ie | CENTER FOR THE GOVERNANCE OF CHANGE

CRYPTO-CURRENCIES AND THE FUTURE OF MONEY

GOING BEYOND THE HYPE: HOW CAN DIGITAL CURRENCIES SERVE SOCIETY?

2019

Contents

Executive Summary

The shortcomings of existing financial systems became widely criticised in the aftermath of the 2007–08 financial crisis leading to an unprecedented wave of interest in new ways of efficiently executing economic transactions while ensuring high levels of transparency and accountability. With over 2,000 in existence at the time of writing this report, cryptocurrencies have received a great deal of attention as a potential tool for radically altering financial landscapes for the betterment of society. The purpose of this report is to provide a comprehensive overview of how crypto-currencies could be used to achieve this purpose. This includes how cryptocurrencies currently function relative to the intentions of their pioneers, and how the general public, use, understand, and trust them.

Some of the main findings include:

- Modern discussions and debates about crypto-currencies tend to confuse 'money' with 'systems of payments' or, the mechanism by which transactions are processed and settled.
- Cryptocurrencies have the potential to vastly improve systems of payments if designed and implemented correctly.
- In practice, existing cryptocurrencies have failed to achive the objectives envisioned by their pioneers and would generally not be considered as money.
- New innovations (stablecoins, proof of stake, CBDCs) are helping to make digital currencies more realistic candidates to replace traditional money and create benefis for users across large volumes of transactions.

In addition to these technical challenges, the value added in this report comes from a unique empirical examination of how citizens undertand cryptocurrencies and trust in different institutions to issue and manage money across a unique sample of eight countries including Argentina, Brazil, France, Germany, Mexico, Spain, the UK and the US.

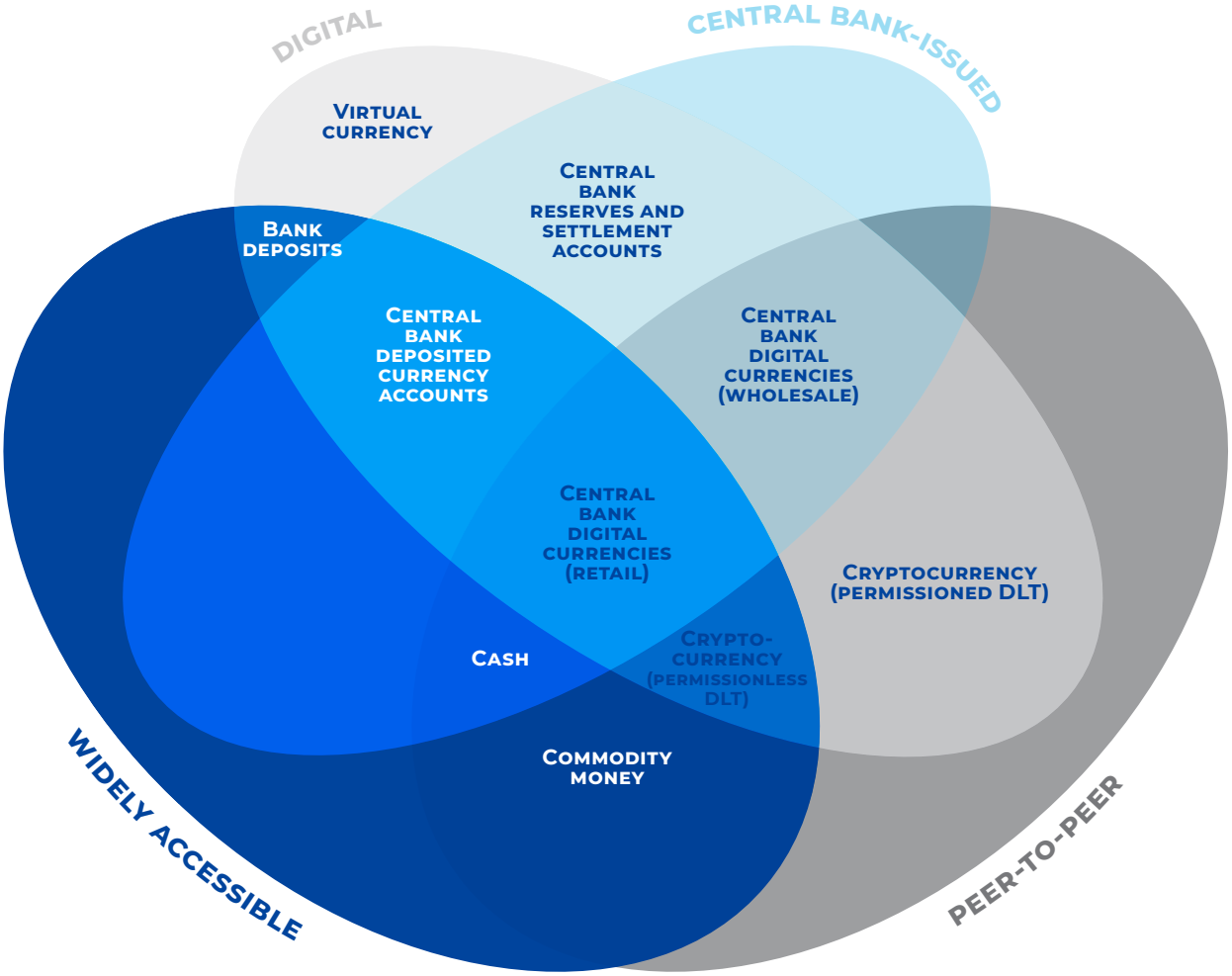
Some of the main findings include:

- Knowledge, use, and understanding, of crypto-currencies remains highly limited in all countries.
- The vast majority of citizens in all countries agree that money should continue to be issued by central banks.
- While all central banks enjoy a significant trust premium when it comes to the creation and management of money, large differences exists between Latin American countries (Argentina, Brazil, Mexico) and European countries (France, Germany, Spain, UK) and the US.
- Countries where central banks experience lower trust premiums are more open to adopting new digital currencies issued by alternative institutions
- Trust in Facebook to issue and manage a currency remains very limited, especially in Europe and the US.
- The degree of acceptability and price stability play a key role in determining preferences for holding of money, regardless of who is issuing it.

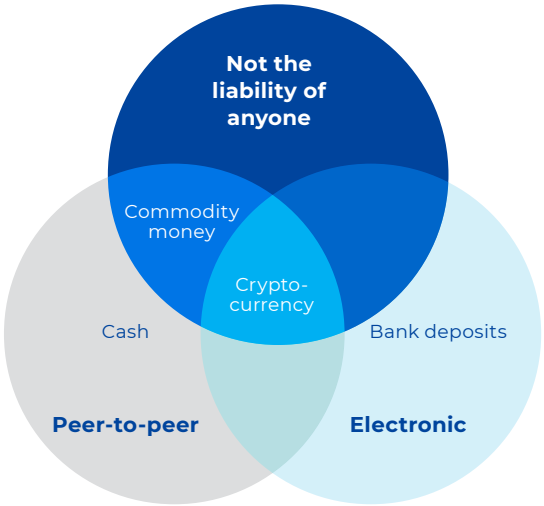
Introduction/ Preface

Since their inception in 2008 and the subsequent enthusiasm, media attention, delusion, reflection, and continuous innovation, 'cryptocurrencies' have become one of the most interesting and perhaps most misunderstood phenomena of the early 21st century. Their popularity and potential for 'disrupting' and improving traditional financial systems, however, have led to an expanding list of media commentaries, research papers, and policy reports. Unfortunately, many of these contributions have tended to focus on the contemporary positivist side of cryptocurrency without considering the normative intentions of its creators or, perhaps more importantly, the historical context under which money and monetary systems have evolved. These contributions have also tended to focus on digital money from a single disciplinary viewpoint (computer science, economics, finance) without a great deal of consideration or integration of the valuable inputs from other perspectives.

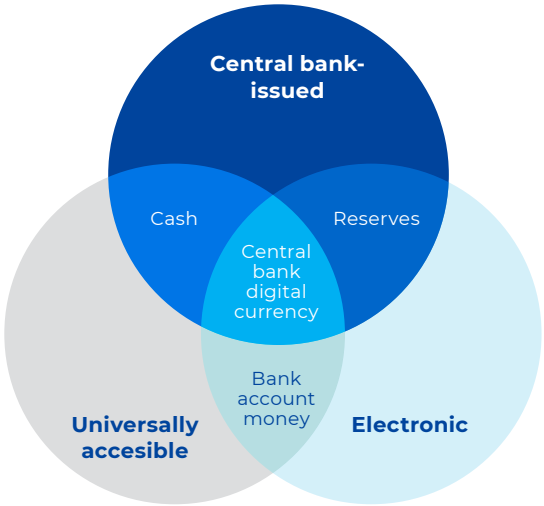
The idea of money has evolved continously over time. In the context of the technological innovations of the 21st century, it has become a phenomenon with a wider range of feasible possibilities, some of which were in fact proposed as far back as the early 20th century. To give some idea of the new range of types of money, the Bank for International Settlements (BIS) published a series of taxonomies including the 'money flower' and more general taxonomies that distinguish between central bank-issued currencies (which are a liability on the central bank balance sheet) and private-sector issued digital currencies (which are not the liability of anyone). Within this wider context, there exists a variety of types of money, each of which has different underlying characteristics, or attributes.



CRYPTOCURRENCY, CPMI (2015)



CENTRAL BANK DIGITAL CURRENCY, BJERG (2017)



Source: Bank for International Settlements (BIS)

For example, a physical cash transaction is issued and is backed by (a liability of) the central bank and is subject to some degree of inflation over time, has low transaction costs and is accepted by all sellers of goods and services. On the other hand, a credit card transaction is backed by (a liability of) a commercial bank, is subject to the same degree of depreciation as cash, may come with some (explicit or implicit) transaction costs, and is accepted by all sellers of goods and services.

Given some of the shortcomings of money and existing financial systems that became apparent in the aftermath of the 2007-08 financial crisis, Nakamoto (2008) proposed a new type of money which would effectively remove many of the third-party participants in transactions, making a more efficient, and less costly, way to make transactions with strangers. With over 2,000 cryptocurrencies in existence at the time of writing this report, cryptocurrencies have since become progressively embraced by speculative investors and growing market caps, but have yet to be adopted by the wider public as a viable form of money due to practical technical challenges along with a lack of trust in the issuing authorities and understanding of how to use them.

Some of the more fundamental questions that deserve closer attention within 'monetary ecosystems' revolve around who creates the money and what is their relationship with the entity who creates and obtains value from it. This is especially important in a fiat currency environment where the value of money (digital or physical) depends on the degree of trust users have in those who issued or back the currency. The purpose of this report is to provide a more comprehensive overview of how cryptocurrencies could be used for the betterment of society, how they currently function and how the general public uses, understands and trusts cryptocurrencies across a sample of eight countries.

The first chapter of this report will examine the normative nature of money including the role of community trust and the role that government plays in ensuring this trust. In this normative framework, we can think about the possibility of cryptocurrency as money and how this might be possible. A key part of this introductory chapter is the idea of trust and money, especially in the fiat currency system that has emerged in the late 20th century.

The second chapter will provide a brief history of money over the 20th century, including the gold standard era, the design of Bretton Woods and the adoption of fiat currencies. This chapter will also touch on some of the historical themes that have re-emerged in the context of cryptocurrencies, including Hayek's idea relating to currency competition and some of the challenges involved with fractional reserve banking systems.

Moving into the 21st century, Chapter 3 will consider the possibility of realistic possibility that 'money' will dramatically change in the coming years with the evolution of cryptocurrencies. This chapter will consider some of the arguments against the use of physical and untraceable cash including fraud and health concerns. More generally, this chapter will consider the social benefits of moving towards digital currencies and the associated risks/barriers.

Chapter 4 will provide an overview of how cryptocurrencies work in terms of their degree of centralization, security and anonymity, token supply and governance (consensus protocols). This chapter will examine cryptocurrencies in terms of what they were meant to be from the perspective of Nakamoto (2008) and what they have become in practice. This chapter will largely draw on the case of Bitcoin, but will also discuss briefly new generation tokens (stablecoins, Libra).

Chapter 5 will consider the arguments for the issuance of Central Bank Digital Currencies, including a review of the literature and survey of what Central Banks are currently doing in terms of the adoption of a central bank-backed cryptocurrency. This chapter will also discuss the implications for monetary policy and financial stability from adopting this new type of digital money.

Lastly, Chapter 6 will discuss the results of the new IE Survey on 'Cryptocurrencies and The Future of Money' in the context of Chapters 1--5. From a diverse sample of countries (Argentina, Brazil, Mexico, France, Germany, Spain, UK, USA). The results show that residents tend to place a trust premium on central banks-backed money. However, significant differences appear across countries, especially those in Latin America.

CHAPTER

1

THE NATURE OF MONEY AND THE POSSIBILITY OF CRYPTO-CURRENCY AS MONEY

By Professor Tony Lawson,
University of Cambridge

A.The Nature of Money

Can forms of cryptocurrency become money? To pursue this question, it is necessary first to be clear on what is meant by money, and on what precisely is required for something to be, or to become, money. The concern of this opening chapter is precisely with this issue, to identify conditions that must be met for a form of cryptocurrency to qualify as money.

A form of money, just like any other social phenomenon, is a property of a particular community, and so typically possessing various community-specific features. Many communities have produced money, however, and the concern here is with commonalities of all the numerous forms.

In this regard, the most obvious common or shared feature is that by which a money can everywhere be identified or recognised. This is its property of being employed as a general means of payment, of being useable to discharge any debt in the community in which the money is produced.

If, say, in any specific money community, an individual participant requests of a seller, a loaf of bread, or perhaps a meal, then, when the bread is handed over, or after the meal has been consumed, the buyer is in debt to the seller. It is an identifying property of money that, in all such transactions (excepting in cases where a specific alternative agreement on means of payment has been reached in advance of a debt being occurred), the money can be used to settle the resulting debt.

A basic condition for a general means of payment to exist in any community is that the latter has a system of value accounting that includes, as a component, a (community-specific) unit of value. This is simply a unit of value measurement or assignment -- such as pound sterling, US dollar, euro -- in terms of which all goods, services, or assets in a community will have their assessed values expressed. Clearly all items of money must also be denominated in the same units as the debts, if the money is to be used to cancel them. So, money will itself be a feature of a system of value accounting that includes a unit of value (or account) as an additional accepted component.

If the nominal property of any money, i.e. that by which it is identified, lies in its being accepted as a general means of payment, a further more fundamental feature that grounds this property is the manner of the money's incorporation as a component of the community's system of value accounting. Most social phenomena (not just money) are in fact constituted through processes whereby certain kinds of things are incorporated into community systems as components. In all cases, the phenomena are created by processes of social positioning, whereby selected kinds of things are allocated to positions, thereby constituting them as different types of phenomena qua system components, and whereupon their uses, qua positioned items or system components, are governed by community-accepted sets of rights and obligations. To see this, it is enough to think of the creation and acceptable uses of means of transport, motorways, car parks, traffic lights, passports, schools and hospitals, etc.[1]

Money is simply a specific conforming instance of this general process of social reality constitution. The

1. See Lawson, 2019.

creation of money involves the community acceptance of a money position within the community's value accounting system and the allocation of a certain kind of thing (currently, it is typically bank debt – see below) to the money position, producing money as a system component. As part of this positioning process, rights and obligations are allocated to community members, determining that holders of instances of the money have the right to use it to cancel their debts and corresponding creditors typically have a matched obligation to accept the money, if it is offered.

The ability of money to serve as a general means of payment is, then, grounded in its additional property of being positioned (in the community's system of value accounting) in such a manner that its uses are governed by the noted rights and obligations.

As with all social phenomena, the existence of money is seen, finally, to depend on community acceptance. However, the notion of acceptance that is key here should be interpreted not as involving any necessary agreement or contentedness of community participants with the situation, only as a willingness to go along with it, at least for the time being. Typically, this general acceptance, in the case of money, takes the form of a preparedness to go along with the declarations of designated bodies to whom authority has been delegated. In modern societies this delegated authority takes the form of the government or central bank.

B. Purchasing Power and Trust

To this point the concern has been on the nature and constitution of money per se. However, the focus of primary interest here is on more than money per se and specifically on a money that *functions successfully*. An additional nominal property for a *successful* money is that (as well as being a general means of payment) it has generalised purchasing power.

The manner in which money is constituted as a component of a community's system of value accounting ensures, as we have seen, that a participant who holds money has the right to use it to discharge any debts already held. However, there is no agreement entailed that participants must become creditors in the first place, that they must allow others to run up debts with them that can be discharged using the money. In countries with hyperinflation, is not unusual to see signs displayed saying goods or services can be acquired only if there is an advance agreement (i.e. prior to a debt being created) for payment to be made in a foreign currency. Thus, a restaurateur, say, will allow customers to order a meal and so acquire a debt if they in effect take out a contact in advance to pay by something other than the local currency.

So, a successful money is in place where participants can easily use it to make purchases, meaning that sellers, etc., are ready to become creditors in the knowledge that the money will be used to discharge the debts that so arise. For this to be the situation, community participants must trust in the money. Trust is key to the successful functioning of any money.[2] Specifically, community participants must trust that if they hold items of money, others will be willing to take such money from them, a condition of which being that no one expects items of money to lose value in the meantime. In short, to function successfully, a money must be trusted as a stable store of liquidity, a store of liquid (i.e. easily transferable) value.

The dominant worry of recent monetary history is that money will lose value, as is markedly the case in episodes of countries experiencing hyperinflation. But an additional concern that can arise, one that will be seen to be especially relevant when considering the possibilities for cryptocurrencies, is that the money instead appreciates in value. In the face of an anticipated decline in its value, participants will not want to hold money; however, in the face of an expected appreciation in its value, participants will not want to let go of it. Either development undermines the usefulness of money for performing its canonical functions.

2. Trust is, of course, fundamental to all social constitution and human action (see Jamie Morgan and Brendan Sheehan, 2015; Stephen Pratten, 2017; Lawson, 2019 chapter 1), a condition for rights/obligations everywhere to work, though often difficult to sustain in the economic sphere, not least where money is involved.

C. Money as Positioned Bank Debt

What, then, are the capacities or capacity required of a successfully functioning money? It is precisely an ability to instil trust in community participants that the money so formed through its positioning will be a stable form of liquid value. This will be most easily achieved where prior to positioning, the money has been found to be a store of value that is easy to pass on.

Currently the money position, was indeed already regarded as a store of value, and became so positioned precisely to instil a trust in the money so hold. This is *bank* debt.

Here the term *debt* is understood to be an obligation held by a debtor to satisfy a creditor. It is internally related to a *credit*, where the latter, technically and legally speaking, means a specific right to payment or satisfaction. Credit and debt, in other words, are two aspects of the same social relation - a credit/debt (or debt/credit) relation - connecting a creditor and a debtor; you cannot have one aspect without the other. Credit is simply this relation viewed from the perspective of the creditor; it is debt from the point of view of the debtor. In fact, in classical accounting terms, this credit/debt relationship was seen as an exchange of *credere* ('to trust') for *debere* ('to owe'),[3] which concluded in the exchange of real underlying assets. Simply put, two entities bind themselves, at a specific point in time, to remain bound to, and trust each other, over the course of the agreement.

How does bank debt/credit (positioned) as money work? Two forms of bank debt are involved, commercial and central bank debt. If, for example, a commercial bank makes a loan to a customer, it records the amount of that loan in the customer's account. The entry shown (or resulting increase in any entry) marks an amount of money thereby acquired by the customer. In the case of the loan, this money is created on the spot. It is done so through the formation of a debt of the bank to the

3. Pacioli's Summa, 1494.

customer. But the result is automatically an amount of money. For, since bank debt was at the relevant point in history first positioned as money, all new items of bank debt come into the world already positioned as money. That is, just as a child of members of the UK Royal Family arrives in the world already positioned as royal, or indeed a child born in the UK of two UK citizens arrives in the world already positioned as a UK citizen, so, currently, all instances of bank debt arrive in the world already positioned as money.

Of course, not all money held in an individual's deposit account was created by loans. But all the money there recorded takes the form of commercial bank debt positioned as money.

The ability to create new debt/credit as money generally lies in the power of commercial banks and the central bank. The central bank can create money by extending loans to commercial banks in the form of the latter's reserves. Many indeed refer to the two cases as producing *commercial bank money* and *central bank money* respectively, the two together being *bank money*.[4]

So, the occupant of the money position currently relied upon to instil trust in a money formed out of it is bank debt (a kind of thing that to serve its intended role usually also requires a degree of continuous state backing, an orientation that can involve, but does not reduce to a reliance upon, laws of legal tender).

Finally, as is the current situation with bank debt, the item positioned as money is not observable, a necessary additional feature of a community's system of value accounting is a set of markers or identifiers of money, or of those that hold it. In the case of commercial bank money, its markers are electronic entries in the community participant's bank account. In the case of central bank money, the markers may take the form of, first, cash, in particular where the money is held by the public, and, second, electronic markers, indicating money held as deposits at the central bank, including commercial bank reserves. So strictly speaking, neither electronic records nor cash are money but rather are markers of it.

To summarise, a community's money possesses generalised debt-discharging power and, when it functions successfully, generalised purchasing power. The first of these powers is grounded in money's property of being positioned as component of a community's system of value accounting in a manner such that its uses are governed by a specific set of community-accepted rights and obligations, in particular that debtors have a right to discharge their debts using the money and the corresponding creditors have an obligation to accept the money when offered. The second of these powers, i.e., generalised purchasing power, is grounded in a community's trust in it as a stable form of liquid value, a trust that, typically at least, is grounded in turn in the trust-instilling capacity of money backed up by the support of the state-backed banking system.

4. This terminology is fine, as long as these terms are always taken to distinguish forms of money (rather than debt).

D.The Possibility of Forms of Cryptocurrency as Money

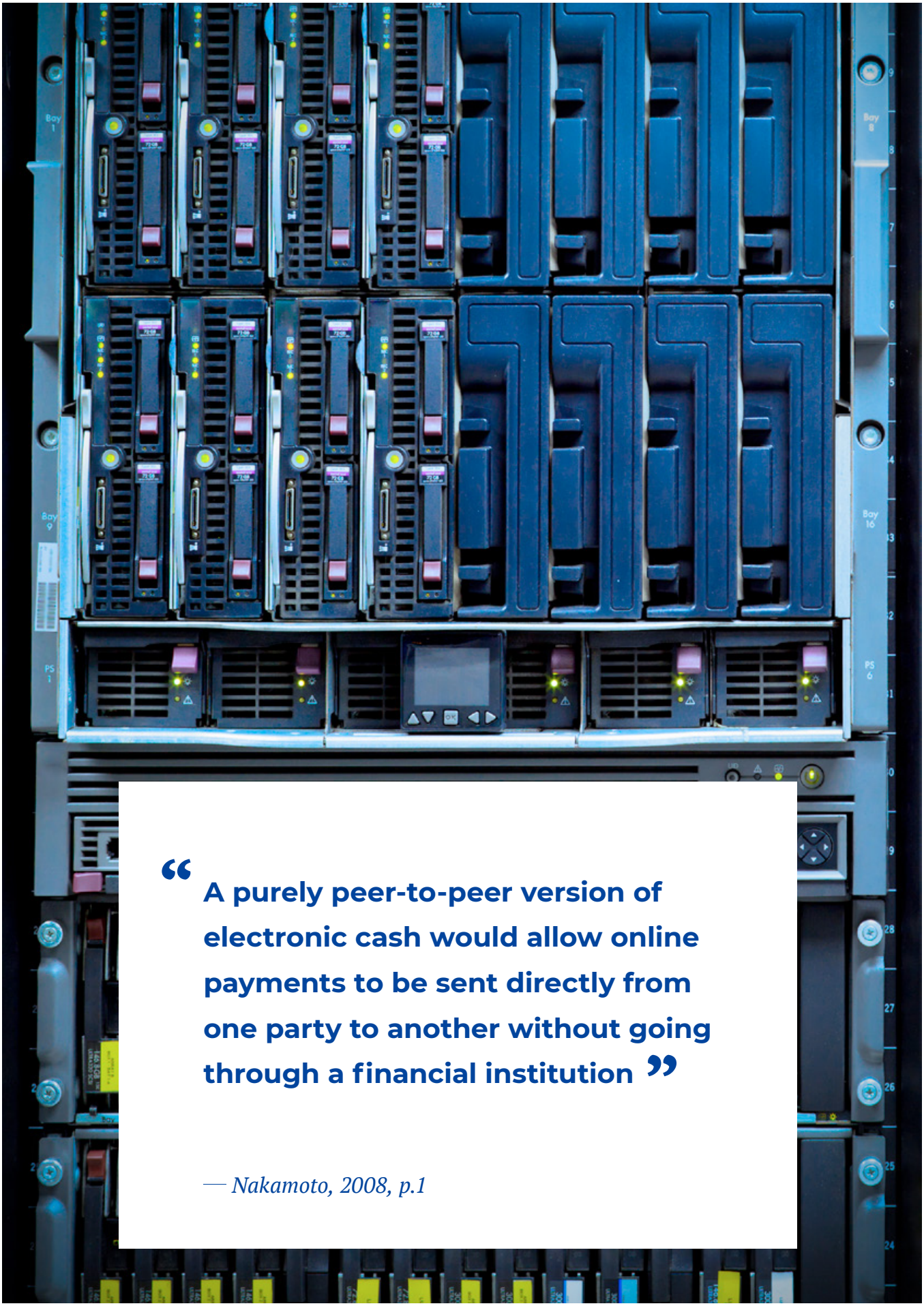
It follows that there are two basic properties that must be possessed by a form of cryptocurrency that is to function successfully as a community's money. First it must be accepted throughout the community as being a component of its system of value accounting and its use is governed by rights and obligations that serve to render it a general means of payment. Second, the money so formed must be trusted as a stable store of liquid value, grounding the property of it being a general form of purchasing power. The basic question to pursue, then, is whether systems based on forms of cryptocurrency can be devised wherein these two basic conditions are met.

If the latter are identified as the essential features of a successfully functioning money, the forgoing outline does also point to additional factors to consider. For example, all cases of money have been seen to take the form of a component of a community's system of value accounting closely related to other components of the same system. This being so, it may be the case that, in order to replace one form of community money with another, it is necessary to replace or transform other internally related components of the system of value accounting. For example, had the UK joined the European Monetary System, then not only would a different form of central bank debt have been involved, but the markers of money referred to as cash would have changed, as indeed would the unit of account (from pounds sterling to euros).

Forms of cryptocurrency do indeed come as (sub) systems in themselves. To consider the most familiar case, that of Bitcoin, it seems this label is indeed best used for a whole subsystem rather than any one component. In actual practice the term Bitcoin tends to be used variously: for the proposed system as a whole, a revised unit of account, and both a money position and its occupant (to the extent that they are distinguished).

An additional matter to consider is the nature of the community for which the money is intended. For, with all social phenomena being found to be community-relative, the possibilities of a form of cryptocurrency being accepted as money will depend on the specific community that is being considered. The central focus here is a national community like the UK. But it may be that forms of cryptocurrency can serve, and perhaps have already served, as money in some relatively small communities, especially illegal ones concerned with activities like the buying and selling of illicit goods online.

At present, general acceptance in modern national or international communities requires authorisation by central authorities. Fundamental to the monetary workings of such communities at present are banking systems that issue, seek to control/regulate, and endeavour to maintain a stable value of, money. Prima facie, developments like Bitcoin not only do not make any appeal to regulators and bankers, but the very reason for their design is to bypass them, to leave these institutional factors out of the value accounting system entirely. At the heart of it all is a desire to create a peer-to-peer electronic system of buying and selling that does not require the necessary mediation or intervention of any financial institution or other agency. As Nakamoto (2008) indicates in the opening sentence of the paper introducing bitcoin:



> **A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution**

— Nakamoto, 2008, p.1

To gain general acceptance, then, any such proposed cryptocurrency system must prove to be either 1) so widely popular or backed by organisations so powerful (as is presumably the intention, for example of Facebook's Libra, with the proposed launching of its own global cryptocurrency backed by significant assets) that the state or states involved is/are unable to resist it; or 2) adapted/oriented so as to work through existing financial and government institutions, in which case its use would not be, as originally intended, to displace existing institutions and processes but to facilitate the working of the existing systems in some way.

More can be said too on the task of achieving trust. As noted, an essential challenge is to achieve a situation wherein a form of cryptocurrency is trusted as a stable store of liquidity. This is the central form of trust to be achieved. However, other forms are essential too, albeit in ways, or for reasons, that depend on the particulars of the money form.

Certainly, all forms of money are open to abuse. Money in the form of a positioned valuable commodity was subject to clipping (the practice of cutting small pieces from, especially, gold or silver coins, with cut-off pieces often used to make counterfeit coins; this being a practice thought to be so undermining of the money process of Britain in the seventeenth century that clipping was deemed a matter of high treason, punishable by death). And, there are continuous (more or less successful) attempts to produce counterfeit versions of modern cash. Further, with the rise of electronic records of money, there are attempts to defraud through the duplication of these records. Without institutional intervention to prevent this under the current system, it would be possible for one and the same electronic record of money to be used to ground two or more expenditures (the so-called double spending problem). Cryptocurrencies involve peer-to-peer verified blockchain technologies designed just to avoid this sort of fraud. Community participants must trust that such efforts are usually successful.

