V. Cryptocurrencies: looking beyond the hype

Less than 10 years after their inception, cryptocurrencies[1] have emerged from obscurity to attract intense interest on the part of businesses and consumers, as well as central banks and other authorities. They garner attention because they promise to replace trust in long-standing institutions, such as commercial and central banks, with trust in a new, fully decentralised system founded on the blockchain and related distributed ledger technology (DLT).

This chapter evaluates whether cryptocurrencies could play any role as money: looking beyond the hype, what specific economic problems, if any, can current cryptocurrencies solve? The chapter first reviews the historical context. Many episodes of monetary instability and failed currencies illustrate that the institutional arrangements through which money is supplied matter a great deal. This review shows that the essence of good money has always been trust in the stability of its value. And for money to live up to its signature property – to act as a coordination device facilitating transactions – it needs to efficiently scale with the economy and be provided elastically to address fluctuating demand. These considerations call for specific institutional arrangements – hence the emergence of today's independent and accountable central banks.

The chapter then gives an introduction to cryptocurrencies and discusses the economic limitations inherent in the decentralised creation of trust which they entail. For the trust to be maintained, honest network participants need to control the vast majority of computing power, each and every user needs to verify the history of transactions and the supply of the cryptocurrency needs to be predetermined by its protocol. Trust can evaporate at any time because of the fragility of the decentralised consensus through which transactions are recorded. Not only does this call into question the finality of individual payments, it also means that a cryptocurrency can simply stop functioning, resulting in a complete loss of value. Moreover, even if trust can be maintained, cryptocurrency technology comes with poor efficiency and vast energy use. Cryptocurrencies cannot scale with transaction demand, are prone to congestion and greatly fluctuate in value. Overall, the decentralised technology of cryptocurrencies, however sophisticated, is a poor substitute for the solid institutional backing of money.

That said, the underlying technology could have promise in other applications, such as the simplification of administrative processes in the settlement of financial transactions. Still, this remains to be tested. As cryptocurrencies raise a host of issues, the chapter concludes with a discussion of policy responses, including regulation of private uses of the technology, the measures needed to prevent abuses of cryptocurrencies and the delicate questions raised by the issuance of digital currency by central banks.

Putting the rise of cryptocurrencies into perspective

A good way to examine whether a new technology can be a truly useful addition to the existing monetary landscape is to step back and review the fundamental roles of money in an economy and what history teaches us about failed attempts to create new private moneys. Then one can ask whether money based on this new technology can improve upon the current monetary landscape in any way.[2]

A brief history of money

Money plays a crucial role in facilitating economic exchange. Before its advent millennia ago, goods were primarily exchanged for the promise to return the favour in the future (ie trading of IOUs).[3] However, as societies grew larger and economic activity expanded, it became harder to keep a record of ever more complex IOUs, and default and settlement risks became concerns. Money and the institutions issuing it came into existence to address this growing complexity and the associated difficulty in maintaining trust.

Money has three fundamental and complementary roles. It is: (i) a unit of account – a yardstick that eases comparison of prices across the things we buy, as well as the value of promises we make; (ii) a medium of exchange: a seller accepts it as a means of payment, in the expectation that somebody else will do the same; and (iii) a store of value, enabling users to transfer purchasing power over time.[4]

To fulfil these functions, money needs to have the same value in different places and to keep a stable value over time: assessing whether to sell a certain good or service is much easier if one is certain that the received currency has a guaranteed value in terms of both current and future purchasing power. One way to achieve this is by pure commodity moneys with intrinsic value, such as salt or grain. But commodity money by itself does not effectively support exchange: it may not always be available, is costly to produce and cumbersome in exchange, and may be perishable.[5]

The expansion of economic activity required more convenient moneys that could respond to increasing demand, be efficiently used in trade and have a stable value. However, maintaining trust in the institutional arrangements through which money is supplied has been the biggest challenge. Around the world, in different settings and at different times, money started to rely on issuance by centralised authorities. From ancient times, the stamp of a sovereign certified a coin's value in transactions. Later, bills of exchange intermediated by banks developed as a way for merchants to limit the costs and risks of travelling with large quantities of coinage.[6]

However, historical experience also made clear an underlying trade-off, for currencies that are supplied flexibly can also be debased easily.[7] Sustained episodes of stable money are historically much more of an exception than the norm. In fact, trust has failed so frequently that history is a graveyard of currencies. Museums around the world devote entire sections to this graveyard – for example, room 68 of the British Museum displays stones, shells, tobacco, countless coins and pieces of paper, along with many other objects that lost their acceptability as exchange and found their way to this room. Some fell victim to the expansion of trade and economic activity, as they were rendered inconvenient with a larger scale of use. Some were discarded when the political order that supported them weakened or fell. And many others fell victim to the erosion of trust in the stability of their value.

History proves that money can be fragile whether it is supplied through private means, in a competitive manner, or by a sovereign, as a monopolist supplier. Bank-issued money is only as good as the assets that back it. Banks are meant to transform risks, and therefore, under certain extreme scenarios, confidence in privately issued money can vanish overnight. Government-backed arrangements, where assuring trust in the instrument is a centralised task, have not always worked well either. Far from it: a well known example of abuse is the competitive debasement of coins issued by German princes in the early 17th century, known as the Kipper- und Wipperzeit (clipping and culling times).[8] And there have been many others, up to the present-day cases of Venezuela and Zimbabwe. Avoiding abuse by the sovereign has thus been a key consideration in the design of monetary arrangements.

The quest for solid institutional underpinning for trust in money eventually culminated in the emergence of today's central banks. An early step was the establishment of chartered public banks in European city-states during the period 1400–1600. These emerged to improve trading by providing a high-quality, efficient means of payment and centralising a number of clearing and settlement operations. Such banks, set up in trading hubs such as Amsterdam, Barcelona, Genoa, Hamburg and Venice, were instrumental in stimulating international trade and economic activity more generally.[9] Over time, many of these chartered banks functioned in ways similar to current central banks. Formal central banks, as we know them today, also often emerged in direct response to poor experiences with decentralised money. For example, the failures of wildcat banking in the United States eventually led to the creation of the Federal Reserve System.

The current monetary and payment system

The tried, trusted and resilient way to provide confidence in money in modern times is the independent central bank. This means agreed goals: clear monetary policy and financial stability objectives; operational, instrument and administrative independence; and democratic accountability, so as to ensure broad-based political support and legitimacy. Independent central banks have largely achieved the goal of safeguarding society's economic and political interest in a stable currency.[10] With this setup, money can be accurately defined as an "indispensable social convention backed by an accountable institution within the state that enjoys public trust".[11]

In almost all modern-day economies, money is provided through a joint public-private venture between the central bank and private banks, with the central bank at the system's core. Electronic bank deposits are the main means of payment between ultimate users, while central bank reserves are the means of payment between banks. In this two-tiered system, trust is generated through independent and accountable central banks, which back reserves through their asset holdings and operational rules. In turn, trust in bank deposits is generated through a variety of means, including regulation, supervision and deposit insurance schemes, many ultimately emanating from the state.

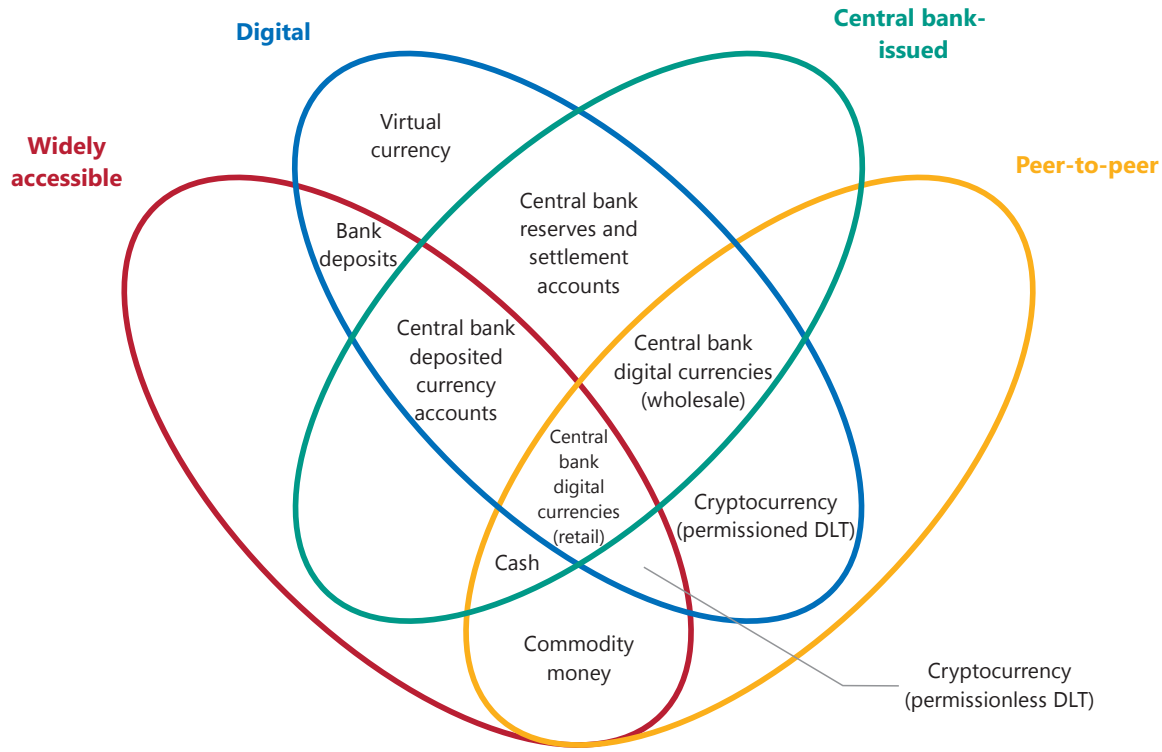
As part of fulfilling their mandate to maintain a stable unit of account and means of payment, central banks take an active role in supervising, overseeing and in some cases providing the payments infrastructure for their currency. The central bank's role includes ensuring that the payment system operates smoothly and seeing to it that the supply of reserves responds appropriately to shifting demand, including at intraday frequency, ie ensuring an elastic money supply.[12]

Thanks to the active involvement of central banks, today's diverse payment systems have achieved safety, cost-effectiveness, scalability and trust that a payment, once made, is final.

Payment systems are safe and cost-effective, handling high volumes and accommodating rapid growth with hardly any abuse and at low costs. An important contributor to safety and cost-effectiveness is scalability. In today's sophisticated economies, the volume of payments is huge, equal to many multiples of GDP. Despite these large volumes, expanding use of the instrument does not lead to a proportional increase in costs. This is important, since an essential feature of any successful money and payment system is how widely used it is by both buyers and sellers: the more others connect to a particular payment system, the greater one's own incentive to use it.

