Morten Bech
morten.bech@bis.org

Rodney Garratt
garratt@ucsb.edu

Central bank cryptocurrencies[1]

New cryptocurrencies are emerging almost daily, and many interested parties are wondering whether central banks should issue their own versions. But what might central bank cryptocurrencies (CBCCs) look like and would they be useful? This feature provides a taxonomy of money that identifies two types of CBCC – retail and wholesale – and differentiates them from other forms of central bank money such as cash and reserves. It discusses the different characteristics of CBCCs and compares them with existing payment options.

JEL classification: E41, E42, E51, E58.

In less than a decade, bitcoin has gone from being an obscure curiosity to a household name. Its value has risen – with ups and downs – from a few cents per coin to over $4,000. In the meantime, hundreds of other cryptocurrencies – equalling bitcoin in market value – have emerged (Graph 1, left-hand panel). While it seems unlikely that bitcoin or its sisters will displace sovereign currencies, they have demonstrated the viability of the underlying blockchain or distributed ledger technology (DLT). Venture capitalists and financial institutions are investing heavily in DLT projects that seek to provide new financial services as well as deliver old ones more efficiently. Bloggers, central bankers and academics are predicting transformative or disruptive implications for payments, banks and the financial system at large.[2]

Lately, central banks have entered the fray, with several announcing that they are exploring or experimenting with DLT, and the prospect of central bank crypto- or digital currencies is attracting considerable attention. But making sense of all this is difficult. There is confusion over what these new currencies are, and discussions often occur without a common understanding of what is actually being proposed. This feature seeks to provide some clarity by answering a deceptively simple question: what are central bank cryptocurrencies (CBCCs)?

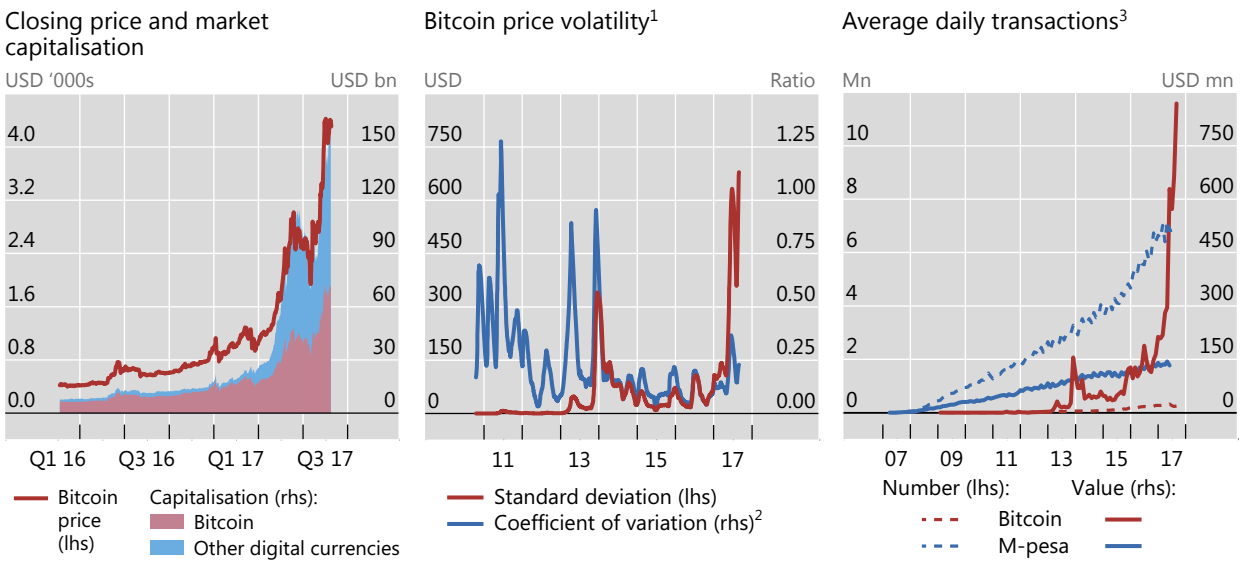
To that end, we present a taxonomy of money that is based on four key properties: *issuer* (central bank or other); *form* (electronic or physical); *accessibility* (universal or limited); and *transfer mechanism* (centralised or decentralised). The

[1] The views expressed in this article are those of the authors and do not necessarily reflect those of the BIS. We thank Claudio Borio, Stijn Claessens, Benjamin Cohen, Dietrich Domanski, Hana Halaburda, Krista Hughes, Jochen Schanz and Hyun Song Shin for comments as well as Aleksander Berentsen, James Chapman and Paul Wong for insightful discussions. We are grateful to Codruta Boar for excellent research assistance.

[2] See Andolfatto (2015, 2016), Broadbent (2016), Raskin and Yermack (2016) and Skingsley (2016).

Bitcoin

Graph 1



[1] Ninety-day moving averages. [2] Ratio of standard deviation to mean. [3] Monthly averages. For bitcoin, estimated transaction value in USD; for M-pesa™, transaction value in KES converted into USD.

Sources: Central Bank of Kenya; CoinDance; CoinDesk; www.blockchain.info; authors' calculations.

taxonomy defines a CBCC as an electronic form of central bank money that can be exchanged in a decentralised manner known as *peer-to-peer*, meaning that transactions occur directly between the payer and the payee without the need for a central intermediary.[3] This distinguishes CBCCs from other existing forms of electronic central bank money, such as reserves, which are exchanged in a centralised fashion across accounts at the central bank. Moreover, the taxonomy distinguishes between two possible forms of CBCC: a widely available, consumer-facing payment instrument targeted at retail transactions; and a restricted-access, digital settlement token for wholesale payment applications.[4]

But what might the two types of CBCC offer that alternative forms of central bank money cannot? For the consumer-facing kind, we argue that the peer-to-peer element of the new technology has the potential to provide anonymity features that are similar to those of cash but in digital form. If anonymity is not seen as important, then most of the alleged benefits of retail CBCCs can be achieved by giving the public access to accounts at the central bank, something that has been technically feasible for a long time but which central banks have mostly stayed away from.

On the wholesale side, the assessment of CBCCs is quite different. Wholesale payments today do not offer cash-like anonymity. In particular, transactions that occur in wholesale systems are visible to the central operator. Hence, the case for wholesale CBCCs depends on their ability to improve efficiency and reduce settlement

[3] The purest form of peer-to-peer transaction is a cash exchange. On a computer network, the peer-to-peer concept means that transactions can be processed without the need for a central server.