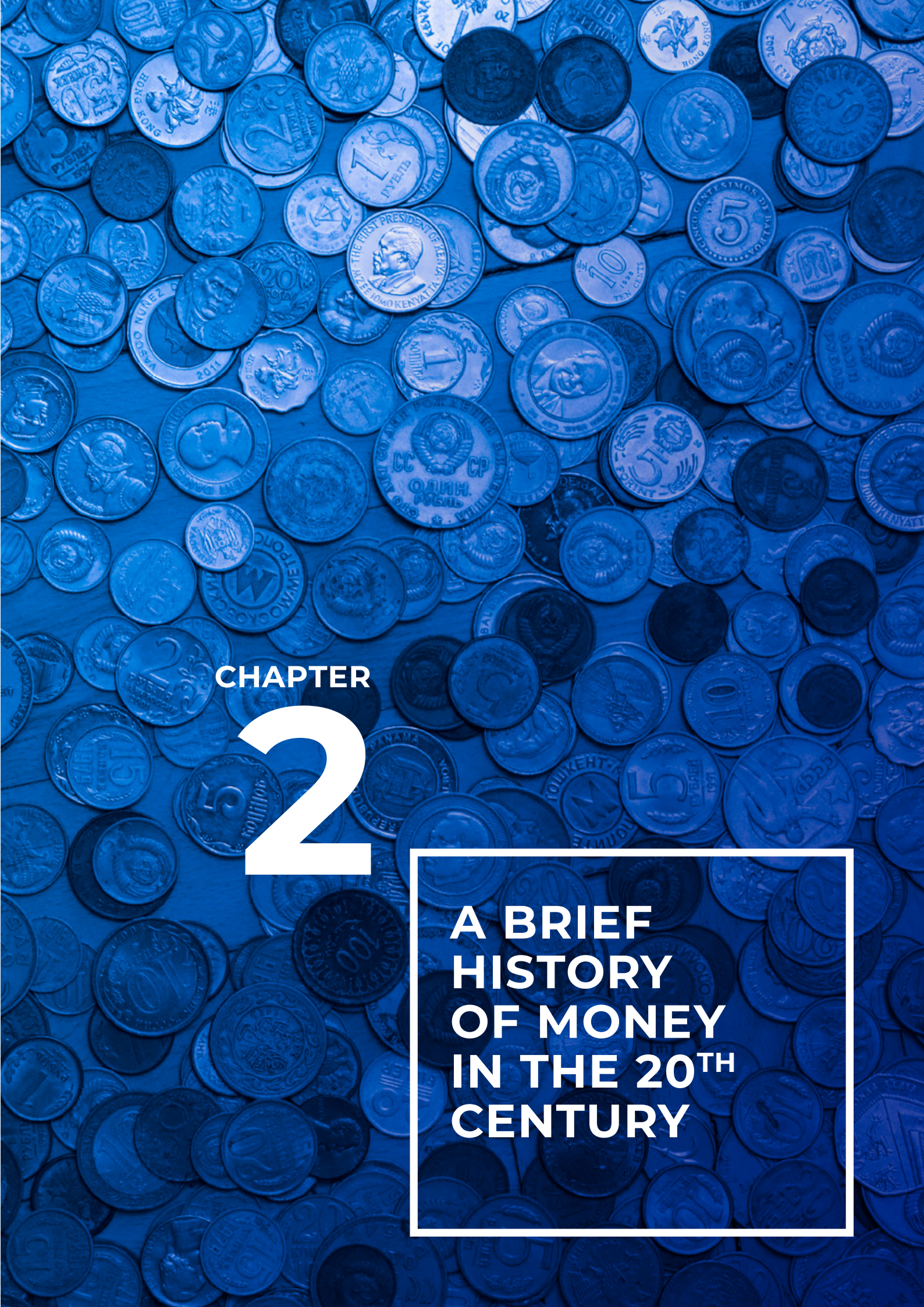
But these context-specific and contingent technical issues of trust generation aside, most significant of all is whatever the form of money developed, there must be a trust that the money so formed would prove to be a stable form of liquid value. In the case of a form of cryptocurrency, with no pre-existing record of attained trust (prior to its being positioned as money, were this to happen), and with potentially the displacement of all (state or bank) administrators who under the current system help stabilise a money's value through regulating actual transactions, the task of attaining the requisite sort and levels of trust would not be straightforward. Specifically, the task of creating a form of cryptocurrency that could be, and prior to positioning would be expected to be, a stable form of liquid value is a significant challenge.

One final matter that might be raised here is the question of whether more than one form, and if so, how many forms, of cryptocurrency could simultaneously be constituted as money. For, if one form managed to overcome all the obstacles including acceptance by the state (and so for example accepted by the state as a means of discharging tax debts) then presumably many forms could do so.

E. Conclusion

Money is commonly identified as that component of a community's system of value accounting that is accepted throughout the community to serve as a general means of payment and, when functioning successfully, as a general form of purchasing power. Its property of being a general means of payment is grounded in the money being accepted as a component of the system, governed by a specific set of rights and obligations that work precisely to ensures that it serves this function. Typically, this allocates to debtors the right to have their debts settled by handing over money (of the appropriate value) and to creditors the obligation to accept it. Money's property of possessing generalised purchasing power is grounded in the community's trust in it as a stable form of liquid value. Such trust, in part, has typically been achieved by positioning money a specific kind of thing that has the capacity to instil this trust. How this works in practice is contingent and varies over time.

The challenge, then, for those seeking to render form(s) of cryptocurrency as money lies both in getting it positioned as a legitimate general means of payment (governed by relevant rights and obligations ensuring this) and so also trusted in the sense that if positioned as money it can serve as a store of liquid value.

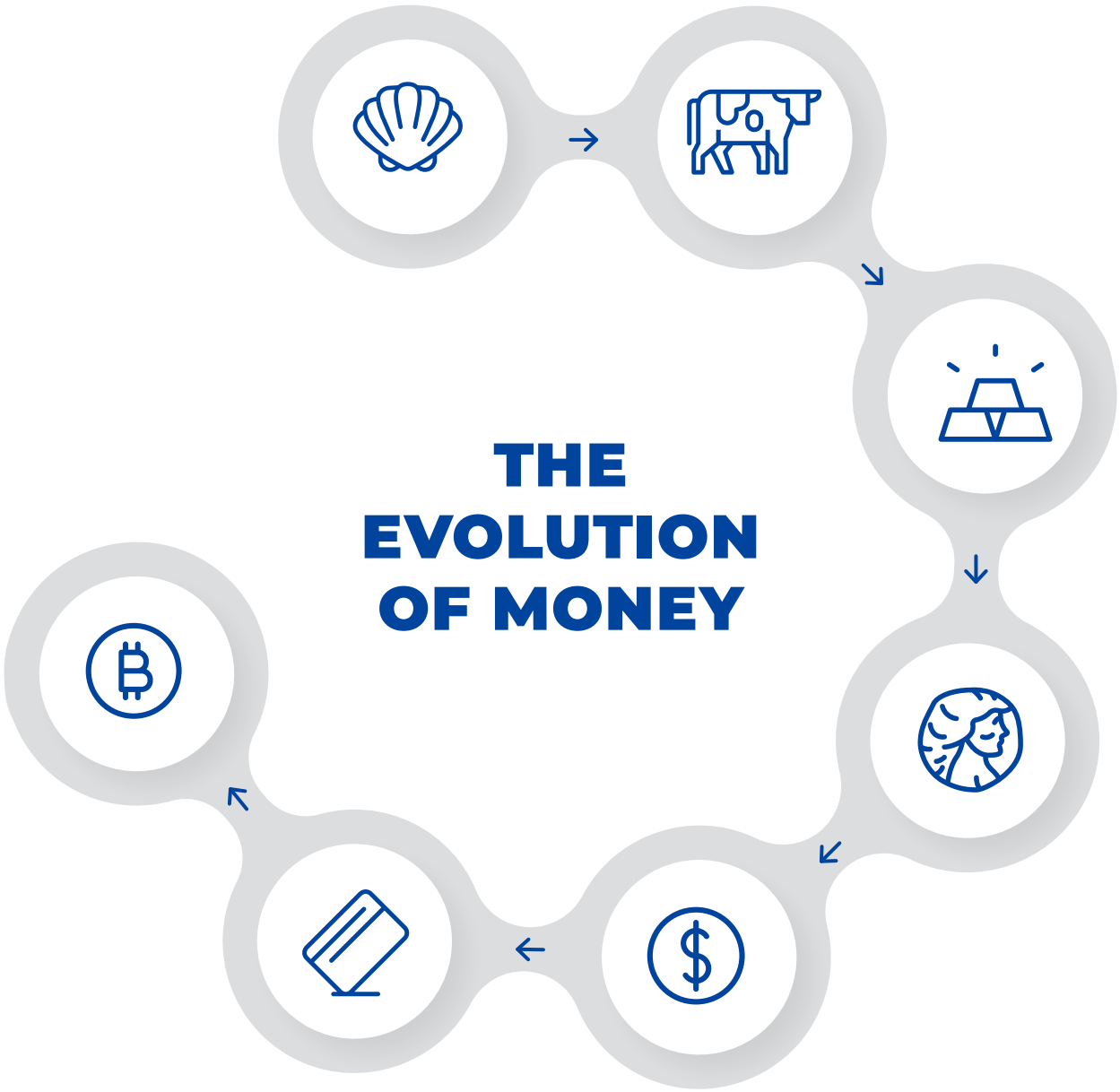


CHAPTER

2

A BRIEF HISTORY OF MONEY IN THE 20TH CENTURY

To understand money in the 21st century, it is helpful to understand its recent history. The twentieth century was notable in that it witnessed the collapse of two international monetary regimes. These are especially prevalent in the context of 'cryptocurrencies', which adopt aspects of the gold standard and revive arguments from the Austrian School of economics, notably Hayek's currency competition and Fisher's Chicago Plan.



Source: steemit.com, 2017.

A.The Gold Standard and the Adoption of Fiat Money

Money in the 20th century can broadly be divided into three parts: 1900–1933 when the international gold standard ensured that money was backed by the possession of physical gold, 1934-1971 when the dollar devaluation and the Bretton Woods System emerged, and 1972-1999 when fiat money was introduced and adopted (Mundell, 2000).

THE GOLD STANDARD ERA (1900–1933)

Under the gold standard, money is backed by the value of physical gold held by a country. Because a given amount of paper money can be converted into a fixed amount of an underlying physical asset, in this case gold, countries on the gold standard are prevented from increasing the supply of paper money in circulation without also increasing their holdings of gold reserves. This system was effective in preventing any irresponsible governments from taking advantage of their monopoly on money by printing too much of it. This allowed holders of that money to feel that the value of their paper money was 'insured', or 'collateralized' by the underlying gold that backed it.

While the gold standard was generally regarded as an essential source of economic trust and prosperity in the late 19th and early 20th century, deflation and depression in the 1930s revealed some of the defects of the inflexibilities in the gold standard. To understand why the gold standard was abandoned, it is important to understand the deflationary bias of the gold standard, which triggered deflation and depression in the 1930s. During the gold standard era, gold flowed across different countries. As a result, some countries possessed more gold than necessary for conversion against its total money supply, in accordance to the fixed conversion ratio (the gold-surplus countries), while others possessed less than required (the gold-deficit countries). Economic historian Peter Temin pointed out an asymmetry between gold-surplus and gold-deficit countries in their monetary response to gold flows (Temin, 1989).

Since gold-deficit countries had more money supply than could be supported by their gold reserve, they were forced to reduce their money supply and deflate; failing to do so could trigger people to worry about the convertibility of their domestic currency, scramble for gold, and would eventually lead to a complete loss of gold reserves in the country. Hence, gold-deficit countries faced plenty of incentive to deflate their currency to prevent devaluation. On the other hand, gold-surplus countries had insufficient money supply for conversion against their gold reserve. To prevent undervaluation of their domestic currency given the fixed conversion ratio, they were supposed to expand their money supply and inflate. The asymmetry was that no sanctions prevented gold-surplus countries from sterilizing gold inflows and accumulating gold reserves indefinitely.

Such asymmetric dynamics led to a deflationary bias in the gold standard. The bias was not obvious during the pre-war periods, since the gold standard was centred around the operations of Bank of England, which as a profit-making institution strived to avoid gold accumulation as opposed to interest-paying assets. However, WWI led to the decline of British economy. Meanwhile, as economic historian Barry Eichengreen showed, the two major gold-surplus countries of the interwar periods, the United States and France, did

little to avoid gold accumulation (Eichengreen, 1986). As a result, the deflationary bias of gold standard began to manifest itself by the end of 1920s.

THE GREAT DEPRESSION (1930S)

There exists a great deal of literature focusing on the gold standard as a mechanism that "turned an ordinary business downturn into the Great Depression." (Eichengreen and Temin, 1997, p.1) argue that "the most important barrier to actions that would have arrested or reversed the decline was the mentality of the gold standard" which "sharply restricted the range of actions they were willing to contemplate." The result of this cultural condition was "to transform a run-of-the-mill economic contraction into a Great Depression that changed the course of history" (Eichengreen and Temin, 2000, p.183). This was largely due to a reliance on the tested usefulness of past money and risk aversion when it came to new methods of creating and managing money.

Image Source: https://perspectivesofww2.weebly.com/before-wwii.html

Former chair of the Federal Reserve Ben Bernanke and economic historian Harold James proposed a financial mechanism in which deflation can trigger economic recession. For example, bank liabilities such as deposits are fixed in nominal terms, whereas bank assets such as debt instruments are fixed in real terms. In this case, deflation reduces the value of bank assets disproportionally and heightens pressure on the bank capital. In response, banks call in loans or refuse new ones, in turn worsening the positions of borrowers. But borrowers such as firms may lay off workers or curtail investments to improve their financial positions, contributing to an economic recession.[5] Unfortunately, the United States and other countries on the gold standard could not expand their money supplies to stimulate the economy. Such unbearable inflexibility led Great Britain to drop the gold standard in 1931, influencing many countries to follow shortly thereafter.

THE BRETTON WOODS ERA (1934-1971)

Influenced by economist and presidential advisor George Warren, the United States adopted a flexible exchange rate in 1933 for one year and devalued the dollar. It was expected that the lower exchange rate would boost the competitiveness of US products in the world economy, assisting economic recovery. The rise of the price of gold was also expected to raise the import price and thus the domestic price level, as a measure to counter the deflation problem. As a result, the wholesale price level in the United States did increase by almost 30 percent between 1933 and 1937. With the official price of gold raised by 69% to $35 an ounce, the United States restored pegging its currency to gold in April 1934.

In 1936, the United States, Britain, and France signed the Tripartite Accord establishing new rules for exchange rate management. These new arrangements were eventually ratified at Bretton Woods in 1944. The monetary system become a gold-dollar standard whereby the United States pegged the price of gold, and the rest of the world pegged their currencies to the dollar (Bordo, 1995). Consequently, the US dollar emerged as a key reserve currency for the rest of the world, substi-

5. See Bernanke and James 1990.

tuting for scarce gold as an international unit of account, medium of exchange, and store of value.

For the system to operate smoothly it was crucial that the United States maintain stable monetary and fiscal policy, which occurred until the 1960s. Based on Keynesian philosophy, the Kennedy and Johnson administrations prioritized increasing US growth and reducing unemployment below 4% using aggregate demand management policies by expanding the fiscal deficits. Meanwhile, the chairman of Federal Reserve William Martin, in the 1950s and 1960s prioritized cooperation with government administration over central bank independence. In response to the Kennedy tax cut, and the build-up of government expenditure for the Vietnam War and the Johnson's Great Society programs, the Federal Reserve deployed expansionary monetary policy to accommodate one half of the increase in the fiscal deficit. This led to the steady increase in US inflation rate in the 1960s.

Martin pursued a contractionary monetary policy right before he left the Federal Reserve, which contributed to a recession during the Nixon administration in 1970 and soaring unemployment. Economic historian Michael Bordo argued that Nixon's perception of why he lost the 1960 election to John Kennedy had triggered his paranoia about the political consequences of rising unemployment. This in turn led Nixon to apply immense political pressure onto the new Chairman of Federal Reserve Arthur Burns to reverse Martin's policies and expand money growth in 1971 (Bordo, 2018). The rekindled US inflation contributed to the undervaluation of gold. Under the significant balance of payment deficit of the United States since WWII, Nixon feared that the British would convert their dollar holdings into gold and threaten the US gold reserve. As a result, Nixon announced his New Economic Policy on 15 August 1971, closing the US gold window and effectively declaring the death of the Bretton Woods System.

Image Source: http://content.time.com/time/business/article/0,8599,1852254,00.html

THE FIAT MONEY ERA (1972-PRESENT)

Fiat money is a medium of exchange that is neither a commercial commodity nor title to any such commodity. It is "not convertible by law into anything other than itself and has no fixed value in terms of an objective standard" (Keynes, 1930). The value of fiat money is derived from a premium based on a collective trust in the continued existence and stability of the entity issuing it. In simple terms, the difference between the cost of producing money and its value to people who own it is the trust they place in it.

The fiat money era solved many of the problems of the gold standard era by allowing policymakers greater levels of flexibility to adapt to economic circumstances and/or influence the economic decision making of households and corporations. The adoption of fiat currencies effectively expanded the central banker's toolbox to allow adjustment of the supply of money through interest rates and capital reserve requirements.

Nevertheless, the fiat money era also opened opportunities for abuse by irresponsible policymakers – under the gold standard, policymakers were forced to demonstrate ownership of an underlying asset (gold) that could act as collateral against the paper money they printed. Fiat money, however, is uncollateralized and thus is only as valuable as people believe it to be. This potential for abuse was recently summarized by the Governor of the Bank of England:

> **“Most forms of money, past and present, have nominal values that far exceed their intrinsic ones. And this gap has meant that money has a long and sorry history of debasement. Over the centuries, forms of private money, such as the notes issued by American banks during the free banking of the 19th century, have inevitably succumbed to oversupply and eventual collapse.”**

– Mark Carney, 2018 [6]

Episodes of extreme inflation caused by irresponsible policymakers are dotted throughout history, often causing long-lasting economic hardships on a country’s population, due to the irresponsible printing of new money (often to finance government debt). A few well-documented cases are shown below (Zimbabwe) and to the right (Mexico, Brazil, Venezuela).

ZIMBABWE’S HYPERINFLATION

Date	Month-over-month inflation rate (%)	Year-over-year inflation rate (%)
March 2007	50.54	2,200.20
April 2007	100.7	03,713.90
May 2007	55.40	4,530.00
June 2007	86.20	7,251.10
July 2007	31.60	7,634.80
August 2007	11.80	6,592.80
September 2007	38.70	7,982.10
October 2007	135.62	14,840.65
November 2007	131.42	26,470.78
December 2007	240.06	66,212.30
January 2008	120.83	100,580.16
February 2008	125.86	164,900.29
March 2008	281.29	417,823.13
April 2008	212.54	650,599.00
May 2008	433.40	2,233,713.43
June 2008	839.30	11,268,758.90
July 2008	2,600.24	231,150,888.87
August 2008	3,190.00	9,690,000,000.00
September 2008	12,400.00	471,000,000,000.00
October 2008	690,000,000.00	3,840,000,000,000,000,000.0014
November 2008	79,600,000,000.00	89,700,000,000,000,000,000,000.00

Notes: The Reserve Bank of Zimbabwe reported inflation rates for March2007–July 2008. The authors calculated rates for August 2008–14 November 2008. Sources: Reserve Bank of Zimbabwe (2008a) and authors’ calculations.

Source: Hanke and Kwok, 2009.

6. Speech given by Mark Carney, Governor of the Bank of England to the inaugural Scottish Economics Conference, Edinburgh University (2 March 2018).

TABLE 1

Select Episode of High Inflation

INFLATION IN MEXICO (1981 – 1995)

Year	% change (inflation)	CPI (1980=100)
1980	n/a	100
1981	27.414	128.125
1982	98.9	254.6875
1983	80.701	459.375
1984	59.184	731.25
1985	63.739	1196.875
1986	105.755	2464.063
1987	159.174	6384.375
1988	51.657	9682.813
1989	19.697	11590.63
1990	29.93	15059.38
1991	18.795	17890.63
1992	11.938	20026.56
1993	8.009	21629.69
1994	7.051	23154.69
1995	51.966	35187.5

INFLATION IN BRAZIL (1981 – 1995)

Year	% change (inflation)	CPI (1980=100)
1980	n/a	100
1981	95.66	195.66
1982	104.80	400.71
1983	164.00	1057.87
1984	215.28	3335.25
1985	242.25	11414.84
1986	79.66	20507.49
1987	363.41	95034.50
1988	980.22	1026582.74
1989	1972.91	21280159.75
1990	1620.97	366224414.23
1991	472.69	2097313107.45
1992	1119.09	25568186003.62
1993	2477.15	658930002302.86
1994	916.43	6697581091643.00
1995	22.41	8198434012165.97

INFLATION IN VENEZUELA (2010 – 2024) [7]

Year	% change (inflation)	CPI (2010=100)
2010	27.36	100.00
2011	28.987	128.99
2012	19.527	154.17
2013	52.662	235.37
2014	64.687	387.62
2015	159.693	1006.61
2016	302.637	4053.00
2017	968.95	43324.58
2018*	1,555,146*	673803764
2019*	10,000,000*	67381050226261
2020*	10,000,000*	6738172403899950000
2021*	10,000,000*	673823978584751000000000
2022*	10,000,000*	67383071684689000000000000000
2023*	10,000,000*	673837455176407000000000000000000000
2024*	10,000,000*	6738441935509620000000000000000000000000

*Forecast

Source: IMF World Economic Outlook, April, 2019.

The global adoption of fiat currency, together with free capital mobility and diminishing cross-border information and transaction costs, also paved the way for the modern process of currency competition anticipated by the Nobel laureate economist Friedrich Hayek.

7. Rebased by author to reference year.

B. Currency Competition and the Chicago Plan

HAYEK AND CURRENCY COMPETITION

Throughout the 20th century, money creation remained a monopoly of government/central banks and commercial banks. History has taught us that a monopoly on money coupled with irresponsible policymakers and/or commercial bankers under a fiat currency monetary system can create dire consequences for the populations they govern. Hayek argued that competition would alleviate this problem by producing "good money". This was attributed to the idea that competition is a discovery process with constant experimentation in which various improvements are offered to users of money (Hayek, 1978b). Of necessity, such improvements are subjective and dependent on changeable market opinions and demands. As a result, economist Anthony Endres suggests that there may be no point in drawing a sharp distinction between what is money and what is not; competition over different forms of monies should result in discoveries, modifications and service innovations that no one currency producer anticipates or intends (Endres, 2009). It would be unconvincing to suppose that currency was invented in a manner that determines its properties and use for all times and places. This viewpoint led Hayek to question the usefulness of any international agreement to adopt a monetary management system:

> **"Why should we not let people choose freely what money they want to use? … the best thing we could wish governments to do is for, say, all the governments of the Atlantic Community, to bind themselves mutually not to place nay restrictions on the free use within their territories of an another's – or any other – currencies, including the purchase and sale at any price the parties decide upon, or on their use as accounting units."**
>
> — *Hayek, 1978a.*

Since currencies issued by governments pursuing responsible monetary policy would tend to displace gradually those of a less-reliable character, competition would "impose the most effective discipline on governments" for the appropriate management of the quantity of currency in circulation (Hayek, 1978a, p.21), protecting money from political manipulations such as those of Nixon and Burns. To avoid the inflationary bias inherent in any international monetary policy coordination, Hayek suggested that national currencies should be related by a system of flexible, market-determined exchange rates, and individuals should be allowed to substitute between various currencies without government prohibition. As evidence, economist Benjamin Craig showed that the Russian monetary authority in the 1990s was induced to target a lower level of inflation as dollars were increasingly held and used illegally by residents (Craig, 1996).

As every currency is potentially capable of playing a role as an international vehicle for quoting prices and settling trades across national borders, Harvard political economist Benjamin Friedman sees that the diminishing effectiveness of national monetary policies are inevitable, if not desirable. Diminishing loyalty to any single central-bank-issued money, the growth of non-bank credit, and technological advances are weakening the monetary control of central banks (Friedman, 1999). In recent years we have already witnessed the emergence of various global digital currencies, in line with the claim of economic historian Charles Kindleberger who argued that the market will create additional money to suit it's needs and where official sources limit it's supply, the market will react by producing more (Kindlegerger, 1989)." It seems the discovery process of currency competition envisioned by Hayek has been in full force, and we are to expect more discoveries from private innovation in the dynamic process of opinion formation in the market.

Critics of Hayek have argued that bad money will drive out good money. This has become known as Gresham's Law, which argues that when two forms of commodity monies are in circulation, and both are accepted as legal tender with the same face value, the intrinsically more valuable money will gradually disappear from circulation as people hoard their 'good money' and spend their 'bad money'. The principle was demonstrated in the United States when older half dollar coins with 90% silver were hoarded and melted down by the public after the government had introduced newer ones with only 40% silver in 1965. These newer coins eventually also disappeared from circulation when the government gave up including any silver in half dollar coins in 1971. This shows that legal tender laws could motivate buyers/debtors to offer only money with the lowest commodity value (bad money), since sellers/creditors are required by laws to accept such money at face value.

In absence of effective legal tender laws, Gresham's Law could also work in reverse. This was demonstrated in post-WW1 Germany when consumers fled from cash to hard assets as circulating medium of exchange after the hyper-inflation in 1922 (a similar trend was observed during the hyper-inflation events in Zimbabwe). Given the choice of what money to accept, sellers/creditors can now demand only money with the highest long-term value, further reducing the acceptability and value of bad money. This coincides with Hayek's insight

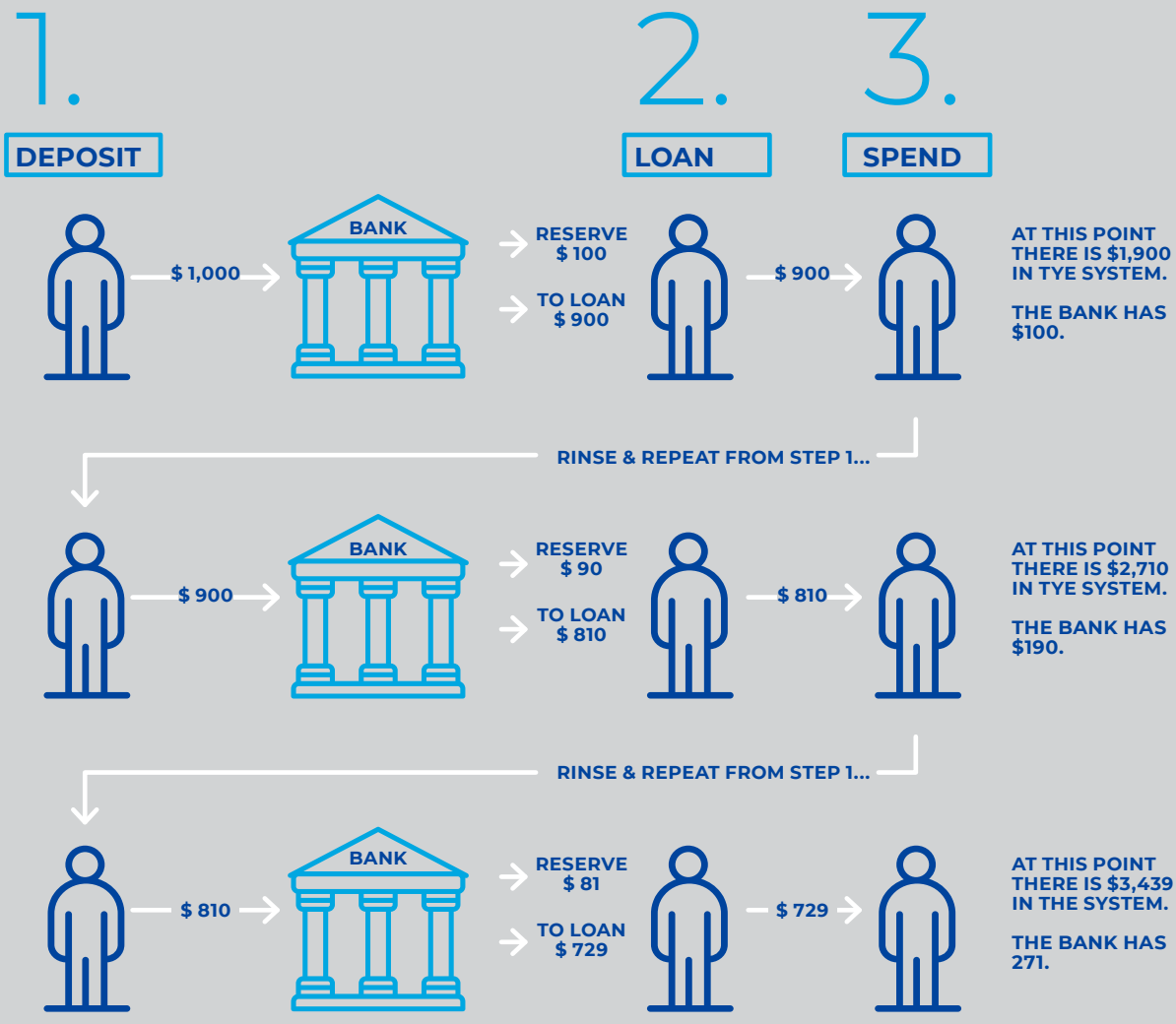
that when government does not intervene in people's choice of money in transaction, competition naturally produces good money. Robert Mundell therefore proposes modifying Gresham's Law into "bad money drives out good if they exchange for the same price." (Mundell, 1998)

THE FRACTIONAL RESERVE SYSTEM

As the international monetary system evolved in the 20th century, fractional reserve banking has remained widespread. In fact the practice dates as far back as the 1300s, [8] but is not well understood by the public or academic textbooks.

The fractional reserve system is a banking system in which all depository institutions-commercial banks, credit unions and other banks—are required to maintain reserves against transaction deposits, which include demand deposits, negotiable order of withdrawal accounts, and other highly liquid funds. Reserves against these deposits can take the form either of currency on hand (vault cash) or balances at the Central Bank.

FIGURE 1 **The Basic Fractional Reserve Banking Cycle**



Source: altexploit.wordpress.com, 2017.

