

Policy issues on crypto-assets

Carlo Gola
Andrea Caponera

Policy issues on crypto-assets

Carlo Gola*, Andrea Caponera**

Abstract

This paper describes the economic characteristics of crypto-assets and the regulation of the exchanges and custodian wallet providers adopted in various jurisdictions. The possible accounting and prudential treatments are then analysed. The paper provides a taxonomy of DLT digital tokens based on mutually exclusive classes. Bitcoin belongs to the class of private digital tokens with no underlining claim or liability against an issuer, exchangeable at a floating rate, which operate through an electronic protocol called permissionless distributed ledger technology (DLT). The literature on the subject shows that this type of crypto-assets do not fall within the category of money and financial instruments. The instability of their price must be considered when evaluating these instruments from an accounting and prudential point of view. The paper describes the basic features of initial coin offerings (ICOs), smart contracts, and other related aspects.

JEL Classification: E40, E42, E51, G20, G21, G28, K20, M40.

Keywords: crypto-assets, digital tokens, initial coin offerings, accounting standards, prudential regulation.

1. Introduction¹

This paper describes the economic characteristics of crypto-assets such as bitcoin and the regulation of the gatekeepers (e.g. custodian wallet providers, trading platforms and centralized exchanges) adopted in various jurisdictions. This type of crypto-assets (usually called virtual currencies or cryptocurrencies) belongs to the class of private digital tokens not representing any financial claim or liability against an issuer, exchangeable at a floating rate, which operate through an electronic protocol called permissionless distributed ledger technology (DLT). As we will see below, the literature shows that the price of virtual currencies is not only highly volatile, but is also – according to some authors (e.g. Garratt and Wallace, 2018) – intrinsically unstable, undetermined or characterized by a possible zero-price equilibrium. In fact, their price is not anchored to any fundamental economic factor, or to trust in a public authority².

* Bank of Italy, Regulation and Macroprudential Analysis Directorate. Email carlo.gola@bancaditalia.it

** Bank of Italy, Regulation and Macroprudential Analysis Directorate, Accounting and Financial Reporting Division. Email andrea.caponera@bancaditalia.it

¹ The opinions expressed are those of the authors and do not necessarily reflect those of the Bank of Italy. Any errors or inaccuracies are attributable exclusively to the authors. The authors would like to thank: Fabrizio Borselli, Jon Frost, John Kiff, Carlo Lanfranchi, Antonio Marrone, Raffaella Menzella, Pasquale Munafò, Alessandro Negri della Torre, Andrea Pilati, Antonio Renzi, Giovanni Rumolo, Lidja Schiavo and Prof. Ivan Visconti for their useful suggestions. The authors are also grateful to: Stefano Bernardi, Zeeshan Feroz, Tomoya Yamashita, Caroline Le Moign and Martin Schmalzried, for the useful information provided. A special thanks goes to Paolo Angelini, for his thoughtful comments, as well as to Giovanni Tirino, Michele Lanotte and Marco Giornetti for some suggestions relating to the section on prudential treatment. The paper is a revised version of Caponera and Gola (2019).

² The analysis of the financial stability risks related to crypto-assets are beyond the scope of this paper. On these aspects see: FSB (2018a,b,c).

Having an intrinsically unstable price, virtual currencies are not well suited for performing the traditional functions of money. Based on these considerations, the paper analyses the possible accounting and prudential treatments within the current framework, about which significant uncertainties remain. The paper provides a taxonomy of the various types of DLT digital tokens (of which virtual currencies are a subset), and describes the basic features of initial coin offerings (ICOs), smart contracts, and other related aspects. The provided taxonomy helps to unambiguously identify different types of payment tokens, security tokens and utility tokens, and distinguish them from crypto-assets such as bitcoin. This is a pre-condition to any form of possible regulation.

At the international level, the policy options relating to crypto-assets have focused on three alternatives: isolate, regulate or integrate.³ The first alternative would prevent crypto-assets from being part of banking and financial intermediation; the second option would result in issuing a sector-specific regulation; and the third option would be based on an adaptation of the existing regulatory framework, so as to accommodate these new instruments. Overall, there is currently no consensus among the policy makers as to which of these options is advisable⁴. However, most regulatory bodies and competent authorities share the common view that - while deeply interlinked - the assessment of crypto-assets should be complemented by a specific scrutiny of appropriate standards for the underlying technology (the DLT), which deserves its own assessment. These two assessments must consider, respectively, on the one hand the economic and legal nature of DLT digital tokens (functionalities, existence of legal rights, negotiability and properties of the possible equilibrium or equilibria), on the other hand the governance, robustness, scalability, interoperability, and efficiency of the underlining protocol including the type of consensus algorithm.⁵ The crypto-assets such as bitcoin not only are often used for illicit activities, but are also a source of negative externalities due to the inefficient use of electricity needed by the mining process. If the DLT were able to solve the problems mentioned above, it could have relevant potential,

³ See: Carney (2018), p. 10. For a discussion of the three proposed policy options, see: Demertzis and Wolff (2018), pp. 12-13; Amstad (2019); Blandin *et al.* (2019), pp. 41-42 (with a distinction between bespoke regulation and bespoke regulatory regime); Himino (2018), which considers the following options: prohibit, regulate, monitor or ignore. See also: Landau, J. and Genais, A., (2018); Banque de France (2018).

⁴ Recently the FSB has published a report on crypto-assets, presenting an overview of the work underway by various standard setting bodies and international organizations, on possible regulatory approaches and potential gaps. It notes that views differ among FSB members on whether an appropriate multilateral response requires more coordination among international organisations and, if so, the priority that should be given to it at the present time (FSB 2019c, p. 9).

⁵ This second set of attributes, which are mainly technological, are outside the scope of this paper. On these aspects, see: ESMA (2017); CEN and CENELEC (2018); EU Blockchain (2019); Auer (2019).

especially for decentralized cryptographic archives and networking, in the use of smart contracts, the issuing of security and payment tokens (Catalini and Gans, 2018).

The key points of the paper are:

1. Digital tokens operating through DLT are a highly heterogeneous class: it is important to distinguish – from an economic and regulatory point of view – different types of digital tokens. This paper identifies – differently from the current practice – granular, mutually exclusive digital token classes. In particular, the virtual currencies such as bitcoin, Ether, etc. are clearly distinguished from the other types of digital tokens, including: *payment tokens*, issued by a private legal entity one-to-one with fiat money; *utility tokens*, used to unlock the utility of its related applications or to represent (in our definition) non-transferable and non-negotiable economic rights; and *security tokens*, which include all transferable and negotiable digital tokens representing economic, governance, or financial rights. In our taxonomy the discriminating factors are the negotiability of the instrument and the presence of at least one economic or legal right. This implies a clear definition of negotiability and of trading venue.
2. In our view, if a digital token represents economic or financial rights and is transferable or negotiable, it should be regulated in order to contain possible market failures such as the effects of information asymmetries or market manipulations. It is important to avoid regulatory arbitrage, particularly at cross-border level, while preserving financial innovation.
3. Among the three possible policy options mentioned above (isolate, regulate or integrate), one policy alone will not be appropriate for all types of digital tokens. Here, we argue that appropriate policy responses must be differentiated depending to the characteristics of DLT digital tokens. In addition, the policy makers should be cognizant that the technology is not neutral: public DLT (or *permissionless* DLT), where no entity is accountable, especially if associated with the use of decentralized exchanges (DEXs), could favour the creation of a monetary and financial system, parallel to the traditional one, that is difficult to control; such a system would have considerable drawbacks from a financial stability point of view.
4. In many jurisdictions, the firms offering services related to crypto-assets are regulated for anti-money laundering and contrasting the financing of terrorism (AML/CFT) purposes. The use of DEXs makes it difficult to identify and verify

the customer and the beneficial owner of the crypto-asset. This can give rise to forms of regulatory blind spots.

5. From an accounting prospective, an analysis of the international accounting standards (IAS/IFRS) excludes the possibility of considering bitcoin-like crypto-assets as cash, cash equivalent or financial instruments. The existing accounting rules seem to leave room for the use of the accounting categories of intangible assets or inventories. The International Accounting Standards Board (IASB) has decided to consult the IFRS - Interpretation Committee⁶, the only body with the task of providing authentic interpretations of the IAS/IFRSs.
6. In the European Union, the EBA (2014) discouraged intermediaries from buying, holding or selling virtual currencies. We support this view. However, the current EU law does not prohibit financial institutions from holding or gaining exposure to virtual currencies. A clarification about the prudential treatment of these instruments is therefore necessary. The Basel Committee has yet to take a formal position: should the option of considering them intangible assets prevail, the intermediaries should then deduct them entirely from their own highest quality regulatory capital (CET1).
7. Finally, we stress that virtual currencies such as bitcoin, in our opinion, should not be used as underlying assets for financial instruments or to fund initial coin offerings (ICOs). This is not so much because of their high volatility, as their absence of clear intrinsic value, legal rights or public trust, the indeterminacy of their price, and the non-controllability by the regulator for AML/CFT purposes. Different - and in our opinion more acceptable - is the use of *fiat-backed stable coins* for these purposes.

The paper is organized as follows: first, an analysis of the economic characteristics of crypto-assets is presented (Section 2). Subsequently, a description of some critical aspects related to the crypto-exchanges and wallet providers, as well as the problem of pseudo-anonymity is explained (Section 3). In the following section, the paper illustrates the main regulatory initiatives adopted in the various jurisdictions (Section 4). Once these aspects have been clarified, those relating to the accounting (Section 5) and prudential (Section 6) treatments of the crypto-assets are then considered. Section 7 provides some concluding remarks.

⁶ See IASB (2019a and 2019b).

2. Economic aspects

A DLT digital token is a digital representation of (perceived or inherent) value or legal rights, which make use of cryptography and DLT (see Glossary). In the present paper we deal mainly with a subset of DLT digital tokens called virtual currencies, while providing elements to distinguish them from other types of digital tokens (see Box 1).⁷ According to the EU legislation, “*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”⁸.

A bitcoin-type virtual currency is not a liability of an institution; it is not a coin with an intrinsic value, like gold or silver.⁹ None of the typical functions of money¹⁰ are fully satisfied by bitcoins or similar cryptocurrencies: to date, bitcoin has been used as a medium to exchange goods and services only to a very limited extent.¹¹ Transactional costs and high price volatility make virtual currencies unsuitable for these functions. Having said that, with the advent of various forms of digital currencies, the functions of money can be separated. A payment token can perform the role of a vehicle currency to transfer remittances abroad. Moreover, the blockchain of bitcoin can work (though very inefficiently) as a platform for the provision of many utilities.

Some supporters of virtual currencies, inspired by the ideas of F.A. von Hayek,¹² believe that these currencies could, in the future, abolish the public monopoly of money in favour of a system based on competition between private currencies. In particular,

⁷ The literature on the topic uses the following terms: virtual currency, digital currency, crypto-currency, virtual assets and crypto-assets. They are all digital tokens that represent value in an encrypted and electronic way and that operate using DLT technology. By bitcoin-type virtual currencies, we mean all digital tokens that use a protocol based on the following principles: 1) open-source (the code can be read, modified, copied and exchanged by everyone.); 2) permissionless (there is no manager that can restrict access to the network); 3) no-censorship (nobody is able to prevent the confirmation of a valid transaction); 4) irreversible (it is impossible to change a transaction once it is finalized); 5) pseudonymous (user identification is not required but all transactions are public); 6) fungible (all digital tokens are equal and expendable, and 7) limited (the supply of digital tokens is limited by the protocol and cannot be changed). For a description of the open-source features of the bitcoin protocol, see Van Valkenburgh (2018).

⁸ See: Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (or AMLD5), art 1. (2 (d) 18).

⁹ Gold is outside money. Unlike inside money, it does not have a corresponding liability (therefore it does not disappear upon consolidation). For a discussion of this aspect in relation to central banking digital tokens, see Prasad (2018).

¹⁰ The well-known functions of money are as: a unit of account (a numerary accepted by all); a medium of exchange (tool to avoid multiple barter transactions); and a store of value, stable over time and space (non-interest bearing instrument aimed at preserving purchasing power over time while maintaining the characteristics of maximum liquidity and able to represent value in a non-corruptible manner) (J.W. Jevons, 1875).

¹¹ On theoretical and empirical factors that explain the limited use of bitcoins as a medium of exchange, see: Athey, *et al.* (2016); Jonker (2018); Luther (2013); and He, D. *et al.*, (2016). Quotations of virtual currencies are available here: <https://coinmarketcap.com/>; for a Volatility Index see: <https://www.buybitcoinworldwide.com/volatility-index/>.

¹² See: von Hayek F.A. (1990), first edition 1976.

they argue that virtual currencies are still in a nascent phase, but that they will be accepted as money by a community over time. However, economic theory and historical experience (Eichengreen, 2019) seem to suggest that this will not be the case due to the absence of two fundamental elements: a law that guarantees their integrity and imposes their general use, often linked to their acceptability as an instrument for paying taxes; and a central trusted authority that - thanks to its reputation and through monetary policy - in a certain sense, coordinates the market, setting an anchor on inflation expectations. Obviously, even traditional currencies can - under certain circumstances - be subject to significant changes in the exchange rate or purchasing power. However, when these changes become particularly large and persistent, the currencies in use tend to be rejected by the public in exchange for more stable foreign currencies (as sometimes happens in emerging countries). In extreme situations of hyperinflation, a barter-based economy often returns to use. It is equally clear that a crypto-asset can be used to buy a good or a service, however this does not mean that it has all the requirements of traditional money.

Box 1 – Types of DLT digital tokens: a functional approach¹³

A DLT digital token is a digital representation of an interest, a (perceived or inherent) value, a right to receive a benefit or perform specified functions. All digital tokens here considered make use of cryptography and DLT. A DLT digital token sometimes incorporates financial rights or rewards (see Contractual or legal rights in the Glossary). This taxonomy identifies mutually exclusive classes of DLT digital tokens, some of them having multiple economic functions:¹⁴

DT1 – virtual currencies: these digital tokens (for example bitcoin) have no incorporated legal rights or promises.¹⁵ They do not represent a financial claim on, or a

¹³ A possible, alternative, approach is based on technological differences (for instance the use of private v. public DLTs; different consensus algorithms (proof of work v. proof-of-stake), etc.. As extensively discussed in the paper, a robust technology is a pre-condition for the development of all types of digital tokens. The competent global standard setters should promote appropriate standards and good governance. For instance, private DLT or blockchain sponsored by an entity are preferable because the regulator has the possibility to interact with the promoter (or promoters) of the initiative.