Users not only need to have trust in money itself, they also need to trust that a payment will take place promptly and smoothly. A desirable operational attribute is thus certainty of payment ("finality") and the related ability to contest transactions that may have been incorrectly executed. Finality requires that the system be largely

The money flower: a taxonomy of money Graph V.1



Source: Adapted from M Bech and R Garratt, "Central bank cryptocurrencies", *BIS Quarterly Review*, September 2017, pp 55–70.

free of fraud and operational risks, at the level of both individual transactions and the system as a whole. Strong oversight and central bank accountability both help to support finality and hence trust.

While most modern-day transactions occur through means ultimately supported by central banks, over time a wide range of public and private payment means has emerged. These can be best summarised by a taxonomy characterised as the "money flower" (Graph V.1).[13]

The money flower distinguishes four key properties of moneys: the issuer, the form, the degree of accessibility and the payment transfer mechanism. The issuer can be a central bank, a bank or nobody, as was the case when money took the form of a commodity. Its form can be physical, eg a metal coin or paper banknote, or digital. It can be widely accessible, like commercial bank deposits, or narrowly so, like central bank reserves. A last property regards the transfer mechanism, which can be either peer-to-peer, or through a central intermediary, as for deposits. Money is typically based on one of two basic technologies: so called "tokens" or accounts. Token-based money, for example banknotes or physical coins, can be exchanged in peer-to-peer settings, but such exchange relies critically on the payee's ability to verify the validity of the payment object – with cash, the worry is counterfeiting. By contrast, systems based on account money depend fundamentally on the ability to verify the identity of the account holder.

Cryptocurrencies: the elusive promise of decentralised trust

Do cryptocurrencies deliver what they promise? Or will they end up as short-lived curiosities? In order to answer these questions, it is necessary to define them more

precisely, to understand their supporting technology and to examine the associated economic limitations.

A new petal in the money flower?

Cryptocurrencies aspire to be a new form of currency and promise to maintain trust in the stability of their value through the use of technology. They consist of three elements. First, a set of rules (the "protocol"), computer code specifying how participants can transact. Second, a ledger storing the history of transactions. And third, a decentralised network of participants that update, store and read the ledger of transactions following the rules of the protocol. With these elements, advocates claim, a cryptocurrency is not subject to the potentially misguided incentives of banks and sovereigns.

In terms of the money flower taxonomy, cryptocurrencies combine three key features. First, they are digital, aspiring to be a convenient means of payment and relying on cryptography to prevent counterfeiting and fraudulent transactions. Second, although created privately, they are no one's liability, ie they cannot be redeemed, and their value derives only from the expectation that they will continue to be accepted by others. This makes them akin to a commodity money (although without any intrinsic value in use). And, last, they allow for digital peer-to-peer exchange.

Compared with other private digital moneys such as bank deposits, the distinguishing feature of cryptocurrencies is digital peer-to-peer exchange. Digital bank accounts have been around for decades. And privately issued "virtual currencies" – eg as used in massive multiplayer online games like World of Warcraft – predate cryptocurrencies by a decade. In contrast to these, cryptocurrency transfers can in principle take place in a decentralised setting without the need for a central counterparty to execute the exchange.

Distributed ledger technology in cryptocurrencies

The technological challenge in digital peer-to-peer exchange is the so-called "double-spending problem". Any digital form of money is easily replicable and can thus be fraudulently spent more than once. Digital information can be reproduced more easily than physical banknotes. For digital money, solving the double-spending problem requires, at a minimum, that someone keep a record of all transactions. Prior to cryptocurrencies, the only solution was to have a centralised agent do this and verify all transactions.

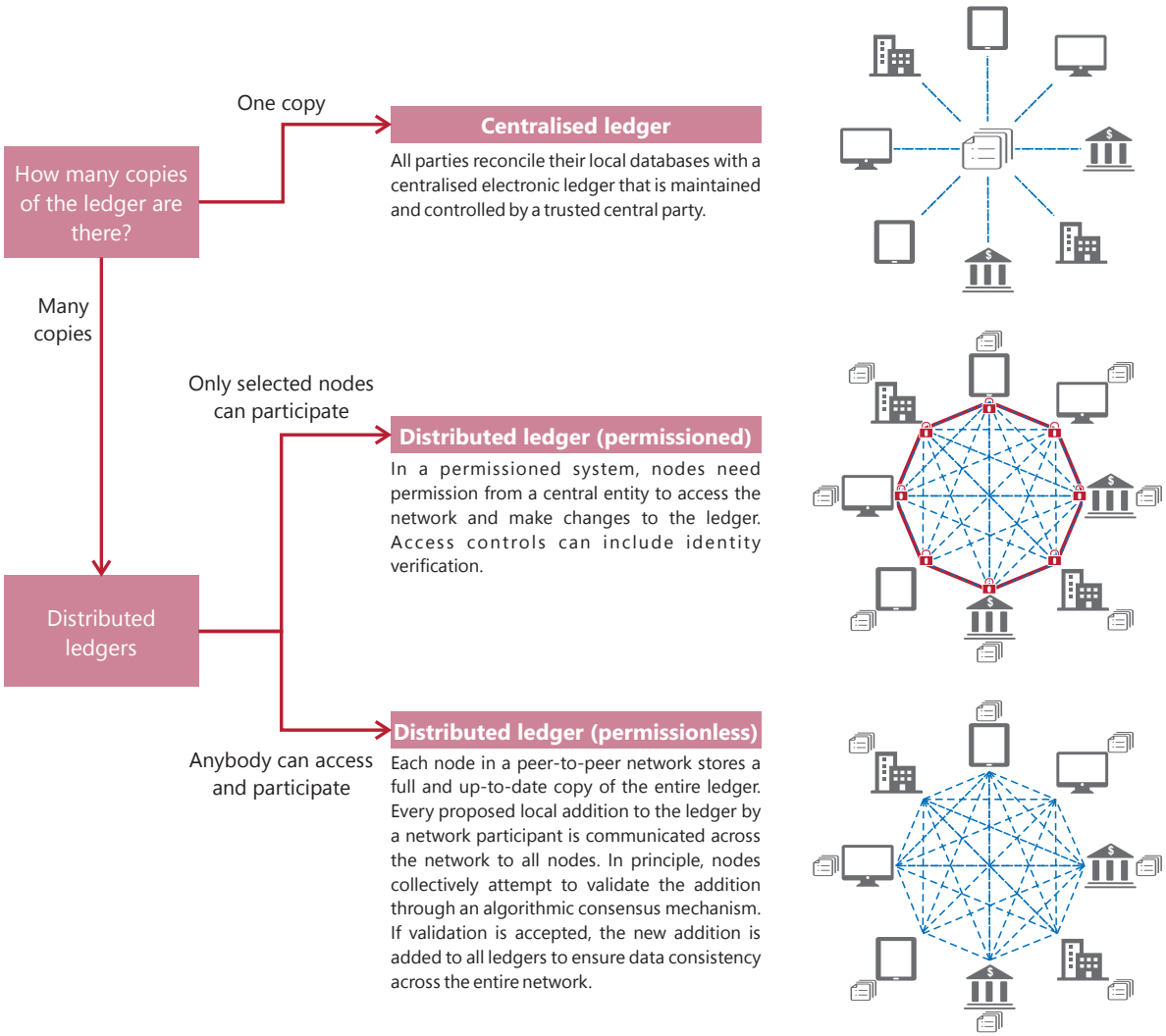
Cryptocurrencies overcome the double-spending problem via decentralised record-keeping through what is known as a distributed ledger. The ledger can be regarded as a file (think of a Microsoft Excel worksheet) that starts with an initial distribution of cryptocurrency and records the history of all subsequent transactions. An up-to-date copy of the entire ledger is stored by each user (this is what makes it "distributed"). With a distributed ledger, peer-to-peer exchange of digital money is feasible: each user can directly verify in their copy of the ledger whether a transfer took place and that there was no attempt to double-spend.[14]

While all cryptocurrencies rely on a distributed ledger, they differ in terms of how the ledger is updated. One can distinguish two broad classes, with substantial differences in their operational setup (Graph V.2).

One class is based on "permissioned" DLT. Such cryptocurrencies are similar to conventional payment mechanisms in that, to prevent abuse, the ledger can only be updated by trusted participants in the cryptocurrency – often termed "trusted nodes". These nodes are chosen by, and subject to oversight by, a central authority,

Centralised ledger and permissioned/permissionless decentralised ledgers

Graph V.2



		Private electronic money based on fiat system	Privately issued cryptocurrencies	
			Permissioned	Permissionless
1	Storage of balances/holdings	Ledger (accounts) stored centrally by banks and other financial institutions	Decentralised storage of ledger	
2	Verification to avoid double-spending	Identity-based concept	Peer-to-peer concept: distributed ledger can be checked to see whether a specific unit of a currency has already been spent	
3	Processing of transactions	Accounts updated by bank	Updating of ledger via trusted nodes	Updating of ledger via proof-of-work Rule to follow longest chain
4	Finality/settlement concept	Settlement ultimately via central bank	Settlement in cryptocurrency itself	Probabilistic concept of finality via rule to follow longest chain
5	Elasticity of supply	Central bank policy, eg regarding intraday credit	Protocol can be changed by trusted nodes	Protocol-determined
6	Trust-creating mechanisms	Reputation of banks and central banks, banking supervision, lender of last resort, legal tender laws, central bank independence and accountability, AML/CFT checks, cyber-security	Reputation of issuing firm and nodes Trusted nodes, some of which may be subject to regulation	Proof-of-work requires honest computing majority

Sources: Adapted from H Natarajan, S Krause and H Gradstein, "Distributed ledger technology (DLT) and blockchain", World Bank Group, *FinTech Note*, no 1, 2017; BIS.

eg the firm that developed the cryptocurrency. Thus, while cryptocurrencies based on permissioned systems differ from conventional money in terms of how transaction records are stored (decentralised versus centralised), they share with it the reliance on specific institutions as the ultimate source of trust.[15]

