


# Trust Without a Trustee? Rethinking Cryptocurrencies through the Locus of Trust

**Meriem Essoussi**
PhD Scholar, Cadi Ayyad University, Marrakech, Morocco

* Corresponding Author: **Meriem Essoussi**

## Article Info

**ISSN (online):** 2583-8261
**Volume:** 05
**Issue:** 06
**Received:** 10-09-2026
**Accepted:** 08-10-2026
**Published:** 06-11-2026
**Page No:** 47-55

**Abstract**
Cryptocurrencies are described as currencies, payment instruments, financial assets or commodities, depending on the institution and the discipline, and the literature has treated the technology and the economics of these assets largely apart. This conceptual article links the two through a single idea: cryptocurrencies are answers to the problem of keeping a shared record of ownership without a trusted keeper. We decompose institutional definitions and show that they diverge because each promotes a feature that matters to its own mission, and we define cryptocurrencies by three constitutive conditions: digital representation of value, cryptographic authentication of ownership, and validation by a protocol enforced by participants. We then argue that decentralised validation relocates trust instead of eliminating it, drawing on evidence about exchanges, mining and custody, and we map cryptocurrencies on two dimensions, the locus of trust and the anchor of value. The map positions payment cryptocurrencies, platform coins, tokens, stablecoins, permissioned projects and central bank digital currencies without overlap, and yields four propositions on risk, stability, regulation and investor behaviour. The framework offers economics, finance, computer science, law and Islamic finance a shared vocabulary and testable hypotheses.

**DOI:** https://doi.org/10.54660/IJSSER.2026.5.6.47-55

**Keywords:** cryptocurrency, trust, blockchain, stablecoin, central bank digital currency, typology, regulation

## 1. Introduction

When the Bitcoin white paper appeared in October 2008, it proposed a technical solution to a narrow problem: how to make electronic payments directly between two parties without going through a financial institution (Nakamoto, 2008) [38]. It appeared in the midst of the financial crisis, at a time of widespread distrust of banks, monetary authorities and regulators (Sebastião *et al*., 2021) [44]. Eleven years later, almost four thousand cryptocurrencies were listed and their combined market capitalisation exceeded 200 billion US dollars (Sebastião *et al*., 2021) [44]; the market has expanded considerably since. Some of these assets are used to pay, others to run applications, to vote on the rules of a protocol, to represent a share or a bond, or simply to hold a stable amount of dollars on a ledger.

This diversity has not been matched by conceptual clarity. International institutions, regulators and market practitioners each define cryptocurrencies in the way that suits their mandate, and the definitions rely largely on negation: a cryptocurrency is money that is not issued by a state, not regulated, not backed by anything intrinsic. Definitions by negation are fragile. They describe what the object is not, they say little about what it does, and they cease to be true when the context changes, for instance when a jurisdiction decides to regulate. Classifications suffer from a similar weakness. The usual lists place side by side categories defined on different bases, such as function (payment), technical layer (tokens), stabilisation mechanism (stablecoins) and issuer (central bank digital currencies), so that one asset can belong to several of them, and the lists have to be rewritten each time the market invents a new instrument.

A further difficulty is disciplinary. As Sebastião *et al*. (2021) [44] observe, cryptocurrencies and blockchain are intimately linked but have mostly been treated separately: blockchain has been studied chiefly in computer science, information systems and

cryptography, whereas cryptocurrencies, being tradable assets, have drawn the attention of economists, whose work focuses on price formation, efficiency and connectedness (see also Holub and Johnson, 2018; Corbet *et al*., 2019; Merediz-Sola and Bariviera, 2019; Giudici *et al*., 2020) [16, 25, 27, 36]. What is missing is a framework that explains how technical design choices translate into economic properties, and therefore why assets that carry the same label behave so differently.

This article proposes a different starting point. We argue that cryptocurrencies become intelligible once they are seen as answers to a single problem: how to maintain a shared record of who owns what when no participant is trusted to keep it. Every cryptocurrency addresses this problem, but each gives a different answer to two questions. The first is who produces agreement about the state of the ledger, which we call the *locus of trust*. The second is what, if anything, supports the value of the units, which we call the *anchor of value*. We contend that the disagreements over definitions, the differences in risk, the unequal monetary behaviour of crypto-assets and the diversity of regulatory treatment all follow from the combination of these two answers.

The article makes three contributions. First, it defines cryptocurrencies by the problem they solve rather than by what they lack, which makes it possible to explain why institutional definitions diverge and to separate the conditions that define the object from the features that merely vary. Second, it shows that decentralised validation relocates trust instead of eliminating it, and it links each design choice of the technology to a specific place where risk reappears, using the empirical evidence on exchanges, mining and custody. Third, it builds a map of cryptocurrencies on the two dimensions above, which replaces single-axis lists, locates stablecoins, permissioned projects and central bank digital currencies with precision, and yields four propositions that connect the position of an asset to its monetary, behavioural and regulatory characteristics.

The argument is conceptual and deliberately cross-disciplinary. It draws on economics for the theory of money, on computer science for the architecture of distributed ledgers, and on finance and law for the questions of price behaviour, risk and regulation, and it uses the empirical literature reviewed by Sebastião *et al*. (2021) [44] as a body of evidence against which the framework can be read. It is addressed both to scholars who study crypto-assets as a phenomenon and to those who use them as an empirical setting, for instance in behavioural finance or Islamic finance, where it matters to specify exactly which object is being studied.

The article proceeds as follows. Section 2 recalls why money is an institution of trust. Section 3 defines cryptocurrencies by the problem they solve. Section 4 explains how trust is produced without a trustee and where it reappears. Section 5 presents the map. Section 6 discusses the propositions and their implications, and Section 7 concludes.

## 2. Money as an Institution of Trust

Money works because each person accepts it in the expectation that others will accept it in turn. This circular expectation rests on two distinct forms of trust, and keeping them apart is the key to what follows.

