Digital money

We provide a brief overview of the most popular forms of money available to the general public today, with a particular emphasis on digital money. We contrast current monetary arrangements with privately issued crypto coins, such as Bitcoin, and argue why the latter will likely never be able to perform the economic functions of money well. We relate our discussion to the current international debate on the potential introduction of central bank-issued digital currencies as a new form of digital money.

Paul Pichler,
Alexander Schierlinger-Brandmayr,
Martin Summer[1]

JEL classification: E5, E58, E50, E59
Keywords: digital money, Bitcoin, blockchain, digitalization

The term *money* is ubiquitous in everyday conversations: we use money to purchase goods and services, we have money in our wallets and save it in the bank, we refer to rich people as those having a lot of money or earning a lot of money. These examples show that the term money often denotes very different things, for instance cash, wealth or income. In economics, however, the term money is not used as a synonym for wealth and income, and it also includes more than just cash. The popular undergraduate textbook *The Economics of Money, Banking and Financial Markets by Frederic Mishkin (2015)* refers to money as *"anything that is generally accepted in payment for goods and services and in the repayment of debts."* More broadly, economists define money by its three economic functions: being a widely accepted *medium of exchange*, a *store of value* and a *unit of account*. Anything that satisfies all of these three functions qualifies as money, irrespective of its particular representation.

The aim of this article is to provide an overview of the different forms of money used for everyday transactions today, with a particular emphasis on *digital money*. We proceed as follows. In section 1 we discuss currency and deposit money, arguably the two most popular faces of money today. In section 2 we discuss privately issued crypto coins, focusing on Bitcoin, and we discuss whether such crypto coins could become the popular face of money in the future. In section 3 we discuss the current international debate on the introduction of central bank-issued digital currencies. Finally, in section 4 we draw conclusions.

1 Currency and deposits: the two popular faces of money today

The most visible face of money, with which even young children are familiar, is currency: coins and banknotes. Today currency is mostly produced by or on behalf of central banks and is issued only by these institutions.[2] Modern money is firmly embedded in a strict set of legal rules that regulate its creation and the way it is distributed.[3] The intrinsic, material value of banknotes and coins is far below its nominal value. As a rule, central banks are not obliged to exchange coins and

Refereed by:
Santiago Fernández de Lis, BBVA Research

[1] *University of Vienna, Department of Economics, paul.pichler@univie.ac.at; University of Vienna, Vienna Graduate School of Economics, alexander.schierlinger-brandmayr@univie.ac.at; and Oesterreichische Nationalbank (OeNB), Economic Studies Division, Martin.Summer@oenb.at (corresponding author). Opinions expressed by the authors of this study do not necessarily reflect the official viewpoint of the OeNB, the University of Vienna or the Eurosystem. The authors would like to thank Martin Hellwig, Carlos Lenz Jonathan Thaler and Beat Weber as well as the referee for helpful comments and valuable suggestions.*

[2] *In the euro area, the central banks of the participating countries have the sole right to produce and distribute coins and banknotes.*

[3] *See Weber (2018).*

banknotes in circulation for other assets, such as gold, silver or foreign currencies. They are merely obliged to exchange banknotes and coins for new banknotes and coins, which in turn they can produce at virtually zero cost. For this reason, modern money is often referred to as *fiat* money.

Why is it then that people accept currency in exchange for goods and services? The answer is surprisingly simple: because they trust that they will be able to use the same currency in the future to purchase goods and services themselves. They trust that currency has economic value. This faith is rooted in the trust in the economic strength of the issuing state. It is crucial for the stability of the economic value of fiat currency. Fiat currency depends on people's trust in sound future policymaking and, with that, the future value of currency as a means of payment. This, in turn, is crucial for the current economic value of fiat currency. After all, nobody would accept intrinsically worthless currency today if they had any doubts about whether this currency could be used to make purchases tomorrow.

The economic value of currency depends not only on trust in government institutions, but also on technology. In order to have any value, banknotes and coins must be difficult, if not impossible, to forge, because their value hinges on their scarcity. If the state cannot ensure a limited supply of banknotes and coins, for example because they can easily be reproduced illegally, the economic value of currency in circulation will quickly erode. To prevent such a scenario, central banks today use modern materials and state-of-the-art security techniques in the production of currency. The euro banknotes, for example, have a variety of security features such as watermarks, holograms and security threads.

The second face of money all of us are familiar with is the *deposit money* we hold in our bank accounts. Even though this form of money has no physical representation, we can use it to make payments by asking our bank to debit our own account while crediting the bank account owned by the recipient of the payment. Transfers of deposit money thus essentially boil down to changes in a system of registers maintained by banks.

