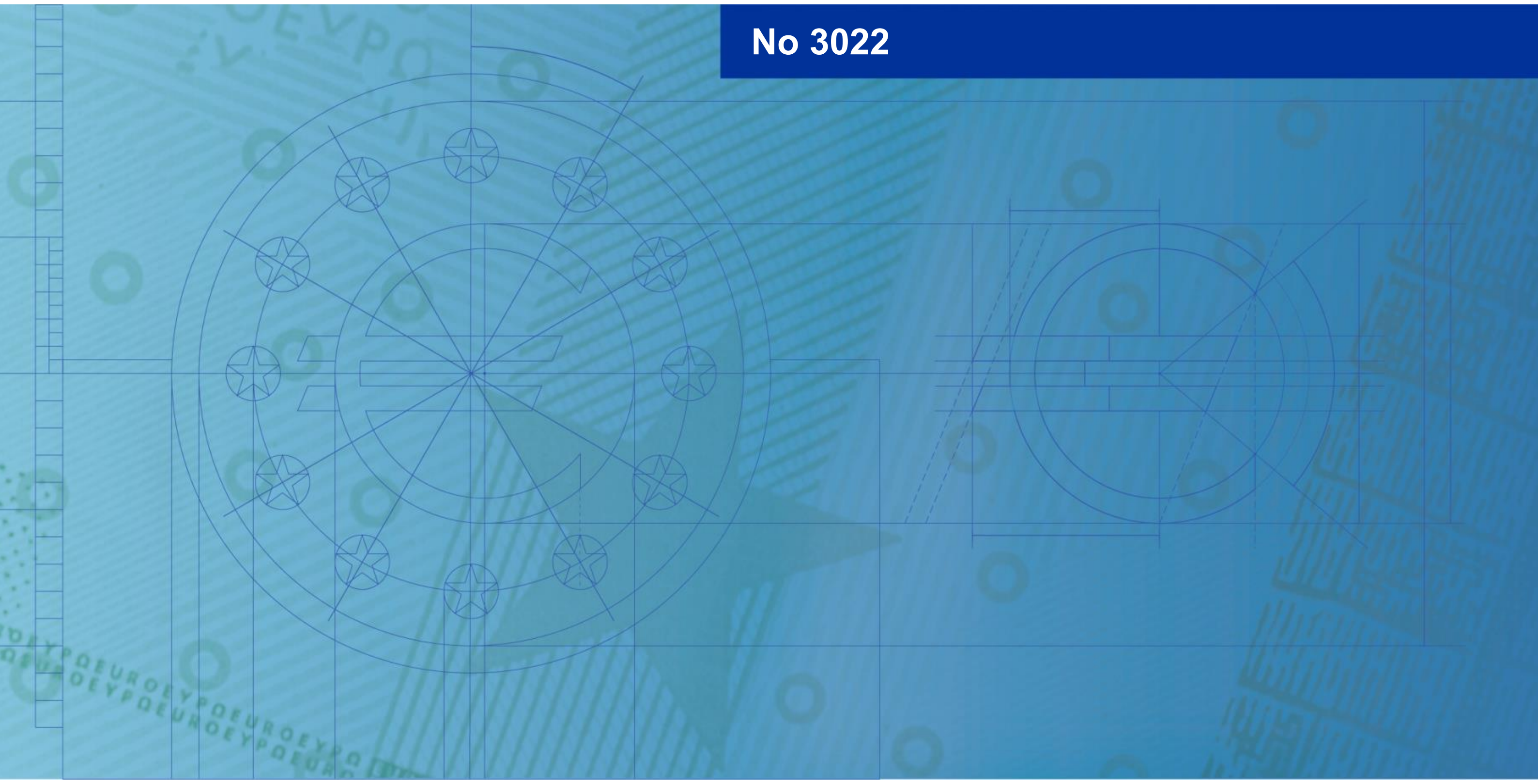
EUROPEAN CENTRAL BANK
EUROSYSTEM

Working Paper Series

Ulrich Bindseil, Charles-Enguerrand Coste,
George Pantelopoulos

Digital money and finance: a critical review of terminology



No 3022

Disclaimer: This paper should not be reported as representing the views of the European Central Bank (ECB). The views expressed are those of the authors and do not necessarily reflect those of the ECB.

Abstract

The digitalisation of payments has accelerated over the last decades with the internet and ever faster and cheaper computing. Now, many believe that decentralised finance (“DeFi”) offers fundamentally new possibilities for trading, payments and settlement. Moreover, for a few years central banks have launched work on what has been called retail and wholesale central bank digital currencies (“CBDC”). Concurrent to the rise of innovative technologies has been the advent of new terminology, which is widely used, but which often seems to be biased, confusing, or is used inconsistently. By providing an etymology of key concepts and reviewing terminology and definitions, this paper also provides a new approach to clarifying the essence of new technologies in the field of payments to facilitate ongoing discussions about their eventual merits and use cases.

Key Words: Digital assets, DeFi, DLT, Tokenization, CBDC

JEL classification: B26; E42

Non-technical summary

Since 2008, crypto-currencies and decentralised finance (DeFi) have become popular themes and – despite doubts on some of the claimed use cases have created (i) significant wealth (through the substantial valuation of unbacked crypto-assets); (ii) large technology investments; (iii) new business models (like crypto-exchanges and service provision; stablecoin issuance etc.) and (iv) a large community of enthusiasts. And since 2016, central banks have started to work on "central bank digital currencies" (CBDC) in reaction to the continuous digitalisation of payments. In parallel, a terminology has developed, which is however often confusing, as a result of the speed of development of the field; the often technical nature of the functional architecture and processes of payment and settlement as well as the desire to represent these with intuitive and catchy terms; the even more technical world of IT architecture, database logic and processes that constitute cryptography, blockchain and DLT; the strong interests of crypto-asset (in particular Bitcoin) owners, DeFi grassroot fans, DeFi investors, and sometimes politicians and public sector organisations wanting to promote new technology and keep momentum and belief; terminological path-dependencies and hysteresis, in particular once terminology has been enshrined in laws and regulations. Inconsistent and misleading terminology is however a serious issue in general, and in particular in this case, because of the mix of plausible and less plausible use cases, large investments, the huge market capitalisation of unbacked crypto-assets and last but not least the massive presence of retail investors and enthusiasts with strong beliefs and expectations. Crypto-enthusiasts seem to perceive the world in a particular way that has been affected by language and also established economists and official institutions have promoted inconsistent terminology and contributed to settle in people's minds conceptual misunderstandings.

To contributing to a more effective debate, the paper identifies authoritative current definitions; explores the origins and evolution of currently used common terms (i.e. etymology – being the study of the origin and evolution of a term's semantic meaning across time); and seeks to address issues in the terminology that contribute to confusion which could be addressed by redesigning elements of the terminology. Where necessary/appropriate, the paper reviews the basic functional and technological content of the terms and checks if similar functionality had been identified and named previously to pinpoint redundancies in terminology. To achieve its objectives, every term (or group of terms) is discussed following the same structure: (a) current definition(s); (b) etymology; (c) discussion: review of terminological (and definitional) quality; substance; other terms that have been used for the same concept; similar concepts that existed before where new names in crypto were nevertheless invented; and where appropriate, possible proposals for improving terminology.

The paper concludes with suggestions with regards to the emerging DeFi vocabulary:

- **Crypto-assets:** this term should not be used for assets which are only *represented* on a DLT platform as their economic nature does not depend on the nature of the platform in which their ownership is recorded and in which ownership can be transferred. Bitcoin as an unbacked "DeFi-native" asset could still be called a crypto-asset, but a bond represented on a DLT platform is still a bond and should not be called a crypto-asset but a "Bond held on a DLT-platform". This is independent of whether the bond's primary issuance (i) took place in a standard way, and it only later was represented on a DeFi platform, or (ii) was directly via such a platform. Some legal and technical details relating to the bond may be impacted by it being on a DLT platform, but this is analogous to a bearer bond and a registered bond having each certain specificities. One might also go one step further and avoid the term crypto-assets also for Bitcoin and other unbacked, DeFi-native ledger entries. For those, the term "virtual assets" could be used to emphasize that no assets actually exist or only in a “virtual reality” created by the ledger entries in the DeFi platform and the surrounding narrative and terminology. Alternatively, one could avoid the term “asset” all together to emphasize that no (real world) asset exists and use a term like “virtual ledger entries”.

- **Smart contracts:** this term, which is meant to designate computer code to execute financial processes on a DLT platform, is untransparent and biased. Such code is neither per se smart, nor is it a contract. The term should therefore be avoided. The same applies to other terms in the “crypto-verse” like “mining”, etc.
- **Stablecoin:** the term could be considered misleading and redundant. It is misleading because “Coin” (also in "Bitcoin”, “Altcoin” “Meme-coin”, etc.) wrongly suggests a bearer instrument (like “token”), but these “coins” are registered and transferred in a system-of-accounts database. “Stablecoin” is a redundant term in analogy of not calling assets tokenized into a DLT platform “crypto-assets”: e-money represented on a DLT platform is still e-money and should keep that name (with a possible qualification regarding the way it is represented and transferred). Unbacked (algorithmic) constructs which also have been called stablecoins have turned out to be unstable (or even unviable) so that using the term “stablecoin” for them was misleading not only in terms of the suggested bearer property of a “coin” but also regarding the term “stable”.
- **Tokenisation:** the term is misleading. First, “token” suggests that the asset is a bearer instrument (at least this seems to be the historical meaning of token which was also taken up in the term “token-based CBDC” which was used prominently in 2017-2019), but it is now used for designating representation in (distributed) ledgers. Second, “tokenisation” seems to be about the act of representing in a legal and technical sense the ownership and the recording of transactions of an asset in a specific ledger, but it is unclear why the term would be reserved to DLT platforms, as the nature of this act seems independent of whether the ledger is distributed or central. It would be sufficient to refer to the act of newly representing the ownership of an asset on a ledger (a “ledger” being understood in this context, in contradiction with its traditional meaning before 2008, as a system of accounts to record ownership of an asset and its transfers).
- **Retail CBDC:** the term “digital” in CBDC could be replaced by “electronic” to remove ambiguity on whether retail CBDC means central bank money held on a DeFi platform (it does not). Moreover, the term “currency” should be replaced by “money” as “central bank money” is a common and well-fitting term while “central bank currency” is not. **“Retail central bank electronic money” (rCBEM)** would be defined as means of payments issued by the central bank in electronic form with broad access including by natural persons.
- **Wholesale CBDC:** the term as used in a technological sense in CPMI (2018) could be discontinued as it is non-transparent and inconsistent with the functional interpretation of “retail CBDC”. The meaning in CPMI-MC (2018) could be replaced by “wholesale central bank money represented on a DLT platform”. As there is no paper-based wholesale central bank money, a qualifier “electronic” would not be needed at all in the context of wholesale central bank money: wholesale central bank money is always electronic and never based on paper tokens.

1. Introduction

The digitalisation of society has accelerated over the last three decades with the internet and ever faster and cheaper computing. This has also affected currencies, retail payments and financial services. Moreover, since 2008, crypto-currencies and decentralised finance (DeFi) have become popular themes and – despite doubts on some of the claimed use cases and losses of some investors because of false value promises and scams – have created significant wealth (through the substantial valuation of unbacked crypto-assets); large technology investments; new business models (like crypto-exchanges and service provision; stablecoin issuance etc.); and a large community of enthusiasts. In response, the public sector has acted as legislator (e.g. EU MiCA Regulation), supervisor/overseer, and operator (work on issuing a retail central bank digital currency and experimenting with payment infrastructures based on distributed ledger technology, DLT).

In parallel, a terminology has developed, which is however often confusing, as a result of (1) the speed of development of the field; (2) the often technical nature of the functional architecture and processes of payment and settlement as well as the desire to represent these with intuitive and catchy terms; (3) the even more technical world of IT architecture, database logic and processes that constitute cryptography, blockchain and DLT; (4) the strong interests of crypto-asset (in particular Bitcoin) owners, DeFi grassroot fans, DeFi investors, and sometimes politicians and public sector organisations wanting to promote new technology and keep momentum and belief; (5) terminological path-dependencies and hysteresis, in particular once terminology has been enshrined in laws and regulations. Inconsistent and misleading terminology is however a serious issue in general, and in this case, because of the mix of plausible and less plausible use cases, large investments, the huge market capitalisation of unbacked crypto-assets and last but not least the massive presence of retail investors and enthusiasts with strong beliefs and expectations. Crypto-enthusiasts seem to perceive the world in a particular way that has been affected by language and as also noted by Milne (2024), established economists and official institutions have promoted inconsistent terminology and contributed to settle in people's minds conceptual misunderstandings. Wittgenstein's (2010) aphorisms "to imagine a language means to imagine a form of life" (p. 80) or "A picture held us captive. And we could not get outside it, for it lay in our language and language seemed to repeat it to us inexorably" (p. 48) apply.

To contribute to a better debate, **this paper reviews the emerging terminology and provides an etymology of key terms and relevant concepts associated with the digitisation of money and the crypto-verse.** As Budin (2001) notes, "the history of science is at the same time a history of terminology in the sense of constantly coining new terms, creating new concepts, changing the meaning of existing terms, re-arranging the conceptual structures in theories". ISO704 (2000, 2) considers that "through observation and a process of abstraction called conceptualization, objects are categorized into mental constructs or units of thought called concepts which are represented in various forms of communication." This vision of the nature of terminology may however underestimate the role of vested interests and deliberate marketing in the emerging digital asset and payment field. Indeed, often a term is proposed at the same moment as the object it is supposed to conceptualise (say in a crypto-asset white paper), and the term is chosen in a way to make the object appealing, e.g. by building in characteristics that are essential to the argued merits of the newly proposed object. Our paper extends the work of Milne (2024) who also "documents widespread inconsistencies in terminology and misleading use of analogy in current economic and policy discussions of these developments in digital money and payments. This is more than just a terminological concern. Failure … has resulted in incoherent economic policy debate. Implicit assumptions have hampered understanding of the central economic issue…" While our analysis is consistent with the one of Milne (2024) on e.g. the misuse of the term "token", "tokenisation" and “smart contracts” we cover additional terminology and also provide etymologies. We also go one step further by suggesting alternative terminology. An earlier study on improving the consistency of terminology in (wholesale) payments and finance is Chisholm and Milne (2013).

The challenges associated with applying consistent terminologies have led to various attempts to define terms and to develop glossaries of terminology. Definitions can be found explicitly or implicitly in various sources, including:

- Notes and reports by academics, official sector institutions, or the industry
- Legislative texts
- Glossaries of authoritative public (e.g. BIS, BIS-CPMI, ECB) or private institutions
- Technical standardisation body outputs.

Across sources (and even within sources), definitions can unfortunately be either contradictory (one term is defined and used in different ways), or different terms are used to mean the same thing. For legislative texts, definitions used can be heterogeneous across jurisdictions. Moreover, terminologies can be counterintuitive or inefficient. Principles, methods and terminology work can be found for example in the ISO Standard 704:2022 (“Terminology work”[2]) and ISO 860:2007.[3]

For key DeFi terminology, the paper: **(1) identifies authoritative current definitions**; **(2) explores the origins and evolution of currently used common terms** (i.e. etymology – being the study of the origin and evolution of a term's semantic meaning across time); and **(3) seeks to address issues in the terminology that contribute to confusion which could be addressed by redesigning elements of the terminology.** Where necessary/appropriate, the paper reviews the basic functional and technological content of the terms and checks if similar functionality had been identified and named previously to pinpoint redundancies in terminology. To achieve its objectives, every term (or group of terms) will be discussed following the same structure: current definition(s); etymology; discussion: review of terminological (and definitional) quality; substance; other terms that have been used for the same concept; similar concepts that existed before where new names in crypto were nevertheless invented; and where appropriate, possible proposals for improving terminology.

The rest of the paper proceeds as follows: section 2 restates criteria for good terminology and for good definitions as well as systems of definitions. Sections 3-6 each deal with a specific group of terms in the field of digital money and finance. Section 3 covers foundational and often technology related terms from the crypto-verse; section 4 turns to terminology for crypto-assets and stablecoins; section 5 covers tokenization. Finally, section 6 treats CBDC. Section 7 concludes and offers some suggestions with regards to alternative terminologies, with an annex providing a non-exhaustive list of official and private sector glossaries.

[2] ISO standard 704:2022 “establishes the basic principles and methods for preparing and compiling terminologies both inside and outside the framework of standardization. It describes the links between objects, concepts, definitions and designations. It also establishes general principles for the formation of terms and proper names and the writing of definitions. This document is applicable to terminology work in scientific, technological, industrial, legal, administrative and other fields of knowledge.”

[3] ISO standard 860:2007 specifies a methodological approach to the harmonization of concepts, concept systems, definitions and terms. It applies to the development of harmonized terminologies, at either the national or international level, in either a monolingual or a multilingual context.

