MARISARIA MAUGERI

DISTRIBUTED LEDGER TECHNOLOGY, CRYPTOASSETS AND FINANCIAL MARKETS

PROTECTION OF CONSUMERS AND RETAIL HOLDERS

Publication funded by PRIN 2022 - projects of significant national interest 2022 - "Private law aspects of open banking : focus on consumer protection, personal data privacy and competition ", cup B53D23033830006 , P.I. : prof. Enrico Camilleri

Table of contents

Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market. - 6. Coordination of consumer protection rules with MiCAR.

References

Preface

A few years ago, in 2021, I wrote a short book, *Smart Contracts and Contract Law*. The idea behind that work was that the circulation of wealth also makes use of distributed ledger technology (DLT) and that consequently jurists are called upon to understand whether and how traditional rules are capable of governing this new reality. Since then, much has changed: the market related to DLT has evolved, the EU has taken action to regulate the crypto-assets market, and central bank governors have expressed some concerns about the potential impact of these new instruments on the geopolitical landscape.

Therefore, it is necessary to revisit the topic, assessing whether the arguments put forward at that time still hold true and addressing the fresh issues arising out of the adoption of the new rules.

In this book, however, I will focus exclusively on the use of the technologies in question in the financial markets. This is because very complex sector-specific rules have been issued, which no longer allow us to cover everything in a single book, as was possible even just a few years ago. Specifically, in this book, I will focus on consumer protection in the financial markets that use distributed ledger technology. Indeed, the digital transition is an absolute priority for the European Union over the coming decade. As Charles Michel, the former President of the European Council, emphasised in a speech (at the FT-ETNO Forum) on 29 September 2020, digital strategy in general and the development of digital finance in particular should be based on European values and effective risk regulation.

Consumers are increasingly using digital financial services and trading crypto-assets, typically remotely. Therefore, it is necessary to consider what kind of protection they receive in the context of financial markets that use distributed ledger technology. Hypothetically, this context could also be affected by technological constraints.

In the title of the book, I have paired the term 'consumer' with the term 'retail holder'. Indeed, as will be seen in the final chapter, the EU's regulatory framework on crypto-assets uses the latter term to refer to "any natural person who is acting for purposes which are outside that person's trade, business, craft or profession". It is clear to anyone that this definition aligns with that used in a wide range of uniform laws, rules and regulations to define a consumer.

As can be inferred from the above, this book is not a second edition of the 2021 one. Some areas will not be covered again, such as the use of smart contracts in the electricity market, while entirely new issues will be addressed. I wondered whether

to dedicate a chapter to describing the relevant technologies in this book as well, as I had done in the previous one. I felt it was my duty to do so, updating the previous work, not only because this book is also intended for university students, who may have no knowledge of the technologies at all, but also because, even today, in the legal literature, there are still those who continue to confuse the various new technologies, believing, for example, that smart contracts overlap with developments in artificial intelligence. As I will explain in more detail later, it is clear that these two technologies can be used together, and that this will happen more and more in the future. However, the phenomena of DLT and smart contracts are distinct, both from a technical and a legal standpoint.

Accordingly, in addressing the whole topic, the first chapter will be devoted to seeking to understand what is meant specifically by distributed ledger technology, blockchain, smart contracts and crypto-assets, with a focus also on the main ways in which DLT is used in the financial markets and in payment instruments.

The second chapter will address the question of whether or not contracts can be concluded on distributed ledgers. At that juncture, it will be considered whether there are any obstacles to the applicability of national and EU contract law when agreements are concluded via DLT.

The third chapter will examine the EU's new regulatory framework on crypto-assets in order to understand whether and how it can be coordinated with the pre-existing consumer protection rules governing distance contracts.

Chapter 1. The Use of Distributed Ledger Technology in Financial Markets

CONTENTS: 1. The new technology and its use in the financial sector. - 2. Blockchain. - 3. Bitcoin: between software and crypto(currency). - 4. Ethereum, smart contracts and the tokenisation of assets: the second generation of blockchains. - 5. Differences between unbacked crypto-assets and stablecoins. The growth of the latter on the global market. Towards CBDCs? - 6. DeFi. - 7. Initial conclusions.

1. THE NEW TECHNOLOGY AND ITS USES IN THE FINANCIAL SECTOR

The focus of this book is distributed ledger technology (DLT), a technology that is used in various contexts but undoubtedly its most significant developments relate to the financial markets (consider, for example, the importance that it has taken on in relation to payment instruments).

By now, the term 'blockchain', which refers to the best-known form of distributed ledger technology, has entered the common lexicon. Newspapers often report on transactions involving the exchange of crypto-assets, and almost everyone has heard of Bitcoin. Despite this, however, people continue to conflate this type of technology with artificial intelligence (AI) or other technologies, especially when discussing the topic of smart contracts.[1]

---

[1] See, among others, E. Tamborlini, *Smart contracts: dall'uso all'abuso il passo è breve*, in *Vita Notarile*, 2023, pp. 937 ff.

The two technologies, AI and DLT, operate according to different models,[2] pose different challenges and are governed, at both the national and EU levels, by rules that do not overlap.

Forms of integration between these technologies are underway,[3] leading to the emergence of hybrid architectures in which blockchains are combined with artificial intelligence models (for example, AI-driven smart contracts). At present, however, that is not widespread. This means that, while in the future it will likely be necessary to assess the new reality from a legal standpoint, at present, it is appropriate to focus on the most widely used operating model.

DLT was originally associated with the cypherpunk sociocultural movement, a crypto-anarchist movement that advocated the use of cryptography as a means of disrupting the existing order and establishing a new form of democracy.[4] Today, the technology discussed here is used even by institutional investors, so it appears that the original approach is no longer the prevailing one.[5]

---

[2] See M. Kaulartz and J. Heckmann, *Smart Contracts – Anwendung der Blockchain-Technologie*, in *Computer und Recht*, 2016, p. 618; *Study on Blockchains. Legal, Governance and Interoperability Aspects (SMART 2018/0038)*, a study prepared for the European Commission DG Communications Networks, Content & Technology, 2020, available at https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038, p. 58; A.U. Janssen and F.P. Patti, *Demistificare gli Smart Contracts*, in *ODCC*, 2020, p. 34.

[3] On this point see, for example, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, a thematic report prepared by the EU Blockchain Observatory and Forum, available at https://agi.agroapps.gr/wp-content/uploads/2020/04/Legal-and-regulatory-framework-of-blockchains-and-smart-contracts.pdf, p. 22, according to which:

"If you add various kinds of 'intelligence' to the smart contracts, whether simple if/then types of routines or complex, AI-driven decision making, you can make these programs highly autonomous: able to react to their environment and make decisions, including about buying and selling, on their own. In a similar way, you can 'hard code' the rules for complex organisational structures into smart contracts, creating a trusted, immutable and tamper-resistant organisation where all members are held to the rules via the code. Such organisations can even be automated, creating decentralised autonomous organisations (DAOs) which, once set free in the wild, go about their business on their own with no human intervention."

[4] The Crypto-Anarchist Manifesto is reported in S. Capaccioli, *Smart contracts: traiettoria di un'utopia divenuta attuabile*, in *Ciberspazio e diritto*, 2016, pp. 26–27, and in M.L. Perugini, *Distributed Ledger Technologies e sistemi di Blockchain. Digital Currency, Smart Contract e altre applicazioni*, Milan, Key, 2018, p. 30.

[5] But see the observations of M. Lehmann*, Crypto Economy and International Law. Determining the Regulatory and Private Law Rules Governing the Blockchain*, Leiden, Brill Nijhoff, 2025, p. 3, who, with reference to cryptocurrencies, states:

"They lend themselves to many types of criminal or otherwise illegal activity. They can serve as a conduit for tax evasion, money laundering or terrorist funding; they can represent high risks for private investors, who are in danger of falling victim to fraud, theft or extortion; and they also challenge the monopoly of central banks on issuing currency, which may potentially affect their ability to prevent and mitigate financial and economic crises. This darker aspect of cryptocurrencies is no accident but was intended by their creators, who wanted them to be an alternative to

In the past, cryptography and computer science experts used certain terms in a non-exclusive manner.[6]

Nowadays, however, distributed ledger technology is described using shared models. When determining the scope of application of certain rules, Italian and EU lawmakers have also provided definitions of the technology under discussion that are not dissimilar to one another. In Italy, for example, the first paragraph of Article 8-*ter* of Law Decree No 135 of 14 December 2018 ('Simplification Decree', converted into Law No 12 of 11 February 2019)[7] defines distributed ledger technologies as "computer technologies and protocols that use a shared, distributed, replicable, simultaneously accessible, architecturally decentralised ledger on a cryptographic basis, enabling the recording, validation, updating and storage of both unencrypted

---

traditional money issued by the state (so-called 'fiat money'). Their goal was to create a medium of exchange that would not depend on financial institutions and not be subject to the control of state regulators and central banks. Cryptocurrency pioneers saw blockchain technology as a way to supersede all national institutions of democratic capitalism and to create a global 'crypto anarchy' instead. They mostly expected and accepted the harm this would do to interests currently protected by the law."

[6] See also M. Maugeri, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, Bologna, Il Mulino, 2021, p. 28. In that work, I highlighted how, with reference to the notion of smart contracts, some authors distinguished between data-oriented contracts, computable contracts and Ricardian contracts, while others limited the use of smart contracts to protocols running on DLT that include both a description of the exchange and its execution. On that point, in that book I also referred to what was stated in *Study on Blockchains. Legal, Governance and Interoperability Aspects*, cit., p. 57, according to which:

"The meaning of the term 'smart contract' is controversial in itself. Some literature points out that 'smart contracts' are legal contracts implemented by a particular type of computer code, while others claim that it is a type of code which – when uploaded to a blind consensus platform – precludes operational interference. Nick Szabo, who first introduced the term 'smart contract', considered these to be mechanisms for enforcing legal contracts – computerised transaction protocols executing the contractual terms. Hence, Szabo saw them as a type of code rather than a legal contract. However, these pieces of computer code do not necessarily have to be a legal contract (they can simply be computer code that has no contractual implications) and the terminology can indeed be confusing. Vitalik Buterin, who introduced the terminology of the smart contract into the blockchain space has in fact expressed regret at his choice of terminology, suggesting he should rather have called these tools 'persistent scripts'. The reality is that smart contracts are computer code that, depending on the precise context of its use, may be considered to constitute a legal contract – or not. Given their nature, they can and have been used in a variety of contexts for a number of decades already, such as vending machines (an example given by Szabo in his early reflections on the topic) or financial transactions. Where used on blockchains, they assume the properties of the underlying infrastructure – such as tamper-resistance or decentralisation – which is the key reason why they have triggered a range of legal discussions."

See also R. de Caria, *Defining Smart Contracts: The Search for Workable Legal Categories*, in N. Aggarwal, H. Eidenmüller, L. Enriquez, J. Payne and K. van Zwieten (eds), *Autonomous System and the Law*, München, C.H. Beck/Nomos, 2019, pp. 27 ff. This issue will be discussed again below.

[7] See G. Remotti, *Blockchain smart contract: primo inquadramento e prospettive d'indagine (commento all'art. 8 ter D.L. 14 dicembre 2018, n. 135)*, in *ODCC*, 2020, pp. 189 ff.

and further cryptographically protected data that is verifiable by each participant, non-alterable and non-modifiable".

At EU level, on the other hand, a definition of distributed ledger technology can be found in Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('MiCA Regulation' or 'MiCAR'), which will be the subject of the third chapter of this book.

Specifically, Article 3 contains the following definitions:

1. "distributed ledger technology" or 'DLT': a technology that enables the operation and use of distributed ledgers;
2. "distributed ledger": an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism;
3. "consensus mechanism": the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated;
4. "DLT network node": a device or process that is part of a network and that holds a complete or partial replica of records of all transactions on a distributed ledger.

At first glance, it may appear to be difficult to understand the mechanism described. One can infer that the use of these technologies[8] may make it possible to have data and information in a secure and unalterable form, that this information is shared and that multiple copies of the data exist, but the overall picture may seem unclear. Accordingly, at the outset it might be worth providing, in this chapter, some technical clarification on the operating model of blockchains,[9] which, as mentioned above, represent the most well-known specific type of DLT[10].

---

[8] One of the earliest works on the potential of these new technologies and their impact from a legal perspective is A. Wright and P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 10 March 2015, available on SSRN at https://ssrn.com/abstract=2580664. In Italy see, among many others, D. Di Sabato, *Gli Smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, 2017, pp. 378 ff.; M.L. Perugini, *Distributed Ledger Technologies e sistemi di Blockchain. Digital Currency, Smart Contract e altre applicazioni*, cit. Most recently, see the excellent description of these new technologies in Remotti, *Blockchain smart contract: primo inquadramento e prospettive d'indagine (commento all'art. 8-ter D.L. 14 dicembre 2018, n. 135)*, cit., pp. 189 ff.; M. Doria (coordinator), F. Bassan, M. Rabitti, A. Sciarrone Alibrandi and U. Malvagna, *Caratteristiche degli Smart Contracts*, Quaderno di Banca d'Italia, No 863, 2024.

[9] For T. Cutts, *Smart Contracts and Consumers* (18 March 2019), LSE Legal Studies Working Paper No 1/2019, p. 14, available on SSRN at https://ssrn.com/abstract=3354272: "The term 'smart contract' is now rarely used without a reference to blockchain technology."

[10] Attention can be limited solely to blockchains because other types of DLT, for example, DAG (Directed Acyclic Graph), are of little or no importance in relation to the financial markets.

This chapter will also focus on understanding the main ways in which DLT is used in the financial markets and payment instruments sector.

2. BLOCKCHAIN

As mentioned above, blockchain is the best-known type of distributed ledger technology. But what is a blockchain? It can be imagined as an infinite indelible blackboard, a distributed ledger where every change requires the approval of all nodes. A blackboard, so to speak, on which one can read to whom certain assets belong and which allows one to trace, in an indelible way, all the transactions involving the assets concerned.[11] It can also be described as a tamper-proof ledger.[12]

---

[11] A simple description of how the blockchain operates can be found in M. Pilkington, *Blockchain Technology: Principles and Applications* (18 September 2015), in F. Xavier Olleros and M. Zhegu (eds), *Research Handbook on Digital Transformations*, Cheltenham (UK)–Northampton (MA), Edward Elgar, 2016, pp. 225–253, on SSRN at https://ssrn.com/abstract=2662660.

[12] M. Lehmann, *MiCAR – Gold standard or regulatory poison for the crypto industry?*, in *Common Market Law Review*, 2024, p. 702. However, the same author, in another work, highlights that immutability and tamper-resistance have sometimes been disproven. See, in fact, Lehmann, *Crypto Economy and International Law*, cit., p. 9:

"However, the famous immutability is not an absolute truth. Several times, the blockchain has already been split into two opposing versions. This phenomenon is known as a 'hard fork'. In contrast to 'soft forks', continuously created but overcome by the miners' preference for the longest chain, a hard fork leads to a persistent split of the blockchain into two. Hard forks may be caused intentionally or unintentionally. A famous unintentional hard fork occurred in March 2013. A new version of the Bitcoin protocol had been introduced, which was not backward compatible with the older one. A certain number of nodes operating under the new version of the protocol had accepted a blockchain, which was rejected by the other nodes that had failed to download the new version of the protocol. For a short time, the same private key could be used twice for payments on two different networks. This situation was resolved by the nodes collectively downgrading to the previous version. An intentional hard fork was caused in 2016 when a group of programmers suggested improving the scalability of the Bitcoin blockchain, i.e., the number of transactions the network can process simultaneously in a single block. The proposal was not accepted by most nodes, which were concerned it might compromise the security and stability of the network. Frustrated, two coders published an alternative protocol called 'Bitcoin XT', which raised the block size from one to eight megabytes. Only a fraction of the Bitcoin community downloaded the new protocol, which led to a hard fork in January 2016. Bitcoin XT was eventually abandoned because it failed to gain mass adoption. However, in 2017, a similar dispute over efficiency resulted in an altered version of Bitcoin called 'Bitcoin Cash' (BCH). The new cryptocurrency was distributed free of charge (through 'airdrop') to those who held the original. Both versions continue alongside each other. Examples of such intentional hard forks exist for other cryptocurrencies as well. In practice, intentional hard forks remain rare exceptions. This is because they involve significant costs. Not only do they lead to duplication and, consequently, inflation of assets on competing blockchains, but they also undermine a core goal of the technology, which is to create user trust in the network. If users can no longer rely on the permanency of the blockchain and the values stored therein, they will turn their attention to other types of investment. Consequently, it is not economically rational to implement a hard fork to cancel a single transfer."

