RISK MANAGEMENT MAGAZINE

Vol. 19, Issue 1
January – April 2024

EXCERPT

https://www.aifirm.it/rivista/progetto-editoriale/

A method for classifying blockchains and crypto-assets using 'switching circuits'

Carlo Gola, Guido Befani, Patrizio Fiorenza, Federica Laurino, Lorenzo Lesina

A method for classifying blockchains and crypto-assets using 'switching circuits'

Carlo Gola (Bank of Italy), Guido Befani (University of Trieste), Patrizio Fiorenza (Bank of Italy), Federica Laurino (Bank of Italy), Lorenzo Lesina (Bank of Italy) ([1])

Corresponding author: Carlo Gola (carlogola@hotmail.com)

Article submitted to double-blind peer review, received on 9th February 2024 and accepted on 5th April 2024

Abstract

The work provides a method for classifying blockchains and crypto-assets, facilitating their comparison for business and regulatory purposes. Blockchains - and more generally systems based on Distributed Ledger Technology (DLT) - adopt different technologic configurations, each distinguished by the activities performed, technical characteristics, and governance structures. Particular noteworthy is the difference between some DLTs, which integrate automated organizational procedures with traditional decision-making processes, and others that adopt entirely algorithmic governance. Equally complex is the task of identifying types of crypto-assets, also known as digital tokens, generated and transferred through this technology. The work outlines the primary characteristics of DLTs and crypto-assets, utilizing 'switching circuits' to visually represent or express them in a simple formula. The proposed methodology, applicable both in the EU and in the US, untangles a given DLT/crypto ecosystem and reassembles it through logic maps, facilitating the identification of the technologic, economic, and legal features and overcoming the risk of a rigid and easily outdated taxonomy. The ultimate purpose of the paper is to propose a working method capable of accommodating every possible configuration of DLT and digital token and their potential evolutions. Practical examples of regulatory application and two case studies (Ethereum and Polkadot) are provided.

JEL codes: E42, G21, K23, O33, L86, M15.

Keywords: blockchain, DLT (Distributed Ledger Technology), crypto-assets, decentralized finance (DeFi), banking and financial regulation.

1. Introduction

Distributed Ledger Technology (DLT) is a computer system that enables the functioning and use of shared electronic records by synchronized electronic devices (nodes) through the use of a consensus mechanism. Blockchains are a subset of DLTs, possessing two additional properties: (a) their ledger is structured in the form of transaction blocks (which constitute the elementary units for updating the ledger's state), and (b) the blocks are chained together through the use of specific cryptographic functions, allowing the ledger to be updated by adding new data without modifying previous blocks. In the following, the two terms will be used interchangeably, as commonly used.

Identifying the characteristics of decentralized finance (DeFi) systems, which encompass financial services built on decentralized technologies such as blockchains, poses a significant challenge ([2]). These include the degree of openness of the computer protocol to the public, the presence or absence of a governance structure predefined by the algorithm, the degree of interoperability with other blockchains, and the ability to support a wide range of activities efficiently, securely, and flexibly.

Equally complex is the precise identification of types of crypto-assets (also known as digital tokens) generated and transferred through this technology. They can be fungible, transferable, traded bilaterally or through a multilateral market, assignable to the holder through a random or deterministic process, and finally, possess rights or claims, or lack them.

The purpose of this work is to provide a tool for representing the technologic characteristics of a blockchain and its related crypto-assets. The use of logic circuits (or "switching circuits"), allows the description of blockchains, including various bodies or collective systems of management and operational control (developers, technical committees, executive committees, etc.), even in mixed configurations that are difficult to classify into traditional permissionless and permissioned categories ([3]). The work also facilitates the identification of various types of tokens and their possible hybrid forms from a legal perspective. This should support their classification within the regulatory systems of different jurisdictions, including Europe and the United States. We believe that the proposed methodology could facilitate the issuance of guidelines or technical standards, for example, in the EU, by the European Securities and Markets Authority (ESMA), following the provisions of the Regulation on Markets in Crypto-Assets (MiCA) and the Digital Operational Resilience Act (DORA).

The proposed methodology is multifactorial and fully flexible; it does not rely on a simple taxonomy, but takes into account various qualifying factors. In doing so, regulatory arbitrage risks arising from overly rigid or restrictive approaches, such as 'closed lists' of identification, should be reduced. Finally, the purpose of the work is not to analyze the risks of blockchain or crypto-assets, but rather to identify the variables that could be useful for discriminating and identifying differences that might be helpful for this purpose. Furthermore, this paper introduces the fundamental difference between *governance tokens* and *management (or administrative)*

[1] The views expressed are individual and do not bind the associated institutions. While this paper represents a collaborative effort by all authors, sections 5, 5.1, 5.2, and 5.3 are attributed to Guido Befani, whose contribution has been developed within the interdisciplinary reflections of the international research project: "Digitalización, Sostenibilidad y Derechosde los Ciudadanos/Consumidores en el Sector Financiero (PID2021-128447OB-I00), financiado porel MCIN/ AEI/ FEDER, UE." lead by the University of Valencia, under the scientific supervision of Professor Beatriz Belando Garìn. The paper was presented at the Artificial Intelligence in Banking and Capital Markets conference, hosted by the University of Rome 'La Sapienza' - Centre of the European Commission Faculty of Economics, Rome, on December 11th and 12th, 2023. The authors express their gratitude for the comments received during the event. Special thanks are extended to Prof. Silvio Micali, Parma Bains, Federico D'Antoni, Josh Miller, and Ricardo De Bonis and for their invaluable suggestions. The authors remain responsible for any potential errors or omissions.

[2] See, Auer et al., (2023); ESMA (2023).

[3] On these aspects, and more generally on the governance of blockchains, see (Gola, et al., 2023a).

tokens; the former confer rights (implicit or explicit) to the owner for the management of the DLT and potentially also associated cash flows; the latter only provide the authority to administer it in ordinary management. The paper emphasizes that only an integrated analysis incorporating technologic profiles, which are typically overlooked by regulators, can properly make this distinction.

The structure of the work is as follows: First, the main characteristics of blockchains are presented (paragraph 2). They are: consensus protocol, degree of decentralization, type of settlement; distinction between 'native' and 'non-native' tokens, irreversibility, blockchain upgradability, distinction between algorithmic (on-chain) and traditional (off-chain) governance, interoperability, traceability, transparency, privacy, notary functions, scalability, and finally, environmental efficiency. A logic map is then provided to identify various types of blockchains (paragraph 3): the above-mentioned characteristics are aggregated through a logic map along three sets of features: type of activities and functions performed; level of decentralization; type of governance, including the distinction between mechanisms for updating and managing the blockchain. After analyzing the blockchain, the paper moves on to crypto-assets (paragraph 4). In particular, after introducing the main characteristics of tokens (fungibility, transferability, negotiability), their functions are analyzed: purely speculative (s. 4.1), allocative and governance (s.4.2) and monetary (s.4.3). This section also discusses the peculiarities of 'stablecoins' and their criticalities. A legal analysis is then proposed (paragraph 5) aimed at capturing the approaches followed in various jurisdictions (mainly the EU and the USA) leading them to a coherent and compatible framework. In particular, after illustrating the definitions adopted in Europe by the MiCA regulation (s. 5.1), a broader framework is proposed (s.5.2), which includes aspects not addressed by MiCA and which links to the notion of 'financial instrument' adopted by MiFID II (based on a 'closed list' of instruments), with other European regulations (AML/CFT, Pilot Regime, PSD2, etc.). The same analysis is done for the notion of 'public offering of financial investment,' particularly with reference to the USA legislation, mainly based on Howey's texts (s.5.3). The work then introduces a second logic map for digital tokens (paragraph 6), able to integrate in a granular yet coherent manner all the above-described elements. Finaly, a regulatory application (paragraph 7) illustrates the use of 'switching circuits' in a regulatory context, integrating the two maps (one for DLT and the other for digital tokens) into a single logic formula. After providing some final remarks, the methodology has been applied to case studies (Ethereum and Polkadot) (Annex).

2. Main Characteristics of a Blockchain

A blockchain is characterized by the following aspects: a high degree of decentralization (the raison d'être of this technology); efficiency (technologic, economic, and environmental); system robustness (reliability, integrity, and resilience to external attacks through the use of cryptographic techniques). There are various trade-offs among these three sets of features. In particular, a very high degree of decentralization is often less efficient, while a reduction in the degree of decentralization is often associated with lower system robustness. These configurations reflect the needs and functionalities that the system must support. Before moving on to the description of the logic map capable of representing such configurations, it is useful to provide some information about the technical characteristics of blockchains ([4]).

First and foremost, it is important to consider three aspects:

i) Type of activities carried out by DLT. Some examples include the setting up of a shared ledger, the ability to perform settlement activities (deterministic or probabilistic), the ability to deploy smart contracts ([5]), the creation of tokens with specific characteristics, etc.

ii) Type of editing of the DLT algorithm: backward compatible v. non-backward compatible. As we will see below, in the first case, editing involves ordinary, purely administrative activities of the shared ledger, such as code corrections (bugs) or non-disruptive improvements without significant effects for participants. In the second case, it involves non-ordinary corrections with significant impacts, even economic ones, for users.

iii) Type of governance (on-chain or off-chain) and voting rights. In the case of entirely on-chain governance (or fully algorithmic), the computer protocol predefines decision-making methods, coordination of designated entities, incentive and delegation mechanisms. In the case of off-chain governance, decisions are made through traditional governance processes, taking into account the powers and voting rights of participating entities (nodes) or group of entities (a consortium or federated system). In reality, there is often a mix of on-chain and off-chain governance.

Below, we disentangle these elements and, through the use of a logic map (or switching circuit), reassemble them in a manner adaptable to any possible blockchain configuration. In this process, it is essential to simultaneously consider the technologic, economic and legal nature of DTLs and related tokens, as we will see later on.

Let's now examine the components of a DLT:

Consensus Protocol: Firstly, it is necessary to mention that in blockchain systems there is a close relationship between decentralization and mutual trust. In a centralized system, a reliable agent accepted by all participants is required to perform a shared function (for example, in finance, clearing and settlement functions by a central counterparty), while a decentralized open system requires an algorithm (called consensus protocol) capable of achieving the same result without relying on mutual trust among participants.

An architecture of this kind is a distributed system composed by nodes ([6]) that interact with each other according to specific properties and need to agree on the final state of a public ledger ([7]). Therefore, decentralization could be defined as the ability to build

[4] On blockchain technology (Yaga, et al., 2018), and its implications (Bains, P., 2022). On the crypto-assets ecosystem, see (BIS, 2023).
[5] *Smart contracts* are self-executing pieces of codes that fulfil the terms and conditions of a transaction in an automated manner.
[6] A *node* refers to a device or a computer application that is part of a network and holds a partial (light node) or complete (full node) copy of the records of all operations executed through the distributed ledger. Nodes are anonymous or pseudonymous (identifiable through specific investigations on the IP address), numerous, and often equal.
[7] The *consensus protocol* of a blockchain is a set of mathematical and cryptographic rules aimed at ensuring agreement among a sufficient number of nodes on the "state" of the system (e.g., the state of updating a ledger of economic transactions).

a state of mutual trust among parties who do not know each other without resorting to a trusted third party. In circumstances where it is not possible or desirable to identify one or more actors who can act as trusted third parties to manage the system on behalf of participants, blockchain architectures offer a valid solution.

In the field of computer science, since the 1980s, the challenge of achieving consensus among different actors has been framed as determining how to reach a "state" of synchronization (a "consensus") among a discrete number of autonomous systems (nodes) with a certain degree of tolerance. The objective was to establish under which conditions the system could operate correctly even in the presence of a certain number of nodes exhibiting anomalous behaviours (malfunctioning or resulting from malicious activities). It has been demonstrated that there are critical tolerance thresholds (for example, 2/3 of nodes operating correctly at a given moment) above which the system continues to function correctly as a whole (Lamport, et al., 1982).

One of the innovations introduced by the Bitcoin blockchain, thanks to the consensus mechanism known as Proof-of-Work (or Nakamoto's protocol), was to show that it is possible to achieve – albeit probabilistically – a substantially similar result (i.e., consensus on a shared ledger) even in an open peer-to-peer system without requiring explicit communication among participants identified in advance ([8]). In DLTs adopting Proof-of-Work (PoW) consensus mechanisms, the consensus-reaching process is configured as a competition to solve a computationally expensive cryptographic problem; this corresponds to a high computational and, consequently, economic cost.

This computational cost discourages potential malicious participants to perform a so-called *sybil attack* ([9]). Notably, the cryptographic problem involved is deliberately designed to be difficult to solve but easy to verify. This characteristic ensures that while participants engage in a competitive race to find a solution, the verification of the correctness of the solution by all participants is a quick and straightforward process, contributing to the security and efficiency of the consensus mechanism. The goal of uncoordinated cooperation among nodes that are not pre-identified is, therefore, achieved through an economic incentive assigned to actively participating nodes in the process (the so-called *miners*), resulting in the creation of a non-duplicable message (a pre-defined number of native tokens, for example bitcoins) awarded to nodes winning the competition to solve the aforementioned cryptographic problem. The incentive system is based on the assumption that the token has an economic value connected to its scarcity, since the maximum number of producible tokens is predefined by the algorithm.

The algorithm is designed to "align incentives" among nodes (or group of nodes called *mining pool*[10]), meaning that it is more advantageous to behave correctly than to attempt to compromise the network's integrity. There is a wide variety of consensus protocols (in addition to Nakamoto's proof-of-work, there is proof-of-stake, delegated proof-of-stake, pure proof-stake, proof-of-authority, etc.) ([11]). Each uses different incentive mechanisms and "voting" methods. In particular, the *proof of stake* (PoS) model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it. Stake is often an amount of cryptocurrency that the blockchain network user has invested into the system (through various means, such as by locking it via a special transaction type, or by sending it to a specific address).

Permissionless, Permissioned, and Hybrid: There are different types of blockchains, classifiable into three broad categories: permissionless, permissioned, and hybrid. *Permissionless* blockchains are managed through a network where all participants (single nodes) may perform all relevant activities: reading, administrating (editing), and "governing" the distributed ledger. *Permissioned* blockchains require permission or authorization to perform the above-mentioned activities or subset of activities. *Hybrid* blockchains combine elements of both: in this case, only a subset of nodes has the power to perform the above- mentioned activities, or a subset of them (see Table 1). Blockchains are called *public* when access for performing some activities is not limited to authorized nodes, or *private* otherwise. As we will see extensively later on, access restrictions can be dictated by traditional (*off-chain*) or algorithmic (*on-chain*) governance rules.

