



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

in cotutela con VRIJE UNIVERSITEIT BRUSSEL

DOTTORATO DI RICERCA IN
LAW, SCIENCE AND TECHNOLOGY

Ciclo 38

Settore Concorsuale: 12/H3 - FILOSOFIA DEL DIRITTO

Settore Scientifico Disciplinare: IUS/20 - FILOSOFIA DEL DIRITTO

DECENTRALISED FINANCE, CRYPTO ASSETS AND CONSUMER PROTECTION
WITHIN THE EUROPEAN UNION.

Presentata da: Emilia Richiello

Coordinatore Dottorato

Antonino Rotolo

Supervisore

Monica Palmirani

Co-supervisore

Marco Giacalone

Esame finale anno 2026

Abstract

Crypto assets and decentralised finance represent one of the most significant innovations of this century. They constitute the new frontier of blockchain technology and the global market, promising investors a system without intermediaries and with reduced costs. Decentralised finance and, more broadly, the crypto-asset market, replicate traditional banking and financial services through technological innovations and implementations that offer greater accessibility and inclusion for investors. However, these instruments also pose risks to consumers, as they require an understanding of both technological and financial concepts.

Recently, with the adoption of the MiCA Regulation, the European Union has sought to regulate this phenomenon in order to make the market safer and to protect consumers from potential abuses.

This thesis aims to investigate the risks faced by consumers and to assess whether the European approach provides an effective and adequate response to mitigate them. To this end, the analysis begins with an overview of the blockchain and crypto-asset ecosystem, as well as of decentralised finance. In particular, it describes their structure, functioning, and various use cases. The study then examines the recently introduced European regulatory framework, analysing its most relevant innovations and the approach adopted by the EU legislator. Finally, Italian case law in this field is discussed to identify the main interpretative issues that have emerged and to explain why these should be taken into consideration when shaping future European legislation.

A mamma, papà e Federico.

Table of Contents

Introduction.....	10
Background and research problem.	10
Research question and objective.....	11
Methodology.....	12
Thesis outline.....	13
Chapter 1 – Blockchain and crypto asset foundations.	15
0. Introduction.....	15
1. The genesis of blockchain technology. A general overview.	16
1.1 Distributed Ledger Technologies (DLT).	19
1.2 Components.	20
1.3 Blockchain. Definition and features.	23
1.4 Classifications.	28
1.5 Functioning.	29
1.6 Case studies of blockchain protocols. Bitcoin and Ethereum.....	30
2. Cryptocurrency and Crypto asset.....	32
2.1 Categories of crypto assets. Classification by function.	34
2.2 Classification by technological generation.	34
2.3 Classification by value stability. Stablecoins.	35
2.4 Stablecoin use cases.....	37
2.5 Non-Fungible Tokens.	38
3. Smart Contracts.	39
3.1 Precursors to Smart Contracts.	40
3.2 Smart contract code and smart legal contract.	41
3.3 Smart contracts use cases. Examples.....	42
3.4 Initial Coin Offerings (ICOs) and Decentralised Autonomous Organisations (DAOs).	44
4. Conclusions.....	46
Chapter 2 – Decentralised Finance Ecosystem	48
0. Introduction.....	48
1. Fintech. A literature review.	49
1.1 Evolution.....	51
1.2 Applications of fintech. Examples.....	52

2. Decentralised Finance (DeFi).	56
2.1 Definitions. A literature review.	57
2.2 Origins of DeFi. Decentralised Finance (DeFi) and Traditional Finance (TradFi).	63
2.3 Features and key concepts.	66
2.4 Use cases.	68
3. Conclusions.	71
Chapter 3 – Risks related to crypto assets and DeFi.	73
0. Introduction.	73
1. Risks in DeFi.	74
1.2 Risks in TradFi and DeFi.	75
2. Consumer Protection. A general overview of the EU framework.	78
3. Risks for consumers in crypto asset transactions.	79
3.1 Frauds, scams, hacks and illicit activities.	82
3.2 Scamming techniques.	84
4. Conclusions.	86
Chapter 4 – European Regulation and Crypto Assets.	88
0. Introduction.	88
1. The importance of regulating fintech in the internal market.	89
2. From zero to MiCAR.	90
2.1 European Regulation on Crypto Assets and technological neutrality.	93
2.2 Markets in Crypto Assets Regulation. The rationale.	96
2.3 The regulation.	97
2.4 Categories of tokens.	98
2.5 Main provisions of MiCAR.	100
3. The pilot regime for market infrastructures based on distributed ledger technologies.	101
4. Conclusions.	102
Chapter 5 - Crypto assets in Commercial and Private and Criminal Italian law.	105
0.1. Introduction.	105
0.2. Methodology.	107
0.3. Lexicon and acronyms.	108
0.4. Chapter outline: contents and division.	109

0.5 Implementation of European Regulation at the Italian level.	112
1. The judgment of the Italian Corte di Cassazione.....	113
1.1 Corte di Cassazione’s decisions on cryptocurrencies.	114
1.2 Cassazione penale, sez. II, 17/09/2020, n. 26807.	116
1.3 Cassazione penale, sez. II, 10/11/2021, n. 44337.	117
1.4 Cassazione penale, sez. II, 26/10/2022, n. 44378.	120
1.5 Legal considerations.	123
2. Italian merit case law on cryptocurrencies.	128
2.1. The “in-kind” contribution of crypto assets (Tribunale di Roma, n. 7932/2022).	131
2.1.1. A key precedent on cryptocurrencies contribution. Tribunale di Brescia n. 7556/2018 and Corte d’Appello di Brescia n. 207/2018.	133
2.2. The qualification of cryptocurrency deposits as regular or irregular as a requirement to declare bankruptcy. Tribunale di Firenze n. 18/2019.....	134
2.3 Consob sanctions ex art. 94 TUF. Why is an energy token a financial instrument? Corte di Appello di Roma n. 5866/2023.....	136
2.4 Legal considerations.	138
3. Conclusions.....	141
Conclusions.....	144
Bibliography	147
Legislation	161
Judicial decisions	162

Introduction

Background and research problem.

The advent of new technologies has brought significant change over the past two decades, transforming how people communicate and interact across almost every area of modern life.

The gradual advance of technological innovation, combined with the enhanced capabilities of digital devices, has led to the widespread automation of tasks once carried out exclusively by humans.

These transformations have inevitably affected legal relations, particularly in the contractual sphere, introducing new challenges in the field of consumer protection.

Among these technologies, one of the most significant is blockchain: an immutable ledger that permanently records transactions and ensures their proper execution through smart contracts. These are self-executing computer programmes that verify whether the conditions of an agreement have been met and, when they are, carry out the contract automatically without the need for human intervention.

Blockchain was initially conceived as the underlying technology supporting Bitcoin, the first cryptocurrency ever created. Since then, this innovation has given rise to a parallel market that operates alongside the traditional financial system and accommodates a growing range of crypto-assets and related services. Although such assets do not constitute legal tender, they are increasingly used worldwide as instruments of exchange and investment, generating profits and contributing to market expansion. This evolution has led to the emergence of *decentralised finance* (DeFi): a financial ecosystem parallel to the centralised, intermediary-based system, designed to make access to credit and financial opportunities more democratic and inclusive.

Decentralised finance, and more generally any operation involving the use of crypto-assets, nevertheless represents a risk for consumers. Until a few years ago, those wishing to invest had to rely on a bank or another intermediary. Today, thanks to the internet and the development of such digital systems, anyone can invest, buy, or access services related to crypto-assets.

Investment activity, however, requires specific skills that consumers do not always possess. Likewise, crypto-assets are neither simple financial products nor ordinary currencies. They are complex entities that certainly have an exchange value, but they do not follow the normal logic of the market. The lack of understanding of the particular features of crypto-assets and of the functioning of decentralised finance may lead consumers to take reckless decisions that go against their own interests.

In addition, the spread of crypto-assets has created an opportunity for fraudsters and criminal organisations to develop new strategies. Numerous cases of fraud,

misappropriation, and theft have been reported. In many instances, tracing those responsible proves extremely difficult, preventing victims from obtaining adequate protection.

Consumer protection is therefore at serious risk in this context. The world of crypto-assets and decentralised finance is still a very recent phenomenon, and its full understanding requires a high level of technical expertise. As a result, there is a lack of effective remedies and an absence of specific enforcement measures at both national and EU levels. In practice, this has led to insufficient protection for consumers and a lack of proper tools to help them understand these technologies.

At the European level, efforts have been made to regulate this phenomenon through specific legislation dedicated to crypto-assets and distributed ledger technologies. The MiCA Regulation and the DLT Pilot Regime have introduced a series of standards and requirements that providers must meet to operate in the European market. This legislation aims not only to protect users from the risks arising from these systems but also to regulate the sector in order to attract providers and create a safe market environment. The framework, which sets out standards and obligations that providers must follow, complements existing financial services legislation (MiFID II) and the *acquis communautaire* on consumer protection.

However, the regulation works mainly as a preventive measure. It establishes a compliance system that providers must satisfy to operate. The framework also provides for enforcement measures, the effectiveness of which will become clear in the coming years. Nonetheless, the preventive compliance system alone may not be sufficient to guarantee a safe environment for consumers or to offer effective protection against fraudulent behaviour by malicious actors.

Research question and objective.

The purpose of this study is to determine whether the (new?) European regulatory framework can be considered an effective tool for mitigating the risks that currently characterise the field of crypto-asset activities.

- *Does the European regulatory framework address risks related to crypto assets and decentralised finance?*

In connection with this central question, the research also seeks to identify and analyse the concrete risks that consumers face when operating within the crypto-asset market and the broader decentralised finance ecosystem.

- *What are the risks that consumers face related to crypto assets and decentralised finance?*

This research aims to provide an overview of how crypto assets have evolved during the last years and what exactly is decentralised finance.

- What are crypto assets and decentralised finance?

The objective of this research is to provide the reader with an in-depth view of the world of crypto-assets and decentralised finance, to understand not only their potential but, above all, the risks that affect consumers in their everyday lives. To this end, legal scholars and practitioners must develop an awareness of the technical functioning of these technologies and their main use cases.

At the European level, the protection of consumer interests has become increasingly important, alongside other fundamental values such as technological neutrality. However, these two principles do not always align. For this reason, it is necessary to understand both the functioning and the risks associated with a given technology, so as to achieve a legislative framework that is not only technologically neutral but also effective in practice.

This study also aims to demonstrate that the analysis of judicial case law represents a fundamental tool for observing the legal consequences and interpretative uncertainties that arise in real-world practice. As will become evident throughout this work, judicial decisions serve as indicators of the legal issues that are currently emerging and that are likely to persist in the future. They must therefore be taken into account when shaping legislative initiatives to ensure that future regulation is properly oriented and responsive to real needs.

Methodology.

Since the new European legislative framework entered into force only in 2024 and given the absence of sufficient data to conduct an empirical analysis, this study addresses the research question through an innovative methodology designed to identify consumer-related risks.

These risks are identified through the examination of case law from both merit courts and courts of last resort and are subsequently compared with those highlighted in existing academic literature.

Literature on consumer risks related to crypto-asset activities is largely based on empirical data drawn from factual events and investigative reports. Such contributions constitute an important part of the overall picture, as they document how these risks arise and the dynamics through which they manifest.

However, in the author's view, the development of adequate remedies must also consider the study of judicial decisions and the patterns emerging from court practice. This type of analysis not only reveals which legal concepts are most debated but also helps to understand the limits and challenges judges encounter when resolving such disputes.

A legislative framework that takes these aspects into account is likely to be a successful one. It provides judges with the necessary tools to resolve disputes and, at the same time, can help to prevent them from arising.

The methodology adopted in this study is qualitative. The first part of the work is technical in nature and follows a mainly descriptive approach aimed at outlining the current state of the art. The section devoted to the analysis of legislation is both descriptive and analytical, while the final part consists of the examination of selected judicial case studies.

Thesis outline.

The structure of this thesis is organised as follows.

The first chapter, entitled *Blockchain and Crypto-Asset Foundations*, aims to describe the state of the art regarding blockchain technology and crypto-assets. By providing this technical and conceptual groundwork, it directly supports the subsequent chapters, which build upon these definitions to explore decentralised finance, associated risks, and the European regulatory responses. This analysis is essential to understanding both the evolution that financial blockchain has undergone over the past two decades and the legal implications that these instruments entail. The chapter, therefore, illustrates the main features of distributed ledger technologies, together with the different configurations they may assume and their respective characteristics. Secondly, the chapter focuses on the presentation and analysis of crypto-assets. The discussion reveals a highly diverse landscape, which reflects the complexity and the varying effects of these instruments within commercial transactions. Finally, the chapter examines smart contracts, decentralised autonomous organisations, and initial coin offerings. These three phenomena represent distinct developments that have emerged within the blockchain ecosystem and have contributed to its growth and implementation. They correspond respectively to the contractual sector, corporate management, and crowdfunding.

The second chapter, entitled *Decentralised Finance Ecosystem*, aims to describe and analyse the concept of decentralised finance within the broader framework of fintech. This discussion follows logically from the first chapter and deepens the inquiry by shifting from the technological to the functional dimension of blockchain in the financial domain. The term “decentralised finance” is increasingly used to refer to a field of financial operations conducted through blockchain technology. However, since there is no uniform or legally binding definition of this concept, its meaning remains only partially clear. This chapter, therefore, examines the existing academic literature, as well as relevant use cases, in order to determine what decentralised finance actually is, its defining characteristics, and its main areas of application. In addition, a comparative analysis with traditional finance helps to illustrate how this ecosystem essentially reproduces conventional financial and banking services, while introducing innovations and improvements.

The third chapter, entitled *Risks Related to Crypto-Assets and DeFi*, examines the risks associated with the purchase of products and services in crypto-assets and within the decentralised finance ecosystem. Building on the conceptual and functional analyses of the first two chapters, this section identifies the consumer vulnerabilities that will form the empirical and normative basis for assessing the effectiveness of the European

regulatory response. The purpose of this chapter is to demonstrate that these technologies, however, are not without their drawbacks. They undoubtedly facilitate and simplify access to financial services and credit, yet they also pose significant dangers for inexperienced consumers. The analysis of risk in DeFi is carried out from two complementary perspectives. First, the study considers risk in general terms, referring to traditional risk categories and comparing them with those present in conventional finance. Second, it focuses on the specific risks that directly affect consumers. This dual approach provides a comprehensive overview of the risks inherent in DeFi and highlights the need to establish appropriate measures to protect affected parties.

The fourth chapter, entitled *European Regulation on Crypto-Assets*, examines the European legislation concerning crypto-assets and distributed ledger technologies. This chapter operationalises the central research question by directly testing whether the MiCA Regulation and the DLT Pilot Regime can mitigate the specific risks identified in Chapter 3. The analysis focuses on the regulatory framework adopted to govern the phenomenon of crypto-activities and evaluates whether the existing enforcement mechanisms are adequate to ensure compliance by market operators. The chapter also includes a specific focus on the principle of technological neutrality and on the legislator's obligation not to constrain technological development through law. Furthermore, it presents an assessment of potential breaches of European Union law arising from the current framework.

The fifth chapter, entitled *Crypto-Assets in Italian Commercial, Private, and Criminal Law*, analyses the decisions of the Italian courts of merit and legitimacy concerning crypto-asset activities. It translates the theoretical findings of the preceding chapters into an applied legal dimension, showing how national courts concretely interpret and apply the new regulatory framework and existing legal principles. Its purpose is to examine judicial decisions and to identify the main legal issues related to crypto-assets that emerge from court practice. Judicial rulings represent a valuable tool for identifying not only the most debated questions linked to new phenomena, but also the various types of disputes that these innovations have generated in practice.

The concluding section brings together the findings of the study in order to answer the research question. It offers a new interpretative framework for analysing the risks associated with these technologies and provides guidance for shaping future legislative and regulatory policies.

Chapter 1 – Blockchain and crypto asset foundations.

0. Introduction - **1.** The genesis of blockchain technology. A general overview. - **1.1** Distributed Ledger Technologies (DLT). - **1.2** Components. - **1.3** Blockchain. Definition and features. - **1.4** Classifications. - **1.5** Functioning. - **1.6** Case studies of blockchain protocols. Bitcoin and Ethereum - **2.** Cryptocurrency and Crypto asset. - **2.1** Categories of crypto assets. Classification by function. - **2.2** Classification by technological generation. - **2.3** Classification by value stability. Stablecoins. - **2.4** Stablecoin use cases. - **2.5** Non-Fungible Tokens - **3.** Smart contracts. - **3.1** Precursors to Smart Contracts. - **3.2** Smart contract code and smart legal contract. - **3.3** Smart contracts use cases. Examples. - **3.4** Initial Coin Offerings (ICOs) and Decentralised Autonomous Organizations (DAOs). – **4.** Conclusion.

0. Introduction.

Blockchain technology represents a major innovation in the technological, economic, and legal landscape. The study of its legal implications necessarily requires a technical analysis of its components and features. To understand the importance of providing effective guidance and protection for consumers, it is essential first to understand what blockchain technology is and how it operates.

This first chapter provides the technological foundation needed to understand the phenomenon of blockchain and its legal implications. It corresponds to the first step identified in the general introduction, namely the need to establish the technical underpinnings of crypto-assets before addressing their financial, regulatory, and consumer protection implications.

The objective of the chapter is to provide a comprehensive overview of the technical features of blockchain and crypto-assets. This analysis serves as the necessary precondition for the following chapters, which will examine how these technologies underpin decentralised finance and generate specific legal risks. The research question underlying this chapter is:

- *what is blockchain and what are crypto-assets?*

To answer this question, the chapter analyses the essential components of blockchain technology and crypto-assets, providing an overview of their historical and technological development. It also presents the main categories of crypto-assets, classifying them according to their function, and examines the operation of smart contracts as one of the key innovations associated with blockchain.

The methodology adopted is qualitative and descriptive. It consists of the explanation and analysis of these concepts from a technical perspective, following existing literature and recognised scientific sources. The works cited come mainly from the field of computer science and engineering. The language used throughout remains simple and accessible, since this thesis is addressed to an interdisciplinary audience that includes readers without a technical background.

The objective of the chapter is to provide a comprehensive overview of the technical features of blockchain and crypto-assets. The aim is to give readers the necessary tools to understand the complexity of this architecture and to recognise the potential risks it may pose to non-expert users.

1. The genesis of blockchain technology. A general overview.

Blockchain is a cryptographic, decentralised, and distributed digital ledger technology that enables users to record transactions securely. The principles behind this technology allow unknown users to exchange goods and services without needing to trust one another. Every transaction is stored in a shared ledger that tracks the assets held or transferred by each user¹. Blockchain operates like a public database, maintaining a permanent, ordered record of all exchanges that have taken place².

Blockchain was introduced on October 31, 2008, when Satoshi Nakamoto - the pseudonym of an unknown individual - published the results of his technological work³. His whitepaper immediately drew attention from both the economic and scientific communities⁴.

The model was developed in response to the 2008 financial crisis. According to the whitepaper, it was designed to enhance the security of users' investment processes. It includes two main elements: first, Bitcoin, a cryptocurrency that can serve as an alternative payment method; and second, the blockchain itself, a digital ledger that employs a specific cryptographic method to permanently record transactions without the possibility of later modifications.

¹ Corrales, M., Fenwick, M., & Haapio, H. (2019). Legal tech, smart contracts and blockchain. In *Perspectives in law, business and innovation*. <https://doi.org/10.1007/978-981-13-6086-2>

² Ibid.

³ Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>

⁴ Nakamoto's work was also inspired by that of other authors who had conducted studies in the field. For example, the contribution of Ralph Merkle, co-inventor of public key cryptography, was fundamental. His work enabled the development of a system that, while protecting users' identities, allowed anyone to view the transactions carried out. See W. DAY, *B-money*, in <http://www.weidai.com/bmoney.txt>, 1998; H. Massias, X.S. Avila, e J.-J. Quisquater, *Design of a secure timestamping service with minimal trust requirements*, in 20th Symposium on Information Theory in the Benelux, 1999; Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99–111. <https://doi.org/10.1007/bf00196791>; Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital Time-Stamping. In *Springer eBooks* (pp. 329–334). https://doi.org/10.1007/978-1-4613-9323-8_24; Haber, S., & Stornetta, W. S. (1997). Secure names for bit-strings. *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 28–35. <https://doi.org/10.1145/266420.266430>; Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure*. <http://nakamotoinstitute.org/static/docs/hashcash.pdf>; Merkle, R. C. (1980). Protocols for public key cryptosystems. *IEEE Symposium on Security and Privacy*, 122–133. <https://doi.org/10.1109/sp.1980.10006>; Feller, W. (1958). An introduction to probability theory and its applications. *Journal of the Franklin Institute*, 265(1), 73–74. [https://doi.org/10.1016/0016-0032\(58\)90688-4](https://doi.org/10.1016/0016-0032(58)90688-4).

The system rapidly attracted global attention, primarily due to its innovative software, improved hardware, and the validation process carried out by specific users known as miners⁵.

According to Nakamoto, Bitcoin and blockchain would enable users to exchange money without involving a financial institution, resulting in lower costs and no need to adhere to third-party regulations. The system works through a peer-to-peer network, where users participate both as service recipients and validators, confirming the accuracy of transactions. Once a transaction is confirmed, it is timestamped using a special algorithm and added to a block. These blocks are chained together; once the data is inserted into the chain, it cannot be changed⁶.

Nakamoto's primary goal was to establish a system where users could trade without intermediaries, simplifying even occasional exchanges and eliminating the restrictions typically imposed by banks or other institutions. In traditional systems, intermediaries often require guarantees even for small transactions, exposing a vulnerability in this dependence⁷. Nakamoto's model aims to overcome this limitation, facilitating free and open transactions and challenging the capitalist structure that governs most exchanges. With Bitcoin and blockchain, transaction costs are eliminated, and solvency is verified by the system itself through algorithms that assess both parties⁸. If a user doesn't have

⁵ Strawn, G. (2019). BLOCKCHAIN. *IT Professional*, 21(1), 91–92. <https://doi.org/10.1109/mitp.2018.2879244>.

⁶ The Author, in his manifesto, cites three articles by Stuart Haber and W. Scott Stornetta. These two scientists, who inspired Nakamoto in the development of his work, published a paper in 1991 titled “How to Time-Stamp a Digital Document” with the aim of illustrating a new computing model capable of performing timestamping on submitted documents.

Already by the end of the twentieth century, the two scientists were aware of the challenges that would arise in an increasingly digitalized world. In particular, they highlighted an issue concerning the protection of intellectual property. When the date and time of a document's creation were recorded, it was highly plausible that the timestamping systems in place would not be sufficient to guarantee adequate protection for their users.

Haber and Stornetta had identified flaws in the digital timestamping system, pointing out how easily it could be tampered with: digital recording techniques are easily manipulated and, unlike alterations made to paper records, leave no trace. Once a document has been tampered with, it becomes impossible to recover its original form or determine what change was made.

To address these risks, the two scientists devised a timestamping system in which it was impossible to alter the data once inserted. Their major insight - which would later inspire Nakamoto - was the idea of generating, via a hash algorithm, a unique identifier to be assigned to each document. Once the identifier was generated, the timestamp would be executed. This timestamp would then be added, along with others, to a chain maintained by the agency's servers. The algorithms were eventually made public through publication in the New York Times.

Although the model developed by the two scientists did not achieve the same level of recognition as Nakamoto's creation, their work deserves credit for identifying cryptography as a tool capable of ensuring the permanence and immutability of data and, even more importantly, for developing a system of chaining and embedding data that can be compared to the block structure of the blockchain. See Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document, cit..

⁷ See Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, cit.: «*Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes.*».

⁸ Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.*, cit.

enough Bitcoin, the miners will not approve the block, and the transaction will not proceed.

The system also introduces relevant privacy implementations. Each user has a private cryptographic key (used to initiate transactions) and a public, anonymous address (visible to other users). This setup allows all participants to view every transaction on the blockchain without disclosing the identities of those involved. In particular, the system combines transparency and pseudonymity. Therefore, the content of transactions is available, but the identities of the involved parties remain unknown. However, this feature raises potential concerns. The impossibility of associating transactions with specific individuals makes the system suitable for illicit activities, such as money laundering.

Nevertheless, these innovations enabled the Bitcoin-Blockchain system to draw immediate global attention. One of the most relevant aspects was the rapid increase in Bitcoin's value, which soared from having no market value to reaching a record high of \$17,549.67 on December 11, 2017. This trend attracted investors and shareholders worldwide.

However, the true innovation lies in the underlying technology: blockchain. Without blockchain, Bitcoin transactions would not be possible. This technology is a fundamental requirement for cryptocurrency exchanges. Consequently, many companies have chosen to adopt platforms akin to Bitcoin's to enhance security and faster operations. Some states are also exploring the use of blockchain in civil and land registry systems.

As noted, one of the first critical issues surrounding Bitcoin emerged when the system began to be used for illicit activities⁹. The absence of specific regulation governing blockchain made the system vulnerable to misuse. In many cases, Bitcoin has often been used as an alternative means of payment to legal tender. This led to several challenges, mainly since existing regulations regarding monetary transactions could not be applied.

This situation drew the attention of national governments for the first time. It became evident that a specific legal framework was essential to define the scope of the phenomenon and provide appropriate regulation. The concerns and distrust surrounding Bitcoin gradually diverted public focus toward blockchain technology, which initially emerged as the technological infrastructure behind cryptocurrencies. Its features - such as anonymity, transparency, and data immutability - suggested potential applications for various operations beyond cryptocurrencies.

These characteristics attracted the interest of software developers, prompting deeper exploration of this technology's potential uses. In this context, the contribution of programmer Vitalik Buterin was essential. Through his work, he expanded the

⁹ Panisi, F. (2017). Blockchain and "Smart Contracts": FinTech innovations to reduce the costs of trust. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3066543>

functional scope of blockchain¹⁰. Indeed, the launch of the Ethereum¹¹ platform marked the beginning of a new phase in blockchain development, allowing for the exchange of digital value and enabling the creation of software programs capable of executing contracts. Developers can use the platform to build decentralised applications that process transactions. Once created, these applications can be released on the market, allowing developers to generate profit¹².

1.1 Distributed Ledger Technologies (DLT).

Once the main aspects concerning the development of blockchain have been clarified, it is worth focusing on the definition of such technologies and their main features. Even though the terms ‘blockchain’, ‘distributed ledger technologies’ and ‘cryptocurrencies’ are now widely used, the distinction between these concepts is not always clear. This is also due to the numerous, complicated and inconsistent definitions that are provided by practitioners¹³. For this reason, it is necessary to provide a clear definition of such phenomena.

A distributed ledger technology (DLT) is a multi-party system that operates without a central authority¹⁴ and is managed by several participants¹⁵. The ledger is made of chained blocks that store information through the activity of nodes. Nodes are the computational resources that, by using processing power and electricity, validate transactions and add them to the distributed ledger.

The term *distributed* refers to the decision-making process and should not be confused with the term *decentralisation*¹⁶. In a distributed network, computing resources and hardware are spread across multiple data centres but remain under the ownership and control of the network provider. Data, however, usually belongs to the user, who also manages it directly. By contrast, in a decentralised network, resources are owned and shared by the network’s participants. Each member holds an identical copy of the

¹⁰ Attico, N. (2018). *Blockchain. Guida all’ecosistema. Tecnologia, business, società*. goWare & Guerini Next.

¹¹ Buterin, V. (2013). Ethereum White Paper. *GitHub Repository*. https://static.peng37.com/ethereum_whitepaper_laptop_3.pdf

¹² These types of programs are known as smart contracts. Once a smart contract is created, it becomes accessible to users. The contract includes all the conditions necessary for it to produce legal or economic effects. Its execution depends on a mathematical computation, which checks whether the required conditions are met. If the outcome is positive, and the requirements are satisfied, the contract is validated and executed.

¹³ Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2018). Distributed Ledger Technology Systems: a Conceptual framework. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3230013>

¹⁴ Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2018). Distributed Ledger Technology Systems: a Conceptual framework, cit.

¹⁵ Ugarte, R. (2014). Distributed ledger technology (DLT): introduction. *Banco De Espana*, 19/18. <https://ssrn.com/abstract=3269731>

¹⁶ Vergne, J. (2020). Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform. *Organization Theory*, 1(4). <https://doi.org/10.1177/2631787720977052>.

distributed ledger, and information can only be added to the ledger if there is consensus among the group of users¹⁷.

Rauchs, Michel, et al. (2018) defined the DLT technology as a “system of electronic records that enables independent entities to establish a consensus around a shared ‘ledger’ - without relying on a central coordinator to provide the authoritative version of the records”¹⁸.

1.2 Components.

In this regard, every DLT are characterised by three elements¹⁹: public and private key cryptography²⁰, distributed peer-to-peer networks (P2P)²¹ and consensus mechanisms.

Cryptography. According to Menezes et al. (2018), “cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication”²².

Cryptography is then adopted to ensure that information on the networks is available only to those authorised (*confidentiality*) and identified (*authentication*), without the possibility of data alteration or manipulation (*data integrity*).

Each user of a DLT holds a private key that allows access to their account and enables them to carry out transactions, as well as a public key that helps establish a secure

¹⁷ See <https://aws.amazon.com/it/web3/decentralization-in-blockchain/>

¹⁸ Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2018). Distributed Ledger Technology Systems: a Conceptual framework, cit.

¹⁹ Ioini, N. E., & Pahl, C. (2018). A review of distributed ledger technologies. *Lecture Notes in Computer Science*, 277–288. https://doi.org/10.1007/978-3-030-02671-4_16

²⁰ Z. Allam, *On Smart Contracts and Organisational performance: a Review of Smart Contracts through the Blockchain technology*, in Review of Economic & Business studies, 2018.

²¹ Perna, A. (2015). Le origini della blockchain. In *Blockchain e Smart Contract*. Lefebvre Giuffrè.

²² Menezes, A. J., Vanstone, S. A., & Van Oorschot, P. C. (1997). Handbook of applied cryptography. *Choice Reviews Online*, 34(08), 34–4512. <https://doi.org/10.5860/choice.34-4512> “1. **Confidentiality** is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

2. **Data integrity** is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

3. **Authentication** is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

4. **Non-repudiation** is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.”

digital identity visible to other participants on the platform²³. This configuration allows every participant in the system to verify each transaction, without revealing any information that links it to a specific user. Indeed, this configuration enhances data protection and communication between the participants of the network²⁴.

Peer-to-peer network (P2P). A peer-to-peer (P2P) network is a type of computer network where the nodes work with a flexible hierarchy. A comprehensive definition of P2P network has been provided by Schollmeier (2001):

“A distributed network architecture may be called a Peer-to-Peer (P-to-P, P2P,...) network, if the participants share a part of their own hardware resources (processing power, storage capacity, network link capacity, printers...). These shared resources are necessary to provide the Service and content offered by the network (e.g. file sharing or shared workspaces for collaboration). They are accessible by other peers directly, without passing intermediary entities. The participants of such a network are thus resource (Service and content) providers as well as resource (Service and content) requestors (Servent-concept)”.²⁵

Another definition has been elaborated by Androutsellis-Theotokis and Spinellis (2004):

“Peer-to-peer systems are distributed systems consisting of interconnected nodes able to self-organize into network topologies with the purpose of sharing resources such as content, CPU cycles, storage and bandwidth, capable of adapting to failures and accommodating transient populations of nodes while maintaining acceptable connectivity and performance, without requiring the intermediation or support of a global centralized server or authority”²⁶

A P2P network is characterised by the absence of a central authority, and users' devices act both as clients and servers. Once the network is distributed on a global scale, this structure becomes nearly impossible to arrest, since there is no central server that can be targeted or disabled²⁷. A P2P network is used to ensure scalability, eliminate failure, and prevent control by a single actor or a small group of participants²⁸.

²³ Allam, Z. (2018). On Smart Contracts and Organisational Performance: A Review of Smart Contracts through the Blockchain Technology. *Review of Economic and Business Studies*, 11(2), 137–156. <https://doi.org/10.1515/rebs-2018-0079> «private keys by the users in the blockchain network is made for signing their own transactions; the public key on the other hand are used to address the users»

²⁴ Masood, F., & Faridi, A. R. (2018). Consensus Algorithms In Distributed Ledger Technology For Open Environment. In *2018 4th International Conference on Computing Communication and Automation (ICCCA)* (pp. 1–6). <https://doi.org/10.1109/ccaa.2018.8777695>

²⁵ Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *Proceedings first international conference on peer-to-peer computing* (pp. 101–102). <https://doi.org/10.1109/p2p.2001.990434>

²⁶ Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys*, 36(4), 335–371. <https://doi.org/10.1145/1041680.1041681>

²⁷ A. Perna, *Le origini della blockchain*, cit.

²⁸ El Ioini, N., and Pahl, C. (2018). *A review of distributed ledger technologies*. cit.

In this regard, *scalability* refers to the network's ability to accommodate a growing number of nodes and increasing data traffic without significant degradation in performance²⁹. On the other hand, "*eliminate failure*" describes the system's resilience to node malfunctions, achieved through decentralisation, which prevents reliance on a single point of control or vulnerability³⁰.

Consensus mechanism. The consensus mechanisms - also known as consensus protocols or algorithms - are the processes through which operations are validated and approved within distributed ledger technologies. These mechanisms are used to verify transactions and ensure the security of the system. Since operations carried out on a DLT must be verified, consensus mechanisms enable the independent validation of transactions by peer-to-peer networks. Once the consensus procedure is successfully completed, the validated information is incorporated into the system. The different types of consensus mechanisms will be further discussed in the dedicated section on blockchain.

There are different kinds of DLT. The different types of DLT are distinguished based on: (a) type of network, (b) consensus mechanism, and (c) ledger structure³¹. The typology of network determines who can be part of the system and how new members are admitted³². It defines their role in the validation process as well. The consensus mechanism determines how the ledger is updated. It affects the system's ability to resist malicious actions and, in general, how data is recorded and secured. The ledger structure refers to how data is organised and structured in the system.

El Ioini and Pahl (2018) reviewed and snapshot four main types: (1) blockchain, (2) tangle, (3) hashgraph and (4) sidechain. All of them have the same main features of a DLT, but differ in data structure, fault tolerance and consensus mechanisms used³³.

Blockchain is a cryptographic, decentralised, and distributed digital ledger that allows transactions to be recorded. In particular, transaction history is recorded into blocks. Each block is chained to the previous one through a hash code. This structure ensures immutability and allows all network participants to access the stored data³⁴.

Tangle is a DLT model developed by IOTA to eliminate transaction fees. Information is stored through a directed acyclic graph (DAG), instead of blocks. Nodes in DAG are called sites. Each site represents a transaction, and their connections represent their validation³⁵.

²⁹ Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. ACM computing surveys, cit.

³⁰ Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. ACM computing surveys, cit.

³¹ Gaschi, A., & Portale, V. (n.d.). La definizione di blockchain e distributed Ledger, in blockchain e smart contract. In *Blockchain e Smart Contract*. Lefebvre Giuffrè.

³² Ibid.

³³ El Ioini, N., and Pahl, C. (2018). *A review of distributed ledger technologies*. cit.

³⁴ Ibid.

³⁵ Ibid.

Hashgraph also uses DAG for data structure and a gossip consensus protocol to validate transactions. Gossip protocol implies that users can choose other users to communicate about an occurred transaction³⁶.

Sidechain combines private and public blockchain architecture to overcome some limitation of the blockchain system. On the one hand, a central blockchain manages access requests (public blockchain); on the other hand, there are sidechains in charge for local transactions (private blockchain)³⁷.

1.3 Blockchain. Definition and features.

The first application of a DLT technology has been blockchain³⁸. Blockchain³⁹ is a cryptographic, decentralised, and distributed digital ledger that allows transactions to be enacted and recorded⁴⁰. The ledger is made of chained blocks that store information through the activity of nodes. Nodes are the computational resources that, by using processing power and electricity, validate transactions and add them to the distributed ledger. Transaction history is recorded into blocks. Each block is chained to the previous one through a cryptographic hash code⁴¹. This structure ensures immutability and allows all network participants to access the stored data.

On the one hand, blockchain is a platform that enables the execution of commercial transactions with a high degree of security and without intermediation⁴². On the other hand, considering data collection and data maintenance set-up, it may be qualified as a ledger in which the sharing and management of information assets are decentralised and entrusted to a plurality of users.

The scope is to eliminate intermediation and the related transaction costs⁴³. In traditional payment systems, the presence of a third party is essential to ensure the proper execution of the transaction. These systems are described by Nakamoto as trust based. In his white paper, he proposes an alternative model that relies on cryptographic proof rather than trust.

³⁶ Ibid.

³⁷ Ibid.

³⁸ Maull, R., Godsiff, P., Mulligan, C., Brown, A., & Kewell, B. (2017). Distributed ledger technology: Applications and implications. *Strategic Change*, 26(5), 481–489. <https://doi.org/10.1002/jsc.2148>.
Ugarte, R. (2018). Distributed ledger technology (DLT): introduction, cit.

³⁹ Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.
Michael, J., Cohn, A. L. A. N., & Butcher, J. R. (2018). Blockchain technology. *The Journal*, 1(7), 1-11.

⁴⁰ Tabatabaei, M. H., Vitenberg, R., & Veeraragavan, N. R. (2022). Understanding blockchain: definitions, architecture, design, and system comparison. *arXiv (Cornell University)*. <https://doi.org/10.48550/arxiv.2207.02264>.

⁴¹ Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, 52, 102039. <https://doi.org/10.1016/j.seta.2022.102039>

⁴² Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit.

⁴³ Ibid.

Lin and Liao (2017) identify six features for blockchain technology⁴⁴:

- decentralisation
- transparency
- open source
- autonomy
- immutability
- anonymity

Decentralisation. Decentralisation, as already specified in paragraph _x_, implies that data are not stored on a central server, but are shared across multiple nodes in the network, each contributing to validate and record information. Each node retains a record of transactions and verifies them⁴⁵. This process updates a shared global state, which serves as an efficient cumulative snapshot of all prior transactions⁴⁶.

Transparency. Transparency allows each node to view the data record and verify updates, fostering trust on the blockchain system. The reliability of data is essential to achieve transparency⁴⁷. However, this feature also concerns with the exposure of personal information⁴⁸. Although blockchain addresses are not directly linked to real-world identities, transaction patterns and propagation time can be analysed to infer connections between addresses and even identify the originating IP addresses of a transaction⁴⁹.

Open source. An open-source system allows users to access the protocol, examine past records, and potentially use the technology to develop new tools or applications. What differentiates an open-source system from a proprietary system is the license⁵⁰. In both cases, the license remains to the user. The proprietary system allows for the use of a copy of the program. In the open-source system, the rights of end users are broader⁵¹. Users can in fact use, modify, copy⁵² and, in general, operate in a deeper way on the program. In any case, the copyright remains to the creator.

⁴⁴ Lin, I., & Liao, T. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, 19(5), 653–659. [https://doi.org/10.6633/ijns.201709.19\(5\).01](https://doi.org/10.6633/ijns.201709.19(5).01)

⁴⁵ Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, 32(3), 1779–1794. <https://doi.org/10.1007/s12525-022-00536-0>

⁴⁶ Ibid.

⁴⁷ Bertino, E., Kundu, A., & Sura, Z. (2019). Data transparency with blockchain and AI ethics. *Journal of Data and Information Quality (JDIQ)*, 11(4), 1-8. <https://doi.org/10.1145/3312750>

⁴⁸ Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations, cit.

⁴⁹ Biryukov, A., & Tikhomirov, S. (2019, June). Deanonymization and linkability of cryptocurrency transactions based on network analysis. In 2019 IEEE European symposium on security and privacy (EuroS&P) (pp. 172-184). <https://doi.org/10.1109/eurosp.2019.00022>

⁵⁰ Franco, P. (2014). *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons. <http://ci.nii.ac.jp/ncid/BB17851910>

⁵¹ Ibid.

⁵² Ibid.

Autonomy. Autonomy refers to the possibility for each node to validate and transmit information autonomously, according to the consensus mechanism procedures and functioning. The consensus mechanism allows participants to solve the mathematical problem necessary to validate the operation, and consequently to add blocks to the system⁵³. This operation does not require the collaboration between nodes nor the intermediation of a central authority.

Immutability. Immutability refers to the fact that once recorded in the blockchain, data is immutable. Changes can be adopted if 51% of the nodes agree on that. Even when information is modified - for instance, due to the transfer of an asset from one holder to another - the system preserves all previously recorded data. As a result, the blockchain displays the full sequence of transactions related to a given asset and, more generally, all changes made to specific information over time.

Anonymity. Anonymity of transaction is a fundamental factor to allow the acceptance of a system where data are publicly accessible⁵⁴. Thanks to anonymity, users can preserve their identity and operate securely, without the risk of being traced⁵⁵. However, anonymity does not guarantee that the identity of a user remains unknown. For instance, a study of Goldfeder et al. (2017) demonstrated that third-party trackers can identify blockchain transactions and link them to the owners; similarly, trackers can link more trades of the same user⁵⁶.

In the blockchain model developed by Nakamoto, the essential technical and functional components mentioned in the white paper are:

- a peer-to-peer network
- hash cryptography for digital signature
- the use of public and private key cryptography
- the Proof of Work (PoW) consensus mechanism
- nodes and miners

Peer-to-peer network. As previously mentioned in the section on DLTs, a peer-to-peer (P2P) network is a distributed system in which each node shares its resources (such as computing power, storage, or bandwidth) directly with other nodes, without relying on a central server. In this model, devices operate both as clients and servers, enabling a resilient and self-organising structure that remains functional even in the event of

⁵³ Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations* (pp. 225-253). Edward Elgar Publishing. <https://doi.org/10.4337/9781784717766.00019>

⁵⁴ Andola, N., Yadav, V. K., Venkatesan, S., & Verma, S. (2021). Anonymity on blockchain based e-cash protocols—A survey. *Computer Science Review*, 40, 100394. <https://doi.org/10.1016/j.cosrev.2021.100394>

⁵⁵ Averin, A., Samartsev, A., & Sachenko, N. (2020, September). Review of methods for ensuring anonymity and de-anonymization in blockchain. In *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 82-87). IEEE. <https://doi.org/10.1109/itqmis51053.2020.9322974>

⁵⁶ Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *Proceedings on Privacy Enhancing Technologies*, 2018(4), 179–199. <https://doi.org/10.1515/popets-2018-0038>

failures⁵⁷. Once the transaction is broadcast into the P2P network, the miners verify the transaction through mathematical computation.

Hash cryptography. Hash cryptography refers to the use of mathematical algorithms (known as hash functions) that convert input data of any length into a shorter fixed-length output⁵⁸. These functions are designed to be extremely difficult to reverse⁵⁹. It means that it is computationally infeasible (almost impossible) to reconstruct the original input from the hash value. They are also highly sensitive to changes in input and are commonly used for data integrity purposes⁶⁰. Even a minor alteration in the input results in fact in a different output.

The implementation of the blockchain is made through a timestamp server. The timestamp is imprinted in the hash together with the previous one⁶¹. In this way, the blocks with the timestamps are chained, reinforcing the information integrated before⁶².

Consensus mechanism. Consensus mechanism has already been defined in paragraph 1.2 as the process through which operations are validated and approved within distributed ledger technologies. The consensus mechanism, therefore, consists of the set of rules used to determine which blocks and transactions are valid. Fahim et al. (2003) have defined it as “*a mechanism that manages which participants in the network get to set the state of truth that everyone else follows and agrees on*”⁶³.

In the Bitcoin system, the Proof-of-Work (PoW) mechanism is adopted, and consensus is reached through the activity of nodes and miners. The blocks, aggregated by miners, are approved only if the nodes reach consensus about the validity of the transaction⁶⁴.

Before specifically analysing Proof-of-Work and other mechanisms, it is worth focusing on the concepts of node, miner and user.

Nodes, users and miners. The user is the natural or legal person who holds a public and a private key and carries out transactions on the blockchain. The user does not contribute to the validation or storage of data.

⁵⁷ Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. ACM computing surveys, cit.

⁵⁸ Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In *Journal of Physics: Conference Series* (Vol. 1168, p. 032077). IOP Publishing. <https://doi.org/10.1088/1742-6596/1168/3/032077>

⁵⁹ Pilkington, M. (2016). Blockchain technology: principles and applications, cit.

⁶⁰ Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain, cit. According to the Authors their features are susceptibility, unidirectionality, collision resistance, and high sensitivity.

⁶¹ Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit..

⁶² Ibid.

⁶³ Fahim, S., Rahman, S. K., & Mahmood, S. (2023). Blockchain: A Comparative Study of Consensus Algorithms POW, POS, POA, POV. *International Journal of Mathematical Sciences and Computing*, 9(3), 46–57. <https://doi.org/10.5815/ijmsc.2023.03.04>

⁶⁴ Franco, P. (2014). *Understanding Bitcoin: Cryptography, engineering and economics*, cit.

The node is the computational resource that validates transactions to insert them into the chain. Nodes monitor transactions to ensure that only legitimate ones are validated, thereby solving the problem of double spending. This prevents the same cryptocurrency from being spent twice, thereby preserving trust in the system. In fact, if cryptocurrency could be spent more than once, no one would trust the blockchain platforms to perform operations.

Miners are nodes that, in exchange for compensation, aggregate transactions into blocks, adding them to the blockchain after solving complex cryptographic calculations. This computational search activity is called mining and consists, precisely, in the creation and addition of new blocks as a result of the calculations. The proper conduct of miners in performing this activity is ensured by a compensation mechanism that incentivises participants not to engage in abusive behaviour.