2. Principles of terminology

Best practices of terminology are enshrined for example in the ISO standard 704 (IS0704, 2022). ISO704 (2022, vi) explains **objects, concepts, definitions and designations** as fundamental elements of terminology work. Below we summarise key criteria to assess the validity of both linguistic designations, i.e. terminology (section 2.1) and the description of concepts through definitions (section 2.2).

2.1 Criteria for good terminology

Consider the following six key criteria for good terminology broadly based on ISO704 (2022). The criteria often cannot be met fully at once, thus creating trade-offs. We also provide some illustrative examples of the criteria not being met from the field of digital finance and money (some of which will be expanded upon throughout the paper).

1. **Monosemy:** one concept should be represented by one term only, and one term should be used for one concept only. In case of near-synonyms, the difference between the terms should be clear and in which cases or contexts which term is to be used. ISO704 (2022, 57) defines "monosemy" as the relation between designation and concepts in which one designation represents only one concept ("homonymy" being the case of one word designating two concepts and "synonymy" two words having the same meaning) and notes that ideally "a given term is attributed to only one concept and a given concept is attributed to only one term, a condition called monosemy. This condition reduces ambiguity while homonymy and synonymy can lead to ambiguity". For example, the MiCA Regulation uses "e-money token" for what is commonly referred to as a "stablecoin". Also, the term "tokenisation" has been used for describing very different concepts. "Digital" has been used for years with different meanings ("based on DLT" vs. "something electronic, not on paper").
2. **Transparency:** ideally, the key conceptual meaning and the structural and semantic origin of a word must be directly clear so that it can be understood without further explanations and context. It should be avoided that the user without having additional information will likely misinterpret the term. ISO704 (2022, 54) defines that a "term or proper name is transparent when the concept that it designates can be inferred, at least partially, without a definition or other type of information supplementing or replacing a definition… In other words, the concept expressed by a term or proper name can be deduced from their linguistic elements. For a term or proper name to be transparent, a key characteristic – usually a delimiting characteristic – is expressed in the term or proper name itself." Also, it should be avoided that vocabulary is suggestive and tries to promote connotations of a term for marketing reasons that are not sufficiently founded. Wittgenstein's (2010, 37) "[u]ttering a word is like striking a note on the keyboard of the imagination" applies and provides incentives in fields of new technology with strong economic interests to choose vocabulary which transmits unfounded promises. While technical experts may have no difficulties with interpreting the meaning of a term in a specific context, non-experts (which includes diverse groups such as consumers and high-level policymakers) may easily use the terms erroneously and confusingly if they are not sufficiently self-explanatory. In the field of digital money and finance, this issue is particularly relevant since technical concepts are discussed in an inevitably superficial way by consumers, policymakers and legislators etc. For example, it is not transparent that "digital" would mean "based on DLT" even if it is often used in this sense. Many DeFi terms lead to confusion because the settlement layer (i.e. the way an asset is transferred, e.g. in a central ledger or by

way of DLT) is not separated adequately from the object layer (e.g. an unbacked electronic asset or a transferable and redeemable/convertible liability of an issuer), although this separation is a basic architectural and logical feature. The term "coin" (as also contained in Bitcoin, Stablecoin, Altcoin, etc.) has been used to suggest the similarity of these digital value representations with metal coins (presumably precious metal coins, like gold coins, as Bitcoin is suggested to be the "digital gold" of the 21st century) and their implied autonomy from market infrastructures as they would/can circulate from bearer to bearer, hand-to-hand (although this view does not match the online nature of digital coins and the heavy processes and high number of parties involved to sustain the soundness and stability of the exchange mechanism in distributed ledgers). The term "smart contract" violates transparency as it is used to designate in essence a program running on a shared programmable platform, which is neither a contract nor necessarily smart. Other crypto-terms are also subject to this issue, such as e.g. "mining", "gas fee", "burning", which all evoke some real-world processes to support a specific real-world interpretation of certain abstract IT processes.

3. **Consistency**: inconsistencies can have various reasons and dimensions. ISO704 (2022, 54) defines this objective as meaning that "Existing terms and proper names as well as new terms and new proper names should integrate into and be consistent with the relevant concept system." The ISO704 objective of **"appropriateness"** seems to be related to this and is subsumed here under consistency ("Proposed terms and proper names should adhere to familiar, established linguistic patterns used in a given natural language. Formations that cause confusion should be avoided"). For instance, the terms "retail CBDC" and "wholesale CBDC" use underlying concepts in a contradictory way (in one case the term "digital" means the same as "electronic", in the second case it is used to strictly mean "relying on DLT"). Blockchain and DLT are frequently used synonymously, even though they are distinct technologies. The term "token" is used in various inconsistent ways.
4. **Conciseness and easiness:** terms should ideally be short, easy to remember and to pronounce. At the same time, these objectives should not undermine consistency. The ISO704 (2022, 55) states that "A term or proper name should be as concise as possible. Undue length is a serious shortcoming. It violates the principle of linguistic economy and it frequently leads to ellipsis (omission)". One solution to the trade-off between consistency and conciseness is to also propose acronyms when coining a new term, such as "CBDC" for "central bank digital currency".[4]
5. **Neutrality:** terms without any judgemental connotations help to avoid misunderstandings and controversy. For example, "fiat money" is commonly used by DeFi supporters to suggest that money issued by central banks has no backing, and that unbacked crypto-assets are a more solid alternative which cannot be manipulated by authorities. Also, the term "TradFi" has been launched by the DeFi community to represent traditional finance as outdated and to suggest that the two forms of finance are of similar importance. Moreover, the intonation of "TradFi" seems unpleasant compared to "DeFi". The term "smart contract" (see above) invokes positive connotations instead of trying to transmit the essence of the concept.
6. **Adherence to grammatical and orthographical rules**: the ISO704 (2022, 55) objective of "linguistic correctness" means that "When new terms, new appellations or new proper names are coined, they should adhere to the morphological, morphosyntactic and phonological norms of the natural language in question." For example, "blockchain" and "stablecoin" all merge two words against English language rules.

[4] That said, CBDC as a term is subject to scrutiny in section 6.

One may add that in the space of crypto-assets, **internationality** of terminology seems to be no issue. Word fragments that are used internationally (with Greek, Latin, English elements) facilitate easier mutual understanding. ISO704 (2000, 27) still seemed to promote an opposite objective: “Preference for native language: even though borrowing from other languages is an accepted form of term creation, native language expressions should be given preference over direct loans”. In the case of digital assets and payments (and also in other technologies and applications – e.g. the internet, social media, cloud computing, etc.), this (outdated) ISO704 objective from 2000 seems unfeasible or at least unrealistic and goes against the international nature of decentralised finance and money and finance topics in general.

2.2 Criteria for proper definitions

Definitions provide the essential characteristics of a concept and thus distinguish it from other concepts. ISO704 (2022, 33) also provides some quality requirements for definitions that are briefly recalled below and generally classifies definitions into intensional ones and extensional ones. With regard to **intensional definitions:**[5]

> *“[Intensional definitions] provide the minimum amount of information that forms the basis for conceptualization and that allows one to recognize a concept and differentiate it from other concepts, especially coordinate concepts. An intensional definition shall define the concept as a unit with an unambiguous intension reflecting a corresponding extension. Intensional definitions shall begin by stating the immediate, i.e. closest, superordinate concept, followed by the delimiting characteristic(s)…. In practice, intensional definitions are preferable to other types of definitions and should be used whenever possible as they most clearly reveal characteristics of a concept within a concept system.”*

ISO704 (2022, 34) explains that an **extensional definition** is (ISO704, 2022, 34) consists of:

> *“[A] list of designations that represent the concept’s immediate subordinate concepts, under just one criterion of subdivision... The subordinate concepts correspond to objects making up the extension of the concept. … Extensional definitions are useful only in very limited circumstances. … Extensional definitions shall be used only if the number of subordinate concepts to be enumerated is finite; the list of subordinate concepts is complete under one criterion of subdivision; and the subordinate concepts can be clarified by intensional definitions or are well known.”*

We distinguish four key quality criteria for definitions. As with the criteria for good terminology, these cannot be in many cases fulfilled at the same time, creating trade-offs.

A. **Non-circularity:** definitions must not be circular. According to ISO704 (2022, 42) circularity occurs if “one concept is defined using a second concept, and if that second concept is defined using the designation or elements of the designation representing the first concept, the resulting definitions are said to be circular. Circular definitions, sometimes called tautological definitions, make it impossible to understand the concept and shall be avoided.” Circularity can occur within a single definition or within a system of definitions. “A definition is circular within a system of definitions when two or more concepts are defined by means of each other.” An example of circularity within a definition is “tokenization means issuing a token on a platform”, instead of saying that “tokenization means representing an asset on a platform”. An example for circularity within a system of definitions is “Tokens are representations of

[5] For example, “Stablecoins are crypto-asset which aim at a stable value expressed in a unit of central bank money” is an intensional definition (although not one which fares well in terms of conceptual consistency).

financial objects on a programmable platform. A programmable platform is a platform on which financial objects have been tokenized".

B. **Accuracy:** ISO704 (2022, 43) note that "A definition shall describe the concept precisely. It should be neither too narrow nor too broad. Otherwise, the definition is considered inaccurate. Non-delimiting or irrelevant characteristics in the definition can result in an extension where objects are unintentionally included or excluded. A definition is considered too broad if the characteristics selected to describe the concept include objects that should not be part of the extension. A definition is considered too narrow if the characteristics selected exclude objects that should be part of the extension."

C. **Singleness**: a definition should describe only one concept, and not several ones at the same time. For example, the latter part of the following statement should be removed and the term cryptography should be defined separately: "A stablecoin aims at having a stable value in terms of a central bank money unit and is based on cryptography, which is the technique to keep information (or more specifically, messages) 'cryptic' – i.e. secret – from third-parties."

D. **Conciseness**: definitions should provide only the essential characteristics of a concept which distinguish it from other concepts. "Unlike an encyclopedic description…, a definition's main purpose is not to provide all details about a given concept" (ISO704, 2022, 33). Secondary and explanatory information shall not be part of the definition but shall be given in a note that complements the definition. Such a note shall be clearly distinguished from the definition.

It is important to keep in mind that concepts and definitions do not exist in isolation but are **systemic**. ISO704 (2022, section 5.5) explains that concepts are always in relation to each other. Concepts are organized into a concept system within a certain context and for a certain audience. At least four relations can be used to develop a concept system: hierarchical relations; generic relations; partitive relations; associative relations (ISO704, 2022, 8). Concepts can be connected in **hierarchical relations** and are thus superordinate, subordinate or coordinate concepts in relation to each other. A hierarchy is constituted if there is at least one subordinate concept below a superordinate concept (ISO704, 2022, 9). For example, unbacked crypto-assets and stablecoins are often presented as subordinate concepts of crypto-assets. They are thus coordinate concepts to each other. Stablecoins can be algorithmic or backed. Stablecoins are thus both a subordinate concept (to crypto-assets) and a superordinate concept (relative to e.g. backed stablecoins). This case is also consistent with a **generic relation:** "the intension of the subordinate concept includes the intension of the superordinate concept plus at least one additional delimiting characteristic. For example, the intension of 'optical mouse' comprises that of 'computer mouse' plus the delimiting characteristic 'detecting movement by means of light sensors'. Conversely, the extension of the superordinate concept includes that of the subordinate concept" (ISO704, 2022, 10). While concepts connected by a generic relation inherit characteristics, concepts connected by a **partitive relation** (ISO704, 2022, 16) do not. For example, a permissioned blockchain consists in the (i) relevant computer code, (ii) a governance and access protocol. **Associative relations** are derived from any underlying relations between objects (ISO704, 2022, 23 provides various cases of associative relationships and examples).

A good terminological system – e.g. in the field of digital money and finance – will not only have to rely on good individual terms and definitions looked at in isolation, but the overall consistency and accuracy of the terminology will be decisive for achieving clarity and efficiency of analysis and communication in the field.

Finally, it is also worth pointing out that there **could be cases where the actual term may violate several of the principles associated with good terminology (say, principles 1, 3 and 5 for instance), but the definition of the concept is adequate.** For instance, the term "wholesale CBDC" is a misleading term (e.g. principle 3 of good terminology is not observed), but definitions of the term “wholesale CBDC”, such as “wholesale CBDC is electronic central bank money accessible only to eligible banks and relying on DLT” are more or less adequate from the perspective of good criteria for definitions. On the other hand, it could be that the term is itself adequate when viewed against the criteria for good terminology, but definitions can be poor.

3. Crypto- and blockchain technology and applications

Underpinning the “crypto-verse” are various guises of technologies. In this section we consider a number of definitions and in doing so evaluate terminologies, beginning with cryptography (section 3.1); blockchain (section 3.2); smart contracts (section 3.3); programmability (section 3.4); and DeFi (section 3.5).

3.1 Cryptography

a. Current definition(s)

The online glossary of NIST[6] provides the following definition of the term **“cryptography”**:

> *“The science of information hiding and verification. It includes the protocols, algorithms and methodologies to securely and consistently prevent unauthorized access to sensitive information and enable verifiability of the information. The main goals include confidentiality, integrity authentication and source authentication.”*

This definition is consistent with other contemporary interpretations of the term (see e.g. ISO22739, 2024).

b. Etymology

Rosenheim (1996, 20) suggests that the term “cryptography” was first introduced in 1641, and goes on to describe that Poe (1843)[7] was the earliest to employ the cognate term “cryptograph” – meaning encoded/enciphered text (i.e. cipher-text). However, it remains somewhat ambiguous as to who/where the term “cryptography” was first definitively used. In any case, what was implied by early authors with regards to cryptography was something that was hidden and written (since the literal meaning of cryptography means something that is hidden and written). However, it is also worth clarifying – as denoted by Rosenheim (1996, 254) – that cryptography in its original form only referred to the process of enciphering, but the lay usage of the term also included deciphering (i.e. decryption, where cipher-text is transformed back into plain-text).

More broadly, cryptographic techniques/protocols consist of cryptographic primitives (i.e. tools). Cryptographic techniques are, as suggested by the term, a way to keep information (or more specifically, messages) “cryptic” – i.e. secret – from third-parties. Messages are not per se necessarily kept hidden, as “[t]he methods of cryptography...do not conceal the presence of a secret message but render it unintelligible to outsiders by various translations of the plaintext” (Kahn, 1967, xiii). If the actual message were to be hidden, this would an example of “steganography”.

[6] https://csrc.nist.gov/glossary/term/cryptography

[7] https://www.eapoe.org/works/tales/goldbga2.htm

Though the usage of the actual term “cryptography” (or “cryptograph”) seems to be fairly novel in historical terms, cryptographic techniques in the form of encryption/decryption have been used for millennia, including in ancient Egypt, India, Greece, Rome and Persia (see e.g. Langie, 1922; Pincock, 2006). Kahn (1967, 82) describes how cryptography was used by the Spartans around 2500 years ago:[8]

> *“It was the Spartans, the most warlike of the Greeks, who established the first system of military cryptography. As early as the fifth century B.C., they employed a device called the ‘skytale’, the earliest apparatus used in cryptology…The skytale consists of a staff of wood around which a strip of papyrus or leather or parchment is wrapped close-packed. The secret message is written on the parchment down the length of the staff; the parchment is then unwound and sent on its way. The disconnected letters make no sense unless the parchment is rewrapped around a baton of the same thickness as the first: then words leap from loop to loop, forming the message.”*

The contemporary meaning of cryptography has seemingly drifted, in that modern interpretations of cryptography encompasses an entire field of computer science, as opposed to the conversion of plain-text into cipher-text etc. for the purposes of transmitting secret messages. For instance, a perusal of several textbooks (see e.g. Schneier, 1996, 22; Menezes, Van Oorschot and Vanstone, 1997, 4)[9] with regard to the meaning of cryptography reveals that it not only incorporates **confidentiality** in the form of secret messages, but that the term also means the facilitation of information security in various other facets, predominantly by way of (1) **data integrity** – tamper-resistance (i.e. the data has not been tampered/altered in any way); (2) **non-repudiation** – meaning that one entity cannot deny that a specific action took place; and (3) **authentication** – that a message was transmitted/authorised by a particular.

c. Discussion

Current definitions seem to adequately describe the underlying concepts that pertain to the idea of modern cryptography. Taken in this context, current definitions are therefore adequate in terms of e.g. principles B and D of good definitions.

While a frequent contemporary interpretation of cryptography implies information security (e.g. data integrity, non-repudiation etc.), the traditional/historical meaning of cryptography only emphasises the secrecy of information. To illustrate the point, one can compare current definitions of cryptography to their historical counterparts, such as that as provided by the National Security Agency (1953, 9), who describe cryptography as a “…branch of cryptology which treats of the means, methods, and apparatus for converting or transforming plaintext messages into cryptograms, and for reconverting the cryptograms into their original plaintext form by a simple reversal of the steps used in their transformation.”[10] In this regard, the term “cryptography” is homonymic – it is linked to two concepts; being that of secrecy of information on one hand, and information security in general on the other.