¹⁴ This taxonomy - based on economic, not legal principles - has some affinities, but also significant differences, with that proposed by Security and Markets Stakeholder Group (2018), ESMA (2019), EBA (2019), Blandin *et al.*, (2019) and FCA (2019). In particular, it is more granular and based on mutually exclusive classes of digital tokens. On the subject of classification and regulatory implications, see Maas (2019). This paper provides a useful analysis on the stylized issues discussed in our taxonomy. Are also useful: Hacker and Thomale (2018); Rohr and Wright (2018); Soleranski (2018); Bonneau (2018); Burnie et al. (2018); Bech and Garratt (2017); Van Valkenburgh (2018); SEC (2019).

¹⁵ Nakamoto (2008), defines an electronic coin as “a chain of digital signatures”, (p. 2). The users do not have any contractual or legal right; they only possess a password which allow them to access a set of information saved in an electronic database. Whether some crypto-assets fall into the category DT1 remains unclear (see for example <https://xbt.net/blog/is-ripple-xrp-a-security/>).

liability of, any entity. They are, however, negotiable and exchangeable into legal currency (fiat money) or other virtual currencies at a floating exchange rate. Virtual currencies are neither e-money, as defined by the EU E-Money Directive (EMD2), nor “payment instruments”, as defined by the EU Payment Services Directive (PSD2), since there is no payment service provider (art. 4(14)) (see Maas, 2019, p. 55). If the DT1 were associated with legal rights or promises, they would be classified in the categories, shown below;

DT2 – payment tokens: instruments that are designed only to replicate the functionality of the money, and keep a fixed value. They are:¹⁶

a) *stable-coins*: they are issued by a private entity at a fixed price with fiat money. If (and only if) they are one-to-one with a unit of fiat money (or a legally equivalent type of funds) segregated in an account of a regulated entity, they are e-money settled through a DLT (EBA 2019) (see Electronic money in the Glossary for more details). We call this class of token *fiat-backed stable coins*. The market is currently producing a variety of digital tokens that are not one-to-one with fiat money (or a legally equivalent type of funds).¹⁷ They are not in our view electronic money;

b) *central bank digital currencies*: a possible new form of central bank money denominated in an existing unit of account and is a central bank liability.¹⁸;

c) *non-convertible digital coins*: they are digital tokens that promote bartering. They give the right to exchange goods or services among the participants in the circuit.¹⁹ They are distinguished from other DLT digital tokens because they are not exchangeable with a legal currency or with other virtual currencies.

DT3 – security tokens: also called *investment tokens* or *asset-backed tokens*, they are transferable and negotiable.²⁰ They are typically, but not necessarily, offered

¹⁶ For more information on DT2, see: the Bank for International Settlements (BIS) (2018); Bech and Garratt, (2017); Garratt, (2016); Bordo and Levin (2017); FCA (2017); He, *et al.* (2017); Pinna and Ruttenberg (2016); Mills *et al.* (2016).

¹⁷ Some of these DLT digital tokens are backed by crypto-assets, real assets or by a pure algorithm that promises to stabilize the price against fiat money (for instance with respect to the dollar). In our view these tokens should be classified as DT3. On various types of stable-coins, see: <https://coincentral.com/types-of-stablecoins/>. On the financial stability implications of stable-coins, see Adrian (2019).

¹⁸ Several central banks are actively exploring the issuance of central bank digital currencies (CBDCs) based on DLT or similar technologies. For a comprehensive survey of central bank digital currencies, see Prasad (2018). See also CPMI (2018); Panetta, (2018b); Bech and Garratt (2017); Berentsen, A. and Schär (2018); Barontini, C. and Holden, H. (2019). As Garratt (2016) notes, describing the Fedcoin project, for each digital central bank token issued and managed by DLT, a corresponding amount of monetary base would be removed, which would therefore remain unchanged.

¹⁹ Similar to this class of digital tokens are local moneys. Local moneys, however, although digital, do not use DLT. Note that European legislation does not consider either local moneys, or the digital tokens used in online gaming as virtual currencies (see Directive AML/CFT, 2018/843). The economic rationale of these digital tokens is to favour coordination or to exploit network economies between economic agents that share the same values or interests.

²⁰ The legal and regulatory status of security tokens remain uncertain, despite recent clarifications from various bodies. In the United States, security tokens are considered an “investment contract” if there is no direct involvement of the

through an Initial Coin Offering (ICO) or by a Security Token Offering (STO) (see Glossary, “Initial Coin Offerings”). The DLT can enable existing assets to be transferred and settled using cryptography (a phenomenon called “tokenization”). In the taxonomy proposed here, they must give one or more economic or financial rights, or promises (by an entity or by a group of people) to the person holding them, such as: rights on shares of capital, shares of funds or on standardized tradable goods (commodities); voting rights or participation in the project, dividends, cash flow rights, and transferable and negotiable rights of use (administrative rights). Security tokens seem to be similar to dematerialized securities or financial products such as derivatives which are, however, transferred via DLT and negotiable against fiat money.²¹ Security tokens having as underlying only virtual currencies (DT1) remain in class DT1. DLT digital tokens having more than one function (*hybrid tokens*) remain in class DT3.²²

DT4 – utility/consumer tokens: in our taxonomy they are non-transferable, and non-negotiable digital tokens that only offer administrative or utility rights, such as access to a platform or a facility. In some cases (called “app-coins”) these utility tokens only provide the capabilities to use the platform or the decentralized open-source protocol. The utility tokens are used, for instance, to decentralize on-line P2P services.²³ Unlike DT2c, they can be purchased (directly or associated with the sale of goods or services) in exchange for fiat money or other virtual currencies. If the utility token granted the holder any rights (for instance the right to use a platform) but were transferable, negotiable or capable of being negotiable on a secondary market (or became such during their life-cycle), they would lose – according to our taxonomy – the utility tokens feature and become security tokens (DT3)²⁴. For a slightly different position, see FCA

digital token subscriber in the project, which is left solely (or mainly) to the promoters of the initiative (see: SEC (2019); Glossary “ICOs and the Howey test”). In Europe, the leading criteria are the standardization, transferability and negotiability of digital tokens. In both jurisdictions, the financial information asymmetries are the fundamental reasons behind the necessity to regulate (Hacker and Thomale, 2018; ESMA, 2019). Moreover, an asset is negotiable if it has the characteristics for being traded on a trading platform (transferable, fungible, standardized and so on). MiFID2 defines transferable securities as follows: “classes of securities that are negotiable on the capital market, with the exception of instrument of payment” (Article 4 (1) (44)). See Glossary: Financial instrument (normative definition). The European Securities and Markets Authority (ESMA) has asked the European institutions (Parliament, Commission and Council) to clarify whether security tokens can be considered as transferable securities under the MiFID2 Directive or other directives and whether the platforms that exchange them are equivalent to Organized Trading Facilities (OTF) or Multilateral Trading Facilities (MTF) (ESMA, 2019).

²¹ For a description of the formidable set of problems that the financial market regulator needs to deal with in this new class of financial assets, see: Brummer *et al.* (2018); Wright, A., De Filippi, P. (2019).

²² As rightly underlined by Maas (2019), “it is more appropriate to [bring] hybrid tokens under the umbrella of security tokens than under any of the other main categories of tokens” (p. 25).

²³ Decisions over how to write and rewrite that software can be made through ex-ante specified voting rules (on-chain governance). Moreover, all of these user interactions (whether voting, uploading, viewing, curating, providing infrastructure or developing the software) are recorded (perhaps using a pseudonym for privacy) and the identities of contributors are validated, (see, Van Valkenburgh, 2018, pp. 41-42).

²⁴ Moreover, as underlined by Maar (2009), “a substantial amount of utility tokens confer a right to claim services from the issuer in return for the token. In this sense, the token can be seen as a sort of liability towards the token holder, and it could arguably be deemed a form of securitized debt” (p. 50).

(2019, p. 29). For the FCA a token that does not confer any financial right but is tradable on a secondary market is a utility token.²⁵

In summary²⁶

DLT digital tokens outside the regulatory perimeter

- Virtual currencies (DT1), without embedded rights, such as bitcoin or Ether;
- All DLT digital tokens (including “native” ICOs tokens) having DT1 as underlying;
- DLT digital tokens not exchangeable (DT2c) against currencies (fiat money) or other virtual currencies;
- DLT utility tokens which, despite having an incorporated right, are not transferable and negotiable (DT4);

DLT digital tokens within the (current or *ad hoc*) regulatory perimeter²⁷

- DLT digital tokens that are collateralized one-to-one with a currency (fiat money or equivalent legal forms; central bank money) are “electronic money” or “money” (DT2a; DT2b);
- All other types of transferable and negotiable DLT digital tokens (including hybrid tokens) with incorporated a governance, economic or financial rights are “security tokens” (DT3);
- All DLT tokens usually defined as “utility tokens” representing at least one economic or administrative right and that are transferable and negotiable are - according to this taxonomy - “security tokens” (DT3).

2.1. Short survey of the literature

The literature on the subject concurs on the fact that bitcoin or similar crypto-assets are characterized by extreme volatility and price jumps or discontinuities. In particular, several authors believe that this is due to the fact that their price is not explained by any fundamental economic variable, such as purchasing power parity or uncovered interest rate parity (Yermack, 2013; Lo and Wang, 2014; Ciaian, *et al.*, 2016). Having neither intrinsic value, nor a central authority that preserves its stability, price dynamics are mainly based on self-fulfilling expectations. The equilibrium price seems to be indeterminate or equal to zero (Garratt and Wallace 2018).

According to Biais *et al.* (2017), while the strategy of mining the longest chain proposed by Nakamoto (2008) is indeed an equilibrium, there are other equilibria due to blockchain forks that cause potential instability²⁸. Moreover, the negative externalities arising in proof-of-work consensus algorithms cannot easily be addressed through a Pigovian taxation, given the international decentralization of the mining process. This suggests moving from proof-of-work to other algorithms, such as the proof-of-stake. In

²⁵ It is worth mentioning that the FCA defines three classes of digital tokens: exchange tokens (a means of exchange not issued by a central authority and outside the regulatory perimeter); security tokens (meeting the definition of the Specified Investments as set out by the FSMA (2000) – Regulated Activity Order - (RAO)); and utility tokens (that do not grant holders rights as described by the RAO and might meet the definition of e-money in certain circumstances and, as such, are regulated). See also: HM Treasury, FCA, and Bank of England, (2018).

²⁶ We are here considering only a possible regulation on the DLT digital tokens: all exchanges and custodian wallet providers need a regulation (see Section 4).

²⁷ A per-condition is the development of a robust, sustainable, scalable, accountable, interoperable and efficient DLT and a clear, legal definition of token negotiable on a venue platform.

²⁸ For a simple description of non-malicious forking, see Van Valkenburgh (2018), pp.9-11.

this case the coordination on blockchain updates is enforced by ensuring that transaction verifiers pledge their coin holdings as guarantees that their payment confirmations are accurate. Under this configuration without miners, is not necessary to use computing power and energy to propose blocks for consensus. However, according to Biais *et al.*, the proof-of-stake system is exposed to the same coordination problems as proof-of-work, since in both protocols participants must choose which blocks to accept and are rewarded when the others agree with their choice. In addition, proof-of-stake comes with its own problems, in particular the “nothing-at-stake” effect: a participant can stake his cryptocurrency units on different branches, thus hindering the emergence of a consensus. As observed by Biais *et al.* this points to a major dilemma for distributed ledgers: on the one hand, the anonymity and decentralization of public blockchains expose them to co-ordination failures and externalities, on the other hand, private blockchains can restore coordination and internalize externalities, but only to the extent that they involve the intervention of a centralized authority, which goes against the fundamental motivation for blockchain.

Abadi and Brunnermeier (2018) explore further the above aspects in a general model of ledger competition. In particular, they study more deeply the trade-offs (in public and private blockchains) between correctness, decentralization, and cost efficiency (the blockchain trilemma). This is related to the fact that a centralized record-keeper extracts rents due to its monopoly on the ledger. Its franchise value dynamically incentivizes correct reporting. Blockchains drive down such rents by allowing the free entry of record-keepers and the portability of information to competing forks, at the cost, however, of a pure waste of resources. Blockchains therefore sacrifice cost efficiency for decentralization and more robust correctness.

The analysis proposed by Budish (2018) is in line with those who think that the anonymous, decentralized trust enabled by the Nakamoto (2008) blockchain, while ingenious, is expensive and potentially unstable. The paper concludes that blockchain is vulnerable to collapse if either conditions change in the specialised chip market or if the Bitcoin blockchain becomes economically important enough (e.g. if it became a store of value akin to gold) to tempt a saboteur. This suggests – observes Budish – that there are intrinsic limits to how economically important bitcoin can become.

Transaction fees, paid by the bitcoin users and profit-seeking miners who maintain the blockchain infrastructure, are analysed by Huberman *et al.* (2017) in an equilibrium of

congestion queueing model, where a certain level of congestion is imperative to raise sufficient revenues.

Some authors have tried to show that the price of bitcoin is similar to that observed for speculative asset bubbles (Eng-Tuck and Fry, 2015; Cheung, *et al.*, 2015).²⁹ The price is also influenced by news deriving from market events, including cyber-attacks, market manipulation and sudden changes in expectations (Wang and Vergne 2017, Gandal, *et al.*, 2018; Gronwald 2014). The volatility could also reflect international deviation from the law of one price (Aloosh 2017). This gives rise to arbitrage opportunities, that are larger across than within the same country (Makarov and Scholar, 2018). Hale *et al.* (2018) show that the introduction of bitcoin future trading on the Chicago Mercantile Exchange allowed pessimist to enter the market, which contributed to the reversal of the bitcoin price on December 2017. Auer and Claessens (2018) show that the prices, volumes and user bases react to news about possible regulatory actions.

Other authors, following a different approach, have tried to estimate the role of structural factors using proxies of the governance of virtual currencies as explanatory variables (Hsieh *et al.*, 2018; Wang and Verge 2017). Recently, Pagnotta and Buraschi (2018) have proposed a model that simultaneously identifies the demand and supply of bitcoins in a fully decentralized network economy. The authors show that there are two equilibria. In the first, the bitcoin price is zero. It corresponds to the situation in which the degree of aversion to the rules (censorship aversion) and/or the degree of trust in the blockchain protocol are null. In the second, the price is positive and growing in its degree of trust, which in turn increases in relation to the degree of participation in the network. The price, however, is highly volatile: for example a demand shock deriving from an expected change in the use of the network following an exogenous event, leads to a high variability in the price. The latter does not depend on speculative bubbles, but on the presence of significant non-linearities in the model. Their work does not consider the demand of bitcoins for speculative reasons.