Deterministic or Probabilistic Settlement System: The consensus mechanism of the protocol that regulates the creation and finalization of transactions can be deterministic or probabilistic. In a blockchain with a *probabilistic consensus* system, such as Bitcoin, once a block is propagated, it waits for confirmation. As more blocks are added to the chain, the probability of that block being changed decreases. In this way, the blockchain becomes more secure and reliable over time (usually a few minutes). In a blockchain with a *deterministic consensus* system, the transition is valid and final when a certain consensus threshold among identified nodes is reached (for example, two-thirds of properly functioning nodes at a given moment). Subsequently, each network node updates its ledger simultaneously, as in traditional payment systems.

Native and non-native tokens: In this work, we use the term crypto-assets (or *tokens*) to refer to any digital representation of value transferable through this technology. It is important to distinguish between native and non-native tokens.

Native tokens are generated by the blockchain, and are used to operate on it, for instance to pay transaction fees and transfer digital tokens. They are "intrinsic" to the underlying protocol and form an integral part of the system's functionality. These tokens allow for

[8] The term *peer-to-peer* refers to a distributed computer system in which all nodes perform the same functions on an equal footing. This system contrasts with client-server architectures, where some nodes take on the role of service providers (the servers), and others act as users (the clients). The latter model is the most common in the development of distributed computer applications, while the former is historically known for its use in platforms for data sharing and exchange.

[9] A *sybil attack* is a type of attack on a computer network service in which an attacker subverts the service's reputation system by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence.

[10] A *mining pool* is a collaborative group of cryptocurrency miners who combine their computational resources over a network in order to increase the chances of successfully mining a block and receiving rewards. When a block is successfully mined by any participant in the pool, the rewards are distributed among all the contributors based on their contributed computing power or the number of shares they have submitted. Joining a mining pool does involve relying on a central entity (the pool operator). These entities provide the infrastructure and coordination needed for miners to work together effectively. Some of the well-known mining pool operators include companies like F2Pool, Slush Pool, Antpool, and others, depending on the cryptocurrency being mined.

[11] For a description of the main consensus mechanisms, see: Yaga et al. (2028)

updating the blockchain and serve as a means of facilitating and securing transactions within the network. Examples of native tokens include BTC on the Bitcoin or ETH on the Ethereum ledger.

Non-native tokens operate as smart contracts atop the blockchain (as a second layer). These tokens adhere to a standardized set of rules, allowing for compatibility across various decentralized applications (DApps) within the ecosystem. On the Ethereum blockchain, the two primary token standards for non-native tokens are the Ethereum ERC-20 and ERC-721, which respectively define a common interface to create fungible tokens and non-fungible tokens (NFTs). Unlike native tokens, ERC-20 tokens are not directly integrated into the blockchain's core protocol but leverage the existing infrastructure for their functionality.

It's worth noticing that Bitcoin has also evolved to support simple smart contracts, allowing for more advanced functionality beyond its original use case. Despite these advancements, Ethereum stands out for its comprehensive smart contract capabilities, enabling the creation of intricate decentralized applications. Ethereum's ERC-20 tokens, for instance, showcase the platform's versatility by facilitating a wide array of use cases, giving them a broader utility value compared to Bitcoin's native token. While Bitcoin's pure token remains fundamental to its role as digital cash, Ethereum's ERC-20 tokens exemplify a more expansive and adaptable ecosystem within the blockchain space.

Table 1 – Role of nodes and type of activities

Bitcoin (1)	**Nodes: level of authorisation**	
Activities performed	Unrestricted access to all nodes	Limited access for authorized nodes
Reading	Yes	No
Administrating (2)	Yes	No
Governing (3)	n.a.	No

Ethereum (1)	**Nodes: level of authorisation**	
Activities performed	Unrestricted access to all nodes	Limited access for authorized nodes
Reading	Yes	No
Administrating (2)	Yes (1)	No (1)
Governing (3)	No	Yes

(1) = standard configuration
(2) = transactions validation or backward-compatible editing of the DLT (es. fixing a "bug")
(3) = non-backward-compatible editing of the DLT (es. change of the consensus mechanism)

Irreversibility of Transactions: This characteristic directly stems from the "append-only" nature of blockchains, i.e., the ability to update their state only by adding new information (new blocks) and never by deleting or modifying previously added information (blocks already part of the chain), unless a parallel blockchain is created through a fork. Since the only way to update the ledger is by adding new transactions, once a transaction is included, it becomes immutable. Immutability is a double-edged sword: on one hand, it makes it difficult to alter/falsify on-chain data, making public and permissionless ([12]) blockchains very interesting architectures for building systems resistant to external attacks; on the other hand, in the case of incorrect transactions (e.g., payments made to incorrect addresses), it is impossible to correct errors without the cooperation of third parties. Since a transaction cannot be deleted, the only way to nullify its effects is to create a new one that is equal and opposite. Permissioned blockchains, having the ability to coordinate a subset of authorized and therefore identifiable nodes, can more easily address this issue.

Blockchain Update and Hard Fork Risk: Like all software, blockchains require updates to add features, fix programming errors, and reduce vulnerabilities. These updates can be problematic in the absence of a centralized decision-making process. Two aspects need consideration: the types of improvements needed and what happens in case of disagreement among active nodes (*full nodes*).

Updating a blockchain involves modifying the software code (the main blockchain or native protocol) while preserving the history and integrity of the distributed ledger. There are various types of updates. Some are simple programming error fixes and are backward-compatible, while others are more significant changes, such as block size validation, validator fees, or structural changes to the consensus protocol.

In open-source systems, more radical change proposals with economic implications for participants can lead to divergent views. In permissionless blockchain systems, if there is no agreement, a group of nodes may decide not to update the software. In this case, those opposed (often a minority) can continue to use the old standard, creating a "fork": if the new software is incompatible with the old one, a blockchain split occurs, a process called *hard forking*. Two networks are then created, each with its followers (nodes, end users) and its own token. The price of the new token reflects the market's preference for the two standards, rewarding the one considered more valid (a concrete example is the split of Bitcoin into Bitcoin Cash or Ethereum into Ethereum Classic). Notably, in some cases, a fork can be beneficial for the system, introducing innovations and improvements. Moreover, it can have positive effects on the price dynamics of the two new tokens, offering opportunities for value creation and diversification. Furthermore, during a hard

[12] In the case of private and permissioned blockchains, the presence of one or more platform-managing nodes with a supervisory role – technical or business – makes it easier to manage these scenarios, intervening to remedy errors in some way.

fork, participants often acquire tokens from both the original and the forked blockchain. If the modification is backward-compatible, and only some nodes need to be updated, it is called a *soft fork*. In these cases, nodes that do not update the protocol can still participate in the network, although they may not have access to the new features introduced by the minor update. Soft forks do not create a blockchain split.

A *non-forkable* blockchain does not allow nodes to change the consensus rules of the network unless there is a procedure allowing the blockchain to be modified in predefined ways. For example, in the case of Polkadot, network nodes have the computational characteristic of being able to follow protocol rules without saving them on the node itself. The protocol rules are directly stored on the Polkadot blockchain, which can only be updated through on-chain voting, and then read by various nodes that can only execute the rules. If blockchain variations are backward-compatible, the likelihood of a hard fork is much lower.

*Non-vulnerability to "accidental forks"***:** This event occurs when there is a temporary divergence in the blockchain's transaction history due to conflicting blocks being added to the chain by different nodes or miners. This can happen due to network latency. During such forks, the principle that every asset has a single owner could be violated; it is, therefore, fundamentally important in finance. Indeed, one of the major concerns during a fork is the potential for double spending; if different branches of the fork accept conflicting transactions, it may be possible for a user to spend the same cryptocurrency units twice, exploiting the inconsistency in the network. Algorand is among the few blockchains designed to prevent "accidental forks", while remaining in a permissionless setting.

On-chain (algorithmic) and Off-chain (traditional) governance: *On-chain governance* processes are defined as a set of rules related to the governance of the blockchain written in the native protocol. These complete algorithmic governance processes can change the protocol rules according to predetermined forms and methods. In this context, rules related to voting mechanisms, block or transaction sizes, and interface methods (API/RPC) could, for example, be decided and directly inscribed in the protocol. The decision-making process is predefined and immutable. Decisions proposed, for example, by developers operating on the network, are made through referendums according to procedures established by the computerized process. There may be supervisory bodies, committees, aggregation groups, but such bodies do not have power over the final decision (see the Polkadot case in the Annex).

Off-chain governance processes are not directly written into the native blockchain protocol but interact with it after performing organizational or decision-making functions outside of it. As in the previous case, there may be technical committees or bodies, but decisions take place off-chain, as in a traditional organizational structure. Understanding these decision-making processes, power and responsibility allocations, delegation mechanisms, etc., is crucial. Indeed, at the off-chain level, opacity, fragility, distortions (including excessive concentration of power) can occur, as the operational mode does not guarantee the transparency levels of on-chain automated processes. On the other hand, off-chain processes have the advantage of being able to rely on traditional corporate governance safeguards, including the allocation of responsibilities and accountability (see the Ethereum case in the Annex).

Interoperability: In addition to aspects internal to the structure of a given blockchain (degree of openness to participants, management and control methods of the protocol, security, etc.), an efficient ecosystem must have technologic characteristics that allow different blockchains to "communicate", interface, and be *interoperable*. Interoperability must involve both processes and data, including those from external systems (so-called oracles). This aspect is not only crucial to avoid fragmentation between systems that should interact efficiently but also to maintain high market contestability (access by potential entrants even in the presence of scale or network economies). When interoperability is not initially designed in the blockchain architecture, it is often achieved through smart contracts known as *bridges*. These bridges act as connectors between different blockchains, facilitating the exchange of information and assets, and enabling a more seamless interaction between disparate blockchain networks.

Traceability, transparency and privacy: These aspects refer to the property that on-chain recorded data (through the native protocol) must be accessible and verifiable, preserving, however, privacy. Transparency is essential to support trust in the security of the system: each node is autonomously capable of inspecting and verifying the validity of blocks and transactions, without the need to rely on a third party to do so. This means that any transaction on a public blockchain can be inspected for forensic purposes by analysing the information stored on the shared ledger (see below). On the other hand, this also implies that to preserve privacy on a public blockchain, additional techniques are necessary ([13]). Moreover, as the size of the blockchain grows, it becomes more burdensome for a node to download the entire history of the system. Only nodes with expensive and dedicated hardware and software devices (called full nodes) have the capacity to verify the truthfulness of all transactions.

Identification of the End User and Nodes - The identifiability of both the end user (e.g., one who purchases a crypto-asset) and those validating transactions is an aspect with clear implications for combating illicit activities. In the presence of a permissioned blockchain and/or a centralized entity like a crypto-asset service provider (e.g., an exchange or a wallet provider), it is possible to identify users. It is different when operating through a peer-to-peer permissionless blockchain or an *unhosted wallet*. In this case, the only publicly available information is the wallet address (a string of numbers and letters), and only through market intelligence or police investigations is it possible to attempt to identify the owner of the crypto-assets. There are also algorithmic systems (so-called mixers or tumblers) that make it complex to associate the wallet with its owner or crypto-assets (such as Monero), where it is not possible to link two transactions or determine the source or destination of funds (not even as a public address).

Certification Function: A crucial aspect concerns the potential ability to provide "legal certainty" to the information recorded in various transactions (so-called notarization). This issue is particularly complex, especially in light of the effects of European provisions that introduce a legal framework for secure electronic identification, the recognition of electronic signatures, and related trust services within the EU (the eIDAS Regulation - Electronic Identification Authentication and Trust Services, EU Regulation No. 910/1014).

In particular, Article 41 of the regulation grants the following legal effects to blockchain records:

[13] There are companies dedicated to this sector, known as "blockchain forensics," with the most notable being probably Chainanalysis (www.chainanalysis.com). Achieving strong privacy goals, however, requires the adoption of specific techniques, also known as Privacy Enhancing Techniques (PETs); for a detailed description of these techniques focused on digital payments, see (ECB, Bank of Japan, 2020).

1. The legal effects and admissibility as evidence in legal proceedings cannot be denied to electronic time-stamping solely because of its electronic form or because it does not meet the requirements of qualified electronic time-stamping.
2. Qualified electronic time-stamping enjoys the presumption of accuracy of the date and time it indicates and the integrity of the data to which that date and time are associated.
3. Qualified electronic time-stamping issued in one Member State is recognized as qualified electronic time-stamping in all Member States.

In this sense, notwithstanding other legal challenges ([14]), the issue of guaranteeing the trustworthiness and authenticity of the substance of the data transcribed on the blockchain remains legally unresolved. The legal effects apply primarily to the "registry" container and not to the "registered" content ([15]).

Scalability: Another crucial aspect that has led to the development of complex blockchain configurations is *scalability*. This is defined as the system's ability to process a high number of transactions per unit of time and by numerous nodes ([16]). In this case, there is a trade-off, commonly referred to in the literature as the "blockchain trilemma," as it is challenging to have a blockchain that simultaneously achieves scalability, high decentralization, and security ([17]). Since scalability is a necessary characteristic for various practical uses of blockchains, especially in public and large-scale environments, different solutions have been proposed to address the problem. Broadly, these solutions can be grouped into two categories: (i) "on-chain" or Layer 1 solutions (where Layer 1 is the ledger itself), involving modifications to the blockchain by upgrading the underlying ledger – for example, supporting larger block sizes or different consensus algorithms than the original; (ii) "off-chain" solutions, involving the addition of layers on top of the base ledger – for example, solutions based on Layer-2 networks or those involving the creation of side-chains ([18]).

Environmental Efficiency: Another aspect concerns the poor energy efficiency of blockchains based on the proof-of-work (PoW) consensus mechanism. The issue is well-known, and it is not necessary to delve into it here ([19]). The crucial point is that the transition to more efficient and environmentally friendly technologic systems (e.g., based on *proof-of-stake* or *proof-of-authority*) requires a governance system capable of managing this transition. Alternatively, off-chain processes must be used, which, in turn, need to be managed and monitored.

