EU policy makers could take into account in the future amendments of the MiCA framework and regulatory developments in the EU's crypto-markets?"*.

In Chapter 2, the reader is presented with the background information and problem analysis that identifies research gaps and translates it into the research objective and research questions. Chapter 3 presents the research methodology and explains how interviews are used to carry out the evaluation. In Chapter 4, the perceptions of the legal experts on the MiCA framework are presented and followed by the perceptions of crypto-asset issuers, CASPs and institutional investors on the need for regulation and the regulatory approach. Chapter 4 highlights the shortcomings of the MiCA policy from the perspective of the interviewees and provides valuable insight into the potential improvements the regulators can adopt in the current regulatory approach. Chapter 5 presents the World Economic Forum risk framework and how these risks were ranked in criticality during the interview rounds. Chapter 6 describes the summative content analysis to assess the extent to which the risks identified in this study are addressed in the framework. Finally, Chapter 7 presents the conclusion of the research, limitations, further research, EPA relevance and academic contributions.

2

Problem Analysis

2.1. Summary of the Chapter

This chapter presents the problem analysis of the research by providing the necessary background information on the relevant concepts, MiCA regulation and system. Moreover, the chapter presents the research gap addressed by the study which is translated into the research objective, which is *"to provide an evaluation of the MiCA framework by investigating the perceptions of the industry experts and performing a content analysis of the policy to assess what and whose risks are addressed by the EU policy makers"*. The research questions used to achieve this objective and research diagram are also presented in this chapter

Section 2.2 provides a brief introduction to Decentralized Finance and its application in the financial sector. In Section 2.3, an overview and general description of the MiCA framework is provided, followed by an actor analysis in Section 2.4. The knowledge gaps, resulting problem statement and the research objective are presented in Sections 2.5 and 2.6 respectively. Lastly, the research questions are presented and described in Section 2.7 and the research diagram is visualized and explained in Section 2.8.

2.2. Introduction to Decentralized Finance

In 2008, an author under the pseudonym Satoshi Nakamoto published a white paper called *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008). Bitcoin was the first example of the distributed cryptocurrency that has made the basis for the rapid development of the area in the next decades. The blockchain, or Distributed Ledger Technology (DLT), presents an application of hash functions that generate blocks on the chain to verify and execute transactions.

The technology was initially proposed for finance and cryptocurrency applications as it allows users to bypass intermediaries and centralized institutions such as banks, lawyers, etc. and provides security as well as confidentiality to the user (Radanović & Likić, 2018). Today, blockchain has come a long way in its development and is currently in its fourth generation phase. Known as Blockchain 4.0, the latest technology specializes in public ledger and distributed real-time databases, allowing it to be applied in Industry 4.0 via use of smart contracts and consensus mechanisms (Holland et al., 2018). In the past several years, blockchain has seen use cases in many industries varying from supply chains to healthcare applications. Blockchain technology has also a tremendous disruptive potential in the financial sector, especially in transforming the operations related to financial transactions and services (Fanning & Centers, 2016).

The concept of blockchain-based financial system is often referred to as *Decentralized Finance (DeFi)*, because in theory it has no central authority in absolute control as in the traditional financial system. In this report, Decentralized Finance will be used interchangeably with the term crypto-markets, as referred to in the MiCA framework. Meegan (2020) defines DeFi as *"the transformation of traditional financial products into products that operate without an intermediary via smart contracts on a blockchain"* (Meegan, 2020), but a more general definition proposed by the ING white paper is formulated as "financial services that operate on a public permissionless blockchain" (Meegan & Koens, 2021). The same paper gathers 10 properties that DeFi must possess based on a literature review, which include: (i) composability, (ii) flexibility, (iii) decentralization, (iv) accessibility, (v) innovativeness, (vi) interoperability, (vii) borderlessness, (viii) transparency, (iv) automation of business processes and (x) finality. Moreover, the financial services that can operate on blockchain are monetary banking services, P2P/pooled lending and borrowing, Decentralized Exchanges (DEX), Tokenization, Predictions and Derivatives markets (Popescu et al., 2020). Despite being a relatively novel technology, blockchain has been gaining strong momentum in the financial technology (FinTech) sector and is often believed to be the most promising innovation in the field as a whole (Du et al., 2019). It is particularly valuable for payment systems, as it allows for decentralized peer-to-peer (P2P) transactions using public key infrastructure (PKI), where pairs of public and private keys are applied to ensure security of data transfer which is further protected by methods of encryption and cryptography (Abramova & Böhme, 2016).

Financial transactions taking place on blockchain technology are enabled through the use of cryptocurrency, which can be defined as a tokenized digital asset that performs ultimately the same functions as fiat currency, but only in a digital form for digital exchanges (Seele, 2018). The point of cryptocurrency, as originally proposed by Nakamoto, is to create a virtual asset that can substitute traditional fiat currency and fall out of central banks' jurisdictions, bypass intermediaries, enable P2P exchanges and outperform fiat in terms of efficiency, speed and security (Masciandaro, 2018). Bitcoin was the first cryptocurrency to be launched and accessible to the public in 2009, but ten years later there were hundreds of cryptocurrencies to be found on exchanges and publicly traded, each with their own special applications and features (Hu et al., 2019) (Brauneis & Mestel, 2018). As of August 2022, the total cryptocurrency global market capitalization is at USD 1 trillion (CoinMarketCap, 2022).

2.3. Overview of the MiCA Framework

In the second half of 2020, the EU responded to the needs for regulation of crypto-assets by proposing a Union-wide legislative framework referred to as Markets in Crypto-Assets (MiCA), or in full Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, an element of the Digital Finance Package and Digital Finance Strategy. The objective of the proposal is to introduce laws on issuance, trading and provision of other financial services on blockchain that do not qualify under the judicial scope of electronic money, financial instruments or deposits under the existing laws of MiFID (European Commission, 2020a).

When adopted and enforced as planned by 2024, MiCA will establish a single licensing regime that will allow issuers and service providers of crypto-assets operate freely across every EU Member State. Both companies that are located inside and outside the European Union will be under the scope of MiCA regulation as long as they serve EU clients. However, the companies also have a choice to not get the common EU license and operate under the national law of a specific Member State (European Commission, 2020a).

The MiCA framework is a product of a large scale market monitoring and engagements in international decision making, and is guided by European Banking Authority (EBA) and European Securities and Market Authority (ESMA). Furthermore, MiCA's policies are partially derived from public consultations taking place in the span of December 2019 - March 2020 (Zetzsche et al., 2020).

As presented in the proposal, The European Commission aims to achieve the following policy objectives by introducing MiCA:

1. Provide a*"sound legal framework, clearly defining the regulatory treatment of all crypto-assets that are not covered by existing financial services legislation".* - Context of the Proposal, p2
2. Introduce a *"safe and proportionate framework to support innovation and fair competition".* - Context of the Proposal, p2
3. Establish *"appropriate levels of consumer and investor protection and market integrity given that crypto-assets not covered by existing financial services legislation present many of the same risks as more familiar financial instruments".* - Context of the Proposal, p2
4. *"Ensure financial stability".* - Context of the Proposal, p3

In Title I, Article 3, pages 34-37 MiCA provides a list of 28 definitions that are used throughout the framework. Some of the more important definitions are extracted and presented in Table 2.1 to explain how the EU regulators use certain terms. To refer to blockchains, MiCA uses the synonymous term "distributed ledger technology" or "DLT", while cryptocurrencies or digital currencies are referred to as "crypto-assets". A type of cryptocurrency that are widely known as "stablecoins" are referred to as "asset-referenced tokens" in case of being pegged to the value of several assets, or "electronic money token" in case of being pegged to the value of one legal tender fiat currency. Moreover, the MiCA framework makes a distinction between issuers and service providers of crypto-assets. From the definitions presented in the table it is seen that the issuers are those offering the assets to the public, while the service providers are those who perform services and functions around the crypto-assets. It is also important to note that MiCA defines these actors as "a legal person" for issuers and "any person" for service providers, implying that the businesses are centralized and have legally responsible individuals. However, not all issuers and service providers always have such forms of management. As explained in the World Economic Forum's white paper on DeFi by Deshmukh et al. (2021), some issuers and services in the crypto-markets are decentralized, meaning they are run by an open-source code in a system of anonymous voting mechanisms. There are no distinctions between the levels or categories of

centralization defined in the framework, and thus these are the only definitions for issuers and service providers presented in the regulation.

Though the MiCA framework does make a distinction for ”significant” asset-referenced and e-money tokens. The regulation requires such issuers to adhere to additional, more strict standards when it comes to authorization process, governance rules and reserve management requirements. It is not yet explained what thresholds determine the significance of an issuer, but technical assessments will be created by the European Banking Authority in the future (European Commission, 2020a).

In Table 2.2, an overview of the MiCA framework and its structure is presented. The regulation has 9 titles, some of which have several titles. Title I sets down the focus, scope and presents the definitions, some of which are listed in Table 2.1. Title II presents the rules for crypto-assets that are not asset-referenced tokens or e-money tokens. Title III is focused solely on asset-referenced tokens with 6 chapters providing rules on different aspects and operations of the issuers. Title IV provides similar rules for e-money tokens, but it can be seen that this title is much shorter than Title III. Title V lays down the policies for crypto-asset service providers in 4 chapters, while Title VI discusses market abuse laws applicable to all stakeholders. Title VII discusses the authority and responsibilities of EBA in the subject matter. Title VIII concludes the framework and Title IX provides the outlook of further action.

Table 2.1: Definitions presented in the MiCA framework

Term	Definition as presented in MiCA
distributed ledger technology or ‘DLT’	type of technology that support the distributed recording of encrypted data
crypto-asset	a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology
asset-referenced token	a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets
electronic money token or e-money token	a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender
utility token	a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token
issuer of crypto-assets	a legal person who offers to the public any type of crypto-assets or seeks the admission of such crypto-assets to a trading platform for crypto-assets
crypto-asset service provider	any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis
crypto-asset service	any of the services and activities listed below relating to any crypto-asset: (a) the custody and administration of crypto-assets on behalf of third parties; (b) the operation of a trading platform for crypto-assets; (c) the exchange of crypto-assets for fiat currency that is legal tender; (d) the exchange of crypto-assets for other crypto-assets; (e) the execution of orders for crypto-assets on behalf of third parties; (f) placing of crypto-assets; (g) the reception and transmission of orders for crypto-assets on behalf of third parties (h) providing advice on crypto-assets;

Table 2.2: Overview of the MiCA framework

Title	Chapter	Name	Articles
I	N/A	Subject matter, scope and definitions	1-3
II	N/A	Crypto-assets, other than asset-referenced tokens or e-money tokens	4-14
III	1	Authorisation to offer asset-referenced tokens to the public and to seek their admission to trading on a trading platform for crypto- assets	15-22
III	2	Obligations of all issuers of asset-referenced tokens	23-31
III	3	Reserve of assets	32-36
III	4	Acquisitions of issuers of asset-referenced tokens	37-38
III	5	Significant asset-referenced tokens	39-41
III	6	Orderly wind-down	42
IV	1	Requirements to be fulfilled by all issuers of electronic money tokens	43-48
IV	2	Significant e-money tokens	49-52
V	1	Authorisation of crypto-asset service providers	53-58
V	2	Obligation for all crypto-asset service providers	59-66
V	3	Obligations for the provision of specific crypto-asset services	67-73
V	4	Acquisition of crypto-asset service providers	74-75
VI	1	Prevention of market abuse involving crypto-assets	76-80
VII	1	Powers of competent authorities and cooperation between competent authorities, the EBA and ESMA	81-91
VII	2	Administrative measures and sanctions by competent authorities	92-97
VII	3	Supervisory responsibilities of EBA on issuers of significant asset-referenced tokens and significant e-money tokens and colleges of supervisors	98-102
VII	4	The EBA's powers and competences on issuers of significant asset-referenced tokens and issuers of significant e-money tokens	103-120
VIII	N/A	Delegated acts and implementing acts	121
IX	N/A	Transitional and final provisions	122-126

2.4. Actor Analysis

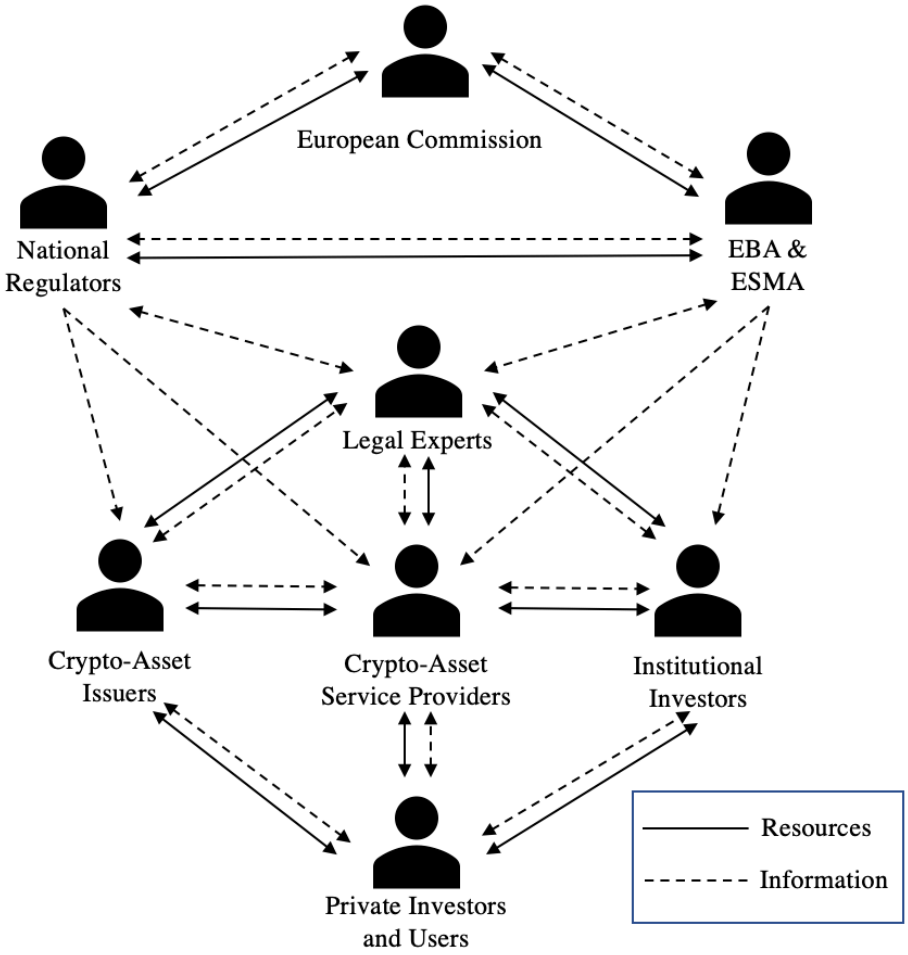

Figure 2.1: Information-Material Diagram

In order to better explore the context of the regulation of crypto-markets, it is useful to conduct a brief actor analysis as demonstrated in the information-material diagram in Figure 2.1. The actors presented on the diagram are directly or indirectly influencing or are influenced by the regulation of crypto-assets and crypto-asset services. To better understand the dynamics between each actor, their interactions are visualized using directed arrows (dashed arrows represent information flow and the filled arrows represent monetary resources flow). In the scope of crypto regulations, the European Commission is the ultimate decision maker supported by the advice from European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) (EBA, 2019; ESMA, 2019). National regulators also play a significant role in the regulatory field, as currently there is no EU-wide framework for crypto-assets and services, meaning most of the regulated EU-based private sector is operating under the national licenses (Zetzsche et al., 2020). Hence, the diagram illustrates an exchange of both information and resources between the public sector actors that are central in creation of the regulations in the crypto-markets.

Once the regulators presented in the top triangle of the diagram agree on the Union framework, the regulations are released and the private sector consisting of crypto-asset issuers, crypto-asset service providers (CASPs) and institutional investors are expected to comply. These three stakeholders eventually create a sub-environment in the larger system where mutual exchange of information and resources is identified, as their existence in the crypto-asset market can be argued to be co-dependent. Service providers need issuers to provide the said services, while the

issuers have more to benefit if there are services provided related to their crypto-assets. Moreover, institutional investors need both issuers and service providers in order to participate in the crypto-market and to be able to connect their clients to it. It is also possible for an institutional investor to become a service provider under the MiCA regulation if they start to offer any of the services related to crypto-assets. Legal experts are another actor that consists of legal entities that study and interpret the new policies and regulations in order to help the private sector be compliant. Moreover, legal experts also communicate with the national regulators, EBA and ESMA when discussing the new regulations and occasionally providing advice and feedback to the regulators. Thus, this group is well-connected with both the regulators and the private sector as they understand both crypto-markets and regulation well.

In this study, the definitions for issuers of crypto-asset and crypto-asset service providers will adopted from the MiCA framework for consistency. Thus, a crypto-asset issuer is *"a legal person who offers to the public any type of crypto-assets or seeks the admission of such crypto-assets to a trading platform for crypto-assets"*, while a CASP is *"any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis, where the services are (a) the custody and administration of crypto-assets on behalf of third parties; (b) the operation of a trading platform for crypto-assets; (c) the exchange of crypto-assets for fiat currency that is legal tender; (d) the exchange of crypto-assets for other crypto-assets; (e) the execution of orders for crypto-assets on behalf of third parties; (f) placing of crypto-assets; (g) the reception and transmission of orders for crypto- assets on behalf of third parties; (h) providing advice on crypto-assets.* A legal expert is a person or entity that provides legal services in the crypto-markets to the market participants in exchange for compensation. Legal experts include lawyers and policy experts, typically with a financial regulation background, focused on the regulation of crypto-markets. Institutional investors are defined in this study as persons or entities offering financial services in the traditional financial sector that are exploring or experimenting with crypto-assets and services with the intention of joining the market in the future. These 4 actors will be collectively referred to as the industry experts.