Deposit money held in the account of a particular bank is a liability of this bank. This is because deposit money reflects the promise of a commercial bank to deliver physical currency on demand, and unlike the central bank, it cannot produce coins and banknotes itself. Therefore, physical currency plays an important role in the functioning of deposit money in our current monetary system: it ultimately defines the content of most claims vis-à-vis commercial banks.[4] Accordingly, the economic value of deposit money hinges directly on the economic value of currency. However, it also critically depends on people's trust in the banking system. People are willing to hold and use deposit money only if they trust in the ability of banks to fulfill their financial promises, and if they trust in the integrity of bank accounts and payment system technology. To establish and maintain this trust, policymakers have, over time, introduced a complex set of legal rules and a sophisticated system of regulation and supervision. The ultimate aim of this system is to provide a safeguard for the public that banking and payment systems function correctly, which ensures that – like currency – deposit money is safe and cannot be "forged" easily.[5]

[4] *See Hellwig (2018).*

[5] *For a more detailed description of the modern monetary system and its "hybrid" nature of central bank money creation through the issuance of banknotes and the creation of reserves as well as private money creation by banks through deposit money, we refer interested readers to chapter 2 in Weber (2018).*

Unlike coins minted from precious metals and banknotes made from cotton paper or similar materials, deposit money issued by banks has no physical representation. It exists only as entries in the ledgers maintained by the banking system. Deposit money serves as a medium of exchange because holders can always ask their banks to transfer funds to the account of someone else, possibly with another bank. Whereas in the past, such orders relied on paper (transfer orders, checks etc.), today transactions are mostly initiated via payment cards, online banking or banking apps for smartphones. Banks and payment card providers use state-of-the-art secure data transmission technologies and sophisticated cryptographic techniques to ensure the legitimacy of all transactions. Thus, modern deposit money is *digital money*, i.e. money that exists only as bits and bytes in a network of interconnected computers.

The ECB's payment statistics[6] illustrate the increasingly important role of digital payments in the EU. In 2016, the number of cashless payments in the EU increased by 8.5% to a total of 122 billion transactions, corresponding to more than 3,800 transactions per second. Of these 122 billion transactions, 59 billion were made using payment cards, suggesting an increase by more than 12% compared to 2015. The total value exchanged via card payments amounts to roughly EUR 3 trillion in 2016, i.e. approximately EUR 50 per payment. While both the number of payment cards in circulation and the number of card payments has been increasing continuously over the last years, the number of ATMs provided by banks in the EU has been declining slowly but steadily. This reflects the increased usage of digital money rather than physical currency for everyday transactions.

This trend is likely to gather momentum in the future. To make digital payments even more convenient, the Eurosystem has developed its TARGET Instant Payment Settlement (TIPS) service. Starting in November 2018, TIPS will offer payment service providers final and irrevocable settlement in central bank money in real time and around the clock, 365 days a year. This will provide the basis for new and better payment services offered to end users, such as instant person-to-person mobile payments. Still, the efficiency of international transactions sent to jurisdictions not covered by TIPS is still relatively slow, and cross-border transactions to these areas are expensive. That said, these transactions amount to only 1% of total transactions. The significant increase in the convenience and speed of euro payments will likely contribute to a further rise in digital payments in the EU.

While modern deposit money is mostly digital, there is still no digital form of official (central bank-issued) currency. When we want to transfer money online, for example to pay for online shopping, we have no choice but to use the services offered by private financial intermediaries, such as commercial banks and payment card providers. Moreover, digital payments cannot be made truly anonymously, as the identities of senders and receivers of deposit money need to be known to the banks which act as financial intermediaries. This lack of anonymity, together with a loss of trust in the banking system in the midst of the global financial crisis, has spurred a private initiative to establish a decentralized electronic cash system: Bitcoin.

[6] *The Payment Statistics for 2016 are available at http://sdw.ecb.europa.eu/reports.do?node=1000004051*

2 Bitcoin and beyond: are privately issued crypto coins the new face of money?

Bitcoin was introduced in late 2008, first to a small community of cryptographers and IT specialists, by the publication of a white paper explaining its key working principles (Nakamoto, 2008). The scientific paper was accompanied by the open source client software *Bitcoin core*, which allows users to exchange Bitcoin tokens and engage in activities to create new tokens. Up until the time of this writing (July 2018), more than 17 million Bitcoins had been created and the market capitalization of Bitcoin amounted to approximately EUR 100 billion.

