

Cryptocurrencies and monetary policy

Grégory Claeys, Maria Demertzis
and Konstantinos Efstathiou

Executive summary

GRÉGORY CLAEYS (gregory.claeys@bruegel.org) is a Research Fellow at Bruegel.

MARIA DEMERTZIS (maria.demertzis@bruegel.org) is Deputy Director of Bruegel.

KONSTANTINOS EFSTATHIOU (konstantinos.efstathiou@bruegel.org) is an Affiliate Fellow at Bruegel.

This policy contribution was prepared for the Committee on Economic and Monetary Affairs of the European Parliament (ECON) as an input for the Monetary Dialogue of 9 July 2018 between ECON and the President of the ECB. The original paper is available on the European Parliament's webpage ([here](#)). Copyright remains with the European Parliament at all times.

THIS POLICY CONTRIBUTION tries to answer two main questions: can cryptocurrencies acquire the role of money? And what are the implications for central banks and monetary policy?

MONEY IS A social institution that serves as a unit of account, a medium of exchange and a store of value. With the emergence of decentralised ledger technology (DLT), cryptocurrencies represent a new form of money: privately issued, digital and enabling peer-to-peer transactions.

HISTORICALLY, CURRENCIES FULFIL their main functions successfully when their value is stable and their user network sufficiently large. So far, cryptocurrencies are arguably falling short against these criteria. They resemble speculative assets rather than money. Primarily this is because of their inherent volatility, which is the by-product of their inelastic supply, and which limits their widespread use as a medium of exchange.

CRYPTOCURRENCY PROTOCOLS COULD theoretically evolve to limit their volatility and correct their current deficiencies. If successful, this could lead to an increase in their popularity as an alternative to official currencies. A successful alternative to official currencies could put pressure on those who manage official currencies to provide better policies.

BUT THE WIDESPREAD substitution of central bank currency for cryptocurrencies would effectively create parallel currencies. This by itself could create risks to the effectiveness of monetary policy, to financial stability and ultimately to growth.

NEVERTHELESS, THE RISKS of cryptocurrencies becoming serious contenders remain small as long as fiat currencies issued by the world's major central banks continue to deliver effectively the three traditional functions of money. It would take a deep crisis of trust in official currencies for their widespread substitution by cryptocurrencies to materialise.

FOR CRYPTOCURRENCIES TO replace official currencies they would have to overcome a triple challenge. First, the supply of cryptocurrency would need to act as an instrument (or identify a different instrument) that affects the economy. Second, in the presence of fractional reserve banking, the supply would need to respond to liquidity crises and act as a lender of last resort in order to safeguard financial stability. Third, there would need to be a system of checks and balances to keep the agent, ie the cryptocurrency issuer, accountable to the principal, ie society, which is not possible because cryptocurrencies are automatically and privately-issued. For these reasons, official currencies controlled by inflation-targeting independent central banks still appear to be a far superior technology than cryptocurrencies to provide the money functions.

1 Introduction

The emergence of cryptocurrencies enabled by the development of intelligent digital technologies could be a challenge to the monopoly of official central bank-controlled currencies. Cryptocurrencies are increasingly thought of as actual currencies that can be used as mediums of exchange.

In this Policy Contribution we address two main issues. First, what are the main characteristics of money and to what extent do cryptocurrencies have these characteristics, and can cryptocurrencies play the same role and replace central bank-controlled money? Second, we discuss how the emergence of cryptocurrencies could change the nature of monetary policy, and whether the management of a currency – the essence of monetary policy – can be done by algorithms and still fit within the system of checks and balances required for any policy, including monetary policy, in democratic societies.

Understanding the capacity of cryptocurrencies to replace current currencies requires an examination of how well cryptocurrencies fulfil the main attributes of money: namely a measure of value, a store of value and a medium of exchange. We show that the attractiveness of a currency rests on two characteristics: first, its stability – knowing that the value it represents in terms of what it can buy (be it a particular commodity like gold or a basket of goods and services included in the consumer price index) is broadly constant – and second, how widely accepted it is, known as the extensiveness of the network. Our analysis shows that the volume of transactions carried out using cryptocurrencies is still insignificant compared to those carried out using official currencies. This implies that, at least for the moment, cryptocurrencies are not real contenders to replace official currencies.

However, cryptocurrencies do have interesting characteristics that make them attractive in ways other currencies are not. They are truly global in nature and easily accessible to potential users. The US dollar and possibly the euro are global currencies, but might not always be as readily available (for instance, if a government wants to restrict their use in its jurisdiction). Also, the fact that they are not backed by a government protects them from political influence and the threat of manipulation.