Moreover, **“crypto” has also become an abbreviated term for alleged means of payments in the form of “crypto-currencies”.** In public debate, the link between crypto and crypto-currencies is

[8] One of the most widely known encryption techniques is that of “Caeser’s cipher”, in which plain-text is transformed into cipher-text by way of substituting each plain-text letter by a letter three places to the right of it.

[9] For instance, Menezes, Van Oorschot and Vanstone (1997, 4) define the term “cryptography” as “…the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.”

[10] Cryptography as a term also violates grammatical rules and is also used inconsistently.

sometimes suggesting that cryptography as a science began with the foundation of so-called means of payments that are underpinned by cryptographic primitives, like Bitcoin. For instance, a google search of the term “crypto” does not immediately disclose results for cryptographic primitives etc., but for crypto-currencies and their associated trading platforms (e.g. Coinbase). Even official publications have at times not segregated cryptographic primitives/techniques from the idea of crypto-currencies. To this end, the BIS (2023b, 2) purports that “[t]he birth of crypto dates to the introduction of Bitcoin in 2009: a decentralized, peer-to-peer means of transferring value on a shared public ledger…” Aside from the fact that the Bitcoin white paper was first published in 2008, cryptography has been around for thousands of years. Moreover, several attempts were made to create means of payments based on cryptographic primitives prior to Bitcoin (see e.g. Narayanan et al, 2016, ix-xxvii).

3.2 Blockchain

a. Current definition(s)

According to the US Rules Committee (2024, 4; see also NIST online glossary; Yaga et al, 2018; ECB Crypto-Asset Task Force, 2019, 7), **“blockchain”** is:

> *“...any technology...where data is...(i) shared across a network to create a public ledger of verified transactions or information among network participants; (ii) linked using cryptography to maintain the integrity of the public ledger and to execute other functions; and (iii) distributed among network participants in an automated fashion to concurrently update network participants on the state of the public ledger and any other functions...”*

b. Etymology

It is unclear where the actual term “blockchain” originated. For instance, while some (see e.g. Narayanan et al, 2016) attribute the idea of “chaining” information to Haber and Stornetta (1991) – as the authors described a mechanism to produce linked time-stamps by way of hash functions (as well as digital signatures) – the authors only mentioned the word “chain” twice, and never referred to a “block”, “blocks” or “blockchain”. Chaum (1982, 7; see also p. 92) also referred to chaining information, “[m]any blocks can be ‘chained’ together”, and in addition described the basis for creating a tamper-evident database analogous to the contemporary interpretation of a blockchain (but again, did not use the term “blockchain”):

> *“The present work assumes the use of block schemes, like the Data Encryption Standard, which make it very difficult to modify part of an encrypted block of information without causing drastic changes to the entire decrypted block. A large serial number can be appended to a block before encryption; its presence after decryption provides authentication of the block as a valid block that has not been altered. In such systems, it becomes extremely difficult for someone without a key to create a block that will contain a desired serial number when it is decrypted by a keyholder. Two communicants with a common key can converse using encrypted blocks of data, checking the serial number of each received block to ensure that it has arrived in the proper sequence, and to ensure that it has not been altered.”* [11]

Intriguingly, the Bitcoin whitepaper (Nakamoto, 2008) never actually used the phrase “blockchain”. Instead, Nakamoto noted that “blocks are chained” (p. 3), that nodes work on creating “the next block

[11] Chaum (1982) also discussed the use of public-key cryptography, as opposed to merely considering private-key (i.e. symmetric) cryptography. What Chaum did not include however was a consensus mechanism (e.g. proof-of-work etc.).

in the chain" (p. 3), and also referred to a "chain of blocks" (p. 7). What in essence Nakamoto described was a type of database underpinned by cryptographic primitives (e.g. hash functions, digital signatures etc.), whereby "blocks" of transactions are linked together to form a "chain" of transactions[12] – hence colloquially the concept has become known as a "blockchain"; with the suffix reflective of the process as to how the database is extended: by linking blocks. The innovation of Nakamoto was to amalgamate several pre-existing innovations that had existed for several decades (e.g. the "chaining" of blocks of data, digital signatures etc.) to form a complete construct.

The etymology of blockchain raises the question of whether publications/reports etc. consider blockchain in a **"literal" sense** – i.e. the actual database – or if they contextualise blockchain in a more **"holistic" sense** with regard to the actual operative environment in which the database resides and functions – i.e. a "blockchain network" (or "blockchain system" in the vocabulary of ISO22739, 2024). In this regard, Yaga (2018, 1) from NIST sought to explicitly establish more clarity that with regard to what was implied by the term "blockchain" in the NIST publication of Yaga et al (2018):

> *"NISTIR 8202 attempts to present the topic of blockchain technology as simply and straightforward as possible. Each section builds on concepts introduced in previous sections. The introduction section sets the stage, presenting the scope of the document as well as the nomenclature for some terms up front. It was noted early on that the term 'blockchain' itself was overloaded. It meant the ledger, the technology, an entire field of research, a network, as well as a specific instance of a technology. The authors attempt to be explicit in the document, by specifically using which aspect of the term 'blockchain' meant."*

What Yaga (2018) is seemingly emphasising is that rather than depicting blockchain in a vanilla/literal sense, Yaga et al (2018) interpret "blockchain" in the more holistic sense (blockchain = blockchain network) in which the blockchain exists/functions namely by way of:

- **(1) the ledger** – the blockchain itself in its most literal form;
- **(2) the network** – the specific arrangement whereby participants (i.e. nodes) operate within a specific environment to maintain the ledger;
- **(3) The consensus mechanism** – the process by which nodes agree as to the correct state of the ledger to facilitate settlement etc.[13]

Similarly, current definitions of "blockchain" are often in reference to a "blockchain network". The origins of blockchain networks can be in-part attributed to Chaum (1982; see also Chaum, 1979), where the central premise was to provide a synopsis for a system whereby the maintenance of the system could be accomplished (and the system itself could be trusted to perform certain tasks) by mutually suspicious participants.[14]

[12] The approach by Narayanan et al (2016) is to always segregate the terms "block" and "chain".

[13] In a nutshell, consensus entails a procedure through which the network arrives at a common accord as to which bundles of transactions are valid and thus can agree as to the correct state of the blockchain, block-by-block. Consensus mechanisms are in effect consensus algorithms, which can be segregated into two main types based on whether malicious nodes exist or not. The type of consensus algorithms that assume the presence of malicious nodes are known to exhibit "Byzantine fault tolerance". The two predominant consensus mechanisms – proof-of-work and proof-of-stake – are Byzantine fault tolerant consensus algorithms, where although it is assumed that malicious nodes exist, participants are "steered" away from acting in a malicious manner through incentives. The foundations of proof-of-work are found in Back (2002).

[14] Fiester (1970) also investigated the functionalities of similar types of networks which could operate in a hostile environment.

c. Discussion

Despite some clarifications, inaccuracies still linger widely with regard to definitions of "blockchain" (i.e. whether blockchain in the literal vs holistic sense is being described). Like the term "crypto", it is a homonym, since "blockchain" could be the actual database, or, could also be interpreted to mean the environment which database resides and functions – a blockchain network.

Current definitions of blockchain such as those cited above do however shed some light (albeit via "the back door" as it were) on the *relationship* between blockchain and DLT, **in that by interpreting blockchain in the more holistic sense, it is subtly emphasized that blockchain is a *form/type* of DLT.** The approach adopted by the digital euro online glossary of the ECB (see also ISO22739, 2024) seems to adopt such a perspective, as a "blockchain" is "[a] type of distributed ledger technology (DLT) in which transactions are validated and recorded in a distributed ledger in separate but connected batches known as blocks." Similarly, the Banca d'Italia (2022) clarify that the blockchain is a *class* of DLT. Likewise, Mills et al (2017, 10; see also CPMI, 2017, 3; Cunliffe, 2023) from the Fed point out that:

> *"One specific type of distributed ledger is a blockchain, which adds changes to the database via a series of blocks of transactional data that are chronologically and cryptographically linked to one another. The terms "distributed ledger technology" and "blockchain technology" are often treated as synonyms in the industry even though blockchain is actually a specific type of distributed ledger."*

The fact that some current definitions interpret blockchain in the holistic sense in that it is a type of DLT brings across the idea that **blockchain in the literal sense is not DLT**. Blockchain (in the literal sense) and DLT form a symbiotic relationship in that by the blockchain (i.e. the database) residing in its operative environment, blockchain = blockchain network, which is a form/type of DLT. Thus, despite their symbiotic relationship, blockchain (the literal interpretation) and DLT are strictly distinct.[15] In any case, **DLT does not automatically imply the existence of a blockchain**. For instance, google sheets that are say used to record transactions/account balances shared within a group is a form of DLT, but does not use a blockchain, and thus does not imply the existence of a blockchain network.

Finally, it may be noted that the term **"ledger" in "distributed ledger technology" (DLT)** is also inconsistent with the use of the term "ledger" before DLT came up, i.e. certainly before 2008. In the DLT related recent use, the term "ledger" is meant as an ownership recording and transfer system of assets, i.e. a payment and settlement system. However, before that, the term had been understood for centuries as the book of accounts of a firm in which its asset and liabilities and transactions are recorded, including possibly the profit and loss accounting. Once more, previously well-defined vocabulary was recycled into the crypto-asset world in a confusing way that however allowed to transmit a sense of innovation, and which was immediately accepted without any debate.

3.3 Smart contracts

a. Current definition(s)

With regard to **"smart contracts"**, ESMA (2023, abstract; see also Garrat and Monnet, 2023, 2; IBM, 2022) divulge that:

> *"Smart contracts are computer programmes stored on the blockchain and run when predetermined conditions are met. They are designed to facilitate financial transactions among blockchain users,*

[15] At the risk of stating the obvious, that blockchain networks are a form/type of DLT also does not imply that a *blockchain network is DLT*.

> *without the need for trusted intermediaries that characterises traditional finance... DeFi advocates argue that the 'trustless' nature of smart contracts is set to alter the financial environment. By eliminating the need for intermediaries such as banks and brokers, they argue, smart contracts grant individuals with complete autonomy over their finances, lessening their reliance on centralised agencies and making central institutions, including supervisors and standard setters, obsolete."*

CPMI (2024, 31) defines smart contract as "protocol or code that self-executes when certain conditions are met," which is however not very restrictive and would apply the term to broad sets of computer code for which the term is so far never used.

b. Etymology

There is a consensus (see e.g. Schär, 2021) that the foundation and usage of the term "smart contracts" was set down by Szarbo (1994; see also Szarbo, 1997):

> *"A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries..."*

While the underlying spirit of smart contracts has not changed (e.g. if "X" occurs, then do "Y"), the implementation of smart contracts typically incorporate and reside on a blockchain/blockchain network (see e.g. Buterin, 2014). The integration of smart contracts on top of blockchains have culminated in "decentralized autonomous organizations" (or "DAOs"), in which the blockchain provides the underlying settlement layer (Naudts, 2023).

c. Discussion

Current definitions of smart contracts are circular as descriptions refer to DeFi, whereas at the same time, definitions of DeFi (see below) often refer to smart contracts. Moreover, **the term smart contract is untransparent (as smart contracts are neither contracts nor a priori smart) and biased (to the positive):** Smart contracts are not "smart", as they are merely computer codes that execute tasks upon the fulfilment of preconditions, in which the preconditions pertaining to the terms of the contract may be inputted by humans (Mik, 2017; Grimmelmann, 2019); the smart contract cannot "think for itself" so to speak. This point is raised by Allen (2024), in that "…computer programs cannot anticipate all future states of the world, and the speed and automation of self-execution can cause problems when the world has changed in ways that were not contemplated…." As a consequence, smart contracts can be constructed in such a way that the terms of a trade (e.g. payment flows) can be changed by "oracles"; i.e. third-parties that interact between the "outside world" and the smart contract (De Filipi and Wright, 2018, 75; IOSCO, 2022). Further to the point of relying on third-parties, if the "libertarian" assumption that it is the responsibility of end-users to audit the code is relaxed – given that the underlying code is open source and hence publicly available (BIS, 2023) – smart contracts are not trustless, as trust must be placed in third-parties that originally developed the code (particularly as there are no formal auditing procedures – IOSCO, 2022, 2023).

There may also be cases where some mismatch may occur between what was imputed into the code and what was intended by a participant(s), particularly if the terms of a trade includes verbal communications (Werbach and Cornell, 2017; Mik, 2017; Bacon et al, 2018). As explained by Buterin (2016), "...the very definition of smart contract theft or loss, is fundamentally about differences between implementation and intent." End-users must then rely on legal processes – i.e. a vetting authority – to reconcile disputes (Buckley, Didenko and Trzecinski, 2023). This is despite – as noted by Werbach and Cornell (2017; see also Werbach, 2018) – many enthusiasts claiming that smart contracts are able to exist without any overarching legal framework.

The inclusion of the term "contract" in smart contract is also misleading, since smart contracts are not contracts in the legal sense (Bacon et al, 2018).[16] As Mik (2019, 2, 21) puts it:

> *"As 'smart contracts' are contracts in name only, trying to analyze them within the context of contract law resembles 'trying to fit a square peg into a round hole'...'Smart contracts' can bring about the formation of performance of contracts – but they are not contracts."*

Indeed, since a contract is an enforceable agreement, it is the presence of law (and thus the judicial process) that puts the "enforceability" into any agreement. But since smart contracts are allegedly above the law in the sense that recourse to legal proceedings will be superfluous/not necessary, how is it that agreements can be enforceable? In the words of Werbach and Cornell (2017, 339-340):

> *"The central feature of the smart contract...is that legal enforcement will not be necessary, or even possible. In a very real way, smart contracts are not intended to be legally enforceable...the question of legal enforcement should never arise. In this sense, smart contracts are not intended to be enforced in a legal proceeding. This lack of intent may lead to the conclusion that, even conceptually, smart contracts are not truly contracts at all. They look more like so-called 'gentlemen's agreements', intended to be carried out, but never intended to reach a courtroom."*

Finally, the term "smart contract" is also somewhat redundant (violating monosemy), as the term is used to bring across a concept which is analogous to that of "programmability" (see immediately below); i.e. "if X happens, do Y".

3.4 Programmability

a. Current definition(s)

"Programmability" according to the Oxford dictionary is "the property of being programmable".[17] Hojo and Hatogai (2022, 1; see also JP Morgan, 2024, 5; Lavayssière and Zhang, 2024) from the Bank of Japan explain:

> *"Although there is no commonly agreed definition of programmability at the moment, it is said to be the ability of a computer program to control the behavior of digitally recorded funds and securities that circulate within payment and settlement systems."*

IOSCO (2022, 5; see also BIS, 2023, 85) disseminate the idea of programmability in a little more detail in the context of the crypto-verse:

> *"Crypto-assets can take many forms, from those created and distributed by centralized participants, including fiat-based stablecoins, to those that are created and distributed through mining or by using smart contracts. Design decisions implemented in a blockchain's core code and in smart contracts define the features of each crypto-asset and how users interact with it, such as: the crypto-asset's total supply and how that supply is controlled (including issuance, circulation, and removal from circulation); types*

[16] Szabo (1996) likened the ancestors of smart contracts to vending machines (whereby in using the vending machines, users enter into a "contract" with the vending machine), however there are numerous ongoing debates as to whether using a vending machine is akin to entering into a contract (see e.g. Rohr, 2019; Klass, 2023).

[17] https://www.oed.com/dictionary/programmability_n?tl=true

> *of transactions the crypto-asset is permitted to be a part of; whether assets are technologically 'fungible' with other crypto-assets or are in some respects unique; and how users are incentivized to participate and interact with the crypto-asset. Because these features are set by the code or smart contract that is used to create the asset, these crypto-assets are often referred to as 'programmable'."*

Programmability is intertwined with **"programmable money",** which seems to be intricately linked with DLT. For instance, the BIS (2023, 85) propose that through "tokenization",[18] means of payments can reside on programmable platforms, like a blockchain:

> *"Today, the monetary system stands at the cusp of another major leap. Following dematerialisation and digitalisation, the key development is tokenisation – the process of representing claims digitally on a programmable platform. This can be seen as the next logical step in digital recordkeeping and asset transfer."*

Programmable money would thus enable specific functionalities like **"programmable payments"** (where the underlying settlement layer will be buttressed by a blockchain). As defined by the Deutsche Bundesbank (2020, 4):

> *"Programmable payments are defined as transfers of money for which the time, payment amount and/or type of transfer are determined by conditions specified in advance rather than being set ad hoc during the payment process."*

b. Etymology

Setting aside that it is not evident where the term programmability originated, the idea of programmability (as an extension of a computer "program") has appeared in the field of computer science etc. for decades. From an IT programmer's perspective, the term "programmable" can also be used to designate the feasibility of translating a process or the solution to a problem into a computer program: "The calculation of the Shapley value is programmable in BASIC, although slow". However, in the context of means of payments/payments, many definitions of programmability (e.g. BIS, 2023) ostensibly imply that it is coupled with forms/types of DLT. Why programmability is seemingly enabled by a blockchain is that some form of **programmable script is integrated directly into the blockchain (or by way of smart contracts functioning in parallel with the blockchain)**.[19] However, program code is obviously also embedded in any traditional payment system (e.g. determining which conditions need to be fulfilled to let a payment pass: "if name of payee is not in a sanction list database, and if sufficient funds are in the account of the payer, then effectuate payment, otherwise reject payment"). Moreover, payment systems accessed via an application programming interface (API)[20] creates the link between the underlying records and external systems that enable external conditions to determine payments (see e.g. Lee, 2021; Mills et al, 2017; BIS, 2023). For example, a direct debit is effectuated when the camera of a carpark recognizes the number plate of a registered car (and the car can then leave the carpark without any manual payment).