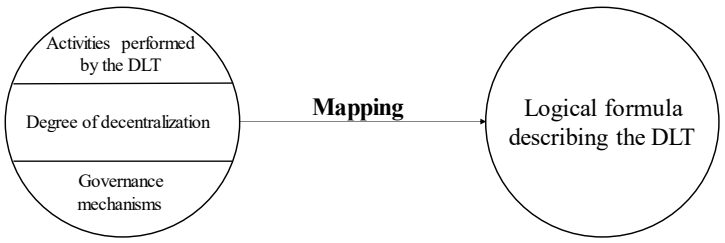
3. Logic Map for Classifying Blockchains

We have observed that blockchains can possess highly diverse technical features to address various scalability, efficiency, security, and immutability requirements of the shared ledger. We've referred to three major classes, permissionless, permissioned, and hybrid: this last class reflecting a broad spectrum of configurations where certain nodes, users or administrators, have restricted or special roles. There are also blockchains with various decision-making and control bodies (which can operate on-chain or off-chain). How these powers are allocated, what the decision-making rules are, and to what extent some nodes are accountable for their actions are crucial aspects of a clear and well-designed governance structure. The type of activity the blockchain must perform, either directly or through parallel protocols, and the degree of decentralization are relevant considerations. To achieve this, it is necessary to clearly identify various types of blockchains, taking into account different technical, economic, and governance characteristics.

3.1 Various Types of Blockchains and Their Governance Structure

Below, a logic framework inspired by logic circuits is provided, capable of stylizing different possible blockchain configurations and their governance structures. This can be accomplished through a function that, taking as input a series of configurations (related to the activities performed, the degree of decentralization, and governance mechanisms), provides, as output, a logic formula capable of describing that specific blockchain (see Figure 1).

Figure 1 – Logic Scheme for Mapping Blockchains



[14] As highlighted by Consideration No. 5 of EU Regulation 2022/858 of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (DLT Pilot regime), "... there are regulatory gaps due to legal, technologic, and operational specificities related to the use of distributed ledger technology and crypto-assets falling within the definition of financial instruments. For example, no transparency, reliability, or security requirements have been imposed on protocols and 'smart contracts,' which underlie crypto-assets falling within the definition of financial instruments. The underlying technology could also pose new forms of risks that are not adequately addressed by existing regulations."
[15] On this aspect, (Befani, 2021).
[16] For a literature review, see (Hafid, 2020).
[17] For a discussion of the blockchain trilemma and a possible solution, see (Micali 2019).
[18] By off-chain solution, it is meant a system that supplements the native blockchain (typically permissionless) with other blockchains (usually permissioned and sometimes private) that connect to the first layer after performing different functions, (Schär, 2021; BIS, 2023).
[19] For a discussion on these aspects, see (Gola, Sedlmeir, 2022)

The *first part* involves a traditional mapping of the activities carried out by a particular blockchain, indicated by {Ai} (see Table 2). In principle, each activity is associated with specific risks, manageable through a set of self-governance rules, both internal and external, that should be adhered to in order to monitor and mitigate the risks associated with the proper functioning of the blockchain.

Table 2 - List of Possible Activities Performed by the Blockchain

A0: Creation of a shared and readable ledger (e.g., for supervisory purposes)
A1: Creation of native or non-native tokens
A2: Implementation of smart contracts and atomic swaps ([20])
A3: Interface with other systems (interoperability)
A4: Non-vulnerability to "accidental forks"
A5: Deterministic v probabilistic settlement
A6: Certification or notarial activity
A7: Identifiability of the end user and respect of privacy
A8: The transaction complies with AML/CFT criteria
An: Other activities

The *second part* addresses the degree of decentralization in blockchains. Simplistically, three configurations can be identified: *permissioned*, where usually there is a subject or node with a leadership role, and only authorized entities have access to data in reading (e.g. Hyperledger Fabric, R3 Corda); *hybrid*, for instance in the case of a polycentric system where only a limited number of nodes have special functions, but where any entity has access to data in reading (e.g. ICON, Dragonchain, and, to some extent, Ethereum); *permissionless*, which in general corresponds to a decentralized system characterized by a high number of nodes operating in the network without entry and exit constraints and in a generally equitable manner (e.g. Bitcoin).

The *third part* of the map represents the governance mechanisms of the blockchain, denoted as {Ri}. Blockchains can indeed have a variety of governance and control mechanisms, including enabled groups of validators, technical committees, as well as open-source protocol developers interacting through more or less decentralized methods (e.g., a referendum). Governance mechanisms can be, as specified earlier, both on-chain and off-chain. Clearly, a "robust" blockchain (whose robustness level is calibrated based on the activities it needs to support) must simultaneously have good governance and effective risk management.

What has been said is represented in Figure 2. The map functions like a switching or logic circuit (note the 'switches'_ _) ([21]). The circuit is traversed from left to right, starting with the relevant DLT's information and concluding with the white paper (symbolized as WP), representing the illustrative document of the blockchain. Each blockchain operates by activating certain functions or 'activities' {Ai} (see Table 2 for a full list), as shown in the first part of the circuit; its configuration (degree of decentralization of nodes and consensus mechanism) is represented in the second part of the map; finally, the third part of the circuit concerns the set of internal processes and rules {Ri}. The entire circuit closes if and only if the circuits at the top, in the middle, and at the bottom of the map close simultaneously.

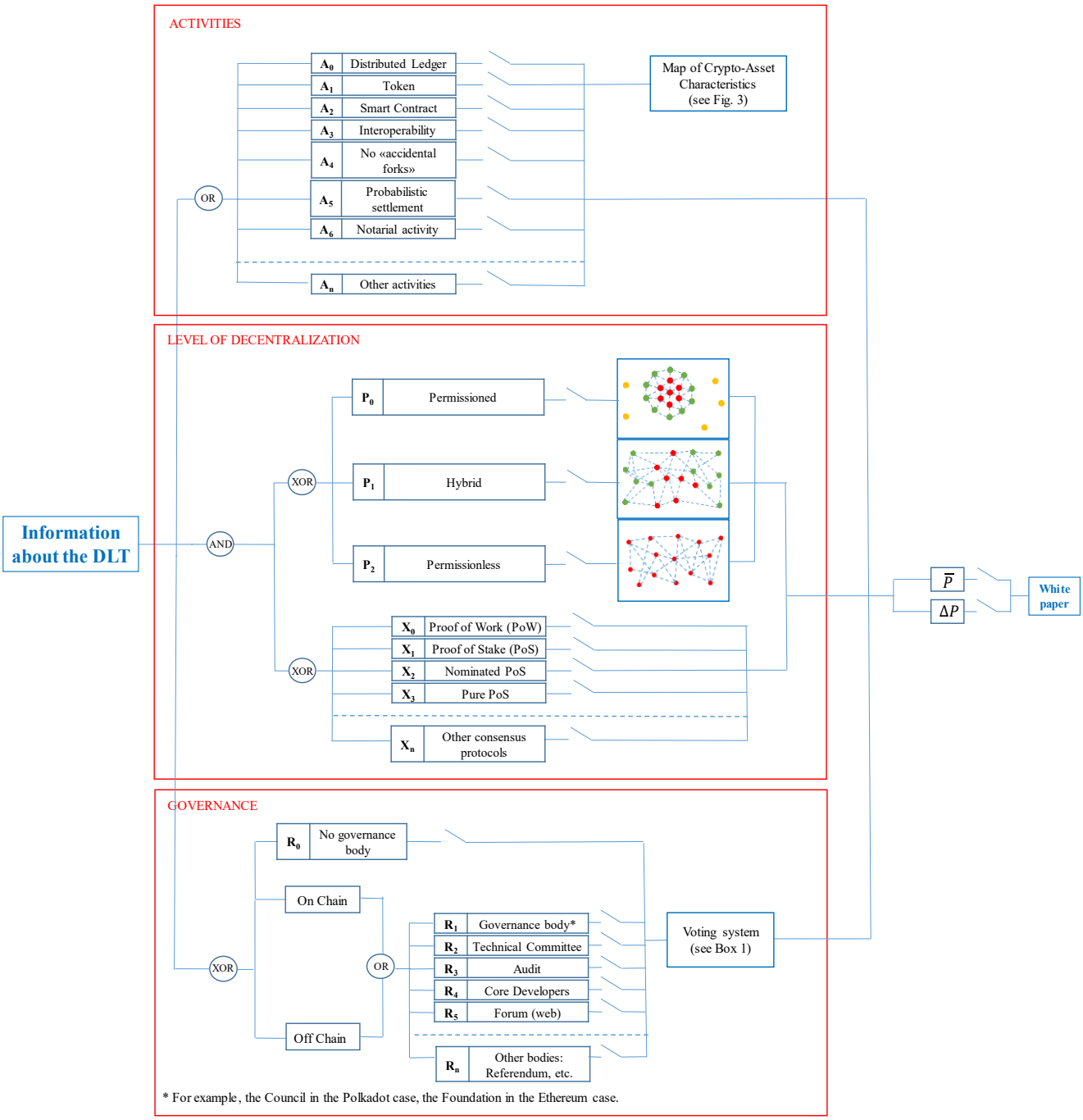
This logic map provides a structured approach to understanding and categorizing different blockchain configurations, considering their activities, decentralization levels, and governance mechanisms. Each blockchain, with its unique combination of these elements, fits into a specific category, allowing for clearer comparisons and assessments based on their intended use cases and design principles. For example, in a simplified manner, let's see how the map represents the Bitcoin blockchain. In the top part of the circuit, it activates three functionalities: creating a distributed cryptographic ledger (activity A0), generating the Bitcoin token (activity A1), and probabilistically finalizing transaction blocks (activity A5). In the middle part of the circuit, the switches corresponding to a permissionless public blockchain (P2) with a PoW-based consensus mechanism (X0) are closed. The circuit does not involve any governance body (R0). Given its characteristics, Bitcoin is not predisposed to handle an orderly and predefined upgrading process, so it may be subject to forks ($\bar{P}$). The Bitcoin blockchain can be represented by the following formula: (A0∧A1∧A5) ∧ (P2∧X0) ∧ R0∧$\bar{P}$.

Blockchains with more complex functionalities will activate other paths with more articulated governance structures. The map shows, for illustrative purposes, two complex blockchains, Ethereum and Polkadot (described in the Annex). Also, among the requirements imposed by the regulator, there might be the need for changing the native protocol. In this case, the circuit closes only in the presence of a consensus protocol predisposed for this purpose or capable of achieving the same result during the blockchain's lifecycle, through a recursive or adaptive process ([22]).

This property requires the presence of a consensus protocol and specific governance mechanisms. The recent 'migration' of Ethereum from PoW to PoS shows that changing the native protocol is possible. This property necessitates the existence of a consensus protocol and specific governance mechanisms. Sush 'migration' demonstrates that altering the native protocol is achievable, although this process is highly complex, as the blockchain is not upgradeable (symbol ($\bar{P}$), see Figure 2)) and, therefore, is subject to forking. The suggested approach is very flexible and should be able to 'map' every type of blockchain, adapting the map appropriately to capture, even in detail, all possible configurations of blockchains. In fact, this methodology can be used to include subsets of logic circuits having other activities or functions.

[20] Atomic swaps are smart-contract protocols based on sequences of transactions executed on multiple DLTs that allow counterparts to coordinate on the exchange of native tokens in a trustless environment and without intermediaries.
[21] A *logic* circuit is based on two-positions switches (on-off), serving as a logic representation of a necessary and sufficient condition for a specific state to be true. See Chapter 8 of (Mendelson, 1970).
[22] On this aspect, see (Gola, 2023a), paragraph 4.3.

Figure 2 – A logic map for classifying blockchains



Examples

$Bitcoin \rightarrow (A_0 \wedge A_1 \wedge A_5) \wedge (P_2 \wedge X_0) \wedge (R_0) \wedge \bar{P}$

$Ethereum \rightarrow (A_0 \wedge A_1 \wedge A_2 \wedge A_5) \wedge (P_2 \wedge X_1) \wedge (R_1 \wedge R_4 \wedge R_5)_{OffChain} \wedge \Delta P$

$Polkadot \rightarrow (A_0 \wedge A_1 \wedge A_3 \wedge A_n) \wedge (P_2 \wedge X_2) \wedge (R_1 \wedge R_2 \wedge R_n)_{OnChain} \wedge \Delta P$

$Algorand \rightarrow (A_0 \wedge A_1 \wedge A_2 \wedge A_3 \wedge A_4 \wedge A_5 \wedge A_6) \wedge (P_2 \wedge X_3) \wedge (R_1 \wedge R_2 \wedge R_3 \wedge R_4 \wedge R_5)_{off\ Chain} \wedge \Delta P$

Legend

$\{A_i\} = list\ of\ possible\ activities$
$\{R_i\} = corporate\ governance$
$\{X_i\} = consensus\ protocol$
$\bar{P} = not\ upgradable \rightarrow Forkable\ protocol$
$\Delta P = upgradable \rightarrow not\ Forkable\ protocol$
$AND\ (in\ symbols \wedge) = logical\ conjunction$
$XOR = exclusvie\ OR$
$OR\ (in\ symbols \vee) = logical\ disjunction$

3.2 Token Allocation for Updating and Managing the Blockchain

The logic map can be furtherly expanded to classify voting mechanisms and token allocation. Indeed, tokens (see paragraph 4) can be allocated through various methods, including random selection, and can confer different types of voting rights. Classifying this aspect can facilitate regulatory framing of tokens and the underlying IT infrastructure.

In particular, a blockchain can be designed for the allocation of tokens with voting rights to nodes participating in its management. The allocation of tokens serves both for the regular functioning of the blockchain (e.g., transaction validation and updating the shared ledger) and for carrying out *extraordinary* activities (e.g., changing the technical parameters of the native protocol or even the

consensus system). Only for this specific purpose, governance tokens (or voting right tokens) have been introduced in some blockchains.

The logic underlying some blockchain voting systems is to *limit concentration*, not only during the project launch phase but also over time, and to strengthen incentives—either through a reward or through a participatory mechanism (*skin-in-the-game*). This is done through various means, such as the random allocation of participation rights in the initiative through voting (randomization). In fact, an excessive concentration of voting rights not only has obvious governance implications but also has a negative effect on the security of the system through Sybil attacks. Another problem is the presence of a high number of voting rights holders who do not vote in decisions related to managing protocol changes. They are the equivalent of absentee or passive shareholders in capital companies. Mechanisms of *temporary delegation* assigned through random processes have been developed. It is also necessary to maintain the involvement of the entity participating in the system over time. This is done through *staking* (collaterals), rewards in the form of tokens that act as an incentive to provide intellectual or economic contributions, 'loyalty rewards,' and penalties for improper behaviour. Box 1 lists some possible token allocation systems (not necessarily mutually exclusive).