Having clarified the rules of such entities, we can now focus on consensus algorithms. Fahim et al. (2023) have provided a study of consensus algorithms, comparing the main ones in terms of security, energy efficiency, scalability and IoT compatibility. The study highlights how every consensus mechanism has its strengths and weaknesses, impacting the blockchain performance and security features.

Proof-of-Work (PoW). The consensus mechanism used by Nakamoto for Bitcoin is Proof-of-Work. In terms of security, PoW is the best consensus algorithm for blockchain⁶⁵. Proof-of-Work is based on a reward system aimed at compensating miners who correctly guess a specific numerical sequence. The first miner to identify it will receive a financial incentive for their work, after other nodes have verified the accuracy of the sequence. The name "Proof-of-Work" refers to the fact that each validated block contains a hash that represents the miner's work⁶⁶. However, considering consumption, this consensus mechanism requires a large amount of energy. The calculation of the algorithms requires computers that uses a lot of energy.

Proof-of-Authority (PoA). Proof-of-Authority is mostly used in private blockchains. Only approved participants, called validators, can create new blocks. These validators must prove their identity. Identification gives trust to the system since validators don't want to have a bad reputation. Validators are selected through a strict approval process. Once approved, they use software to group transactions into blocks. The process is automatic and uses very little energy. Validators do not need to compete with each other⁶⁷. PoA is fast and efficient, but it is less decentralised. Only a small number of people are allowed to validate blocks.

Proof-of-Stake (PoS). In Proof-of-Stake, there are no miners but validators. To become one, the user must stake (lock) a certain number of coins in the network: a sort of deposit. The more coins a validator locks, the higher the chance they will be chosen to create the next block. If they validate bad transactions, they lose part of their stake.

⁶⁵ Fahim, S., Rahman, S. K., & Mahmood, S. (2023). Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV, cit.

⁶⁶ Ibid.

⁶⁷ Ibid.

This helps keep them honest. PoS uses much less energy than Proof-of-Work since other validators cannot operate if one has already started. It is more accessible, but people with more coins still have more power and could approve fraudulent transactions.

Proof-of-Vote (PoV). Proof-of-Vote is used in consortium blockchains. The system is based on voting. There are four roles: commissioners, butler candidates, butlers, and regular users. Commissioners vote and choose Butlers. Butlers create new blocks, but without using a lot of energy. Before a block is added, it must be approved by a vote. Candidates need to apply, pay a deposit, and get a recommendation. Regular users can only watch or send messages unless they are authorised. PoV is fast and energy efficient. It avoids chain splits and keeps the network stable. But it is only for closed, permissioned systems.

1.4 Classifications.

A first classification concerns the accessibility of the system. One can distinguish between public and private blockchains, depending on whether access is open to anyone (for example, Bitcoin, which is global and has no entry barriers⁶⁸) or restricted to a group of selected participants, often linked by the same type of business relationships⁶⁹.

The second classification refers to the type of action a user can perform in the blockchain⁷⁰. In permissionless blockchains, users can not only view information but also take part in the consensus process. This allows a more active role on the platform. This kind of structure supports a free market system, where no one can stop a transaction from being executed and recorded on the blockchain.

In permissioned blockchains, on the other hand, users' rights are defined in advance⁷¹. Their level of involvement is decided on a case-by-case basis. In some cases, users can only view data⁷². In others, they may also be allowed to validate transactions and/or write data to the system.

⁶⁸ Sarzana Di S. Ippolito, F., & Nicotra, M. (2018). *Diritto della Blockchain, Intelligenza artificiale e Iot*. Wolters Kluwer Italia.

⁶⁹ Jaikaran, C. (2018). *Blockchain: Background and Policy Issues* (No. R45116). Congressional Research Service. <https://www.congress.gov/crs-product/R45116>

⁷⁰ Ibid. «Discussing a blockchain as public or private refers to the level of freedom users have to create identities on that blockchain. Discussing a blockchain as permissioned or permissionless refers to the level of access the user would have on that blockchain».

⁷¹ For a different classification, see Sarzana Di S. Ippolito, F., & Nicotra, M. (2018). *Diritto della Blockchain, Intelligenza artificiale e Iot*, cit., who simplify this framework by associating public blockchains with permissionless systems and private blockchains with permissioned ones, identifying accessibility and involvement as necessarily complementary elements. The authors also identify a third category, the so-called hybrid blockchain, in which the consensus mechanism is controlled by pre-selected nodes.

This classification seems to contradict the fact that there are also public blockchains where user participation is limited, and which can therefore be related to the permissioned model (e.g., public registries).

⁷² Jaikaran, C. (2018). *Blockchain: Background and Policy Issues*, cit.

Permissioned blockchains rely on roles within the system. These roles can be seen as hierarchical, since the level of participation is set beforehand. This structure fits well with the needs of businesses and public administrations, where order and control are necessary. It would not be acceptable for anyone to make changes to official content (e.g. a registry office issuing birth certificates).

In these cases, the actors behind a permissioned blockchain provide rules of behaviour (governance). Usually, permissioned blockchains do not use the same validation mechanisms as permissionless blockchains do.

In permissioned blockchains, instead, trust and security are related to the infrastructure that governs the platform. Only the authorised entities can validate transactions and define the rules.

In any case, features from these classifications can be combined, leading to different blockchain models⁷³. The main reference model is still the public permissionless blockchain, where anyone can create an identity and access all functions. However, other configurations are possible - for example, public blockchains where only some users can add blocks, while others can only view their content.

1.5 Functioning.

As already explained, permissionless blockchain like Bitcoin works through a decentralised, peer-to-peer network. This paragraph describes how the features illustrated before are implemented in a blockchain.

In a blockchain, each user holds a pair of cryptographic keys: a public key and a private one. The public key acts as an account address. It is visible to other users and used to receive funds. The private key is kept secret and allows the user to sign transactions and prove ownership of the coins.

The user who wants to start a transaction enters the recipient's address and the amount to send. Then, the user digitally signs the transaction with the private key. It proves that the user is authorised to spend those funds.

The signed transaction is broadcast to the network, reaching all nodes. Miners, collect these transactions and put them into a new block. But before the block can be added to the blockchain, it must be validated. To this end, miners compete to solve a computational problem. Once a miner finds a valid solution, they propose the block to the network. The other nodes verify it. If the solution and the transactions are correct, the block is accepted and stored in the blockchain, becoming a permanent and immutable part of the ledger.

Each block contains:

- a list of verified transactions

⁷³ Patti, L. (2016). Dal codice civile al codice binario: blockchain e smart contracts. *Cyberspazio E Diritto*, 325–344.

- a timestamp marking the moment the block was created
- the cryptographic hash of the previous block, ensuring the chain's continuity

This last element links the blocks together and guarantees immutability. After validation, the new block is replicated across all nodes, and each participant may see the same updated version of the blockchain.

The entire system works through this distributed verification. It removes the need for intermediaries. It also guarantees that no transaction can be changed once it has been added to the chain.

1.6 Case studies of blockchain protocols. Bitcoin and Ethereum.

We are now going to analyse how these tokens are integrated into different blockchains⁷⁴.

Bitcoin. Bitcoin was the first crypto asset developed using blockchain technology. The term "Bitcoin" refers both to the digital currency itself and to the blockchain platform that enables its use for instant global payments. As previously explained, blockchain operates as an open-source, peer-to-peer system, accessible to anyone who wishes to participate. Bitcoin is not only a means of payment but is also regarded as a speculative investment. Its sharp increase in value has attracted significant interest from investors. For instance, in May 2016, one bitcoin was worth approximately €400. By May 2025, its value had risen to over €96,000.



The Bitcoin protocol includes a built-in mechanism to gradually reduce the number of new bitcoins issued per block. This reduction occurs roughly every 210,000 blocks, or about every four years, as a way to control inflation. As a result, the rewards granted to miners decrease over time. To sustain miners' engagement and offset the diminishing block rewards, the network compensates by increasing transaction fees.

⁷⁴ Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University-Computer and Information Sciences*, 34(9), 6793-6807 <https://doi.org/10.1016/j.jksuci.2021.08.005>

Ethereum. Ethereum⁷⁵ is a blockchain network that implements smart contracts and Bitcoin blockchain system⁷⁶. Smart contracts are programmed in Solidity. Ethereum allows developers to embed logical structures (e.g. conditions) into transaction scripts, a feature that sets Ethereum apart from Bitcoin. This kind of structure, known as control flow, defines how and when certain actions are executed during a transaction⁷⁷. Ethereum enables the creation of fully digital economic systems, where money can be handled like data, and then in a fast way⁷⁸. Unlike traditional banks, which involve long delays and high transaction costs, Ethereum allows users to transfer small payments globally in real time, without relying on complex infrastructures or financial intermediaries. Initially, Ethereum used a modified version of the GHOST protocol to reach consensus in a Proof of Work (PoW) system, where even blocks not included in the main chain (so-called uncle blocks) could still receive partial rewards⁷⁹. However, since “The Merge” in September 2022, Ethereum has transitioned to a Proof of Stake (PoS) model, where validators are selected based on the amount of cryptocurrency they stake, rather than on computational power. This change significantly reduced energy consumption and marked a major evolution in Ethereum’s consensus mechanism.

Beyond Bitcoin and Ethereum, numerous other blockchains have been developed to optimise specific aspects of the protocol. For example, Cardano is a blockchain network created in 2017 by Charles Hoskinson, one of the original developers of Ethereum. Like Ethereum, Cardano is capable of processing transactions rapidly while supporting smart contracts and decentralised applications (dApps). The platform’s structure has been enhanced to improve both the scalability and environmental sustainability of the blockchain. Cardano uses a Proof of Stake (PoS) consensus algorithm, which results in lower energy consumption. As noted in the previous paragraph, Ethereum also transitioned to PoS in 2022. Another example of blockchain technology is Hyperledger. One of its main distinctive features is the possibility of choosing which consensus mechanism to employ⁸⁰. This characteristic is particularly relevant when considering the significant energy consumption associated with certain consensus systems. IOTA likewise represents an innovative blockchain model, not only for having created a feeless market, but also for establishing partnerships with private companies to test and implement real-world applications⁸¹.

⁷⁵ Buterin, V. (2013). Ethereum white paper, cit..

⁷⁶ Tikhomirov, S. (2017, October). Ethereum: state of knowledge and research perspectives. In *International symposium on foundations and practice of security* (pp. 206-221). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-75650-9_14

⁷⁷ Dannen, C. (2017). *Introducing Ethereum and solidity* (Vol. 1, pp. 159-160). Berkeley: Apress.

⁷⁸ Ibid.

⁷⁹ Vujičić, D., Jagodić, D., & Randić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)* (pp. 1-6). IEEE. <https://doi.org/10.1109/infoteh.2018.8345547>

⁸⁰ Kareem, Y., Djenouri, D., & Ghadafi, E. (2024). A survey on emerging blockchain technology platforms for securing the internet of Things. *Future Internet*, 16(8), 285. <https://doi.org/10.3390/fi16080285>

⁸¹ Ibid.; For case studies in the financial sector, see Polyviou, A., Velanas, P., & Soldatos, J. (2019). Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies. *MDPI*, 7. <https://doi.org/10.3390/proceedings2019028007>

2. Cryptocurrency and Crypto asset.

Blockchain was introduced to eliminate intermediaries and enhance transparency in contracts. Nakamoto also introduced a new currency to be exchanged in the blockchain: Bitcoin. In the white paper, he mentions the word bitcoin only twice: in the title and the subtitle. Additionally, the word ‘*currency*’ appears only in the abstract. The paper is in fact directed to explain the functioning of the platform rather than the value exchanged. However, the community’s interest was immediately directed to the financial opportunity that Bitcoin could generate. The advent of Bitcoin has had relevant repercussions in economic exchanges. Its usage resulted in an increasing growth of virtual currencies both for commercial purposes and financial investments. The absence of cost and intermediation attracted investors to new financial opportunities. Bitcoin started to be used as compensation in transactions and as a financial product.

Bitcoin is a cryptocurrency. A cryptocurrency is a type of virtual currency, a digital representation of value issued by a private developer. It can be used as a means of payment or as a speculative asset.

Virtual currencies are divided into first-generation and second-generation currencies. First-generation virtual currencies emerged within the context of web-based gaming, where monetary conversion was required to purchase in-game items. These currencies are unidirectional: they can be converted into virtual items but cannot be reconverted into real-world money. Conversely, second-generation virtual currencies can be generated and exchanged in both directions. They can be converted at any time, based on an exchange rate determined by market supply and demand. It is this bidirectionality that distinguishes them from earlier forms of virtual currencies⁸².

Virtual currencies can also be divided into centralised convertible currencies and decentralised convertible currencies⁸³. The first category is issued and controlled by a central authority that manages the trade of the value. The second one is based on blockchain technology and traded in a decentralised way. Bitcoin cryptocurrencies belong to this category. Virtual currencies must be distinguished from official legal currencies, issued by institutional entities or companies, and electronic money, which is substantially a digital record of a banking account and can be used for payments⁸⁴.

As anticipated, the value of virtual currency is determined by a supply-and-demand system. Its use as consideration is left to the will of the parties that have to recognise it as a means of payment. Virtual currency is not legal tender. Its exchange value is

⁸² Chierici, M. (2018). La blockchain: una lettura giuridica per uno sguardo verso il futuro. *Cyberspazio E Diritto*, 19(61), 385–419.

⁸³ Chikh, F. (2024). Cryptocurrencies: An etymological approach. *International journal of economic perspectives*, 18(7), 1057-1064.

⁸⁴ Ibid.

solely determined by the contingent fact that a plurality of parties recognise it as a monetary unit suitable to serve as consideration⁸⁵.

The term cryptocurrency was not coined by Nakamoto, who referred to a peer-to-peer currency, but originated in online forums and media⁸⁶. The word crypto might seem to refer only to cryptography, but it also reflects ideas from the cypherpunk movement: a group that promoted the use of anonymous and untraceable payments to support systems free from central control⁸⁷. Bitcoin reflects this vision, as stated in Nakamoto's white paper, where the system replaces trust in third parties with cryptographic proof⁸⁸.

Cryptocurrency is also defined as a digital asset⁸⁹ primarily used as a means of exchange. The term digital asset is more general and refers to every asset stored in a computer or on the internet in binary form and includes the right to use it⁹⁰. In general, a digital asset is an intangible asset and could be an image, a video or a file. If referring to a cryptocurrency, it could include the rights of property, usage, voting, etc. Other digital assets are stablecoins, digital tokens and central bank digital currencies⁹¹.

Then, cryptocurrency can be defined as a virtual currency created by a private developer that cannot be traced back to legal tender since it is not issued by any central bank⁹². It has been created as a token to be exchanged in blockchain, as a sort of digitisation of an asset's value⁹³.

According to the European Central Bank, cryptocurrency is also a speculative asset; investors could then gain profit, but there is also the risk of losing money⁹⁴. It can be exchanged electronically, and its value is determined by the general consensus among a plurality of parties recognising it as a suitable monetary unit for transactions. It is not, in fact, a generally accepted form of payment⁹⁵.

The European Commission, in its Regulations, refers to them as crypto assets. In this regard, former BCE president Mario Draghi affirmed that "*Bitcoin and cryptocurrency, or anything like that, are not really currencies, they are assets. One*

⁸⁵ Cosa sono i bitcoin?, in <https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.it.html>, 2018.

⁸⁶ Pernice, I. G., & Scott, B. (2021). Cryptocurrency. *Internet policy review*, 10(2). <https://doi.org/10.14763/2021.2.1561>

⁸⁷ Ibid.

⁸⁸ Ibid.

⁸⁹ Milutinović, M. (2018). Cryptocurrency. *Ekonomika*, 64(1), 105–122. <https://doi.org/10.5937/ekonomika1801105m>

⁹⁰ Toygar, A., Rohm Jr, C. E., & Zhu, J. (2013). A new asset type: digital assets. *Journal of International Technology and Information Management*, 22(4). <https://doi.org/10.58729/1941-6679.1024>

⁹¹ Kochergin, D. (2022). Crypto-assets: Economic nature, classification and regulation of turnover. *International organisations research journal*, 17(3), 75-130. <https://doi.org/10.17323/1996-7845-2022-03-04>

⁹² Abramowicz, M. (2016). Cryptocurrency-based law. *Ariz. L. Rev.*, 58, 359.

⁹³ Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., & Li, L. (2022). Cryptocurrency trading: a comprehensive survey. *Financial Innovation*, 8(1), 13. <https://doi.org/10.1186/s40854-021-00321-6>

⁹⁴ <https://www.ecb.europa.eu/ecb-and-you/explainers/tell-me/html/what-is-bitcoin.en.html>

⁹⁵ Ibid.

*euro is one euro: today, tomorrow, in a month, it's always one euro*⁹⁶. Accordingly, the European Union (EU) in its legislative acts refers to them as crypto assets. The EU defines them as a digital representation of a value or of a right that can be transferred and stored electronically using distributed ledger technology or similar technology⁹⁷. The proper term to be used when referring to cryptocurrency should then be “crypto asset”.

2.1 Categories of crypto assets. Classification by function.

Several types of crypto assets have been created in recent years. Having regard to their function, it is possible to identify⁹⁸:

- payment cryptocurrency
- utility tokens
- security tokens
- governance tokens

Payment/exchange crypto assets. Payment crypto asset is a digital currency used as a means of exchange and a form of electronic cash to facilitate transactions. It is usually used as a payment method and acts in the same way as virtual currencies. Bitcoin is an example of this kind of currency.

Utility token. The utility token is a currency that gives access to products and services within a specific blockchain ecosystem. The first utility token – the Ether - was created with Ethereum by Vitalik Buterin. Utility tokens allow for the usage of smart contracts or decentralised autonomous organisations.

Security tokens. Security tokens can represent the ownership or, more broadly, other rights of an asset's owner. Through tokenisation, a digital representation of the right is stored on a blockchain and can be exercised by the owner⁹⁹. They can be assimilated to traditional financial instruments (stock, bonds, etc)¹⁰⁰.

Governance tokens. Governance tokens allow participation in the network decisions. They are often issued in decentralised autonomous organisations and provide the decision-making power to their owner. They include the right to vote.

2.2 Classification by technological generation.

Considering the technology generation used and purpose, it is possible to classify:

- first-generation crypto assets
- second-generation crypto assets

⁹⁶ Interview available at link: <https://www.youtube.com/watch?v=IRc7eLQ34Ts>

⁹⁷ Art. 3, Regulation (EU) 2023/1114 on markets in crypto-assets (MiCAR).

⁹⁸ <https://corporatefinanceinstitute.com/resources/cryptocurrency/types-of-cryptocurrency/>

⁹⁹ <https://www.investopedia.com/terms/s/security-token.asp>

¹⁰⁰ Kochergin, D. (2022). Crypto-assets: Economic nature, classification and regulation of turnover, cit.

- third-generation crypto-assets

First generation. First-generation crypto assets, such as Bitcoin, are directed to perform transfers of value and exchanges. These crypto assets are based on PoW to enable P2P transactions and integrate the functionalities described in Nakamoto's white paper.

Second generation. Second-generation crypto assets are related to the implementation of smart contracts within the blockchain ecosystem. A smart contract is an IT program capable of incorporating and executing the terms of a contract¹⁰¹. Execution is triggered once the system verifies that the necessary conditions for its enforcement have been met¹⁰². With the creation of the Ethereum platform, blockchain functionalities have been extended to the realm of contracts¹⁰³. Through these features, it is now possible to develop decentralised applications (or dApps) that, like Bitcoin transactions, are executed in a decentralised manner. In essence, Ethereum provides a platform where users can create applications capable of self-execution. These dApps are written using Ethereum's dedicated programming language, Solidity, and can involve virtually any type of transaction. Once created, they are made available to users, who can purchase and use them across a wide range of sectors.

Third generation. Third-generation crypto assets aim to address the scalability, limitations of first and second-generation cryptos¹⁰⁴. The necessity of a large amount of energy and the slow transaction speed could disincentive users from joining the network. The new generation of crypto assets tries to overcome these issues related to scalability by implementing more efficient consensus mechanisms and greater system flexibility¹⁰⁵. An example of third third-generation system is Cardano. Cardano uses a peer-reviewed PoS protocol, which drastically reduces energy use while maintaining security. It offers higher transaction capacity and supports interoperability features. Another example is Solana, which includes decentralised finance and non-fungible token applications. Solana uses a consensus mechanism called Proof-of-History (PoH) that, combined with PoS, achieves very high throughput (up to 50,000 TPS) and low transaction costs.

2.3 Classification by value stability. Stablecoins.

Another important distinction is between volatile crypto assets and stablecoins. The first distinction is between:

¹⁰¹ Szabo, N. (1994). *Smart Contract*.

<https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>

¹⁰² Goldenfein, J., & Leiter, A. (2018). Legal engineering on the blockchain: 'Smart contracts' as legal conduct. *Law And Critique*, 29(2), 141–149. <https://doi.org/10.1007/s10978-018-9224-0>

¹⁰³ Yuan, R., Xia, Y., Chen, H., Zang, B., & Xie, J. (2018). ShadowETH: Private Smart Contract on Public Blockchain. *Journal of Computer Science and Technology*, 33(3), 542–556. <https://doi.org/10.1007/s11390-018-1839-y>; Attico, N. (2018). *Blockchain. Guida all'ecosistema. Tecnologia, business, società*, cit.

¹⁰⁴ <https://www.rennoco.com/blog/a-new-age-of-cryptocurrencies-3rd-generation-coins>

¹⁰⁵ Ibid.

- *unbacked crypto assets*, crypto assets without a stabilisation mechanism that anchors their value to a reference asset (such as Bitcoins and algorithmic stablecoins, whose stabilisation mechanism is based on an algorithm that conditions their supply and demand in the market);
- *asset-linked stablecoin*, crypto assets backed by underlying assets that aim to maintain a stable value relative to a fiat currency, a specific asset, a pool or a basket of assets, commodities, tangible assets or economic measures¹⁰⁶.

Stablecoins are virtual currencies¹⁰⁷ pegged to a fiat currency or other values that do not expose investors to the high and consistent risks associated with cryptocurrency¹⁰⁸. They are based on DLT technology and secured by cryptography. The term ‘stablecoin’ was coined by the development team behind the Dai Stablecoin system. The introduction of stablecoins addresses the excessive volatility and fluctuations associated with popular digital assets¹⁰⁹. Volatility is in fact a factor that has curbed the development of credit and debit exchanges in the market of crypto assets¹¹⁰. Their stability is ensured by the link with an underlying specified asset (such as USD)¹¹¹ or a basket of assets¹¹². This kind of asset has been created to enhance the potential of permissionless DLTs¹¹³.

All stablecoins are designed to keep their price close to a reference value, typically one unit of fiat currency such as the US dollar¹¹⁴. This target value is known as peg¹¹⁵, and it defines the fixed price level the system aims to maintain. When the market price deviates from this peg, the protocol must act to restore balance. The most common solution is to adjust the supply: if the price is too high, the system increases the number of tokens in circulation; if it is too low, the supply is reduced.

¹⁰⁶ <https://www.blockchain.com/ru/static/pdf/StablecoinsReportFinal.pdf>

¹⁰⁷ Kochergin, D. (2022). Crypto-assets: Economic nature, classification and regulation of turnover, cit.

¹⁰⁸ European Commission, “European Financial Stability and Integration Review” (2022) SWD(2022) 93 final/2 https://finance.ec.europa.eu/system/files/2022-04/european-financial-stability-and-integration-review-2022_en.pdf.

¹⁰⁹ The Dai Stablecoin System (2017) <https://makerdao.com/whitepaper/DaiDec17WP.pdf>, Liao, G. Y., & Caramichael, J. (2022). Stablecoins: growth potential and impact on banking. *International Finance Discussion Paper*, 2022.0(1334), 1–26. <https://doi.org/10.17016/ifdp.2022.1334>

¹¹⁰ <https://www.blockchain.com/ru/static/pdf/StablecoinsReportFinal.pdf>

¹¹¹ Bindseil, U., & Pantelopoulos, G. (2023). Unbacked Crypto-Assets, stablecoins and CBDC. In *Springer texts in business and economics* (pp. 125–152). https://doi.org/10.1007/978-3-031-39520-8_9

¹¹² van der Merwe, A. (2021). A Taxonomy of Cryptocurrencies and Other Digital Assets. *Review of Business*, 41(1).

¹¹³ Brooks, S., Jurisevic, A., Spain, M., & Warwick, K. (2018). *A decentralised payment network and stablecoin*, v0.7. Havven. https://cryptorating.eu/whitepapers/Havven/havven_whitepaper.pdf

¹¹⁴ Moin, A., Sekniqi, K., & Sirer, E. G. (2020). SoK: A classification framework for stablecoin designs. In *Financial cryptography and data security: 24th international conference, FC 2020, kota kinabalu, Malaysia, february 10–14, 2020 revised selected papers 24* (pp. 174–197). Springer International Publishing.

¹¹⁵ Peg indicates the target value the stablecoin aims to maintain, typically set at a 1:1 ratio with a fiat currency such as the US dollar. When the market price of the stablecoin deviates from this reference point, specific mechanisms are triggered to bring it back in line.

The economic features of stablecoin are¹¹⁶:

- diffusion by identified issuers on DLTs (which differentiates it from crypto assets)
- maintenance of stability through a peg with a fiat value/other asset, or algorithmic technologies
- suitability to be used as a medium of exchange, payment and other functions.

Liao and Caramichael (2022) classified three types of stablecoins:

- *public reserve-backed stablecoins*, crypto assets supported by cash equivalent assets (e.g. bank deposits, treasury bills, etc.), commonly known as custodial stablecoins. They are issued as reserves by intermediaries that hold the corresponding reserves and guarantee the redeemability of tokens;
- *public algorithmic stablecoins*, crypto assets relying on a smart contract that liquidate automatically when their value falls below a certain threshold; the peg is maintained through smart contracts that adjust supply and demand by trading the stablecoin against a linked governance token. Control over these protocols is typically linked to governance tokens, which grant holders the ability to vote on protocol updates or governance decisions.
- *institutional or private stablecoins*, crypto assets issued by financial and non-financial institutions. They are used for internal transactions, liquidity management, and transactions between user accounts within the same private network in permissioned DLTs.

2.4 Stablecoin use cases.

Stablecoin's current use spans several areas of the digital economy.

*Digital markets and payments*¹¹⁷. In digital markets, stablecoins function as a reliable trading pair, providing a convenient bridge between traditional currencies and blockchain-based assets. Their capacity to support fast and direct transactions makes them particularly effective in this domain. Beyond trading, stablecoins are frequently utilised for both domestic and international payments. Their design facilitates near-instant transfers, which can occur at any time, eliminating the need for traditional financial intermediaries.

*Store of value*¹¹⁸. Stability enables these assets to function as a store of value, especially in contexts where users need to secure liquid reserves to cover future costs (e.g. miners covering hardware and electricity expenses). In contrast, unbacked crypto assets are generally too volatile to serve this function effectively. Stablecoins offer a safer way to preserve capital, particularly during periods of market uncertainty.

¹¹⁶ Kochergin, D. (2022). Crypto-assets: Economic nature, classification and regulation of turnover, cit.

¹¹⁷ Liao, G. Y., & Caramichael, J. (2022). Stablecoins: Growth potential and impact on banking, cit.

¹¹⁸ <https://www.blockchain.com/ru/static/pdf/StablecoinsReportFinal.pdf>

*Internal transfers*¹¹⁹. Some companies and financial institutions use stablecoins to move money between their own departments or branches. This helps them manage liquidity more easily and reduces the need to rely on banks or external payment systems.

*Decentralised applications (dApps)*¹²⁰. Blockchain-based decentralised applications require stable-value assets to be reliable. If an asset value fluctuates unpredictably, users are less likely to use it. Stablecoins help avoid this problem by keeping their value stable, which makes it easier for people to use them within decentralised ecosystems.

Derivatives. Derivatives are used to hedge financial risk. Today, most derivative contracts are settled in fiat and processed through traditional banking systems and clearing houses. Stablecoins could allow these transactions to occur directly on-chain via smart contracts, minimising costs and removing the need for centralised counterparties.

*Decentralised finance*¹²¹. Stablecoins are a core component of decentralised finance platforms. They make possible a wide range of financial operations, including lending, trading, and asset management, all within systems that operate independently of traditional banks.

2.5 Non-Fungible Tokens.

A non-fungible token (NFT) is “a unit of digital information (token) that is stored on a blockchain and is not inherently interchangeable with other digital assets”¹²². The main features of these assets are their non-fungibility and uniqueness. Each token is individual and cannot be exchanged on a one-to-one basis with another. Blockchain technology and smart contracts¹²³ ensures that every non-fungible token is genuinely unique and cannot be replicated. Each NFT carries an identification code that distinguishes it and is certified by the blockchain. NFTs function as digital certificates of ownership, which can be linked either to digital or to physical assets. With regard to digital assets, an NFT may certify ownership rights over multimedia content (for example, videos or images)¹²⁴. In this way, the transfer of ownership becomes simpler, as it only requires the transfer of the token itself. As previously mentioned, NFTs may also concern physical goods, such as real estate property or copyright over a work.

¹¹⁹ Liao, G. Y., & Caramichael, J. (2022). Stablecoins: Growth potential and impact on banking, cit.

¹²⁰ <https://www.blockchain.com/ru/static/pdf/StablecoinsReportFinal.pdf>

¹²¹ Liao, G. Y., & Caramichael, J. (2022). Stablecoins: Growth potential and impact on banking, cit.

¹²² Chohan, U. W. (2021). Non-Fungible Tokens: blockchains, scarcity, and value. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3822743>

¹²³ Hammi, B., Zeadally, S., & Perez, A. J. (2023). Non-fungible tokens: A review. *IEEE Internet of Things Magazine*, 46–50.

¹²⁴ Vella, G. (2025, September 19). NFT cosa sono: applicazioni ed esempi di Non Fungible Token. Osservatori.net. https://www.osservatori.net/blog/blockchain-web3/non-fungile-token-nft-cosa-sono-applicazioni-esempi/#Cosa_sono_gli_NFT

3. Smart Contracts.

Another element used in blockchain is the smart contract. With the creation of the Ethereum platform, the functionalities of blockchain have been extended to the contractual domain, giving rise to what is known as Blockchain 2.0. Through the potential of this new phase, it is possible to develop decentralised applications (*dApps*) that, like Bitcoin transactions, are executed in a decentralised manner.

Ethereum provides a platform where users can build applications capable of self-execution. These *dApps* are written using Ethereum's dedicated programming language, Solidity, and can be designed to handle any type of transaction. Once developed, they are made available to users, who can purchase and deploy them in a wide range of sectors.

While Bitcoin uses blockchain primarily for payments and the transfer of value, Ethereum integrates this technology for a broader set of functionalities, including contractual operations through the usage of smart contracts.

The first definition of smart contracts was provided by Nick Szabo, a computer programmer who, in the early 1990s, theorised their existence based on initial prototypes that had begun to emerge in practice. According to his view, smart contracts are digital protocols designed to facilitate negotiation between parties. Szabo developed the concept to highlight their functionalities, independence from intermediaries, and precision in performance.

Therefore, a smart contract is an IT programme capable of incorporating and executing the terms of a contract¹²⁵ once the system verifies that the necessary conditions are met¹²⁶. More specifically, it is an automated execution protocol which, upon the occurrence of a certain condition, receives a corresponding input and automatically performs the related contractual obligation. The smart contract combines two components: a software element, which encodes the contractual instructions, and a hardware element, which executes the commands¹²⁷.

This technology offers several advantages. Since it operates independently from any human intervention, it ensures strict compliance with payment terms, preventing delays or failures caused by negligent or obstructive behaviour. This configuration also eliminates the need for intermediaries, significantly reducing transaction costs¹²⁸. Moreover, smart contracts can enhance privacy protection, thanks to a pseudonymity system that prevents the identification of the contractual parties.

¹²⁵ N. Szabo, *Smart Contracts*, in <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeechCDRO-M/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>, 1994.

¹²⁶ J. Goldenfein e A. Leiter, *Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct*, cit.

¹²⁷ Manente, M. (2019). L.12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note. www.notariato.it.

¹²⁷ Szabo, N., *Smart Contracts*, cit.

¹²⁸ Capaccioli, S. (2016). Smart contracts: traiettoria di un'utopia divenuta attuabile, cit.

Among all features, the most significant innovation lies in the guaranteed execution of the contract. The program guarantees the correct execution of contractual obligations precisely because it is not subject to human manipulation¹²⁹. Once a command is sent to the hardware, the process cannot be stopped. For instance, if the programme receives the instruction “upon the occurrence of condition X, Y bitcoins must be transferred to Tizio's wallet,” no further objections can be raised to prevent the fulfilment of the obligation. In short, the programme enforces performance, making non-performance practically impossible.

3.1 Precursors to Smart Contracts.

The use of digital technologies to facilitate the execution of contracts is not, in fact, a new development¹³⁰. One example is the so-called *Electronic Data Interchange* (EDI) systems, which allow businesses to exchange commercial information electronically. Another example is online sales contracts concluded through digital means, where the negotiation is reduced to a simple click¹³¹. In these cases, although they offer notable simplifications in contract formation and some automation in the negotiation process, they merely consist of contracts concluded in a digital format and are therefore entirely comparable to contracts executed in writing. The only difference lies in the medium used to record the terms of the agreement. Contract execution is not automatic; it still depends on further actions by the parties, such as sending information from one computer to another or delivering the good to a courier who then completes the transaction.

Data oriented contracts and computable contracts. A different case applies to so-called data-oriented contracts and computable contracts, which more closely resemble the definition of smart contracts. Data-oriented contracts are agreements that can self-execute once the parties have entered the terms and conditions into the system. Computable contracts, on the other hand, are mechanisms that provide the processing system with the ability to automatically assess whether certain conditions comply with what is required under the contract¹³². These models, already used in algorithmic trading, involve some degree of automation in execution, making them predecessors of smart contracts. However, they cannot be fully assimilated to them, as human agents can always intervene to interrupt or reverse the process.

Ricardian contracts. Also worth mentioning are the so-called Ricardian contracts¹³³. A Ricardian contract is a digital document containing terms of an agreement. It is designed to function both as a traditional legal document and as a structured data file that can be read by computers. It is a design pattern in which the parties' intentions are

¹²⁹ Borgogno, O. (2018). Smart Contracts as the (new) Power of the Powerless? The Stakes for Consumers. *European Review of Private Law/Revue Européenne De Droit Privé/Europäische Zeitschrift Für Privatrecht*, 26(Issue 6), 885–902. <https://doi.org/10.54648/erpl2018060>

¹³⁰ Sarzana Di S. Ippolito, F., & Nicotra, M. (2018). *Diritto della Blockchain, Intelligenza artificiale e Iot*, cit.

¹³¹ Ibid.

¹³² Ibid.

¹³³ Grigg, I. (2004). The Ricardian contract. In *Proceedings. First IEEE International Workshop on Electronic Contracting* (pp. 25–31). <https://doi.org/10.1109/wec.2004.1319505>

defined, and the legal prose is converted into computer code, allowing the contract to be executed automatically by the program. The main advantage of a Ricardian contract is that it can be used in court if a disagreement arises between the parties¹³⁴. Unlike smart contracts, which are just lines of code that carry out instructions, a Ricardian contract is in fact an enforceable agreement, which also includes legal terms that can be enforced by a judge in case of disputes¹³⁵.

Despite representing a significant innovation in digital contracting, these models differ fundamentally from the one proposed by Szabo: in their case, execution can be interrupted or blocked beforehand¹³⁶. A true smart contract, once deployed, cannot be altered or stopped by external factors¹³⁷. It is therefore designed in a way that makes non-performance technically impossible¹³⁸.

3.2 Smart contract code and smart legal contract.

When it comes to defining smart contracts, two main approaches can be identified.

Smart contract code. A first group of definitions describes the concept from a purely technical perspective. In this view, the term “smart contract” refers to a piece of code that automates business processes or negotiation between two or more parties. Some authors describe these systems as “*smart agents*” or “*software agents*”¹³⁹, acting as auxiliary actors in contractual operations. These smart contracts are often associated with blockchain-based protocols, as they are systems capable of transferring digital assets automatically according to predefined rules. This interpretation excludes the idea that smart contracts are a distinct type of legal agreement, framing them instead as simple executors of contractual clauses¹⁴⁰.

Smart legal contract. Other scholars, however, consider smart contracts to be legal contracts, that is, a specific form of agreement with legal force. These are contracts that rely on coded protocols to incorporate agreed-upon terms and ensure that performance takes place without breach¹⁴¹. In this sense, a smart contract can be described as an agreement that is partly or fully expressed and/or executed through software. The terms of the contract are written directly into the code, and the agreement

¹³⁴ <https://www.leewayhertz.com/all-about-ricardian-contracts/>

¹³⁵ Ibid.

¹³⁶ Sarzana Di S. Ippolito, F., & Nicotra, M. (2018). *Diritto della Blockchain, Intelligenza artificiale e Iot*, cit.

¹³⁷ Duke, A. (2019). What does the CISG have to say about smart contracts? A legal analysis. *Chicago Journal of International Law*, 20(1), 4. <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1755&context=cjil>

¹³⁸ Sarzana Di S. Ippolito, F., & Nicotra, M. (2018). *Diritto della Blockchain, Intelligenza artificiale e Iot*, cit.

¹³⁹ Cannarsa, M. (2018). Interpretation of contracts and smart contracts: smart interpretation or interpretation of smart contracts? *European Review of Private Law/Revue Européenne De Droit Privé/Europäische Zeitschrift Für Privatrecht*, 26(Issue 6), 773–785. <https://doi.org/10.54648/erpl2018054>

¹⁴⁰ Stark, J. (2016). Making Sense of Blockchain Smart Contracts. *CoinDesk*. <https://www.coindesk.com/making-sense-smart-contracts/>

¹⁴¹ Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law Innovation and Technology*, 9(2), 269–300. <https://doi.org/10.1080/17579961.2017.1378468>

itself exists within a digital environment. According to this view, the smart legal contract is a distinct legal category, characterised by a high degree of predetermined terms and an automated mechanism that verifies and enforces the conditions of the agreement. Once the conditions are met¹⁴², the system proceeds with performance as specified by the contract.

Focusing too much on the distinction between smart contract code and smart legal contract may lead to confusion. These two expressions should not be treated as separate concepts, but rather as closely related¹⁴³. Structurally, they are identical: both consist of coded instructions executed by software. The only difference lies in their legal effect. The *smart legal contract* is a binding legal act between parties, capable of generating legal obligations. However, in order to produce such effects, it must be implemented in code so that the contractual data can be collected and automatically executed. This structure is also found in *smart contract code*, which, although not legally binding on its own, is made of the same digital architecture and executes commands as programmed. In conclusion, smart contract code represents the structural foundation of a smart legal contract. Since both are built in the same way, the difference lies solely in the latter's ability to produce legal effects in the real world.

3.3 Smart contracts use cases. Examples.

It is now necessary to examine how smart contracts are used in practice. The U.S. Commodity Futures Trading Commission outlines several practical examples that help illustrate how smart contract works¹⁴⁴.

Self-executing insurance. The first example involves a so-called self-executing insurance contract. Imagine that someone purchases a pineapple plantation in Hawaii. Concerned that weather conditions might harm his business, the buyer - John - decides to purchase insurance from a company called "PineSafe," which offers policies managed through smart contracts. John accepts the terms and digitally signs the agreement. Once signed, the contract is saved and embedded in a blockchain. The arrangement works as follows: John pays a monthly premium to PineSafe via the blockchain platform. Upon receiving confirmation of payment, the system activates a daily weather-monitoring process. If the weather conditions defined in the contract as triggering an indemnity are detected, the system automatically transfers the compensation to John's account.

Transportation Rental. The second example involves a bike rental service within a city. The service is managed by a company called RentCo, which has installed bike stations across the urban area. Users can access the service by registering through a dedicated app. After entering their personal details and credit card information, users can rent a bike. They go to a rental point, submit a command, and the system unlocks

¹⁴² Stark, J. (2016). Making Sense of Blockchain Smart Contracts, cit.

¹⁴³ SDA & Linklaters. (2017). *Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective*. <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>

¹⁴⁴ Commodity Futures Trading Commission, A Primer on Smart Contracts (2018), https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf

a bike for use. The software then tracks the user's movements and distance travelled to calculate the amount owed. When the bike is returned to any rental station, the smart contract locks it and transfers the due payment to RentCo. Here too, the entire process is recorded on a blockchain, which logs the journey data, payments, refunds, and applicable transport taxes. The system may also rely on an oracle connected to each bike, capable of reporting the user's speed or notifying the system in case of an accident. The blockchain is accessible to all parties involved, ensuring full visibility over how the contract is executed.

Credit default swap. The final example provided by the American authority concerns the use of smart contracts in financial services. It considers a case where a bank enters a credit default swap (CDS) with a company - Company X - to hedge against the risk of customer default. A CDS is a type of insurance contract in which credit risk is transferred from the creditor to a third party (the protection seller or swap dealer) in exchange for periodic payments. In this scenario, the bank holds claims on multiple clients. To protect itself from possible losses (e.g. client's bankruptcy) the bank pays a recurring fee to Company X, which in turn assumes the risk. If one of the bank's clients' defaults, Company X must pay the bank the amount owed by the defaulting customer. In this case, the smart contract manages the relationship: every three months, it calculates the premium and transfers it from the bank's account to Company X. A dedicated oracle constantly monitors the clients' credit status. If it detects a default, the oracle reports the event to the smart contract, which then calculates the indemnity and transfers the corresponding sum to the insured bank. Essentially, the smart contract automates the payment process and ensures immediate protection in the event of default.

The examples above clearly show that a thoughtful application of computer technology to contracting practices can overcome many traditional obstacles. The use of automated and standardised procedures not only results in significant savings in terms of time and cost, but also ensures a high level of accuracy in the execution of contractual obligations. Fulfilment is no longer subject to delays caused by human behaviour, as performance is guaranteed by the system's automatic operation.

The U.S. Commodity Futures Trading Commission (CFTC) highlights that the integration of blockchain technology adds an extra layer of certainty to smart contracts. At the moment of the execution, the blockchain nodes verify the necessary requirements and then proceed with authentication¹⁴⁵, following the procedures described in the first part of this work. The use of cryptographic techniques ensures that the integrity of the algorithm cannot be compromised in any way: the system does not allow modifications or interruptions and will carry out the predetermined actions.

Same as Bitcoin transactions, the execution of the operation will result in an update to the blockchain state, which means the addition of a new block to the chain. Once the process is successfully completed, proof of the transaction will be publicly recorded on the platform and accessible to anyone, without the possibility of altering the content of the ledger. Thanks to decentralisation, a copy of the contract is distributed across

¹⁴⁵ Attico, N. (2018). *Blockchain. Guida all'ecosistema. Tecnologia, business, società*, cit.

all network nodes. This broad dissemination makes it nearly impossible to alter the contract without mutual agreement, as every node holds a record of the original terms. It is no coincidence that blockchain is widely recognised as a breakthrough in the development of smart contract technologies¹⁴⁶.

3.4 Initial Coin Offerings (ICOs) and Decentralised Autonomous Organisations (DAOs).

Blockchain technology has also had a notable impact on funding mechanisms.

Initial Coin Offerings. One example is the Initial Coin Offering (ICO), a financing tool for entrepreneurial initiatives that originated on the Ethereum platform. The primary purpose of ICOs is to raise funds for the development of a specific project. The capital is gathered through a public sale of cryptocurrencies in exchange for rights linked to the investment¹⁴⁷. In most cases, these are projects that will only become operational once the necessary funds have been secured¹⁴⁸.

Individuals looking to launch a new business can use a smart contract to collect investments from potentially anyone active on the Ethereum network¹⁴⁹. One of the main features of ICOs is indeed their openness to an indefinite number of investors. After making a cryptocurrency contribution, the investor receives a token from the smart contract that represents their investment. This token may either entitle the holder to use a service offered by the issuing company (utility tokens) or represent a share in the company itself (security tokens)¹⁵⁰.

This tool marks a significant innovation in the financial sector, as it allows startups and small or medium-sized enterprises to raise capital on a large scale¹⁵¹ without relying on financial intermediaries. Another novel aspect is the use of blockchain technology and smart contracts, which respectively enable disintermediation of the investment process and automation of its procedures.

*Decentralized Autonomous Organizations*¹⁵². Another financial application of smart contracts is found in Decentralized Autonomous Organizations (DAOs). DAOs are

¹⁴⁶ Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, 26, 377-40

¹⁴⁷ Sarzana Di S. Ippolito, F., & Nicotra, M. (2018). *Diritto della Blockchain, Intelligenza artificiale e IoT*, cit.

¹⁴⁸ Consob. (2019). *Le offerte iniziali e gli scambi di cripto-attività*. https://www.consob.it/documents/1912911/1972122/doc_disc_20190319.pdf/2044537e-487c-5093-112e-3eacc69b12d4

¹⁴⁹ Attico, N. (2018). *Blockchain. Guida all'ecosistema. Tecnologia, business, società*, cit.

¹⁵⁰ Ibid.