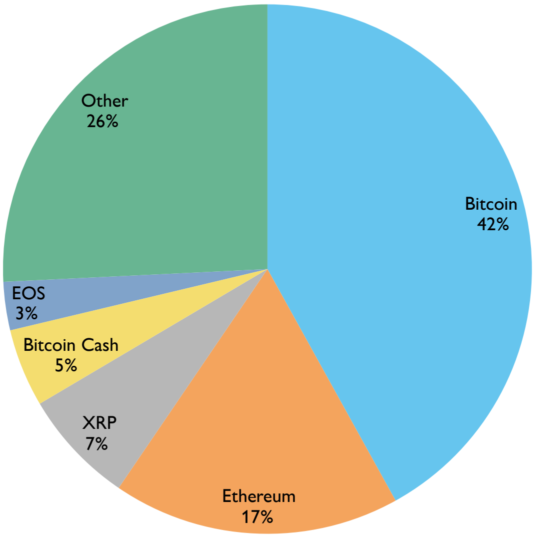
Moreover, in recent years, hundreds of other crypto coins (also referred to as *altcoins*) have been developed, some of which have turned out successful in raising investor funds and achieving high market prices. Today, the total market capitalization of all crypto coins together amounts to roughly EUR 240 billion. Three-quarters of this amount are accounted for by the five largest players on the crypto coin market (Bitcoin, Ethereum, XRP, Bitcoin Cash and EOS), as is visualized in chart 1.

2.1 The technology behind Bitcoin

Bitcoin set out to establish an electronic cash system that allows for truly anonymous and completely nonreversible payments over the Internet. Similar to bank deposits, Bitcoin tokens have no physical representation but are merely entries in a digital ledger. Unlike deposits, however, this ledger is not maintained by a central institution such as a bank but rather maintained jointly by all participants in the Bitcoin system. Each single participant can keep a local copy of the ledger and can propose changes to the ledger. This technology of using a *distributed ledger* raises a fundamental problem: if everyone can make changes to the ledger, how to reach a consensus about the true state of the ledger at a given point in time? How to ensure that the same money is not spent twice? After all, given the absence of a central authority that sees and verifies all transaction requests, fraudulent behavior by an individual who may ask different participants in the network to send the same Bitcoin token to different recipients may not be detected in time.

Chart 1

Market shares of crypto coins



Source: https://coinmarketcap.com, data retrieved on July 5, 2018.

The key innovation of Bitcoin is that it establishes a set of rules and economic incentives that solve the double-spending problem and allow for reaching consensus about a distributed ledger, even though the true identities of all participants in the Bitcoin system are well hidden behind pseudonyms. This is achieved by resorting to cryptographic techniques and game theoretical concepts.

2.1.1 The Bitcoin network

Bitcoin is organized as a decentralized peer-to-peer network of users (nodes). To enable anonymity, the Bitcoin ledger does not contain any information about the true identity of a user but only lists transactions (flows of Bitcoins) between alpha-numeric addresses, which are similar to bank account numbers. By means of the Bitcoin core software any user can create Bitcoin addresses anonymously and in unlimited quantity. Contrary to the opening of a bank account, opening a "Bitcoin account" does not involve a third party. Hence, no one except the initial creators themselves are eventually able to link a Bitcoin address to their true identity.

All nodes in the network are equal and can communicate with each other. The Bitcoin protocol only restricts the format of messages that can be exchanged over the Bitcoin network. Any owner of Bitcoins who wishes to transfer funds from their address to another address can do so by sending a message requesting the transaction to its neighboring nodes in the Bitcoin network, which in turn pass on this message to their own neighbors, etc. Over time, the message will spread over the entire network provided that the network is not partitioned. As transaction requests are broadcasted through an unsecure peer-to-peer network, where they can in principle be manipulated by nodes passing on the message, it becomes essential that all nodes can easily verify the legitimacy of a message they receive. The Bitcoin system allows for easy verification of transaction legitimacy by using asymmetric cryptography (which is also used with traditional card payments and in e-commerce) to digitally sign messages and validate signatures.

2.1.2 Verifying legitimate transactions: the role of cryptography

Every Bitcoin address is associated with a private key and a public key, both consisting of a relatively long series of characters. The private key is known only to the creator of a Bitcoin address, whereas all nodes have access to the public keys associated with all Bitcoin addresses. The public and the private key of a particular address are linked through a signature algorithm, a mathematical procedure for digitally signing messages and validating signatures. Any message sent on behalf of a given address, such as a transaction request, is considered legitimate by other Bitcoin nodes if and only if it is digitally signed with the private key associated with the address. The digital signature can be verified fast and easily by any user with access to the public key. The mathematical procedure employed in this process relies on trapdoor functions. These are functions that are easy to evaluate, yet extremely difficult to invert. The use of these functions is important because it makes it possible to decrypt a given signature using the public key of an address, but it is still impossible to generate a signature with the public key alone. Messages that are correctly digitally signed have thus almost surely been initiated by someone with access to the private key of the sending address, and hence they have almost surely been initiated by the legitimate owner of funds.