Auer (2019) explores the critical limitations of the bitcoin blockchain, namely that the proof-of-work can only achieve payment security if mining income is high, but the transaction market cannot generate an adequate level of income. As a result, liquidity is likely to fall dramatically as the block rewards are phased-out. Given these considerations, the paper concludes with a discussion of different technological solutions, such as the Lightning Network that, in principle, could improve the

²⁹ For a different view, see, J. Cochrane (2017).

economics of payment security while mitigating the scaling limits of the traditional blockchain where transactions are on-chain (see also Poon *et al.*, 2016). Other alternatives have been put forward: as mentioned before, the most important one is to replace proof-of-work by proof-of-stake. Replacing costly computations by an essentially resource-free betting game has, however, the caveat of a lack of clear criteria for distinguishing between different blockchains with alternative payment histories (the “nothing-at-stake” problem mentioned before).

The literature seems to agree that the purchase of these instruments is done mainly by betting on the expectations of other economic agents, as is the case with many financial instruments. This is a well-known feature, also highlighted by Keynes in a famous passage of his *General Theory*.³⁰ However, in the case of bitcoin (or similar virtual currencies) this random component is not only dominant, but is also extended to the underlying production mechanism.³¹ In particular, the *mining* process is nothing but the effort of solving a cryptographic puzzle (see Glossary) that makes it possible to win bitcoins. Given these characteristics, there could be a decision to regulate the exchanges of virtual currencies (DT1 in our taxonomy) through a license issued by the gambling authorities.³² In Europe, for instance, the European Commission has been promoting a regulatory framework for online gaming aimed at protecting consumers since 2012, encouraging responsible advertising, preventing fraud, money laundering, cyber-attacks and so on. This approach has the advantage of keeping virtual currencies and the regulated financial sector separate and, at the same time, protecting the consumer and fighting against the illegal use of these instruments.

Crypto-assets used for underlying financial instruments - Market information shows that some financial instruments have been developed using the following as underlying virtual currencies: futures, speculative mutual funds, funds based on exchange traded notes (ETNs) and contracts for differences (CFDs). These are sporadic cases with very modest market volumes so far. The European authority ESMA is discussing the topic, but it seems oriented to not authorizing the production of funds for the retail sector based on cryptocurrencies.³³ In the US, the Security Exchange Commission (SEC) believes there are still significant issues that need to be addressed before products

³⁰ See J. M. Keynes (1936), Chapter 12, pp. 154-55.

³¹ The market price of crypto-currencies “is like lottery tickets that pay off in a dystopian future” (K. Rogoff, 2018), while the proof-of-work “is mathematically equivalent of rolling a dice” (R. Auer, 2019).

³² For the requirements for obtaining a gambling license, see: European Commission (2013), p. 3). See also: European Commission (2012); Council of the European Union (2012).

³³ Indeed, even in the presence of increasing transaction volumes, it seems difficult to believe that the characteristics described above would allow bitcoin (and similar crypto-assets) to meet the criteria required by UCITS with reference to eligible assets. See: UCITS Eligible Assets Directive (Article 1 (8) and Article 19 (1) of Directive 85/611/EEC).

such as ETFs can be offered to the retail sector.³⁴ Recently, the German authority BaFin has authorized a security token denominated in the crypto currency Stellar (Mazières, 2016) and funded by fiat money or other crypto currencies. The security token was launched by a crowdfunding company.

The fundamental difference between a virtual currency and a financial product based on this instrument is that it uses an undefined and intrinsically unstable economic object to produce a fully regulated financial instrument. This phenomenon is worrying, in our opinion, since a possible collapse of the bitcoin system or similar crypto-assets would drag the financial instruments on which they are based with it. Moreover, from a macro-prudential standpoint, it would increase the interconnectedness between these highly volatile and ungovernable assets and the traditional intermediation channels.

3. Virtual currency exchanges and wallet providers

An exchange is a platform that allows virtual currencies to be traded with traditional money or with other virtual currencies. Generally, the exchanges accept credit cards, bank transfers and prepaid cards. Most of the exchanges are centralized, but there are also decentralized exchanges (DEXs), i.e. applications available on the internet that exchange virtual currencies at P2P level (see below). Custodian wallet providers are companies that sell applications to store, transfer, and manage virtual currencies. The electronic wallets can be saved online (“hot storage”) or offline (“cold storage”). In the first case, the wallets are managed and stored on behalf of the client by specialized companies; in the second, they are saved remotely, for example on a PC or on the user’s smart-phone. It should be noted that if users operate through a wallet provider as custodian/manager of their password (private keys), they can lose all their digital tokens with a single event (a cyber-attack) against the platform. This risk (single point of failure) of course does not occur if the users manage the private keys themselves.

The traceability of transactions and users - The blockchain enables complete traceability (even backwards³⁵) of all transactions but makes it difficult - compared with traditional electronic payment methods - to identify the subjects that make transactions

³⁴ In a letter from the SEC to a subject who applied to register an ETF in cryptocurrencies the authority posed the following very relevant questions: “Would funds have the information necessary to adequately value cryptocurrencies or cryptocurrency-related products, given their volatility, the fragmentation and general lack of regulation of underlying cryptocurrency markets [...]? How do funds develop and implement policies and procedures to value, and in many cases fair value, cryptocurrency-related products? How would funds be used for accounting and valuation policies? For example, when the blockchain for a cryptocurrency diverges into different paths (i.e., to “fork”), which could result in different cryptocurrencies with potentially different prices” (see SEC (2018), p.2).

³⁵ For this reason, blockchain technology poses complex problems in terms of compliance with the personal data management rules, in particular the right to be forgotten, recently introduced by the General Data Protection Regulation (GDPR); see EU Blockchain (2018).

(pseudo-anonymity). In fact, the transactions with blockchain make it possible to identify the wallet owners if and only if the users turn to a specialized company that manages the wallet on the behalf of the client and if that specialized company is regulated. This does not happen if the users download the app³⁶ from internet and manage the wallet themselves, or if they buy the virtual currencies directly from a miner. In this case the traceability of the subjects would only be possible through investigations, for instance by the postal police on the IP addresses associated with the wallets. If the users operate through platforms located in jurisdictions where these entities are not regulated, significant traceability problems arise. There are also applications available on internet (anonymizers, mixers or tumblers) that allow the chain of transactions carried out on the blockchain to be obscured (Heilman, *et al.*, 2017; Houben and Snyers, 2018). Since it is not possible to link individual transactions to the wallet holders, it is difficult to fulfill the actual owner obligations under the anti-money laundering regulation, as recommended by the FATF (2018; 2019).

Decentralized trading platforms or applications - Decentralized exchanges (DEXs) or “atomic swaps” are open-source applications that allow users to make transactions at P2P level. The decentralized exchanges operate through the use of smart contracts (see Glossary) that allow the functions of trading and post-trading to be performed automatically, matching demand and supply in an anonymous way. Once a wallet stored by the user on his own device is activated, he will be able to complete transactions without going through a centralized exchange or a custodian wallet provider. This is done by maintaining full possession of the funds at all times through the control of the private cryptographic key. Supporters of this organizational model (for now it seems limited to exchanges between virtual currencies) underline the lower risks of cyber-attacks against a model based on a centralized entity. The use of these protocols, however, favours the anonymity and circumvention of anti-money laundering rules.³⁷

Pseudo-anonymity facilitates the use of crypto-assets for different types of crimes, often at a transnational level. In particular:³⁸

³⁶ On these aspects, see the recommendations of the FATF (2015, 2018); recently, this body has recommended also including the exchanges that exchange virtual currencies with other virtual currencies and financial services providers for ICOs. Lo and Wang's work (2014) considers these aspects. See also Houben and Snyers (2018).

³⁷ See European Parliament – TERR Committee, (2018), pp. 40-42; Madeira, A., (2018); European Union Blockchain Observatory and Forum (2019, p. 26); Buchko, S. (2018). On “atomic swaps” see: <https://coincentral.com/what-are-atomic-swaps-a-beginners-guide/>; see also Houben and Snyers (2018), p. 77.

³⁸ See Foley, *et al.* (2018); Christin (2012); Internet Security Threat Report (2017); Moore and Christian (2013).

- i) *cyber-attacks for extortion (ransomwares)*: these are cyber-attacks associated with the request for virtual currencies to decrypt the data of the subjects affected (often institutions, banks, universities and so on). The best known case was WannaCry (May 2017);
- ii) *money laundering*: this involves converting illicit money into virtual currencies or selling illicit goods in exchange for virtual currencies, sometimes with the complicity of a miner. This can happen without going through a centralized exchange;
- iii) *thefts or frauds and other misbehaviour*: cyber-attacks that can cause the loss or theft of private cryptographic keys. Forms of fundraising through ICOs having characteristics similar to Ponzi schemes can also be included in this class of misbehaviour.³⁹

4. The regulatory approaches adopted by the main jurisdictions

The complexities described in the previous paragraph are reflected in the wide variety of regulatory, tax and prudential approaches adopted in the main jurisdictions, which we outline briefly, for the sole purpose of showing the fragmentary nature of the interventions adopted so far and the legal uncertainties that still remain (FSB, 2019b; Blandin et al. 2019).

United States – Currently in the US, several competent authorities use different definitions of virtual currencies. The Financial Crimes Enforcement Network (US Treasury) has established that virtual currencies such as bitcoins are a “medium of exchange that operates as a currency in some environments”; the US tax authority (IRS) has issued guidelines that treat virtual currencies as a property;⁴⁰ the U.S. Commodity Futures Trading Commission has established that virtual currencies are a “commodity” under the Commodity Exchange Act. As such, they have been subject to the general rules against fraud and market manipulation. Several rulings by American judges (e.g. the SEC vs Shavers case) concluded that bitcoin is a currency or a form of money.⁴¹

It is worth noting that the New York State Department of Financial Services was among the first authorities to introduce (in June 2015) a specific licence for exchange

³⁹ See Chen, *et al.* (2018). The authors have identified over 400 Ponzi schemes operating on Ethereum.

⁴⁰ See, SEC (2014). For a review of regulations and publications on cryptocurrencies globally, see the Law Library of Congress website (2018): <https://www.loc.gov/law/help/cryptocurrency/index.php>.

⁴¹ United States District Court Eastern District of Texas Sherman Division, SEC vs Shavers, Case No. 4:13-CV-416, Memorandum Opinion and Order, by Judge Mazzant.

platforms in virtual currencies. In particular, the licence imposes minimum capital requirements, internal governance criteria, provisions for operational risks, the use of segregated accounts and so on. The permitted activities are: collection of virtual currencies, retention, possession, custody (or control) of virtual currencies on behalf of third parties; purchase, sale, exchange of virtual currencies as a business activity; control, administration or issue of virtual currencies. The same authority has recently approved some start-ups that have launched projects of digital coins (stable coins) collateralized with fiat money segregated in a special account.⁴²

The State Banking regulators oversee certain US and foreign virtual currency spot exchanges largely through state money transfer laws, while the Treasury's Financial Crimes Enforcement Network (FinCEN) monitors virtual currency transfers for anti-money laundering purposes; since March 2013 it requires crypto exchanges to be registered as money services business.

In the US, as in other jurisdictions, there is an intense debate on whether some types of crypto-assets are financial instruments. It should be noted that the collection of funds against the issuance of a virtual currency through initial coin offerings (ICOs) could be attributable to an investment proposal and subject to specific regulation. To check whether an ICO configures the offer of an investment contract and, as such, if it is subject to regulation, the Howey test applies.⁴³ The test is based on the existence of a contract, transaction or scheme whereby a person invests his money in a common enterprise (see Glossary, Howey test and ICOs). The rationale of the legislation is that the existence of a third party creates an information asymmetry (of the principal-agent type) that needs to be mitigated through an appropriate regulation (mainly the publication of the prospectus).⁴⁴

On 25 July 2017, the Securities and Exchange Commission (SEC) established that the collection of funds against the issue of a virtual currency through initial coin offerings (ICOs) could be due to an investment proposal and subject to specific regulation (Exchange Act Rel. No. 81207). On 12 November 2018, the SEC issued the first cease-and-desist order against a cryptocurrency exchange platform (the EtherDelta)

⁴² See: <https://www.dfs.ny.gov/about/press/pr1809101.htm>.

⁴³ Under the Securities Act it applies Howey test, based on the Supreme Court decision "SEC v. W. J. Howey Co." (328 U.S. 293 (1946)).

⁴⁴ Release No. 81207 / July 25, 2017, Report of Investigation Pursuant to Section 21 (a) of the Securities Exchange Act of 1934: The DAO (<https://www.sec.gov/litigation/investreport/34-81207.pdf>). See also: "Statement on Cryptocurrencies and Initial Coin Offerings" (<https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>).

based on a DLT protocol (ERC20, Ethereum Blockchain), since the platform did not comply with the Exchange Act Rel. referred to above.

Japan – Since April 2017, cryptocurrency exchange businesses operating in Japan have been regulated by the Payment Services Act (PSA)⁴⁵. The PSA defines a cryptocurrency as a property value that can be used as payment for the purchase of goods or services, can be mutually exchangeable, and is transferable and storable via electronic data processing systems and electronic devices. Under the PSA, only business operators registered with a competent local Finance Bureau are allowed to operate cryptocurrency exchange businesses.

The operator must be a stock company or a foreign cryptocurrency exchange business, namely a company having a representative office in Japan. The foreign cryptocurrency exchange business is a service provider that is registered with a foreign government in the foreign country under a law that provides an equivalent registration system to the system under the PSA. The regulation and supervision of the exchanges follows the usual approach: for instance, the Act requires cryptocurrency exchange businesses to establish security systems to protect the business information they hold. When such a business entrusts part of its operations to a contractor, it must take measures to ensure that business is appropriately conducted. Cryptocurrency exchange businesses must manage customers’ money or cryptocurrency separately from their own and are subject to money laundering regulations.

Europe – At the EU level, the only piece of legislation for regulating crypto-assets is the Fifth Anti-Money Laundering Directive (AMLD5). While most member states, following several recommendations by the three European Supervisory Authorities (ESAs),⁴⁶ issued a number of warnings to consumers on the risks related to crypto-assets and ICOs, the current situation is characterized by a variety of legislative and regulatory approaches.

On 30 May 2018, the European Parliament approved the fifth revision of the Anti-Money Laundering Directive (AMLD5). In particular, the AMLD5 introduced two new types of entities: exchanges, defined as providers engaged in exchange services between virtual currencies and fiat currencies and; the custodian wallet providers.⁴⁷ The directive establishes that “[m]ember States shall ensure that providers of

⁴⁵ This section is based on the contribution prepared by S. Umeda for the Law Library of Congress (2018).

⁴⁶ The three European Supervisory Authorities are: the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA).