2.5. Knowledge Gaps

Among the most significant challenges of blockchain, and hence DeFi adoption highlighted by academics is security (Eyal & Sirer, 2014) and government regulation (Reid & Harrigan, 2013). Before MiCA, there have been numerous studies explaining the urgent need for blockchain regulations (De Filippi, 2014), mostly to facilitate adoption in tightly regulated industries, such as banking (Nguyen, 2016). An early 2022 detailed white paper on DeFi by the ING Bank has discussed the need for regulation and favourable policy that is likely to accelerate adoption among financial institutions, specifically legislation clarifying liability in case of a faulty DeFi protocol (Meegan & Koens, 2021). Some academics have called for government regulations focusing on smart contracts that run on blockchain (Yeoh, 2017; Sun Yin et al., 2019), and others expressed criticism towards regulators' reactive policies, inability to properly understand blockchain technology (Yeoh, 2017) and failure implement a proactive policy-making approach (Ali et al., 2020). As a result, for over a decade DeFi-related industry stakeholders faced legal uncertainties and jurisdictional issues when considering adoption of blockchain for financial applications (Guadamuz & Marsden, 2015). However, the studies calling for regulation often do not address the means and structure of such legislation (Caporale & Zekokh, 2019; Wei, 2018).

It is not known whether the MiCA framework addresses these issues and provides the necessary legal clarity for the market participants. It is also unclear whether the regulation is favourable to the development and adoption of crypto-markets and how it will impact the industry. The reason is that there is very little literature in the academic field about MiCA. Upon searching for literature on the matter, using the search term ("Markets in Crypto-Assets") AND ("regulation" OR "policy" OR "framework") AND ("evaluation" OR "analysis" OR "commentary") across the titles and abstracts on Google Scholar, most of the 468 search results are not focused, but rather related to the MiCA framework. Nevertheless, there are several studies providing certain assessments or evaluations of the framework. Wanat (2021) discusses the environmental aspects of crypto-markets and evaluates the framework in terms of the European Green Deal. Zetzsche et al. (2020) reviews MiCA through the legal lens and discusses potential issues with conflict of definitions and scoping with the preceding MiFID regulation, while Raffaele (2022) discusses the MiCA framework from the Italian and EU perspective and mentions the lack of certainty how the regulation addresses decentralized protocols. Bočánek (2021) studies the MiCA framework to assess the implementation and enforceability matters and Novakovic (2021) discusses the implications of MiCA for the Estonian License system. Palomäki (2021) focuses on the reasons and work that led to the MiCA proposal and Bolt et al. (2022) discussed the co-existence of public and private money under the EU regulation. Moreover, the EC carried out its own evaluation in the form of an Impact Assessment on the framework that has indicated that more mature cryptocurrency issuers may face costs up to 87,000 USD to comply with white paper requirements and up to 28 million USD one-off compliance costs (European Commission, 2020b). Furthermore, an extensive study on EU regulations of crypto-assets and services has concluded that MiCA may pose significant strains on the novel blockchain ecosystem by applying strong prescriptive policies as opposed to implementing more general approaches (Ferreira & Sandner, 2021).

In the Context of the Proposal section of the MiCA framework, it is described that President Ursula von der Leyen called for *"a common approach with Member States on cryptocurrencies to ensure we understand how to make the most of the opportunities they create and address the new risks they may pose"* that led to the proposal European Commission (2020a). However, none of the existing literature, to the best knowledge of the author, assesses what risks does the MiCA framework address and to what extent are they addressed. Since this is one of the central motivations behind the regulation, it is of great importance that it is assessed whether this motivation was realized.

2.6. Problem Statement and Research Objective

Hence, the problem statement is formulated for this research problem and is expressed as:

MiCA aims to provide a proportionate regulatory framework to accelerate the adoption and innovation of crypto-assets and crypto-asset services in the EU, while mitigating their risks and ensuring safety for users and legal clarity in the industry. However, there has been no evaluation of the MiCA framework in the academic field that assesses whether MiCA addresses the risks perceived by the industry experts, and how they perceive the proposed regulation.

In order to address the problem at hand, the following research objective is constructed:

The research objective is to provide an evaluation of the MiCA framework by investigating the perceptions of the industry experts and performing a content analysis of the policy to assess what and whose risks are addressed by the EU policy makers.

2.7. Research Questions

Based on the problem statement and research objective, the central question answered in this report is presented as follows:

"What are the policy considerations that EU policy makers could take into account in the future amendments of the MiCA framework and regulatory developments in the EU's crypto-markets?"

The central research question is addressed by answering 4 sub-questions presented in the table below. The first sub-question is answered by the means of interview to obtain insights into the views and opinions of industry experts with respect to the MiCA regulation. If the participants are not aware or familiar with MiCA, they are asked to discuss their views on regulation of crypto-assets and services in a more general manner. The second sub-question is answered by asking the interview participants about the risks of DeFi they perceive from their viewpoint, and those risks are then discussed in light of academic literature obtained from desk research. Moreover, the participants are presented the 18 risks discussed in section 5.2 and are asked to select the five most critical risks and rank them in order of criticality. As a result, the ranking provides a list of the most critical risks perceived among all stakeholder groups. Thereafter, the third sub-question is designed to understand what risks are addressed, partially addressed or not addressed in the MiCA framework by the means of content analysis. As a result, these 3 sub-questions can provide insights that will be translated into policy considerations for the future amendments of the MiCA framework and regulatory developments in the crypto-markets in the EU.

Table 2.3: Research Questions and Materials

RQ Nr.	Question	Research Materials and Methods
1	What is the perception of the industry experts with respect to the (MiCA) regulation and the current regulatory approach?	Interviews
2	What are the most critical risks perceived by the industry experts?	Interviews + Desk Research
3	To what extent does MiCA address the risks of the industry experts?	Interviews + Policy Review

2.8. Research Diagram

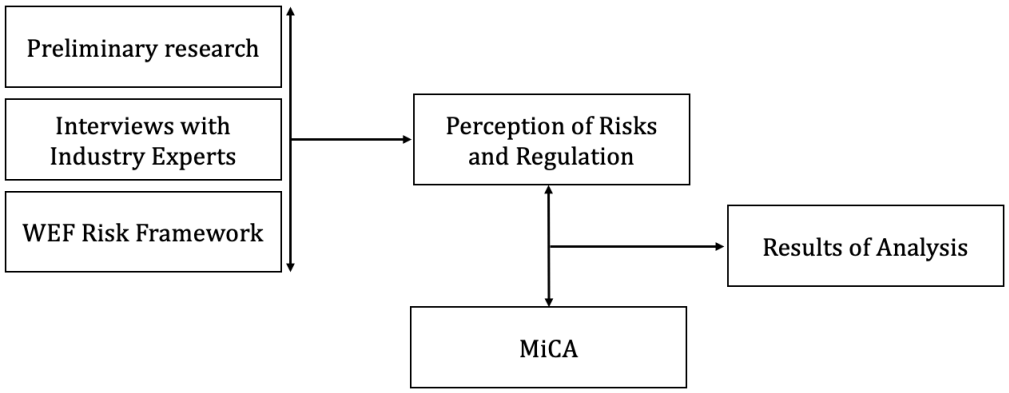

Figure 2.2: Research Diagram

Research diagram plays an important role in constructing a comprehensive theoretical background and helps one understand how the key concepts can be tied to addressing the problem statement. On Figure 2.2, the research diagram for this project is illustrated by visualizing the steps presented in boxes and how they are used to provide an evaluation of the MiCA framework.

In this study, preliminary research, interviews with industry experts from each category of actors are conducted to obtain the following insights: perception of (MiCA) regulation, risks of DeFi perceived by the stakeholders, as well as ranking of the pre-determined 18 risks presented in Chapter 5. The ranking of risks provides the opportunity to understand what are the most critical risks perceived by all actors and specific groups, as well as what policy considerations could be taken into account to address more risks of crypto markets. It is also checked whether the risks identified in the interviews are covered in the MiCA regulation. This done by performing a summative content analysis of the MiCA framework using the keywords of each of the 18 risks. Moreover, the perceptions of the interview respondents with respect to the MiCA framework are analyzed and processed using directed content analysis using topic encoding and the relevant policy considerations are presented.

3

Research Methodology

3.1. Summary of the Chapter

Chapter 3 describes the research methodology implemented in this research, specifically the interview process from selection methodology to the analysis of results. This study employs interviews as the main data collection method to answer the central research question *"What are the policy considerations that EU policy makers could take into account in the future amendments of the MiCA framework and regulatory developments in the EU's crypto-markets?"*". In this research, interviews are used to generate knowledge on the perceptions of industry experts on the MiCA regulation and the general regulatory approach on crypto-markets in the EU, perceptions of the most critical risks faced by the respondents. This information is crucial for the policy evaluation and is used to construct the results in Chapters 4-6.

Section 3.1 provides the general overview of the interviews. Section 3.2 describes the selection methodology used to select the participants for the study. Section 3.3 explains the interview setup and presents the questions that were asked to the participants, and finally Section 3.4 describes how the interviews were analyzed to arrive at the results presented at the end of Chapters 4 and 5.

3.2. Overview of Interviews

Conducting interviews has been selected as the central tool in answering the main research question. According to Kothari, 2004, interviews are effective for generating in-depth information and can provide valuable insights that would otherwise be difficult to obtain (Kothari, 2004). Moreover, interviews are particularly useful in addressing research questions that cannot be answered by performing desk research due to the novel nature of the problem (Gill et al., 2008). Since there are no academic papers ranking a predetermined set of risks by industry experts and no research discussing industry insights on the European crypto regulation, interviews are exceptionally valuable for generating knowledge to help policy makers construct more comprehensive and inclusive decisions. Therefore, this study is carried out by conducting 19 interviews with industry stakeholders from all stakeholder groups presented in Chapter 1. The list of the interviewees participating in the research is presented in the table below:

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

Table 3.1: List of Interviewees

3.3. Selection Methodology

In order to conduct the 19 interviews presented above, numerous strategies and selection methodologies were employed in the searching and invitation phases. Firstly, it has been decided that there is a need to get the perceptions of all actors from the Actor Analysis in Chapter 2, with the exclusion of retail investors and users due to inability to assess or confirm their knowledge and understanding of the crypto regulation and risks. Hence, an open invitation for interviews was posted on LinkedIn and promoted by the research group. The publication called upon any experts working in the crypto-markets and employed either by the European regulator, national regulator, legal firm, crypto-asset issuer firm, a crypto-asset service provider firm or an institutional investment firm that is participating in the crypto-markets or developing an entry strategy. Moreover, the research team reached out to their networks and sent out personal invitations to industry experts from every category described above. In total, more than 170 personal invitations were sent out. Once some responses were obtained, the selection criteria for the interviews were set out as follows: (1) the interviewee must be professionally involved in the crypto-assets and services, or has been involved in the past (2) the interviewee must possess at least 2 years of professional experience in the crypto-assets and services industry (legal, regulatory or private sector), (3) the interviewee must be employed by an EU institution, or by a non-EU institution (except for employees at regulator institutions) that is serving or planning to serve EU clients (thus falling within the regulatory scope of MiCA) (4) well-familiar with MiCA (for legal firm employees and regulator employees) or general crypto regulatory practices in the EU (for private sector) (5) have an understanding and awareness of risks perceived by their employer firm. All of these requirements were reflected in the interview selections and are satisfied by all 19 interviewees for this study. However, it is important to note that sample is not random in the scientific sense as these interviews have not been extracted randomly from a larger population sample. Therefore, it could be that with a set of different experts the results presented in this report could vary, as the sample size in this study is not very large to make up for the individual differences of the interviewees with respect to knowledge, experience and outlook on risks and regulations.

3.4. Interview Setup

The interviews were held with the industry experts on a one-on-one basis for approximately one hour in a video call. To ensure safety and complete freedom for voicing opinions on regulation and risks the respondents are presented anonymously and are referred to by their Interviewee ID. The interviewees were asked mostly the same questions, yet the time spent on each question varied depending on their knowledge and background. The questions asked to the respondents are presented below:

1. Are you aware of the MiCA regulation? If yes, could you share your thoughts about the framework? If not, could you share your thoughts on regulation of DeFi in general?
2. How do you see the co-existence of MiCA and decentralized crypto-asset and -services projects?
3. What in your opinion could be improved in current and future regulations, and do you have any further advice on regulatory approaches that should be taken with regards to crypto-assets and services?
4. What risks of DeFi do you perceive in your line of work? Why are they important?
5. You are presented 18 risks of DeFi derived from literature. Could you specify which of those risks do you find applicable to your line of work in the industry?
6. Among those that apply to you as a stakeholder, could you rank the 5 most critical risks in a criticality order?
7. Does regulation already address the selected risks? If not, what advice do you have based on your experience that could minimize these risks? Are they applicable to policy?

3.5. Analysis of Interviews

The interviews are analyzed by performing content analysis since question 1,2,3,4 and 7 are open-ended. When asked about the MiCA regulation, legal experts that are well-familiar with it discuss different aspects of the framework which leads to 8 unique answers. Despite the differences in particular aspects of the regulation discussed by each interviewee, some themes or topics are overlapping, and by identifying them it is possible to combine information by providing various insights of different experts on the same topic. As a result, a coherent and structured flow is generated. This is performed by reading the interview transcripts after all interviews with the legal experts are completed and encoding different topics they touch upon. When more than one interviewee discussed a certain topic, it is presented as a subsection within the regulation perception analysis in Chapter 4. A similar approach is used with the crypto-asset issuers, CASPs and institutional investor groups. Thus, Chapter 4 is divided into two parts, perceptions of legal expert group, and perceptions of the other 3 groups. This choice is made because legal experts are very well-familiar with the MiCA framework due to their professional focus, while the other groups are only able to share thoughts on the general regulatory approach, and not specifically on the MiCA framework. Nevertheless, they still generate valuable insights on how the industry players perceive the regulatory environment and developments in the EU.

The second part of the interview is focused on discussing and ranking perceived risks of the interview respondents with respect to their line of work. The interviewees are presented 18 risks in a single table and are first asked to go through the risks together with the interviewer and indicate whether they perceive the risk in their line of work or not. After that, they select the 5 most critical perceived risks and rank them in descendent order of criticality from 1-5. Moreover, the interviewees are asked how do they believe this risk can be addressed and what they are currently doing, if anything, to reduce this risk in their line of work. At the end of the 19 interviews, this data will reveal the most critical risks among each respondent group and help identify any under- or over-representation of certain groups by the EU regulators when addressing risks of crypto-markets.

4

Perceptions on MiCA and The EU's Regulatory Approach

4.1. Summary of the Chapter

This chapter addresses the first sub-question of the research: *What is the perception of the industry experts with respect to the MiCA regulation and the current regulatory approach?* It is answered by the means of conducting interviews with experts employed by entities that belong in one of the four categories: (1) crypto-asset issuers, (2) crypto-asset service providers, (3) institutional investment and (4) legal. The perceptions of the interviewees are split into two parts, since legal experts were able to discuss the MiCA framework in detail, while the other three groups preferred to express their views and thoughts about the EU's regulatory approach on a more general level. The analysis is conducted by the means of a directed content analysis, where the common themes and topics that emerged during the interviews are synthesized and summarized in relevant sub-sections.

In Chapter 4, perceptions of Legal Experts on the MiCA framework are found in Section 4.1, while the perceptions of the respondents from crypto-asset issuer, crypto-asset service provider and institutional investment institutions are presented in Section 4.2. Each section starts with the first sub-section on the respondents' perceptions and views on the needs and benefits of MiCA and general existence on regulations of crypto-markets in the EU, followed by sub-sections on perceived shortcomings of crypto regulation.

To summarize, there is a general consensus among all interviewees from all respondent groups that MiCA was a much needed introduction of regulation into the crypto-markets and that it provides the first legal basis and rules into the crypto market to build upon in the future. However, one of the recurring topics of discussion among all respondent groups was the concern that MiCA may be introducing overly strict compliance procedures that may in turn hinder adoption. The legal experts also discussed that there may be potential challenges arising from lack of concrete definitions related to assets and no distinction between centralized and decentralized crypto-markets. Numerous interviewees across all groups called for more innovative regulatory approaches and closer collaboration between the regulators and industry players.

4.2. Perceptions of Legal Experts on MiCA

Among the 19 interviewees who participated in the research, only the 8 legal experts with legal or policy background were well-familiar with the MiCA proposal to discuss its specific aspects. Overall, the legal experts were positive about introducing a regulatory framework into the crypto-asset and -services space, yet most of them also underlined the shortcomings and challenges of the MiCA framework, as well as the need for further improvements and regulations. In the following two subsections, the benefits and drawbacks of MiCA as perceived by the legal experts are presented.

4.2.1. The Need for MiCA in the View of Legal Experts

When the legal experts were asked about their views and thoughts on the MiCA framework as an open-ended question, many started by discussing the need for regulation of crypto-assets and services, namely about the positives of introducing legal clarity for the industry players and opening more opportunities for institutional investors to participate in the market, which is generally perceived as a positive trend in the adoption of crypto-assets.