In a blockchain, there is no central database as it is replaced by nodes, which are computers connected to the network that operate as distributed ledgers and are updated simultaneously. The blockchain is thus a ledger shared by all the nodes participating in the system. It is a system that leverages cryptography[13] and enables the storage of digital information, ensuring the integrity and the date of the records. It is transparent[14] and secure. Each node contains the entire, up-to-date history of the blockchain.

The functional unit of the blockchain is the block. Each block is added to the database at a specific time interval (for Bitcoin, the transmission time for a single block is 10 minutes; for other blockchains, it is shorter or longer).[15] The block contains the individual transactions[16] and the data from the previous block. Transactions are generated by entering inputs and outputs[17] (for example, how many coins I want to send and to whom)[18] and are then signed using the private cryptographic key. The transaction is then sent to the blockchain, which will include it in the block. Each block must be validated by the nodes. The validated block is then propagated. Using the public key, it is possible to verify the authenticity of the signatures associated with the transaction.

For the purpose of this book it is not necessary to explain how so-called consensus algorithms (proof of work, proof of stake, proof of authority, proof of history, etc.) – which ensure the proper functioning of the mechanism described[19] – operate, nor to describe how blockchains manage to prevent so-called double

---

[13] The cryptographic hash function applied to a file creates a small string that changes every time the file is modified, even slightly. The blockchain system uses this technology to make the contents of the blocks and their chronological order immutable.

[14] The issue of transparency is particularly important and will be discussed further in the body text. Suffice it so say here that, with reference to a single transaction, the transaction's hash/ID is recorded, along with the sender's and recipient's addresses (shown as a 34-character hexadecimal string), the exchange address (also to allow that, if there is an unspent transaction output, UTXO, it can be redirected to the exchange address), the Unix timestamp, i.e. the time at which the transaction was sent, and the amount. Pseudonyms are used.

[15] For the blockchain operating model, see also C. Kerrigan, *Crypto and Digital Assets Law and Regulation*, London, Sweet & Maxwell, 2024, pp. 1 ff.

[16] In the body text the expression transaction is used as a synonym for transfer, not for contract. The first phase of the blockchain concerns the validation of transactions.

[17] The output also includes the so-called change, i.e. the excess of the input sent back (for example, if I have one Bitcoin and want to transfer 0.4 of it, I transfer the BTC and 0.6 is returned to me).

[18] The so-called fee is also included, i.e. the amount to be paid when the transaction is validated. This value affects the priority in block validation because validators will focus on transactions with higher fees.

[19] Some brief mention can be found below, in a footnote, with reference to the Bitcoin mechanism.

spending[20]. They are complex technical mechanisms, which have no bearing on the analysis conducted here of the legally relevant aspects.

Blockchains are divided into permissionless blockchains, which are open networks that allow anyone to participate in the consensus process without the need to obtain approval, permission or authorisation, and permissioned blockchains, which are private networks that do not allow everyone to verify transactions and interact with the information recorded on their distributed ledgers.

3. BITCOIN: BETWEEN SOFTWARE AND CRYPTO(CURRENCY)

The recording method briefly described above is typical of Bitcoin. The launch of the Bitcoin software is associated with the figure of Satoshi Nakamoto,[21] whose identity remains a mystery. The Bitcoin (software) enables the recording and transfer of Bitcoin,[22] which is a digital currency generated by the program itself and not linked to external factors, such as monetary policies.[23] The first Bitcoin transaction took place on 3 January 2009. Satoshi Nakamoto capped the maximum supply of Bitcoin at 21 million units.[24]

Bitcoin, as a virtual currency, is

---

[20] On confirmation against double-spending, see N. Vandezande, *Crypto-assets: The European Legal Framework*, Antwerp–Chicago–Cambridge, Larcier/Intersentia, 2023, p. 55.

[21] S. Nakamoto's 2009 article, *Bitcoin: A Peer-to-Peer Electronic Cash System*, is still considered essential reading for anyone wishing to study how Bitcoin works. It is also available in Italian at https://bitcoin.org/it/documento-bitcoin. On what preceded Satoshi Nakamoto's insight, see M. Giaccaglia, *Considerazioni su Blockchain e Smart Contracts (oltre le criptovalute)*, in *Contratto e impresa*, 2019, p. 944.

[22] For a description of Bitcoin's operating model, see Perugini, *Distributed Ledger Technologies e sistemi di Blockchain*, cit., pp. 57 ff. In particular, the author describes Bitcoin production as follows: "In the production of bitcoins, or mining as it is called, network nodes use their computing power to compose and verify the blocks that record new transactions to be added to the logical chain (blockchain). These complex mathematical calculations have to be validated by a 'proof of work', which is particularly difficult to obtain: the operation generates an output block of bitcoins that is awarded as a prize to the first computer to solve the problem and is added to the logical chain along with all the associated transactions. The system is designed to keep the rate of block production constant at a rate of one block every 10 minutes or so: the effect is that the difficulty required to produce the proof of work increases in proportion to the computational power involved." Proof of work consumes a lot of energy.

[23] V. Pasquino, *Smart Contracts: caratteristiche, vantaggi e problematiche*, in *Diritto e processo*, 2017, p. 240.

[24] On this point, see R. De Bonis and M.I. Vangelisti, *Moneta. Dai buoi di Omero ai Bitcoin*, Bologna, Il Mulino, 2019, p. 167. The authors add: "There is a set limit on the number of Bitcoins to be issued, regardless of economic conditions. This predetermined number of Bitcoins is a key difference from traditional currency, which central banks influence by taking into account trends in inflation and the economic cycle."

> 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.[25]

Bitcoin, like other cryptos, is often referred to as a cryptocurrency, which means 'hidden' currency. Here, I prefer to use the term crypto(currency) to emphasise from the outset that money as such is not involved. Crypto(currency) can be classified as a species of the genus crypto-assets, understood as a sequence of digital records representing rights, created, stored and transferred using DLT-based technologies.

As stated on the website of the Italian supervisory authority for securities markets, CONSOB, "some concepts traditionally used for legal tender, such as 'wallet', have also been adapted to the context of crypto(currencies), where one speaks of a 'digital/electronic wallet' (or simply e-wallet)".[26]

Broadly speaking one can say that wallet service providers safeguard users' accounts and handle the recording of payments and information on account balances, trading platforms facilitate the matching of supply and demand, and exchangers buy and sell crypto-assets in exchange for other currencies, also enabling the trading of crypto-assets between themselves.[27]

Since 2009, Bitcoin has experienced exponential growth in value,[28] accompanied by high volatility[29].

---

[25] See Article 1(2)(d) of 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. The definition of "virtual currencies" was incorporated into Italian law through Legislative Decree No 90/2017 (Article 1(2)(qq)).

[26] *Le Criptovalute*, at https://www.consob.it/web/investor-education/criptovalute.

[27] See De Bonis and Vangelisti, *Moneta*, cit., p. 171.

[28] Id., p. 170: "One of the obstacles to the widespread adoption of Bitcoin is technical: the system is slow and expensive. Bitcoin is produced by miners, who use computer programs to solve mathematical problems and receive a certain number of units in return. The electronic process is ingenious, providing incentives to people wishing to act as miners, but it involves very high electricity consumption: some researchers have argued that the production of cryptocurrencies raises environmental sustainability issues. It is estimated that a single Bitcoin transaction consumes around 150 kWh, at a cost in Italy of around EUR 20. For this reason, miners are largely located in countries such as China, Mongolia and Ukraine, where electricity is virtually free compared to the West. Another factor limiting the use of Bitcoin as a means of payment is its slowness: the waiting time for confirmation that a transaction has been successfully completed is measured in minutes, not seconds as is the case with card payments."

[29] See, among others, Lehmann, *MiCAR – Gold standard or regulatory poison for the crypto industry?*, cit., p. 701. Since 2015, the Bank of Italy has begun warning savers about the risks associated with investments in crypto-assets.

Following the crashes that began in May 2022, the market capitalisation of crypto(currencies) fell below USD 1 trillion, compared to USD 3 trillion in November 2021. By contrast, Donald Trump's victory in the United States presidential election in 2024 led to an increase in Bitcoin's market capitalisation, which rose from USD 1.3 trillion to USD 2 trillion.[30] Overall, Bitcoin is undoubtedly the most highly capitalised crypto(currency).

With the exception of the Central African Republic, no country recognises Bitcoin, or any other crypto(currencies), as legal tender. Even El Salvador, which in September 2021 had recognised Bitcoin as the country's official currency, approved a reform on 29 January 2025 that revoked its status as legal tender.

In Italy, Bitcoin is not legal tender, although it can be easily converted into major fiat currencies.

Legal scholarship in Italy appears unanimous in ruling out the equivalence of crypto(currency) and money. In this regard, it has been correctly argued that,

> regardless of whether one adheres to statist or economic-functional theories concerning the definition of currency, […] the main objection arises from the consideration that cryptocurrencies are not legal tender within the national territory and that, therefore, the use of cryptocurrencies as a means of payment requires the creditor's acceptance. Moreover, even if one were to concede that the function of a medium of exchange is effectively fulfilled, the other functions typically attributed to 'traditional' currency (unit of account and store of value) are difficult to identify in cryptocurrencies, given the marked volatility that has historically characterised these assets, leading to fluctuations in value over time which, combined with the inherent impossibility of implementing expansionary or restrictive monetary policies, appear incompatible with the function of a store of value (in this respect, the 'barren' nature of virtual cryptocurrencies stands out, since only 'liquid and collectible claims for sums of money bear interest as of right').[31]

Again in Italy, doubts have arisen regarding the possibility of classifying Bitcoins as goods in the sense of property. However, these doubts have been largely resolved by both the legal literature and case law, which consider them to be intangible assets that circulate as movable, fungible and non-consumable property.[32] In case law, the District Court of Florence has stated that "cryptocurrencies […] may be considered 'goods' within the meaning of Article 810 of the Civil Code, insofar as they are the subject of rights, as now recognised by the national legislature itself, which also

---

[30] At the same time, the total capitalisation of the crypto market grew from USD 2,200 billion to USD 3,400 billion, an increase of over 150%.

[31] L. Lentini, *Conferimenti di criptovalute e società di capitali*, in L. Calcagno, A. Ciriello, M. Maugeri, and G. Finocchiaro (eds), *Rapporti patrimoniali e nuove tecnologie*, Rome, Istituto Poligrafico e Zecca dello Stato, 2024, pp. 64 ff.

[32] Ibid.

considers them, but not exclusively, as a medium of exchange",[33] holding that the relationship between the intermediary operating the crypto(currency) exchange and custody platform and the client-investors could be likened to an irregular deposit.

4. ETHEREUM, SMART CONTRACTS AND THE TOKENISATION OF ASSETS: THE SECOND GENERATION OF BLOCKCHAINS

The description provided so far pertains to what one might consider the first generation of blockchain infrastructures. Today, a second generation of networks enables more complex operations through the use of smart contracts and DApps.[34]

The first blockchain that can be considered second-generation is Ethereum. Ethereum is a system derived from Bitcoin, with the difference from the first version of Bitcoin being that Ethereum has been designed for the writing smart of contracts.

Ethereum's reference currency is Ether. The blockchain was created through a crowdfunding campaign in 2014. The software was developed by Vitalik Buterin[35] with input from Gavin Wood[36]. The programming language used is Solidity, while the computation engine is the Ethereum Virtual Machine (EVM).[37]

The real difference from (the first version of) Bitcoin lies in the fact that, as already mentioned, in addition to enabling transactions, Ethereum also implements smart contracts. In other words, Ethereum makes it possible to develop and run decentralised applications.

In this chapter, what can be done with smart contracts will be explored.

Smart contracts were first theorised in a 1994 post[38] (*Smart Contracts*) by Nick Szabo, well before the creation of Ethereum. The post was followed by three articles

---

[33] Trib. Firenze, judgment no 18 of 21 January 2019. It concerned the declaration of bankruptcy of a company that managed an exchange platform.

[34] F. Bassan and M. Rabitti, *Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai "contracts on chain"*, in *Rivista di diritto bancario*, 2023, pp. 596 ff, discuss third-generation blockchains. See also C. Attanasio, *Inadempimento dello smart contract, sistema rimediale e tutela effettiva*, in *Rivista di diritto civile*, 2024, p. 729.

[35] *Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform,* 2014, at https://courses.cs.duke. edu/spring23/compsci512/papers/ethereum.pdf.

[36] *Ethereum: A Secure Decentralised Generalised Transaction Ledger,* at https://ethereum.github.io/yellowpaper/paper.pdf.

[37] The EVM is not exclusive to Ethereum but is used also by other blockchains including but not limited to Polygon, Arbitrum and Avalanche.

[38] At http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterscho

by the same author, two from 1997 (*Formalizing and Securing Relationships on Public Networks*[39] and *The Idea of Smart Contracts*[40]) and one from 1998 (*Secure Property Titles with Owner Authority*[41]), in which Szabo took his cue from a vending machine to describe the transfer of certain utilities in execution of an algorithm.

In his 1994 post Szabo maintained that a smart contract was a computerised transaction protocol capable of executing the terms of a contract and that the general objectives of smart contract design were to satisfy standard contractual conditions.[42]

The advantage that Szabo saw was a drastic reduction of human intervention, which would radically cut costs and guarantee certainty of execution.[43] Indeed, on an IT level, the procedure for initiating the computerised protocol of a smart contract is said not to be revocable. Thus for Szabo, a smart contract was not a traditional contract in a legal sense but just a code suitable for executing the terms of a contract.[44]

Szabo's smart contracts made no reference to distributed ledger technologies and were just thought of as algorithms that would prevent the parties from choosing whether or not to perform. Algorithms that entrusted machines with the task of constraining performance.

Only later did Buterin[45] and Wood put Szabo's idea into practice, succeeding in ensuring that computer code that would prevent parties from choosing whether or not to perform could be incorporated into distributed ledger-based systems.[46]

---

ol2006/szabo.best. vwh.net/smart.contracts.html.

[39] At https://firstmonday.org/article/view/548/469.

[40] At https://nakamotoinstitute.org/the-idea-of-smart-contracts/.

[41] At https://nakamotoinstitute.org/secure-property-titles/.

[42] The following is the terminology used by Szabo in his 1994 post: "A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs. Some technologies that exist today can be considered as crude smart contracts, for example POS terminals and cards, EDI, and agoric allocation of public network bandwidth."

[43] In 1998 Wei Dai (in B-money) theorised about the creation of an independent contractual system to be implemented in a non-traceable network, with predetermined enforcement rules, and the exchange of digitally signed messages between persons identified by a digital pseudonym. Both Szabo and Wei Dai thus envisaged self-enforcing outcomes of the conditions. On the converging positions of Szabo and Wei Dai see, see Perugini, *Distributed Ledger Technologies e sistemi di Blockchain*, cit., p. 176.

[44] See T. Cutts, *Smart Contracts and Consumers (18 March 2019)*, cit., p. 24.

[45] In 2014, Vitalik Buterin (co-founder of Ethereum), at a summit on blockchains, explained how smart contracts work as follows: "Contracts are translated into computer language and stored in

Therefore, smart contracts running on distributed ledger technology (after Ethereum, other blockchains have been developed that support the use of smart contracts) are computer codes embedded within the blockchain. These codes are triggered when a specific event occurs.[47]

Programmers insert a series of instructions into the smart contract (or code), expressed in computer language and visible to everyone. The code is then transcribed onto the blockchain and, as a result, becomes immutable. The smart contract has an address that allows users to interact with it, and it is activated when the condition that the programmer specified when writing it is met. The logic followed is "if-then". Roughly speaking, the code will contain a command along the following lines: if condition X is met, then instruction Y must be executed.

When describing the operating model of smart contracts, it is helpful to refer to the concept of the oracle.[48] This is also relevant because the next chapter will highlight inter alia how the stated certainty of execution for a transaction entrusted to a smart contract could be undermined if the oracle functions incorrectly.