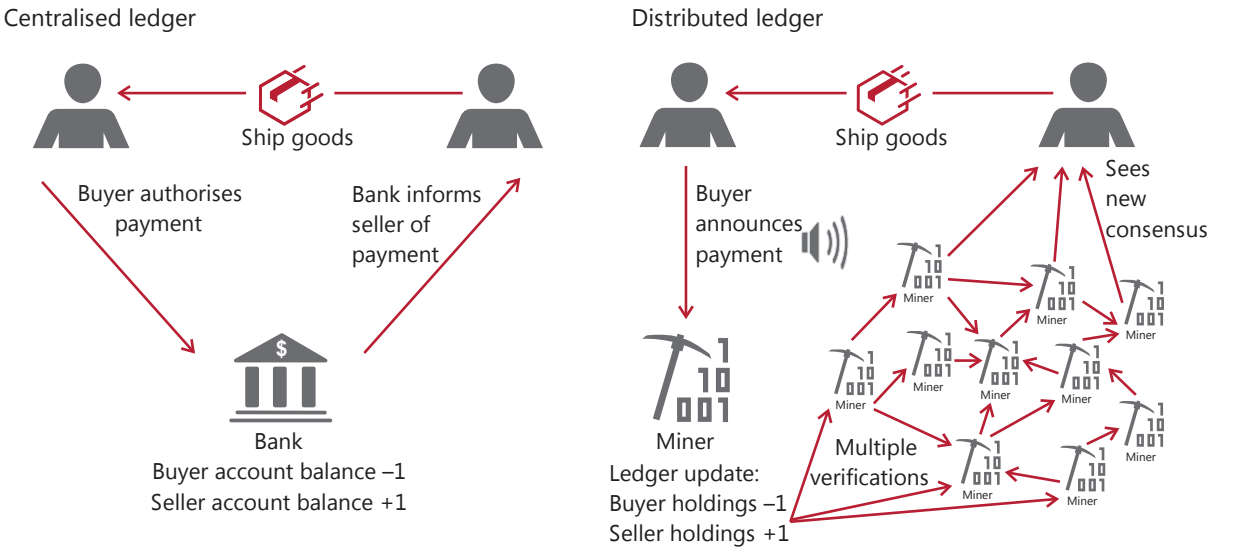
In a much more radical departure from the prevailing institution-based setup, a second class of cryptocurrencies promises to generate trust in a fully decentralised setting using "permissionless" DLT. The ledger recording transactions can only be changed by a consensus of the participants in the currency: while anybody can participate, nobody has a special key to change the ledger.

The concept of permissionless cryptocurrencies was laid out for the case of Bitcoin[16] in a white paper by an anonymous programmer (or group of programmers) under the pseudonym Satoshi Nakamoto, who proposed a currency based on a specific type of distributed ledger, the "blockchain". The blockchain is a distributed ledger that is updated in groups of transactions called blocks. Blocks are then chained sequentially via the use of cryptography to form the blockchain. This concept has been adapted to countless other cryptocurrencies.[17]

Blockchain-based permissionless cryptocurrencies have two groups of participants: "miners" who act as bookkeepers and "users" who want to transact in the cryptocurrency. At face value, the idea underlying these cryptocurrencies is simple: instead of a bank centrally recording transactions (Graph V.3, left-hand panel), the ledger is updated by a miner and the update is subsequently stored by all users and miners (right-hand panel).[18]

Valid transactions in a centralised ledger/bank account and in a permissionless cryptocurrency

Graph V.3



A buyer purchases a good from the seller, who initiates shipment upon perceived confirmation of the payment. If the payment takes place via bank accounts – ie via a centralised ledger (left-hand panel) – the buyer sends the payment instruction to their bank, which adjusts account balances debiting the amount paid from the buyer's account and crediting it to the seller's account. The bank then confirms payment to the seller. In contrast, if payment takes place via a permissionless cryptocurrency (right-hand panel), the buyer first publicly announces a payment instruction stating that the cryptocurrency holdings of the buyer are reduced by one, while those of the seller are increased by one. After a delay, a miner includes this payment information in a ledger update. The updated ledger is subsequently shared with other miners and users, each verifying that the newly added payment instruction is not a double-spend attempt and is authorised by the buyer. The seller then observes that the ledger including the payment instruction emerges as the one commonly used by the network of miners and users.

Source: Adapted from R Auer, "The mechanics of decentralised trust in Bitcoin and the blockchain", *BIS Working Papers*, forthcoming.

Underlying this setup, the key feature of these cryptocurrencies is the implementation of a set of rules (the protocol) that aim to align the incentives of all participants so as to create a reliable payment technology without a central trusted agent. The protocol determines the supply of the asset in order to counter debasement – for example, in the case of Bitcoin, it states that no more than 21 million bitcoins can exist. In addition, the protocol is designed to ensure that all participants follow the rules out of self-interest, ie that they yield a self-sustaining equilibrium. Three key aspects are the following.

First, the rules entail a cost to updating the ledger. In most cases, this cost comes about because updating requires a "proof-of-work". This is mathematical evidence that a certain amount of computational work has been done, in turn calling for costly equipment and electricity use. Since the proof-of-work process can be likened to digging up rare numbers via laborious computations, it is often referred to as mining.[19] In return for their efforts, miners receive fees from the users – and, if specified by the protocol, newly minted cryptocurrency.

Second, all miners and users of a cryptocurrency verify all ledger updates, which induces miners to include only valid transactions. Valid transactions need to be initiated by the owners of funds and must not be attempts to double-spend. If a ledger update includes an invalid transaction, it is rejected by the network and the miner's rewards are voided. The verification of all new ledger updates by the network of miners and users is thus essential to incentivise miners to add only valid transactions.[20]

Third, the protocol specifies rules to achieve a consensus on the order of updates to the ledger. This is generally done by creating incentives for individual miners to follow the computing majority of all other miners when they implement updates. Such coordination is needed, for example, to resolve cases where communication lags lead to different miners adding conflicting updates – ie updates that include different sets of transactions (Box V.A).

With these key ingredients, it is costly – though not impossible – for any individual to forge a cryptocurrency. To successfully double-spend, a counterfeiter would have to spend their cryptocurrency with a merchant and secretly produce a forged blockchain in which this transaction was not recorded. Upon receipt of the merchandise, the counterfeiter would then release the forged blockchain, ie reverse the payment. But this forged blockchain would only emerge as the commonly accepted chain if it were longer than the blockchain the rest of the network of miners had produced in the meantime. A successful double-spend attack thus requires a substantial share of the mining community's computing power. Conversely, in the words of the original Bitcoin white paper, a cryptocurrency can overcome the double-spending problem in a decentralised way only if "honest nodes control a majority of [computing] power".[21]

Assessing the economic limitations of permissionless cryptocurrencies

Cryptocurrencies such as Bitcoin promise to deliver not only a convenient payment means based on digital technology, but also a novel model of trust. Yet delivering on this promise hinges on a set of assumptions: that honest miners control the vast majority of computing power, that users verify the history of all transactions and that the supply of the currency is predetermined by a protocol. Understanding these assumptions is important, for they give rise to two basic questions regarding the usefulness of cryptocurrencies. First, does this cumbersome way of trying to achieve trust come at the expense of efficiency? Second, can trust truly and always be achieved?

As the first question implies, a key potential limitation in terms of efficiency is the enormous cost of generating decentralised trust. One would expect miners to compete to add new blocks to the ledger through the proof-of-work until their

anticipated profits fall to zero.[22] Individual facilities operated by miners can host computing power equivalent to that of millions of personal computers. At the time of writing, the total electricity use of bitcoin mining equalled that of mid-sized economies such as Switzerland, and other cryptocurrencies also use ample electricity (Graph V.4, left-hand panel). Put in the simplest terms, the quest for decentralised trust has quickly become an environmental disaster.[23]

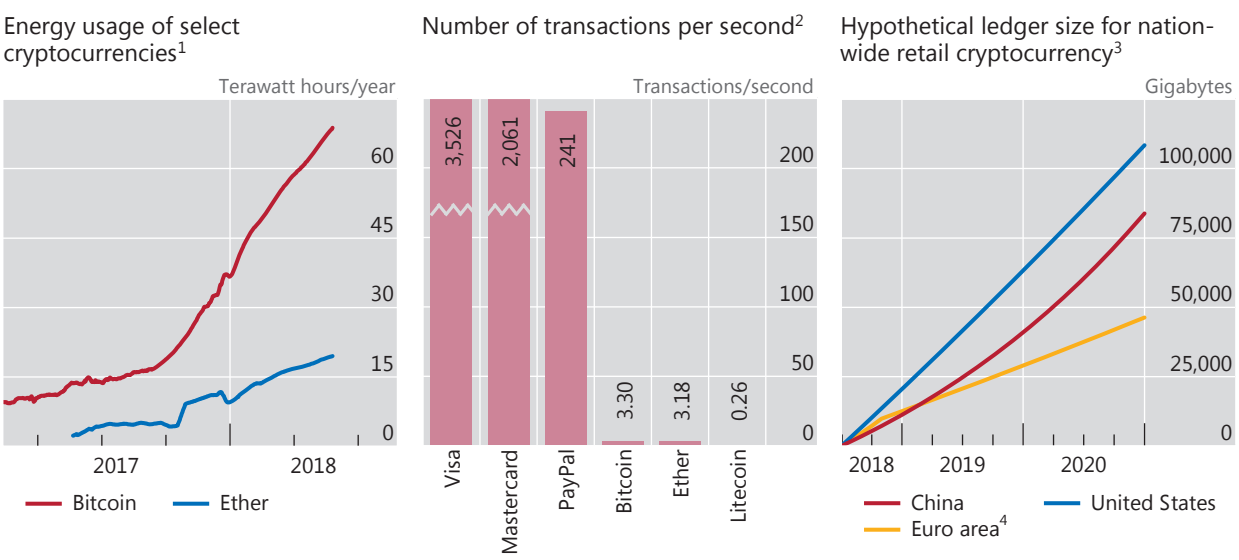
But the underlying economic problems go well beyond the energy issue. They relate to the signature property of money: to promote "network externalities" among users and thereby serve as a coordination device for economic activity. The shortcomings of cryptocurrencies in this respect lie in three areas: scalability, stability of value and trust in the finality of payments.

First, cryptocurrencies simply do not scale like sovereign moneys. At the most basic level, to live up to their promise of decentralised trust cryptocurrencies require each and every user to download and verify the history of all transactions ever made, including amount paid, payer, payee and other details. With every transaction adding a few hundred bytes, the ledger grows substantially over time. For example, at the time of writing, the Bitcoin blockchain was growing at around 50 GB per year and stood at roughly 170 GB. Thus, to keep the ledger's size and the time needed to verify all transactions (which increases with block size) manageable, cryptocurrencies have hard limits on the throughput of transactions (Graph V.4, centre panel).