"Overall, I am positive about MiCA because it sets out clear boundaries for such an important topic as e-money tokens, asset-referenced tokens that are covered under the umbrella term of stablecoins, and these are very important in the picture of the overall market" - Interviewee 1

According to Interviewee 1, an EU-based legal expert, MiCA is a "great step forward" in introducing some clarity for stablecoins and setting up appropriate rules to address market manipulation, as well as addressing the custody rules for CASPs and issuers.

"Also, for market manipulation, that is so important having clear rules in such a market where pump-and-dumps and manipulation techniques, in general, are very, very common. Plus, also I really like the third aspect, which is the custody, adding clear rules about the crypto-asset custody is vital" - Interviewee 1

Interviewee 11, a crypto policy expert, claims that MiCA was "something that everyone needed", despite its shortcomings. Interviewees 15 and 16 also underlined that MiCA was a necessary regulation given lack of applicability of existing financial laws to crypto-assets and services. Interviewee 19 considers the MiCA framework to be "quite complete, quite broad in the horizontal way", suggesting that it does grasp the wide diversity of the current crypto market. According to Interviewee 11, introducing the framework will have a positive effect not only on consumer's confidence, but also on institutional investors.

"I think it's a good thing for all involved because the moment you have clarity in framework, it puts every everyone at ease. This is especially important for institutional investors, because as you know, especially the big banks are heavily regulated and they can't just trade in anything and so the moment that there's an actual legal framework for them to rely on, it's a lot easier for them to step into the market and actually trade in crypto, hold assets for clients" - Interviewee 11

4.2.2. MiCA's Shortcomings in the View of Legal Experts

After giving credit to the regulators for introducing MiCA to the crypto-markets, the legal experts discussed their topics of concern when it comes to the framework. Interviewees discussed the risk of introducing heavy compliance, challenges associated with classification of crypto-assets services, a potentially sub-optimal regulatory approach and lack of clarity with respect to regulation of decentralized entities. All of these topics are discussed in this sub-section.

4.2.3. Heavy Compliance

Interviewees 2 and 18 noted that MiCA framework reflects and tests some principles of the existing regulation from traditional finance, such as MiFID 2, often using the same regulatory concepts. Interviewee 16 also stated that while it is a "first major step towards regulating crypto-assets", it is in their view that MiCA is "to a large degree a copy-paste of MiFID". Interviewee 19 even suggested that the EC could have used MiFID and ESMA's Prospectus Regulation to regulate the crypto markets, yet the expert agrees that MiCA is a more appropriate tool for the job. Interviewees 1 and 2 suggested that a more libertarian approach to crypto markets should be implemented to provide more room for experimentation and innovation.

"I think it's the first iteration of the text and with regards to the scope and the obligations, I think most of the industry participants don't consider the text to be perfect, far from it." - Interviewee 15

According to Interviewee 15, MiCA is likely to be a reactive policy of the EU regulators to address the risks posed by stablecoins, following the announcement of Facebook's own cryptocurrency Libra. The interviewee considers the obligations towards stablecoin issuers, referred to as asset-referenced token issuers in MiCA, to be "exorbitant" and may be viewed as "hindering" by the issuers. In fact, numerous legal experts expressed concerns with respect to the burdens imposed on the issuers and service providers. Interviewee 1 stated that the compliance requirements are "quite heavy" and may pose entry barriers to start-ups in the crypto space.

4.2.4. Challenging Classification of Assets and Services

During the interviews, several respondents highlighted the challenges in understanding the definitions and classifications of crypto-assets in the MiCA framework. While such definitions are purposefully broad in nature, it may be difficult for the industry players to understand under which class do their assets fall.

"There are no exact and clear and straightforward principles that allow you to say with 100% confidence that you're not providing a financial service, or you're under MiCA, or you are not regulated by any regulation. For example NFTs, they might fall under the financial regulation, they might fall under the MiCA regulation or they might not be regulated at all, and sometimes it's hard to distinguish or to assess with 100% confidence that you're in one of the three scenarios, so that's the hardest part of our job. But as new project are always ongoing and their forms are quite hybrid and particular, it's not that easy to say you're under the financial regulation or under MiCA or not regulated at all. So we will see. We will expect a lot of flows in the regulations." - Interviewee 2

Interviewee 15 also shared that, in practice, it is highly challenging to understand which projects fall within and outside of MiCA's scope. Moreover, when discussing volume thresholds for issuers, the policy expert expressed their criticism towards lack of clarity in trading volume definitions due to various ways in which such terms may be interpreted in the crypto space. Interviewee 11 further elaborated on the lack of clarity when dealing with definitions and classifications of crypto-assets.

"It's still very difficult. Especially for the hybrids, it's just very difficult. You'll have clear case, a project, DeFi project or crypto assets, that you can just put in the box and that's it. You're done. But you'll find that a large part of the market is going to be in that gray zone where you're gonna have to discuss and have clarification as to do we fall into this definition?" - Interviewee 11

4.2.5. Regulatory Approach

Several legal experts stated that MiCA and other traditional financial regulations may not be well-suited to regulate crypto-assets and -services. Interviewee 1 stated that there is a need for a "more creative approach", especially concerning AML and travel rule in the crypto space. They further stated that the regulators are lacking cooperation between authorities and are experiencing missed opportunities by not implementing blockchain forensic analytics. In their view, supervisory authorities lack technical capabilities to utilize software that could enable them to address AML measures more effectively.

"They should not have a punitive approach, a biased approach, just because the financial markets are changing, or let's say the technology in the markets is changing. They shouldn't be too conservative. [...] I would be very liberal in terms of innovation and let the players create new products and new business model using these new tools and the technology that enables these new tools, but I would be very strict in terms of market manipulation, and in terms of custody, there the approach should be straight." - Interviewee 1

4.2.6. Co-Existence of MiCA and Decentralized Projects

One of the questions the interviewees were asked was about the co-existence of MiCA and projects on the more decentralized spectrum of centralization. Unlike in traditional finance or CeFi, decentralized projects do not necessarily operate under a human-run registered company. Examples of decentralized services include DEXs, self-sustained wallet providers, decentralized insurances, loaning and borrowing services, and any DAOs that do not operate under the traditional organizational structure, but are instead automated by the means of smart contracts. MiCA requires licensing, authorization and custodian services for the crypto-asset issuers and service providers (European Commission, 2020a). However, the process can be extremely tricky when dealing with decentralized projects that do not necessarily have liable individuals, but are run by an open-source code that has been agreed upon by the users.

On 30th of June, 2022, the tripartite discussions ended with several changes to the final version of the MiCA framework, which included the removal of decentralized crypto-asset and services from its scope. However, as explained by Interviewee 1, it is not clear what factors and elements constitute to assessing the level of decentralization. According to the interviewee, there is a paradox since some projects refer to themselves as decentralized, yet there is an established Treasury, Board of Directors that could be legally liable for the project. Moreover, Interviewee 19 explained that as long as there are people involved in running a decentralized protocol, they could be viewed as the responsible individuals for the given protocol.

"It is my understanding that MiCA is really made with centralization in mind and centralized exchanges, issuers of stablecoins, etc., that's the starting point of this framework, and it does not really fit the framework of Decentralized Finance" - Interviewee 19

According to Interviewee 11, the reason why decentralized projects are left out of the scope of MiCA is because they are still somewhat insignificant on the macro scale of financial services. However, the expert believes that it is still "very under the radar" of the regulatory authorities and more policies are to be expected in the near future.

"In the EU, I think the biggest question that's going to have to be discussed by regulators is a shift from entity-based regulation to activity-based regulation, because most financial services regulation is entity-based. So what type of entity are you? Are you accredited institution? OK, then if you're a bank we will regulate you like a bank, but DeFi, that is a bit more blurry. So I think what we are going to struggle with the most at the EU level is a shift in thinking between entity-based to activity-based, but they will certainly take lessons from MiCA." - Interviewee 11

4.3. Perceptions of Issuers, CASPs and Institutional Investors on Regulation

In this research, there were 2 respondents from crypto-asset issuer entities, 6 respondents from CASP entities and 3 respondents from institutional investment entities who shared their opinions on the current regulation of crypto-assets and services. Most of these interviewees possess hands-on experience on technical development and/or business implementation side of crypto-assets and services. However, since they are not legal or compliance experts, there were not always able to specifically discuss the MiCA framework, but still provided valuable input when discussing the current regulatory climate in the EU and potential ways in which the regulators can better construct future policies and regulations.

4.3.1. The Need for Regulation

In general, the respondents welcome regulation in the crypto markets as it can help stabilize the market and facilitate the entry of traditional financial institutions into the space.

"I think the more we end up regulating [crypto-assets and services], the more things stabilize, the more it starts becoming attractive for the masses. I think eventually that's gonna be a good thing." - Interviewee 8

When discussing their thoughts on regulation of crypto-assets and -services, most of the interviewees stated that if done correctly, regulation can benefit the industry by encouraging institutional and mass adoption and reduce malicious behavior. Interviewee 9, a CASP firm employee, stated that while regulation can add complexity to the operations of companies in the space, it is also vital to the growth of the crypto-markets: *"I feel that in general, policies and regulations are important to bring the cryptocurrency market to the next level because without these regulations and policies, the really big players, like the traditional financial banks and companies, cannot really go to dive into it without these policies and regulations. So I feel that that it's a good thing that these things are happening."* - Interviewee 9

Indeed, similar thoughts have been shared by the employees at institutional investment firms, Interviewees 6, 7 and 10, who discussed that traditional financial institutions are heavily regulated and undergo strong compliance procedures. For them, it is highly important to have legal clarity and policies that would allow them to partake in the market of crypto-assets and -services. Unlike for crypto-issuers and CASPs, there are strict laws and guidelines for banks, hedge funds and centralized exchanges with respect to what assets and services can they provide to their clients.

"I think it's necessary for the crypto markets to evolve into a situation where you would have more registered and licensed entities, being able to not only seize the opportunity that the industry is actually providing, but also to protect customers better. It's a part of the necessary development that needs to take place for a large traditional finance institution to actually increase activity in this space. So I welcome it." - Interviewee 7

"Certainly we need regulation. If we want to take this niche, isolated, DeFi world and expose it to more traditional finance entities, there needs to be regulation that will actually spur growth into this segment of the market. Without it we are stuck to retail, and it's been important until now, but to keep going we need to allow regulation, regulation that doesn't hamper innovation. It needs to just put all of this into some sort of a legal framework, but without being too restrictive, which is also something that that it's worrying. Right now the space is kind of like the Wild West because of the lack of regulation." - Interviewee 10

On the other hand, Interviewee 17, an EU-based CASP employee, is concerned with increasing

regulation in the EU and believes that the current approach may negatively impact the market. According to them, there should not be a strict regulatory framework imposed on crypto-issuers and -service providers.

"Personally, I don't really like to see regulation, at least not too much. I think regulation is sensible, but in really in minimal ways. (...) I think that projects should be allowed to fail, first of all. Because this is how progress is made. This is how it was in the IT industry's dot-com era. You just do something and if you didn't calculate something properly, you failed. Then you rise from the ashes, you learn from your mistakes, you create a new one. But when it does fail, there's always a question whether it was a scam, whether it was planned, whether it was these kind of things, especially with companies with small litigation possibilities and skills. They will just lose, and then they might go to jail or just let go of all of their remaining assets." - Interviewee 17

4.3.2. Lack of Cooperation

While most of the interviewees agree that to regulation can contribute to consumer protection, institutional investments and mass adoption, the current approach taken by regulators needs to improve and adapt to the technological nature of blockchain-based financial systems. Numerous interviewees also called for more dialogue between the industry and the regulators. Interviewee 8, an ex-employee at an EU-based crypto-asset issuer firm, explained that since regulation is "inevitable", the industry should help the regulator construct policies and frameworks that will not hinder innovation. In addition, interviewee considers barrier to entry and innovation to be their main concern with respect to regulation of crypto markets.

"As long as like financial bodies have a better grasp of what is happening on blockchain networks, if they have a better idea of what tools to use to analyze transaction data and if they work a little bit more with the people that create it, I think there is a much higher chance for them to weed out financial crime, to weed out laundering, terrorism financing and stuff like that. Because for most blockchain platforms all the stuff is public, if they knew how to use Chainalysis for instance, they would just be able to track down criminals pretty easily." - Interviewee 8

As also called for by Interviewee 3, a non-EU-based crypto-asset issuer employee, there needs to be more cooperation between the regulators and the industry players, as the regulators may not possess the necessary knowledge and understanding of the blockchain technology to construct effective DeFi regulations.

"There may be a possibility that the regulators may take a certain decision, but they may not be aware of all the intricacies and the challenges these systems post. So the primary stakeholders would be the users and the builders, and they should definitely have a say." - Interviewee 3

4.3.3. Regulation and Progress

Interviewee 17 discussed how regulation, in their view, can hinder progress and negatively impact small businesses that do not have the means to survive the regulatory pressure.

"I think (regulation) will stop the the progress and evolution. This can also be used and abused by lobby makers to make sure that the traditional financial service stays as a leader and that the new participants are not allowed to the market. So you could also present it as caring for the investors, but in fact you might pursue different goals by introducing these kind of things, in my personal opinion. I think also the regulations are somewhat tightening in the recent years. We could see also that in the money laundering regulations, the (unregulated) amounts are shrinking, the reporting amounts and reporting requirements are broadening, and then banks complain that they have more and more money being spent on the on this kind of enforcement. This essentially just squeezes out the small businesses which have limited budget, limited investment and don't have a lot of money.

The bill for compliance is rising and they are just squeezed out." - Interviewee 17

4.3.4. Lack of Competence

Interviewee 14, an EU-based CASP employee, provided extensive criticism on today's regulatory approach for crypto-markets. In their view, regulation introduces the risk of creating homogeneity in the industry by forcing all companies to adopt a certain structure and leaving little to no freedom for difference, which can in result make the industry less resilient. Secondly, they believe that regulation poses a high entry barrier for start-ups who seek to provide financial services in the crypto-markets, as larger amounts of capital will be required to launch projects. Thirdly, the interviewee explained that there may be the risk of incurring an "assumption of truth", which in their words is a bias associated with believing that just because an entity is regulated, everything the entity states is true and in the best interest of consumers.

"Whenever you have a regulated business, there is this assumption of truth. If you're a regulated business and you say something, kind of by default, the consumer would think that whatever is said is true, which obviously we know is not necessarily true. Not everything a regulated business says is in the best interest of users or necessarily a good investment advice. So for instance, as of today in crypto, you have this idea that crypto is not regulated, so by default everything else is a scam. So by default, I will not trust any project. By default, I will not invest in any projects. By default, I have to do my own research and really understand who's behind this project and so on, which I think is the right attitude that every consumer should always have. If crypto were regulated in any way and you would have the seal of the European Central Bank or Commission or whatever, saying this project has been audited by the European Commission, then from a consumer perspective, people would feel that it is kind of a safe project to invest in or safe product to use, and I don't know if a bunch of people in a regular regulatory institution have the ability to actually audit and process all the information that has to be processed in order to make this type of statements." - Interviewee 14

According to Interviewee 4, an EU-based CASP employee, MiCA adds an initial security layer for consumers, which could be a positive change to the industry, but it also tries to apply its focus mostly on market manipulation issues, which in their view lacks breadth and depth.

Regulation of crypto and DeFi is still quite limited in my opinion. MiCA, from what I understand, tried to address some of the scams in crypto: rug pulls, pump-and-dumps, those type of projects, which is nice, but I believe that's only the surface of it and there is a still a long way to go until we have full regulations. (...) If it comes to KYC and AML type of regulations, then there's a long, long way to go for DeFi to implement all of those, because as it currently stands, it's relatively impossible to do. For example, on Ethereum you have UniSwap, and doing KYC on every single wallet and try to find out where the money is coming from, try to find out if this person is a fraud or if he launders money is in my opinion very impossible to do right now with the current structure. It could be possible in the future with different blockchains, maybe, but that's for up for speculation." - Interviewee 4

4.3.5. Inefficient approach

Interviewee 17 proposed an alternative approach to regulation in crypto-markets inspired by the US crypto community on social media, which essentially entails that users sign and submit a form to the SEC which states that they understand the risks of interacting with Decentralized Finance and will be able to use the services as they wish. Moreover, the interviewee believes that introducing regulations that are similar to traditional financial policies in the DeFi space will significantly hinder progress and give rise to anonymous markets, where users and developers will go anonymous to avoid compliance and giving out their personally sensitive data such as IDs and passports which may be compromised during a cyber crisis.

"So I think (regulation and DeFi) can coexist, but sometimes it could be possible that it will be against the rules and then the rules will have to adapt. Similar with Uber and AirBnB, for instance in the Netherlands, but also in other European countries, where it was at first, ten years ago, met with a lot of criticism from the taxi lobby, from the hotel lobby. They would just say it's not safe, you risk people getting robbed to getting killed or whatever. Some of these points are valid, but I think sometimes you can just over exaggerate some points to an extent and it's just not allowed to happen. In Chile, Uber is perfectly operating, but it's not legal. The government sees that and then comes to conclusion that you cannot really stop it and says let's just regulate it, let's just try to take some text out of it, but not not forbid, not restrict anything. I think that is what could be happening with the DeFi industry as well." - Interviewee 17

Furthermore, as stated by Interviewee 13, a non-EU-based CASP employee, regulators are too slow with implementation of policies and thus face the risk of being constantly behind the fast moving crypto market.