---

blocks. The parties to the contracts, which are copied to distributed ledgers, are kept 100 percent anonymous. The code snippet is ready with specific tasks and details (time limit, what goes where, from where to where, etc.). When the time comes, it takes action to fulfil the transaction, and if the necessary conditions are met, the transaction is successfully completed or cancelled before completion.", at https://www.youtube.com/ watch?v=TDGq4aeevgY.

[46] The "Smart Contracts" Report from the European Commission's project, EU Blockchain Observatory Forum, 2022, available at https://blockchainobservatory.ec.europa.eu/document/download/53a0aeb4-d1444054-841e-dc169b44f94d_en?filename=SmartContractsRepo rt_Final.pdf, 5, describes smart contracts in the following terms: "Smart contracts pre-exist blockchain and can exist without blockchain technology, like in the vending machine example. Due to technological limitations, smart contracts have been out of the spotlight for some time. The emergence of blockchain technology brought them back from obscurity and into the mainstream of technological advancement. Blockchain has enabled the progress of smart contracts from simple automated contracts to fully autonomous self-executing and self-enforced contracts built on decentralized platforms and supported by a blockchain ecosystem. Smart contracts combine a number of technological advancements, including electronic contracting, cryptography and tamper-proof and algorithmic executions based on consensus."

On this point, reference may also be made to Maugeri, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, cit., p. 30.

[47] According to Doria (coordinator), Bassan, Rabitti, Sciarrone Alibrandi, and Malvagna, *Caratteristiche degli smart contracts*, cit., p. 5: "Smart contracts have unique characteristics compared to other types of software in that: i) the program code is recorded on the blockchain and thus becomes immutable, secure and transparent, as guaranteed by the shared ledger; ii) the execution of the program is deterministic and the result of the execution is stored on the blockchain; iii) the program automates the execution of certain operations on the blockchain, for example by acting as a repository for digital assets (including cryptocurrencies), approving the transfer of assets and recording specific information in the ledger."

[48] For further information on this topic, please refer to Maugeri, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, cit., p. 34.

An oracle is defined as the machine or human that sends the receiving input to the machine.[49] Thus, the oracle is a third-party that sends the input to the system. A distinction is made between an automatic oracle, such as a sensor connected to the website, and a human oracle, such as the courier who delivers the package or an expert with powers of assessment. For example, AXA has devised an insurance contract whereby if an airplane is delayed, a sum of money will be automatically paid out.[50] In this case, the oracle will be the flight arrival time notification system, which will be consulted and will trigger the immediate transfer of the sum in the event of a delay.[51]

The first smart contracts were very simple. Subsequently, people began to combine them, creating what are known as DApps (decentralised applications), which utilise multiple smart contracts and function, roughly speaking, like apps.[52] Now, by combining multiple smart contracts, previously unthinkable financial

---

[49] In the *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*, an oracle is defined as follows: "Service that updates a DISTRIBUTED LEDGER (e.g., a BLOCKCHAIN) using data from outside a DISTRIBUTED LEDGER system (outside the BLOCKCHAIN context). An ORACLE transmits OFF-CHAIN information in a computer-readable form to the network", at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_ Technology__Smart_Contracts_and_Consumer_Protection.pdf, p. 20.

According to Doria (coordinator), Bassan, Rabitti, Sciarrone Alibrandi and Malvagna, *Caratteristiche degli smart contracts*, cit., p. 6, no 20: "An oracle provides the smart contract with information, sourced from outside the network, which constitutes the conditions under which the smart contract is triggered to perform the desired functions. The conditions for execution can be obtained and verified directly on-chain if they are events detectable by the blockchain itself (as in the case of digital currency transactions between multiple wallets linked to the smart contract); in other cases, however, the elements or events that trigger the smart contract are external to the network (off-chain), and therefore exist and occur solely in the real world: in these circumstances, the oracle serves to ensure the connection between what happens on the blockchain and what happens outside it, 'certifying' the authenticity and accuracy of the data entered onto the blockchain."

[50] Regarding the use of smart contracts for compensation due to flight delays or cancellations, pursuant to Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91, see Janssen and Patti, *Demystifying Smart Contracts*, cit., pp. 37 ff.

[51] According to P. Cuccuru, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *NGCC*, 2017, II, p. 111, "the oracle mechanism has […] the inevitable disadvantage of reintroducing a degree of uncertainty into the system. The formalised relationship is, in fact, exposed to the risk of malfunction or tampering with the external information sources on which it relies".

[52] According to Doria (coordinator), Bassan, Rabitti, Sciarrone Alibrandi, and Malvagna, Caratteristiche degli smart contracts, cit., p. 5, no 15, DApps are "applications that can operate autonomously, typically through the use of smart contracts, which are executed on a decentralised computer system, a blockchain or another distributed ledger system. Every DApp or other blockchain-based application is built using smart contract code to perform operations on the chosen blockchain. What sets them apart, therefore, from most common applications is that their back-end code runs on a decentralised peer-to-peer network".

transactions can be carried out on the blockchain: consider, for example, liquidity management.

Smart contracts are also used in ecosystems where there are natural persons and legal entities who are involved in the issuance, public offering or admission to trading of crypto-assets or who provide services related to crypto-assets.

One of the first functions performed by smart contracts running on Ethereum involved crowdfunding and the issuance of new tokens in exchange for a contribution (Initial Coin Offering or ICO).

ICOs really took hold in 2017[53] and are used to raise funds in exchange for tokens (digital representations of value or a right). The entities issuing the tokens can be companies, individuals or networks of product developers. To achieve this goal, two smart contracts need to be recorded on the blockchain: one to create the token and another to distribute it to the contributors.

From 2018 onwards, however, interest in ICOs began to wane, probably due to the numerous scams investors had encountered. As a result, investors have shifted their focus to exchanges that witness the presence of exchange operators. In other words, fundraising for projects is administered by an exchange that acts as a filter, first checking the soundness and seriousness of the project.

It has been stated that, in general, it is possible to issue tokens and transfer them on the network. From a technical standpoint, tokens are strings of encrypted digital codes, generated electronically using algorithms. The term 'crypto-asset' may also be used to refer to them.

As mentioned before, those encrypted codes are exchanged via DLT. Therefore, the 'assets' are exclusively 'digital' in nature.[54]

There are various types of crypto-assets, and each has its own characteristics, such as the maximum number of units that can be produced, the methods of creation and the rules for transfer.[55] It is impossible to provide a comprehensive and

---

[53] On 19 March 2019, CONSOB published a discussion document on ICOs. The consultation period closed on 5 June 2019, and the final report was published on 2 January 2020 titled *Le offerte iniziali e gli scambi di cripto-attività. Rapporto finale*, available at consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.

[54] On the debate regarding the nature of crypto-assets with reference to English law, see N. Gaggero, *Liability for Wrongful Interference with Crypto-assets. Their Proprietary Status and Its Practical Implications*, in *ODCC*, 2025, pp. 265 ff.

[55] Regarding crypto-assets, see, among others, M. Cian, *La nozione di criptoattività nella prospettiva del MiCAR. Dallo strumento finanziario al token e ritorno*, in G. Gitti and M. Maugeri (eds), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, special issue of ODCC, 2022, pp. 59 ff. See also M. Cian and C. Sandei, *Le cripto-attività: spunti per un inquadramento concettuale e disciplinare*, in F. Annunziata and A. Sciarrone (eds), *Cripto-attività. La disciplina europea nel contesto globale*, Bologna, Il Mulino, 2024, pp. 227 ff.

universally accepted taxonomy. Here, suffice it to say that a distinction is typically made between unbacked crypto-assets, which lack a stabilisation mechanism that pegs their value to a reference asset, and asset-backed stablecoins, which are crypto-assets backed by underlying assets, a topic that will be addressed in the next section of this chapter.

Based on the economic function performed, a distinction can be made between: payment tokens, i.e. means of payment for the purchase of goods or services or instruments intended for the transfer of money and value; security tokens, which represent economic rights linked to the performance of a business venture and/or administrative rights (e.g. voting rights on certain matters); and utility tokens, which represent different rights linked to the ability to use the product or service that the issuer intends to create.

Furthermore, a distinction can be made between fungible tokens, i.e. those that have equivalent value and characteristics and are therefore interchangeable, and non-fungible tokens, which have unique and unrepeatable characteristics or identify a specific asset (e.g. a work of art).[56]

However, it is precisely the impossibility of providing an exhaustive taxonomy that has led the EU, as will be seen in more detail below, to regulate certain tokens by identifying them using wording couched in the negative, namely, "crypto-assets other than asset-referenced tokens and electronic money tokens".

5. DIFFERENCES BETWEEN UNBACKED CRYPTO-ASSETS AND STABLECOINS. THE GROWTH OF THE LATTER ON THE GLOBAL MARKET. TOWARDS CBDCs?

By leveraging the potential of distributed ledger technologies, the market has sought to respond to Bitcoin's volatility by developing what are known as stablecoins.

Unlike Bitcoin, stablecoins are issued by identified entities and aim to stabilise their value through collateral (collateralised stablecoins) or by means of algorithms that

[56] There are also so-called meme coins, which are "crypto assets named after trends, humorous or fun topics. They are usually created to engage a community and can be used in peer-to-peer payments, speculative investing, or trading. In many cases, they are accompanied by websites with comical themes, sometimes nonsensical terms, and their creators and fans market a sense of community to attract others" (EBA, EIOPA, and ESMA, *Crypto-assets explained: what MiCA means for you as a consumer*, available at https://www.esma.europa.eu/sites/default/files/2025-10/Joint_ESAs_Factsheet_on_crypto-assets.pdf).

regulate their supply (algorithmic money).[57] More specifically, stablecoins are digital tokens that aim to maintain a stable value relative to a reference asset, including a fiat currency, such as the U.S. dollar or the euro.

Unlike unbacked crypto-assets, such as Bitcoin and Ether, stablecoins are designed to be redeemable. Bitcoin and Ether are also considered native crypto(currencies) and are therefore regarded as distinct from tokenised crypto, which are created on existing blockchains.

In 2025, the market capitalisation of cryptocurrencies exceeded USD 4 trillion, and stablecoins accounted for approximately 7.5% of the cryptocurrency market, representing around USD 300 billion. Dollar-pegged stablecoins (e.g. Tether's USDT and Circle's USDC) currently account for 98% of the global market, while Euro-pegged stablecoins represent only 0.2% of the total.[58]

One can only agree with those who assert as follows:

> [t]hese instruments may offer novel solutions to long-standing issues in payments and financial intermediation, particularly in the cross-border context. However, their growth also raises important questions about governance, stability, their potential misuse for illicit purposes, and the consistency of oversight across jurisdictions. As we navigate this landscape, it is essential that we remain open to the opportunities presented by modern technologies, while carefully evaluating their potential impact on the broader financial system. Striking the right balance between enabling innovation and safeguarding key policy objectives – such as financial stability, monetary sovereignty, financial inclusion, consumer protection, and trust in money – remains a major challenge for public authorities.[59]

In his Concluding Remarks on fiscal 2024, the Governor of the Bank of Italy, Fabio Panetta, also authoritatively highlighted how stablecoins still expose

> holders to risks relating to the soundness of the issuers and to volatility in the value of the underlying asset. In the absence of adequate regulation, their suitability as a means of payment is doubtful, to say the least. However, if large foreign-based technology platforms decided to promote the use of stablecoins for payments between their customers, this could lead to new systemically important payment schemes operating on a global scale. Traditional means of payment used domestically – such as banknotes and cards – could be crowded out, negatively

---

[57] De Bonis and Vangelisti, *Moneta*, cit., p. 171.

[58] On stablecoins, see C. Scotti, *Stablecoins in the Payment Ecosystem: Reflections on Responsible Innovation*, 18 September 2025, available at https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/ int-dir-2025/20250918-scotti/index.html, from which the capitalisation data cited are taken.

[59] Ibid.

> affecting monetary sovereignty, personal data protection, and credit intermediation, which so far has always been integrated with and complementary to the provision of payment services.[60]

Faced with serious and authoritative concerns, such as those mentioned above, it is therefore not surprising that the EU, on the one hand, has adopted a regulation on markets in crypto-assets ('MiCAR', mentioned above), which will be discussed in the final chapter of this book, and, on the other hand, is accelerating the introduction of the digital euro.

In this regard, Governor Panetta's words seem clear:

> But we would be remiss to think that the evolution of crypto-assets can be controlled only through rules and restrictions. What is needed is a response that matches the ongoing technological transformation, one capable of meeting the demand for secure, efficient and accessible digital payment instruments, all while preserving the role of central bank money. The digital euro project stems precisely from this need.[61]

The issuance of the digital euro would ensure that public money remains

> an option available to everyone, providing a European-wide payment instrument that is easy to use. It would also provide an alternative payment network to those operated by major card and online payment solutions providers, often non-European, thereby facilitating the provision of new services by supervised intermediaries at European level.[62]

The digital euro would be a CBDC, i.e. a Central Bank Digital Currency[63]. Therefore, it would not be issued by private entities, as is the case with stablecoins, but by the central bank.

In the geopolitical context, a very recent news item (September 2025) appearing in the media is worthy of note: nine major European banks are reportedly about to jointly launch a stablecoin pegged to the euro, thereby creating a potential turning point for the digital asset market on the Old Continent.

Looking beyond Europe, it is evident that the United States dominates the stablecoin market. Furthermore, the phenomenon appears to have garnered strong support, especially after 2024, the year of President Trump's election. Indeed, in 2025, the first federal (public) strategic reserve of Bitcoin and other crypto(currencies) was ordered, estimated at USD 17 billion.

---

[60] *The Governor's Concluding Remarks, Annual Report*, Rome, 30 May 2025, available at https://www.bancaditalia.it/pubblicazioni/interventi-governatore/integov2025/cf_2024.pdf.

[61] Ibid.

[62] Bank of Italy, *Why a digital euro?*, at https://www.bancaditalia.it/focus/euro-digitale/perche/index.html.

[63] On the digital euro, see also G. Carriero, *Euro digitale e tutela dell'utente*, in S. Ruperto (ed.), *Studi per Cesare Ruperto nel centesimo genetliaco*, Milan, Lefebvre Giuffrè, 2025, pp. 173 ff.

Stablecoins are regulated by the Genius Act (Guiding and Establishing National Innovation for U.S. Stablecoins), enacted on 18 July 2025. There is debate as to whether the framework set out in the Genius Act is 'equivalent' to that set out in MiCAR. It is beyond the scope of this paper to examine how different regulations in the global market may affect the protection of market participants and the resilience of systems. However, it can be said that the ongoing debate highlights potentially serious risks.

It is worth noting that, in the United States, a bill (the Anti-CBDC Surveillance State Act) is currently pending that would prohibit the Fed from creating a digital currency.

In Japan, crypto(currency) has received a form of recognition through the Virtual Currency Act, which considers it a property value. In 2025, Japanese Finance Minister Katsunobu Kato acknowledged that crypto(currencies) deserve a place in diversified investment portfolios. In fact, during the Web3 Conference WebX 2025 in Tokyo, he stated that "although cryptocurrencies carry a risk of high volatility, by creating an appropriate investment environment, they can become an option for diversifying investments".

In September 2025, Japan Post Bank announced the launch of DCJPY, a fully backed digital currency designed to simplify payments and financial transactions on the blockchain. It will not be a speculative cryptocurrency, nor a traditional stablecoin; rather, it will be the yen going digital. DCJPY was created as a tokenised deposit. Each digital unit will correspond to one real yen held at the bank, on a 1:1 basis, with a full institutional guarantee. However, it will not be issued by the central bank and, therefore, will not be a CBDC.

At the same time, in the Land of the Rising Sun, work is underway to issue an actual CBDC.

China, which is highly advanced in the use of new technologies in the field of payment instruments,[64] has shown hostility toward Bitcoin and other crypto(currencies).[65] In fact, on 15 September 2021, it declared them illegal. Specifically, the document prepared by the People's Bank of China and other institutions states as follows:

> Virtual currencies do not have the same legal status as legal tender. Bitcoin, Ethereum, Tether, and other virtual currencies share the following distinctive characteristics: they are not issued by monetary authorities, they are based on cryptography and distributed ledger technologies and the

---

[64] On this point, please refer to M. Maugeri, *Viaggio in Cina: cashless andata e ritorno?*, December 2024, available at https://rivistailmulino.it/a/viaggio-in-cina-cashless-andata-e-ritorno.