The first is trust in the record. Most money today exists as entries in ledgers kept by banks and settlement systems, and a payment is an instruction to change those entries. For the system to work, participants must believe that the ledger is accurate, that it cannot be altered at will, and that each unit can be spent only once. The second is trust in the unit. Holders must believe that the unit will keep enough value, over the time they hold it, to be accepted in exchange and to serve as a standard for pricing. This second form of trust is what allows money to fulfil its three classical functions of medium of exchange, unit of account and store of value (Yermack, 2015) [57].

In modern economies, institutions supply both forms of trust. Banks and clearing systems keep the record, supervised by public authorities. The unit is guaranteed by the state and by a central bank whose mandate is to preserve its value, and legal tender status obliges creditors to accept it. These arrangements are effective, but they place trust in specific parties, who can fail, make errors, restrict access or debase the unit. The attraction of cryptocurrencies, and the reason they emerged against the backdrop of the 2008 financial crisis, lies in the promise to dispense with a trusted party for the first form of trust (Nakamoto, 2008; Sebastião *et al*., 2021) [38, 44]. Cryptocurrencies have no legal tender status, so their acceptance rests on the confidence of their users (Sebastião *et al*., 2021) [44].

Seen in this light, any new form of money, whatever its technology, has to answer two questions. Who keeps the record, and why should participants believe in it? And what gives the unit its value, and why should that value hold? Cryptocurrencies give a distinctive answer to the first question: the record is distributed among participants and its rules are enforced by a protocol rather than by an operator. Their answers to the second question vary widely, from nothing other than scarcity and demand, to a promise of redemption, to a reserve of external assets. We take these two questions as the axes of the analysis. The first defines what we call the locus of trust, and the second the anchor of value. Section 3 shows that the first question defines what a cryptocurrency is, whereas the second is the main source of the differences between cryptocurrencies.

## 3. Defining Cryptocurrencies by the Problem They Solve

### 3.1. Why Institutional Definitions Diverge

Institutional definitions are usually reviewed one by one, which shows what each institution thinks but not why they disagree. Read together, they reveal a pattern. The European Central Bank (2012) [20], concerned with monetary sovereignty, describes a type of unregulated digital money, issued and usually controlled by its developers and accepted within a specific virtual community. The International Monetary Fund, as reported by He *et al*. (2016) [26], treats cryptocurrencies as an advanced form of virtual currency and stresses a purely digital representation of value, issuance by non-government entities and a proper unit of account. The Bank for International Settlements (2017) [3], concerned with financial stability, presents digital currency systems whose value is set by supply and demand, comparable to a commodity such as gold but without intrinsic value, relying on distributed ledgers that allow peer-to-peer exchange without intermediaries. The Financial Action Task Force (2014) [22], concerned with money laundering, insists on convertibility into conventional currencies and on the use of public and private keys to transfer value. The World Bank (2018) [55] distinguishes cryptocurrencies, a subset of digital currencies, from electronic money by their reliance on decentralised consensus obtained through cryptographic

techniques. The general-language definition of Larousse (2022) [31] describes a virtual means of payment, used mainly on the Internet, that relies on cryptography to secure transactions and the creation of units and that escapes the control of regulators and central banks.

Only one feature is common to all of these definitions: a digital representation of value. Every other feature appears in some of them and not in others, and in each case it is the feature that matters for the institution's own mission. Most institutions nonetheless converge on treating cryptocurrencies as a subset of digital assets or virtual currencies with a strong autonomy from the traditional financial system. The divergence is therefore not an error but the effect of different vantage points. Moreover, several of the features retained are negations: unregulated, not issued by a state, without intrinsic value, escaping central banks. A definition built on negation depends on the surrounding institutional context. It ceases to be true when the context changes, which is exactly what happens when a jurisdiction decides to regulate.

### 3.2. Three Constitutive Conditions

We propose to define the object by the problem it solves, as set out in Section 2: keeping a shared record of ownership without a trusted keeper. This leads to the following definition. *A cryptocurrency is a digital representation of value whose ownership is authenticated by cryptographic techniques and whose creation and transfer are recorded and validated by a protocol enforced by network participants rather than by a central operator.* It rests on three conditions, each of which is constitutive in the sense that the object would become a different kind of object without it.

The first is that value is represented digitally. Without this condition there is no digital asset to speak of. The second is that ownership is authenticated by cryptography. The word itself points in this direction: the prefix comes from the Greek for hidden, and cryptography is the set of techniques that secure transactions, control the creation of units and make these assets resistant to forgery. A holder proves the right to spend a unit by producing a digital signature that only the holder of a private key can produce (Antonopoulos, 2017) [2]. Without cryptographic authentication, a participant could claim units that belong to someone else, and an operator would be needed to settle the dispute. The third condition is that validation is performed by a protocol enforced by participants and not by a central operator. This is what separates a cryptocurrency from electronic money or from a bank database, a distinction the World Bank (2018) [55] itself makes. It is also the most demanding condition, since it requires a solution to a problem that digital money has always solved through an institution. Section 4 explains how it is met.

The features on which institutional definitions diverge are contingent in the same sense: they can vary between assets or over time without altering the nature of the object. The identity of the issuer ranges from a dispersed community to a company. Regulatory status differs between jurisdictions and changes over time. Stability, convertibility and the existence of a proper unit of account depend on how each asset is designed and used. These features do not decide whether an asset is a cryptocurrency. They decide where it stands among cryptocurrencies, and for that reason they supply the dimensions of the map developed in Section 5. In this sense the disagreements in the literature are not noise: they are an informal first draft of a classification.

### 3.3. A Cryptocurrency Is Not Necessarily Money

The definition says how the record is kept. It says nothing about whether the unit is trusted, and therefore nothing about whether the asset is money. This is a separate, empirical question, which can be asked of each asset using the three classical functions of money.