⁴⁷ On the recent review of the AMLD5 and related regulations (i.e. Fund Traded Regulation and Cash Control Regulation), see Houben, R., Snyers, A., (2018), pp. 53-85.

exchange services between virtual currencies and fiat currencies, and custodian wallet providers” need to be registered by the competent authority. The directive underlines that “[t]he anonymity of virtual currencies allows their potential misuse for criminal purposes”. The legislator is therefore aware that “the inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers. To combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency” (AMLD5, recital 9). It is worth mentioning that, in Europe, from a legal standpoint, virtual currencies are not:

- electronic money, as defined by the Electronic Money Directive (EMD2)⁴⁸;
- funds, as defined by the Payment Services Directive (PSD2);
- deposits or other repayable funds (Capital Requirements Regulation (CRR, art. 4(1));
- gaming currencies, used on dedicated platforms (AMLD5, r(10));
- local or complementary moneys (AMLD5, r(10)).

As in the US, there is no consensus on the legal status of virtual currencies. Competent authorities often refer to the position adopted by the European Court of Justice, but this only relates to the tax treatments of these instruments. In particular, the Court of Justice, on examining a case submitted by the Swedish administrative court concerning a question about the obligation to pay value added tax (VAT), considered bitcoin as a “means of contractual payment”, and therefore – according to the Court - in the event of trading, as exempt from VAT. The Court noted, however, in taking a position on the case under consideration, that “it is common ground that bitcoin virtual currency has no other purpose other than a means of payment and that it is accepted for that purpose by certain operators (s.53).” This qualification seems to underline that the deliberation of the Court aims only and exclusively to avoid differences in the application of the VAT system from one Member State to another.

⁴⁸ The European Banking Authority (EBA) has recently stated that a subset of crypto-assets can be included in the definition of e-money, under the e-money directive (EMD2) (see EBA 2019).

Below, we present a short summary of the main regulatory initiatives adopted by Germany, France and Italy for crypto-assets.

In Germany, BaFin, the financial market authority, transposing the Markets in Financial Instruments Directive (MiFID), included the units of account in the financial instruments category.⁴⁹ The units of account, like private currencies, are comparable to foreign currencies, with the only difference that they are not issued as legal tender. As a consequence, in Germany, virtual currency exchanges are obliged to operate under a licence. For similar reasons, again in Germany, mining activities require a licence, as well as the management of a multilateral trading facility or proprietary trading activity. However, the Berlin Court of Appeal recently decided (on 25th September 2018) that bitcoin is not a financial instrument as per the German Banking Act (KWG) and that there would therefore be no need for the exchanges to apply for a licence.

The French authorities consider virtual currencies to be equal to a private contract between the parties, but do not consider them to be a financial instrument or a payment instrument.⁵⁰ Recently, a report promoted by the French authorities (the Landau report) suggested introducing a licensing regime for the exchanges (called Euro Bitlicense), similar to that of the State of New York or the one introduced by the Japanese authorities (see Landau and Genais, (2018), p. 59). Moreover, the French Finance Ministry has established that the competent authority (the Autorité des marchés financiers - AMF) will be able to grant licences to companies that want to raise funds through ICO operations, once the bill now under consultation has been approved (see Glossary, Initial coin offerings).

In Italy, Legislative Decree 90/2017 made changes to the anti-money laundering regulations by introducing operators in virtual currencies that are considered similar to the other non-financial operators. The decree defines such operators as any “natural or legal person providing third parties, on a professional basis, with services aimed at using, exchanging, and keep storage of virtual currencies as well as the service of exchanging virtual currencies with fiat money”.⁵¹ A competent authority, called the Organismo degli Agenti e Mediatori (Organization of Agents and Mediators), shall keep the register of the above-mentioned operators. The decree specifies that only the activity of conversion of virtual currencies and fiat money (and vice versa) must comply with anti-money laundering obligations (customer due diligence, adequate verification,

⁴⁹ See, BaFin https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html

⁵⁰ See Ministère des Finances et des Comptes Publics (2014).

⁵¹ See the Ministero dell'Economia e delle Finanze - MEF (2018).

conservation of documents, reporting to the Financial Intelligence Unit (FIU) any suspected money laundering and financing of terrorism operations and so on). Recently, the Italian authority on financial markets, Consob, has launched a public consultation on ICOs, proposing to regulate the "security tokens" within the current legislative framework, but with an opt-in/opt-out regime. It also proposed to settle crypto-assets exchanges in the Italian regulation concerning equity crowdfunding platforms (Consob, 2019). See Table 1 for a summary of various approaches.

Table 1 – Regulatory approaches to crypto-exchanges

	Pros	Cons	Example
No intervention	No endorsement of virtual currencies (VCs). Strong reliance on market discipline (users know they are not protected).	Risks related to AML/CFT; operational risks, unmitigated market risks. No protection for users.	In most jurisdictions this situation has rarely been found.
Passive tolerance or Soft regulation Issuing of a warning by the financial authority on the risks of VCs and an invitation to intermediaries not to buy, hold or sell on their own account; Enrolment in a public register for AML/CFT purposes.	Containing the risks of money laundering and terrorist financing; poor endorsement of VCs. Relevant reliance on market discipline. Partial traceability of users of VCs (subjects using decentralized exchanges or “atomic swaps” are excluded).	No protection for VC users from the point of view of fraud, the operational risks of exchanges; exposure to market risks.	Most jurisdictions, including the USA and several European countries, have published a warning for consumers. Some authorities (including Italy, Portugal, Lithuania and Romania) have discouraged the regulated intermediaries from buying, selling or holding VCs. In Italy, establishment of a register for recording the exchanges mainly for AML/CFT purposes (proposed optional regime for ICOs platforms and for exchanges).
Licensing or Full regulation of the platforms	Containment of the risks of money laundering and financing of terrorism; operational risks and market integrity. Partial traceability of the users of VCs (subjects using decentralized exchanges or “atomic swaps” are excluded).	Endorsement of VCs; possible moral hazard and/or risk of not being able to contain the risks of the platforms; Financial regulation for activities that are not financial instruments and have no intrinsic value.	VCs: full license USA (State of NY); Malta (specific legislation on VVs); Gibraltar; France (optional regime for ICOs platforms). Authorization Japan (with provisions similar to a licence), Germany (for professional operators), France, Estonia (for wallet providers), Australia, Luxembourg, UK (FCA).
Prohibition (of one or more activities related to virtual currencies)	Reduction of risks associated with VCs	Difficult/Problematic enforcement; incentives for forms of regulatory arbitrage.	Russia, Ecuador, Bolivia, South Korea, Indonesia, China (*), India.

Source: Jia and Zang (2018); EBA (2018); FSB (2018c; 2019b <https://www.fsb.org/wp-content/uploads/P050419.pdf>); ECB (2015). For more details, see: Blandin *et al.* (2019). The table is purely indicative, and simplifies the various regulatory approaches. (*) Recently, the Chinese competent authority introduced a regulation on blockchain providers. See: <https://www.btctrade.com/politics/10.html?lang=en>

5. Accounting treatment: applying the current IAS/IFRS

The current international accounting standards (IAS/IFRSs) do not explicitly refer to crypto-assets or crypto-currencies.⁵² There are also no interpretations by the IFRS Interpretations Committee (IFRS-IC), the only body of the International Accounting Standards Board (IASB) with the task of providing authentic interpretations of the IAS/IFRSs. Similarly, the US-GAAPs (issued by FASB) do not contain a specific accounting treatment for crypto-currencies.

To date, at the international level, there are some preliminary analyses on the possible accounting treatment of crypto-currencies under IAS/IFRS⁵³. Moreover, they do not reach a single conclusion, and raise different interpretative issues that will only be solved by an official pronouncement by the IASB.

In relation to holdings of crypto-currencies, the IASB asked the IFRIC-IC to: a) provide information about how an entity might apply existing IAS/IFRS Standards in accounting for holdings of crypto-currencies⁵⁴ and crypto-currencies issued in an ICO;⁵⁵ b) consider whether the application of existing IAS/IFRS standards provides users with sufficient financial information about holdings of crypto-currencies; and c) provide advice to the IASB about whether standard-setting is necessary and should be a priority for holdings of crypto-currencies.

In March 2019, IFRIC-IC published for consultation a preliminary interpretation on the possible accounting treatment of crypto-currencies under IAS/IFRS⁵⁶.

While waiting for a possible decision by the IASB and the IFRIC-IC, it is possible to make some preliminary considerations on the current debate.

Accounting classification under the IAS/IFRSs – In the absence of an IAS/IFRS and of an interpretation that specifically applies to a transaction, other event or condition, the IAS 8 - *Accounting Policies, Changes in Accounting Estimates and Errors* provides that

⁵² Since we think the terminology is very important, in this section we decided to use the term adopted by the IFRS, namely crypto-currency (a sub-set of crypto-assets).

⁵³ See Australian Accounting Standards Board (AASB) (2016); Pricewaterhouse Coopers (PWC) 2016, 2017 and 2018; Chamber of Digital Commerce (2017); IASB (2018a; 2018b; 2018c; 2019a; 2019b); EFRAG (2018); Ernst & Young (EY) (2018a; 2018b); and Chartered Professional Accountants of Canada (2018). Some standard setters have undertaken research into the accounting for crypto-currencies, while some have expressed a view on what they consider to be appropriate accounting under the IFRS. For example, in Japan, the standard setter has issued authoritative guidance for the accounting of crypto-currencies under the Japanese GAAP. See Accounting Standards Board of Japan (2018).

⁵⁴ See IASB (2018b), Agenda Paper 4A.

⁵⁵ See IASB (2018b), Agenda Paper 4C.

⁵⁶ In particular the IFRIC-IC considered a subset of crypto-assets with all the following characteristics: a) a cryptocurrency is a digital or virtual currency that is recorded on a distributed ledger and uses cryptography for security; b) a cryptocurrency is not issued by a jurisdictional authority or other party; c) a holding of a cryptocurrency does not give rise to a contract between the holder and another party. See IASB (2019a and 2019b).

management should make use of its own judgment in developing and applying an accounting standard.⁵⁷

On the basis of an initial analysis of the current IAS/IFRS criteria by the IASB,⁵⁸ by some National Accounting Standards⁵⁹ as well as by some auditing firms,⁶⁰ it would seem possible to exclude a classification of crypto-currencies among cash or cash equivalents, under IAS 7 - *Statement of Cash Flows*, because, among other things, they are neither convertible to known amounts of cash nor are they subject to an insignificant risk of change in value. Moreover, crypto-currencies do not meet the definition of financial assets under IAS 32 - *Financial Instruments: Presentation*, because, for example, they do not give the holder a contractual right to receive cash or other financial assets.

The two viable options would seem to be the categories of intangible assets under IAS 38 - *Intangible Assets* and inventories under IAS 2 - *Inventory*, even if according to these classifications there are interpretative doubts and different accounting practices on the part of holders.⁶¹ In particular, an analysis of IAS/IFRSs shows that:

1) *intangible assets* – Under IAS 38 an intangible asset “is an identifiable non-monetary asset without physical substance”.⁶² Crypto-currencies could be included in the category of intangible assets if the following conditions are met:

- I. identifiability. In particular, an asset is identifiable if it:
 - a. is separable, i.e. is capable of being separated or divided from the entity and sold, transferred, licensed, rented or exchanged, either individually or together with a related contract, identifiable asset or liability, regardless of whether the entity intends to do so; or
 - b. arises from contractual or other legal rights, regardless of whether those rights are transferable or separable from the entity or from other rights and obligations.⁶³

⁵⁷ See IAS 8, paragraph 11.

⁵⁸ See IASB (2018b), Agenda Paper 4A.

⁵⁹ See AASB (2016), pp. 9-12.

⁶⁰ See PWC (2016, 2017 and 2018) and EY (2018a and 2018b).

⁶¹ The difficulties and uncertainties encountered in interpreting and implementing the IAS/IFRS are reflected in different accounting treatments of crypto-assets. For example, as noted by the Australian Accounting Standards Board (AASB), some companies have considered bitcoins as intangible assets with an indefinite useful life; others as inventory (see *Australian Accounting Standards Board* (2016), pp. 22-23). For a recent survey on the various possible accounting treatments of the crypto-assets adopted by a sample of companies, see IASB (2018b), Agenda Paper 4B, pp. 6-8.

⁶² See IAS 38, paragraph 8.

⁶³ See IAS 38, paragraph 12. See also PWC (2016), page 5.

- II. control over a resource. An entity controls an asset if it has the power to obtain the future economic benefits flowing from the underlying resource and to restrict the access of others to those benefits,⁶⁴ and
- III. the existence of future economic benefits. The future economic benefits flowing from an intangible asset “may include revenue from the sale of products or services, cost savings, or other benefits resulting from the use of the asset by the entity. For example, the use of intellectual property in a production process may reduce future production costs rather than increase future revenues”.⁶⁵

From an analysis of the problem, the majority of members of the IFRS-IC believe that the aforementioned requirements are respected and, therefore, they consider crypto-currencies as intangible assets.⁶⁶

2) *inventory* – A second hypothesis is to consider crypto-currencies as inventory. IAS 2 does not require inventory to be tangible. Inventories are assets (see IAS 2, paragraph 6): “a) held for sale in the ordinary course of business;⁶⁷ b) in the process of production for such a sale; or c) in the form of materials or supplies to be consumed in the production process or in the rendering of services”. This classification as inventory could be used by operators specialized in cryptocurrencies (for example, exchanges or wallet providers) or by commodity broker-traders. The latter are defined by the IAS 2 as those who buy or sell commodities for others or on their own account, principally acquired with the purpose of selling (or of acquiring) in the near future and generating a profit from fluctuations in prices or from the broker-traders’ margin (see IAS 2, paragraph 5). It should be noted, however, that this classification is only possible because IAS/IFRSs do not have a definition of commodity.⁶⁸ For example, in the United States, where IAS/IFRS standards are not used, the definition of inventory (used

⁶⁴ See IAS 38, paragraph 13.

⁶⁵ See IAS 38, paragraph 17. There is currently no agreement on compliance with this requirement. In this regard IOSCO considers that ‘holdings of cryptocurrencies typically do not generate the same types of future economic benefits from their use, as the primary purpose for a reporting entity to hold cryptocurrency is not to generate revenue from the sale of its products or services, are not principally used as cost saving instruments by the entity, nor are they providing other benefits from their use (such as intellectual property in a production process). Cryptocurrencies are significantly different in nature from those examples because the future economic benefits generally arise only from subsequent sale of the asset’. See IOSCO (2019b).

⁶⁶ See IASB (2019a and 2019b).

⁶⁷ See AASB (2016), page 13.