2.1.3 Avoiding double spending

Because many nodes in the Bitcoin network receive the same transaction requests, it is difficult to select a node that is allowed to incorporate the (verified) transaction into the ledger. Selecting one node to do this is important to ensure that the same transaction is not incorporated twice or more often by different nodes. Moreover, if transactions were incorporated on a one-by-one basis, the ledger would have to be updated several times per second, and it would be almost impossible for all network nodes to have the same version of the ledger at a given point in time. The Bitcoin protocol addresses this problem by not handling transactions individually but bundling them in blocks, and by ensuring that subsequent blocks cannot be added to the register too quickly. This provides ample time for sharing a new block across the network before the next block arrives.

2.1.4 The blockchain

Blocks usually contain up to a few thousand transactions and are added to the ledger one after the other. When a new block is created it needs to contain a reference to the state of the ledger to which the new block is linked. The Bitcoin ledger thus essentially forms a chain of blocks of transactions and is hence referred to as the *blockchain*. The reference to the previous block is computed from the precise contents of the newly created block and a random nonce using hash functions. Hash functions are irreversible trapdoor functions that take a piece of information of any length and transform it into a unique set of numbers and letters of a fixed length, a so-called hash value.[7] Each modification of the block contents or the nonce change the hash value in an unpredictable way, and it is impossible to design the input to the hash function, e.g. the random nonce, in such a way that the hash value has certain desired characteristics. As will become clear soon, this is an important property employed by the Bitcoin protocol to reach a consensus about the true state of the ledger.

2.1.5 Bitcoin mining

The creation of blocks requires computing power. Each participant in the network can individually decide whether and how much computing capacity they are willing to provide for the creation of blocks. Nodes which provide this capacity and produce blocks are referred to as *miners*. Bundling transactions in new blocks is technically trivial and can be done extremely fast, even with standard desktop computers. This creates a problem for reaching a consensus about the true state of the ledger. If it were possible for every miner to just add a block of transactions whenever they wish, there would be no time to exchange the new version of the ledger across nodes fast enough to ensure, e.g., that the same transactions are not incorporated multiple times. Different versions of the ledger would then coexist, and it would be impossible to judge which version of the ledger is the correct one. To allow for consensus, the process of adding blocks to the blockchain must thus be slowed down artificially. The Bitcoin protocol achieves this by accepting only blocks to the blockchain whose identifier fulfills certain hard-to-satisfy characteristics. It requires that the hash value must begin with a certain number of leading zero bits. The required characteristics (i.e. the required number of leading zero bits) are updated regularly so as to ensure that the entire mining community manages to compute a block with an identifier that satisfies those characteristics only every ten minutes on average, which usually leaves ample time to globally exchange the updated ledger after the inclusion of a new block and before the next block arrives. However, there is still the possibility that two blocks are added

[7] *Lancaster (2016) provides a good illustration. The hash function used by Bitcoin would for instance take the entire text of James Joyce's Ulysses and transform it into the hash value 6ff1c1a80b68b5414423a7e2e061d5f2fc09f7c4e86c4987e573bebc4e4991dd. When you want to check whether the text was transformed correctly you just have to run the function and check the output. It would, however, be impossible given current computer technology to take this hash value and reconstruct the text of Ulysses from it, i.e. the hash function is irreversible.*

(almost) simultaneously to the same referenced block, which would result in two competing versions of the ledger. To resolve potential disputes in such a situation, the Bitcoin protocol stipulates that the valid version of the ledger is the longest chain of blocks only. Accordingly, when the next block is added to either of the two competing blocks mentioned above, the other one becomes invalid and the transactions bundled in the invalid block are reversed.

2.1.6 Incentivizing honest behavior: the role of game theory

Due to the use of cryptography as described above, any node in the Bitcoin network is *able* to verify the legitimacy of the transactions it receives and *able* to propose changes to the ledger by computing new blocks. But this still leaves open the question of why they should be *willing* to engage in block creation activities and to make sure that only legitimate transactions are included in the ledger. The Bitcoin protocol solves this problem by providing nodes with the proper economic incentives, building on key insights from game theory.

Whenever a node has successfully created a block satisfying the required characteristics, it is granted a certain amount of newly created Bitcoin tokens. The income generated from this so-called coinbase transaction, and any fees a miner might collect from the transactions in their new block, compensates the miners for the work (computing power) they had to invest upfront in order to create the new block. If, however, their block at some point in the future is no longer part of the longest chain, the miners again automatically lose their compensation (and all transactions in the block become reversed). This can happen, for example, because other miners agree that the block contains illegitimate transactions such that these miners choose to extend the blockchain from a different block onward. This easy way of punishment through the (honest) community provides incentives for every individual miner to behave honestly. Specifically, if more than half of the computing power employed in mining is controlled by honest nodes, then the longest chain will eventually be the one containing only legitimate transactions. Behaving honestly therefore is the optimal strategy for any miner who believes that most other miners behave honestly themselves. This establishes a Nash equilibrium where all miners behave honestly. Only if dishonest nodes who cooperate to attack the system control the majority of mining power, illegitimate transactions are sustainable. This incentive structure, referred to as Bitcoin's "proof-of-work" concept, is the key innovation that allows for a fully decentralized verification of transactions in the Bitcoin network.