As a medium of exchange, cryptocurrencies allow peer-to-peer transfers without a bank, including across borders, but acceptance remains narrow. Katz (2017) [28] reported that only five of the top 500 online merchants accepted Bitcoin at the end of 2016, and three at the end of 2017, a decline that supports the view of Bitcoin as a vehicle for speculation rather than payment (Baur *et al*., 2018b; Sebastião *et al*., 2021) [6, 44]. As a unit of account, Yermack (2015) [57] concludes that cryptocurrencies provide an inferior service, and goods and wages are almost never priced in them. As a store of value, the capped supply of some assets suggests scarcity, which led Selgin (2015) [45] to describe Bitcoin as a synthetic commodity money that has no nonmonetary value, like fiat money, but is absolutely scarce, like commodity money. Yet price volatility weakens the function considerably. Over 2014–2019, the daily standard deviation of Bitcoin returns was 3.91 per cent, against 2.32 per cent for crude oil, 0.78 per cent for gold and 0.50 per cent for the USD/EUR exchange rate (Sebastião *et al*., 2021) [44]. The evidence on safe-haven properties is mixed (Dyhrberg, 2016a; Baur *et al*., 2018a; Smales, 2019) [5, 19, 46], and on 12 March 2020 the Bitcoin price fell by about 37 per cent in twenty-four hours while traditional markets were also falling (Conlon and McGee, 2020; Sebastião *et al*., 2021) [15, 44].

The conclusion is that the monetary character of a cryptocurrency is a matter of degree and varies from one asset to another. It does not follow from the technology, which is common to all of them, but from the second form of trust identified in Section 2, trust in the unit. This is why the second dimension of the analysis, the anchor of value, is the most revealing.

## 4. How Trust Is Produced Without a Trustee

### 4.1. Agreeing on One History

A digital file can be copied at no cost. A digital unit of value therefore requires a mechanism that prevents the same unit from being spent twice, the double-spending problem. Earlier attempts at digital cash, such as e-cash, hashcash, b-money or bit gold, did not thrive because they relied on a trusted third party to solve this problem (Narayanan and Clark, 2017; Sebastião *et al*., 2021) [39, 44]. In conventional systems a bank or a payment operator keeps the ledger, puts transactions in order and rejects the second attempt to spend a unit. Nakamoto (2008) [38] proposed to obtain the same result in a peer-to-peer network where no participant is trusted individually. The question is how a group of strangers can agree on a single, ordered history of transactions.

The answer combines several elements. Each participant holds a copy of the ledger, so there is no central server to attack or to trust. Ownership is established by public-key cryptography: when a person A wishes to send bitcoins to a person B, A signs the transaction with a private key, and the nodes of the network verify the signature with A's public key (Antonopoulos, 2017; Nakamoto, 2008) [2, 38]. The keys are

held in wallets, which means that owning a unit is the same thing as controlling a private key (Antonopoulos, 2014) [1]. Valid transactions are grouped into blocks, and each block is linked to the previous one by a cryptographic fingerprint, so that altering past data would be evident and would require rewriting the whole ledger from the tampered block onwards, against the independent verification of all the other nodes (Sebastião *et al*., 2021) [44]. The chain of blocks, copied across the network, forms a distributed ledger (Narayanan *et al*., 2016) [40].

Two further elements complete the architecture. The first is the consensus mechanism, which decides which block is added next when several participants propose different ones. Together with incentives that reward honest validation and penalise dishonesty, it replaces the operator's authority with a rule that participants have an interest in respecting. The second is programmability. Smart contracts, computer programs that encode agreements and execute automatically on the ledger (Szabo, 1997; Swan, 2015) [49, 50], were present in a limited form in the original Bitcoin ledger and were popularised by Ethereum, whose language can in principle express any computation (Sebastião *et al*., 2021) [44]. Here the trust that was once placed in an institution is placed in a procedure, and in code.

Blockchain is therefore a technology broader than cryptocurrencies, which are one application of it, and it has uses in sectors such as health, logistics and public governance (Tapscott and Tapscott, 2016; Swan, 2015) [49, 51]. The distinction matters for regulators, who must avoid stifling the technology by treating it as identical to the assets built on it. Sebastião *et al*. (2021) [44] go further and argue that blockchain is here to stay whereas cryptocurrencies, as they exist today, are probably the poorest example of how to use it.

### 4.2. Three Design Choices and What Each Asks Participants to Trust

At each step of this architecture, designers make choices. Three of them matter most, because each one changes what participants must trust.

The first concerns access to validation. In a permissionless ledger anyone can take part in validating and adding blocks, as in Bitcoin, Litecoin and Bitcoin Cash. In a permissioned ledger, access is controlled by an administrator or a consortium and only identified participants can validate; some permissioned ledgers can be read by anyone, others are closed altogether. Ripple, used mainly for interbank transfers, is usually cited as an example of the permissioned design (Swan, 2015) [49]. Because participants are known, the consensus algorithms can be computationally lighter and faster, as with Round Robin, Proof of Authority or Proof of Elapsed Time (Castor, 2017) [11], and misbehaviour can be handled by revoking access and by legal means (Yaga *et al*., 2019) [56]. Openness favours resistance to censorship, whereas restriction favours control and efficiency. In the first case participants trust the open network, and in the second they trust the admitted validators.

The second concerns the consensus mechanism. Under Proof of Work, validators known as miners compete to solve computationally costly puzzles, and the right to add a block goes to the first to succeed (Antonopoulos, 2017) [2]. Rewriting history would require redoing an enormous amount of computation, which gives the ledger its security, at the price of high energy consumption (Nakamoto, 2008) [38]. Estimates of that consumption differ widely: an index based on mining revenues gave 73.12 TWh for the second half of 2019, whereas a lower bound computed from the hash rate and the efficiency of the best hardware gave 23.38 TWh per year (Li *et al*., 2019; Sebastião *et al*., 2021; see also de Vries, 2018) [18, 33, 44]. Participants under Proof of Work trust that no single party can command a majority of the computing power. Under Proof of Stake, validators lock up a quantity of the cryptocurrency and are selected in proportion to their stake, a design used by Cardano or NEO that uses far less energy (Narayanan *et al*., 2016; Zheng *et al*., 2017) [40, 60]. Participants then trust that the stake is sufficiently dispersed, and critics note that the largest holders validate more often and earn more, which may lead to progressive concentration. The distinction is not static. Ethereum, the second largest network, moved from Proof of Work to Proof of Stake in September 2022, and Cambridge estimates put the resulting reduction of its electricity consumption at more than 99.9 per cent (Neumueller, 2023) [41]. Governments can also internalise the environmental externalities of energy-intensive designs through fiscal and regulatory tools (Truby, 2018) [52].