¹⁵¹ Mignon, V. (2019). Blockchains - perspectives and challenges. In *Edward Elgar Publishing eBooks*. <https://doi.org/10.4337/9781788115131.00007>

¹⁵² Christopher, C. M. (2024). Recognizing DAOs as legal entities: Balancing public policy, innovation, and consistency. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5220994>

autonomous organizations built on blockchain technology that use decentralization as the core of their operational model.

Their structure is similar to that of ICOs, with one key difference: governance. Token holders not only own a stake in the organization but also participate in its decision-making processes. Although DAOs were originally conceived as an alternative to traditional corporate structures, token holders effectively exercise voting power proportionate to the number of tokens they hold¹⁵³. Despite this participatory element, DAOs operate autonomously, following the rules set forth in their founding protocol. These rules, concerning investments, transfers, or other decisions, are codified on the blockchain and automatically enforced via smart contracts once the required conditions are met.

It is important to emphasize that each operation still requires approval by token holders, who vote on its appropriateness before execution. In essence, when the organization is established, its operating rules are encoded and remain in force throughout the DAO's existence. These rules, including the specific actions to be performed, are embedded in a smart contract, which will execute them automatically once the required vote is cast and the necessary conditions are verified.

Interest in classifying Decentralised Autonomous Organisations (DAOs) grew after the so-called *TheDAO* case. In that episode, a breach of the digital address holding the organisation's funds led to losses of around 50 million US dollars. The incident was examined by the United States Securities and Exchange Commission (SEC), the federal authority responsible for supervising the securities market¹⁵⁴.

In particular, in order to determine whether the case fell within the scope of securities law, the SEC carried out an analysis of the legal nature of the phenomenon. The Commission concluded that the organisation's tokens qualified as financial instruments and that the transactions made on the platform amounted to investment contracts.

Under US law, an investment contract is an agreement involving the (1) *investment of money* in a common enterprise, with the (2) *reasonable expectation of profits* derived from the (3) *managerial or entrepreneurial efforts of others*¹⁵⁵. The assimilation of the DAO to this definition was explained as follows.

As to the *investment of money*, the Commission clarified that the investment does not have to be made in legal tender but may take other forms of value. The *reasonable expectation of profits* was also present, since participants expected to gain financially from their investment in the DAO and the purchase of tokens. It was therefore clear

¹⁵³ Ortolani, P. (2019). Decentralized Anonymous Organizations: inquadramento giuridico de jure condito e prospettive de jure condendo. In *Blockchain e Smart Contract*. Giuffrè.

¹⁵⁴ Securities and Exchange Commission. (2017). *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Release No. 81207). Retrieved March 3, 2025, from <https://www.sec.gov/files/litigation/investreport/34-81207.pdf>

¹⁵⁵ SEC v. Edwards, 540 U.S. 389, 393 (2004); SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946); see also United Housing Found., Inc. v. Forman, 421 U.S. 837, 852-53 (1975).

that the DAO operated as a profit-making entity, through which investors sought economic returns. The *entrepreneurial or managerial efforts of others* referred to the work of the founders and curators of the organisation. They selected the projects to be submitted to a vote and constantly monitored market trends and investors' positions¹⁵⁶.

Given the presence of the essential elements of an investment contract, the SEC concluded that the transactions were subject to securities law. Consequently, the entity issuing the tokens should have registered all offers and sales of financial instruments: something that did not occur. Likewise, entities providing exchange services for financial instruments are required to register with the Securities Commission. According to the SEC, these rules are designed to provide investors with adequate protection, including access to the information needed to make informed decisions. Such obligations apply regardless of whether the issuer is a traditional company or a decentralised autonomous organisation, whether the instruments are purchased in US dollars or virtual currencies, and whether they are issued in certificated form or through distributed ledger technology.

4. Conclusions.

Blockchain technology represents a diverse and constantly evolving ecosystem. Over the years, it has expanded far beyond its original function as a digital ledger for recording transactions. It is no longer only a register of transactions but a model with wide potential for innovation.

From the first blockchain, created to support Bitcoin transactions, the technology has developed into more complex structures such as Blockchain 2.0, which introduced smart contracts: programmable codes capable of automatically executing transactions when specific conditions are met. These advances have transformed blockchain into a broader infrastructure for digital interaction, capable of supporting entire economic and contractual systems.

However, alongside its potential, blockchain also presents specific risks for consumers that must be carefully considered.

First, the technical complexity of the system is significant. Each blockchain can have a different structure and level of security. The choice of consensus algorithm also affects performance and energy use. For example, systems based on Proof of Work require high energy consumption, while Proof of Stake models are more sustainable but rely on different validation rules. Understanding these mechanisms is essential to assessing the reliability of the network being used.

¹⁵⁶ Although investors contributed to the creation of the enterprise, this did not mean that they possessed any significant managerial power over it. While token holders had voting rights, such rights were limited and largely superficial: participants in the DAO could only express their opinion, by way of voting, on proposals formulated by the co-founders. Thus, rather than genuinely distributed management, it would be more accurate to speak of limited decision-making power, as ultimate control remained with the co-founding company *Slock.it*.

Second, cryptocurrencies do not all share the same level of stability. Some, such as stablecoins, are linked to a reference value like a fiat currency. Others fluctuate according to market demand. Users must therefore understand what kind of asset they are dealing with before making a transaction or investment. Price volatility can expose them to significant financial losses.

Third, there are different types of tokens, each associated with distinct rights and obligations. Tokens vary in function and legal meaning. Payment tokens, utility tokens, security tokens, and governance tokens all give different rights and duties. Knowing what type of token one owns is essential to understand one's position within the system, and any related responsibilities or risks.

Finally, the rise of crowdfunding and investment initiatives, such as Initial Coin Offerings (ICOs) and Decentralised Autonomous Organisations (DAOs), introduces additional layers of risk. These instruments often lack transparency, and participants may not fully understand the projects or entities they are funding. The absence of intermediaries and the technical nature of the platforms can make it difficult to identify fraud or evaluate the credibility of the initiatives.

This first chapter has therefore provided an overview of the main components of the blockchain ecosystem, highlighting both its technological complexity and the depth of knowledge required to interact safely with it. Understanding how blockchain works is the foundation for recognising where vulnerabilities may arise and how legal frameworks can be designed to address them.

Chapter 2 – Decentralised Finance Ecosystem

0. Introduction. - **1.** Fintech. A literature review. - **1.1** Evolution. – **1.2** Applications of fintech. Examples. - **2.** Decentralised Finance (DeFi) - **2.1** Definitions. A literature review. - **2.2** Origins of DeFi. Decentralised Finance (DeFi) and Traditional Finance (TradFi). - **2.3** Features and key concepts. - **2.4** Use cases. – **3.** Conclusions.

0. Introduction.

Blockchain technology has evolved considerably since the invention of Bitcoin. One of the areas where this evolution has shown the greatest progress in terms of adoption and development is finance. The emergence of new forms of economic value on the web has created a genuine financial market that runs parallel to the traditional one. In particular, there has been a steady growth in both exchange platforms and service providers, as well as in the variety of crypto-assets available. This ecosystem has attracted, and continues to attract, a large number of investors, many of whom are inexperienced.

This chapter, following a similar structure to the previous one, aims to analyse the current state of decentralised finance and to clarify the meaning of so-called Decentralised Finance (DeFi). In continuity with Chapter 1, it translates the technical concepts of blockchain and crypto-assets into the functional context of financial operations, thereby advancing the thesis's progression from technology to market practice. DeFi represents a new and rapidly expanding sector that has not yet been specifically regulated and therefore still shows uncertain boundaries. The chapter seeks to review the existing literature to understand what decentralised finance actually is and how it differs from traditional finance. Alongside the theoretical definitions found in academic and institutional sources, practical use cases will be presented to illustrate how decentralised finance can complement or even replace traditional banking and financial services.

The analysis follows a qualitative and descriptive approach, drawing on both academic studies and institutional reports, and other international bodies. The aim is to offer a comprehensive yet accessible overview of fintech and DeFi suitable for readers from both legal and non-technical backgrounds.

The objective is to clarify the contours of this emerging category and to highlight its developments and use cases. By doing so, the chapter prepares the analytical ground for Chapter 3, where the focus will shift from the definition of DeFi to the concrete risks and vulnerabilities that such a system entails for consumers.

Furthermore, this analysis serves as a foundation for understanding the risks faced by consumers when engaging with decentralised financial platforms.

1. Fintech. A literature review.

The financial market has undergone significant changes with the evolution of technology. Even if there is no common definition of fintech¹⁵⁷, interpreters refer to it to encompass a broad spectrum of services for businesses and private individuals, such as banking, financial, and insurance facilities¹⁵⁸. In other words, Fintech is ‘a new financial industry that applies technology to improve financial activities’¹⁵⁹ or, simpler, ‘financial innovation realised by information technology (IT)’¹⁶⁰

The term is a merger of the words *finance* and *technology*, indicating the application of technology to provide financial solutions. The primary feature of this design model is the implementation of information technology (IT), utilised to enhance monetary transactions and financial risk management. In most cases, these financial products and services are developed by start-up companies.

Schueffel (2018), Giglio (2016), and other authors conducted a literature review on the definition of fintech. The result is that interpreters refer to the term fintech with a different meaning. For instance, some authors refer to fintech as a new emerging sector of the financial industry¹⁶¹. Others define fintech as the technology¹⁶² used to implement the financial sector and as a new business model¹⁶³. In any case, all the definition refers to a phenomenon involving the usage of information technologies for financial purposes and the provision of products and services based on such technologies.

The principal definitions reconnect fintech in the following categories:

Fintech as a financial service model. Arner et al. (2015) define fintech as ‘technology-enabled financial solutions’, comprehending all the services, products and solutions

¹⁵⁷ Schueffel, P. (2017). Taming the Beast: A scientific definition of Fintech. *Journal of Innovation Management*, 4(4), 32–54. https://doi.org/10.24840/2183-0606_004.004_0004

¹⁵⁸ Ibid., Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, 59(1), 69–76. <https://doi.org/10.1007/s12599-017-0464-6>, Ratecka, P. (2020). Zjawisko FinTech – ujęcie definicyjne, taksonomiczne oraz historyczne. *Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej W Tarnowie*, 45(1), 53–67. <https://doi.org/10.25944/znmwse.2020.01.5367>, Giglio, F. (2021). Fintech: a Literature Review. *EUROPEAN RESEARCH STUDIES JOURNAL*, XXIV(Issue 2B), 600–627. <https://doi.org/10.35808/ersj/2254>

¹⁵⁹ Schueffel, P. (2016). Taming the beast: A scientific definition of fintech., cit.

¹⁶⁰ Takeda, A., & Ito, Y. (2021). A review of FinTech research. *International Journal of Technology Management*, 86(1), 67–88. <https://doi.org/10.1504/ijtm.2021.115761>

¹⁶¹ Micu, I., & Micu, A. (2016). Financial Technology (Fintech) and its implementation on the Romanian non-banking capital market. *SEA - Practical Application of Science*, 11, 379–384. <https://doaj.org/article/450238100bd1405fb401a1eafd533fac>; Shim, Y., & Shin, D. H. (2016). Analyzing China’s fintech industry from the perspective of actor–network theory. *Telecommunications Policy*, 40(2–3), 168–181. <https://doi.org/10.1016/j.telpol.2015.11.005>

¹⁶² Bettinger, A. (1972). FINTECH: A Series of 40 Time Shared Models Used at Manufacturers Hanover Trust Company. *Interfaces*, 2(4), 62–63.

¹⁶³ Maier, E. (2016). Supply and demand on crowdlending platforms: connecting small and medium-sized enterprise borrowers and consumer investors. *Journal of Retailing and Consumer Services*, 33, 143–153. <https://doi.org/10.1016/j.jretconser.2016.08.004>

related to the financial services industry¹⁶⁴. Other authors¹⁶⁵ affirm that fintech is a new financial sector where technology is used to facilitate the provision of services, trades, insurance products, but also risk management and authentication services. Kim et al. (2016) refer to fintech as a service sector ‘which uses mobile-centred IT technology to enhance the efficiency of the financial system’¹⁶⁶.

Fintech as technology. Other definitions emphasise the technological nature of fintech. Fintech is, moreover, a synthesis of the words financial and technology¹⁶⁷, and the Oxford dictionary defines it as ‘computer programs and other technology used to provide banking and financial services’¹⁶⁸. According to Barberis (2014), ‘the term refers to the application of technology within the financial industry’¹⁶⁹. Similarly, Lončarski (2016) relates fintech to the evolution of technology in the financial business sector¹⁷⁰.

Fintech as an industry. Another meaning provided for the term fintech is the one referring to a new industry involving the usage of technologies for financial purposes and to make them more efficient¹⁷¹. For instance, McAuley (2015) defines fintech as ‘an economic industry composed of companies that use technology to make financial systems more efficient’¹⁷².

Fintech as a business model. Fintech weekly (2016) defines fintech as ‘a business that aims at providing financial services by making use of software and modern technology’¹⁷³. Ernst & Young (2016) referred to the development of the financial services as the result of ‘organisations combining innovative business models and technology’¹⁷⁴.

From this analysis, it becomes clear that fintech is a broad concept encompassing multiple sectors. Firstly, fintech refers to the application of technology in the financial

¹⁶⁴ Arner, D. W., Barberis, J. N., & Buckley, R. P. (2015). The evolution of Fintech: a new Post-Crisis paradigm? *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2676553>

¹⁶⁵ Micu, I., & Micu, A. (2016). Financial Technology (Fintech) And Its Implementation On The Romanian Non-Banking Capital Market, cit.; Shim, Y., & Shin, D.-H. (2016). Analyzing China’s Fintech Industry from the Perspective of Actor–Network Theory, cit.

¹⁶⁶ Kim, Y., Choi, J., Park, Y. J., & Yeon, J. (2016). The adoption of mobile payment services for “Fintech”. *International Journal of Applied Engineering Research*, 11(2), 1058-1061. <http://scholarworks.bwise.kr/ssu/handle/2018.sw.ssu/34412>

¹⁶⁷ Bettinger, A. (1972). FINTECH: A Series of 40 Time Shared Models Used at Manufacturers Hanover Trust Company, cit.

¹⁶⁸ <https://www.oxfordlearnersdictionaries.com/definition/english/fintech>

¹⁶⁹ Barberis, J. (2014). *The rise of Fintech*, in https://thefintechbook.com/media/uploads/resources/reports/fintech.hk/2015/07/14/05_30_48/The%20Rise%20of%20FinTech%20-%20Nov%20-14.pdf

¹⁷⁰ Lončarski, I. (2016). Risk Management (2016). *Risk Management*, 18(1), 1-3. <https://doi.org/10.1057/rm.2016.2>

¹⁷¹ Čižinská, R., Krabec, T., & Venegas, P. (2016). FieldsRank: the network value of the firm. *International Advances in Economic Research*, 22(4), 461–463. <https://doi.org/10.1007/s11294-016-9604-x>

¹⁷² Giglio, F. (2021). Fintech: A literature review, cit.

¹⁷³ <https://www.fintechweekly.com/fintech-definition>

¹⁷⁴ <https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2019/09/ey-global-fintech-adoption-index.pdf>

and banking sectors. The usage of IT for improving financial and banking services, as will be seen in the following paragraph, is not a novelty but dates to the 19th Century. In the last decades, this implementation has increased due to the advancement occurred in the development of new technologies. In general, considering the peculiarity of services and products provided by fintech, it can be considered a new type of industry, entailing a new business sector.

1.1 Evolution.

According to Arner et al. (2015), the evolution of fintech can be divided into three phases¹⁷⁵.

Fintech 1.0 (1866-1967). The use of technology for financial purposes dates back to the 19th century. Technological instruments (e.g. the telegraph and railway networks) began to be used to facilitate the transmission of financial information. The peak of this early phase was reached after the First and Second World Wars, with the appearance of the first computers (e.g. code code-breaking tools developed by IBM and financial calculators provided by Texas Instruments) and credit cards from the 1950s onwards.

Fintech 2.0 (1967-2008). The second phase of fintech began with the introduction of the ATM in 1967 by Barclays and the shift from analogue to digital technology. The electronic payment system facilitated and speeded up financial flows. The establishment of the Inter-Computer Bureau in 1968 of the Society of Worldwide Interbank Financial Telecommunications (SWIFT) in 1973 was significant. Another significant moment in this phase was the introduction of the NASDAQ (National Association of Securities Dealers Automated Quotations) index in 1971, which enabled the transition to a modern, no longer physical system of selling and buying securities. NASDAQ is an electronic stock exchange founded in the United States in 1971, which revolutionised the way financial securities are traded. With NASDAQ, a digital and automated trading system was gradually introduced, reducing the transaction costs of physical trading. The creation of the Bloomberg terminal was also an important point. The Bloomberg terminal (or Bloomberg Terminal) is a professional computer system, developed in the early 1980s by Michael Bloomberg, which provides real-time access to a huge range of financial data, economic news, analytical tools and trading functions. The terminal led to a centralisation and digitisation of financial information, integrating a professional platform capable of providing a considerable amount of information to investment banks, hedge funds, asset managers, listed companies, analysts, etc.

At this stage, there is an increasing focus by regulators on financial affairs, especially with regard to international trade.

The latest turning point came with the introduction of the internet in the 1990s and the establishment of home banking services. The early 2000s then saw the creation of the

¹⁷⁵ Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm, cit.. See also Giglio, F. (2021). Fintech: A literature review., cit.

first online banks, which had no physical branches. The process of digitisation of banking and financial services is now complete.

Fintech 3.0 (2008-current). The emergence of fintech 3.0 stems in part from the 2008¹⁷⁶ financial crisis and, in particular, the decline in individuals' trust in banks, as well as the emergence of a new working class resulting from the massive layoffs that occurred during the financial crisis period. The regulatory approach that was developed in the aftermath of the crisis, in fact, introduced severe limitations to banks' operations, effectively reducing their competitiveness. The main feature of fintech 3.0 is the continuous acceleration in the development of technology. A new paradigm is thus beginning to emerge whereby the provision of financial services is not the sole prerogative of banks and institutions. The creation of numerous start-ups to provide financial solutions in place of banks is certainly one of the reasons for the advancement of financial technologies. In addition, banks have also been continuously upgrading their systems by implementing technology to provide services¹⁷⁷. Precisely within the context of fintech 3.0, crypto assets have developed. On the other hand, the massive post-crisis redundancies meant that nearly 9 million workers needed to redeploy their skills acquired in the financial sector, effectively redeploying them in what would become fintech 3.0.

Decisive was therefore the policy choice made in several countries to tackle the economic crisis and foster post-crisis economic recovery. For example, the JOBS Act adopted in the US in 2012 took measures to promote financing for small and medium-sized emerging companies in order to revive the economy. In particular, companies were also allowed to find financing outside traditional channels, being able to use P2P platforms to raise funds. The financing of start-ups, therefore, constituted the springboard for the development of all those enterprises that would later develop the financial models of fintech 3.0.

1.2 Applications of fintech. Examples.

As anticipated, fintech affects many sectors of the financial and banking industry. For this reason, some authors (see the paragraph on definitions) refer to fintech as a new industry, encompassing specific products. According to literature¹⁷⁸, the main areas affected are:

Crowdfunding. One of the most interesting areas of fintech is that of so-called crowdfunding and, more generally, of raising resources through publicly accessible platforms. As mentioned in the previous chapter, P2P networks and, specifically, DAOs and ICOs make it easy to raise capital without the excessive use of capital and

¹⁷⁶ Ibid. (Arner).

¹⁷⁷ Jalal, A., Mubarak, M. A., & Durani, F. (2023). Financial Technology (Fintech). In *Artificial Intelligence and Transforming Digital Marketing* (Vol. 487, pp. 525–536). Studies in Systems, Decision and Control, Springer. https://doi.org/10.1007/978-3-031-35828-9_45

¹⁷⁸ Giglio, F. (2021), Fintech: A literature review, cit.

without the need for banks¹⁷⁹. Decentralisation has, in fact, made it possible to flexibilise and speed up the use of credit.

Investment management. One area affected by fintech is investment service management. One example is high-frequency trading and algorithmic trading. Algorithmic trading is a computerised trading system managed by software using an algorithm. It is therefore an instrument capable of making market decisions on the basis of impulses from calculations made by algorithms¹⁸⁰. These algorithms are, in fact, able to take in all the information relating to market trends and then determine accordingly the behaviour to be adopted when trading and exchanging securities¹⁸¹. High-frequency trading, on the other hand, is a particular automated market strategy which uses machines capable of analysing market information and quickly proceeding to countless buy or sell orders, and then possibly cancelling or confirming them on the basis of information that arrives in the same time frame¹⁸². The system's strong point is the computers' ability to act at very high speed: they are able to acquire market information quickly and constantly, allowing them to adapt their conduct to even the slightest fluctuations in market trends¹⁸³. Other phenomena worth mentioning are copy trading and robo-advising¹⁸⁴. In copy trading, successful traders make their strategies and investments available in exchange for a sum of money. The term robo-advising refers to the financial planning and investment coaching service that is provided by an algorithm¹⁸⁵. Through a series of questions regarding the investor's financial status and objectives, the robo-advisor makes its suggestions. These financial management techniques certainly allow greater access and democratisation of the financial markets. Indeed, the absence of physical intermediation allows greater access to resources by investors.

Payments. The payment system has undergone major evolutions thanks to the development first of credit cards and then of the internet and home banking systems. One thinks, for example, of contactless payments developed in recent years. In general, the payment sector underwent a major development with the introduction of debit and credit cards in the 20th century. The introduction of dematerialised payment

¹⁷⁹ Vives, X. (2017). The impact of FinTech on banking. *European Economy*, (2), 97-105, https://blog.iese.edu/xvives/files/2018/02/EE_2.2017.pdf#page=99

¹⁸⁰ Puorro, A. (2013). High frequency trading: una panoramica (High frequency trading: an overview). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2369311>. The Author defines Algorithmic Trading as a trading method whose parameters are determined by a specific set of rules aimed at automating investment decisions, thereby eliminating emotional and behavioural components. Trading algorithms typically specify the timing, price, quantity, and routine of orders, while continuously monitoring market conditions.

¹⁸¹ Shorter, G., & Miller, R. S. (2014). *High-Frequency Trading: background, concerns, and regulatory developments*. https://digital.library.unt.edu/ark:/67531/metadc332977/m1/1/high_res_d/R43608_2014Jun19.pdf

¹⁸² A. Massey, (2014), *High-Frequency Trading: Elements, Considerations, Perspectives*. (Trade Issues, Policies and Laws), Hauppauge: Nova Science Publishers.

¹⁸³ Di Ciommo, F. (2019). Smart contract e (non-)diritto: il caso dei mercati finanziari. *Nuovo Diritto Civile*, 1, 257–295. <https://www.diciommoandpartners.com/wp-content/uploads/2020/09/Smart-contract-x-Nuovo-dir-civ..pdf>

¹⁸⁴ Thakor, A. V. (2020). Fintech and banking: What do we know?. *Journal of financial intermediation*, 41, 100833. <https://doi.org/10.1016/j.jfi.2019.100833>

¹⁸⁵ <https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp>

instruments has, in fact, enabled a streamlining of payment transactions and the implementation of international and cross-border payments, also thanks to the introduction of international payment circuits (e.g. SEPA circuit). While companies such as Visa or Mastercard continue to lead the sector, the development of PayPal or the payment systems Google Pay or Apple Pay is undoubtedly a scenario destined to expand¹⁸⁶. In the last decade, the provision of payment systems is in fact no longer the prerogative of banks. Indeed, these payment systems make it possible to facilitate transactions through immediate payments, as well as to exchange money without the need to have an account. In this context, the introduction of Bitcoin represented a disruptive innovation in the payments sector. Bitcoin and crypto assets in general allow investors to make use of an innovative payment instrument (see Chapter 1), which does not need to be guaranteed by central authorities

Credit and deposit. An example of a fintech application is P2P lending, that is, when money is lent online through a service that allows supply and demand to meet without intermediaries. The increase in the use of such services dates back to the period of the financial crisis and has grown exponentially to reach the sum of USD 300 billion in 2022¹⁸⁷. The lending process begins with the borrower submitting a loan application through an online platform. The platform conducts an initial credit assessment and assigns a grade, indicating the borrower's credit risk¹⁸⁸. Once the listing is published, individual investors indicate the amount they are willing to lend and the interest rate they expect in return. The platform then selects qualifying bids and aggregates them into a single loan that is disbursed to the borrower. A feature of this model is that the platform itself does not provide any funding. Unlike traditional banks (which finance loans using a mix of deposits, subordinated debt, and their own equity capital) P2P platforms operate without committing their own financial resources. As a result, the funds used to finance loans come entirely from external investors and can therefore be viewed as a form of investor equity. In this sense, P2P lending is described as “non-intermediated finance” because there is no financial intermediary assuming risk or engaging in qualitative asset transformation by using its own balance sheet¹⁸⁹.

Shadow banking system. Another phenomenon that has found its way into the legal system thanks to the development of financial technologies is the shadow banking system. The term shadow banking refers to the set of markets, institutions and intermediaries that provide banking services without being subject to the relevant regulation because they are outside the perimeter of application of the relevant rules¹⁹⁰. This phenomenon has been made possible by the development of new technologies capable of outsourcing banking services, taking them outside the regulatory perimeter through structured investment vehicles (SIVs). Shadow banks are characterised by high leverage. They lend more money than they have in their reserves. Increased

¹⁸⁶ Vives, X. (2017). The impact of FinTech on banking. *European Economy*, cit.

¹⁸⁷ Thakor, A. V. (2020). Fintech and banking: What do we know?, cit.

¹⁸⁸ Ibid.

¹⁸⁹ Ibid.

¹⁹⁰ <https://www.consob.it/web/investor-education/intermediazione-finanziaria-non-bancaria>

leverage means the possibility of a higher profit, but also a higher loss if the investment turns out to be unsuccessful.

Big data, risk management and compliance. The term “big data” refers to the process of examining large and varied amounts of data for analytical purposes. The analysis of big data enables the optimisation of choices by providing an overview of the content analysed from the collected data. Its application to fintech is very useful as it allows investors' preferences to be analysed in the first place and personalised solutions to be proposed based on their needs and budget¹⁹¹. Customer segmentation, i.e. the subdivision of customers into specific areas of interest, is an element that benefits the company, as it allows it to propose solutions that are more coherent and suited to its customers. Data analysis is also useful in order to prevent or detect fraud or risks to the company. Analysis of market trends is useful to prevent losses or unfavourable investment choices¹⁹². Similarly, asset monitoring allows the detection of fraudulent activities that could jeopardise the company. Finally, data analysis applied to fintech can be useful for compliance purposes with a regulation or company rules. The presence of numerous industry regulations requires careful compliance with current regulations (e.g. Anti-Money Laundering (AML) Regulation).

Insurance. Fintech has also found application in the insurance sector¹⁹³, especially in business-to-consumer (B2C) relationships¹⁹⁴. Technology has enabled the development of three trends: personalisation, connectivity and simplification. An example of such an application is pay-as-you-drive solutions in which the adjustment of car insurance premiums is connected to the readings made by a device in cars¹⁹⁵. These systems also enable the reconstruction of the accident dynamics through sensor readings. The investment in insurance systems is growing steadily, registering a market revenue of \$532.7 million for the year 2018¹⁹⁶.

Medical sector. Fintech applications also affect the medical sector¹⁹⁷. Fintech systems allow rationalisation in payment processes, enabling health insurance, financial plans for managing medical expenses and tailor-made payment methods. The use of P2P networks in the medical sector is also used for crowdfunding purposes. For instance, patients can share their stories and needs in order to find financial resources for their treatment or to borrow money. Crowdfunding is also used for the financing of

¹⁹¹ Koushal, A. (2024, August 7). *How Fintech and Big Data Analytics Work Together*. LinkedIn. Retrieved June 6, 2025, from <https://www.linkedin.com/pulse/how-fintech-big-data-analytics-work-together-anurag-koushal-8eync/>

¹⁹² Mhlanga D. (2024). The role of big data in financial technology toward financial inclusion. *Frontiers in big data*, 7, 1184444. <https://doi.org/10.3389/fdata.2024.1184444>.

¹⁹³ Thakor, A. V. (2020). Fintech and banking: What do we know?, cit.

¹⁹⁴ Puschmann, T. (2017), Fintech, cit.

¹⁹⁵ Puschmann, T. (2017), Fintech, cit.

¹⁹⁶ Thakor, A. V. (2020). Fintech and banking: What do we know?, cit.

¹⁹⁷ Das, A. S., Sumathy, M., & Nabeel K., M. (2024). Fintech Innovations In Medicine: Transforming Healthcare Through Financial Technology. *Research Explorer*, XII(42), 109–112. https://www.researchgate.net/publication/381887171_Fintech_Innovations_In_Medicine_Transforming_Healthcare_Through_Financial_Technology; Grassi, L., & Fantaccini, S. (2022). An overview of Fintech applications to solve the puzzle of health care funding: state-of-the-art in medical crowdfunding. *Financial Innovation*, 8(1). <https://doi.org/10.1186/s40854-022-00388-9>

scientific advancement studies in the medical field. This allows funders to be involved in the funding process from the very beginning, enabling higher returns in the long term. The use of technology for medical purposes has also made it possible to incorporate monitoring tools into portable devices (e.g. smartwatches). Insurance companies have begun to use this data to provide personalised plans to their clients and reward systems for those who adopt a healthier lifestyle.

2. Decentralised Finance (DeFi).

After the introduction of Bitcoin, the term Decentralised Finance (DeFi) was coined to define a new *species* of FinTech *genus*, characterised by a decentralised digital environment and the absence of intermediation¹⁹⁸. In particular, DeFi is a blockchain-based ecosystem that seeks to overcome the centralised approach of traditional finance¹⁹⁹ through decentralisation. It is a branch of crypto asset systems²⁰⁰.

DeFi application encompasses a wide range of financial services, configuring an alternative but interchangeable market. The services offered are approximately the same as traditional markets: payment, deposit, crowd-investing, and speculative trading. According to the systematic literature review of Meyer et al. (2022), the decentralised financial protocols are built with trustless smart contracts developed on permissionless and public blockchain²⁰¹.

The financial services operate in this ecosystem through automated procedures called smart contracts. Smart contracts – IT protocols that facilitate negotiations among affiliated parties²⁰² – enabled the implementation of complex financial services²⁰³. In particular, the term *smart contract* refers to a computer code capable of automating business processes or negotiations between two or more parties²⁰⁴. Some authors refer to this concept as *smart agents* or *software agents*²⁰⁵, indicating a form of subsidiary

¹⁹⁸ EUBlockchain Observatory and Forum. (2022). Decentralised Finance (DeFi). In <https://blockchain-observatory.ec.europa.eu>. https://blockchain-observatory.ec.europa.eu/publications/decentralised-finance_en?prefLang=sv

¹⁹⁹ De La Roche W., M., & Zichichi, M. (2023). Bringing clarity to the DeFi sector: A cross-sector proposal for a unified DeFi definition. In *IOTA Foundation*. https://files.iota.org/comms/Bringing_clarity_to_the_DeFi_sector.pdf

²⁰⁰ Roukny, T. (2022). *Decentralized finance: Information Frictions and Public Policies : Approaching the Regulation and Supervision of Decentralized Finance*. Publications Office of the European Union. <https://doi.org/10.2874/444494>

²⁰¹ Meyer, E., Welp, I. M., & Sandner, P. G. (2021). Decentralized Finance—A systematic literature review and research directions. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4016497>

²⁰² Capaccioli, S. (2016). Smart contracts: traiettoria di un'utopia divenuta attuabile. *Cyberspazio E Diritto* (Mucchi Editore), 17(55).

²⁰³ Meyer, E., Welp, I. M., & Sandner, P. G. (2021). Decentralized Finance—A systematic literature review and research directions, cit.

²⁰⁴ Madir, J. (2024). Smart contracts. In *Fintech* (pp. 244 - 267). <https://doi.org/10.4337/9781035314751.00020>

²⁰⁵ Cannarsa, M. (2018). Interpretation of contracts and smart contracts: smart interpretation or interpretation of smart contracts? *European Review of Private Law/Revue Européenne De Droit Privé/Europäische Zeitschrift Für Privatrecht*, 26(Issue 6), 773–785. <https://doi.org/10.54648/erpl2018054>

agents acting on behalf of legal subjects in contractual operations. Smart contracts are often associated with protocols operating on a blockchain, as they are specifically systems designed to automatically transfer digital assets based on pre-established conventional rules²⁰⁶.

DeFi constitutes a paradigm that allows the usage of blockchain, DLTs and smart contracts for the implementation of financial operations.

2.1 Definitions. A literature review.

Scholars have elaborated multiple definitions of decentralised finance.

Zetzsche et. Al (2020) refers to DeFi as neither a legal nor technical term. Decentralised finance encompasses the decentralised ‘*provision of financial services through a mix of infrastructure, markets, technology, methods, and applications*’²⁰⁷. Decentralisation refers to the dislocated provision of services by users enhanced by technology.

Shueffel (2021) defines DeFi as a new paradigm impacting the creation, distribution and use of financial services, making the action of centralised bodies unnecessary. The technologies at the base of DeFi are automation of processes and blockchain²⁰⁸.

Jensen et al. (2021) refer to DeFi applications as ‘*a new type of open financial applications deployed on publicly accessible, permissionless blockchains*’ and composed as smart contracts²⁰⁹.

Chen and Bellavitis (2020) define DeFi as a financial paradigm connected to blockchain, whose main characteristics are decentralisation and disintermediation. DeFi is still in its early stages and has great potential for creating new business models and financial inclusion²¹⁰

These initial definitions illustrate how the term 'decentralised finance' refers to a specific sector of fintech that employs decentralised models, including blockchain, and aims to eliminate intermediaries while promoting greater financial inclusion.

²⁰⁶ Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law Innovation and Technology*, 9(2), 269–300. <https://doi.org/10.1080/17579961.2017.1378468>. Such a definition excludes the possibility of considering smart contracts as a distinct type of contract, instead identifying them as simple executors of clauses (the so-called smart contract code).

²⁰⁷ Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance (DEFI). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3539194>

²⁰⁸ Schueffel, P. (2021). Defi: Decentralized finance-an introduction and overview, cit.

²⁰⁹ Jensen, J., Von Wachter, V., & Ross, O. (2021). An introduction to Decentralized Finance (DEFI). *Complex Systems Informatics and Modeling Quarterly*, 26, 46–54. <https://doi.org/10.7250/csimq.2021-26.03>

²¹⁰ Chen, Y., & Bellavitis, C. (2019). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13, e00151. <https://doi.org/10.1016/j.jbvi.2019.e00151>

However, finding a universal definition is not simple. Notable works that simplify and rationalise the existing literature include studies by Meyer et al. (2022) and the Iota Foundation (2023).

Meyer et al. (2022) have conducted a literature review of 83 articles. The review, by identifying the definition of decentralised finance, divides the articles into three categories: 1) micro-level, 2) meso-level and 3) macro-level. The articles in the micro-level category analyse the components that characterise DeFi. Within the macro level, three subcategories are identified: 1.1) financial smart contract research, 1.2) financial tokens in DeFi, and 1.3) DeFi applications (so-called DeFi Dapps). The meso-level category includes studies aimed at describing the different configurations that DeFi can assume. Two subcategories are identified: 2.1) DeFi single-chain ecosystem insights and 2.2) scaling beyond stand-alone DeFi ecosystems. The first category includes empirical studies on DeFi platforms, while the second focuses on possible interconnections between blockchain systems. The macro-level category follows a holistic approach and collects articles that study the DeFi phenomenon as a whole. Two subcategories are identified: 3.1) research on the DeFi space as a whole and 3.2) DeFi in the broader societal context. The first subcategory focuses on the characteristics of the DeFi ecosystem and, in particular, on risks, opportunities and case studies. The second subcategory collects papers that study the impact of DeFi on society and the financial system, as well as the necessary legal measures to be taken.

Based on the review, they concluded that DeFi is essentially a financial protocol built using smart contracts, trustless, and developed on public and permissionless blockchains.

This initial definition already reveals some essential elements that must be present: (1) it is based on a smart contract, (2) there are no intermediaries or central entities that confer trust on the operation, and (3) the blockchain is configured as permissionless and public²¹¹.

According to this interpretation, permissioned and private blockchains should be excluded from the scope of DeFi. They do not guarantee the accessibility and stability of the system. Private blockchain operators could change the rules of the blockchain or intervene in transactions. Similarly, in permissioned blockchains, access is limited to certain parties. The concept of DeFi is therefore limited to all those decentralised systems that ensure unrestricted accessibility and immutability of rules. The DeFi paradigm is therefore inspired by a logic of democratisation of financial processes and access to the operations provided by the blockchain.

The Iota Foundation also conducted a study on the definition of DeFi. The research aims to define the concept of decentralised finance²¹². The study begins with a literature review and provides an initial definition of DeFi.

²¹¹ Meyer, E., Welp, I. M., & Sandner, P. G. (2022). Decentralized finance—A systematic literature review and research directions, cit.

²¹² De La Roche W., M., & Zichichi, M. (2023). Bringing clarity to the DeFi sector: A cross-sector proposal for a unified DeFi definition, cit.

According to Iota's definition based on the literature review, DeFi is a financial system. It is decentralised and does not need intermediaries. It enables transparent transactions thanks to DLTs and smart contracts. Other features are: 1) provision of financial freedom, 2) trustless interaction, 3) user's self-reliant management of transactions, 4) absence of a centralised authority to enable transactions, and 5) decentralised governance.

Subsequently, the definition is reformulated based on an open survey of three different categories: (1) the crypto community, (2) industry professionals, and (3) investors and founders. The survey involved 183 individuals belonging to these categories and is based on questions designed to gauge their familiarity with these concepts.

The study revealed that both the crypto community and industry professionals refer to DeFi as a new financial system, while investors and founders primarily associate the concept with absolute financial freedom from a legal standpoint and, in general, individual autonomy, while still considering DeFi as a new financial system.

The definition was ultimately revised in light of the contributions of some legal scholars and is as follows. It can be divided into five parts:

'Decentralized Finance (DeFi) is based on blockchain technology and aims to create open-source financial building blocks. It refers to a paradigm that operates through the integration of various technologies with common characteristics, as opposed to operating as a cohesive unit like traditional financial systems.'

The first part represents the core of the definition and reconnects DeFi to blockchain. The definition, therefore, excludes other distributed ledger technologies from the scope of DeFi, including only blockchain-based technologies.

'At its core, DeFi embodies the principle of absolute financial freedom arising from absolute responsibility on the part of users. This causes it to extend beyond the boundaries of conventional financial systems, encompassing and influencing every economic activity in our lives.'

The second part expresses the main purpose of decentralised finance, namely to facilitate and promote the financial autonomy of individuals, both as individuals and with regard to any possible restrictions imposed by traditional financial systems.

'DeFi encompasses various activities managed without intermediaries, including but not limited to exchange, lending, and tokenization.'

The third part emphasises the suitability of DeFi to include more financial services and activities, providing an illustrative but non-exhaustive list.

'However, achieving a high level of DeFi often requires a balance between decentralization and security.'

The fourth part highlights the role of security in transactions and the need to balance it with decentralisation. Platform security is an essential requirement for the functioning of blockchain and, in general, DLTs. As analysed in the first chapter of this paper, security and the functioning of DLTs are fundamental concepts that influence each other. Security is guaranteed through consensus algorithms that aim to confer trust in the system. However, the consensus algorithm mechanism can sometimes compromise the speed of operations (e.g. Proof of Work), and vice versa.

‘DeFi can be viewed as both globally accessible and transnationally operated. It serves as a universal platform that transcends geographical boundaries, providing financial services to individuals worldwide. Simultaneously, it fosters collaboration and knowledge-sharing across different jurisdictions, enabling a decentralized financial ecosystem that connects participants from various countries. This dual perspective highlights DeFi’s aim to establish a borderless and interconnected financial landscape, unrestricted by traditional system limitations.’

The last part emphasises the transnational and global nature of DeFi. Its structure and characteristics enable the use of DeFi platforms and their services anywhere. Anyone can access a permissionless blockchain and carry out a transaction. Similarly, anyone can participate in blockchain governance to ensure its proper functioning.

Definitions have also been elaborated by institutional bodies, even if without legally binding provisions. It is worth noting that in these definitions, ‘blockchain’ is not mentioned as a fundamental requirement.

The European Central Bank defines decentralised finance as ‘*a novel way of providing financial services that cuts out traditional centralised intermediaries and relies on automated protocols instead*’²¹³. Participants join a P2P network where assets can be transferred automatically. The products and services exchanged or provided are usually the same of the traditional financial system. However, decentralised finance does not rely on centralised intermediaries. The main feature, according to this view, is its contraposition to traditional finance.

According to the European Securities and Markets Authority, decentralised finance ‘*seeks to provide financial services using blockchain or distributed ledger technologies in an open, decentralised and permissionless way*’ without involving traditional financial intermediaries²¹⁴. This implementation is possible thanks to the exploitation of blockchain technology and smart contracts.

A report of the Directorate-General for Financial Stability, Financial Services, and Capital Markets Union (DG FISMA) refers to DeFi in the following way

²¹³https://www.ecb.europa.eu/press/financial-stability-publications/macprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html.

²¹⁴ European Securities and Market Authority. (2023). *Decentralised Finance in the EU: Developments and risks* (No. ESMA50-2085271018–3349). ESMA Economics, Financial Stability and Risk Department. https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf

*‘Decentralized Finance (DeFi) relies on publicly distributed ledgers and automated digital (smart) contracts to provide financial services without requiring the presence of intermediary agents. As such it offers an alternative view to the traditional model of financial intermediation which grants central authorities privileged rights such as controlling access to markets, information and asset holding’*²¹⁵.

The UK government, in a consultation paper directed to provide a new regulation for financial technologies, defines DeFi as ‘an *umbrella term used to cover a range of financial services – including lending, exchange, asset management and insurance – which are offered without the use of traditional financial intermediaries*’. This implementation is possible thanks to the creation of smart contracts combined with the provision of decentralised apps (dApps)²¹⁶.

Banca d’Italia, the Italian central bank, defines DeFi as the market for the provision of financial instruments and services based on the use of smart contracts: computer programs or protocols that execute, manage, and document legally relevant actions and events on the blockchain, based on agreements between parties. The use of such contracts allows for the complete disintermediation of transactions, that is, the absence of centralised intermediaries such as brokerage firms, stock exchange companies or banks²¹⁷.

The National Bank of Slovakia (Národná banka Slovenska) refers to DeFi as a ‘*financial system built on distributed ledger technology, primarily blockchain, without the need for traditional financial intermediaries such as banks or securities dealers*’. This is possible thanks to smart contracts²¹⁸.

Banque de France, the national bank of France, adopts a similar definition, qualifying DeFi as ‘*a set of crypto assets that are similar to financial services and carried out without the intervention of an intermediary*’. It is based on the principle of decentralisation and makes it possible for relevant innovation in the field of contracts, such as automated clause execution tools²¹⁹.

Deutsche Bundesbank, the national German bank, refers to DeFi applications as instruments that provide financial services “*in combination with crypto tokens across distributed networks, replacing intermediaries such as banks, exchanges or insurers*”²²⁰. This provision of services is characterised by the use of blockchain

²¹⁵ Roukny, T. (2022). *Decentralized finance: Information Frictions and Public Policies*, cit.

²¹⁶ HM Treasury. (2023). *Future financial services regulatory regime for cryptoassets: Consultation and Call for Evidence*. https://assets.publishing.service.gov.uk/media/63d94ea68fa8f51881c99eb4/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf

²¹⁷ <https://www.bancaditalia.it/footer/glossario/index.html?letter=f>.

²¹⁸ <https://nbs.sk/en/financial-market-supervision1/fintech/financial-technology/what-is-decentralized-finance-defi/>.

²¹⁹ <https://acpr.banque-france.fr/en/publications-and-statistics/publications/decentralised-or-disintermediated-finance-what-regulatory-response>.

²²⁰ Deutsche Bundesbank (2021), *Crypto tokens and decentralised financial applications* (Monthly report),

technologies and consensus mechanisms that enable the replacement of trust in intermediaries and reduce the need for administrative intervention in the services offered.

A similar definition is adopted by the US Securities and Exchange Commission (SEC),

Efforts to provide a definition have also been made by other organisations. The International Association for Trusted Blockchain Applications (INTBA), in a proposal for DeFi regulation for the Securities and Exchange Commission (SEC), defines decentralised finance as a financial system built on blockchain technology. The authority recalls the Iota Foundation study and describes it as *‘automated, open-source, trust-less financial systems operating through decentralized, open-source protocols, built on top of decentralized, robust blockchains, and supported by transparent, open-source smart contract code, which executes deterministic operations once certain data fields and on-chain fees have been submitted by any and all wallet address’*²²¹.

The International Organisation of Security Commissions (IOSCO) specified that the term DeFi encompasses *‘financial products, services, arrangements, and activities that use distributed ledger or blockchain technologies (DLT), including self-executing code referred to as smart contracts’*²²².

This literature review reveals a strong interest in the phenomenon of decentralised finance. The fact that numerous state entities and international organisations have published reports and recommendations on the regulation of this new financial ecosystem is an indicator of the importance and spread of this phenomenon in recent times. It is no coincidence that there have been regulatory initiatives (e.g. UK) and the publication of guidelines.

Decentralised finance is a broad concept that encompasses numerous activities and services. Since this system is intended to complement traditional finance, it is necessary to understand its characteristics and functions in order to ensure the protection of the market and, above all, the consumer.