Our second issue is how cryptocurrencies might alter the nature of monetary policy and its application. The management of traditional money by monetary policy authorities (ie central banks) is partly automatic (or at least rules-based) and partly discretionary. A cryptocurrency's protocol is operated by a predefined algorithm, making its management fully automatic. It is currently difficult to imagine how algorithms could be fully effective in dealing with complex decisions in an uncertain world. More importantly however, the lack of a real person behind the automatic decision-making implies that such algorithms could not be held to account. This is an important shortcoming because the value of a currency is a crucial component of a society's ability to prosper and therefore decision making in relation to that currency is a power that should be carefully monitored. Monetary policymakers who are granted that power are part of the package of national policies that are subject to monitoring and review. Monetary policymakers can ultimately be dismissed if deemed necessary.

2 Cryptocurrencies: a role as money?

Money is a social convention that, in particular, facilitates trade when there is a lack of a double coincidence of wants, by solving the problem of a lack of trust in exchanges.

In practice, money tends to be defined by the three functions it traditionally performs: first, a unit of account, as it serves as a common measure of value for goods and services traded in an economy; second, a medium of exchange, as an item accepted for the payment

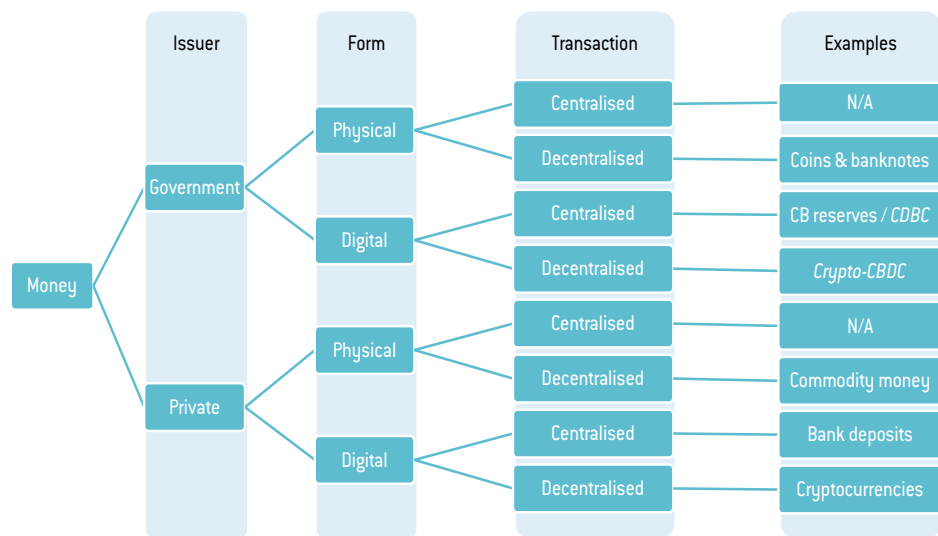
of goods and services, and for the repayment of debts; third, a store of value, a way to store wealth in order to transfer purchasing power from the present to the future.

To perform these tasks, money can take various forms, including non-perishable goods and non-financial and financial assets. Various goods and assets have been used and even co-existed as money, but some have been very successful while others have led to monetary instability and have been replaced. Therefore, money can vary both with respect to its characteristics and its relative success in performing its three main functions.

2.1 A taxonomy of money: where do cryptocurrencies fit in?

Before we turn to the conditions for the success of a particular form of money, it is useful to classify the various types of money to understand how cryptocurrencies differ from other forms of money. We focus on three main criteria (among others discussed by Bech and Garratt, 2017): a) the issuer: government or private; b) the form it takes: physical or digital; and c) how transactions are settled: centralised or decentralised.

Figure 1: A taxonomy of money



Source: Bruegel based partly on the typology proposed by Bech and Garratt (2017). Note: CDBC stands for Central Bank Digital Currency (not discussed further in this Policy Contribution).

Cryptocurrencies would thus represent a form of money that was not previously available as a particular combination in the money taxonomy. Specifically, cryptocurrencies are:

- Privately issued. This is not new *per se*. Privately-issued currencies have been used and have performed well in the past. However, unlike bank deposits for instance, they are not a liability and cannot be redeemed.
- Digital. This is also not new *per se*; it is similar to electronic money issued by central and commercial banks. Like this type of money, cryptocurrencies are also fiduciary (they have no intrinsic value).
- Allowing the settlement of transactions in a decentralised fashion. Exchanges via cryptocurrencies are peer-to-peer. Decentralised ledger technology (DLT) – for example, the blockchain – is used to avoid the so-called ‘double spending problem’ that arises with digital currencies because of their easy replicability and which is traditionally solved through record-keeping by a trusted central agent. This means that with a DLT there is no central authority needed for the settlement of digital transactions between counterparties¹. In

¹ See BIS (2018) for details on how a DLT works in practice.

fact, no single entity is responsible for operating cryptocurrencies, though a number of intermediaries are needed to provide technical services (a digital wallet is needed to use the cryptocurrencies, and intermediaries are involved when exchanging them with other currencies, etc). Essentially, the novelty of cryptocurrencies is the feasibility of peer-to-peer digital transactions (see Figure 1).