[4] It is common to divide payments into retail and wholesale segments. Retail payments are relatively low-value transactions, in the form of eg cheques, credit transfers, direct debits and card payments. By contrast, wholesale payments are large-value and high-priority transactions, such as interbank transfers. The distinction might become less relevant in a world with CBCCs. In that case, our usage would reflect the types of payment primarily targeted by CBCCs.

costs. Here, the answer depends on a number of technical issues that still need to be resolved. Some central banks have experimented with wholesale CBCCs, but none has announced yet that it is ready to adopt this technology.

The first section presents the taxonomy underlying our definition. The following two sections discuss the features of the two basic CBCC types, retail and wholesale, drawing on historical examples and projects that are currently under way. A concluding section reflects on some of the issues that central banks need to consider in this area going forward.

A new form of central bank money

Our starting point for defining CBCCs is a report on cryptocurrencies published in 2015 by the Committee on Payments and Market Infrastructures (CPMI (2015)).[5] This report sought to provide a definition of the new class of currencies represented by bitcoin and altcoins (alternatives to bitcoin) that had emerged using the same technology. The report identifies three key characteristics of cryptocurrencies: they are *electronic*; are *not the liability of anyone;* and feature *peer-to-peer* exchange.[6]

Cryptocurrencies utilise DLT (Box A) to allow remote peer-to-peer transfer of electronic value in the absence of trust between contracting parties. Usually, electronic representations of money, such as bank deposits, are exchanged via centralised infrastructures, where a trusted intermediary clears and settles transactions. Previously, peer-to-peer exchange was restricted to physical forms of money.

Some – but not all – of these features are also common to other forms of money (Graph 2, left-hand panel). Cash is peer-to-peer, but it is not electronic, and it is a central bank liability. Commercial bank deposits are a liability of the bank that issues them. Nowadays, they are in electronic form and are exchanged in a centralised manner either across the books of a given bank or between different banks via the central bank. Most commodity monies, such as gold coins, may also be transferred in a peer-to-peer fashion but are neither the liability of anyone nor electronic.[7]

It may seem natural to define CBCCs by adapting the CPMI's definition to say that they are electronic central bank liabilities that can be used in peer-to-peer exchanges. But this ignores an important feature of other forms of central bank money, namely *accessibility*. Currently, one form of central bank money – cash – is of course accessible to everyone, while central bank settlement accounts are typically available only to a limited set of entities, mainly banks (CPSS (2003, p 3)). In this spirit, Bjerg (2017) includes *universally accessible* (ie easy to obtain and use) in addition to *electronic* and *central bank-issued* in defining the new concept of central bank digital currency (Graph 2, right-hand panel).

[5] The report's title is *Digital currencies*, but it notes that such schemes are frequently also referred to as "cryptocurrencies", reflecting the use of cryptography in their issuance and their validation of transactions.

[6] Cryptocurrencies have no intrinsic value and are only held in the belief that they might be exchanged for goods or services at a later point in time.

[7] In the Middle Ages, payments at times required the services of a money changer to assay and value the coins being used.

Box A

What is distributed ledger technology?①

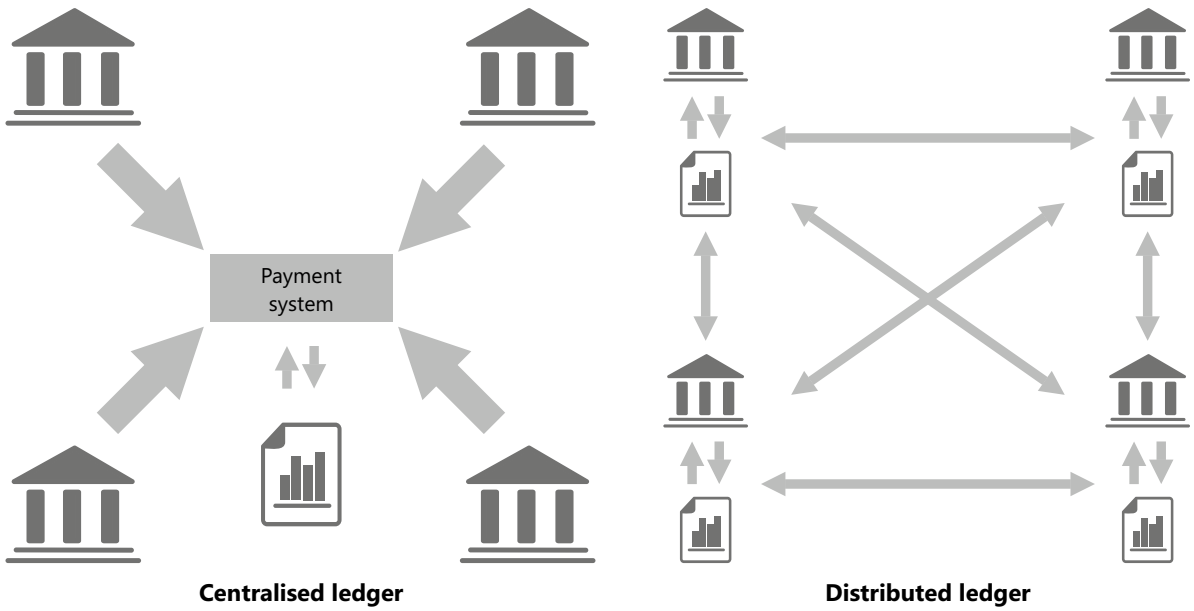
Distributed ledger technology (DLT) refers to the protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronised way across a network. The idea of a distributed ledger – a common record of activity that is shared across computers in different locations – is not new. Such ledgers are used by organisations (eg supermarket chains) that have branches or offices across a given country or across countries. However, in a traditional distributed database, a system administrator typically performs the key functions that are necessary to maintain consistency across the *multiple copies* of the ledger. The simplest way to do this is for the system administrator to maintain a master copy of the ledger which is periodically updated and shared with all network participants.

By contrast, the new systems based on DLT, most notably Bitcoin and Ethereum, are designed to function without a trusted authority. Bitcoin maintains a distributed database in a decentralised way by using a consensus-based validation procedure and cryptographic signatures. In such systems, transactions are conducted in a peer-to-peer fashion and broadcast to the entire set of participants who work to validate them in batches known as "blocks". Since the ledger of activity is organised into separate but connected blocks, this type of DLT is often referred to as "blockchain technology".