[18] We will discuss the concept of tokenisation below in section 5.

[19] Though smart contracts are not embedded into it, the Bitcoin blockchain employs "transacting scripting" in which a small program is attached to all value within the system. As the scripting language is not "Turing complete", the scripting language only enables two possible outcomes – successful/not successful – where in the successful case, the payment is validated (see Narayanan et al, 2016, 55-64 for an in-depth discussion).

[20] The API provides the connection between end-user interfaces and the underlying web server/database. APIs are therefore akin to payment gateways in terms of their functionality/purpose.

c. Discussion

Current definitions of programmability in the context of payments are broad. Elements of circularity are also widespread, as definitions of programmability often refer to smart contracts, while definitions of smart contracts refer to programmability.

Moreover, **the notion of programmability and thus programmable means of payments/payments is not something that is necessarily exclusive to the crypto-verse or crypto-verse technologies/innovations**.[21] In other words, the notion that "programmability" is synonymous with forms of DLT is misguided and therefore raises issues of transparency and consistency.[22] In the words of Hojo and Hatogai (2022, 2; see also Deutsche Bundesbank, 2020):

> *"Although programmability of payment and settlement systems is often associated with DLT, its essence lies in the fact that various entities can write programs and automatically move funds and securities…In light of this, programmability is a characteristic that can be found in not only future settlement systems but also existing ones."*

Similarly, as explained by Lee (2021):

> *While…references to programmable money typically describe it as being enabled by distributed ledger technology (DLT) or blockchain systems, this is not universally the case, and the term remains ill-defined. Two natural components of the definition are a digital form of money and a mechanism for specifying the automated behavior of that money through a computer program".*

For instance, what is the difference between what is recognised as programmable money in the crypto-verse sense, and conventional means of payments like commercial bank money (e.g. bank deposits) in regards to their underlying ability to be "programmed"? Couldn't it be argued that monthly subscription payments to Netflix via direct debit, the means of payment – in this case bank deposits – is no less "programmable" than other means of payments where the blockchain provides the underlying settlement layer etc.?[23] An analogous case of programmability could be where say an electronic money institution (EMI)/Fintech were to provide the means of payment (e-money). Further still, if the EMI were to not offer deposits but still instead trigger the payment for the Netflix subscription by effectuating the payment on behalf of the account providing institution (i.e. act as a dedicated payment institution), wouldn't this suggest the existence of programmability? If one accepts that commercial bank money is "programmable" as it were, then so-called programmable money is not exclusive to the crypto-verse.

That commercial bank money/e-money is able to be programmable (if we do not adopt the nominal definition that programmable money only exists in the absence of APIs etc.) suggests that commercial bank money/e-money can be used for programmable payments, raising the issue that the means of payment is akin to a voucher (see e.g. Panetta, 2023)[24] and can only be used as a means of payment

[21] If we relax the assumption that programmable money nominally instils that no distinction can be made between the underlying database and some automated logic integrated into the blockchain, versus the case of traditional payment systems, where some kind of API exists to provide the link between the underlying records and another technology system that facilitates some kind of programmability.

[22] The term "programmability" is also not monosemic as the identical concept of "if X happens, do Y" is intertwined with smart contracts.

[23] This is why Deutsche Bundesbank (2020, 4) argue that "[i]n many cases, the current need for money in programmable applications can be sufficiently met with a programmable payment that does not necessarily require programmable money." (see also p. 6).

[24] As clarified by JP Morgan (2024), programmable money constitutes the "embedding of rules within the store of value itself that defines or constrains its usage." (i.e. a voucher).

for a narrow set of specific things, like e.g. purchasing goods from a particular store. But needless to say, commercial bank money/e-money in the general sense are not vouchers etc.

To provide some clarity, the ECB (2023; see also ECB digital euro glossary; BIS, 2023, 71, Box III.A; Lavayssière and Zhang, 2024) now suggests that a **distinction needs to be made between conditional payments and programmable payments**, and that the former term will now replace the latter:

> *"Conditional payments...which is understood as the ability to instruct a payment automatically when pre-defined conditions are met...These payments were formerly referred to as 'programmable payments'. The new term [i.e. conditional payments] will be used going forward in public communication."*

ECB (2023b, 11) highlight further the distinctions between programmable and conditional payments:

> *"Conditional payments should not be mistaken for programmable money, which has been excluded ex ante for use cases now and in the future. Programmable money would entail units of digital euro being used only to buy specific types of goods and/or services, or to buy them only within a certain period/geography. Programmable money contradicts the guiding principles of the digital euro endorsed by the Governing Council, as convertibility at par with other forms of the currency could not be guaranteed. The Eurosystem has therefore concluded that a digital euro would never be programmable money."*

3.5 DeFi

a. Current definition(s)

IOSCO (2023, 1; see also BIS, 2023b, 2; Auer et al, 2024, 58) provide the following general description of **"DeFi":**

> *"DeFi commonly refers to financial products, services, activities, and arrangements that use distributed ledger or blockchain technologies (DLT), including self-executing code referred to as smart contracts. DeFi aims to operate in a disintermediated and decentralized manner, eliminating some traditional financial intermediaries and centralized institutions, and enabling certain direct investment activities."*

Building on the definition of IOSCO (2023), Coinbase further emphasises the alleged "democratic" characteristics of DeFi:[25]

> *"DeFi (or "decentralized finance") is an umbrella term for financial services on public blockchains, primarily Ethereum. With DeFi, you can do most of the things that banks support — earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, and more — but it's faster and doesn't require paperwork or a third party. As with crypto generally, DeFi is global, peer-to-peer (meaning directly between two people, not routed through a centralized system), pseudonymous, and open to all. … DeFi takes the basic premise of Bitcoin — digital money — and expands on it, creating an entire digital alternative to Wall Street, but without all the associated costs (think office towers, trading floors, banker salaries). This has the potential to create more open, free, and fair financial markets that are accessible to anyone with an internet connection."*

The German Federal Financial Supervisory Authority – i.e. BaFin (2024) – suggests that only permissionless public blockchain can support DeFi, thereby implicitly excluding permissioned blockchain networks and qualify as "fake DeFi" arrangements that do not have on-chain & transparent governance:

[25] https://www.coinbase.com/en-au/learn/crypto-basics/what-is-defi

> *Decentralised finance (DeFi) enables new types of applications in the financial industry that are executed on openly accessible blockchains (permissionless public blockchains) with smart contract functionality. Technical solutions, such as algorithmically controlled consensus mechanisms and automated programmes (smart contracts or DApps), are expected to replace the need for trust in traditional financial intermediaries. (…) While some centralised business models use the DeFi context for marketing purposes, they generally have nothing to do with DeFi in doing so, as they do not use on-chain governance or smart contracts/DApps and thus lack the transparency and automation of DeFi protocols (fake DeFi).”*

b. Etymology

Though it is unclear who first used the term “DeFi”, it is thought according to various websites[26] that the inception of the term began only around 2018. As brought across by current definitions and as widely understood, DeFi is an umbrella-like term that is used to disseminate the idea that financial services can be in effect disintermediated by way of eliminating traditional financial intermediaries/centralized institutions (e.g. banks), where via decentralization end-users interact with smart contracts, rather than with an institution (Auer et al, 2024). To further emphasise the alleged advantageous properties/functionalities of DeFi, enthusiasts have founded the disparaging term “TradFi” to distinguish between DeFi and conventional financial services etc.[27]

As emphasized by e.g. IOSCO (2022), Auer et al (2024) and Schär (2021), permissionless blockchain networks (i.e. “public blockchains”) are the basis of DeFi, in which the blockchain provides the underlying settlement layer. Similar to arrangements outside of the crypto-verse (see e.g. Bindseil and Pantelopoulos, 2023, chapter, 4), other layers are then “stacked” in a hierarchical manner of sorts on top of the settlement layer to form a complete DeFi ecosystem. On the flipside, under the definition of BaFin (2024), decentralized protocols established on permissioned blockchains would not qualify as DeFi even when they are built on DLT. This could be as “finance” is normally considered to consist only in the union of two distinct sets being “TradFi” on the one hand and “DeFi” on the other; that said, a permissioned blockchain using DLT would hardly be considered “TradFi”.

While there is consensus with regards to what constitutes the settlement layer, the terms used to label the other layers – and what a specific layer encompasses – within the stack however generally differ. Furthermore, it can be that a particular term applied to a specific layer means different things. For instance, Schär (2021) incorporates the actual crypto-assets (fungible/non-fungible tokens) within an “asset layer”, whereas Auer et al (2024) integrate crypto-assets within a broader “DLT application layer” that resides above the settlement layer, in which the DLT application layer is itself composed of sub-layers, with an “interface layer” forming the top of the stack (i.e. websites/mobile apps so that end-users may interact with the smart contract(s)). Confusingly however, both Schär (2021) and IOSCO (2022) interpret what Auer et al (2024) define as the interface layer as the application layer. Moreover, while IOSCO (2022) incorporate “tokens”, “bridged tokens”, “fiat/asset-backed stablecoins” and “crypto-backed/algorithmic stablecoins” into the asset layer, both Auer et al (2024) and Schär (2021) are harmonious in that they employ broader terms – “fungible/non-fungible tokens”.

[26] https://www.amberdata.io/defi-decentralized-finance-primer; https://www.mawsoninc.com/the-history-of-defi/#:~:text=First%20Usage&text=It's%20believed%20that%20Ethereum%20developers,peer%20currency%20in%20the%20world.

[27] Similar to many of the terminologies used in the crypto-verse, it is unclear when (or by whom) the term “TradFi” was first used.

c. Discussion

Setting aside that current definitions of DeFi lack specificity, it does not appear that all layers in the DeFi "stack" are decentralised. This includes the settlement layer, i.e. permissionless blockchain networks. In practice they too **contain inherent degrees of centralisation** in terms of **record-keeping** (who stores a full copy of the ledger); **validation** (who can add new blocks to the blockchain); and **functionality** (who controls how the system works in terms of rules etc.). In this regard, Aramonte, Huang and Schrimpf (2021) label DeFi as having a "decentralisation illusion"; said differently, the term is not transparent.

For instance, in terms of both **record-keeping and validation**, the vast majority of nodes in many protocols with proof-of-work consensus mechanisms (including Bitcoin) function as "lightweight nodes", rather than "full nodes".[28] Moreover, given the exorbitant computing requirements associated with solving the cryptographic puzzle, many miners aggregate their activities within so-called "mining pools" (Werbach, 2018; Sultanik et al, 2022). The pooling of resources also applies to protocols with proof-of-stake consensus mechanisms, like Ethereum; nodes/validators will pool their respective stakes together to form "stake pools" (or cartels) to increase the probability that they will be selected to create new blocks (Bains, 2022).

Many blockchain networks are also not exactly decentralised with regard to **functionality.** It is worth quoting Yaga et al (2018, 35; see also BIS, 2023, 85; Walch, 2019) from NIST at length:

> *"The phrase 'no one controls a blockchain!' is often exclaimed. This is not strictly true... Permissionless blockchain networks are often governed by blockchain network users, publishing nodes, and software developers. Each group has a level of control that affects the direction of the blockchain network's advancement. Software developers create the blockchain software that is utilized by a blockchain network...However, not every user will have the ability to do this, which means that the developer of the blockchain software will play a large role in the blockchain network's governance...For example, in 2013 Bitcoin developers released a new version of the most popular Bitcoin client which introduced a flaw and started two competing chains of blocks. The developers had to decide to either keep the new version...or revert to the old version...The developers made a choice, reverted to the old version, and successfully controlled the progress of the Bitcoin blockchain...[On the other hand]...although the developers maintain a large degree of influence, users can reject a change by the developers by refusing to install updated software. Of the blockchain network users, the publishing nodes have significant control since they create and publish new blocks. The user base usually adopts the blocks produced by the publishing nodes but is not required to do so. An interesting side effect of this is that permissionless blockchain networks are essentially ruled by the publishing nodes and may marginalize a segment of users by forcing them to adopt changes they may disagree with to stay with the main fork."*

Even if permissionless blockchains were to contain zero degrees of centralisation, the underlying blockchain is only providing the settlement layer within the DeFi stack. Though this may at first glance qualify the veracity of the term "DeFi", end-user interfaces like websites and mobile apps which constitute the application layer (or interface layer) typically rely on centralised service providers, meaning that the layer functions in an analogous manner to that in the world of "TradFi" and implying that the term is not transparent. The inference here is that in actuality, **the reality of DeFi is in practice**

[28] Full nodes are actors within the blockchain network that maintain a full/complete copy of the blockchain and must stay permanently connected to the network. Lightweight nodes can be differentiated from full nodes in that they do not store a complete copy of the entire blockchain, but only store information that is directly relevant to their activities, such as verifying transactions that only concern them by checking block headers. For instance, some crypto-asset service providers (CASPs) like centralised exchanges who offer wallet services to their clients incorporate lightweight nodes.

somewhat contradictory to what is portrayed by DeFi enthusiasts (see e.g. Schär, 2022, 35; Narayanan et al, 2016, 28; IOSCO, 2022, 9-10, Box 1). In this way, the term "DeFi" is in large part a sloppy one and attempts to segregate the crypto-verse from the conventional financial system by utilising terms like TradFi is in many ways erroneous/misleading. It is also somewhat ironic that while centralised exchanges (such as Coinbase) seemingly support the notion of DeFi, by definition their operational construct contradicts the whole idea of disintermediation with regard to the provision of financial services. Last but not least the only country using Bitcoin as legal tender foresees the use of a state-provided wallet ("Chivo") and settles Bitcoin payments in a central ledger outside the Bitcoin-verse. All in all, aside from the term DeFi not being transparent, the term lacks neutrality – DeFi could be considered as being essentially a marketing term.

4. Crypto-assets and stablecoins

4.1 Crypto-assets

a. Current definition(s)

Several inconsistent definitions of **"crypto-assets"** can be found in the literature.

The online ECB glossary purports that a crypto-asset (ECB Crypto-Asset Task Force, 2019, 2020) is:

> *"[a]n asset recorded in digital form and enabled by the use of cryptography that is not and does not represent a financial claim on, or a liability of, any identifiable entity."*

The above definition stresses that while the asset is recorded digitally and that the functionality of the asset is enabled by way of cryptography, a further key characteristic of crypto-assets is that the asset is not representative of a claim vis-à-vis some debtor. By contrast, many definitions do not include the idea that the asset must not be at the same time a financial liability, but rather, highlight cryptography as the key property of crypto-assets, as in the case of MiCA:

> *"'crypto-asset' means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology…"*

Furthermore, the FSB (2022, 3; see also EBA, 2019) introduce the idea that crypto-assets are private-sector assets and that this classification does not fit public-sector assets:

> *"[c]rypto-assets are a type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology"*

Crypto-assets can be categorized as either "native" or "tokenized". Native crypto-assets, like Bitcoin, exist solely on a distributed ledger, while tokenized assets represent (technically and legally) assets that exist outside the ledger on which they are tokenised but are mirrored on it such as securities or real estate. Often, such tokenized assets are considered as crypto-assets which can lead to confusion. The method of holding an asset may alter some of its legal and technical characteristics, but normally not the essence of its cash flow characteristics. For example a bond remains a bond regardless of whether it is a bearer bond, a registered bond, or a tokenized bond, and often fungibility between the different ways to allow to hold a bond (if different ways are offered in parallel) is ensured. Therefore, from a linguistic perspective, it would be excessive to start calling a bond once being represented on a DLT platform as "crypto-asset", in the same way it would be excessive to call a bearer bond on paper a "paper-asset". It seems more proportionate to add the representation of the bond as a qualified, such as "a bond represented on a DLT", or if one wants to use the term "tokenization": "a tokenized bond".

b. Etymology

It is difficult to exactly pinpoint when the term “crypto-assets” emerged. Following the growth in the popularity of crypto-currencies,[29] central banks – to better differentiate Bitcoin and its unbacked siblings from central bank issued currencies – adopted the term crypto-assets. The term crypto-assets was however also applied later-on to “stablecoins” (see section 4.2 below), even though many stablecoins are fully backed with liquid financial assets, and are thereby analogous to e-money constructs from a functional perspective.[30]

c. Discussion

The term “crypto-asset” is transparent but inconsistently applied; some definitions exclude public sector assets issued on distributed ledgers, while others exclude assets that are not liabilities, like in the case of the Crypto-Asset Task Force (2019, 7):

> *“Although Bitcoin is the most prominent application of blockchain-based DLT, the use of this technology is currently necessary but not sufficient to characterize crypto-assets as a new asset class. In fact, the distinctive feature of crypto-assets...is the lack of an underlying claim/liability.”*

One could argue that in MiCA defining crypto-assets as digital representations of value or rights using cryptographic technology has the quality of being tautological: a crypto-asset is simply an asset (which can be for instance a native representation of value or a tokenized representation of rights) on a cryptographic key, and the lack of an underlying claim or liability should not disqualify something as a crypto-asset as it is irrelevant both to the cryptographic nature of the asset and its status as an asset; commodities, for example, are assets without being liabilities.