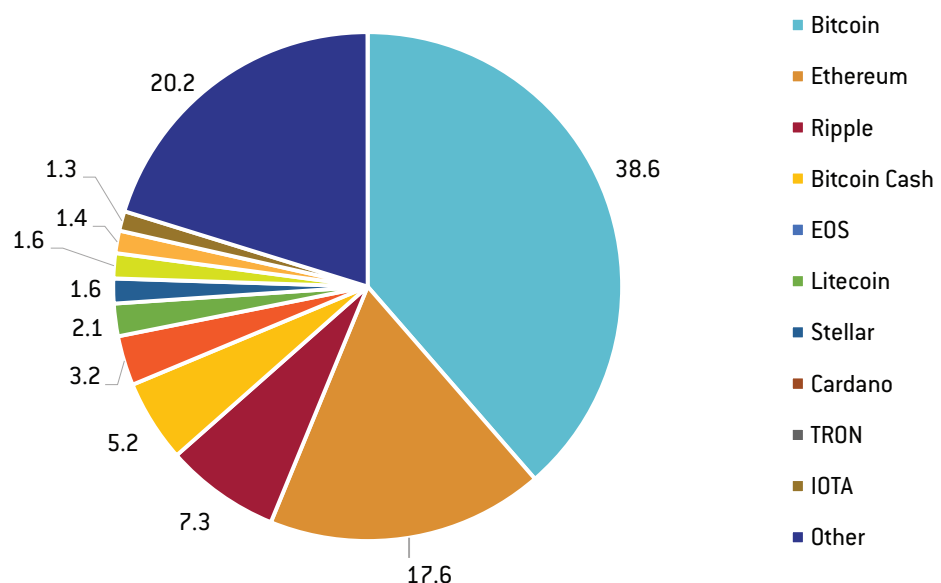
What could be the main advantages of cryptocurrencies given these main characteristics?

- Decentralisation would ensure (almost) anonymity of transactions, which is good for privacy, although it could also mean that cryptocurrencies can facilitate transactions related to illegal activities or tax evasion. Arguably cryptocurrencies are even more prone to such activities than cash given the enhanced possibility to handle large transactions. The DLT is also in principle less vulnerable to malicious attacks compared to centralised systems and therefore should allow a reliable ledger of past transactions to be maintained;
- Private issuance is decided not by a political institution but by an algorithm which is seen by supporters of cryptocurrencies as a way to avoid discretionary decisions that can lead to too much inflation. The automatic issuance of cryptocurrencies would also increase transparency (for anyone able to read the algorithm at least) and the predictability of their 'monetary policy'. As we will later discuss, this is also a disadvantage because discretionary decision-making allows for flexibility to deal with shocks.
- The digital form of cryptocurrencies and the absence of a link to a particular jurisdiction allow for a truly global and easily accessible currency that could facilitate global trade.

2.2 The state of cryptocurrencies

At least 1500 cryptocurrencies exist but a vast majority of cryptocurrency transactions are done in just a few of them. At the end of May 2018 cryptocurrencies represented around \$330 billion in terms of market value (Figure 2). The 10 most important represented 80 percent of the total market, while the two most important, bitcoin and ethereum, represented around 55 percent of the market value. For comparison, bills and coins issued by the Fed represented at the same time \$1.6 trillion, while those issued by the European Central Bank represented €1.2 trillion.

Figure 2: Market shares of cryptocurrencies (market prices, May 2018, in %)



Source: Bruegel based on coinmarketcap.com. Note: 'Other' represents more than 1500 other cryptocurrencies currently exchanged.

Table 1 compares the euro and bitcoin in terms of number and value of transactions. It shows that cryptocurrencies are nowhere close to replacing today's major currencies. In addition, transactions in euro and in bitcoin are not directly comparable: the euro-area number excludes financial institutions and records only transactions resulting from the exchange of goods and services. Transactions in bitcoin include all changes in the blockchain ledger (and therefore also financial transactions such as foreign-exchange transactions between bitcoin and other currencies), which means that this number is biased upwards. The values of these transactions also tend to be overestimated by the strong increase in the bitcoin value in 2017.

Table 1: Transactions in € vs. bitcoin

		Number of annual transactions (billions)	Average transaction value	Value of all annual transactions (billions)
Euro area (in €)	Non-cash (exc. MFI)	79	1,860	146,452
	Cash	129	13	1,653
Bitcoin	In €	0.1	34,228	3,582
	In bitcoin	0.1	9	0.9

Sources: Bruegel based on tradeblock.com, Bloomberg, ECB, Esselink & Hernández [2017]. Notes: data for transactions in € is from 2016 while the data for bitcoin transactions is for 2017.