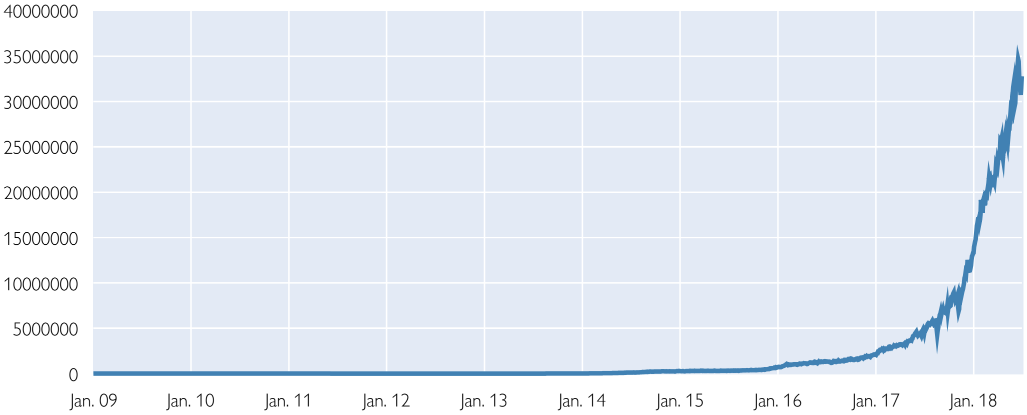
2.1.7 The downside of anonymity and decentralization

While decentralization and anonymity may be appealing at first, unfortunately they come at a high price for society, which is not fully reflected in the price of Bitcoin. To allow for a decentralized consensus, the Bitcoin protocol must ensure that subsequent blocks are not created too quickly, and it does so by dynamically adjusting the difficulty of computing a block. Accordingly, the more aggregate computing power is devoted to mining, the harder it must be to create blocks, and hence the more energy must be devoted to the involved computations in order to keep the expected time between blocks constant at ten minutes. This property, which is key to the functioning of the decentralized consensus mechanism, has led to a massive rise in the energy consumption of the Bitcoin network over the last

Chart 2

Hash rate

Estimated number of tera hashes per second (trillions of hashes per second) that the Bitcoin network performs



Source: www.blockchain.com.

years.[8] By the end of 2018, Bitcoin mining is expected to use 0.5% of the world's energy, which is comparable with the energy consumption of a country like Austria. This massive level of energy consumption exceeds the energy needs of the traditional payment system by several orders of magnitude, and it contributes significantly to environmental pollution and climate change (De Vries, 2018).

2.2 Are privately issued crypto coins the new face of money?

Do privately issued crypto coins such as Bitcoin or Ethereum constitute the new and modern face of money today? To discuss this question in an economic context we need to go back and look at the three fundamental economic functions of money: It is a widely accepted *medium of exchange*, a *store of value* and a *unit of account*. Do private crypto coins fulfill these three functions well?

Looking at the current situation, the quite obvious answer to this question is *no*. First, while crypto coins do technically allow users to exchange value over the Internet, at present they are certainly far from being widely accepted as a means of payment by the general public. It is still almost impossible to use Bitcoins, let alone other crypto coins, for daily purchases of goods and services, except at some small online shops and retailers (who arguably accept these currencies mostly for marketing reasons.) Second, due to their extremely volatile prices, crypto coins do not function well at all as a store of value.[9] In fact, their inherent volatility makes crypto coins attractive means of financial speculation rather than a means of payment. Indeed, empirical evidence suggests that most owners of crypto coins today are hoarding coins in the hope of future price increases rather than using them to make purchases. Finally, hardly anywhere are prices of goods and services denominated and shown in units of crypto coins, i.e. these currencies are not being used as a unit of account. To conclude, privately issued crypto coins clearly do not

[8] *Chart 2 visualizes the energy consumption of the Bitcoin network by showing the number of tera hashes that the network computes per second. Data source: www.blockchain.com.*

[9] *Stablecoins such as Tether (USDT) are a notable exception in this regard. Price stability is achieved, for example, by pegging the crypto coins against the U.S. dollar or other fiat currencies.*

perform the three economic functions of money today, and hence do not qualify as *money* in the economic sense of the term.