[65] For further information on China's position, see Lehmann, *Crypto Economy and International Law*, cit., pp. 62 ff.

like, and they exist in digital form. Due to these characteristics, they are not legal tender and should not and cannot circulate as currency in the market. Activities related to virtual currencies are illegal financial activities.

In this context, China is certainly far ahead in developing a CBDC, the e-CNY.[66] The e-CNY67 has been launched and promoted in several pilot regions.[67]

6. DeFi

Decentralised finance (DeFi) has grown significantly in recent years. The term DeFi is used to describe a range of services offered in the world of crypto-assets that aim to replicate the services provided in the traditional financial system.

In DeFi, the role of

financial institutions and market infrastructures is replaced to varying degree by self-executing code, or so-called smart contracts, deployed to public blockchains. DeFi emerges primarily as a crypto-based alternative and competitive peer-to-peer/pool marketplace of financial services, covering various activities like trading, borrowing, or lending, so far overwhelmingly within the crypto-asset space.[68]

The DeFi ecosystem is complex. For the purposes of this discussion, it is sufficient to note that traditional services, such as trading, borrowing or lending, are carried out through the use of smart contracts and within permissionless blockchain infrastructures.[69]

It can undoubtedly be said that smart contracts are the key innovation that has enabled the development of DeFi. Within the DeFi ecosystem, services for crypto-assets are provided in a fully decentralised manner, without any intermediaries.[70]

---

[66] On the introduction of this currency and on CBDCs in general, see B. Rosa and C. Larsen, *Smart Money. How Digital Currencies will Win the New Cold War – and Why the West Needs to Act Now*, London, Bloomsbury, 2024.

[67] See H. Bai, L.W. Cong, M. Luo and P. Xie, *Adoption of Central Bank Digital Currencies: Initial Evidence from China*, FEB-RN Research Paper No 43/2025, 15 March 2024, on SSRN at https://ssrn.com/abstract=5022129, or, at http://dx.doi.org/10.2139/ssrn.5022129.

[68] *Financial Stability Board, The Financial Stability Risks of Decentralised Finance*, at https://www.fsb.org/uploads/P160223.pdf, 1.

[69] See D. Lupini e C. Kerrigan, *Smart Contracts*, in C. Kerrigan, *Crypto and Digital Assets Law and Regulation,* Toronto, Thomson Reuters, 2024, p. 75.

[70] However, as Lehmann, *Crypto Economy and International Law*, cit., p. 107, reminds us, it is important to note as follows: "The smart contracts underlying DeFi are programmed by some individuals, and even in DeFi some persons may intervene when the code is not working properly. This was exemplified by the Terra-Luna debacle, in which validators stopped the activity of the network and halted the blockchain to prevent a further meltdown of token prices. This incident vividly illustrated that DeFi is not immune to human intervention. Still, it may be difficult for law

The terms and conditions under which these services are provided are set out in the DeFi protocols. Through graphical interfaces, the protocols enable interaction with smart contracts (using the aforementioned DApps). DeFi, in the terms that will be seen below, is not expressly regulated by MiCAR, dwelt on in the final chapter. Of course, this does not mean that the phenomenon is entirely unregulated.

7. INITIAL CONCLUSIONS

The financial markets that use distributed ledger technologies are highly complex, and their operating models are intricate.

First-generation blockchains are limited to enabling 'transfers' of wealth. In that context, the reason for the transfers lies outside the infrastructure. The situation is different with regard to second-generation blockchains, where smart contracts operate.

For the purposes of the scope of this book, it can be said that there are fully automated financial market operating models based on distributed ledger technology, in which trades are conducted – typically on open infrastructures – exclusively through the use of one or more smart contracts. On the other hand, there are models in which identifiable public and private entities operate, issuing, offering, transferring and admitting to trading crypto-assets, or providing services related to crypto-assets. In some ways, these models are easier to regulate than fully decentralised models. Smart contracts are also used in this latter context.

From an economic and political standpoint, so-called stablecoins, which are crypto-assets issued by identifiable entities with the aim of maintaining a stable value relative to a reference asset, are gaining particular importance. The EU appears to be focused not only on regulating the phenomenon but also on finding a way to contain it through the creation of the digital euro.

Lawmakers in various parts of the world have taken action to either block, regulate or encourage the use of this new technology.

We must now ask ourselves:

---

enforcement agencies to get hold of the core developers of blockchains or DeFi applications. Often they will be abroad, highly mobile and able to flee to other jurisdictions. The same may be said of the validators and mining pools: Despite their considerable infrastructure, they have shown in the past the ability to migrate to other countries if necessary. The problem with decentralisation is thus not so much that a human being to which orders could be addressed would be lacking. It is rather the distribution of the relevant individuals and knowledge all over the globe."

- first, whether in Italy and at EU level there are rules aimed at protecting consumers who use crypto-assets, including as payment instruments and, if not, whether this results in a lack of protection for consumers; and,
- second, whether and how any new rules will be coordinated with the pre-existing ones.

The following chapters will address those questions.

Chapter 2. Contract Formation via Smart Contracts: Applicable Law

CONTENTS: 1. Smart contracts and traditional contracts in a legal sense. - 2. The arguments that the technical characteristics of smart contracts prevent the application, in whole or in part, of the law of contract in the case of agreements concluded via distributed ledger technologies. Critique - 3. The earliest rules aimed at giving legal effect to agreements concluded through smart contracts. - 4. EU rules on smart contracts. - 5. Italian law. - 6. Consumers and digital financial services. Scope of the study.

1. SMART CONTRACTS AND TRADITIONAL CONTRACTS IN A LEGAL SENSE

In the previous chapter, we described how distributed ledger technology works. In this one, we will seek to determine whether contracts can be concluded through the mechanisms described and, if so, what legal framework can be applied to them. Specifically, we will consider whether consumers who enter into contracts through the new technologies are afforded protection.

As mentioned before, first-generation blockchains are limited to enabling 'transfers' of wealth. It follows that, in that context, the justification for such transfers lies outside the infrastructure. In other words, the infrastructure merely enables the execution of agreements entered into by the parties elsewhere. The situation is different with regard to second-generation infrastructure, where smart contracts operate.

A smart contract that runs on a distributed ledger is not in itself a legal contract as such, i.e. a contract in a legal sense. As mentioned before, it is, in fact, merely computer code recorded on a second-generation blockchain.[1]

[1]For information on the various functions that a smart contract can perform, please refer to Maugeri,

However, through the use of one or more smart contract, it is possible to conclude an agreement between parties (an exchange of offer and acceptance) that concerns the parties' assets.[2] In other words, smart contracts can be used to set the terms of the economic transaction, as well as to perform the services. When this occurs, for example, in Italy, there is a contract within the meaning of Article 1321 of the Civil Code (which provides that a contract is "an agreement between two or more parties to establish, regulate or terminate an economic legal relationship"[3]).

With regard to the functions of smart contracts, as already discussed in the previous chapter, for example, a contract in a legal sense would not exist if, using a smart contract, a token were issued but not exchanged. On the other hand, if the entire transaction were carried out on a blockchain,[4] a contract in a legal sense would exist if the issued token were exchanged, using a different smart contract, for another token or for crypto(currencies).

Again with reference to the functions of smart contracts described above, if the code provided for the payment of a sum of money in the event of a flight delay, this might not even constitute a contract in a legal sense but merely the execution of a contract concluded outside the blockchain.[5]

Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law, cit., pp. 31 ff.

[2] In the *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*, cit., p. 14, there is a fifth principle, worded as follows: "Legal Nature of Transactions on a Blockchain: The triggering of TRANSACTIONS, or of elements of TRANSACTIONS, performed on a BLOCKCHAIN may amount to an offer, acceptance, or any other contractual declaration where, depending on the specific nature of the SMART CONTRACT, such triggering can reasonably be understood as a declaration of will and is attributable to the relevant party." On page 25 of the ELI document it is stated that a "SMART CONTRACT can be a legally binding declaration of will, such as an offer or acceptance, or constitute a legal agreement itself".

[3] I believe it is more accurate to use the expression found in the body text, "there is a contract", rather than "are contracts", as I had previously done in the book on *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, cit., p. 33.

[4] Clearly, even the exchange of tokens can only be the execution of a contract entered into outside the blockchain, for example, via email or another type of message.

[5] Certainly, no contract would be concluded if a smart contract were drawn up like the one depicted in an online tutorial *Cos'è uno Smart Contract? (con esempio pratico*), available at https://www.youtube.com/watch?v=FDGcsJuCywE). In fact, the creator of the tutorial envisions a smart contract designed to allow a person to lock away a sum of money during the sales period. In other words, the smart contract would be written by an individual to avoid giving in to temptation during the *Black Friday* shopping period. The smart contract in question would allow this individual to deposit the sum into the smart contract, with the provision that the sum would be released and returned at a date after the end of the sales period. In the case described, there would be no agreement between two or more parties and, therefore, the essential terms of the contract would certainly not be included.

The fact that contracts may be involved raises the question of the legal framework applicable to exchanges of value carried out through agreements made on a blockchain.[6]

The following sections of this chapter will address that issue.

2. THE ARGUMENTS THAT THE TECHNICAL CHARACTERISTICS OF SMART CONTRACTS PREVENT THE APPLICATION, IN WHOLE OR IN PART, OF THE LAW OF CONTRACT IN THE CASE OF AGREEMENTS CONCLUDED VIA DISTRIBUTED LEDGER TECHNOLOGIES. CRITIQUE

First, let us try to determine whether, in the context of smart contracts running on distributed ledger technologies and blockchains, it has ever been called into question whether contract law can be applied.

Indeed, it has been argued that, leaving aside the possibility in general of classifying smart contracts as traditional contracts in a legal sense or – as seems preferable – as computer codes through which it is possible to conclude an agreement between parties concerning their assets, it is precisely the technical characteristics of smart contracts that rule out, in whole or in part, the actual prospect of applying the general law of contract to them.

---

[6] Some scholars propose distinguishing between smart contract code and smart legal contract. The latter term should be used when the smart contract is employed "to set out, verify, and enforce an agreement between the parties" (see, among others, Doria (coordinator), Bassan, Rabitti, Sciarrone Alibrandi, and Malvagna, *Caratteristiche degli smart contracts*, cit., p. 2 *et passim*). Although the need to use a taxonomy to simplify the discussion is well understood and widely accepted, I believe it is preferable – as I have also argued in the past – not to adopt the aforementioned distinction, as it could lead to confusion. Indeed, in the literature, this term fails to identify homogeneous groups of cases. Indeed, at times, it is used to refer to smart contracts that enable the conclusion of an agreement between parties concerning their assets; at other times, however, it is used to designate smart contracts that enable even the mere execution of agreements made outside DLT. For example, the UK Law Commission, *Smart Legal Contracts. Advice to Government*, Law Com No 401, 2021, p. 1, uses the term smart legal contract, defining it as "a legally binding contract in which some or all of the contractual obligations are defined in and/or performed automatically by a computer program", at https://webarchive.nationalarchives.gov.uk/ukgwa/20250109110910mp_/https://cloud-platforme218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2021/11/6.7776_LC_Smart_Legal_Contracts_2021_Final. pdf.

On this point, please refer to Maugeri, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, cit., p. 33. On *Smart Legal Contracts*, see also Lupini and Kerrigan, *Smart Contracts*, cit., pp. 75 ff.

I am referring, first of all, to the school of thought that holds that smart contracts do not need law because they are themselves an alternative to contract law, which will therefore disappear.[7]

According to that view, which echoes Lessig's idea of "code Is law",[8] a smart contract, first, could never give rise to problems of non-performance, and, second, even if it were vitiated by fraud or duress or were otherwise invalid, it could never lead to modifying the blockchain database *ex post*, if not at the cost of undermining the very functioning of the latter.

Indeed, the author in question admits that there may be room for actions for damages and/or restitution but, first, he considers these to be unlikely given the difficulty of identifying the parties, and, second, reiterates that they could never affect the functioning of the blockchain in any event.[9]

That view cannot be shared not only because, as I will explain in greater detail later, it is not entirely true that a smart contract always guarantees proper performance, but, more importantly, because – even if one were to accept the idea that a remedial mechanism that coercively affected the blockchain, in addition to not being technically feasible at present, would also be entirely at odds with the functioning of the blockchain itself – there would be no reason whatsoever to rule out

---

[7] See A. Savelyev, *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law*, 21 National Research University Higher School of Economics, Working Paper No BRP 71/LAW/2016, 2016, at https://papers.ssrn.com/sol3/papers. cfm?abstract_id=, according to whom "smart contracts […] may operate without any overarching legal framework. De facto, they represent a technological alternative to the whole legal system. Apart from conclusions already mentioned above, it means that there is no need in conflict of laws provisions, since there are no collisions of various legal systems. Mathematics is universal human language. Thus, smart contracts are truly transnational and executed uniformly regardless of the differences in national laws".

He adds: "Whether it was concluded for mistake, as a result of fraudulent misrepresentation, coercion or threats, unfair exploitation of relationship of trust – it is completely irrelevant for its performance in contrast to classic contracts, where such circumstances serve as a basis for court interference in all the legal systems. Moreover, such consideration of such vitiating factors is in contradiction with the main feature of Blockchain-based databases of transactions: their 'single version of truth' for everyone. If such factors may serve as a basis for changing the content of such database post factum, it will undermine the trust in Blockchain and depreciate its value. Therefore, in smart contracts there cannot be a collision between intent and its expression, what really matters is only an expression of intent represented in computer code. Such an approach can be viewed as a triumph of protection of the certainty and market. Of course, there is some residual possibility to apply relevant provisions on invalidity of contract and its consequences (damages claims, obligation to return everything received under the agreement, etc.). But this will be possible only if the party to the smart contract is identified and within the jurisdictional reach of the enforcement authority. Anyway, such enforcement actions won't have impact on the content of Blockchain database, unless it is created on different principles than the currently known Blockchain in Bitcoin."

[8] L. Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999; L. Lessing, *Code. Version 2.0*, 2006, at http://codev2.cc/ download+remix/Lessig-Codev2.pdf.

[9] See footnote 7 above.

remedies that lie outside the aforementioned blockchain.[10] Indeed, there is no evidence that the interests that have historically justified the existence of contract law (e.g. the interest in not having transfers of wealth capable of harming public economic order, morality or the values that are protected by mandatory rules) have ceased to exist. Nor is there any evidence that it is impossible to employ remedies other than those of modifying the transactions recorded on the blockchain.[11] This means, for example, that if one of the parties were to refuse to return what it received on the basis of an invalid agreement by creating a smart contract capable of executing a reverse transaction, the court could very well order it to pay compensation for an equivalent amount.[12]

This is by no means to suggest that contract law cannot adapt, as far as possible, to new developments, potentially by revising rules that appear out of step or insufficiently 'effective' in light of how new technologies work.

---

[10] On this point, please refer to Maugeri, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, cit., p. 53. See also Lehmann, *Crypto Economy and International Law*, cit., pp. 130 ss.; A. D'Adda, *Smart contract e diritto generale dei contratti*, in Gitti e Maugeri (eds), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, cit., p. 113.

[11] On this point, see O. Meyer, *Stopping the Unstoppable: Termination and Unwinding of Smart Contracts*, in *EuCML*, 2020, p. 20.

[12] Some scholars believe that, in order to overcome certain difficulties in reconciling smart contracts with contract law, we should increasingly rely on so-called hybrid smart contracts, i.e. advanced forms of smart contracts that aim to combine the on-chain blockchain infrastructure with off-chain data and calculations. It is argued that such hybridisation would take place through decentralised oracle networks (DONs). On this point, see N. Selvadurai, *Mitigating the Legal Challenges Associated with Blockchain Smart Contracts: The Potential of Hybrid On-Chain/Off-Chain Contracts*, in *Washington and Lee Law Review*, 80, 2023, pp. 1163 ff.

A different form of hybridisation is found, however, in the scenario considered by Doria (coordinator), Bassan, Rabitti, Sciarrone Alibrandi, and Malvagna, *Caratteristiche degli smart contracts*, cit., p. 5, No 17. According to the authors: "Commercial contracts often contain clauses that protect the parties from various borderline cases and that do not always lend themselves to being represented and executed through code. Let us imagine that a supplier of goods enters into a smart contract with a retailer. The payment terms could be defined in code and executed automatically upon delivery. The retailer will likely insist that the contract include an indemnification clause, whereby the supplier agrees to indemnify and hold the retailer harmless from claims for damages arising from a defective product. It would make no sense to represent this clause in code, as it is a clause that is not intended to be self-executing, but rather to be interpreted and applied by the parties and, in the event of a dispute, by the competent court."