3 What are the conditions for currencies to fulfil the functions of money?

Historically two key features have characterised successful currencies: price stability and a sufficiently large network of users. Among the three functions of money, being a good store of value appears to be a necessary condition for the other two (unit of account and medium of exchange). In other words, unless the value of money is relatively stable over time, it will not be widely used, either as an accounting device or a medium of exchange. Stability in the value of the currency, in turn, requires that supply follows demand in a way that avoids both high inflation (rapid loss of value) and deflation (rapid gain in value). In practice, the former requires that the supply of the currency is somehow constrained, whereas the latter requires a supply that can be sufficiently elastic in order to keep up with demand.

But beyond value stability, for a currency to be successful requires a critical mass of users. The two features are complementary and mutually reinforcing. Currencies are widely used if they have a stable value. However, this is not sufficient: the extent of the network of users is also crucial to the success of a stable currency. As a social convention, a currency relies on the expectation that there will be enough users to transact with it. Historically, in order to build up that network of users, currencies have traditionally relied on some form of backing, coercion, or a combination of the two.

A currency's stability and the extent of its network of users are founded on different forms of trust and are closely intertwined. Ultimately, the success of money can be attributed to the institutional arrangements (or rules) that underpin it and the degree to which they provide stable and predictable purchasing power, a wide network and common knowledge about both. The rules that underpin the management of official currencies are part of the greater

system of rules governing any nation. The quality of the currency is inexorably linked to them.

Today's fiat currencies issued by the world's major central banks (and the bank deposits that can be exchanged against them at par) perform well all three traditional functions of money. In jurisdictions where independent central banks have a price stability mandate and fulfil it, currency is a reliable store of value, the predominant medium of exchange and the unit of account.

The state had been instrumental in ensuring the ascendance of fiat money. To build a network of users, states often resorted to some sort of backing, originally in the form of a non-financial asset with intrinsic value (commodity money, eg gold) and/or coercion. This took the form of legal tender (ie the mandatory acceptance of banknotes and coins for their full face-value to make payments and to discharge debt) or the obligation to pay taxes in the official currencies. But once the network is established and consolidated, as long as its participants maintain trust in the stability of the currency, backing and coercion become less important.

Today, central banks provide an elastic supply of their currencies to fulfil their price stability mandates in an accountable but discretionary institutional setup: inflation targeting. This framework allows central bankers to use many instruments (short-term interest rate changes, asset purchases, expectation management) and does not bind them with any intermediate target (such as money or credit growth), as long as they ensure price stability. This high degree of flexibility in decision making on the part of the monetary committees allows central banks to react to changes in the economy and how it functions by changing their 'supply protocols.' In other words, central banks have the capacity to make changes to all instruments at hand when they deem it necessary. In turn, accountability, if done in the right way, should give the right incentive to the central bankers to fulfil their mandates and achieve price stability, which should increase trust in the currency.

However, the current pre-eminence of currencies under the control of central banks, like the euro and the US dollar, does not rule out the emergence and adoption of other currencies, in particular cryptocurrencies. But how these currencies will perform as money will depend heavily on their characteristics and on their ability to perform the same economic functions as official currencies.

4 Evaluating the money role of cryptocurrencies

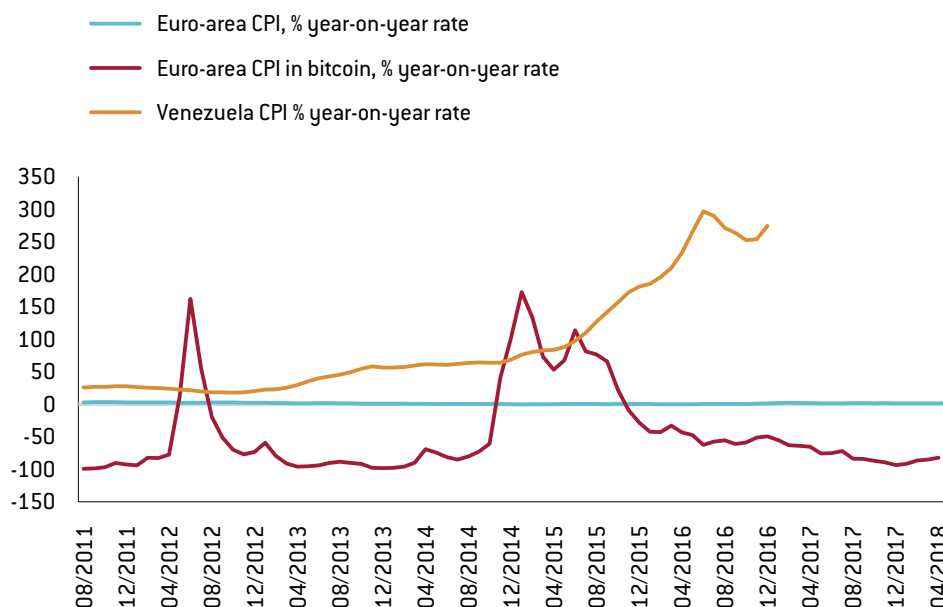
4.1 Today: More of an asset than a currency

Arguably, the cryptocurrencies available today are not performing the functions of money very well. As a result, they can only be considered as speculative assets, which are expected to yield returns only as a result of capital gains.