This initial analysis reveals that there are some recurring elements in the notion of decentralised finance. In some cases, reference is made to the concept of a “financial system”, while in others, direct reference is made to the activities provided and their specific characteristics. Certainly, the common elements that emerge are: the use of distributed ledger technologies, execution through smart contracts, the absence of intermediaries, and accessibility

<https://www.bundesbank.de/resource/blob/873132/74fc658db07569219ff74f4e4e55c36f/mL/2021-07-kryptotoken-data.pdf>.

²²¹ International Association for Trusted Blockchain Applications (2025), DeFi Self-Regulation: A Proposal for the Industry, <https://www.sec.gov/files/ctf-written-input-inatba-053025.pdf>.

²²² IOSCO (2023), Policy Recommendations for Decentralised Finance (DeFi), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf>.

2.2 Origins of DeFi. Decentralised Finance (DeFi) and Traditional Finance (TradFi).

To understand decentralised finance, it is useful to start with the concept of traditional finance (TradFi).

Finance can be defined as ‘*the application of economic principles that involves the allocation of money under conditions of uncertainty*’²²³. It encompasses the creation, management, and investment of funds, aiming to bring together borrowers and depositors²²⁴. Finance plays a fundamental role in the economy because it enables efficient investment of money and productivity of the economic system²²⁵.

The term traditional finance (TradFi) refers to the conventional approach that institutions, investors and consumers take to financial activities. The traditional financial system is based on reliance on authorised intermediaries and the presence of a centralised structure.

In traditional financial systems, the intermediary fulfils a fundamental function, acting as a conduit between investors and savers, thereby facilitating the matching of supply and demand and fostering the conversion of savings into productive investments. Precisely for this reason, in many legal systems intermediation is subject to duties of transparency and disclosure towards investors. The intermediary may be a bank or another entity providing financial services. It should nevertheless be specified that, at the European level, no harmonisation exists concerning the regulation of financial intermediaries other than banks, save for the case of entities subject to the control of EU credit institutions.

The establishment of intermediaries, therefore, entails a significant responsibility. In the European securities market, intermediaries must be authorised by central banks and are required to meet specific standards of soundness and reliability²²⁶.

Traditional finance, as previously noted, is also characterised by the presence of a centralised structure responsible for managing market rules and ensuring compliance. Within the European market, central banks fulfil this role, authorising activities and the exchange of financial instruments. The concept of centralisation also pertains to the ways in which the financial platform is managed, as a central entity oversees such a platform. In this context, reference is made to *centralised finance (CeFi)*. Even transactions carried out through distributed technologies - including blockchain - may

²²³ Drake, P. P., & Fabozzi, F. J. (2010). *The basics of finance: An introduction to financial markets, business finance, and portfolio management* (Vol. 192). John Wiley & Sons.

²²⁴ Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi--Comparing Centralized to Decentralized Finance. *arXiv preprint arXiv:2106.08157*.

²²⁵ Ibid.

²²⁶ Art. 5, Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (Mifid II) “Each Member State shall require that the provision of investment services and/or the performance of investment activities as a regular occupation or business on a professional basis be subject to prior authorisation in accordance with this Chapter. Such authorisation shall be granted by the home Member State competent authority designated in accordance with Article 67”.

nevertheless be centralised. Indeed, the majority of operations involving blockchain technology are, in practice, managed within a centralised system.

From a quantitative perspective, traditional finance constitutes the largest industry at the globally and accounts for the majority of economic transactions involving the exchange or purchase of financial assets²²⁷.

It should be noted that the term *TradFi* is mainly employed to highlight its limitations when compared to decentralised finance²²⁸. The services provided by traditional finance in fact constitute the starting point for the development of *DeFi* and for the enhancement of efficiency within the financial system. As outlined in the preceding paragraphs, decentralised finance pursues full accessibility and the disintermediation of markets, thereby making the purchase and exchange of financial products available to all. The creation of new financial dynamics and platforms designed to this end thus represents both a response to such limitations and, at the same time, a new investment opportunity.

Compared to TradFi, DeFi aims to achieve the following objectives:

1. the elimination of intermediaries;
2. the decentralisation of platform management;
3. the automation of protocols;
4. the enhancement of the efficiency of financial products and services offered.

A study conducted by the European Central Bank has summarised how the services provided by DeFi platforms operate compared to those offered within TradFi²²⁹.

²²⁷ International Association for Trusted Blockchain Applications (2025), *DeFi Self-Regulation: A Proposal for the Industry*, cit.

²²⁸ Ibid.

²²⁹ https://www.ecb.europa.eu/press/financial-stability-publications/macprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html.

Financial service	Decentralised finance	Traditional finance
Credit	Smart contracts facilitate lending and borrowing. Lenders post their crypto-assets into liquidity pools, from which borrowers borrow crypto-assets posting other crypto-assets as collateral. Interest rates are often determined automatically depending on the demand and supply of liquidity. Largest DeFi protocols: Compound, Aave	Banking
Trading	Decentralised exchanges (DEXes) facilitate the trading of crypto-assets by matching and executing trades through smart contracts without the involvement of a (centralised) third party. Trading often happens against a liquidity pool. Largest DeFi protocols: Uniswap, Curve	Brokers, stock exchanges, over-the-counter (OTC) markets
Payments	Peer-to-peer transfers of value are facilitated, either directly "on-chain" or via DeFi protocols that facilitate smaller value transfers off-chain, before reconciling them in batches back "on-chain". Largest DeFi protocols: Flexa, Sablier Finance	Cash, credit/debit cards, current accounts
Insurance	Customers of insurance DeFi protocols buy tokens in exchange for cover against specific digital asset-related risks, such as cyberattacks and theft. Token holders from within the protocol decide on insurance claims by voting yes/no on payouts. Largest DeFi protocols: Armor, Nexus Mutual	Lloyds of London insurance market, insurance firms
Investment (assets and derivatives)	Protocols replicating asset management functions where crypto-assets from users are automatically deposited in those protocols/pools with the highest yields based on preset risk tolerance. They also include protocols creating cryptoasset indices and those creating derivatives, including synthetic assets, options or perpetual futures. Largest DeFi protocols: Yearn Finance, dYdX	Investment funds, investment firms, investment banks

Figure 1 - Alexandra Born, Isabella Gschossmann, Alexander Hodbod, Claudia Lambert and Antonella Pellicani elaboration for ECB based on FSB (2022), Aramonte et al. (2021), IOSCO (2022) and largest protocols from DeFi Llama

The study examines how various financial and payment services operate within both traditional and decentralised finance. The comparison reveals that DeFi systems enable more immediate access to services and, more importantly, a direct involvement of the participants. Access to credit, traditionally provided by banks, is facilitated through the use of smart contracts, which automate buying and selling processes. In terms of trading, decentralised exchange systems streamline the matching of supply and demand. For both trading and credit, DeFi platforms utilise liquidity pools. These liquidity pools are collective funds that aggregate digital assets and enable their exchange through smart contracts, thereby eliminating the need for intermediaries²³⁰. The smart contract determines the token price based on an algorithm that responds to supply and demand dynamics. The platforms collect tokens and ensure the liquidity of exchanges through a reward system that compensates the individual who deposits the assets (liquidity provider).

Through DeFi implementations, traditional financial services are thus replicated, eliminating intermediaries and providing more accessible and efficient systems²³¹.

Decentralised finance originated with Ethereum, the platform that enabled the integration of smart contracts into the blockchain²³². Bitcoin had already introduced

²³⁰ <https://www.bitpanda.com/academy/it/lezioni/liquidity-pool-spiegati-in-modo-semplice/>

²³¹ https://www.ecb.europa.eu/press/financial-stability-publications/macprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html.

²³² Deutsche Bundesbank (2021), Crypto tokens and decentralised financial applications (Monthly report), cit.

the first online exchange of financial assets without intermediaries²³³. Ethereum and its smart contracts, however, opened the way to the development of tailored financial products and services, such as liquidity pools.

Regarding the total value locked (TVL), the exponential growth of DeFi began in 2021, rising from 15 billion US dollars in January to 175 billion US dollars in December. A decline occurred between 2022 and 2024, while from 2024 onwards the value of assets locked in DeFi started to grow again. In 2022, the collapse of the Terra platform triggered a contagion effect that caused a 40% drop in TVL²³⁴. From that moment, the value fluctuated between 40 and 50 billion dollars until 2024, when growth resumed.

Terra was a blockchain platform used for the exchange of algorithmic stablecoins. As mentioned earlier, a stablecoin differs from traditional cryptocurrencies in that it offers greater stability, since its value is pegged to a fiat currency. Terra's stablecoin (Terra USD or UST) was designed to maintain stability by being pegged to the cryptocurrency LUNA. Its value was kept stable through an algorithm-based reward mechanism. In May 2022, a series of imbalances triggered by a group of investors - at a time of high volatility and the planned launch of new platform functionalities²³⁵ - led investors to sell UST, causing the collapse of the algorithm underpinning its stability. From that moment, the price of both UST and LUNA collapsed.

As of August 2025, the total value locked (TVL) is approximately 150 billion US dollars. Ethereum accounts for 60.36% of the total, followed by Solana with 7.6%, Bitcoin with 4.97%, and other platforms comprising the remaining 27.07%. According to ESMA (2024), there are over 3.4 million DeFi users, and about 2800 DeFi protocols are active, though most are relatively small²³⁶. Moreover, the total value locked of DeFi constitutes 6% of the crypto market capitalisation²³⁷.

2.3 Features and key concepts.

The purpose of DeFi is to provide the same services as traditional finance, while offering the added benefits of transparency and a decentralised system. As previously noted²³⁸, the essential components of a DeFi system are:

- a distributed ledger technology or blockchain, depending on interpretation, that is permissionless and public;

²³³ Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi--Comparing Centralized to Decentralized Finance, cit.

²³⁴ European Securities and Market Authority (2023), *Decentralised Finance in the EU: Developments and risks*, cit.

²³⁵ <https://www.credem.it/content/credem/it/scopri-credem-banca/educazione-finanziaria/blog/panic-selling--il-caso-terra-luna.html>

²³⁶ European Securities and Market Authority (2023), *Decentralised Finance in the EU: Developments and risks*, cit.

²³⁷ Ibid.

²³⁸ Meyer, E., Welp, I. M., & Sandner, P. G. (2022). Decentralized finance—A systematic literature review and research directions, cit.

- the use of smart contracts for platform development and the execution of operations;
- the absence of intermediaries.

About structure, decentralised finance platforms are characterised by a multi-layered architecture, relying on several interrelated technological layers. Specifically, the following levels can be identified²³⁹:

- *Settlement layer*. The settlement layer corresponds to the permissionless blockchain. The settlement layer enables transactions and serves as the foundation for the protocol's operation.
- *Asset layer*. Developers can create crypto assets to be exchanged and used for different purposes. It encompasses native tokens, stablecoins and non-fungible tokens (NFTs)²⁴⁰.
- *Application layer*. Smart contract-enabled applications represent the application layer. These applications are further divided into three subgroups: crypto assets, DeFi protocols, and DeFi compositions. This layer encompasses all the possible use cases and applications of DeFi.
- *User-friendly layer*. The user-friendly layer provides an accessible interface enabling users to benefit from the services offered by the platform.

Concerning the functional characteristics that distinguish decentralised finance systems, these partly overlap with those of distributed ledger technologies. Other features, however, stem from their multi-layered structure. In particular, the following properties can be identified²⁴¹:

- *Universal access*. The permissionless configuration of blockchains and DLTs allows unrestricted access for anyone, both to use the services provided by the platform and to participate as validators or developers. The possibility for developers to build projects on top of existing platforms without the need for licensing represents a significant innovation compared to traditional finance.
- *Transparency*. All transactions executed on the blockchain are publicly visible, as the transaction ledger is open and accessible. At the same time, the identities of the parties remain pseudonymous: observers can view the transaction but cannot directly link it to its actual author, seeing only the numerical code corresponding to the public key. Transparency also extends to the open-source nature of blockchain infrastructures, which enables anyone to review the code.

²³⁹ European Securities and Market Authority (2023), *Decentralised Finance in the EU: Developments and risks*, cit.

²⁴⁰ <https://www.bankofcanada.ca/2023/10/staff-analytical-note-2023-15/>

²⁴¹ Roukny, T. (2022). *Decentralized finance: Information Frictions and Public Policies*, cit.

This multifaceted transparency makes DeFi²⁴² a highly advanced and innovative system.

- *Non custodial services.* In DeFi protocols, users have full control over their wallets and assets. This management autonomy is made possible by protocols that, for most operations, include collateral or guarantee mechanisms.
- *Interoperability and composability*²⁴³. The multi-layered structure of DeFi enables platforms to interconnect and combine in diverse configurations²⁴⁴. The permissionless nature of blockchains allows anyone to leverage the infrastructure of an existing platform to create new applications. A prominent example is Ethereum, which serves as the foundational layer for the majority of decentralised applications. With regard to interoperability, a distinction can be made between *functional interoperability*, referring to the ability of different applications within the same platform to interact, and *technical interoperability*, which concerns the interaction between different platforms²⁴⁵. Both interoperability and composability are made possible by the multi-layered architecture of DeFi systems.

2.4 Use cases.

Similar to Fintech, DeFi may be used for different purposes. Scholars and legal entities describe different use cases of decentralised finance²⁴⁶:

Payments and trading (decentralised exchange protocols). Payments are a crucial component of the DeFi ecosystem, with Bitcoin serving as a prime example. Likewise, the exchange of tokenised assets within the platform represents a key use case. Trading platforms are regarded as highly secure because users maintain full control over their crypto assets through a non-custodial system. This setup is made possible by dual-key mechanisms, which prevent malicious actors from misappropriating others' assets. Transactions are also governed by smart contracts that verify compliance with necessary conditions and automatically execute actions once these conditions are satisfied²⁴⁷.

Deposits and loans (decentralised lending platforms). Similar to fintech, platforms based on DLTs allow users to deposit and lend funds, providing access to liquidity. Interest payments and principal repayment are secured through smart contracts, which

²⁴² Khan A., & Sandner, P. (2024). DeFi: an overview of use cases and a status quo analysis of the ecosystem. *The Elgar Companion to Decentralized Finance, Digital Assets, and Blockchain Technologies*, 5-34. <https://doi.org/10.4337/9781035307760.00006>

²⁴³ European Securities and Market Authority (2023), *Decentralised Finance in the EU: Developments and risks*, cit., Roukny, T. (2022). *Decentralized finance: Information Frictions and Public Policies*, cit.

²⁴⁴ European Securities and Market Authority (2023), *Decentralised Finance in the EU: Developments and risks*, cit.

²⁴⁵ Khan A., & Sandner, P. (2024). DeFi: an overview of use cases and a status quo analysis of the ecosystem, cit.

²⁴⁶ Schueffel, P. (2021). Defi: Decentralized finance-an introduction and overview, cit.; Deutsche Bundesbank (2021), *Crypto tokens and decentralised financial applications (Monthly report)*, cit.

²⁴⁷ Khan A., & Sandner, P. (2024). DeFi: an overview of use cases and a status quo analysis of the ecosystem, cit.

automate the process and reduce counterparty risk. The easy access to decentralised markets, along with the absence of intermediaries, makes these platforms particularly appealing to both borrowers and lenders, as obtaining credit becomes faster and simpler. However, the volatility of crypto asset values and the lack of traditional intermediaries may threaten the repayment of borrowed funds. To address this, platform developers have introduced mechanisms to enhance loan security. The most common method is the use of collateral²⁴⁸: borrowers secure their loans with their own tokens, which must exceed the value of the borrowed amount. If the token value drops to the level of the loan, a smart contract automatically liquidates the position. This setup is known as an over-collateralised loan²⁴⁹. Examples of DeFi lending platforms are Maker Aave protocols²⁵⁰. MakerDAO operates a lending system centred around the stablecoin Dai, which is pegged to the US dollar. As mentioned earlier, loans are granted only if the borrower provides adequate collateral. The lender is thus protected by a smart contract that triggers liquidation as soon as the value of the collateral falls below a predetermined threshold²⁵¹. The Aave protocol is distinctive for its provision of flash loans. In this case, loans are unsecured but must be repaid within the same transaction block. If repayment does not occur, the block is not validated, and the transaction is cancelled.

In general, the primary motivation for participants to engage in DeFi lending platforms lies in the prospect of earning rewards and conducting leverage trading²⁵². Certain platforms (e.g., Compound) distribute rewards to both lenders and borrowers, which can incentivise borrowing spirals aimed at maximising token accumulation and stimulating loan activity. Leverage trading, instead, refers to the practice whereby a trader invests by purchasing one asset (e.g., ETH) using another asset (e.g., DAI), with the expectation that the value of the former will increase over time, thereby generating profit.

Decentralised derivatives. DeFi can also be employed for the creation and trading of derivatives (e.g., options, futures, and swaps). The term *decentralised derivatives* refers to crypto tokens whose value depends on an underlying asset and on the occurrence of specific conditions²⁵³. They operate in a similar way to stablecoins, but since they are not pegged to a legal tender currency, their value is more volatile. For this reason, collateral guarantees are required. In the case of decentralised derivatives, such collateral is provided in the form of tokens. Once the collateral is supplied, the derivative is issued. The value of the derivative ultimately depends on the information

²⁴⁸ Deutsche Bundesbank (2021), Crypto tokens and decentralised financial applications (Monthly report), cit.

²⁴⁹ An over-collateralized loan is one in which the value of the collateral exceeds the value of the loan. This mechanism provides a safety margin for the lender in the event of borrower default, as the excess collateral can be liquidated to recover the loan amount.

²⁵⁰ Xu, J., & Vadgama, N. (2022). From Banks to DeFi: the Evolution of the Lending Market. In *Future of business and finance* (pp. 53–66). https://doi.org/10.1007/978-3-030-78184-2_6

²⁵¹ Ellinger, E. W., Mini, T., Gregory, R. W., & Dietz, A. (2023). Decentralized Autonomous Organization (DAO): The case of MakerDAO. *Journal of Information Technology Teaching Cases*, 14(2), 265–272. <https://doi.org/10.1177/20438869231181151>

²⁵² Xu, J., & Vadgama, N. (2022). From Banks to DeFi: the Evolution of the Lending Market, cit.

²⁵³ Deutsche Bundesbank (2021), Crypto tokens and decentralised financial applications (Monthly report), cit.

transmitted to the oracle²⁵⁴. The creation of derivatives within the DeFi landscape is particularly straightforward due to the platform's open-access configuration. An example is Synthetix, a protocol that issues synthetic assets. These synthetic assets are tokens that represent derivatives and can therefore be traded directly on the blockchain. Compared to traditional derivatives, tokenised derivatives are fully traceable and thus offer greater security. The protocol relies on oracles to monitor the value of underlying elements, thereby enabling trading and liquidity provision²⁵⁵. Moreover, the Synthetix derivative system is collateralised through a debt pool, which ensures stronger security and solvency of outstanding positions.

Asset management. The term asset management refers to the management and optimisation of the value of goods and resources (the 'assets') to achieve specific goals, such as maximising profits, minimising costs, and reducing risks. In relation to DeFi, the concept of asset management includes portfolio management and, more generally, the allocation of assets across various platforms through automated systems. Smart contracts are capable of managing investors' assets and reallocating them across different decentralised applications (dApps). In this context, a significant innovation is represented by on-chain funds, which are investment funds wholly operated on the blockchain via smart contracts. On-chain²⁵⁶ funds automate core processes such as subscriptions, portfolio rebalancing, NAV calculation, and redemptions. These processes are executed automatically through embedded controls (rules encoded in smart contracts), oracles (to acquire external data such as market prices), and programmatic accounting²⁵⁷.

Insurance. The DeFi ecosystem is also suited to providing insurance services. The system relies on oracles and smart contracts to verify the occurrence of the specified condition and, consequently, to execute payments covering losses. The use of automated mechanisms brings significant benefits in terms of transparency and fairness in contractual operations, enabling swift settlements without the need for additional verification or intervention. Furthermore, the accessibility of the system, stemming from the public and permissionless nature of the blockchain, allows anyone to utilise such services. The concept of insurance in DeFi extends beyond activities occurring off-chain (e.g., flight cancellations or car damage) to encompass events that occur within the blockchain itself. Indeed, insurance can cover losses related to external attacks on DeFi protocols or smart contract malfunctions.

An example of DeFi insurance service is constituted by Etherisc. Etherisc was founded by a startup and provides insurance services related to flight delays, natural disasters,

²⁵⁴ Ibid.

²⁵⁵ <https://quantstamp.com/blog/the-protocols-bringing-derivatives-to-defi?utm>

²⁵⁶ On-chain refers to transactions and processes that are executed and recorded directly on the blockchain, ensuring transparency and immutability. Off-chain refers to activities taking place outside the blockchain, typically offering greater speed and lower costs but with reduced transparency and reliance on external entities.

²⁵⁷ <https://chain.link/article/tokenized-vs-on-chain-funds?utm>

crypto wallet and crop²⁵⁸. For example, in case of damage to the crops, the materials attached by the insured are compared with the ones available through other attendible sources (e.g. satellites)²⁵⁹. This verification is automated and allows for transparency and fairness in contracts. Another interesting protocol is Insurwave. Insurwave monitors the movement of ships in the sea and adjusts pricing according to the location, taking into account the specific risks of the area.

3. Conclusions.

This chapter has shown that decentralised finance has grown into a parallel ecosystem alongside traditional financial markets. The services it provides (payments, lending, asset management, or insurance) are similar to those offered by banks and other intermediaries. What changes is how these services are delivered. Transactions and contracts are executed automatically through code, rather than through institutions.

DeFi does not replace the existing system but transforms it. By removing intermediaries, it opens financial markets to anyone with an internet connection, offering faster and more flexible services. At the same time, this openness creates new challenges for users, who must take full responsibility for managing their assets and understanding how these systems operate.

The analysis has also shown that DeFi is organised across several layers. The settlement layer, based on public and permissionless blockchains, guarantees security and transparency. The asset layer includes the tokens and stablecoins that circulate in the system. The application layer hosts decentralised applications and smart contract protocols, while the user interface layer allows access through simple digital tools. Together, these layers create a structure that resembles the traditional financial architecture, but with much greater flexibility.

Some key features distinguish this model. Universal access allows participation without geographic or institutional barriers. Transparency stems from the public nature of the blockchain ledger, where all transactions can be verified. Non-custodial services give users direct control over their wallets and assets, eliminating the need for intermediaries but also removing the safety net they provide. Interoperability and composability further enhance innovation: platforms can interact and build upon one another, allowing new financial products to develop quickly.

DeFi therefore presents both opportunities and risks. Its openness and automation can make financial services more inclusive and efficient. Yet, its technical complexity, market volatility and lack of supervision expose users to significant dangers. Many of these risks fall directly on consumers, who may not have the expertise to evaluate

²⁵⁸ Averin, A., Musaev, E., & Rukhlov, P. (2021). Review of existing Blockchain-Based insurance solutions. *2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 140 -143.
<https://doi.org/10.1109/itqmis53292.2021.9642748>

²⁵⁹ Ibid.

them. The next chapter will focus precisely on these aspects. It will examine the vulnerabilities of decentralised finance.

Chapter 3 – Risks related to crypto assets and DeFi.

0. Introduction. - **1.** Risks in DeFi. - **1.2** Risks in TradFi and DeFi. - **2.** Consumer Protection. A general overview of the EU framework. - **3.** Risks for consumers in crypto asset transactions. **3.1** Frauds, scams, hacks and illicit activities. - **3.2** Scamming techniques. - **4.** Conclusions.

0. Introduction.

Distributed ledger technologies and, more generally, decentralised finance represent a complex and articulated ecosystem. Building upon the definitions and conceptual framework outlined in Chapters 1 and 2, this chapter moves from a descriptive to an evaluative dimension, focusing on the risks and limitations associated with the use of crypto-assets and DeFi. As analysed in the previous chapters, this ecosystem constitutes a significant technological and financial challenge. Decentralisation and, more broadly, accessibility to financial services represent a major opportunity for investment, as well as for involving consumers in new forms of financial growth. Moreover, the transparency of transactions increases the security of these services, allowing users to view the operations being carried out and, where possible, to understand the functioning of the protocol.

Decentralised finance, by virtue of its open-source nature, constitutes a transparent and accessible model not only in terms of investment opportunities but also with regard to the creation of applications. Anyone may consult such a protocol and replicate it. Similarly, anyone may develop applications and smart contracts to create and deploy their own programmes.

However, this activity is not without risk. Risk must be assessed not only in relation to a given business or potential cyber harm, but also in light of the activity's place in the legal order. When a professional deals with a consumer, specific duties of transparency and protection apply to safeguard the weaker party. These obligations represent one of the greatest achievements of the modern era, as they ensure the protection of the weaker contracting party against possible abuses by the stronger one.

In the European Union, consumer protection reflects years of policy and directives harmonising minimum standards for services and goods. Such protection, however, may at times require the introduction of specific policies and ad hoc regulations designed to govern a particular phenomenon, ensuring that it complies with minimum protection standards. The European framework on crypto-assets and distributed-ledger technologies moves in this direction.

Through the introduction of a system of authorisations and standards, the new European regulations pursue, among other objectives, the protection of consumers and the transparency of the activities offered. The technique employed to achieve this goal consists in regulating the access requirements for the provision of such services, by means of prescribed information models. As in other legal and economic frameworks (e.g., MiFID II), decision-making on certain aspects is entrusted to highly specialised public authorities in the relevant sectors. This choice is justified by the higher level of

expertise required in a field of significant technical complexity, and by the need to delegate the definition of specific aspects to authorities possessing greater data resources to ensure more accurate regulation.

This chapter examines the main risks associated with the use of crypto-assets and decentralised finance (DeFi) platforms. It focuses on the challenges that arise for consumers who participate in these markets, either as investors or users of digital financial services. Unlike traditional systems, where institutions act as intermediaries and are bound by clear legal duties, decentralised systems often lack comparable safeguards. The complexity of the underlying technology, the volatility of digital assets, and the absence of effective oversight expose users to financial losses and fraudulent conduct. The aim of the chapter is to answer to the following question:

- *What are the risks related to crypto assets and decentralised finance?*

The methodology used is qualitative and descriptive, based on literature and institutional sources and reports. The discussion begins with a conceptual analysis of risk, distinguishing between the categories that affect all financial systems and those specific to DeFi. It then explores the main types of risk identified by academic and institutional studies - strategic, operational, financial, and emerging risks - and highlights how these manifest in decentralised contexts. Particular attention is given to consumer-related vulnerabilities such as counterparty risk, market volatility, lack of transparency, product complexity, and fraud.

The purpose of this chapter is then to provide a foundation for understanding why regulation is necessary. This argument acts as a direct bridge to Chapter 4, where the effectiveness of the European regulatory framework will be assessed in light of the risks identified here. By identifying the concrete risks faced by users, it becomes possible to assess whether existing and forthcoming legislation, such as the MiCA Regulation and the DLT Pilot Regime, can offer effective protection.

1. Risks in DeFi.

The previous chapters have outlined the specific characteristics of systems based on distributed technologies and decentralised finance protocols. The use of distributed ledger technologies (DLTs) and smart contracts offers significant advantages in terms of speed, security, and cost²⁶⁰.

Regarding transaction speed, blockchain protocols operate without intermediaries and rely on validation systems that reward, in economic terms, the participant who validates the transaction first. This ensures faster and more efficient operations compared with traditional financial systems. The absence of intermediaries also reduces transaction costs, which are often limited to minimal fees.

In terms of security, as discussed previously, the peer-to-peer system based on dual-key cryptography provides a high level of protection in managing digital wallets.

²⁶⁰ Roukny, T. (2022). *Decentralized finance: Information Frictions and Public Policies*, cit.

Likewise, the block-based structure guarantees transparency and traceability of operations.

In decentralised finance specifically, the open-source nature of these systems allows anyone to access and reuse the underlying protocol, fostering the development of applications and new forms of investment. For instance, crowdfunding initiatives—albeit of modest size—can be funded and managed by investors worldwide. Similarly, the execution of agreements through smart contracts facilitates smoother and more reliable contractual performance. The use of trusted oracles to verify the fulfilment of contractual conditions ensures certainty in execution and prevents disputes.

From an environmental perspective, the development of new consensus algorithms requiring less energy for transaction validation contributes to the protection of the ecosystem and to increasing compliance with environmental standards.

Nevertheless, the use of such protocols is not without challenges and risks. Before analysing them, it is necessary to clarify the concept of risk itself. A wide range of academic and institutional publications on DeFi dedicate specific attention to the risks inherent in these protocols. Some of these studies compare DeFi risks to those of traditional finance (TradFi), while others focus exclusively on DeFi-specific vulnerabilities. This section will first address the risks unique to decentralised finance and then compare them to those typical of traditional finance. Particular attention will be given to risks involving consumer-protection breaches and the relevant EU directives.

1.2 Risks in TradFi and DeFi.

The risks associated with DeFi partly overlap with those found in traditional finance. To identify the specific risks of DeFi, a comparison with TradFi is required.

The International Association for Trusted Blockchain Applications (INATBA, 2025) provides an in-depth analysis of the types of risk affecting economic operators in both traditional and decentralised finance. The report first identifies existing categories of risk and then compares the likelihood of their occurrence in the two systems.

Broadly, four main categories of risk may be identified for financial entities²⁶¹:

- Strategic risk
- Operational risk
- Financial risk
- Emerging risk

Strategic risk. Strategic risk stems from an entity's own business activities and decisions regarding commercial and communication strategies. It includes business

²⁶¹ International Association for Trusted Blockchain Applications (2025), DeFi Self-Regulation: A Proposal for the Industry, cit.

risk, i.e. risks related to the economic and financial performance of the entity, influenced by market choices and applicable legislation.

Strategic risk also encompasses legal and capital risks. Legal risk concerns actions or omissions that may give rise to legal proceedings, compliance failures, or breaches of laws governing the relevant activity. Capital risk relates to the insufficiency of financial resources needed to meet corporate obligations.

Further, reputational risk - damage to the image or integrity of the entity - falls within this category, as it results from strategic choices affecting public perception and trust. Environmental, social, and governance (ESG) risks are also part of strategic risk and refer to adverse consequences arising from: (a) failure to adopt environmental policies or engaging in environmentally harmful practices; (b) conduct detrimental to workers, consumers, or human and labour rights; and (c) poor governance practices such as corruption or lack of transparency²⁶².

Such conduct may expose an undertaking to lawsuits, financial loss, or diminished stakeholder confidence.

According to INATBA's analysis, strategic risk is substantially similar in both TradFi and DeFi, though the latter is in some respects more vulnerable. The absence of a clear regulatory framework makes compliance more complex for service providers. However, the introduction of the Markets in Crypto-Assets Regulation (MiCA), the DLT Pilot Regime, and national regulatory sandboxes is expected to mitigate these vulnerabilities. The existence of uniform standards and controlled testing environments reduces the likelihood of breaches and ensuing harm.

Operational risk. Operational risk refers to losses resulting from inadequate or failed internal processes, human errors, system malfunctions, or external events²⁶³. Such risks can impair an entity's efficiency and have therefore been addressed in EU legislation concerning banks and financial intermediaries.

To mitigate operational risks, intermediaries and banks are required to establish sound governance mechanisms and effective processes for identifying, monitoring, mitigating, and assessing these risks²⁶⁴.

²⁶² Bernoville, T. (2024, December 13). *ESG risk: Definition and best practices to mitigate it*. Plan a Academy. Retrieved September 15, 2025, from <https://plana.earth/academy/esg-risk#:~:text=ESG%20risk%20refers%20to%20environmental,%2C%20social%2C%20and%20governance%20factors>.

²⁶³ Banca d'Italia. (2006). *Recepimento della nuova regolamentazione prudenziale internazionale (nuovo accordo sul capitale di Basilea e nuova direttiva c.e. sui requisiti di capitale delle banche e delle imprese di investimento)*. <https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/D oc Cons Rischi operativi.pdf>.

²⁶⁴ Ibid.

Operational risk also includes internal and external fraud. Fraud is conduct typically involving human intent to misappropriate items of commercial or economic value and may be committed by internal or external actors through various techniques²⁶⁵.

Internal fraud refers to breaches committed by insiders - such as corruption, tax evasion, or embezzlement - which directly affect the company and may entail legal liability. External fraud is perpetrated by outsiders, including clients or business partners, through actions such as hacking or the theft of confidential information.

Other subcategories of operational risk include workplace safety, unfair commercial practices, damage to physical assets, business interruption, and contract execution failures.

Operational risk exists in both TradFi and DeFi. In DeFi, a specific concern arises from cyberattacks targeting digital protocols. To prevent such risks, resilient protocol design and secure voting mechanisms are crucial, reducing the likelihood of fraud and ensuring compliance with security standards. In general, DeFi features such as transparency and automated smart-contract execution render decentralised systems less exposed to certain operational vulnerabilities.

Financial risk. Financial risk relates to the use and management of financial resources within the entity. It includes:

- a) *credit risk*, which is the exposure to losses from counterparties failing to fulfil financial obligations, whether through unpaid investments or delayed payments²⁶⁶;
- b) *concentration risk*, which is the exposure arising from an undiversified or limited client base.
- c) *liquidity risk*, which is the inability to meet obligations due to insufficient liquid assets;
- d) *market risk*, which refers to the exposure to adverse movements in market variables.
- e) *emerging risk*, which refers to consequences not yet precisely identified.

A degree of financial risk is inherent in all investment activity, given its speculative and uncertain nature. In DeFi, this risk is heightened for crypto-assets not pegged to stable values or lacking collateralisation. The collapse of the *Terra Luna* cryptocurrency demonstrated how a narrow client base can trigger exponential losses. Regarding liquidity risk, collateralisation mechanisms in DeFi lending have emerged as a partial safeguard.

Emerging Risk. Emerging risks are those not yet clearly identified, which may materialise in connection with a specific activity or operating environment.

²⁶⁵ Saccone, U. (2014). Lo sviluppo di un sistema antifrode: considerazioni programmatiche e ruolo della Security. In www.sicurezzanazionale.gov.it.

²⁶⁶ This risk does not only concern investments made, but also the methods used to request payments from customers, for example by requesting immediate payments or payment deferrals.

An example of emerging risk concerning crypto assets is the environmental risk. As explained in previous chapters, crypto transactions use consensus algorithms to validate transactions. The consensus algorithms used to validate nodes may be responsible for the adverse effects on the environment. Not all the consensus algorithms present the same characteristics. For instance, the PoW consensus algorithm implies a higher consumption of energy than the PoS one²⁶⁷. Concerning the PoW mechanism, the operation's success requires 50% + 1 of the miners' approval and the validation of nodes constitutes an expensive activity in terms of energy. Consequently, less polluting consensus algorithms have been consequently created to empower a more sustainable blockchain.

2. Consumer Protection. A general overview of the EU framework.

A defining feature of decentralised finance is its open-access nature. As explained earlier, anyone can access and operate within a public distributed-ledger network.

While this openness reduces costs and democratises finance, it also exposes consumers - who occupy a weaker contractual position - to specific risks.

Since the 1980s, the European Union has developed a comprehensive framework governing consumer-professional relations. Under Article 4(f) of the Treaty on the Functioning of the European Union (TFEU), consumer protection falls under shared competence. Articles 114 and 169 TFEU further enshrine a high level of consumer protection and the safeguarding of consumer interests, including access to information, education, safety, fair advertising, equitable contractual relations, and efficient public services.

As these provisions are implemented through directives, their transposition and enforcement are the responsibility of each Member State. The principal aim of EU consumer law is to provide non-derogable protection to consumers when contracting with professionals²⁶⁸.

A *consumer* is defined as a natural person acting for purposes outside any trade, business, craft, or profession²⁶⁹, while a *professional* is any natural or legal person acting within such professional capacity, including intermediaries.

Professionals typically possess superior knowledge, which may place consumers at a disadvantage. Accordingly, EU consumer law imposes duties of transparency and care on professionals, establishing corresponding rights and remedies for consumers to prevent harm arising from professional misconduct.

In Italy, for instance, the transposition of EU directives was achieved through the adoption of a consumer code (Codice del Consumo), a unified legislative text

²⁶⁷ Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Frontiers in Blockchain*, 6. <https://doi.org/10.3389/fbloc.2023.1151724>

²⁶⁸ Trabucchi [integra citazione]

²⁶⁹ art 3, comma 1, lett. a) del Codice del Consumo.

complementing the Civil Code. In case of conflict between the special provisions of the consumer code and the general rules of the Civil Code, the former prevails. The code provides multiple layers of protection, corresponding to its five parts:

- 1) Protection of general consumer interests;
- 2) Information duties and unfair commercial practices;
- 3) Contractual regulation and remedies;
- 4) Product safety and quality;
- 5) Collective actions and injunctions.

For the purposes of this analysis, information obligations and provider liability are of particular importance. Professionals offering services must disclose specific information about their products; failure to do so may trigger sanctions or render contracts void. These obligations are reinforced in the banking and financial sectors, where the consolidated banking act (Testo Unico Bancario) and the consolidated finance act (Testo Unico Finanziario) impose additional disclosure duties beyond general consumer-protection requirements.

In the field of cryptocurrency operations, the MiCA Regulation imposes specific information obligations for the offering or sale of crypto-assets that fall within its scope. This confirms the need to adapt consumer-protection rules to the peculiar characteristics of these services. However, such specific obligations apply only to activities falling outside the financial sector, for which the MiFID II framework remains applicable.

3. Risks for consumers in crypto asset transactions.

The use of crypto-assets constitutes a particularly vulnerable area for consumers. Products and services involving crypto-assets are structurally complex. On the one hand, smart contracts and blockchain technology introduce new technical instruments enabling the automation and reliability of operations. Understanding how these technologies function is essential to assessing whether a platform can be regarded as trustworthy. On the other hand, economic transactions involving crypto-assets are often based on speculation or collateralisation mechanisms. The degree of risk assumed depends on the type of financial or economic guarantee offered by the platform and on the nature of the product involved, for instance, whether it is a cryptocurrency or a stablecoin. Another relevant factor is the universal accessibility of such services. As they are offered online, these products can be provided by virtually anyone, from any jurisdiction. While such openness promotes market freedom and access to finance, an uncontrolled and largely unregulated environment may generate serious concerns. Typical examples include the absence of essential information regarding the nature of the product or service, or exposure to cyber-fraud. Consumers may be unable to identify potential risks and may enter into contractual obligations without the necessary awareness or safeguards.

In this regard, both scholars²⁷⁰ and regulators²⁷¹ have identified a range of risks arising for consumers from the use of decentralised finance platforms and services. These risks - although also present in traditional finance and in private-law transactions - manifest themselves in distinct ways within decentralised finance and, more broadly, in operations involving crypto-assets.

The following risks can be identified:

- counterparty risk
- price movement and losses
- liquidity risks
- misleading information
- product complexity
- limited protection
- frauds, scams, hacks and illicit activities

*Counterparty risk*²⁷². Counterparty risk refers to the possibility that one of the contracting parties fails to perform its obligations. In decentralised finance, this risk should be mitigated through the use of smart contracts and collateralisation mechanisms. Smart contracts execute performance only when all contractual conditions are fulfilled. Collateralisation, as previously noted, ensures that the counterparty maintains sufficient reserves and, if the funds fall below a defined threshold, automatically triggers liquidation of the corresponding amount. Another factor influencing counterparty risk is the nature of the underlying asset. When the currency is pegged to a stable value - such as in the case of a stablecoin - financial fluctuations are less likely to affect contractual performance. Conversely, when the asset is not pegged to any stable reference value and its price depends solely on market supply and demand, volatility may significantly impair the ability of the holder to meet obligations. However, as illustrated by the collapse of the *Terra* ecosystem, collateralisation does not eliminate risk entirely, particularly when the client base is not sufficiently diversified. Moreover, not all platforms offering crypto-asset services provide stable or transparent guarantee systems. In some cases, the existence or reliability of such mechanisms is not properly disclosed to users. Collateralisation may also impose a significant burden on borrowers, who are often required to lock in assets

²⁷⁰ Scharfman, J. (2023). Introduction to cryptocurrency and digital asset fraud and crime. In *Springer eBooks* (pp. 1–16). https://doi.org/10.1007/978-3-031-23679-2_1; Scharfman, J. (2023b). The Cryptocurrency and Digital Asset Fraud Casebook. In *Springer eBooks*. <https://doi.org/10.1007/978-3-031-23679-2>; Alekseenko, A. P. (2023). Model Framework for Consumer Protection and Crypto-Exchanges Regulation. *Journal of Risk and Financial Management*, 16(7), 305. <https://doi.org/10.3390/jrfm16070305>; Bele, D. (2020). Financial scams, frauds, and threats in the digital age. In *Modern approaches to knowledge management development: collective monograph* (pp. 39–50). Ljubljana School of Business.

²⁷¹ European Securities and Market Authority. (2023). *Decentralised Finance in the EU: Developments and risks*, cit.; U.S. Department of the Treasury. (2023). *Illicit Finance Risk Assessment of Decentralized Finance*. Retrieved September 9, 2025, from <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>;

²⁷² European Securities and Market Authority. (2023). *Decentralised Finance in the EU: Developments and risks*, cit.

of substantially higher value than the loan itself. The absence of adequate awareness regarding these risks constitutes a major issue from the standpoint of consumer protection, as users may engage in transactions without having received a full and clear explanation of the risks involved.

Price movements and losses. The value of crypto-assets tends to be unstable, especially when referring to those not linked to stable benchmarks. The fluctuation of Bitcoin is a clear example of how a crypto-asset can move from a low to a very high value in a short period of time. Since the value of such assets depends solely on supply and demand, and there are no intermediaries or regulations governing them, even small market shifts can cause significant changes in price. A consumer who decides to invest in a cryptocurrency is not always aware that: (a) its value is inherently unstable because it relies entirely on market demand and supply; and (b) there is a difference between a cryptocurrency and a stablecoin. This lack of understanding may lead to uninformed decisions and, consequently, to financial losses of variable value, depending on the amount invested.

*Liquidity risk*²⁷³. As already noted in the general discussion on risks associated with crypto-asset operations, liquidity risk refers to the situation in which, at a given time, the possibility of converting an asset into liquid funds is limited. This risk affects not only service providers - whose platforms may become insolvent or fail - but also consumers using such services. In periods of market stress, it may become difficult to sell a particular currency, thereby causing financial harm to consumers seeking to recover the liquidity corresponding to their assets (see Terra collapse in chapter 2).

Misleading information. Crypto-assets are typically offered and sold online. The platforms involved do not always provide clear or comprehensive information about the products they market. In some instances, aggressive sales techniques are employed, which may induce consumers to purchase without fully understanding the risks or the actual nature of the product. Social media platforms are also frequently used as promotional tools for such investment schemes, leading consumers to rely on the promoter's reputation or perceived financial expertise. In these circumstances, the risk of uninformed decision-making is particularly high, as the consumer's only point of contact is often a party engaged in promoting the product and who fails to supply the information necessary for a well-founded and conscious choice.

Product complexity. The issue of misleading information is closely linked to the intrinsic complexity of crypto-asset products. As highlighted in the first two chapters, these products are highly heterogeneous in nature. As will be examined in the following chapter, not all of them are subject to the same disclosure requirements. The applicable legal framework varies according to the characteristics of the asset and the nature of the service provided, whether financial or non-financial. It is self-evident that crypto-assets with a financial character may entail considerably higher risks than simple private law exchange operations. However, even contractual relationships falling within the scope of private law may result in substantial consumer harm. A

²⁷³ https://www.esma.europa.eu/sites/default/files/2025-10/Joint_ESAs_revised_warning_on_crypto-assets.pdf

notable example is the case of funds deposited with a crypto-asset service provider that subsequently becomes insolvent. Such situations have already been examined by Italian courts of first instance and, as will be discussed in the last chapter, may lead to severe economic losses for consumers and interpretative issues for courts.

Limited protection. Legal protection in the case of crypto-assets is limited for several reasons. First, it should be clarified that where proper information has been provided regarding the (financial) product sold, any losses resulting from market fluctuations cannot generally be challenged. In the absence of adequate pre-contractual information, liability may arise mainly on a pre-contractual basis. However, without delving here into the specific legal classifications, it must be noted that many crypto-asset service providers use VPNs to deliver their services. This makes it difficult to trace the actual geographical location of the server and to identify the provider. In cases of fraud, criminal networks are often structured in such a way that they disappear as soon as the funds have been collected, transferring the money to accounts that are extremely difficult to trace. In such circumstances, identifying those responsible becomes nearly impossible, and as a result, the issue of legal protection becomes largely theoretical.

3.1 Frauds, scams, hacks and illicit activities.

Crypto-assets can easily become the object of fraud and other illicit activities. Fraud generally refers to any conduct which, by exploiting an individual's naivety - sometimes through deceit, trickery, or similar techniques - aims to obtain an unlawful advantage, thereby causing harm to the victim's patrimonial sphere. In legal terms, fraud may have both criminal and civil relevance. For instance, under the Italian legal system, fraud constitutes a criminal offence under the criminal code (Codice penale)²⁷⁴; however, even where not all the constitutive elements of the offence are met, such conduct may still have civil relevance and give rise to a right to compensation for damages²⁷⁵.