There are also good reasons to believe that private crypto coins will never be able to perform all three functions of money well. One reason is their limited scalability. Fully decentralized crypto coins such as Bitcoin are necessarily slow in processing transactions and have limited capacity. This is because – to reach consensus – the current version of the ledger must ideally be exchanged among all users globally before any new transactions are processed. Hence, fully decentralized crypto coins like Bitcoin will never be able to perform instant online payments, which after the full implementation of TIPS will soon be possible in Europe. This limits crypto coins' attractiveness as a means of payment also in the future. From a payment system perspective, crypto coins are thus highly inefficient compared to the systems in place at the moment: they are slow, limited in scale and – given the high energy costs associated with the consensus protocol – very expensive.

2.3 Blockchain applications and the role of cryptocurrencies

Then what is the potential future economic role of private crypto coins? The answer to this question is strongly linked to the future economic potential of fully decentralized (i.e. public) blockchain applications.[10] Various proposals for such applications have recently gained wide attention, including decentral authorization and verification, crypto assets, smart property and smart contracts (see, e.g., Berentsen and Schaer, 2017). Claims have frequently been made that public blockchain technology will fundamentally revolutionize the business world, eliminating the need for trust and making intermediaries such as lawyers or bankers completely redundant.

Even though crypto coins are inefficient for regular payments, they do fulfill a key function in the context of blockchain applications that fiat currencies cannot fulfill. In particular, the consensus mechanism employed in fully decentralized blockchains must necessarily compensate miners through payments in crypto coins rather than fiat currencies. Only in this case can the honest mining community easily punish dishonest miners in case of misbehavior, by simply extending the blockchain from a different block onward, thereby reversing all transactions in the dishonest block including the coin base transaction. If instead miners were compensated in U.S. dollars or euro, block rewards could not be easily reversed. Then, the incentive mechanism keeping up truthfulness in the consensus protocol would not work anymore.[11]

If public blockchain applications indeed revolutionized the business world, then crypto coins that support such applications (e.g. Ethereum) would likely play an important role in the future. However, there are good reasons to doubt that

[10] *It might be useful at this stage to point out that the public discussion – in particular in the media and in business circles – has led to an ambiguous use of the term blockchain. While the major innovation introduced by the Bitcoin blockchain is the feature that the distributed ledger of transactions is maintained in an anonymous and decentralized manner, it has become common in the past few years to use the term blockchain also for distributed ledgers maintained by known and trusted parties. This, however, is a standard case of a distributed database with up-to-date version control, modern cryptography and multiple access by different parties for easy search and update, a technology that has been in place for many years now and is a part of well established, standard modern database technology (see Wattenhofer, 2016). The key innovation of Bitcoin is the feature of anonymous and decentralized trust that emerges from the consensus protocol based on the proof of work (Budish, 2018).*

[11] *This is a severe problem for public blockchains, which are fully decentralized and anonymous, but a lesser problem for private or Consortium blockchains where only selected (known) nodes are allowed to update the ledger.*

this will be the case, because applying a public blockchain outside the domain of crypto coins may well be strongly limited. In a recent article, Budish (2018) analyzes the economic limits of public blockchains. He points out that the deliberate exclusion of trusted central parties is very expensive on top of the high energy costs usually discussed in the context of Bitcoin. This is because the blockchain protocol needs to provide miners with large enough economic incentives to avoid a so-called *majority attack*, where more than half of the computing power is used by cooperating dishonest nodes that seek to manipulate the ledger in their favor. Specifically, the equilibrium block reward paid to miners must be large relative to the one-off benefit of attacking the blockchain (see Budish, 2018, p. 5); the higher the one-off benefit of a possible attack, the higher must be the regular block reward for miners, and thus the higher are the costs of maintaining a public blockchain.

In the case of Bitcoin and other applications where only crypto coins are traded via the blockchain, the one-off benefit of a majority attack is relatively small. After all, the value of the crypto coins would likely collapse to zero after a successful majority attack, so any stolen coins would essentially be worthless. If, however, property rights for assets with a clear fundamental value, e.g. real estate, diamonds or gold, are traded over a public blockchain (in a legally binding way), the benefits of a majority attack will be potentially very large. Even if the crypto coins used on the blockchain become worthless after an attack, the attackers will still be in the possession of valuable real assets. This shows that, for applications beyond crypto coins, the block rewards paid to miners must likely be large relative to the value of the assets traded on the blockchain, which makes solutions based on public blockchains very expensive in most real-world applications. Distributed databases with trusted third parties seem to be cheaper and more attractive for most businesses and also the public sector.

Let us finally note that when access to the blockchain is limited, for instance when anonymous miners are replaced by an authorized consortium of known participants, the size of block rewards necessary to reach consensus in a blockchain could be significantly reduced. However, in this case there is also no longer a compelling reason to compensate miners through crypto coins rather than fiat currencies.