According to the UK Law Commission, *Smart legal contracts. Advice to Governmen*t, cit.: "A hybrid smart legal contract is a contract in which some contractual obligations are defined in natural language and others are defined in the code of a computer program. Some or all of the contractual obligations are performed automatically by the code. At one end of the spectrum, the terms of a hybrid contract could be primarily written in code with a few natural language terms setting out, for example, the governing law and jurisdiction. At the other end of the spectrum, the terms of a hybrid contract could be primarily written in natural language and include just one or two terms written in code. In addition, the same contractual term(s) can be written in both natural language and in code. The natural language terms can be incorporated in an accompanying natural language agreement, or in natural language comments included in the code."

It is just a question of pointing out that it is not true that the entire field of contract law has lost any meaning in the context of a wealth circulation model that leverages new technologies.

It is now time to assess the validity of the scholarly opinion that smart contracts are also contracts in legal sense and the general rules would therefore certainly apply to them, with the exception, however, of those on performance, because smart contracts are self-executing. According to that view, this would lead to a significant alteration of the traditional function assigned to the courts,[13] which is typically that of providing contract enforcement.

Indeed, those who maintain that in the case of smart contracts there can no longer be a problem of non-performance fail to consider that the oracle (human or otherwise)[14] could err in assessing proper performance, and that the parties, at least in Italy, are bound not only by what is provided for in the agreement but also by all that which stems therefrom according to law or, failing that, according to custom and equity (Article 1374 of the Civil Code). This means that the proper execution of the code may not result in the proper performance of the contract.

I am aware of course that while the first circumstance is not beyond the realm of possibility in the present world of smart contracts, the second seems more theoretical than practical (which however does not mean that it should not be taken into account).

The contract could also be partially agreed upon outside the platform.[15] Clearly, in that scenario, nothing would preclude recourse to the courts to obtain protection in the event of non-performance by a party of the element not included in the smart contract. Building on (and reformulating) the above argument, I believe it can still be said that the widespread use of smart contracts can reduce litigation. Such not only for ideological reasons (i.e. subscribing to the crypto-anarchist cypherpunk

---

[13] K. Werbach and N. Cornell, *Contracts ex machina*, in *Duke Law Journal*, 2017, p. 106, according to whom: "Contract law is a remedial institution. Its aim is not to ensure performance ex ante, but to adjudicate the grievances that may arise ex post. Smart contracts bring this core function of contract law into sharper relief, as they eliminate the act of remediation by admitting no possibility of breach. But, the needs that gave rise to contract law do not disappear. If the parties do not or cannot represent all possible outcomes of the smart contract arrangement ex ante, the results may diverge from their mutual intent. The parties' expression may also not produce legally sanctioned outcomes, as in the case of duress, unconscionability, or illegality. Promise-oriented disputes and grievances will not disappear, but their complexions will shift. In such scenarios, either the parties or the state will seek to reintroduce the machinery of contractual adjudication. Once one properly appreciates what is – and what is not – the function of contract law, it becomes evident that the reports of its death are 'greatly exaggerated'."

[14] See Chapter 1 above.

[15] See the example considered in footnote 12 regarding indemnification.

movement[16] and the ensuing lack of faith in the judicial system), but also and above all because disputes related to non-performance of the contract, precisely because smart contracts are largely self-executing, would decrease significantly.

Therefore, contract law also applies in the context of the smart contracts under consideration here.[17]

3. THE EARLIEST RULES AIMED AT GIVING LEGAL EFFECT TO AGREEMENTS CONCLUDED THROUGH SMART CONTRACTS

Few legal systems have explicitly adopted a legal framework aimed at giving legal effect to agreements concluded through the use of smart contracts.

The first legislation, which took a step in that direction, was enacted in the United States, where there has been a positive response to the use of the new technologies in question from the outset[18] and where it has long been accepted that smart contracts can be used as a means of entering into contracts in a legal sense.[19]

---

[16] See above.

[17] See also, among others, A. Kaulbach, *Private Rechtsdurchsetzung durch Smart Contracts*, in *Juristen Zeitung*, 80, 2025, p. 383; V. Verdicchio, *Lo Smart Contract tra autonomia e autotutela*, in *ODCC*, 2025, pp. 3 ff.

[18] As further evidence of the overall favourable attitude toward the use and development of these new technologies, it should be noted that in 2018, the Joint Economic Committee recommended that "policymakers and the public should become more familiar with digital currencies and other uses of blockchain technology, which will have a wide range of applications in the future" and that "government agencies at all levels should consider and examine new uses for this technology that could make the government more efficient in performing its functions" (Joint Economic Committee of the Congress of the United States, *Joint Economic Report*, 13 March 2018, pp. 225–226, available at https://www.congress.gov/115/crpt/).

[19] Cf. L.A. DiMatteo and J.C. Jang, *Blockchain-Based Financial Services and Virtual Currencies: United States*, in *EuCML*, 2019, p. 251, according to whom: "On the private side of the law, smart contracts are considered to be rooted in traditional contract or sales law. Their enforceability will be decided by contract law despite their immutability. The difference may only be in perspective and not in a new body of rules. Usually the judicial system adjudicates contractual disputes and enforces terms. Smart contracts embed performance issues in the ex ante agreement resulting in immutable self-performance and the impossibility of breach, however, courts will still control their enforceability through the application of traditional contract law post hoc litigation."

On this point, see also Chamber of Digital Commerce, *Smart Contracts Legal Primer. Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable*, January 2018, available at https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf, which correctly answers the question "Is A Smart Contract Always a Legal Contract?" as follows:

"No. Because a smart contract is computer code, a smart contract may represent all, part, or none of a valid legal contract under U.S. law. Smart contracts function – in whole or in part – to give effect to legal contracts. Thus, smart contracts are the programmatic means by which some or all of the terms

Specifically, in Arizona, provisions were added to the Arizona Revised Statutes on 29 March 2017 stipulating that a contract may not be denied effect merely because it contains a "smart contract term".[20]

Wyoming law defines a smart contract as:

> an automated transaction, as defined in W.S. 40-21102(a)(ii), or any substantially similar analogue, which is comprised of code, script or programming language that executes the terms of an agreement, and which may include taking custody of and transferring an asset, or issuing executable instructions for these actions, based on the occurrence or non-occurrence of specified conditions.[21]

Tennessee law defines smart contracts as:

> an event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: Take custody over and instruct transfer of assets on that ledger; Create and distribute electronic assets; Synchronize information; or Manage identity and user access to software applications.

---

of the legal contract are performed. It is the underlying contractual terms that are given legal effect."

It then goes on to state: "Existing frameworks for legal contracts apply to smart contracts. […] There is no reason to believe that contracts processed, executed, or otherwise enforced via smart contract technology are not subject to these existing laws, just like any other contracts that use electronic technology to execute terms."

[20] Title 44, Chapter 26, Section 5 (Blockchain Technology) of the Arizona Revised Statutes provides as follows: "44-7061. Signatures and records secured through blockchain technology; smart contracts; ownership of information; definitions: A. A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature. B. A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record. C. Smart contracts may exist in commerce. A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term. D. Notwithstanding any other law, a person that, in or affecting interstate or foreign commerce, uses blockchain technology to secure information that the person owns or has the right to use retains the same rights of ownership or use with respect to that information as before the person secured the information using blockchain technology. This subsection does not apply to the use of blockchain technology to secure information in connection with a transaction to the extent that the terms of the transaction expressly provide for the transfer of rights of ownership or use with respect to that information. E. For the purposes of this section: 1. 'Blockchain technology' means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth. 2. 'Smart contract' means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger."

For further information on U.S. contract law, please refer to Maugeri, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, cit., pp. 39 ff.

[21] See Doria (coordinator), Bassan, Rabitti, Sciarrone Alibrandi and Malvagna, *Caratteristiche degli smart contracts,* cit., pp. 18-19.

However, the fact that there were no specific rules did not prevent various legal systems from holding that contracts could be concluded through smart contracts.[22] One can only agree, for example, with those who argue that

> a smart contract might be used to bring about a contract between natural or legal persons or any other parties endowed with legal personality. This is the contract in the legal sense and must not be confused with the bytes and bits constituting the smart contract. The smart contract concerns merely the formalities surrounding the conclusion of a contract.[23]

4. EU RULES ON SMART CONTRACTS

The European Union, as well, has long been moving in the direction of giving legal effect to activities taking place via distributed ledger technologies.

First of all, it is worth mentioning European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation. That resolution emphasises that the EU has an excellent opportunity to become the global leader in the field of DLT and to be a credible actor in shaping its development and markets worldwide, in collaboration with its international partners, outlining possible initiatives to foster the implementation of these new technologies.

Also worth mentioning is European Parliament resolution of 13 December 2018 on blockchain: a forward-looking trade policy, which – in highlighting that currently smart contracts may in general not be sufficiently mature to be considered legally enforceable within any sectoral regulation – implicitly acknowledges that, conversely, in some sectors, they may already be considered binding.[24]

Further evidence of the desire to accord importance to the phenomenon described thus far can be found in European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online.

However, the most relevant rules, which unequivocally demonstrate that the EU considers that a contract in a legal sense can be concluded via distributed ledger technologies, including through the use of smart contracts, are those set out in the previously mentioned Regulation (EU) 2023/1114 of the European Parliament and of

---

[22] Cf., for example, Lupini and Kerrigan, *Smart Contracts*, cit., p. 79; Lehmann, *Crypto Economy and International Law*, cit., p. 220 *et passim*.

[23] Lehmann, *Crypto Economy and International Law*, cit., p. 220 *et passim*.

[24] Point 29: "highlights that, at the moment, smart contracts may not be sufficiently mature to be considered legally enforceable within any sectoral regulation and further assessment of risks is

the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('MiCAR'), which will be discussed in more detail in the next chapter.

Among other things, Recital 29 MiCAR expressly states that Council Directive 93/13/EEC of 5 April 1993, on unfair terms in consumer contracts, remains applicable to offers to the public of crypto-assets where they concern business-to-consumer relationships, and Article 3(1)(5) MiCAR defines a "crypto-asset" as a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology

Therefore, it is clear that EU law considers that there may be transactions using distributed ledger technologies that meet the criteria for the application of the directives on contracts concluded between traders and consumers.

A definition of a smart contract, which affords it legal recognition but appears neutral on the question of whether or not the contract law framework can be applied to any agreements concluded using distributed ledger technologies, is provided in the EU's Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828). The Data Act, in regulating the right of access to data generated by IoT (Internet of Things) devices and within the broader context of a European Data Strategy, has included specific provisions on smart contracts. The definition of a smart contract is set out in Article 2 ("Definitions"), which states that such a contract means "a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering", and that it is subject to the requirements of the Data Act only if used "for the making available of data" (see Article 2, point 39).

5. ITALIAN LAW

In Italy, there appears to be no doubt that transactions on a distributed ledger can constitute a contract in a legal sense.

Indeed, Article 8-*ter* of Law-Decree No 135 of 14 December 2018 (so-called Simplification Decree, converted by parliament into Law No 12 of 11 February 2019)[25] introduced not only, as mentioned before, a definition of distributed ledger

---

needed".

[25] Cf. Remotti, *Blockchain smart contract: primo inquadramento e prospettive d'indagine (commento all'art. 8 ter D.L. 14 dicembre 2018, n. 135)*, cit., pp. 189 ff.

technologies but also a definition of a smart contract, according to which the execution of a smart contract automatically binds two or more parties based on the effects predefined by them and may also satisfy the requirement of the written form.

Indeed, the second paragraph of the said Article 8-*ter* defines a smart contract as follows:

> a computer program that runs on distributed ledger technologies and whose execution automatically binds two or more parties on the basis of effects predetermined by them. Smart contracts meet the requirement of the written form after computer identification of the parties involved, through a process meeting the requirements set by the Digital Italy Agency with guidelines to be adopted within 90 days after the entry into force of the act of parliament converting the law decree.

The Digital Italy Agency (AGID) has not yet taken action to establish guidelines regarding the form of the written contract.

The question has arisen as to whether the execution referred to in the provision defining a smart contract ("a computer program […] whose execution automatically binds") refers to the contract or to the program.[26] The reference to the program seems obvious. In the sense that it is the computer action that gives rise to the binding ties and not the performance of the contract in the legal sense.[27]

Those who advocate the alternative solution fail to consider the fact that a smart contract can be programmed to provide for the performance of the service on a date different from the date of execution of the code. Indeed, the defining characteristic of a smart contract is its programmability. The time of execution of the computer code and the time of performance of the service may coincide, but that simultaneousness is not necessary.

The arguments espoused by those who believe that smart contracts are real contracts in a legal sense[28] is not persuasive, because in the case in point there is no *traditio*, i.e. delivery of an object. Rather, we are dealing with the conclusion of a contract by conduct.

---

[26] See M. Nicotra, *L'Italia prova a normare gli smart contract, ecco come: pro e contro*, at https://www.agendadigitale.eu/documenti/litalia-prova-a-normare-gli-smart-contract-ecco-come-pro-e-contro/, accessed 27 February 2020, and the slides from L. Parola, *Blockchain e Smart Contract*, p. 16, at https://associazioneaiden.it/images/downloads/Aiden_Blockchain_16_aprile_2019_AVV_Lorenzo_Parola, accessed 27 February 2020.

[27] Likewise, M. Manente, L. 12/2019 – *Smart Contract e tecnologie basate su registri distribuiti – Prime note,* National Council of Notaries, approved by the IT Committee on 4 April 2019, p. 6, available at https://www.notariato.it/sites/default/files/S-1-2019DI.pdf.

[28] Nicotra, *L'Italia prova a normare gli smart contract*, cit.

Under certain conditions, a smart contract satisfies the requirement of written form.

According to some legal scholars, the rule is superfluous because a smart contract is an electronic document in any event.[29]

On the other hand,[30] since a smart contract is a computer program, doubts may arise as to its equivalence. According to that school of thought (which appears more persuasive), the rule appears absolutely appropriate in the absence of an express provision on fulfilment of the requirement of non-modifiability referred to in Article 3(2) of Prime Ministerial Decree of 13 November 2014 and the provisions of Article 4(3) of Prime Ministerial Decree of 22 February 2013, further to which a computer document containing macro-instructions or executable codes (the latter contained, by definition, in a smart contract) cannot be considered as non-modifiable. Indeed, in the absence of an express provision, a smart contract could well fail to fall within the scope of the category of unmodifiable computer document, with the consequence that it would lose its validity.

The fact that it is the smart contract itself, as a computer program, that fulfils, under certain conditions, the requirement of a written form offers little room for attributing binding force to 'natural' language translations that may be attached to the smart contract, or at least offers little room for those parts of the translation that overlap with the parts regulated by the algorithm.

Article 26(1) of Legislative Decree No 36 of 31 March 2023 - Public Procurement Code, tasks AGID with establishing the procedures for the certification of digital procurement platforms.

In 2023[31] AGID took action and inter alia established the characteristics of platforms for managing surety bonds that operate using distributed ledger technologies. In particular, it established that

> the recording of the issued surety bond in the distributed ledgers is carried out by means of a smart contract, which must ensure that the operation can only be performed by a party that is authorised to issue surety bonds pursuant to Article 106(3) of the Code and is authorised to record entries in the distributed ledger, subject to electronic identification with a substantial or high level of assurance in accordance with the eIDAS Regulation.[32]

---

[29] Parola, *Blockchain e Smart Contract*, cit., p. 16.

[30] Nicotra, *L'Italia prova a normare gli smart contract*, cit.

[31] AGID, *Regole tecniche. Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale*, 1 June 2023, available at https://www.agid.gov.it/sites/agid/files/2024-07/regole_tecniche_e-procurement.pdf.

[32] See points 6.2-5.2.

6. CONSUMERS AND DIGITAL FINANCIAL SERVICES. SCOPE OF THE STUDY

Based on the above, it can be concluded that under Italian law contracts can be concluded on distributed ledgers, including through the use of smart contracts, and that remedies for any breaches of domestic and EU contract law can also be pursued outside of the DLT framework concerned. Both general and sector-specific contract law rules will apply to those contracts.

That said the author of a monographic work like this book can only select the contract-related aspects to which they intend to devote their attention. To that end the next chapter will address the issue of consumer protection in distance contracts in the financial markets that use distributed ledger technologies.