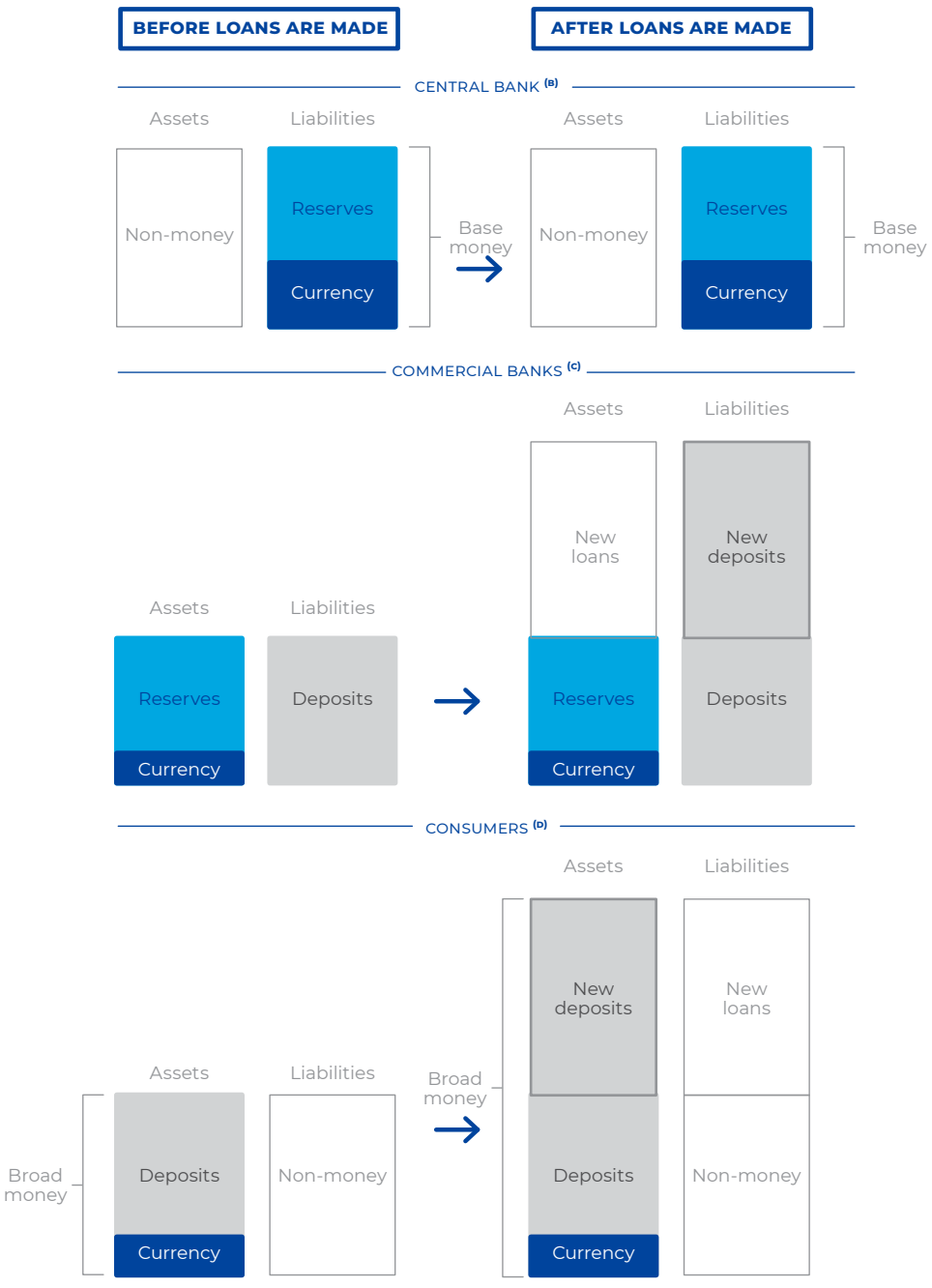
8. See Bardi and Peruzzi, 1345; Pisano and Tiepolo, 1584; Bank of Amsterdam, 1791; Goldsmiths, 1630.

Fractional reserve banking can be simply explained using the scenario to the left where 1,000 units of central bank issued 'base money' is deposited at a commercial bank. Where the bank is required to hold a percentage (10 in this case) of their loan liabilities in reserves, they can loan out 900 units backed by a 100-unit deposit (first row). If we suppose that the household taking the loan purchases a house from another household, the house seller will likely deposit those funds back in the bank. In this case, the bank can again lend out 90% of those new deposits (second row). As this cycle continues, the amount of 'broad money' in the economy grows significantly (second and third row). In the last row, there is now 3,439 units of total money in the economy from the initial 1,000 units in central bank-issued money.

To give a practical example, in the UK about 97% of the broad money supply is made up of uncollateralized loans, with only about 3% supported by actual cash. This system comes with both advantages (more liquidity for small businesses and households) and disadvantages (the moral hazard problem and boom-bust cycles). Central banks still maintain control over the supply of money but this is through a combination of influencing interest rates and setting capital reserve requirements and adequacy ratios.

FIGURE 2

Money Creation by the aggregate banking sector making additional loans [A]



(A) *Balance sheets are highly stylised for ease of exposition: the quantities of each type of money shown do not correspond to the quantities actually held on each sector's balance sheet.*

(B) *Central bank balance sheet only shows base money liabilities and the corresponding assets. In practice the central bank holds other non-money liabilities. Its non-monetary assets are mostly made up of government debt. Although that government debt is actually held by the Bank of England Asset Purchase Facility, so does not appear directly on the balance sheet.*

(C) *Commercial banks' balance sheets only show money assets and liabilities before any loans are made.*

Source: Mcleay et al., 2014.

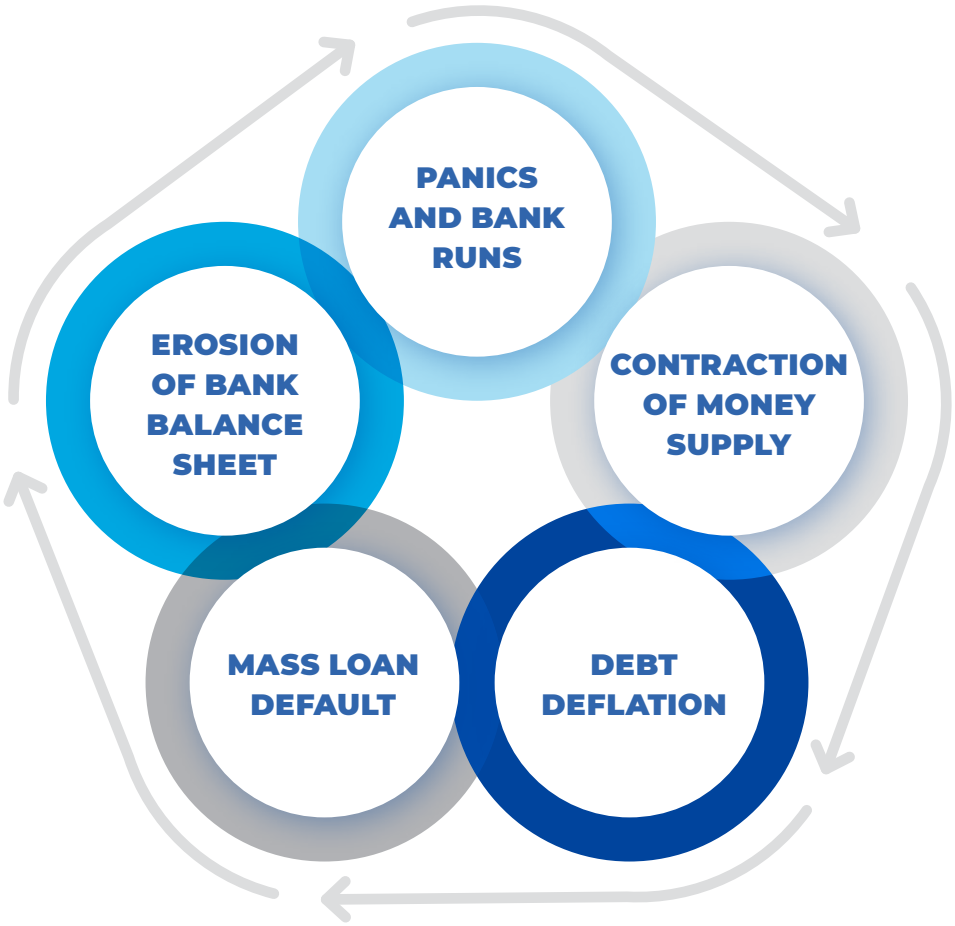
> **“The ultimate constraint on money creation is monetary policy. By influencing the level of interest rates in the economy, the Bank of England’s monetary policy affects how much households and companies want to borrow. This occurs both directly, through influencing the loan rates charged by banks, but also indirectly through the overall effect of monetary policy on economic activity in the economy. As a result, the Bank of England is able to ensure that money growth is consistent with its objective of low and stable inflation.”**

— *Mcleay et al., 2014.*

Much like the move from the gold standard to fiat money, fractional reserve banking relies on an uncollateralized reliance on public trust – as long as there are no runs on the bank, fractional reserve banking can function well, with commercial banks creating new money through uncollateralized loans to finance innovative new companies. The flexibility in creating loans and money facilitates business borrowing and investment, hence further expanding economic activities during booms. However, fractional reserve banking is a double-edged sword: the very same flexibility can also aggravate economic contraction during busts.

To understand the mechanism, notice that money (demand deposits) in a fractional reserve banking system is either backed up by cash or created through bank loans. Whenever a bank loan is repaid, the total amount of cash remains unchanged. A reduction in bank loan hence implies a reduction of money supply in the system. In other words, bank loan reduction – either by repayment or declaration as bad debt - destroys money.

The negative effect of such monetary contraction channels was demonstrated in the United States during the Great Depression. As the stock market crash in October 1929 made it difficult for businesses to repay their loans, the balance sheets of many US banks eroded. To satisfy the legal reserve requirement, these banks had to call loans to reduce their demand deposits, which led to even more bad debt, given many businesses were already experiencing financial difficulty. As a result, panics spread and generated the first wave of bank runs in late 1930, with 352 banks failing in December 1930 alone.



Through the mechanism explained above, money supply contracted substantially, leading to debt deflation and further bad debt. The contagion of fear and propagation of bank runs continued until Spring of 1933, in total cutting the price level in the United States by half and destroying eight billion dollars or one-third of demand deposits in the United States. Having observed this vicious cycle during the Great Depression, Nobel laureate economist Irving Fisher proposed the Chicago Plan as a way insure 100% of reserves.

THE CHICAGO PLAN

The origins of the Chicago Plan can be attributed back to the United Kingdom where the 1921 Nobel Prize winner in chemistry, Frederick Soddy shifted his focus to the inefficiencies and unfairness inherent in fractional reserve systems of 'virtual wealth' (Soddy, 1933). The ideas of Soddy were embraced by Professor Frank Knight in 1927 at the University of Chicago. In practice, however, the challenges of fractional reserve banking are made clear only during times of panic or financial crises. In the aftermath of the Great Depression, a significant conglomerate of University of Chicago economists, along with prominent monetary economist Irvin Fisher at Yale, supported Knight's proposals to reform the financial system and sent a detailed memorandum to President Roosevelt in November 1933 (see Simons et al.,1933). Following the Great Depression, Fisher envisioned the Chicago Plan as "a way to use monetary policy to affect debtor-creditor relations through reflation, in an environment where, in his opinion, over-indebtedness had become a major source of crises for the economy". (Benes and Kumhof, 2012). Fisher was a pioneer in advocating for the requirement of a 100% cash reserve behind all demand deposits, a proposal subsequently known as the Chicago Plan (Fisher, 1936; Simons, 1946). Fisher observed that the volume of demand deposits was highly unstable because of the fractional reserve banking system. By eliminat-

ing the possibility of bank runs, he believed the proposal would speedily and permanently prevent an economic recession from spiralling into depression by i) increasing control of sudden increases and contractions of bank credit and of the supply of bank-created money, ii) eliminating the possibility of bank runs, iii) dramatically reducing the net public debt and iv) dramatically reducing private debt (as money creation would no longer require simultaneous debt creation) (see Tobin, 1985; Minsky, 1992, 1994; Benes and Kumhof, 2012).

In simple terms, under the Chicago Plan, all demand deposits held by commercial banks must be matched by an underlying asset such as cash. This means that these banks cannot lend out customers' demand deposits as they do under the fractional reserve system, which would significantly decrease liquidity in 100%-backed reserve countries (for example 97% of money in the UK would need to be replaced with central bank base money). As banks can only lend against proven reserves, the risk of bank runs would vanish, so that banks need not call loans during economic downturn to worsen the liquidity of businesses. On top of resolving the coordination failure of banks during bad times, banks could also benefit from such arrangements, as more savings and time deposits would be brought to banks due to freedom of the economy from great booms and depressions.

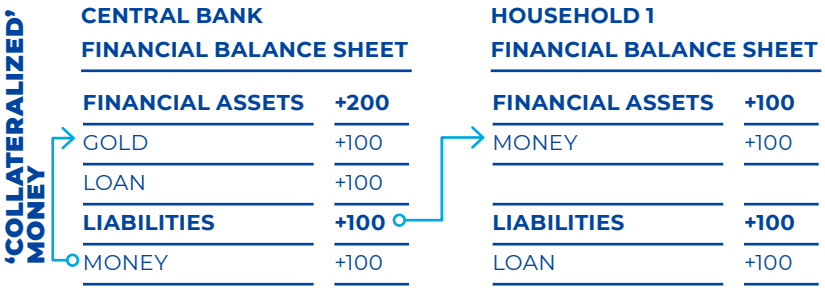
More importantly, the government could regain its sovereign power over money under the Chicago Plan. By prohibiting banks from manufacturing the money they lend, but still allowing banks to lend money as they please, the government could nationalize money without nationalizing banking. With a 100% cash reserve requirement, all the money on deposits now fully belong to the depositors, so that banks act merely as their trustees or custodians. The absence of leverage in the Chicago Plan, Fisher believed, could therefore prevent the freezing of loans during a depression, and effectively eliminate the management and domination of industry by banks during bad times. In the words of Martin Wolf, chief economics commentator at the Finance Times, this will end the "too big to fail" for banking (Wolf, 2014).

C. How does this fit into the era of digital currencies?

We can get a better idea of the role that trust has come to play in money by examining four simple scenarios from a balance sheet perspective.

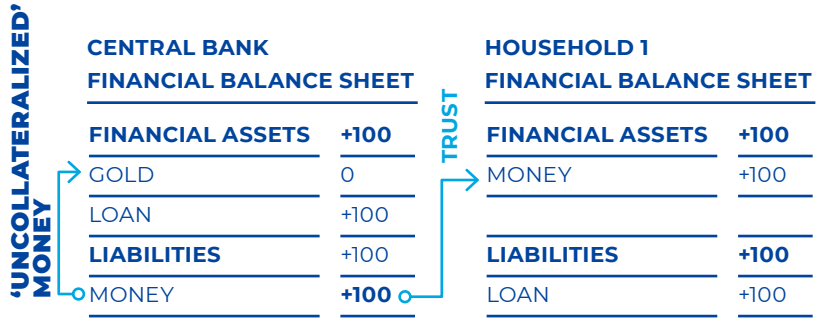
The first scenario involves a transaction between the central bank and household under the gold standard (or any other asset-backed money such as stablecoins). Because paper money is backed by physical gold (or another valuable asset), this scenario does not require households to have an implicit trust in the central bank, as each unit they borrow is backed by a unit of physical gold of the same value.

1. CENTRAL BANK PRINTS 100 UNITS BACKED BY 100 UNITS OF GOLD RESERVES AND PROVIDES A LOAN TO HOUSEHOLD 1



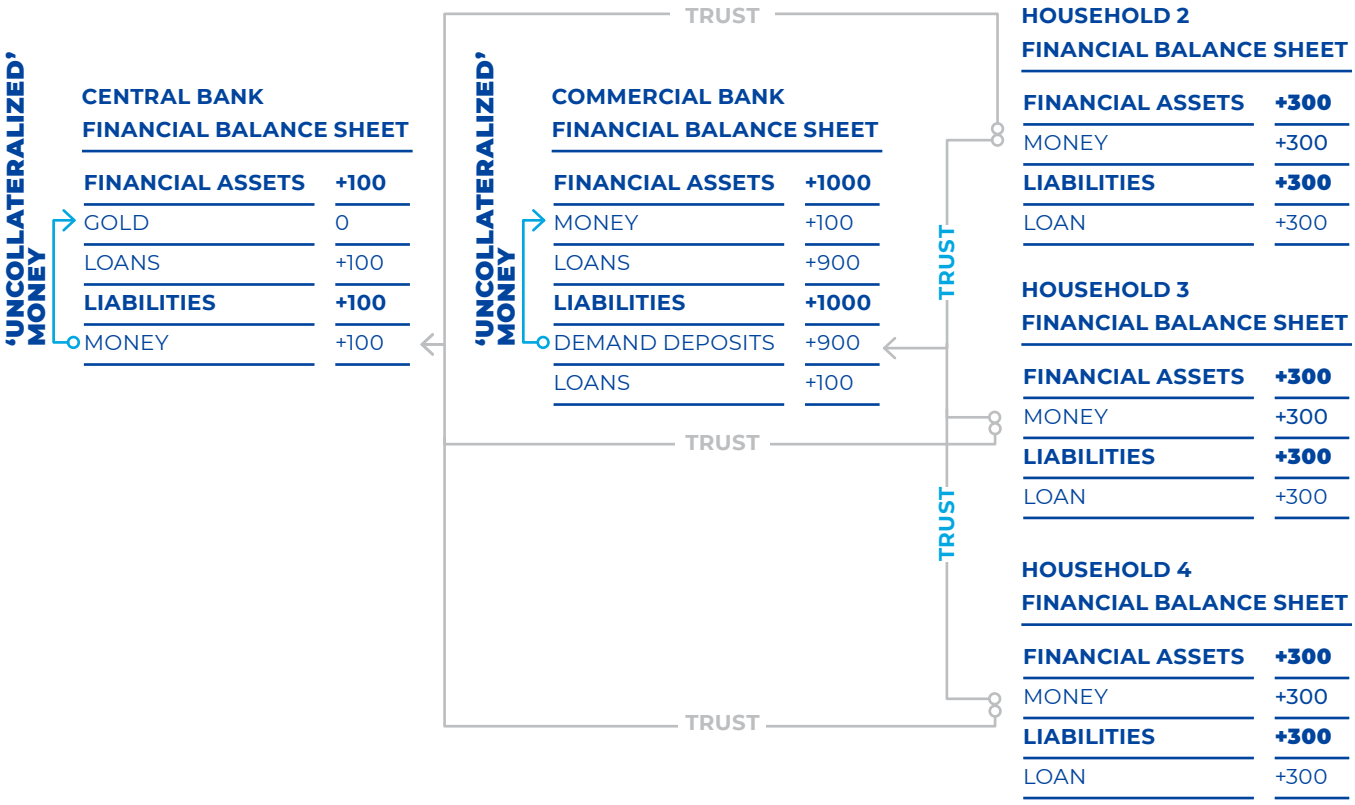
The second scenario involves a similar transaction between the central bank and a household under fiat money. Because paper money is not backed by physical gold, there is now a difference between the cost of producing the paper money and the value to its users. This creates a premium (seignorage) which requires a relationship of trust and confidence in the issuing authority.

2. CENTRAL BANK PRINTS 100 UNITS FIAT CURRENCY AND PROVIDES A LOAN TO HOUSEHOLD 1



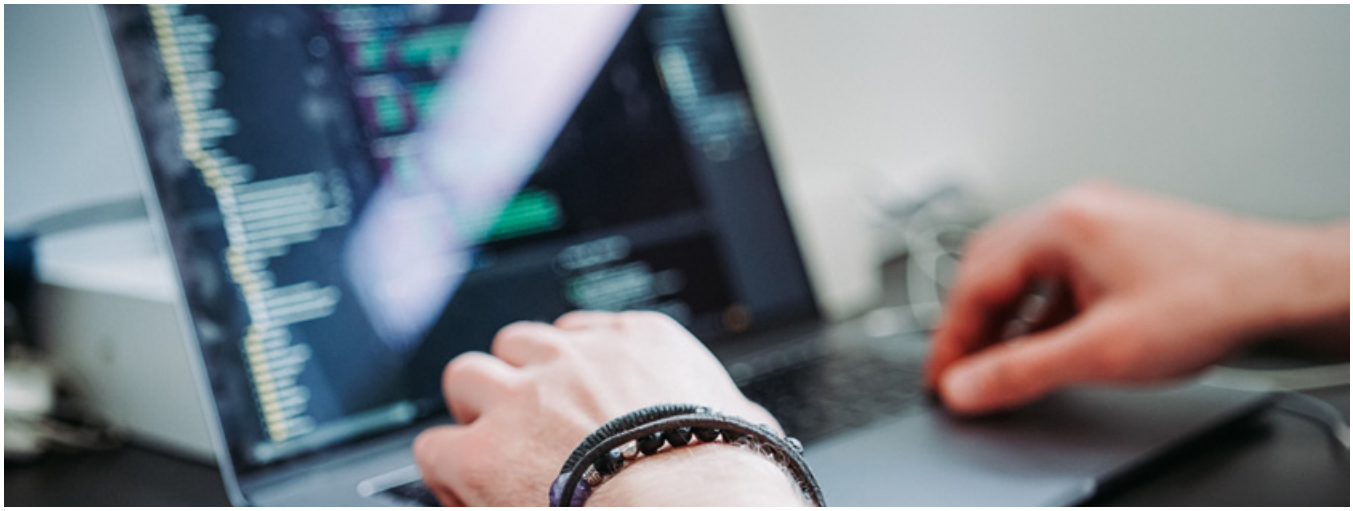
In the third more realistic scenario, the central bank lends 100 in fiat currency to a commercial bank who, under fractional reserve banking, can lend out more money than they hold on deposits (say 90%). In this case there now exists several relationships of trust between commercial banks, depositors, borrowers, and the central bank.

3. COMMERCIAL BANK BORROWS 100 UNITS FROM CB AND LENDS 900 TO HOUSEHOLDS 2, 3, AND 4

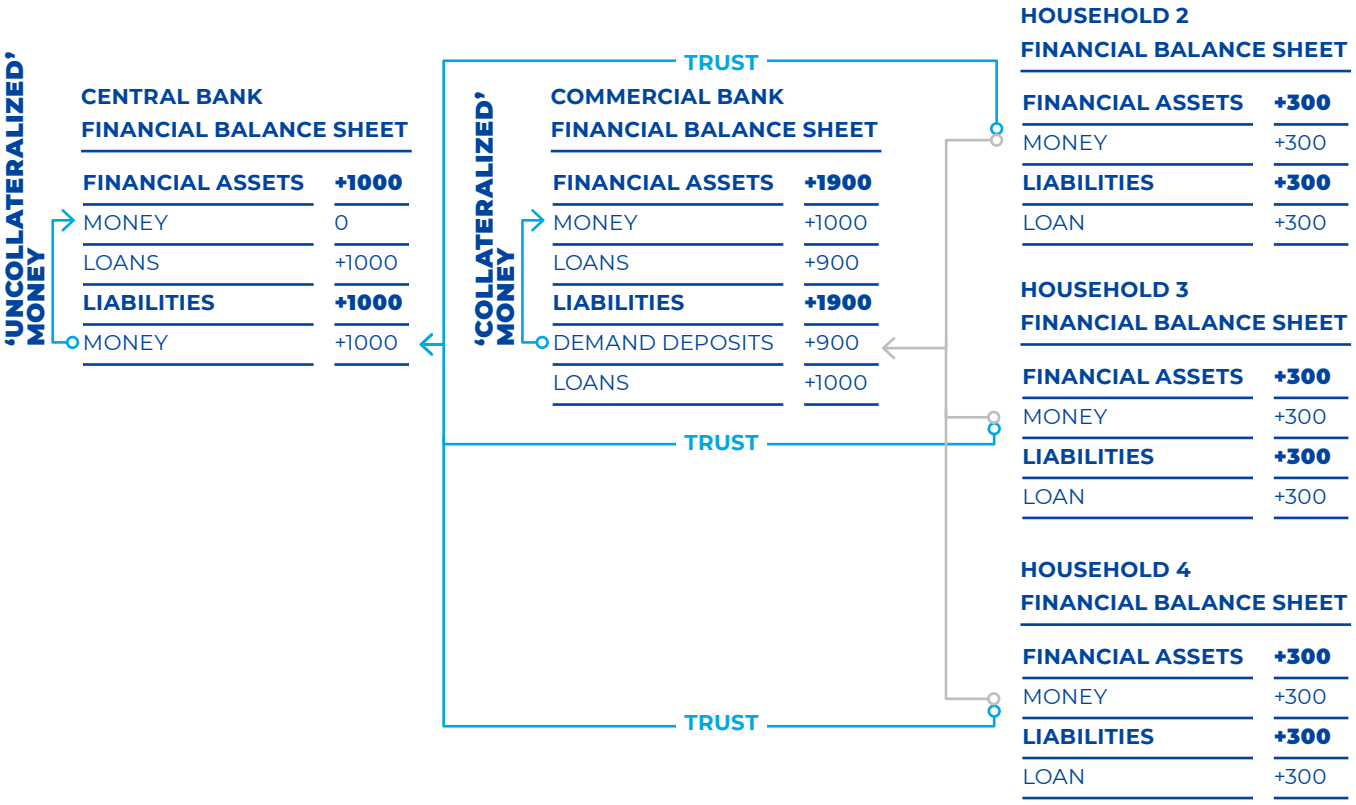


At this point, there exists 100 units in central bank (narrow/outer) money, which requires a relationship of trust between the central bank and households, and 900 in commercial bank (inner) money which requires a relationship of trust between households and commercial banks. As noted above, the only time where the vulnerabilities are exposed in the fiat currency fractional reserve system is when trust in these institutions erodes.

Lastly, in scenario 4 we can impose the Chicago Plan restrictions on scenario 3, which now requires commercial banks to hold an equivalent value of assets to their liabilities (demand deposits). In this case, commercial banks would need to borrow at least 900 units from the central banks in order to fulfil the 100% reserve requirement.

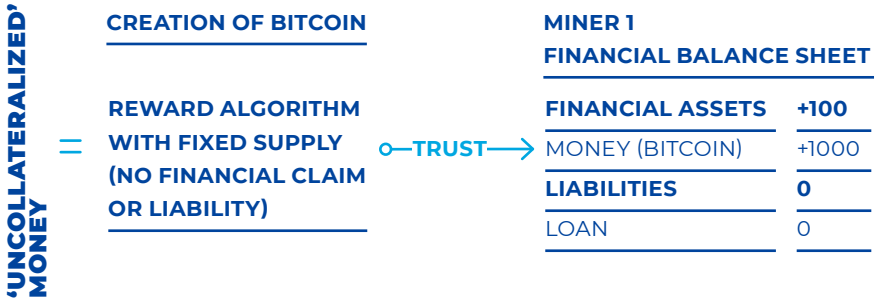


4. COMMERCIAL BANK BORROWS 1000 UNITS FROM CB AND LENDS 900 UNITS TO HOUSEHOLDS 2, 3, AND 4 UNDER CHICAGO PLAN



Comparing this with a peer-to-peer issued cryptocurrency, like Bitcoin, in scenario 5 no liability is created when a bitcoin is mined. For example, the supply of bitcoin is increased by rewarding those who successfully validate transactions making it a transaction and not a financial contract (as was the case with bank money). The issuer is not an institution or entity and the currency is not backed by any authority. This creates a challenge when accounting for Bitcoin. One option is to treat it like monetary gold, which is the only existing financial asset with no liability. But as noted by the BOE,[9] gold is a tangible asset that you can physically store.

5. BITCOIN MINER 1 RECEIVES 100 UNITS FOR SOLVING A BLOCK



A second option, shown in scenario 6, used by stablecoins (i.e. Libra), is to fully collateralize all digital money with other liquid assets such as high quality government and corporate bonds, in which case the scenario is similar to that under the gold standard from scenario 1, where there is no need for a relationship of trust to be created given the backing of that digital currency by other high quality financial assets.

9. See the Economics of Digital Currencies – BOE Quarterly Bulletin 2014 Q3.

6. STABLECOIN CRYPTOCURRENCY ISSUER CREATES 100 UNITS BACKED BY 100 UNITS OF UNDERLYING ASSETS AND SELLS TO HOUSEHOLD 1

'COLLATERALIZED' MONEY

DIGITAL CURRENCY ISSUER FINANCIAL BALANCE SHEET	
FINANCIAL ASSETS	**+200**
UNDERLYING ASSETS	+100
LOAN	+100
LIABILITIES	**+100**
MONEY	+100

HOUSEHOLD 1 FINANCIAL BALANCE SHEET	
FINANCIAL ASSETS	**+100**
MONEY	+100
LIABILITIES	**+100**
LOAN	+100

Once cryptocurrencies have been acquired, users do not need rely on trust between themselves or any institution to ensure its value because of the collective security embedded in the blockchain technology. This means that miner 1 can make transactions with miner 2 without any requirement that they trust each other. (see scenario 7 below) Again, this is similar to trading with physical gold (or under the gold standard) but does not require a physical validation of the legitimacy of the gold.

7. CRYPTOCURRENCY OWNER 1 MAKES TRANSACTION OF 100 WITH OTHER NETWORK MEMBER 2

'COLLATERALIZED' MONEY

DIGITAL CURRENCY ISSUER FINANCIAL BALANCE SHEET	
FINANCIAL ASSETS	**+200**
UNDERLYING ASSETS	+100
LOAN	+100
LIABILITIES	**+100**
MONEY	+100

HOUSEHOLD 1 FINANCIAL BALANCE SHEET	
FINANCIAL ASSETS	**+100**
MONEY	+100
LIABILITIES	**+100**
LOAN	+100

Note that cryptocurrencies in this example are limited to transactions and not financial contracts. This means that no financial relationships are created and no liabilities will exist on anyone's balance sheet. In the case of Bitcoin, these tokens are created by a mining reward algorithm and backed by the collective pool of people who own it. If that collective pool loses trust in bitcoin, its value diminishes. In the case of stablecoins, the collective pool is assured of the value of their currency by the holding of high-quality assets of equivalent value.

In summary the leveraged way in which money is currently being created has the potential to (again) destabilize financial systems only when trust in those institutions erodes. These destabilizations often lead to short revivals of Austrian school ideas regarding the role of money and banking in society (for example, Fishers seminal paper following the Great Depression). It is likely no coincidence that the Nakamoto (2008) paper emerged at the same time as the most recent financial crisis was occurring. In fact, one of the core motivations of Bitcoin's creators was the eradication of middlemen and/or money creators who profit from these activities.

CHAPTER

3

MONEY IN THE 21ST CENTURY

In its simplest form, “money is identified by what it does”. Whatever form it takes, a traditional consensus amoungst those who study the functions of money is that it is must serve as unit of account, a means of payment, and a store of value. From the opening discussion, in order to fulfil these criteria, a successful form of money must also be universally trusted by buyers and sellers. In the context of digital currencies, modern discussions and debates often confuse ‘money’ with ‘systems of payments’ or, the mechanism by which transactions are processed and settled. In the context of modern debates and confusion about digital vs. physical money, it is important to distinguish between types of money and systems of payments.