Box 1 – Voting Mechanisms and Token Allocation

V1: "One or more tokens based on computing power (CPU)": the decision-making power is linked to the possession of hardware with high computational power; this principle forms the basis of the PoW algorithm (mining). It does not provide any specific power to manage the blockchain, but only to validate transactions.

V2: "One token, one vote": the decision-making power is linked to the number of tokens owned and placed in deposit ('*staking*') In some systems, the vote can be repeated (multi-round voting) or "timed" (coin aging).

V3: "One head, one vote": all participants have the right to vote (only possible in permissioned DLT).

V4: "Two-stage lottery": random token – random committee ([23]).

V5: "Pure lottery": the right to vote is randomly distributed to a defined number of participants without constraints.

V6: "Lottery only for active nodes in management": like pure lottery, but the right can only be conferred to those actively involved in managing the blockchain (e.g., developers).

V7: "Lottery with delegation": the right to vote is randomly conferred to participants, who can in turn delegate a limited number of other nodes with specific skills. Over time, the delegate earns a reputation.

V8: Other voting mechanisms.

4. Economic and Financial Characteristics of Crypto-Assets

We have previously analysed the technologic and functional characteristics of blockchains and the implications arising from different configurations. A second aspect concerns the various types of crypto-assets that a blockchain can generate or transfer.

There are various ways to describe the characteristics of crypto-assets ([24]). A first method concerns the prevalent economic function: monetary function, medium of exchange, allocative function (through, for example, financial instruments). Relevant in this context are the characteristics of fungibility, transferability, negotiability on an organized market.

A second method pertains to the legal characteristic of tokens: the ability to represent values, incorporate rights, performances, promises, or contractual constraints. In this paragraph, we will address the first of these aspects, while in paragraph 5, we will provide a legal foundation to analyse the second. This will be done considering both the legal approach of the United States and that adopted in Europe. Later (paragraph 6), we will provide a logic framework that allows for the integrated representation of the technologic, economic, and legal aspects considered.

Before delving into the topic, it may be helpful to recall some definitions subsequently used ([25]):

Fungibility: An asset is fungible if it is interchangeable with other similar assets; it is homogeneous and divisible into smaller units of account. Money is a typical fungible asset. Commodities (gold, oil, soy, etc.) are also fungible, having homogeneous characteristics according to very precise standards; this makes them suitable for trading on organized markets.

Transferability: The ownership (property) of an asset is transferable through the blockchain without resorting to a third-party trustee. In some cases, however, the blockchain makes the token non-transferable ("locks" it) for a certain period, for example, to strengthen the user's incentive to participate in a particular blockchain. The token is transferable peer-to-peer (from one electronic wallet to another).

Negotiability: Negotiability refers to the legal ownership of the instrument that can be easily transferred from one owner to another through delivery or endorsement. Although any financial instrument can potentially be negotiated, only a security programmed to be traded on an organized or over-the-counter (OTC) market is "negotiable". The OTC market involves only the parties trading the security directly, while a security traded on an organized and regulated exchange has a price formation through a multilateral and transparent process.

[23] So called "Pure Proof-of-Stake" used by Algorand. It is a two-phase process: in the first phase, a single token is randomly selected, and its owner is the user who proposes the next block; in the second phase, a given (1000) number of tokens are selected among all tokens currently in the system; the owners of such tokens are selected to be part of a 'committee' which approves the block proposed by the first user. Therefore, to belong to the committee, one of the coins owned the active node must win a cryptographically fair lottery. See Micali (2019).
[24] See (Gola, C., Caponera, A. 2019).
[25] See (IMF-BIS-ECB, 2015).

As indicated by the IMF Handbook: "The criteria for a financial instrument to be considered negotiable are: (1) the ability to be transferred to another person's legal ownership (or offset in the case of financial derivatives); (2) standardization (often evidenced by fungibility) and an eligible International Securities Identification Number (ISIN); and (3) no right of recourse against previous holders of the relevant asset" (IMF-BIS-ECB, 2015).

Crypto-assets are often fungible, transferable, and in most cases, negotiable as well. Some tokens are transferable but not negotiable, as is the case with certain classes of shares that only provide the right to participate in an entrepreneurial initiative. The ownership of a single asset (such as real estate or a work of art) is transferable from one owner to another through an economic transaction or a notarial deed but is not directly negotiable; it is only negotiable when associated with a title representing ownership. This happens, for example, in real estate funds whose shares are negotiable on organized markets. A non-fungible token (NFT) representing, for example, a digital artwork is not directly negotiable; it can become negotiable only when associated with a smart contract that allows its fractionalization (i.e., the use by multiple parties of the same, as in the case of timeshares for real estate). Negotiability on a "frequent" and efficient market is crucial for the liquidity of the token (the ability to sell it at any time at a non-fire-sale price) ([26]).

4.1. Purely speculative function

"Pure tokens" *('unbacked crypto-assets")*: The first and most widespread class of crypto-assets is that introduced in 2008 by Nakamoto with the Bitcoin token. Its main characteristics are the non-duplicability of the token, its fixed producible quantity, and its transferability without resorting to a centralized third party. As we have seen, crypto-assets like Bitcoin (sometimes called *unbacked crypto-assets*) are created through a process called mining and serve (as 'gas') to operate the blockchain. They are not associated with ownership rights to other assets or financial instruments; they do not promise cash flows and do not provide administrative rights (as the utility tokens); their value is primarily determined by market expectations of their future price.

These digital tokens are fungible and can be transferred, stored, and exchanged electronically on a peer-to-peer level. As will be extensively discussed in paragraph 4.3, crypto-assets like Bitcoin are not legal tender ("fiat money"), "deposits", or other "funds". They are not a liability of an institution (bank or financial intermediary); nor are they a currency with intrinsic value like gold, which, due to this characteristic, was universally accepted as money in the past. None of the typical functions of money is fully satisfied by Bitcoin or similar "crypto-currencies". Above all, two fundamental elements are missing: a law guaranteeing its integrity and imposing generalized discharge power, often linked to acceptability as a means to pay taxes, and; it is not issued by a central trust authority that, by anchoring inflation expectations and regulating supply based on economic performance, promotes the stability of purchasing power. To date, Bitcoin is used to exchange goods and services only to a very marginal extent; its high price volatility, almost exclusively tied to market expectations, makes it unsuitable for this function. Instead, it is functional for speculative purposes or for transferring funds without going through traditional channels, often for illicit reasons.

4.2. Allocative and Governance functions

In this context, the allocative function can be realized in two ways: through the use of financial instruments or by allocating usage or administrative rights. The allocative function through other channels (such as credit or crowdfunding) is not discussed here as it is currently less developed.

Some crypto-assets exhibit characteristics of financial instruments or financial products. In various jurisdictions and international organizations' documents, there are different definitions of a "financial instrument" ([27]). However, the essential element is the presence of a contract that gives rise to a financial asset for one entity and a financial liability or an equity instrument for another entity. These instruments must also be fungible, transferable, and tradable bilaterally or through multilateral market infrastructures (regulated markets). They can be either a primary or derivative financial instrument, meaning their value is tied to the price of an underlying asset. Not considered financial instruments are means of payment, artworks, real estate, and commodities (including gold). However, contracts whose value is linked to the price of these individual goods or baskets of goods are financial instruments.

The following types of tokens can be distinguished.

Governance Tokens and Management Tokens: These tokens, created through a smart contract and assigned to 'active nodes' confer specific rights to the holder regarding the current or future management of the project (see Box 2). In our definition, *government tokens* (contrary to *management tokens*) may promise future cash flows related to the project's realization, similar to administrative and/or equity rights. Asymmetric information issues arise if governance tokens are linked to a platform where decisions are predominantly made 'off-chain', and/or the project's promoter is a third party compared to the investor.

Tokenized Financial Debt Instruments: These tokens, created through smart contracts, represent commitments such as bonds issued by companies or financial institutions. Holders of these tokens enjoy specific rights typical of the underlying instruments, such as the right to periodic payments or the repayment of the entire invested capital and accrued interest at a specified maturity date. Regulatory measures may be necessary to protect subscribers due to principal-agent information asymmetries inherent in such instruments. This situation also applies to "tokenized" shares of mutual funds or other financial products.

Non-Fungible Tokens (NFTs) and Utility Tokens: Some crypto-assets do not have financial characteristics as they are non-fungible. For example, they may represent rights to artworks or are artworks themselves. Only securitization would make them tradable and, as such, classifiable as 'tokenized financial instruments'. Other tokens provide access to the use of specific services,

[26] See (ISDA, 2022).

[27] See: IAS/IFRS Accounting Principles (especially IAS 32); prudential regulation CRR (art. 4(1) (50); MiFID2 market regulations (art. 4(1)). In the United States, under the Securities Act of 1933, the decision of the Supreme Court "SEC v. W.J. Howey Co." (328 U.S. 293 (1946)) applies. On these aspects, see paragraph 5.

such as gaming activities, the metaverse, issuance of coupons, or "local currencies" without general spendability. These tokens allow economic agents to access certain goods or services. Due to their legal nature, a more exhaustive analysis is provided in paragraph 5.

Box 2 – The difference between Governance and Management Tokens

Governance tokens play a crucial role in blockchain networks that employ decentralized governance models. These tokens provide holders with decision-making power over fundamental aspects of the blockchain. As such, they grant the owner rights (explicit or implicit) over any cash flows resulting from the good governance of the blockchain. *Management tokens*, on the other hand, are distributed in exchange for a service ("effort") provided by a miner, as a form of compensation. Finally. unlike purely speculative tokens, governance tokens confer the right to participate in the decision-making processes of the blockchain network and, unlike management they are not tied to the "ordinary" improvement of the blockchain or the simple updating of the shared ledger. They provide the holder not with compensation but rather a "lottery ticket" for the effort related to the mining process. Only an integrated analysis of the technologic, economic, and legal aspects can allow for understanding these difference.

The issuance and distribution of governance tokens are integral to the functioning of decentralized autonomous organizations (DAOs) and other blockchain ecosystems that prioritize decentralized governance. Holders of governance tokens often have voting rights, enabling them to influence protocol upgrades, parameter adjustments, or other key decisions. The concept aligns with the broader principle of stakeholder participation in the governance of blockchain networks.

The unique feature of governance tokens lies in their ability to represent influence rather than ownership or monetary value. They serve as a means for participants to express their preferences and steer the direction of the blockchain community. The mechanics of governance tokens vary across different blockchain projects, with some employing proportional voting mechanisms based on token holdings.

It is essential to note that governance tokens introduce a layer of complexity beyond the purely speculative nature of some crypto-assets. Their value is tied not only to market dynamics but also to the perceived effectiveness of the governance processes they enable. Successful governance, reflected in sound decision-making and community alignment, can enhance the value and credibility of governance tokens within the blockchain ecosystem. Conversely, governance failures or disputes may lead to fluctuations in token value and could impact the overall governance structure of the blockchain network.

In summary, while purely speculative tokens derive value, mainly from market expectations, governance tokens derive value also from their role in shaping the governance and decision-making processes of blockchain networks. Their significance extends beyond financial considerations, contributing to the evolving landscape of decentralized and community-driven governance in the blockchain space. This also differs from *management tokens* in that the latter only concern the non-extraordinary management of the DLT. The Bitcoin blockchain does not offer compensation in exchange for upgrading the protocol (e.g. fixing a bug), but only a reward ('lottery') for nodes participating in updating the shared ledger (see paragraph 3.2).

4.3 Monetary and payment function

Before delving into crypto-assets with characteristics of money, it is necessary to recall some relevant aspects of the monetary function. As known, for something to be considered money, it must simultaneously fulfil three functions: a unit of account (currency used as a metric for exchanges); a medium of exchange (a tool to avoid multiple barter transactions); and a non-corruptible and constant store of value, issued by a third-party trustee (the central bank) that regulates its supply based on the economic cycle. Money is a highly liquid and low financial risk instrument that enhances social welfare through the aforementioned functions. In modern monetary systems, there are two types of money: "public" central bank money, consisting of circulating ("cash") and reserves held by banks at the central bank, and 'private' money provided by commercial banks through collecting activities (via deposits, sometimes remunerated, and by issuing bonds) and supplying liquidity (loans or credit lines). In doing so, banks perform liquidity and maturity transformation activities. This transformation process is particularly risky, as a 'run on the bank' requires the ability to liquidate a significant portion of the bank's assets very quickly (typically within a day) and at sustainable prices. Note that even short-term, high-rated securities can be challenging to liquidate in adverse market conditions. These aspects are emphasized because they are also relevant to the activities of offering payment means (electronic money) or crypto-assets with similar characteristics.

For many years, a significant portion of transactions has occurred digitally, whether they are interbank transactions, transactions between banks and the public, or transactions involving specialized intermediaries. Electronic money (e-money) is a form of "private money" provided by banks, payment institutions, or electronic money institutions that manage various retail payment instruments (below), such as credit and debit cards, prepaid cards, ATMs, etc. In this context, liquidity and maturity transformation are (or should be) minimal, as the balance sheet assets of entities providing these services are based on liquid and short-term instruments (cash or high-quality short-term bonds). Prudential supervision limits the risks of instability for these intermediaries as well.

The following describes the characteristics of two classes of "tokenized money" (central bank digital currency and "tokenized" private electronic money that uses DLT); then, a comparison is made with so-called "stablecoins" that aim to replicate the functions of electronic money.

Central Bank Digital Currency (CBDC): CBDC is a form of digital currency for retail payments issued and regulated by a central bank. There are two technical ways to introduce CBDC ([28]). The first (so-called account-based CBDC) relies on a traditional (centralized) payment system where every citizen can hold their own account with the central bank. The second (DLT-based CBDC) - of interest in this context - is based on Distributed Ledger Technology (DLT) adapted accordingly. Beyond technologic aspects, still in the experimental phase, the literature on the subject has highlighted pros and cons in introducing CBDC. In particular, CBDC

[28] For a survey of the topic, see (ECB, 2020), (De Bonis, Ferrero, 2022).

introduction may be a response by central banks to a potential growing digitization process by a few major global players (such as Google, Amazon, Facebook/X, Apple), resulting in excessive concentration in the global retail payment systems market. Another reason is the need to keep a public payment system active as a support solution in case the private sector cannot cope with excessive demand peaks, as seen during the Covid-19 crisis. A third reason is the need to avoid possible fragmentation resulting from the development of different non-integrated private systems (with poor interoperability). Among the negative aspects, the loss of monetary sovereignty is emphasized, particularly for less developed countries or those with an unstable monetary system, due to a substitution effect between domestic currency and the global digital token (e.g., denominated in dollars) easily accessible via electronic devices. This effect (known as dollarization or euroization) reduces or makes it impossible to implement an effective monetary policy by the central bank of the country subject to this phenomenon ([29]).