⁶⁸ See AASB (2016), page 13 to 14.

by US-GAAP) establishes that it must be a physical asset, consequently not crypto-currencies.⁶⁹

Accounting implications – The diversity of choice in the accounting classification of crypto-currencies has repercussions on the evaluation criterion to be used and, consequently, on the representation in the financial statements of the effects of valuation and realization of such assets. In particular, under IAS/IFRS:

- 1) Intangible assets are initially recognized at cost. There are two subsequent measurement approaches under IAS 38 that can be used, namely: the cost model (at cost less any amortization and impairment) or the revaluation model (an entity can only apply the revaluation model if the fair value can be determined by reference to an active market, which is defined by IFRS 13 - *Fair Value Measurement* as “a market in which transactions for the asset or liability take place with sufficient frequency and volume to provide pricing information on an ongoing basis”⁷⁰). Under the revaluation model, intangible assets are measured at their fair value on the date of revaluation, less any subsequent amortization and impairment losses. The net increase in fair value over the initial cost of the intangible asset is recorded in the revaluation reserve via other comprehensive income. A net decrease below cost is recorded under profit or loss. The cumulative revaluation reserve may be transferred directly to retained earnings upon derecognition, but IAS 38 does not allow the revaluation reserve to be transferred via profit or loss.
- 2) Inventories are initially recognized at cost. Subsequently IAS 2 requires measurement at the lower of cost and net realizable value. As a result, decreases in net realizable value would be recorded in the statement of profit or loss, while increases in net realizable value in excess of previously recorded decreases would not be recorded. However, the accounting treatment is different for commodity broker-traders. Broker-traders may evaluate inventories of commodities “at fair value less costs to sell” and “changes in value are recorded in profit or loss” (see paragraph 3(b) of IAS 2). This accounting treatment is only available to those entities that can be defined as commodity broker-traders.

The application of the measurement of both IAS 38 and IAS 2 mentioned above could not provide meaningful information about/on:

⁶⁹ See Chamber of Digital Commerce (2017), page 8 to 9.

⁷⁰ In this regard, few crypto-currencies (among the hundreds of crypto-currencies listed by the exchanges) have an active and liquid market under normal market conditions.

- 1) the value of crypto-currencies, in the event of application of the cost model both inventories and intangible assets, and
- 2) their volatility, in the event of application of the fair value measurement to intangible assets, since under IAS 38 revaluation changes are not reflected in profit or loss (as they would be, for example, for the exchange differences on foreign currencies classified in the cash and cash equivalents and the changes in the fair value of the assets held by the commodity broker-traders).

In summary, the current IAS/IFRS standards do not allow us to consider crypto-currencies as currency or financial instruments. Instead, the accounting standards would seem to favour the use of the categories of intangible asset or inventory⁷¹ (see Table 2 below), even if, in our opinion, developments in crypto-assets and the peculiar nature of these assets could lead in the future the IASB to define specific requirements for crypto-currency.

⁷¹ The tentative agenda decision on holdings of cryptocurrencies published by the IFRS Interpretations Committee would confirm this conclusion. See IASB (2019a and 2019b).

Table 2 – IAS/IFRS: how crypto-assets might be categorized

Asset	Accounting treatment based on IAS/IFRS	Consideration	Explanation
Cash	Foreign currency monetary items are translated using the closing rate. Exchange differences are recognized in/under profit or loss.	It is not possible	The exchangeable crypto-currencies with a floating exchange rate do not have the characteristics of fiat money.
Cash equivalent		It is not possible	The high price volatility does not make the crypto-currencies equivalent to liquid assets similar to fiat money.
Financial instrument	It is established on the basis of the accounting portfolio in which the financial asset is classified (fair value or amortized cost)	It is not possible	Crypto-currencies (such as bitcoin) do not meet the definition of a financial asset because, for example, they do not give the holder a contractual right to receive cash or another financial asset from another entity.
Inventory	Measurement at the lower of cost and net realizable value (any decreases in net realizable value would be recorded in the statement of profit or loss). However, the accounting is different for commodity broker-traders. Broker-traders measure inventories of commodities at fair value less costs to sell, and changes in value are recorded in/under profit or loss.	It would be possible (but it would require particular provisions to take into account the specificities of crypto-currencies)	Crypto-currencies are homogeneous economic units and traded on platforms like commodities, but they do not have the characteristics of a tangible physical asset. Inventories are not necessarily physical assets, but they must be held for sale in the ordinary course of business (e.g. as commodities held by broker-traders). Crypto-currencies are not always held for sale; if held for investment purposes, they cannot be considered as inventories.
Intangible asset	There are two measurement approaches that can be used: the cost model (at cost less any amortization and impairment) or the revaluation model (in this case revaluation changes are not reflected in profit or loss)	It would be possible (but it would require particular provisions to take into account the specificities of crypto-currencies)	Crypto-currencies would be specific intangible assets held for investment purposes. IAS 38 does not provide for a distinction between those held for investment purposes and those held for own use or consumption. According to a recent preliminary interpretation of the IFRS-IC (IASB, 2019a and 2019b), "crypto-currencies" meet the definition of an "intangible asset" in IAS 38 on the grounds that they are capable of being separated from the holder and sold or transferred individually; and they do not give the holder a right to receive a fixed or determinable number of units of currency

6. Prudential treatment: a preliminary analysis

Our analysis of the economic and accounting aspects of crypto-currencies allows us to state with a certain firmness that they cannot be assimilated into any of the traditional economic, monetary or financial categories.⁷² While waiting for a possible decision by the competent international bodies and recalling the EBA's opinion discouraging intermediaries from holding positions in crypto-currencies,⁷³ it may nevertheless be useful to make some considerations regarding their possible prudential treatment under the European Capital Requirements Regulations and Directives (CRD/CRR).

At the outset, we should underline that a comprehensive analysis of the problem would require an assessment of the prudential treatment of risks (credit, market, counterparty, liquidity risk and so on) arising from crypto-currencies. This analysis should be done for each type of exposure: direct owning of crypto-currencies, lending against crypto-currency collateral, lending to entities dealing directly or indirectly with crypto-currencies, clearing or trading derivatives based on crypto-currency and so on. For the sake of simplicity, we will focus on some limited aspects, in order to highlight the complexities that these particular class of instruments pose to investors and regulators.

Given that there is no specific prudential treatment for crypto-assets under the Basel framework and the existing CRR, it could be useful to rely on the accounting classification. Possible capital requirements stemming from direct investment in crypto-assets are assessed as part of Pillar 1, having some similarities with intangible assets. Material risks relating to crypto-assets not covered by Pillar 1 could potentially be addressed via the supervisory review and evaluation process (SREP). The key purpose of the SREP is to ensure that institutions have adequate arrangements, strategies, processes and mechanisms as well as capital and liquidity to ensure the sound management and coverage of risks to which they are or might be exposed, including those revealed by stress testing, as well as risks institutions may pose to the financial system.

In the event that the Basel Committee decides that the prudential treatments will be based on an assessment/classification of crypto-currencies as intangible assets,⁷⁴ institutions shall deduct crypto-currencies from Common Equity Tier 1, given that they

⁷² As in the previous section in this part we use the term crypto-currency (a sub-set of crypto-assets).

⁷³ See EBA (2014); Banca d'Italia 2015a,b; 2018.

⁷⁴ In Europe, under CRR - Article 4(1)(115) - intangible assets has "the same meaning as under the applicable accounting framework and includes goodwill".

cannot readily and in a reliable manner use these assets in cases of losses or increases in their risk profile.

Accounting treatments other than intangible assets (such as commodities) leave some possibilities for an alternative (but we think less satisfactory) prudential treatment as part of the current CRR market risk framework.

Market Risk – Firstly, it should be noted that the calculation of prudential requirements applies not only to commodity positions, but also to derivatives having such assets underlying them. From a prudential point of view, commodities are subject to the calculation of capital requirements for market risks regardless of their classification (trading book or banking book). However, while a hypothetical inclusion of crypto-currencies as a commodity would seem possible with reference to the banking book, compliance with the quality requirements provided for in the CRR for the trading book need some qualifications.

According to article 4 (86) of the CRR, a trading book includes “all positions in financial instruments and commodities held by an institution either with trading intent, or in order to hedge positions held with trading intent”. The CRR sets out how to include these positions in the trading book. The most important aspects to consider are that:

1. positions in the trading book “shall be either free of restrictions on their tradability or able to be hedged” (Article 102);
2. among the policies and procedures for determining which position to include in the trading book, institutions shall at least address “the extent to which a position can be marked-to-market daily by reference to an active, liquid two-way market” and for positions that are marked-to-model “the extent to which the institution can: i) identify all material risks of the position; ii) hedge all material risks of the position with instruments for which an active, liquid two-way market exists; and iii) derive reliable estimates for the key assumptions and parameters used in the model” (Article 104);
3. finally, all trading book positions “shall be subject to the standards for prudent valuation [...]” (Article 105).

As we can see, these conditions are scarcely respected by crypto-assets, and in particular by those that do not have an active market. Once again, we want to stress that the peculiarity of this class of “assets” is not so much the volatility (which is

particularly high), but rather the absence of intrinsic value or public trust and the related indeterminacy of their price.

Liquidity risk – For the purposes of the short-term liquidity indicator (Liquidity Coverage Ratio - LCR), crypto-currencies, given their characteristics, do not qualify as non-binding high quality liquid assets (HQLA) able to cover the total net cash outflows (deriving, for example from massive withdrawals, a sharp reduction in sight liabilities, or a significant increase in credit lines) for a period of 30 days in a liquidity stress scenario.

Counterparty risk – If there were positions in derivatives, in order to hedge exposure to crypto-currencies (also through OTC contracts), it would be necessary to mitigate the counterparty risk.⁷⁵ Currently, counterparty risk is managed either through the use of internal models, or through three standardized methods (mark-to-model, ordinal exposure and standardized method).⁷⁶ As we noted before, how to model this risk is highly problematic.

Operational and other risks – As illustrated above, the need to manage virtual currencies through a specific e-wallet exposes the investor to significant IT risks, primarily related to use of a private cryptographic key. If these risks occur, all the digital coins invested could be lost. In the absence of a comprehensive survey of the frequency and impact of these events, it is not possible to provide indications on how to mitigate the operational risks. Besides these difficulties, it is worth mentioning (EBA, 2014) that in most jurisdictions significant legal uncertainties remain, while the illegal use of these instruments might create reputational risk for the institutional investor.

To conclude this part on prudential treatment, it is clear that the current regulatory framework does not seem to be tailored to adapt easily to the complexities of this potential class of intangible assets. The lack of modelling experience and the difficulty to proxy their performance through other assets should exclude crypto assets such as bitcoin from the internal model-based approaches, for the purposes of market risk, counterparty credit risk and credit valuation adjustment risk capital requirements. Moreover, they should not be eligible neither for credit risk mitigation purposes, nor, as mentioned above, as high-quality liquid assets. This is even more the case if we reflect that our brief and initial considerations are only based on the economic nature of these

⁷⁵ Since December 2017 the Chicago Mercantile Exchange has been trading futures with bitcoins underlying them. The contract commits the counterparty to buy or sell a bitcoin at a price established at the time of purchase; deadlines are monthly, bi-monthly and quarterly.

⁷⁶ See CRR, articles 274-282.

objects, almost completely disregarding another equally important dimension, namely the robustness of the underlying technology.

7. Concluding remarks

Innovation theorists seem to agree that an emerging technology should have the following attributes: a radical novelty with respect to existing technologies; the ability to spread rapidly and persistently over time, with a potential impact on economic agents, institutions and relational models, as well as knowledge production processes. Its prominent feature, however, is a certain degree of uncertainty and ambiguity in its emerging phase (Rotolo, D. *et al.* 2015). These are all features that seem to fit well with the blockchain protocol and the related digital token.

Beyond the political design of the inventor (or inventors) of bitcoin, it is beyond dispute that bitcoin and the underlying technology have introduced a new technological paradigm.

Despite the great uncertainty that still characterizes this issue, which is reflected in the variety of definitions and regulatory frameworks adopted in the various jurisdictions, three elements appear to emerge clearly. Every possible intervention aimed at “governing” this new technological paradigm must come to terms with them. They are:

- (i) the blockchain system based on the “proof-of-work”, at the base of the digital bitcoin token, has very serious criticalities both of a functional nature (large electricity demand) and of governance. Alternative decentralized validation systems still seem to be at an early stage;
- (ii) the diffusion of decentralized cryptographic protocols (DLT) favours the proliferation of digital tokens, contract automation (smart contracts) and authentication (cryptographic notarization), with a plurality of functions; in its permissioned form, DLT has the potential to reshape the relationships between economic agents, with vast and as yet uncertain effects on the efficiency and governance of the economic system;
- (iii) permissionless DLT, particularly if integrated with the use of decentralized exchanges, could favour the creation of a monetary and financial system that is difficult to control, parallel to the traditional one. This, in some cases, could create a sort of “shadow banking” intermediation⁷⁷.

⁷⁷ See, Gola et al. (2017), p. 30; FSB (2019a), pp.11-12.

Once the unresolved technological problems have been solved, we will then enter uncharted territory both from an institutional and a macro-prudential point of view, with implications well beyond the aspects dealt with in this work.

Key takeaways:

From a regulatory perspective, it is imperative to have an unambiguous taxonomy of digital tokens. Crypto-assets such as bitcoin are intrinsically unstable. For these reasons, intermediaries should deduct them entirely from their own highest quality regulatory capital. Crypto-assets such as bitcoin should not be used as underlying assets for financial instruments or to fund initial coin offerings (ICOs); *fiat-backed stable coins* are more appropriate for this purpose. The technology is not neutral, and the pre-conditions for the extensive use of DLT in the banking, financial and payment systems are technological and governance robustness and controllability by a competent authority, where appropriate. The decentralized ledger and the related digital tokens should be supported by a sustainable equilibrium.

Glossary

Contractual or legal rights: a digital token of the DT1 type (see Box 1) does not confer any contractual or legal rights on the owner, who only has access to the public DLT through a password (or private key). The cases of digital tokens that incorporate one or more contractual rights (such as the rights to financial entitlement and entitlement in kind) are different. In particular, the owner of the digital token holds towards the person who organizes the project: i) rights on cash flows (dividends) or participation rights (ownership or voting rights); ii) property rights, where there is the possibility of converting the received digital token into a sum equal to that initially paid; and iii) administrative rights (for example, access rights to the platform, use of certain applications, licenses that are similar to use) or vouchers (coupons) whose possession does not lead to a dilution of the issuing party's capital (see: Security and Markets Stakeholder Group-SMSG, 2018; ESMA 2019).

Cryptographic puzzle: the blockchain uses a mathematical function that makes solving the cryptographic puzzle created by the protocol very expensive in computational terms, while the ex-post verification by 51 per cent of the participants in the system is very simple, once the solution is made public by the miners. The cryptographic algorithm (SHA256) uses a non-invertible mathematical function that transforms a very long binary series into a sequence of very short numbers and letters. A small change in the initial binary sequence is sufficient to obtain a completely different result. The only way to recreate the input data from the output of a cryptographic function is to try a search with the "brute force" of calculation by inserting

possible inputs to see if there is a match. Once the result is known, it is easy to verify the correctness of the transaction.