The third concerns the issuance policy. Some assets have a capped or scheduled supply, as Bitcoin does with its limit of 21 million units, which makes them deflationary by design, whereas others have an open-ended supply, which gives their managers more flexibility and exposes holders to dilution. These are tendencies, not rules: supply policy is a design choice that applies to native coins and tokens alike. Here participants trust that the rule will not be changed.

These three choices are largely independent of one another. An asset can be permissionless and capped, or permissioned and open-ended, and so on. This independence is one reason why no single list of categories can describe the field.

### 4.3. Trust Relocated, Not Abolished

Blockchain is often said to make intermediaries obsolete, since trust is no longer guaranteed by an institution but by cryptographic mechanisms and the nodes of the network (Yermack, 2017) [58]. The evidence suggests a more careful statement: trust is displaced, not eliminated. It no longer rests on a bank, but it still rests on something, and what it rests on differs from one asset to another. Three places where it reappears can be documented.

The first is the exchange. Peer-to-peer interactions are now marginal, and most trades occur through centralised online exchanges (Rauchs *et al*., 2018) [43]. The first of them, Mt.Gox, held more than 80 per cent of the market in 2010–2012 (Brandvold *et al*., 2015) [9], and eight exchanges have accounted for roughly 90 per cent of Bitcoin trading volume since 2014 (Sebastião *et al*., 2021) [44]. These intermediaries hold users' keys and connect them to national currencies, and they have been the site of thefts, of reports of fictitious trading volumes and of price manipulation schemes such as pump-and-dump (Gandal *et al*., 2018; Sebastião *et al*., 2021) [24, 44].

The second is the miner and the holder. The increase in capital requirements and the fall in mining rewards have created barriers to entry, and the five largest miners mined more than 85 per cent of Bitcoin blocks in 2016 (Vranken, 2017) [54], while most Bitcoins are held by a handful of large holders (Sebastião *et al*., 2021) [44]. The third is the code and its maintainers. The immutability of the ledger holds only if no attacker can dominate more than half of the nodes, errors in the software or in smart contracts can produce erroneous

behaviour, and permissioned ledgers need governance mechanisms of their own (Yaga *et al*., 2019) [56]. Rules that cannot be changed by an operator can still be changed by a sufficiently large coalition, as protocol forks have shown. Sebastião *et al*. (2021) [44] conclude that the libertarian ideal that underlay the creation of Bitcoin has been subverted. The Bank for International Settlements (2017) [3] accordingly warns that removing intermediaries raises challenges of security and liquidity and calls for a regulatory framework adapted to the technology.

The question to ask of any cryptocurrency is therefore not whether it needs trust but where trust now lies. We call this the locus of trust, and we distinguish three cases: an open protocol and the participants who validate it, a restricted set of admitted validators, and a central operator such as a central bank. This is the first dimension of the map in Section 5.

## 5. A Map of Cryptocurrencies

### 5.1. Two Dimensions

The two questions raised in Section 2 and refined in Section 4 give the two dimensions of the map. The first dimension is the locus of trust: who produces agreement about the state of the ledger. We distinguish an open protocol, in which anyone may validate, a restricted set of admitted validators, and a central operator. The second dimension is the anchor of value: what supports the value of the unit. We distinguish four cases. In the first, nothing supports the value other than scarcity and demand, so that value depends on the beliefs of holders and on the supply rule. In the second, value is supported by use or by rights: demand arises from the need to use a network or a service, or from rights attached to the asset, such as voting power. In the third, value is supported by an external asset or claim held by an issuer, such as a reserve of national currency, a pool of other crypto-assets, a commodity, or a share or bond. In the fourth, the anchor is sovereign: the unit is legal tender guaranteed by the state. The usual functional labels, payment, platform, governance and so on, are not an additional axis. They follow from the position of an asset on the map and can be read as a secondary description of it.

**Table 1:** The locus of trust and the anchor of value: a map of cryptocurrencies

| Locus of trust | Scarcity and demand only | Use or rights | External asset or claim | Sovereign |
|---|---|---|---|---|
| Open protocol | Bitcoin, Litecoin, Monero, Dogecoin, Bitcoin Cash | Ether (fuel of a smart-contract platform); Storj (service token); MKR (governance token) | Tether and other stablecoins backed by national currency, crypto-assets or commodities; security tokens | Not possible: legal tender requires the state |
| Restricted validators | Rare | Tokens used within consortium platforms | Libra project (association-governed ledger with a reserve of assets); JPMorgan Coin on Quorum | Wholesale CBDC prototypes (Project Jasper, Project Ubin) |
| Central operator | Contradictory: a central issuer controls supply | Rare | Rare | Retail CBDC (digital yuan, Sand Dollar) |

***Source:*** author elaboration. Examples are illustrative and not exhaustive; real assets may lie between cells.

### 5.2. Reading the Map

The upper left cell contains cryptocurrencies in the strictest sense of Section 3: participants trust only a protocol, and nothing supports value other than scarcity and demand. Bitcoin and its imitators belong here. This is the position in which monetary behaviour is weakest, since the second form of trust, trust in the unit, has nothing to rest on except the belief of holders.

Moving to the right along the first row, each step adds an anchor, and each anchor reintroduces a trustee. The value of Ether is supported by the need to pay for operations on its network, which places trust in the continued viability of the platform. Service and governance tokens rest on the continued usefulness of the service or on the authority of the community that votes. Stablecoins push the logic further. Their units circulate on an open ledger, so the record is protected by the protocol, but their value depends on a reserve held by someone, usually a company; they are designed to limit price fluctuations, and different designs exist, with different risks (Bullmann *et al*., 2019) [10]. Two kinds of trust coexist, trust in the protocol for the record and trust in an issuer for the unit. The practical lesson is that stability is bought by reintroducing a trustee. Algorithmic designs attempt to obtain stability from protocol rules alone, leaving the anchor column empty, and their fragility, illustrated by the collapse of TerraUSD in May 2022, suggests that rules and incentives cannot easily replace a credible anchor.