E-money Tokens: These are crypto-assets that aim to maintain a stable value compared to an official currency, replicating the characteristics of "electronic money." The latter is defined as a monetary value electronically stored, represented by a credit towards the issuer, and issued against "funds" to carry out retail payment operations.

In this context, it is also necessary to mention payment services. Payment services are a set of services that allow depositing or withdrawing cash from a payment account (dedicated solely to such activities) and all the operations required for managing this account. It includes, among other things, the execution of payment transactions, such as transferring funds to a payment account at the payment service provider or entering into payment transactions; money remittance; services for the initiation of payment orders; account information services provided by third parties. A payment instrument is a personalized device or a set of procedures agreed upon between the user and the payment service provider and used to initiate a payment order. If an entity decides to provide a "payment service," the digital token must strictly adhere to the criteria that define "electronic money". In a traditional system, in the case of cross-border money remittance, funds are delivered by a payer without opening payment accounts in the name of the payer or the beneficiary. The cross-border transfer of crypto-assets occurs directly (without going through a central counterparty or a custodian bank). If, however, the fund transfer involves a traditional currency, the process can take place through a crypto asset that plays a role we could call a "vehicle token" for transferring funds (including different currencies) between one country and another (as in the case of Ripple, see Box 3).

Box 3 – The Case of Ripple and the Ruling of the New York Court

An example of a "vehicle token" is XRP. It is a token without an underlying asset, without assets and liabilities, but with embedded rights. It is associated with the money transfer system developed by Ripple Labs Inc. The system is based on an algorithm called Ripple Transaction Protocol (RTXP) and the RippleNet network. XRP is the native cryptocurrency used within this network. RippleNet facilitates the international transfer of funds, including different currencies, through a network of financial institutions such as banks and payment service providers. The network is organized through a series of payment service providers that act as entry and exit points for the Ripple network. These providers allow users to deposit money in their local counterparts and receive XRP in return. When a payment is sent, the system automatically determines the most efficient path through the network to convert the original currency into XRP and then into the destination amount in the destination currency. Ripple uses blockchain technology to record and verify transactions. Once a transaction is validated, through a particular consensus protocol known as the Ripple Protocol Consensus Algorithm (RPCA), funds are transferred from the sender to the recipient almost instantly.

It should be noted that on July 13, 2023, the Southern District Court of New York (1) ruled on the accusation filed by the Securities and Exchange Commission (SEC) against Ripple Labs Inc for conducting an unregistered securities offering through the sale of the XRP token. This accusation was based on the assumption that XRP was a security, and therefore, its sale without proper registration constituted a violation. The NY Court identified three modes of public XRP sales: i) sales through written contracts and through Ripple subsidiaries of XRP tokens to institutional investors or hedge funds; ii) the sale of XRP through exchange platforms using trading algorithms ("Programmatic Sales") that operate through a "blind bid/ask transactions" system; iii) the distribution of XRP to Ripple employees as compensation for their activities. According to the Court, only the first method of offering would qualify (based on the Howey test) as the public sale of a "security" and, as such, should be regulated. The court did not find this in the other two offering methods. For further details, see paragraph 5.3.

(1) See: https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf.

The economic features of stablecoins: Certain crypto-assets are designed with the objective of maintaining a fixed price (peg) relative to a reference currency (dollar, euro, etc.) or a basket of assets. Worth mentioning that, contrary to centralised finance, DeFi cannot support fiat currencies (since fiat currencies are not available 'on-chain'). Stablecoins are therefore essential to the operations of DeFi markets. They facilitate fund transfers between users and across protocols, are used as deposits and collateral in DeFi protocols, and eliminate the need for multiple conversions to and from fiat money (ESMA, 2023, p. 5).

These instruments most of the time possess assets and liabilities. In some cases, they replicate the economic structure of constant net asset value (NAV) money market funds (MMFs), with the significant difference that MMFs are typically used to allocate wholesale liquidity and not for small retail transactions. MMFs are special funds, essentially similar to demand deposits, which predominantly invest in liquid assets (cash or short-term high-quality securities, such as commercial paper, sovereign securities, repo contracts). Despite these characteristics, they may be subject to liquidity crises in adverse market conditions, requiring central bank intervention, as observed during the 2008-'09 financial crisis and more recently during market turbulence following Covid-19 ([30]). Some stablecoins

[29] On these aspects, see (Armas, Singh, 2022).
[30] See (FSB, 2020).

have a value anchored to that of the underlying basket of assets but with a variable price; the price of these tokens fluctuates, as is the case with any variable NAV fund, contrary to what their name might suggest.

Crypto-assets known as *algorithmic stablecoins* don't have underlying assets. They typically work by automatically adjusting the coin's supply in response to changes in demand. For example, if the price of the stablecoin is above its target value, the algorithm may increase the coin's supply by minting new tokens or incentivizing users to create more coins (and vice versa). Algorithmic stablecoins have experienced difficulties during market turbulences, as exemplified by projects like Iron Finance and Terra-Luna.

5. Legal Characteristics

As anticipated in the previous paragraph, among the possible ways to describe crypto-assets, in addition to their predominant economic functions, are their legal characteristics. The latter are not uniform and depend on the possibility of classification into different categories based on legal characteristics adopted in various jurisdictions. In the following, we confine the legal analysis to the European Union, with particular reference to the classification of certain types of digital tokens within the concept of a "financial instrument." Subsequently (paragraph 5.3), the analysis will also expand to the aspect related to the public offering of a token with an investment function. This aspect, the latter, is particularly debated in the United States through a common law approach based on the so-called Howey test (infra).

In purely economic terms, a token can be referred to generically as a "financial instrument," i.e., a negotiable asset on a market with assets and liabilities. The same cannot be said on the legal level, where - at least in Europe - the notion of a financial instrument is precisely defined by the MiFID II directive, which provides a "closed" list of financial instruments without admitting extensions "by analogy." Although some crypto-assets, especially those already classifiable as financial instruments, fall fully within the scope of the relevant legislative acts on financial services, other crypto-assets are excluded. Only by understanding their different functioning, types and practical applications (fungible tokens, non-fungible tokens, financial tokens, utility tokens, etc.) and the type of performance (right or claim) that is "incorporated," it is possible to provide a comprehensive and granular legal framework for the phenomenon. The current possible regulatory gap exposes holders of this latter type of crypto-asset to substantial risks to market integrity, including market abuse and financial crime, especially in sectors not governed by consumer protection regulations ([31]).

5.1 MiCAR definitions

The EU Regulation 2023/1114 on markets in crypto-assets (MiCAR) defines crypto-assets as follows: "a digital representation of a value or right that can be transferred and stored electronically, using distributed ledger technology or a similar technology" (Article 3, paragraph 1, number 5). Although MiCAR has provided in Recital 16 that "the terms 'crypto-assets' and 'distributed ledger technology' should be defined in the broadest possible way so as to encompass all types of crypto-assets that currently fall outside the scope of Union legislation on financial services," Article 3 of MiCAR has delimited the scope to the following crypto-assets:

- "**e-money tokens (EMT)**": a type of crypto-asset that aims to maintain a stable value by referencing the value of an official currency ([32]);
- "**Asset-referenced token (ART)**": a type of crypto-asset that is not an electronic money token and aims to maintain a stable value by referencing another value or right or a combination of the two, including one or more official currencies;
- "**Utility token**": a type of crypto-asset intended solely to provide access to a good or service provided by its issuer.

This regulation, in Recital 9 and Article 2, has excluded from its scope crypto-assets that can be classified as: i) "financial instruments" as defined by Directive 2014/65/EU; ii) "deposits" ([33]) as defined by Directive 2014/49, including "structured deposits" ([34]) as defined by Directive 2014/65/EU; iii) "funds" ([35]) as defined by Directive 2015/2366, except when they qualify as electronic money tokens; iv) "positions in securitization" ([36]) as defined by Regulation 2017/2402; v) non-life or life insurance contracts, pension

[31] For the legal approach to uncertain taxonomy, see (Pappano, d'Atri, Befani, Zanardo, 2021).

[32] Defined in turn as an official currency of a country issued by a central bank or another monetary authority. Note that "electronic money" (traditional) is defined in Article 2, point 2, of Directive 2009/110/EC as "monetary value electronically stored, including magnetic. As explicitly outlined in Consideration No. 19 of MiCAR, electronic money and crypto-assets with an official currency as the reference currency differ in some crucial aspects. Holders of electronic money, as defined by Directive 2009/110/EC, always possess a credit against the electronic money issuer and have the contractual right to obtain, at any time and at face value, the reimbursement of the monetary value of the electronic money held. Conversely, some crypto-assets with an official currency as the reference currency do not provide their holders with such credit against the issuers of these crypto-assets and may not fall within the scope of Directive 2009/110/EC. Additionally, according to MiCAR, other crypto-assets with an official currency as the reference currency do not provide credit at the face value of the reference currency or impose limits on the repayment period. The fact that holders of such crypto-assets do not have credit against the issuers of the relevant crypto-assets, or that such credit is not at the face value of the reference currency of the crypto-assets, could undermine the confidence of the holders of such crypto-assets.

[33] "Deposit": a credit balance resulting from funds deposited in an account or from transient situations arising from normal banking operations, which the credit institution must repay according to applicable legal and contractual conditions, including a fixed-term deposit and a savings deposit, but excluding a credit balance when: a) its existence can only be proven through a financial instrument as defined in Article 4(17) of Directive 2004/39/EC, unless it is a savings product represented by a certificate of deposit referring to a specific person and existing in a Member State on July 2, 2014; b) its capital is not repayable in full; c) its capital is repayable in full only based on a specific guarantee or agreement provided by the credit institution or a third party.

[34] "Structured deposit": a deposit as defined in Article 2(1)(c) of Directive 2014/49, which is fully repayable at maturity based on terms where any interest or premium will be repaid (or is at risk) according to a formula including factors such as: a) an index or a combination of indices, except for variable-rate deposits whose return is directly linked to an interest rate such as Euribor or Libor; b) a financial instrument or a combination of financial instruments; c) a commodity or a combination of commodities or other fungible, tangible, or intangible assets; or d) an exchange rate or a combination of exchange rates.

[35] "Funds": banknotes and coins, scriptural money, or electronic money as defined in Article 2(2) of Directive 2009/110/EC.

[36] "Position towards a securitization": an exposure towards a securitization.

products, or social security schemes falling within the scope of Directive 2016/2341 or falling within the insurance classes listed in Annexes I and II of Directive No. 2009/138/EC.

MiCAR also excludes crypto-assets that are unique and non-fungible with other crypto-assets, including digital art and collectibles whose value is attributable to the unique characteristics of each crypto-asset and the utility it offers to the token holder (cf. Recital 10). The regulation also does not apply to crypto-assets representing services or tangible activities such as product guarantees or real estate. MiCAR also excludes digital assets accepted only by the issuer or offeror and that are technically impossible to transfer directly to other holders (cf. Recital 17). An example of such digital assets is represented by loyalty programs where loyalty points can be exchanged for benefits only with the issuer or offeror of such points.

Therefore, the correct legal classification must be carried out starting from the economic-social function pursued by the token holder and will depend precisely on the performance (claim) contained in it, i.e., the activities or rights represented therein. Crypto-assets that do not fall within the scope of MiCAR must be subject to existing Union legislative acts on financial services or must remain regulated by the existing regulatory framework, regardless of the technology used for their issuance or transfer.

5.2 A Possible Legal-Regulatory Framework

Seeking to develop a regulatory framework capable of systematically and comprehensively considering all types of digital tokens, it is necessary to integrate the previously considered economic functions with their potential legal nature in a given jurisdiction. In Europe, the following four autonomous and legally relevant categories seem to emerge:

i) Pure tokens (cryptocurrencies in the strict sense and "virtual currencies" ([37]) under Directive 2018/843, the so-called 5th Anti-Money Laundering Directive), such as Bitcoin, which assumes the legal nature of movable property because, despite having an independent and variable exchange value, it does not serve a monetary function, does not incorporate or confer any other utility, and does not grant any right to the reimbursement of the nominal value ([38]);

ii) Financial tokens representing a "participatory instrument" in a financial activity of broader nature, potentially representing dividends, shares, or units of investment funds falling within the definition of "DLT financial instrument" provided by Regulation 2022/858 (the so-called DLT Pilot Regime)[39] as the "financial instrument issued, registered, transferred, and stored using distributed ledger technology". They fall within the scope of legislative acts on financial instruments.

Specifically, depending on various usage modes, the expectation of economic return, the possible production of interest, and the "recognition" of the associated performance, there will be the following subcategories:

- Investment tokens, with a speculative purpose similar to financial instruments;
- Asset tokens, representing titles of a specific fungible and listed/commodity in a regulated or OTC market;
- Debt tokens, representing a debt similar to corporate bonds;
- Equity tokens: representing a "share" in the issuing entity;
- Governance tokens, representing distributed votes to carry out "extraordinary" activities on the reference blockchain platform, conferring effective control prerogatives to the respective holders over the governance system of the DLT[40] (on this aspect, refer to the two cases described in the Annex);

iii) Utility tokens, to benefit from a good, service, or right to a specific performance. In addition to tokens representing works of art, there are those that allow access to gaming platforms, metaverse, or other activities. They are comparable to physical tokens or coupons not usable outside the issuing platform and without general spendability. Additionally, they do not generate interest. Utility tokens, by virtue of the general principle of the "freedom of issuance" of securities, rather than being legally configured as mere documents of legitimacy (such as a ticket for a show), can fall into the category of atypical and decentralized credit securities if the three characteristics of abstraction, literalness, and autonomy are present ([41]). For example, we mention:

---

[37] According to art. 1, par. 2 lett. d) of the 5th Anti-Money Laundering Directive, "virtual currencies" means «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».

[38] See (Befani, 2019).