3 Central bank digital currencies

The public hype about crypto coins and the blockchain technology has also spurred a growing international debate about central banks issuing digital currency (CBDC). The key question in this debate is whether the state should provide to its citizens an official digital means of payment similar to banknotes and coins so that online payments do not necessarily have to go through private financial intermediaries. There is a growing literature and also a policy debate on central bank digital currencies. An in-depth discussion of this issue would require a paper on its own and we cannot cover the literature here.

Instead we would like to highlight some of the key issues in the context of our discussion by referring to recent Bank of Canada staff discussion paper by Engert and Fung (2017). This paper provides an in-depth overview of possible motivations for a central bank to issue digital currency and explores the possible implications of such a step, assuming that the central bank issues digital currency in addition to, rather than instead of, coins and banknotes (and central bank reserves).

According to the authors, there are six possible reasons why a central bank might want to make CBDC available to the general public: (1) to ensure adequate central bank money for the public and preserve central bank seigniorage revenue; (2) to reduce the lower bound on interest rates and support unconventional monetary policy; (3) to reduce aggregate risk and improve financial stability; (4) to increase contestability in payments; (5) to promote financial inclusion; and (6) to discourage criminal activity. The authors also clearly point out that a central bank digital currency might also work using current payment system technology and the blockchain technology is not a necessary ingredient of a CBDC.

With regard to advanced economies and in particular Canada, Engert and Fung (2017) consider only one of these six possible reasons for a CBDC to be plausible and well founded: increasing contestability in payments. Providing a digital alternative to banknotes, checks, debit cards and credit cards, they argue, may increase competition and improve the efficiency of existing payment systems.[12] The remaining five possible reasons are not viewed as compelling. The supply of adequate central bank money to the public and central bank seigniorage revenue are both not at risk in most advanced economies, since the value of outstanding banknotes is not declining.[13] Supporting unconventional monetary policy and promoting financial inclusion can be achieved by means other than CBDC in a potentially better way. Finally, according to the authors, the effects of CBDC on financial stability and criminal activity are ambiguous a priori, and likely depend on the specific attributes of CBDC.

The international debate is mostly focused on two different possible implementations of CBDC, reflecting the two popular faces of money we have discussed in the beginning of this article. The first implementation closely mimics physical currency. Proponents of this implementation envision CBDC to become legal tender and to be denominated in the local currency, convertible at par to banknotes and deposits with unrestricted access around the clock for all citizens, anonymous and non-interest-bearing. The second implementation more closely mimics bank deposits. Notably, the central bank is then assumed to pay interest on its digital currency, or even earn interest when it sets negative interest rates.

Regarding the desirability of introducing currency-like CBDC, Engert and Fung (2017) conclude that there will likely be no significant implications for central bank seigniorage revenue, monetary policy or the banking system. There may be some efficiency gains in retail payments, but on the other hand currency-like CBDC would also facilitate criminal activity due to its anonymity features, which in turn would bring about social costs. Regarding the desirability of introducing deposit-like CBDC, Engert and Fung (2017) arrive at a very similar conclusion. Neither will monetary policy be notably affected by interest-bearing CBDC, as the interest paid on reserves and CBDC will likely be similar due to arbitrage opportunities. However, they caution that interest-bearing CBDC might lead to a modest contraction of intermediation and increased financial volatility; the possibility that households and firms can more easily shift from bank deposits to CBDC in times of stress may present a challenge to financial stability.

[12] *However, the resulting benefits may still be small so that efficiency enhancements may not be a sufficient motivation to issue CBDC (Fung and Hallaburda, 2016).*

[13] *Sweden is a remarkable exception in this regard. Globally, the demand for cash is still high. For empirical evidence, see Jobst and Stix (2017).*

Overall, the analysis by Engert and Fung (2017) suggests that the case for introducing CBDC in most advanced economies is not very strong. This assessment is currently shared by most central banks including the Bank for International Settlements (BIS),[14] the Federal Reserve System,[15] and the Bank of Australia,[16] among others. A notable exception, however, is Sveriges Riksbank. Unlike in most advanced economies, currency in circulation in Sweden has steadily declined over the past decade.[17] As Sweden is moving toward a cashless society, the Riksbank has launched a project aimed at examining whether the krona should not only be issued in physical form but also in an electronic form, referred to as the *e-krona*. The e-krona would not replace cash but rather act as a complement to cash, with the main benefit being that *"by functioning independently from the infrastructure used by the commercial bank system, the e-krona system could also make the payment system more robust in the event of disruptions to, for instance, the system for card payments"* (Riksbank, 2017). While it is not yet clear on what technology the digital currency would be based, for example whether it would be based on blockchain technology, the main working principles of a potential e-krona have already been agreed upon. For example, the e-krona would primarily be intended for smaller payments between consumers, companies and authorities, and it would constitute a direct claim on the Riksbank that does not accrue any interest. The Riksbank's investigation into the topic is expected to be finalized by the end of 2019, with one potential outcome still being that the Riksbank could decide not to issue an e-krona after all.