With regard to crypto-related frauds, these are particularly widespread. The United States Federal Trade Commission (FTC) reported over 46,000 cases of fraud amounting to approximately one billion dollars for the period between January 2021

²⁷⁴ Art. 640 c.p. "*Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità ; 2-bis. se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7"*

²⁷⁵ Cesareo, T. (2020). L'illecito al confine tra truffa contrattuale e inadempimento civilistico. *Cammino Diritto*, 3/2020. https://rivista.camminodiritto.it/public/pdfarticoli/4808_3-2020.pdf

and March 2022²⁷⁶. In most of these cases, payments were made using the cryptocurrencies Bitcoin, Tether, and Ether. In this respect, the United States Securities and Exchange Commission (SEC) initiated 193 enforcement actions to block cryptocurrency-related projects and to ensure proper conduct by service providers²⁷⁷. During the same period (January 2021 – March 2022), the majority of frauds - worth around USD 573 million - concerned investment-related scams. These were followed by so-called “romance scams”, valued at USD 185 million, typically perpetrated through dating applications where the fraudster offers to explain how to invest in crypto-assets or requests that crypto-assets be sent directly. Finally, the FTC reported “business and government impersonation” scams amounting to USD 133 million. In these cases, fraudsters contacted users while posing as government authorities or banks, alarming them about alleged risks to their accounts. Victims were instructed to transfer their funds to external accounts by converting them into cryptocurrencies, which were then diverted to the fraudsters’ accounts.

Brazil has also witnessed a significant expansion of the crypto-asset market, accompanied by several frauds and hacking incidents. One such case concerned the *Bitcoin Banco Group*. Its owner reported the loss of 7,000 Bitcoins (approximately EUR 300 million) allegedly caused by a hacker attack. However, subsequent investigations revealed that no such attack had occurred, leading authorities to open proceedings against the company for various offences, including money laundering and embezzlement. Around 200 investors brought civil actions seeking compensation, with claims ranging from USD 3,000 to USD 3 million²⁷⁸.

Within the European Union, no official government report has yet consolidated all data relating to the economic losses caused by investments and contractual operations involving crypto-assets. Nevertheless, from various investigations and reports issued by official governmental bodies, the scale of the phenomenon can be discerned.

In Italy, in 2020, law enforcement authorities executed precautionary measures against an individual operating a cryptocurrency exchange platform, accused of computer fraud amounting to EUR 120 million, fraudulent bankruptcy, and self-laundering. The suspect is alleged to have been responsible for a financial shortfall of approximately EUR 120 million on the hacked Bitgrail platform and for having defrauded over 230,000 investors²⁷⁹.

In Belgium, a report published in January 2025 by the Financial Services and Markets Authority (FSMA) quantified the losses suffered by consumers in the second half of

²⁷⁶ Fletcher, E. (2022). Reports show scammers cashing in on crypto craze. In *ftc.gov*. Federal Trade Commission. <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze>

²⁷⁷ <https://www.sec.gov/about/divisions-offices/division-enforcement/cyber-crypto-assets-emerging-technology>

²⁷⁸ Karu, C. (2021, July 8). Brazil’s ‘Bitcoin King’ arrested over alleged \$300M embezzlement. *CoinGeek*. <https://coingeek.com/brazil-bitcoin-king-arrested-over-alleged-300m-embezzlement/>

²⁷⁹ <https://www.poliziadistato.it/articolo/165fe09d895a115662371850>

2024 due to fraudulent trading platforms and cryptocurrencies at over EUR 12 million, representing 79% of the total losses reported by consumers during that period²⁸⁰.

In Spain, the national authority, in cooperation with Europol and the national authorities of Estonia, France, and the United States, identified a criminal network responsible for cryptocurrency-related frauds. The network is believed to have laundered EUR 460 million and defrauded more than 5,000 consumers worldwide. It allegedly relied on accomplices to attract clients and divert funds through crypto-asset transfers²⁸¹.

More recently, Eurojust has conducted an investigation into a cross-border fraud affecting several Member States, involving more than EUR 100 million. The inquiry uncovered a long-running scheme in which fraudsters lured clients by promising high returns and creating a platform with a professional and credible layout. When account holders requested withdrawal of their funds, the provider demanded additional fees and subsequently shut down the websites. As a result, consumers lost their funds, which were later laundered through Lithuanian accounts²⁸².

3.2 Scamming techniques.

The schemes used to attract customers and carry out illicit activities are numerous. In particular, the following categories can be identified²⁸³:

- Ponzi and pyramidal schemes
- rug pull
- romance scam
- Phishing scams
- giveaway
- airdrop

Ponzi scheme. One of the most frequently used techniques is the *Ponzi scheme*. A Ponzi scheme is a fraud based on a pyramidal system. The scammer gains profits from the sums paid by new investors. The perpetrator usually promises high rewards to those who join the project and uses those same funds to pay the rewards of previous

²⁸⁰ Financial Services and Markets Authority. (2025). Investment fraud and unlawful offers - Dashboard 2nd half of 2024. In *fsma.be*. Retrieved October 12, 2025, from https://www.fsma.be/sites/default/files/media/files/2025-01/20250116_dashboard_investment_fraud.pdf

²⁸¹ Europol. (2025, June). *Crypto investment fraud ring dismantled in Spain after defrauding 5000 victims worldwide*. europol.europa.eu. Retrieved October 12, 2025, from <https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide#:~:text=The%20investigation%20identified%20that%20the,Islands%20and%20%20in%20Madrid>)

²⁸² Eurojust. (2025, September 23). *Eurojust coordinates action to halt cryptocurrency fraud of over 100 million euros across Europe*. eurojust.europa.eu. Retrieved October 12, 2025, from <https://www.eurojust.europa.eu/news/eurojust-coordinates-action-halt-cryptocurrency-fraud-over-100-million-euros-across-europe>

²⁸³ Scharfman, J. (2023b). *The Cryptocurrency and Digital Asset Fraud Casebook*, cit.

participants. As this is a pyramidal system financing an increasing number of investors, a constant inflow of new participants is needed to keep payments going. The scheme works until the chain stops, either because no new investors enter or because participants request the withdrawal of their deposits²⁸⁴. This kind of fraud has also affected the crypto-asset sector. In such cases, the promoter claims to use algorithms that analyse market trends and are supposedly able to protect the investor in case of downturns²⁸⁵.

Rug pull. A rug pull is a fraudulent technique through which the founders of a financial project attract investors by promising profits, only to later abandon the project and leave investors with no returns. Instead of using the collected funds to develop the promoted initiatives, the founders misappropriate the money and disappear. As a result, investors are left holding worthless tokens and suffering the loss of their funds²⁸⁶.

Romance scam. A romance scam is a technique that exploits dating applications or websites to approach victims and persuade them to transfer funds or invest in certain platforms or investment projects by taking advantage of a romantic relationship established with the victim. Conversations usually begin on dating sites and are then moved to platforms such as WhatsApp, where the controls and safety measures of dating applications no longer apply. This makes it easier for the fraudster to send fraudulent links and engage in illicit conduct without being detected or blocked by the platforms. The romance scam is also known as the *pig butchering scam*, a term that reflects the gradual way in which victims are deceived and financially exploited²⁸⁷.

Phishing scams. Phishing scams aim to obtain information from victims through digital bait that promises rewards or profits. Phishing frequently relies on *spoofing* techniques to gain the victim's trust²⁸⁸. Spoofing involves contacting the victim using a phone number or email address that closely resembles that of a person or entity known to them, thereby attracting attention and creating a false sense of legitimacy. Phishing techniques are therefore designed to deceive individuals into revealing personal information, including account keys and passwords, which is then used to unlawfully access and misappropriate funds. In the field of crypto-assets, these

²⁸⁴ Alekseenko, A. P. (2023). Model Framework for Consumer Protection and Crypto-Exchanges Regulation, cit. “For example, in 2016, the New York Bitcoin Savings and Trust cryptocurrency exchange fraudulently received about 146,000 Bitcoins from investors. Its founders guaranteed weekly gains at the rate of 7%, which they made from receiving new investments while spending funds on their own personal needs”.

²⁸⁵ Scharfman, J. (2023b). The Cryptocurrency and Digital Asset Fraud Casebook, cit. The author, in his book, mentions several Ponzi schemes involving companies that emerged in Brazil, Zimbabwe, Egypt, and Bulgaria.

²⁸⁶ Ibid. “This effectively pulls the rug out from under the victims who are left holding worthless digital assets and tokens on a now abandoned project”

²⁸⁷ <https://dfpi.ca.gov/news/insights/pig-butcherer-how-to-spot-and-report-the-scam/> “The term refers to the agricultural practice of fattening pigs before slaughter, symbolizing how scammers “fatten” their victims with false attention before exploiting them financially.”.

²⁸⁸ <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing>

methods are employed to obtain the private keys of wallet holders and to gain unauthorised access to their digital funds.

Fake giveaway. Giveaways are free competitions, often circulated on social networks, through which promoters promise a prize to participants. Fraudsters using this technique to obtain funds create fake profiles of well-known individuals to advertise the initiative and attract victims. In some cases, scammers hack the actual social media accounts of celebrities and spread the scheme directly through their genuine channels. In this way, they persuade users to send them money or cryptocurrencies with the promise of receiving a higher amount in return. In reality, the fraudsters misappropriate the funds and then disappear²⁸⁹.

Airdrop fraud. An airdrop is a marketing technique that involves giving away tokens to attract new participants. It is a legitimate technique, but it has been used by scammers to steal funds from victims. Scammers usually send a small amount of free tokens to a user, who will then try to convert or exchange them. At this point, the scammer directs the victim to a link, explaining that in order to use their tokens, they must enable them on a third-party site. By following this link, the user will be tricked into entering their account's private keys, allowing the scammer to take over the wallet and take possession of the user's real tokens²⁹⁰.

4. Conclusions.

The chapter identified several categories of risk that affect both traditional and decentralised finance but manifest differently in each context.

The first part of the chapter has illustrated the general risks related to DeFi. Strategic and operational risks remain relevant, especially where the lack of clear governance exposes users to market failures or platform insolvencies. Financial risks, such as liquidity shortages and counterparty defaults, are particularly severe in decentralised markets, where the value of assets can fluctuate dramatically and the mechanisms of collateralisation are often opaque. Emerging risks, including those related to environmental impact and technological dependency, add another layer of uncertainty.

The comparison carried out with traditional finance (TradFi) has shown that in some sectors the level of risk is lower than in the traditional category. However, in other cases, the risks are not eliminated, and the complete reliance on platforms operating

²⁸⁹ One of the most famous scams in this context was perpetrated on Twitter in July 2020. Approximately 70 Twitter profiles of prominent figures were hacked. Users were asked to deposit Bitcoin in exchange for double the amount, which would then be provided to them. The scam spread widely as it involved personalities such as Elon Musk, Warren Buffet, and Bill Gates. In addition, users were invited to donate the sums to charity. See Iyengar, R. (2020, July 16). Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others. *CNN Business*. <https://edition.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html>

²⁹⁰ <https://support.metamask.io/stay-safe/safety-in-web3/scammers-and-phishers-rugpulls-and-airdrop-scams/>

without intermediaries or central authorities can become critical in times of crisis resolution (for example, in cases of concentration or liquidity risk).

The second part of the analysis has illustrated the specific risks to which consumers are exposed within the context of decentralised finance and crypto assets.

The analysis shows that, although blockchain technology can ensure the functional security of operations, there are several additional risks to which consumers remain exposed. In some cases, these risks stem from a lack of knowledge or awareness on the part of consumers. They also face exposure to misleading information, product complexity, and the absence of effective protection mechanisms. In other cases, risk arises from the unlawful conduct of providers. As illustrated by numerous instances of fraud and hacking, the open and borderless nature of DeFi makes enforcement extremely difficult and the recovery of losses almost impossible.

Overall, this chapter highlights that the risks linked to crypto-assets are not merely technical or speculative. They have direct implications for consumer rights, legal certainty, and market stability. In the absence of intermediaries or central authorities, traditional safeguards such as due diligence, disclosure duties, and financial supervision are either weakened or missing altogether. These findings confirm the need for a clear regulatory response. Effective consumer protection cannot rely solely on technological solutions but requires coherent legal frameworks that establish standards of transparency, liability, and supervision. The next chapter will therefore analyse how the European Union has addressed these challenges through the Markets in Crypto-Assets Regulation (MiCA) and the DLT Pilot Regime, assessing whether these instruments can provide adequate protection for consumers while supporting innovation in decentralised markets.

Chapter 4 – European Regulation and Crypto Assets.

0. Introduction. - **1.** The importance of regulating fintech in the internal market. – **2.** From zero to MiCAR. - **2.1** European Regulation on Crypto Assets and technological neutrality. - **2.2** Markets in Crypto Assets Regulation. The rationale. **2.3** The regulation. - **2.4** Categories of tokens. - **2.5** Main provisions of MiCAR. - **3.** The pilot regime for market infrastructures based on distributed ledger technologies. – **4.** Conclusions.

0. Introduction.

As demonstrated in the first three chapters, the crypto-asset ecosystem displays considerable complexity, both structurally and functionally. Having previously identified the technological foundations (Chapter 1), the operational scope of decentralised finance (Chapter 2), and the associated consumer risks (Chapter 3), this chapter evaluates the regulatory response adopted at the European level. Consumers engaging with this type of technology and financial product are often unable to fully understand the risks it entails. Similarly, in the context of banking operations, consumers often lack the necessary skills to assess whether the service provided is reliable or whether the systems used by the platform to guarantee the return of funds are stable.

The analyses conducted in the previous chapters have shown that the crypto-asset sector is highly volatile and complex. The absence of appropriate precautionary measures can result in significant economic losses for users of such services. It is therefore a particularly sensitive area that requires the adoption of measures ensuring proper information disclosure and consumer protection.

To this end, the European Union has adopted two regulations addressing this field: Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology and Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). These instruments pursue several objectives, including the establishment of a more regulated and reliable crypto-asset market that ensures the trustworthiness of service providers. The new framework complements existing legislation on financial products and services as well as on consumer protection. The regulations will therefore apply to areas not already covered by existing legislation or will operate alongside measures that continue to apply.

This chapter aims to assess whether the new regulations, together with the pre-existing legal framework, constitute an instrument that adequately takes consumer protection into account. The guiding research question is as follows: does the European regulatory framework effectively and adequately protect consumers from the risks associated with decentralised finance and crypto-assets?

The purpose of this chapter is to illustrate the recently adopted European legislation and to verify whether the measures introduced adequately address the risks and gaps identified in the first chapters of this thesis. This evaluation not only responds directly

to the main research question formulated in the general introduction but also serves as the conceptual bridge to the following chapter, which will explore the national judicial application of these frameworks in the Italian context. The MiCA Regulation and the DLT Pilot Regime constitute highly detailed and complex instruments. As emerges from their recitals, they pursue multiple aims and seek to achieve a range of policy objectives. In such cases, there is a risk that excessive detail and complexity may render compliance burdensome for companies while failing to provide effective remedies for the protection of vulnerable parties.

The methodology adopted is qualitative in nature. The discussion alternates descriptive and analytical sections concerning the measures adopted to provide a comprehensive response to the research question. The first part will provide an overview of the legislative acts that may find application regarding crypto assets. Crypto assets, as anticipated, affect many fields, and not all are regulated by the same act.

1. The importance of regulating fintech in the internal market.

The competence of the European Union for FinTech regulation is based on Articles 2, 4, 26 and 114 of the Treaty on the Functioning of the European Union²⁹¹. The proposal is founded on Article 114 of the TFEU, which empowers the European Union to adopt measures aimed at harmonising the laws of the Member States to ensure the establishment and proper functioning of the internal market²⁹².

Indeed, crypto assets fall into the category of the internal market. In this regard, the European Union has the power to adopt measures to implement the functioning of the internal market together with Member States.

²⁹¹ Art. 2 (2) “When the Treaties confer on the Union a competence shared with the Member States in a specific area, the Union and the Member States may legislate and adopt legally binding acts in that area. The Member States shall exercise their competence to the extent that the Union has not exercised its competence. The Member States shall again exercise their competence to the extent that the Union has decided to cease exercising its competence”.

Art. 4 (1) (2) “The Union shall share competence with the Member States where the Treaties confer on it a competence which does not relate to the areas referred to in Articles 3 and 6.

Shared competence between the Union and the Member States applies in the following principal areas: (a) internal market; [...]”.

Art. 26 “The Union shall adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties.

The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.

The Council, on a proposal from the Commission, shall determine the guidelines and conditions necessary to ensure balanced progress in all the sectors concerned.”

²⁹² European Commission. (2021). *Market in Crypto Assets (MICA)* (PE 739.221). European Parliamentary Research Service.

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI\(2022\)739221_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI(2022)739221_EN.pdf)

The internal market includes the free movement of goods and capital, and the freedom of establishment and provision of services. The aim is to create a free space for the circulation of goods and capital within the European Union²⁹³.

FinTech concerns all these sectors in this framework, representing a marketplace where providers and consumers can trade values or provide specific services. Regulation is so necessary to guarantee adequate protection to users, but also to foster the usage of such technology. FinTech represents, in fact, a large portion of investments. Indeed, distributed ledger technologies enhanced access to the market through systems that do not require intermediation.

The potential of such technology attracted investors all over the world. This aspect represents both an opportunity for the growth of the European economy and competitiveness, and a risk for consumers. Consequently, the European Union has initiated a process of rationalising and harmonising DLTs and FinTech regulation. The intention is to foster decentralised financial markets without imposing limitations on technology, with a view to the principle of technological neutrality. Technological neutrality means that the regulation of a service or good is applied regardless of the technology used. The principle is consistently relevant, considering that limiting technological progress could negatively affect the competitiveness of European Markets.

In addition, considering the cross-border nature of cryptos, regulation should enhance and implement international trade. It is fundamental to promote the development of such technologies to make the European Union more competitive with other international markets.

2. From zero to MiCAR.

Before analysing the legislation, it is necessary to consider how the MiCA Regulation and the DLT Pilot Regime came to be adopted.

As highlighted in the first two chapters, the phenomenon of crypto-assets dates back to 2008. It has since undergone constant development over the following years, eventually acquiring a truly global dimension.

In 2018, the European Commission published the *FinTech Action Plan* with the aim of making Europe more competitive in the financial sector²⁹⁴. The plan set out some concrete measures to foster innovation within the European financial sector. Its objectives were to enable innovative business models to scale up at EU level, to

²⁹³ <https://eur-lex.europa.eu/IT/legal-content/glossary/internal-market.html>

²⁹⁴ European Commission. (2018). *FinTech Action plan: for a more competitive and innovative European financial sector* (COM(2018) 109 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109> (see also: https://finance.ec.europa.eu/publications/fintech-action-plan-more-competitive-and-innovative-european-financial-sector_en).

promote the adoption of emerging technologies such as blockchain and to strengthen both cybersecurity and the integrity of the financial system.

The Action Plan underlined that financial technologies could bring significant benefits by simplifying supervisory procedures, improving access to finance, and enhancing financial inclusion. The need to protect investors and consumers was already recognised in this document as a key guiding principle of EU financial policy²⁹⁵.

In 2019, the European Markets and Securities Authority (ESMA) published a report on initial coin offerings and crypto assets, providing clarity on some aspects, such as legal basis and potential gaps²⁹⁶. In the report, ESMA specifies that although the size of the crypto-asset market remains relatively limited and does not constitute a threat to financial stability, it requires continuous monitoring. The Authority nonetheless expresses concern about the risks that crypto-assets may pose to investor protection²⁹⁷.

Most importantly, ESMA identified a potential gap in the existing EU financial services rules when crypto-assets do not qualify as MiFID financial instruments. Only a limited number of the crypto assets issued are likely to qualify as financial instruments. They generally fall outside the scope of existing EU financial services legislation. In such cases, investors are not afforded the safeguards provided by these rules. Moreover, investors may find it difficult to distinguish between crypto-assets that fall within the EU regulatory framework and those that do not, particularly when both types are traded on the same platforms²⁹⁸.

In September 2020, the European Commission adopted the Digital Financial Strategy, providing a framework for future reforms in digital finance²⁹⁹. Among the four priorities identified by the European Commission, two specifically concern consumers and investors:

- The first priority is to address fragmentation within the Digital Single Market for financial services. The aim is to enable European consumers to access cross-border services more easily and to support European financial firms in scaling up their digital operations.³⁰⁰;
- The second priority is to ensure that the EU regulatory framework promotes digital innovation in a way that benefits consumers and enhances market efficiency. Distributed ledger technology (DLT) and artificial intelligence (AI)

²⁹⁵ Ibid. “Europe’s regulatory and supervisory frameworks should allow firms operating in the EU Single Market to benefit from financial innovation and provide their customers with the most suitable and accessible products. Such frameworks should also ensure a high level of protection for consumers and investors and ensure the resilience and integrity of the financial system”

²⁹⁶ European Securities and Markets Authority. (2019). *Initial Coin Offerings and Crypto-Assets*. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

²⁹⁷ The most significant of these risks are identified as arising from potential fraud, cyberattacks, money laundering, and market manipulation.

²⁹⁸ Ibid.

²⁹⁹ European Commission, (2020), Communication on a Digital Financial strategy for the EU, COM/2020/591 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591>

³⁰⁰ Ibid.

have the potential to improve financial services for both consumers and businesses. The regulatory framework should therefore ensure that such technologies are deployed responsibly and in accordance with EU values³⁰¹.

According to the European Commission, in the digital era, consumers and investors have access to a wider range of financial services, which are often more affordable and innovative. The use of interoperable digital identities facilitates remote and cross-border access to such products. However, feedback from the public consultation revealed broad agreement that as technology companies expand their presence in the financial sector, consumers may face additional risks, including the potential negative effects of reduced market competition³⁰².

The Digital Financial Strategy also focuses on risks, adopting for financial stability the principle of ‘same activity, same risk, same rules’, not because they are operated by technologies³⁰³.

The Digital Financial Strategy led to the adoption of three regulations:

- *Regulation 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology.*

This regulation allows for temporary exemptions from certain EU financial rules to enable innovation and test DLT-based solutions within a controlled environment (regulatory sandbox³⁰⁴). It serves as a transitional mechanism intended to inform future legislative adjustments, ensuring that DLT infrastructures can be progressively integrated into the broader financial system

- *Regulation 2023/1114 on markets in crypto assets (MiCAR).*

MiCAR governs crypto asset activities that extend beyond the strictly financial sector, encompassing transactions generally considered within the scope of private law³⁰⁵. Before MiCAR, many crypto-related transactions were outside any specific regulatory framework, leaving consumers unprotected. One of the regulations' objectives is to provide a legal framework for assets and operations not covered by existing legislation³⁰⁶. This gap prompted the introduction of

³⁰¹ Ibid.

³⁰² Ibid.

³⁰³ Zetzsche, D. A., Annunziata, F., Arner, D. W., & Buckley, R. P. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal*, 16(2), 203–225. <https://doi.org/10.1093/cmlj/kmab005>

³⁰⁴ Ibid. “While MiCA deals with crypto-assets (understood as ‘a digital representation of values or rights that can be stored and traded electronically’) the DLT Infrastructure Regulation will introduce a so-called ‘sandbox’ approach for DLT-based market infrastructures, allowing temporary derogations from existing rules to assist regulators’ gaining of experience”

³⁰⁵ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

³⁰⁶ *Market in crypto assets (MiCAR)*, European Parliamentary Research Service, PE 739.221, November 2022.

consumer protection rules to ensure transparency of information and impose operational limits on service providers.

- *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).*

The DORA Regulation aims to strengthen and harmonise cybersecurity requirements across the European financial sector. It also establishes specific risk management obligations concerning information and communication technologies (ICT). Starting from January 2025, the entities concerned will be required to comply with a set of obligations, including the adoption of an internal governance framework for ICT risk management, the implementation of ICT risk control and mitigation plans, and the conduct of testing activities based on a risk-oriented approach³⁰⁷.

The three regulations are closely interlinked, as they respond to the objectives set out in the Digital Finance Strategy and aim to ensure a coherent and comprehensive regulation of digital finance.

2.1 European Regulation on Crypto Assets and technological neutrality.

The DORA, MiCA and DLT Pilot Regime Regulations each have a specific operational scope and aim, depending on the case, either to establish a horizontal legislative framework (as in the case of DORA) or to fill existing regulatory gaps (as in the case of MiCA).

As previously noted, MiCA was adopted to address a legal gap, providing a comprehensive legislative framework for situations not covered by existing EU financial legislation. The new MiCA Regulation aims to create a controlled and organised ecosystem for crypto-assets transactions. The rules of the mentioned regulation are mostly directed to discipline the vigilance duties and the authorisation process. From 2025 onwards, the providers of crypto assets service disciplined by MiCAR should be authorised by the vigilance authorities of each Member State. The authorisation system aims to admit to the supply of crypto-assets services only the providers with the indicated requirements. The provision of such a system of authorisations will enable a more secure and controlled financial ecosystem.

However, the new regulation does not affect the discipline of legal relationships between providers and users. According to the principle of technological neutrality, crypto activities should be governed by existing regulations. Regulators should look beyond the technology itself and concentrate primarily on the functionality offered by a financial service³⁰⁸. According to recital 18 of Directive 2002/21/EC on a common

³⁰⁷ Chiamenti. (2023). *L'attuazione del Digital Finance Package a tre anni dalla proposta*. https://www.chiamenti.net/media/filer_public/4f/68/4f68c9bb-51e2-4d79-b88d-88a34d564156/newsletter-dora-n1-2023-004-1.pdf

³⁰⁸ M. Amstad (2019), *Regulating Fintech: Objectives, principles, and practices*, *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3491982>. “*Technology neutrality entails regulators looking through the technology and focusing mainly on the functionality that a financial service provides. For*

regulatory framework for electronic communications networks and services, the principle does not impose the adoption of any specific type of technology and allows for the implementation of proportionate measures to support specific services when justified³⁰⁹. Technological neutrality aims to avoid disruptions to the technological market selection process and discrimination in the usage of specific technologies³¹⁰.

This principle regards both internal law and European law.

For this reason, crypto-assets transactions qualified as financial services are disciplined by Directive 2014/65/EU on markets in financial instruments, Directive 2014/49/EU on deposit guarantee schemes, and Directive 2015/2366/EU on payment services in the internal market.

The principle of technological neutrality entails the application of a specific regulation considering the nature of the good and service, without considering the technology used. Existing regulation is so applicable to the decentralised operation, regarding the specific legal institute of reference. In general, the regulations applicable in general to crypto assets are:

- Directive 2014/49/EU on deposit guarantee schemes.
- Directive 2014/65/EU on markets in financial instruments (MIFID II).
- Directive (EU) 2015/2366 on payment services in the internal market.
- Regulation (UE) 2017/2402 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation.
- Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- Directive (EU) 2018/1673 on combating money laundering by criminal law.

example, with the onboarding of new clients, which is a key element in financial services, a technology-neutral regulation defines specific requirements regarding anti-money laundering, regardless of whether the on-boarding is done non-digitally at the classic bank counter or through a dedicated online solution.”.

³⁰⁹ Recital 8, Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services “*The requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified, for example digital television as a means for increasing spectrum efficiency.*”.

³¹⁰ Kamecke, U., & T. Korber. (2008). Technological neutrality in the EC regulatory framework for electronic communications: A good principle widely misunderstood. *European Competition Law Review*, 29(5), 330. https://koerber.jura.uni-koeln.de/sites/koerber/user_upload/Technological_neutrality_in_the_EC_.Kamecke-Koerber_ECLR08_29_5_330-339.pdf.

- Regulation 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology.
- Regulation 2023/1114 on markets in crypto assets (MiCA)

With particular regard to blockchain financial regulation, the principle of technological neutrality is stated by recitals 9 and 10 of DLT pilot regime³¹¹. Recital 9 specifies that references to a specific type of distributed ledger technology are to be avoided. Compliance with the principle of technology neutrality is also provided by MiCA Regulation for crypto-asset activities, including those falling outside the scope of financial services.³¹²

It follows that, in order to determine which regulatory framework applies, attention must be given to the type of activity, service, or asset involved rather than to the technology employed.

It is therefore important to clarify from the outset that the MiCA Regulation does not govern all operations involving crypto-assets, but only those that do not fall within the scope of financial services or products already regulated under the MiFID II Directive. In this context, MiFID II remains the main reference for financial activities, and crypto-asset service providers must comply with its provisions whenever their operations fall within its regulatory scope.

³¹¹ Paragraph 9, DLT Pilot regime “*Union legislation on financial services is intended to be neutral as regards the use of any particular technology over another. Therefore, references to a specific type of distributed ledger technology are to be avoided. Operators of DLT market infrastructures should ensure that they are able to comply with all applicable requirements, irrespective of the technology used*”.

³¹² Paragraph 9, Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

Area of Interest	Regulation
Financial products and banking operations	• Directive 2014/49/EU on deposit guarantee schemes. • Directive 2014/65/EU on markets in financial instruments (MiFID II). • Directive (EU) 2015/2366 on payment services in the internal market. • Regulation (EU) 2017/2402 laying down a general framework for securitization.
Crypto assets not included in the first category	• Regulation 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology. • Regulation 2023/1114 on markets in crypto assets (MiCA).
Crypto assets and criminal law	• Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. • Directive (EU) 2018/1673 on combating money laundering by criminal law.

Table 1: Overview of European Regulations Related to Financial Instruments and Crypto Assets

As anticipated, the principle of technological neutrality does not refer only to European law. This also results in the application of existing national legislation. In the next chapter, the analysis of this kind of application will be shown and explained in order to demonstrate the multidimensionality of the principle.

2.2 Markets in Crypto Assets Regulation. The rationale.

The most disruptive legislations on crypto assets are Regulation 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology and Regulation 2023/1114 on markets in crypto assets (MiCA).

The two legislative acts were adopted to fill a gap in regulation.

As anticipated the operations related to financial transactions, deposit guarantee schemes, and payment services in the internal market are in fact regulated by Directive 2014/65/EU on markets in financial instruments (MiFID II), Directive 2014/49/EU on deposit guarantee schemes and Directive (EU) 2015/2366 on payment services in the internal market, regardless of the value utilized.

The MiCA Regulation governs crypto activities that extend beyond the strictly financial sector, encompassing transactions generally considered within the scope of private law. Before MiCAR, many crypto-related transactions were outside any specific regulatory framework, leaving consumers unprotected.

One of the regulations' objectives is to provide a legal framework for assets and operations not covered by existing legislation³¹³. This gap prompted the introduction of consumer protection rules to ensure transparency of information and impose operational limits on service providers.

2.3 The regulation.

The Regulation 2023/1114 integrates uniform rules for the offer and trading of crypto assets. The regulation is based on specific principles: transparency and disclosure, supervision of providers by authorities, protection of clients and holders of crypto assets, and preventive action against insider dealing and market manipulation (Art. 1).

Article 2 illustrates the scope of the regulation and the field of application. In particular, the exclusion of financial services, deposits, funds, securisation positions, non-life or life insurance and some pension products is expressly stated. This confirms that products and services related to these activities fall outside the MiCAR and are covered by the above-mentioned legislation.

Article 3 provides for definitions of the object of regulation. The provision constitutes a decisive instrument for the interpreters since there was no legal European definition of such instruments and assets. In particular:

- a *distributed ledger technology* is a technology that enables the operation and use of distributed ledgers, which are information repository that keeps records of transactions and that are shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism;
- the *consensus mechanism* consists of the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated;
- the *crypto asset* is a digital representation of a value or of a right that can be transferred and stored electronically using distributed ledger technology or similar technology
- the *crypto-asset service provider* is a legal person whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59.

The norm also brings clarity to the activities that belong to the category of crypto asset services. In particular, there are included: the provision of custody and administration, the management of the platform, the exchange of crypto assets with funds or other crypto assets, execution of orders for clients, and other services such advice provision, management and transfer services of crypto assets.

³¹³ European Commission. (2021). *Market in Crypto Assets (MICA)*, cit.

2.4 Categories of tokens.

The regulation identifies three types of crypto assets: (1) asset-referenced tokens (ART), (2) electronic money tokens (EMT) and crypto-assets other than asset-referenced tokens or e-money tokens, ensuring a legal framework also for values not included in the traditional definitions (Articles 3 and 4). In particular, the Regulation mentions and defines different values:

- **Asset-referenced token (ART)** is a type of crypto-asset that is not an electronic money token and that aims to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies (Art. 3 n.6).
- **Electronic money token or e-money token (EMT)** is a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency (Art. 3 n.7).
- **Utility token** is a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issue (Art. 3 n. 9).
- **Crypto-assets other than asset-referenced tokens or e-money tokens:** the category refers to crypto assets that are not included in the mentioned categories. The norm constitutes the extrema ratio of the system and aims to prevent gaps in regulation.

The regulation provides specific requirements to allow offers to the public and admission to trading. In particular, providers should publish a white paper of the service offered. The document shall contain specific information about the company, the project, the obligations, the technology used, and the risks arising from the operations. The regulation aims to guarantee transparency and fairness of the operations to enhance consumer protection.

The Regulation does not expressly refer to *stablecoins*, but the two main categories it introduces, *Asset-Referenced Tokens* (ART) and *E-Money Tokens* (EMT), can both be considered to encompass them. Moreover, the legislative act does not provide an explicit list of token types but instead defines their characteristics. From this, it follows that *stablecoins* may fall within either category, depending on whether they are pegged to a single official currency or to other assets, among which an official currency may also be included.

The scope and nature of the two categories become clearer when examined in light of the relevant recitals.

Asset-Referenced Tokens. An ART, by contrast, aims to maintain a stable value by referring to another value or a combination of values, which may also include official currencies. For a token to qualify as an ART, it is not required that its value be inherently stable, but rather that it purports to maintain stability³¹⁴. In addition, unlike

³¹⁴ Tomczak, T. (2022). Crypto-assets and crypto-assets' subcategories under MiCA Regulation. *Capital Markets Law Journal*, 17(3), 365–382. <https://doi.org/10.1093/cmlj/kmac008>

EMTs, ARTs are linked to other assets or rights beyond a single fiat currency. EMTs, instead, must always be tied to a specific and stable official currency.

Recital 18 further clarifies that this category was introduced to prevent regulatory circumvention and to ensure that the Regulation remains future-proof, avoiding gaps that might otherwise leave certain types of crypto-assets outside the scope of regulation. Most stablecoins currently fall into this category³¹⁵.

E-Money Tokens. Recital 18 explains that the first category includes crypto-assets that seek to maintain a stable value by referring to a single official currency. An EMT is a crypto-asset that seeks to maintain a stable value by referring exclusively to an official currency. Their function is similar to that of electronic money as defined in Directive 2009/110/EC. Like electronic money, these crypto-assets act as digital substitutes for coins and banknotes and are primarily intended to be used for payment purposes. EMTs, precisely because they are linked to a stable and official value, can effectively be used as a means of exchange, as they refer to the value of a fiat currency with legal tender status³¹⁶.

Utility tokens. Utility tokens confer to their holders certain rights or access privileges within a company's ecosystem, products, or services. They may also entitle users to participate in the governance of the issuing entity (e.g. right of voting). In many cases, these tokens function similarly to prepaid licences or crowdfunding mechanisms³¹⁷. Unlike traditional securities or financial instruments, utility tokens are not designed to generate future cash flows; rather, their primary purpose is to facilitate functional engagement and interaction within a blockchain-based environment³¹⁸.

Crypto-assets other than asset-referenced tokens or e-money tokens. The third category encompasses all crypto-assets that do not qualify as asset-referenced tokens (ARTs) or e-money tokens (EMTs). This residual group ensures that MiCAR applies comprehensively to all crypto-assets not otherwise covered, thereby avoiding regulatory gaps. Under Title II of the Regulation, these crypto-assets are defined as digital assets that are neither ARTs nor EMTs, nor otherwise excluded from MiCAR's scope pursuant to Article 2(4). From 30 December 2024, the provisions of Title II will apply directly to issuers and offerors of such tokens, as well as to persons seeking their admission to trading on a trading platform.

Issuers and offerors of crypto-assets under this category are subject to specific obligations, including³¹⁹:

³¹⁵ Martino, E. D. (2022). Regulating Stablecoins as Private Money. A Critical Take on the EU Proposal between Liquidity and Safety. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4203885>

³¹⁶ Delfini, F. (2022). Le discipline a tutela del consumatore e il coordinamento con la proposta di Regolamento MiCA. *Osservatorio Del Diritto Civile E Commerciale*, 267–294. <https://doi.org/10.4478/106711>

³¹⁷ Zetzsche, D. A., Annunziata, F., Arner, D. W., & Buckley, R. P. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy, cit.

³¹⁸ Ibid.

³¹⁹ <https://www.centralbank.ie/regulation/markets-in-crypto-assets-regulation?utm>

- Notification of the crypto-asset white paper to the competent authority prior to any public offer or admission to trading (Article 8 MiCAR);
- Compliance with requirements on marketing communications, which must be fair, clear, and not misleading (Article 7 MiCAR);
- Observance of conduct of business rules, ensuring honesty, fairness, and professional diligence (Article 14 MiCAR); and
- Liability for the accuracy and completeness of information contained in the white paper (Article 15 MiCAR).

2.5 Main provisions of MiCAR.

MiCAR regulates the crypto asset sector by imposing a series of obligations on service providers. These duties and obligations can be divided into categories. In particular³²⁰:

Authorisation regime. Both ARTs and EMTs are subject to an authorisation process. Only legal entities established within the European Union and holding a specific licence are permitted to issue ARTs or EMTs. To obtain such authorisation, the issuer must submit to the competent authority comprehensive documentation regarding its legal form and governance structure, as well as evidence demonstrating the suitability and integrity of its management and controlling shareholders³²¹. With regard to ARTs, these may be issued only by legal persons established in the EU and duly authorised by the competent authority (Article 16). EMTs, by contrast, may be issued exclusively by credit institutions or electronic money institutions (Article 48). The authorisation may be revoked by the competent authority if the issuer no longer fulfils the applicable requirements.

Disclosure obligations. The Regulation imposes specific periodic reporting obligations on ART issuers when the aggregate value of the issued tokens exceeds a certain threshold (Article 22).

Civil liability and duty of care. The Regulation establishes the civil liability of ART and EMT issuers for any information provided in the white paper that is incomplete, unclear, inaccurate, or misleading (Articles 26 and 52). Any exclusion or limitation of liability is considered legally void. The burden of proof, however, lies with the token holder. Moreover, ART issuers are subject to a specific duty of diligence: operators must act honestly, fairly, and professionally in the best interests of their clients (Article 27). The same standards of diligence apply to marketing communications, both for ARTs and EMTs, in relation to public offerings.

³²⁰ Alcorta, J. G. (2025). Regulating stablecoins in the European Union. Asset-Referenced tokens and E-Money tokens. In *Law, governance and technology series* (pp. 147–176). https://doi.org/10.1007/978-3-031-74889-9_7

³²¹ Martino, E. D. (2022). Regulating Stablecoins as Private Money. A Critical Take on the EU Proposal between Liquidity and Safety. Cit.

Holder's right to reimbursement. Token holders are entitled to request the redemption of their tokens at any time. The redemption procedures must be clearly set out and communicated in advance, and no fees may be charged for the reimbursement.

Publication of a white paper. One of the essential prerequisites for admission to trading is the publication of a white paper containing specific information. For ARTs, the white paper must include details such as the issuer's identity, governance structure, the rights and obligations of token holders, the stabilisation mechanism, the reserve policy, the associated risks, and complaint-handling procedures. The white paper must be approved by the competent authority of the Member State before publication.

Regime for marketing communications. Issuers and offerors must ensure that all marketing communications are fair, clear, and not misleading, and that they remain consistent with the information contained in the approved white paper.

Requirements for the investment of funds. ART issuers must maintain own funds amounting to at least EUR 350,000, 2% of the average amount of the reserve assets, or one quarter of the fixed overheads of the preceding year, whichever is higher. Of particular importance is the obligation to hold a reserve of assets that adequately covers both the risks associated with the specific activity referenced by the token and liquidity risks. Such reserves may only be invested in highly liquid financial instruments with minimal market, credit, and concentration risks.

3. The pilot regime for market infrastructures based on distributed ledger technologies.

Regulation 2022/858 - on a pilot regime for market infrastructures based on distributed ledger technology - represents an effort to align token emission model with market legislation.

The DLT Pilot Regime is a regulatory sandbox, allowing authorised financial operators to develop and operate infrastructures for the issuance and trading of tokenised financial instruments (security tokens). This entails temporary exemptions from certain existing rules, including those laid down in the MiFID II Directive and the CSDR Regulation. Such exemptions may concern requirements related to market access and intermediation, transaction reporting obligations, and the participation of entities that do not fall within the traditional categories established by MiFID II or CSDR.

The Regulation addresses the need to make the EU legal framework technology-neutral, allowing the development of a market for financial instruments issued using DLT, which would otherwise be hindered by existing regulatory constraints³²².

The regime is initially set for a three-year period (2023–2026), which may be extended up to six years (2023–2029). At the end of this period, the European Commission will

³²² Chiomenti. (2023). *L'attuazione del Digital Finance Package a tre anni dalla proposta*, cit.

assess its outcomes and decide whether to establish the framework as a permanent part of EU financial legislation.

The emergence of new contract structures based on DLTs and automated transactions has raised both practical and interpretive challenges, as MiFID II was not designed to address such unique financial configurations. This new regulation complements MiCA Regulation and MiFID II directive by establishing a legal framework for financial products associated with distributed ledger technologies (DLTs). For this purpose, Article 18 modifies Article. 4, paragraph 1, point (15); the MiFID II's definition of financial instruments includes now expressly instruments issued by distributed ledger technology.

The Regulation contains exemptions from the MiFID II regulation in order to ensure an adequate adaptation of legislative action of financial instruments to the digital era. The pilot regime also aims to promote the development and competitiveness of such technologies. The exemptions to financial regulation allow providers to foster the usage and advancement of such technologies, guaranteeing investor's protection. The primary scope of the European legislator is in fact promoting the expansion and progression of such activities and testing the decentralised infrastructures in the market. The Regulation provides for an authorization system less rigorous than the one required by Regulation 909/2014 and Directive 2014/65/UE. The infrastructures included in the regulation are:

- DLT multilateral trading facilities (DLT MTF): a multilateral trading facility that only admits to trading DLT financial instruments (Art. 2, n. 6).
- DLT settlement systems (DLT SS): a system that settles transactions in DLT financial instruments against payment or against delivery, irrespective of whether that settlement system has been designated and notified in accordance with Directive 98/26/EC, and that allows the initial recording of DLT financial instruments or allows the provision of safekeeping services in relation to DLT financial instruments (Art. 2, n.7)
- DLT trading and settlement systems (DLT TSS): DLT MTF or DLT SS that combines services performed by a DLT MTF and a DLT SS (Art. 2, n.10);

4. Conclusions.

In this chapter, the main legislative developments of recent years concerning crypto-asset regulation have been presented, with particular reference to the three key instruments that form the new European framework: the Markets in Crypto-Assets Regulation (MiCA), the Distributed Ledger Technology (DLT) Pilot Regime, and the Digital Operational Resilience Act (DORA).

The adoption of these regulations reflects the European Union's objective to create a coherent legal environment that both promotes the internal market and ensures robust safeguards against market and consumer risks.

This chapter has focused primarily on the MiCA Regulation, which in the coming years is expected to become the main compliance model for all issuers of the tokens defined within it. The Regulation introduces a comprehensive set of obligations for service providers, including the requirement to obtain prior authorisation, publish a detailed white paper, act with transparency and diligence towards clients, maintain reserve assets, and comply with ongoing disclosure and reporting duties.

As discussed, the ultimate aim of MiCAR is to establish a unified regulatory framework that protects consumers and investors while simultaneously enhancing the Union's competitiveness in the capital and financial markets sector. The Regulation primarily targets stablecoins. Although the term is not explicitly used, both Asset-Referenced Tokens (ARTs) and E-Money Tokens (EMTs) fall within this category.

However, MiCAR expressly excludes from its scope crypto-asset services that are provided in a fully decentralised manner without any intermediary³²³. Recital 22 states that where crypto-assets have no identifiable issuer, they should not fall within the Regulation's scope. This exclusion may raise questions regarding the applicable legal framework, especially in cases where Bitcoin is used not for financial purposes but for other types of activities.

The Regulation also excludes non-fungible tokens (NFTs), which are defined as unique and non-interchangeable crypto-assets representing ownership or rights over a specific item or asset.

This analysis has also highlighted the increasingly important role of both national and European supervisory authorities, which are responsible for conducting periodic and targeted assessments of operators' conduct and compliance with MiCAR requirements. The Regulation strengthens oversight powers, granting authorities the ability to intervene, revoke authorisations, and impose sanctions where breaches occur.

MiCAR undoubtedly represents a significant step forward in regulating crypto-asset activities and in preventing systemic and consumer risks. The establishment of compliance requirements and the attribution of supervisory powers contribute to a more secure and transparent market environment.

Nevertheless, the Regulation's highly detailed and technical nature may make it difficult for consumers to fully understand their rights. A user who falls victim to fraud or interacts with a non-compliant provider may struggle to assess the extent of their exposure. Furthermore, the inclusion of civil liability and information duties, already enshrined in most national legal systems, may appear somewhat redundant.