The first reason for this is the inherent volatility of the values of today's main cryptocurrencies, which are by-products of their supply protocols. In the case of bitcoin, the quantity supplied is fixed at an upper limit (21 million), which is approached following a predictable, near-predetermined path. Importantly, the supply does not match the quantity demanded. The inelastic nature of the supply embedded in the protocol rules (which for bitcoin looks like a rule derived from the gold standard) results in volatility, which prevents these currencies from functioning as good stores of value. This, in turn, also limits their adoption and keeps the network of users relatively small, thus reducing their role as mediums of exchange and as units of account. These two problems reinforce each other because the high volatility of today's cryptocurrencies is also partly the result of their limited use and the fact that the networks of users consist mainly of speculators.

Figure 3 shows that given its volatility, bitcoin cannot perform well the basic function expected from a currency. With inflation (and deflation) rates closer to those observed in Venezuela than those observed in the euro area, bitcoin is clearly not a good store of value. This also means that most retailers who accept bitcoin do not want to take the exchange rate risk and thus update their prices in bitcoin frequently and exchange bitcoins just after the transactions (highlighting bitcoin's limitation as a unit of account) (see Koning, 2015).

Figure 3: Inflation in the euro area (in €, bitcoin) and in Venezuela



Sources: Bruegel based on Bloomberg, ECB and IMF. Note: Venezuelan CPI is not available in monthly frequency after the end of 2016. However, the IMF reports a yearly inflation rate for 2017 of 1087.5 percent.

The second reason why cryptocurrencies are not a good medium of exchange is the cost of the transactions and the time they take to be recorded in the decentralised ledger. Despite the absence of the fixed cost associated with building a centralised network, the amount of computing power needed to validate cryptocurrency transactions in order to avoid any falsification of the ledger is energy inefficient and represents a significant waste of resources.

The borderless nature of today's main cryptocurrencies could also be a major issue: price stability means that the basket of goods and services included in the CPI of a particular (homogenous) jurisdiction has a stable price. But current cryptocurrencies are global and not attached to a particular country or region. From a monetary policy perspective, a global cryptocurrency area is unlikely to be an optimal currency area, as this would lead to an inability to adjust exchange rates within the 'area'. The result would thus be a crypto-monetary policy (ie its supply protocol) that would be consistently too tight and too accommodative for different countries at different times.

Other major risks that could undermine trust in cryptocurrencies could arise from market concentration (which could lead to the falsification of the ledger and to 'double spend' issues), from the manipulation of the value of the currency via insider trading and from the reliance on unregulated intermediaries necessary to use cryptocurrencies².

² See for instance Griffin and Shams (2018), who show how the cryptocurrency Tether might be used to provide price support and manipulate other cryptocurrency prices.

4.2 A money role in the future?

Despite the clear limitations of current cryptocurrencies, it is possible that developers will be able to improve their supply protocols to limit the volatility of their currency values resulting from their supply rule, at least in normal times. The developers of cryptocurrencies could learn from past experience in order to improve their algorithms to supply the currencies in ways that are more responsive to demand conditions and to correct other deficiencies of today's cryptocurrencies (in particular their negative environmental impact).

There are already cryptocurrencies that are trying to solve these issues and provide so-called 'stablecoins'. For example, the creators of a new currency called 'Basis' aim to provide a currency of which the supply can expand and contract with demand to maintain a stable value relative to an official currency (eg the US dollar). Should Basis manage to overtake the dollar in use, then its creators' intention is to tie its supply directly to a Consumer Price Index measured in that currency. This runs against the international nature of cryptocurrencies that are not tied to any jurisdiction. The creators of Basis acknowledge that it might be better to have a currency related to a particular (homogenous) jurisdiction that reflects better an optimal currency area. The details of the Basis supply protocol are still problematic (see Cochrane, 2018, for a very critical explanation of how the Basis protocol works), but it shows that designing a stable cryptocurrency might be the next step.