"The plan is to introduce (MiCA) in 2024. It should have been introduced two or three years ago. They are extremely behind the caravan and that is a problem. They should have been doing this a long time ago, and the USA is much more forward looking. (...) Between here and 2024 and a lot of things will have happened, so you are shooting at a moving target here. It is a challenge." - Interviewee 13

In fact, another interviewee also suggested that the US is moving forward faster than the EU with respect to regulation of crypto-assets and -services. Interviewee 8 also highlighted that the US is trying to cooperate with the industry and create more liberal frameworks, while the EU may have a more "break neck" approach as stated by the respondent. Meanwhile, Interviewee 13 believes that the UK has a more effective regulatory approach than the EU based on a compensation scheme, referring to the Financial Services Compensation Scheme (FSCS). In the UK, FSCS allows users to receive monetary compensation in case of loss of assets, only eligible for regulated tokens under the national regulatory permit. Such a scheme provides an incentive for users to deal with more reputable and regulated digital assets (Authority, 2019).

"The UK that did a very smart thing. Instead of having a 10,000-page document, they said that if the provider is certified a good provider, and they have exams, and they do the right thing, then there's a competitive compensation scheme for the user. The result is that only really good service providers enter the market and those in there to scam or make something good for themselves and bad for the customer, they go out. So that's a very smart thing of doing a compliance or a regulation, just to make sure that the good people are the ones that win this game. In MiCA that is somehow not there and they are trying to make a lot of words on pages and in the long run that doesn't work." - Interviewee 13

4.3.6. Challenging Implementation

Moreover, Interviewee 13 discussed that borderlessness of DeFi poses a major challenge for regulations, as lack of coordination and unified global framework poses risk of regulatory arbitrage. A potential solution for this, in the view of the interviewee, is excluding non-EU-based issuers and service providers dealing with EU customers from the potential compensation scheme.

"It's definitely possible to regulate DeFi. The trouble is that this is a global market. If we in Europe have a regulation and the service provider in the Bahamas or Fiji or any of those tax havens, then it's a trouble because people can use them anyway. But if the compensation scheme is there, if you are fooled as a user and a part of the scam is based out of the Bahamas, you don't get that compensation so. This is the reason that regulation should be global. It should be all over the world, absolutely, 100% all over the world."

4.4. Results of Analysis

Based on the information obtained from the interviewees as an answer to the open-ended question on views on MiCA and EU crypto regulation, it is possible to construct considerations for the future crypto-policy. Thus, this section answers the first sub-question of the research *"What is the perception of the industry experts with respect to the (MiCA) regulation and the current regulatory approach?"*

In general, all interviews agree that regulation is needed in the crypto-markets at least to some extent. In that sense, the European regulators have addressed the need for legal clarity necessary for future development, something that has been called upon in both academia, as explained in Chapter 2, and the industry, as revealed during the interviews.

According to the legal experts, classifications of assets themselves are not specific enough to be able to certainly assess whether a certain crypto-asset falls within the scope of MiCA or does not. MiCA classifies crypto-assets into broad categories, namely crypto-assets, asset-referenced tokens, electronic (e-money) tokens and utility tokens. These definitions are provided on page 34, paragraph 1 of the framework. During the interview rounds, 3 legal expert respondents explained that the classification is challenging since these definitions are not mutually exclusive, and one asset may at the same time satisfy more than one condition. Moreover, it is uncertain under what category do crypto-assets such as NFTs fall into. To avoid regulatory arbitrage, confusion among the market participants and easier registration and licensing process, one may further explore how crypto-assets can be better categorized and classified in the MiCA framework.

One of the bigger discussions that took place during the interviews was the question of coexistence between MiCA and decentralized projects that do not have a central board, a registered entity or an active human management and monitoring. There are thousands of crypto-asset issuers and service providers that are open-source, decentralized communities run by anonymous users who use token-based voting systems to make decisions. In this case, it is not possible to register such companies under the EU license due to the absence of legally responsible individuals that are in charge of the organization. MiCA does not make a distinction between the levels of centralization in the crypto-markets and does not explain how such firms would be regulated. In order to improve customer protection and allow the decentralized eco-systems to develop, it is needed to explore how this space can be regulated given that the traditional methods may not apply. Since EBA and ESMA are required to provide a report with market trends within the 36 months of MiCA's entry into force, it is likely to emerge as a topic of discussion within the EU's regulatory structures.

To successfully regulate the crypto-markets, given the wide spectrum of centralization in this space, the regulator may need to explore novel and more creative approaches in the upcoming future. According to some of the legal experts interviewed in the study, MiCA heavily resembles its predecessor MiFID in many of the rules and concepts present in the framework. This is a shortcoming of MiCA since page 147 of the framework presents the Commission's proposal for MiCA, stating that *"where a crypto-asset qualify as a MiFID II financial there is a lack of clarity on how the existing regulatory framework for financial services applies to such assets and services related to them. As the existing regulatory framework was not designed with crypto-assets and DLT in mind, NCAs (National Competent Authorities) face challenges in interpreting and applying the various requirements under EU law, which can hamper innovation."* Despite this reasoning at the motive of the new regulation, MiCA employs many of the past requirements and procedures, simply with varying definitions. The respondents among crypto-asset issuers, CASPs and institutional investors shared that the EU's current general approach with respect to the crypto regulation is not very suitable for the blockchain-based financial services, thus a shift in thinking may yield more productive regulatory efforts. It could be helpful to employ more activity-based rather than entity-based regulation due to the highly hybrid nature of crypto-companies, as sug-

gested by one of the legal experts.

Furthermore, closer cooperation between the industry and the regulatory bodies may yield more timely, productive and practical regulatory efforts due to the general lack of knowledge and experience of the regulators within the blockchain field. On page 6 of the MiCA framework, there is a provided explanation on the stakeholder consultation sessions which include an open public consultation (3 months), an impact assessment (1 month), a Member State experts consultation (2 occasions) and a webinar Digital Finance Outreach 2020 (1 occasion). However, it is not explained how many respondents were consulted, who were the respondents and what exactly has been consulted. Due to the lack of transparency in the process and absence of response from the EU or national regulatory bodies about the interview invitations, it is not possible to in any way assess whether the consultation and cooperation has been sufficient. Nevertheless, as opposed to one-time consultation periods every several years, it could be more productive to maintain constant cooperation between the regulators and the industry. This has been voiced by numerous interviewees who believe that the regulator may not possess all the necessary knowledge and tools to effectively regulate, monitor and enforce their rules. Therefore it may be useful to provide higher transparency on the consultation sessions, implement a closer cooperation with the industry and demonstrate this effort to the general public.

5

Ranking The Risks of Crypto-Assets and Services

5.1. Summary of the Chapter

Chapter 5 answers the sub-question: *What are the most critical risks perceived by the industry experts?* In order to address this question, the study adopted 17 risks obtained from World Economic Forum's Whitepaper on Decentralized Finance, added an additional risk to the list, and asked the interview respondents to identify which risks are applicable to them, and which 5 risks from the list are the most critical risks in their view. This allowed the study to reveal which risks are perceived as most critical by which of the 4 respondent groups, allowing the following chapter to explore whose perceptions may be over- or under-represented in the MiCA framework.

Sections 5.1 and 5.2 present a brief introduction to the crypto-assets and DeFi, followed by Section 5.3 which explores WEF's risk list by elaborating on them and providing examples of relevant risk occurrences. Section 5.4 presents an overview into the ranking of the risks by the respondents during the interview rounds and explains which risks are deemed most critical across all respondents. In latter subsections under 5.4.1, the risk perceptions of respondent groups are presented individually, followed by the results of analysis in Section 5.5.

When combining the risk perceptions of all respondents, it is revealed that fraud and market manipulation, market risk, key management, financial crime and smart contract risk are the most critical perceived risks in the corresponding order. However, due to the uneven number of respondents from each group, this is not fairly representative of all 4 respondent groups. When looking at separate risk rankings for each group, it is seen that there is a significant amount of overlap, especially due to financial and legal compliance risks consistently ranked high across all groups, yet with technical risks, such as smart contract risk and key management risk, perceived consistently as critical accross all groups.

5.2. WEF's DeFi Risk Framework

Despite highly innovative and cutting-edge financial technology being constantly developed in the DeFi field, blockchain technology is still relatively new and possesses many risks that make DeFi a controversial concept. Scholars such as Geiregat (2018) and Shahzad et al. (2018) have indicated that issues such as investment losses, anonymity and decentralization of exchanges, lack of price stability, lack of mass adoption, irreversible transactions and money laundering are contributing to the negative image of Decentralized Finance. Furthermore, researchers have categoratized challenges and risks of blockchain technology for financial applications into those of regulatory and technical & business character (Lewis et al., 2017). Regulatory issues focus on currency control and security, while technical & business issues revolve around operational challenges of network performance indicators and privacy-related risks. Upon conducting a brief background research into the risks of decentralized finance in the academic literature, it has been discovered that most of the risks directly or indirectly fall under the 17 risks outlined by the World Economic Forum's White Paper *Decentralized Finance Policy-Maker Toolkit* (Deshmukh et al., 2021). The risks have been collected as a result of extensive industry collaboration and input from experts across various entities involved in digital assets. The report presents 16 content contributors who occupy technical and business leadership positions in the private sector of DeFi. Given the solid risk framework provided by the white paper, it has been decided to directly utilize the risks in the latter sections of analysis. In the rest of this subsection, the risks and their explanation are listed and briefly explained in light of the WEF's white paper and other academic literature.

5.2.1. Market Risk

As defined in the WEF white paper, market risk is a downward trend in assets value associated with market conditions, idiosyncratic behavior of traders and novel market information (Deshmukh et al., 2021). Market risk can also be generally defined in the scope of decentralized assets as increases and decreases on the value of a position or portfolio that occurs due to fluctuations in market prices (Hartmann, 2010). This risk is a very general financial risk that can occur in trading of any assets where factors such as interest rates, commodity prices and interest rates can affect the market (Fantazzini & Zimin, 2020). The importance of this risk in trading digital assets is mainly posed by challenges related to comparing digital tokens to real-life fundamentals that may cause significant fluctuations of prices, often driven purely by traders' trust and expectations related to the digital tokens.

5.2.2. Counterparty Risk

The general definition of counterparty risk provided in this study is a risk of a counterparty's willing or unwilling failure to fulfill their end of financial instrument obligations, which can also involve a credit risk or settlement risk (Deshmukh et al., 2021). The criticality of credit risk in DeFi is largely posed by volatility that can generate under-collaterilization. Moreover, the anonymous nature of DeFi creates challenging processes to determine whether a party can be trusted with a credit loan. Since counterparty risk in DeFi is mostly associated with credit risk, it is important to provide a suitable definition in the scope of cryptocurrencies. The traditional definition of credit risk does not apply as payment of interests and reimbursement of principal amounts is not a characteristic of cryptocurrencies (Fantazzini & Zimin, 2020). Furthermore, cryptocurrencies can be argued to enter a "dead" state as described by Feder et al. (2018), where a crypto-asset is defined as dead once the daily trading volume is less than or equal to 1% of the highest recorded volume. Additionally, unlike in traditional finance dead cryptocurrency projects have been revived numerous times within a span of several years. Thus, the following definition of credit risk has been adopted within the scope of this study from Fantazzini & Zimin (2020): *"Credit risk is the gains and losses on the value of a position of a cryptocurrency that is*

abandoned and considered dead according to professional and/or academic criteria, but which can be potentially revived and revamped". With respect to the settlement risk, the biggest risk perceived by the users of DeFi is failure to receive expected assets as a result of fraud, misinformation, uneducated investment choices and inability to understand the smart contract that oversees the completion of payments.

5.2.3. Liquidity Risk

As defined by WEF, liquidy risk presents the risk of incurring insufficient funds or assets to support the value of a financial asset (Deshmukh et al., 2021). Liquidity risk can be faced by both users and issuers of a crypto-asset. If there is lack of liquidity for a user, the trading position can be forcefully liquidated, resulting in loss of funds and assets. For a crypto-asset service provider, lack of liquidity can result in an inability to support the transactions on the trading platform, severely affecting its operational performance. This risk is very similar to the one of traditional finance liquidity risk, yet is more critical in dealing with crypto-assets due to their notorious volatility.

5.2.4. Transaction Risk

Transaction risk is a technical risk resulting from a failing or dysfunctional Layer 1 blockchain network, potentially causing double-spending, overly expensive transactions and insufficient throughput, which then ultimately affects the application layer (Deshmukh et al., 2021). Transaction risk can be caused by a malicious attack on the network, for example by a spam attack or by a double spending attack. A spam attack can be defined as a malicious action that utilizes network inefficiencies and weaknesses to reduce its transaction speed and delay block generations. Meanwhile, a double spending attack is identified when there are more than one transactions relating to the same cryptocurrencies, or in other words spending a single token more than once (Begum et al., 2020).

5.2.5. Smart Contract Risk

The idea of smart contracts was initially proposed in 1994 by an American computer scientist Nick Szabo, which essentially is designed to computerize and execute transaction protocols of a traditional contract (Don & Alex, 2016). Today, they are the backbone of the financial systems running on the blockchain as a smart contracts are responsible for verifying and executing transactions based on occurence of predetermined and agreed upon contract terms. Once prepared and launched on the blockchain, a smart contract cannot be altered and is operating in an automated manner (Giancaspro, 2017). However, despite their efficiency smart contracts, as all software, present inherent risks due to their open-source nature and potential vulnerabilities resulting in programming errors, flaws and misintended executions (Deshmukh et al., 2021).Even though distributed ledgers are not susceptible to a single point failure as attackers must target numerous points of the network for a successful hack, the novel and untested nature of the said technology presents opportunities for malicious behavior. For example, Juels et al. (2015) reported cases when smart contracts have been linked to criminal activity. For example, in 2022 an Ethereum liquidity provider XCarnival suffered a loss of four million USD after a malicious attack exploiting its smart contract vulnerability. Such attack resulted in a paid ransom of 1.8 million USD by XCarnival, while no legal charges have been filed against the hacker in exchange for return of the stolen funds (Sanyalt, 2022). Another larger scale attack also took place in 2022 when a hacker exploited flawed design of a pay-to-earn crypto game Axie Infinity to steal 625 million USD. The users were only reimbursed for 1/3 of their losses (Khalid, 2022).

5.2.6. Miner Risk

Miner risk is a risk of market manipulation by miners that order and execute transactions and enable certain parties to profit faster than others (Deshmukh et al., 2021). In blockchain systems, miners are individuals that are paid a fee for processing transactions into blocks after deciding in which order to complete them. Since miners have the power to rearrange transactions as they see fit, they possess an advantages over non-miners when it comes to token offerings and arbitrage trades (Shevchenko, 2020).

5.2.7. Oracle Risk

Due to the absent interoperability of blockchains with the real world, so-called oracles play a significant role as the main interface between the two realms (Antonopoulos & Wood, 2018). Oracles by definition are external third-party centralized entities on which a smart contract relies to execute its protocols (Deshmukh et al., 2021). If oracle data is compromised, users may be at risk of observing manipulated on-chain prices. The risk is that blockchains may use trusted oracles using experience-based selection methods that are unsafe or inauthentic (Egberts, 2017). Moreover, a 2020 systemic literature review into applications of blockchain revealed that only 15% of 142 selected studies mentioned oracles and less than 14 papers discussed oracle risk, making it a highly underrepresented risk (Caldarelli, 2020).

5.2.8. Risk of Challenging Routine Maintenance and Upgrades

The DeFi space is highly autonomous, and its decentralized nature poses new challenges in establishing effective response protocols for system malfunctions. As fewer individuals have influence to take down a service, fewer individuals have the influence to repair it (Deshmukh et al., 2021). Decentralized services inherently carry a risk of challenging implementation of routine maintenance and upgrades as the platforms and activities cannot be shut down, fixed and relaunched as in traditional servers.

5.2.9. Forks

Forks are developed and launched as an option for individuals who would like to use a particular DeFi service, yet with an altered set of parameters of the original service (Deshmukh et al., 2021). Sometimes, a (code) fork can gain higher popularity and activity than the initial service. Forks are usually an option for minorities, but when they achieve high traffic and usage forks may become expensive and misinform their users. One of the arguably most famous cases of a fork attack in the DeFi space has been witnessed in September 2020, when an anonymous developer Chef Nomi created a fork of a well-known DEX Uniswap to launch SushiSwap (SUSHI). The fork was identical to Uniswap with the only difference of rewarding users with SUSHI when they deposited Uniswap's LP tokens used as a means of exchange on its platform. As a result, Uniswap's liquidity was drained to SushiSwap, and after just 10 days Chef Nomi passed the platform to a centralized exchange and obtained 13 million USD worth of ETH by selling his entire SUSHI holdings. This event is known as the first "vampire mining" in the DeFi space (The Defiant, 2020).