[39] The "DLT Pilot Regime" introduces authorization and supervision requirements for financial market infrastructures (central securities depositories – CSDs or multilateral trading facilities – MTFs) based on DLT technology (DLT MI). This regime is anchored by the designated national competent authorities through sectoral regulations (MiFID II and CSDR). The Pilot Regime allows DLT market infrastructure, unlike traditional infrastructures (MTFs and CSDs), to combine the offering of trading and settlement services for securities within a single DLT MI (DLT trading and settlement system). The Regulation, in the experimental spirit of the rule, imposes strong restrictions on instruments (stocks, bonds, debentures of private limited companies, units of UCITS) issued and transferred within a distributed ledger. It is noteworthy that currently, the Payment Services Directive (PSD2) does not include so-called payment tokens in the definition of "funds." However, to account for developments in digitalization applied to payments and for the purposes of payment system surveillance, the Eurosystem's "PISA framework" now refers to a more general concept of "value transfer" (instead of "funds transfer"), thus paving the way for surveillance of digital payment tokens.

[40] It's worth noting that both *governance tokens* and *equities* may possess ownership rights, voting rights, transferability, and negotiability, along with other typical aspects of financial instruments; however, while equities may entitle shareholders to dividends or other forms of profit sharing, depending on the company's profitability and dividend policy, governance tokens in some cases do not provide direct financial rewards such as dividends. Instead, holders may benefit indirectly from the success of the protocol or platform through appreciation in token value, increased usage, or other mechanisms. In order to avoid confusion, if a token does not promise future cash flows, is called in this paper "*management token*".

[41] In legal terms, when defining the characteristics of a security, it is said to be "abstract," "literal," and "autonomous." In particular: 1) an *abstract* security is independent of the underlying contract or transaction that generated it. In other words, its value and associated rights exist independently

- Art tokens, which are non-fungible and confer only the enjoyment of the digital work;
- Game tokens, with limited fungibility that enable only the enjoyment of entertainment offered on the gaming platform;
- Management tokens, representing computational capacity to perform "ordinary" blockchain operations, enabling only participation in the functioning of the platform without attributing any specific power in the "extraordinary" management of the blockchain (e.g., changing the consensus protocol; the number of generable tokens; fees for participants) but only to maintain the platform and validate transactions (see Annex).

iv) Stablecoins, which are pegged to an underlying value anchor. Depending on the type of underlying chosen, this category of "stable tokens" can be categorized into the three subcategories below (or a combination of them):

- E-money tokens (a subspecies comparable to electronic money tokens if the reference is to a single official currency);
- Tokenized financial debt instruments, configurated as "bearer debt instruments";
- Asset tokens, configurated as "commodity representative securities" (commodities, such as gold) or algorithmic stablecoin, without underlying assets.

The distinction between the various types is determined by the different systems used to "collateralize" the underlying value, often expressed by a sum of money in function of a "reference currency" and by the different modes of binding the value reserve as collateral (with or without reimbursement of the nominal value), constituting a kind of irregular deposit certificate or abstract title representing goods. If these tokens are issued in series to solicit financial investments from the mass of savers, overlapping with financial tokens, they would encounter additional limits resulting from the necessary controls exercised by competent supervisory authorities to ensure the stability of the financial/credit system.

5.3 The Legal Concept of "Financial Investment" in Europe and the United States

The described legal taxonomy of tokens allows for the identification of a common element, given by the digital representation of an "external value" that, in some cases, are not intrinsic to the token itself but are attributed by the involved parties based on the principle of supply and demand. This means that the value is subjective and based solely on the individual interest of the buyer of the crypto-asset.

The economic and financial characteristics of the various forms of crypto-assets so far described overlook another relevant aspect, particularly the characteristics of the *initial issuance offer*. The legal consequences of the issuance phenomenon, in fact, diverge depending on the type of token to be placed, and can be structured as follows:

- Initial Coin Offering (ICO) for the offer of pure tokens;
- Utility Coin Offering for the offer of utility tokens;
- Security Token Offering for all financial tokens and stable coins falling within the definition of financial instruments.

Although the risks of these new resource-raising methods have already attracted the attention of various supervisory authorities ([42]), the current state of European legislation on crypto-assets lacks specific regulations that can bind exchange platforms to the information obligations provided for in the provision of financial services (with the exception of aspects considered in the Pilot Regime DLT directive, mentioned earlier).

MiCAR itself provides that the mere admission to trading or the publication of buying and selling prices should not, in itself, be considered a public offering of crypto-assets. Under MiCAR, such admission or publication should constitute a public offering of crypto-assets only if it includes communication that constitutes a public offer.[43]

For a token to fall within the notion of a financial instrument, it should demonstrate being able to represent risk capital, debt capital, money market or allowing the acquisition of other financial instruments or their indices.

In this sense, the exclusion of certain forms of crypto-assets from the category of financial instruments is enhanced by the regulation of MiCAR where (Recital 29) has provided that although some offers of crypto-assets other than tokens linked to activities

---

of any underlying transaction. This implies that, even if the main agreement were to be voided or breached, the abstract security can be exercised or transferred separately; 2) a *literal* security is based on the written words within the document itself. The provisions of the security are clear and definitive, and the involved parties must adhere to the conditions set out in the document. This means that the meaning of the security can be directly determined from the written text, without the need for external interpretations; 3) an *autonomous* security is self-sufficient and can circulate independently of the main contract or underlying transaction. In other words, the security has intrinsic value and can be traded or used without having to refer to the original agreement or any other related documents. These three characteristics are crucial as they provide clarity and certainty in financial transactions, facilitating smoother circulation of securities and enhancing legal security.

[42] Of particular significance is the stance taken by the European Securities and Markets Authority in November 2017 (Esma 50-157-828), urging issuers to assess whether their activities could fall under the Prospectus Directive, MiFID, AIFMD, or the Fourth Anti-Money Laundering Directive. Notably, Directive 2003/71/EC aims to ensure that information provided to investors by companies raising capital in the EU is adequate, requiring the pre-publication of a prospectus approved by the competent authority before the offer of securities and financial products to the public.

[43] Public offerings of tokens linked to activities in the Union or applications for admission to trading should only be allowed if the competent national authority has authorized the issuer of such crypto-assets to proceed and has approved the relevant White Paper on crypto-assets. To ensure the protection of retail holders, issuers of tokens linked to activities should always provide holders of such tokens with complete, accurate, clear, and non-misleading information. The White Paper on crypto-assets related to tokens linked to activities should contain information on the mechanism for stabilizing the value of the token compared to the value of the weighted average of the underlying assets, the investment policy of the reserve assets, the custody arrangements of the reserve assets, and the rights recognized to holders.

(ART) or electronic money tokens (EMT) are exempt from various obligations of the same, "Union legislative acts ensuring consumer protection, such as Directive 2005/29/EC or Directive 93/13/EEC, including the information obligations contained therein, remain applicable to public offers of crypto-assets when they concern relations between businesses and consumers";

In order to ensure a clear distinction between crypto-assets regulated by MiCAR and other financial instruments, Recital 14 and Article 2(5) of MiCAR have provided that the European Securities and Market Authority must issue, by December 30, 2024, guidelines on criteria and conditions for the qualification of crypto-assets as financial instruments, and these guidelines should allow for a better understanding of cases where crypto-assets that are otherwise considered unique and non-fungible with other crypto-assets could be qualified as financial instruments ([44]);

Pending the adoption of these guidelines, it is useful to attempt to provide some operational indications on the legal concept of investment in this working document, considering that the European system envisages a clear distinction between "consumer investments" and "financial investments".

The search for a "bridge" between the EU and US approaches - The connecting line and potential overlap between the notion of offering "financial instruments" to the public and offering investment services is determined by the presence of three elements to configure an "investment," namely:

- The use of capital;
- The expectation of a return;
- The assumption of a risk directly connected and correlated to the use of capital.

In this sense, the possible demarcation line proposed here would like to shift the focus not on the "speculative" use of capital (which would be inherent in any type of economic activity) but only on the object of such activity, where the interpretative distinction can be resolved in the opposition between investment in "financial assets" and investment in "real assets" (meaning goods and services of the real economy). Because these latter activities, even if concluded with speculative intent, are essentially aimed at providing the investor with the enjoyment of a "good of life." In other words, as it is evident that investments in diamonds, stamps, precious metals, ancient coins, or works of art do not constitute financial products, as they are consumer investments, the same identical approach must be followed for the described classifications of tokens.

For the proper legal delineation of the concept of "financial investment," it is appropriate to refer to the American experience of the Howey Test, as determined in the United States by the historic Supreme Court decision of 1946 (SEC vs. W.J. Howey Co - 328 U.S. 293 ([45]), which applies to any contract, scheme, or transaction, regardless of whether it has the formal characteristics of typical securities.

The Howey Test - It represents the discretionary criterion used to determine whether a specific "investment" activity in the form of an "investment contract" can be classified as a security subject to the prudential regulation of the Securities Act of 1933 and the Securities Exchange Act of 1934, in addition to the supervisory powers of the Securities and Exchange Commission.

The Supreme Court has identified the following four criteria to define and delineate an "investment contract":

1. It must be an investment of money;
2. Investors' fortunes are linked together in a common enterprise (i.e. they have a 'common interest'): the success or failure of one investor is tied to the success or failure of other investors in the same enterprise;
3. There must be an expectation of profit;
4. Profit must come from the efforts of parties other than the investors.

In this sense, although the Howey Test appears particularly useful to identify in detail which crypto-assets can be qualified as securities and therefore subject to existing financial regulations, it is not equally applicable to pure tokens like Bitcoin, which in the USA are defined as commodity ([46]) (which, for example, has never been funded through ICOs to promote or develop its technology) or Ether.

---

[44] Consideration No. 14 of MiCAR further establishes that " In order to promote a common approach towards the classification of crypto-assets, EBA, ESMA and the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (EIOPA), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council (the 'European Supervisory Authorities' or 'ESAs') should promote discussions on such classification. Competent authorities should be able to request opinions from the ESAs on the classification of crypto-assets, including classifications proposed by offerors or persons seeking admission to trading. Offerors or persons seeking admission to trading are primarily responsible for the correct classification of crypto-assets, which might be challenged by the competent authorities, both before the date of publication of the offer and at any time thereafter. Where the classification of a crypto-asset appears to be inconsistent with this Regulation or other relevant Union legislative acts on financial services, the ESAs should make use of their powers under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 in order to ensure a consistent and coherent approach to such classification."

[45] The Howey Test originated from a 1946 U.S. Supreme Court case, SEC v. W.J. Howey Co. This case involved the sale of agricultural land with citrus groves in Florida owned by the Howey Company for investment purposes. Specifically, the contractual operation involved a sale and lease-back formula, where investors, lacking agricultural experience or the ability to intervene in plantations, would purchase portions of citrus groves and then lease the land to the Howey Company, which would manage the crops for each agricultural year, paying profits to the investors. In that case, the Court ruled that a transaction constitutes an investment contract (and therefore a security) since it involved an investment of money in a common enterprise with an expectation of profits primarily from the efforts of others. This contractual scheme was not registered as a security under U.S. law, therefore leading to regulatory intervention by the SEC.

[46] At this purpose, it has to be considered that in an enforcement action of 2015 (*In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29*) the U.S. Commodity Futures Trading Commission defined Bitcoin and other virtual currencies as commodities

Therefore, in addition to the Howey Test, it is particularly significant to refer to the European financial regulatory system, which precisely identifies the legal scope of "investment services and activities" as defined in Article 4(1)(2) of MiFID II Directive 2014/65/EU as "any service or activity mentioned in Section A ([47]) of Annex I related to one of the instruments listed in Section C of Annex I" ([48]).

The importance of such a reference is evident for the various regulations that implement it and criminally sanction anyone who, without authorization, provides investment services or activities, or "offers at a distance" or "promotes or places through distance communication techniques" financial instruments or "investment services or activities".

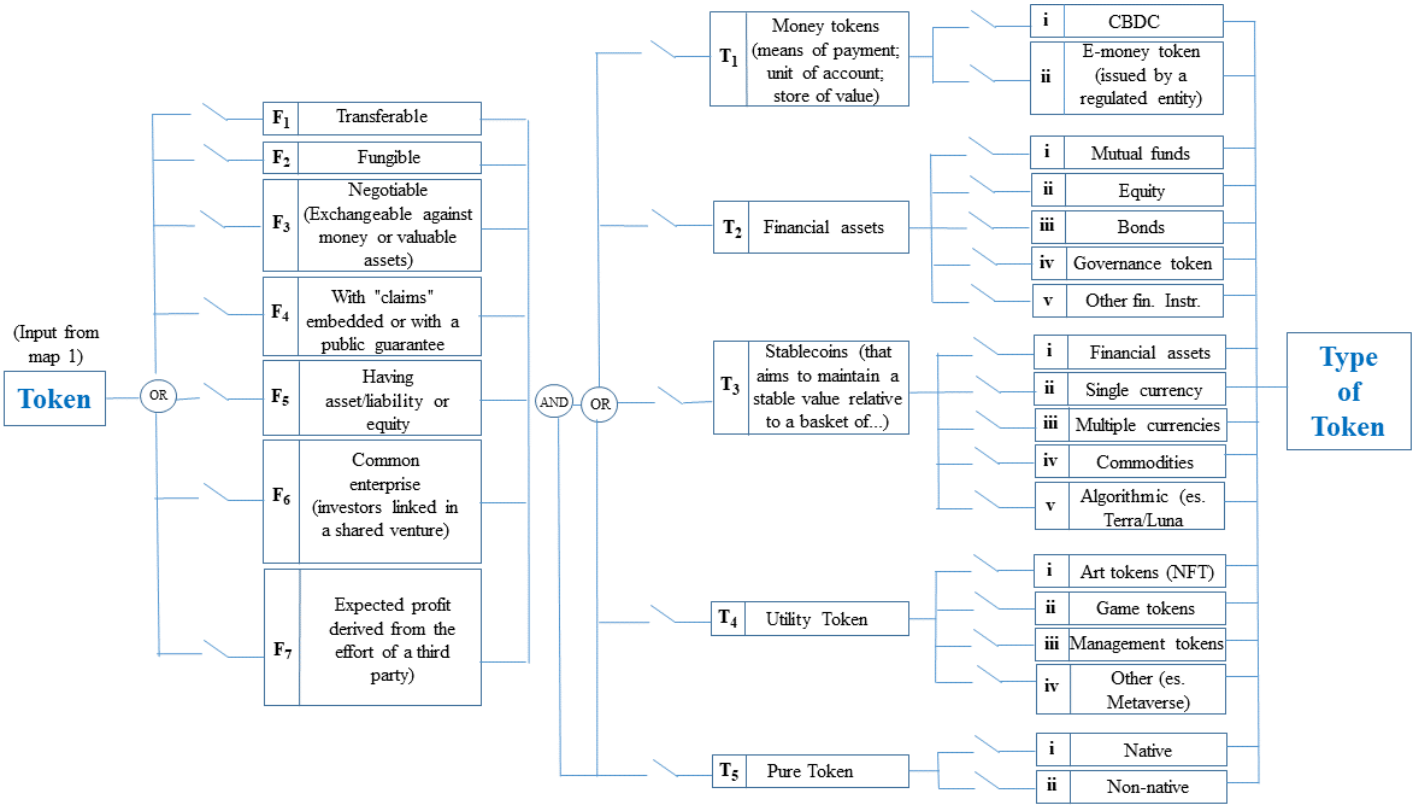
In this way, the focus of supervisory authorities can shift from the individual token being the subject of investment (where only for financial tokens would all current financial provisions be directly applicable) to the methods of promoting investments in tokens or promoting those tokens (e.g., e-money tokens) that would constitute a "savings collection," strictly prohibited and criminally sanctioned for entities other than banks and legislatively understood as "acquiring funds with an obligation of repayment, either in the form of deposits or in another form".