However, whatever the quality of their protocol, just like any other fiat currency, cryptocurrencies would be inherently vulnerable to changes in beliefs and expectations that can lead to undesirable self-fulfilling inflationary episodes. In other words, even with a sophisticated supply protocol, there is no reason to believe that the equilibrium with stable prices will always prevail over unstable equilibria. This implies that elastic supply is a necessary but insufficient condition to obtain price stability. Central bank-managed currencies have a number of additional properties that help establish their acceptability and guide economic agents towards the desirable equilibrium. First, they are deemed *legal tender*, in other words recognised by the underlying legal systems as an acceptable means of settling financial obligations. Second, the sovereign accepts them as means of settling taxes and, third, they operate within a set of institutional rules that gives them incentives and means to achieve price stability. In addition, currencies issued by central banks now benefit from several decades of price stability experience, good practices and established networks of users, giving them natural monopolies as units of account, mediums of exchange and as the ultimate stores of value.

For all these reasons, even if developers manage to design a supply protocol able to offer cryptocurrencies with an elastic supply, it is doubtful that this will be enough to encourage the wider use of cryptocurrencies and replace currencies issued by governments.

5 Cryptocurrencies and monetary policy

5.1 Crypto- and official currencies: a 'peaceful' coexistence?

At the moment, cryptocurrencies operate alongside official currencies. The current volumes are small and do not challenge the position of official money as the main currency. But as algorithms improve to limit the volatility of cryptocurrencies, their popularity and use could increase. This would lead to a coexistence with other official currencies. We examine whether such coexistence would entail risks for central bank monetary policy. Could the central bank lose its grip on the economy as a result?

The interaction between cryptocurrencies and central bank monetary policy is treated in detail by Fernandes-Villaverde and Sanches (2018). Their theoretical model predicts that the coexistence of central bank and private money depends on the type of monetary policy the former follows. In particular, privately-issued currencies would be used if the official curren-

cies do not ensure price stability, but would lose their value as a medium of exchange when the central bank credibly guarantees the real value of money balances.

The ramifications are two-fold. First, the coexistence of government money and cryptocurrencies that are valued as mediums of exchange is not a theoretical impossibility. Second, the central banks have the advantage: by choosing a specific type of monetary policy they can prevent cryptocurrencies from being valued as a medium of exchange (but they could still be valued for other reasons, for instance as a pure speculative asset).

From this perspective, rather than posing a threat, the coexistence of government money and cryptocurrencies can have a positive effect by acting as a disciplining device on central banks. This is a partial vindication of Hayek (1976), who argued in favour of breaking the state monopoly on money as a way to ensure the stability of the official currency.

Nevertheless, from a more practical standpoint, central banks could face some risks from the emergence of cryptocurrencies as relevant mediums of exchange with stable purchasing power.

First, the extent of the substitution by economic agents of cash and bank deposits for cryptocurrencies will determine the effectiveness of monetary policy. Extensive substitution of bank deposits in particular would translate to reduced control over monetary conditions, because of the shrinking of the amount of broad money in the economy. At the extreme, the provision of base money and the resulting influence over interest rates would be rendered ineffective. However, as Stevens (2017) points out, as long as money issued by central banks retains the role of unit of account, the switch to cryptocurrencies as a medium of exchange would be limited and thus the associated threat to monetary control would also be limited.

Second, the shrinking role of central bank money creates a possible fiscal risk in the form of reduced seigniorage revenue. The response could be higher distortionary taxes that would hurt growth. That said, such risks appear to be exaggerated given that seigniorage revenues make up an insignificant fraction of total government revenue.

The last, but probably most pertinent, threat does not emanate from the potential use of cryptocurrencies as money, but from their attractiveness as investment assets. As a speculative investment – an investment made in expectation of a return from capital gains only – cryptocurrencies will be prone to bubbles. The collapse of a cryptocurrency bubble could reverberate into wider financial instability if households, corporates and financial institutions hold unhedged debt positions. Central banks would then face a double risk: first to the stability of financial institutions they supervise, from the potentially unregulated cryptocurrency debt markets, and, second, to price stability, from the effects on the real economy of deleveraging and defaulting by economic agents.

5.2 Financial stability implications of a potential cryptocurrency takeover

Given the natural monopoly enjoyed by central bank-controlled currencies, it would take a deep crisis of trust for a cryptocurrency to replace an established currency in full. An episode of very high inflation could be such a shock, but even then, agents might wish to switch to other established safe-haven currencies (such as the US dollar or the Swiss franc) before resorting to cryptocurrencies. However, as argued earlier, the broad accessibility of cryptocurrencies, compared to other currencies, might offer an easy path to switch. How would the financial system and the broader economy be affected?

In particular, we can ask ourselves if a fractional reserve banking system, as we have today, would be possible in a cryptocurrency world and how the cryptocurrency protocol could influence it. In a fractional reserve banking system, bank deposits are matched by currency (bills, coins and central bank reserves) only up to a fraction. In such a system, bank deposits are the result of the provision of loans by commercial banks to companies and households, and, therefore, money and credit creation are closely intertwined.