A thought experiment illustrates the inadequacy of cryptocurrencies as an everyday means of payment (Graph V.4, right-hand panel). To process the number of digital retail transactions currently handled by selected national retail payment systems, even under optimistic assumptions, the size of the ledger would swell well beyond the storage capacity of a typical smartphone in a matter of days, beyond that of a typical personal computer in a matter of weeks and beyond that of servers in a matter of months. But the issue goes well beyond storage capacity, and extends

Energy consumption and scaling issues

Graph V.4



[1] Estimated. [2] 2017 data. [3] The displayed hypothetical size of the blockchain/ledger is calculated assuming that, starting from 1 July 2018, all non-cash retail transactions of either China, the United States or the euro area are processed via a cryptocurrency. Calculations are based on information on non-cash transaction numbers from CPMI (2017) and assume that each transaction adds 250 bytes to the ledger. [4] BE, FR, DE, IT and NL.

Sources: Committee on Payments and Market Infrastructures, *Statistics on payment, clearing and settlement systems in the CPMI countries*, December 2017; www.bitinfocharts.com; Digiconomist; Mastercard; PayPal; Visa; BIS calculations.

to processing capacity: only supercomputers could keep up with verification of the incoming transactions. The associated communication volumes could bring the internet to a halt, as millions of users exchanged files on the order of magnitude of a terabyte.

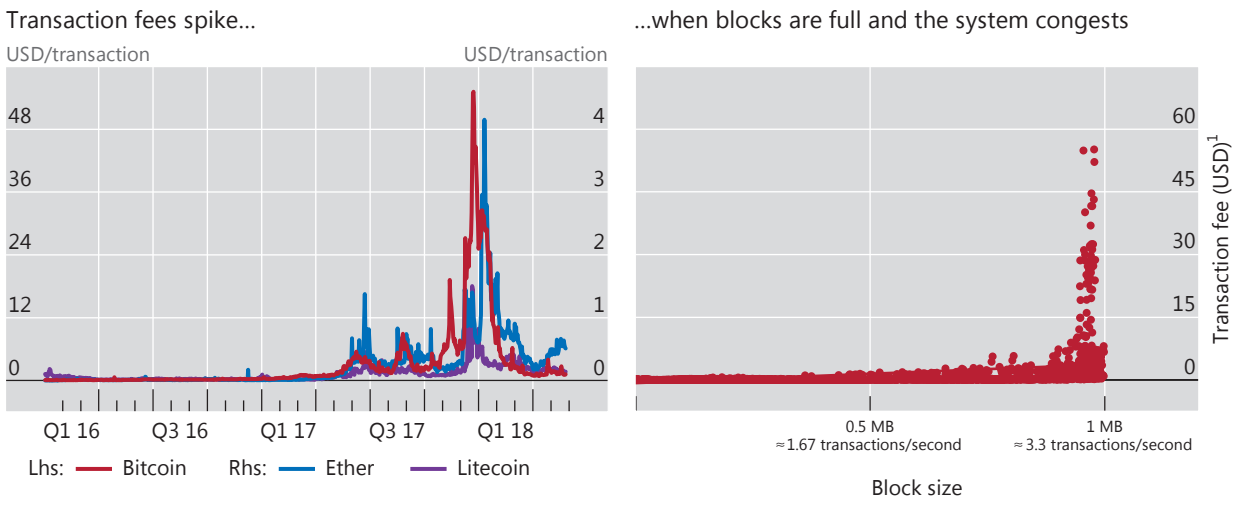
Another aspect of the scalability issue is that updating the ledger is subject to congestion. For example, in blockchain-based cryptocurrencies, in order to limit the number of transactions added to the ledger at any given point in time, new blocks can only be added at pre-specified intervals. Once the number of incoming transactions is such that newly added blocks are already at the maximum size permitted by the protocol, the system congests and many transactions go into a queue. With capacity capped, fees soar whenever transaction demand reaches the capacity limit (Graph V.5). And transactions have at times remained in a queue for several hours, interrupting the payment process. This limits cryptocurrencies' usefulness for day-to-day transactions such as paying for a coffee or a conference fee, not to mention for wholesale payments.[24] Thus, the more people use a cryptocurrency, the more cumbersome payments become. This negates an essential property of present-day money: the more people use it, the stronger the incentive to use it.[25]

The second key issue with cryptocurrencies is their unstable value. This arises from the absence of a central issuer with a mandate to guarantee the currency's stability. Well run central banks succeed in stabilising the domestic value of their sovereign currency by adjusting the supply of the means of payment in line with transaction demand. They do so at high frequency, in particular during times of market stress but also during normal times.

This contrasts with a cryptocurrency, where generating some confidence in its value requires that supply be predetermined by a protocol. This prevents it from being supplied elastically. Therefore, any fluctuation in demand translates into changes in valuation. This means that cryptocurrencies' valuations are extremely volatile (Graph V.6, left-hand panel). And the inherent instability is unlikely to be fully overcome by better protocols or financial engineering, as exemplified by the experience of the Dai cryptocurrency. While engineered to be fixed to the US dollar

Transaction fees over time and in relation to transaction throughput

Graph V.5



[1] Transaction fee paid to miners over the period 1 August 2010–25 May 2018; daily averages.

Sources: www.bitinfocharts.com; BIS calculations.

at a rate of one to one, it reached a low of $0.72 just a few weeks after its launch in late 2017. Other cryptocurrencies designed to have a stable value have also fluctuated substantially (centre panel).

This outcome is not coincidental. Keeping the supply of the means of payment in line with transaction demand requires a central authority, typically the central bank, which can expand or contract its balance sheet. The authority needs to be willing at times to trade against the market, even if this means taking risk onto its balance sheet and absorbing a loss. In a decentralised network of cryptocurrency users, there is no central agent with the obligation or the incentives to stabilise the value of the currency: whenever demand for the cryptocurrency decreases, so does its price.

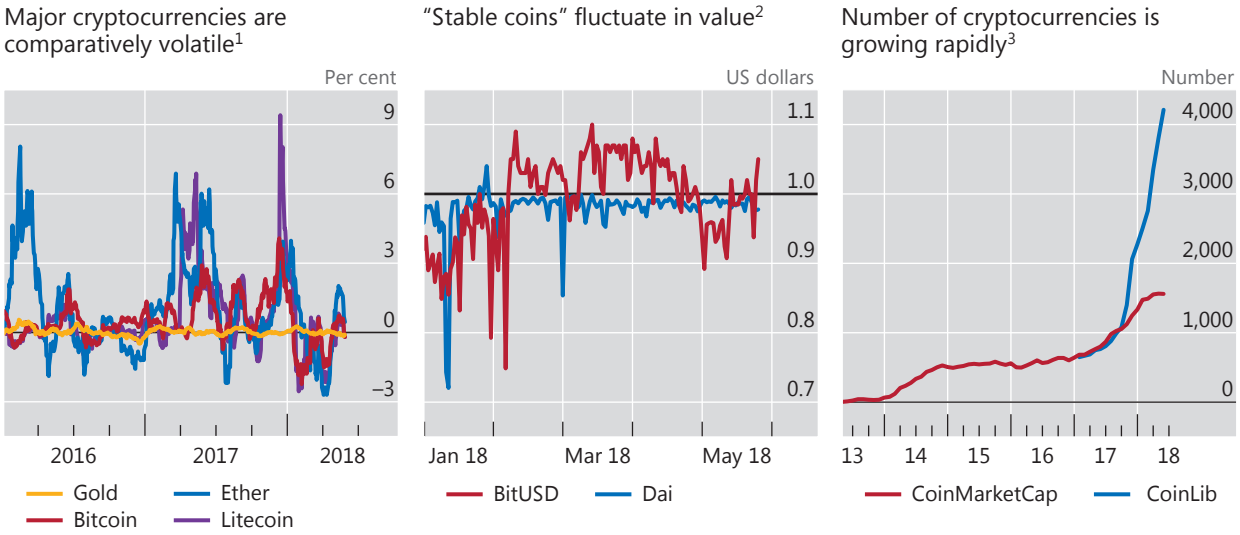
Further contributing to unstable valuations is the speed at which new cryptocurrencies – all tending to be very closely substitutable with one another – come into existence. At the time of writing, several thousand existed, though proliferation makes reliable estimates of the number of outstanding cryptocurrencies impossible (Graph V.6, right-hand panel). Recalling the private banking experiences of the past, the outcome of such liberal issuance of new moneys is rarely stability.

The third issue concerns the fragile foundation of the trust in cryptocurrencies. This relates to uncertainty about the finality of individual payments, as well as trust in the value of individual cryptocurrencies.

In mainstream payment systems, once an individual payment makes its way through the national payment system and ultimately through the central bank books, it cannot be revoked. In contrast, permissionless cryptocurrencies cannot guarantee the finality of individual payments. One reason is that although users can verify that a specific transaction is included in a ledger, unbeknownst to them there can be rival versions of the ledger. This can result in transaction rollbacks, for example when two miners update the ledger almost simultaneously. Since only one of the two updates can ultimately survive, the finality of payments made in each ledger version is probabilistic.

Volatility of select cryptocurrencies and number of cryptocurrencies

Graph V.6



[1] Thirty-day moving averages of daily returns. [2] Daily price minimum. [3] Based on monthly snapshots from two different providers. CoinMarketCap includes only cryptocurrencies with a minimum 24-hour trading volume of $100,000; CoinLib does not use a threshold.

Sources: www.bitinfocharts.com; www.coinlib.io; www.coinmarketcap.com; Datastream.