In other words, just as an intermediary who wishes to solicit and promote investment activities in diamonds or raise capital from savers must be subject to prior authorization, the same applies to intermediaries offering and promoting investment activities in crypto-assets, whether they are in the form of pure tokens, utility tokens, or stable coins (and their various subcategories), even if they do not pass the Howey Test to be directly classified as securities.

6. A Logic Framework for Classifying Crypto-Assets

In the initial part of this study, we conducted an overview of different blockchain types and proposed a logic map capable of representing various possible configurations of this technology; these can also be synthesized using simple formulas. The same methodology can be applied to represent various types of crypto-assets, their primary functions, and legal characteristics (Figure 3).

Figure 3 – Map of Crypto-Asset Characteristics



The aim is to capture the key aspects of the regulatory approach followed by a give jurisdiction (for instance, the EU or the United States). Specifically, while the European Union tends to frame the phenomenon within the legal category of "financial instruments" (characterized, as seen earlier, by their transferability, fungibility, negotiability, and the presence of an asset or liability), in the United States, the differentiator seems to be related to the elements comprising the Howey test, or, as in the case of Bitcoin, the resemblance

under the U.S. Commodity Exchange Act (the CEA) because the Section 1a(9) of the Act defines "commodity" to include, among other things, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in." 7 U.S.C. § 1a(9). The definition of a "commodity" is broad. See, e.g., Board of Trade of City of Chicago v. SEC, 677 F. 2d 1137, 1142 (7th Cir. 1982). Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.

[47] Related to 1) Reception and transmission of orders concerning one or more financial instruments. 2) Execution of orders on behalf of clients. 3) Trading on own account. 4) Portfolio management. 5) Investment advice. 6) Underwriting of financial instruments and/or placement of financial instruments based on an irrevocable commitment. 7) Placement of financial instruments without an irrevocable commitment. 8) Operation of multilateral trading facilities. 9) Operation of organized trading facilities.

[48] This attachment provides a list of considered instruments, including securities, money market instruments, units in collective investment undertakings, options, futures, swaps, contracts with derivative components, including contracts for difference.

to commodities. The map presented in Figure 3 relies again on the use of logic operators (and/or) and switches that "close" to represent a particular native or non-native token ([49]). As for the blockchains, the map can be enriched with sub-maps representing second layers and related tokens. Note that some characteristics are mutually exclusive (symbol XOR), while others are not. Of course, regulators could enhance the map with additional specifications based on the introduction of new regulations and/or new classes of tokens. As an illustrative example, the following are the "formulas" that could represent some crypto-assets with very different characteristics:

Bitcoin: (F1∧F2∧F3) ∧ (T5(i))
ETH-20: (F1∧F2∧F3∧F7) ∧ (T2(iv)∧T4(iii)∧T5(i))
Ripple (XRP): {A} or {B} or {C}, where:
{A} = offered through exchangers = (F1∧F2∧F3∧F4∧F7) ∧ (T5(i))
{B} = offered to institutional investors = (F1∧F2∧F3∧F4∧F6∧F7) ∧ (T5(i))
{C} = offered to developers as an incentive = (F1∧F2∧F3∧F4∧F7) ∧ (T2(iv)∧T5(i))
Tokenized bond issued by a bank: (F1∧F2∧F3∧F4∧F5∧F6∧F7) ∧ (T2(iii))
Tether: (F1∧F2∧F3∧F4∧F5) ∧ (T3(ii))
Algorand (ALGO) ([50]): (F1∧F2∧F3∧F7) ∧ (T4 (iii)∧T5(i))

Clearly the formula changes if the type of token supported by a given blockchain are different. For instance, Ethereum is a blockchain platform that supports the creation and deployment of smart contracts, allowing for the development of various types of tokens. Here are some examples of token classes on the Ethereum blockchain:

ERC-20 Tokens: These are the most common standard for fungible tokens. ERC-20 tokens follow a set of rules, allowing them to be easily exchanged with one another. Examples include DAI (a stablecoin), Chainlink (LINK), and Uniswap (UNI). In this case the formula is reported above.

ERC-721 Tokens (Non-Fungible Tokens - NFTs): These tokens are unique and indivisible, often representing ownership or proof of authenticity for digital or physical assets. Popular examples include CryptoKitties, Decentraland (LAND), and Cryptopunks. In this last case the formula would be: (F1∧F4∧F5) + (T4 (i))

It is essential to note that the formulas above must be combined with those related to the blockchain where the digital token is generated or exchanged: two tokens with the same characteristics could be "generated" by two different blockchains, with evident implications for their potential regulation.

7. Applying the switching circuits in a regulatory setting

The proposed methodology can be implemented by a hypothetical competent authority (privacy watchdog, monetary authority, AML/CFT authority, financial regulator, etc.). Below, we provide three examples: the issuance of a piece of digital artwork (art token); the issuance of a monetary token (e-money token); and the issuance of a financial instrument.

The examples provided do not reflect regulatory guidance, nor any existing regulation, but are intended purely to explain how the suggested method works.

Art token – The token, also called non-fungible token (NFT), can operate in the jurisdiction if and only if (⇔) the Distributed Ledger Technology (DLT) complies with the following features: it is designed to avoid "accidental forks" (A4); it provides legal certainty ("notary function") (A6); the user is identifiable and privacy is respected (A7);the transaction complies with AML/CFT criteria (A8); and the token has the following characteristics: it is transferable (F1); it has an underlying claim (F4); it provides utility to the token holder (T4(i)). Finally, the token can be either native (T5 (i)) or non-native (T5(ii)).

Monetary token – The token can operate in the jurisdiction if and only if:

(i) The DLT has the following characteristics: it allows full interoperability (A3); it is designed to avoid "accidental forks" (A4); it does not use a probabilistic settlement (¬ A5); it provides legal certainty ("notary function") (A6); the user is identifiable and privacy is respected (A7); the transaction complies with AML/CFT criteria (A8); the system is permissioned (P0) and does not use the Proof-of-Work consensus protocol (¬ X0); it has a governance body (R1); it has an audit unit (R3); the protocol P is upgradable (ΔP). Alternatively, the DLT could be permissionless (P2), but in this case it should be non-vulnerable to 'hard-forks' and "accidental forks" (A4).

(ii) The token has the following characteristics: it is transferable (F1); it is fungible (F2); it is negotiable (F3); it has an underlying claim (F4); it has assets and liabilities (F5); it is issued by a supervised entity as an electronic money intermediary (T1(ii)); it has as

[49] The key distinction between native and non-native token relies in whether the token is integral part of the primary blockchain or created by users leveraging the blockchain's smart contract capabilities. Native tokens are typically the platform's core currency, while non-native tokens are created on top of the blockchain for specific purposes determined by smart contracts.

[50] The Algorand's full formula (both a for DLT and token), is:

$$F = (A_0 \wedge A_1 \wedge A_2 \wedge A_3 \wedge A_4 \wedge A_5 \wedge A_6) \wedge (P_2 \wedge X_3) \wedge \left(R_1 \wedge R_2 \wedge R_3 \wedge R_4 \wedge R_{5\,(V4)}\right)_{offChain} \wedge \Delta P \wedge [(F1 \wedge F2 \wedge F3 \wedge F7) \wedge T4(iii) \wedge T5(i)$$

To clarify the criteria behind the formula, it is useful to clarify some points: i) Algorand's settlement relies on a PoS consensus called Pure PoS, based on a random selection of the token of the node proposing the block and, on a subsequent random selection, of a set of nodes chosen in each validation (individual cryptographically fair lottery); this latter aspect is represented by the symbol V4 (see box 1 in the text). ii) The settlement is classified as *probabilistic* (A5) and designed to avoid "accidental forks" (A4). The symbol ΔP is introduced in the formula, because Algorand is upgradable (staking allows off-chain "management powers"); iii) its blockchain is permissionless (symbol P2), but it can also be configured in permissioned mode (with a default tolerance of 2/3 of active nodes). The token is of the native "pure" type (T5 (i)). Unlike Ethereum, it does not rely on a privileged role for certain governance or management entities.

an underlying a basket, even composed of a single unit, consisting of a financial asset (T3(i)) or a currency (T3(ii)); both native token (T5 (i)) and non-native token (T5(ii)) are allowed by this hypothetical regulator.

Financial token – The token can operate in the jurisdiction if and only if the DLT complies with the same features of the monetary tokens (see above) and the token has the following characteristics: it is transferable (F1); it is fungible (F2); it is negotiable (F3); it has an underlying claim (F4); it has assets and liabilities (F5); the investors have a common interest (F6) and expected profit from the effort of a third party (F7); the token is a digital representation of a bond ((T2 (iii)), which is "tokenized" through a smart contract (A2). Both native token (T5 (i)) and non-native token (T5(ii)) are allowed by this hypothetical regulator.

The three formulas would be, respectively:

Art token (NFT): compliant ⇔ (DLT: A4 ∧ A6 ∧ A7∧ A8) ∧ (Token: (F1 ∧ F4 ∧ T4(i) ∧ (T5 (i) ∨ T5 (ii)))

Monetary token: compliant ⇔ (DLT: A3 ∧ A4 ∧ (¬ A5) ∧ A6 ∧ A7∧ A8∧ P0 ∧ (¬ X0) ∧ R1 ∧ R3 ∧ (ΔP)) ∧ (Token: F1 ∧ F2 ∧ F3 ∧ F4 ∧ F5 ∧ T1(ii) ∧ (T3(i) ∨ T3(ii)) ∧ (T5(i) XOR T5(ii)).

Financial token: compliant ⇔ (DLT: A4 ∧ (¬ A5) ∧ A6 ∧ A7 ∧ P0 ∧ (¬ X0) ∧ R1 ∧ R3 ∧ (ΔP) ∧ (Token: F1 ∧ F2 ∧ F3 ∧ F4 ∧ F5 ∧ F6 ∧ F7 ∧ T5(ii) ∧ T2(iii) ∧ (T5(i) ∨ T5(ii)).

Please note that the formulas do not describe the entire characteristics of the blockchain crypto-assets system, (already illustrated above), but rather only the necessary and sufficient conditions required by a hypothetical regulator to operate within its jurisdiction.

Two practical applications:

MiCAR – The transliteration of MiCA into our framework would result as follows (we put in square brackets aspects we consider implicit). The regulation defines crypto assets (CA) as follows: a digital representation of 'value', generated by DLT (T5) [both 'native' (i) and 'non-native' (ii) tokens] or 'rights' (F4), which are fungible (F2) [since non-fungible tokens are excluded] and transferable via DLT (F1). MiCAR does not apply to 'financial instruments' covered by MiFID II. It disciplines only three types of CA[51]:

EMT, defined as that token "that aims to maintain a stable value by referencing the value of an official currency (T1(ii) ∧ T3(ii));
ART, defined as that token "that is not electronic money (¬ EMT), and aims to maintain a stable value by referencing another 'value' or 'right', or combination thereof, including one or several official currencies (T3);
Utility token, defined as: that token "intended solely to provide access to a good or service (T4(ii) or) provided by its issuer.

SEC - In this case, the interpretation would be attributable to compliance with the Howey test described in paragraph 5.3: a token falls into the category of publicly offered investments if investors having a common interest (F6) expect a profit generated by the efforts of third parties (F7).

If the representation above is correct, the formulas, simplified from repetitions, would be:

- A {CA} is eligible under MiCAR iff: (T5 (i) ∧ T5 (ii)), F1, F2, F4), otherwise, is 'out of scope' [F3 should be infer MIFID II];
- IF a crypto-asset is: {CA} ∧ (T1 (ii) ∧ T3 (ii)), => is e-money token (EMT).
- IF a crypto-asset is: {CA} ∧ (¬ EMT) ∧ (T3(i) ∧ T3(ii) ∧ T3(iii) ∧ T3(iv) ∧ T3(v)) => is Asset-referenced token (ART).
- IF a crypto-asset is: {CA} ∧ T4 , => is Utility token (also called 'Other than').
- IF a crypto-asset is: [F1∧F2∧F3∧F4] ∧ F5 ∧ F6 ∧ F7, => is a USA definition of 'financial investment'.

As mentioned before, ∧ represents 'AND', indicating all conditions in a list such as (F1, F2, F3) must be satisfied, while ∨ represents 'OR', indicating at least one condition in a list like (T1, T2, T3, T4) needs to be true, and XOR denotes mutual exclusivity, for instance, T5 (i) XOR T5 (ii)). To close the 'circuit', however, either T5(i) or T5(ii) mast be true. The symbol '¬' means 'not'; => means 'then'.

8. Conclusions

This work provides a method for classifying blockchains and their related crypto-assets based on technologic features, economic functions, and legal nature. Each configuration can be visually represented on a "map", depicting the blockchain through switching circuits and a logic formula.

Concerning the technologic characteristics of the blockchain, the map considers the following aspects: 1) the degree of decentralization (permissioned, hybrid, and permissionless) and their consensus protocols; 2) activities performed by the protocol (creation of a shared ledger, token creation, use of smart contracts; interoperability with other blockchains; based on a deterministic or probabilistic settlement system; 'forkable' or 'non-forkable'; capable of supporting certificatory or notarial functionalities); 3) type of governance (without any entity; with algorithmic governance structures embedded in the protocol or of a traditional type; associated with various voting mechanisms).

[51] MiCAR also covers many aspects that go beyond the scope of this paper, such as the rules for Crypto-assets Service Providers engaging in activities like trading, custody and administration, execution and transmission of orders on behalf of clients, etc.