In practice however, the term “tokenized assets” is often preferred for real-world assets represented on a blockchain, while "crypto-assets" tends to refer to native crypto-assets. This distinction has the advantage of clarifying the nature of the asset – whether it exists independently or is a digital representation of something external. Financial securities like bonds are often qualified by the way they are held.[31]

If useful, the form and nature of the registry which documents ownership can be added as qualifying feature: “a bond held in paper format” (or bearer bond), “a bond held with a bank” (a registered bond) or “a bond represented in a blockchain” (a tokenised bond, if we want to use the term “tokenisation”). If a stablecoin is in essence an e-money construct, then it should not be called “crypto-asset” but “e-money represented in a blockchain” (or tokenised e-money). This is in contrast to the approach as for example taken in MiCA[32] Article 3(1)(5) which defines a “crypto-asset” as “…a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology.”

[29] Bearing in mind that the term “crypto-currencies” is problematic, as many in their unbacked guises – e.g. Bitcoin – are not fully fledged means of payments etc.

[30] In the sense that the issuer of the stablecoin fully backs its liabilities by say holding deposits at a commercial bank etc., which is analogous to issuers of e-money (i.e. Fintechs etc.).

[31] For instance, registered bonds, bearer bonds, and tokenised bonds.

[33] https://eur-lex.europa.eu/resource.html?uri=cellar:6f2f669f-1686-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF

4.2 Stablecoins

a. Current definition(s)

The FSB (2020) defines a **“stablecoin”** as:

> *“[A] cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets”.*

This definition is still used in e.g. CPMI (2024). What seems unusual in this definition is the insistence on *aiming* at something instead of *being* something. The FSB distinguishes between two types of stablecoins depending on their stabilization mechanisms: “Asset-linked stablecoins” that “purport to back stablecoins with fiat currency, assets or other cryptocurrencies” and “algorithm-based stablecoins” that “seek to use algorithms to increase or decrease the supply of stablecoins in response to changes in demand”. This definition is extensive and covers any type of asset. Algorithmic stablecoins are considered by now as unviable and do not play a relevant role relative to fully backed stablecoins. The “aim at” in the FSB definition probably relates to these dubious stablecoins which were not keeping their promise of a stable value. For other financial instruments, even if they failed sometimes in the past to keep their promises, definitions go however straight to what the instrument should do, and CPMI (2024) could therefore have streamled the definition.

Bullmann, Klemm and Pinna (2019, 9) define stablecoins more narrowly, encompassing only crypto-assets pegged to currencies and not to other types of assets, although again they emphasise the possible inability of the instrument to deliver on its promise:

> *“[D]igital units of value that are not a form of any specific currency (or basket thereof) but rely on a set of stabilisation tools which are supposed to minimise fluctuations of their price in such currency(ies)”.*

The Tether (2014) white paper does not use the term "stablecoin" but describes an asset-backed/pegged cryptocurrency as:

> *"[A]ny cryptocurrency whose price is pegged to a real-world asset, i.e., it is not a 'utility-backed' cryptocurrency." It describes Tether as "a digital token backed by fiat currency," with each unit, "TetherUSD" or "tUSD," representing a single unit of "cryptoUSD."*

In essence, the terms "asset-backed” or “asset-pegged” cryptocurrency used by Tether covers the same assets as the FSB's term "stablecoins”, making them synonyms (while the definition of Tether seems clearer because of avoiding the “aim at” or “supposed to” in the two previous definitions above). However, the term "asset-backed" implies that the peg is maintained through ownership of the pegged asset, while "asset-pegged cryptocurrency" does not require this. Algorithmic stablecoins, for example, can be *asset-pegged* but not *asset-backed*.

In the EU, MiCA does not explicitly define the term stablecoin and uses it only once, and refers to *“so-called algorithmic ‘stable coins’ that aim to maintain a stable value in relation to an official currency”*, highlighting that legislators take distance with the term stablecoins and in particular with algorithmic stablecoins. However, Articles 3(1)(6) and 3(1)(7) of MiCA distinguishes between two types of assets that the market would name stablecoins depending on which type of assets they are pegged to:

> *“Electronic money token’ or ‘e-money token’ is a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency;*
>
> *Asset-referenced token’ is a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies”*

The European Commission’s proposal for regulation on the establishment of the digital euro[33] of 2023 defines a stablecoin as *“a crypto-asset that references a fiat currency or a portfolio of liquid assets to stabilise its market value.”* This definition puts emphasis on fiat currencies or liquid assets hinting that the Commission compares them with money-like instruments.

In the US, the Clarity for Payment Stablecoins Act of 2023[34] does not define the term “stablecoin” but instead describes a “payment stablecoin” as:

> *“[A] digital asset…that is or is designed to be used as a means of payment or settlement; (B) the issuer of which— (i) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value; and (ii) represents will maintain or creates the reasonable expectation that it will maintain a stable value relative to the value of a fixed amount of monetary value; and (C) that is not— (i) a national currency; or (ii) a security issued by an investment company registered under section 8(a) of the Investment Company Act of 1940 (15 U.S.C. 80a–8(a)).*

In this way, US legislators seemingly emphasize their characteristic as a means of payment in addition to the reasonable expectation of value stability.

b. Etymology

The term "stablecoin" merges "stable" – which signifies steadiness or constancy – with "coin," a prevalent term in the crypto-currency realm applied to various forms of digital tokens. The crypto-community use of the term “coin” wrongly emphasises the money-ness of unbacked crypto-assets; the choice of "coin" links back to the foundational elements of digital currency introduced in the Bitcoin white paper, in which Nakamoto (2008) described an electronic coin as “a chain of digital signatures”—a concept central to all subsequent crypto assets which replaces the traditional definition of coin[35] of “a small, round piece of metal…that is used as money.”

Stablecoins are thus named because they attempt to combine the digital nature of crypto assets with the stability typically associated with real or perceived stores of value. Stablecoins aim at addressing the high volatility that characterizes most digital tokens and making them more suitable for everyday transactions and as a store of value. The importance of stability for a means of payment has been discussed from the earliest days of Bitcoin. Following (one of) Satoshi’s first forum posts presenting Bitcoin on 11 February 2008, Sepp Hasslberger highlighted on 20 February 2008 that “stability of the coins' value is desirable for long term use.”[36]

The term stablecoin regularly emerged on the forum BitcoinTalk between 2011 and 2014 but did not have a consistent meaning and was used to discuss vastly different projects, ideas, thought experiments, or simple considerations. In 2011, one user presented a proposal for a crypto-asset called a “stablecoin” designed to adjust its supply to maintain a consistent value compared to a currency at a specific point in time and follow a price index thereafter.[37] Concurrently, another participant[38] called a stablecoin an asset that would be made of 50% Bitcoin and 50% Bitcoin shorts,

[33] https://eur-lex.europa.eu/resource.html?uri=cellar:6f2f669f-1686-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF

[34] https://www.congress.gov/bill/118th-congress/house-bill/4766/text

[35] Cambridge dictionary: https://dictionary.cambridge.org/dictionary/english/coin

[36]https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?id=2003008%3ATopic%3A9402&page=1#comments

[37] https://bitcointalk.org/index.php?topic=29135.0

[38] https://bitcointalk.org/index.php?topic=44568.0

presumably to keep a stable value to the USD. In 2013, a contributor[39] proposed a definition for the term "stablecoin" as a class of crypto-currencies engineered to prevent their value from reaching extreme highs or lows regardless of adoption levels or external value changes, and defined sub-classes of stablecoins for coins pegged to different assets or currencies. That same year, another user[40] called "stablecoin" a crypto-asset for which the total market capitalization would remain stable (rather than the coin itself) by adjusting the quantity of coins in circulation based on their current market price. Others[41] suggested calling stablecoin a crypto-asset similar to Bitcoin but adjusting mining rewards to target a 2% annual growth rate rather than as an asset with a finite cap on coins. The concept of "stablecoin" was also used to describe a distributed ledger built around a coin mixing service[42] without any reference to price stability. Buterin (2014)[43] developed a theoretical framework for developing stablecoins by employing "vol-coins" and "stable-coins." In this model, stable-coins are pegged to a value of $1, while vol-coins function as a real currency that users can possess in amounts ranging from zero upwards. It is to be noted that in this model, stable-coins are effectively contracts-for-difference, meaning any negative balance in stable-coins represents a debt, secured by collateral worth at least twice the amount in vol-coins. These early discussions and proposals, ranging from insightful to rudimentary, highlighted the diverse and exploratory nature of the community's approach to conceptualizing stablecoins. However, it is to be noted these early concepts were primarily built toward algorithmic and decentralized solutions.

The modern term of stablecoins emerged in 2014. Lipton et Al (2020) highlight that the first notable internet searches for the word "stablecoin" began in 2014 and most sources on the history of stablecoins (see e.g. Coinchange, 2023; Daly, 2024)[44] date the first stablecoin projects to that year. Yet the specific term "stablecoin" was still rarely mentioned in foundational documents and proposals for cryptocurrencies designed to maintain stable values. For instance, early projects like BitUSD[45], the first dollar-pegged coin collateralized by BitShares, NuBits (2014)[46] collateralized by Bitcoin, and Tether (2014), purportedly supported primarily by bank deposits and other real-world assets, did not use the term in their initial white papers. Furthermore, academic proposals such as that of Iwamura et al (2014) – which sought to amend Bitcoin to enhance price stability – also did not incorporate the term. This absence of terminology extends to thought experiments like that of the former vice president of the St. Louis Fed Andolfatto (2015), who presented the idea of "Fedcoin" – a central bank digital currency aimed at ensuring exchange rate stability with the USD – without referring explicitly to "stablecoin" or acknowledging existing projects under that category. This indicates that while the principles of stablecoins were being explored, the term itself had not yet gained widespread acceptance within the cryptocurrency community by 2014.

c. Discussion

First, generally, the use of the term "coin" for both unbacked crypto-assets ("Bitcoin") and in "stablecoin" seems misleading because a coin is a bearer instrument while a blockchain/DLT rely on

[39] https://bitcointalk.org/index.php?topic=179918.0
[40] https://bitcointalk.org/index.php?topic=176748.0
[41] https://bitcointalk.org/index.php?topic=190030.0
[42] https://bitcointalk.org/index.php?topic=227766.0 and https://bitcointalk.org/index.php?topic=349198.0
[43] https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency
[44] See also https://www.deltecbank.com/news-and-insights/the-history-of-stablecoins/; https://www.oed.com/dictionary/stablecoin_n?tl=true#:~:text=The%20earliest%20known%20use%20of,stable%20adj.%2C%20coin%20n
[45] https://blog.bitmex.com/wp-content/uploads/2018/06/173481633-BitShares-White-Paper.pdf
[46] https://nubits.com/whitepaper

entry in ledgers. The choice of the term “coin” likely aimed at overselling decentralization achievable through DeFi.

Second, the definition of “stablecoin” provided by the FSB and market actors is broad and encompasses all crypto-assets that aim to maintain a stable value relative to any other asset(s), without distinguishing their (i) specific use cases, (ii) the type of assets they are pegged to, (iii) their backing mechanisms, (iv) their fungibility with the pegged assets (see Coste and Pantelopoulos, 2024), (v) their regulatory status, (vi) convertibility mechanisms, or (vii) potential remuneration.

A problem with this broad definition is that the term “coin” as used in common language is for money-like instruments, and that “stability” refers to a displayed goal but not necessarily to a credible attribute of the token which is often used as a marketing-like argument rather than to describe the intrinsic credibility of the peg. To this end, the term “stablecoin” should only be used to describe tokens that (1) have a credible means to achieve stability against a (2) currency or an asset that serves as a currency. The definition would not need to refer to an “aim” or what the instrument is “supposed to do”. Other terms like "asset-linked token” or “asset-referenced tokens” should be preferred for crypto-assets pegged to non-money like instruments or indexes. The scope of the term “stablecoin” should be broader than scope of the term “electronic money token”, or “tokenised e-money”, because the term e-money explicitly uses the term “money” which implies a state-sponsored reconnaissance that the token is of sufficient quality to be classified by legislators as money. From this perspective, MiCA was right not to use the term stablecoin and rather builds on the definition of electronic money tokens in relation with e-money to highlight the link and similarity between both.

Moreover, the overarching adoption of a widely used market term but insufficiently granular without clear, distinguishing details leads to semantic ambiguity and misinterpretation risk. A tokenized money market fund,[47] a payment instrument such as an electronic money token, and an alleged fraudulent scheme (see U.S. Securities and Exchange Commission, 2023) like TerraUSD can all meet the definition of stablecoin indexed to the USD and are regularly marketed to the public as such. This broad categorization is misleading, as it suggests a uniformity in stability and purpose among these varied products, which is contrary to reality.

In the US, the lack of regulatory clarity over the qualification of stablecoins led to legal disputes between the SEC and several market actors on the qualification of stablecoins as payment instruments.[48] Issuers have weighted on policy views to support that their products should be classified as payment instruments. Circle, the issuer of USDC, described its product as “payment stablecoin” lacking the profit generating attribute of an investment contract, while claiming that its largest competitors, Tether, and BUSD, were less “payment stablecoin” but more of a “trading stablecoin” mostly used for speculative activities (Liao, 2023). Further, the term "stablecoin" connotes stability, yet the mechanisms for maintaining such stability can vary significantly and are not apparent from the term itself. In practice, the stability of these coins largely depends on the specific mechanisms in use.

Regarding alternative options, Carter and Walsh (2020) proposed the term "cryptodollars" to classify currencies on the blockchain, drawing a parallel to Eurodollars[49] as dollars held in banks outside the US financial system. Their definition encompasses all stablecoins pegged to a currency and includes

[47] A money market fund tries to keep their net asset value (NAV) at a stable $1.00 per share https://www.investor.gov/introduction-investing/investing-basics/glossary/money-market-fund

[48] This is because the qualification of the product drives the regulatory requirements to which the issuer must adhere.

[49] Eurodollars refer to deposits of U.S. dollars in banks outside the U.S.

both those that are convertible for some assets held in reserve and those which attempt to target the return of some reference currency without offering convertibility. Derivaux (2024)[50] proposed a narrower definition of cryptodollars that exclusively includes dollar-denominated stablecoins redeemable for higher-level money. This focused approach may provide a clearer understanding of the specific characteristics and financial mechanics underlying these assets.

Finally, the term stablecoin is to some extent redundant, as after the demise of algorithmic stablecoins should be reserved for representations of e-money on a distributed ledger (and perhaps to other non-regulated stablecoins that are able to achieve stability in a credible way by being backed by a stock of high-quality assets). Fully backed stablecoins (i.e. those who indeed have credibility to be stable) are similar to e-money, and the fact that a financial asset is registered and transferable on a DLT is not per se changing its nature. Therefore, a better expression could be "e-money on a distributed ledger", or, if another asset is represented, such as gold: "gold represented on a distributed ledger", etc.

5. Tokenisation

a. Current definition(s)

The term **"tokenisation"** has been used in many ways. The traditional, 19th and 20th century meaning is recalled by Milne (2024, 5). More recently, but still not relating to DeFi, it refers in the field of payments to specific security related techniques within a payment process. For example, CPMI-World Bank (2020, 11) defines tokenisation as:

> *"…the process whereby sensitive data are replaced with a surrogate value, known as a token, in order not to expose the original data. More specifically, tokens used in payments are a disguised representation of underlying sensitive payment data (i.e. data that can be leveraged to carry out fraud), such as transaction account or payment card numbers, with the ultimate objective of protecting the underlying accounts…The use of tokens does not alter the normal course of payment processing, apart from the tokenisation and de-tokenisation processes."*

Buterin (2014) describes tokens as value counters in contracts in the original Ethereum whitepaper:

> *"on-blockchain token systems have many applications ranging from sub-currencies representing assets such as USD or gold to company stocks, individual tokens representing smart property, secure unforgeable coupons, and even token systems with no ties to conventional value at all, used as point systems for incentivization".*

CPMI (2024) defines token as "a representation of something else" which seems very broad even taking into account the diverse usages of the term. Also, one wonders if a token is not a "representation of something" instead of "of something *else*".