In theory, there is nothing that prevents fractional reserve banking from emerging in a full cryptocurrency regime. However, money creation by private banks would reduce the level of control the cryptocurrency protocol exerts over the money supply, placing additional

complexity on the supply algorithm. In fact, central banks that have tried to target the total stock of money in the past renounced it because they found it difficult to achieve price stability with that strategy. Today, the money stock that is created by private banks is ultimately influenced, but not fully controlled, by the central bank. Monetary policy operates mainly through the interest rate at which the central bank provides currency to private banks. Successful influence over monetary conditions in the presence of a fractional reserve banking system would, thus, require an algorithm that is able to affect the lending behaviour of banks.

Even if this were to be achieved, these banks would still be vulnerable to bank runs. Under a fractional reserve system, banks generate profits by engaging in maturity transformation: using short-term, money-like deposits as funding for illiquid, long-term loans. This leaves them vulnerable to the possibility of bank runs. When there is such a general flight to liquidity, the central bank acts as a lender of last resort to restore confidence in the banks and in financial stability. Arguably cryptocurrencies would not be able readily to provide liquidity in times of crisis. This is not unlike the gold standard, where new currency could not be mined in real time and made available to absorb excessive demand. Similarly, deposit guarantees would not be available as a solution in a crypto-financial system.

A third *ex-post* solution would be for the banks themselves to suspend the convertibility of their deposits into the cryptocurrency. However, the existence of such *ex-post* risk would translate to an *ex-ante* discount of each bank's respective IOUs. The 'singleness' of money would then break down, as private-bank issued money would fragment into assets that are not traded at par with the predominant cryptocurrency (which is in some way similar to what happened during the free-banking era in the US between 1836 and 1864³). Therefore, the *ex-ante* absence of credible solutions to bank runs would increase their likelihood and lead to instability in the system.

Does that mean, at the opposite end of the spectrum, that we could see the emergence of a financial system similar to full reserve banking? In such a system, the bank's IOUs that serve as money (eg bank deposits) are fully backed by a government fiat currency or by a commodity. Here, the cryptocurrency could play the role played traditionally by official fiat currencies. This would have two main advantages: first, money supply would be decoupled from credit and would thus only depend on the cryptocurrency algorithm; and, second, there would be no bank runs.

However, one has to ask what forces would give rise to banking in such a cryptocurrency world. In the case of today's fiat government currency, the possibility for users to hold and store its physical form (ie bills and coins) is fraught with security risks and inconvenience. Full-reserve banks (which do not provide lending for productive investments) would at least provide a solution to this problem, by serving their clients' needs to make payments. In a cryptocurrency world by contrast, full-reserve banks would be irrelevant: as payments would be done directly in the decentralised ledger, there would be no need to resort to an intermediary to complete a payment.

To sum up, it seems that in a full crypto-financial system, savers would have to choose between holding IOUs labelled in a cryptocurrency unit of account issued by unstable banks (not benefiting from a lender of last resort) or sticking to cryptocurrencies that stay idle in the ledger. In that case, who would provide lending to the rest of the economy? One possibility is direct peer-to-peer lending but this would force individuals to screen, monitor and diversify their investments themselves, unless individuals pool their wealth (in cryptocurrencies) to share risks and lend to other agents. However, these entities that would provide loans to the economy would look more like investment funds than banks, as their funding sources (in cryptocurrencies) would not be deposits but equity. Although liquidity risk would be less of a concern for the holders of equity, they would also be more exposed to credit risk than bank depositors, because they would not benefit from the seniority that bank depositors enjoy in case of default compared to other creditors. This risk could thus disincentivise savers from lending and could thus lead to a severe credit squeeze that would clearly be detrimental for the economy.

3 See details in Frieden (2016).

5.3 Money and power: ensuring a system of checks and balances

The potential of cryptocurrencies to credibly challenge official currencies cannot only be based on the intelligence of underlying algorithms. Technology and our understanding of underlying economic mechanisms can always help improve those algorithms just as they currently inform monetary policy decisions. But is that all we need, or is there something more intrinsic to the power of the money issuer? Can a cryptocurrency ever be a credible money?

Currency management has a societal value – effectively the societal value of monetary policy. The value and stability of money is what enables societies to function well and is not separate from broader choices governments make when they run policy. It is therefore also a part of what constitutes the social contract (Collard, 2017) between the principal (the citizen) and the agent (the government). Manipulating a currency has historically been a powerful means of enabling the sovereign to pursue certain objectives, including financing wars. In other words, this power of controlling money can be used and abused. This is why in modern democracies currency management goes through appropriate layers of legitimacy and accountability. A modern authority that controls the currency will be evaluated according to how well it sticks to the implicit social contract agreed through democratic procedures. This means that any authority can be released for not delivering on what the social contract dictated.