A. Types of Money

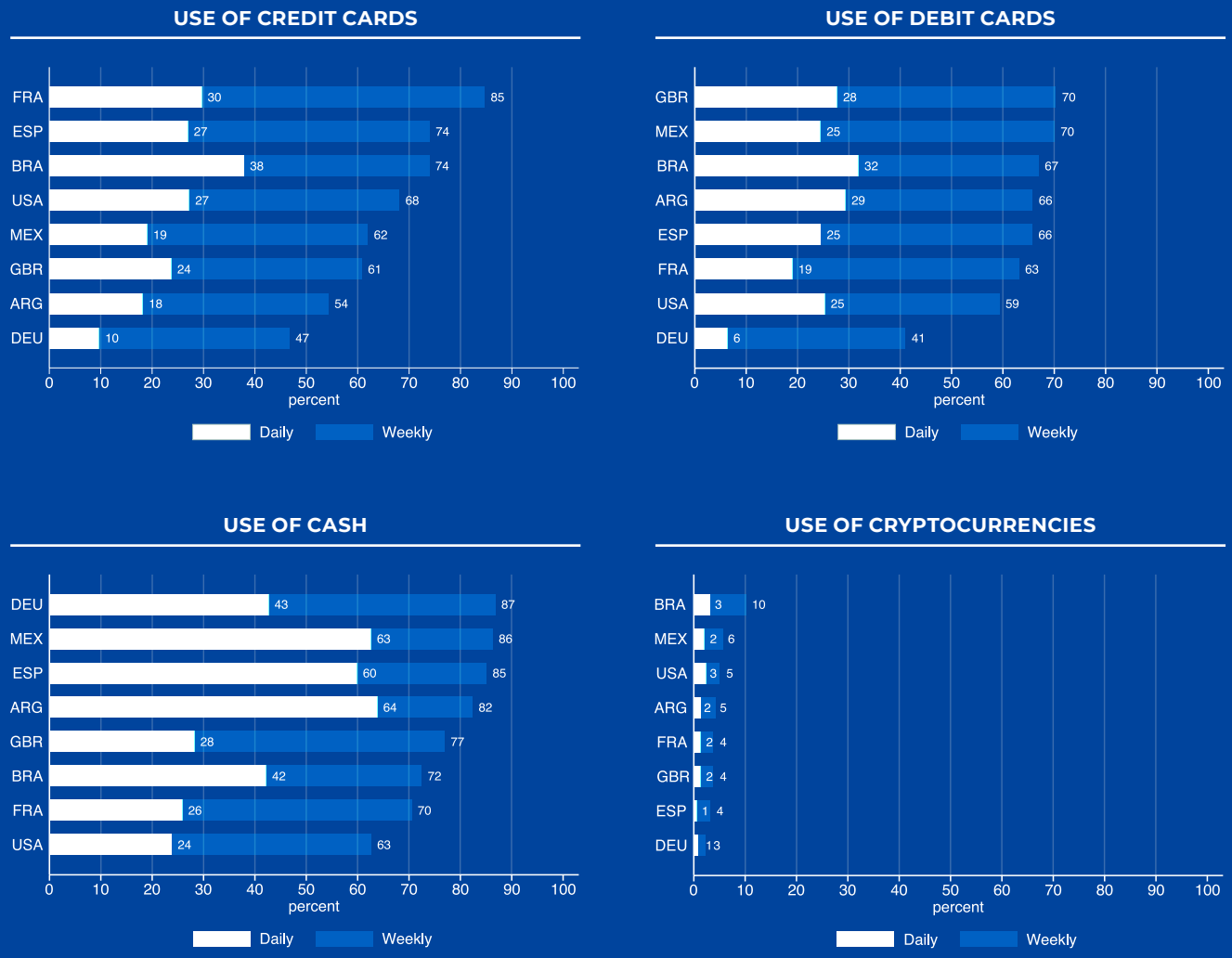
According to modern international standards, "broad money" is defined as "all liquid financial instruments held by money-holding sectors that are widely accepted in an economy as a medium of exchange, plus those that can be converted into a medium of exchange at short notice at, or close to, their full nominal value." [10] (IMF, 2016, p.180) In a 21st century context, these would include, fiat currencies issued by central banks, short-term digital credit facilities (swaps, credit cards, paypal, googlepay, payday loans, WePay, AliPay, M-Pesa, etc.), digital currencies issued by private sector/nonprofits or central banks (Bitcoin, Libra, etc). From the discussion in Chapters 1 and 2, we can begin by distinguishing currency types across five attributes, including: i) who issues and backs the currency, ii) how acceptable is the currency, iii) are there transaction costs, iv) how stable is the value over time (inflation/deflation), and, v) is it digital/electronic or physical.

Each type of money has both benefits and drawbacks in terms of its usefulness. For example, a credit card (digital) is widely accepted but may come with transaction costs and is backed by a private sector corporation, while cash (physical) may be less widely accepted but has no transaction costs and is backed by the central bank. This is why many forms of money coexist. In fact, it is not uncommon for people to use more than one form of money in a given day/week, making some payments with cash (a central bank liability) and some others with transfers or credit cards (which are private sector forms of money). To get a better understanding of current usage of types of money, we asked 1,000 respondents across eight countries (Argentina, Brazil, France, Germany, Mexico, Spain, UK, USA) what types of money they most commonly use. The results are shown below.

9. IMF Monetary and Finance Statistics Manual 2016.

FIGURE 3

Use of Money types across Countries



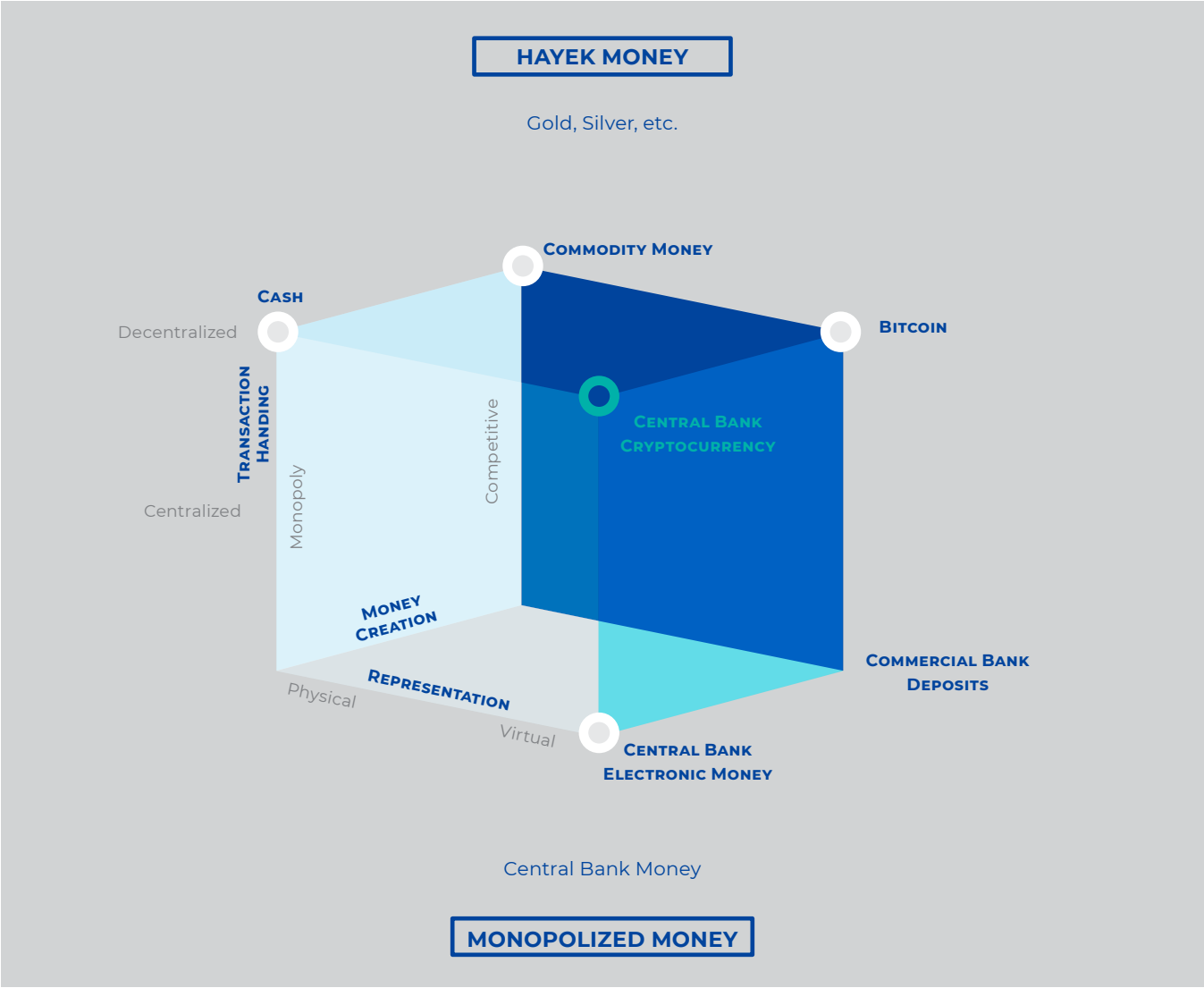
Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

Existing research has focused on the degree of centralization (issuer/backer), accessibility, and digital/physical nature of money. For example, Berentsen & Schar (2018b) studied the different types of currencies and systems of payments and their properties. In their research, they argue that Bitcoin specifically, but other decentralized cryptocurrencies in general, use blockchain technology to present a unique type of currency. Each "coin" (unit of money) is issued in a competitive setting and has both a virtual representation and a decentralized transaction process. Because of these properties, decentralized cryptocurrencies like Bitcoin can be considered a fundamentally different type of money when compared to the traditional forms we are used to (commodity money, cash, and others).

In their study of the different types of currencies, Berentsen & Schar (2018b) propose a control structure to visually represent these different types according to three dimensions. Figure 4 presents this control structure and where in this visual classification different types of currencies are located.

FIGURE 4

Control Structure of Currencies

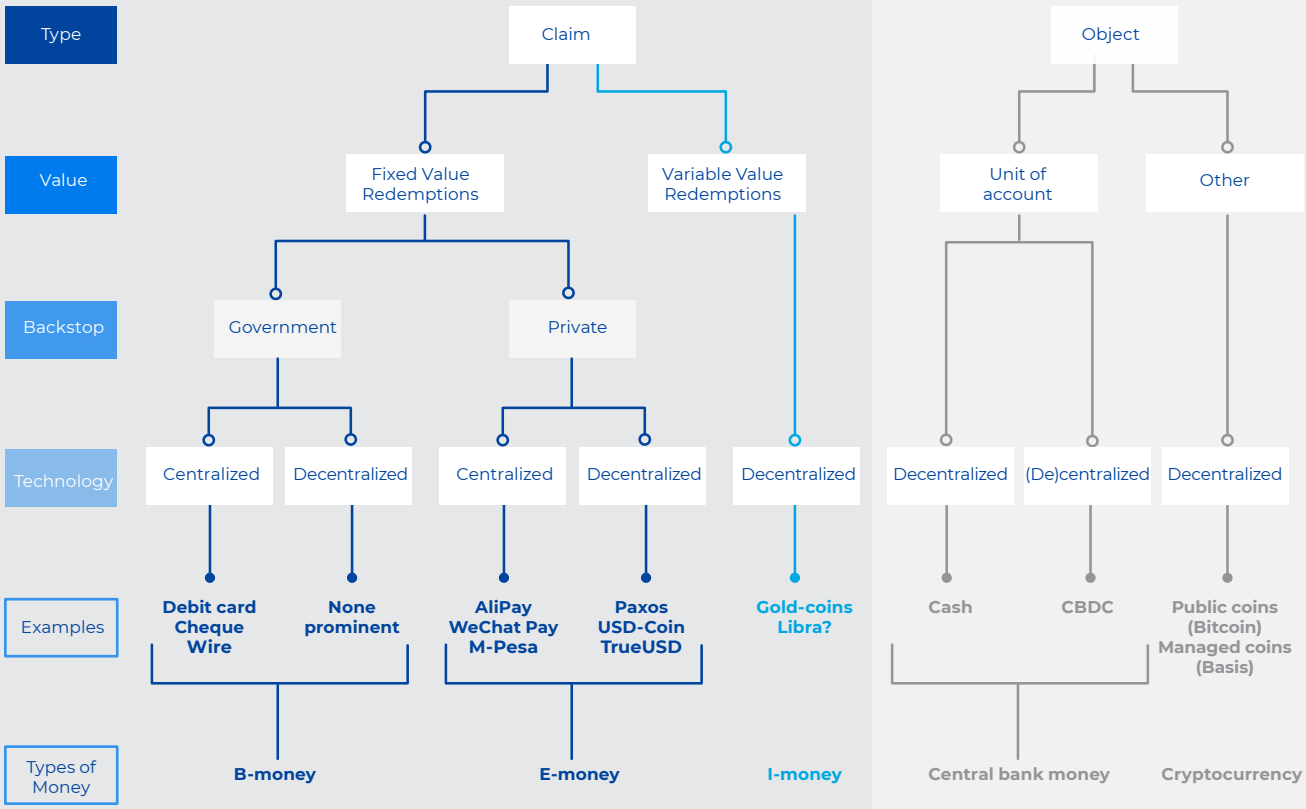


Source: adapted from Bernsten and Schar, 2018a.

As demonstrated in Chapter 2, it is important here to distinguish between narrow money that is created by central banks from broad money created by commercial bank deposits and central bank cash. Both of these centralized institutions make up almost all of money we currently use and act as clearing houses for almost all of our money transactions (system of payments). A recent IMF report has argued that these "two most common forms of money today will face tough competition and could even be surpassed. Cash and bank deposits will battle with e-money, electronically stored monetary value denominated in, and pegged to, a common unit of account such as the euro, dollar, or renminbi, or a basket thereof" (Adrian and Mancini-Griffoli, 2019, p.1). Building on this and the work of other academics/institutions, the IMF has recently provided a further dissection of money according to its 'type' (is it a claim on another entity or an object), 'value' (fixed, variable or a unit of account), 'backstopper' (government, private sector), and, degree of centralization ('technology'). From Figure 5 below, we can see that several types of digital money have already been widely adopted (AliPay, WeChat Pay, M-Pesa), while others probably do not qualify as money based on our definition of broad money above.

FIGURE 5

Types of Money in the Digital Era



Source: Adrian and Mancini-Griffoli, 2019.

Thinking about this in the context of cryptocurrencies, these are interesting because they bring a combination of new and old ideas about money. Firstly, ownership rights are managed in a decentralized network as argued by Hayek using a distributed ledger (no backstop). Because of this, there is no central authority responsible for managing currency ownership rights, ensuring price stability, and regulating illicit transactions. Blockchain technology also has a decentralized accounting system where "miners" are the book keepers and no debtor/creditor relationship (i.e. cryptocurrencies are not a liability on anyone's balance sheet). This decentralized management of ownership of digital assets is a fundamental innovation of Nakamoto (2008). More importantly, the system of payments infrastructure envisioned by Nakamoto (2008) was created with the intention to disrupt the current financial system, by affecting all business and government agencies that have monopolized the creation of money in the 20th century. With these new innovations in the early 21st century, some writers have argued that this will mark the death of cash.

B. The End of Cash?

WHY REPLACE CASH?

In order to change a system, it helps to have a problem with the existing one. This is a view shared by many economists and policymakers who see physical cash and existing digital money created by the central bank and commercial banks as doing a pretty good job, meaning there is no need to take unnecessary risks by adopting an entirely new, and potentially risky, form of money. So why has there been such a large push for the adoption of digital currencies?

Some of the well-known downfalls of physical money are the need for the buyer and the seller to be physically present at the same location, or have a geographical connection to deliver the cash, which makes its use time consuming and impracticable for online commerce.

Studies have also found that physical cash is a public health concern, finding traces of faecal matter, cocaine, heroine, and bacteria (among others) on dollar bills, making it a good candidate for spreading disease across large populations, leading experts to conclude that "if the question of a cashless society is approached purely from a public health standpoint, the answer seems clear" (Maron, 2017). [10] This would be especially important in low income countries who are more vulnerable to epidemics.

"THE MONEY IN YOUR WALLET MIGHT BE COVERED WITH POOP, MOLD, AND COCAINE"

— *Tuttle, 2017.*

Another drawback of cash relates to tax evasion and the financial operations of illegal activities, which have become increasingly salient since the publication of Panama Papers in 2015 and Paradise Papers in 2017. Money laundering, financing of illegal activities and tax evasion all pose a pervasive challenge to society in both developing and developed countries. In his study of how physical cash is related to the daily financing of these illegal activities, Sands (2016) suggests an interesting approach in order to fight these financial crimes. His proposal is to eliminate high denomination notes (he gives as examples the €500 note, the $100 bill, the CHF1,000 note and the £50 note). According to the author, these notes are preferred in illegal activities, given the anonymity and lack of transaction record in cash payment system. Moreover, because they are of high value, it is easier to transport and execute payments of large value. By eliminating high denomination notes, it is argued that we would make life a lot harder for those perusing tax evasion, financial crime, terrorist finance and corruption. Without being able to use high denomination notes, those engaged in illicit activities would face higher costs and greater risk of detection. The author concludes that the benefits from the elimination of such high denomination notes far outperform the drawbacks. Given the availability and effectiveness of electronic payment alternatives, these high denomination notes play little role in the

10. See: Maron, D. (2017). Dirty Money, Scientific American. https://www.scientificamerican.com/article/dirty-money/

functioning of the legitimate economy, yet a crucial role in the underground economy.

In "The Curse of Cash", Rogoff (2017) goes one step further. While Sands (2016) advocates for the eradication of high denomination notes, Rogoff (2017) advocates getting rid of cash once and for all. He extends the argument of Sands (2016) by linking the increasing amount of money in circulation to the volume of cash being used for tax evasion, corruption, terrorism, the drug trade, human traffic; in summary, by all sorts of illegal activities. Nevertheless, he expands the benefits of eliminating cash to monetary policy. If policy makers not only eradicated high denominations, but all notes (except very small denomination ones and coins), Rogoff (2017) argues that this would in fact increase the effectiveness of monetary policy by, for example, allowing for negative interest rates. The idea of Sands (2016) and Rogoff (2017) that physical cash makes the financing of illegal activities significantly easier cannot be ignored. In fact, Brazil's Car Wash operation, the biggest corruption scandal ever uncovered in history, showed that companies involved in illegal donations to parties developed very sophisticated methods to raise physical cash. They collected cash from different small business, sometimes even paying a premium in order to hold cash, so that they could use this cash to perform their illegal activities.

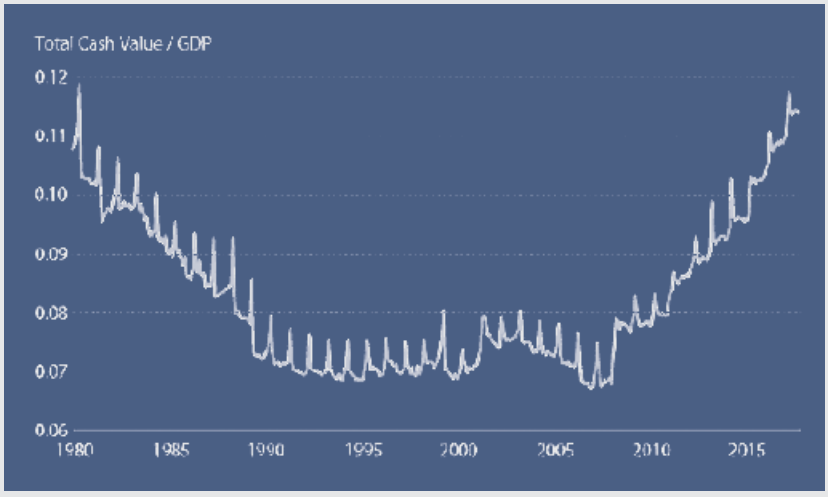
Cash, however, still maintains some unique advantages in comparison to other existing types of currencies discussed above. Users of cash can remain anonymous, in the case of stable advanced economies it is widely accepted/trusted by sellers, and there is free access to cash payment systems (no transaction costs). Users of cash also do not need to open bank accounts or create a digital wallet to use physical cash. Transactions are final and people can engage in trade even if they do not know or trust each other. The electronic money that we currently hold in commercial banks, on the other hand, involves counterparty risk, requires the use of a bank account and often has charges relating to transactions (for example, transfers to other accounts). [11]

Berentsen and Schar (2018a) believe that there is a great demand for currencies issued by a trusted party to save outside the financial system. To prove their point, they present the number of Swiss Francs in circulation as a fraction of GDP from 1980 to 2017 (see Figure 6 below). We can see that after the crisis the demand for Swiss Francs increased significantly.

FIGURE 6

Cash in Switzerland as fraction of GDP

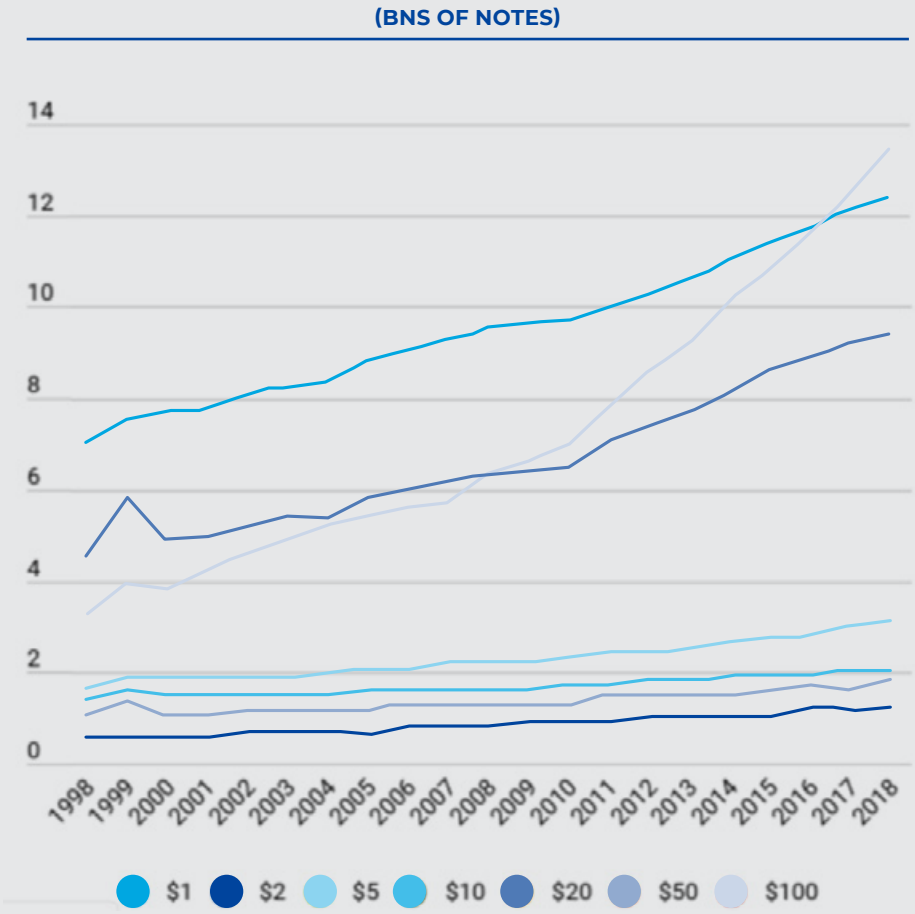
SWISS FRANCS IN CIRCULATION AS A FRACTION OF SWISS GDP



Source: Swiss National Bank and Organisation for Economic Co-operation and Development.

11. When we make a payment with a debit card, for example, we are exchanging a good or service by a claim from a private bank. This means that bank deposits are a liability of the issuer and holders of bank deposits (current and savings accounts) are providing credit to their bank.

FIGURE 7. **Figure 7: US Currency in circulation by bill type**



Source: Weir, 2019.

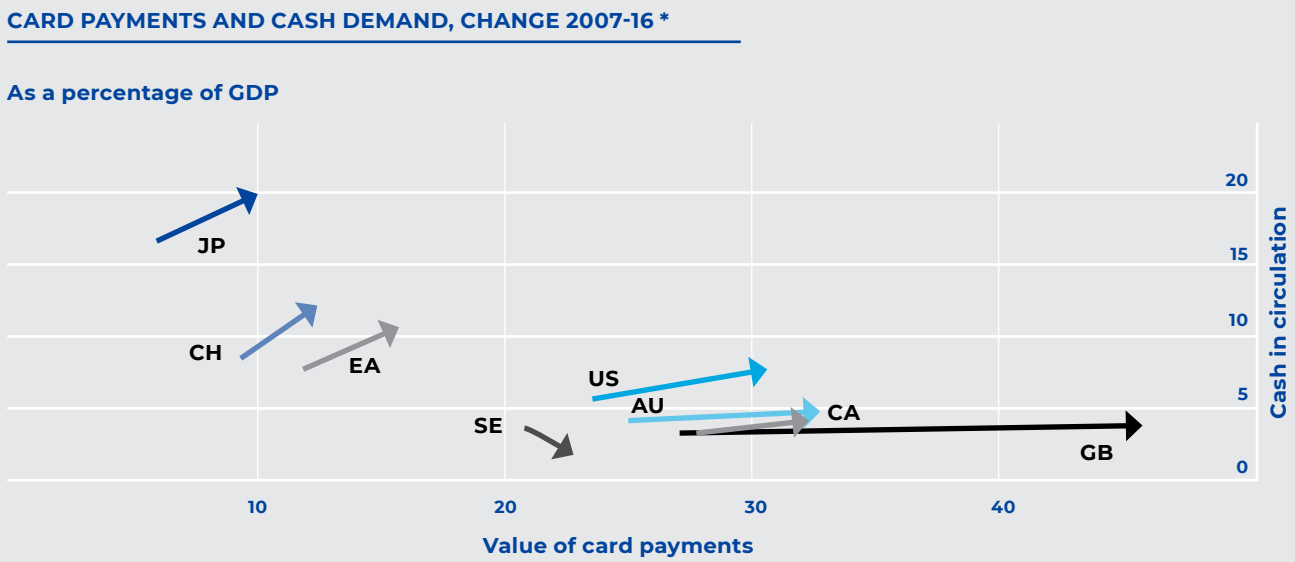
This shift is explained as a move to safety - the financial crisis and the subsequent euro crisis have increased the demand for cash exactly because it is the most liquid asset for savings outside of the private financial system. In other words, cash has been used as an insurance against the insolvency of financial institutions.

Further evidence of the growing demand for physical cash issued by a trusted backer was shown by a 2019 IMF Finance and Development article ('Boom in the Benjamins') which attributed a rise in $100 bills to an increased global demand for the US dollars as a safe haven, as well as its ideal anonymous role in illicit transactions in the underground economy. High denomination notes also offer higher seignorage returns for the Federal Reserve, making the $100 bill the most profitable to print. This combination of factors lead the authors to conclude that American dollar bills are not likely to dissipate any time soon (Weir, 2019).

The extent that fiat money will be used as an insurance mechanism depends on the degree of trust that holders of that money have in its issuer. In this sense, Switzerland and the US would be exceptional cases where a run to safety resulted in an increase in the demand for cash in stable economies. Bech et al. (2018) show that the amount of cash in circulation has increased or remained stable in a large number of stable advanced economies (see Figure 8). Although the value of card payments has increase significantly, Sweden is the only country where the cash in circulation has actually decreased between 2007 and 2016.

FIGURE 8

Card Payments and Cash Demand, Change 2007-2016 (%GDP)

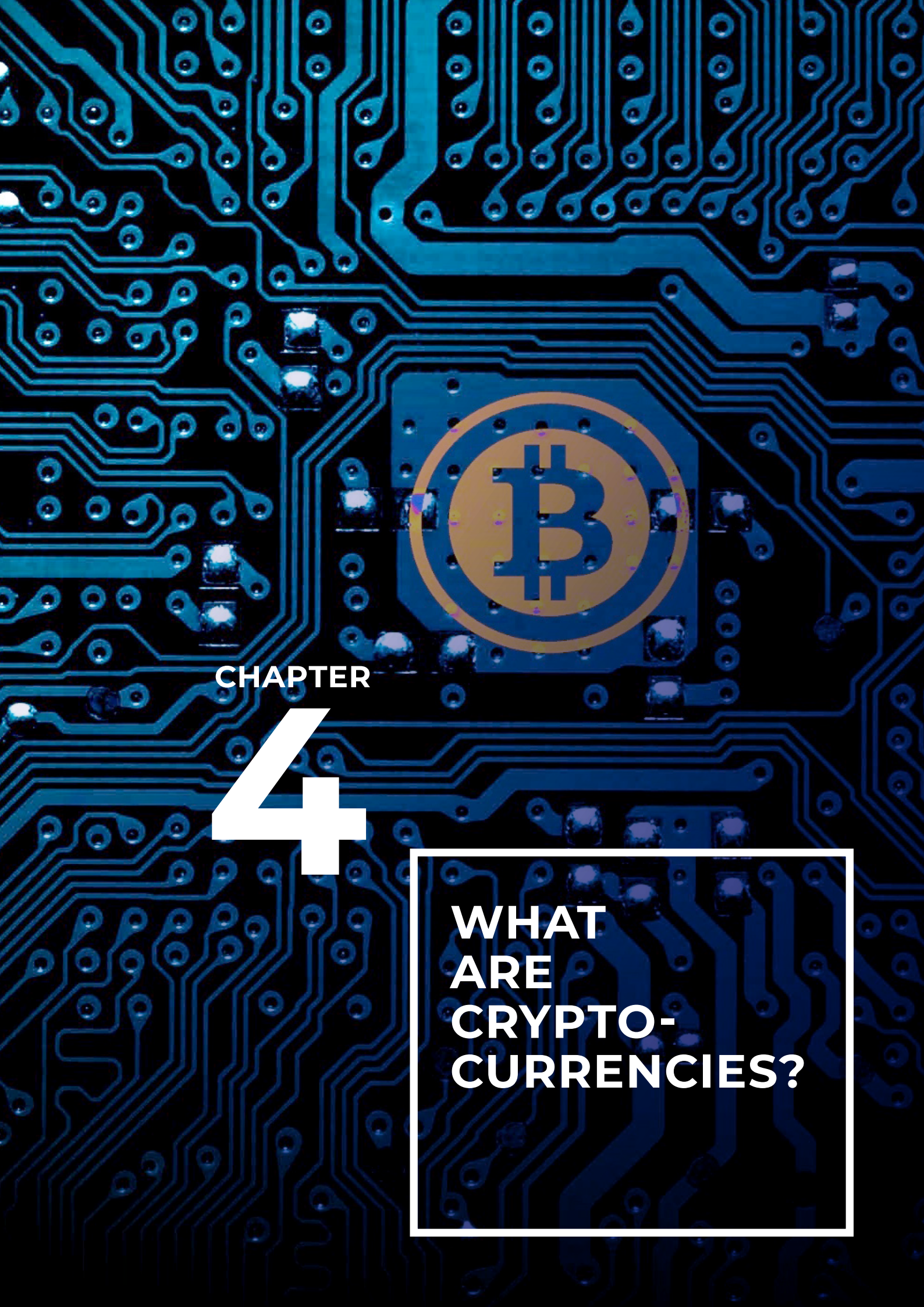


* The start of an arrow represents 2007 data while the end represent 2016

Source: Bech et al., 2018.

WHAT COULD REPLACE CASH?