5.2.10. Key Management

Loss of cryptographic key pairs is a risk faced by all systems built on blockchains (Deshmukh et al., 2021). There are many DeFi services that do not use custodial services for the cryptographic

keys, meaning that the burden of not losing the keys to the user's assets is placed on the user themselves, while the responsibility of not losing the keys to the DeFi service platform solely rests on the shoulders of those who run the service. Therefore, key management is a highly important in DeFi, and the loss of keys to the wallets can result in users and service providers permanently losing access to their assets and services (Deshmukh et al., 2021). For example, in early 2019 a Canadian exchange QuadrigaCX was plugged off due to extreme monetary damages valued at over USD 200 million incurred by 76,319 users as a result of its Founder's passing, the sole person at possession of encrypted keys to the platform's offline reserves. The company filed for bankruptcy, while investors' and clients' losses could not be recovered (Alexander, February, 2019). This major incident sparked all sorts of controversies, criticism for crypto-asset exchanges and conspiracy theories on social media platforms, with various people even claiming that the 30-year-old Founder and CEO of QuadrigaCX faked his own death. The story was also covered in a highly popular documentary *"Trust No One: The Hunt for the Crypto King"* (Toby & Lawrence, 2022).

5.2.11. Governance Mechanisms

Governance mechanisms is the risk of abuse of governance voting mechanisms through bribery, concentrated token control and aggressive acquisition of tokens to gain influence over the system Deshmukh et al. (2021). In Proof-of-Stake blockchain systems, the block creator is selected based on their stake, or in other words token ownership. Unlike in Proof-of-Work systems, the block creator does not get compensated for creating it, but instead earns a transaction fee Bilotta & Botti (2019). Once a certain actor owns 51% of the network by token ownership, they are able to create a malicious block and abuse the system, making this a severe risk in the crypto-markets.

5.2.12. Redress of disputes

Unlike in traditional finance, redress of disputes is a challenging governance risk as it is often unclear how to resolve a conflict which occurred on a decentralized platform using a centralized judicial system (Deshmukh et al., 2021). Since a smart contract cannot be paused, altered or reversed by a third-party government authority using a court order, individuals seeking redress resulting from a software failure, market manipulation or misinformation may not be able to effectively receive help from the outside. A smart contract's eligibility under the traditional contract law is still debated, as the programming language used to write them cannot be understood by someone who does not possess the knowledge and skills to fully comprehend its meaning (Giancaspro, 2017). Moreover, correcting and relaunching a smart contract is often impossible or is highly challenging, thus any alteration requirements or procedures similar to traditional contracts may simply not be an option given the nature of blockchains.

5.2.13. Financial Crime

Financial crime is a risk associated with criminal activity such as money laundering, terrorism financing and evasion of financial sanctions (Deshmukh et al., 2021). Since users are anonymous by default and prevention of transactions is impossible in DeFi systems, lack of know-your-customer (KYC) regimes are not available. Thus anti-money laundering (AML) and countering the financing of terrorism (CFT) monitoring is difficult to establish in DeFi.

5.2.14. Fraud and Market Manipulation

Fraud and market manipulation is a risk that is associated with malicious behavior of actors in the DeFi spaces intended to misinform and scam the users (Deshmukh et al., 2021). A 2022 systemic

literature review into the types of cryptocurrencies fraud discussed in academic literature has discovered that the most represented fraud cases were Initial Coin Offering (ICO) scams, Ponzi schemes, phishing, mining malware, pumps and dumps and wallet scams (Trozze et al., 2022). Based on this research, there is consensus among experts that there are no clear definitions with respect to the specific crypto-native frauds, causing implications in assessing the risk levels of these fraud events. Nevertheless, it is clear that the cryptocurrency frauds can be usually classified as cyber-enabled frauds, meaning that information and communication technologies are used to commit crimes that could otherwise be also possible offline, yet on a much larger scale (McGuire & Dowling, 2013). The frauds associated with market manipulation in DeFi are often very similar to those of traditional finance, yet are now enabled with novel technology (Bartoletti et al., 2018; Reddy & Minnaar, 2018).

5.2.15. Regulatory Evasion

Regulatory evasion is a risk of failure to comply with regulatory standard of a traditional financial service, yet with a different underlying technology (Deshmukh et al., 2021). Since many DeFi services are by nature similar to traditional banking services (investing, borrowing, lending, insurance, etc.), they may still need to comply with the traditional regulations and may not be exempted from it simply due to performing these services using an alternative technology, such as blockchain. This creates regulatory tensions and risk of accidental or purposeful failure to comply with already existing financial services regulations.

5.2.16. Dynamic Interactions

Risk that does not exist in traditional finance as DeFi offers cross-border, unlimited user interaction that may result in emergent unprecedented risks (Deshmukh et al., 2021). This risk is still largely unexplored as it is also not clear how large-scale DeFi adoption will impact the global financial system. Moreover, experts have voiced concerns that there may be emergent risk due to interoperability of DeFi and traditional finance (Dale, July, 2020).

5.2.17. Flash crashes or price cascades

Flash crashes or price cascades is a risk of significant loss of assets due to price cascades that cannot be stopped or frozen in a traditional manner (Deshmukh et al., 2021). When the number of liquidations dramatically increases in a short period of time, the extreme decrease in asset price results in large losses for the investors. In traditional finance, brokers are able to freeze transactions to prevent this from happening, but such strategies are not suitable for blockchain systems governed by smart contracts.

5.2.18. Regulation Risk

The risk of regulation is the 18th risk that was decided to add to the list of risks of Decentralized Finance to assess whether the industry will perceive regulation itself to be a risk to the crypto-markets. While regulation is necessary to create legal clarity and protect DeFi users as outlined in the goals of MiCA, it can also pose the risk of creating barriers to innovation and technology development (European Commission, 2020a). Researchers in the field of DeFi regulation have highlighted that the current retroactive policy approach could have disastrous effects on the industry and be even counter-productive in addressing the AML and CFT concerns (Salamatin, 2021). Thus, there exists a risk of regulations that result in effects that are opposite of the intended goals.

5.3. Ranking of the Risks

The 18 risks of Decentralized Finance listed in the previous section were demonstrated to the interviewees. The interviewees were asked to go through the list and first identify which of the 18 risks are perceived by them to be a risk on a simple ”yes” or ”no” basis. This approach allows the researcher to understand who perceives the specific risks of DeFi depending on their position in the crypto markets and provides an opportunity for the interviewees to carefully go through the list and understand the risks before ranking them, as well as to ask any questions or clarifications about the risks. After that, the interviewees were asked to select the five most critical risks in their view and rank them in order of criticality, where criticality is explained to the interviewee as the importance that a particular risk is minimized.

5.3.1. Analyzing the Responses

In the following subsections, the 18 risks are listed on the left side of the ranking tables, while the identified risks and rankings are indicated in each column, referring to a specific respondent. The cells filled with an ”x” indicate that this risk is identified as ”perceived and applicable” to the interviewee. If a cell is empty, the interviewee did not perceive the risk or found it inapplicable to their line of services, while N/A indicates that the respondent was not able to assess whether they perceive the risk or find it applicable. If a cell is color-filled with purple, marked with an ”x” and is accompanied by a number 1-5, it means that the interviewee identified it to be one of the 5 most critical risks, with number 1 being the most critical, and 5 the least critical among the top 5. The interviewees are listed on the top row and are represented with their Interviewee ID and stakeholder group: LE = legal expert, CI = crypto-issuer firm Employee, CASP = CASP firm employee, II = institutional investment firm employee.

Once all of the rankings are compiled in the same table, it is possible to derive the most critical perceived risks with the highest total weighted points. This is done by assigning scores to the identified and top 5 risks. If the interviewee answered ”yes” whether they perceive a specific risk, it was marked with ”x” and is assigned 1 point. If the interviewee placed a risk on the 5th place among the top 5 most critical risks, the risk is assigned 2 points. Consequently, 4th place corresponds to 3 points, 3rd place to 4 points, 2nd place to 5 points and 1st place - the most critical perceived risk - to 6 points. The weight of all interviewees in the ranking is assumed to be same. It is also worth noting that some interviewees, such as 18 and 14, were not able to distinguish the level of criticality between certain risks and ranked more than one risk the same spot in the top 5. In this case, the points still counted towards the total score of the specific risk. The scoring system is summarized below in Table 5.1.

Table 5.1: Risk Ranking Scoring System

Symbol	Points
x1	6
x2	5
x3	4
x4	3
x5	2
x	1

5.3.2. Legal Expert Group

By analyzing the risk rankings of the respondents from the legal expert groups presented in Table 5.2, it can be seen that fraud and market manipulation is ranked as the most critical risk since it has the highest total weighted score of 37 points. Financial crime possesses the second highest total score of 36 points, while smart contract risk is tied at the 3rd place with key management at 31 points. Governance mechanisms and counterparty risk, which occupy 4th and 5th highest total score rank, have 16 and 15 points respectively. It is also worth noting that it is one of the two respondent groups, along with the institutional investment group, where some respondents were not able to assess whether a certain risk is perceived by them. Legal experts often deal with legal issues around crypto-markets and work closely with policies, and are likely to deal with the legal implications of almost any of the 18 risks' occurrences. However, interviewee 12 was not able to answer if oracle risk and challenging routine maintenance and upgrades present a risk, while interviewee 16 was not able to assess miner risk. While this has a minor impact on the scores, the interviewees were allowed to not provide an assessment as this is also a finding. It could indicate that the legal experts were not well-familiar with the unanswered risks, or not sure how the occurrence of the risk would impact them. Moreover, some interviewees were not able to rank the most critical risks from 1 to 5. For example, interviewee 18 responded that while they can select the most and second most critical risk, they cannot make the distinction in criticality between miner risk, challenging routine maintenance and upgrades, forks and governance mechanisms risks. Thus, the interviewee awarded all of these 4 risks with the 3rd place. In a way, it is also a finding and shows that not everybody is able to make a distinction in criticality and sometimes several risks can be perceived as equally critical by one respondent. Furthermore, one may also notice that miner risk and risk of challenging routine maintenance and upgrades are the some of the least perceived risks in this group, only above redress of disputes and dynamic interactions risks. However, a low total weighted score does not necessarily mean that the respondents do not consider the risk to be important, but more likely less applicable and frequent in their line of work. To summarize, the risks with the 5 highest total weighted points are listed below:

- 1. Fraud and market manipulation - 37 points
- 2. Financial crime - 26 points
- 3. Key management and smart contract risk - 19 points
- 4. Governance mechanisms - 16 points
- 5. Counterparty risk - 15 points

Table 5.2: Risk Rankings by the Legal Expert Group

Num	Risks	1 LE	2 LE	11 LE	12 LE	15 LE	16 LE	18 LE	19 LE	Total Weighted Points
1	Market risk	x	x	x		x	x3	x	x	10
2	Counterparty risk	x	x	x	x5	x2	x		x3	15
3	Liquidity risk	x	x	x4		x5	x	x	x	10
4	Transaction risk	x	x		x4	x	x	x	x	9
5	Smart contract risk	x2	x1		x		x	x	x2	19
6	Miner risk	x		x	x		N/A	x3	x	7
7	Oracle risk	x3	x2		N/A		x	x	x	12
8	Routine maintenance and upgrades	x			N/A		x	x3	x	7
9	Forks	x					x	x3	x	7
10	Key management	x4		x1	x	x1	x	x	x	19
11	Governance mechanisms	x	x4	x	x		x4	x3	x4	16
12	Redress of disputes	x		x	x		x5	x		6
13	Financial crime	x	x5	x	x2	x3	x1	x1	x	26
14	Fraud and market manipulation	x1	x3	x5	x1	x4	x2	x2	x1	37
15	Regulatory evasion	x	x	x3	x3		x	x		12
16	Dynamic interactions	x	x		x		x	x		5
17	Flash crashes or price cascades	x	x	x		x	x	x	x5	8
18	Regulation risk	x 5		x2			x	x	x	10

5.3.3. Crypto-Asset Issuers Group

There were only 2 respondents from the crypto-asset issuer group in this study, Interviewee 3 and 8, thus the insights in this section are more limited compared to the other groups. The calculation of total scores of risk perceptions of this group is presented in Table 5.3. Due to the low number of interviewees, there is a significant overlap in scores between numerous risks, especially those that have not been selected in the top 5 most critical risks by either of the respondents. Both interviewees were also very risk perceptive, as Interviewee 3 identified all 18 risks as perceived and applicable, while Interviewee 8 only did not perceive counterparty risk and miner risk. Since there are only 2 respondents, the highest total weighted score reaches only a 7, which is shared by the smart contract risk, key management and regulation risk. It is the only group to have 3 risks share the same number of points. The second highest score of 6 is assigned to financial crime, while market risk liquidity risk are tied on the third place with a score of 5. On the fourth spot, with a mutual score of 4, the group placed miner risk and oracle risk.

The only score lower than 4 in this group is 2, and all of the remaining risks, besides counterparty risk, automatically score these points if they were perceived by the respondent but not placed in the top 5. It would not make sense to place 9 risks on the 5th spot, thus it has been decided that since none of these 9 risks were perceived as top 5 most critical by any of the 2 respondents, no risk is placed on the 5th rank. It is also consistent across other groups that a risk placed in the group's top 5 ranking is listed in the top 5 most critical risks by at least one respondent in that group. To summarize, the crypto-asset issuer group perceives the following risks to be most critical according to the analysis:

- 1. Smart contract risk, key management and regulation risk - 7 points
- 2. Financial crime - 6 points
- 3. Market risk and liquidity risk - 5 points
- 4. Miner risk and oracle risk - 4 points
- 5. N/A

Table 5.3: Risk Rankings by the Crypto-Asset Issuer Group

Num	**Risks**	3 CI	8 CI	Total weighted points
1	Market risk	x	x3	5
2	Counterparty risk	x		1
3	Liquidity risk	x5	x4	5
4	Transaction risk	x	x	2
5	Smart contract risk	x2	x5	7
6	Miner risk	x3		4
7	Oracle risk	x4	x	4
8	Routine maintenance and upgrades	x	x	2
9	Forks	x	x	2
10	Key management	x1	x	7
11	Governance mechanisms	x	x	2
12	Redress of disputes	x	x	2
13	Financial crime	x	x2	6
14	Fraud and market manipulation	x	x	2
15	Regulatory evasion	x	x	2
16	Dynamic interactions	x	x	2
17	Flash crashes or price cascades	x	x	2
18	Regulation risk	x	x1	7

5.3.4. CASP Group

Looking at the analysis of risk rankings by the CASP group presented in Table 5.4, it is seen that market risk is by far the most critical perceived risk among this group. The CASP respondent groups is more diverse compared to the other groups, as the activities and services in which the respondents participate vary greatly from advice provision to provision of financial services such as banking, exchange or insurance. Nevertheless, it is clear that the concern for market risk is shared by every respondent of this group, since all 6 of them have identified it in their top 5 most critical perceived risks, while Interviewees 5,9,13 and 14 ranked it as the first most critical, allowing it to score 30 points. The second highest score is assigned to liquidity risk at 20 point, with 4/6 respondents placing it in their top 5. At 16 points, the third place is occupied by both key management and regulation risk. Just one point below, the fourth spot is occupied by regulatory evasion, followed by the final 5th rank tied between smart contract risk and fraud and market manipulation at 13 points.

Similarly to the legal experts' responses, the last 3 highest total scores have a relatively small difference, indicating that with a larger response sample these ranks could change to at least some extent. When looking at the least perceived risks it is easy to see from the table that technical risks such, namely miner risk and oracle risk, and operational risks such as challenging routine maintenance and upgrades and forks have received very low scores varying from 3 to 6 points and have not once appeared in any respondent's top 5 list. However, all 6 respondents did perceive the risk of challenging routine maintenance and upgrades of blockchain-based systems as a risk, but none of them considered it to deserve a spot in the top 5. The risks with the highest 5 scores are summarized below:

- 1. Market risk - 30 points
- 2. Liquidity risk - 20 points
- 3. Key management and Regulation risk - 16 points
- 4. Regulatory evasion - 15 points
- 5. Smart contract risk and Fraud and market manipulation - 13 points

Table 5.4: Risk Rankings by the Crypto-Asset Service Provider Group

Num	Risks	4 CASP	5 CASP	9 CASP	13 CASP	14 CASP	17 CASP	Total weighted points
1	Market risk	x3	x1	x1	x1	x1	x5	30
2	Counterparty risk		x	x5	x	x5		6
3	Liquidity risk	x1	x4	x2	x3	x	x	20
4	Transaction risk	x	x3		x	x		7
5	Smart contract risk	x5			x2	x2	x	13
6	Miner risk		x	x			x	3
7	Oracle risk	x	x	x	x			4
8	Routine maintenance and upgrades	x	x	x	x	x	x	6
9	Forks		x		x	x		3
10	Key management	x2	x2	x	x	x4	x	16
11	Governance mechanisms		x	x	x		x3	7
12	Redress of disputes		x	x	x	x	x	5
13	Financial crime		x	x	x4		x	6
14	Fraud and market manipulation	x	x5	x	x	x2	x4	13
15	Regulatory evasion		x	x4	x	x3	x2	15
16	Dynamic interactions	x	x	x	x		x	5
17	Flash crashes or price cascades	x4	x	x	x5	x	x	9
18	Regulation risk	x		x3	x	x3	x1	16