The lack of payment finality is exacerbated by the fact that cryptocurrencies can be manipulated by miners controlling substantial computing power, a real possibility given the concentration of mining for many cryptocurrencies (Graph V.7, left-hand panel). One cannot tell if a strategic attack is under way because an attacker would reveal the (forged) ledger only once they were sure of success. This implies that finality will always remain uncertain. For cryptocurrencies, each update of the ledger comes with an additional proof-of-work that an attacker would have to reproduce. Yet while the probability that a payment is final increases with the number of subsequent ledger updates, it never reaches 100%.[26]

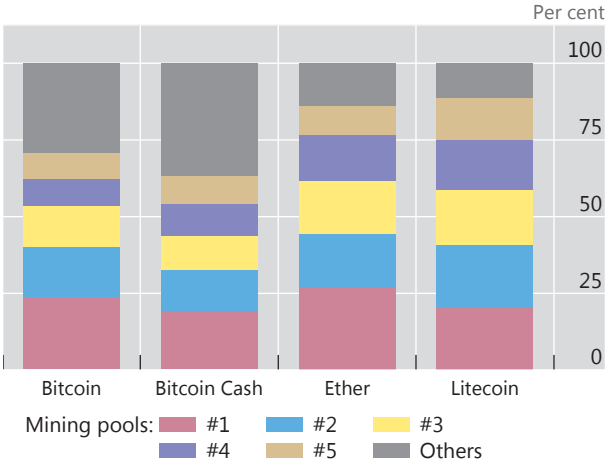
Not only is the trust in individual payments uncertain, but the underpinning of trust in each cryptocurrency is also fragile. This is due to "forking". This is a process whereby a subset of cryptocurrency holders coordinate on using a new version of the ledger and protocol, while others stick to the original one. In this way, a cryptocurrency can split into two subnetworks of users. While there are many recent examples, an episode on 11 March 2013 is noteworthy because – counter to the idea of achieving trust by decentralised means – it was undone by centralised coordination of the miners. On that day, an erroneous software update led to incompatibilities between one part of the Bitcoin network mining on the legacy protocol and another part mining using an updated one. For several hours, two separate blockchains grew; once news of this fork spread, the price of bitcoin tumbled by almost a third (Graph V.7, right-hand panel). The fork was ultimately rolled back by a coordinated effort whereby miners temporarily departed from protocol and ignored the longest chain. But many transactions were voided hours after users had believed them to be final. This episode shows just how easily cryptocurrencies can split, leading to significant valuation losses.

An even more worrying aspect underlying such episodes is that forking may only be symptomatic of a fundamental shortcoming: the fragility of the decentralised consensus involved in updating the ledger and, with it, of the underlying trust in the cryptocurrency. Theoretical analysis (Box V.A) suggests that coordination on how the ledger is updated could break down at any time, resulting in a complete loss of value.

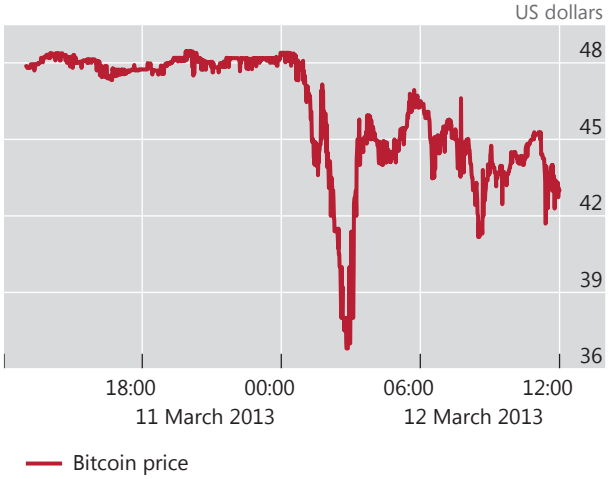
Mining concentration and bitcoin value during a temporary fork

Graph V.7

Mining is highly concentrated across all cryptocurrencies[1]



Value of bitcoin during a 2013 temporary fork[2]



[1] Data for the largest mining pools as of 28 May 2018. [2] Bitcoin price dynamics during Bitcoin fork on 11–12 March 2013.

Sources: www.btc.com; www.cash.coin.dance; CoinDesk; www.etherchain.org; www.litecoinpool.org.

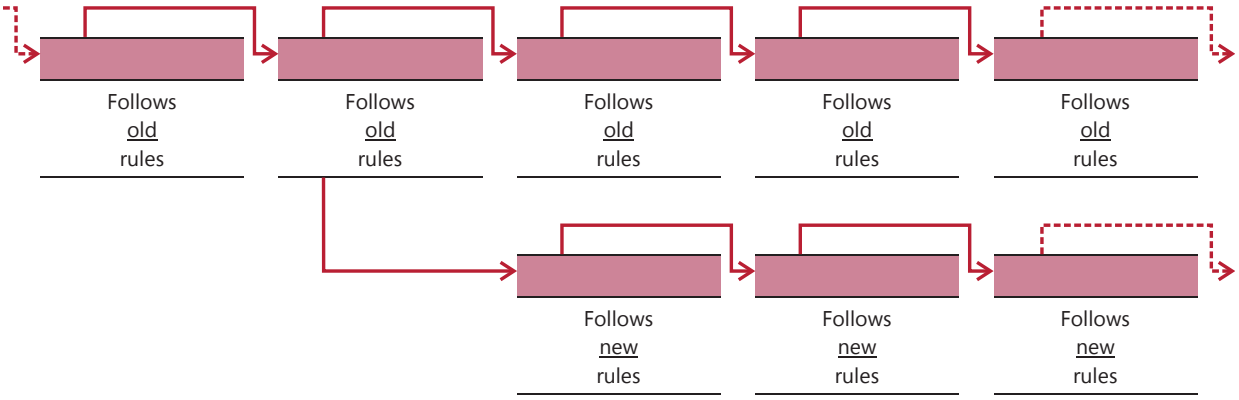
Box V.A

Forking and the instability of decentralised consensus in the blockchain

Forking has contributed to the explosive growth in the number of cryptocurrencies (Graph V.6, right-hand panel). For example, the month of January 2018 alone brought to the fore the Bitcoin ALL, Bitcoin Cash Plus, Bitcoin Smart, Bitcoin Interest, Quantum Bitcoin, BitcoinLite, Bitcoin Ore, Bitcoin Private, Bitcoin Atom and Bitcoin Pizza forks. There are many different ways in which such forks can arise, some permanent and others temporary. One example is termed a "hard fork" (Graph V.A). It arises if some of the miners of a cryptocurrency coordinate to change the protocol to a new set of rules that is incompatible with the old one. This change could involve many aspects of the protocol, such as the maximum permitted block size, the frequency at which blocks can be added to the blockchain or a change to the proof-of-work required to update the blockchain. The miners who upgrade to the new rules start from the old blockchain, but subsequently add blocks that are not recognised by the miners who have not upgraded. The latter continue to build on the existing blockchain following the old rules. In this way, two separate blockchains grow, each with its own transaction history.

Example of a hard fork

Graph V.A



Source: BIS.

Frequent episodes of forking may be symptomatic of an inherent problem with the way consensus is formed in a cryptocurrency's decentralised network of miners. The underlying economic issue is that this decentralised consensus is not unique. The rule to follow the longest chain incentivises miners to follow the computing majority, but it does not uniquely pin down the path of the majority itself. For example, if a miner believes that the very last update of the ledger will be ignored by the rest of the network of miners, it becomes optimal for the miner to also ignore this last update. And if the majority of miners coordinates on ignoring an update, this indeed becomes a new equilibrium. In this way, random equilibria can arise – and indeed frequently have arisen, as indicated by forking and by the existence of thousands of "orphaned" (Bitcoin) or "uncle" (Ethereum) blocks that have retroactively been voided. Additional concerns regarding the robustness of the decentralised updating of the blockchain relate to miners' incentives to strategically fork whenever the block added last by a different miner includes high transaction fees that can be diverted by voiding the block in question via a fork.①

① For an analysis of the uniqueness of the updating of the blockchain, see B Biais, C Bisière, M Bouvard and C Casamatta, "The blockchain folk theorem", *TSE Working Papers*, no 17–817, 2017. For an analysis of strategic motives to create a fork, see M Carlsten, H Kalodner, S M Weinberg and A Narayanan, "On the instability of Bitcoin without the block reward", *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*.

Overall, decentralised cryptocurrencies suffer from a range of shortcomings. The main inefficiencies arise from the extreme degree of decentralisation: creating the required trust in such a setting wastes huge amounts of computing power, decentralised storage of a transaction ledger is inefficient and the decentralised

consensus is vulnerable. Some of these issues might be addressed by novel protocols and other advances.[27] But others seem inherently linked to the fragility and limited scalability of such decentralised systems. Ultimately, this points to the lack of an adequate institutional arrangement at the national level as the fundamental shortcoming.

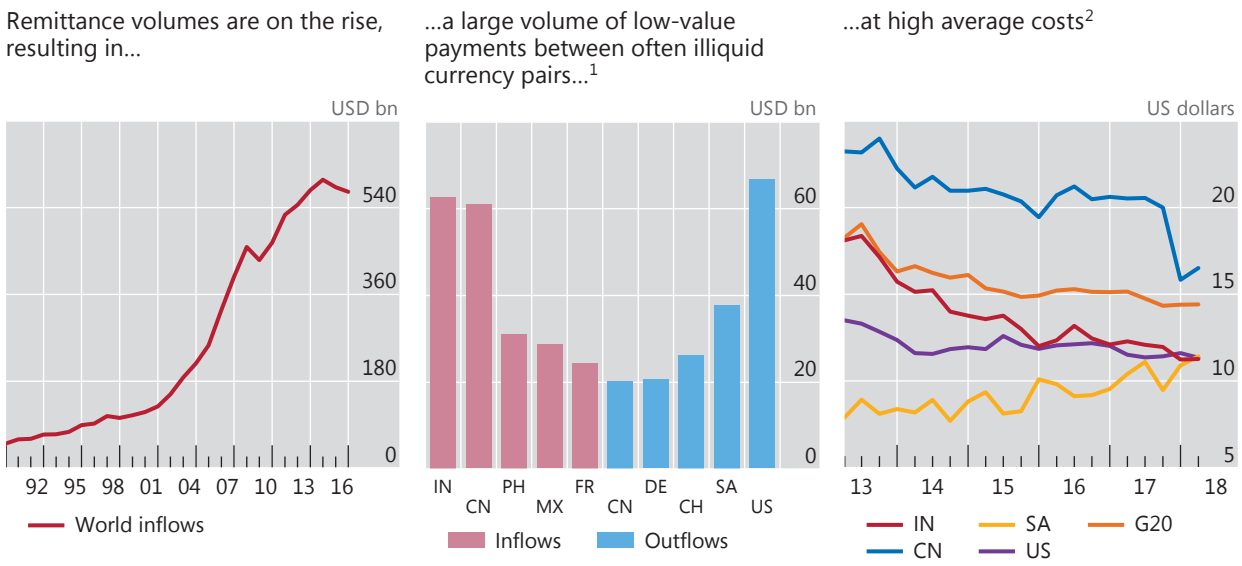
Beyond the bubble: making use of distributed ledger technology

While cryptocurrencies do not work as money, the underlying technology may have promise in other fields. A notable example is in low-volume cross-border payment services. More generally, compared with mainstream centralised technological solutions, DLT can be efficient in niche settings where the benefits of decentralised access exceed the higher operating cost of maintaining multiple copies of the ledger.