Distributed ledger technology (DLT) and the blockchain: a DLT is a means of recording information through a distributed ledger. A distributed ledger is a collection of data that is spread across multiple nodes (see below) and whose consistency is enforced by means of a distributed ledger technology (DLT). These technologies enable nodes in a network to propose, validate, and record state changes (or updates) consistently across the network's nodes - with no need to rely on a central trusted party to obtain reliable data.⁷⁸ A blockchain is a form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated. The DLT enables the creation of smart contracts (see below) and the transfer of digital tokens. DLT also makes it possible to create public archives. Unlike a normal central database with shared access by password, DLT permits a decentralized management and updating of the process, without the need for a reliable and trusted third party. There are three types of DLT: public (or permissionless) DLT protocols with an entirely decentralized management on the Internet, through the action of specialized subjects called miners, as in the bitcoin DLT, called Blockchain; private DLT protocols, where the role of the validators is only accessible to subjects enabled by the authorized IT protocol manager (this class of DLT can also operate without miners);⁷⁹ and hybrid protocols, characterized by a mix of the two models.

Electronic money: “electronic money means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in Article 4 point 5 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer”.⁸⁰ The Directive specifies that this definition should cover electronic money whether it is held on a payment device in the electronic money holder’s possession or stored remotely on a server and managed by the electronic money holder through a specific account for electronic money. This definition, according to the EMD2, should be broad enough to avoid hampering

⁷⁸ For an introduction, see : Swan (2015); Morabito (2017); World Bank (2017); Bonneau, J., *et al.* (2015); Auer, R. (2019).

⁷⁹ In this organizational model, the promoter of the initiative can modify the DLT protocol, control the number of nodes and how to create new digital tokens. Moreover, unlike the permissionless model, private DLTs can operate without the incentive based on the creation of tokens and the highly inefficient process of mining. However, according to some authors, private DLT still has unresolved technological problems (see Narayanan, 2018; Li *et al.*, 2018).

⁸⁰ See Article 2 of Directive 2009/110/EC, on electronic money institutions (E-Money Directive - EMD2).

technological innovation and to cover not only all the electronic money products available today on the market but also those products which could be developed in the future (see EMD2, s. 8). Virtual currencies such as bitcoin (DT1 in our taxonomy) are not electronic money, since they do not have a monetary value as represented by a claim on the issuer. Some payment tokens (DT2 in our taxonomy), could respect the definition of electronic money stated above. The European Banking Authority (EBA, 2019, p. 4) has recently published a Notice to the European Commission saying that “the EBA identifies [...] only limited cases in which crypto-assets may qualify as electronic money”. When this is the case, that specific payment instrument would also fall under the Payment services directive (PSD2).

Fiat money: means of payment issued exclusively by a central bank (banknotes, metallic currency) or by a private institution under its authority. Only fiat money is guaranteed by the law, which regulates the issuance and confers legal value and public trust. Fiat moneys are typically legal tender: a form of payment that a creditor is legally obliged to accept from a debtor in order to extinguish a debt, including tax obligations. Bank money (scriptural money) is legal currency held by banks to make payments. In Europe, these distinctions are established by the articles 128 of the Treaty on the Functioning of the European Union (TFEU) and 16 of the attached Protocol 4 (Statute of the European System of Central Banks and of the European Central Bank). Cryptocurrencies issued by a government entity, although not considered the equivalent of fiat currency, could in principle count as legal tender if the government were to decree this.

Financial instrument (accounting definition): from the point of view of the IAS / IFRS international accounting standards (in particular, IAS 32 “Financial instruments: presentation in the financial statements”), a financial instrument is any contract that gives rise to a financial asset for an entity and a financial liability or an equity instrument (equity) for another entity. A financial asset is, for example, any asset that is cash, an instrument representing the capital of the entity (equity), a contractual right to receive cash or another financial asset from another entity.

Financial instrument (normative and prudential definition): In the European Union, many directives and regulations define the term financial instrument. We can refer to the MiFID II (Article 4 (1) 15 Section C, Annex I) which lists financial instruments. They are: transferable securities, money market instruments, fund units, options, futures and derivatives and emission allowances. In this context, the definition of transferable

securities adopted by the MiFID II is relevant, which defines them as securities tradable on a capital market, such as: shares, bonds, other securities.⁸¹ It should be noted that not all member countries have used the same definition of a financial instrument when transposing the directive; some have established a specific (closed set) list of tools. According to some authors (Hacker and Thomale (2018, p.19), European legislation generally uses, as a discriminating factor, the attributes of transferability, standardization, and marketability, the effect of which is the emergence of an information asymmetry between the investor and the issuer. The types of digital token that can be considered as a financial instrument is still under consideration by the competent authorities (see SMSG, 2018). According to the Swiss authority FINMA (2018), which is among the few authorities to take an explicit position, if the digital tokens exchanged via DLT are similar to an atypical security (uncertificated security), are standardizable, and suitable for massive trading, then they can be considered securities and - as such - they are subject to the regulation of the case. On these aspects, see Maas (2019); FCA (2019).

The Basel framework (Part 2, first pillar, Minimum Capital Requirements) uses the following definition: “a financial instrument is any contract that gives rise to a financial asset of one entity and a financial liability or equity instrument of another entity. Financial instruments include both primary financial instruments (or cash instruments) and derivative financial instruments [...]”, (paragraph 686). The CRR, Article 4 (1) (50) - uses the following definition “a) a contract that gives rise, for one part, to a financial asset and, for another, to a financial liability or an instrument of capital; b) any instrument specified in Section C of Annex I of Directive 2004/39/EC (for example, transferable securities, money market instruments, units in a collective investment undertaking and option contracts); c) a derivative financial instrument; d) a primary financial instrument; e) a spot instrument. The instruments referred to in points (a), (b) and (c) are financial instruments only if their value is derived from the price of an underlying financial instrument or another underlying item, by a rate or an index”.

Governance of the blockchain system: the miners are numerous, but the growing computational costs (and therefore the need to use increasingly powerful computers)

⁸¹ In particular, MIFID II -Article 4 (1) (44) uses the following definition: transferable securities: categories of values [classes of securities], excluding payment instruments, which may be traded on the capital market, for example: a) shares of companies and other securities equivalent to shares in companies, partnerships or other entities and certificates of shareholding; b) bonds and other debt securities, including certificates of deposit relating to such securities; and c) any other transferable security that permits the acquisition or sale of such securities or which involves a fixed spot settlement with reference to transferable securities, currencies, interest rates or returns, commodities or other indices or measures”.

have led to the formation of mining pools; a few subjects that globally hold a significant share of the computational power necessary to make the public DLTs work; they coordinate hundreds of miners in the various countries. In theory, this concentration could facilitate a malicious hard fork.⁸² From the point of view of the governance of the blockchain system, the concentration of miners is a double-edged situation: on the one hand, it provides greater power to a few subjects (depleting, in fact, a fundamental element of the philosophy of this technology), but on the other hand, it can solve critical situations. For example, in March 2013 a software review caused a hard fork in the public DLT, which could have created a generalized double-spending problem (Buterin 2013). Only the timely intervention of two mining pools allowed the system to resume its proper functioning (Musiani, *et al.* 2018).⁸³ Finally, it should be recalled that the economic equilibrium of the blockchain is based on game theory principles of economic rationality. Different behaviors, based not on economic utility, but, for instance, on political objectives, are ruled out.

Initial coin offerings (ICOs): ICOs are operations (coordinated by a company or a group of natural persons organized on the network), aimed at raising resources (fiat money or other virtual currencies) from the public through the internet, in exchange for digital tokens.⁸⁴ ICOs representing investment assets that are within the perimeter of the security regulations are called Security token offerings (STOs). The new digital tokens are issued and credited to the investors' wallet (through a smart contract) when certain conditions have been reached, including a minimum amount of funds raised for the project (otherwise the funds received are returned).⁸⁵ If the project finds support, the smart contract activates a series of predefined functions and rights for the subscribers. Most ICO initiatives create digital tokens (utility tokens and so on) by adapting the Ethereum DLT (based on the ERC-20 standard). This favours a certain interoperability (compatibility) between different initiatives.

The purpose of an ICO is to promote an economic project, often linked to digitization (launch of new virtual currencies, development of projects related to DLT, development

⁸² As underlined by Van Valkenburgh (2018, p. 21): "It's important to point out that such an attack does not give the attacker the ability to spend any funds sent to Bitcoin addresses for which she/he does not have the corresponding private keys, nor does it give her/him the ability to create new bitcoins out of thin air." "[a] 51% attack does not enable the attacker to fundamentally change Bitcoin; it merely enables the attacker to block new transactions and, potentially, double-spend transactions that were initiated after she/he obtained majority control".

⁸³ In market situations where the participation of miners is poor, malfunctions (more precisely, malicious fork events) are more likely, as experienced for instance by Bitcoin Gold, Verge and Zen cash. On the critical issues related to governance, see also Landau and Genais (2018), pp. 24-25, who emphasize the frequency of bifurcation events and the possibility that the system can stop/break down because it is no longer profitable in the event of a fall in the price of the virtual currency created.

⁸⁴ In our opinion, the ICOs (like any form of capital injection) should not be financed by "virtual currencies" (DT1 in the classification of Box 1) for the reasons fully described in the second paragraph of this paper.

⁸⁵ For further details, see Van Valkenburgh (2018), pp. 12-17.

of platforms or digital banking intermediaries and so on). In some cases digital tokens include rights to the project for the decentralized legal entity.⁸⁶ Their development favours a process of disintermediation compared with traditional channels for financing the economy, introducing, however, new complexities in the financial markets.⁸⁷

From the regulatory point of view, it is worth mentioning that the IOSCO (whose objectives are to enhance investor protection, maintain fair, efficient and transparent markets and address systemic risk) is working on how the crypto-assets platforms are traded and regulated. It is also examining the regulation of investment funds with exposures to crypto-assets (IOSCO, 2019a).

The French authorities are promoting the development of ICOs through specific legislation.⁸⁸ The bill provides for the possibility of financing an ICO also through the use of virtual currencies and does not provide for restrictions on the type of digital token issued, provided that the criteria of transparency and adequacy of the investor are met. The bill establishes that once the issuer has obtained the “visa” from the competent authority (the MFA), they will have to inform the buyer on the status of the project and on the possible sale on a secondary market of tokens, following the rules of the public offering of securities.⁸⁹ As already mentioned, recently, the Italian authority on financial markets has launched a public consultation on ICOs (Consob, 2019).

ICOs and the Howey test: in the United States, to check whether an ICO configures the offer of an investment contract and, as such, if it is subject to regulation, the Howey test is applied, according to which a contract, transaction or scheme where a person invests money in a common enterprise. The rationale of the rule is that the existence of a third party creates an information asymmetry (of the principal-agent type) that the

⁸⁶ This is the case of the Decentralized autonomous organizations (DAOs), which are attempts to establish forms of corporate governance through an electronic protocol similar to a smart contract associated with voting systems based on the possession of digital tokens. The best-known case, organized through the Ethereum blockchain, dissolved after collecting 250 million dollars in a few days. For a detailed reconstruction of this event see DuPont (2018). On the legal profiles of the ICOs, see Zetzsche et al. (2017); Sorelanski, L (2018). See Hacker and Thomale (2018), especially for the European context; Rohr and Wright (2018), for the application of the Howey test. The topic was also addressed by ESMA (2018c), FSB (2018a), OECD (2018a, 2018b).

⁸⁷ For instance, Chod and Lyanders (2018) propose a model for financing an entrepreneurial venture by issuing security tokens through an ICO. The focus of the paper is on the benefits and costs of ICOs relative to traditional equity-based financing such as venture capital. Assuming that both markets are regulated, they show that, on the one hand, unlike traditional financing, an ICO allows a risk-averse entrepreneur to transfer part of the venture risk to diversified investors. Transferring risk to investors by retaining part of revenues does not dilute the entrepreneur's control rights. On the other hand, the entrepreneur's ability to choose the investment level after securing the financing creates an agency conflict between the entrepreneur and the ICO investors, causing underinvestment compared with traditional sources of financing.

⁸⁸ The recent draft law (“Plan of action for the creation and transformation of enterprises (PACTE)”), in addition to introducing rules on ICOs, allows funds to invest in digital assets (virtual currencies validated by the AMF (Le Moign (2018), p.22) For a summary of this proposed law, see Kramer and Levin (2018).

⁸⁹ See the draft law under discussion in the French Parliament:
http://www.assemblee-nationale.fr/dyn/15/dossiers/Croissance_transformation_des_entreprises.

regulator tries to mitigate this with an appropriate regulation (above all the information prospectus).

The Howey test can be divided into four different factors: 1) a person invests money; 2) money is invested in a common enterprise; 3) profits are expected from the investment; 4) deriving from the efforts of the project promoter or third party. All these conditions must be met.⁹⁰ The Supreme Court embraced a flexible interpretation, changing the wording “profits to come solely from the effort of others”, to “principally from the effort of others” (see, for example, Pierce, 2019). According to the SEC, where the tokens covered by the ICOs meet the aforementioned requirements, they must be considered financial instruments for all purposes, in the same way as securities are, and are subject to the Securities Law. This is true regardless of whether the project is launched by a traditional entity or by a group of independent persons organized through a set of smart contracts (Decentralized Autonomous Organization (DAO) (Hinman, 2018). The issuing body will therefore be responsible for recording the offers and sales of the instruments in question and be subject to anti-money laundering legislation.⁹¹

After a detailed analysis of the applicability of the Howey test to crypto-assets, Van Valkenburgh (2018, pp. 59-60) concludes that: highly decentralized cryptocurrencies (e.g. Bitcoin, Litecoin) are ill-suited to pass the Howey test because of the lack of a discernible third party or promoter upon whose efforts investors rely. The same applies to App-Coins or Distributed Computing Platforms (e.g. Ethereum), because – according to Van Valkenburgh - participants seek access to these tokens for their use-value rather than an expectation of profits. On the contrary, closed-source cryptocurrencies with permissioned ledgers or a highly centralized community of transaction validators are well-suited to the Howey test (and should therefore be regulated as securities), because if the operation of the technology is not visible, there is no reason to believe that profits come from anything other than a promoter’s hype.

Node miners and node non-miners: a node is a processor (equipped with an operating system and dedicated software) connected to the network. The pool of miners is a set of specialized data centres that connect thousands of computers in parallel. There are two types of nodes that operate DLT (although this distinction is not

⁹⁰ The Securities and Exchange Commission has recently published a framework for “investment contract” analysis of digital assets (SEC, 2019).