The meaning of tokenisation in the context of DeFi is provided for example by Lavayssière and Zhang (2024, 7-8):[51]

[50] https://cryptobanking.network/crypto-banking-101/

[51] Lesavre, Varin and Yaga (2021, 3) also underline the role of DLT (i.e. blockchain networks) during the course of tokenisation, while at the same time clarifying that in general many terms used can be misleading: "For the purpose of this paper, cryptographic digital tokens (or cryptoassets) will be referred to as tokens, with tokenization designating the concept of representing assets as tokens using blockchain networks. Certain terms

> *"Tokenization: Process of issuing a financial asset on a shared, programmable, and trust-minimized platform. This process involves legal and technical operations… Tokenization is the issuance of financial assets on a ledger that presents certain characteristics, such as being shared by several participants and providing trust."*

Watsky et al (2024) also highlight that tokenisation involves transforming assets stored on a conventional ledger to one where assets are stored on a distributed ledger (rather than say morphing assets stored on a conventional ledger to another conventional ledger), but also emphasise the role of smart contracts in the process of tokenisation:

> *"'Tokenized assets' and 'asset tokenization' refer to the product and process by which an entity uses smart contracts to issue tokens representing assets not conventionally issued on blockchains… Definitions of 'asset tokenization' tend to refer to the representation of traditional assets more broadly on blockchains or other DLTs, but we pay particular attention to the smart contracts responsible for issuing the tokens on the blockchain."*

Intensifying the idea that tokenisation can lead to revolutionary changes in the field of payments and settlement (but not necessarily through the use of distributed ledgers, but rather via some form of programmable platform), chapter 3 of the BIS (2023) annual report argues that:

> *"Tokenisation of money and assets has great potential, but initiatives to date have taken place in silos without access to central bank money and the foundation of trust it provides. A new type of financial market infrastructure – a unified ledger – could capture the full benefits of tokenisation by combining central bank money, tokenised deposits and tokenised assets on a programmable platform."*

The idea seems to be that by creating a "universal" (but permissioned) global distributed ledger system and by representing (tokenising) all key financial assets on it (central bank currencies, commercial bank money, securities, etc.), a new significantly more efficient global financial market infrastructure could be achieved and overcome complex layering and associated settlement risk.

b. Etymology

The use of the term "tokenization" has massively expanded in terms of meanings and popularity**. Over the last few years, at least four different interpretations of this term have been observed:**

(1) Tokenization in the payments-sphere initially referred to the process of replacing sensitive information like account data with non-sensitive data for the use in one transaction. Tokens allow the secure transfer of sensitive data by replacing it with a unique string of characters.

(2) For a brief period, there was much discussion regarding tokenization in the context of "account based" versus "token based" CBDC. CMPI-MC (2018) explains:

> *"Money is typically based on one of two basic technologies: tokens of stored value or accounts… Cash and many digital currencies are token-based, whereas balances in reserve accounts and most forms of commercial bank money are account-based."*

(3) The report seems to insinuate that tokenization in the electronic sphere is associated with the use of DLT. However, viable DLT infrastructure also ensure the integrity of positions of participants in a ledger and of related transfers, quite similar to accounts in a single ledger, and very differently from the circulation of money outside any ledger, like in the case of cash.

used in this paper do not have a fixed and well established meaning. While all terms used in this paper aim to adequately characterize the concepts and technologies discussed here, certain semantics may likely require further scrutiny."

The concept of token vs account based CBDC has rightly been considered as misleading (see also Pantelopoulos, 2025, chapter 11). Already Lee et al (2020) conclude that “these terms should be retired to avoid further confusion”. This has materialized and such distinctions have more or less disappeared in the course of 2023 at the latest.The crypto-verse has typically described tokenization in the context of the creation of so-called digital tokens on a blockchain to represent either digital or physical assets (e.g. gold). Tokens can be designed as fungible or non-fungible, such as NFTs.

(4) BIS (2023) presents tokenization as the future of (wholesale) payments without however referring to prominently to DLT in its definition of tokenization[52] and in its development of its idea of a “universal ledger” for tokenized financial assets:

> *“Traditional ledger systems and tokenised systems operate under fundamentally different rules. In traditional ledger systems, account managers are entrusted with maintaining and updating an accurate record of ownership. In contrast, in a tokenised setting, money or assets become “executable objects” that are maintained on programmable platforms. They could be transferred through the execution of programming instructions issued by system participants without the intervention of an account manager. While tokenisation does not eliminate the role of intermediaries, it changes the nature of that role. The role of the operator in a tokenised environment is as a trusted intermediary serving in a governance role as the rule book’s curator, rather than as a bookkeeper who records individual transactions on behalf of account holders. The claims traded on programmable platforms are called tokens. Tokens are not merely digital entries in a database. Rather, they integrate the records of the underlying asset normally found in a traditional database with the rules and logic governing the transfer process for that asset…”*

The emphasis has thus shifted from the idea of distributed ledgers to the one of programmability. One could find it contradictory that on one side tokenization was understood as representing assets by way of DLT, while in BIS (2023) it is a representation within a “unified ledger”. The two might be reconciled by considering that a unified ledger means a one single distributed ledger encompassing all assets being represented there as tokens. The unified ledger would therefore exist as a permissioned ledger with strong central governance and control by public authorities, which in turn however seems to betray some essential ideas of decentralized finance.

c. Discussion

The essence of tokenization seems to be the act of moving, from a legal and technical perspective, the representation of ownership in an asset (and the transferability of ownership) into a ledger. It is unclear why the essence of this act would be specific to DeFi platforms. For example, paying in banknotes (central bank money) into a bank and obtaining a bank deposit for it could be called “tokenization” in the sense that it is a technique used to transform the way a claim is registered from one form to another, although not necessarily using DLT/cryptographic techniques etc. Or, in the process of securities settlement in T2S, the security is represented in accounts controlled by the T2S system (they have been “tokenized” from a technical and legal perspective into these accounts) and can be exchanged against central bank money by way of DvP.

[52] This is despite BIS (2023) frequently referring to wholesale CBDC, which seems to imply the use of DLT (see section 6 below).

It could therefore be argued that the term "tokenization" and its common definition suffer from a lack of transparency, a monosemy and neutrality:

- **Transparency:** the term "token" has traditionally had the connotation of being a representation *outside of a ledger*, such as in the earlier use in discussions of "token-based vs. account based CBDC" (see also the detailed discussion in Milne, 2024, 4-6). Using it for issuance in DeFi was meant to suggest that decentralized ledgers are not ledgers at all and that the "tokens" in them could circulate like cash. This was misleading (and partially marketing) because an electronic record will never be like cash in terms of an absence of records of the effectuated transfer and change of ownership.[53] Relating to that, it is not clear why the term "tokenization" should be reserved to DLT (which are ledgers, even if "distributed" ones) and doing so over-emphasizes the specificity and novelty of DeFi.
- **Monosemy:** tokenization is in essence "representation" of ownership on a ledger, and it could be argued that the term already had a synonym and therefore was not needed.
- **Neutrality:** by not associating the term to the act of moving the representation of ownership of an asset to a traditional ledger, the term was used as a marketing device to over-emphasise the idiosyncratic nature and novelty of DeFi platforms. This does not imply that one should/can deny the idiosyncratic nature and novelty of DeFi platforms, but that the act of representing ownership of an asset on a platform is not specific to DeFi.

In sum: tokenization is in essence "representation" of ownership and transferability on a ledger, and the term is therefore largely redundant. Moreover, by creating the false connotation with a bearer instrument, the term has been misleading and mis-used to over-emphasise the idiosyncratic nature and novelty of DeFi platforms.

6. CBDC

In pre-electronic times, from early central banking in the 16th century to the times of the gold standard, central banks were rather liberal in grating access to their ledger money to non-banks.[54] Once banknotes appeared in the 17th century, central bank money could serve surface economies and settle payments taking place *remotely* away from the premises of the central bank. Remote *electronic* access to central bank ledgers *by banks* and the electronic recording of the ledger (instead of on paper) developed gradually over the 20th century.[55] Remote electronic access to central bank money *by*

[53] One side effect of the association of DLT and "crypto" with the concept of "tokens" has been that many retail users seem to believe that Bitcoin and other "crypto assets" are encrypted files that wholly reside in their crypto wallet. These holders wrongly believe that their assets are being transferred directly wallet-to-wallet on a true peer-to-peer basis (just as cash is). Of course, in reality, only the keys are in their wallet and the ledger entry is in the respective address on the respective blockchain. Holders feel as if, unlike a bank account, they really own the asset since they believe that they possess and completely control the crypto asset. That is, they believe that they would own and control a bitcoin or tokenised asset even if the blockchain were to disappear (in, for example, a disaster where either the blockchain was disrupted and/or the internet was unavailable and where they might otherwise have relied on gold). In contrast to crypto-assets, peer-to-peer encrypted file transfers of money are being developed. See e.g. Chaum et al (2021) and Goodell et al (2023).

[54] See Bindseil (2022, 4).

[55] See e.g. Smith (1956) or Board of Governors of the Federal Reserve System (1974), in which both shed some light on the case of the Fed, with a focus on Fedwire.

individuals and the ability to use it for payments (person-to-person and person-to-business) is not new either. The Bank of Finland experimented with pre-funded central bank money payment smart cards in Finland in 1987, launched the scheme in 1992 and operated it for three years.[56] According to CPSS (2003, 82), central bank employees in France, Germany, Switzerland and the UK had a central bank (electronic) current account in the 1990s and could use it for payments.

6.1 Retail CBDC

a. Current definition(s)

Definitions of "CBDC"

CPMI-MC (2018) defines CBDCs as "a digital form of central bank money that is different from balances in traditional reserve or settlement accounts". This would include retail electronic central bank money, while wholesale central bank money only to the extent that it would be "different" from existing balances in central bank accounts. Others seem to have assumed that "CBDC" means retail central bank money available in electronic form (e.g. Stanley, 2022; IMF, 2023).

Similarly, the Bank of England explains on its website that CBDC is "digital money a country's central bank can issue alongside cash" and in its further explanations considers it as the extension of electronic central bank money for retail payments.

The PBoC follows the same logic as MU (2022) notes that "CBDC as a new form of money and payment method could potentially facilitate enhancing resilience of the retail payment system, contribute to a better financial system, improving efficiency of the central bank payment system, and promoting financial inclusion of the society."

The US White House ("Technical evaluation of a US central bank digital currency system", September 2022) defines CBDC as "a digital form of a country's sovereign currency", thereby encompassing both the retail and wholesale electronic central bank money (including "traditional" RTGS balances).

Board of Governors (2022) defines CBDC as "a digital liability of a central bank that is widely available to the general public. In this respect, it is analogous to a digital form of paper money." Although reference is being made in the report to **"**the use of distributed ledger technology for wholesale payments" the term CBDC is not used in this context, suggesting that "CBDC" is again equivalent to "retail CBDC". The report also suggests that "newer technologies, such as blockchain" are only one possible technical option.

Definitions of retail CBDC

Others have focused directly on defining "retail" CBDC; i.e. the exclusive meaning of CBDC before CPMI-MC (2018).

According to the ECB (2024 - digital euro glossary) a retail CBDC is a "central bank liability in digital form offered to the general public (e.g., individual users, business users and governments or other public authorities) for retail payments." As the ECB has been using the term "digital" as a synonym of

[56] The business entity that issued Avant cards was fully owned by – and therefore on the balance sheet of – the central bank. After three years Avant became a privately held enterprise and was no longer backed by the central bank (Grym, 2020).

"electronic" in the context of CBDC, it is not clear why it does not refer in the definition to the available synonym "electronic" (to avoid circularity).

The EU Commission's draft legislation on digital euro states that "Like cash, a retail CBDC would be an official form of central bank money directly accessible to the general public, endowed with the status of legal tender. It would thus adapt the official forms of the currency to technological development, complementing cash."

The Bank of Japan (2020) uses the "general purpose" CBDC term from CPMI-MC (2018) and defines it as "CBDC intended for a wide range of end users, including individuals and firms." It adds that "There are two main variants of CBDC: 'wholesale' CBDC and 'general purpose' CBDC." In later reports on the BoJ on their CBDC experiments they no longer use the "general purpose" qualification and use the term "CBDC" as equivalent to "retail CBDC".

b. Etymology

The term "CBDC" was first used by the Bank of England around 2015. The ones who invented the term CBDC and worked first on the idea in the Bank of England seemed to have had in mind central bank money settled *on a blockchain/DLT* and thereby would have used the term "digital" specifically with that meaning in mind. The term CBDC started to be used in publications since 2016, with Barrdear and Kumhof (2016) already providing confusion on whether they had DLT in mind or not. In the abstract, they define CBDC as "a universally accessible and interest-bearing central bank liability, implemented via distributed ledgers, that competes with bank deposits as medium of exchange." However on p. 7, they provide a technology agnostic definition: "By CBDC, we refer to a central bank granting universal, electronic, 24x7, national-currency-denominated and interest-bearing access to its balance sheet." Today's (retail) CBDC projects are typically not universally accessible (the digital euro foresees restrictions in terms of geographical use and only natural person residents will be able to hold it, and only up to a certain threshold). Moreover, all announced CBDCs will be non-remunerated (see e.g. Bindseil and Senner, 2024 for an in-depth discussion).

Dyson and Hodgson (2016, 1) note (emphasis added):

> *"The Bank of England has already posed questions about the potential of digital cash, prompted by the ongoing rise of electronic means of payment, and the emergence of alternative currencies such as Bitcoin. One of the key questions to come out of the Bank's One Bank Research Agenda, released in early 2015, was: "From a monetary and financial stability point of view, what are the costs and benefits of making a new form of central bank money accessible to a wide range of holders?"*

And Dyson and Hodson (2016, 4) also note with great clarity (emphasis added):

> *"The Bank of England's research question couples the concept of digital currency with the technology of a distributed ledger payment system. This distributed ledger is the technology underlying Bitcoin … But the Bank of England is capable of issuing digital cash even without the distributed ledger technology. As Haldane (2015) put it: "In one sense, there is nothing new about digital, state-issued money. Bank deposits at the central bank are precisely that." … . Consequently, a central bank can provide 'digital cash' simply by allowing members of the public (and businesses) to hold digital deposit accounts at the Bank of England. This requires a 'centralised ledger' – essentially a collection of computers owned and maintained by the Bank of England. This negates the need for a distributed ledger system modelled loosely on Bitcoin."*

The need to make this clarification in 2016 despite the fact that a number of central banks provided electronic central bank accounts (obviously based on central ledgers) and related debit cards to staff already since the 1990s suggests that some researchers or central bankers already linked granting electronic access to central bank accounts to all citizens (a major functional innovation) with the sub-option to use a very specific and new “digital” technology for it (meaning DLT/blockchain etc.).[57]

The first major common report of central banks on electronic retail central bank money is CPMI-MC (2018) written in 2017 and published in March 2018. This report uses and finally establishes the term “CBDC” in the global central banking community. At the same time, this report caused linguistic ambiguity (discussed further below).

c. Discussion

The term “CBDC” could be generally ambiguous in that the term “digital” was initially used in the sense of “central bank money being distributed via DeFi”. In the field of retail CBDC, this ambiguity continues to a limited extent until today: while most now use the term “retail CBDC” for the idea to make central bank money accessible electronically to everyone (e.g. via a mobile phone, the money being recorded and settled electronically in some presumably central ledger), few sometimes still interpret the term “digital” in “CBDC” as referring to “crypto” technology (i.e. blockchain and DLT). In terms of naming their CBDCs, some central banks have opted for “electronic” (e-CNY, e-Krona, e-Naira) while others used “digital” (digital euro, digital pound, digital renminbi being renamed in 2021 to e-CNY).[58] Although some jurisdictions therefore use “electronic” in the name for their specific national retail electronic currency, no central bank has since 2018 tried to avoid the term CBDC (for the benefit of an acronym using “electronic”) when designating electronic access by non-banks to central bank money.

In line with Dyson and Hodges (2016), retail CBDC means granting access to central bank money in electronic (non-paper) form to parties (in particular natural persons, but possibly also non-bank firms) who over at least the last century had only access to central bank money in the form of banknotes; i.e. essentially non-banks. Central banks consider this to be a natural evolution in view of the digitalization of large parts of everyday life and of the economy, which also extends to payment transactions. In the euro area, for example, the share of cash payments at the point-of-sale (i.e. in physical shops) declined from 79% to 59% between 2016 and 2022, mainly for the benefit of card payments. In the US, cash use fell from 40% in 2012 to 19% in 2020, and in Sweden from 33% to 10% over the same period. If this trend continues or even accelerates, the role of cash and thus central bank money would decrease significantly for the benefit of private payment service providers. This would likely lead to a reduced usability of central bank money and frequency of conversion of bank deposits into central bank money. Retail (and non-bank firms) payment instruments in commercial bank money were also paper-based for a long time, notably relying on bills of exchange and cheques. Electronic retail payment instruments based on commercial bank money appeared in the last decades

[57] A 2017 paper published in the BIS Quarterly Review of 2017 introduced the term “Central bank crypto-currencies” (Bech and Garratt, 2017), but the term was not really used afterwards.