The second row is where large private and public projects have looked for a compromise. The Libra project announced in 2019 by a consortium led by Facebook had three parts: a secure and scalable blockchain, a reserve of assets designed to give the unit an intrinsic value and avoid wide fluctuations, and an independent association to govern the system (Libra Association, 2019) [35]. In the vocabulary of the map, validation was restricted to the members of the association and the anchor was an external reserve. Strong regulatory pressure, owing to the systemic risks identified by central banks, led the founders to scale the project back (Sebastião *et al*., 2021) [44], and it was later wound down. Banks follow the same logic with permissioned platforms: JPMorgan, for instance, was reported to be considering a digital coin supported by its own Quorum blockchain, a platform already used to run an interbank network of more than 300 banks (Chang and Harano, 2020; Sebastião *et al*., 2021) [12, 44]. Central banks, for their part, have simulated real-time gross settlement on distributed ledgers whose participants are identified, as with Project Jasper in Canada and Project Ubin in Singapore (Chapman *et al*., 2017; Monetary Authority of Singapore, 2017) [13, 37], which place wholesale central bank digital currency prototypes in the restricted-validator row with a sovereign anchor.

The lower right cell holds retail central bank digital currencies. They combine a central operator with a sovereign anchor, and they have the strongest monetary properties of all, since they are legal tender and are guaranteed by the state. They may use technologies close to those of cryptocurrencies, but they fail the third condition of the definition, since validation is not enforced by participants rather than by a central operator. They are therefore a boundary case, included to show what the opposite pole looks

like: transactions can be traced by the authorities, tax levies can be applied automatically, and holders do not enjoy the anonymity or the decentralisation of Bitcoin. In 2019, a survey of 63 central banks, covering about 80 per cent of the world population and 90 per cent of world output, found that half of them were experimenting with the technology and a quarter had or would soon have the authority to issue a digital currency (Barontini and Holden, 2019) [4]. The motivations are efficiency and resilience of payments, financial inclusion and, above all, the effectiveness of monetary policy, which a widely accepted private cryptocurrency could undermine (Bech and Garratt, 2017; Sveriges Riksbank, 2017; Sebastião *et al*., 2021) [7, 44, 48]. Projects such as the digital yuan, the Bahamian Sand Dollar and the Swedish e-krona have since moved from analysis to experimentation, and they raise their own risks of disintermediation of banks and of bank runs towards risk-free central bank money (Bech and Garratt, 2017) [7].

The empty cells are informative. A central issuer that controls supply cannot credibly offer scarcity alone as an anchor, and an open protocol cannot offer a sovereign anchor, since legal tender requires the state. The space of viable designs is therefore smaller than the number of assets suggests, and most of the diversity of the market lies along the first row.

### 5.3. What the Map Corrects

The map removes four difficulties of the usual lists. The most common classification distinguishes payment cryptocurrencies, tokens, stablecoins and central bank digital currencies. It is useful as a first map, and the map proposed here can be seen as its derivation from first principles: each of its categories is a region of the grid. Payment cryptocurrencies such as Bitcoin, Litecoin, Monero, Dogecoin or Bitcoin Cash occupy the upper left cell. Tokens, issued on top of an existing ledger (Ethereum was the first to make this possible at scale), occupy the use-or-rights column and, for security tokens, the external-claim column, with utility, service, security and governance functions as sub-descriptions. Stablecoins occupy the external-asset column. Central bank digital currencies occupy the sovereign column. Four corrections follow. The map removes overlaps: an asset such as Tether, which is at once a token, a stablecoin and a payment instrument in the usual typologies, has one position. It reduces the distinction between coins and tokens to a technical descriptor, whether the asset has its own ledger or is issued on another, which is independent of its position: Ether is the native coin of its network and powers its smart contracts and decentralised applications, whereas many tokens are issued on top of it, and a classification that treats the former as a token hides this difference. It replaces the idea that stability means backing by national currencies with a set of mechanisms that carry different risks: reserve and counterparty risk when the anchor is an external asset, liquidation risk when it is a pool of crypto-assets, and failure of the design when it is a rule. And it treats central bank digital currencies as a pole of comparison rather than a category of cryptocurrency.

The map also absorbs new objects without redesign, by asking the same two questions of them. Non-fungible tokens certify unique items and differ mainly in function. Wrapped or bridged assets represent an asset of one ledger on another and typically add a custodian, which means that an operator reappears in the locus of trust. Decentralised finance protocols issue governance and liquidity tokens that sit in the use-or-rights column.

## 6. Discussion

### 6.1. Four Propositions

The map is more than a classification if it leads to expectations that can be tested. Four propositions follow from the argument, each linking a position on the map to a characteristic that matters in practice.

**P1. Risk follows trust.** The dominant risk of an asset lies where trust has been relocated. For an asset on an open protocol with no external anchor, the dominant risks are those of the protocol: flaws in the code, concentration of computing power or stake, and changes of rules imposed by a coalition. For an asset supported by an external asset or claim, the dominant risks are those of the party that holds the anchor: reserve quality, redemption and counterparty failure. For a central bank digital currency, the dominant risks are those of policy and of state control over holders. If this is right, failures should cluster at the places where trust has been concentrated, such as exchanges, custodians and issuers, and not randomly across the network, which is consistent with the record of exchange failures and manipulation documented in Section 4.3.

**P2. Stability is bought with a trustee.** The monetary properties of an asset improve with the credibility of its anchor, but credible anchors generally require a party that holds them. Assets that obtain stability from protocol rules alone should therefore be more fragile than assets with an external or sovereign anchor, and assets with a strong anchor should be less decentralised than assets without one. The proposition amounts to saying that no position on the map combines full decentralisation with strong monetary properties. It is the central trade-off that the technology leaves unresolved, and it explains why the search for a decentralised stable money has proved so difficult.