The blockchain version of DLT has successfully powered Bitcoin for several years However, the system is not without drawbacks: it is costly to operate (preventing double-spending without the use of a trusted authority requires transaction validators (miners) to employ large amounts of computing power to complete "proof-of-work" computations);② there is only probabilistic finality of settlement; and all transactions are public. These features are not suitable for many financial market applications. Current wholesale DLT payment applications have therefore abandoned the standard blockchain technology in favour of protocols that modify the consensus process in order to allow enhanced confidentiality and scalability. Examples of protocols currently being tested by central banks include Corda and Hyperledger Fabric. Corda replaces blockchain with a "notary" architecture. The notary design utilises a trusted authority and allows consensus to be reached on an individual transaction basis, rather than in blocks, with limited information-sharing.

Distributed ledger system

Graph A

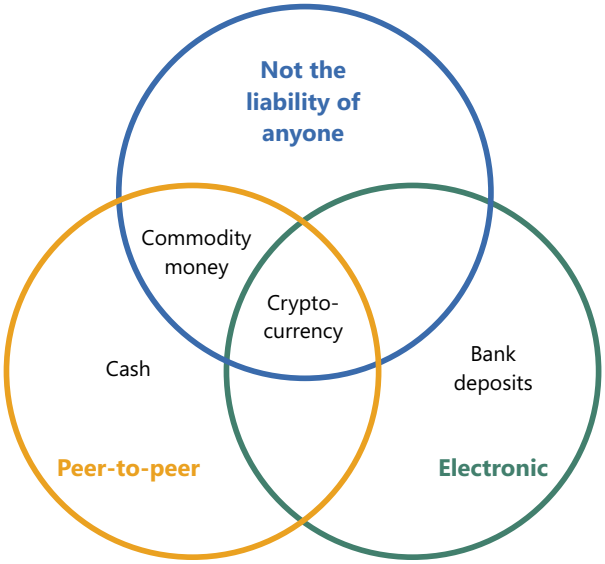


Source: Santander InnoVentures (2015).

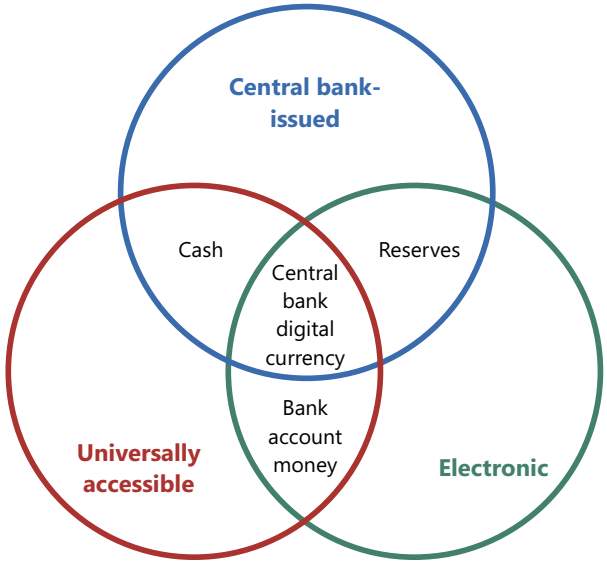
① See also Chapman et al (2017), CPMI (2015) and Benos et al (2017). ② The amount of energy currently being used by Bitcoin miners is equal to the energy consumption of Lebanon and Cuba (see http://digiconomist.net/bitcoin-energy-consumption). For a detailed description of proof-of-work, see https://en.bitcoin.it/wiki/Proof_of_work.

Two taxonomies of new forms of currency Graph 2

Cryptocurrency, CPMI (2015)



Central bank digital currency, Bjerg (2017)



We combine the properties discussed in CPMI (2015) and Bjerg (2017) to establish a new taxonomy of money. Our properties are: *issuer* (central bank or other); *form* (electronic or physical); *accessibility* (universal or limited); and *transfer mechanism* (centralised or decentralised, ie peer-to-peer). This taxonomy reflects what appears to be emerging in practice and distinguishes between two potential types of CBCC, both of which are electronic: central bank-issued and peer-to-peer. One is accessible to the general public (retail CBCC) and the other is available only to financial institutions (wholesale CBCC). Again, a Venn diagram is useful for illustration.[8] The four-ellipse version in Graph 3, which we call the *money flower*, shows how the two potential types of CBCC fit into the overall monetary landscape.

In principle, there are four different kinds of electronic central bank money: two kinds of CBCCs (the shaded area) and two kinds of central bank deposits. The most familiar forms of central bank deposits are those held by commercial banks – often referred to as settlement accounts or reserves. The other form is, at least in theory, deposits held by the general public. Tobin (1987) refers to this form as *deposited currency accounts* (DCAs).[9] So far, central banks have generally chosen not to provide DCAs.

Universally accessible forms of money that are not issued by the central bank include (privately created) cryptocurrency, commodity money, commercial bank

[8] A four-circle Venn diagram covers only 14 of the $2^4 = 16$ possible combinations. Hence, in the case of four sets, Venn (1881) suggested using ellipses in order to show all cases.

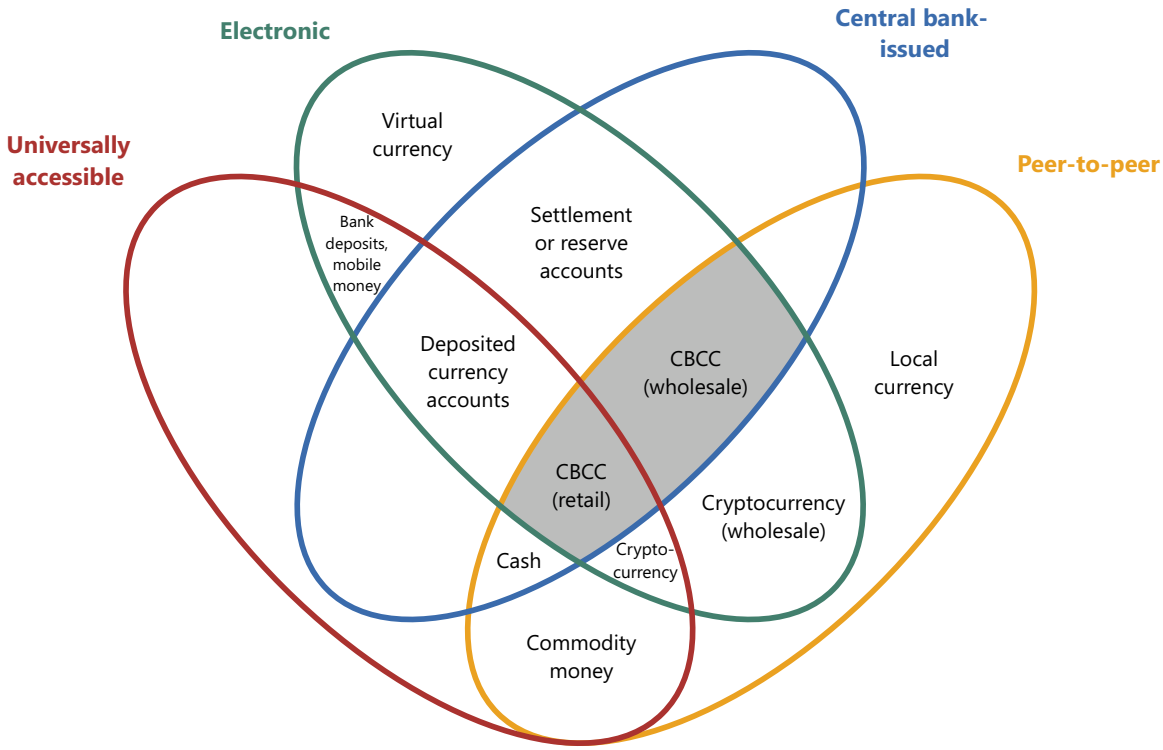
[9] In a 1987 speech, Nobel laureate James Tobin argued that, in order to avoid relying too heavily on deposit insurance to protect the payment system, central banks should "make available to the public a medium with the convenience of deposits and the safety of currency, essentially currency on deposit, transferable in any amount by check or other order" (Tobin (1987, p 6); see also Tobin (1985)). That is, people should be able to store value without being subject to the risk of bank failure.