[58] It is also useful to distinguish between “currency” on one side and the underlying transfer system on the other side. So far, the term “retail CBDC” seems to be mainly used to refer to the digital/electronic version of physical cash (i.e. the “currency”) irrespective of the underlying system used to transfer it. By contrast, it seems that the term wholesale CBDC is often thought of as the combination of the currency and the underlying transfer system/platform, which is where the DLT part comes in. This has some oversight and regulatory implications, for example when considering the question of whether CBDC is an FMI and hence potentially subject to the PFMI (CPSS-IOSCO, 2012). Another similar distinction is between access to account information and for launching transfer orders (for example via the internet, using a mobile device on the user side) and how the accounts are stored. For the former the term “electronic access” is standard, while for the latter the potential distinction between electronic and digital might apply.

of the 20th century and have now practically crowded out their paper based-predecessors (cheques and bills of exchange). It would be counter-intuitive if only central banks were to not move on and continue relying exclusively on 17th century technology despite the progress of technology and the profound changes of society and payment habits. The electronification when transitioning from banknotes to retail CBDC refers both to the "currency" itself and the way the users hold and access it (banknotes in a physical wallet vs. holdings in or through e.g. a mobile-based wallet) and the settlement layer (banknotes are a single position in the central bank liabilities, while they are settled through physical hand-over; retail CBDC is essentially recorded in individual electronic ledger positions and transferred electronically within this ledger).

That said, the use of the term "CBDC" is inconsistent and hence there is still a heterogeneity of definitions in use, that in some cases, leads to the term "CBDC" becoming homonymic:

- The Board of Governors, the Bank of England and the IMF seem to use "CBDC" as implicitly meaning "retail CBDC" and without specific technology connotation (i.e. "digital" means "electronic").
- The ECB uses CBDC to mean any form of electronic central bank money, including RTGS balances.
- CPMI-MC (2018) introduced the term "wholesale CBDC" (see below) and proposed the definition that CBDC would be "different" from existing forms of digital bank reserves held with the central bank.
- Many central banks followed CPMI-MC (2018) and ever since have assumed that CBDC has two sub-forms, retail and wholesale CBDC and that wholesale CBDC does not include RTGS balances (see section 6.2).
- Very few still consider CBDC to imply generally the reliance on a blockchain (Mastercard 2024), but the large majority does not see such a link for retail CBDC.

A solution to the confusion could be to define **CBDC as central bank money in electronic form.** This is regardless of the exact IT architecture of the settlement layer. If CBDC is based on a particular ledger technology, this should simply be added as a qualification, like "CBDC settled in a central ledger" or "CBDC settled in a permissioned blockchain". "Retail CBDC" would be defined as "CBDC accessible and usable for citizens and possibly non-bank firms." Of course the term "CBDC" may also be replaced as it suffers from two issues: first the association by many of the term "digital" with blockchain/DLT technology and second that "central bank currency" is an unusual term, and instead "central bank money" is common. Both would suggest to use the term "central bank electronic money" and thus for the retail variant "retail central bank retail electronic money" – see also the related discussion below in section 6.2.3.

6.2 Wholesale CBDC

a. Current definition(s)

Panetta (2022), at that time member of the ECB's executive Board, defined wholesale CBDC as the "settlement of interbank transfers and related wholesale transactions in central bank reserves." The IMF (2023) seems to follow this logic and states that "[w]holesale CBDCs refer to digital forms of central bank reserves whose access is limited to banks and other financial institutions." The context of the statement makes clear that the term "digital" is used here as synonym to "electronic", i.e. without any connotation of DLT.

Consistent with CPMI-MC (2018), the BIS (2021) defines in its annual economic report wholesale CBDC as "a CBDC for use by financial institutions (wholesale transactions) that is different from balances in traditional bank reserves or settlement accounts". The SNB (press release 23 November 2023 on SNB launches pilot project with central bank digital currency for financial institutions) follows this BIS definition and uses the term wholesale CBDC as associated with DLT.

b. Etymology

The term "wholesale CBDC" was created by CPMI-MC (2018) and is subject to an inconsistency since the term "digital" in wholesale CBDC was – different from its use in "retail CBDC" meant to be identical to the one used by the DeFi industry when referring to "digital assets". The application of the term "wholesale CBDC" was limited to solutions using DLT/blockchain to avoid applying the newly introduced term CBDC to "traditional" deposits held by commercial banks with central banks. This approach perpetuated the ambiguity whether the "digital" in CBDC should be interpreted as "using DLT/blockchain".[59] At the same time CPMI-MC (2018) uses the term "CBDC" for retail ("general purpose") CBDC consistently in a *functional* sense (and not technology related manner, i.e. without a link to DLT and blockchain). The report somewhat acknowledges the problem in using "CBDC" for both retail electronic central bank money and for "wholesale central bank money based on DLT", but nevertheless proposes this definition with a sort of reference to its purpose: that it would help to highlight what is "different" from the existing central bank ledger money:

> *"CBDC is not a well-defined term. It is used to refer to a number of concepts. However, it is envisioned by most to be a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value. This would be an innovation for general purpose users but not for wholesale entities. Central banks already provide digital money in the form of reserves or settlement account balances held by commercial banks and certain other financial institutions at the central bank. This mix of new and already existing forms of central bank money makes it challenging to precisely define what a CBDC is. In fact, for purposes of analysing what may change, it is easier to define a CBDC by highlighting what it is not: a CBDC is a digital form of central bank money that is different from balances in traditional reserve or settlement accounts."*

The claim of CPMI-MC (2018) that "CBDC is not a well-defined term" was partially true in view of the ambiguities in the definitions provided for example by Barrdear and Kumhof (2016), but instead of proposing clarification of the term, the report perpetuated linguistic ambiguity by introducing the concept of "wholesale CBDC" in a way that was inconsistent with the standard understanding of the meaning of "retail CBDC".

[59] Excerpts illustrating how the report re-created the confusion of terminology: "Two main CBDC variants are analysed in this report: a wholesale and a general purpose one. The wholesale variant would limit access to a predefined group of users, while the general purpose one would be widely accessible." (p. 1); "Wholesale CBDCs, combined with the use of distributed ledger technology, may enhance settlement efficiency for transactions involving securities and derivatives." (p. 1); "In terms of wholesale markets, the main argument made is that settlement systems for financial transactions could be made more efficient – in terms of operational costs and use of collateral and liquidity – and more secure by using wholesale CBDC. … To meet evolving needs from financial markets and to ensure an overall stable and sound financial system, a number of central banks have been conducting experiments involving CBDC and its related underlying technology (in particular DLT). … Doubts remain regarding the maturity of the technology and the size of efficiency gains associated with the use of DLT."

c. Discussion

Ever since the 2018 report of CPMI-MC (2018), most central banks, but also BIS (2023a), WEF (2024), Atlantic Council (2024), etc. have used the term "digital" inconsistently across retail CBDC and wholesale CBDC (and more generally, i.e. beyond CBDC, "digital" is sometimes meant as synonym of "electronic" and sometimes meant to specifically refer to DLT/blockchain). For retail CBDC, it is used without any connotation to DLT/blockchain, i.e., simply meaning the access to electronic central bank money for all, while for wholesale CBDC, it is used with strict connotation to DLT ("or similar technology"), since electronic central bank money has been the reality for banks for many decades. The inconsistency of this approach was highlighted already by Panetta (2022):

> *"Let me start by clarifying some frequent misunderstandings about wholesale CBDC. First, there is confusion surrounding the term "wholesale"… , there is a widespread misconception that wholesale CBDC does not yet exist. In fact, central bank money has been available in digital form for wholesale transactions between banks for decades. This misconception is fuelled by the commonly held assumption that wholesale CBDC needs to be operated using DLT. But wholesale CBDC is not synonymous with DLT, as it can be based on any digital technology. In the euro area, the Eurosystem offers banks the possibility of settling wholesale digital transactions through its TARGET Services using a centralised ledger."*

Beyond the terminological issues in CPMI-MC (2018), it also seems counterproductive to treat the such-defined "retail" and "wholesale" in one go, be it in reports and analysis (BIS, 2018, BIS, 2023a, WEF, 2024; Atlantic Council, 2024), in statistics ("number of central banks worldwide working on CBDC" is frequently used as indicator as if it would be meaningful to aggregate the two) or in projects.

Following Panetta (2022), a meaningful definition of "wholesale CBDC" which avoids inconsistency with the common understanding of "retail CBDC" (and the definition given to it by CPMI-MC (2019)) would be: **"central bank money in electronic form only accessible to banks and a well-defined set of market infrastructures, public authorities and possibly non-bank financial institutions". An alternative solution would be to use "digital" in the context of CBDC (including retail) as meaning "based on DLT/blockchain" and "electronic" as meaning "accessed with electronic devices and stored electronically", i.e. not relating to a specific IT technology.** This would require that "retail CBDC" is renamed into "retail CBEC", i.e. retail central bank *electronic* currency. "Retail CBDC" would be a subcategory and only apply to "retail CBEC based on DLT/blockchain". The ECB could then consider renaming its "digital euro" into "electronic euro", analogous to e-krona and e-CNY. As a further improved variant to solution 2, one may use "central bank electronic money" (CBEM) instead of "central bank electronic currency". This would be somewhat more consistent with the use of the term "central bank money" (money issued by the central bank) while the term "central bank currency" is uncommon.. The variant to solution 2 would however have much higher transition costs. Moreover, it could appear that solution 2 would rely on a somewhat arbitrary definition of electronic v digital that is not based on linguistics but originates from early branding/marketing by the crypto industry. Furthermore, over the past decade or so, the term "electronic payments" has been replaced to a significant extent with "digital payments" for all type of non-paper-based payments (i.e. other than banknotes/coins and cheques). While using "digital" as synonym for "DLT/blockchain" might provide clarity and consistency for CBDCs it would possibly create issues for payments terminology more broadly. It would also have knock-on impacts on the use of the term digital in other domains (digital banking, digital ID, digital infrastructure, digitization etc.). Overall, we would nevertheless conclude that "central bank electronic money (CBEM)" would be the best term instead of CBDC, with "wholesale central bank electronic money" to designate the case of access only for banking institutions.

The definition we propose would include positions in central bank money held with the central bank's electronic ledgers, such as an RTGS system. It could then be further qualified for example with regards to the technology: "wholesale CBDC settled in a central ledger" or "wholesale CBDC settled in a permissioned blockchain", etc. Wholesale CBDC "based on DLT" could be implemented in different ways, as also explained in Neuhaus and Plooij (2023).

Under the above proposed definitions of retail and wholesale CBDC (which should be designated by the term CBEM), the differentiation relates to the access (in the same way as one would generally differentiate wholesale and retail central bank money). Over the last century, central banks have generally tended to restrict access to their ledger to domestic banks and government entities. In early central banking, access was typically unrestricted, and any merchant, corporate or wealthy citizen could open a deposit account with the central bank (Bindseil, 2019). Recent debates on broadening the set of eligible depositors are summarized in Bindseil and Senner (2024). Broadening access to central bank accounts beyond domestic banks is a policy issue which is independent of the discussion on the use of DLT for wholesale CBDC.

7. Conclusion

DeFi has become widespread since 2008. Despite doubts on some of the claimed use cases and losses of some investors because of false value promises and scams, DeFi is believed to have high potential for revolutionising payments and finance. In parallel to the rise of DeFi, an overall rather misleading terminology has developed, which can be explained by a combination of several factors. First, DeFi developed very rapidly since 2008. Second, ICT, database architecture, cryptography, and the functional architecture and processes of payment and settlement are technical and often complex. Last but not least, crypto-asset and crypto-infrastructure investors and DeFi grassroot fans have an interest to introduce and popularise terms which suggest the novelty and huge potential of DeFi.

Public sector institutions should be free of financial interests and marketing intentions and have a responsibility to help the public understand new technologies within the scope of their mandates. Sound terminology is the very basis for this. In a world of rapid innovations, terminology can initially appear adequate, but at a later stage turn out to be suboptimal or even inadequate and there is no reason to fatalistically accept path dependencies in this case, and thereby perpetuate confusion.

The paper identified a number of issues with the emerging key DeFi vocabulary, such as:

- **Crypto-assets:** this term should not be used for assets which are only *represented* on a DLT platform as their economic nature does not depend on the nature of the platform in which their ownership is recorded and in which ownership can be transferred. Bitcoin as an unbacked "DeFi-native" asset could still be called a crypto-asset, but a bond represented on a DLT platform is still a bond and should not be called a crypto-asset but a "Bond held on a DLT-platform". This is independent of whether the bond's primary issuance (i) took place in a standard way, and it only later was represented on a DeFi platform, or (ii) was directly via such a platform. Some legal and technical details relating to the bond may be impacted by it being on a DLT platform, but this is analogous to a bearer bond and a registered bond having each certain specificities. One might also go one step further and avoid the term crypto-assets also for Bitcoin and other unbacked, DeFi-native ledger entries. For those, the term "virtual assets" could be used to emphasize that no assets actually exist or only in a "virtual reality" created by the ledger entries in the DeFi platform and the surrounding narrative and terminology.

Alternatively, one could avoid the term “asset” all together to emphasize that no (real world) asset exists and use a term like “virtual ledger entries”.

- **Smart contracts:** this term, which is meant to designate computer code to execute financial processes on a DLT platform, is untransparent and biased. Such code is neither per se smart, nor is it a contract. The term should therefore be avoided. The same applies to other terms in the “crypto-verse” like “mining”, etc.
- **Stablecoin:** the term could be considered misleading and redundant. It is misleading because “Coin” (also in "Bitcoin”, “Altcoin” “Meme-coin”, etc.) wrongly suggests a bearer instrument (like “token”), but these “coins” are registered and transferred in a system-of-accounts database. “Stablecoin” is a redundant term in analogy of not calling assets tokenized into a DLT platform “crypto-assets”: e-money represented on a DLT platform is still e-money and should keep that name (with a possible qualification regarding the way it is represented and transferred). Unbacked (algorithmic) constructs which also have been called stablecoins have turned out to be unstable (or even unviable) so that using the term “stablecoin” for them was misleading not only in terms of the suggested bearer property of a “coin” but also with regard to the term “stable”.
- **Tokenisation:** the term is misleading. First, “token” suggests that the asset is a bearer instrument (at least this seems to be the historical meaning of token which was also taken up in the term “token-based CBDC” which was used prominently in 2017-2019), but it is now used for designating representation in (distributed) ledgers. Second, “tokenisation” seems to be about the act of representing in a legal and technical sense the ownership and the recording of transactions of an asset in a specific ledger, but it is unclear why the term would be reserved to DLT platforms, as the nature of this act seems independent of whether the ledger is distributed or central. It would be sufficient to refer to the act of newly representing the ownership of an asset on a ledger (a “ledger” being understood in this context, in contradiction with its traditional meaning before 2008, as a system of accounts to record ownership of an asset and its transfers).
- **Retail CBDC:** the term “digital” in CBDC could be replaced by “electronic” to remove ambiguity on whether retail CBDC means central bank money held on a DeFi platform (it does not). Moreover, the term “currency” should be replaced by “money” as “central bank money” is a common and well-fitting term while “central bank currency” is not. **“Retail central bank electronic money” (rCBEM)** would be defined as means of payments issued by the central bank in electronic form with broad access including by natural persons.
- **Wholesale CBDC:** the term as used in a technological sense in CPMI (2018) could be discontinued as it is non-transparent and inconsistent with the functional interpretation of “retail CBDC”. The meaning in CPMI-MC (2018) could be replaced by “wholesale central bank money represented on a DLT platform”. As there is no paper-based wholesale central bank money, a qualifier “electronic” would not be needed at all in the context of wholesale central bank money: wholesale central bank money is always electronic and never based on paper tokens.

We hope that this paper triggers further debate on, and ultimately improvements of terminology in the field of digital money and decentralized finance. This will also allow discussing their merits in a more focused, neutral, and productive way.

References

Allen, H., J. (2024). Hearing on next generation infrastructure: how tokenization of real-world assets will facilitate efficient markets, prepared statement. Wednesday, June 5, 2024.

Andolfatto, D. (2015). Fedcoin: On the desirability of a government cryptocurrency. *Macromania*. Available at: https://andolfatto.blogspot.com/2015/02/fedcoin-on-desirability-of-government.html

Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review*, December 2021, 21- 36.

Atlantic Council (2024). Standards and interoperability: The future of the global financial system, Issues brief by Ananya Kumar, Alisha Chhangani, Jennifer Lassiter, and Katherine Haar.

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2024). The technology of decentralized finance (DeFi). *Digital Finance*, *6*(1), 55-95.

Back, A. (2002). Hashcash-a denial of service counter-measure. Available at: http://www.hashcash.org/papers/hashcash.pdf

Bacon, J., Michels, J. D., Millard, C., & Singh, J. (2018). Blockchain demystified: a technical and legal introduction to distributed and centralized ledgers. *Richmond Journal of Law and Technology.*, *25*, 1.

BaFin (2024). Decentralised finance (DeFi) and DAOs

Bains, P. (2022). Blockchain consensus mechanisms: a primer for supervisors. *International Monetary Fund FinTech Notes* 2022/003.