As noted above, several centralized digital alternatives to physical cash have already become successful systems of payments. For example, M-Pesa in Kenya (see Jack and Suri, 2014; Kaminska, 2015), AliPay in China, and PayPal in the US (among many others). Cryptocurrency enthusiasts, central banks, and entrepreneurs are also continually improving the design of blockchain-based digital currencies to rectify some of the practical defects in previous designs. For example, Facebooks Libra will be backed by a portfolio of underlying assets and will be managed to maintain price stability (a 'stablecoin') which was a key fault in Bitcoin's ability to function as a true currency. While these 'updated' cryptocurrencies still have practical drawbacks such as high fees, scaling issues, and a lack of widespread trust, these problems could be improved upon over time with the emergence of large-scale off-chain payment networks and transparent management. It is also important to remember that digital currencies are still fiat money which relies on a relationship of trust between the issuer and the user.



CHAPTER

4

WHAT ARE CRYPTO-CURRENCIES?

To understand cryptocurrencies, we need to distinguish between what they were envisioned to be and what they currently are. The ambition in Nakamoto (2008) was to create a fair, borderless, and secure currency that can be transacted in a secure way across a network of anonymous participants. This stood on the shoulders of decades of innovation in databases, cryptography and network protocols, which all combined to give the innovation of blockchain technology. From a technical perspective, the real achievement of Bitcoin relies on the coordination of the underlying features of blockchain technology, embedded with a pre-programmed economic incentive scheme (akin to a monetary policy).

Blockchain technology enables an exchange of trust via a tamperproof, publicly auditable record of transactions between parties with no requirement of a pre-existing trust in each other or need for a central authority to govern and manage the network. The initial underlying philosophy behind the Bitcoin system (or broadly any 'decentralised' network) was to ensure that no one entity can act to censor transactions or prevent person(s) from joining the network. Rather, each participant in the network has a 'voting' right given they have computational processing power. In the context of this chapter, cryptocurrencies are any form of currency that only exists digitally as part of a payment system that has no central issuing or regulating authority and uses a decentralised system to record transactions and manage the issuance of new units/tokens, and that relies on cryptography to prevent counterfeiting and fraudulent transactions. This definition excludes 'Central Bank Digital Currencies' (CBDCs), which will be discussed in Chapter 5.

A. Principles of Cryptocurrencies

Cryptocurrencies are built on the principles of blockchain technology or what is more accurately known as distributed ledger technologies (DLTs). There are theoretically two types of DLTs, open and closed, more formally, 'permission-less (open)' and 'permissioned (closed)' blockchain.

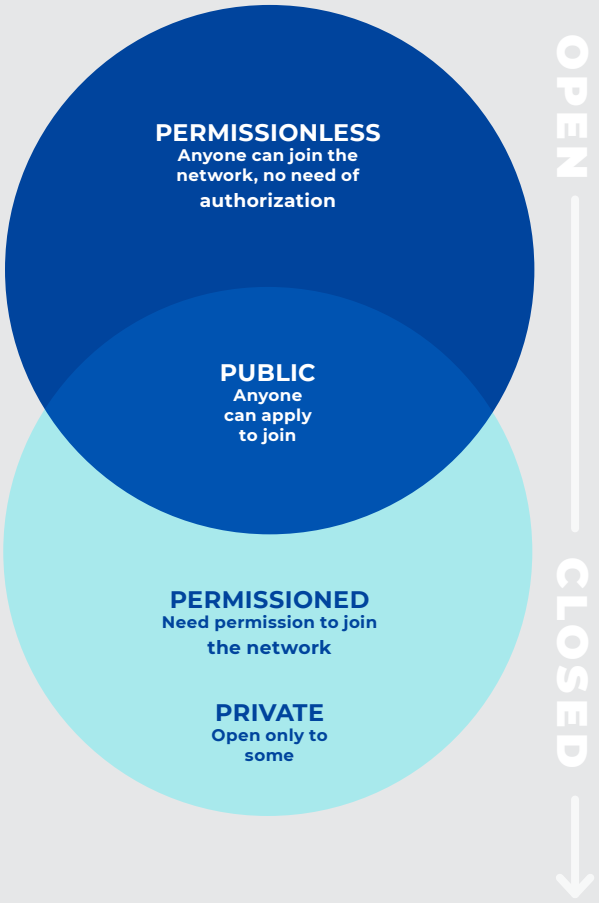
PERMISSIONLESS AND PERMISSIONED BLOCKCHAINS

To understand the difference between permission-less and permissioned blockchains, it is important to understand how the source code of the software applications is managed (that is to view code, copy it, learn from it, alter it, or share it). Most cryptocurrencies are based on decentralized permission-less blockchains, including Bitcoin and Ethereum, whose transparency is built on open-source code (accessible to everyone on the network). Permission-less blockchain-based cryptocurrencies allow anyone to access the Bitcoin code, inspect it, copy it and improve it. (For example, click here to see bitcoin source code).

Permissioned blockchains on the other hand are typically more centralized, closed systems, whereby there is a known custodian of the blockchain network who qualifies participants based on certain pre-defined criteria in order to access and use the blockchain data. Permissioned blockchains are typically used by large, private groups of enterprise organisations who require a great deal of trust, as they are likely to be using the blockchain for its technological efficiency gains in specific use cases, as opposed to its economic digital currency features and capabilities.

FIGURE 9

Permissionless and Permissioned Network



Source: Coindesk, 2019.

LEDGERS

Ledgers have existed and evolved as a form of accounting for over a millennium. For example, ledgers were found to be used by Mesopotamian's (modern day Iraq) as far back as 3200 BC to record expenditures, traded goods and record accounts payable on Clay Tablets (kept safe in temples, considered banks of the time). Then ledgers were used in 633 BC by Persian civilisations as an auditing tool to regulate the collection of alms (wealth tax). During the Middle Ages, there was a scarcity in gold across Britain, which caused a decline in circulation of coins; as a result the Exchequer introduced tally sticks as a physical proof of payment, whereby the stick would be split in half. One half was kept as stock by the payer (contract), and the other half as debt retained by the Exchequer. Hence, when accounts were audited, the pieces were fitted together to check they 'tallied'. [12] By the 14th century, tally sticks had spread across Europe, fundamentally acknowledging the emergence of debt and contracts, which were used to pay wages to workers and taxes to the state, and also traded to buy and sell items, similar to coins. They were different in that they also acted as an 'IOU' pledge, whereby whoever issued the stock was liable to pay in gold whoever owned the other half of the stick. Thus, the stock had a value in gold, and could be spent accordingly to the same value of actual gold. Thus far, a 'ledger' is defined as an information store that keeps a final and definitive records of transactions, and a 'transaction' is defined as a smallest unit of work process resulting in a state change (ISO, 2008, definition 3.5).

By 1497 Merchants in Venice had advanced accounting systems to create a new financial services industry. This was captured by the Italian church father and mathematician Luca Bartolomes Pacioli, who published the first book on double entry system of accounting, highlighting that any given new transaction fundamentally changes either the debit or credit position of the account, to give an actual value of a business. Other than advancements in technology and general digitalisation, accounting and bookkeeping have not really progressed beyond Excel spreadsheets and have become more complex, which requires qualified professionals to maintain accounting records across multiple accounts (ledgers).

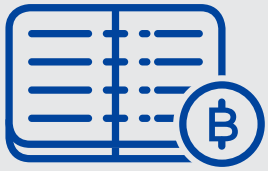
From an accounting perspective, key advancements in blockchain technology are the abilities for participants to share one single synchronised, distributed ledger of transactions, and for the underlying consensus protocol (a set of rules) to successfully ensure each node on a network agrees on the data being shared on the ledger.

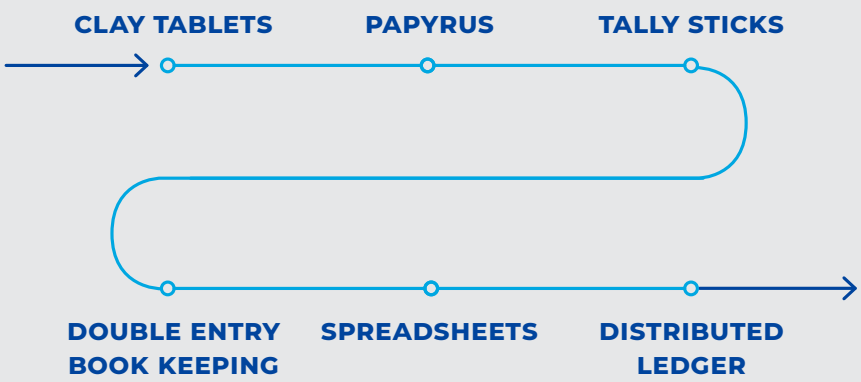
NETWORKS

Blockchains, or DLTs, consist of a network of nodes, where a network is defined as an interconnected system of things. The best way to understand the relationship between nodes and networks is a *visual representation* seen in Figure 11 where decentralized networks have multiple sources of control and distributed networks distribute control equally across all participants in that network, whereas centralised networks have one central source of control.

FIGURE 10

Historical Evolution of Ledgers





Source: Coindesk, 2019.

12. See: Smithin, J. ed. (2000). What is Money?

FIGURE 11

Centralized, Decentralized and Distributed Ledger Technology

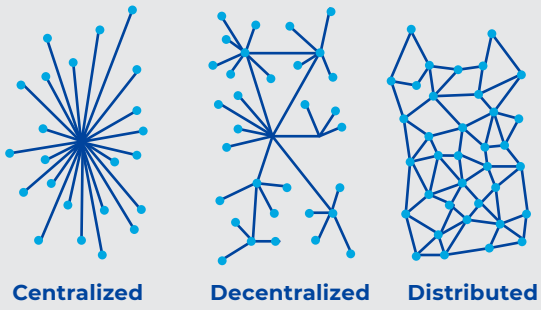


Image Source: Baran, 1964.

The Rand Corporation described these networks back in the 1960s (Barand, 1964), describing the type of interconnection between the nodes and the type of information flow between them for transaction and/or the purpose of validation. For efficiency reasons, systems have historically been designed in a centralised manner. This centralisation dramatically lowers the costs for system configuration, maintenance, adjustment (and the costs of arbitration in case of conflict) as this work must be performed only once in a central place. While highly efficient in many situations, this kind of systems induce a single (or very limited set of) point(s) of failure and suffers from scalability issues (Tasca and Tessone, 2018).

In a highly centralised system, all the nodes (and all the users on a node) are connected to the central node (a 'dictator' model). Most social and monetary networks are centralised systems, where all participants have relationships with centralised hubs (i.e. a central bank). However, the Internet was not really designed to be like that (i.e. for centralised business models), rather, for information to be decentralised and accessible and not controlled by one central hub. The distributed network on the other hand, maintains a strong sense of locality with no tiered hierarchy, critically meaning if one node falters, the whole network will not be taken out.

Both have advantages and disadvantages, making it hard to prescribe a relative value to each extreme end. The centralised system is very efficient but more susceptible to single-point failure (discussed below) whereas a distributed system is robust with no reliance on a central authority, however it could take a long time for data to pass across the network. The main reference is to understand some of the risks of centralisation when applied to business models, which give rise to the motivation behind the creation of crypto currencies.

We can think broadly about cryptocurrencies based on the economic goals of the network (or protocals). As will be shown in section C, there are many types of blockchain based tokens backed by different consensus protocols, most of which fall into one of three main categories:

FIGURE 12

Cryptocurrency Token Categories

TOKEN CATEGORIES

PAYMENT TOKEN	UTILITY TOKEN	ASSET TOKEN
Are synonymous with cryptocurrencies	Are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure	Asset tokens represent assets such as a debt or equity claim on the issuer
Are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer		Tokens which enable physical assets to be traded on the blockchain also fall into this category
Give rise to no claims on their issuer		

Token can change their qualifications over time (e.g. utility token can become a payment token

Tokens that fall within more than one category are qualified as a hybrid token and need to comply with the requirements for all the involved categories

In practice, most popular cryptocurrencies were designed to be payment tokens which is the type that we will consider in the next sections.

B. What were Cryptocurrencies meant to be?

The motivation behind Bitcoin and other DLT apparatuses involves the application of cryptography to monetary networks in order to eliminate trusted third parties across messaging systems. Most people already use cryptography when using internet applications, in sending or signing off on packets of data or messages (e.g. the https protocol for internet browsing or Whatsapp for secure peer-to-peer messaging). *Encrypted* messages prevent observations from an intermediary, and *signing* preventing tampering of data have eliminated the need to trust a third party to carry the message, for example SMSs where data packets go through centralised data exchanges usually administered by Telcom service providers. When considering the innovation of blockchain, it allows the same, the elimination of third parties in financial transactions through the use of payment tokens.

Some of the benefits of blockchain technology applied to monetary systems are:

- **Decentralisation** – no single point of trust, no single point of control (no central authority), no single point of failure
- **Security and Anonymity** – non-repudiation and irreversibility of records with pseudo-anonymous transactions.
- **Transparency, Auditability, and Governance** – anyone can join participants can verify the veracity of records directly, without external querying.

A DECENTRALIZED MONETARY SYSTEM

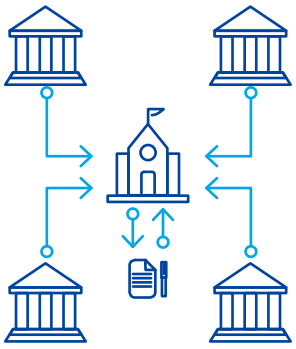
In the original Bitcoin whitepaper, the author envisioned Bitcoin becoming a digital payment system with emphasis on a key innovation called *'decentralisation'*: removing the need for a trusted third-party institution in processing transactions, whose rules are enforced by consensus, with *anyone* being able to participate. Nakamoto frames the discussion around the trusted third-party issue in economic terms, arguing that:

> **"Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services."**

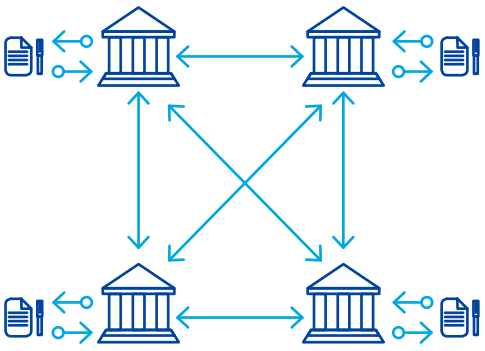
The focal point here is not money itself, but the way money is used and managed (system of payments), specifically with no intermediation. In fact, cryptocurrencies have several similar characteristics to cash (low transaction cost, quasi-anonymity). The key difference envisioned by Nakamoto was the stripping out of a centralized authority and clearing house for money, instead having transactions verified by a global group of participants using blockchain technology (similar to Figure 11).

FIGURE 13

Centralised and Distributed Ledger Monetary Systems



CENTRALIZED LEDGER



DISTRIBUTED LEDGER

Source: Ward, 2019.

As noted above, this change to the system of payments is the true innovation of Nakamoto, not money itself. This was highlighted in a 2016 speech by the deputy governor of the Bank of England:

> **“The main point here is that the important innovation in Bitcoin isn’t the alternative unit of account – it seems very unlikely that, to any significant extent, we’ll ever be paying for things in Bitcoins, rather than pounds, dollars or euros – but its settlement technology, the so-called “distributed ledger”. This allows transfers to be verifiably recorded without the need for a trusted third party. It is potentially valuable when there is no such institution and when verifying such information on a multilateral basis is costly.”**
>
> — *Ben Broadbent, 2016.*

Why Decentralize?

When considering existing (digital) business models, which are all predominantly centralised, there are certain risks involved to network users. [13] Some of these risks include:

- **Single-point failure**
- **Exclusion, abuse, and mistrust**
- **Low Transparency and high transaction fees**

Single Points of Failure

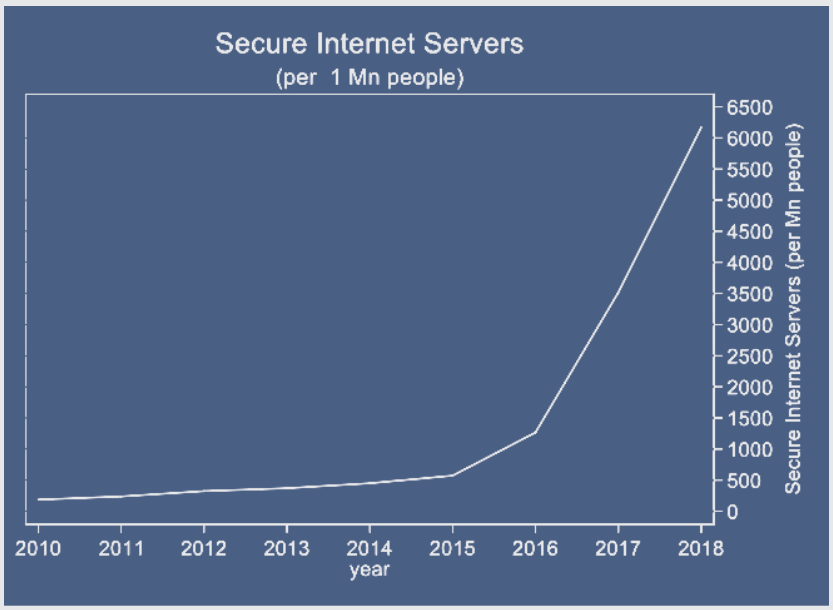
Looking back at previous figures on pages 51 and 53, Figure 11 and Figure 13, it should be clear that a peer-to-peer decentralized payment system is inherently more robust than a payment system requiring an intermediary or clearing house. Bitcoin achieves this by using a blockchain-based consensus mechanism to manage an agreement on the state of a distributed database. While the network relies on the underlying Internet connectivity (which is itself decentralised), there is no single entity whose failure would disrupt the network. Centralised payment systems are exposed to failures of hardware and breaches of security procedures which, in the worst cases, can bring the whole payment network down (as was the case for Visa in Europe on 1 June 2018). Having a decentralised network ensures that the failure or breakdown of any node cannot disrupt the entire system. For example, if a central clearing house (say the central bank) was to suffer an attack, this would prevent the entire monetary system from functioning in a centralised system; whereas, an attack on a server in the Bitcoin network would have no effect on the functioning of the system (i.e. users could still make transactions using Bitcoin).

Exclusion, abuse and mistrust

Blockchain-based permissionless cryptocurrencies have, by design, a uniquely low barrier for entry – any individual can participate in the payment system as long as they have access to an Internet connection. This makes it possible for anyone to actively participate in the system and ensure the accountability of others in the network. With 1.7bn people in the world without access to a bank account, regular payment providers have often failed to provide access to an effective payments system. This is especially true in the midst of a worldwide surge in access to the Internet and secure internet servers as can be seen in the Figure 14 below.

FIGURE 14

World Internet Users and Secure Internet Servers



Data Source: World Bank, 2019.

13. See: Siliski, M. (2018). Blockchain Alternatives, Medium.com. https://medium.com/swlh/blockchain-alternatives-b21184ccc345

The decentralized network also prevents a centralized authority from excluding members participation or abusing their unique position as the only group with access to a private ledger. This lack of transparency in a centralized system can lead to popular mistrust, which is remedied by allowing all participants access to a common decentralized ledger.

High Transaction Fees

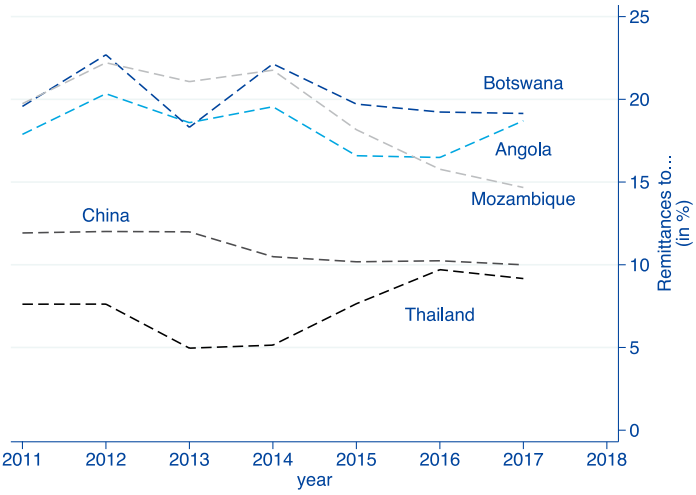
With the invention of electronic transfers (credit cards, debit cards, etc.), financial transactions have become considerably cheaper and more efficient over the past thirty years. There do remain some types of transactions which require significant third-party fees to complete.

The most prevalent of these would be transactions involving multiple currencies (i.e. remittances, tourism, imports/exports of goods and services). For example, looking at data from the World Bank for remittance fees over the 2011–2017 period, we can see that remittance fees to some countries are still close to 20%, and still range around 10% in strong emerging economies like China and Thailand.

A more extreme, and persistent, example of high third-party fees is the exchange of currencies at international airports. While these companies pay high rents for real airport estate, the fees charged by monopolistic money exchange facilities in many UK airports have remained disproportionate for several years without much change. The persistence of this problem has been well documented in the press over several years in the UK. Table 2 below provides select articles with a comparison of the rates charged at airports with spot exchange rates.

FIGURE 15

Average Remittance Fees to Select Countries



Source: World Bank World Development Indicators

TABLE 2

Foreign Exchange Fees in UK Airports (Media Articles)

Article Source	Date	FX (airport)	FX (spot rate)
The Sun	23 August, 2019	1 GBP = 0.9885 USD	1 GBP = 1.23 USD
Daily Mail	31 July, 2019	1 GBP = 0.78 EUR	1 GBP = 1.10 EUR
Independent	30 July, 2019	1 GBP = 1 USD	1 GBP = 1.22 USD
Thisismoney	8 June, 2019	245 GBP = 200 EUR	245 GBP = 276.8 EUR
The Times	20 April, 2019	1 GBP = 0.77 EUR	1 GBP = 1.16 EUR
The Mirror	19 April, 2019	1 GBP = 0.78 EUR	1 GBP = 1.16 EUR
The Independent	14 December, 2018	1 GBP = 1 USD	1 GBP = 1.26 USD
The Guardian	12 Oct, 2016	1 GBP = 1 USD	1 GBP = 1.54 USD

Sources: Calder, S. (2019). Pound worth just 85 euro cents at UK airports as sterling sinks, Independent. https://www.independent.co.uk/travel/news-and-advice/pound-euro-exchange-rate-brexit-gatwick-heathrow-gbp-eur-a9026226.html
Hamilton, S (2019). "'My €200 cost me £245!': Last-minute cash machine currency cost this traveller an eye-watering £68 extra", This is Money. https://www.thisismoney.co.uk/money/holidays/article-7119311/The-minute-ATM -currency-deal-cost-traveller-eye-watering-68.html
Coffey, H. (2018) "'Rip off' airport currency exchange rates hit new lows against the euro and dollar", Independent. https://www.independent.co.uk/travel/news-and-advice/airport-currency-exchange-rate-pound-euro-dollar-holiday-money-stansted-moneycorp-a8506296.html
Knapman, H. (2019). "Holidaymakers being offered less than €1 for £1 at airport money exchanges", The Sun. https://www.thesun.co.uk/money/9784341/holidaymakers-airport-money-exchanges/
Murray, A. (2019). "Airport currency exchanges are accused of exploiting the slump in sterling to charge passengers rip-off rates", Mail Online. https://www.dailymail.co.uk/news/article-7303667/Airport-currency-exchanges-accused-ripping-passengers.html
Andrews, A. (2019). "Holidaymakers 'ripped off with extortionate rates' at airports", Mirror. https://www.mirror.co.uk/money/holidaymakers-ripped-extortionate-rates-airports-14432363
Coffey, H (2019). "Pound hits parity with the dollar for tourists exchanging currency at UK airports", Independent. https://www.independent.co.uk/travel/news-and-advice/pound-dollar-exchange-rate-airports-uk-parity-currency-euros-brexit-a8683156.html
Clatworthy, B (2019). "Currency exchange rate rip-off — why you shouldn't get your money at the airport", The Times. https://www.thetimes.co.uk/article/currency-exchange-rate-rip-off-why-you-shouldnt-get-your-money-at-the-airport-jklh278hb
O'Carroll, L. (2016). "Travellers hit by 'abominable' exchange rates at UK airports", The Guardian. https://www.theguardian.com/business/2016/oct/12/travellers-hit-by-abominable-exchange-rates-airports
Plush, H (2016). "Airport currency exchanges accused of 'taking advantage' of holidaymakers with 'shocking' rates", Telegraph. https://www.telegraph.co.uk/travel/news/currency-exchange-companies-taking-advantage-of-holidaymakers-airports-million-profit

SECURITY AND ANONYMITY OF PARTICIPANTS

While blockchain-based transactions are public by the nature of the payment protocol, blockchain-based cryptocurrencies are 'pseudonymous'. Transactions can be linked to the public keys they originated from and were sent to, but it is much harder to establish a link between a public key and the identity of the person making the transaction. Notably, the transaction is 'pseudonymous' not only from the broader public, but also from the other counterparty – not unlike a cash transaction between two strangers. This security and anonymity removes the risk of a financial intermediary misusing client details, having them unintentionally stolen or legally sharing them with third parties (e.g. a suppressive government) without the explicit consent of the client. This pseudo-anonymity also helps to overcome some of the problems with purely anonymous cash identified by Sands and Rogoff from Chapter 3. For example, large movement of funds could be followed as they move through the network, allowing for law enforcement to track conspicuous transactions across the globe.

TRANSPARENCY, AUDITABILITY AND GOVERNANCE

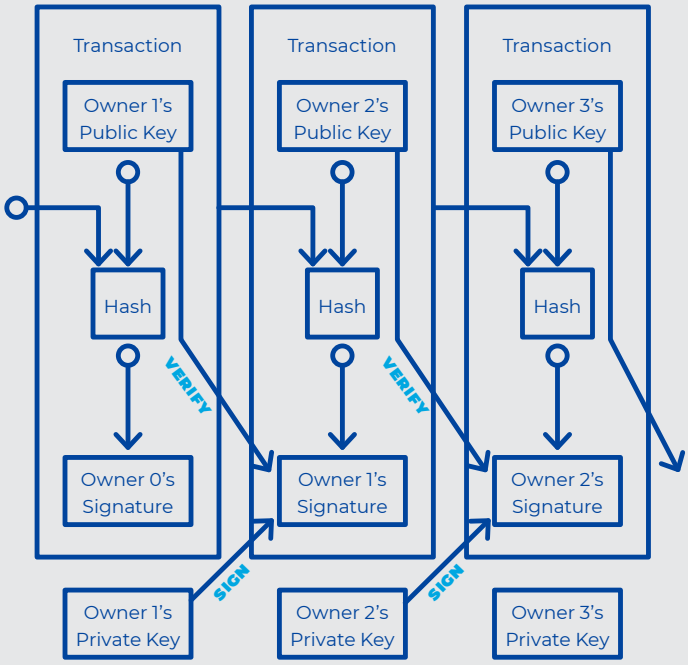
Similar to banks, blockchain-based cryptocurrencies record all transactions in a secure and immutable ledger. The blockchain is a transactions ledger of tokens where the entire history of transactions is recorded. One block contains a group of transactions and has a unique pointer that refers to previous blocks in the chain. In contrast to centralized systems or banks, in the case of Bitcoin, the ledger is not stored in one 'safe' place. Instead, everyone using Bitcoin (i.e. who has the core software) is connected through a peer-to-peer network and saves a replica of the Bitcoin's blockchain (ledger). There are many replicas of the same ledger existing on multiple machines, guaranteeing its safety against system failures or attacks and full transparency for all users on the network. Effectively, this means that anyone can access and audit records of all pseudo-anonymous transactions and does not require intervention or permission from a third party (i.e. a central bank).

As depicted in Figure 16, this system allows buyers and sellers of goods and services to interact in a transparent manner with each other without needing a central bank or commercial bank to act as an intermediary, or backer of the currency used to make the transaction. For example, with Bitcoin, everyone can download the software, transfer fee-free money, store the ledger and even maintain it, democratizing the control over the system.

Transparency is a key component for trust to be established. As modern commercial banks have scaled up

FIGURE 16

Blockchain Transactions



Source: Nakamoto, 2008.

operations from knowing their users personally to cross border business models, participants have become identified as a 'number' and see the running of operations inside the banks as 'black box systems of authority'. This has led to *less direct* means of interaction, transparency, and understanding of what banks actually do (this will be explored further in Chapter 6).[14]

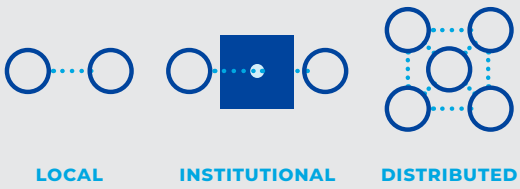
The advantages in building trust through increased transparency and auditability of blockchain-based crytpocurrencies has led some experts to conclude that distributed ledgers will overtake the centralized institutional framework as seen in Figure 17.

For any new technological innovations to be adopted and scaled, there is a trust barrier that needs to be overcome which, as will be shown in Chapter 6, is certainly the case with cryptocurrencies. Technological innovations can arise from a lack of trust in existing systems (for example, lower levels of trust in traditional authorities during periods of hyperinflation). To overcome the trust barrier in cryptocurrencies, it is helpful to review the governance frameworks, or, consensus protocols.

Governance in DLT frameworks is inherently more democratic than the traditional centralised clearing house frameworks. The degree of democratization depends partly on the decision algorithm adopted (consensus protocol). Consensus protocols allow a decentralised network to arrive at an agreement about the state of the blockchain. There are different protocols for different types of blockchains and each has its pros and cons. In general, a DLT participant must validate transactions (either individually or in a set or block) before they can be added to the distributed ledger. This means that general DLT consists of a network of nodes - called 'validators', because nodes are completing validation function. In a permission-less DLT (i.e. for most cryptocurrencies), the set of nodes that can validate transactions are generally not known, so we need a way to ensure that the behaviour of the system matches the expectations of its users.

FIGURE 17

Evolution of trust



Source: Botsman, 2016.

14. See: Botsman, 2016.

In the case of most cryptocurrencies, these are a subset of participants depending on the consensus protocol, which can be broadly classified as:

- **Proof of Work - Mining pools**
- **Proof of Stake - Endogenously wealthy token holders**
- **Exogenously wealthy actors who pay-to-play, in some other cases**

Proof of Work

In the proof of work governance model, prospective validators ('miners') solve a puzzle that is easy to verify but hard to guess without a time-consuming brute-force approach. Some examples would include Bitcoin, Ethereum, Litecoin, Dogecoin, ZCash, Monero (and many more). In terms of advantages, cheating is difficult, given the large volume of participants, and taking over the network is expensive. In terms of disadvantages, the network is run by those who have access to cheap electricity, whose interests may not match those of users in general. Countless computations are spent in a zero-sum arms race with negative externalities such as pollution and depletion of natural resources.