To be sure, such payment solutions are fundamentally different from cryptocurrencies. A recent non-profit example is the case of the World Food Programme's blockchain-based Building Blocks system, which handles payments for food aid serving Syrian refugees in Jordan. The unit of account and ultimate means of payment in Building Blocks is sovereign currency, so it is a "cryptopayment" system but not a cryptocurrency. It is also centrally controlled by the World Food Programme, and for good reason: an initial experiment based on the permissionless Ethereum protocol resulted in slow and costly transactions. The system was subsequently redesigned to run on a permissioned version of the Ethereum protocol. With this change, a reduction of transaction costs of about 98% relative to bank-based alternatives was achieved.[28]

Permissioned cryptopayment systems may also have promise with respect to small-value cross-border transfers, which are important for countries with a large share of their workforce living abroad. Global remittance flows total more than $540 billion annually (Graph V.8, left-hand and centre panels). Currently, forms of

Indicators of the volume and cost of remittances — Graph V.8



[1] Data for 2016. [2] Average total cost for sending $200 with all remittance service providers worldwide. For CN and IN, receiving country average total cost; for G20, SA and US, sending country average total cost.

Sources: World Bank, *Remittance Prices Worldwide*, remittanceprices.worldbank.org; World Bank; BIS calculations.

international payments involve multiple intermediaries, leading to high costs (right-hand panel). That said, while cryptopayment systems are one option to address these needs, other technologies are also being considered, and it is not clear which will emerge as the most efficient one.

More important use cases are likely to combine cryptopayments with sophisticated self-executing codes and data permission systems. Some decentralised cryptocurrency protocols such as Ethereum already allow for smart contracts that self-execute the payment flows for derivatives. At present, the efficacy of these products is limited by the low liquidity and intrinsic inefficiencies of permissionless cryptocurrencies. But the underlying technology can be adopted by registered exchanges in permissioned protocols that use sovereign money as backing, simplifying settlement execution. The added value of the technology will probably derive from the simplification of administrative processes related to complex financial transactions, such as trade finance (Box V.B). Crucially, however, none of the applications require the use or creation of a cryptocurrency.

Policy implications

The rise of cryptocurrencies and related technology brings to the fore a number of policy questions. Authorities are looking for ways to ensure the integrity of markets and payment systems, to protect consumers and investors, and to safeguard overall financial stability. An important challenge is to combat illicit usage of funds. At the same time, authorities want to preserve long-run incentives for innovation and, in particular, maintain the principle of "same risk, same regulation".[29] These are largely recurrent objectives, but cryptocurrencies raise new challenges and potentially call for new tools and approaches. A related question is whether central banks should issue their own central bank digital currency (CBDC).

Regulatory challenges posed by cryptocurrencies

A first key regulatory challenge is anti-money laundering (AML) and combating the financing of terrorism (CFT). The question is whether, and to what extent, the rise of cryptocurrencies has allowed some AML/CFT measures, such as know-your-customer standards, to be evaded. Because cryptocurrencies are anonymous, it is hard to quantify the extent to which they are being used to avoid capital controls or taxes, or to engage in illegal transactions more generally. But events such as Bitcoin's strong market reaction to the shutdown of Silk Road, a major marketplace for illegal drugs, suggest that a non-negligible fraction of the demand for cryptocurrencies derives from illicit activity (Graph V.9, left-hand panel).[30]

A second challenge encompasses securities rules and other regulations ensuring consumer and investor protection. One common problem is digital theft. Given the size and unwieldiness of distributed ledgers, as well as high transaction costs, most users access their cryptocurrency holdings via third parties such as "crypto wallet" providers or "crypto exchanges". Ironically – and much in contrast to the original promise of Bitcoin and other cryptocurrencies – many users who turned to cryptocurrencies out of distrust in banks and governments have thus wound up relying on unregulated intermediaries. Some of these (such as Mt Gox or Bitfinex) have proved to be fraudulent or have themselves fallen victim to hacking attacks.[31]

Fraud issues also plague initial coin offerings (ICOs). An ICO involves the auctioning of an initial set of cryptocurrency coins to the public, with the proceeds sometimes granting participation rights in a startup business venture. Despite

Box V.B

Distributed ledger technology in trade finance

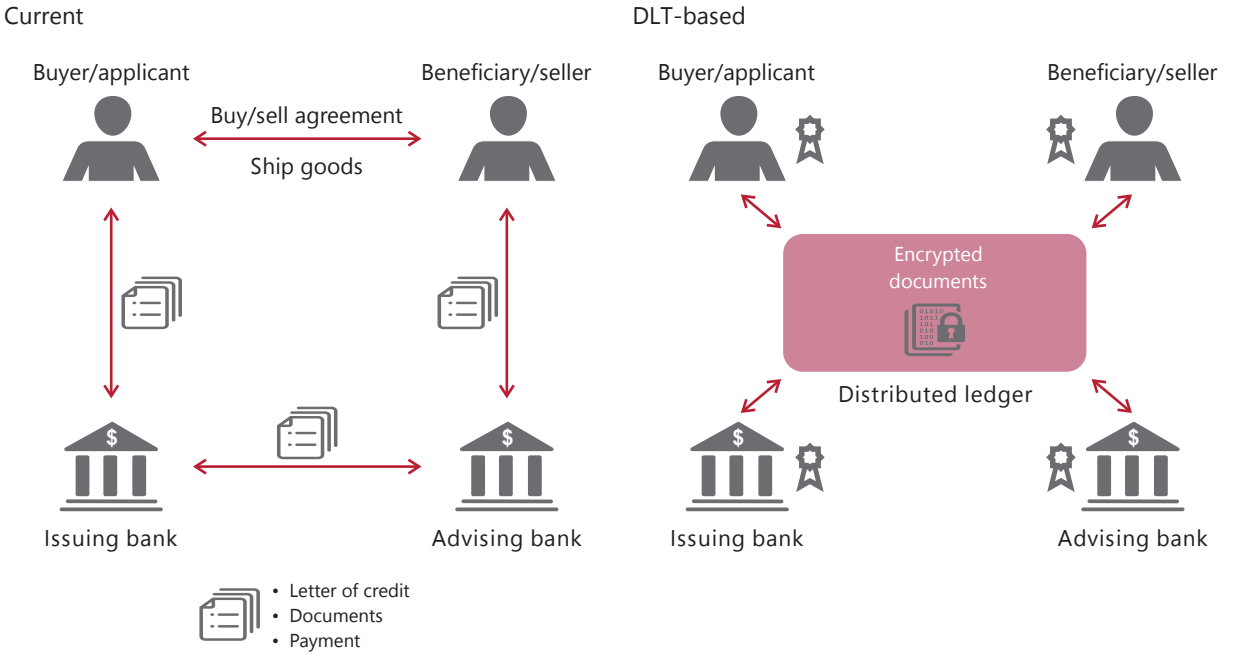
The World Trade Organization estimates that 80–90% of global trade relies on trade finance. When an exporter and an importer agree to trade, the exporter often prefers to be paid upfront due to the risk that the importer will not make a payment after receiving the goods. Conversely, the importer prefers to reduce their own risk by requiring documentation that the goods have been shipped before initiating payment.

Trade financing offered by banks and other financial institutions aims to bridge this gap. Most commonly, a bank in the importer's home country issues a letter of credit guaranteeing payment to the exporter upon receipt of documentation of the shipment, such as a bill of lading. In turn, a bank in the exporter's country might extend credit to the exporter against this pledge, and collect the payment from the importer's bank to complete the transaction.

In its current form (Graph V.B, left-hand panel), trade finance is cumbersome, complex and costly. It involves multiple document exchanges between the exporter, the importer, their respective banks, and agents making physical checks of shipped goods at each checkpoint, as well as customs agencies, public export credit agencies or freight insurers. The process often involves paper-based administration. DLT can simplify the execution of the underlying contracts (right-hand panel). For example, a smart contract might automatically release payment to the exporter upon the addition of a valid bill of lading to the ledger. And the better availability of information on which shipments have already been financed could also reduce the risk that exporters illegally obtain credit multiple times for the same shipment from different banks.

How trade finance on a distributed ledger works

Graph V.B



Source: Adapted from www.virtusapolaris.com.

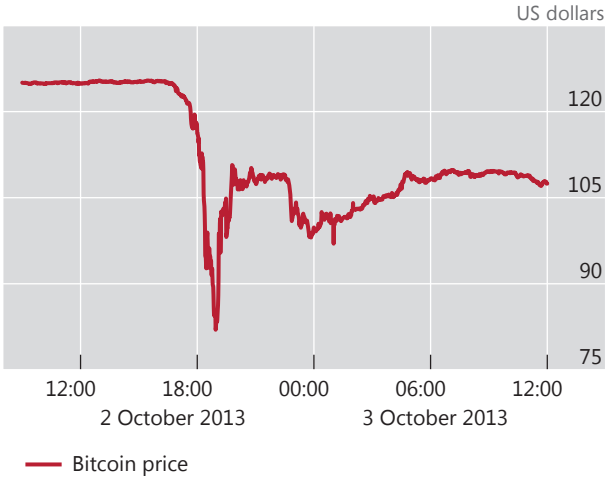
warnings by authorities, investors have flocked to ICOs even though they are often linked to opaque business projects for which minimal and unaudited information is supplied. Many of these projects have turned out to be fraudulent Ponzi schemes (Graph V.9, right-hand panel).

A third, longer-term challenge concerns the stability of the financial system. It remains to be seen whether widespread use of cryptocurrencies and related self-executing financial products will give rise to new financial vulnerabilities and systemic risks. Close monitoring of developments will be required. And, given their novel risk profiles, these technologies call for enhanced capabilities of regulators

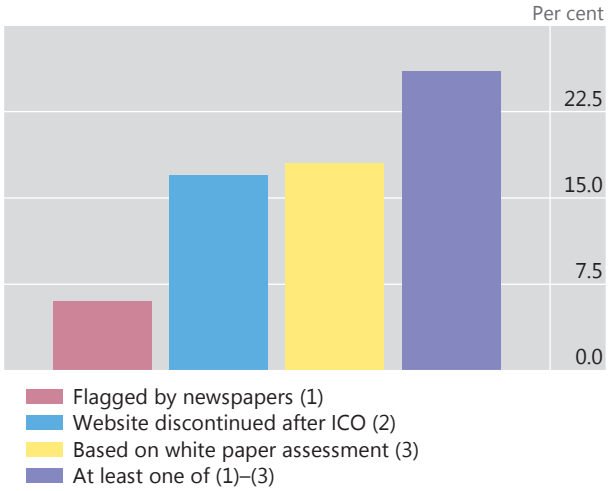
The shutdown of an illegal marketplace and the legitimacy of ICOs

Graph V.9

Cryptocurrency prices react strongly to shutdowns of illegal marketplaces[1]



A large share of initial coin offerings is thought to be fraudulent



[1] Bitcoin price during October 2013 Silk Road shutdown.