**P3. Regulation follows the locus of trust.** The point at which a regulator can act is the point at which trust is concentrated. Where an issuer holds the anchor, regulation can bear on the issuer, through requirements on reserves, redemption and disclosure. Where there is no identifiable issuer, regulation tends to bear on the intermediaries at the access points, such as exchanges and custodians, which are the places where the open protocol meets the conventional financial system. Where the issuer is the central bank, regulation is a matter of monetary policy. The corollary is that a single definition cannot serve regulators well, since the same label covers assets whose points of leverage are completely different.

**P4. A weak anchor makes demand depend on beliefs.** When nothing supports the value of a unit other than scarcity and demand, valuation depends mainly on what holders expect other holders to believe. Biases such as herding and reliance on heuristics should therefore play a larger role in the price dynamics of assets with a weak anchor than in those with a strong one. The existing evidence points in this direction, but it concerns almost exclusively the upper left cell. Bitcoin prices have been found to be driven by attention and popularity, measured by search queries, news volume or

the number of traded coins, rather than by fundamentals (Kristoufek, 2013, 2015; Polasik *et al*., 2015) [29, 30, 42], and to be mostly unrelated to traditional financial and macroeconomic variables (Baur *et al*., 2018b; Corbet *et al*., 2018) [6, 17]. Li and Wang (2017) [34] find that prices were driven by speculative investment at early stages and followed economic factors more closely as the market matured. Herding has been documented (Bouri *et al*., 2019; Vidal-Tomás *et al*., 2019; Stavroyiannis and Babalos, 2019) [8, 47, 53], and the explosive 2017 price rally has been associated with fear of missing out and herding (Sebastião *et al*., 2021) [44]. The contrast with anchored assets, which is the testable content of P4, remains largely unexamined. It should also be conditioned on market maturity, since the evidence suggests that informational efficiency is time-varying and improved after 2017 as liquidity grew (Le Tran and Leirvik, 2020; Sebastião *et al*., 2021) [32, 44], and on the interconnection of the market, since connectedness among cryptocurrencies changes over time and across market conditions (Ciaian *et al*., 2018; Yi *et al*., 2018) [14, 59].

### 6.2. Implications

For the theory of money, the framework changes the question. The debate over whether cryptocurrencies are money has produced contradictory answers because it treats them as a single object. The map shows that the answer depends on position: the technology provides a way to keep a record without a trusted keeper, but monetary status depends on the anchor, and the anchor is where a trustee tends to reappear. Cryptocurrencies are thus better described as institutional designs, which distribute trust in new ways, than as a new kind of money.

For empirical research, and in particular for research on investor behaviour, the framework implies that samples must be specified. Studies that pool all crypto-assets mix assets with different anchors and different loci of trust, and the results may reflect the composition of the sample rather than the behaviour under study. Sebastião *et al*. (2021) [44] note that results on connectedness and information flows depend strongly on the set of cryptocurrencies and on the sample period, which is what the framework would lead one to expect. P4 offers a concrete hypothesis: behavioural effects, such as herding or the influence of heuristics and social signals, should be stronger in the upper left of the map than elsewhere, and comparisons across cells provide a natural identification strategy for survey-based and market-based studies alike.

For regulation, the implication of P3 is that the aim should be to identify the point of leverage rather than to find the right definition. A functional approach that asks who holds the anchor, who validates the ledger and where the system meets the conventional financial sector is more robust than a definition based on the technology or on the intention of the creators, and it reduces the room for regulatory arbitrage between jurisdictions. Recent regulation is consistent with this reading. In the European Union, Regulation (EU) 2023/1114 on markets in crypto-assets treats asset-referenced tokens and e-money tokens, the stablecoin families, separately from other crypto-assets and imposes reserve and redemption requirements on their issuers, while service providers are authorised and supervised; its provisions on stablecoins applied from 30 June 2024 and those on service providers from 30 December 2024 (European Union, 2023) [21]. In Morocco, the draft law on digital assets reported in November 2025 would treat crypto-assets as a distinct category of financial assets rather than as legal means of payment, would give the financial markets authority the supervision of public offers and the licensing of service providers, would entrust the central bank with the framework for stablecoins defined as tokens backed by assets, and would exclude central bank issued currencies, non-fungible tokens and mining from its scope (BAM, 2025). The pattern is the one P3 predicts: the regulatory hook is the issuer where there is an anchor, and the licensed access point where there is not. The same logic applies to the fight against money laundering that motivates the definition of the Financial Action Task Force (2014) [22]: Foley *et al*. (2019) [23] estimate that about a quarter of Bitcoin users and half of Bitcoin transactions are associated with illegal activity, an estimate that is debated but that shows why supervision targets the exchanges where cryptocurrency meets conventional money.

### 6.3. A Reading from Islamic Finance

Crypto-assets have attracted a specific debate among scholars of Islamic finance, because they combine uncertainty, speculation and an unusual form of ownership. The questions concern whether an asset is a lawful object of exchange, whether its price formation involves excessive uncertainty or speculation (*gharar* and *maysir*), and whether the associated activities, such as lending or leverage, involve interest (*riba*). The answers are not uniform, and the map helps to organise them. Where value rests on belief alone, the objections about uncertainty and speculation are likely to be sharpest. Where it rests on an external asset or claim, the questions turn to the nature and ownership of the backing and to the character of the claim that the holder acquires. Where it rests on use or rights, the question is whether the use or the right has a lawful and real content. We do not offer rulings, which belong to qualified scholars, but the framework shows that different assets raise different questions and should not be assessed together.

### 6.4. Limitations and Avenues for Research

The study is conceptual. The two dimensions are deliberately few, and real assets often lie between the categories: a protocol may be open in principle and dominated by a few validators in practice, and an anchor may be partly credible. Much of the empirical evidence mobilised here concerns Bitcoin and a few large assets over 2014–2019, and the market and its regulation have changed since, so examples and regulatory statements may become outdated. Future work could code a sample of assets on the two dimensions, with intermediate values where needed, and test the propositions directly: by comparing volatility and use as a unit of account across cells (P2), by examining the location of failures (P1), by comparing the regulatory treatment of assets in different positions (P3), and by testing behavioural effects in surveys, experiments or market data across cells (P4).