Overall, MiCAR marks an important milestone in the evolution of EU digital finance regulation. Yet it remains not fully aligned with the practical needs of consumers, who continue to face limited avenues for redress in case of harm. The provision that places the burden of proof on the holder of crypto-assets, rather than on the issuer or service

³²³ Annunziata, F. (2023). An overview of the markets in Crypto-Assets Regulation (MiCAR). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4660379>

provider, could also represent a disproportionate obstacle to the effective exercise of consumer rights.

Chapter 5 - Crypto assets in Commercial and Private and Criminal Italian law.

0.1. Introduction. - **0.2.** Methodology. - **0.3.** Lexicon and acronyms. - **0.4.** Chapter outline: contents and division. - **0.5** Implementation of European Regulation at the Italian level. - **1.** The judgment of the Italian Corte di Cassazione. – **1.1** Corte di Cassazione’s decisions on cryptocurrencies. – **1.2** Cassazione penale, sez. II, 17/09/2020, n. 26807. - **1.3** Cassazione penale, sez. II, 10/11/2021, n. 44337. - **1.4** Cassazione penale, sez. II, 26/10/2022, n. 44378. - **1.5** Legal considerations. - **2.** Italian merit case law on cryptocurrencies. - **2.1.** The “in-kind” contribution of crypto assets (Tribunale di Roma, n. 7932/2022). - **2.1.1.** A key precedent on cryptocurrencies contribution. Tribunale di Brescia n. 7556/2018 and Corte d’Appello di Brescia n. 207/2018 - **2.2.** The qualification of cryptocurrency deposits as regular or irregular as a requirement to declare bankruptcy. Tribunale di Firenze n. 18/2019 - **2.3.** Consob sanctions ex art. 94 TUF. Why is an energy token a financial instrument? Corte di Appello di Roma n. 5866/2023.- **2.4** Legal considerations. – **3.** Conclusions.

0.1. Introduction.

As shown in the previous chapter, applying the principle of technological neutrality is fundamental to ensuring technological progress and the consistency of law interpretations. This final analytical chapter builds upon the findings of the earlier sections by observing how theoretical and regulatory constructs translate into judicial interpretation and enforcement. The principle has a dual dimension. On the one hand, the principle is directed towards the legislator, who should not regulate a matter based on the specific technology employed but rather with regard to the type of activity or asset concerned. The legislator must therefore remain neutral towards the technology used, so as not to hinder its development. On the other hand, the principle also applies to those who interpret and enforce the law.

With particular regard to blockchain financial regulation, the principle of technological neutrality is stated by paragraphs 9 and 10 of the DLT pilot regime³²⁴. In recital 9, it is specified that references to a specific type of distributed ledger technology are to be avoided. The compliance with the principle is also provided by MiCA Regulation³²⁵ for transactions falling outside financial services³²⁶.

³²⁴ Paragraph 9, DLT Pilot regime “*Union legislation on financial services is intended to be neutral as regards the use of any particular technology over another. Therefore, references to a specific type of distributed ledger technology are to be avoided. Operators of DLT market infrastructures should ensure that they are able to comply with all applicable requirements, irrespective of the technology used*”.

³²⁵ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

³²⁶ Paragraph 9, Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

The application of technological neutrality also implies that contracts and legal relations arising from the use of crypto assets are subject to the existing rules of the legal system of belonging. Legal operators - both judges and lawyers - should subsume the practice case into a legal institution to apply the law. In particular, the principle represents a challenge to judges to determine what the law governs and its field of application³²⁷. This interpretational activity is not always easy to practice.

With regard to Italian law, Art. 41 of the Constitution states the principle of freedom of economic initiative for private individuals³²⁸. Contractual parties are free to enter into legal transactions that affect their financial sphere. The principle of contractual autonomy is also expressly recognized in Article 1322 of the Civil Code. The parties may choose the contractual scheme they prefer, except for the necessity to respect statutory limitations. Parties may also adopt atypical contractual arrangements, provided that they pursue interests worthy of protection³²⁹.

The principles of technological neutrality and contractual autonomy entail the subsumption of crypto assets transactions into the discipline of private and commercial Italian law. On the other hand, specific limitations and requirements apply when such transactions fall within the category of financial operations. The national courts shall then apply the Italian and European legislation to solve cases arising on such matters.

In this regard, the courts addressed the first case laws involving crypto-assets. The interpretative challenges are significant. As the case law analysis revealed, it could be difficult to determine whether some institutes find applications. Indeed, the legal nature of a transaction is not always clear. The interpreter must, therefore, rely on the general principles of law to identify the applicable legal institutes.

In light of these principles, it is essential to examine how Italian courts have concretely applied existing legal frameworks to disputes involving crypto-assets. This approach directly tests, in practice, the adequacy of the European and national frameworks analysed in Chapter 4, thereby closing the analytical loop that began with the

³²⁷ Greenberg, B. A. (2015), *Rethinking technology neutrality*. Minnesota Law Review, 100, 1495 (p. 1529).

³²⁸ Art. 41 Cost. Original version: “*L’iniziativa economica privata è libera.*

Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana.

La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali e ambientali”.

³²⁹ Cfr. Galgano, F. (2002) voce *Negozio Giuridico (Diritto Privato)*, in Enc. Del diritto, vol. XXVII, Giuffrè, Milano, pag. 934.; Gazzoni, F. (1987), *Manuale di Diritto Privato*, Edizioni Scientifiche Italiane, Napoli, 1987, p. 713. Scognamiglio, R. (1970), *Dei Contratti in Generale. Libro IV, artt. 1321-1352*, in Commentario del Codice civile Scialoja Branca, Zanichelli, Bologna, p. 24. Bianca, C. M. (1987), *Diritto Civile*, III, Il Contratto, Giuffrè, Milano, p. 31. Mirabelli, G. (1980), *Dei contratti in generale*, in Comm. Utet, Torino. Carresi, F. (1987), *Il contratto*, in Trattato Cicu Messineo Mengoni, Milano. Trabucchi, A. (1982), *Il contratto come fatto giuridico. L'accordo, l'impegno*, in Studi in onore di Oppo, Padova. Cataudella, A. (2000) *I contratti, Parte generale*, Torino. Roppo, V. (2006), *Trattato del contratto*, Vol. 7, Milano. Gallo, P. (2000) *Trattato del contratto*, Vol. 3, Torino.; Galgano, F. (2011) *Il contratto*, Padova. Roppo, V. (2011) *Il contratto*, Milano, 2011; Betti, E. (1943), *Teoria generale del negozio giuridico*, Napoli.

identification of consumer risks in Chapter 3. In this regard, the following research question and sub-research question have been elaborated:

- *What are the main issues related to crypto-asset transactions in the Italian courts?*
- *What is the interpretation adopted by judges in the decisions?*

These questions form the foundation of the present chapter, which aims to answer them by analysing how Italian courts - especially the Corte di Cassazione and lower merit courts - approach disputes involving cryptocurrencies. By examining the interpretative approaches and the legal qualification of crypto-asset transactions, this chapter offers insight into the practical challenges of integrating new technologies into the traditional legal framework.

The objective of this chapter is to examine how the Italian judicial system approaches crypto-asset transactions through the principle of technological neutrality, with the aim of identifying the main issues that arise in practice for private individuals. To this end, some judicial decisions will be presented and discussed to show how Italian case law has attempted to incorporate these innovative transactions into the field of private and financial law.

From this chapter it will emerge that the risks consumers face in relation to cryptocurrencies are not limited to those examined by empirical literature, but also include those revealed through the analysis of court decisions. In particular, the courts – especially courts of first instance – provide an effective lens through which to understand the risks that arise both legally and in practice.

0.2. Methodology.

The methodology³³⁰ adopted consists of an analysis of selected decisions issued by Suprema Corte di Cassazione and Italian Courts of merit. In particular, the judgements are selected using two databases: DeJure (<https://dejure.it>)³³¹ and Banca Dati di Merito (<https://bdp.giustizia.it>)³³². DeJure is a legal information system containing judgments, commentaries and articles. Banca Dati di Merito is the official portal for Italian judgments on merits. It contains civil judgments, decrees and orders from 01/01/2016 to the present³³³.

This chapter adopts a primarily descriptive methodological approach, aimed at analysing how Italian courts apply existing legal frameworks to crypto-asset transactions. By systematically examining judicial decisions, the analysis seeks to clarify the interpretative trends and legal qualifications attributed to these emerging technologies. In addition, the chapter introduces a classifying dimension by identifying recurring legal categories applied by courts, thereby highlighting patterns in case law.

³³⁰ Kestemont, L. (2018). Handbook on legal methodology: from objective to method. Intersentia. (Classification angle: national legal system)

³³¹ <https://dejure.it>

³³² <https://bdp.giustizia.it>

³³³ Banca Dati di Merito does not include measures on family, children and personal status.

Where relevant, brief evaluative reflections are provided to assess the coherence and practical legal implications of these judicial interpretations³³⁴.

The choice fell on the Italian legal system since the database of decisions is highly advanced, and it has been possible to select a broad range of cases. Banca Dati di Merito has in fact 85 judgements under the word “criptovaluta”. The presence of a relevant number of decisions is an index of the wide use and diffusion of crypto assets. The judgments’ objects are various and cover a fair number of private law institutes. In the decisions, judges faced legal issues that reflected the difficulty of interpreters in reconducting transactions in crypto assets to civil law institutes.

0.3. Lexicon and acronyms.

The terms utilised to indicate Italian legislation, decisions and tribunals will be the Italian ones. The translation in English of Italian juridical terminology does not guarantee accuracy and exact correspondence. For this reason, a translation and explanation of the terms and acronyms utilised will be hereby explained.

Legislative acts:

- Legge (l.): lit. *law*. The law is the primary legislative source of the Italian legal system and holds the status of a primary norm. Laws are enacted by Parliament following the procedure established by Articles 70 and seq. of the Italian Constitution³³⁵. Once approved by one chamber, every bill must be approved in the same wording by the other. If amendments are made, they must also be approved by the other chamber.
- Decreto legislativo (d.lgs): lit. *legislative decree*. A legislative decree is a normative act with the force of law issued by the Government based on a delegation of legislative power from Parliament. This delegation occurs through a legge delega (lit. delegation law), which sets specific guidelines, principles, and timeframes within which the Government must legislate. Once drafted, the legislative decree is approved by the Council of Ministers and signed by the President of the Republic before becoming law³³⁶.
- Decreto legge (d.l): lit. *law decree*. A law decree is an urgent legislative act issued directly by the Government in situations of necessity and urgency. It has immediate legal effect upon publication but must be converted into law by Parliament within 60 days, or it automatically loses effect. law decrees are used

³³⁴ Kestemont, L. (2018). Handbook on legal methodology: from objective to method. Intersentia,

³³⁵ Art. 70 et seq. Cost.

³³⁶ Art. 76 Cost. Original version: “L’esercizio della funzione legislativa non può essere delegato al Governo se non con determinazione di principi e criteri direttivi e soltanto per tempo limitato e per oggetti definiti.”

to address emergencies or situations requiring immediate regulatory intervention³³⁷.

- Testo Unico Finanziario (TUF): lit. *consolidated law on finance*. The consolidated law on finance is a comprehensive legislative framework that incorporates most of the primary financial regulations enacted in recent decades. It streamlines and harmonizes these regulations, ensuring their compatibility with the broader framework of EU financial market rules.
- Codice Penale (c.p.): lit. *Italian Criminal Code*.
- Codice di Procedura Penale (c.p.p.): lit. *Italian Procedural Criminal Code*.
- Codice Civile (c.c.): lit. *Italian Civil Code*.

Courts:

- Tribunale: Court of first instance. First-instance trial, where the judge examines and rules on a case on its merits for the first time.
- Corte d'Appello: Court of second instance. Appeal trial, where the judge re-examines and rules on the same case for the second time.
- Suprema Corte di Cassazione (or Corte di Cassazione): Supreme Court of Cassation. Judgment of legitimacy, meaning a review of the legality of previous trial levels, conducted before the Court of Cassation

Judicial decisions:

- Tribunale decision: e.g. Tribunale di Roma, n. 7932/2022.
- Corte d'Appello decision: e.g. Corte di Appello di Roma, n. 5866/2023.
- Suprema Corte di Cassazione decision: e.g. Cassazione penale, sez. II, 17/09/2020, n. 26807 or (simplified version) Cass. pen. n. 26807/2020.

0.4. Chapter outline: contents and division.

In this research some rulings have been selected to evidence the variety of the legal matters arising in courts and the interpretative decision adopted by them. The study will reveal that the application of existing legal institutes is possible. However, in some

³³⁷ Art. 77 Cost. Original Version “*Il Governo non può, senza delegazione delle Camere, emanare decreti che abbiano valore di legge ordinaria.*

Quando, in casi straordinari di necessità e di urgenza, il Governo adotta, sotto la sua responsabilità, provvedimenti provvisori con forza di legge, deve il giorno stesso presentarli per la conversione alle Camere che, anche se sciolte, sono appositamente convocate e si riuniscono entro cinque giorni.

I decreti perdono efficacia sin dall'inizio, se non sono convertiti in legge entro sessanta giorni dalla loro pubblicazione. Le Camere possono tuttavia regolare con legge i rapporti giuridici sorti sulla base dei decreti non convertiti.”

cases, the uncertainty of the legal nature of crypto assets leaves legal questions unanswered. As will be discussed in the following paragraphs, the new regulation does not clarify some aspects related to the legal nature of crypto transactions. This aspect could interfere with the homogeneity of the decision adopted and with the trustworthiness of investors in crypto assets.

The first part of the chapter is dedicated to the analysis of the decisions adopted by Suprema Corte di Cassazione: the Italian court of last resort for legal issues. Corte di Cassazione is the highest court in the ordinary jurisdiction. Among its various functions, it ensures the correct application and uniform interpretation of the law, the consistency of national objective law, and compliance with the limits of different jurisdictions³³⁸. It serves a nomophylactic function in interpreting national law³³⁹.

This analysis will therefore examine whether the Court of Cassation has issued any legal definitions concerning cryptocurrencies.

In particular, the following decisions will be analysed:

- Cassazione penale, sez. II, 17/09/2020, n. 26807.
- Cassazione penale, sez. II, 10/11/2021, n. 44337.
- Cassazione penale, sez. II, 26/10/2022, n. 44378.

The decisions concern the criminal law sector. However, since this analysis concerns Private law, only Financial and Private law aspects will be dealt with. In particular:

- 1) the first decision concerns an order of preventive seizure for unauthorised financial activity under Art. 166 paragraph 1, letter c) TUF. For the application of the norm, it is necessary to determine whether cryptocurrencies are means of payment or financial products.
- 2) The second decision regards the probationary seizure of a website considered as corpus delicti and assets related to the offence. The decision concerns the application of financial crimes regulation when a virtual currency works as an investment instrument.
- 3) The third decision concerns an online fundraising campaign explicitly advertised as an investment offering. In particular, whether the Initial Coin Offering (ICO) could be classified as an offer of investment services or activities.

For every decision an explanation of the judgement will be provided. A table will illustrate the interpretative statements (*massime*) adopted by the judges of the court, in order to have a complete knowledge of the principles adopted by the jurisprudence in the Italian legal system.

³³⁸ Art. 65, legge fondamentale sull'ordinamento giudiziario del 30 gennaio 1941 n. 12.

³³⁹ Carratta, A. (2006). La riforma del giudizio in Cassazione. In Riv. trim. dir. proc. civ. (p. 1117).

It should be premised that all the decisions have been adopted before the enforcement of the MiCA Regulation³⁴⁰, the DLT pilot regime and the d.lgs. n. 129/2024³⁴¹. Then, the definitions provided do not consider the ones affirmed in the new European regulation. Interpretation is based only on the existing regulation at the time and demonstrates the interpretative issues arisen in the field of Private and Financial law.

The second part will analyse cases of merits case law of the first and second instance Italian merit courts. Courts of merit have jurisdiction to judge both questions of law and fact. The judgments examined will therefore also contain the evaluation of factual elements, relevant to the definition of legal cases.

In particular, the following decisions will be analysed:

- Tribunale di Roma, n. 7932/2022.
- Tribunale di Firenze, n. 18/2019.
- Corte di Appello di Roma, n. 5866/2023.

The decisions concern specific sectors of private and company law. In particular:

- 1) The first judgment refers to the qualification of crypto assets' contributions as in-kind ones. Such a qualification is necessary to determine if a contribution of crypto assets is admitted by the Italian legal system.
- 2) The second decision regards the qualification of a cryptocurrency deposit contract as regular or irregular. The inclusion in the second category is in fact necessary to declare the bankruptcy of a company.
- 3) The last case law analysed concerns the application of a sanction for missing publication of the informative prospectus in case of public offer. The decision presents interpretative criteria to determine if a token is a financial instrument or not.

The analysis of these cases will reveal the complexity and the variety of possible questions arising in the financial technology sectors.

³⁴⁰ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

³⁴¹ Decreto Legislativo n. 129 del 5 settembre 2024. The decree designates Consob and Banca d'Italia as the authorities responsible for enforcing the regulation. Each authority will have a specific role based on its area of expertise. Consob will apply the rules in Title II of Regulation (EU) 2023/1114, which govern crypto-asset market operators, with a focus on investor protection and market transparency. Banca d'Italia is responsible for enforcing Title IV, which focuses on financial system stability and managing risks associated with crypto-assets. For Title III, which covers trading platforms and crypto-asset service providers, Consob and the Bank of Italy will work together to ensure effective oversight. Franza E., Attuazione del MiCA, le novità del decreto 129/2024, <https://www.dirittobancario.it/art/attuazione-mica-le-novita-del-decreto-129-2024/#:~:text=protezione%20degli%20investitori,Il%20Decreto%20Legislativo%20n.,in%20base%20alle%20rispettive%20competenze>.

0.5 Implementation of European Regulation at the Italian level.

Before starting the analysis of the decision concerning crypto assets, a mention of the implementation measures adopted in Italy must be made. These implementations do not directly affect the decision adopted by judges, but they give an idea of the measures adopted and the roles that national authorities will cover in the coming years.

The European regulation on crypto assets have been implemented at the Italian national level. Regarding the Italian legal system, particular attention should be given to decreto legge 2019, n. 34/2019³⁴² and decreto legislativo 129/2024³⁴³.

With d.l. 34/2019, the Italian government provided for the institution of an experimentation on FinTech activity. The government commissioned the Italian banking authority (Banca d'Italia), the Italian Markets Authority (CONSOB) and the Ministry of Economy and Finance (MEF) to define the conditions and modalities of procedures³⁴⁴ (art. 36, sub. 2-bis. et seq., d.l. 34/2019). According to the regulation, the admission of companies allows a derogation from the guidelines and general acts of the supervisory authority. Indeed, the decree provides for the institution of a committee on Fintech, responsible for defining programs and projects on financial technologies, and for legislative projects aimed at promoting the encounter between business operators and institutions.

The Ministry of Economy and Finance published an implementing decree regulation, providing the necessary measures of implementation³⁴⁵. The regulation defines FinTech as service and product innovation activities in banking, finance and insurance through new technologies. Decreto ministeriale 100/2021 identifies the application area of the regulatory sandbox and the eligibility conditions. Currently, three projects have been admitted to the regulatory sandbox and are registered on the website of the Ministry of Economics and Finance.

Lastly, decreto legislativo 129/2024 adapted the national legal system to MiCA Regulation. In particular, the regulation designated Banca d'Italia and the Italian Markets Authority (CONSOB) as the competent authority to define the technical implementation of the European regulation. In particular, the mentioned authorities have supervisory and investigative powers (art. 4). Such powers are described in Art. 94 of Regulation 2023/1114 and includes the suspension or the prohibition of the financial activity in case of reasonable grounds for suspecting the infringement of the Regulation. The authorities also have regulatory power (art. 5). Banca d'Italia and

³⁴² Decreto-legge 30 aprile 2019, n. 34. Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi.

<https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019;34-art35>

³⁴³ Decreto legislativo 5 settembre 2024, n. 129. adeguamento della normativa nazionale al regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle crypto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

<https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-05;129>

³⁴⁴ Art. 36, sub. 2-bis. et seq., decreto-legge 30 aprile 2019, n. 34.

³⁴⁵ Decreto ministeriale 30 aprile 2021, n. 100.

<https://www.gazzettaufficiale.it/eli/id/2021/07/02/21G00109/sg>

CONSOB have the power to discipline the implementing provisions of the legislative decree, having regard to the guidelines and interpretation of European vigilance authorities. The power should be exercised in compliance with the principle of loyal cooperation.

1. The judgment of the Italian Corte di Cassazione.

Considering that the only decisions of Corte di Cassazione related to cryptocurrencies are the ones adopted in criminal law, it is necessary to provide a brief overview of the appeal to the criminal sections of the court.

Corte di Cassazione is a judicial body responsible for harmonising and coordinating the interpretation and application of laws to ensure a consistent evolution of case law³⁴⁶. Article 65 of the Judicial System³⁴⁷ states that the Court, as supreme judicial authority, guarantees the correct application and uniform interpretation of the law, the unity of national objective law, and compliance with jurisdictional boundaries. It also resolves conflicts of jurisdiction and competence and carries out other duties assigned by law³⁴⁸. Art 111 of the Italian Constitution establishes that an appeal to the Court of Cassation is always allowed in cases of a violation of the law³⁴⁹.

Article 568, paragraph 2, c.p.p. states that an appeal to Corte di Cassazione is always permitted for rulings in which the judge decides on personal freedom and for judgments that are not otherwise subject to appeal³⁵⁰. Therefore, appellate judgments and non-appealable judgments can be contested³⁵¹. However, procedural acts and non-final decisions cannot be appealed.

For the criminal sector, an appeal to the Court of Cassation is allowed only for the grounds listed in Art. 606 c.p.p.³⁵². In general, the appeal may be filed for the following

³⁴⁶ Luiso F.P., *Diritto Processuale Civile*, Vol. 2, p. 428, Giuffrè Editore, 2015.

³⁴⁷ Regio decreto 30 gennaio 1941, n. 12.

³⁴⁸ Regio decreto 30 gennaio 1941, n. 12.

³⁴⁹ Art. 111, paragraph 7, Cost. Original version: “*Contro le sentenze e contro i provvedimenti sulla libertà personale, pronunciati dagli organi giurisdizionali ordinari o speciali, è sempre ammesso ricorso in Cassazione per violazione di legge.*”

³⁵⁰ Art. 568, paragraph 2, c.p.p. Original version: “*2. Sono sempre soggetti a ricorso per cassazione [606], quando non sono altrimenti impugnabili, i provvedimenti con i quali il giudice decide sulla libertà personale e le sentenze [111 Cost.], salvo quelle sulla competenza che possono dare luogo a un conflitto di giurisdizione o di competenza a norma dell'articolo 28.*”

³⁵¹ Tonini P., *Manuale di procedura penale*, p. 955, Giuffrè Editore, 2018.

³⁵² Art. 606 c.p.p. Original version: “*1. Il ricorso per cassazione può essere proposto per i seguenti motivi: a) esercizio da parte del giudice di una potestà riservata dalla legge a organi legislativi o amministrativi ovvero non consentita ai pubblici poteri; b) inosservanza o erronea applicazione della legge penale o di altre norme giuridiche, di cui si deve tener conto nell'applicazione della legge penale; c) inosservanza delle norme processuali stabilite a pena di nullità, di inutilizzabilità, di inammissibilità o di decadenza; d) mancata assunzione di una prova decisiva, quando la parte ne ha fatto richiesta anche nel corso dell'istruzione dibattimentale limitatamente ai casi previsti dall'articolo 495, comma 2; e) mancanza, contraddittorietà o manifesta illogicità della motivazione, quando il vizio risulta dal testo del provvedimento impugnato ovvero da altri atti del processo specificamente indicati nei motivi di gravame.*

2. Il ricorso, oltre che nei casi e con gli effetti determinati da particolari disposizioni, può essere proposto contro le sentenze pronunciate in grado di appello o inappellabili. 2-bis. Contro le sentenze

reasons: (a) the judge exercised a power reserved by law to legislative or administrative bodies or exercised authority not permitted to public powers; (b) failure to observe or incorrect application of criminal law or other legal provisions that must be considered in applying criminal law; (c) Violation of procedural rules established under penalty of nullity, inadmissibility, inapplicability, or forfeiture; (d) Failure to admit decisive evidence, when a party requested it during the trial phase, but only in cases provided for by Article 495, par. 2, c.p.p.; (e) Lack, contradiction, or manifest illogicality of reasoning, when the defect is evident from the text of the contested ruling or other case documents specifically indicated in the grounds of appeal.

The three decisions analysed concern orders of preventive and probationary seizures. For these cases, Art. 325, paragraph 1, c.p.p. states that an appeal to the Court of Cassation is allowed only for violations of the law.³⁵³ The Court of Cassation's review in cases like these is much more limited compared to the general scope outlined in Article 606 c.p.p.. This restriction is due to the temporary nature of preventive measures. In fact, the effects of the seizure remain only if the confiscation of the seized items is ordered in the final conviction³⁵⁴.

In application of this legal provision, appeals based on grounds that go beyond a strict violation of the law are not admissible³⁵⁵.

1.1 Corte di Cassazione's decisions on cryptocurrencies.

According to the database DeJure, there are 29 decisions of Suprema Corte di Cassazione from 2020 to 2025 under the word "*criptovalute*" (lit. cryptocurrencies), all belonging to the criminal sector³⁵⁶. 14 interpretative legal statements have been elaborated for 6 of the 29 decisions adopted by the criminal sections of the court. This statement is called "*massima*" and represents one of the most important instruments to

di appello pronunciate per reati di competenza del giudice di pace, il ricorso può essere proposto soltanto per i motivi di cui al comma 1, lettere a), b) e c).

3. Il ricorso è inammissibile se è proposto per motivi diversi da quelli consentiti dalla legge o manifestamente infondati ovvero, fuori dei casi previsti dagli articoli 569 e 609 comma 2, per violazioni di legge non dedotte con i motivi di appello".

³⁵³ Art. 325, paragraph 1, c.p.p. Original version: "*1. Contro le ordinanze emesse a norma degli articoli 322 bis e 324, il pubblico ministero, l'imputato e il suo difensore, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione possono proporre ricorso per cassazione per violazione di legge*"

³⁵⁴ Art. 323, par. 1, c.p.p.

³⁵⁵ Cass. Pen. 44337/2021, Cass. Pen. 18951/2017. According to established case law and considering the references of Articles 355, par. 3, 324 and 325 c.p.p., an appeal to Corte di Cassazione against orders concerning probative seizures (just like those related to preventive seizures) is allowed only for violations of the law. This category includes both errors in judgment (*errores in iudicando*) and procedural errors (*errores in procedendo*), as well as as well as serious flaws in reasoning that render the justification of the ruling completely absent or lacking the minimum requirements of coherence, completeness, and reasonableness. If the reasoning is so deficient that it fails to make the judge's logical process understandable, an appeal may be allowed.

³⁵⁶

https://dejure-it.ezproxy.unibo.it/#/ricerca/giurisprudenza_lista_risultati?isCorrelazioniSearch=false

ensure the nomophylactic function of the court³⁵⁷. A “*massima*” is a concise statement of the legal principle affirmed by the court in a decision and constitutes the legal basis of the decision adopted. The principles are identified by Ufficio del Massimario: an office in charge to identify nomophylactic principles established in the decisions of the Court of Cassation. The purpose is to create the necessary conditions to ensure the widespread dissemination of legal principles. The process consists of multiple stages and culminates in the publication and online dissemination of the “*massima*”, making them accessible to the legal community.

There are no longer decisions adopted by the civil sections of Corte di Cassazione, related to private law institutes. This information is significant, considering that in the civil merit case law database (Banca Dati di Merito) there are 85 decisions registered. The data is probably related to the fact that Corte di Cassazione decides only on legal issues. This means that most of civil decisions regards the factual situation, whereas legal interpretation issues have arisen mostly regarding criminal law.

However, the decisions adopted, and the interpretative guidelines provided in such criminal judgements affects also civil law. Indeed, the crimes dealt with in these decisions often regard financial contracts. This means that the interpretation to be adopted must also refer to private and commercial law institutes. Therefore, the statements assessed in the judgements are relevant also for the private and commercial law sectors.

The decisions concern financial intermediation, securities market, and competition law. Non-compliance with financial regulations could result in financial crimes. Financial intermediation in the Italian legal system is disciplined by a decree: d.lgs. 24 febbraio 1998, n. 58 “*Testo unico delle disposizioni in materia di intermediazione finanziaria*”. The decree has legal force and is the result of the reorganization of Italian financial regulation, which took place in the context of the implementation of Directives 93/22/CEE³⁵⁸ and 93/6/CEE³⁵⁹. In recent decades, the European Union has acquired an increasing role in defining common financial rules for all member states, which has resulted in the amendment of many parts of the financial text³⁶⁰.

About this analysis, the decisions mainly concern the definition of financial investment and instrument, the institutions of the public offer and the obligations of the financial

³⁵⁷https://www.cortedicassazione.it/resources/cms/documents/SINTESI_CRITERI_DELLA_MASSIMAZIONE_CIVILE_E_PENALE.pdf

³⁵⁸Council Directive 93/22/EEC of 10 May 1993 on investment services in the securities field. The Directive is no longer in force and is repealed by Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC. The Directive is no longer in force and is repealed by Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance.

³⁵⁹ Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions.

³⁶⁰ Annunziata F., La disciplina del mercato dei capitali, Giappichelli, pp. 7-8, 2023.

operator. Failure to comply with these rules may constitute general offences (e.g. money laundering and self-laundering) or financial crimes (unauthorized financial practice). The use of cryptocurrencies for financial purposes raised questions about the inclusion of such a category in the operativity of financial regulation. As Cassazione's decisions reveal, the inclusion prescinds from the technological category of belonging.

The criteria followed in the illustration of cases are chronological and functional to highlight the connections between decisions. Only passages related to financial and private law regulation will be discussed since the analysis of criminal regulation issue would require a separate and deeper study. As it will result from the paragraphs, the cases are all related to the inclusion of the activity in the field of financial ones.

1.2 Cassazione penale, sez. II, 17/09/2020, n. 26807.

The first decision concerns an order of preventive seizure³⁶¹ of a sum of money and other assets directed to a person under investigation. The person is accused of multiple offences, including unauthorized financial activity under Art. 166, paragraph 1, letter c) of d.lgs. 58/1998 (TUF). The provision sanctions anyone who, without authorization, offers, promotes, or distributes financial products, financial instruments, investment services, or investment activities outside a registered office or through remote communication methods.

In the grounds for appeal, the defendant argued that, according to Article 1 of the TUF, payment instruments are not financial products but merely means of payment. As a result, they should not fall within the scope of financial regulations. Indeed, Article 1, paragraph 2 of the TUF expressly excludes payment instruments from being classified as financial instruments. Moreover, this interpretation is consistent with the European Court of Justice's preliminary ruling of October 22, 2015, which stated that Bitcoin serves no purpose other than as a means of payment³⁶².

The court rejected this interpretation. The reasoning for the seizure pointed out that the sale of cryptocurrencies (Bitcoin) was promoted as an investment opportunity. On the website, indications were provided to help potential investors consider whether or not

³⁶¹ Tonini P., *Manuale di procedura penale*, p. 955, Giuffrè Editore, 2018. In the Italian legal system, preventive seizure is regulated by Art. 321 et seq. c.p.p. Its purpose is to prevent an asset related to the crime from being used to worsen or prolong its consequences over time. In addition to preventive seizure, Italian law also provides for conservatory seizure and probative seizure. Conservatory seizure (Art. 316 c.p.p.) is a measure aimed at preventing the reduction or dissipation of the convicted person's financial guarantees. Probative seizure (Art. 253 et seq., c.p.p.) is a means of gathering evidence, allowing authorities to remove an asset from the possessor, regardless of ownership, if it is relevant to the investigation.

³⁶² Judgment of the Court (Fifth Chamber) of 22 October 2015. *Skatteverket v David Hedqvist*, C-264/14. *“It must be held, first, that the ‘bitcoin’ virtual currency with bidirectional flow, which will be exchanged for traditional currencies in the context of exchange transactions, cannot be characterised as ‘tangible property’ within the meaning of Article 14 of the VAT Directive, given that, as the Advocate General has observed in point 17 of her Opinion, that virtual currency has no purpose other than to be a means of payment.”* (par. 24) Link: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0264>

to join the financial initiative. Specifically, phrases were included suggesting that those who had invested in Bitcoin over two years had gained more than 97%.

As a result, the activity falls under the regulatory requirements set out in Article 91 and following of the TUF. Failure to comply with these obligations constitutes the offence outlined in Article 166, paragraph 1, letter c) of the TUF.

Two interpretative statements have been elaborated in the decision. The first one concerns the application of financial regulation to the sale of cryptocurrencies if promoted as investment opportunities. The activity of promotion can be deduced by factual elements such as a declaration on the website referring to the convenience of the operation and possible gains. The second statement is directly connected to the first one. If the product is qualified as financial, the seller is subject to the requirements Articles 91 et seq. of the TUF. The norms discipline financial issuers' activity and the failure to comply to such regulation constitutes the crime of unauthorized financial activity under Art.166, paragraph 1, letter c) of the TUF.

Decision	Interpretative statement (massima)
Cassazione penale, sez. II, 17/09/2020, n. 26807.	(1) The online sale of Bitcoin as a virtual currency is subject to financial instrument regulations. In the context of financial intermediation, the online sale of Bitcoin, when promoted as an investment opportunity for savers – providing them with information on the profitability of the initiative – is an activity subject to the regulatory requirements set forth in Articles 91 et seq. of the TUF. Failure to comply with these obligations constitutes the offense outlined in Art. 166, paragraph 1, letter c) of the TUF. (2) Cryptocurrencies: Sale promoted as an investment proposal and the crime of unauthorized financial activity. Cryptocurrencies (virtual currencies or Bitcoin) qualify as financial products when their sale is promoted as an investment opportunity. In such cases, since this activity falls under the regulatory requirements of the TUF, failure to comply constitutes the offense of unauthorized financial activity under Art. 166, paragraph 1, letter c) of the TUF (d.lgs. 58/1998).

The most relevant element in this decision is the qualification of cryptocurrencies as financial products instead of means of payment. The interpretation significantly impacts practice since it results in applying financial legislation.

1.3 Cassazione penale, sez. II, 10/11/2021, n. 44337.

The principles stated in the above decision have also been affirmed in another judgment. The case concerned the appeal of a website probationary seizure. In particular, the website was considered corpus delicti (body of evidence) and asset relevant to the offence, as it was used to advertise illegal activities and offer services to clients. These promotional tools were deemed essential for introducing electronic currency into circulation.

The defence counsel appealed the decision, arguing that the ruling violated Articles 91 and 166 of the TUF, Article 355 c.p.p., and, indirectly, Article 125 c.p.p. The defence

contested the lack of sufficient legal grounds to support the allegation of unauthorized financial activities and, therefore, the seizure.

Citing relevant case law, the defence emphasized that cryptocurrency sales are subject to financial regulations only when marketed as an investment. The Tribunal's reasoning, which equated Bitcoin with digital gold³⁶³, was insufficient to classify its sale as a financial investment under the law. Bitcoin was not the only available instrument for investing in digital gold. The defence stressed that cryptocurrencies are not financial instruments and thus do not fall under the scope of the TUF, except in limited cases where their sale is directly influenced by the promotional strategies employed by the seller.

The court clarified the definitions of virtual currency, which is defined in Directive (EU) 2018/843 as a *“digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically”*³⁶⁴. According to the Court, it is clear that the purpose of the directive is evidently to regulate the relationship between virtual currency and traditional currency, without precisely defining the phenomenon itself.

This definition is complemented by Recital 10 of the Directive, which states *“although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies”*³⁶⁵.

The Italian Legislator's definition can be found in Article 1 of d.lgs. 231/2007, as amended by d.lgs. 125/2019. The norm defines virtual currency as a digital representation of value that is neither issued nor guaranteed by a central bank or public authority. The virtual currency is not necessarily linked to a currency with legal tender and is used as a means of exchange for the purchase of goods and services or for

³⁶³ Gold tokenization is a process that converts the value of physical gold into digital tokens (also known as digital gold or crypto-gold), which can be traded on a blockchain. Each token represents a specific amount of gold. According to Maouchi, Y. et al. (2024) Gold-backed cryptocurrencies (GBCs) do not consistently act as a hedge against other digital assets analyzed. However, due to their low positive correlation, they can provide diversification benefits for investors with digital asset portfolios. Lastly, GBCs vary in their role as a safe haven, shifting between weak and strong protective behavior depending on market conditions. Maouchi, Y., Fakhfekh, M., Charfeddine, L., & Jeribi, A. (2024). Is digital gold a hedge, safe haven, or diversifier? An analysis of cryptocurrencies, DeFi tokens, and NFTs. *Applied Economics*, 56(60), 9158–9173. <https://doi-org.ezproxy.unibo.it/10.1080/00036846.2023.2299217>.

³⁶⁴ Art. 1, let. c, point 18, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

³⁶⁵ Point (10), Directive (EU) 2018/843, cit.

investment purposes, and is transferred, stored, and traded electronically³⁶⁶. Compared to the EU definition, the Italian definition explicitly includes investment purposes.

Considering these premises, the court recalled decision 26807/2020, which stated the principle that when Bitcoin is marketed as an investment opportunity, the activity is subject to the regulatory requirements of Articles 91 et seq. TUF. According to Art. 91 TUF, the Consob authority exercises the powers provided for in this section to protect investors and ensure the efficiency and transparency of corporate control and capital markets.

Failure to comply with these requirements constitutes an offence under Article 166, paragraph 1, letter c) TUF, which penalizes those who offer, promote, or distribute financial products, financial instruments, or investment services outside a registered office or through remote communication techniques.

Therefore, Bitcoin qualifies as a financial product when purchased for investment purposes. When a virtual currency functions as an investment instrument, i.e., when its "concrete cause" (*causa concreta*) is that of a financial product, it must be regulated under financial intermediation laws (Articles 94 et seq. TUF). These provisions ensure comprehensive and specialised investor protection through a unified legal framework.

However, the consideration that Bitcoin cannot be equated to digital gold and, consequently, treated as a financial instrument constitutes an error in judgment (*error in iudicando*), is not permissible for appeal to Corte di Cassazione. According to Articles 355, c. 3 and 325 c.p.p., an appeal to the Court of Cassation against orders relating to probationary seizures (as with precautionary ones) is only permitted for violations of law. Such violations encompass errors in judgment (*errores in iudicando*) or in procedure (*errores in procedendo*), as well as deficiencies in reasoning that are so serious as to render the decision incomprehensible or lacking in logical coherence. Conversely, the manifest illogicality of reasoning cannot be cited as a ground for appeal to the Suprema Corte di Cassazione unless it results in a completely absent or merely apparent justification. In this case, the appellant does not allege an absence of reasoning but contests the Tribunal's assessment equating Bitcoin to digital gold. Such an argument is a matter of merit, not of law, and is therefore inadmissible before this Court.

For this decision, the Court elaborated one interpretative statement, confirming the interpretation of Cass. pen. n. 26807/2020.

In this judgment, the Court emphasized the principles of investor protection, market efficiency, and transparency as the ones characterising the regulatory framework governing financial instruments. Then, when Bitcoin is an investment opportunity, it falls within the scope of Articles 91 et seq. TUF, which gives Consob the authority to supervise and safeguard these principles.

³⁶⁶ Decreto Legislativo n. 90 del 2017 amended by Decreto legislativo n. 125 del 2019 “

The Court clarified that compliance with these rules is essential, and any failure - such as offering, promoting, or distributing financial products or services outside a registered office or through remote means - constitutes the offence outlined in Article 166, paragraph 1, letter c) TUF.

Decision	Interpretative statement (massima)
Cassazione penale, sez. II, 10/11/2021, n. 44337.	The sale of Bitcoin, when promoted as an investment opportunity, is subject to financial instrument regulations. When the sale of Bitcoin is advertised as an investment proposal, it falls under the regulatory requirements of Articles 91 et seq. TUF. These provisions empower Consob to oversee investor protection, as well as the efficiency and transparency of the corporate control and capital markets. Failure to comply with these obligations constitutes the offense outlined in Article 166, paragraph 1, letter c) TUF, which penalizes those who offer, promote, or distribute financial products, financial instruments, or investment services remotely or outside a registered office. Therefore, Bitcoin may be considered a financial product when purchased for investment purposes. When virtual currency serves the function – or “concrete cause” – of an investment instrument, and thus qualifies as a financial product, it must be regulated under the financial intermediation framework (Articles 94 et seq. TUF), which ensures investment protection through a unified and specialised legal framework.

Moreover, the Court underlined the need to assess the function (*causa concreta*) of the transaction: if a virtual currency like Bitcoin serves the function of an investment instrument, it must be considered as a financial product³⁶⁷. In such cases, it is subject to the regulatory regime provided by Articles 94 et seq. TUF, which offers a unified and specialised legal framework aimed at protecting investments.

1.4 Cassazione penale, sez. II, 26/10/2022, n. 44378.

The third decision concerns the offence of unauthorized financial activity under Art. 166 TUF. In the specific case, the activity consisted of an online fundraising campaign explicitly advertised as an investment offering. The decision also concerns the preventive seizure of a wallet containing 30 bitcoins, deemed to be the object of the offence of self-laundering under Art. 648-ter c.p.p.

Tribunale di Brescia had rejected the request for preventive seizure as the existence of concrete elements that make it plausible that a crime has been committed (*fumus commissi delicti*) was missing. The public prosecutor appealed the order. Specifically, he argued that it was necessary to determine whether the Initial Coin Offering (ICO) could be classified as an offer of investment services or activities. This assessment was crucial to establish potential liability under Article 166 TUF. According to the prosecutor, the conduct in question qualified in fact as an investment offer.

³⁶⁷ Cian, M. (2023). Noterelle su finanziarietà e non finanziarietà nei crypto-assets: la Suprema Corte sulla natura del servizio di exchange. *Banca Borsa Titoli di Credito: rivista di dottrina e giurisprudenza*, 76(2), 8. According to the Author, it is not the promotional activity that defines the “concrete cause” of the Bitcoin offering as an investment purpose, but rather the typical interest that currently drives those who hold capital to invest in this cryptocurrency.

The Supreme Court examined whether the rules on financial intermediation (Articles 94 et seq. TUF) applied to the sale of Bitcoin when advertised as an investment offer³⁶⁸. In the analysis, the court reviewed the definition and the interpretation of European and Italian legislation on cryptocurrencies at the moment. Specifically, it was essential to determine whether cryptocurrency could serve an investment purpose. Such as Cass. pen. n. 44337/2021, the court recalled the definition of Directive (EU) 2018/843, by extending anti-terrorism and anti-money laundering regulations to activities involving the exchange of virtual currencies into legal tender and viceversa. Virtual currencies are in fact digitally represented values that are not issued by a central bank or public authority, and are not necessarily linked to a legal tender. However, it is accepted by individuals and businesses as a means of exchange and can be electronically transferred, stored, and traded³⁶⁹.

Moreover, the court mentioned the Recital 10 of Directive (EU) 2018/843³⁷⁰ and the d.lgs. 125/2019 which specify that virtual currencies may also be used for investment purposes³⁷¹. In this regard, the decision recalls also the definition of exchanger as the technological platform that allows buying and selling cryptocurrencies to gain profits. In this regard, the legislative decree included cryptocurrency service providers in the category of the subjects obliged to subscribe to the register of financial agents and credit brokers³⁷² and to communicate their activity to the Ministry of Economics and Finance.

The court recalled the judgement analysed in the first paragraph of this chapter – Cass. pen. n. 26807/2020 – to confirm the principle according to which the online sale of Bitcoin, when promoted as an investment opportunity for savers - providing them with information on the profitability of the initiative - is an activity subject to the regulatory requirements set forth in Articles 91 et seq. TUF³⁷³.

The court also mentioned the interpretation adopted by Tribunale di Verona with decision n. 195/2017³⁷⁴. In particular, such decision qualified as financial instruments

³⁶⁸ Razzante R., Le cripto attività come prodotti finanziari, IUS Penale, fasc., 16 Febbraio 2023.

³⁶⁹ Art. 1, let. c, point 18, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

³⁷⁰ Recital 10, Directive (EU) 2018/843, cit.

³⁷¹ Art. 1, D.Lgs. n. 231/2007 as modified by D.Lgs. n.125/2019.

³⁷² The register is held by OAM (Organismo competente in via esclusiva ed autonoma per la gestione degli Elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi).

³⁷³ See Razzante, R. Le cripto attività come prodotti finanziari. A proposito di Cass. Pen., Sez. II, 22 novembre 2022, n. 44378. *“Nel caso di specie, quindi, la Corte riteneva che, dal momento che i destinatari della proposta di investimento hanno fornito bitcoin, per ottenere monete virtuali che avrebbero consentito la partecipazione alla piattaforma successivamente, con valore variabile a seconda del momento dell’acquisto e con ritorno maggiore in caso di successo della piattaforma stessa, questi avessero assunto un rischio d’investimento corrispondente al capitale investito.”*

³⁷⁴ Tribunale di Verona was asked to rule on a case involving a crowdfunding initiative. A group of investors had transferred funds to a company that was supposed to reinvest them by converting the amounts into virtual currency, something that ultimately never happened.

In its decision, the court adopted the interpretation offered by the Court of Justice of the European Union (Skatteverket/David Hedqvist, C-264/14) and clarified that the activity in question fell within the scope

those who imply: 1) use of capital of money or a use of capital, generally referable to money or, more generally, to an asset, which may also correspond to a virtual currency, b) an expectation of profitability, c) a risk inherent in the chosen activity, directly related to the use of capital³⁷⁵. Such features all characterise the case examined. The activity concerns in fact a provision of bitcoin to customers with profit expectation and risk-taking.