In its March 2018 report from the Committee on Payments and Market Infrastructures and the Markets Committee, the BIS argues that the issuance of CBDC could challenge the two-tier banking system, as it gives the central bank a greater role in credit allocation. This might well impede the use of decentralized knowledge in society and cause economic losses. Moreover, the BIS points out that for currencies widely used in cross-border transactions, the issuance of CBDC would come with international externalities, including first-mover advantages and economies of scale. In some economies, the cross-border availability of a foreign CBDC could lead economic agents to substitute away from the domestic currency, which could pose severe challenges to domestic monetary policy. A CBDC available globally could lead to large international capital movements and thereby affect exchange rates and asset prices in undesired ways. Finally, for token-based CBDC it might become hard if not impossible to impose anti-money laundering regulations or measures to combat the financing of terrorism. All these complications would likely arise if residents and nonresidents would be allowed to hold and transact in CBDC already in normal times, but even more so in times of economic stress and generalized flight to safety.

[14] *See the March 2018 report from the Committee on Payments and Market Infrastructures (CPMI) and the Markets Committee, available at https://www.bis.org/cpmi/publ/d174.htm.*

[15] *See Brainard (2018).*

[16] *See Lowe (2018).*

[17] *In 2017, the average value of banknotes and coins in circulation in Sweden amounted to only SEK 57 billion, while in 2013 the average value was SEK 88 billion. This reflects a decrease of 35% over a five-year period.*

4 Conclusion

Interest in the digitalization of money has received new and strong impulse from the public discussion of Internet-based electronic value transfer systems such as Bitcoin. This focus sometimes makes us forget that a huge part of the money we use in everyday transactions today is already digital money. Still, there does not yet exist a form of digital central bank-issued currency. We discuss the potential of systems like Bitcoin to be useful as such a new form of digital money. Based on a step-by-step analysis of the technology and economics behind Bitcoin, we argue that it is very unlikely that crypto coins like Bitcoin and related systems will be the future face of money because they lack key features of money: They do not simultaneously serve as a medium of exchange, a store of value and a unit of account. Issues of scalability also limit their widespread adoption. This makes crypto coins not very attractive as means of payment. We argue that the future economic role of private crypto coins will be strongly linked to the future economic potential of fully decentralized blockchain applications because this is the context within which crypto coins find their most natural role. We argue that public blockchains are very expensive to maintain not only because of their high energy consumption but also for incentive reasons. This limits public blockchain applications beyond a pure crypto coin context. We finally discuss the potential role for central bank-issued digital currencies. The current discussion suggests that the case for introducing such a currency seems to be not very strong.

References

Berentsen, A. and F. Schär. 2017. Bitcoin, Blockchain und Kryptoassets. Universität Basel.

Brainard, L. 2018. Cryptocurrencies, Digital Currencies and Distributed Ledger Technologies: What Are We Learning? Speech at the Decoding Digital Currency Conference. https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm

Budish, E. 2018. The economic limits of the blockchain. http://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Blockchain.pdf

De Vries, A. 2018. Bitcoin's Growing Energy Problem. Joule 2, 801-809. May 16.

Engert, W. and B. Fung. 2017. Central Bank Digital Currency: Motivations and Implications. Staff Discussion Paper 2017-16. Bank of Canada.

Fung, Ben S. C. and H. Halaburda. 2016. Central Bank Digital Currencies: A Framework for Assessing Why and How. Available at SSRN: https://ssrn.com/abstract=2994052 or http://dx.doi.org/10.2139/ssrn.2994052

Hellwig, M. 2018. Bargeld, Giralgeld, Vollgeld: zur Diskussion um das Geldwesen nach der Finanzkrise. In: Zeitschrift für das gesamte Kreditwesen. Vol. 8. 37–41.

Jobst, C. and H. Stix. 2017. Doomed to disappear? The surprising return of cash across time and across countries. CEPR Discussion Paper 12327.

Lancaster, J. 2016. When bitcoin grows up. In: The London Review of Books 38(8). 21. 3–12.

Lowe, P. 2017. An eAUD? Address to the 2017 Australian Payment Summit. December. https://www.rba.gov.au/speeches/2017/sp-gov-2017-12-13.html

Mishkin, F. 2015. The Economics of Money, Banking and Financial Markets. Addison Wesley, 11th edition.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

Riksbank. 2017. The Riksbank's e-krona project. https://www.riksbank.se/en-gb/financial-stability/payments/e-krona/the-e-krona-projects-first-interim-report/

Wattenhofer, R. 2016. The Science of the Blockchain. Inverted forest publishing.

Weber, B. 2018. Democratizing Money? Debating Legitimacy in Monetary Reform Proposals. Cambridge University Press.