.

Chapter 3. Consumer Protection in the Crypto-asset Financial Market

CONTENTS: 1. Consumers and digital financial services. - 2. Does MiCAR protect consumers? - 3. On the non-applicability of Directive 2011/83/EU of 25 October 2011 on consumer rights to financial markets. - 4. On the applicability of Directive 2002/65/EC of 23 September 2002 concerning the distance marketing of consumer financial services to tokenised financial instruments. - 5. Derogations from Directive 2002/65/EC introduced by Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market. - 6. Coordination of consumer protection rules with MiCAR.

1. CONSUMERS AND DIGITAL FINANCIAL SERVICES

The digital transition is an absolute priority for the European Union over the next decade. As Charles Michel, the former President of the European Council, emphasised in a speech (at the FT-ETNO Forum) on 29 September 2020, digital strategy in general and the development of digital finance in particular should be based on European values and effective risk regulation.

Consumers are increasingly using digital financial services and trading crypto-assets, typically remotely. Therefore, it is necessary to consider the type of protection they receive in the context of the financial markets that use distributed ledger technologies. This context could, hypothetically, also be affected by technological constraints. When considering the protection of those who trade in crypto-assets, the first thing that comes to mind is the digital finance package, presented on 24 September 2020, and in particular the previously mentioned Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May

2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('MiCAR').[1]

However, it is sometimes forgotten that, even before MiCAR, there were rules in place to protect consumers entering into distance contracts in the financial markets. There come to mind, for example, the provisions contained in the following directives: Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts; Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive'), as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 ('Omnibus Directive'); Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights and Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services, which will remain in force until 18 June 2026[2]; and, lastly, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market ('PSD2'), which does not protect just consumers only.

---

[1] See, among others, Annunziata and Sciarrone (eds), *Cripto-attività. La disciplina europea nel contesto globale*, cit.; P. Maume, Consumer Protection, in P. Maume, L. Maute, and M. Fromberger, *The Law of Crypto Assets. A Handbook*, Munich-New York-Oxford-Baden-Baden, Beck/Nomos/Hart, 2022, pp. 109 ff.; M. Maugeri, *Criptoattività, proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore*, in *Contratto e impresa Europa*, 2022, pp. 1 ff.; M. Maugeri, *Proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore nella commercializzazione a distanza*, in Gitti and Maugeri (eds), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, cit., pp. 236 ff.; L. Modica, *La proposta di regolamento MiCA e la disciplina delle pratiche commerciali scorrette*, id., pp. 295 ff.; S. Pagliantini, *La proposta MiCAR e le clausole abusive: una prima lettura*, id., pp. 333 ff.; P. Sirena, *La tutela del consumatore nella commercializzazione a distanza di cripto-attività*, id., pp. 315 ff.

On MiCAR in general, see P. Maume, *The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?,* in *European Company and Financial Law Review*, 2023, pp. 243 ff.; T. van der Linden and T. Shirazi, *Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Cryptoassets?*, in *Financial Innovation*, 2023, pp. 22 ff.; F. Annunziata, *An Overview of the Markets in Crypto-Assets Regulation (MiCAR)*, *EBI Working Paper Series*, 2023, No 158; T. Tomczak, *Crypto-assets and Crypto-assets' Subcategories Under MiCA Regulation*, in *Capital Markets Law Journal*, 2022, pp. 365 ff.; F.P. Patti, *L'offerta al pubblico di cripto-attività nel titolo II del Regolamento MiCA*, in *Rivista di diritto civile*, 2024, pp. 97 ff.

On the issue of the burden of proof, see V. Profeta, *Profili giuridici dell'e-money token (EMT)*, in V. Profeta (ed), *Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento*, in the series *Quaderni di Ricerca giuridica*, 103, Bank of Italy, 2025, p. 125.

[2] Unless otherwise specified, after 18 June 2026 references herein to Directive 2002/65/EC are be understood as referring to Chapter IIIa (Rules concerning financial services contracts concluded at a distance) of Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC.

To be fair, some of the aforementioned legislation has, to date, been applied only sporadically – indeed, I would say rarely – within the sector under consideration here. Nevertheless, the directives in question exist, and it is important to be aware of them.

Here, I will focus exclusively on the last three, namely, Directive 2011/83/EU, Directive 2002/65/EC and Directive (EU) 2015/2366. In other words, I will attempt to determine which legal framework applies in the event that a consumer enters into a distance contract in the crypto-asset financial market, and how PSD2 operates with regard to crypto-assets that meet the criteria for payment services.

Below, I will attempt to elucidate the relationship between the aforementioned sets of rules and MiCAR. First, however, I will devote a few words to MiCAR in order to better explain why I believe we should address the issue of coordination with consumer protection law.

2. DOES MiCAR PROTECT CONSUMERS?

MiCAR is the first European attempt to regulate the phenomena described in the preceding pages. The EU's primary aim was to regulate stablecoins. Indeed, the lawmakers were primarily concerned about the possibility that stablecoins, as we discussed in Chapter 1, could undermine financial stability.

MiCAR applies from 30 December 2024.

As already mentioned,

> MiCAR contains many rules that resemble mini-versions of existing regulations for financial services. For instance, it contains disclosure rules for the whitepaper that are similar to, but less extensive than those governing the prospectus required for the issuance of financial instruments under the Prospectus Regulation; it also provides rules for "investment service providers" that are reminiscent of those governing market operators and investment firms (MiFID II/MiFIR); it furthermore features capital requirements which are similar to those that apply to banks and securities firms; and it even includes rules on on-going disclosure, insider trading and market manipulation that are modelled on those reigning on traditional capital markets (MAD/MAR).[3]

Below, we will attempt to determine whether MiCAR also includes rules that align with the framework of consumer protection law.

The core purpose of MiCAR is to regulate crypto-assets, defined as digital representations of "a value or of a right that is able to be transferred and stored

[3] Lehmann, *Crypto Economy and International Law*, cit., pp. 85-86.

electronically using distributed ledger technology or similar technology" (Article 3(1)(5).

MiCAR applies to e-money tokens, asset-referenced tokens, and crypto-assets other than asset-referenced tokens and e-money tokens (Article 1).

However, it does not apply to crypto-assets issued by the ECB, national central banks, the European Investment Bank, the European Financial Stability Facility, the European Stability Mechanisms and public international organisations (Article 2). It also does not apply to unique non-fungible crypto-assets (Article 2), although MiCAR's definition of NFTs does not coincide with the definition used in common parlance, so it is questionable whether MiCAR can be said not to apply to NFTs in general.

Furthermore, it does not apply to financial instruments, including those in tokenised form, governed by MiFID II, to deposits, to funds as defined by PSD2 (unless they qualify as e-money tokens), to securitisation positions, or to insurance and pension products (Article 2).

Finally, it appears that it does not apply to DeFi. In reality, however, it would be more accurate to say that it does not apply to crypto-assets that circulate in a fully decentralised manner without the involvement of intermediaries and to crypto-assets that do not have an identifiable issuer, adding that, in any event, crypto-asset service providers that provide services in relation to such crypto-assets should nevertheless fall within the scope of the Regulation. Indeed, Recital 22 states the following:

> This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation. This Regulation covers the rights and obligations of issuers of crypto-assets, offerors, persons seeking admission to trading of crypto-assets and crypto-asset service providers. Where crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation. Crypto-asset service providers providing services in respect of such crypto-assets should, however, be covered by this Regulation.

Among the tokens regulated by MiCAR, the first type are e-money tokens (EMTs) consisting of crypto-assets that aim to stabilise their value by referencing only one official currency. The function of such crypto-assets is very similar to the function of electronic money as defined in Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Like electronic

money, such crypto-assets are electronic surrogates for coins and banknotes and are likely to be used for making payments.

The second type are asset-referenced tokens (ARTs), which aim to stabilise their value by referencing another value or right, or combination thereof, including one or several official currencies.

Finally, the third type are crypto-assets other than asset-referenced tokens and e-money tokens, and covers a wide variety of crypto-assets, including utility tokens.

MiCAR is expressly intended to protect the "retail holder"[4] as well. The latter is defined as "any natural person who is acting for purposes which are outside that person's trade, business, craft or profession" (see Article 3(1)(37)). In other words, the term is defined in the same way as it is defined within the EU in the legislation designed to protect consumers when entering into distance contracts.

Therefore, MiCAR addresses relationships that are already subject to EU regulation, thereby making it necessary to understand how MiCAR fits in with the pre-existing rules.

3. ON THE NON-APPLICABILITY OF DIRECTIVE 2011/83/EU OF 25 OCTOBER 2011 ON CONSUMER RIGHTS TO FINANCIAL MARKETS

Although Directive 2011/83/EU expressly does not apply to financial services (Article 3(3)(d)), defined as "any service of a banking, credit, insurance, personal pension, investment or payment nature" (Article 2(12)), some authors have argued that the rules contained therein could be applied to the crypto-asset sector within the financial markets.

Support for this argument appeared to be provided in the initial version of the proposal for the regulation on markets in crypto-assets, in which Recital 16 stated that Directive 2011/83/EU was to remain applicable, thereby implicitly accepting the idea that that directive could be applied within financial markets. However, that reference no longer appears in MiCAR as actually adopted. Therefore, the EU appears

---

[4] The choice to use the term "retail holder" likely stems from the belief, not uncommon among experts in financial markets law, that *consumer* transactions cannot occur in the sector in question. For example, in his essay on *Regolazione finanziaria e consumeristica in tema di offerta di servizi finanziari e di investimento*, in *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza*, Milan, Giuffrè Francis Lefebvre, 2019, pp. 355 ff., A. Genovese expresses doubts about the possibility, the systematic coherence, and the usefulness of integrating private-law and contractual protections for the retail customer.

to have intended to take a position in favour of its inapplicability in the sector under consideration.

However, this may not be conclusive. Before wrapping up this discussion, it is therefore appropriate to pay due attention to the main issue that has led some legal scholars to opine that Directive 2011/83/EU on consumer protection does actually apply to the financial sector. I am referring to the question of whether or not the sale (or transfer) by the issuer of shares, bonds or funds, including tokenised ones, can also be treated as falling within the category of "financial services".

This issue was recently examined in depth by Philipp Maume. According to that scholar, the only applicable framework in the case of the acquisition of tokens (i.e. the acquisition of a share, a bond or a fund unit) is that set out in Directive 2011/83/EU.[5]

In other words, the author distinguishes between a contract for the "acquisition of financial products" and a "financial services contract", maintaining that Directive 2011/83/EU on consumer rights applies to the former while Directive 2002/65/EC on the distance marketing of consumer financial services applies to the latter.

This interpretation is not persuasive. Truth be told, the list contained in Directive 97/7/EC on the protection of consumers in respect of distance contracts, which was repealed and replaced by Directive 2011/83/EU and to which the author expressly refers in order to delimit the scope of application of the latter (which, as mentioned, derives from Directive 97/7/EC), is explicitly described as "non-exhaustive" in Article 3 of the 1997 directive itself. Furthermore, Directive 2002/65/EC, which regulates the "distance marketing of consumer financial services" (Article 1), defines a distance contract as

> any contract concerning financial services concluded between a supplier and a consumer under an organised distance *sales*[6] or service-provision scheme run by the supplier, who, for the purpose of that contract, makes exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded.

---

[5] In particular, when addressing the consumer's right of withdrawal, the author argues in *Consumer Protection*, cit., p. 110, that "not relevant [...] is Directive 2002/65/EC on financial services and direct marketing (Financial Services Directive, FSF). It applies to the provision of financial services online. The Directive mentions typical financial services as examples: bank accounts, credit cards, portfolio management, etc. [...] The non-crypto equivalent of a token acquisition (which would be the acquisition of a share, bond, or fund) is not mentioned. That is straightforward because selling something to someone is not the same thing as providing a service for someone. Token sales are more comparable to the sale of goods, which generally falls within the scope of Directive 97/7/EC on distance contracts (Rec. 10 FSD) and its successor, the CRD. Thus, issuing tokens is not a financial service within the scope of FSD".

[6] Emphasis added.

This fact makes it clear that the directive in question does not at all exclude sales (or purchase) contracts from its scope of application. In other words, the rules pertain to the sector and not to the type of contract.[7]

And it is plausibly in line with the interpretation proposed here that the reference to Directive 2011/83/EU contained as aforesaid in Recital 16 in the initial version of the proposal for the regulation on markets in crypto-assets was intentionally removed from MiCAR as adopted.

Indeed, in the preparatory works from April 2021, we can read the following:

> Directive 2011/83/EU does not apply to financial services; referring it would be contradictory with the purpose of restricting the scope to financial like products/services.

The reference to products, in addition to services, clearly demonstrates support for the view that Directive 2002/65/EC applies to the financial sector in general.

4. ON THE APPLICABILITY OF DIRECTIVE 2002/65/EC OF 23 SEPTEMBER 2002 CONCERNING THE DISTANCE MARKETING OF CONSUMER FINANCIAL SERVICES TO TOKENISED FINANCIAL INSTRUMENTS

Therefore, the framework that applies to distance contracting within the financial sector, in BtoC relationships, is that set out in Directive 2002/65/EC. There is no reason to believe that the "marketing" of crypto-assets could fall outside the scope of that legislation.[8]

That directive, like Directive 2011/83/EU, defines financial services as "any service of a banking, credit, insurance, personal pension, investment or payment nature" (Article 2, point (b)). That same directive establishes information obligations vis-à-vis the consumer prior to the conclusion of a distance contract (Article 3),

---

[7] Directive 2011/83/EU makes express reference to contracts in the financial "area" when defining its scope of application (see Recital 32). For further information on this point, please refer to Maugeri, *Proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore nella commercializzazione a distanza*, cit., pp. 236 ff.

[8] On 24 January 2017 the District Court of Verona (https://www.ilcaso.it/giurisprudenza/archivio/16726.pdf) held that the provisions of the Italian Consumer Protection Code transposing Directive 2002/65/EC were applicable to a transaction involving the exchange of traditional currency for Bitcoin.

formal requirements for the communication of contractual terms and conditions and the prior information (Article 5), and the consumer's right of withdrawal (Article 6).

The information to be provided to the consumer concerns: i) the supplier (e.g. identity, main business, geographical address, trade register in which it is registered, details of its registration); ii) the financial service (including, among other things, the main characteristics of the product, the total price, any relationship between the financial service and instruments that present particular risks or whose price depends on market fluctuations, the existence of any taxes or costs not paid via the supplier, payment methods, and any additional costs); iii) the distance contract (e.g. the existence or absence of a right of withdrawal, the duration of the contract, the method for exercising the right of withdrawal, and the applicable law); and iv) redress (out-of-court complaint procedures, existence of guarantee funds, etc.).

Communications must be made on paper or another durable medium. It is further provided that at "any time during the contractual relationship the consumer is entitled, at his request, to receive the contractual terms and conditions on paper". Overall, this provision appears outdated and, in the context of the crypto-asset market, decidedly out of step with the times.

Therefore, it is no coincidence that the right of withdrawal no longer appears in Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC.

The right of withdrawal does not apply to financial services whose price depends on fluctuations in the financial markets outside the supplier's control (Article 6(2)).

Recital 16 of the said Directive (EU) 2023/2673, which will apply from 19 June 2026, states as follows:

> In order to ensure legal certainty, and to ensure that there are no duplications or overlaps, it should be clarified that, where other Union acts governing specific financial services contain rules on pre-contractual information, on the right of withdrawal or on adequate explanations, and irrespective of the level of detail of those rules, only the respective provisions of those other Union acts should apply to those specific consumer financial services unless otherwise provided in those acts, including the explicit option for Member States to exclude the application of those specific rules.

Furthermore, Article 16a(10) of Directive 2011/83/EU, as inserted by Directive (EU) 2023/2673 as regards financial services contracts concluded at a distance, provides as follows:

> Where another Union act governing specific financial services contains rules on the information to be provided to the consumer prior to the conclusion of the contract, only the rules of that Union

act shall apply to those specific financial services, irrespective of the level of detail of those rules, unless otherwise provided in that Union act.

5. DEROGATIONS FROM DIRECTIVE 2002/65/EC INTRODUCED BY DIRECTIVE (EU) 2015/2366 OF 25 NOVEMBER 2015 ON PAYMENT SERVICES IN THE INTERNAL MARKET

However, while the framework described above is generally applicable to consumer protection in the context of crypto-assets in the financial markets, it is now necessary to pay particular attention to the context of payment services, which are also affected by MiCAR.