The reconstruction of the facts in the contested order leads to the conclusion that the defendant's conduct constitutes unauthorised financial activity under Article 166, letter c) of d.lgs. 58/1998. This provision penalises anyone who offers, promotes, or distributes financial products, financial instruments, or investment services and activities outside a registered office or through remote communication methods.

The Court elaborated three interpretative statements, in line with the reasoning already expressed in Cass. pen. n. 26807/2020 and Cass. pen. n. 44738/2022. In particular, the Court confirmed that cryptocurrencies qualify as financial products when used for investment purposes, and are therefore subject to the regulatory framework of the TUF. This includes, above all, the rules on financial intermediation (Articles 94 et seq. TUF), which are designed to protect investors through a unified and specialised legal framework.

As a consequence, service providers operating in this sector are required to meet specific obligations. These requirements aim to ensure that consumers receive adequate information to understand the economic and contractual features of the transaction and to make informed decisions.

The Court further clarified that, within the scope of financial intermediation, the online sale of virtual currencies, when promoted as an investment opportunity, is an activity regulated under Articles 91 et seq. TUF. If these rules are not observed, the conduct may amount to the criminal offence of unauthorized financial activity, as provided by Article 166, paragraph 1, letter c) TUF.

It was also emphasized that virtual currencies are to be considered financial investment instruments since they are financial products, and their professional trading requires prior authorization under the applicable financial intermediation laws.

Finally, the creation and exchange of virtual currencies were regarded as a form of public offering of investment services or activities. If such operations are carried out without proper authorization, they qualify as unauthorized financial activity, again falling under the offence set out in Article 166 TUF.

of financial services. More specifically, the Tribunal found that the transaction involved distance contracts for financial services concluded with consumers, and was therefore subject to the rules laid down in d.lgs. 206/2005 (Italian Consumer Code).

On the basis of this qualification, the judge found that the company had failed to comply with its pre-contractual disclosure obligations and, as a result, declared the contract null and void, ordering the intermediary to return the sums received.

³⁷⁵ Tribunale di Verona, 24 Gennaio 2017, n. 195.

Decision	Interpretative statement (massima)
Cassazione penale, sez. II, 26/10/2022, n. 44378.	(1) Virtual currency constitutes an investment instrument because it qualifies as a financial product. Virtual currency must be considered an investment instrument as it qualifies as a financial product and, therefore, must be regulated under the provisions on financial intermediation (Articles 94 et seq. TUF), which ensure investor protection through a unified special legal framework. Consequently, those providing such services are obliged to increase disclosure obligations towards consumers to enable them to understand the contents of the economic-contractual transaction and to make an informed contractual decision. (2) The online sale of virtual currency is an activity subject to the regulatory requirements governing financial instruments. In the context of financial intermediation, the online sale of virtual currency, when advertised as an investment opportunity for savers, is an activity subject to the requirements provided for by the legislation on financial instruments under Article 91 et seq. of the TUF. Failure to comply with these obligations constitutes the offense outlined in Article 166, paragraph 1, letter c) TUF. (3) Virtual currencies constitute financial investment instruments, and their professional trading is subject to compliance with financial intermediation regulations, including the necessary authorisation of the intermediary. (4) The creation and exchange of virtual currency without proper authorization constitutes the offense of unauthorized financial activity. The creation and exchange of virtual currency constitute a case of public offering of investment services or activities. If carried out by an operator without the required authorization, this activity qualifies as unauthorized financial activity under Article 166 TUF.

1.5 Legal considerations.

The decisions analysed represent the first attempt to provide interpretative guidelines on crypto assets within the Italian legal framework. The first important aspect to note is that all three rulings concern financial law and financial crimes. In particular, the Court's reasoning focuses on the following legal provisions:

- Art. 91 et seq. of TUF.
- Art. 94 et seq of TUF
- Art 166 of TUF

Art. 91 et seq. of TUF are provisions containing the general rules governing issuers. In particular, issuers are entities that provide financial instruments to fund their operations, and whose instruments are intended to be traded on the market. The main issuers are corporate entities, public bodies, and the State. Title I of TUF (Articles 91 et seq TUF) provides for the macro-objectives that Consob must consider in its supervision activity. These macro-objectives are:

- 1) investors protection;
- 2) efficiency and transparency of the corporate control market;
- 3) efficiency and transparency of the capital markets.

From these objectives derive Consob's supervisory functions, which are organised in differentiated models according to the specificities of the issuers and the instruments

offered³⁷⁶. In particular, these functions concern: the information provided to potential investors (investment) and to holders of instruments to whom disinvestment is directed, compliance with equal treatment and other principles governing the conduct of offers, the information to be provided by issuers of listed and disseminated instruments on a regular basis, the obligations imposed on issuers to protect the rights of shareholders, on ownership structures, on compliance with corporate governance rule³⁷⁷.

Articles 93-bis et seq. TUF regulate the public offering of financial instruments and products. These provisions are designed to protect investors, promote market transparency, and ensure that those offering financial instruments comply with authorisation requirements. The legislation regulates the public offering of the following financial products:

- securities and units of closed-end collective investment undertakings (OICR³⁷⁸) (Article 93-bis, paragraph 1, letter a) of the TUF);
- units or shares of open-ended collective investment undertakings (OICR), as regulated (Articles 98-ter et seq. of the TUF);
- other financial products (**Articles 94 et seq. of the TUF**).

Within this framework, the publication of a prospectus plays a central role. The prospectus serves as a public information tool. Its primary purpose is to provide essential, clear, and reliable information to individuals who do not have the means or

³⁷⁶ <https://www.consob.it/web/investor-education/la-vigilanza-sugli-emittenti>

³⁷⁷ <https://www.consob.it/web/investor-education/la-vigilanza-sugli-emittenti>

³⁷⁸ Collective investment undertakings (OICR) are defined in Art. 1, letter k, k-bis, k-ter) of the TUF. A collective investment undertaking (OICR) is an entity established to provide collective asset management services. Its capital is raised from a number of investors through the issuance and offering of units or shares. This capital is pooled and managed independently from the investors, in their interest, and is invested in financial instruments, loans (including those granted to non-consumer entities), equity stakes, or other movable or immovable assets, according to a predefined investment policy. An OICR can be either open-ended or closed-ended. An open-ended OICR allows participants to request the redemption of their units or shares based on the fund's assets, in accordance with the terms and frequency set out in the fund's regulations, by-laws, and offering documents. A closed-ended OICR, on the other hand, is a type of investment fund where investors can subscribe to units only at the time of the fund's establishment. Typically, redemptions are allowed only at the fund's maturity, and not during its operation. Original version “k) *“Organismo di investimento collettivo del risparmio” (Oicr): l'organismo istituito per la prestazione del servizio di gestione collettiva del risparmio, il cui patrimonio è raccolto tra una pluralità di investitori mediante l'emissione e l'offerta di quote o azioni, gestito in monte nell'interesse degli investitori e in autonomia dai medesimi nonché investito in strumenti finanziari, crediti, inclusi quelli erogati, a favore di soggetti diversi da consumatori, a valere sul patrimonio dell'OICR, partecipazioni o altri beni mobili o immobili, in base a una politica di investimento predeterminata;* k-bis) *“Oicr aperto”: l'Oicr i cui partecipanti hanno il diritto di chiedere il rimborso delle quote o azioni a valere sul patrimonio dello stesso, secondo le modalità e con la frequenza previste dal regolamento, dallo statuto e dalla documentazione d'offerta dell'Oicr;*, k-ter) *“Oicr chiuso”: l'Oicr diverso da quello aperto;”*

expertise to independently search for and evaluate the data necessary to make an informed investment decision using their financial resources³⁷⁹.

Art. 166 of the TUF³⁸⁰ regulates the offence of unauthorised financial activity. It penalises anyone who, without proper authorisation, carries out investment services, investment activities, collective asset management services, or one of the activities provided by Art. 166, paragraphs b, c, c-bis of the TUF

The offence protects both individual interests, such as personal assets and savings, and public interests, including the proper functioning of administrative oversight over economic activities. Moreover, the provision also aims to safeguard the orderly functioning of the banking and financial markets, ensure fair competition, and, more broadly, protect the public economy³⁸¹.

All three decisions focus on whether or not the rules set out in the TUF apply to cryptocurrencies. The main issue in each case was whether the sale of cryptocurrencies, under certain conditions, could be considered a financial product.

This classification is important because, if confirmed, it triggers the application of financial regulations, including the obligation to meet specific legal and procedural requirements.

In the first case (**Cass. pen. n. 26807/2020**), the Court upheld the seizure of funds, finding that Bitcoin had been promoted as an investment, with promises of high returns. This marketing strategy brought the activity within the scope of Articles 91 et

³⁷⁹ Palmieri, M. (2020). Offerte al pubblico e sollecitazione al risparmio. In *Il Testo Unico Finanziario* (Vol. 2, p. 1301). Zanichelli.

³⁸⁰ Art. 166 of the TUF (original Italian version): “1. È punito con la reclusione da uno a otto anni e con la multa da euro quattromila a euro diecimila chiunque, senza esservi abilitato ai sensi del presente decreto:

a) svolge servizi o attività di investimento o di gestione collettiva del risparmio;

b) offre in Italia quote o azioni di OICR;

c) offre fuori sede, ovvero promuove o colloca mediante tecniche di comunicazione a distanza, prodotti finanziari o strumenti finanziari o servizi o attività di investimento;

c-bis) gestisce un APA o un ARM a cui si applicherebbe la deroga prevista dall'articolo 2, paragrafo 3, del regolamento (UE) n. 600/2014 e dai relativi atti delegati(1).

2. Con la stessa pena è punito chiunque esercita l'attività di consulente finanziario abilitato all'offerta fuori sede senza essere iscritto nell'albo indicato dall'articolo 31.

2-bis. Con la stessa pena è punito chiunque esercita l'attività di controparte centrale di cui al regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, senza aver ottenuto la preventiva autorizzazione ivi prevista.

3. Se vi è fondato sospetto che una società svolga servizi o attività di investimento o il servizio di gestione collettiva del risparmio o la gestione di un APA o di un ARM a cui si applicherebbe la deroga prevista dall'articolo 2, paragrafo 3, del regolamento (UE) n. 600/2014 e dai relativi atti delegati ovvero l'attività di cui al comma 2-bis senza esservi abilitata ai sensi del presente decreto, la Banca d'Italia o la Consob denunciano i fatti al pubblico ministero ai fini dell'adozione dei provvedimenti previsti dall'articolo 2409 del codice civile ovvero possono richiedere al tribunale l'adozione dei medesimi provvedimenti. Le spese per l'ispezione sono a carico della società.”.

³⁸¹ Consulich, F. (a cura di). (2024). *Reati in materia bancaria e finanziaria*. Torino: Giappichelli. ISBN: 9791221106466.

seq. TUF, and failure to comply with regulatory obligations constituted unauthorised financial activity under Article 166 TUF.

The second case (**Cass. pen. n. 44337/2021**) involved the seizure of a website used to promote the sale of Bitcoin. The Court rejected the defence's argument that Bitcoin is merely a payment tool, affirming instead that when promoted as an investment, it qualifies as a financial product. The decision also clarified the importance of the concrete function (*causa concreta*) of the transaction in determining its legal nature.

The third case (**Cass. Pen. n. 44378/2022**) concerned an Initial Coin Offering (ICO) advertised as an investment, along with the preventive seizure of some Bitcoins suspected to be involved in self-laundering. The Court reaffirmed that, when cryptocurrency is used for investment purposes, it must comply with the TUF's rules on financial intermediation. The ruling confirmed that such offers qualify as public investment services, and if carried out without authorisation, amount to unauthorised financial activity under Art. 166 TUF.

In all three decisions, the Court concluded that the offering of cryptocurrencies can fall within the category of financial products, provided certain conditions are met. In particular, both Cass. Pen. n. 26807/2020 and Cass. Pen. n. 44337/2021 highlight the importance of promotional conduct that suggests the nature of the transaction as an investment opportunity.

Typical behaviours include promising returns or emphasising the profitability or convenience of the purchase, features commonly associated with the marketing of financial products. It is precisely these elements that lead to the legal classification of cryptocurrencies as financial products under the TUF, when such promotional strategies are employed.

In this regard, it becomes clear that an Initial Coin Offering (ICO) is not so far different from a traditional financial investment offer. In the cases analysed, there is the use of one's own capital in exchange for an expected return, while from the investor's perspective, there is an acceptance of investment risk.

Precisely because of this shared purpose between an ICO and a financial investment offer, it appears appropriate to apply Articles 94 et seq. of the TUF to cases involving investment offers based on crypto assets³⁸².

Another interesting point concerns the classification of virtual currencies within the financial system. According to some interpretations, they do not fall under the definition of financial instruments, because they are not securities, do not grant participation rights, are not fund investments, and are not linked to public

³⁸² Razzante, R. Le crypto attività come prodotti finanziari. A proposito di Cass. Pen., Sez. II, 22 novembre 2022, n. 44378.

authorities³⁸³. They are also not derivatives, although they may act as indicators of financial operations.

However, they could still be considered financial products, depending on how that term is interpreted. One clear approach sees financial products as a broader category that includes financial instruments and securities as more specific types. This is consistent with the broad definition in Article 1, paragraph 1, letter u) of TUF³⁸⁴, which defines financial products as financial instruments and any other form of financial investment³⁸⁵.

The possibility that cryptocurrency transactions may fall under either general private law operations or financial operations is further confirmed by the entry into force of the MiCA regulation³⁸⁶. This regulation is specifically designed to apply to crypto-asset activities that do not qualify as financial operations, which remain governed by MiFID II directive³⁸⁷.

The existence of these two separate legal frameworks highlights the importance of conducting a legal interpretation based on the concrete function of the transaction under examination. As underlined by Cass. Pen. n. 44337/2021, this assessment must be made in practical terms. The evaluation should therefore focus on the actual role that a given legal transaction plays within the legal system, without relying solely on abstract or formal classifications.

³⁸³ Agnino, F. (2020), Vendita di bitcoin e intermediazione finanziaria abusiva, Cass. Pen. sez. II, 17 settembre 2020, n. 26807, IUS Penale, fasc.

³⁸⁴ Art. 1, paragraph 1, letter u) of TUF, Original Italian version: “u) *“prodotti finanziari”: gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria; non costituiscono prodotti finanziari i depositi bancari o postali non rappresentati da strumenti finanziari”*”.

³⁸⁵ Agnino F., Vendita di bitcoin e intermediazione finanziaria abusiva, Cass. Pen. sez. II, 17 settembre 2020, n. 26807, IUS Penale, fasc., 9 OTTOBRE 2020.

³⁸⁶ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

³⁸⁷ Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II).

2. Italian merit case law on cryptocurrencies.

As already reported, since the emergence of crypto assets, Italian courts have adopted many judgements regarding them. The official database³⁸⁸ of merit Italian civil sentences has 85 judgements under the word “crypto assets”.

As anticipated, this data is in contrast with the limited number of decisions adopted by the Suprema Corte di Cassazione. Several factors likely explain this difference. First, not all lower court rulings are appealed to the Supreme Court. Second, due partly to case backlogs and the high number of cases, the slow pace of proceedings may delay judgments³⁸⁹. Third, appeals to the Court of Cassation are allowed only on specific legal grounds, and factual reassessments are excluded.

As a result, Corte di Cassazione’s rulings are fewer than those issued by lower grade courts. However, as the following analysis will show, trial-level decisions are highly valuable for legal interpretation. Judges and lawyers often assess whether a transaction falls under a specific legal category based on factual elements, which help determine the legal classification of the case. The decisions examined provide several factual and legal insights, making them a useful tool for legal interpreters looking to reconstruct the legal framework applicable to crypto assets.

Before analysing the decisions, it is useful to provide some background on civil trial proceedings on the merits.

First of all, a judgment on the merits ends with a court ruling, which may concern either procedural issues or the substance of the case. A merit judgment issues actual judicial measures with typical content such as condemnation, recognition, or constitution of rights³⁹⁰. As such, it has a direct impact on the parties’ legal and financial positions. The trial focuses on substantive issues and begins with the judge’s task of reconstructing the facts underlying the legal claim³⁹¹. This phase, known as the fact-finding stage, leads the judge to confirm or deny the existence of legally relevant facts, which may be constitutive, extinguishing, or obstructive. Once the facts are established, the judge proceeds to the legal assessment, applying the relevant substantive rules to the verified factual situation. This phase is the legal evaluation of the trial³⁹².

³⁸⁸ The database contains civil judgments, decrees and orders from the Sistema Informativo del Settore Civile (SICI) from 01/01/2016 to the present. It doesn’t include measures on family, children and personal status. Link: <https://bdp.giustizia.it>

³⁸⁹ For instance, the criminal division of the Suprema Corte di Cassazione issue approximately 48,000 rulings. Giura, G., & De Felice, D. (2016). Selettività della giurisprudenza di merito: giudizio di legittimità e giurisprudenza locale. *Sociologia del diritto*: 1, 2016, 135-158.

³⁹⁰ Fazzalari, E., ‘sentenza civile’ in *Enc. Dir.* [XLI 1989], Giuffrè, Milano.

³⁹¹ *Ibid.*

³⁹² *Ibid.* The two phases of the judgment — the fact-finding stage and the legal evaluation — while distinct in their object and structure, are closely interrelated in practice. On the one hand, to determine which facts need to be established, the judge begins with a hypothetical application of a specific substantive legal framework.

Merit judgments provide valuable insight into how specific factual elements justify the application of legal provisions. Studying these rulings is important because it reveals how lawyers and judges interpret new types of cases, thus initiating the interpretative process of law.

In the context of cryptocurrencies, it is particularly interesting to examine the legal reasoning used to determine whether, and how, existing regulations apply to concrete situations. As seen in Corte di Cassazione's cases, applying a legal framework is never automatic. On the contrary, it requires careful analysis of multiple legal factors. In first or second-instance judgments, this analysis is enriched by a broader and more detailed assessment of the facts, which helps in constructing the legal classification of the case.

These interpretations not only lay the groundwork for case law on crypto assets, but also guide future decisions. This analysis therefore helps to identify both the main interpretative challenges related to crypto-assets and the legal tools and institutions being used to integrate cryptocurrencies into the legal system.

In this regard, it is worth to note that a wide range of different legal issues have been covered in the decisions of Tribunali and Corti d'Appello. The three selected decisions in fact deal with diverse institutions within Civil and Commercial law, demonstrating that cryptocurrencies are used for a variety of purposes and that their presence in the legal landscape is broad and growing.

In **decision n. 7932/2022 (Tribunale di Roma)**, the court examined whether cryptocurrencies could be used as a capital contribution in kind during a corporate capital increase. Since cryptocurrencies cannot be classified as money, the court assessed whether they could qualify as assets with reliable patrimonial value. The court ruled against this, citing high volatility, lack of intrinsic value, and the difficulty in verifying and measuring their worth, all of which conflict with the legal requirements for share capital. Though not deemed illegal, crypto contributions were found incompatible with the purpose of capital stability, leaving the issue in legal uncertainty.

In **decision n. 18/2019 (Tribunale di Firenze)**, the court assessed whether cryptocurrency deposits on a trading platform constituted a regular or irregular deposit. The classification was decisive in declaring the company's insolvency after an 80% asset shortfall caused by a system malfunction. The court found the deposit to be irregular, as the platform had control and ownership over the funds, and users lacked private keys. Given the fungible nature of cryptocurrencies, the company was obliged to return an equivalent amount. Its failure to do so confirmed its insolvency and justified bankruptcy.

In **decision n. 5866/2023 (Corte di Appello di Roma)**, the court upheld a Consob sanction against a company that launched a blockchain-based token offering to fund a photovoltaic project without publishing a prospectus, violating Article 94 of the TUF.

Once the facts are verified, the judge may confirm that the initial legal hypothesis applies to them. Alternatively, the factual findings may reveal a situation incompatible with the original legal assumption, requiring the application of different substantive rules.

Although the company claimed the tokens - labelled "energy tokens" - were not financial instruments, the court found that their structure and promotional materials presented them as investment opportunities with expected financial returns. The court emphasized that the economic substance, not the label, determines whether a product falls under financial regulation. The ruling reinforces the importance of transparency, investor protection, and regulatory compliance in crypto fundraising.

Judgment No.	Legal Institutes	Details
7932/2022 <i>Tribunale di Roma</i>	In-kind contribution; capital injections	The Court examined whether cryptocurrencies could be used as a capital contribution in kind during a corporate capital increase. According to the Court, cryptocurrencies cannot be classified as in-kind contributions, considering the necessity for the company's share capital to be measurable and verifiable. These characteristics are fundamental to protect creditors' interests and maintaining trust in corporate transactions.
18/2019 <i>Tribunale di Firenze</i>	Declaration of bankruptcy; deposit contract	To declare bankruptcy, it must first be determined whether the cryptocurrency deposit contract is regular or irregular. In this case, based on the expert report, the Court has classified the contract as irregular. As a result, the economic shortfall allows for the declaration of bankruptcy to proceed.
586/2023 <i>Corte di Appello di Roma</i>	Public offer (art. 94, comma 1, TUF); sanctions	Article 94, paragraph 1, of the TUF provides for the application of sanctions by Consob in case of missing publication of the informative prospectus. However, the appellant argues that in this case tokens (energy tokens) do not qualify as financial instruments, and therefore the provisions of this regulation should not apply.

This analysis will highlight both the widespread use of cryptocurrencies and their versatility in serving various purposes. In such cases, the main challenge for judges lies in determining which contractual framework best fits the specific situation (Tribunale di Firenze, n. 18/2019) and whether certain legal institutions from Italian law can be applied by analogy.

However, this hermeneutic approach is not always allowed, especially where it may endanger higher-ranking legal interests (Tribunale di Roma, n. 7932/2022). Similarly, the need to protect public interests, such as safeguarding investors or ensuring fair competition, may require the application of public law norms, especially in the fields of financial regulation and consumer protection (Corte di Appello di Roma, n. 5866/2023).

It will therefore be particularly interesting to observe how judges have chosen to apply (or not apply) civil, commercial, and financial law institutions, always aiming to uphold the principle of legality and the principle of technological neutrality, both essential in ensuring coherent and fair legal development in the face of innovation.

2.1. The “in-kind” contribution of crypto assets (Tribunale di Roma, n. 7932/2022).

The first case (Tribunale di Roma, n. 7932/2022) concerns the possibility of using cryptocurrencies as a contribution to a capital increase, categorising them as a contribution in-kind.

In the Italian legal system, capital contributions can be conferred through money or goods with a reliable patrimonial value (contributions in kind). Excluding that cryptocurrencies can be considered as money, it is necessary to assess whether cryptocurrencies can be assets with a reliable patrimonial value.

In the current case, a notary declined to formalise a resolution concerning a corporate contribution made in cryptocurrencies. As a result, the shareholders petitioned the court for compulsory registration, contending that cryptocurrencies qualify as assets eligible for in-kind contributions. The shareholders argued that Directive 77/91/CEE, as amended, expanded the range of assets that can be contributed in kind to include any entity with a reliable patrimonial value.

However, Tribunale di Roma rejected this argument. According to the Court, cryptocurrencies cannot be classified as in-kind contributions. The Court noted that, due to their function, the contribution would more closely resemble a cash contribution. Nevertheless, it does not fit within this category because cryptocurrencies, lacking the function of a unit of account, are highly volatile.

Furthermore, this incompatibility is underscored by the necessity for the company’s share capital to be measurable and verifiable. These characteristics are fundamental to protect creditors’ interests and maintaining trust in corporate transactions; such features confer in fact certainty and stability to the company’s patrimony. These attributes are incompatible with the nature of cryptocurrencies, which are exposed to a level of risk that exceeds that inherent in contracts, hindering stable capital valuation. Indeed, their value is determined by private agreements and trading platforms, lacking the intrinsic qualities required to support a stable and reliable valuation for corporate capital.

A prior decision had already stated the same principle. In 2018, a notary denied a capital increase in bitcoin, considering the absence of legal requirements established by law. Similar to the reviewed decision, the dissent was based on the idea that the volatility of cryptocurrencies prevents an accurate assessment of the allocated amount and the contribution's effectiveness³⁹³. In the second instance judgment, the Court of Appeal clarified that although the virtual currency is structurally comparable to goods, its most accurate classification from a functional perspective is as money³⁹⁴.

This interpretation was also adopted by the Tribunale di Roma. Specifically, it was noted that share capital must be measurable and verifiable. It must have a certain value

³⁹³ Tribunale di Brescia, Sezione Imprese, 18 luglio 2018, decreto n. 7556/2018.

³⁹⁴ Corte d’Appello di Brescia, 24 ottobre 2018, decreto n. 207/2018.

and stability according to generally accepted valuation standards. Such features are conspicuously absent in cryptocurrencies, whose market value is indeed determined by private agreements and trading platforms. In fact, cryptocurrencies lack any intrinsic value. Consequently, the contractual risk associated with them is greater than that of a standard contract and cannot serve as a basis for establishing a company.

After stating the impossibility of proceeding with the increase, the court clarified that this conclusion does not imply the illegality of cryptocurrency contributions. However, their admissibility cannot rely solely on their classification for tax purposes.

The shareholders had in fact invoked tax regulations, particularly those governing VAT. These regulations attribute fiscal significance to cryptocurrencies, subjecting them to taxation. However, the court highlighted that although tax regulations acknowledge cryptocurrencies as assets subject to fiscal obligations, this recognition does not automatically make them suitable as contributions to corporate capital.

The court stressed that their compatibility with share capital requirements must be assessed independently of tax considerations.

The judgment highlighted that the necessity of ensuring the stability and efficacy of share capital outweighs the freedom of economic initiative. This balance aims to protect creditors' interests and maintain the integrity of the corporate framework. As cryptocurrencies lack the attributes of stability, certainty, and verifiability, they cannot serve as a reliable basis for establishing or increasing share capital.

However, the reported statement - *the impossibility of proceeding with capital increase does not imply the illegality of cryptocurrency contributions in the capital* - raises significant uncertainties regarding the actual suitability of such assets to constitute an object of contribution³⁹⁵. Indeed, on the one hand, cryptocurrencies are regarded as equivalent to money. On the other hand, the intrinsic contractual risk of their value precludes their use as objects of increase. As such, it appears these values are not permitted even if they are not illegal. The decision is made by the notary following an evaluation of the features of the asset conferred.

This interpretation generates uncertainties about the potential for using crypto assets for private purposes. In the context of companies, the necessity of ensuring stability and efficacy in share capital is justified by the need to protect creditors' interests. The safeguarding of such interests appears to outweigh the freedom of economic initiative. Nonetheless, an official clarification from the legislator would be advisable for legal certainty purposes.

³⁹⁵ Tribunale di Roma, n. 7932/2022, p. 6. Original version: “*Non assume alcun significato positivo nel contesto in esame, inoltre, la valutazione della controparte che attribuisce una valenza tributaria alle criptovalute atteso che ogni incremento patrimoniale, anche di natura illecita, è assoggettato ad imposizione fiscale (vds. Cass. N. 31930/2021; Cass. N. 29142/2021). Ciò non vuol dire che il conferimento in criptovalute sia illecito, ma non può essere la qualificazione in termini tributari a far ritenere ammissibile detto conferimento*”.

2.1.1. A key precedent on cryptocurrencies contribution. Tribunale di Brescia n. 7556/2018 and Corte d'Appello di Brescia n. 207/2018.

As noted in the Tribunale di Roma decision³⁹⁶, a key precedent is found in a similar case examined by both Tribunale and Corte di Appello di Brescia³⁹⁷. The dispute concerned a notary's refusal to register a corporate resolution approving a capital increase in Bitcoin. The company challenged the refusal under Article 2436, par. 3, c.c., which governs the registration of corporate resolutions³⁹⁸.

The notary refused the registration because cryptocurrencies, due to their volatility, did not allow for a reliable valuation of the contribution nor verification of the actual execution of the capital increase. Tribunale di Brescia rejected the company's challenge, stating that cryptocurrencies could not be used as capital contributions because they do not meet the requirements of Article 2464, par. 2, c.c., which allows only assets that can be reliably and objectively valued and liquidated, and subject to enforcement³⁹⁹.

The court stressed three key conditions for valid in-kind contributions:

1. The asset must have a certain and stable value,
2. It must be part of a market that allows quick and trustworthy liquidation,
3. It must be subject to enforcement procedures.

In this case, none of these conditions were met. The court noted the lack of a trustworthy public exchange platform (except those linked to the crypto's creators), making the valuation self-referential and unsuitable for legal certainty (conditions 1 and 2). Additionally, no method was provided to enforce the foreclosure of the bitcoins, as they are protected by private cryptographic keys, making judicial enforcement impossible without the cooperation of the debtor (condition 3).

The Court of Appeal of Brescia upheld the decision but made some conceptual clarifications. While acknowledging that cryptocurrencies could be structurally assimilated to goods, the court argued that functionally, they should be considered more like money, as they are used as a medium of exchange, albeit in a limited context.

However, due to the lack of legal tender status, their high volatility, and the absence of a reliable valuation method, the court concluded that cryptocurrencies do not meet the conditions for being used in capital increases. It ruled out the idea that they could

³⁹⁶ Tribunale di Roma, n. 7932/2022.

³⁹⁷ Tribunale di Brescia, Sezione Imprese, 18 luglio 2018, decreto n. 7556/2018 and Corte d'Appello di Brescia, 24 ottobre 2018, decreto n. 207/2018.

³⁹⁸ Art. 2436, par. 3, c.c. Original Italian version: "*Se il notaio ritiene non adempiute le condizioni stabilite dalla legge, ne dà comunicazione tempestivamente, e comunque non oltre il termine previsto dal primocomma del presente articolo, agli amministratori. Gli amministratori, nei trenta giorni successivi, possono convocare l'assemblea per gli opportuni provvedimenti oppure ricorrere al tribunale per il provvedimento di cui ai successivi commi; in mancanza la deliberazione è definitivamente inefficace*".

³⁹⁹ Art. 2464, par. 2, c.c. Original Italian version: "*Possono essere conferiti tutti gli elementi dell'attivo suscettibili di valutazione economica*".

be considered “goods, services or other utilities” with economic value, and instead framed them as alternative currencies, used in limited contexts and operating outside official monetary systems.

2.2. The qualification of cryptocurrency deposits as regular or irregular as a requirement to declare bankruptcy. Tribunale di Firenze n. 18/2019.

The second issue (18/2019 Tribunale di Firenze) concerns the requirements for declaring a company's bankruptcy. Specifically, in the decision under review, the classification of cryptocurrency deposits as regular or irregular is decisive.

In this case, a company had provided an online service for cryptocurrency deposits and exchanges. Subsequently, a shortfall of approximately 80% of the deposited assets was reported. In particular, the shortfall has been attributed to the multiple requests of a client, who had exploited the malfunctioning of the blockchain system to withdraw money. The software of the platform was unable to manage users' withdrawal requests, which resulted in multiple unauthorized withdrawals.

The company's manager then informed users that the remaining 20% of the cryptocurrencies could be accessed only if they refrained from pursuing legal action and agreed to participate in a repayment plan. In response, the counterparties initiated bankruptcy proceedings, asserting that the company was in a state of insolvency. The evaluation of the company's financial instability focused on the legal qualification of the relationship between the platform and its users.

Determining whether the deposit is classified as regular or irregular directly affects the integration of insolvency and, consequently, the application of bankruptcy.

According to Art. 1766 c.c., A deposit contract is an agreement by which one party receives movable property from another party, with the obligation to safeguard it and return it in its original condition⁴⁰⁰. The deposit is irregular if the contract involves a sum of money or other fungible goods, and the depositor grants the depositary the right to use them⁴⁰¹. In this case, the depositary acquires ownership of the goods, with the obligation of returning an equivalent quantity of the same kind and quality.

If the deposit is classified as regular, as the company argued, fulfilling the required standard of diligence and care negates any obligation to return the assets. According to Article 1780 c.c., if the depositary lost the detention of the good without any fault on his part, he is released from his obligation to return the things⁴⁰². As a

⁴⁰⁰ Art. 1766 c.c., original Italian version: “*Il deposito è il contratto col quale una parte riceve dall'altra una cosa mobile con l'obbligo [1771] di custodirla e di restituirla in natura*”.

⁴⁰¹ Art. 1782 c.c., original Italian version: “*Se il deposito ha per oggetto una quantità di danaro o di altre cose fungibili, con facoltà per il depositario di servirsene, questi ne acquista la proprietà ed è tenuto a restituirne altrettante della stessa specie e qualità.*
In tal caso si osservano, in quanto applicabili, le norme relative al mutuo”

⁴⁰² Art. 1780 c.c., original Italian version “*Se la detenzione della cosa è tolta al depositario in conseguenza di un fatto a lui non imputabile, egli è liberato dall'obbligazione di restituire la cosa, ma deve, sotto pena di risarcimento del danno, denunziare immediatamente al depositante il fatto per cui ha perduto la detenzione.*”

supplementary condition, he should immediately notify the depositor of the lost custody. In this regard, the defence claimed the execution of the necessary measure of diligence by the provider society to avoid the loss of goods.

Conversely, if the deposit is deemed irregular, the diligence of the depositary is irrelevant. The depositary acquires in fact the property of the good, with the obligation of returning an equivalent quantity of the same kind and quality. Creditors supported this interpretation, emphasizing the fungible nature of cryptocurrencies. In this case, the depositary retains ownership of the assets and is required to return a corresponding amount of the same nature. Therefore, the impossibility of restoring the creditors implies the application of bankruptcy to compensate part of the obligation. Moreover, while seeking to qualify the deposit as regular, the society didn't notify the creditor about the loss of goods.

Based on findings from the official technical expert, the court rejected the company's interpretation and classified the deposit as irregular. In this case, cryptocurrencies must necessarily be considered fungible assets. While not legal tender, cryptocurrencies are assets of the same nature and quality as they adhere to the same technical protocol. The platform manager had control over the deposited funds and the authority to use them. For instance, the funds deposited in wallets were periodically transferred to a main address controlled exclusively by the platform operator. This practice demonstrated the platform's role as the owner and user of the funds, consistent with an irregular deposit.

The court further highlighted that the platform's terms of use and operational structure reflected the characteristics of an irregular deposit. Users could not independently manage their cryptocurrency holdings because they lacked private keys to execute transactions autonomously. All transactions required the platform's intermediation, further evidencing the platform's control over the assets⁴⁰³.

Based on these considerations, the court qualified the agreement as an irregular deposit and trading contract. This classification imposed on the depositary both ownership of the deposited funds and an obligation to return an equivalent quantity of the same kind and quality. The platform's inability to fulfil this obligation, due to the significant shortfall in assets, established the company's insolvency, justifying the declaration of bankruptcy.

Il depositante ha diritto di ricevere ciò che, in conseguenza del fatto stesso, il depositario abbia conseguito, e subentra nei diritti spettanti a quest'ultimo".

⁴⁰³ Furthermore, the irregular nature of the deposit is evidenced by the platform manager's control over the deposited funds and the authority to use them. Indeed, the society had the control of deposited funds, having the faculty to use them. In particular, only the platform operator could process withdrawal requests, providing for intermediation activity. In addition, the funds deposited by users in wallets were periodically withdrawn and transferred to the main address.

Indeed, the legal nature of the deposit is deducted by the terms of use of the contract, which includes the provision of various services. In this context, the depositary was the only one able to manage the transactions. The users couldn't operate without the service provider's intermediation since they didn't have private keys to action the transactions autonomously.

From this case study, it becomes evident how critical the qualification of contracts as regular or irregular deposits can be. In the case of regular deposits, the application of the necessary diligence could prevent the enforcement of bankruptcy laws, thereby affecting creditors' ability to protect their financial interests. Conversely, if the contract is classified as an irregular deposit, the parties involved are afforded greater protection, as they can more easily seek the restitution of their claims. Nonetheless, this case also highlights the challenges associated with cryptocurrency-based investments. The uncertainty surrounding the nature of the contract and the obligations for restitution in the event of non-compliance translates into a significant risk for investors. Clear legislative guidelines are essential to mitigate these risks and provide a stable legal framework for cryptocurrency-related transactions.

2.3 Consob sanctions ex art. 94 TUF. Why is an energy token a financial instrument? Corte di Appello di Roma n. 5866/2023.

The third case (5866/2023 Corte di Appello di Roma) concerns the classification of energy tokens as financial instruments and the related obligation to publish a prospectus under Article 94, paragraph 1, of the Testo Unico Finanziario (TUF). The Italian financial regulatory authority, Consob, sanctioned a company for not publishing the required prospectus of a public offering.

The company had in fact launched a complex fundraising initiative to develop an innovative photovoltaic panel. To finance the project, blockchain-based tokens were issued and offered for pre-sale to interested investors. According to the promotional materials and the structure of the offering, the tokens granted certain economic advantages to their holders.

Consob authority classified the activity as a financial offering and imposed a sanction on the company. In particular, the missing publication of the prospectus before the offering promotion constituted a violation of Article 94, paragraph 1, of the Testo Unico Finanziario (TUF).

In response, the company appealed Consob's decision to seek its annulment before Corte di Appello di Roma. The company argued that the tokens in question - referred to as energy tokens - could not be classified as financial instruments. It asserted that the tokens were not intended to generate financial returns for their holders but were tools to support innovative renewable energy projects. In particular, these tokens served as economic support tools for renewable energy innovation projects and lacked the typical features of loans or financing instruments.

However, the Court of Appeal found the existence of the elements necessary to classify the activity as financial and confirmed the sanction. The court conducted a detailed analysis of the nature and structure of the tokens, focusing on their economic substance rather than their formal classification. It emphasized that the key determinant for classifying an instrument as financial is its functionality and the expectations it creates among investors. In this case, the tokens were structured in a way that aligned them closely with traditional financial products. Specifically, they offered rights to periodic

financial benefits, including potential returns linked to the profitability of the photovoltaic project.

Moreover, the court outlined a series of factual and legal aspects that allowed the company's conduct to be categorised as a financial activity under the applicable law framework. First, the promotional materials and the accompanying whitepaper explicitly described the tokens as investment opportunities. They outlined financial incentives, such as bonus tokens and profit-sharing arrangements, designed to attract investors. Second, the tokens incorporated elements of risk and reward, similar to those inherent in securities. Investors were required to contribute capital in exchange for tokens that promised returns based on the project's success. These characteristics placed the tokens within the regulatory framework governing public offerings of financial products.

The Court's decision also emphasized the broader regulatory principle that the form or label of an offering is secondary to its economic substance. While the company referred to the tokens as "energy tokens" and portrayed them as tools for environmental innovation, their actual structure and advertised benefits demonstrated their financial nature. This principle serves as a safeguard against attempts to circumvent financial regulations through innovative terminologies or technological mechanisms.

The Court further noted that the absence of tangible harm to investors or completed transactions did not impede the regulatory violation. Under Article 94 of the TUF, the obligation to publish a prospectus arises from the act of making a public offering of financial products, regardless of the outcome. This provision reflects the preventative nature of the regulatory framework, which aims to ensure transparency and protect potential investors from inadequate disclosures or misrepresentations.

The judgment carries significant considerations for the field of blockchain-based fundraising. It underscores that issuers must carefully evaluate whether their token offerings fall within the scope of financial regulations. Even when tokens are marketed as supporting innovative or non-financial projects, their functional characteristics can trigger regulatory obligations. Compliance with existing laws cannot be eluded only by relying on the object of trading. This ruling reinforces the importance of transparency requirements, such as publishing a prospectus, to safeguard investor confidence and market integrity.

Additionally, the case highlights the role of regulatory authorities like Consob in maintaining oversight of new fundraising mechanisms. As financial markets evolve, supervisory authorities like Consob have a growing role in overseeing how financing promotions are conducted, in order to ensure transparency, fair market practice, and consumer protection.

The importance of a transparent market practice is also evidenced by the sanction applied and the role it has in the financial and legal ecosystem. The company claimed in fact that the penalty was excessive, particularly given the lack of evidence of actual investor harm. However, the court argued that the penalty was consistent with the minimum prescribed under the law. The regulatory framework's primary goal is to

prevent potential harm by ensuring compliance with disclosure requirements. The imposition of sanctions serves as a deterrent against non-compliance and reinforces the importance of adhering to legal obligations in public offerings.

2.4 Legal considerations.

The decisions analysed in these three cases represent only a small portion of the broader case law on cryptocurrencies. However, even from this limited sample, it is already possible to see the variety of legal institutions involved. In particular, the three rulings focused on the following areas:

- Corporate contributions, both in cash and in-kind (Art. 2436 c.c., 2464 c.c.).
- The deposit contract and issues related to bankruptcy (Articles 1766 et seq. c.c.)
- The public offering of financial products (Article 94, paragraph 1, TUF)

Articles 2436 and 2464 c.c. respectively govern amendments to the company's articles of association and capital contributions in limited liability companies.

Article 2436 c.c. establishes that the notary who records a shareholders' resolution modifying the articles of association must, within thirty days, verify compliance with legal requirements and request registration with the Companies Register along with the filing of the resolution. However, if the notary finds that the legal conditions have not been met, they must promptly notify the company's directors. Within thirty days, the directors may either call a new shareholders' meeting or challenge the notary's refusal in court. If they do not act, the resolution becomes definitively ineffective.

Article 2464 c.c. governs capital contributions in limited liability companies. It states that capital may be increased through contributions of any asset with economic value (so-called in-kind contributions). However, unless otherwise specified in the articles of association, contributions must be made in cash.

From this, it is clear that contributions can fall into two categories⁴⁰⁴:

- Cash contributions, which are the default;
- In-kind contributions, allowed when the assets have a measurable economic value and are legally permitted.

This analysis pays particular attention to the legal classification of cryptocurrencies and their unsuitability as objects of capital contribution. Applying the rules on contributions requires that the cryptocurrencies can be placed within either cash or in-

⁴⁰⁴ Zanarone, in Comm. Gabrielli, Milano, 2015. The regulation, different from the one of joint-stock company, reaffirms the traditional functions of capital contributions in companies. In particular, these include: (1) the productive function, aimed at providing the company with the necessary resources to pursue its corporate purpose; (2) the protective function for third parties, who, by entering into contractual relationships with the company, can rely on the share capital as the portion of corporate assets that cannot be returned to shareholders to their detriment; (3) the organisational function, which helps define the extent of the rights attributable to each shareholder.

kind contributions. However, the uncertainty surrounding the legal nature of cryptocurrencies is clearly expressed by the Court of Appeal of Brescia. While it acknowledged that cryptocurrencies may technically resemble goods, it argued that functionally, they behave more like money, since they're used to buy goods and as a medium of exchange, though within a limited market.

From this, the court concluded that cryptocurrencies could be considered as a form of money. Still, it stressed that the existing rules can't apply because of the high volatility of crypto assets and the absence of a reliable platform to determine their value. This uncertainty makes it impossible to assign a stable value to a capital increase made in cryptocurrency.

The Tribunale di Roma echoed this position, ruling that crypto assets can't qualify as in-kind contributions. However, it also clarified that this doesn't make cash contributions in cryptocurrency illegal. This clarification seems to suggest a kind of legal grey area, or at least a situation where the lack of legislative guidance is becoming increasingly problematic and calls for a clearer regulatory response.

Articles 1766 et seq. c.c. govern the contract of deposit, which is defined as an agreement in which one party hands over movable property to another, who undertakes to safeguard it and return it in the same condition.

The deposit may be either regular or irregular, depending on whether it involves movable goods or a sum of money (or other fungible items). In the first case, the depositary holds custody of the item. In the second, the depositary becomes its owner, with the obligation to return an equivalent quantity of the same kind and value. Because of this shift in ownership, the rules on loan contracts (*mutuo*) apply to irregular deposits⁴⁰⁵.

The type of deposit also affects the rules governing restitution. In the case of a regular deposit, the depositary must return the same thing received. On the other hand, if the deposit is irregular the depositary is required to return an item of the same kind and quality.

With regard to the obligation of restitution, Article 1768 c.c. states that the depositary must exercise the care of a prudent person in safeguarding the item. The obligation of custody is the core duty in a deposit relationship, defining the standard of care required from the depositary.

According to consistent case law, the duty of custody is considered an obligation of result. This means that the depositary cannot simply prove that they acted with the

⁴⁰⁵ Dalmartello & Portale, (1964), voce *Deposito*, in *Enc. dir.*, XII, Milano. Forchielli, P. (1952), *I contratti reali*, Milano. Galasso, A., & Galasso G., (1989), *Deposito*, in *Dig. civ.* Majello, U. (1958), *Custodia e Deposito*, Napoli. Majello, U. (1961), *Il deposito nell'interesse del terzo*, in *Banca, borsa tit. cred.* 1961, I, 311. Mastropaolo, F. (1988) *Deposito (in generale)*, in *Enc. giur.*, Roma. Salomoni, A. (2014), *La responsabilità del custode per la perdita della detenzione del bene ricevuto*, in *Resp. civ. prev.* 2014, fasc. 5, 1435.

expected level of diligence (as per Article 1768); instead, under Article 1218 c.c., they must show that non-performance was due to a cause not attributable to them⁴⁰⁶.