Economic and financial characteristics go beyond traditional criteria of fungibility, transferability, and negotiability, including aspects that distinguish between "pure tokens" (without incorporated rights and primarily used for speculative purposes); financial and governance instruments (having a contract or implicit agreement that gives rise to a financial asset for one entity and a financial liability or equity and related possible future cash flows); instruments with other economic functions (such as non-fungible tokens and utility or management tokens); and, finally, instruments with monetary and payment functions.

Legal characteristics are outlined with particular attention to two jurisdictions (the European Union and the United States). Starting from recent regulation on crypto-assets (MiCAR), a broader and more granular "open and flexible" taxonomy is proposed to encompass various types of digital tokens currently observable, or others with different characteristics, using legal categories and possible economic-financial functions. An analysis of the legal concept of offering financial investment is conducted, attempting to bridge the gap between the continental approach and the common law approach adopted in the United States. In this context, the presence of a commitment of capital, with an expectation of profit by individual entrepreneurs having a common interest in an entrepreneurial initiative managed by third parties, becomes decisive.

Understanding the mechanisms of governance and "ordinary" or "extraordinary" management of the blockchain becomes crucial. In this regard, two case studies related to permissionless DLT (Ethereum and Polkadot) have been provided in the Annex, showing significant differences: the former associates decision-making bodies and functionalities that operate outside the main protocol (off-chain); the latter aims to develop algorithmic governance entirely embedded in the protocol (on-chain).

The intention of this work is to provide promoters of these initiatives with an easily applicable scheme in the illustrative prospectus (White paper) through a "visual map" and a logic formula. The approach is flexible, as a change in the structure of the blockchain or the economic and legal nature of a token can be represented by a variation in the formula. This facilitates an integrated comparison between technologic, economic, and legal profiles of various initiatives and their monitoring by regulators, even belonging to different jurisdictions.

References

Armas, A., and Singh, M., (2022, "Digital Money and Central Banks Balance Sheet", IMF working paper, WP/22/206, October.

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P. and Victor, F., (2023). 'The technology of decentralized finance (DeFi)', BIS Working Papers, No 1066.

Bains, P., (2022), "Blockchain Consensus Mechanisms: A Primer for Supervisors", IMF, Fintech Note 003, January.

Befani, G., (2019), "Contributo allo studio sulle criptovalute come oggetto di rapporti giuridici", in Il diritto dell'economia, 3/2019, pp. 381-421.

Befani, G., (2021), "Certezza, consenso e certificazioni informatiche: problemi e prospettive di un approccio giuridico al fenomeno delle tecnologie basate sui registri distribuiti," in, Il diritto dell'economia, 2/2021, pp. 77-114.

BIS (2023), The crypto ecosystem: key elements and risks, July.

De Bonis, R., Ferrero, G. (2022), Technologic progress and institutional adaptations: the case of the central bank digital currency (CBDC), Questioni di Economia e Finanza (Occasional Papers) n. 690, Bank of Italy.

ECB, (2020), "Report on a digital euro," October.

ECB – Bank of Japan, (2020), "Balancing confidentiality and auditability in a distributed ledger environment".

ESMA (2023), Decentralised Finance in the EU: Developments and risks, October.

FSB, (2020), Holistic Review of the March Market Turmoil, November.

Gola, C., Caponera, A., (2019), Policy issues on crypto-assets, LIUC - Università Cattaneo, Working paper n.7.

Gola, C., Sedlmeir, J. (2022), "Addressing the Sustainability of Distributed Ledger Technology," Questioni di Economia e Finanza (Occasional Papers) 670, Bank of Italy.

Gola, C., Cappa, V., Fiorenza, P., Laurino, F., Lesina, L., Lorizzo, F., Marcelli, G., (2023a), "The governance of blockchains and systems based on the distributed ledger technology", LIUC - Università Cattaneo, Working paper, April, n. 17.

Gola, C., Fiorenza, P., Laurino, F., Lesina, L., (2023b), "The use of logic circuits to classify blockchains", Questioni di Economia e Finanza (Occasional papers) No. 774, June (only in Italian), Bank of Italy.

Hafid, A., Senhaji, A., Samith, M., (2020), "Scaling blockchain: A comprehensive survey," Institute of Electrical and Electronics Engineering (IEEE), vol. 8.

IMF-BIS-ECB, (2015), "Handbook on securities and statistics".

ISDA, (2022), "Crypto-asset Risks and Hedging Analysis," May; BCBS (2022), "Prudential treatment of crypto-asset exposure" December.

Lamport, L., Shostak, R., e Pease, M. (1982), *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, 4:3, pp. 382-401.

Mendelson, E., (1970), "Boolean Algebra and Switching Circuits" McGraw Hill.

Micali, S. (2019), Algorand's Core Technology (in a nutshell), April: https://medium.com/algorand/algorands-core-technology-in-a-nutshell-e2b824e03c77.

Pappano, D., d'Atri, G., Befani, G., Zanardo, E., (2021) "Criptomonedas y valores digitales la difícil colocación sistemática y regulatoria del fenómeno entre la informática y el derecho", in Belando Garìn (cur.) La criptomonedas a debate, Thomson Reuters-Aranzadi, pp. 113-156.

Schär, F. (2021), Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review, 103(2), pp. 153-74.

Yaga, D., Mell, P., Roby, N., Scarafone, K. (2018), "Blockchain Technology Overview," National Institute of Standards and Technology, U.S. Department of Commerce, October.

ANNEX

Two Case Studies: Ethereum and Polkadot ([52])

Throughout the text, Ethereum and Polkadot DLTs have been mentioned several times. The reasons for selecting these two DLTs are as follows: Ethereum is the second most widely used network globally after Bitcoin ([53]), and it was chosen because its governance model involves a balance between on-chain and off-chain processes, like numerous other blockchains; Polkadot represents an example of a blockchain that aims to have a completely algorithmic governance.

A – Ethereum: it is an open-source computer project launched in 2015 with the goal of creating a fully programmable ([54]) public permissionless DLT (open in both writing and reading). Ethereum was designed as a "distributed computing system," not exclusively as a decentralized payment system; it was designed from the beginning to allow the execution of software in a decentralized manner (smart contracts).

Until 2022, Ethereum used a Proof-of-Work consensus mechanism. However, to contain the high computational and, consequently, energy/environmental costs, and to improve protocol performance and lower fees, there has recently been a transition to a more environmentally friendly and efficient Proof-of-Stake (PoS) protocol ([55]) . The planning and execution of this transition in Ethereum, called "the merge", were managed off-chain, analogous to the processes in Ethereum that govern the development and application of changes to the DLT's code.

The transition to the new consensus system required extensive preparation. It was necessary to ensure the robustness of PoW while achieving a more flexible and efficient system. The system used was a combination of introducing a security deposit (skin-in-the-game) and the random allocation of both tokens (rewards) and nodes with voting powers. Mining was replaced with forging, the PoS block creation process.

Nodes wishing to participate in the creation of transaction blocks were initially required to "lock up" a minimum of 32 Ether (ETH) (about 53 thousand euros at mid-May 2023) in the protocol itself as a guarantee of the proper performance of their validator role. Although it is possible to deposit more ETH than the minimum amount required, this does not increase a node's chances of being selected as a validator but only its potential reward. Validators are chosen using a random ("randomized") process, which contains concentration phenomena among a few entities. Every 12 seconds, a validator is elected to create a new block. The transactions in this block are further verified by a group of validators, also randomly selected, tasked with expressing a final "vote" on their validity. Blocks deemed correct by the majority of validators are then added to the blockchain, while other blocks are discarded.

The Ethereum upgrade required various interactions among stakeholders. The starting point was the formal proposal for modification (called Ethereum Improvement Proposal – EIP ([56])), which can be formulated and published on the web by any member of the Ethereum community ([57]). Before formally publishing the EIP, there was a discussion on the community ([58]) forum to exclude weak proposals or those already explored in the past. After passing the peer review phase, the proposal was formalized and screened by the community (including developers). The final version of the EIP was reviewed by protocol developers - the so-called "Core Developers" - and, after verification, included in an Ethereum network upgrade program. This governance model has the limitation of foreseeing long and uncertain processes with the risk of a blockchain fork. In fact, this occurred with the "merge" when a minority of nodes maintained the Proof-of-Work-based model, creating the minority network "Ethereum PoW."

Although the founder of the initiative, Vitalik Buterin, remains a charismatic figure, there is a significant difference compared to what is observed in traditional open-source projects, where often the founder continues to have substantial veto power over change proposals emerging from the community.

B – Polkadot: It is a protocol designed to facilitate interoperability between blockchains by sharing the same security mechanism. It also aspires to develop a fully algorithmic, open, and democratic governance structure where decision-making processes, voting mechanisms, and enforcement are executed on-chain. Polkadot would allow blockchains with different characteristics (e.g., based on PoW, PoS, PoA, permissionless, permissioned) to communicate with each other through connection to a central blockchain called the Relay Chain. The goal is to create a global ecosystem where every DLT-based project can interface securely and reliably due to the central role of the Relay Chain. To avoid excessive concentration of power while ensuring appropriate governance and control bodies, various solutions have been introduced, including the distinct assignment of voting rights for "ordinary" and "extraordinary" management of the DLT. Below are the essential lines of the project, still in development.

---

[52] For a more in-depth analysis of these two DLTs, refer to (Gola, et al. 2023b).
[53] For updated statistics, reference can be made to https://coinmarketcap.com.
[54] For this purpose, a model of a distributed virtual machine has been created among all nodes participating in the network, called the "Ethereum Virtual Machine" (EVM); to develop code for this virtual machine, specific programming languages have been developed (Solidity and Vyper). Among the most representative members of the developer group that conceived Ethereum, a prominent role is played by Vitalik Buterin, who is still one of the main leaders in the evolution of Ethereum, and Gavin Wood, who conceived the Solidity programming language and later promoted the development of the Polkadot blockchain.
[55] The upgrade process, quite elaborate, took several years to solve technologic problems and, above all, to find an agreement among the majority of network participants. It initially involved creating a separate network called the "Beacon Chain" with a PoS consensus mechanism; subsequently, the main Ethereum network ("mainnet") was unified with the Beacon Chain. The unification of the two networks allowed, in simplified terms, to resume the state of the first and the consensus mechanism of the second.
[56] EIPs are technical standards for preparing proposals related to protocol changes such as the implementation of new processes and features.
[57] The community includes all ETH holders. However, given the high technical level required to submit a well-made EIP, usually, most authors of EIPs are application or protocol developers.
[58] Ethereum Magicians Forum, https://ethereum-magicians.org.

The Relay Chain's consensus mechanism is entirely on-chain and involves the election of validator nodes responsible for block creation, known as Nominated Proof of Stake (NPoS). It is a Proof-of-Stake consensus algorithm, as potential candidates for the validator node position must lock up a certain amount of Polkadot's native tokens, called DOT, which will be returned to them at the end of their tenure, unless misconduct occurs, along with a reward for the work done. Unlike Ethereum, in addition to candidate validator nodes, there are also so-called "nominator" nodes, participating in the election of validators by financially supporting a set of candidates through a security deposit of a certain amount of DOT.

If the validators chosen by the nominator are indeed elected and produce at least one block, a portion of the validator's reward is retroactively given to the nominators. Validators are elected based on their stake (a function of the amount and time of token lockup) through an algorithm that ensures proportional representation of minorities (i.e., validators supported by fewer nominators), provided they are supported by a sufficient amount of DOT, and they remain in office for a defined period. This computationally expensive algorithm is executed on a blockchain external to the main one to avoid slowing down the block creation process. The presence of nominators ensures greater security and a more equitable distribution of decentralized voting rights in the participant community.

Regarding governance, a significant innovation introduced by Polkadot compared to other blockchains like Ethereum is the management of protocol changes through on-chain mechanisms. Changes to the Polkadot protocol can be proposed by any DOT holder or one of the two governance bodies, the Council and the Technical Committee (see below). Changes are voted on through an on-chain referendum mechanism ([59]). Referendums occur approximately every 30 days, with each associated with a single proposal. All DOT holders can exercise their voting rights by staking their DOT for a specified period to: i) support one or more proposals in the pre-referendum phase; only the proposal with the most support becomes the subject of the referendum; ii) participate in the referendum. The weight of the vote depends on the amount of DOT staked and the time it is decided to lock them up; this provides the possibility for nodes with few DOTs to increase the weight of their vote by extending the lockup period. It is also possible to cast a vote without staking anything, but in this case, the vote has very little weight. A node can also choose to delegate voting power to another node, and in this case, the staking of the delegating node adds to that of the delegated node.

As mentioned earlier, Polkadot has two governance bodies. The Council is a body composed of 13 DOT-holding users who remain in office for a predetermined period (13-26 weeks) and serves to represent "passive" nodes that do not actively participate in governance decisions. The Council has the power to propose referendums useful to the community, elect the technical committee, and cancel a referendum if 2/3 of the members agree. When Council members participate in a referendum regarding proposals they themselves formulated, their votes are considered on a per-member basis and not based on the DOT staked; this prevents members from having control over the approval of such proposals in referendums with low turnout.

The Technical Committee is tasked with identifying any technical issues within the system (e.g., security issues) and proposing emergency referendums to address them. Any group that has successfully implemented at least part of the Polkadot protocol can run for membership in the Technical Committee, and such groups can be added or removed from the committee with a majority vote from the Council ([60]). An emergency proposal, to proceed to the referendum phase, needs the approval of at least 3/4 of the Council or at least 2/3 of the Technical Committee. The Technical Committee also has the power to cancel a referendum with unanimity.

Currently, it is possible to delegate one's voting power to only one third party – differentiating the delegate based on the importance of the referendum (so-called Multirole Delegation). In addition, referendums can be cancelled if the network of nodes votes in favor of elimination. The Technical Committee will be replaced by the Fellowship, which will represent the technical coordination body of the protocol and will have less restrictive access conditions for developers who want to join, thus expanding the pool of potential participants. Each member of the Fellowship will be assigned a level of expertise that will influence the weight of their vote. However, the methods by which levels will be assigned have not been defined, considering that the assignment must be done in such a way that the Fellowship or small groups of developers do not have voting power that allows them to control the entire network.

[59] Alternating choice between the public proposal and the most supported Council proposal.
[60] Any DOT-holding node can apply to be a Council member, and the election takes place in the same way as that of validators, so it occurs on-chain, and users vote.