deposits and mobile money.[10] Cryptocurrency borders CBCC given that only one of its properties differs. The other three currency forms are more removed because they are, in addition, either physical or "not peer-to-peer". A number of other forms of money are not universally accessible. Local (physical) currencies, ie currencies that can be spent in a particular geographical location at participating organisations, populate the right-hand petal of the flower. The upper left-hand petal contains virtual currencies, which are "electronic money issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" (ECB (2012)). There is also the possibility of a private sector wholesale version of cryptocurrency. It would be transferred in a peer-to-peer fashion by means of a distributed ledger, but only between certain financial institutions.

Box B uses this taxonomy to classify different examples of money from the past, present and future according to where they would fit in the money flower. The remainder of this feature discusses the two types of CBCC in further detail and highlights some of the many issues central banks will need to consider if they ever chose to adopt them. We start with the retail variant and then turn to the wholesale one.

The money flower: a taxonomy of money

Graph 3



[10] Mobile money is an electronic wallet service that allows users to store, send and receive money using their mobile phones. The value stored in the wallets may be liabilities of the service provider or claims on money held in trust at a commercial bank.

Box B

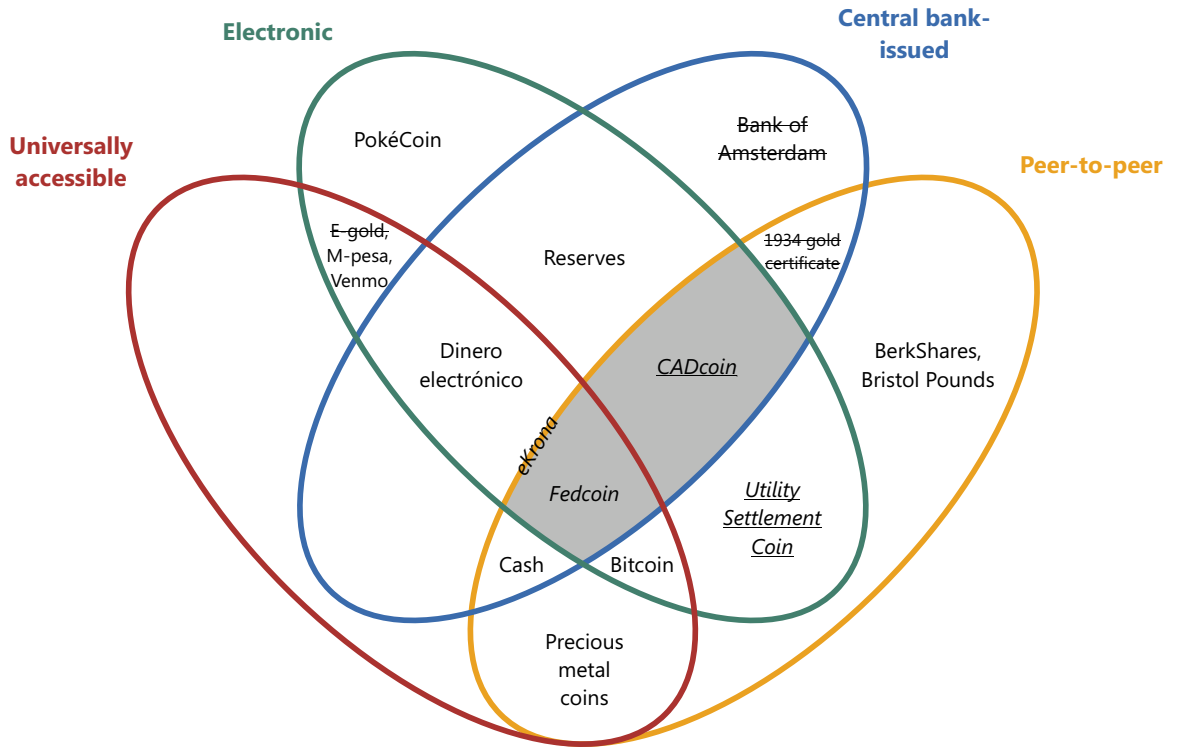
The money flower with selected examples

Graph B fills out the money flower with examples of money from the past, present and possibly the future. Starting at the centre, we have **Fedcoin**, as an example of a retail CBCC. The concept, which was proposed by Koning (2014) and has not been endorsed by the Federal Reserve, is for the central bank to create its own cryptocurrency. The currency could be converted both ways at par with the US dollar and conversion would be managed by the Federal Reserve Banks.① Instead of having a predetermined supply rule, as is the case with Bitcoin, the supply of Fedcoin would, much like cash, increase or decrease depending on the desire of consumers to hold it. Fedcoin would become a third component of the monetary base, alongside cash and reserves. Unlike Bitcoin, Fedcoin would not represent a competing, private "outside money" but would instead be an alternative form of sovereign currency (Garratt and Wallace (2016)).

CADcoin is an example of a wholesale CBCC. It is the original name for digital assets representing central bank money used in the Bank of Canada's proof of concept for a DLT-based wholesale payment system. CADcoin has been used in simulations performed by the Bank of Canada in cooperation with Payments Canada, R3 (a fintech firm), and several Canadian banks but has not been put into practice.