5.3.5. Institutional Investors

Similarly to the crypto-asset issuer group, there were only a few interviewees from the institutional investment firms. As a result, the difference between risks' total weighted points is also relatively small, with overlaps of the same weighted score for numerous risks. The analysis is presented below in Table 5.5. The most critical risk perceived by the 3 experts from the institutional investment group is revealed to be regulation risk, scoring a total of 13 points. Regulation risk appeared in the top 5 most critical risk list of every respondent, being ranked as second most critical for Interviewee 6, and third most critical for Interviewee 7 and 10. As explained in the previous chapter's section on perceptions of CASPs on regulation in the EU, institutional investors are heavily regulated and strict crypto regulations pose risks to the ability of these institutions to engage in activities and services related to crypto-markets. The second highest total weighted score of 11 is assigned to financial crime, the risk which 2/3 interviewees listed in their top 5. The third highest score is 9, and is shared between fraud and market manipulation and market risk, while just 1 point lower smart contract risk and key management occupy the 4th highest score. Lastly, oracle risk and governance mechanisms have the 5th highest score of 4, and appear in at least one of the respondents' top 5 most critical risk. Also, it is important to note that this is the only group where none of the interviewees identified a certain risk to be their perceived risk, in this case the risk of challenging routine maintenance and upgrades. One of the interviewees (ID 7) also responded with "not able to assess" when asked about this risk. In summary, the risks with the 5 highest total weighted points in the institutional investor group are listed below:

- 1. Regulation risk - 13 points
- 2. Financial Crime - 11 points
- 3. Fraud and market manipulation and market risk - 9 points
- 4. Smart contract risk and key management - 8 points
- 5. Oracle risk and governance mechanisms - 4 points

Table 5.5: Risk Rankings by the Institutional Investor Group

Num	Risks	6 II	7 II	10 II	Total weighted points
1	Market risk	x1	x4		9
2	Counterparty risk	x	x		2
3	Liquidity risk	x	x	x	3
4	Transaction risk		x	x	2
5	Smart contract risk	x	x	x1	8
6	Miner risk		x	x	2
7	Oracle risk	x	x	x5	4
8	Routine maintenance and upgrades		N/A		0
9	Forks		x		1
10	Key management	x5	x	x2	8
11	Governance mechanisms		x	x4	4
12	Redress of disputes		x	x	2
13	Financial crime	x3	x1	x	11
14	Fraud and market manipulation	x4	x2	x	9
15	Regulatory evasion	x	x	x	3
16	Dynamic interactions		N/A	x	1
17	Flash crashes or price cascades	x	x5		3
18	Regulation risk	x2	x3	x3	13

5.4. Results of Analysis

This sections provides an answer to the second sub-question *"What are the most critical risks perceived by the industry experts?"*. As can be seen in the table below, the risks with 5 highest total weighted criticality scores are presented for each group. Even though all interviewees were asked to select the 5 most critical perceived risks among the list of 18, due to a limited number of interviewees, especially in crypto-asset issuer and institutional investor groups, more than one risk occupies a spot in the top 5 criticality rank due to the tie in points between several scores. Most of the top 5 spots are occupied by 1 or 2 risks, with several having 3 risks matching in total points. However, in the crypto-asset issuer group, since there are only 2 respondents, almost all the risks after the top 4 scores are in a tie, mostly because the interviewees identified them to be a perceived risk, but not placing them in the top 5, resulting in many risks with a total of 2 points. Thus, since none of these two risks with 2 points were selected by the interviewees as "top 5 critical", Chapter 6 will not consider them as critical in the combined analysis.

Table 5.6: Differences in Risks with the Highest 5 Total Weighted Points Across all Respondent Groups

Rank by total weighted points	LE	CI	CASP	II
1	Fraud and market manipulation	Smart contract & Key management & Regulation risk	Market risk	Regulation risk
2	Financial crime	Financial crime	Liquidity risk	Financial crime
3	Key management & Smart contract risk	Market risk & Liquidity risk	Key management & Regulation risk	Fraud and market manipulation & Market risk
4	Governance mechanisms	Miner risk & Oracle risk	Regulatory evasion	Smart contract risk & Key management risk
5	Counterparty risk	N/A	Smart contract risk & Fraud and Market Manipulation	Oracle risk & Governance mechanisms

Looking at the overview of the risks with the 5 highest total points across all groups, there are certain trends that emerge. Fraud and Market Manipulation is a risk that is ranked high in legal expert group, CASP group and institutional investor group. Similarly financial crime is perceived as one of the most critical risks in all groups except for the CASP group. The only 2 risks that were consistently perceived as critical across all groups is key management and smart contract risk. Another insight obtained from the analysis is that the regulation risk, which is not originally a risk in the WEF, was ranked as one of the most critical risks perceived by crypto-asset issuers, CASPs and institutional investors. Looking at which risks did not make the top 5 spots, it is seen that transaction risk, risk of challenging routine maintenance and upgrades, forks, dynamic interactions, flash crashes and redress of disputes were not identified as most critical by any groups. However, it does not mean that these risks are unimportant to address or minimize, it only means that the interviewees were on average not very perceptive of these risks.

6

Analysis of Risks in MiCA

6.1. Summary of the Chapter

This chapter answers the last sub-question of the research: *To what extent does MiCA address the risks of the industry experts?*. The question is addressed by performing a summative content analysis on the MiCA framework to understand whether the 18 risks presented in Chapter 5 are addressed in the regulation. This is carried out by initially reviewing the MiCA framework and creating keywords for each of the 18 risks to then assess how they are dealt with in the framework. The extent to which the risks are addressed are categorized into 3 types: addressed, partially addressed and not addressed. Once each risk is assessed and categorized, the results of Chapter 5 are combined with the content analysis assessment to demonstrate which stakeholders' risks are addressed, partially addressed or not addressed in MiCA.

Section 6.2 explains the methodology of the content analysis and how the keywords and indicators are used to assess to what extent a risk is addressed in the regulation. Section 6.3 presents the content analysis itself, with each subsection corresponding to each of the 18 risks presented in Chapter 5. At the end of each subsection, a choice for one of the 3 categories is made based on the analysis methodology. Section 6.4 presents the overview of content analysis, and Section 6.5 presents the combined overview of risk perception from Chapter 5 and content analysis from Chapter 6. Finally, Section 6.6 concludes the chapter by providing a reflection on the results.

To summarize the chapter, the content analysis revealed that the market and legal compliance risk are largely addressed or partially addressed in the MiCA framework, while many of the technical and operational risks remain unaddressed. Most of the risks classified as "addressed", with an exception of redress of disputes, were identified as most critical by at least 1 respondent group. Similarly, at least 3 out of 4 respondent groups identified 3 out of 5 risks classified as "partially addressed" as most critical. Even though dynamic interactions (emergent risks) and flash crashes or price cascades are partially addressed in the framework, no respondent group ranked these risks in their top 5 ranking. Lastly, among the risks classified as "not addressed", smart contract risk is perceived as most critical by all respondent groups, while 2 of the other "unaddressed risks", miner risk and oracle risk, were only identified as the most critical by crypto-asset issuers.

6.2. Methodology: Content Analysis

In the previous chapter, the ranking of the risks presented in this report is obtained by the means of expert interviews from different parts of the field. This analysis revealed what risks are perceived by each group of industry experts, and in this chapter the process and results of the content analysis of the MiCA frameworks are presented to explore and demonstrate which risks are currently addressed and missing from the regulation.

The content analysis is performed by reviewing the entire MiCA framework and understanding what risks of crypto-assets and services are addressed by the articles. Ideally, a policy is always designed to achieve specific strategic goals (Schouwstra & Ellman, 2006). Therefore, since reducing risks of crypto-markets and consumer protection is one of the main goals of the MiCA framework, it is useful to know what risks does it address and whose risks does it not address.

To understand what risks are addressed in the MiCA framework, a framework is needed in order to systematically categorize the risks according to the extent to which they are addressed in the MiCA framework. This has been carried out according to the classification presented in Table 6.1, based on the Summative Content Analysis methodology for qualitative research adopted from (Hsieh & Shannon, 2005).

Firstly, the risks are divided into three classes: ”addressed”, ”partially addressed” and ”not addressed”. A risk is considered to be addressed in the MiCA framework if it is directly mentioned, elaborately addressed and addressed by an article or chapter that is designed to minimize the said risk. If it is indirectly mentioned, briefly explained and only partially addressed in a limited manner and only for specific cases, then the risk is considered to be ”partially addressed”. Lastly, a risk is considered ”not addressed” if it is not directly mentioned, defined and reflected by an article or chapter in the MiCA framework. In order to direct the content analysis, keywords are used to search for the risks The keywords are the risks and any synonymous or relevant terms that may aid in locating the risk when inspecting the MiCA framework. An example of an ”addressed” risk is the risk of fraud and market manipulation. It is the most covered risk in the entire framework with numerous articles addressing it both directly and indirectly, providing also definitions and elaborate explanations of what constitutes to be market manipulation and insider dealing. Key Management is an example of a ”partially addressed” risk, as it only addresses the situation where custodial solutions are possible, thus excluding the decentralized open-source projects from the scope. Finally, smart contract risk is classified as ”not addressed”, as it is inconsistently presented in the framework under various terms and does not have its own article or chapter, being only present as one of the many requirements in white paper descriptions and authorization process. More information on these risks will be presented in the further sections.

Table 6.1: Content Analysis Methodology - Risk Classification and Examples

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

6.3. Content Analysis

In this section, the content analysis is presented to assess which risks are addressed, partially addressed or not addressed in the MiCA framework. Each risk will be explored in terms of its presence in the framework, followed by the classification decision and the supporting justification.

6.3.1. Market Risk

Keywords: Market risk, financial risk, monetary risk, price, loss, depreciation, devaluation, volatility, fluctuation

Since market risk is the broadest risk in the WEF's risk framework, the assessment of the extent to which it is addressed in the MiCA framework can be more subjective. As explained in Chapter 3, market risk is resulted from (1) market conditions, (2) idiosyncratic behavior of traders and (3) novel market information. However, market risk in crypto-markets is especially critical due to the high volatility. Market conditions are a result of many different factors that may lie outside of the market itself, and even the most regulated markets are not safe from this risk (Hartmann, 2010).

Nevertheless, MiCA introduces regulations on many previously unregulated types of crypto-assets, such as asset-referenced tokens (stablecoins), which as of July 2022 have a market capitalization of over 150 billion USD and daily trading volume of over 50 billion USD. If such issuers are unregulated, mismanaged or unsupervised, there is a significantly increased market risk for the investors, as shown by the 40 billion USD crash of stablecoin Terra-Luna ($LUNA) in 2022 (Mukherjee, 2022).

Chapters 1-6 (Articles 15-41) of the MiCA framework provide broad and extensive regulatory requirements for stablecoin issuers, ranging from authorization for operation to being subject to strict compliance and constant monitoring from the supervisory authorities. Moreover, there are specific rules with respect to the governance arrangements (Article 30), conflict of interest (Article 28), reserve management (Article 32-33) and investment rules (Article 34). Moreover, Title VI: "Prevention of Market Abuse involving crypto-assets", and more specifically Article 80, addresses "false signals of supply, demand or price of crypto-assets", price manipulation causing "an abnormal or artificial level", "dissemination of information leading to false signals" and other forms of manipulation that may pose market risk to the participants. Therefore, it can be argued that the market risk is "addressed" in the MiCA framework. However, this only applies to the regulated crypto-markets that fall within the scope of MiCA framework. Decentralized projects with no legally liable individuals running or operating on open-source smart contracts are not addressed in the MiCA framework.

6.3.2. Counterparty Risk

Keywords: Counterparty, credit risk, settlement risk

Counterparty risk is an the risk of a counterparty's willing or unwilling failure to fulfill their end of financial instrument obligations and by the WEF's definition includes credit risk and settlement risk. Due to the authorization and licensing procedures for asset-referenced tokens issuers, e-money issuers and CASPs, counterparty risk is indirectly addressed on the institution-to-institution level due to the presence of liable individuals in licensed crypto-asset issuer and service companies. However, it is not directly defined or addressed anywhere in the framework and is only mentioned on page 65, Article 34, paragraph 3: *"All profits or losses, including fluctuations in the value of the financial instruments referred to in paragraph 1, and any counterparty or*

operational risks that result from the investment of the reserve assets shall be borne by the issuer of the asset-referenced tokens. In other words, if an asset-referenced token issuer decides to invest their reserve assets (*"only in highly liquid financial instruments with minimal market and credit risk"* - paragraph 1), they bear the burden of counterparty risk. Credit risk is not addressed explicitly in the framework either, with the exception of minimal credit risk requirement for investments in Article 34, paragraph 1, and assessment of credit risk in Article 32, paragraph 4, clause (c). However, settlement risk is addressed in Article 35, paragraph 2, clause (d), stating that issuers of asset-referenced tokens are obliged to construct policies on *"settlement conditions when those rights are exercised"*, referring to the rights of token holders explained in paragraph 1 of the article. Moreover, Article 68, paragraph 1, clause (h) obligates trading platforms to *"set procedures to ensure efficient settlement of both crypto-asset transactions and fiat currency transactions"*, while paragraph 8 adds that *"Crypto-asset service providers that are authorised for the operation of a trading platform for crypto-assets shall complete the final settlement of a crypto-asset transaction on the DLT on the same date as the transactions has been executed on the trading platform"*. In conclusion, MiCA addresses the settlement risk for consumers when dealing with stablecoin issuers and CASPs, allowing counterparty risk to be classified as "partially addressed".

6.3.3. Liquidity Risk

Keywords: Liquidity, reserve

Liquidity risk is the risk of incurring insufficient funds or assets to support the value of a financial asset. Liquidity risk is mentioned and addressed in the MiCA framework in numerous articles related to crypto-asset issuers and service providers. Article 17, 21 and 30 require asset-referenced tokens issuers to communicate the mechanisms ensuring liquidity and liquidity management policy in their whitepaper during the authorization process. Article 32, paragraph 4, clause (c) requires the asset-referenced token issuers to provide a *"detailed assessment of the risks, including credit risk, market risk and liquidity risk resulting from the reserve assets"*. Article 35, paragraph 5, clause (a) states that EBA and ESMA *"shall develop further technical standards specifying the obligations imposed on the crypto-asset service providers ensuring the liquidity of asset-referenced tokens"*. Moreover, Article 41 provides additional liquidity monitoring requirements for issuers. With respect to CASPs, MiCA outlines required operational rules in Article 68, paragraph 1, clause (f), stating that the rules must at least *"set conditions for crypto-assets to remain accessible for trading, including liquidity thresholds and periodic disclosure requirements"*. Therefore, liquidity risk is addressed by the regulators in the MiCA framework for both crypto-asset issuers and CASPs. However, there will be more specific guidelines from EBA and ESMA in the future with respect to the liquidity management.

6.3.4. Technical Risks

Keywords: Transaction risk (transaction, layer 1, blockchain/DLT, malfunctioning, double spending, expensive transactions), smart contract risk (smart contract, contract, protocol, mechanism, terms, conditions, rules), miner risk (miner risk, mining, proof-of-work, validation, abuse), oracle risk (oracle, information, communication), risk of challenging routine maintenance and upgrades (routine, maintenance, upgrade, update, operation, inspection), forks (fork, protocol change)

Transaction risk, smart contract risk, miner risk, oracle risk, risk of challenging routine maintenance and upgrades, and forks are the technical risks of crypto-markets that are not addressed or mentioned anywhere in the MiCA framework. Therefore, the content analysis related to these risks is combined in this subsection due to the absence of definitions and articles related to them. Smart contracts, which provide essential functionalities for the blockchain systems, are not the central topic of any articles. Article 13, which lists obligations of crypto-asset issuers, states in paragraph 1, clause (d) that issuers must *maintain all of their systems and security access protocols*

to appropriate Union standards, which broadly encompasses technical and IT related risks, but without any further specification. This is because the standards are still to be developed by EBA and ESMA, as stated in the detailed overview of the MiCA framework. However, there are occasional mentions of technical aspects of crypto-assets and services. Article 21, paragraph 1 lists relevant material modifications that must be reflected in the whitepaper, which includes *"the mechanism through which asset-referenced tokens are issued, created and destroyed"*, *"the mechanisms to ensure the redemption of the asset-referenced tokens or to ensure their liquidity"*, and *"the protocols for validating the transactions in asset-referenced tokens"*, referring to the consensus mechanisms. The only technical aspects mentioned in the MiCA framework include obligations for asset-referenced token issuers to describe their cyber security and ICT systems in authorization procedures (Article 16, paragraph 2, clause (n)) and the liability of CASPs in case of cyber attacks and malfunctions. Due to the lack of definitions, articles, guidelines, standards and any concrete points of action for market participants, transaction risk, smart contract risk, miner risk, oracle risk, risk of challenging routine maintenance and upgrades and forks are classified as "not addressed" in the MiCA framework.

6.3.5. Key Management

Keywords: keys, cryptographic keys, key management, access, custody, storing, reserve management

Key management is the risk of loss of cryptographic key pairs that is relevant not only for issuers and CASPs, but also for the users. Key management is largely described as "custody" in the MiCA framework and is defined in Article 3, paragraph 10: *"the custody and administration of crypto-assets on behalf of third parties' means safekeeping or controlling, on behalf of third parties, crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys"*. The reason for this is due to the requirement of issuers and CASPs to obtain a third-party custodian for access to the company's reserves. The requirements for reserve access and custodian solutions are elaborated in Article 33 for issuers and Article 67 for CASPs.

"Crypto-asset service providers that are authorised for the custody and administration of crypto-assets on behalf of third parties shall establish a custody policy with internal rules and procedures to ensure the safekeeping or the control of such crypto- assets, or the means of access to the crypto-assets, such as cryptographic keys." - Article 67, paragraph 3

However, MiCA does not provide any guidelines with respect to the decentralized crypto-assets and CASPs with no liable individuals and registered companies, and only addressing the risk of key loss in custodial requirements. Furthermore, there are no obligations or guidelines that are set out for decentralized assets and services that do not have KYC protocols to address the key management risk for users. Thus, key management is classified as "partially addressed" in the MiCA framework.