How could an intelligent algorithm that is automatic and anonymous ever be held responsible for failing to deliver agreements? The complexity of currency management implies that the system will fail sometimes, just like financial crises periodically happen. No algorithm, no matter how intelligent (and indeed benevolent), will remove the possibility of crisis. The automation of monetary policy would remove it also from the system of checks and balances. This type of ‘independence’ of monetary policy effectively also makes accountability impossible, and makes monetary policy exogenous to the process that identifies, monitors and evaluates agreements⁴.

It is only the existence of this system of checks and balances that allows modern lenders of last resort to create money out of nothing and provide ample liquidity in times of crisis. As soon as this system breaks down and trust in authorities goes, the currency ceases to be an acceptable means of payment or even unit of account. The currency is only as strong as its lender of last resort, and the lender of last resort is only as strong as the backing it has from its constituents. Constituents in turn, build trust depending on how well social contracts are adhered to.

6 Conclusions

The emergence of decentralised ledger technology has allowed innovations in peer-to-peer transactions that were difficult to imagine just a decade ago. This technology has also led to the development of cryptocurrencies and allowed them to challenge the role of money as mediums of exchange.

However, the evidence so far suggests that cryptocurrencies are not as widely used as any official currency and are not real contenders for currency substitution. The design of their protocols, at least so far, is very primitive and arbitrary relative to what the management of modern financial systems requires.

We therefore do not see an immediate risk of cryptocurrencies challenging central

⁴ Although the rules of the blockchain can change based on a majority decision of the participants validating the transactions (see a discussion of so-called ‘hard forks’ in BIS,2018), the weights of the votes are not equal but depend on computing power, rendering the decision-making process less democratic.

bank-controlled currencies, and certainly not international currencies like the US dollar and the euro. Years of good practices and price stability, combined with their legal statuses and strong networks of users, have given official currencies a natural monopoly. However, as the underlying algorithms of cryptocurrencies develop to reflect better demand for money and more general economic conditions, one could envisage an increase in their popularity and use.

But the features that create the hype around cryptocurrencies, such as their international and automated natures and the absence of the risk of political control, set limits in terms of how far they can go in replacing official money.

Control over the value of money is a very significant power to have. This is why those that are given this power are subject to systems of checks and balances designed through social contracts. Taking this power outside the system of checks and balances by rendering it anonymous and automatic could be a serious threat to a society's stability. The stability of a currency necessary for the development of an economy relies on trust and universal agreements. Trust in turn is built on the ability to monitor, review and change.

So, while cryptocurrencies could evolve into legitimate private means of payment, we do not see them evolving in ways that would challenge the powers of official currencies. Ultimately, as a potential competitor to official currencies, cryptocurrencies could even have a positive effect by acting as a disciplining device pushing central banks (especially in countries with histories of lax monetary policy) to take their price stability mandates seriously.

References

- Bech, M. and R. Garratt (2017) 'Central bank cryptocurrencies,' *BIS Quarterly Review September 2017*, Bank for International Settlements
- BIS (2018) *Cryptocurrencies: looking beyond the hype*, BIS Annual Economic Report, Bank for International Settlements
- Cochrane, J. (2018) 'Basecoin,' *The Grumpy Economist - John Cochrane's blog*, 22 April, available at <https://johnhcochrane.blogspot.com/2018/04/basecoin.html>
- Collard, B. (2017) 'Money is the Real Social Contract,' *Foundation for Economic Education Blog*, 25 August, available at <https://fee.org/articles/money-is-the-real-social-contract/>
- Esselink, H. and L. Hernández (2017) 'The use of cash by households in the euro area,' *Occasional Paper Series 201*, European Central Bank
- Fernandes-Villaverde, J. and D. R. Sanches (2018) 'On the Economics of Digital Currencies,' *Working Papers 18-7*, Federal Reserve Bank of Philadelphia
- Frieden, J. (2016) *Lessons for the euro from early American monetary and financial history*, Essay and Lecture Series, Bruegel
- Griffin, J.M. and A. Shams (2018) 'Is Bitcoin Really Un-Tethered?' mimeo, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066
- Hayek, F.A. (1976) 'Choice in Currency: A Way to Stop Inflation,' *Occasional Papers*, The Institute of Economic Affairs
- Koning, J.P. (2015) 'The dollarization of bitcoin,' *Moneyness Blog*, 12 June, available at <http://jpkoning.blogspot.com/2015/06/the-dollarization-of-bitcoin.html>
- Stevens, A. (2017) 'Digital currencies: Threats and opportunities for monetary policy,' *NBB Economic Review June 2017*, National Bank of Belgium