The money flower: example

Graph B



A standard font indicates that a system is in operation; an *italic* font indicates a proposal; an *italic and underlined* font indicates experimentation; a ~~strikethrough~~ font indicates a defunct company or an abandoned project.

In Sweden, the demand for cash has dropped considerably over the past decade (Skingsley (2016)). Already, many stores do not accept cash and some bank branches no longer disburse or collect cash. In response, the Riksbank has embarked on a project to determine the viability of an **eKrona** for retail payments. No decision has yet been taken in terms of technology (Sveriges Riksbank (2017)). Hence, the eKrona is located on the border between deposited currency accounts and retail CBCCs.

Dinero electrónico is a mobile payment service in Ecuador where the central bank provides the underlying accounts to the public. Citizens can open an account by downloading an app, registering their national identity number and answering security questions. People deposit or withdraw money by going to designated transaction centres. As such, it is a (rare) example of a deposited currency account scheme. As Ecuador uses the US dollar as its official currency, accounts are denominated in that currency.

Bitcoin is an example of a non-central bank digital currency. It was invented by an unknown programmer who used the pseudonym Satoshi Nakamoto and was released as open-source software in 2009 along with a white paper describing the technical aspects of its design (see Box A for further details).

PokéCoin is a currency used for in-game purchases in the Pokémon Go game and an example of a virtual currency.

Utility Settlement Coin (USC) is an attempt by the private sector to provide a wholesale cryptocurrency. It is a concept proposed by a collection of large private banks and a fintech firm for a series of digital tokens representing money from multiple countries that can be exchanged on a distributed ledger platform (UBS (2016)). The value of each country's USC on the distributed ledger would be backed by an equivalent value of domestic currency held in a segregated (reserve) account at the central bank.

The **Bank of Amsterdam** (the Amsterdamse Wisselbank) was established in 1609 by the City of Amsterdam to facilitate trade. It is often seen as a precursor to central banks. A problem at the time was that currency, ie coins, was being eroded, clipped or otherwise degraded. The bank took deposits of both foreign and local coinage at their real intrinsic value after charging a small coinage and management fee. These deposits were known as bank money. The Wisselbank introduced a book-entry system that enabled customers to settle payments with other account holders. The Dutch central bank was established in 1814 and the Bank of Amsterdam was closed in 1820 (Smith (1776), Quinn and Roberds (2014)).

The **1934 series gold certificate** was a $100,000 paper note issued by the US Treasury and used only for official transactions between Federal Reserve Banks. This was the highest US dollar-denominated note ever issued and did not circulate among the general public. It is an example of non-electronic, restricted-use, government-backed, peer-to-peer money.

Examples of privately issued local currencies include the **Bristol Pound** and **BerkShares**, located in the right-hand petal. Stores in Bristol, United Kingdom, give a discount to people using Bristol Pounds, whereas BerkShares are purchased at 95 cents on the dollar and are accepted at retail stores in the Berkshires region of Massachusetts at face value.

Precious metal coins are examples of commodity money. They can be used as an input in production or for consumption and also as a medium of exchange. This is in contrast to fiat money, which has no intrinsic use. Although commodity money is largely a thing of the past, it was the predominant medium of exchange for more than two millennia.

E-gold account holders used commercial bank money to purchase a share of the holding company's stock of gold and used mobile phone text messages to transfer quantities of gold to other customers. Payments between e-gold customers were "on-us" transactions that simply involved updating customer accounts. E-gold ultimately failed. But before it shut down in 2009, it had accumulated over 5 million account holders.② Many current private mobile payment platforms, such as **Venmo** (a digital wallet with social media features popular with US college students) and **M-pesa**™ (a popular mobile money platform in Kenya and other East African countries), employ a similar "on-us" model. Users transfer either bank deposits or cash to the operator, who gives them mobile credits. These credits can be transferred between platform participants using their mobile devices or redeemed from the operator for cash or deposits. The daily number of M-pesa transactions dwarfs those conducted using Bitcoin. However, in terms of value, worldwide Bitcoin transfers have recently overtaken those conducted on the M-pesa platform (Graph 1, right-hand panel).

① Straightforward arguments derived from Friedman (1959) and Klein (1974) suggest that if the Federal Reserve were to maintain one-to-one convertibility with Fedcoin, it would also need to control the supply of Fedcoins. ② The company ran into trouble with the authorities over anti-money laundering violations and for operating a money transmitter business without the necessary state licence; see http://legalupdate.e-gold.com/2008/07/plea-agreement-as-to-douglas-l-jackson-20080721.html. E-gold account statistics can be found at http://scbbs.net/craigs/stats.html.

Retail central bank cryptocurrencies

Retail CBCCs do not exist anywhere. However, the concept of a retail CBCC has been widely discussed by bloggers, central bankers and academics. Perhaps the most frequently discussed proposal is Fedcoin (Koning (2014, 2016), Motamedi (2014)).[11] As discussed in Box B, the idea is for the Federal Reserve to create a cryptocurrency that is similar to bitcoin. However, unlike with bitcoin, only the Federal Reserve would be able to create Fedcoins and there would be one-for-one convertibility with cash and reserves. Fedcoins would only be created (destroyed) if an equivalent amount of cash or reserves were destroyed (created) at the same time. Like cash, Fedcoin would be decentralised in transaction and centralised in supply. Sveriges Riksbank, with its eKrona project, appears to have gone furthest in thinking about the potential issuance of a retail CBCC (Box C).

A retail CBCC along the lines of Fedcoin would eliminate the high price volatility that is common to cryptocurrencies (Graph 1, centre panel).[12] Moreover, as Koning (2014) notes, Fedcoin has the potential to relieve the zero lower bound constraint on monetary policy. As with other electronic forms of central bank money, it is technically possible to pay interest on a DLT-based CBCC. If a retail CBCC were to completely replace cash, it would no longer be possible for depositors to avoid negative interest rates and still hold central bank money.

Any decision to implement a retail CBCC would have to balance potential benefits against potential risks. Bank runs might occur more quickly if the public were able to easily convert commercial bank money into risk-free central bank liabilities (Tolle (2016)). There could also be risks to the business models of commercial banks. Banks might be disintermediated, and hence less able to perform essential economic functions, such as monitoring borrowers, if consumers decided to forgo commercial bank deposits in favour of retail CBCCs. These benefits and costs are, however, not unique to retail CBCCs. They are the same for DCAs. What, then, is the key difference between retail CBCCs and DCAs? The answer lies with the peer-to-peer aspect of CBCCs and, more specifically, with anonymity.