6.3.6. Governance Mechanisms

Keywords: Governance mechanism, governance, governance arrangements, management, voting, abuse, consensus, concentration, bribery

Governance mechanisms present the risk of governance abuse due to concentration of tokens or bribery. MiCA has dedicated numerous articles to governance structures, especially for issuers of asset-referenced tokens. While governance mechanisms are not explicitly defined in the MiCA framework, the requirements are clarified in the detailed description and Article 30:

"Issuers of asset-referenced tokens should have robust governance arrangements, including a clear

organisational structure with well-defined, transparent and consistent lines of responsibility and effective processes to identify, manage, monitor and report the risks to which they are or might be exposed. The management body of such issuers and their shareholders should have good repute and sufficient expertise and be fit and proper for the purpose of anti-money laundering and combatting the financing of terrorism (...)" - Article 30, paragraph 1

Article 16, paragraph 2, clause (e) requires asset-referenced token issuers to provide *"a detailed description of the applicant issuer's governance arrangements"* during the authorization process, and include this description in the whitepaper (Article 17, paragraph 1, clause (a)). Article 20, paragraph 3 states that authorization is "withdrawn" shall governance arrangements suggest a "failure" to the regulator. Article 30 focuses purely on governance of asset-referenced tokens issuers, providing a two-page description of required governance arrangements which include, among other, background checks on governing individuals for competence, compliance and reputation, conflict of interest policies, risk management policies and asset ownership boundaries. Article 31 provides own funds requirements for issuers and Article 32 lists obligations on reserve management, all of which are designed to address the risk of governance mechanism abuse. Similar rules are listed in MiCA for CASPs in Article 54, specifically in paragraph 2, clauses (e), (f) and (g) which present authorization requirements for service providers. Thus, since the regulators provides governance rules, requirements and procedures for all subjects within its scope, it can be concluded that the risks of governance mechanisms are "addressed" in the MiCA framework.

6.3.7. Redress of Disputes

Keywords: Dispute, legal procedure, litigation, court, governance, authority, mediation

Redress of disputes is the risk associated with challenging nature of conflict resolution in platforms different to traditional finance. Due to the current lack of regulatory frameworks, rules and guidelines with respect to crypto-asset issuers and CASPs, it can be challenging to resolve a legal dispute originating from decentralized systems in centralized courts. Partially, the problem also spurs from the debate on legality of smart contracts as actual binding contracts in the traditional court system. Article 27 for crypto-asset issuers and Article 64 for CASPs require the companies to *"establish a complaint handling procedure"*, which could be the first step in addressing disputes between customers and the private sector. Article 91 further elaborates complaint handling protocol by authorities, shall the customer not be able to resolve the dispute with the issuers and service providers:

"Competent authorities shall set up procedures which allow clients and other interested parties, including consumer associations, to submit complaints to the competent authorities with regard to issuer of crypto-assets, including asset- referenced tokens or e-money tokens, and crypto-asset service providers' alleged infringements of this Regulation. In all cases, complaints should be accepted in written or electronic form and in an official language of the Member State in which the complaint is submitted or in a language accepted by the competent authorities of that Member State" - Article 91, paragraph 1

Moreover, Article 92, 93, 94 and 95 provide extensive information on decision-making procedures, sanctions, fines, appeals and publishing of decisions when issuers and service providers are in breach of regulation. Due to introductions of such rules to the newly regulated crypto-markets, it can be argued that the regulator has "addressed" the redress of disputes in the MiCA framework.

6.3.8. Legal Compliance Risks

Keywords: Financial crime (financial crime, crime, criminal, money-laundering, financing of terrorism, tax evasion), fraud and market manipulation (fraud, manipulation, scam, insider, false, dishonest, misleading, misinformation, dealing, bribery, abuse), regulatory evasion (evasion, compliance, registration, authorization)

Financial crime, fraud and market manipulation and regulatory evasion are legal compliance risks the analysis for which is presented jointly in this subsection due to the overlaps in rules and procedures associated with them in the MiCA framework.

While addressing the risk of governance mechanisms, Article 30 requires the management crypto-asset issuers to *"have good repute and sufficient expertise and be fit and proper for the purpose of anti-money laundering and combatting the financing of terrorism"*, which is assessed in the authorization process for issuers Article 16, and for CASPs in Article 59 and 60. Moreover, the management of these companies is required to demonstrate proof of absence of any criminal record in the commercial and finance sectors, and more specifically absence of AML and CFT legislation breaches. Furthermore, MiCA requires all crypto-asset issuers and service providers serving EU clients to establish a registered office in the EU to increase supervision and monitoring (detailed description, page 21, paragraph 27). The Commission also aims to reach coherence between MiCA and the upcoming AML directive to increase efforts in combatting illicit activities in crypto-markets (impact assessment, page 7). Lastly, EBA and ESMA will provide more specific technical standards with respect to the monitoring tools to address the risks of financial crime by inspecting governance arrangements, internal control mechanisms, accounting practices and other aspects listed in Article 30, paragraph 1.

Moreover, fraud and market manipulation rules are arguably the most elaborated rules in the MiCA framework. Title VI, Articles 76-80 provide detailed descriptions of fraud and manipulation in crypto-markets, such as insider information dealing and trading (Article 78), disclosure of classified information (Article 77 and 79), and manipulation of supply, demand and price signals, disrupting trading platforms and creating unfair trading conditions (Article 80). Title VII, Articles 81 to 121 explain lengthy regulatory and enforcement procedures related to the breaches of the regulation. Since MiCA applies these rules to all participants in the crypto-markets, the risk of financial crime, fraud and market manipulation and regulatory evasion are classified as "addressed in the MiCA framework.

6.3.9. Dynamic Interactions

Keywords: Dynamic interactions, emergent risk, new risk, black swan risk, threat, monitoring, trends

Dynamic interactions is an emergent risk resulting of increased use case of blockchain technologies in financial applications. As transactions powered by DLT are instant, often irreversible, unstoppable and cross-border, there is a risk of creating unprecedented situations that themselves pose a risk of the unknown. Due to the vague nature of this risk it is challenging to assess if it is addressed in the MiCA framework. Nevertheless, the Commission recognizes that there may be new risks created with the further adoption of crypto-assets:

"While the crypto-asset market remains modest in size and does not currently pose a threat to financial stability, this may change with the advent of 'global stablecoins', which seek wider adoption by incorporating features aimed at stabilising their value and by exploiting the network effects stemming from the firms promoting these assets" - Context of the Proposal, page 2.

Moreover, Article 122 explains the requirements for the report that will be created by the Com-

mission in consultation with EBA and ESMA 36 months after the date of MiCA's entry into force. This report will provide insights into the developments of *"new means of payment instruments"* (paragraph 1, clause (m)), *"a description of developments in business models and technologies in the crypto-asset market"* (paragraph 1, clause (n)), and *"an appraisal of whether any changes are needed to the measures set out in this Regulation to ensure consumer protection, market integrity and financial stability"* (paragraph 1, clause (o)). The regulator thus established procedures and goals to further investigate the market trends and make necessary changes to the regulation. Since there is no definition and focus on emergent risks, but rather presence of steps that may indirectly produce insights on new risks, dynamic interactions are classified as "partially addressed" by the MiCA framework.

6.3.10. Flash crashes or Price Cascades

Keywords: Flash crashes, price cascades, flash loans, fluctuations, volatility, rapid drop, price volatility

Flash crashes or price cascades pose a risk of significant loss of assets due to rapid loss of asset value, during which the trading platform cannot freeze or stop transactions due to the decentralized nature of DLT-based financial services. This risk is not explicitly defined or explained in the MiCA framework, but according to Article 82 on power of competent authorities, the EBA and ESMA are able to *"request the freezing or sequestration of assets, or both"* (paragraph 2, clause (f)) and *"to impose a temporary prohibition on the exercise of professional activity"* (paragraph 2, clause (g)). Since flash crashes happen almost instantly and the delay in reporting and decisions listed above will not be able to timely order these measures.

However, flash crashes are tied to liquidity, as sufficient liquidity levels would allow for unproblematic liquidations. This aspect is explained in the earlier subsection on liquidity risk. In conclusion, no definitions of flash crashes or price cascades are provided in MiCA, and no articles focus on this specific risk. Although, the risk is indirectly addressed by several articles on liquidity requirements and by the authority of EBA and ESMA to order a freeze on assets and business activity. Despite the low probability of the measures' effectiveness in preventing flash crashes, the risk is still "partially addressed" in the MiCA framework.

6.3.11. Regulation Risk

Keywords: Regulation risk, regulatory risk, pressure, compliance cost, adoption barrier, innovation, conditions

Risk of regulation itself is an additional risk added to the WEF's list of 17 risk as it is an important aspect of constructing regulatory policies. Regulation presents the risk of creating unfavorable conditions for market players, potentially forcing them to relocate their activities outside of the European Union. Moreover, there is a risk of hindering innovation by introducing to many barriers to the market through compliance costs and leaving little to no room for experimentation. This risk has been mentioned numerous times in the MiCA framework:

"One of the strategy's identified priority areas is ensuring that the EU financial services regulatory framework is innovation-friendly and does not pose obstacles to the application of new technologies." - Context of the proposal, page 2

According to the European Commission, the MiCA framework is created with the goal of boosting favorable conditions to the developments of DLT-enabled finance:

"(...)At the same time, it will offer firms full access to the internal market and provide the legal

certainty necessary to promote innovation within the crypto-asset market." - Legal Basis, Subsidiarity and Proportionality, page 4

To ensure a fair system where smaller companies are not overwhelmed by compliance requirements, the Commission introduced the concept of "thresholds" to distinguish crypto-asset issuers from "significant" crypto-asset issuers.

"(...) to specify the criteria and thresholds to determine whether an asset-referenced token or an e-money token should be classified as significant and to specify the type and amount of fees that can be levied by EBA for the supervision of issuers of significant asset-referenced tokens or significant e-money tokens. - Text with EEA relevance, page 29, paragraph 72.

The MiCA framework presents additional obligations for significant crypto-asset issuers Articles 50-52 for significant e-money token issuers, Articles 39-41 for significant asset-referenced tokens. These distinctions seem to be based on number of tokens issued, number of token holders and trading volumes. However, there is no specific information found in the MiCA framework that provides concrete standards and numerical thresholds for these criteria. The Commission also ordered an Impact Assessment to understand the monetary and business implications on issuers and service providers created by the framework, which can be found on page 7 and is cited in the framework. On page 145, a pilot regime proposal is found for new types of crypto-assets and services to alleviate the burden of compliance for micro-sized experiments. Since the Commission does make the decision to distinguish crypto-asset issuers and service providers by size and apply different obligations, the regulation risk is concluded to be "partially addressed" in the MiCA framework.

6.4. Overview of Content Analysis

Having assessed which risks are addressed, partially addressed and not addressed in the MiCA framework using the methodology described in this chapter, the overview is compiled and presented on Figure 6.1. The risks classified as "addressed" are indicated in green and include market risk, liquidity risk, governance mechanisms, redress of disputes, financial crime, fraud and market manipulation and regulatory evasion. The risks indicated in blue are classified as "partially addressed" and include counterparty risk, key management, dynamic interactions, flash loans or price cascades and regulation risk. The risks indicated in red are classified as "not addressed" and consist of transaction risk, smart contract risk, miner risk, oracle risk, routine maintenance and upgrades and forks. The general trend is that none of the risks categorized as technical in the WEF's risk list are addressed in the MiCA framework. Moreover, 2 out of 5 operational risks (routine maintenance and upgrades and forks) are not addressed in the MiCA framework either. Among the market risk category, all 2 out of 3 risks are addressed, while 1 out of 3 is partially addressed. Both of 2 emergent risks, dynamic interactions and flash loans are also partially addressed. All 3 legal compliance category risks are addressed in the MiCA framework. In conclusion, the analysis reveals that the MiCA framework mostly addressed market and legal compliance risk, leaving out technical risks and 2 operational risks.

Figure 6.1: Content Analysis Results of the MiCA Framework

6.5. Combined Overview of Risk Perceptions and Content Analysis

Having carried out the analysis in Chapter 5 and 6, the results can be also combined in a single diagram as presented in Figure 6.2 below. The sunburst diagram presents the 18 risks of crypto-assets and services and categorizes them into 3 sections: addressed, partially addressed and not addressed, making the first 2 layers of the diagram the same as in Figure 6.1. The additional value of this chart lies in the third level of the sunburst diagram, where for every risk it is also indicated which groups had the said risk perceived in the "most critical 5 risks" list. This information is obtained from the final overview of results in Chapter 5.

Figure 6.2: Content Analysis Results of the MiCA Framework

6.6. Results of Analysis

To answer the sub-question ”To what extent does MiCA address the risks of the industry experts?”, one must consider Figure 6.2. By looking at the diagram, it becomes evident that risks perceived most often in the top 5 category among different respondent groups are in the addressed group indicated in green. Among addressed risks, only the redress of disputes risk has not appeared in the top 5 for any of the 4 respondent groups. Looking at the partially addressed risks section in blue, it can be noticed that even though key management, counterparty risk and regulation risk were present in at least 2 groups' top 5 risks, they are only partially addressed in the MiCA framework. On the other hand, MiCA framework partially addresses dynamic interactions and flash crash risk, but not a single respondent group granted them a spot in the top 5 critical risks rank. The red part of the sunburst diagram presenting the unaddressed risks reveals that smart contract risk is one of the biggest concerns of crypto-markets among all respondent groups, yet it has been completely left out from the MiCA framework. Similarly, miner risk and oracle risk occupy a high criticality rank among crypto-asset issuers, but unfortunately are not reflected in the regulatory framework. Forks, risk of challenging routine maintenance and upgrades, as well as transaction risk do not occupy a spot in any of the 4 respondent groups' top 5 critical risk list.

A central insight to the research question that is revealed when visualizing the data obtained from Chapter 5 and 6 is the representation of the respondent groups in the MiCA framework. It can be seen that most of the risks that occupy the top 5 criticality scores in the legal expert group are classified as addressed in MiCA, with the exception of counterparty risk and key management that are partially addressed, and smart contract risk that is not addressed. The representation of CASPs and institutional investors' most critical perceived risks is also relatively strong in the MiCA framework, as only the smart contract risk remains unaddressed for these groups. However, crypto-asset issuers' most critical perceived risks are reflected less in the framework, since not only smart contract risk, but also miner and oracle risks remain unaddressed in MiCA.

7

Conclusions

7.1. Conclusion

In this research, the European Commission's MiCA framework has been evaluated by the means of conducting expert interviews on the perceptions of MiCA and the EU's general regulatory approach, as well as a summative content analysis to assess what risks are addressed and unaddressed in the framework. Thus, the main research question *"What are the policy considerations that EU policy makers could take into account in the future amendments of the MiCA framework and regulatory developments in the EU's crypto-markets?"* has been answered.

The analysis of perceptions of industry experts with respect to the MiCA framework and the EU's regulatory approach yielded numerous insights that could be relevant to the policy makers. Firstly, there was a general consensus that MiCA addresses the industry's need for a regulatory framework and legal clarity, allowing for more confident operations for the industry participants in the EU. However, the policy evaluation conducted in this study revealed that MiCA possesses a lack of clarity in classifications of crypto-assets, distinctions in levels of market significance among crypto-asset issuers and in levels of centralization for crypto-asset issuer and service provider entities. As a result, this poses a risk of difficult registration process, regulatory arbitrage and general confusion among market participants. When it comes to the content analysis with respect to addressing the risks of crypto-assets and services in the MiCA framework, the analysis provides insights into what the MiCA addresses, what it partially addresses and what it does not address at this point of time. While it can be seen that the regulators dedicated more focus on the market and legal compliance risks MiCA, many operational and technical risks are left under the radar. As explained in section 6.4, transaction risk, smart contract risk, miner risk, oracle risk, risk of challenging routine maintenance and upgrades and forks remain completely unaddressed in the framework. Given that one of the central objectives of MiCA is to mitigate the risks of blockchain-based financial applications, it is critical that all risks presented in the World Economic Forum's report on Decentralized Finance are minimized by the regulatory frameworks and standards. While it can be argued that WEF's report is not complete, the interviews demonstrated that smart contract risk is perceived as one of the most critical risks of crypto-assets and services across all respondent groups. As described in section 5.2, technical risks, and especially risk of malfunctioning, unsecured or maliciously created smart contracts pose a significant financial threat in DLT-based financial services. However, none of the technical requirements, standards or guidelines on functional structures of issuers and service providers in white papers are explained in the MiCA framework. Unfortunately, the regulator may not be able to create a safe space for customers in crypto markets as long as there are no standards or guidelines specifically designed for blockchain-based finance. Moreover, it can be seen that 3 out of 6 risks left unaddressed in the MiCA framework, namely oracle risk, miner risk and smart contract

risk, are those perceived as one of the most critical by crypto-asset issuers, indicating that there may have been a lack of communication and cooperation with this group during consultation periods and design phases of the regulation. By closer partnership and frequent exchange between all stakeholder groups identified in the MiCA framework, the regulator may be able to better understand the risks that exist in the industry and address them in an appropriate manner.