Proof of Stake

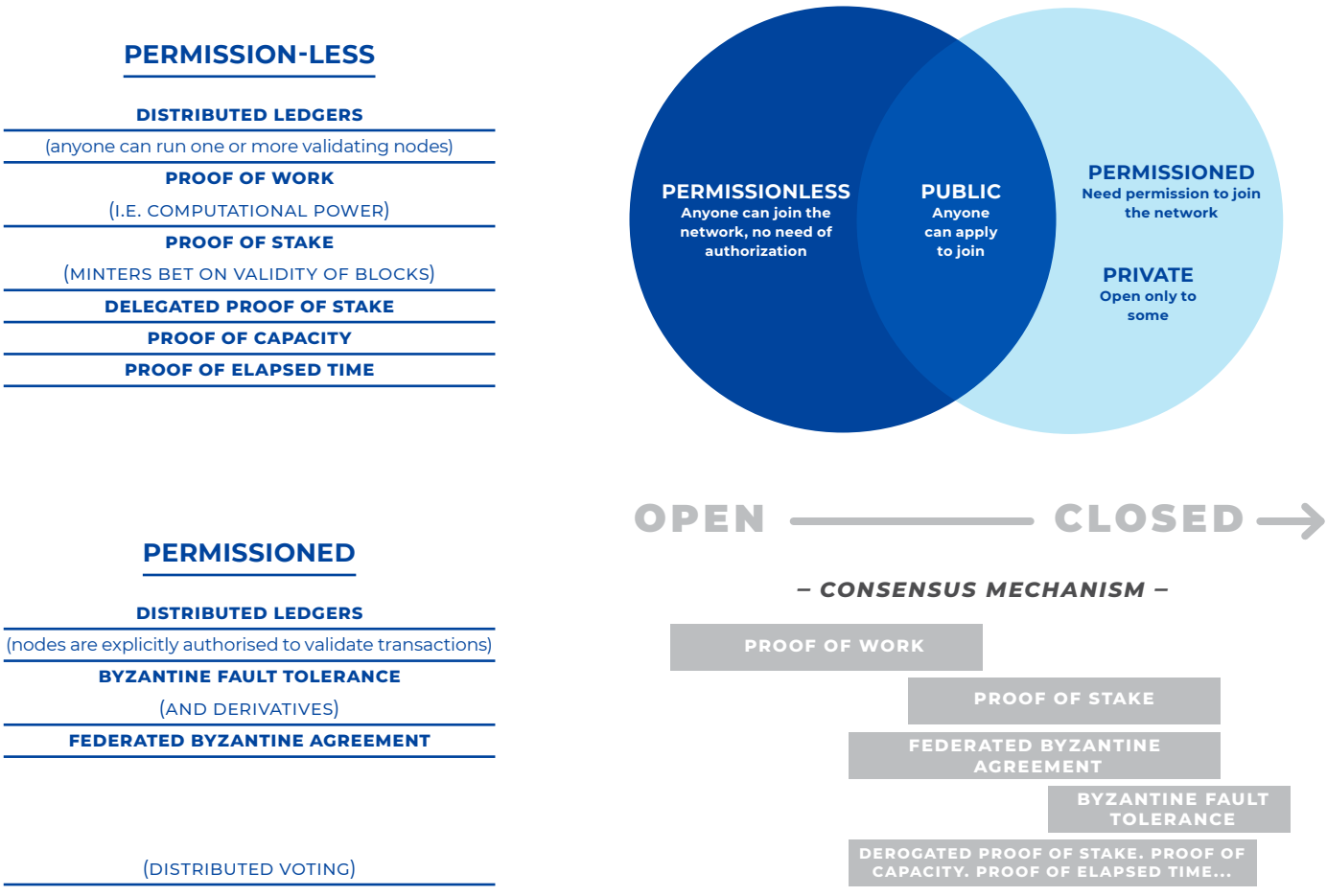
In the proof of stake governance model Prospective validators deposit tokens in exchange for the chance (proportional to the size of the deposit) to be selected for block creation. If a validator pro-

duces (or votes on, depending upon implementation) a block that is added to the chain, then it receives a reward. Otherwise, it loses the security deposit. Some examples would include Ethereum (Serenity), Tendermint, and NXT. In terms of advantages, the Proof of Stake consensus protocol replaces mining with a betting system that is more energy efficient and shifts verification to those with a stake in the success of the network. In terms of disadvantages, control resides in the hands of those with the most tokens, whose interests may not match those of users in general. A broader breakdown of consensus protocols is shown below in terms of their level of centralisation/decentralisation.

In summary, Cryptocurrencies propose to remedy three issues that exist in the current system of payments, mainly, the single point of failure that naturally emerges from centralised/monopolised money, the anonymity of participants, and the exclusion, abuse and trust of users in a system where money is monopolised by potentially irresponsible policymakers (as discussed in Chapter 1). Blockchain-based cryptocurrencies also provide a secure environment to transact with no need for expensive third parties and full transparency to all members of the network using a common distributed ledger. Lastly, the rules governing these currencies are democratised to allow for members to participate based on publicly available consensus protocols.

FIGURE 18

Centralization of Consensus Protocols



C. Cryptocurrencies in Practice

In practice, cryptocurrencies (including Bitcoin) have become something different than what was envisioned by Nakamoto (2008). While there is a great deal of competition (Hayek money) in the cryptocurrency market, Bitcoin and other high-profile cryptocurrencies have failed to stabilize their value and subsequently increase their level of trust and acceptability (see Chapter 6). There are also challenges when comparing specific features of cryptocurrencies discussed in theory (Section B) with cryptocurrencies in practice.

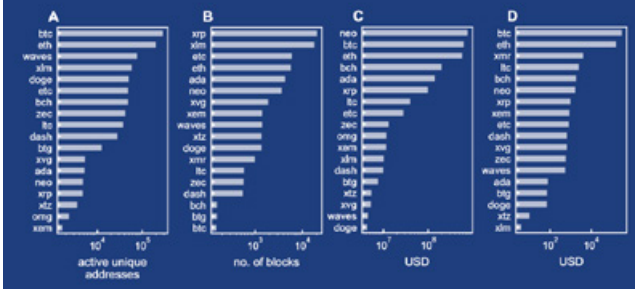
From 2013, the growth in the number of cryptocurrencies has been impressive. A 2019 Institute and Faculty of Actuaries paper reported that there were 66 varieties of crypto-assets in 2013, 644 in 2016, 1,335 at the end of 2017, and 2,116 in January of 2019. (Rochemont and Ward, 2019) The same trend has occurred in terms of market capitalization, where crypto-assets have grown exponentially from around USD 10 billion at end-2013 to USD 572.9 billion at end-2017. In terms of trading platforms for crypto assets, as of April 2018, the number had exceeded 10,000. (Rochemont and Ward, 2019)

Among the over 2,000 cryptocurrencies in existence, the market share distribution is relatively congested. Figure 19 shows a comparison between 18 cryptocurrencies. Using data collected from coinmetrics we show on the next page for the 18 cryptocurrencies the average daily active unique addresses (19A), the average number of blocks generated daily (19B), the average daily adjusted transaction volume (19C) and finally the average daily fees paid to miners (19D). Averages are

calculated over the entire period of data which varies from 438 days (for Tezos) to 3903 days (for Bitcoin). The figure shows that although Bitcoin is the most widely known cryptocurrencies, in terms of the average daily transactions volume relatively new cryptocurrencies such as NEO are more used.

FIGURE 19

Characteristics of most popular Cryptocurrencies



Name	Symbol	Price	Rank (market capitalization)
Bitcoin	Btc	8,466.67	1
Ethereum	Eth	170	2
Stellar	Xlm	0.06	10
NEO	Neo	7.49	21
Bitcoin cash	Bch	227.23	5
Cardano	Ada	0.0397	12
Litecoin	Ltc	57.20	5
Ethereum Classic	Etc	4.84	20
Zcash	Zec	37.82	28
OmiseGo	Omg	0.8361	43
NEM	Xem	0.043	25
Dash	Dash	73.36	17
Bitcoin Gold	Btg	7.84	40
Verge	Xvg	0,0034	73
Waves	Waves	0.87	54
Dogecoin	Doge	0.002216	29
XRP	Xrp	0.247	3
Tezos	Xtz	0.91	19

Source: Coinmetrics, 2019.

With the exponential growth in cryptocurrency 'issuers' comes a great deal of failed or fraudulent attempts to profit from the hype. This can be best characterised in a 2018 article highlighting that "the cryptocurrency landscape is already littered with the ghosts of hundreds of dead coins that were too niche, too dumb, or blatant scams." (Marvin, 2018) Of the 2,000+ surviving cryptocurrencies, Bitcoin remains, by far, the most dominant in terms of market capitalisation.

In terms of usage, it is difficult to measure active participants. The largest and most widely used cryptocurrency is Bitcoin, which, as of July 2014, had almost 41 million addresses listed on the Bitcoin block chain, but only 1.6 million that contained a balance of more than 0.001 bitcoins (roughly £0.35).

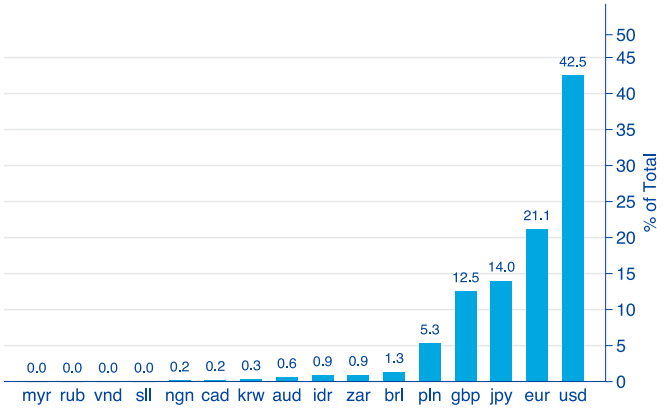
This much smaller figure still overstates the number of users, however, as each user may possess any number of wallets and each wallet may hold any number of addresses. In a 2018 survey of over 200 cryptocurrency owners, the Foundation for Interwallet Operability (FIO) found that only 30% of users sent any coins to a third party or alternative account at least once a month. A total of 43% of respondents sent coins to another party or made a purchase with cryptocurrencies only a few times during the entire year, and 27% sent no coins at all. From this, we could conclude that 70% of cryptocurrency holders either never or rarely used cryptocurrency for making any type of payments. Another way to estimate Bitcoin usage is through the number of venues that accept Bitcoin. According to coinmap.org more the 15,000 venues accept Bitcoin. Leading software companies such as Microsoft accepts payment in Bitcoins. Expedia, the travel fares and hotel aggregator website, also accepts Bitcoin. Most importantly, digital banks such as Revolut allow their users to open accounts in Bitcoins and use it for payments.

Cryptocurrencies are purchased with an underlying unit of account (central bank-issued money). This allows us to see what currencies are being converted into cryptocurrencies, similar to looking at debt or equity by currency type to get an idea of who is holding that debt or equity. In August of 2014, a Bank of England Report estimated that almost 60% of Bitcoin trading was against the Chinese renminbi, 32% traded against the US dollar, 3% against the euro and 1.2% of trading was against the British pound (Ali et al, 2014). Since the publication of these figures, there have been significant changes in this composition.

After a 2017 Chinese government ban on trading bitcoin using renminbi, this composition looks dramatically different as of August of 2019. In the 30 day period leading up to August 24th, the US dollar made up around 43% (up from 32%), euro made up around 21% (up from 3%), yen made up around 14% and British pound made

FIGURE 20

Trading Volume by Currency



Data Source: Bitcoinchart, 2019.

up around 13% (up from 1.2%).

Given the current state of cryptocurrencies in practice, there remain several barriers to overcome when comparing these with the objectives from Nakamoto (2008) discussed above in Section B. We can classify some of these challenges as relating to:

- **Token Supply**
- **Decentralization**
- **Security and Anonymity**
- **Transparency and Governance**

TOKEN SUPPLY

The supply of many cryptocurrencies increases at a fixed 'controlled' rate every year and is not actively managed by any centralized authority, which has led to wide swings in their value – for example, the value of 1 Bitcoin climbed to almost 20,000 USD to fall back to around 3,000 USD before slightly rebounding and fluctuating around 10,000 USD over a short two-year period.

In practice, the supply of Bitcoin is increased at a fixed rate by rewarding miners who are incentivized through award determined by a fixed schedule pre-programmed in the Bitcoin source code. As of 2019, the reward amounted to 12.5 BTC; however, every 210,000 blocks Bitcoin halves this reward to regulate the total supply of Bitcoin. Miners also can be rewarded by fees attached to the transactions they help record in a decentralized ledger. This ability to increase the supply of Bitcoin through mining is similar to the supply of money under the gold standard, where it cannot be adjusted to meet economic circumstances. Recalling from Chapter 1, this was a significant contributor to the gold standard working "as the mechanism that turned an ordinary business downturn into the Great Depression" (Eichengreen and Temin, 1997, p.1).

Because the supply of money cannot be actively adjusted to meet demand dramatic fluctuations in value of the most popular cryptocurrencies have occurred since their inceptions. This has led many observers, based on the three basic characteristics of money (unit of account, store of value, means of exchange) to rightly conclude that most cryptocurrencies are, in fact, not money.

In response to the large fluctuations in value, a second generation of cryptocurrency has been designed that pegs a token's value to an existing currency or basket of currencies. 'Stablecoins' are currently being used primarily as a tool for exchanges to trade between fiat and cryptocurrencies, and privately between large enterprises to settle trades. While stablecoins are very new at the time of writing this report, the future looks optimistic as evidenced by some high-profile projects listed below in Table 3.

DECENTRALISATION

In Section B, several advantages of blockchain-based cryptocurrencies were identified, over other forms of money, mainly, overcoming the risks associated with single

TABLE 3

Stablecoin Projects (Inception date and capitalization)

Cryptocurrency Stablecoins by inception date	Permissioned Stable Tokens (Enterprise)
Tether (2015) $4.1B	Fnality (aka Utility Settlement Coin, 14 Banks – 5 Fiat Currencies)
USD Coin (2018) $477M	JPM Coin (JP Morgan)
Paxos Standard (2018) $260M	IBM Blockchain World Wire (47 currencies, 44 banking endpoints plus 6 stable value coins)
TrueUSD (2018) $195M	
DAI (2017) $82M	
Stasis Eurs (2018) $35M	
Gemini Dollar (2017) $10M	
Token X (2019) $5M	
Digital Garage JPY-Token (2019)	

point failures preventing exclusion, abuse and mistrust, and reducing unreasonably high fees. In practice, these still have barriers to overcome.

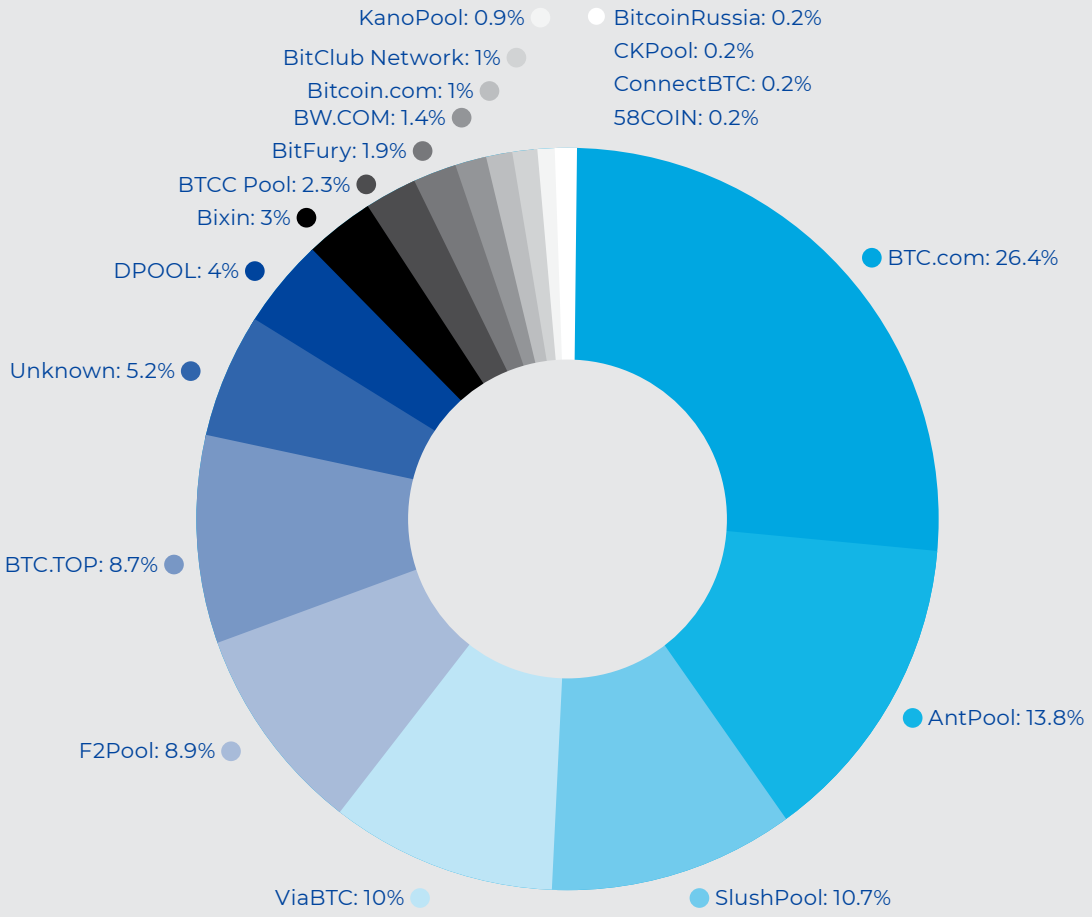
Single Point of Failure

While the mining activity is, in principle, decentralised and has very low barriers to entry (a computer with Internet access), over time there are incentives for a degree of centralisation in the activity. With centralisation of mining activity, the issue of Single Point of Failure is no longer resolved through a decentralized network, since a large mining pool could compromise the integrity of the whole network. For example, a dishonest miner who has more than 50% of the total ability of the network to generate blocks may be able to successfully confirm fraudulent transactions.

Another factor which would lead to further centralisation is the very low expected payoff to individual miners – a single miner has an extremely low chance of finding a solution to the block. In order to smooth the cashflow from newly minted Bitcoins and transaction fees, miners have an incentive to coordinate and work in large mining pools instead, to ensure regular cashflow.

FIGURE 21

Mining Pools with Highest Hash Rate



Source: bitcoin.stackexchange.com, 2019.

Lastly, there are economies of scale to mining – companies specialising in mining can negotiate better rates with mining equipment producers and local electricity providers and can further benefit from locating and moving their activity depending on the current electricity market conditions. In this case, unregulated mining pools would grow to become fewer and fewer in number – as seen in Figure 21, there is already significant degree of centralisation in mining.

The environment for natural monopolies to flourish has led the Bank of England to concluded as far back as 2014 that, "a significant risk to digital currencies' sustained use as payment systems is therefore that they will not be able to compete on cost without degenerating — in the limiting case — to a monopoly miner, thereby defeating their original design goals and exposing them to risk of system-wide fraud." (Ali, Barrdear, Clews and Southgate, 2014) (Ali et al, 2014, p.6).

Exclusion, abuse and mistrust

As discussed above, the centralisation of mining could lead to a situation where a few cooperating pools have more than 50% of a network's hash-rate, in which case

they could, as is the case with any centralised system, accept a double-spent transaction or abuse their power to censor certain transactions. Arguably, neither would be in their long-term interest, as in the end miners' profitability depends on the value of the network itself, especially in the case of Proof of Stake models, and their sunk costs (mining equipment and infrastructure) are heavily specialised and of little use for other tasks. However, this could work as a short term 'get rich quick' scheme where a conglomerate of miners could defraud the system and quickly sell all of their cryptocurrency gains for a more reliable type of money (or other financial asset).

In July 2014 the mining pool Ghash.io exceeded 50% of Bitcoin computational power. This is not the only option to break the honest mining assumption; another possibility is collision between miners. In fact, there are different possible attack strategies, incentives and condition in which the stability of the consensus mechanism is in threat (Bahack, 2013; Garay, 2014; Sirer, 2014).

This possibility of miners, along with influential players altering and forcing specific rules on the Bitcoin network challenges the assumptions of decentralisation. Recently, the Bitcoin community witnessed a panic by a suggestion of Binance CEO of "reorganizing the chain" after the exchange was hacked and lost $40 million in Bitcoin.

Fortunately, influential actors advised not to go through with the idea in fear of losing trust in Bitcoin. This conclusion was the main argument of Nakamoto against the majority miner attack, where he argued that "in the long term, it is better to play by the rules" (Nakamoto, 2008).

Lower Fees

Despite not being classified as money, Bitcoin has succeeded in providing a cheap way of transferring large amounts of capital. While the transaction fees have changed significantly over time, on average it cost less than $1 to have a transaction settle on blockchain with an expected time of 10 minutes (one block). The challenge comes when we consider a network for micropayments, as the blockchain fee is (approximately) fixed regardless of the value of the transaction. This makes day to day transactions using Bitcoin no cheaper than using a debt, a credit card or other third-party payment systems. There are plans to ramp up the speed and efficiency of Bitcoin transactions, which could help to bring down costs in the future.

There also exist significant, and well-documented, electricity costs associated with Proof of Work frameworks, requiring huge amounts computational power for a vast network of users, the scale of which was perhaps not envisioned by Nakamoto in 2008. The electricity requirements for solving blocks makes this a popular activity in countries with subsidized electricity such as

Mongolia. This creates additional issues regarding the degree of centralised control for consortiums in a supposedly decentralised network.

SECURITY AND ANONYMITY

For all practical purposes, Bitcoin provides 'pseudo-anonymity' only. As the history of all transactions is openly available, with sufficient investigative resources one can often statistically infer the identity of a person behind a public key.[15] There exist useful advantages of cryptocurrencies in sending international transfers to countries where they would otherwise be seized by the banking system, as well as a store of value in countries with rampant inflation rates [see examples in Chapter 2]. There has been little evidence of governments in countries expending significant effort in curbing this activity.

Another important drawback of currencies that are anonymous and fully independent of state control relates back to the same arguments made by Sands (2016) and Rogoff (2017). If a given type of currency offers anonymity and the guarantee that nobody, including law enforcement, would be able to access the record of transactions, it is very likely that criminals would use this for their financial transactions. In fact, from the perspective of those who wish to perform illegal activities, fully anonymous digital currencies are even better than cash. At least cash has a serial number in most countries, which helps to trace its path. Moreover, because of its physical nature, transferring large amounts of cash is a cumbersome activity that requires a lot of effort from criminals. With a non-trackable digital form of money, illegal financial transactions could be done instantly and on a global scale.

A good example of how financial innovations in the field of currency can quickly become a tool for the daily financial routine of illegal activities is Liberty Reserves. Liberty Reserve was a company based in Costa Rica that allowed people to send and receive secure payments without revealing account numbers or real identities. This was done via the company's private money, Liberty Reserves, which could be converted into Euros and Dollars. The company started to operate in 2006 and, a few years later, in 2013 it was closed by the US government for being charged for money laundering and other financial crimes. In 2016, the founder of Liberty Reserve, Arthur Budovsky, pleaded guilty to conspiring to commit money laundering and was sentenced to 20 years in jail. Examples like Liberty Reserves show us that the use of privately issued currencies, with no state backing, will require some form of regulatory and law enforcement authority to ensure the legitimacy of its use.

The good news is that cryptocurrencies in practice are not anonymous (as discussed in section B). The pseudo-anonymity of cryptocurrencies allows for easier tracking of transactions than is the case with cash. There exist costs to tracking transactions which means transactions, however, of average people will remain anonymous but law enforcement agencies can trace illegal activities.

An excellent example come from Chainanalysis who enabled law enforcement in thirty-eight countries to make over 330 arrests of alleged pedophiles and rescue 23 children from abusive situations.

GOVERNANCE AND CONSENSUS PROTOCOLS

While the intention of Proof of Work consensus protocols like Bitcoin was to create a democratic decentralised system where all participants have some ability to contribute, it has been found that "the distribution of computing power in Bitcoin reveals that the power of dedicated 'miners' far exceeds the power that individual users dedicate to mining, allowing few parties to effectively control the currency" (Gervais, Karame, Capkun, and Capkun, 2014). At the time the cited article was published, the top-three (centrally managed) mining pools controlled more than 50% of the computing power in Bitcoin. Furthermore, Bitcoin users do not have any direct influence over the appointment of the administrators making governance frameworks, which is not very dissimilar

15. Source: Bohannon, J. (2016). Why criminals can't hide behind Bitcoin, Science Mag. https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

from those found on Monetary Policy Committees in Central Banks. [16]

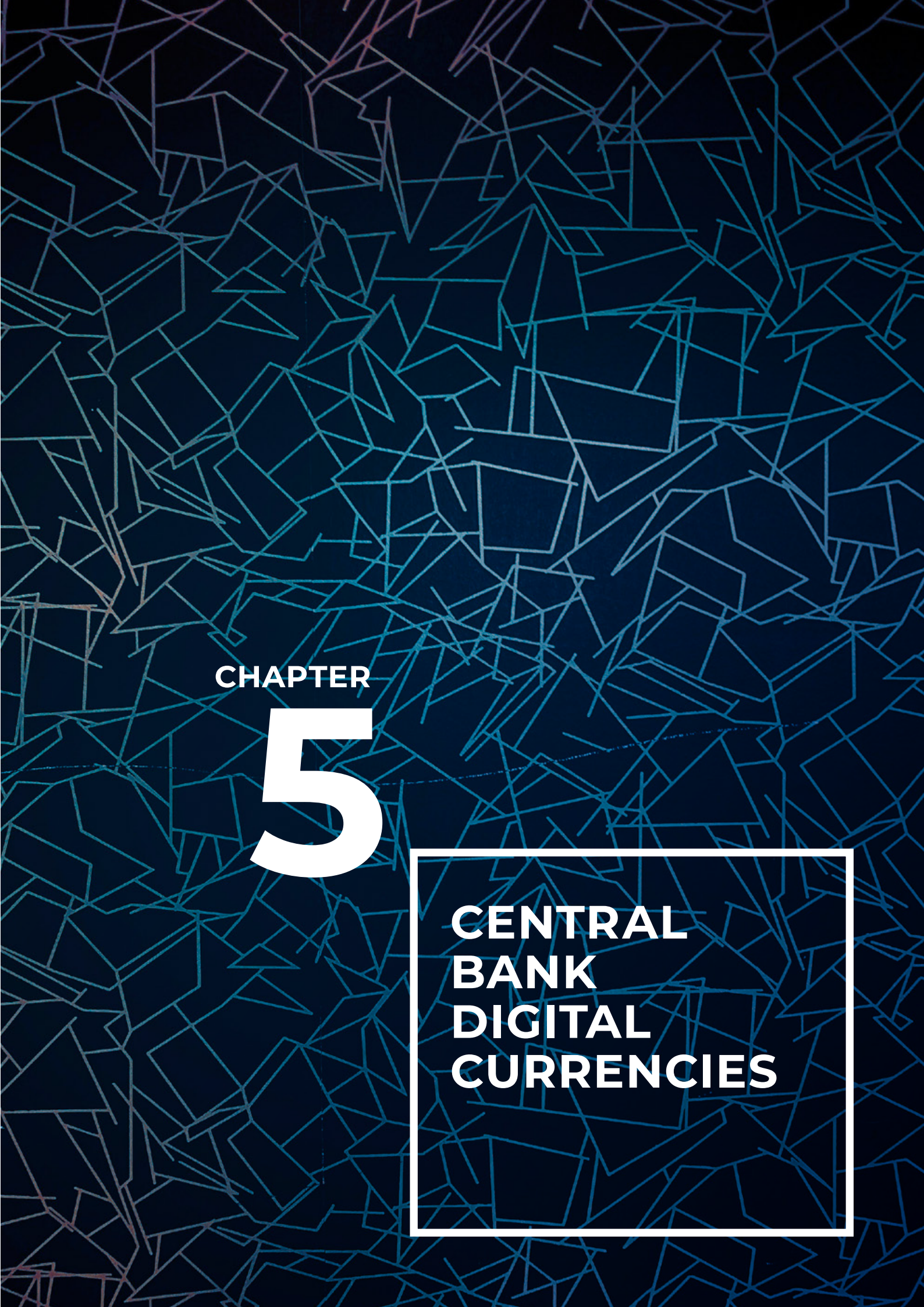
With Proof of Stake, consensus protocol control resides in the hands of those with the most tokens, whose interests may not match those of users in general. The quasi-anonymity of these users also allows them to make decision without a very high degrees of transparency. While Proof of Stake ensures that all participants gain or lose from the network's success or failure, there is opportunity for short-term gains with less transparency than is currently provided from traditional money managers like Central Banks and commercial banks. From a governance perspective, this could potentially be a step in the wrong direction when it comes to the democratization of money management.

Because of the challenges for cryptocurrencies, as they currently exist to become viable widely used forms of money, it has been argued that "digital currencies do not currently serve a substantial role as money in so-

16. See Gervais, A.; Karame, G. O.; Capkun, S.; Capkun, V., 2014

ciety and,... face significant challenges to their widespread use over the long run" (Ali et al, 2014, p.281). Given that consumers and businesses "already make retail payments electronically using debit and credit cards, payment applications, and the automated clearinghouse network" and "are finding easy ways to make digital payments directly to other people through a variety of mobile apps" (Brainard, 2018).

In summary, cryptocurrencies are struggling uphold their creator's objectives. To date, no existing cryptocurrency has been universally successful in fulfilling the role of 'money'. This is partly due to the technical issues raised throughout this chapter, and partly due to the fact that policymakers, academics and the general public have all held generally negative attitudes about the prospects of money being issued and managed in a decentralized framework and/or by private sector actors. From this perspective, central banks in most advanced economies have built a trust premium compared to private sector companies, which should make them better candidates for issuing money and managing/regulating financial transactions. We will look at this more closely in Chapter 6 for the US, UK, Germany, France, Brazil, Argentina, Mexico and Spain.