Anonymity

Bitcoin was designed to be a "peer-to-peer version of electronic cash" (Nakamoto (2009, p 1), and this allows transactions to be anonymous. All bitcoin transactions are publicly recorded using the payer's and the payee's public addresses.[13] However, very much like e-mail addresses, bitcoin public addresses do not need to reveal the true identity of users.[14] This means that a person sending bitcoin to a public address

[11] The Federal Reserve has not endorsed or officially commented on the proposal.

[12] See Yermack (2015), Bolt and van Oordt (2016) and Garratt and Wallace (2016) for discussions relating to digital currencies and price volatility.

[13] Luther and Olson (2015) argue that bitcoin is a practical application of what is termed "memory" in the monetary economics literature. Kocherlakota (1998) shows that both money and memory are devices capable of facilitating exchange. Memory can, however, implement more allocations than money, so that money can be viewed as a form of memory but not the other way around.

[14] See Nakamoto (2009, Section 10).

Box C

The case of Sweden

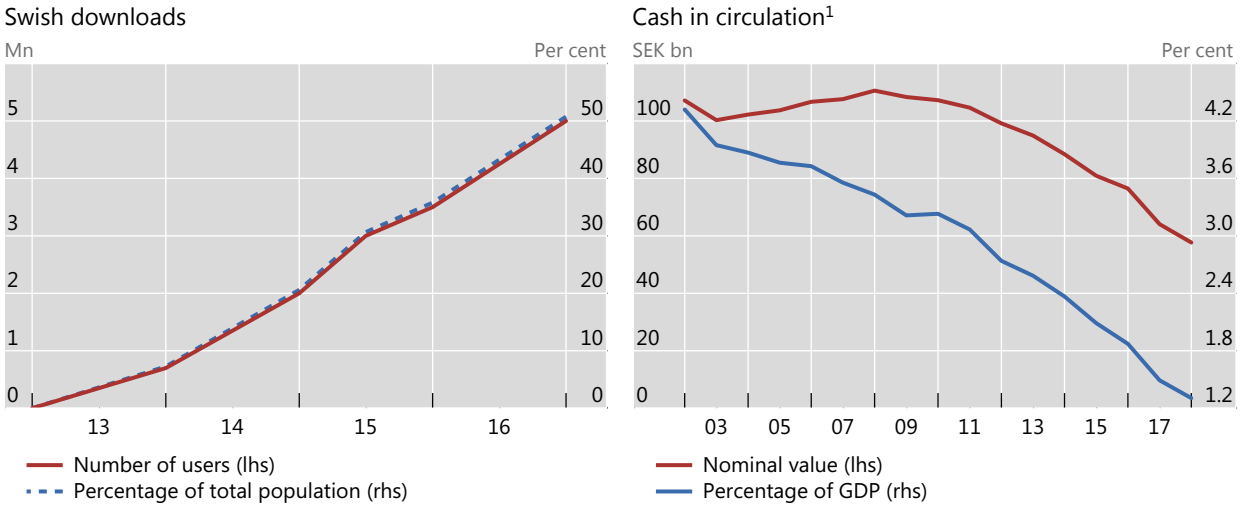
Sweden has one of the highest adoption rates of modern information and communication technologies in the world. It also has a highly efficient retail payment system. At the end of 2016, more than 5 million Swedes (over 50% of the population) had installed the Swish mobile phone app, which allows people to transfer commercial bank money with immediate effect (day or night) using their handheld device (Graph C, left-hand panel; see also Bech et al (2017)).

The demand for cash is dropping rapidly in Sweden (Graph C, right-hand panel). Already, many stores no longer accept cash and some bank branches no longer disburse or collect cash. These developments are a cause for concern for the Riksbank (Skingsley (2016)). Will the payment system continue to be safe and efficient without cash? Even if cash is not used every day, it is a backup option in crisis situations. Will those without access to bank services still be able to manage their payments?

The Riksbank currently has a so-called eKrona project under way to determine whether it should supply digital central bank money to the general public. The project is considering different technical solutions, but no decision has been taken as to whether to focus on a DCA or a retail CBCC structure. The project is expected to be finalised in late 2019 (Sveriges Riksbank (2017)).

Sweden

Graph C



[1] Measured as an annual average.

Sources: IMF, *International Financial Statistics*; United Nations, *World Population Prospects*; www.getswish.se; national data; authors' calculations.

need not reveal his/her true identity to the recipient (*counterparty anonymity*) or to other members of the Bitcoin community (one form of *third-party anonymity*).[15]

Kahn et al (2005) and McAndrews (2017) emphasise legitimate reasons for counterparty anonymity in transactions. Payees and payers may want to reduce the risk of identity theft, the possibility that the counterparty might follow them home and rob them, or more innocuous annoyances like directed advertising and solicitations (spamming). Similarly, a lack of third-party anonymity may be regarded as revealing too much information about a person's private activities. In his proposal

[15] Third-party anonymity means that a person's true identity is not revealed to anyone not directly involved in a transaction. In more general applications, this would include a system operator.

for *Digicash*, David Chaum (1983) makes this argument by pointing out that "knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can reveal a great deal about the individual's whereabouts, associations and lifestyle".[16]

Counterparty anonymity seems less controversial than third-party anonymity. Many observers have argued that third-party anonymity in payments should not be allowed because it facilitates criminal activity, such as tax evasion, terrorist financing or money laundering. Rogoff (2016) argues that $100 bills should be removed from circulation for the same reasons.

It is unclear how much consumers actually value anonymity of either sort in order to protect their privacy. Athey et al (2017) look at how much effort people make to protect their privacy in relation to digital currencies. In an experimental setting, they find that subjects, in general, do not devote the small amount of time needed to read through the e-wallet description that is necessary to meet their own stated preferences for privacy. Similar findings emerged from a survey of economics students at the University of California, Santa Barbara, on usage of Venmo (a digital wallet with social media features). Of the 669 respondents, 80% were users. Of these users, 44% allowed their Venmo transactions to be public (visible to everyone on the internet) and another 21% allowed all of their Facebook friends to see their transactions. Finally, while Digicash is regarded as a precursor to bitcoin, there may not have been sufficiently high demand for the third-party anonymity it provided as it was never widely adopted. It filed for bankruptcy in 1998.[17]

The technology behind CBCCs could allow central banks to provide a digital cash substitute with anonymity properties similar to those of cash. In its role as issuer, the central bank would need to decide whether or not to require customer information (the true identity behind the public address). This would determine the extent to which the retail CBCC would provide third-party anonymity.