Sources: C Catalini, J Boslego and K Zhang, "Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings", *MIT Working Papers*, forthcoming; CoinDesk.

and supervisory agencies. In some cases, such as the execution of large-value, high-volume payments, the regulatory perimeter may need to expand to include entities using new technologies, to avoid the build-up of systemic risks.

The need for strengthened or new regulations and monitoring of cryptocurrencies and related cryptoassets is widely recognised among regulators across the globe. In particular, a recent communiqué of the G20 Finance Ministers and Central Bank Governors highlights issues of consumer and investor protection, market integrity, tax evasion and AML/CFT, and calls for continuous monitoring by the international standard-setting bodies. It also calls for the Financial Action Task Force to advance global implementation of applicable standards.[32]

However, the design and effective implementation of strengthened standards are challenging. Legal and regulatory definitions do not always align with the new realities. The technologies are used for multiple economic activities, which in many cases are regulated by different oversight bodies. For example, ICOs are currently being used by technology firms to raise funds for projects entirely unrelated to cryptocurrencies. Other than semantics – auctioning coins instead of shares – such ICOs are no different from initial public offerings (IPOs) on established exchanges, so it would be natural for securities regulators to apply similar regulation and supervision policies to them. But some ICOs have also doubled as "utility tokens", which promise future access to software such as games. This feature does not constitute investment activity and instead calls for the application of consumer protection laws by the relevant bodies.[33]

Operationally, the main complicating factor is that permissionless cryptocurrencies do not fit easily into existing frameworks. In particular, they lack a legal entity or person that can be brought into the regulatory perimeter. Cryptocurrencies live in their own digital, nationless realm and can largely function in isolation from existing institutional environments or other infrastructure. Their legal domicile – to the extent they have one – might be offshore, or impossible to establish clearly. As a result, they can be regulated only indirectly.

How can authorities implement a regulatory approach? Three considerations are relevant.

First, the rise of cryptocurrencies and cryptoassets calls for a redrawing of regulatory boundaries. The boundaries need to fit a new reality in which the lines demarcating the responsibilities of different regulators within and across jurisdictions have become increasingly blurred.[34] Since cryptocurrencies are global in nature, only globally coordinated regulation has a chance to be effective.[35]

Second, the interoperability of cryptocurrencies with regulated financial entities could be addressed. Only regulated exchanges can provide the liquidity necessary for DLT-based financial products to be anything but niche markets, and settlement flows ultimately need to be converted into sovereign currency. The tax and capital treatment rules for regulated institutions wanting to deal in cryptocurrency-related assets could thus be adapted. Regulators could monitor whether and how banks deliver or receive cryptocurrencies as collateral.

Third, regulation can target institutions offering services specific to cryptocurrencies. For example, to ensure effective AML/CFT, regulation could focus on the point at which a cryptocurrency is exchanged into a sovereign currency. Other existing laws and regulations relating to payment services focus on safety, efficiency and legality of use. These principles could also be applied to cryptocurrency infrastructure providers, such as "crypto wallets".[36] To avoid leakages, the regulation would ideally be broadly similar and consistently implemented across jurisdictions.

Should central banks issue digital currencies?

A related medium-term policy question concerns the issuance of CBDCs, including who should have access to them. CBDCs would function much like cash: the central bank would issue a CBDC initially, but once issued it would circulate between banks, non-financial firms and consumers without further central bank involvement.[37] Such a CBDC might be exchanged between private sector participants bilaterally using distributed ledgers without requiring the central bank to keep track and adjust balances. It would be based on a permissioned distributed ledger (Graph V.2), with the central bank determining who acts as a trusted node.

While the distinction between a general purpose CBDC and existing digital central bank liabilities – reserve balances of commercial banks – may appear technical, it is actually fundamental in terms of its repercussions for the financial system. A general purpose CBDC – issued to consumers and firms – could profoundly affect three core central banking areas: payments, financial stability and monetary policy. A recent joint report by the Committee on Payments and Market Infrastructures and the Markets Committee highlights the underlying considerations.[38] It concludes that the strengths and weaknesses of a general purpose CDBC would depend on specific design features. The report further notes that, while no leading contenders have yet emerged, such an instrument would come with substantial financial vulnerabilities, while the benefits are less clear.

At the moment, central banks are closely monitoring the technologies while taking a cautious approach to implementation. Some are evaluating the pros and cons of issuing narrowly targeted CBDCs, restricted to wholesale transactions among financial institutions. These would not challenge the current two-tier system, but would instead be intended to enhance the operational efficiency of existing arrangements. So far, however, experiments with such wholesale CBDCs have not produced a strong case for immediate issuance (Box V.C).

Box V.C

Wholesale central bank digital currencies

In recent decades, central banks have harnessed digital technologies to improve the efficiency and soundness of payments and the broader financial system. Digital technology has enabled central banks to economise on liquidity provision to real-time gross settlement (RTGS) systems. Linking these systems through Continuous Linked Settlement (CLS), commercial banks around the world settle trillions of dollars of foreign exchange around the clock every day. CLS helps to remove Herstatt risk – the risk that a correspondent bank in a foreign exchange transaction runs into financial trouble before paying the equivalent foreign currency to the designated recipient – which had previously posed a significant financial stability risk. More recently, faster retail payments have spread across the world, and central banks are actively promoting and facilitating this trend.

As part of their broader ventures into new payment technology, central banks are also experimenting with wholesale CBDCs. These are token-based versions of traditional reserve and settlement accounts. The case for wholesale DLT-based CBDCs depends on the potential for these technologies to improve efficiency and reduce operational and settlement costs. The gains could be substantial, to the extent that many current central bank-operated wholesale payment systems rely on outdated and costly-to-maintain technologies.

There are two key challenges for the implementation of wholesale CBDCs. First, the limitations of permissionless DLT also apply to CBDCs, meaning that they need to be modelled on permissioned protocols. Second, the design choices for the convertibility of central bank reserves in and out of the distributed ledger need to be implemented carefully, so as to sustain intraday liquidity while minimising settlement risks.

A number of central banks, including the Bank of Canada (Project Jasper), the ECB, the Bank of Japan (Project Stella) and the Monetary Authority of Singapore (Project Ubin), have already run experiments operating DLT-based CBDC wholesale RTGS systems. In most cases, the central banks have chosen a digital depository receipt (DDR) approach, whereby the central bank issues digital tokens on a distributed ledger backed by and redeemable for central bank reserves held in a segregated account. The tokens can then be used to make interbank transfers on a distributed ledger.

Central banks are now publishing the results. In their initial stages, each of the experiments largely succeeded in replicating existing high-value payment systems. However, the results have not been clearly superior to existing infrastructures.①

① See M Bech and R Garratt, "Central bank cryptocurrencies", *BIS Quarterly Review*, September 2017, pp 55–70; and Committee on Payments and Market Infrastructures and Markets Committee, *Central bank digital currencies*, March 2018.

Endnotes

[1] Terminology on this topic is fluid and evolving, with related legal and regulatory ambiguities. The use of the term "cryptocurrencies" in this chapter is not meant to indicate any particular view of what the underlying protocol-based systems are; typically, they have some, but not all, of the characteristics of a sovereign currency and their legal treatment varies across jurisdictions. In some cases, the chapter refers to specific cryptocurrencies or cryptoassets as examples. These examples are not exhaustive and do not constitute any endorsement by the BIS or its shareholders of any cryptocurrency, firm, product or service.

[2] On this issue, see also Carstens (2018a,c).

[3] Graeber (2011) argues that money only became widespread with the invention of coinage, which appeared in China, India and Lydia almost simultaneously around 600–500 BCE. He further shows that, contrary to popular belief, prior to the use of money, exchange took place mostly through bilateral IOUs rather than barter.

[4] These functions of money have been studied extensively in the literature. A few key examples are the following: Kiyotaki and Wright (1989) show how money, when used as a medium of exchange, can improve on barter. Kocherlakota (1996) shows that when perfect record-keeping and commitment are not possible, money improves outcomes by serving as "memory". Samuelson (1958) shows in an overlapping generations model that money can improve efficiency when used as store of value. Doepke and Schneider (2017) show how using a common unit of account improves outcomes and why government money is the unit of account and the medium of exchange at the same time.

[5] Examples of items used as commodity money include shells in Africa, cocoa beans in the Aztec civilisation and wampum in North American colonies. Even in these cases, credit relationships no doubt coexisted with these arrangements. See eg Melitz (1974) for a more detailed discussion.

[6] On the evolution of letters of credit and the pivotal role they have played in the development of monetary systems in general, and the financing of trade in particular, see De Roover (1948, 1953). For a detailed analysis and history, see Kindleberger (1984) for a general treatment and Santarosa (2015) for the importance of the introduction of joint liability.

[7] Commodity-backed government money, such as the gold standard, was another attempt to strike a balance. While offering stability in normal times, its constraints have tended to limit the central bank's ability to elastically supply currencies at times of financial and economic strains. In extreme circumstances, these constraints have often simply been discarded, with a shift to inconvertibility. For example, under the gold standard, one could regard the function of convertibility into gold as constraining the sovereign's ability to overissue and debase the currency. The constraint was credible precisely because the commodity has a market value in non-monetary uses, ie other than as a means of payment. This prevented the sovereign from keeping the holders hostage to its monopoly powers. See Giannini (2011) for further discussion.

[8] For a recent treatment, including an analysis of incentives to debase the money, see Schnabel and Shin (2018).

[9] See Van Dillen (1964), Roberds and Velde (2014) and Bindseil (2018). For the link with central banking, see Ugolini (2017), Bindseil (2018) and Schnabel and Shin (2018).

[10] Moreover, central banks have generally had the flexibility to act as lenders of last resort. The recent Great Financial Crisis was yet another reminder of the both the fragility and the adaptability of the current monetary arrangements, even in the most advanced economies. While the crisis laid bare the shortcomings of the prevailing regulatory framework, the increased focus post-crisis on bank supervision and regulation highlights how institutional arrangements can evolve to maintain trust in money within the broad framework of the two-tiered system.

[11] See Carstens (2018a). Giannini (2011) also highlights the importance of institutional arrangements through which money is supplied: "The evolution of monetary institutions appears to be above all the fruit of a continuous dialogue between economic and political spheres, with each taking turns to create monetary innovations … and to safeguard the common interest against abuse stemming from partisan interests."