CHAPTER

5

CENTRAL BANK DIGITAL CURRENCIES

As emphasized throughout the previous chapter and by other contributors,

> **“The key innovation of digital currencies is the ‘distributed ledger’ which allows a payment system to operate in an entirely decentralised way, without intermediaries such as banks. This innovation draws on advances from a range of disciplines including cryptography (secure communication), game theory (strategic decision-making) and peer-to-peer networking (networks of connections formed without central co-ordination).”**
>
> — *Ali et al, 2014.*

The technical evidence from the previous chapter suggests that a Hayek-type digital currency has so far been unsuccessful in achieving achieve its creators’ intended purpose. The technology introduced by Nakamoto (2008), however, is still extremely valuable when it comes to improving money and, more importantly, its payment systems. This can be achieved by incorporating blockchain technology into existing institutions, mainly central banks.

A. Principles of CBDCs

Central bank digital currency (CBDC) can be broadly defined as "any electronic, fiat liability of a central bank that can be used to settle payments, or as a store of value" (Barker et al, 2018, p.2). Note that, unlike the case of cryptocurrencies, CBDCs are considered a liability on the central bank's balance sheet (see last part of Chapter 2) As will be demonstrated in the next section, established central bank currencies have a significant advantage as a trusted form of money rather than an entirely new, and not well understood, option. Lagarde (2018) also argues that monetary authorities will continue to remain a pillar of trust given the breadth of work they do, not only issuing stable money but also regulating the financial and payment system.

While providing greater access to digital forms of currency is not a new idea, [17] it has recently gained traction given the debate about the role of monetary authorities in future currency and systems of payment. Even though it is issued by the same monetary authority, CBDC can be considered as a disruptive change to the existing system of payments, which can be slow and tedious. For example, some international transactions can take several days to pass through regulatory checks and clearing houses. The potential use of blockchain technology for improving the efficiency of money raises many questions about the role of central bank money, direct access to central bank liabilities and the structure of financial intermediation.

Some of the characteristics and advantages of a well-designed CBDC would include a practically costless medium of exchange where individuals could hold accounts directly with the central bank. This would allow the central bank to have an additional tool for conducting monetary policy, better information on potentially fraudulent activities and avoid intermediary costs associated with commercial bank lending, especially for lower-income households. CBDCs could also act as an interest-bearing risk-free store of value, with a rate of return in line with other risk-free assets such as short-term government securities. [18] A well-designed CBDC would also overcome the price stability issue that exists with most privately issued cryptocurrencies (with the exception of stablecoins) by actively managing the supply in line with an underlying basket of goods and services.

The Bank for International Settlements (BIS), which works as central bank 'hub' for central banks, has spent a considerable amount of resources trying to understand how monetary authorities across the globe are tackling this issue of cryptoassets. According to Carstens (2019), central banking committees based at the BIS identified two main varieties of CBDCs:

- **A wholesale CBDC that would be restricted to a limited group of users and used for inter-bank payments and other settlement transactions;**
- **A retail CBDC that would be widely accessible to everyone. This could be based either on digital tokens or on accounts.**

17. See: Tobin, 2018; Brunner and Meltzer, 1971.
18. See Bordo and Levin, 2018.

As noted above, an account-based CBDC could be implemented via accounts held directly at the central bank. Such an approach "would be reminiscent of the early years of central banking, when individuals and nonfinancial firms held accounts at the Bank of England and the Sveriges Riksbank" (Bordo and Levin, 2018, p.7). The reason that these individual accounts were discontinued was largely due to the impractical technicalities involved with maintaining such a large volume of accounts. Given the new technology available to central banks, this barrier should no longer exist with the use of an integrated accounting system into the CBDC framework.

There are clear differences between these types of CBDCs and cash. A CBDC in these forms would not necessarily be anonymous. Moreover, unlike cash, it could pay or charge interest. Figure 22 presents the attributes of these of CBDCs and how they compare to the current forms of central bank money.

FIGURE 22. **Design Features of Central Bank Money**

KEY DESIGN FEATURES OF CENTRAL BANK MONEY

	EXISTING CENTRAL BANK MONEY		CENTRAL BANK DIGITAL CURRENCIES	
			RETAIL	
	CASH	RESERVES AND SETTLEMENT BALANCES	TOKEN	ACCOUNTS
24/7 AVAILABILITY	✓	×	✓	(✓)
ANONYMITY	✓	×	(✓)	×
INTEREST-BEARING	×	(✓)	(✓)	(✓)

✓ EXISTING OR LIKELY FEATURE (✓) POSSIBLE FEATURE × UNTYPICAL OR IMPOSSIBLE FEATURE

Source: Bank for International Settlements

B. Current State of CBDCs

In terms of active and evolving research agendas, the Bank of England was one of the precursors on studies regarding cryptocurrencies and CBDCs (Kumhof and Noone 2018; Barker et al., 2018; Barrdear and Kumhof, 2016; Ali et al., 2014). The UK's monetary authority first raised the possibility of a central bank-issued digital currency in their research agenda in 2015. Since then, the most complete work done by the Bank of England regarding CBDCs and their implications has been Kumhof and Noone (2018). The Sveriges Riksbank is also investigating whether an e-krona would provide the general public with continued access to central bank money and increase the resilience of the payment system (see Skingsley, 2016; Riksbank, 2017). Other than the British and Swedish monetary authorities, several central banks are also developing new research agendas for CBDCs. These include the National Bank of Denmark (Gurtler et al., 2017, the Reserve Bank of Australia (Lowe (2017), the Bank of Canada (Engert et al., 2017) and many others. The Committee on Payments and Markets Infrastructures (CPMI) at the BIS did a survey in 2018 with central banks to understand the current

stage of their work on CBDCs and what were their conclusions regarding this topic. More than 60 central bankers participated, representing countries that count for 80% of the world population.

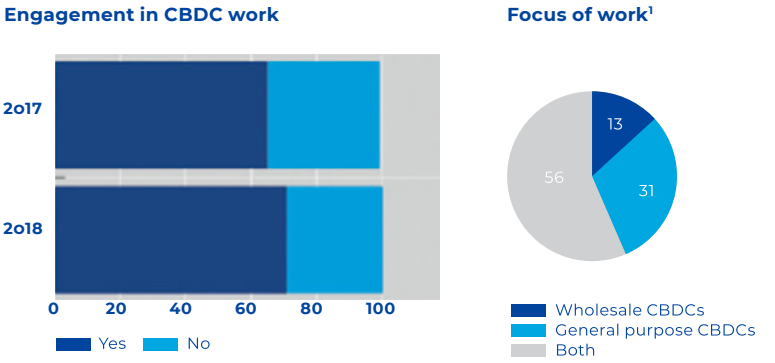
Figure 23 presents the results of this survey. Seventy percent of central banks are working on some sort of CBDC. Nevertheless, only about half of the central banks doing work on CBDCs have actually moved toward testing this idea. According to BIS CPMI's report, this means that central banks are examining the benefits, risks and challenges of potential issuance from a conceptual perspective. Only approximately a tenth of the central banks engaged with CBDCs have moved into the phase of experimenting with the different types of possible technologies, by developing pilot arrangements.

FIGURE 23

CPMI CBDC work in Central Banks

Central Bank CDBC work

Share of respondents

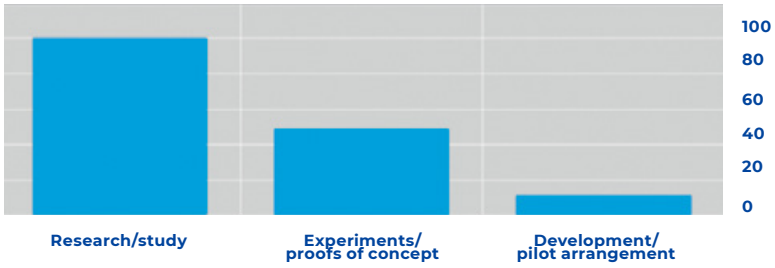


1. *Share of respondents conducting work on CBDCs.*

Source: Bank for International Settlements, 2018.

Type of CDBC work

Share of respondents conducting work on CDBCs

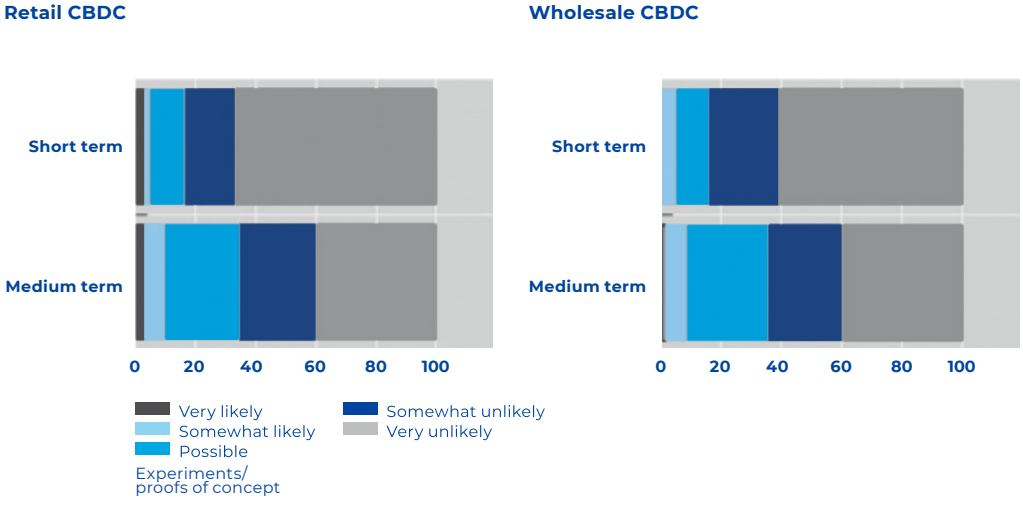


Source: Bank for International Settlements, 2018.

FIGURE 24

Likelihood of Issuing a CBDC in Short/Medium Term[1]

Share of respondents



1. *Short term: one to three years; medium term: one to six years.*

Source: Bank for International Settlements, 2018.

Figure 24 shows the answers of central bankers when asked if they plan to issue a CBDC in the short or medium term. Only a very small amount of these think they are likely to issue a CBDC in the short to medium term. The results are basically the same for retail and wholesale CBDC.

But why have central banks chosen not to provide these digital services? The reason for this lies in probably the most important question regarding the discussion of CBDCs, the impact that the implementation of such currency would have in the financial and monetary systems. Many studies have been made by academics, monetary institutions, and even practitioners in trying to analyse these possible effects. In fact, most of the literature regarding CBDCs has focused on this topic.

C. Impact of CBDCs

> **"If all it did was to reduce the demand for physical cash, it's not clear the macroeconomic effects of a CBDC would be that significant. It's possible the retail payments system might become more efficient. It's also true that, were a CBDC fully to displace paper currency, that would open the door to the possibility of materially negative interest rates."**
>
> — *Ben Broadbent, Deputy Governor for Monetary Policy, Bank of England, 2016.*

In the current fractional reserve system, only commercial banks have access to digital account-based central bank money. By contrast, physical central bank money (i.e. cash) is widely accessible to the general public. As discussed in the previously section, the use of cash will likely diminish as businesses adopt more hygienic and efficient forms of payment. With this possibility, the public would no longer have wide access to central bank money (bank notes), which would need to be replaced with a digital alternative.

If household and business deposits are concentrated in the central bank, CBDC schemes would implicitly end the practice of, and risks associated with, fractional reserve banking. This 'narrowing' of the banking system (depositors deal directly with the central bank) is effectively a revival of the 'Chicago Plan' as discussed in Chapter 2. [19]

In addition to more efficient and safer payments and settlement systems, a CBDC could come with additional benefits. Given that CBDC can allow for digital records and tracing, it could improve the application of rules aimed at anti-money laundering and countering financial terrorism. Moreover, it would also possibly help to reduce informal economic activities. Finally, Lagarde (2018), Coeur and Loh (2018), Broadbent (2016) and many others defend CBDCs as an important tool for financial inclusion, particularly in developing countries, where a significant part of the population is still not included in formal financial systems.

19. See: Raskin and Yermac, 2016.

From a central banker perspective, a CBDC could allow for real-time data on economic activity. Mersch (2017) argues that another benefit from establishing such a CBDC would be to create a direct link between the population and the central bank, hence developing a better understanding of the role of a central bank and the need for such an institution to be independent.

MONETARY POLICY

> **"It is difficult to draw definitive or quantitatively-robust conclusions about the impact of CBDC on the monetary transmission mechanism, due to the large degree of uncertainty around the ultimate design of CBDC, the economic environment it will be introduced into, and the structural changes that may accompany it."**
>
> — *Barker et al., 2018.*

The consequences of CBDC issuance for the implementation and transmission of monetary policy depend on how wide access to CBDC is and whether it is attractively remunerated. Monetary policy arguments for issuing CBDC include strengthening of the pass-through mechanism of the policy rate to money markets and deposit rates, potentially making negative rates a more effective tool in boosting economic activity. Such a change, however, could also bring new risks to monetary policy.

Monetary policy implications are likely to be more pronounced if a CBDC emerges as an attractive asset to hold. According to Coeur and Loh (2018), if a CBDC is set as a new and liquid central bank liability, it is likely to have an impact in the channels of transmission of policy rates to money markets and beyond. Given the high demand for low-risk government-issued assets over the last decade, a CBDC would be likely to affect holdings by investors, particularly in markets for liquid, low-risk instruments (such as government bonds). If institutional investors could hold CBDCs without limits, the interest rate on these would help to establish a hard floor under money market rates, as this financial instrument would be the government bond with shortest (instant) duration.

Regarding households, if a CBDC is implemented in such a way that it becomes a viable alternative to commercial bank deposits, it would be able to make the rates on these deposits more linked to what the central bank would pay on its digital currency. As a result, this is likely to strength the pass-through mechanism of the policy rate to the general public.

Since the 2008 crisis, developed markets have dived into negative rate territories. As we currently stand in 2019, it does not seem like we are surfacing anytime soon. In fact, more recently, interest rates in emerging economies are also converting to historical lows. With even the monetary authorities of emerging markets starting to discuss the possibility of negative interest rates for government bonds, a tool to pass these rates to money markets and deposit rates would be welcomed by central banks.

In the fractional reserve banking system that we have, monetary authorities are able to charge negative rates on bonds and deposits that financial institutions hold at the central banks. Nevertheless, the effectiveness of the monetary stimulus of setting negative rates is limited. Financial institutions cannot pass these rates to client's deposits, since they always have the option of holding cash, which yields a non-negative rate. If monetary authorities were to replace cash by an interest-bearing CBDC, this would open the possibility of expanding negative yields to accounts of households and firms in the real economy, hence increasing the effectiveness of negative interest rates. In fact, Goodfriend (2016) and

Dyson and Hodgson (2016) argue that the issuance of CBDCs could alleviate the pressure on the zero lower bound even if physical cash was not extinct, as long as it came along with a reduced desire for cash holding.

As it currently stands, however, the dependence of key market rates on the policy rate seems to be satisfactory to most central bankers (Coeur and Loh, 2018). Even though these are not perfectly correlated, this does not represent a challenge as long as central banks have enough control over the financial system and its institutions.

Regarding the effectiveness of CBDC as a tool to impose negative interest rates on the general public, it is uncertain how this would work in practice. General equilibrium effects may make the implementation of such strategy unfeasible even with digital currencies. There is no guarantee that society would accept a negative yielding currency to be "imposed" by central banks. By trying to set negative interest rates more broadly, monetary authorities could in fact cause the demise of national fiat money, as people could escape to non-negative yielding competitors, like commodity money or even cryptocurrency alternatives.

The overall effects of CBDC on the term structure of interest rates are very hard to predict and will depend on many factors. More generally, the implications of a CBDC relative to other instruments are likely to depend on each jurisdiction's specific operating environment. Also, since operating environments may change in the future, monetary policy cost-benefit analyses related to CBDCs may need to be revisited periodically.

Finally, weaker demand for cash does not imply the need for CBDCs. In fact, monetary policy can remain effective even without cash. [20] On balance, the study from Coeur and Loh (2018) argues that it is not clear that there is a strong basis at this time to issue a CBDC for the purpose of enhancing the efficacy of monetary policy.

20. See Woodford, 2000.

FINANCIAL STABILITY

Implementing a CBDC would almost certainly imply in a more active role for central banks in financial intermediation. This would not, however, necessarily mean more financial stability. One example is that by having to passively accommodate the demand for CBDC, the central bank could potentially introduce a high level of volatility in the demand for government debt.

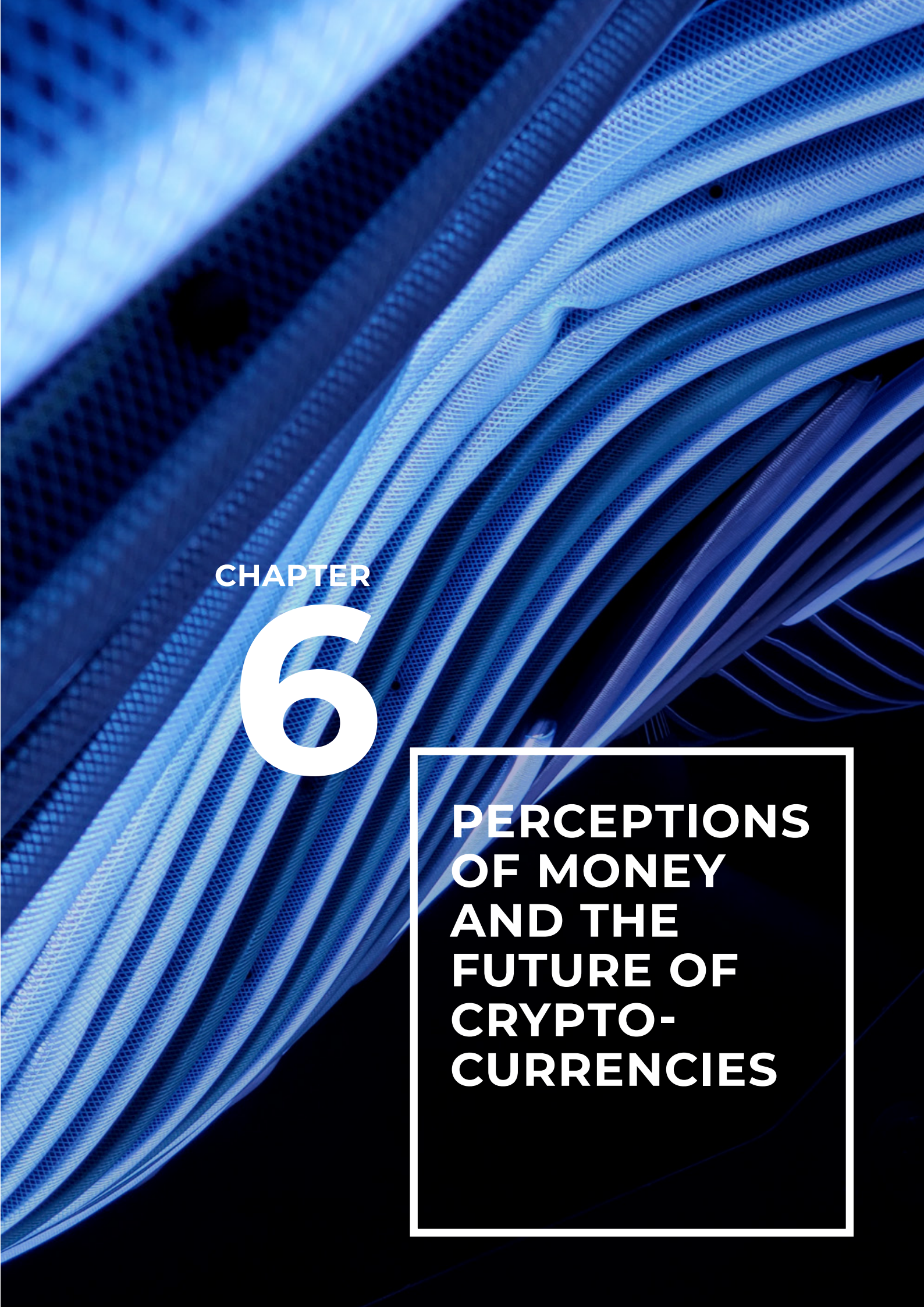
A general purpose CBDC could have a large impact on the structure of financial intermediation and the activity of traditional banks. If this digital currency is attractive to individuals and firms, it could result in a withdrawal of funding to commercial banks. This could lead some banks to raise spreads and increase transaction fees in order to maintain profitability. Depending on how the financial system is organized, banks might have to shrink their balance sheets, with possible adverse economic consequences.

Arguably, the most significant and plausible financial stability risk of a general purpose CBDC is that it can facilitate a flight away from private financial institutions and markets towards the central bank. Faced with systemic financial stress, households and other agents in both advanced and emerging market economies tend to suddenly shift their deposits towards financial institutions perceived to be safer and/or into government securities. Of course, agents can already shift funds towards the central bank by holding more cash. But a CBDC could allow for digital runs towards the central bank with unprecedented speed and scale. Even in the presence of deposit insurance, the stability of retail funding could weaken because a risk-free CBDC provides a very safe alternative.

The central bank could try to manage the interest rate on this CBDC in order to control such runs. Nevertheless, changes on this rate, even towards a negative territory, may be unsuccessful in periods of economic turmoil when agents seek safety at almost any price. Another solution could be to impose quantitative limits on the amount of CBDC that each individual or firm could hold. But this would most likely result in price differences between different types of money, in contradiction to the principle of money being exchangeable at par and hampering the conduct of monetary policy.

Overall, one can notice that a lot of the questions raised by the issuance of CBDC are very similar to the points once discussed by those who advocated for full-reserve banking. Back then, those who defended a narrower banking system - famously Fisher (1936) in what became known as the “Chicago Plan” - advocated that such a setting could make the overall financial system safer because it would limit the ability of the private banks to create money and exacerbate business cycles.

Although narrow banking raises many questions in its own right, the introduction of a CBDC does not necessarily entail the same restrictions of a full-reserve banking system. In fact, the term is used in a general way, but each monetary authority could issue a digital currency and model payment systems tailored to the necessities and idiosyncrasies of the local economy, while considering the cross-border and global dimension of this CBDC.



CHAPTER

6

PERCEPTIONS OF MONEY AND THE FUTURE OF CRYPTO-CURRENCIES

> **"It can be plausibly argued that much of the economic backwardness in the world can be explained by the lack of mutual confidence."**
>
> — *Arrow, 1972.*

A key theme throughout this report is the importance of trust in maintaining a successful fiat currency. This trust has traditionally been vested in public institutions (central bank), but digital methods of payment performed by private companies have successfully existed for many years (credit cards, debit cards, etc.). A more recent example can be found in Kenya where a recent study by Kaminska found that M-Pesa "appears to have succeeded because Safaricom, which is 40% owned by the multinational giant Vodaphone, is trusted by the public more than the Kenyan banking system" (Kaminska, 2015). She notes, however, that that "M-Pesa really resembles a money transmission service more than a standalone currency, since its sponsor collateralizes units of M-Pesa with Kenyan hard currency deposits in escrow accounts" (Kaminska, 2015). In this case, central banks remain responsible for the creation and management of narrow money, but the private sector takes over when it comes to system of payments (transacting with money).

Despite the key role that trust plays in maintaining/preserving the value of fiat currencies, there is surprisingly little empirical work surveying the general public, especially across a diverse sample of countries. In order to help rectify this gap, we designed a two-stage survey across eight countries (US, UK, Germany, France, Spain, Argentina, Brazil, Mexico). The first stage asks respondents about their opinions regarding different types of money (cash, credit cards, digital payment companies (PayPal, AliPay, AmazonPay, etc.) and cryptocurrencies (Bitcoin, Libra)) and their understanding of how money is created and managed. In the second stage, we designed a conjoint survey experiment where respondents were provided with a range of hypothetical currency choices based on five underlying attributes in order to estimate comparable magnitudes for people's willingness to own that type of money. We will provide a demonstration and discuss the results in the second part of this chapter.

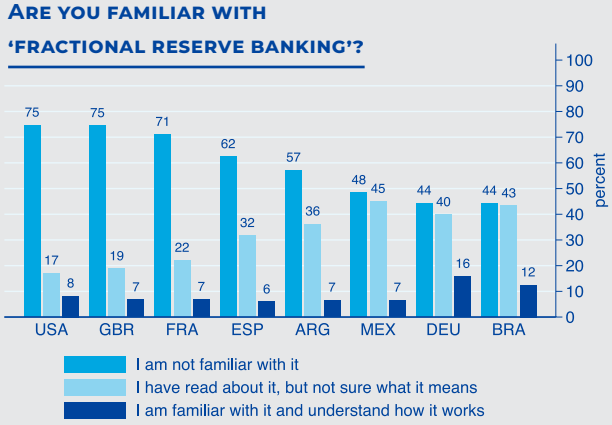
A. Current Understanding of, Trust in, and Preferences for, Money

At present, there is limited general public understanding of how money is created:

> **"The public has almost never really understood what the Fed is or what it does...What's different today is that there is a combination of confusion and strong opinions: People don't quite know what the Fed does, but public trust in the Fed is at a historic low. It's that combination that is dangerous."**
>
> — *Conti-Brown, 2017.*

FIGURE 25

Understanding of Fractional Reserve Banking



Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

New results from the IE Survey on 'The Future of Money' suggest, unsurprisingly, that the majority of respondents are either, not familiar with fractional reserve banking (between 44 and 75%), or, are familiar with it but not sure what it means (between 17 and 43%). Interestingly, the US and UK rank amongst the lowest in terms of understanding fractional reserve banking with around half of the degree of understanding in Germany.

In a 2012 UK Government Office for Science research paper, Dr Y.V. Reddy, (former Governor of the Reserve Bank of India) was quoted saying that: "Trust is difficult to measure, but on the basis of surveys conducted and anecdotes reported in the media, there appears to be an erosion of trust in the financial sector as a whole, and banking in particular, in advanced economies". [21] There

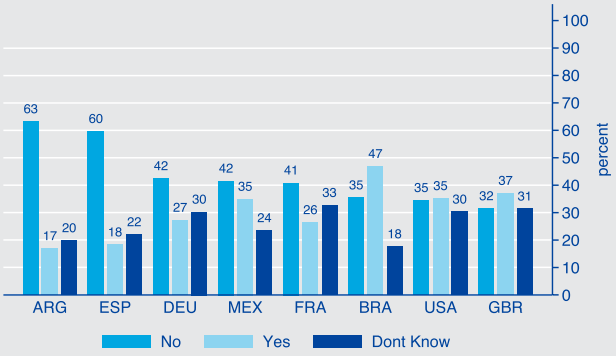
21. See: Vanston, 2012.

is continued evidence of this erosion of trust over ten years after the financial crisis. For example a 2018 YouGov poll of 2,250 adults on behalf of campaign group Positive Money found 66% of adults in Britain do not trust commercial banks to work in the best interests of society, with only 20% stating that they do trust banks to work in the best interest of society (White, 2018).

FIGURE 26

Government response to Financial Crisis

GOVERNMENT HAS TAKEN MEANINGFUL STEPS BY REGULATING THE BANKING SECTOR SINCE 2008 TO PREVENT ANOTHER FINANCIAL CRISIS



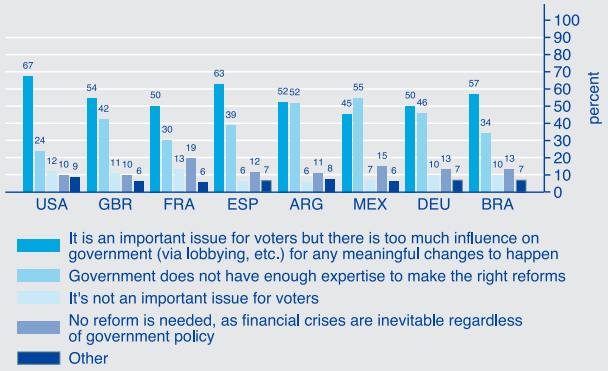
Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

Part of this lack of trust may come from people's attitudes toward the government's regulatory response to the financial crisis. From Figure 26, we can see that many respondents in our survey felt that government has not taken meaningful steps in regulating the banking sector since 2008. From the above figure we can see that there is considerable amount of variation with the majority of respondents in Argentina, Spain, Germany, Mexico and France believing that government has not taken meaningful steps in regulating the banking sector since 2008. In Brazil and the UK, a slight majority believe that government has taken meaningful steps, while Americans were split 35%–35%.

FIGURE 27

Explaining Government Response to Financial Crisis

WHY NO MEANINGFUL STEPS HAVE BEEN TAKEN



Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

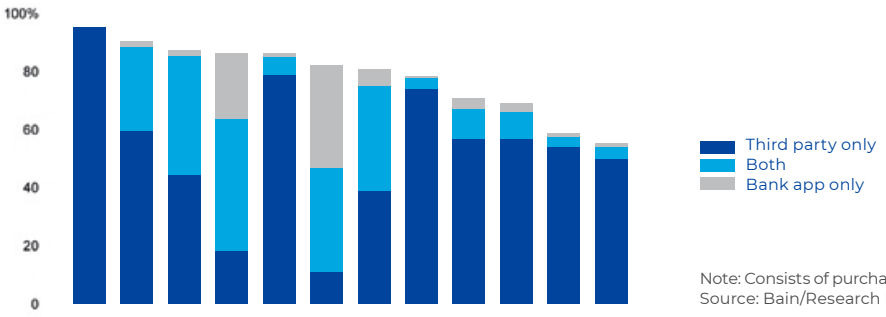
Given the high levels of dissatisfaction with government response to the financial crisis, we asked those respondents who answered 'no' to the previous question to identify why they feel that government has not taken meaningful steps. From Figure 27, it appears that the majority of respondents in almost all countries in our sample felt that it is an important issue for voters in their countries, but lobbying exerts too much influence on government for any meaningful changes to take place'. Interestingly, the two financial centres of the world (along with Spain) had the highest levels of agreement that government was overly influenced by lobbying efforts.

This continued erosion of trust and lack of effective government response may contribute to an increasing willingness for people to adopt alternative ways to store money. For example, a 2018 Bain survey of 151,894 consumers in 29 countries found that 29% of respondents trust at least one tech company more than their primary bank and 54% of respondents trust at least one tech company more than banks in general (Bradley et al., 2018).

FIGURE 28

Distrust of Banks and use of Third-Party Payment Apps

PERCENTAGE OF RESPONDENTS USING BANK OR THIRD-PARTY PAYMENT APPS FOR PURCHASES



Note: Consists of purchases made online or at point of sale in the prior three months.
Source: Bain/Research Now SSI Retail Banking NPS Survey, 2018.

Source: du Toit, G., Bradley, K., Swinton, S., Burns, M., De Gooyer, C. (2018), "In Search of Customers Who Love Their Bank", Bain & Company.