⁹¹ See the Securities Act based on the Supreme Court decision “SEC v. W. J. Howey Co.” (328 U.S. 293 (1946)). See SEC Release No. 81207 / July 25, 2017, Report of Investigation Pursuant to Section 21 (a) of the Securities Exchange Act of 1934: The DAO [https://www.sec.gov/litigation/investreport/34-81207 .pdf](https://www.sec.gov/litigation/investreport/34-81207.pdf); SEC “Statement on Cryptocurrencies and Initial Coin Offerings”. (<https://www.sec.gov/news/public statement/statement-clayton-2017-12-11>).

present in Nakamoto's definition): *node-miners*, which invest large amounts in dedicated computers and in the consumption of electricity to solve particular algorithms created by the blockchain protocol (see Proof of work below). Their primary incentive is the possible winnings from a bitcoin at a market price sufficient to cover - together with a low commission paid by users - the costs and to guarantee a positive profit margin; and the *node non-miners*, which have the task of validating the transaction pending in the blockchain. This activity is not directly remunerated by the protocol.

Proof-of-work: only those miners who can show that they have incurred a cost to solve the cryptographic puzzle are remunerated for their work.⁹² This remuneration (called proof-of-work) is based on a probabilistic process. It should be noted that the validation can also be completed by a few nodes, provided that the majority of the total calculation capacity at that given moment is reached, with obvious implications for governance (see Governance of the blockchain system). The miners also get a modest fee (paid by end users) after the new block of transactions has been saved on the blockchain. On the one hand this system creates an incentive to process the transactions, and on the other hand makes incorrect behaviour, aimed at simultaneously using the same bitcoin for two transactions (double-spending), more expensive. When a transfer is finalized, the transferring public key and the transaction amount are irreversibly recorded on the blockchain (see Validation, storage, update of the blockchain, below).

Smart contract: a smart contract is an algorithm (used for example by the exchanges or in the operations of ICOs) that is characterized by the presence of the following elements: 1) there is an agreement that defines a set of promises that are declined in a set of clauses; 2) the agreement is written in digital form, through a program or software that incorporates these clauses; and 3) the agreement is formalized by a protocol⁹³ that establishes how the parties must process the qualitative and quantitative information of the contract, thereby allowing the parties to satisfy the contractual terms. The algorithm provides a set of rules or triggers (logical conditions and time sequences) that dynamically models the performance of the contract (Szabo, N., 2002). The basic idea is that every relationship between the parties can be defined through an algorithm able to create not only robust contracts, without errors, but also

⁹² There are many other consensus mechanisms, other than the very inefficient bitcoin blockchain, based on proof-of-work. However, according to some cryptographic experts, to date, only proof-of-work DLTs are robust, while other less energy-intensive solutions (such as proof-of-stake) are more vulnerable to cyberattacks (Li *et al.* (2018)). For a description of security profiles and the various types of possible cyberattacks (including the mining pool attacks), see Conti *et al.* (2017); Badertscher *et al.* (2018).

⁹³ Unlike traditional contracts, protocols must necessarily be unambiguous and complete (Szabo 1997, p.12).

new institutions and formalize relations at the basis of these institutions, now possible thanks to the digital revolution”.⁹⁴ The smart contract can be executed either through a central platform (for example through a central depository that manages a security in a dynamic way, for instance for paying dividends), or through the use of DLT.⁹⁵

Validation, storage, update of the blockchain: the process of updating the blockchain occurs through the following steps:⁹⁶ i) the request for a new transaction is put on the network by the user; ii) each node collects the requests put on the network and creates blocks (each block with many transactions to be validated); iii) each node tries to solve the cryptographic puzzle for the job test, necessary to win the bitcoin; iv) the first node that solves cryptographic puzzles (see Cryptographic puzzle) puts the block on the network, making it public to all the other nodes; v) the nodes accept the block only if all the transactions of the block are valid; and vi) the nodes (by majority) express consent by creating a new block and using the code of the previous block. Consent is only reached when 51 per cent of the computing power (CPU) of the nodes agree that the proposed solution is correct.⁹⁷

References

- Abadi J., Brunnermeier M. (2018), “Blockchain economics”, Princeton University, mimeo, December.
- Accounting Standards Board of Japan, (2018), *Practical Solution on the Accounting for Virtual Currencies under the Payment Services Act*, 14 March.
- Adrian, T., (2019), “Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System”, remarks at the IMF-Swiss National Bank Conference, Zurich, May.
- Aloosh A. (2017), “The price of a digital currency”, October, mimeo.
- Amstad M. (2019), “Regulating fintech: Ignore, duck type, or code”, VOX CEPR Policy Portal, March.
- Athey S., Parashkevov I., Sarukkai V., Xia J. (2016), “Bitcoin Pricing, Adoption, and Usage: Theory and Evidence”, Stanford Institute for Economic Policy Research, WP n. 17-033, August.

⁹⁴ See Szabo (1996). This intuition was subsequently developed by Vitalik Buterin: “The logical extension of this [a smart contract] is decentralized autonomous organizations (DAOs) – long-term contracts that contain the assets and encode the bylaws of an entire organization” (Buterin, 2014). See also: Clark *et al.* (2016).

⁹⁵ For an interesting analysis of the legal aspects that would need to be faced if the smart contracts operating with DLT were used for derivative contracts, see ISDA (2017).

⁹⁶ See Nakamoto (2008), p. 3.

⁹⁷ As noted by Nakamoto (2018) “*The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes*”, (p.1); moreover, “If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote” (p.3).

- Auer R. (2019), "Beyond the doomsday economics of proof-of-work in cryptocurrencies", BIS Working papers n. 765, Monetary and Economic Department, January.
- Auer R., Claessens, S. (2018), "Regulatory cryptocurrencies: assessing market reactions", BIS Quarterly Review, September.
- Australian Accounting Standards Board (AASB) (2016), *Digital currency – A case for standard setting activity. A perspective by the Australian Accounting Standards Board*, December.
- Badertscher C., Garay J.A., Maurer U., Tschudi D., Zikas V., (2018), "But Why Does It Work? A Rational Protocol Design Treatment of Bitcoin", *Eurcrypt* (2), pp. 34-65.
- Banca d'Italia (2015a), "Avvertenza sull'uso delle cosiddette «valute virtuali»", 30 January.
- Banca d'Italia (2015b), Comunicazione del 30 gennaio 2015 – Valute virtuali. Provvedimenti di carattere generale delle autorità creditizie, Bollettino di Vigilanza n. 1, January.
- Banca d'Italia (2018), "Avvertenza per i consumatori sui rischi delle "valute virtuali" da parte delle Autorità europee", 19th March.
- Bank for International Settlements (BIS) (2015), *Digital currencies*, Committee on Payment and Market Infrastructure, November.
- Bank for International Settlements (BIS) (2018), "Central bank digital currencies", Committee on Payment and Market Infrastructures, March.
- Banque de France (2018), "The emergence of bitcoin and other crypto-assets: challenges, risks and outlook", *Focus*, n. 16, March.
- Barontini C., Holden H. (2019), "Proceeding with caution – a survey on central bank digital currency," BIS Papers No 101, January.
- Bech D.M., Garratt R. (2017), "Central bank cryptocurrencies", *BIS Quarterly Review*, September.
- Berentsen A., Schär F. (2018), "The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies", *Federal Reserve of St. Louis Review*, second quarter.
- Biais B., Bivière C., Bouvard M., Casamatta C., (2017), "The Blockchain fork theorem", Toulouse School of Economics, Working paper, n. 17, January.
- Blandin, A., Cloots A.S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J.G., Zhang B., and Cloud, K., (2019), *Global Cryptoassets Regulatory Landscape Study*, Cambridge Center for Alternative Finance, University of Cambridge, Judge Business School, January.
- Bonneau T. (2018), "«Tokens», titres financiers au bien divers? ", *Revue de droit bancaire et financier*, January.
- Bonneau J., Miller J., Narayana A., Kroll J.A., Felten W. (2015), "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", mimeo.
- Bordo M. D., Levin A.T. (2017), "Central bank digital currency and the future of monetary policy", NBER, working paper n. 23711, August.
- Brummer C., Kiviat T.I., Massari J. (2018), "What should be disclosed in an Initial Coin Offering", mimeo.
- Buchko S. (2018), "What is the Komodo Platform (KMD)? All you need to know", October.
- Budish E. (2018), "The economic limits of bitcoin and the blockchain", June.
- Burnie A., Burnie J., Henderson A. (2018), "Developing a Cryptocurrency Assessment Framework: Function over Form", in *Ledger Journal.org*.
- Buterin V. (2013), "Bitcoin network shaken by blockchain fork", in *Bitcoin Magazine*.
- Buterin V. (2014) "A next generation smart contracts & decentralized application platform". Ethereum white paper.

- Campbell-Verduyn M. (ed.) (2018), *Bitcoin and Beyond. Cryptocurrencies, Blockchain, and Global Governance*, Routledge, London and New York.
- Caponera, A., Gola, C. (2019), "Aspetti economici e regolamentari delle «cripto-attività»", Banca d'Italia, *Questioni di economia e finanza*, n. 484. March.
- Catalini, C., Gans, J.S. (2018), "Some simple economics of the blockchain", National Bureau of Economic Research (NBER), working paper n. 22952, June.
- Carney M. (2018), "The Future of Money", speech made at the Scottish Economics Conference, Edinburgh University, 2 March.
- Chamber of Digital Commerce (2017), Common letter "Determining the Appropriate Recognition, Measurement, Presentation, and Disclosure for Digital Currencies and Related Transactions", June.
- Chartered Professional Accountants of Canada (2018), "An Introduction to Accounting for Cryptocurrencies", May.
- Chen W., Zheng Z., Cui J., Ngai E., Zheng P. Zhou Y. (2018), "Detecting Ponzi Scheme on Ethereum: Towards Healthier Blockchain Technology", mimeo, April.
- Cheung A., Roca E., Su J.J. (2015), "Crypto-currency bubbles: an application of the Phillips-Shi-Yu (2013) methodology on Mt. Gox bitcoin prices", *Applied Economics*, 47 (23), 2348-2358.
- Ciaian C., Rajacaniova M., d'Artis Kancs (2016), "The economics of bitcoin price formation", *Applied Economics*, n. 48, Issue 19.
- Clark C.D., Bakshi V.A., Braine L. (2016), "Smart contracts templates: foundations, design landscape and research directions", mimeo, November.
- Cochrane J. (2017) "Bitcoin and bubbles", November.
- Council of the European Union (2012), *Communication from the Commission toward to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Towards a comprehensive European framework for online gambling*, n. 157337/12, October.
- Consob, (2019), "Initial Coin Offerings and Crypto-assets Exchanges. Call for evidence", 19 March.
- Conti M., Kumar S., Lal C., Ruj S. (2017), "A survey on security and privacy issues of bitcoin", mimeo.
- Christin N. (2012), "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace", mimeo.
- CPMI (2018), "Central bank digital currencies", Committee on Payment and Market Infrastructures, Markets Committee, BIS, March.
- De Filippi P., Loveluck B. (2016), "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure", *Internet Policy Review*, 5(3).
- Demertzis M., Wolff G. B. (2018), "The economic potential and risks of crypto assets: is a regulatory framework needed?", Policy Contribution, issue n. 14, September, Bruegel.
- DuPont Q. (2018), "Experiment in algorithmic governance. A history and ethnography of *The DAO*, a failed decentralized autonomous organizations". in *Bitcoin and Beyond. Cryptocurrencies, Blockchain, and Global Governance*, Campbell-Verduyn, M. ed., Routledge, London and New York.
- EBA (2014), "EBA Opinion on 'virtual currencies'", (EBA/Op/2014/08), June.
- EBA (2016), "Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)", August.
- EBA (2018), "Discussion note on the preliminary readout from the EBA Questionnaire on virtual currencies and next steps", May.

- EBA (2019), "Report with advice for the European Commission on crypto-assets", January.
- ECB (2015), "Virtual currency schemes: a further analysis", February.
- EFRAG (2018), "Virtual Currencies", European Financial Reporting Advisory Group, Issues Paper 07-03, April.
- Eichengreen B. (2019), "From commodity to fiat and now to crypto: what does history tell us", NBER, working paper n. 25426, January.
- Elliott D.J., de Lima L., Singel R. (2018), "Cryptocurrencies and Public Policy. Key Questions and Answers", Oliver Wyman, February.
- Eng-Tuck C., Fry J. (2015), "Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin", *Economic Letters* (130), pp. 32-36;
- Ernst & Young (2018a), "IFRS (#) Accounting for crypto-assets".
- Ernst & Young (2018b), "Accounting by holders of crypto-assets", August.
- ESMA (2015), "Introduction to DLT", mimeo, October.
- ESMA (2017), "The Distributed Ledger Technology Applied to Securities Markets", February.
- ESMA (2018a), "Note on eligibility of virtual currencies investments by UCITS and retail AIFs" (ESMA34-43-417), February.
- ESMA (2018b), "Note on Application of AIFMD to mining pools for virtual currencies using the blockading technology", January.
- ESMA (2019), "Advice. Initial Coin Offerings and Crypto-Assets", January.
- ESMA, EIOPA, and EBA (2018) "Warn consumers on the risks of Virtual Currencies", February.
- EU Blockchain (2018), "Blockchain and the GDPR", EU Blockchain observatory and forum, October.
- EU Blockchain (2019), "Scalability, interoperability and sustainability of blockchain", EU Blockchain observatory and forum, March.
- European Commission (2012), *Towards a comprehensive framework for online gambling*, COM(2012) 596.
- European Commission (2013), Study on the role of regulators for online gambling: authorization, supervision and enforcement. Markt/2013/09/E3/ST/OP, Final report.
- European Commission (2018), *Fintech Action Plan: For a more competitive and innovative European financial sector*, COM (2018) 109/2.
- European Parliament – TERR Committee (2018), *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*. Director General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, Counter-Terrorism. Study PE 604.970, May.
- FATF (2014), Report on Virtual Currencies. Key Definition and Potential AML/CFT Risks, June.
- FATF (2015), "Virtual Currencies, Guidance for a risk-based approach", June.
- FATF (2018), "Regulation of virtual assets", October.
- FATF (2019), "Public statement – Mitigating risks from virtual assets", February.
- Fanusie Y. J., Robinson T. (2018), "Bitcoin Laundering: an analysis of illicit flows into digital currency services", Center on Sanctions & Illicit Finance, January.
- FCA (2017), "Discussion Paper on distributed ledger technology", Discussion paper, DP/17/3, April.
- FCA (2018), "Binary options. What are binary options?", January.
- FCA (2019), "Guidance on Crypto-assets", Consultation paper CP/19/3, January.