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022a). Regulating the crypto ecosystem: the case of stablecoins and arrangements. *International Monetary Fund FinTech Notes* 2022/008.

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022b). Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets. *International Monetary Fund FinTech Notes*, *2022/*007.

Banca d'Italia (2022). Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, by Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli and Ciro Oliviero, Paper series on Mercati, infrastrutture, sistemi di pagamento, No 26.

Bank of Japan (2020). The Bank of Japan's Approach to Central Bank Digital Currency, October 2020.

Banque de France (2018). Payments and market infrastructures in the digital era, Banque de France.

Barrdear, J. and M. Kumhof (2016). The macroeconomics of central bank issued digital currencies, Bank of England, Staff Working Paper No. 605.

Bech, Morten and Rodney Garrat (2017). Central bank crypto-currencies, BIS Quarterly Review, September 2017, 55-70.

Bindseil, U. (2022). The case for and against CBDC – five years later, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038828

Bindseil, U., & Pantelopoulos, G. (2023). *Introduction to payments and financial market infrastructures*. Springer.

Bindseil, U., & Senner, R. (2024). Macroeconomic modelling of CBDC: a critical review. ECB working paper no. 2978.

BIS (2021). BIS Annual Economic Report 2021. *Bank of International Settlements*, Basle.

BIS (2023). Blueprint for the future monetary system: improving the old, enabling the new. BIS annual economic report for 2023, June 2023, Chapter 3, 85-118.

BIS (2023a). Central bank digital currencies: ongoing policy perspectives, joint report by 7 central banks and the BIS.

BIS (2023b). The crypto ecosystem: key elements and risks, report submitted to the G20 Finance Ministers and Central Bank Governors, *Bank of International Settlements*, Basle.

Board of Governors of the Federal Reserve System (2022). Money and Payments: The U.S.Dollar in the Age of Digital Transformation, Research and Analysis.

Board of Governors of the Federal Reserve System. "Federal Reserve Operations in Payment Mechanism: A Summary." *Federal Reserve Bulletin*, June 1976: 481-489.

Buckley, R. P., Didenko, A. N., & Trzecinski, M. (2023). Blockchain and its applications: A conceptual legal primer, *Journal of International Economic Law*, *26*(2), 363-383.

Budin, G. (2001). A critical evaluation of the state of the art of terminology theory, Journal of the International Institute for Terminology Research – IITF, Volume 12.

Bullmann, D., Klemm, J., & Pinna, A. (2019). In search for stability in crypto-assets: are stablecoins the solution?. *ECB Occasional Paper* No. 230.

Buterin, V. (2014). The search for a stable cryptocurrency. Available at: https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency

Buterin, V. (2016). Thinking about smart contract security. Available at: https://blog.ethereum.org/2016/06/19/thinking-smart-contract-security

Carsten, A. (2018). Money in the digital age - what role for central banks?, Lecture by Mr Agustín Carstens, General Manager of the BIS, at the House of Finance, Goethe University, Frankfurt, 6 February 2018.

Chaum, D. L. (1979). Computer systems established, maintained and trusted by mutually suspicious groups. Memorandum No. UCB/ERL M79/10, University of California, Berkeley, CA, February 22

Chaum, D. L. (1982). Computer systems established, maintained and trusted by mutually suspicious groups, *Doctoral dissertation*, University of California, Berkeley.

Chaum, D., Grothoff, C., Moser, T. (2021). How to issue a central bank digital currency. Swiss National Bank Working Paper 3/2021

Chisholm M. and A. Milne (2013). “The Prospects for Common Language in Wholesale Financial Services”, SWIFT Institute Working Paper No. 2012-005.

Coinchange (2023). The rise and fall of stablecoins: lessons from the history of failed stablecoins. *Coinchange blog*. Available at: https://blog.coinchange.io/the-rise-and-fall-of-stablecoins-lessons-from-the-history-of-failed-stablecoins/

Coste, C-E., & Pantelopoulos, G. (2024). Central Bank Money as a Catalyst for Fungibility: The Case of Stablecoins https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5044955

CPMI (2015). Digital currencies. Committee on Payments and Market Infrastructures November 2015.

CPMI (2017). Distributed ledger technology in payment, clearing and settlement - an analytical framework. *Bank of International Settlements*, Basle.

CPMI and Markets Committee (MC) (2018). Central Bank Digital Currencies, CPMI Paper No. 174.

CPMI and World Bank (2020). Payment aspects of financial inclusion in the fintech era, April 2020.

CPSS (1992). Delivery vs. payments in securities settlement systems, Report prepared by the Committee on Payment and Settlement Systems of the central banks of the Group of Ten countries, Basel, September 1992.

CPSS (2003). The role of central bank money in payments, Committee on Payment and Settlement Systems, August 2012.

CPSS (2012). Innovations in retail payments, Committee on Payment and Settlement Systems, May 2012.

CPSS-IOSCO (2012). Principles for financial market infrastructures, Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commission, BIS.

CPMI (2024). Tokenisation in the context of money and other assets: concepts and implications for central banks, Joint report of the Committee on Payments and Market Infrastructures (CPMI) and the BIS to the G20.

Cunliffe, J. (2023). The digital pound – speech by Jon Cunliffe, given at UK Finance.

Daly, L. (2023). What are stablecoins?, published at fool.com

De Filippi, P., & Wright, A. (2018). *Blockchain and the Law*. Harvard University Press.

Derivaux, S. (2024). Cryptodollars and the Hierarchy of Money, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5000167

Deutsche Bundesbank (2020). Money in programmable applications - Cross-sector perspectives from the German economy, Frankfurt am Main, 21 December 2020. Available at: https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf

Dyson, B. and G. Hodgson (2016). "Digital cash: why central banks should start issuing electronic money," Positive Money. England, Staff WP No. 605

ESMA (2023). Decentralised finance: a categorisation of smart contracts, ESMA TRV risk analysis, 11 October 2023.

ECB (2012). "Virtual currency schemes", Frankfurt am Main, October 2012.

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

——— (2015). "Virtual currency schemes – a further analysis", Frankfurt am Main, February 2015.

ECB (2023). Summary of collected inputs from MAG members, cross-currency and conditional payments.

ECB (2023b). Progress on the investigation phase of a digital euro – third report.

ECB Crypto-Asset Task Force. (2019). Crypto-assets: Implications for monetary policy, financial stability, monetary policy, and payments and market infrastructures. *ECB Occasional Paper Series* No. 223.

ECB Crypto-Asset Task Force. (2020). Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area. *ECB Occasional Paper Series* No. 247.

FATF. (2014). Virtual currencies, key definitions and potential AML/CFT risks, FATF Report, June 2014.

FSB. (2020). Recommendations for the regulation, supervision and oversight of global stablecoin arrangements – executive summary. https://www.bis.org/fsi/fsisummaries/global_stablecoins.pdf

Garratt, R., M. Lee, B. Malone, and A. Martin, "Token- or Account-Based? A Digital Currency Can Be Both," Federal Reserve Bank of New York Liberty Street Economics, August 12, 2020.

Garratt, R., & Monnet, C. (2023). An impossibility theorem on truth-telling in fully decentralised systems. *BIS Working Paper* No. 1117.

Goodell, G., Toliver, D.R., Nakib, H.D. (2023). A Scalable Architecture for Electronic Payments. In: Matsuo, S., et al. Financial Cryptography and Data Security. FC 2022 International Workshops. FC 2022. Lecture Notes in Computer Science, vol 13412. Springer, Cham. https://doi.org/10.1007/978-3-031-32415-4_38

Grimmelmann, J. (2019). All smart contracts are ambiguous. *Journal of Law & Innovation*, *2*, 1.

Grym, Aleksi (2018). The great illusion of digital currencies, Bank of Finland Economic Review, No. 1/2018.

Grym, A. (2020). Lessons learned from the world's first CBDC, Bank of Finland, BoF Economic Review.

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, (3), 99-111.

HM Treasury, FCA and Bank of England. (2018). Cryptoassets Taskforce: final report.

Hojo, M., & Hatogai, J. (2022). Realizing Programmability in Payment and Settlement Systems. *Bank of Japan Review*, No. 8, 2022.

IBM (2022). What are smart contracts? Available at: IBM.com

IMF (2023). Central Bank Digital Currency – virtual handbook, Chapter 2: "How Should Central Banks Explore Central Bank Digital Currency?"; Fintech note 2023/008 November 2023.

IOSCO (2022). IOSCO decentralized finance report, public report. OR01/2022, March 2022.

IOSCO (2023). Final report with policy recommendations for Decentralized Finance (DeFi). FR/14/2023, December 2023.

ISO704 (2022). Terminology work — Principles and, methods, 4th edition, July 2022.

Iwamura, M. & Y. Kitamura, T. Matsumoto, and K. Saito (2014). "Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money," Discussion Paper Series 617, Institute of Economic Research, Hitotsubashi University.

JP Morgan (2024). Understanding Programmable Payments, Programmable Money and Purpose-Bound Money.

Kahn, D. (1967). *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster.

Kalbaugh, G. E. (2016). Virtual currency, not a currency. *J. Int'l Bus. & L.*, *16*, 26.

Klass, G. (2023). How to Interpret a Vending Machine: Smart Contracts and Contract Law. *Geo. L. Tech. Rev.*, *7*, 69.

Koning, J. P. (2020). Programmable money isn't new, we've had it for ages. Available at: https://jpkoning.blogspot.com/2020/11/programmable-money-isnt-new-weve-had-it.html

Langie, A. (1922). *Cryptography*. Constable & Company, Limited.

Lavayssière, X., & Zhang, N. (2024). Programmability in Payment and Settlement. *International Monetary Fund Working Paper* No. 2024/177.

Lee, A. (2021). What is programmable money? *FEDS Notes*, June 2021.

Lesavre, L., Varin, P., & Yaga, D. (2021). Blockchain Networks: Token Design and Management Overview. National Institute of Standards and Technology, Gaithersburg, MD, NIST Interagency or Internal Report (IR) 8301.

Lipton, A., Sardon, A., Schär, F., & Schüpbach, C. (2020). Stablecoins, digital currency, and the future of money. Available at: https://wip.mitpress.mit.edu/pub/17h9tjq7/release/4

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of applied cryptography*. CRC press.

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law, innovation and technology*, *9*(2), 269-300.

Mik, E. (2019). Smart contracts: A requiem. *Journal of Contract Law, Forthcoming*.

Mills, D., Wang, K., Malone, B., Ravi, A., Marquardt, J., Chen, C., ... & Baird, M. (2017). Distributed ledger technology in payments, clearing and settlement. *Journal of financial market infrastructures*, *6*(2-3), 207-249.

Milne, A. (2024), Argument by False Analogy: The Mistaken Classification of Bitcoin as Token Money. Journal of Money, Credit and Banking. https://doi.org/10.1111/jmcb.13061

Mu, Changchun. (2022), "Theories and Practice of exploring China's e-CNY", published on the PBoC website. Available at: http://www.pbc.gov.cn/en/3935690/3935759/4749192/2022122913350138868.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-peer Electronic Cash System. White paper.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

Naudts, E. (2023). The future of DAOs in finance-in need of legal status. *ECB Occasional Paper*, (2023/331).

NuBits. (2014). Nu. *NuBits White Paper*. https://nubits.com/NuWhitepaper.pdf

Panetta, Fabio (2022), "Demystifying wholesale central bank digital currency", Speech, Frankfurt am Main, 26 September 2022.

Panetta, F. (2023). The digital euro: our money wherever, whenever we need it, Introductory statement by Fabio Panetta, Member of the Executive Board of the ECB, at the Committee on Economic and Monetary Affairs of the European Parliament.

Pantelopoulos, G. (2025). *Between payments and credit: an introduction to the IOU economy*. Palgrave Macmillan.

Pincock, S. (2006). *Codebreaker: The History of Secret Communication*. Bloomsbury Publishing USA.

Pinna, A., & Ruttenberg, W. (2016). Distributed ledger technologies in securities post-trading revolution or evolution?. *ECB Occasional Paper* No. 172.

Rohr, J. G. (2019). Smart contracts and traditional contract law, or: the law of the vending machine. *Clev. St. L. Rev.*, *67*, 71.

Rosenheim, S. (1996). *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet*. John Hopkins University Press.

Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*.

Schär, F. (2022). DeFi's promise and pitfalls. *IMF Finance and Development*. September 2022, 33-35.

Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons.

Smith, G. C. The Federal Reserve Leased Wire System: Its Origin, Purposes, and Functions." PhD dissertation (Rutgers University, 1956)

Stanley, A. (2022). The ascent of CBDC, Finance and Development, IMF September 2022, 48-49.

Sultanik, E., Remie, A., Manzano, F., Brunson, T., Moelius, S., Kilmer, E., ... & Schriner, S. (2022). *Are Blockchains Decentralized?: Unintended Centralities in Distributed Ledgers*. New York, NY, USA: Trail of Bits.

Szabo, N. (1994). Smart Contracts. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Szabo, N. (1996). Smart contracts: building blocks for digital markets. Available at: https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf

Szabo, N. (1997). The Idea of Smart Contracts. Available at: https://nakamotoinstitute.org/the-idea-of-smart-contracts

Tether. (2014). Tether: fiat currencies on the Bitcoin blockchain. White Paper.

US Rules Committee. (2024). RULES COMMITTEE PRINT 118–33 TEXT OF H.R. 4763, THE FINANCIAL INNOVATION AND TECHNOLOGY FOR THE 21ST CENTURY ACT.

U.S. Securities and Exchange Commission. (2023). SEC charges Terraform and CEO Do Kwon with defrauding investors in crypto schemes. Press release. Available at: https://www.sec.gov/newsroom/press-releases/2023-32

Walch, A. (2019). Deconstructing "decentralization": Exploring the core claim of crypto systems.

Watsky, C., Liu, M., Ly, N., Orr, K., Seira, A., Vida, Z., & Wu, L. (2024). Tokenized Assets on Public Blockchains: How Transparent is the Blockchain? *FEDS Notes*.

WEF (2024). CBDCs come in two forms: retail and wholesale. What's the difference? Feb 6, 2024.

Werbach, K. (2018). Trust, but verify: Why the blockchain needs the law. *Berkeley Technology Law Journal*, *33*(2), 487-550.

Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke lj*, *67*, 313.

Wittgenstein, L. (2010). *Philosophical investigations*. Initially published in 1953. John Wiley & Sons.

World Bank. (2021). Central bank digital currency, a payments perspective. World Bank Group.

Yaga, D. (2018). One Block at a Time – Helping to Build Blockchain Knowledge, *ITL Bulletin*.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. *NIST Internal Report* 8202.

Annex: List of glossaries

Public-sector glossaries:

- *CPSS (2001/2003), A glossary of terms used in payments and settlement systems, BIS, March 2003. https://www.bis.org/cpmi/glossary_030301.pdf*
- *CPMI Glossary of payments and market infrastructure terminology (2006). https://www.bis.org/cpmi/publ/d00b.htm*
- *ECB (2009), ECB glossary of terms related to payments; clearing and settlement systems. https://www.ecb.europa.eu/pub/pdf/other/glossaryrelatedtopaymentclearingandsettlementsystemsen.pdf*
- *ECB glossary on markets and payments (online). https://www.ecb.europa.eu/services/glossary/html/glossc.en.html*
- *ECB digital euro glossary (online). https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.dedocs220420.en.pdf*
- *US NIST (online). https://csrc.nist.gov/glossary*
- *World Bank (online): https://digitalfinance.worldbank.org/glossary*

DeFi industry glossaries (all online):

- *Coinmarketcap. https://coinmarketcap.com/academy/glossary*
- *Coindesk. https://www.coindesk.com/learn/glossary/*
- *Crypto.com. https://crypto.com/glossary*
- *Binance. https://academy.binance.com/en/glossary*
- *Mastercard. https://www.mastercardservices.com/en/industries/consumer-packaged-goods/insights/glossary-crypto-and-blockchain-terminology*
- *The Digital Pound Foundation (DPF). https://digitalpoundfoundation.com/digital-currency-glossary/*

Acknowledgements

We would like to thank Victoria Cleland, Svetla Daskalova, Ben Dyson, Anneke Kosse, Thomas Lammer, Alistair Milne, Todd Sarris, Bob Seeman, Takeshi Shirakami, Peter Stella, Peter Wierts for helpful discussions and comments. All remaining errors are ours.
This research is independently conducted by the authors and not directly connected to the Eurosystem's digital euro project. It should not be interpreted as reflecting the ECB's position on the design of the digital euro.

Ulrich Bindseil
European Central Bank, Frankfurt am Main, Germany; email: ulrich.bindseil@ecb.europa.eu

Charles-Enguerrand Coste
European Central Bank, Frankfurt am Main, Germany; email: charlesenguerrand.coste@ecb.europa.eu

George Pantelopoulos
Newcastle University Business School, Newcastle, Australia; email: george.pantelopoulos@newcastle.edu.au

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

PDF ISBN 978-92-899-7114-0 ISSN 1725-2806 doi:10.2866/1694378 QB-01-25-064-EN-N