Indeed, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC ('PSD2') establishes derogations from Directive 2002/65/EC with regard to payment services.

In particular, Article 39 PSD2 states that the provisions contained therein are without prejudice to any provision of Union law containing additional requirements on prior information. However, where Directive 2002/65/EC is also applicable, the information requirements set out in Article 3(1) of that directive, with the exception of points (2)(c) to (g), (3)(a), (d) and (e), and (4)(b) of that paragraph, are to be replaced by Articles 44, 45, 51 and 52 PSD2 itself.

Those articles lay down the obligation to disclose information related to the specific nature of the payment instrument. This means that in general Directive 2002/65/EC would appear to continue to apply also in the context of payment instruments. Solely the disclosure obligations appear to be specified in different terms and hence follow the rules set out in PSD2. The new rules, contained in Article 16a(10) of Directive 2011/83/EU, as inserted by Directive (EU) 2023/2673, confirm that outcome also with reference to the period after June 2026.

Although it is not aimed exclusively at protecting consumers, but rather customers in general, it is worth noting that the main security and protection measure provided for by PSD2 is strong customer authentication (SCA), a procedure for validating a user's identity based on the use of two or more authentication factors. SCA is mandatory when a customer accesses their online payment account, when they initiate an electronic payment transaction, and when they perform any action via a remote channel that could pose a risk of payment fraud or other abuse.

In the following sections, we will examine whether strong customer authentication is also required in the case of tokens regulated by MiCAR.

6. COORDINATION OF CONSUMER PROTECTION RULES WITH MiCAR

We will now examine how the two directives mentioned above interact with MiCAR from the perspective of consumer protection.

It should be clarified at the outset that, given the different risks, MiCAR imposes different rules on issuers depending on the type of token (see Recital 18). I will therefore structure the following remarks with those differences in mind. First, let us examine the obligations imposed on issuers of crypto-assets other than asset-referenced tokens and e-money tokens. Those entities, which must be legal persons (Article 4(1)(a)), are required to submit a white paper containing

> general information on the issuer, offeror or person seeking admission to trading, on the project to be carried out with the capital raised, on the offer to the public of crypto-assets or on their admission to trading, on the rights and obligations attached to the crypto- assets, on the underlying technology used for such crypto-assets and on the related risks.[9]

The list of information to be provided in the white paper, set out in Article 6 MiCAR, follows the structure of Directive 2002/65/EC and, in addition to the information required by that directive, also includes further disclosure obligations. Therefore, it would appear that compliance with the MiCAR framework also entails simultaneous compliance with the provisions of the said directive.

The white paper must be published on the websites of the offeror and the persons seeking admission to trading (Article 9). This white paper must also be notified to the competent national authorities (Article 8). The version published on the website and the version provided to the national authorities must be identical (Article 9). The dual requirement (publication on the offeror's website and the identity of that version with the version provided to the national authorities) makes the offeror's disclosure unalterable (with regard to the period in which it is provided). It thus allows the requirements for the disclosure of information on a "durable medium", as stipulated by Directive 2002/65/EC, to be considered as met (mere publication on the website alone would not be sufficient).[10]

Furthermore, Article 11(2) MiCAR expressly provides as follows:

---

[9] Recital 24.

[10] See Recital 20 of Directive 2002/65/EC.

> Offerors and persons seeking admission to trading of crypto-assets other than asset-referenced tokens or e-money tokens that have published a crypto-asset white paper in accordance with Article 9 […] shall not be subject to any further information requirements with regard to the offer to the public or the admission to trading of that crypto-asset.

Therefore, if the information requirements under MiCAR are met, there is no need to provide the person accepting the offer with any additional information. In any case, through MiCAR, the subscriber receives a level of protection in terms of information that is no less than that which they would have received through the application of the Distance Selling Directive. It should also be noted that, as of 19 June 2026, the new Directive (EU) 2023/2673 will apply, which as aforesaid provides as follows:

> Where another Union act governing specific financial services contains rules on the information to be provided to the consumer prior to the conclusion of the contract, only the rules of that Union act shall apply to those specific financial services, irrespective of the level of detail of those rules, unless otherwise provided in that Union act.

This means that the information requirements set out in MiCAR will be the only ones applicable.

The offeror of crypto-assets other than asset-referenced tokens and e-money tokens must guarantee the right of withdrawal to any retail holder who purchases such crypto-assets directly from the offeror or from a crypto-asset service provider placing crypto-assets on behalf of the offeror. This right to withdraw may be exercised within 14 days and begins to run from the date of the agreement of the retail holder to purchase the crypto-assets. Offerors must provide information on the right of withdrawal in the white paper. The right of withdrawal does not apply if the crypto-assets have been admitted to trading on a trading platform prior to their purchase by the retail holder (see Article 13), and this, as clarified in Recital 37, is because "in such a case, the price of such crypto-assets depends on the fluctuations of the markets in crypto-assets".

As can be readily seen, the right of withdrawal is structured in accordance with the provisions of Directive 2002/65/EC (including with regard to forfeiture of the right of withdrawal if the price of the financial product depends on market fluctuations outside the provider's control). It is therefore not surprising that, again in Recital 37 MiCAR, it is specified as follows: "Where the retail holder has a right of withdrawal under this Regulation, the right of withdrawal under Directive 2002/65/EC of the European Parliament and of the Council should not apply."

Therefore, MiCAR explicitly clarifies that, in general terms, even in the event of the offeror transferring crypto-assets other than asset-referenced tokens and e-money tokens, the provisions of Directive 2002/65/EC should apply. However, since

the Regulation contains a specific (and identical) rule on withdrawal, those provisions no longer apply.

Turning now to examine the MiCAR requirements for the admission to trading and offering of e-money tokens, it should be noted at the outset that Article 48(2) MiCAR expressly equates e-money tokens with e-money ("E-money tokens shall be deemed to be electronic money"). There is thus no doubt that PSD2 also applies to these tokens.

MiCAR stipulates that no person shall make an offer to the public or seek the admission to trading of an e-money token, within the Union, unless that person is the issuer of such e-money token (Article 48) (without prejudice, however, to the issuer's ability to delegate the task of offering them to the public or applying for their admission to trading to a third party upon the issuer's prior written consent).

Before offering e-money tokens or seeking their admission to trading on a trading platform, the issuer must publish a white paper (and a summary thereof) on its website (Article 51). The white paper must be notified to the competent authorities.

The list of information to be provided through the white paper, set out in Article 51 MiCAR, follows the structure of Directive 2002/65/EC and PSD2, while also providing for additional disclosure obligations. Therefore, compliance with MiCAR rules simultaneously entails compliance with the provisions of the said directives, in particular those of PSD2, which, as mentioned before, in respect of the types of information to be provided, is the only applicable directive since it derogates from Directive 2002/65/EC concerning the distance marketing of financial services. Again, in this case, the obligation to disclose the existence or absence of the right of withdrawal cannot but be subsumed under the general obligation to provide information on the rights and obligations attached to the electronic money token (Article 51(1)(d) MiCAR).

There are no compatibility issues with the provisions on durable media, as the white paper must be published on the issuer's website and communicated to the competent authorities. Therefore, the notice can be considered unalterable (with reference to the period in which it is provided) and, consequently, apt to fulfil the requirements for the provision of information on a "durable medium" as set out in Directive 2002/65/EC.

At the request of holders of e-money tokens, the issuer is required to redeem the value of the tokens in funds other than e-money, i.e. in banknotes or coins.[11]

---

[11] See the definition of funds in Article 4(1)(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

More specifically, Article 49(4) MiCAR provides as follows:

> Upon request by a holder of an e-money token, the issuer of that e-money token shall redeem it, at any time and at par value, by paying in funds, other than electronic money, the monetary value of the e-money token held to the holder of the e-money token.

The white paper must specify the conditions for redemption (Article 49(5) MiCAR).

This form of protection is even stronger than the right of withdrawal. Nevertheless, currently consumers can also exercise the right of withdrawal provided for by Directive 2002/65/EC. This will remain the case, unless further changes are made, even after 19 June 2026, the date from which the new Directive (EU) 2023/2673 will apply. This is because, with regard to withdrawal, the new rules provides as follows:

> Where another Union act governing specific financial services contains rules on the right of withdrawal, only rules of that Union act on the right of withdrawal shall apply to those specific financial services, unless otherwise provided in that other Union act. Where that other Union act gives Member States the right to choose between the right of withdrawal and an alternative, such as a reflection period, only the corresponding rules of that Union act shall apply to those specific financial services, unless otherwise provided in that other Union act.[12]

With regard to e-money tokens, MiCAR does not provide for rules on withdrawal. Therefore, only the rules on the distance marketing of financial services set out in Directive 2011/83/EU, as amended, can apply.

However, one might wonder whether the withdrawal remedy is not out of step with the phenomenon of crypto-assets running on DLT. It seems to me that, even if one were to accept the idea that a remedial mechanism that coercively impacts DLT – in addition to not being technically feasible at present – could be considered incompatible with the functioning of this new technology, there would be no reason

---

[12] See the new Article 16b(6) of Directive 2011/83/EU, as inserted by Directive (EU) 2023/2673.

That article has been transposed into Italian law by Legislative Decree No 209 of 31 December 2025, introducing Article 59-*octies* into the Consumer Protection Code (Right of withdrawal from distance contracts for financial services), paragraph 9 of which provides as follows: "Where an act of the European Union other than Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 governing specific financial services contains rules on the right of withdrawal, only the rules on the right of withdrawal of that European Union act shall apply to those specific financial services, unless otherwise provided in that other European Union act. Where that other European Union act gives Member States the right to choose between the right of withdrawal and an alternative, such as a reflection period, only the corresponding provisions of that European Union act shall apply to those specific financial services, unless otherwise provided in that other European Union act."

These new rules must be taken into account in the remainder of our discussion.

to rule out the possibility that such a remedy could operate outside DLT. Therefore, there is nothing to prevent the possibility of providing for restitution obligations to be enforced outside DLT (as is the case, for example, with redemption).

Nor can it be argued, as has been said in relation to so-called *other than tokens*, that withdrawal should be excluded when EMTs have been admitted to trading on a trading platform, because "in such a case, the price of these crypto-assets depends on fluctuations in the crypto-asset markets" (see Recital 37, cited above). Indeed, EMTs are pegged to an official currency.

Before concluding this discussion, it is necessary to consider – as mentioned above – whether the use of EMTs as payment instruments requires the application of strong customer authentication.

I had previously argued that SCA should be required, also in light of the current PSD2 reform proposals.[13] This view is now confirmed by the Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens, dated 10 June 2025, which advises competent national authorities not to prioritise the supervision and enforcement of some PSD2 provisions, such as on safeguarding, the disclosure of information to consumers pertaining to the level of applicable charges, the maximum execution time of payment transactions, and the unique identifier (e.g. IBAN), and open banking, while insisting on others, such as the application of strong customer authentication to the accessing of custodial wallets and the initiation of EMT transfers.

It is now time to devote some attention to ARTs. Indeed, given the rules governing issuers and offerors in terms of information and withdrawal, an argument similar to that made for EMTs can be put forward for asset-referenced tokens. Indeed, those entities are also required to prepare a white paper and a summary of it, written in clear and understandable language. The summary must state the possibility of exercising the right of redemption.

Again, the list of information to be provided in the white paper follows the structure of the two aforementioned directives (although there are strong doubts as to whether ARTs can be considered payment instruments) and also includes additional disclosure requirements. Therefore, it would appear that, once again, compliance with the MiCAR framework also entails simultaneous compliance with the provisions of those directives. With regard to ARTs as well, the same considerations apply as those mentioned above concerning the entry into force of the new rules on the distance marketing of financial services.

---

[13] M. Maugeri, *La tutela dei consumatori nel mercato finanziario delle cripto-attività,* in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 2025, pp. 12 ff.

The white paper, approved by the authorities, must be published on the issuer's website and reported by the competent authorities to ESMA, which must enter it in the register of white papers of issuers of asset-referenced tokens made available to the public on the agency's website. Therefore, in this case as well, the communication can be considered unalterable (with regard to the period during which it is provided) and, consequently, capable of meeting the requirements for the communication of information on a "durable medium" set out in Directive 2002/65/EC.

Similarly, with regard to the sale of asset-referenced tokens, there is no provision for withdrawal, but there are provisions for redemption and the right of redemption. Therefore, this constitutes strong protection, but it does not preclude the possibility of exercising withdrawal, for the reasons already mentioned above with reference to the rules on e-money tokens. In this case, however, the price of the ART could depend on fluctuations in the financial markets that outside the provider's control. Therefore, in some cases, Article 6(2) of Directive 2002/65/EC may apply.

Turning now to consider the relationship between the obligations imposed on service providers, as defined in MiCAR, and compliance with the obligations set out in Directive 2002/65/EC and PSD2.

According to Article 3(1)(16) MiCAR, a "crypto-asset service" means:

> any of the following services and activities relating to any crypto-asset:
>
> a) providing custody and administration of crypto-assets on behalf of clients;
>
> b) operation of a trading platform for crypto-assets;
>
> c) exchange of crypto-assets for funds;
>
> d) exchange of crypto-assets for other crypto-assets;
>
> e) execution of orders for crypto-asset on behalf of clients;
>
> f) placing of crypto-assets;
>
> g) reception and transmission of orders for crypto-asset on behalf of clients;
>
> h) providing advice on crypto-assets;
>
> i) providing portfolio management on crypto-assets;
>
> j) providing transfer services for crypto-assets on behalf of clients.

Recital 79 MiCAR states as follows:

> Crypto-asset services should be deemed 'financial services' as defined in Directive 2002/65/EC in cases where they meet the criteria of that Directive. Where marketed at distance, the contracts between crypto-asset service providers and consumers should be subject to Directive 2002/65/EC as well, unless expressly stated otherwise in this Regulation.

Therefore, when marketed at a distance, all contracts concluded between crypto-asset service providers and consumers should be subject to the provisions of Directive 2002/65/EC, unless MiCAR itself provides otherwise.

Furthermore, Recital 90 MiCAR states as follows:

> Some crypto-asset services, in particular providing custody and administration of crypto-assets on behalf of clients, the placing of crypto-assets, and transfer services for crypto-assets on behalf of clients, might overlap with payment services as defined in Directive (EU) 2015/2366.

In the Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens, dated 10 June 2025, the EBA

> advises NCAs[14] during said intervening period to regard the transfer of crypto assets as a payment service under PSD2 where they entail EMTs and are carried out by the entities on behalf of their clients; to regard the custody and administration of EMTs as a payment service under PSD2; and to regard a custodial wallet as a payment account under the PSD2 where the wallet is held in the name of one or more clients and allows to send and receive EMTs to and from third parties. For these services, the No Action letter advises NCAs to require an authorisation under PSD2 through streamlined procedures that make maximum use of information that legal entities have already provided during their CASP authorisation under MiCA. However, NCAs are advised to grant applicants a transition period until 1 March 2026 before the authorisation needs to be held. After that date, NCAs are advised to prevent entities that are not licenced as a PSP or have not entered into a partnership with a PSP, from providing services related to EMTs that qualify as a payment service.

In light of the division identified in the Opinion, we must once again seek to understand what the relationship might be between the rules set out in the two directives and those set out in MiCAR.

The information that crypto-asset service providers must provide to the competent authority in order to obtain authorisation is highly detailed and onerous (Article 59 MiCAR).

Article 66 MiCAR provides inter alia as follows:

1. Crypto-asset service providers shall act honestly, fairly and professionally in accordance with the best interests of their clients and prospective clients.
2. Crypto-asset service providers shall provide their clients with information that is fair, clear and not misleading, including in marketing communications, which shall be identified as such.

---

[14] NCA stands for National Competent Authorities.

Crypto-asset service providers shall not, deliberately or negligently, mislead a client in relation to the real or perceived advantages of any crypto-assets.

3. Crypto-asset service providers shall warn clients of the risks associated with transactions in crypto-assets.

   When operating a trading platform for crypto-assets, exchanging crypto-assets for funds or other crypto-assets, providing advice on crypto-assets or providing portfolio management on crypto-assets, crypto-asset service providers shall provide their clients with hyperlinks to any crypto-asset white papers for the crypto-assets in relation to which they are providing those services.