While it may look odd for a central bank to issue a cryptocurrency that provides anonymity, this is precisely what it does with physical currency, ie cash. Perhaps a key difference is that, with a retail CBCC, the provision of anonymity becomes a conscious decision. It is worth recalling that the anonymity properties of cash are likely to have emerged out of convenience or historical happenstance rather than intent.

[16] Digicash was launched in the 1990s as a means of transferring bank deposits from one customer to another without revealing the payer's identity to his/her bank (ie it provided third-party anonymity). It did this by using cryptographic techniques to create a pool of untraceable Digicash from customer deposits. Digicash is interesting in that it provided third-party anonymity without requiring autonomy from commercial banks. Commercial banks still held and transferred the deposits held by customers using the Digicash scheme.

[17] One potential reason for its lack of success is that it did not provide autonomy from a central authority. Nick Szabo's proposal for "bit gold" offers an autonomous version of e-gold that uses proof-of-work chains. Bit gold represents a big step in the evolution of digital cash towards bitcoin (https://unenumerated.blogspot.ch/2005/12/bit-gold.html).

Wholesale central bank cryptocurrencies

While CBCCs for retail payments remain at the conceptual stage, some central banks have completed proofs of concept for DLT-based applications.[18] One of the reasons for the interest in DLT is that many central bank-operated wholesale payment systems are at the end of their technological life cycles. The systems are programmed in obsolete languages or use database designs that are no longer fit for purpose and are costly to maintain.

Projects Jasper and Ubin

Project Jasper at the Bank of Canada (Chapman et al (2017)) and Project Ubin at the Monetary Authority of Singapore (MAS (2017)) simulate real-time gross settlement (RTGS) systems on a DLT platform. In an RTGS system, payments are processed individually, immediately and with finality throughout the day (CPSS (1997)).

Unlike the retail payment applications discussed above, wholesale systems have restricted access, ie they are permissioned rather than permission-less. Usually, access is restricted to financial institutions. Moreover, the costly proof-of-work validation (Box A) needed to prevent double-spending in retail schemes is replaced by less energy-consuming alternatives, such as a trusted notary (eg the central bank).

A key challenge in any CBCC application is how to transfer central bank money to the distributed ledger.[19] Both Jasper and Ubin chose a digital depository receipt (DDR) approach. A DDR is a claim on central bank reserves held in a segregated account against which the central bank issues digital tokens on the distributed ledger. In Jasper, the digital tokens – initially known as *CADcoins*[20] – are created at the beginning of the day and redeemed at the end. In Ubin, banks acquire or redeem digital tokens at any point during the day and can keep them on the distributed ledger overnight. Hence, transfers on the DLT platform of the Singaporean proof of concept are not restricted to the opening hours of MAS.

Project Jasper also implements a liquidity-saving mechanism (LSM) on the DLT platform. While RTGS systems minimise settlement risk, they can be demanding in terms of liquidity. Consequently, many RTGS systems around the world are augmented by mechanisms that periodically seek to offset payments against each other in a queue and settle only the net amounts (Bech and Soramäki (2001)). Distributed ledgers are decentralised, so implementation of a centralised queue requires a clever work-around (Project Jasper (2017)).

The two projects show that central bank money can be transferred on a distributed ledger in real time, in realistic volumes and with an LSM. Nevertheless, none of the current initiatives to update or replace existing wholesale payment systems are considering the adoption of DLT. Both the Bank of England (2017) and Bank of Canada (Ho (2017)) conclude that DLT is not yet mature enough for current

[18] Central banks have not limited themselves to wholesale payment applications of DLT. The Hong Kong Monetary Authority (HKMA) has developed proofs of concept for trade finance and mortgage loan applications in collaboration with industry participants (HKMA (2016)). The Bank of France has developed a DLT version of its Single European Payments Area (SEPA) Creditor Identifier database (Bank of France (2016)).

[19] The CPMI-IOSCO Principles for Financial Markets Infrastructures hold that settlement should occur in central bank money whenever practical and available.

[20] See Garratt (2016).

adoption. Yet most central banks that are considering modernising their core payment infrastructure stress the need to make new systems inter-operable with future DLT platforms.

Securities settlement

Looking beyond the immediate horizon, many industry participants see significant potential for DLT to increase efficiency and reduce reconciliation costs in securities clearing and settlement.[21] One potential benefit of DLT-based structures is immediate clearing and settlement of securities, in contrast to the multiple-day lags that currently exist when exchanging cash for securities (and vice versa).[22] Progress in this direction was recently achieved by a joint venture between the Deutsche Bundesbank and Deutsche Börse, which developed a functional prototype of a DLT-based securities settlement platform that achieves delivery-versus-payment settlement of digital coins and securities (Deutsche Bundesbank (2016)).

Conclusion

As it stands, cash is the only means by which the public can hold central bank money. If someone wishes to digitise that holding, he/she has to convert the central bank liability into a commercial bank liability by depositing the cash in a bank. A CBCC would allow consumers to hold central bank liabilities in digital form.[23] But this would also be possible if the public were allowed to have central bank accounts, an idea that has been around for a long time.[24] We argue that the main benefit that a consumer-facing retail CBCC would offer, over the provision of public access to (centralised) central bank accounts, is that the former would have the potential to provide the anonymity of cash. In particular, peer-to-peer transfers allow anonymity vis-à-vis any third party. If third-party anonymity is not of sufficient importance to the public, then many of the alleged benefits of retail CBCCs can be achieved by giving broad access to accounts at the central bank.

Whether or not a central bank should provide a digital alternative to cash is most pressing in countries, such as Sweden, where cash usage is rapidly declining. But all central banks may eventually have to decide whether issuing retail or wholesale CBCCs makes sense in their own context. In making this decision, central banks will have to consider not only consumer preferences for privacy and possible efficiency gains – in terms of payments, clearing and settlement – but also the risks it may entail for the financial system and the wider economy, as well as any implications for monetary policy (Bordo and Levin (2017)). Some of the risks are currently hard to assess. For instance, at present very little can be said about the cyber-resilience of CBCCs, something not touched upon in this short feature.

[21] Mainelle and Milne (2016) estimate that synchronised share databases can reduce back office costs by up to 50%. A study led by Santander InnoVentures (2015) estimates that $15–20 billion could be saved annually in the broader banking industry.

[22] Through the use of smart contracts, the technology also allows for the settlement time/date of a transaction to be specified by the relevant parties.