Article 1780 c.c. further states that if the depositary loses possession of the item due to a cause beyond their control, they are released from the duty to return it, provided they promptly notify the depositor, otherwise they may be liable for damages.

These provisions apply only to regular deposits, where the depositary retains custody but not ownership of the item. In contrast, for irregular deposits, these rules have no relevance because the depositary acquires ownership of the goods. In such cases, the obligation to return arises regardless of any loss, as the asset is fungible, and individual identity is not relevant.

In this case, the company manager claimed that the deposit should be classified as regular, arguing that he was not obligated to return the funds because the loss of the accounts resulted from a cause beyond his control.

However, the court classified the contract as an irregular deposit, based on several key elements: (1) the funds deposited by users were periodically transferred to an account managed exclusively by the platform operator; (2) users could not autonomously withdraw funds from their accounts and had to rely on the intermediary for all transactions; (3) the terms and structure of the contract were consistent with the legal framework of an irregular deposit.

Article 94 TUF regulates the public offering of securities. Specifically, it sets out the disclosure obligations that issuers and offerors must comply with when making a public offer, in order to ensure transparency and protect potential investors.

The general rule established by law is that anyone intending to make a public offering of financial products must first publish a prospectus, which cannot be published until it is approved by Consob⁴⁰⁷.

A public offering is defined as any communication addressed to persons that provides sufficient information about the offer conditions and the financial products offered, to allow an investor to decide whether to purchase or subscribe to the products. This includes offerings made through authorised intermediaries. The prospectus must also include a summary note, written clearly and concisely in non-technical language, in the same language in which the full prospectus was originally drawn up. The format and content of the summary, together with the prospectus, must provide adequate information on the essential features of the financial products, helping investors assess whether to proceed with the investment. A violation of Article 94 TUF leads to the application of the sanction set out in Article 191, par. 1 and 5, TUF.

⁴⁰⁶ Cass. III, No. 22807/2014; Cass. III, No. 20809/2010.

⁴⁰⁷ Sangiovanni, V. (2013), *Commento agli articoli 94 e 95-bis Testo Unico Finanza*, in *Commentario breve al diritto dei consumatori* (p.1916-1927) a cura di Giovanni De Cristofaro, Alessio Zaccaria, Cedam.

The Court, in rejecting the company's appeal, outlined a set of criteria indicating the financial nature of the tokens, stressing that the focus should be on their substance rather than their formal classification. In particular, the Court identified several key indicators of a financial activity:

1. The functionality of the token and the expectations it creates among investors;
2. The content of promotional materials and the whitepaper, which explicitly described the tokens as investment opportunities;
3. The presence of elements of risk and reward, similar to those found in traditional financial products.

These factual criteria can certainly assist the interpreter in reconstructing the legal nature of the token.

3. Conclusions

The decisions examined in this article illustrates how Italian courts have sought to adapt traditional legal principles to the challenges posed by crypto-assets, while also revealing the limits of the current regulatory framework.

All these rulings deal with different legal matters, but they share a common feature: the need to clarify which rules apply when cryptocurrencies are involved.

Indeed, current legislation does not always provide a clear and univocal solution, particularly when legal relations involve novel objects such as crypto-assets. As seen in Tribunale di Roma, n. 7932/2022, concerning a corporate capital increase through cryptocurrencies, the court did not identify any explicit legal prohibition. Nonetheless, it ruled out the admissibility of such contributions due to the extreme volatility of the asset. This exclusion was derived from general principles of the legal system. Specifically, the protection of creditors and the need for capital to be certain and measurable prevented an asset with high volatility from qualifying as a valid contribution. Still, it is through the application of such general principles – including technological neutrality – that the court reached this conclusion.

However, given the widespread use of cryptocurrencies, these evaluations should ideally fall under the exclusive competence of the legislature, to avoid conflicting interpretations at the level of merit courts.

In other cases, such as those involving contractual arrangements, contractual autonomy does not prevent the use of innovative models of transaction. The analysis of the facts in Tribunale di Firenze, n. 18/2019 led to the classification of the agreement as an irregular deposit. The emergence of new contractual forms is not a rare phenomenon. In the Italian legal system, the principle of contractual freedom allows for such flexibility, provided that public order, mandatory rules, and the licit object requirement are respected as provided under Italian law.

By contrast, when public interests are at stake - such as investor protection and market transparency - public law limitations apply. This was evident in Corte di Appello di

Roma (n. 5866/2023), where the issuance of so-called *energy tokens* was deemed a financial offering. Despite their innovative character and environmental purpose, the court focused on their economic substance. The decision reaffirmed that technological innovation does not exempt issuers from complying with the disclosure obligations of financial regulation, especially when tokens offer financial benefits to investors.

Unlike the cases analysed of the Suprema Corte di Cassazione, merit decisions concern a variety of legal fields and are not limited to strictly financial matters. Each case illustrates different challenges that arise in real-world transactions and reflects the legal uncertainty often surrounding the use of crypto-assets.

The decisions analysed in this article confirm that the main legal challenges surrounding crypto-asset transactions arise from their hybrid legal nature and technological complexity. Italian merit courts have adopted a case-by-case interpretative approach, grounding their reasoning in fundamental principles such as contractual autonomy, legal certainty, and technological neutrality. While this approach has ensured continuity in the application of existing legal frameworks, it also reveals the need for legislative responses to address the specific features of decentralised technologies and to protect both private and public interests.

The analysis also highlights the essential role played by lower courts in interpreting and applying legal provisions to new technological contexts. These cases demonstrate how interpreting transactions involving digital assets often requires a detailed factual reconstruction and, at times, even technical expert advice (c.t.u). The interpretative work undertaken by judges and legal counsel offers valuable guidance. For instance, in decision n. 5866/2023, Corte di Appello di Roma sets out a series of criteria to determine whether an activity qualifies as financial. Similarly, in ruling no. 18/2019, Tribunale di Firenze identifies key indicators for establishing whether the assets deposited had effectively become the property of the platform operator. In other cases - such as decision no. 7932/2022 - reasoning becomes more nuanced, especially when there are broader interests protected by law, such as creditor protection.

The detailed analysis of this case law is also useful to identify recurring patterns related to the use of cryptocurrencies. Recognising these trends is essential for anticipating and possibly preventing similar legal disputes in the future. This emerging body of jurisprudence should serve as a signal to the Legislator, pointing to the need for clearer rules.

Finally, this chapter highlights the issues that arise before the courts and concern, or will concern, consumers. The existence of a risk may in fact result in a breach of contract or in damage. When a consumer turns to the judge for protection, the range of legal remedies available depends on the rules established by the legal system for their protection. In the case of banking or private law contracts, the applicable legislation is that of the civil code. As seen in the example of deposits, the entire liability regime changes depending on the legal classification of the relationship. These findings demonstrate that the risks consumers face are not only those occurring upstream, but also legal ones, which concern the qualification of their relationship and the protection available before the courts.

As discussed in previous chapters, the new European regulatory instruments - the MiCA Regulation and the DLT Pilot Regime - do not revise or adapt existing legal institutions. Instead, they focus primarily on the authorisation regime, while the application of civil and commercial law continues to depend on the national laws of Member States, in line with the principle of technological neutrality. For these reasons, the role of domestic case law remains central to shaping the legal contours of cryptocurrency transactions.

Conclusions

This thesis aimed to analyse crypto assets and decentralised finance in order to understand their risks and to determine whether the approach adopted by the European legislator represents an effective solution. In particular, it sought to answer the following research questions:

- What are crypto assets and decentralised finance?
- What are the risks that consumers face related to crypto assets and decentralised finance?
- Does the European regulatory framework address risks related to crypto assets and decentralised finance?

The study showed that crypto assets and decentralised finance represent a growing phenomenon that carries significant risks, especially for inexperienced consumers and investors. The European legislator's approach is an important step forward, introducing improvements to the crypto-asset market. However, some problematic scenarios remain uncovered. The analysis of case law proves to be an effective tool for enhancing consumer protection and for shaping more effective legislation.

Having clarified this premise, it is appropriate to retrace the discussion developed throughout this work.

The first chapter introduced the origins and evolution of crypto assets, illustrating their economic and technological foundations. It explained their diffusion and the different categories, showing how they gradually evolved into complex financial instruments. In particular, it clarified that crypto assets are currencies without legal tender status, which can be exchanged through blockchain technology and implemented via smart contracts. Their function and stability vary depending on their structure.

The second chapter examined the concept of decentralised finance, which still lacks a uniform and legally recognised definition. Decentralised finance is a purely decentralised system in which no intermediaries operate and where market participation is fully democratic. There are no intermediaries, only the blockchain. The technology aims to decentralise platform management, automate protocols, and increase the efficiency of financial products and services.

From these first two chapters, it became clear that crypto assets and decentralised finance are interdisciplinary phenomena. They are not only technological, but also economic and legal. They aim to replace traditional finance by reducing costs and simplifying access to credit. These aspects certainly represent an advantage for the free market, but also a risk for consumers. As shown in the third chapter, the risks that consumers may face are significant and not always easy to detect. Two main categories of risk have been identified. The first concerns the lack of financial knowledge on the part of consumers. The second concerns intentional misconduct by fraudsters and criminal organisations. One thing is clear: the Internet is fertile ground for the spread of misleading information, advertisements, and especially fraud.

As shown in the fourth chapter, the legislator did not remain passive in the face of these challenges. Through a series of digital and financial policies, the EU adopted three key regulations to govern the crypto-asset market. These measures mainly introduced requirements and standards that providers must meet in order to operate within Europe, and granted supervisory and regulatory powers to national and European authorities.

The fifth chapter analysed national case law, demonstrating that identifying consumer risks is also possible through judicial decisions. This analysis should be taken into account in future EU legislation to ensure the adoption of more effective consumer remedies. The cases analysed show that courts often deal with the application of contract law, commercial law, and company law.

This fifth chapter provides the basis to answer the research questions. It demonstrates that consumer risks are not only those described in empirical literature, but also those that arise before courts. The decision concerning deposit contracts shows that liability rules depend on the legal qualification of the contract, which may significantly affect the consumer's right to restitution. The same reasoning applies to company contributions. Legal uncertainty about their admissibility is justified by the volatility and unstable value of cryptocurrencies. However, since this was a decision by a lower court and no EU rule explicitly excludes crypto assets from being used as company contributions, future judges may decide differently. Such divergence could harm creditors whose claims may not be satisfied if the contributed asset loses value.

This thesis aimed to demonstrate that we are witnessing a phenomenon with uncertain and risky legal outcomes. These risks, related to the legal classification of assets and the lack of clarity regarding which legal framework applies, are not fully addressed by the EU legislator.

This does not mean that the MiCA Regulation is not a useful and effective instrument for consumer protection. On the contrary, the compliance requirements and the supervisory powers granted to authorities provide a preventive tool to exclude from the market operators that do not meet minimum standards of reliability. The decision to adopt a regulation as the legislative instrument signals the EU's intention to unify the legal framework in this area.

Nevertheless, some uncertainties remain. One example is the provision on civil liability, which places the burden of proof on the token holder, meaning on the consumer. It is questionable how shifting the burden of proof to the weaker party can effectively protect them. Similar concerns arise regarding the absence of specific regulation for fully decentralised markets, which represent the majority of crypto operations. While some products sold on these markets fall under financial legislation, others do not possess the characteristics of financial instruments.

This does not imply that the legislator should regulate every technological aspect. The principle of technological neutrality prevents such an approach and promotes a neutral, activity-based perspective. However, when empirical evidence reveals interpretative

uncertainty and a lack of legal certainty, a more targeted legislative approach should be adopted.

Leaving these doubts unresolved carries the risk that each European country may apply different rules and remedies. This could lead to inconsistent judicial decisions across Member States, undermining the very objective of a common and coherent European policy.

Ultimately, this study highlights the need for continuous legal adaptation to ensure that innovation and consumer protection evolve together within the European digital economy.

Bibliography

- Abramowicz, M. (2016). Cryptocurrency-based law. *Ariz. L. Rev*, 58(359).
- Agnino F., Vendita di bitcoin e intermediazione finanziaria abusiva, Cass. Pen. sez. II, 17 settembre 2020, n. 26807, IUS Penale, fasc., 2020.
- Alcorta, J. G. (2025). Regulating stablecoins in the European Union. Asset-Referenced tokens and E-Money tokens. In *Law, governance and technology series* (pp. 147–176). https://doi.org/10.1007/978-3-031-74889-9_7
- Alekseenko, A. P. (2023). Model Framework for Consumer Protection and Crypto-Exchanges Regulation. *Journal of Risk and Financial Management*, 16(7), 305. <https://doi.org/10.3390/jrfm16070305>
- Allam, Z. (2018). On Smart Contracts and Organisational Performance: A Review of Smart Contracts through the Blockchain Technology. *Review of Economic and Business Studies*, 11(2), 137–156. <https://doi.org/10.1515/rebs-2018-0079>
- Amstad, M. (2019). Regulating Fintech: Objectives, principles, and practices. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3491982>
- Andola, N., Raghav, N., Yadav, V. K., Venkatesan, S., & Verma, S. (2021). Anonymity on blockchain based e-cash protocols—A survey. *Computer Science Review*, 40, 100394. <https://doi.org/10.1016/j.cosrev.2021.100394>
- Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys*, 36(4), 335–371. <https://doi.org/10.1145/1041680.1041681>
- Annunziata, F. (2023). An overview of the markets in Crypto-Assets Regulation (MICAR). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4660379>
- Arner, D. W., Barberis, J. N., & Buckley, R. P. (2015). The evolution of Fintech: a new Post-Crisis paradigm? *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2676553>
- Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Frontiers in Blockchain*, 6. <https://doi.org/10.3389/fbloc.2023.1151724>
- Attico, N. (2018). *Blockchain. Guida all’ecosistema. Tecnologia, business, società*. goWare & Guerini Next.

Averin, A., Musaev, E., & Rukhlov, P. (2021). Review of existing Blockchain-Based insurance solutions. *2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 140–143. <https://doi.org/10.1109/itqmis53292.2021.9642748>

Averin, A., Samartsev, A., & Sachenko, N. (2020). Review of Methods for Ensuring Anonymity and De-Anonymization in Blockchain. In *2020 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 82–87). <https://doi.org/10.1109/itqmis51053.2020.9322974>

Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure*. <http://nakamotoinstitute.org/static/docs/hashcash.pdf>

Banca d'Italia. (2006). *Recepimento della nuova regolamentazione prudenziale internazionale (nuovo accordo sul capitale di Basilea e nuova direttiva c.e. sui requisiti di capitale delle banche e delle imprese di investimento)*. https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Doc_Cons_Rischi_operativi.pdf

Barberis, J. (2012). The rise of Fintech. In https://thefintechbook.com/media/uploads/resources/reports/fintech.hk/2015/07/14/05_30_48/The%20Rise%20of%20FinTech%20-%20Nov%20-14.pdf.

Battaglini, R., & Giordano, M. (2019). *Blockchain e smart contract. Funzionamento, profili giuridici e internazionali, applicazioni pratiche*. Lefebvre Giuffrè.

Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital Time-Stamping. In *Springer eBooks* (pp. 329–334). https://doi.org/10.1007/978-1-4613-9323-8_24

Bele, D. (2020). Financial scams, frauds, and threats in the digital age. In *Modern approaches to knowledge management development: collective monograph* (pp. 39–50). Ljubljana School of Business.

Bernoville, T. (2024, December 13). *ESG risk: Definition and best practices to mitigate it*. Plan a Academy. Retrieved September 15, 2025, from <https://plana.earth/academy/esg-risk#:~:text=ESG%20risk%20refers%20to%20environmental,%2C%20social%2C%20and%20governance%20factors.>

Bertino, E., Kundu, A., & Sura, Z. (2019). Data Transparency with Blockchain and AI Ethics. *Journal of Data and Information Quality*, 11(4), 1–8. <https://doi.org/10.1145/3312750>

Bianca, C. M. (1987), *Diritto Civile*, III, Il Contratto, Giuffrè, Milano, p. 31.

Bindseil, U., & Pantelopoulos, G. (2023). Unbacked Crypto-Assets, stablecoins and CBDC. In *Springer texts in business and economics* (pp. 125–152). https://doi.org/10.1007/978-3-031-39520-8_9

Biryukov, A., & Tikhomirov, S. (2019). Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. <https://doi.org/10.1109/eurosp.2019.00022>

Borgogno, O. (2018). Smart Contracts as the (new) Power of the Powerless? The Stakes for Consumers. *European Review of Private Law/Revue Européenne De Droit Privé/Europäische Zeitschrift Für Privatrecht*, 26(Issue 6), 885–902. <https://doi.org/10.54648/erpl2018060>

Brooks, S., Jurisevic, A., Spain, M., & Warwick, K. (2018). *A decentralised payment network and stablecoin*. https://cryptorating.eu/whitepapers/Havven/havven_whitepaper.pdf

Buterin, V. (2013). Ethereum White Paper. *GitHub Repository*. https://static.peng37.com/ethereum_whitepaper_laptop_3.pdf

Cannarsa, M. (2018). Interpretation of contracts and smart contracts: smart interpretation or interpretation of smart contracts? *European Review of Private Law/Revue Européenne De Droit Privé/Europäische Zeitschrift Für Privatrecht*, 26(Issue 6), 773–785. <https://doi.org/10.54648/erpl2018054>

Capaccioli, S. (2016). Smart contracts: traiettoria di un'utopia divenuta attuabile. *Cyberspazio E Diritto (Mucchi Editore)*, 17(55).

Carratta, A. (2006). La riforma del giudizio in Cassazione. In *Riv. trim. dir. proc. civ* (p. 1117).

Carresi, F. (1987), *Il contratto*, in Trattato Cicu Messineo Mengoni, Milano.

Cataudella, A. (2000) *I contratti, Parte generale*, Torino.

Cesareo, T. (2020). L'illecito al confine tra truffa contrattuale e inadempimento civilistico. *Cammino Diritto*, 3/2020. https://rivista.camminodiritto.it/public/pdfarticoli/4808_3-2020.pdf

Chen, Y., & Bellavitis, C. (2019). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13, e00151. <https://doi.org/10.1016/j.jbvi.2019.e00151>

Chierici, M. (2018). La blockchain: una lettura giuridica per uno sguardo verso il futuro. *Cyberspazio E Diritto*, 19(61), 385–419.

Chikh, F. (2024). Cryptocurrencies: An etymological approach. *International Journal of Economic Perspectives*, 18(7), 1057–1064.

Chiomenti. (2023). *L'attuazione del Digital Finance Package a tre anni dalla proposta*. https://www.chiomenti.net/media/filer_public/4f/68/4f68c9bb-51e2-4d79-b88d-88a34d564156/newsletter-dora-n1-2023-004-_1.pdf

Chohan, U. W. (2021). Non-Fungible Tokens: blockchains, scarcity, and value. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3822743>

Christopher, C. M. (2024). Recognizing DAOs as legal entities: Balancing public policy, innovation, and consistency. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5220994>

Cian, M. (2023). Noterelle su finanziarietà e non finanziarietà nei crypto-assets: la Suprema Corte sulla natura del servizio di exchange. *Banca Borsa Titoli di Credito: rivista di dottrina e giurisprudenza*, 76(2), 8.

Čižinská, R., Krabec, T., & Venegas, P. (2016). FieldsRank: the network value of the firm. *International Advances in Economic Research*, 22(4), 461–463. <https://doi.org/10.1007/s11294-016-9604-x>

Commodity Futures Trading Commission. (2018). *A Primer on Smart Contracts*. https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf

Consob. (2019). *Le offerte iniziali e gli scambi di crypto-attività*. https://www.consob.it/documents/1912911/1972122/doc_disc_20190319.pdf/2044537e-487c-5093-112e-3eacc69b12d4

Corrales, M., Fenwick, M., & Haapio, H. (2019). Legal tech, smart contracts and blockchain. In *Perspectives in law, business and innovation*. <https://doi.org/10.1007/978-981-13-6086-2>

Corrales, M., Fenwick, M., & Haapio, H. (2019). *Legal tech, smart contracts and blockchain*. Springer.

Dalmartello & Portale (1964), voce *Deposito*, in *Enc. dir.*, XII, Milano.

Das, A. S., Sumathy, M., & Nabeel K., M. (2024). Fintech Innovations In Medicine: Transforming Healthcare Through Financial Technology. *Research Explorer*, XII(42), 109–112. https://www.researchgate.net/publication/381887171_Fintech_Innovations_In_Medicine_Transforming_Healthcare_Through_Financial_Technology

De Filippi, P., Wray, C., & Sileno, G. (2021). Smart contracts. *Internet Policy Review*, 10(2). <https://doi.org/10.14763/2021.2.1549>

De La Roche W., M., & Zichichi, M. (2023). Bringing clarity to the DeFi sector: A cross-sector proposal for a unified DeFi definition. In *IOTA Foundation*. https://files.iota.org/comms/Bringing_clarity_to_the_DeFi_sector.pdf

Delfini, F. (2022). Le discipline a tutela del consumatore e il coordinamento con la proposta di Regolamento MiCA. *Osservatorio Del Diritto Civile E Commerciale*, 267–294. <https://doi.org/10.4478/106711>

Di Ciommo, F. (2019). Smart contract e (non-)diritto: il caso dei mercati finanziari. *Nuovo Diritto Civile*, 1, 257–295. <https://www.diciommoandpartners.com/wp-content/uploads/2020/09/Smart-contract-x-Nuovo-dir.-civ..pdf>

Duke, A. (2019). What does the CISG have to say about smart contracts? A legal analysis. *Chicago Journal of International Law*, 20(1), 4. <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1755&context=cjil>

Ellinger, E. W., Mini, T., Gregory, R. W., & Dietz, A. (2023). Decentralized Autonomous Organization (DAO): The case of MakerDAO. *Journal of Information Technology Teaching Cases*, 14(2), 265–272. <https://doi.org/10.1177/20438869231181151>

EUBlockchain Observatory and Forum. (2022). Decentralised Finance (DeFi). In <https://blockchain-observatory.ec.europa.eu>. https://blockchain-observatory.ec.europa.eu/publications/decentralised-finance_en?prefLang=sv

Eurojust. (2025, September 23). *Eurojust coordinates action to halt cryptocurrency fraud of over 100 million euros across Europe*. eurojust.europa.eu. Retrieved October 12, 2025, from <https://www.eurojust.europa.eu/news/eurojust-coordinates-action-halt-cryptocurrency-fraud-over-100-million-euros-across-europe>

European Commission. (2018). *FinTech Action plan: for a more competitive and innovative European financial sector* (COM(2018) 109 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109>

European Commission. (2021). *Market in Crypto Assets (MICA)* (PE 739.221). European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI\(2022\)739221_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI(2022)739221_EN.pdf)

European Commission. (2022). *European Financial Stability and Integration Review* (SWD(2022) 93 final/2). https://finance.ec.europa.eu/system/files/2022-04/european-financial-stability-and-integration-review-2022_en.pdf

European Securities and Market Authority. (2023). *Decentralised Finance in the EU: Developments and risks* (No. ESMA50-2085271018–3349). ESMA Economics, Financial Stability and Risk Department. <https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018->

3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf

European Securities and Markets Authority. (2017). *Initial Coin Offerings and Crypto-Assets*. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

Europol. (2025, June). *Crypto investment fraud ring dismantled in Spain after defrauding 5000 victims worldwide*. europol.europa.eu. Retrieved October 12, 2025, from <https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide#:~:text=The%20investigation%20identified%20that%20the,Islands%20and%20%20in%20Madrid>)

Fahim, S., Rahman, S. K., & Mahmood, S. (2023). Blockchain: A Comparative Study of Consensus Algorithms POW, POS, POA, POV. *International Journal of Mathematical Sciences and Computing*, 9(3), 46–57. <https://doi.org/10.5815/ijmsc.2023.03.04>

Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., & Li, L. (2022). Cryptocurrency trading: a comprehensive survey. *Financial Innovation*, 8(1). <https://doi.org/10.1186/s40854-021-00321-6>

Fazzalari, E., ‘sentenza civile’ in Enc. Dir. [XLI 1989], Giuffrè, Milano.

Feller, W. (1958). An introduction to probability theory and its applications. *Journal of the Franklin Institute*, 265(1), 73–74. [https://doi.org/10.1016/0016-0032\(58\)90688-4](https://doi.org/10.1016/0016-0032(58)90688-4)

Financial Services and Markets Authority. (2025). Investment fraud and unlawful offers - Dashboard 2nd half of 2024. In *fsma.be*. Retrieved October 12, 2025, from https://www.fsma.be/sites/default/files/media/files/2025-01/20250116_dashboard_investment_fraud.pdf

Fletcher, E. (2022). Reports show scammers cashing in on crypto craze. In *ftc.gov*. Federal Trade Commission. <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze>

Forchielli, P. (1952) *I contratti reali*, Milano.

Franco, P. (2014). *Understanding Bitcoin: Cryptography, engineering and economics*. <http://ci.nii.ac.jp/ncid/BB17851910>

Franza E., Attuazione del MiCA, le novità del decreto 129/2024, [dirittobancario.it](https://www.dirittobancario.it/art/attuazione-mica-le-novita-del-decreto-129-2024/#:~:text=protezione%20degli%20investitori,Il%20Decreto%20Legislativo%20n.,in%20base%20alle%20rispettive%20competenze), 2024, <https://www.dirittobancario.it/art/attuazione-mica-le-novita-del-decreto-129-2024/#:~:text=protezione%20degli%20investitori,Il%20Decreto%20Legislativo%20n.,in%20base%20alle%20rispettive%20competenze>

- Galasso A. & Galasso G., (1989) *Deposito*, in *Dig. civ.*
- Galgano, F. (2002) voce *Negoziio Giuridico (Diritto Privato)*, in Enc. Del diritto, vol. XXVII, Giuffrè, Milano, p. 934.
- Galgano, F. (2011), *Il contratto*, Padova.
- Gaschi, A., & Portale, V. (n.d.). La definizione di blockchain e distributed Ledger, in blockchain e smart contract. In *Blockchain e Smart Contract*. Lefebvre Giuffrè.
- Gazzoni, F. (1987), *Manuale di Diritto Privato*, Edizioni Scientifiche Italiane, Napoli, p. 713.
- Giglio, F. (2021). Fintech: a Literature Review. *EUROPEAN RESEARCH STUDIES JOURNAL*, XXIV(Issue 2B), 600–627. <https://doi.org/10.35808/ersj/2254>
- Giura, G., & De Felice, D. (2016). Selettività della giurisprudenza di merito: giudizio di legittimità e giurisprudenza locale. *Sociologia del diritto*: 1, 2016, 135-158.
- Goldenfein, J., & Leiter, A. (2018). Legal engineering on the blockchain: ‘Smart contracts’ as legal conduct. *Law And Critique*, 29(2), 141–149. <https://doi.org/10.1007/s10978-018-9224-0>
- Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *Proceedings on Privacy Enhancing Technologies*, 2018(4), 179–199. <https://doi.org/10.1515/popets-2018-0038>
- Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, 26(4), 377–409. <https://doi.org/10.1007/s10506-018-9223-3>
- Grassi, L., & Fantaccini, S. (2022). An overview of Fintech applications to solve the puzzle of health care funding: state-of-the-art in medical crowdfunding. *Financial Innovation*, 8(1). <https://doi.org/10.1186/s40854-022-00388-9>
- Grigg, I. (2004). The Ricardian contract. In *Proceedings. First IEEE International Workshop on Electronic Contracting* (pp. 25–31). <https://doi.org/10.1109/wec.2004.1319505>
- Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99–111. <https://doi.org/10.1007/bf00196791>
- Haber, S., & Stornetta, W. S. (1997). Secure names for bit-strings. In *Procedings of the 4th ACM Conference on Computer and Communications Security* (pp. 28–35). <https://doi.org/10.1145/266420.266430>

Hammi, B., Zeadally, S., & Perez, A. J. (2023). Non-fungible tokens: A review. *IEEE Internet of Things Magazine*, 46–50.

HM Treasury. (2023). *Future financial services regulatory regime for cryptoassets: Consultation and Call for Evidence*. https://assets.publishing.service.gov.uk/media/63d94ea68fa8f51881c99eb4/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf

Ioini, N. E., & Pahl, C. (2018). A review of distributed ledger technologies. *Lecture Notes in Computer Science*, 277–288. https://doi.org/10.1007/978-3-030-02671-4_16

ISDA & Linklaters. (2017). *Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective*. <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>

Iyengar, R. (2020, July 16). Twitter blames ‘coordinated’ attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others. *CNN Business*. <https://edition.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html>

Jaikaran, C. (2018). *Blockchain: Background and Policy Issues* (No. R45116). Congressional Research Service. <https://www.congress.gov/crs-product/R45116>

Jalal, A., Mubarak, M. A., & Durani, F. (2023). Financial Technology (Fintech). In *Artificial Intelligence and Transforming Digital Marketing* (Vol. 487, pp. 525–536). Studies in Systems, Decision and Control, Springer. https://doi.org/10.1007/978-3-031-35828-9_45

Jensen, J., Von Wachter, V., & Ross, O. (2021). An introduction to Decentralized Finance (DEFI). *Complex Systems Informatics and Modeling Quarterly*, 26, 46–54. <https://doi.org/10.7250/csimq.2021-26.03>

Kamecke, U., & T. Korber. (2008). Technological neutrality in the EC regulatory framework for electronic communications: A good principle widely misunderstood. *European Competition Law Review*, 29(5), 330. https://koerber.jura.uni-koeln.de/sites/koerber/user_upload/Technological_neutrality_in_the_EC_.Kamecke-Koerber_ECLR08_29_5__330-339.pdf

Kareem, Y., Djenouri, D., & Ghadafi, E. (2024). A survey on emerging blockchain technology platforms for securing the internet of Things. *Future Internet*, 16(8), 285. <https://doi.org/10.3390/fi16080285>

Karu, C. (2021, July 8). Brazil’s ‘Bitcoin King’ arrested over alleged \$300M embezzlement. *CoinGeek*. <https://coingeek.com/brazil-bitcoin-king-arrested-over-alleged-300m-embezzlement/>

- Khan, A., & Sandner, P. (2024). DeFi: an overview of use cases and a status quo analysis of the ecosystem. In *Edward Elgar Publishing eBooks* (pp. 5–34). <https://doi.org/10.4337/9781035307760.00006>
- Kim, Y., Choi, J., Park, Y., & Yeon, J. (2016). The adoption of mobile payment services for “Fintech.” *International Journal of Applied Engineering Research*, 11(2), 1058–1061. <http://scholarworks.bwise.kr/ssu/handle/2018.sw.ssu/34412>
- Kochergin, D. (2022). Crypto-assets: Economic Nature, Classification and Regulation of Turnover. *International Organisations Research Journal*, 17(3), 75–130. <https://doi.org/10.17323/1996-7845-2022-03-04>
- Koushal, A. (2024, August 7). *How Fintech and Big Data Analytics Work Together*. LinkedIn. Retrieved June 6, 2025, from <https://www.linkedin.com/pulse/how-fintech-big-data-analytics-work-together-anurag-koushal-8eync/>
- Liao, G. Y., & Caramichael, J. (2022). Stablecoins: growth potential and impact on banking. *International Finance Discussion Paper*, 2022.0(1334), 1–26. <https://doi.org/10.17016/ifdp.2022.1334>
- Lin, I., & Liao, T. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, 19(5), 653–659. [https://doi.org/10.6633/ijns.201709.19\(5\).01](https://doi.org/10.6633/ijns.201709.19(5).01)
- Lončarski, I. (2016). Risk Management (2016). *Risk Management*, 18(1), 1–3. <https://doi.org/10.1057/rm.2016.2>
- Madir, J. (2024). Smart contracts. In *Fintech* (pp. 244–267). <https://doi.org/10.4337/9781035314751.00020>
- Maier, E. (2016). Supply and demand on crowdlending platforms: connecting small and medium-sized enterprise borrowers and consumer investors. *Journal of Retailing and Consumer Services*, 33, 143–153. <https://doi.org/10.1016/j.jretconser.2016.08.004>
- Majello, U. (1958), *Custodia e Deposito*, Napoli.
- Majello, U. (1961), *Il deposito nell'interesse del terzo*, in *Banca, borsa tit. cred.*, I, 311;.
- Manente, M. (2019). L.12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note. www.notariato.it.
- Martino, E. D. (2022). Regulating Stablecoins as Private Money. A Critical Take on the EU Proposal between Liquidity and Safety. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4203885>

Masood, F., & Faridi, A. R. (2018). Consensus Algorithms In Distributed Ledger Technology For Open Environment. In *2018 4th International Conference on Computing Communication and Automation (ICCCA)* (pp. 1–6). <https://doi.org/10.1109/ccaa.2018.8777695>

Massey, A. (2014). *High-frequency trading: Elements, Considerations, Perspectives*. Nova Science Publishers.

Mastropaolo, F. (1988), *Deposito (in generale)*, in *Enc. giur.*, Roma.

Maull, R., Godsiff, P., Mulligan, C., Brown, A., & Kewell, B. (2017). Distributed ledger technology: Applications and implications. *Strategic Change*, 26(5), 481–489. <https://doi.org/10.1002/jsc.2148>

Menezes, A. J., Vanstone, S. A., & Van Oorschot, P. C. (1997). Handbook of applied cryptography. *Choice Reviews Online*, 34(08), 34–4512. <https://doi.org/10.5860/choice.34-4512>

Merkle, R. C. (1980). Protocols for public key cryptosystems. *IEEE Symposium on Security and Privacy*, 122–133. <https://doi.org/10.1109/sp.1980.10006>

Meyer, E., Welp, I. M., & Sandner, P. G. (2021). Decentralized Finance—A systematic literature review and research directions. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4016497>

Mhlanga, D. (2024). The role of big data in financial technology toward financial inclusion. *Frontiers in Big Data*, 7. <https://doi.org/10.3389/fdata.2024.1184444>

Micu, I., & Micu, A. (2016). Financial Technology (Fintech) and its implementation on the Romanian non-banking capital market. *SEA - Practical Application of Science*, 11, 379–384. <https://doaj.org/article/450238100bd1405fb401a1eafd533fac>

Mignon, V. (2019). Blockchains - perspectives and challenges. In *Edward Elgar Publishing eBooks*. <https://doi.org/10.4337/9781788115131.00007>

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law Innovation and Technology*, 9(2), 269–300. <https://doi.org/10.1080/17579961.2017.1378468>

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law Innovation and Technology*, 9(2), 269–300. <https://doi.org/10.1080/17579961.2017.1378468>

Milutinović, M. (2018). Cryptocurrency. *Ekonomika*, 64(1), 105–122. <https://doi.org/10.5937/ekonomika1801105m>

Mirabelli, G. (1980), *Dei contratti in generale*, in Comm. Utet, Torino.

- Moin, A., Sirer, E. G., & Sekniqi, K. (2019). A classification framework for Stablecoin designs. *arXiv (Cornell University)*. <https://doi.org/10.48550/arxiv.1910.10098>
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
- Ortolani, P. (2019). Decentralized Anonymous Organizations: inquadramento giuridico de jure condito e prospettive de jure condendo. In *Blockchain e Smart Contract*. Giuffrè.
- Palmieri, M. (2020). Offerte al pubblico e sollecitazione al risparmio. In *Il Testo Unico Finanziario* (Vol. 2, p. 1301). Zanichelli.
- Panisi, F. (2017). Blockchain and “Smart Contracts”: FinTech innovations to reduce the costs of trust. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3066543>
- Patti, L. (2016). Dal codice civile al codice binario: blockchain e smart contracts. *Cyberspazio E Diritto*, 325–344.
- Perna, A. (2015). Le origini della blockchain. In *Blockchain e Smart Contract*. Lefebvre Giuffrè.
- Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review*, 10(2). <https://doi.org/10.14763/2021.2.1561>
- Pilkington, M. (2016). Blockchain technology: principles and applications. In *Edward Elgar Publishing eBooks*. <https://doi.org/10.4337/9781784717766.00019>
- Polyviou, A., Velanas, P., & Soldatos, J. (2019). Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies. *MDPI*, 7. <https://doi.org/10.3390/proceedings2019028007>
- Puorro, A. (2013). High frequency trading: una panoramica (High frequency trading: an overview). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2369311>
- Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, 59(1), 69–76. <https://doi.org/10.1007/s12599-017-0464-6>
- Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, 52, 102039. <https://doi.org/10.1016/j.seta.2022.102039>
- Ratecka, P. (2020). Zjawisko FinTech – ujęcie definicyjne, taksonomiczne oraz historyczne. *Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej W Tarnowie*, 45(1), 53–67. <https://doi.org/10.25944/znmwse.2020.01.5367>

Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2018). Distributed Ledger Technology Systems: a Conceptual framework. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3230013>

Razzante, R. Le cripto attività come prodotti finanziari. A proposito di Cass. Pen., Sez. II, 22 novembre 2022, n. 44378.

Roppo, V. (2006), *Trattato del contratto*, Vol. 7, Milano. Gallo, P. (2000) *Trattato del contratto*, Vol. 3, Torino.

Roppo, V. (2011) *Il contratto*, Milano, 2011; Betti, E. (1943), *Teoria generale del negozio giuridico*, Napoli.

Roukny, T. (2022). *Decentralized finance: Information Frictions and Public Policies : Approaching the Regulation and Supervision of Decentralized Finance*. Publications Office of the European Union. <https://doi.org/10.2874/444494>

Saccone, U. (2014). Lo sviluppo di un sistema antifrode: considerazioni programmatiche e ruolo della Security. In www.sicurezzanazionale.gov.it.

Salomoni, A. (2014) *La responsabilità del custode per la perdita della detenzione del bene ricevuto*, in *Resp. civ. prev.* 2014, 5, 1435.

Sangiovanni, V. (2013), Commento agli articoli 94 e 95-bis Testo Unico Finanza, in *Commentario breve al diritto dei consumatori* (p.1916-1927) a cura di Giovanni De Cristofaro, Alessio Zaccaria, Cedam.

Sarzana Di S. Ippolito, F., & Nicotra, M. (2018). *Diritto della Blockchain, Intelligenza artificiale e Iot*. Wolters Kluwer Italia.

Scharfman, J. (2023a). Introduction to cryptocurrency and digital asset fraud and crime. In *Springer eBooks* (pp. 1–16). https://doi.org/10.1007/978-3-031-23679-2_1

Scharfman, J. (2023b). The Cryptocurrency and Digital Asset Fraud Casebook. In *Springer eBooks*. <https://doi.org/10.1007/978-3-031-23679-2>

Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *Proceedings first international conference on peer-to-peer computing* (pp. 101–102). <https://doi.org/10.1109/p2p.2001.990434>

Schueffel, P. (2017). Taming the Beast: A scientific definition of Fintech. *Journal of Innovation Management*, 4(4), 32–54. https://doi.org/10.24840/2183-0606_004.004_0004

Schueffel, P. (2021). DEFI: Decentralized Finance - An Introduction and Overview. *Journal of Innovation Management*, 9(3), I–XI. https://doi.org/10.24840/2183-0606_009.003_0001

Scognamiglio, R. (1970), *Dei Contratti in Generale. Libro IV, artt. 1321-1352*, in Commentario del Codice civile Scialoja Branca, Zanichelli, Bologna, p. 24.

Securities and Exchange Commission. (2017). *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Release No. 81207). Retrieved March 3, 2025, from <https://www.sec.gov/files/litigation/investreport/34-81207.pdf>

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, 32(3), 1779–1794. <https://doi.org/10.1007/s12525-022-00536-0>

Shim, Y., & Shin, D. (2015). Analyzing China’s Fintech Industry from the Perspective of Actor–Network Theory. *Telecommunications Policy*, 40(2–3), 168–181. <https://doi.org/10.1016/j.telpol.2015.11.005>

Shorter, G., & Miller, R. S. (2014). *High-Frequency Trading: background, concerns, and regulatory developments*. https://digital.library.unt.edu/ark:/67531/metadc332977/m1/1/high_res_d/R43608_2014Jun19.pdf

Shrimali, B., & Patel, H. B. (2021). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University - Computer and Information Sciences*, 34(9), 6793–6807. <https://doi.org/10.1016/j.jksuci.2021.08.005>

Stark, J. (2016). Making Sense of Blockchain Smart Contracts. *Coindesk*. <https://www.coindesk.com/making-sense-smart-contracts/>

Strawn, G. (2019). BLOCKCHAIN. *IT Professional*, 21(1), 91–92. <https://doi.org/10.1109/mitp.2018.2879244>

Szabo, N. (1994). *Smart Contract*. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>

Tabatabaei, M. H., Vitenberg, R., & Veeraragavan, N. R. (2022). Understanding blockchain: definitions, architecture, design, and system comparison. *arXiv (Cornell University)*. <https://doi.org/10.48550/arxiv.2207.02264>

Takeda, A., & Ito, Y. (2021). A review of FinTech research. *International Journal of Technology Management*, 86(1), 67. <https://doi.org/10.1504/ijtm.2021.115761>

Thakor, A. V. (2019). Fintech and banking: What do we know? *Journal of Financial Intermediation*, 41, 100833. <https://doi.org/10.1016/j.jfi.2019.100833>

Tikhomirov, S. (2018). Ethereum: State of Knowledge and research Perspectives. In *Lecture notes in computer science* (pp. 206–221). https://doi.org/10.1007/978-3-319-75650-9_14

Tomczak, T. (2022). Crypto-assets and crypto-assets' subcategories under MiCA Regulation. *Capital Markets Law Journal*, 17(3), 365–382. <https://doi.org/10.1093/cmlj/kmac008>

Toygar, A., Rohm, C. T., & Zhu, J. (2013). A new asset type: digital assets. *Journal of International Technology and Information Management*, 22(4). <https://doi.org/10.58729/1941-6679.1024>

Trabucchi, A. (1982), *Il contratto come fatto giuridico. L'accordo, l'impegno*, in Studi in onore di Oppo, Padova.

U.S. Department of the Treasury. (2023). *Illicit Finance Risk Assessment of Decentralized Finance*. Retrieved September 9, 2025, from <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

Ugarte, R. (2018). Distributed ledger technology (DLT): introduction. *Banco De Espana*, 19/18. <https://ssrn.com/abstract=3269731>

Van Der Merwe, A. (n.d.). A Taxonomy of Cryptocurrencies and Other Digital Assets. *Review of Business*, 41(1).

Vella, G. (2025, September 19). NFT cosa sono: applicazioni ed esempi di Non Fungible Token. *Osservatori.net*. https://www.osservatori.net/blog/blockchain-web3/non-fungible-token-nft-cosa-sono-applicazioni-esempi/#Cosa_sono_gli_NFT

Vergne, J. (2020). Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform. *Organization Theory*, 1(4). <https://doi.org/10.1177/2631787720977052>

Vives, X. (2017). The impact of FinTech on banking. *European Economy*, 2, 97–105. https://blog.iese.edu/xvives/files/2018/02/EE_2.2017.pdf#page=99

Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)* (pp. 1–6). <https://doi.org/10.1109/infoteh.2018.8345547>

Xu, J., & Vadgama, N. (2022). From Banks to DeFi: the Evolution of the Lending Market. In *Future of business and finance* (pp. 53–66). https://doi.org/10.1007/978-3-030-78184-2_6

Yuan, R., Xia, Y., Chen, H., Zang, B., & Xie, J. (2018). ShadowETH: Private Smart Contract on Public Blockchain. *Journal of Computer Science and Technology*, 33(3), 542–556. <https://doi.org/10.1007/s11390-018-1839-y>

Zanarone, G. (2015), in Comm. Gabrielli, Milano.

Zetzsche, D. A., Annunziata, F., Arner, D. W., & Buckley, R. P. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal*, 16(2), 203–225. <https://doi.org/10.1093/cmlj/kmab005>

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance (DEFI). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3539194>

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019). Research on the application of cryptography on the blockchain. *Journal of Physics Conference Series*, 1168, 032077. <https://doi.org/10.1088/1742-6596/1168/3/032077>

Legislation

Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes <http://data.europa.eu/eli/dir/2014/49/oj>

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments <http://data.europa.eu/eli/dir/2014/65/oj>

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market <http://data.europa.eu/eli/dir/2015/2366/oj>

Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation <http://data.europa.eu/eli/reg/2017/2402/oj>

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing <http://data.europa.eu/eli/dir/2018/843/oj>

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law <http://data.europa.eu/eli/dir/2018/1673/oj>

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology <http://data.europa.eu/eli/reg/2022/858/oj>

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets <http://data.europa.eu/eli/reg/2023/1114/oj>

Legge fondamentale sull'ordinamento giudiziario del 30 gennaio 1941 n. 12

Decreto-legge 30 aprile 2019, n. 34

Decreto ministeriale 30 aprile 2021, n. 100

Decreto legislativo 5 settembre 2024, n. 129

Judicial decisions

Cassazione civile, sez. III, 07/10/2010, n. 20809.

Cassazione Civile, sez. III, 28/10/2014, n. 22807.

Cassazione penale, sez. II, 17/09/2020, n. 26807.

Cassazione penale, sez. II, 10/11/2021, n. 44337.

Cassazione penale, sez. II, 26/10/2022, n. 44378.

Tribunale di Verona, n. 195/2017

Corte d'Appello di Brescia, decreto n. 207/2018

Tribunale di Brescia, decreto n. 7556/2018

Tribunale di Firenze, n. 18/2019

Tribunale di Roma, n. 7932/2022

Corte di Appello di Roma, n. 5866/2023