4. Crypto-asset service providers shall make their policies on pricing, costs and fees publicly available, in a prominent place on their website.

MiCAR also sets out specific information obligations related to the type of service, as well as obligations related to the notices to be provided to customers regarding the conditions under which their order is considered final (see Articles 75 *et seq*.[15]).

Again, it seems to me that the level of information covers the requirements of Directive 2002/65/EC and PSD2, where applicable. However, since there is no explicit exclusion, it would appear that once again the two directives may apply with regard to withdrawal. Therefore, the pre-existing rules and MiCAR seem to be partly overlapping and partly complementary.

With regard to information obligations, the EU has deliberately followed the approach of the directives we have discussed here. Therefore, compliance with MiCAR, with regard to disclosure and formal requirements, also entails compliance with the directives aimed at protecting (among others) consumers. In any case, as of 19 June 2026, the new Directive (EU) 2023/2673 will apply, and the information requirements set out in MiCAR will be the only ones applicable.

At present, withdrawal remains governed by consumer protection directives.

---

[15] For example, the first paragraph of Article 75 (Providing custody and administration of crypto-assets on behalf of clients) provides as follows:

"1. Crypto-asset service providers providing custody and administration of crypto-assets on behalf of clients shall conclude an agreement with their clients to specify their duties and their responsibilities. Such an agreement shall include at least the following:
(a) the identity of the parties to the agreement;
(b) the nature of the crypto-asset service provided and a description of that service;
(c) the custody policy;
(d) the means of communication between the crypto-asset service provider and the client, including the client's authentication system;
(e) a description of the security systems used by the crypto-asset service provider;
(f) the fees, costs and charges applied by the crypto-asset service provider;
(g) the applicable law."

Along with other scholars, I had hoped that the EU would take steps to coordinate the rules referred to when Directive (EU) 2023/2673 was adopted. That call was not heeded.

The aforementioned EBA Opinion calls for all financial activities to be governed by a single legislative act and, in particular, for this to apply to EMTs.

The difficulties in coordinating the various rules, which it has sought to highlight in this chapter, can only lead one to agree with the EBA's opinion, which suggests, among other things, taking advantage of the current process of overhauling Directive (EU) 2015/2366, which is expected to result in the adoption of a new regulation (PSR) and a new directive (PSD3).

Given the EBA's authority, it is to be hoped that, in this case, the EU will heed its advice.

References

AGID, *Regole tecniche. Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale*, 1° giugno 2023, in https://www.agid.gov.it/sites/agid/files/2024-07/regole_tecniche_e-procurement.pdf.

Annunziata, F., *An Overview of the Markets in Crypto-Assets Regulation (MiCAR)*, EBI Working Paper Series, 158, 2023, in SSRN: https://ssrn.com/abstract=4660379 or http://dx.doi.org/10.2139/ssrn.4660379.

Annunziata, F. e Sciarrone, A. (a cura di), *Cripto-attività. La disciplina europea nel contesto globale*, Bologna, Il Mulino, 2024.

Attanasio, C., *Inadempimento dello smart contract, sistema rimediale e tutela effettiva*, in *Rivista di diritto civile*, 4, 2024, pp. 719-743.

Bai, H., Cong, L.W., Luo, M. e Xie, P., *Adoption of Central Bank Digital Currencies: Initial Evidence from China (March 15, 2024)*, Finance, Economics & Banking (FEB-RN) Research Paper Series, 43, 2025, in SSRN: https://ssrn.com/abstract=5022129 or in http://dx.doi.org/10.2139/ssrn.5022129.

Banca d'Italia, *Perché un euro digitale?*, in https://www.bancaditalia.it/focus/euro-digitale/perche/index.html.

Bassan, F. e Rabitti, M., *Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai «contracts on chain»*, in *Rivista di diritto bancario*, 2023, pp. 561-639.

Capaccioli, S., *Smart contracts: traiettoria di un'utopia divenuta attuabile*, in *Ciberspazio e diritto*, 1-2, 2016, pp. 25-45.

Carriero, G., *Euro digitale e tutela dell'utente*, in S. Ruperto (a cura di), *Studi per Cesare Ruperto nel centesimo genetliaco*, Milano, Lefebvre Giuffrè, 2025, pp. 173-177.

Chamber of Digital Commerce, *«Smart Contracts» Legal Primer. Why Smart Contracts Are Valid under Existing Law and Do Not Require Additional Authorization to Be Enforceable*, gennaio 2018, in https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf.

Cian, M., *La nozione di criptoattività nella prospettiva del MiCAR. Dallo strumento finanziario al token e ritorno*, in G. Gitti e M. Maugeri (a cura di), *La nuova disciplina*

europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale, numero speciale di *ODCC*, 2022, pp. 59-78.

Cian, M. e Sandei, C., *Le cripto-attività: spunti per un inquadramento concettuale e disciplinare*, in F. Annunziata e A. -Sciarrone (a cura di), *Cripto-attività. La disciplina europea nel contesto globale*, Bologna, Il Mulino, 2024, pp. 227 ss.

CONSOB, *Le offerte iniziali e gli scambi di cripto-attività. Rapporto finale*, gennaio 2020, in http://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1.

– *Le criptovalute*, in https://www.consob.it/web/investor-education/criptovalute.

Cuccuru, P., *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *NGCC*, 59, 2017, pp. 107-119.

Cutts, T., *Smart Contracts and Consumers (March 18, 2019)*, LSE Legal Studies Working Paper, 1, 2019, in SSRN: https://ssrn.com/abstract=3354272.

D'Adda, A., *Smart contract e diritto generale dei contratti*, in G. Gitti e M. Maugeri (a cura di), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, in *ODCC*, numero speciale, 2022, pp. 105-118.

De Bonis, R. e Vangelisti, M.I., *Moneta. Dai buoi di Omero ai Bitcoin*, Bologna, Il Mulino, 2019.

de Caria, R., *Defining Smart Contracts: The Search for Workable Legal Categories*, in N. Aggarwal, H. Eidenmüller, L. Enriquez, J. Payne e K. van Zwieten (a cura di), *Autonomous System and the Law*, München, C.H. Beck/Nomos, 2019, pp. 27-33.

Di Sabato, D., *Gli Smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, 2, 2017, pp. 378-402.

DiMatteo, L.A. e Jang, J., *Blockchain-Based Financial Services and Virtual Currencies: United States*, in *EuCML*, 8, 2019, pp. 251-256, in SSRN: https://ssrn.com/abstract=3656577 or http://dx.doi.org/10.2139/ssrn.3656577.

Doria, M. (coordinatore), Bassan, F., Rabitti, M., Sciarrone Alibrandi, A. e Malvagna, U., *Caratteristiche degli smart contracts*, Quaderno di Banca d'Italia n. 863, 2024.

EBA, EIOPA ed ESMA, *Le cripto-attività spiegate: che cosa significa il regolamento MiCA per te come consumatore*, 2025, in https://www.consob.it/documents/d/asset-library-1912910/esas_factshee_cripto_20251006.

ELI, *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*, 2023, in https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf.

Ethereum, *A Next-Generation Smart Contract and Decentralized Application Platform (Ethereum Whitepaper)*, 2014, in https://courses.cs.duke.edu/spring23/compsci512/papers/ethereum.pdf.

– *A Secure Decentralised Generalised Transaction Ledger (Ethereum Yellowpaper)*, 2025, in https://ethereum.github.io/yellowpaper/paper.pdf.

EU Blockchain Observatory and Forum, *Legal and Regulatory -Framework of Blockchains and Smart Contracts*, 2020, in https://agi.agroapps.gr/wp-content/uploads/2020/04/Legal-and-regulatory-framework-of-blockchains--and-smart-contracts.pdf.

– *Smart Contracts*, 2022, in https://blockchain-observatory.ec.europa.eu/document/download/53a0aeb4-d144-4054-841e-dc169b44f94d_en?filename=SmartContractsReport_Final.pdf.

European Commission, *Study on Blockchains. Legal, Governance and Interoperability Aspects*, Luxembourg, Publications Office of the European Union, 2020, in https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038.

Financial Stability Board, *The Financial Stability Risks of Decentralised Finance*, 2023, in https://www.fsb.org/uploads/P160223.pdf.

Gaggero, N.A., *Liability for Wrongful Interference with Crypto-assets. Their Proprietary Status and Its Practical Implications*, in *ODCC*, 1, 2025, pp. 265-292.

Genovese, A., *Regolazione finanziaria e consumeristica in tema di offerta di servizi finanziari e di investimento*, in *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza*, Milano, Giuffrè Francis Lefebvre, 2019, pp. 355-368.

Giaccaglia, M., *Considerazioni su Blockchain e smart contracts (oltre le criptovalute)*, in *Contratto e impresa*, 3, 2019, pp. 941-970.

Janssen, A.U. e Patti, F.P., *Demistificare gli smart contracts*, in *ODCC*, 1, 2020, pp. 31-50.

Kaulartz, M. e Heckmann, J., *Smart Contracts – Anwendung der Blockchain-Technologie*, in *Computer und Recht*, 9, 2016, pp. 618-624.

Kaulbach, A.-M., *Private Rechtsdurchsetzung durch Smart Contracts*, in *Juristen Zeitung*, 80, 9, 2025, pp. 382-388.

Kerrigan, C., *Crypto and Digital Assets Law and Regulation*, London, Sweet & Maxwell, 2024.

Lehmann, M., *MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?*, in *Common Market Law Review*, 61, 3, 2024, pp. 699-726.

– *Crypto Economy and International Law. Determining the Regulatory and Private Law Rules Governing the Blockchain*, Leiden, Brill Nijhoff, 2025.

Lentini, L., *Conferimenti di criptovalute e società di capitali*, in L. Calcagno, A. Ciriello, M. Maugeri e G. Finocchiaro (a cura di), *Rapporti patrimoniali e nuove tecnologie*, Roma, Istituto Poligrafico e Zecca dello Stato, 2024, pp. 63-74.

Lessig, L., *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999.

– *Code. Version 2.0*, 2006 in http://codev2.cc/download+ remix/Lessig-Codev2.pdf.

Lupini, D. e Kerrigan, C., *Smart Contracts*, in C. Kerrigan, *Crypto and Digital Assets Law and Regulation*, Toronto, Thomson Reuters, 2024, cap. 6.

Manente, M., *L. 12/2019 – Smart Contract e tecnologie basate su registri distribuiti – Prime note*, Consiglio Nazionale del Notariato, approvato dalla Commissione informatica il 4 aprile 2019, in https://www.notariato.it/sites/default/files/S-1-2019-DI.pdf.

Maugeri, M., *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, Bologna, Il Mulino, 2021.

– *Cripto-attività, proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore*, in *Contratto e impresa Europa*, 1, 2022, pp. 1-8, in https://www.contrattoeimpresaeuropa.eu/mercato-finanziario-cripto-attivita-proposta-di-regolamento-mica-markets-in-crypto-assets-e-tutela-del-consumatore/.

– *Proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore nella commercializzazione a distanza*, in G. Gitti e M. Maugeri (a cura di), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, in *ODCC*, numero speciale, 2022, pp. 229-248.

– *Viaggio in Cina: cashless andata e ritorno?*, dicembre 2024, in https://rivistailmulino.it/a/viaggio-in-cina-cashless-andata-e-ritorno.

– *La tutela dei consumatori nel mercato finanziario delle cripto-attività*, in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 1, 2025, pp. 1-16.

Maume, P., *Consumer Protection*, in P. Maume, L. Maute e M. Romberger, *The Law of Crypto Assets. A Handbook*, -München-New York-Oxford-Baden-Baden, Beck/Nomos/Hart, 2022, pp. 109 ss.

– *The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both*?, in *European Company and Financial Law Review*, 20, 2, 2023, pp. 243-275.

Meyer, O., *Stopping the Unstoppable: Termination and Unwinding of Smart Contracts*, in *EuCML*, 9, 1, 2020, pp. 17-24.

Modica, L., *La proposta di regolamento MiCA e la disciplina delle pratiche commerciali scorrette*, in G. Gitti e M. Maugeri (a cura di), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, in *ODCC*, numero speciale, 2022, pp. 295-314.

Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, in https://bitcoin.org/it/documento-bitcoin.

Nicotra, M., *L'Italia prova a normare gli smart contract, ecco come: pro e contro*, in https://www.agendadigitale.eu/documenti/litalia-prova-a-normare-gli-smart-contract-ecco-come-pro-e-contro/.

Pagliantini, S., *La proposta MiCAR e le clausole abusive: una prima lettura*, in G. Gitti e M. Maugeri (a cura di), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, in *ODCC*, numero speciale, 2022, pp. 333-350.

Panetta, F., *Considerazioni finali sul 2024*, in https://www.bancaditalia.it/pubblicazioni/interventi-governatore/integov2025/cf_2024.pdf.

Parola, L., *Blockchain e Smart Contract*, in https://associazioneaiden.it/images/downloads/Aiden_Blockchain_16_aprile_2019_AVV_Lorenzo_Parola.pdf.

Pasquino, V., *Smart Contracts: caratteristiche, vantaggi e problematiche*, in *Diritto e processo*, 2017, pp. 239-248.

Patti, F.P., *L'offerta al pubblico di cripto-attività nel titolo II del Regolamento MiCA*, in *Rivista di diritto civile*, 1, 2024, pp. 97-132.

Perugini, M.L., *Distributed Ledger Technologies e sistemi di Blockchain. Digital Currency, Smart Contract e altre applicazioni*, Milano, Key, 2018.

Pilkington, M., *Blockchain Technology: Principles and Applications (September 18, 2015)*, in F. Xavier Olleros e M. Zhegu (a cura di), *Research Handbook on Digital Transformations*, Cheltenham-Northampton (MA), Edward Elgar, 2016, pp. 225-253, in SSRN: https://ssrn.com/abstract=2662660.

Profeta, V., *Profili giuridici dell'e-money token (EMT)*, in Id. (a cura di), *Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento*, in «Quaderni di Ricerca giuridica», 103, Banca d'Italia, 2025, pp. 95-127.

Remotti, G., *Blockchain smart contract: primo inquadramento e prospettive d'indagine (commento all'art. 8 ter D.L. 14 dicembre 2018, n. 135)*, in *ODCC*, 1, 2020, pp. 189-228.

Rosa, B. e Larsen, C., *Smart Money. How Digital Currencies Will Win the New Cold War – and Why the West Needs to Act Now*, London, Bloomsbury, 2024.

Scotti, C., *Stablecoins in the Payment Ecosystem: Reflections on Responsible Innovation*, 18 settembre 2025, in https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2025/20250918-scotti/index.html.

Selvadurai, N., *Mitigating the Legal Challenges Associated with Blockchain Smart Contracts: The Potential of Hybrid On-Chain/Off-Chain Contracts*, in *Washington and Lee Law Review*, 80, 3, 2023, pp. 1163-1180.

Sirena, P., *La tutela del consumatore nella commercializzazione a distanza di cripto-attività*, in G. Gitti e M. Maugeri (a cura di), *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, in *ODCC*, numero speciale, 2022, pp. 315-332.

Szabo, N., *Formalizing and Securing Relationships on Public Networks*, in *First Monday*, 2, 9, 1997, in https://firstmonday.org/article/view/548/469.

– *The Idea of Smart Contracts*, in Id., *Papers and Concise Tutorials*, 6, 1997, in https://nakamotoinstitute.org/the-idea-of-smart-contracts/.

– *Secure Property Titles with Owner Authority*, 1998, in https://nakamotoinstitute.org/secure-property-titles/.

Tamborlini, E., *Smart contracts: dall'uso all'abuso il passo è breve*, in *Vita Notarile*, 3, 2023, pp. 937-940.

The 2018 Joint Economic Report, *Report of the Joint Economic Committee Congress of the United States*, Washington, U.S. Government Printing Office, 2018, in https://www.congress.gov/115/crpt/hrpt596/CRPT-115hrpt596.pdf.

Tomczak, T., *Crypto-assets and Crypto-assets' Subcategories under MiCA Regulation*, in *Capital Markets Law Journal*, 17, 3, 2022, pp. 365-382.

UK Law Commission, *Smart Legal Contracts. Advice to Government*, novembre 2021, in https://webarchive.nationalarchives.gov.uk/ukgwa/20250109110910mp_/https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2021/11/6.7776_LC_Smart_Legal_Contracts_2021_Final.pdf.