[12] Indeed, central banks these days oversee payment systems and provide large amounts of intraday credit to secure precisely this outcome, notably in wholesale payment systems. Depending on the specificities of the arrangements, this credit may also be extended overnight or at longer maturities. For a further description of the arrangements, operating procedures and other issues, see BIS (1994) and Borio (1997).

[13] See Bech and Garratt (2017) and CPMI-MC (2018) for a detailed discussion.

[14] Much like with banknotes and other physical tokens, each transaction is verified with reference to the payment object, ie the respective ledger entry. This differs from other forms of electronic money, where verification is based on the identity of the account holder. Cryptocurrencies are hence token-based digital money.

[15] Current or planned examples of cryptocurrencies employing a permissioned model with designated trusted nodes include the coin to be issued by the SAGA Foundation, Ripple and Utility Settlement Coin.

[16] We use "Bitcoin" to denote the protocol and network of users and miners of the cryptocurrency, and "bitcoin" to denote the unit of currency.

[17] Examples include Ethereum, Litecoin and Namecoin.

[18] Auer (2018) presents a detailed description of the technological elements of Bitcoin and other blockchain-based cryptocurrencies such as digital signatures, hashing and the cryptographic chaining of blocks. See also Berentsen and Schär (2018).

[19] Technically, this is implemented via the use of cryptographic hash functions (such as SHA-256 in Bitcoin). These have the property that results are unpredictable, and a specific result can thus only be generated by trial and error.

[20] For a permissionless cryptocurrency to function in an entirely trustless environment, all miners and users need to store an up-to-date copy of the entire ledger. However, in practice many users trust the information provided by others. Some users only verify summary information of the ledger via a process called simplified payment verification. And, much in contrast to the original idea underlying Bitcoin, an even larger number of users can only access their funds through a third-party website. In these cases, the third party alone is in control of its clients' cryptocurrency holdings.

[21] Nakamoto (2009), p 8.

[22] This is achieved by self-calibration of the proof-of-work, which increases the required level of mathematical difficulty up to the point where the combined computing power of all miners just suffices to update the ledger at the speed pre-set by the protocol.

[23] See Carstens (2018a).

[24] While congestion could be removed by allowing for bigger block sizes, this might actually be even more destructive. Block rewards aside, having some congestion is essential to induce users to pay for transactions, for if the system operates below its limit, all transactions will be processed and rational users will thus post almost no transaction fees. The miners would not receive any benefits for updating the transactions, and the equilibrium could break down. See in particular Hubermann et al (2017) and Easley et al (2017), as well as Abadi and Brunnermeier (2018).

[25] In technical terms, the interaction between the users is that of strategic substitutes, not strategic complements. Cryptocurrencies are hence a congestion, rather than a coordination, game.

[26] The probabilistic nature of finality could in particular create aggregate risks if cryptocurrencies were used in wholesale settings, where funds tend to be reinvested without delay. In fact, this would create an entirely new dimension of aggregate risk, as exposures would be linked to each other via the probability of non-finality of the entire transaction history.

[27] There is no shortage of proposed solutions, but most have yet to be proved in practice. On the one hand, future cryptocurrency protocols might do away with costly proof-of-work by replacing it with "proof-of-stake", the underlying idea of which is to achieve credibility by staking cryptocurrency holdings rather than doing costly computational work. Proposed solutions for the scaling problem include the Lightning Network, which essentially shifts small transactions off the main blockchain and into a separate pre-funded environment. There are also new cryptocurrencies, such as IOTA, that aim to replace the blockchain with a more complex ledger and verification structure.

[28] See Juskalian (2018).

[29] See Carstens (2018a,b).

[30] Government officials are also not immune from the lure of cryptocurrencies: two US government agents have been charged with theft of bitcoins confiscated during the closing of Silk Road.

[31] For example, most bitcoin payments made via smartphone are most likely made indirectly via third party, since the current blockchain size exceeds the storage capacity of most smartphones. Reuters (2017) and Moore and Christin (2013) list some of the cases in which such third parties have proved to be fraudulent or have fallen victim to hacking attacks. For an analysis of illicit uses of cryptocurrencies, see Fanusie and Robinson (2018) and Foley et al (2018).

[32] See G20 Finance Ministers and Central Bank Governors (2018).

[33] Clayton (2017), discussing the regulation of ICOs as opposed to IPOs from a US perspective, states that a "change in the structure of a securities offering does not change the fundamental point that when a security is being offered, our securities laws must be followed". FINMA (2018) sets out a regulatory framework in Switzerland that classifies ICOs according to the eventual use of the tokens issued: in payments, as assets or as utility tokens.

[34] Technically, all that is needed for protocol-based cryptocurrencies to operate is for at least one country to allow access. The authorities' difficulties in shutting down illegal download sites such as Napster or The Pirate Bay and download protocols such as BitTorrent underline the associated enforcement problems.

[35] Financial Action Task Force (2015) argues that treating similar products and services consistently according to their function and risk profile across jurisdictions is essential for enhancing the effectiveness of the international AML standards.

[36] One complication is that payments are regulated by a set of authorities and laws with very different goals, such as payment system oversight, prudential supervision, consumer protection and AML/CFT. For example, US-based institutions must adhere to, among others, the Bank Secrecy Act, the USA PATRIOT Act and Office of Foreign Assets Control regulations. Another complication has to do with the applicability of existing legislation to the new instruments. For instance, in the European Union the legal definition of electronic money includes the requirement that balances should represent a claim on the issuer. As cryptocurrencies do not represent any claim, they cannot be considered electronic money and are thus by default not covered by the respective legislation.

[37] There are many potential technical implementations of token-based CBDCs. They could be based on DLT, with similar characteristics to cryptocurrencies, with the difference being that the central bank rather than the protocol itself would be in control of the amount issued and would guarantee the token's value.

[38] CPMI-MC (2018).

References

Abadi, J and M Brunnermeier (2018): "Blockchain economics", Princeton University, mimeo, May.

Auer, R (2018): "The mechanics of decentralised trust in Bitcoin and the blockchain", *BIS Working Papers*, forthcoming.

Bank for International Settlements (1994): *64th Annual Report*, June.

Bech, M and R Garratt (2017): "Central bank cryptocurrencies", *BIS Quarterly Review*, September 2017, pp 55–70.

Berentsen, A and F Schär (2018): "A short introduction to the world of cryptocurrencies", Federal Reserve Bank of St Louis, *Review*, vol 100, no 1.

Bindseil, U (2018): "Pre-1800 central bank operations and the origins of central banking", Mannheim University, mimeo.

Borio, C (1997): "The implementation of monetary policy in industrial countries: a survey", *BIS Economic Papers*, no 47, July.

Carstens, A (2018a): "Money in the digital age: what role for central banks?", lecture at the House of Finance, Goethe University, Frankfurt, 6 February.

——— (2018b): "Central banks and cryptocurrencies: guarding trust in a digital age", remarks at Brookings Institution, Washington DC, 17 April.

——— (2018c): "Technology is no substitute for trust", *Börsen-Zeitung*, 23 May.

Catalini, C, J Boslego and K Zhang (2018): "Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings", *MIT Working Papers*, forthcoming.

Clayton, J (2017): "Statement on cryptocurrencies and initial coin offerings", www.sec.gov/news/public-statement/statement-clayton-2017-12-11, 11 December.

Committee on Payments and Market Infrastructures and Markets Committee (2018): *Central bank digital currencies*, March.

De Roover, R (1948): *Money, banking and credit in mediaeval Bruges: Italian merchant-bankers, Lombards and money changers – a study in the origins of banking*, Mediaeval Academy of America.

——— (1953): *L'évolution de la lettre de change: XIVe-XVIIIe siècle*, Armand Colin.

Doepke, M and M Schneider (2017): "Money as a unit of account", *Econometrica*, vol 85, no 5, pp 1537–74.

Easley, D, M O'Hara and S Basu (2017): "From mining to markets: The evolution of Bitcoin transaction fees", papers.ssrn.com/sol3/papers.cfm?abstract_id=3055380.

Fanusie, Y and T Robinson (2018): "Bitcoin laundering: an analysis of illicit flows into digital currency services", Center on Sanctions & Illicit Finance memorandum, January.

Financial Action Task Force (2015): *Guidance for a risk-based approach to virtual currencies*, June.

Financial Market Supervisory Authority (FINMA) (2018): *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 16 February.

Foley, S, J Karlsen and T Putniņš (2018): "Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?", dx.doi.org/10.2139/ssrn.3102645.

G20 Finance Ministers and Central Bank Governors (2018): Buenos Aires Summit communiqué, 19–20 March.

Giannini, C (2011): *The age of central banks*, Edward Elgar.

Graeber, D (2011): *Debt: the first 5,000 years*, Melville House.

Huberman, G, J Leshno and C Moellemi (2017): "Monopoly without a monopolist: an economic analysis of the Bitcoin payment system", *Columbia Business School Research Papers*, no 17–92.

Juskalian, R (2018): "Inside the Jordan refugee camp that runs on blockchain", *MIT Technology Review*, online edition, 12 April.

Kindleberger, C (1984): *A financial history of western Europe*, Allen & Unwin.

Kiyotaki, N and R Wright (1989): "On money as a medium of exchange", *Journal of Political Economy*, vol 97, no 4, pp 927–54.

Kocherlakota, N (1996): "Money is memory", *Journal of Economic Theory*, vol 81, issue 2, pp 232–51.

Melitz, J (1974): *Primitive and modern money: an interdisciplinary approach*, Addison-Wesley.

Moore, T and N Christin (2013): "Beware the middleman: empirical analysis of Bitcoin-exchange risk", in A-R Sadeghi (ed), *Lecture Notes in Computer Science*, vol 7859.

Nakamoto, S (2009): "Bitcoin: a peer-to-peer electronic cash system", white paper.

Reuters (2017): "Cryptocurrency exchanges are increasingly roiled by hackings and chaos", 29 September.

Roberds, W and F Velde (2014): "Early public banks", *Federal Reserve Bank of Chicago Working Papers*, no 2014–03.

Samuelson, P (1958): "An exact consumption-loan model of interest with or without the social contrivance of money", *Journal of Political Economy*, vol 66, no 6, pp 467–82.

Santarosa, V (2015): "Financing long-distance trade: the joint liability rule and bills of exchange in eighteenth-century France", *The Journal of Economic History*, vol 75, no 3, pp 690–719.

Schnabel, I and H S Shin (2018): "Money and trust: lessons from the 1620s for money in the digital age", *BIS Working Papers*, no 698, February.

Ugolini, S (2017): *The evolution of central banking: theory and history*, Palgrave-Macmillan.

Van Dillen, J G (1964): *History of the principal public banks*, Frank Cass & Co.