## 7. Conclusion

This article started from a puzzle: the word “cryptocurrency” covers objects that differ widely in purpose, design and behaviour, yet definitions and classifications keep describing them by what they lack or by lists that mix criteria. We argued that the field becomes intelligible when cryptocurrencies are seen as answers to a single problem, keeping a shared record of ownership without a trusted keeper, and when the

differences between them are traced to two choices: where trust is placed, and what anchors the value of the unit.

Three results follow. Cryptocurrencies are defined by three conditions, digital representation of value, cryptographic authentication of ownership and protocol-enforced validation, while issuer, regulatory status and stability are features that vary and explain the disagreements between institutions. Decentralised validation displaces trust rather than eliminating it, so the question to ask of any asset is where trust now lies, and the record of exchanges, mining and custody shows where it reappears. And the combination of the locus of trust and the anchor of value yields a map that places payment cryptocurrencies, platform coins, tokens, stablecoins, permissioned projects and central bank digital currencies without overlap, and generates four propositions about risk, stability, regulation and behaviour.

The broader message is that the technology settles how a record is kept, but not whether a unit is trusted, and that the second question is where much of the economics and the regulation of cryptocurrencies is decided. A map that makes this visible gives researchers in economics, finance, computer science, law and Islamic finance a common vocabulary and a set of hypotheses to test, and gives regulators a way to ask where trust is concentrated rather than which label applies.

**References**


1. Antonopoulos AM. Mastering Bitcoin: Unlocking Digital Crypto-Currencies, O'Reilly Media, Sebastopol, CA. 2014.
2. Antonopoulos AM. Mastering Bitcoin: Programming the Open Blockchain, 2nd edn, O'Reilly Media, Sebastopol, CA. 2017.
3. Bank for International Settlements (BIS). Distributed Ledger Technology in Payment, Clearing, and Settlement. 2017. Available from: https://www.bis.org/cpmi/publ/d157.htm
4. Barontini C, Holden H. Proceeding with Caution – A Survey on Central Bank Digital Currency, BIS Papers No. 101, Bank for International Settlements, Basel. 2019.
5. Baur DG, Dimpfl T, Kuck K. 'Bitcoin, gold and the US dollar – a replication and extension', Finance Research Letters, Vol. 25, pp.103–110. 2018.
6. Baur DG, Hong K, Lee AD. 'Bitcoin: medium of exchange or speculative assets?', Journal of International Financial Markets, Institutions and Money, Vol. 54, pp.177–189. 2018.
7. Bech ML, Garratt R. 'Central bank cryptocurrencies', BIS Quarterly Review, September, pp.55–70. 2017.
8. Bouri E, Gupta R, Roubaud D. 'Herding behaviour in cryptocurrencies', Finance Research Letters, Vol. 29, pp.216–221. 2019.
9. Brandvold M, Molnár P, Vagstad K, Valstad OCA. 'Price discovery on Bitcoin exchanges', Journal of International Financial Markets, Institutions and Money, Vol. 36, pp.18–35. 2015.
10. Bullmann D, Klemm J, Pinna A. In Search for Stability in Crypto-Assets: Are Stablecoins the Solution? ECB Occasional Paper No. 230, European Central Bank, Frankfurt; 2019.
11. Castor A. 'A (short) guide to blockchain consensus protocols', CoinDesk. 2017. Available from: https://www.coindesk.com/short-guide-blockchain-consensus-protocols
12. Chang J, Harano K. Blockchain, Digital Currency and Cryptocurrency: Moving into the Mainstream?, J.P. Morgan Perspectives, February. 2020.
13. Chapman J, Garratt R, Hendry S, McCormack A, McMahon W. Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?, Bank of Canada, Financial System Review, June, pp.1–11. 2017.
14. Ciaian P, Rajcaniova M, Kancs, d'A. 'Virtual relationships: short- and long-run evidence from Bitcoin and altcoin markets', Journal of International Financial Markets, Institutions and Money, Vol. 52, pp.173–195. 2018.
15. Conlon T, McGee R. 'Safe haven or risky hazard? Bitcoin during the Covid-19 bear market', SSRN, 24 March; 2020. Available from: https://ssrn.com/abstract=3560361
16. Corbet S, Lucey B, Urquhart A, Yarovaya L. 'Cryptocurrencies as a financial asset: a systematic analysis', International Review of Financial Analysis, Vol. 62, pp.182–199. 2019.
17. Corbet S, Meegan A, Larkin C, Lucey B, Yarovaya L. 'Exploring the dynamic relationships between cryptocurrencies and other financial assets', Economics Letters, Vol. 165, pp.28–34. 2018.
18. De Vries A. 'Bitcoin's growing energy problem', Joule, Vol. 2, No. 5, pp.801–805. 2018.
19. Dyhrberg AH. 'Bitcoin, gold and the dollar – a GARCH volatility analysis', Finance Research Letters, Vol. 16, pp.85–92. 2016.
20. European Central Bank. Virtual Currency Schemes, European Central Bank, Frankfurt, October. 2012.
21. European Union. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, Official Journal of the European Union, L 150, 9 June. 2023.
22. Financial Action Task Force. Virtual Currencies: Key Definitions and Potential AML/CFT Risks, FATF, Paris, June. 2014.
23. Foley S, Karlsen JR, Putniņš TJ. 'Sex, drugs, and Bitcoin: how much illegal activity is financed through cryptocurrencies?', The Review of Financial Studies, Vol. 32, No. 5, pp.1798–1853. 2019.
24. Gandal N, Hamrick JT, Moore T, Oberman T. 'Price manipulation in the Bitcoin ecosystem', Journal of Monetary Economics, Vol. 95, pp.86–96. 2018.
25. Giudici G, Milne A, Vinogradov D. 'Cryptocurrencies: market analysis and perspectives', Journal of Industrial and Business Economics, Vol. 47, No. 1, pp.1–18. 2020.
26. He D, Habermeier K, Leckow R, *et al*. Virtual Currencies and Beyond: Initial Considerations, IMF Staff Discussion Note SDN/16/03, International Monetary Fund, Washington, DC. 2016.
27. Holub M, Johnson J. 'Bitcoin research across disciplines', The Information Society, Vol. 34, No. 2, pp.114–126. 2018.
28. Katz L. 'Bitcoin acceptance among retailers is low and getting lower', Bloomberg, 12 July. 2017.
29. Kristoufek L. 'BitCoin meets Google Trends and Wikipedia: quantifying the relationship between phenomena of the internet era', Scientific Reports, Vol. 3, article 3415. 2013.
30. Kristoufek L. 'What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis', PLoS One. 2015;10(4):e0123923.