- FINMA (2018), "Guidelines for enquiries regarding the regulatory framework for initial coin offerings" (ICOs), February.
- Foley S., Karlsen J.R., Putniņš T.J., (2018), "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", mimeo.
- FSB (2018a), "Financial stability considerations of initial coin offerings and digital token sales", unpublished, March.
- FSB (2018b), "Monitoring of crypto-assets markets. A proposed framework for measuring evolution in financial stability risks", mimeo, May.
- FSB (2018c), "Crypto-assets markets. Potential channels for future financial stability implications", mimeo, October.
- FSB (2019a), "Global Monitoring Report on Non-Bank Financial Intermediation 2018", February.
- FSB (2019b), "Crypto-assets regulators directory", mimeo, April.
- FSB (2019c), "Crypto-assets. Work underway, regulatory approaches and potential gaps", May.
- Gambling Commission (2016), "Virtual currencies, eSport and social gaming", Discussion paper, August.
- Gambling Commission (2017), "Virtual currencies, eSport and social gaming", Position paper, 1, September.
- Gandal R., Hamrick J.T., Moore T., Oberman T. (2018). "Price Manipulation in the Bitcoin Ecosystem", *Journal of Monetary Economics*, 28 January; Workshop on the Economics of Information Security (WEIS).
- Garratt R. (2016), "CAD-coin versus Fedcoin", mimeo, November.
- Garratt R., Wallace N. (2018), "Bitcoin 1, Bitcoin 2, ...: An experiment in privately issued outside monies", *Economic Enquiry*, March.
- Gola, C., Burroni, M., Columba, F., Ilari, A., Nuzzo, G., Panzarino, O. (2017), "Shadow banking out of the shadows: non-bank intermediation and the Italian regulatory framework", Occasional papers, n. 372, Banca d'Italia, February.
- Gola C., Ilari A. (2013), "Financial innovation oversight: a policy framework", Occasional papers, n. 200, Banca d'Italia, September.
- Goldschlag D.M., Stubblebine S. G., (1998), "Public Verifiable Lotteries: Applications of Delaying Functions", mimeo, February.
- Gronwald M. (2014) "The economics of bitcoin. Market characteristics and price jumps", CESifo Area conferences.
- Hacker P., Thomale C. (2018), "Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law", *European Company and Financial Law Review* (forthcoming), June.
- von Hayek F.A. (1990), *Denationalization of Money. The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies*, Institute of Economic Affairs, (first ed. 1976).
- Hale, G., Krishnamurthy, A., Kudlyak, M., and Shulz, P. (2018), "How Futures Trading Changes Bitcoin Prices", Federal Reserve bank of San Francisco, FRBSF Economic Letter, May.
- He D., Habermeier K., Leckow R., Haksar V., Almeida Y., Kashima M., Kyriakos-Saad N., Oura, H., Saadi Sedik T., Stetsenko N., Verdugo-Yepes C. (2016), "Virtual Currencies and Beyond: Initial Considerations", IMF Discussion Note, January.
- He D., Leckow R., Haksar V., Mancini-Griffoli T., Jenkinson N., Kashima M., Khaonarong T., Rochon C., Tourpe H. (2017), "Fintech and Financial Services: Initial Considerations", IMF Discussion note, June, SDN/17/05.

- Heilman E., Al Shenibr E., Goldberg S., Baldimtsi F., Mason G., Scafuro A. (2017), "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub", mimeo.
- Hileman G., Rauchs M. (2017), *Global cryptocurrencies benchmarking study*, Cambridge Centre for Alternative Finance.
- Himino, R., (2018), "FinTech, the future of society and regulation", Financial Services Agency, Japan. Third Beijing Global Fintech Summit hosted by China Finance 40 Forum, Beijing, September.
- Hinman W. (2018), "Digital asset transactions: when Howey met Gay (Plastic)", SEC, speech by the Director of the Division of Corporation Finance, San Francisco, CA, 14, June.
- HM Treasury, FCA, Bank of England (2018), *Cryptoassets Taskforce: final report*, October.
- Houben R., Snyers A. (2018), "Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion", EU Parliament, Study requested by the TAX3 committee, July.
- Hsieh Y-Y, Vergne JP., Wang S. (2018), "The internal and external governance of blockchain-based organizations. Evidence from cryptocurrencies", in *Bitcoin and Beyond. Cryptocurrencies, Blockchain, and Global Governance*, Campbell-Verduyn M. ed., Routledge, London and New York.
- Huberman G. D., Leshno J. C., Moallemi C. (2017), "Monopoly without a monopolist: an economic analysis of the bitcoin payment system", October.
- IASB (2018a), Agenda Paper 12D "Transactions involving commodities and cryptocurrencies— Potential new research project" e IASB Update, July.
- IASB (2018b), Agenda Paper 4A "Holdings of cryptocurrencies"; 4B "Possible standard-setting-holdings of cryptocurrencies"; 4C "Initial Coin Offerings" and IFRIC Update, September.
- IASB (2018c), Agenda Paper 12D "Cryptocurrencies - Potential new research project" and IASB Update, November.
- IASB (2019a), Agenda Paper 4 "Holdings of cryptocurrencies – Item for continuing consideration" and IFRIC Update, March.
- IASB (2019b), Agenda Paper 12 "Holdings of cryptocurrencies – Agenda decision to finalise", June.
- Internet Security Threat Report (2017), volume 22, April.
- IOSCO, (2019a), "Board Priorities. IOSCO work program for 2019", March.
- IOSCO, (2019b), "Comment letter to the IFRS Interpretations Committee's tentative agenda decision on holdings of Cryptocurrencies", May.
- ISDA (2017), "Smart Contracts and Distributed Ledger – A Legal Perspective", Whitepaper, ISDA Linklaters, August.
- Jevons W.S. (1875), *Money and the Mechanism of Exchange*, D. Appleton and Company, Broadway, New York.
- Jia K., Zhang F. (2018), "Between liberalization and prohibition. Prudent enthusiasm and the governance of Bitcoin/blockchain technology", in *Bitcoin and Beyond. Cryptocurrencies, Blockchain, and Global Governance*, Campbell-Verduyn, M. ed., Routledge, London and New York.
- Jonker N. (2018), "What drives bitcoin adoption by retailers?", DNB Working Paper, n. 585, February.
- Keynes J.M. (1936), *The General Theory of Employment Interest and Money*, Macmillan & Company Limited, London.
- Kramer Levin (2018), "A New Legislative Framework for ICOs in France", June.

- Landau J., Genais A., (2018), *Les Crypto-monnaies*, Rapport au Ministre de l'Economie et de finances. La Documentation française, July.
- Law Library of Congress (2018), *Regulation of Cryptocurrencies in Selected Jurisdictions*, June.
- Le Moign C. (2018), "French ICOs – A new method of financing?", Autorité des Marchés Financiers, November.
- Li W., Andreina S. Jens-Matthias Bohli J-M., Karame G. (2018), "Securing Proof-of-Stake Blockchain Protocols", mimeo.
- Lo S., Wang C. (2014), "Bitcoin as Money?", Current Policy Perspectives, n. 14-4, Federal Reserve of Boston.
- Luther J.W., (2013), "Cryptocurrencies, Network Effects, and Switching Costs", Kenyon College, mimeo.
- Maas, T. (2019), "Initial coin offerings: when are tokens securities in the EU and US", Tilburg University, mimeo, February.
- Madeira A., (2018). "What is a Decentralised Exchange?", CryptoCompare, mimeo, September.
- Makarov I., Scholar A. (2018), "Trading and Arbitrage in Cryptocurrencies Markets", mimeo, April.
- Mazières D. (2016), "The Stellar Consensus Protocol: A federated Model for Inter-level Consensus", mimeo, February.
- MFSA (2017), *Discussion paper on initial coin offering, virtual currencies and related services providers*, Malta Financial Services Authority, November.
- Mills D. et.al. (2016), "Distributed ledger technology in payments, clearing, and settlement", Financial and Economics Discussion Series 2016-095, Board of Governors of the Federal Reserve System.
- Ministère des Finances et des Comptes Publics (2014), "Regulating Virtual Currencies. Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering", June.
- Ministero dell'Economia e delle Finanze – MEF (2018), "Valute virtuali: in consultazione pubblica lo schema di decreto per censire il fenomeno", Comunicato stampa n. 22 del 2 febbraio.
- Moore T., Christin N. (2013), "Beware the Middlemen: Empirical Analysis of Bitcoin-Exchange Risk", mimeo.
- Morabito V. (2017), *Business Innovation Through Blockchain. The B³ Perspective*, Springer International Publishing AG.
- Musiani F., Mallard A., Méadel C. (2018), "Governing what wasn't meant to be governed. A controversy-based approach to the study of Bitcoin governance". In *Bitcoin and Beyond. Cryptocurrencies, Blockchain, and Global Governance*, Campbell-Verduyn M. ed., Routledge, London and New York.
- Nakamoto S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System", mimeo.
- Narayanan A. (2018), Hearing on Energy Efficiency of Blockchain and Similar Technologies, United States Senate, Committee on Energy and Natural Resources.
- OECD (2018a), "Issues note on Initial Coin Offerings (ICOs)", Directorate for Financial and Enterprise Affairs Committee on Financial Markets (CMF), mimeo, April.
- OECD (2018b), "Initial Coin Offerings (ICOs) for SMEs", Directorate for Financial and Enterprise Affairs Committee on Financial Markets (CMF), mimeo, October.
- Pagnotta E. S., Buraschi A., (2018), "An Equilibrium Valuation of Bitcoin and Decentralized Network", mimeo.

- Panetta F. (2018a), "Fintech and banking: today and tomorrow", speech at the Harvard Law School Bicentennial. Annual Reunion of the Harvard Law School Association on Europe.
- Panetta F., (2018b), "21st century cash: Central banking, technological innovation and digital currencies", keynote address by the Deputy Governor of the Bank of Italy. Suerf/Baffi Carefin Centre Conference: 'Do we need central bank digital currencies? Economics, technology and psychology', Milan, Università Bocconi, 7th June.
- Parliament of Malta (2018), *Virtual Financial Assets Bill*, Bill n. 44.
- European Parliament (2018), Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU
- Pierce H.M. (2019), "Regulation: A View from Inside the Machine", remarks at protecting the public while fostering innovation and entrepreneurship: first principles for optimal regulation, University of Missouri School of Law, February.
- Pinna A., Ruttenberg W. (2016), "Distributed ledger technologies in securities post-trading. Revolution or evolution?", Occasional Paper Series, n. 172, European Central Bank, April.
- Poon J., Dryja T. (2016), "The bitcoin lightning network: scalable off-chain instant payments", January.
- Prasad E. (2018), "Central Banking in a Digital Age: Stock-taking and Preliminary Thoughts", Hutchins Center on Fiscal & Monetary Policy at Brookings, April.
- PricewaterhouseCoopers (2016), "Accounting Cryptocurrencies", December.
- PricewaterhouseCoopers (2017), "Cracking the cryptocurrency code; or what is a bitcoin anyway?", March.
- PricewaterhouseCoopers (2018), "Cryptographic assets and related transactions: accounting considerations under IFRS", September.
- Rogoff K. (2018), "Cryptocurrencies are like lottery tickets that might pay off in future", December.
- Rohr J., Wright A. (2018), "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets", mimeo, February.
- Rotolo C., Hicks D., Martin B. (2015), "What is an emerging technology?", in *Research Policy*, 44 (10), pp.1827-43.
- SEC (2014), Investor alert: bitcoin and other virtual currency-related investments, 7 May.
- SEC (2017), *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*. Release No. 81207, 25 July.
- SEC (2018), "Engaging on Fund Innovation and Cryptocurrency-related Holdings", Staff letter, 18 January.
- SEC (2019), *Framework for "Investment Contract" Analysis of Digital Assets*, April.
- Security and Markets Stakeholder Group (SMSG) (2018), "Advice to ESMA. Own Initiative Report on Initial Coin Offerings and Crypto-Assets", October.
- Schilling L., Uhlig H. (2018), "Some simple bitcoin economics", Becker Friedman Institute working paper n. 2018-21, April.
- Sorelanski L. (2018), "Réflexions sur la nature juridique des tokens", Bulletin Joly Bourse, May.
- Swan M. (2015), *Blockchain. The Blueprint for a New Economy*, O'Reilly Media Inc.
- Szabo N. (1996), "Smart contracts: Building Blocks for Digital Markets", mimeo.
- Szabo N. (1997), "Formalizing and Securing Relationship on Public Networks", First Monday, Volume 2, n. 9, September.

- Szabo N. (2002), "A formal Language for Analyzing Contracts", mimeo.
- UK Government Chief Scientific Adviser (2015), *Distributed Ledger Technology: beyond block chain*, Government Office for Science, December.
- Van Valkenburgh P. (2018), "Framework for Securities Regulation of Cryptocurrencies," Coin Center Report, August.
- Vasek M., Thornton M., Moore T. (2014), "Empirical analysis of denial-of-service attacks in bitcoin ecosystem", mimeo.
- Visco I. (2018), Welcome address, 1st Biennial Banca d'Italia and Bocconi University Conference on Financial Stability and Regulation, 5 April.
- Yermack D. (2013), "Is bitcoin a real money? An economic appraisal", NBER working paper, 19747.
- Wang S., Vergne JP. (2017), "Buzz factor or innovation potential: what explains cryptocurrencies' returns?", in PLoS One.
- World Bank (2017), "Distributed Ledger Technology (DLT) and Blockchain", FinTech Note n. 1, December.
- Wright A., De Filippi P. (2019), "Decentralized blockchain technology and the rise of *Lex Cryptographia*", mimeo.
- Zetsche D., Ross P., Buckley R.P., Arner D.W., Föhr L. (2017), "The ICO Gold Rush: it's a scam, it's a bubble, it's a super challenge for regulators", University of Hong Kong, Law Working paper n. 11, November.

Biographical note

Carlo Gola

Carlo Gola is currently at the Bank of Italy, Regulation and Macroprudential Analysis Directorate. He obtained his degree in Economics at Modena University (with a thesis on International economics) and an M.Phil in Economics at the University of Oxford.

After a few years working as an economist at IRS (Institute for Social Research in Milan), he joined the Bank of Italy as senior economist. In the early 2000s, following a 5-year experience as Deputy Representative of the Bank of Italy in London, he moved to the IMF, as Senior Advisor for the Italian Executive Director. Throughout his career, has actively worked in several international work streams, including FSB, EBA, ESRB, Joint Forum, and the EU Council during the Italian Presidency semester (working on the reform of Money Market Funds). He is author of several articles and a book on the UK banking system.

Andrea Caponera

Andrea Caponera is currently at the Bank of Italy in the Accounting and Financial Reporting Division (under the Regulation and Macroprudential Analysis Directorate) . Before to join the Bank of Italy he worked for several years at the Italian Banking Association (ABI) where he has actively worked in work streams on the application of the International Accounting Standards (IAS) to the bank's financial statements.

He has a degree in Economics and a master in Tax law both obtained at the University of Rome "Tor Vergata". He is author of articles on the International Accounting Standards (IAS).