[23] One simple reason why a consumer might want to do this is to avoid the credit risk associated with commercial bank liabilities.

[24] Who should and should not have access to central bank money is a recurring policy issue. See CPSS (2003), CGFS (2015) and Bank of England (2017) for more detailed discussions.

References

Andolfatto, D (2015): "Fedcoin: on the desirability of a government cryptocurrency", *MacroMania*, blogpost, 3 February.

——— (2016): "Is bitcoin a safe asset?", *MacroMania*, blogpost, 27 March.

Athey, S, C Catalini and C Tucker (2017): "The digital privacy paradox: small money, small costs, small talk", Stanford University Graduate School of Business, *Research Papers*, no 17–24.

Bank of Canada (forthcoming): "White paper on Project Jasper".

Bank of England (2017): "Bank of England extends direct access to RTGS accounts to non-bank payment service providers", press release, 19 July.

Bank of France (2016): "La Banque de France mène une expérimentation de 'blockchain' interbancaire", press release, 15 December.

Bech, M, Y Shimizu and P Wong (2017): "The quest for speed in payments", *BIS Quarterly Review,* March, pp 57–68.

Bech, M and K Soramäki (2001): "Gridlock resolution in payment systems", Danmarks Nationalbank*, Monetary Review*, December.

Benos, E, R Garratt and P Gurrola-Perez (2017): "The economics of distributed ledger technology for securities settlement", Bank of England*, Staff Working Papers*, no 670, August.

Bjerg, O (2017): "Designing new money – the policy trilemma of central bank digital currency", *Copenhagen Business School (CBS) Working Paper*, June.

Bolt, W and M van Oordt (2016): "On the value of virtual currencies", Bank of Canada, *Staff Working Papers*, no 42, August.

Bordo, M and A Levin (2017): "Central bank digital currency and the future of monetary policy", *NBER Working Papers*, no 23711, August.

Broadbent, B (2016): "Central banks and digital currencies", speech at the London School of Economics, 2 March.

Chapman, J, R Garratt, S Hendry, A McCormack and W McMahon (2017): "Project Jasper: are distributed wholesale payment systems feasible yet?", Bank of Canada, *Financial System Review*, June, pp 1–11.

Chaum, D (1983): "Blind signatures for untraceable payments", *Advances in Cryptology*, proceedings of Crypto '82, pp 199–203.

Committee on the Global Financial System (2015): "Central bank operating frameworks and collateral markets", *CGFS Papers*, no 53, March.

Committee on Payment and Settlement Systems (1997): *Real-time gross settlement systems*, March.

——— (2003): *The role of central bank money in payment systems*, August.

Committee on Payments and Market Infrastructures (2015): *Digital currencies*, November.

Deutsche Bundesbank (2016): "Joint Deutsche Bundesbank and Deutsche Börse blockchain prototype", press release, 28 November.

European Central Bank (2012): *Virtual currency schemes*, October.

Friedman, M (1959): "The demand for money: some theoretical and empirical results", *The Journal of Political Economy*, vol 67, no 4, pp 327–51.

Garratt, R (2016): "CAD-coin versus Fedcoin", *R3 Report*, 15 November.

Garratt, R and N Wallace (2016): "Bitcoin 1, bitcoin 2, ... : an experiment in privately issued outside monies", University of California, Santa Barbara, Department of Economics*, Departmental Working Paper*, October.

Ho, S (2017): "Canadian trial finds blockchain not ready for bank settlements", *Reuters Business News*, 25 May.

Hong Kong Monetary Authority (2016): *Whitepaper on distributed ledger technology*, 11 November.

Kahn, C, J McAndrews and W Roberds (2005): "Money is privacy", *International Economic Review*, vol 46, no 2, pp 377–99.

Klein, B (1974): "The competitive supply of money", *Journal of Money, Credit and Banking*, vol 6, no 4, pp 423–53.

Kocherlakota, N (1998): "Money is memory", *Journal of Economic Theory*, vol 81, no 2, pp 232–51.

Koning, J (2014): "Fedcoin", *Moneyness*, blogpost, 19 October.

——— (2016): "Fedcoin: a central bank issued cryptocurrency", *R3 Report*, 15 November.

Luther, W and J Olson (2015): "Bitcoin is memory", *The Journal of Prices & Markets*, vol 3, no 3, pp 22–33.

Mainelle, M and A Milne (2016): "The impact and potential of blockchain on the securities transaction lifecycle", *SWIFT Institute Working Papers*, no 7.

McAndrews, J (2017): "The case for cash", *Asian Development Bank Institute Working Paper Series*, no 679.

Monetary Authority of Singapore (2017): *The future is here – Project Ubin: SGD on distributed ledger*.

Motamedi, S (2014): "Will bitcoins ever become money? A path to decentralised central banking", *Tannu Tuva Initiative*, blogpost.

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

Project Jasper (2017): "A Canadian experiment with distributed ledger technology for domestic interbank payments settlement", white paper prepared by Payments Canada, R3 and the Bank of Canada.

Quinn, S and W Roberds (2014): "How Amsterdam got fiat money", *Journal of Monetary Economics*, vol 66, September, pp 1–12.

Raskin, M and D Yermack (2016): "Digital currencies, decentralized ledgers and the future of central banking", *NBER Working Papers*, no 22238, May.

Rogoff, K (2016): *The curse of cash*, Princeton University Press.

Santander InnoVentures (2015): *The Fintech 2.0 Paper: rebooting financial services*.

Skingsley, C (2016): "Should the Riksbank issue e-krona?", speech at FinTech Stockholm 2016, 16 November.

Smith, A (1776): *An inquiry into the nature and causes of the wealth of nations*, W Strahan and T Cadell, London.

Sveriges Riksbank (2017): *Project plan for the eKrona*, 14 March.

Tobin, J (1985): "Financial innovation and deregulation in perspective", *Bank of Japan Monetary and Economic Studies*, vol 3, no 2, pp 19–29.

——— (1987): "The case for preserving regulatory distinctions", in *Proceedings of the Economic Policy Symposium*, Jackson Hole, Federal Reserve Bank of Kansas City, pp 167–83.

Tolle, M (2016): "Central bank digital currency: the end of monetary policy as we know it?", *Bank Underground*, blogpost, 25 July.

UBS (2016): "Utility settlement coin concept on blockchain gathers pace", press release, 24 August.

Venn, J (1881): *Symbolic logic*, MacMillan and Co, London.

Yermack, D (2015): "Is bitcoin a real currency?", in D Lee (ed), *The Handbook of Digital Currency*, Elsevier, pp 31–44.