To formulate more actionable considerations for the EU policy makers, it is recommended that the future amendments to MiCA and/or new regulations in the crypto-markets include clearer classifications of assets, clarify the distinctions between significance and centralization levels of issuers and services. To do so, it is recommended to construct clear guidelines that determine whether a certain crypto-asset or service is decentralized, and apply different types of regulations for projects that are placed on different ends of centralization spectrum. Moreover, the EU policy makers are advised to conduct further research into DAOs, NFTs and other emergent types of crypto-backed communities and assets to determine the most suitable regulatory approach for these advancements. In order to produce more effective and timely amendments and introductions to the regulation of crypto in the EU, the policy makers are encouraged to consider to maintain constant collaboration with the industry participants to be sufficiently aware of the market trends and be able to not only react to the market, but anticipate certain technological effects and reflect on emergent risks. For this fast moving market, it may prove more effective to introduce incremental changes to the regulations on a frequent basis, rather than processing a larger amendment once in several years. As was discussed during the interviews, late timing and slow progress of the regulation may result in outdated policies that may simply turn ineffective once enforced. Lastly, the EU regulators are encouraged to collaborate with the industry participants, especially with crypto-asset issuers and service providers to explore the risks of crypto-markets that are posed by its technological nature and prioritize further research on smart contract and key management risks. Since smart contracts play a significant role in the operations of virtually every crypto-assets and services, it is recommended that regulators do not leave this backbone of crypto-market unsupervised.

7.2. Limitations

This research has several limitations that may have had an impact on the accuracy and reliability of the presented results. The first limitation is the number of respondents in the interview round of the research. While 19 interviews would be more than sufficient to provide an in-depth analysis of risk and regulation perception of a single group, the interviewees in this study are categorized into 4 groups, all of which have a different size. While there are 8 legal services employees and 6 crypto-asset service provider employees, there are only 2 respondents from the crypto-asset issuer firms and 3 respondents from institutional investment firms. To reduce this limitation, more interview invitations were sent out to the smaller groups, but the response rate has not improved. Due to strict policies of many issuer companies and institutional investment entities it has been highly challenging to obtain an interview. As a result, as more interviewees are added to the analysis of the 2 smaller groups, the ranking of risks could change significantly. Another limitation lies in the study's assumption that the ranking of each respondent has the same weight towards the total criticality score of risks. It is possible that due to varying years of experience, knowledge and general risk perception, the ranking of the risk criticality could vary. Hence, if the same study would be performed with the same number of respondents but with different experts, the results could vary depending on a multitude of factors that may affect the choices made by interviewees. Thus, both of the limitations could be reduced by employing a much larger respondent sample to compensate for personal and professional differences. It would be possible to realistically achieve such a sample by conducting a survey instead of the interviews, or by focusing only on a single group as opposed to four.

7.3. Further Research

There are several findings and observations that were produced by the research but lie outside of its scope to be analyzed within this study. Nevertheless, these findings could be the direction of research for future studies on risks and regulation of Decentralized Finance. During the interview rounds, it was discovered that interviewees perceived certain risks that were not directly present in the World Economic Forum's DeFi risk framework. Some of the interviewees named risks such as borderlessness, transparency, lack of education among users, environmental risk, reputation loss and inter-connectivity. While not all of them are exclusively relevant to crypto-markets, this information could still be relevant for future researchers to explore whether these risks are relevant to crypto-markets and construct a more complete risk frameworks for future regulations.

Borderlessness risk, as explained by one of the interviewees, is a risk of being unable to effectively establish borders within DeFi, unlike in the traditional banking system. While it is not very easy to move funds cross-border via online banking or physical cash smuggling, DeFi allows for instant, unregulated cross-border fund transfers that may pose all kinds of legal compliance, crime-related and financial risks. Transparency is a risk that is posed by immutability and accessibility of blockchain records. Since all transaction data is visible on public blockchains, malicious actors could employ techniques and tools that may allow them to uncover the real personality behind a certain pseudonymous wallet number, placing users in risk of being potential targets for malicious attacks. Lack of education is a risk voiced by several crypto-asset service providers who believe that low-knowledge or newly introduced users in crypto-markets may face financial or fraud-related risks due to their inability to sufficiently assess risks and understand how to invest and use crypto-assets and services. According to the expert, education of users is a necessary risk to address when providing assets or services in the crypto-market. Environmental risk is self explanatory, and refers to the environmental dangers posed by DeFi related to mining of assets and general operational activities that cause significant energy consumption. Reputation loss is a risk perceived by the crypto-asset issuers and service providers associated with long-term or permanent loss of reputation or good public image due to a poor decision or an unfortunate situation, such as a technical malfunction. Lastly, inter-connectivity is voiced as a risk by a respondent from an institutional investment institution that is associated with permanent mixture of DeFi with traditional finance. According to them, once the funds and users of crypto-markets are integrated with the funds and users of traditional banking system, it would be very difficult or impossible to disintegrate them if necessary.

Another findings of the research that could lead the direction for future research are the potential solutions to the risks presented in this research. Future studies could focus on how the most critical risks perceived by the respondents of this study can be addressed by regulators in the future. When discussing the ways in which the most critical perceived risks can be minimized, the interviewees proposed some solutions based on their professional experience and observations from the industry. For smart contract risk, experts proposed introducing smart contract guidelines and requirements based on best practices to ensure minimization of malfunctioning. Other proposed solutions involved introducing smart contract auditors in the authorization process and hiring ethical hackers to reveal vulnerabilities of smart contracts prior to their launch. For key management risk, experts proposed exploring options such as multisig (also known as threshold cryptography), social recovery and zero-knowledge proofs in future regulations and guidelines. According to the interviewees, these solutions could be particularly effective for decentralized entities where custodian solutions may not be possible.

7.4. Relevance to EPA

Effective regulation of crypto-markets is a part of the larger regulation of the global financial system, which can be argued to be a grand challenge as it possesses an international nature, a multi-actor system with conflicting interests and has no binary ”right” or ”wrong” solutions, while effectiveness of regulation is also a subjective metric. In fact, these properties make effective regulation of crypto-markets a ”wicked problem”, as the above listed characteristics belong to its definition (Rittel & Webber, 1973). This report aims to contribute towards addressing this wicked problem by providing an evaluation of the first crypto-market regulation in the EU by the means of conducting expert interviews and content analysis to provide the public and policy makers with additional insights for future amendments and regulations. Thus, the graduation project presented in this report is analytical in nature, exhibits a multi-actor perspective and is directly relevant not only in the public policy domain, but also in the private sector for those who seek to better understand the market perceptions and the regulatory climate.

7.5. Academic Contributions

According to Ladik & Stewart, in the academic context *“a contribution is made when a manuscript clearly adds, embellishes, or creates something beyond what is already known”*. This research contributes to the existing knowledge by providing 3 main findings otherwise not available in other academic literature. Firstly, the study offers an insight into the risk perception of various industry participants in the crypto-market, expressed by a quantitative scoring system which helps one understand what risks are most perceived by what actors in the system. This information can be useful in addressing said risks by observing which actors are more likely to participate in the risk minimization first. It also gives the policy makers additional insights on the risks they could help address to create a safer space for users. Secondly, this study offers additional qualitative data analysis on perceptions of regulation from legal experts on concrete points in the MiCA framework, and on the general regulatory approach and environment in the EU from the industry stakeholders. These findings can be useful for policy makers in improving the EU crypto regulation, and for the general knowledge on public policy in academia. Thirdly, the research provides the first content analysis of the MiCA framework that assess what and whose risks the regulation addresses, knowledge that is crucial in understanding the current state of the regulation and shedding light on the necessary future amendments and policies in the EU crypto-markets.

References

Abramova, S., & Böhme, R. (2016). Perceived benefit and risk as multidimensional determinants of bitcoin use: A quantitative exploratory study.

Alexander, D. (February, 2019). Crypto ceo dies holding only passwords that can unlock millions in customer coins.

Ali, O., Ally, M., Dwivedi, Y., et al. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management*, *54*, 102199.

Antonopoulos, A. M., & Wood, G. (2018). *Mastering ethereum: building smart contracts and dapps*. O'reilly Media.

Authority, F. C. (2019). Cryptoassets. Retrieved from `https://www.fca.org.uk/consumers/cryptoassets`

Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting bitcoin ponzi schemes. In *2018 crypto valley conference on blockchain technology (cvcbt)* (pp. 75–84).

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

Bilotta, N., & Botti, F. (2019). *Libra and the others: The future of digital money*. JSTOR.

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

Bolt, W., Lubbersen, V., & Wierts, P. (2022). Getting the balance right: Crypto, stablecoin and central bank digital currency. *Journal of Payments Strategy & Systems*, *16*(1), 39–50.

Brauneis, A., & Mestel, R. (2018). Price discovery of cryptocurrencies: Bitcoin and beyond. *Economics Letters*, *165*, 58–61.

Caldarelli, G. (2020). Real-world blockchain applications under the lens of the oracle problem. a systematic literature review. In *2020 ieee international conference on technology management, operations and decisions (ictmod)* (pp. 1–6).

Caporale, G. M., & Zekokh, T. (2019). Modelling volatility of cryptocurrencies using markov-switching garch models. *Research in International Business and Finance*, *48*, 143–155.

Chin, M. (2020). Telegram shuts down its cryptocurrency operation. Retrieved from `https://www.theverge.com/2020/5/12/21256407/telegram-cryptocurrency-shutdown-sec-gram`

CoinGecko. (2022). Stablecoins by market capitalization. Retrieved from `https://www.coingecko.com/en/categories/stablecoins`

CoinMarketCap. (2022). Today's cryptocurrency prices by market cap. Retrieved from `https://coinmarketcap.com/`

Dale, B. (July, 2020). Mempool manipulation enabled theft of $8m in makerdao collateral on black thursday: Report. *Coindesk*. Retrieved from `https://www.coindesk.com/mempool-manipulation-enabled-theft-of-8m-in-makerdao-collateral-on-black-thursday-report`

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

Deshmukh, S., Warren, S., & Werbach, K. (2021). Decentralized finance (defi) policy-maker toolkit. *World Economic Forum*.

Don, T., & Alex, T. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business and the world. *Penguin*.

Du, W. D., Pan, S. L., Leidner, D. E., & Ying, W. (2019). Affordances, experimentation and actualization of fintech: A blockchain implementation study. *The Journal of Strategic Information Systems*, *28*(1), 50–65.

EBA. (2019). Report with advice on crypto-assets.

Egberts, A. (2017). The oracle problem-an analysis of how blockchain oracles undermine the advantages of decentralized ledger systems. *Available at SSRN 3382343*.

ESMA. (2019). Advice on initial coin offerings and crypto-assets.

European Commission. (2020a). Proposal for a regulation of the european parliament and of the council on markets in crypto-assets, and amending directive (eu) 2019/1937. , *593 final*. Retrieved from `https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF`

European Commission. (2020b). Proposal for a regulation of the european parliament and of the council on markets in crypto-assets and amending directive (eu) 2019/1937. , *COM(2020) 593 final - SEC(2020) 306 final - SWD(2020) 381 final*. Retrieved from `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0380&from=EN`

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436–454).

Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, *27*(5), 53–57.

Fantazzini, D., & Zimin, S. (2020). A multivariate approach for the simultaneous modelling of market risk and credit risk for cryptocurrencies. *Journal of Industrial and Business Economics*, *47*(1), 19–69.

Feder, A., Gandal, N., Hamrick, J., Moore, T., & Vasek, M. (2018). The rise and fall of cryptocurrencies. In *Workshop on the economics of information security*.

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

Friedrich, A. (1983). von hayek,"denationalisation of money. *An Analysis of the Theory and Practice of Concurrent Currencies" Trad. La desnacionalización del dinero, Madrid, Unión Editorial*, 19.

Geiregat, S. (2018). Cryptocurrencies are (smart) contracts. *Computer law & security review*, *34*(5), 1144–1149.

Giancaspro, M. (2017). Is a 'smart contract'really a smart idea? insights from a legal perspective. *Computer law & security review*, *33*(6), 825–835.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, *204*(6), 291–295.

Groß, J., Herz, B., Schiller, J., et al. (2019). *Libra-concept and policy implications* (Tech. Rep.). Wirtschaftswissenschaftliche Diskussionspapiere.

Guadamuz, A., & Marsden, C. (2015). Blockchains and bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, *20*(12-7).

Hartmann, P. (2010). *Interaction of market and credit risk* (Vol. 34) (No. 4). Elsevier.

Holland, M., Stjepandić, J., & Nigischer, C. (2018). Intellectual property protection of 3d print supply chain with blockchain technology. In *2018 ieee international conference on engineering, technology and innovation (ice/itmc)* (pp. 1–8).

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research*, *15*(9), 1277–1288.

Hu, B., McInish, T., Miller, J., & Zeng, L. (2019). Intraday price behavior of cryptocurrencies. *Finance Research Letters*, *28*, 337–342.

Huillet, M. (2019). Walmart is trying to patent its own 'libra' like digital currency. Retrieved from `https://cointelegraph.com/news/walmart-is-trying-to-patent-its-own-libra-like-digital-currency`

Juels, A., Kosba, A., & Shi, E. (2015). The ring of gyges: Using smart contracts for crime. *aries*, *40*, 54.

Khalid, A. (2022). 'axie infinity' is back open for business following $625 million hack. *Engadget*.

Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

Lewis, R., McPartland, J., Ranjan, R., et al. (2017). Blockchain and financial market innovation. *Economic Perspectives*, *41*(7), 1–17.

Masciandaro, D. (2018). Central bank digital cash and cryptocurrencies: Insights from a new baumol–friedman demand for money. *Australian Economic Review*, *51*(4), 540–550.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1–35.

Meegan, X. (2020). Identifying key non-financial risks in decentralised finance on ethereum blockchain. *MIP Politecnico di Milano*.

Meegan, X., & Koens, T. (2021). Lessons learned from decentralised finance (defi). *ING. URL: https://new. ingwb. com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi_white_paper_v2. 0. pdf*.

Mukherjee, S. (2022). Terra co-founder's home raided as s.korea investigates luna crash. Retrieved from `https://coinquora.com/terra-co-founders-home-raided-as-s-korea-investigates-luna-crash/`

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nguyen, Q. K. (2016). Blockchain-a financial technology for future sustainable development. In *2016 3rd international conference on green technology and sustainable development (gtsd)* (pp. 51–54).

Novakovic, M. S. (2021). The reform of the crypto licenses system in estonia and the regulation on markets in crypto assets proposal. *Strani Pravni Zivot*, 687.

Palomäki, R. S. (2021). *Crypto-asset investor protection and market integrity under the proposal for a regulation of the european parliament and of the council on markets in crypto-assets and amending directive (eu) 2019/1937.* (Unpublished master's thesis).

Popescu, A.-D., et al. (2020). Decentralized finance (defi)–the lego of finance. *Social Sciences and Education Research Review*, *7*(1), 321–349.

Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied health economics and health policy*, *16*(5), 583–590.

Raffaele, L. (2022). Cryptocurrencies and crypto-assets in the italian and eu perspective. *Вестник Санкт-Петербургского университета. Право*, *13*(1), 219–229.

Reddy, E., & Minnaar, A. (2018). Cryptocurrency: A tool and target for cybercrime. *Acta Criminologica: African Journal of Criminology & Victimology*, *31*(3), 71–92.

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197–223). Springer.

Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy sciences*, *4*(2), 155–169.

Salamatin, M. (2021). Balancing innovation and protection: Understanding the landscape for defi regulation. *Available at SSRN 3918656*.

Sanyalt, S. (2022). Attacked ethereum platform offers us$1.8m bounty and no legal charges to its hackers. *Analytics Insight*.

Schouwstra, M. C., & Ellman, M. J. (2006). A new explanatory model for policy analysis and evaluation.

Seele, P. (2018). Let us not forget: Crypto means secret. cryptocurrencies as enabler of unethical and illegal business and the question of regulation. *Humanistic Management Journal*, *3*(1), 133–139.

Shahzad, F., Xiu, G., Wang, J., & Shahbaz, M. (2018). An empirical investigation on the adoption of cryptocurrencies among the people of mainland china. *Technology in Society*, *55*, 33–40.

Shevchenko, A. (2020). Researcher suggests miners are manipulating ethereum blocks to exploit defi. *Cointelegraph*.

Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. *Journal of Management Information Systems*, *36*(1), 37–73.

The Defiant. (2020). *Sushiswap's vampire scheme: Hours away and with $1.3b at stake*. The Defiant. Retrieved from `https://newsletter.thedefiant.io/p/sushiswaps-vampire-scheme-hours-away`

The Libra Association. (2019). An introduction to libra: White paper. *The Libra Association.(2020). Libra white paper v2*.

Toby, B., & Lawrence, L. (2022). What netflix's quadrigacx documentary gets right – and wrong – about one of crypto's worst scandals. *Coindesk*. Retrieved from `https://www.coindesk.com/business/2022/03/31/what-netflixs-quadrigacx-documentary-gets-right-and-wrong-about-one-of-cryptos-worst-scandals/`

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1–35.

Wanat, E. (2021). Are crypto-assets green enough?–an analysis of draft eu regulation on markets in crypto assets from the perspective of the european green deal. *OER Osteuropa Recht*, *67*(2), 237–250.

Wei, W. C. (2018). Liquidity and market efficiency in cryptocurrencies. *Economics Letters*, *168*, 21–24.

Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*.

Zetzsche, D. A., Annunziata, F., Arner, D. W., & Buckley, R. P. (2020). The markets in crypto-assets regulation (mica) and the eu digital finance strategy.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2021). Regulating libra. *Oxford Journal of Legal Studies*, *41*(1), 80–113.