31. Larousse. 'Cryptomonnaie', Dictionnaire de français Larousse, online edition. 2022.
32. Le Tran V, Leirvik T. 'Efficiency in the markets of crypto-currencies', Finance Research Letters, Vol. 35, article 101382. 2020.
33. Li J, Li N, Peng J, Cui H, Wu Z. 'Energy consumption of cryptocurrency mining: a study of electricity consumption in mining cryptocurrencies', Energy, Vol. 168, pp.160–168. 2019.
34. Li X, Wang CA. 'The technology and economic determinants of cryptocurrency exchange rates: the case of Bitcoin', Decision Support Systems, Vol. 95, pp.49–60. 2017.
35. Libra Association. An Introduction to Libra: White Paper. 2019. Available from: https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf
36. Merediz-Sola I, Bariviera AF. 'A bibliometric analysis of Bitcoin scientific production', Research in International Business and Finance, Vol. 50, pp.294–305. 2019.
37. Monetary Authority of Singapore. The Future is Here – Project Ubin: SGD on Distributed Ledger, Monetary Authority of Singapore and Deloitte, Singapore. 2017.
38. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available from: https://bitcoin.org/bitcoin.pdf
39. Narayanan A, Clark J. 'Bitcoin's academic pedigree', Communications of the ACM, Vol. 60, No. 12, pp.36–45. 2017.
40. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, Princeton, NJ. 2016.
41. Neumueller A. Ethereum's electricity consumption before and after the Merge, Cambridge Digital Assets Programme, Cambridge Judge Business School. 2023. Available from: https://www.jbs.cam.ac.uk/2023/blockchain-sustainability-ethereum/
42. Polasik M, Piotrowska AI, Wisniewski TP, Kotkowski R, Lightfoot G. 'Price fluctuations and the use of Bitcoin: an empirical inquiry', International Journal of Electronic Commerce, Vol. 20, No. 1, pp.9–49. 2015.
43. Rauchs M, Blandin A, Klein K, Pieters GC, Recanatini M, Zhang BZ. 2nd Global Cryptoasset Benchmarking Study, Cambridge Centre for Alternative Finance, University of Cambridge, Cambridge. 2018.
44. Sebastião HMCV, da Cunha PJOR, Godinho PMC. 'Cryptocurrencies and blockchain. Overview and future perspectives', International Journal of Economics and Business Research. 2021;21(3):305-342.
45. Selgin G. 'Synthetic commodity money', Journal of Financial Stability, Vol. 17, pp.92–99. 2015.
46. Smales LA. 'Bitcoin as a safe haven: is it even worth considering?', Finance Research Letters, Vol. 30, pp.385–393. 2019.
47. Stavroyiannis S, Babalos V. 'Herding behavior in cryptocurrencies revisited: novel evidence from a TVP model', Journal of Behavioral and Experimental Finance, Vol. 22, pp.57–63. 2019.
48. Sveriges Riksbank. The Riksbank's e-krona Project, Report 1, Sveriges Riksbank, Stockholm. 2017.
49. Swan M. Blockchain: Blueprint for a New Economy, O'Reilly Media, Sebastopol, CA. 2015.
50. Szabo N. 'Formalizing and securing relationships on public networks', First Monday, Vol. 2, No. 9. 1997.
51. Tapscott D, Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio/Penguin, New York. 2016.
52. Truby J. 'Decarbonizing Bitcoin: law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies', Energy Research & Social Science, Vol. 44, pp.399–410. 2018.
53. Vidal-Tomás D, Ibáñez AM, Farinós JE. 'Herding in the cryptocurrency market: CSSD and CSAD approaches', Finance Research Letters, Vol. 30, pp.181–186. 2019.
54. Vranken H. 'Sustainability of Bitcoin and blockchains', Current Opinion in Environmental Sustainability, Vol. 28, pp.1–9. 2017.
55. World Bank. Europe and Central Asia Economic Update, Spring 2018: Cryptocurrencies and Blockchain, World Bank, Washington, DC. 2018.
56. Yaga D, Mell P, Roby N, Scarfone K. Blockchain Technology Overview, arXiv preprint, arXiv:1906.11078. 2019.
57. Yermack D. 'Is Bitcoin a real currency? An economic appraisal', in Handbook of Digital Currency, Academic Press, Cambridge, MA. 2015:31-43.
58. Yermack D. 'Corporate governance and blockchains', Review of Finance, Vol. 21, No. 1, pp.7–31. 2017.
59. Yi S, Xu Z, Wang GJ. 'Volatility connectedness in the cryptocurrency market: is Bitcoin a dominant cryptocurrency?', International Review of Financial Analysis, Vol. 60, pp.98–114. 2018.
60. Zheng Z, Xie S, Dai H, Chen X, Wang H. 'An overview of blockchain technology: architecture, consensus, and future trends in 2017', IEEE International Congress on Big Data (BigData Congress), Honolulu, Hawaii, pp.557–564. 2017.



**How to Cite This Article**

Essoussi M. Trust without a trustee? rethinking cryptocurrencies through the locus of trust. Int J Soc Sci Except Res. 2026;5(6):47-55.
doi:10.54660/IJSSER.2026.5.6.47-55



**Creative Commons (CC) License**

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.