Despite people's movement towards private third-party payment systems, our survey results suggest that they still prefer that central banks create and manage money. From Figure 29 we can see that the majority of respondents (between 65% and 89%) in all of the countries in our sample trust central banks and commercial banks to create and manage money (as their first/second choice). Specifically, central banks are the most trusted across all countries and commercial banks, with the exception of Germany, which prefers the central government to commercial banks, are the second choice for respondents. In the case of Mexico, the central bank and commercial banks have fairly equal levels of trust, while the government has incredibly low levels of trust.

FIGURE 29

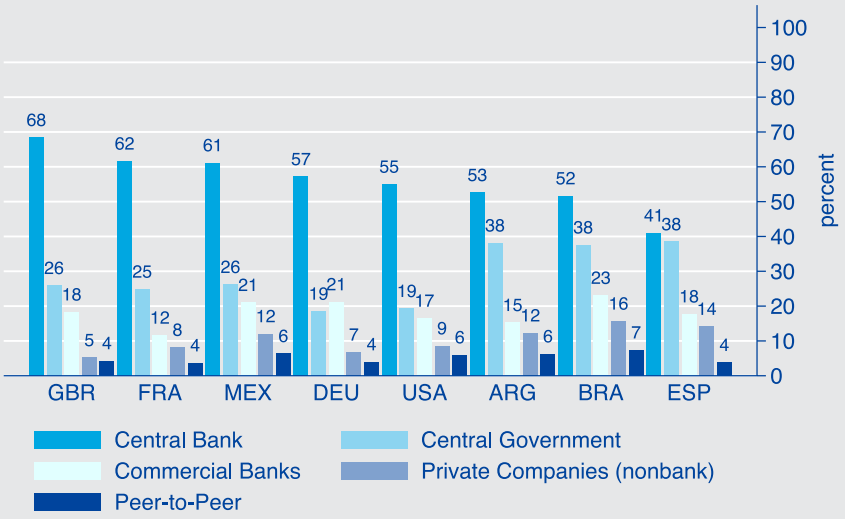
Trust in Institutions for Creating and Managing Money

Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

These results do not show very optimistic prospects for the successful launch of Hayek-type currencies with very limited support for private companies (i.e. Facebook) or peer-to-peer networks to create and manage money. Putting this together we can see from Figure 30 below that central banks are the most preferred institution for creating and managing money.

FIGURE 30

Who Should Create and Manage Money in your Country?



Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

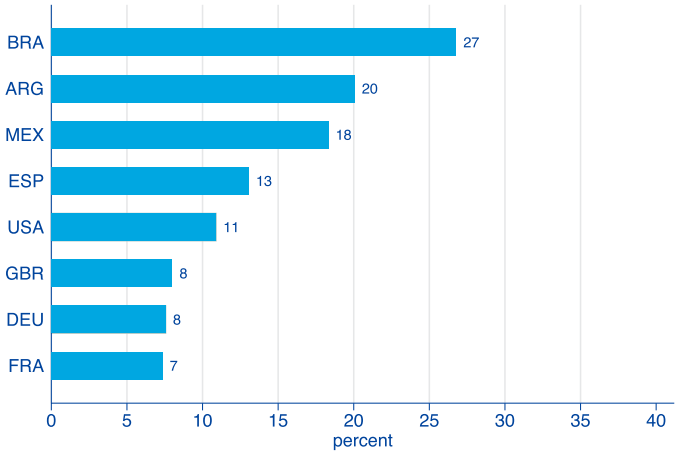

THE THIRD GENERATION
9999 FINE

B. Ownership of Cryptocurrency

In a June 2018 ING survey on cryptocurrencies, 8% of Americans, 6% of UK residents, 8% of German residents, 6% France residents and, 10% Spain residents reported owning cryptocurrencies.[22]

FIGURE 31

Ownership of Cryptocurrencies



Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

In the 2019 IE survey, there has been an increase in all countries with the exception of Germany, which remained unchanged. Specifically, there was a 3% increase in American ownership of cryptocurrencies, a 2% increase in UK ownership, a 1% increase in French ownership and a 3% increase in Spanish ownership.

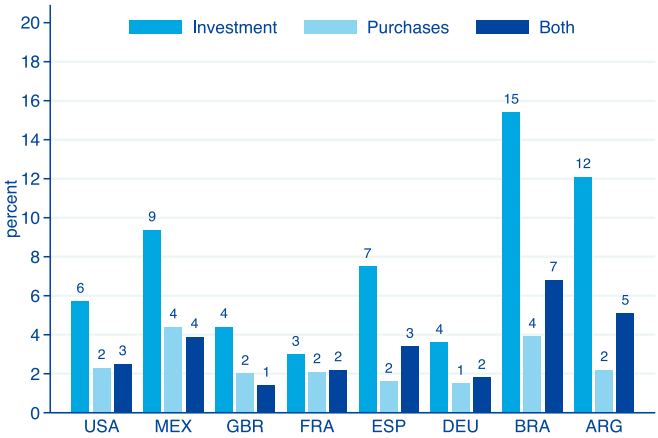
Among owners of cryptocurrencies, these are predominantly held as investments, especially in countries where the ownership levels are highest. In almost all countries, only about 2% or owners claim to use these specifically for purchases.

22. See: Exton, 2018.

FIGURE 32

Reason for Ownership of Cryptocurrencies

DO YOU OWN CRYPTOCURRENCY AS AN INVESTMENT OR FOR PURCHASES?

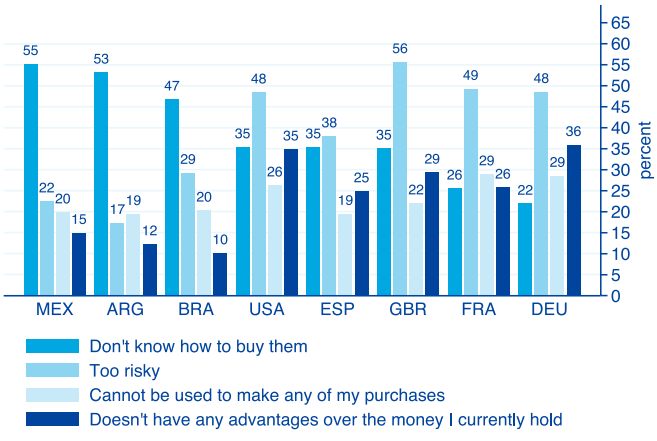


Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

FIGURE 33

Reason for not Owning of Cryptocurrencies

WHY DO YOU NOT OWN CRYPTOCURRENCIES



Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

For those who don't own cryptocurrencies, we found that, in the case of Mexico, Argentina and Brazil, the reason for not owning cryptocurrency was not due to a lack of interest, but not knowing how to buy them. In the case of Mexico, 55% of respondents said they did not own cryptocurrencies because they didn't know how to buy them with 53% and 47% in Argentina and Brazil, respectively.

For the US, UK, Spain, France and Germany, the majority of respondent did not own cryptocurrencies because they felt they were too risky. There was also a higher emphasis on cryptocurrencies not having ant advantage over the currencies which were currently being used. In general, these results suggest that countries with a less stable history of monetary stability are more open to new types of money. This brings us to the future of cryptocurrencies.

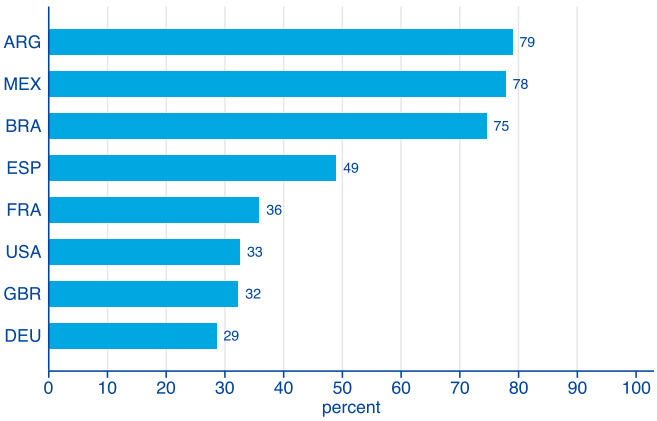
C. Future of Cryptocurrencies

As discussed in the previous section, cryptocurrencies have not yet manifested themselves as intended by their creators, mainly, as useful form of money, relative to other already established options (physical and digital). This does not mean that cryptocurrenices will not become slowly integrated into societies as their infrastructure improves. For example, Facebook's Libra aims to widen access to financial services and lower transaction costs while ensuring the value of the coin by being fully backed by 'low-volatility assets, including bank deposits and government securities in currencies from stable and reputable central banks'. Holders of Libra will not be paid interest that the underlying assets generate – the cashflow will be used for the Foundation. The presence of negative interest rates on some of the underlying assets may force the foundation to rebalance their holdings to avoid passing a loss on to their customers or to pass on these costs to owners of that currency. Banking system may well ride on the back of it – not unlike the existent repo-based shadow-banking system in Bitcoin. The blockchain starts as permissioned, with a prospect of being permissionless – again, it is unclear why the founding partners (i.e. the 'permissioned' parties) would choose to give up this privilege in the future.

To get an idea of willingness to use an effective cryptocurrency (one that fulfils all of the requirements of a successul form of money), we asked respondents about their willingness to use this type of money if issued by a private company.

FIGURE 34

Willingness to use of a New Effective Cryptocurrency



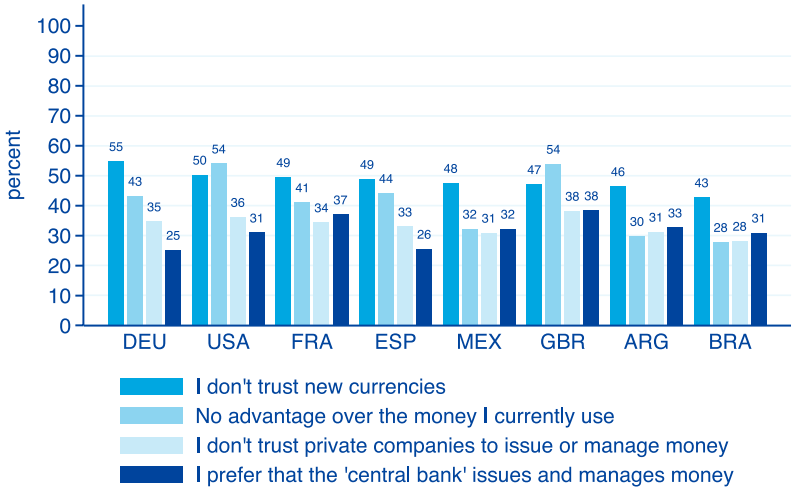
Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

Suppose that a new cryptocurrency was designed by a private company (or group of companies) that could be used to make all of your day-to-day transactions (it is accepted by all sellers) and has a stable value over time (low inflation/deflation). This currency could also be converted to other currencies at a very small cost. Would you prefer to use this currency over your current method of payment?

For those who answered 'no' to the above proposition, our survey followed up by asking respondents why they would not prefer an effective privately issued cryptocurrency to their existing currency options.

FIGURE 35

Reasons for Not Supporting a New Effective Cryptocurrency



Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

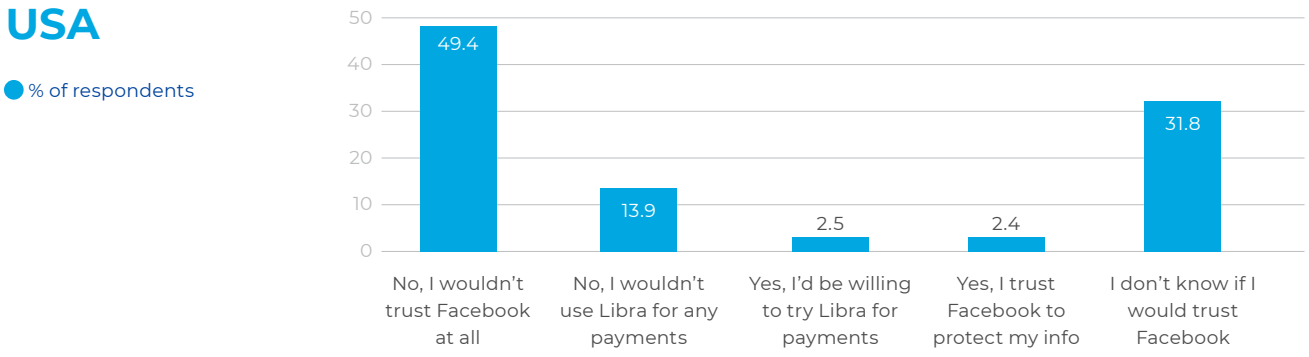
As can bee seen from Figure 35, in all but two countries (US and UK), the most likely reason to not support this hypothetical cryptocurrency was a lack of trust in new currencies. In the case of the US and UK, respondents felt that cryptocurrencies do not offer any advantages over the money they already use.

The recent high profile announcement of Facebook's Libra has led to a variety of surveys and articles written on its viability in terms of consumers' willingness to trust it. The results have not been overly positive. For example, a June 2019 Viber survey of 1,000 US and 1,000 UK residents found that nearly half of respondents in both countries (49%) say they would not trust Facebook at all, and less that 3% and 2% of US and UK respondents, respectively, said they would be willing to try Libra for payments (Viber, 2018).

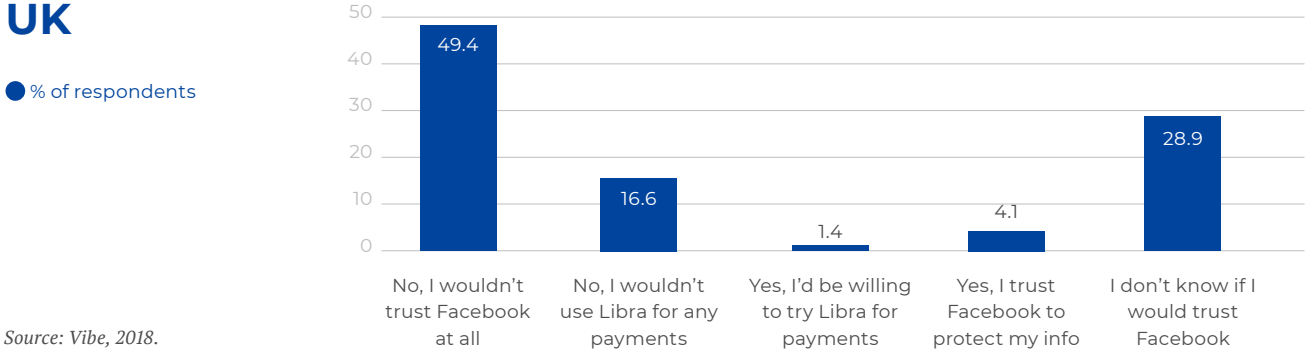
FIGURE 36 **Trust in Facebook in the US and UK**

Would you trust Facebook to keep your information secure when using its new crypto payment service, Libra?

USA



UK

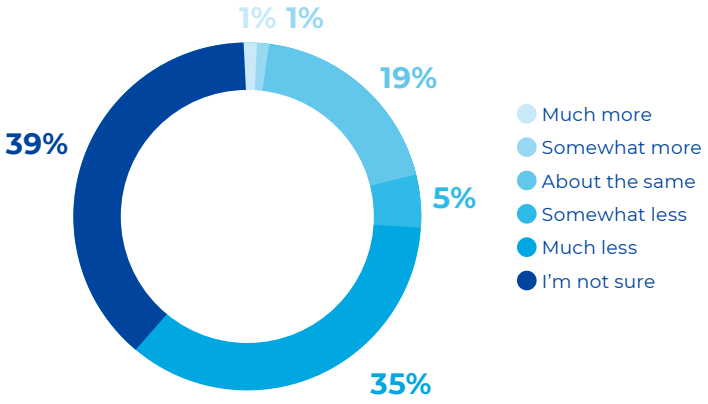


Source: Vibe, 2018.

Another July, 2019 CivicScience survey of 1,799 American adults found that 40% of respondents claimed that they trusted Libra less (35% much less) than Bitcoin and other cryptocurrencies. Only around 2% of all respondents claimed that they trusted Libra more than other more established cryptocurrencies.

2% OF AMERICANS TRUST FACEBOOK'S LIBRA MORE THAN BITCOIN: RESEARCH

Compared to Bitcoin and similar cryptocurrencies, how much do you trust Facebook's new "Libra" currency and digital wallet?



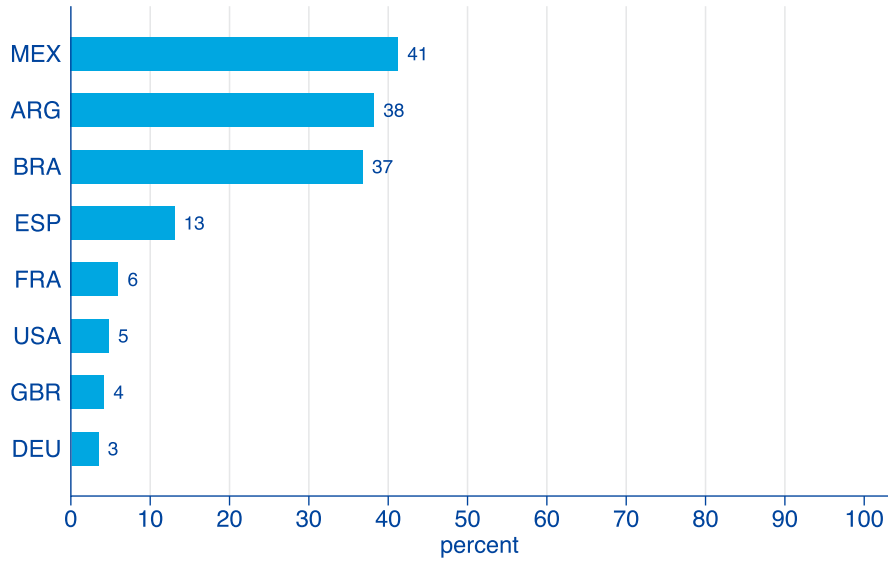
1,770 responses, weighted by U.S. Census 18+

This sentiment is similar in Germany where a July 2019 German citizen's movement survey of 2,093 adult residents found that 71% of respondents were sceptical about Libra with only 12% claiming they would welcome it (Finanzwende, 2019).
To gain a broader understanding of people's trust in the Libra across a wider range of countries, we asked 1,000 respondents in each of the eight countries in our sample whether they would trust Facebook to issue and manage a new cryptocurrency. The results widely vary across countries.

In Mexico, Argentina, and Brazil, there is a much higher willingness to trust a new Facebook issued currency with over 40% of Mexico residents saying they would trust the Libra. In contrast to these three countries, residents of Germany, the UK, US, and France were much less willing to trust the Libra with only between 3 and 6% saying they would trust the Libra.

FIGURE 37

Trust in Facebook to Issue and Manage a New Currency across Eight Countries



Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

CONJOINT ANALYSIS

To gain a deeper understanding of what people want in an ideal currency, we provided 1,000 survey respondents in each of the eight countries in our sample, with ten frames, each of which provided them with a choice between three hypothetical currencies with varying attributes. For the purpose of this exercise, we characterized 'money' as having five underlying attributes:

1. **Issuer/backer** refers to who issues and/or backs that currency. This could be a central bank, a commercial bank (private sector company), or a peer-to-peer nonprofit like Bitcoin (private sector peer to peer).
2. **Acceptability** refers to where are able you use the currency. Is your currency accepted by all sellers of goods/services or only some sellers of goods/services (within the area in which you buy/sell goods and services)?
3. **Transaction costs** are there costs involved in making the transaction (these are commonly known as 'fees', 'premiums' or 'spreads').
4. **Price Stability** refers to the expected change in the amount of goods and/or services you can buy over the course of a month with the same amount of currency (i.e. x$ in October will be worth y$ in November)
5. **Digital/physical**. All currency that is stored outside of your personal physical possession can be considered as digital.

Each of these attributes was assigned between two and four options shown in the table below.

TABLE 4

Attributes and Attribute Options for types of Money

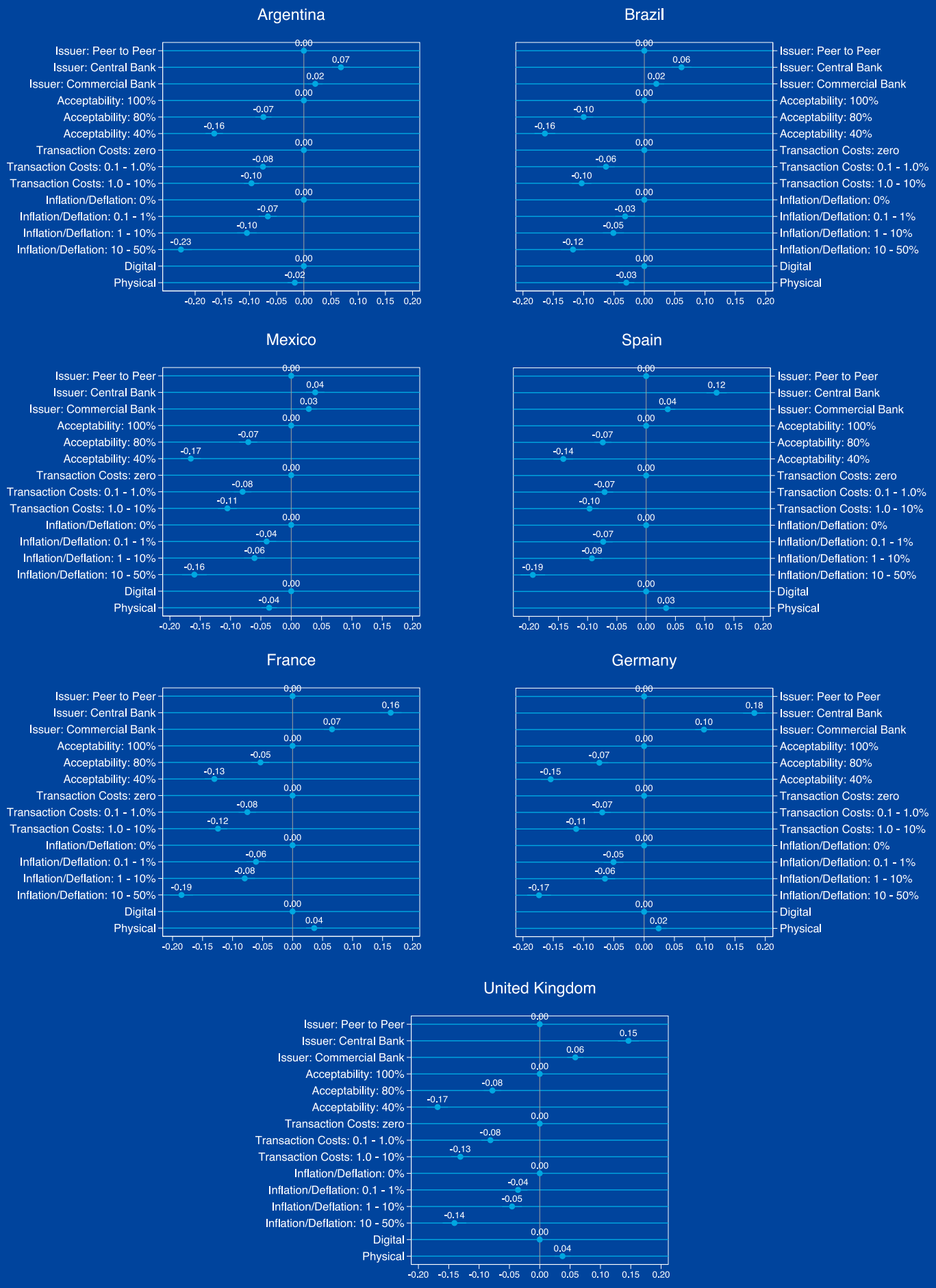
MONOPOLIZED MONEY

ATTRIBUTE	OPTIONS
Issuer/Backer	Central bank Private sector commercial bank Private Sector peer-to-peer network
Acceptability	All sellers accept the currency 80% of sellers accept the currency 40% of sellers accept the currency
Transaction Cost	Zero 0.1-1% of the transaction value 1-10% of the transaction value
Price Stability	Max monthly inflation/deflation of 0 % (100=100) Max monthly inflation/deflation of 0 - 1% (100 = 99, or 100=101) Max monthly inflation/deflation of 1 - 10% (100 = 90, or 100=110) Max monthly inflation/deflation of 10 - 50% (100 = 50 or 100 = 150)
Digital/Physical	Digital Physical

This produced 80,000 observations reflecting the preferences of residents in Argentina, Brazil, France, Germany, Mexico, Spain, the US and UK, for money across our five attributes. The most straightforward way to interpret the results is by examining the average marginal effects of each attribute choice. Effectively, these can be viewed as premiums/discounts placed on specific characteristics of money that are comparable with each other in magnitudes. The results are shown in Figure 38 for each country separately. The general results are consistent with the findings throughout this report.

Mainly, respondents place a significant premium on money created by central banks, with the least preferred option being peer-to-peer. The magnitudes vary quite a bit across countries with Germany placing a very large premium on central bank money (0.18) and Mexico placing a lower premium on central bank money (0.04). Acceptability had a relatively consistent impact across all countries with American respondents placing the largest discount on low-acceptability types of money. Transaction cost effects were also fairly consistent across countries with significant aversions when moving from 0% to between 0.1 and 1%, but only slightly higher aversion rates when moving from 0.1 and 1% to between 1 and 10% of the transaction costs. With respect to inflation, it appears that while respondents certainly prefer no inflation/deflation, they are much more comfortable in the 0.1-10% range that beyond that. This is especially true in the case of Argentina (-.023 compared with no inflation). Interestingly, the results for digital vs. physical money were mixed across countries. In Argentina, Brazil and Mexico, respondents preferred digital money to physical money. While the magnitudes were not large (between 0.02 and 0.04) there were statistically significant. In Spain, France, Germany, the UK, and US, respondents still marginally preferred to own physical cash over digital money. Again, the magnitudes here were not large compared with other attributes but were statistically significant.

FIGURE 38. **Attributes of Money Conjoint Analysis Results**



Thinking about these results in the context of current types of money, cash, credit cards, and debit cards, all have very high levels of acceptability and relatively low transaction costs in most advanced economies. Central banks with a history of stable inflation and/or a reputation as trustworthy creators and managers of money lead to the expectation of low levels of inflation with cash, credit cards and debit cards. Overall, these three highly used types of money score quite highly in the context of our conjoint analysis. Existing cryptocurrencies, however have low levels of acceptability and large price fluctuations, which are two of the least-desired characteristics of money. As noted above, these is also a trust premium enjoyed by central banks, creating an additional trust barrier for the much less preferred alternatives, including Facebook. In general, the results suggest that cryptocurrencies, especially those which are privately issued, have a long way to go before they might be able to compete with or overtake traditional forms of money like cash, credit cards and debit cards backed by central and commercial banks.

Conclusion

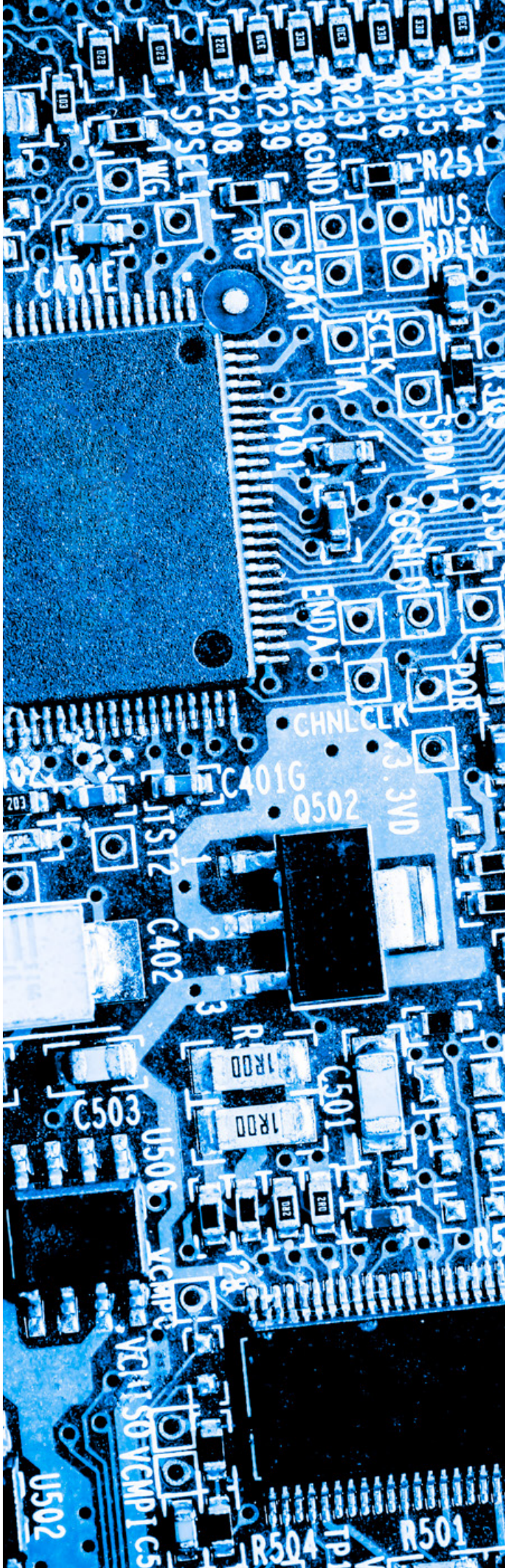
Over the past ten years, attention to money and the financial systems has come under greater scrutiny by a wider public concerned with current levels of transparency, management, accountability and fairness. Accompanying this scrutiny is an era of unprecedented technological innovations that open up the range of possibilities for how money works, some of which were proposed by Austrian School economists in the early 20th century. Destabilisations in financial markets often lead to short revivals of these Austrian school ideas regarding the role of money and banking in society making it no coincidence that the Nakamoto (2008) paper emerged in the aftermath of the 2007/08 financial crisis.

The widespread distrust arising from the financial crisis and greater public scrutiny led to the seminal contribution from Nakamoto (2008) and subsequent invention of Bitcoin. The decentralized nature and democratic consensus protocol of Bitcoin was envisioned to become a digital payment system with emphasis on removing the need for a trusted third-party institution in processing transactions, whose rules are enforced by consensus, with anyone being able to participate. There are other good reasons to move from cash to blockchains based electronic payment systems including the elimination of a sourse of illicit financial activity, public health benefits and overall efficiency of not having to be physically present to make very fast transactions with strangers. In fact, digital payment systems have been slowly replacing physical cash for many years with the majority of respondents to the IE Survey on the Future of Money using credit cards and debit cards as frequently as cash. Several other digital alternatives to physical cash have already become successful systems of payments (M-Pesa, AliPay, Paypal, etc.).

Unfortunately, in practice, cryptocurrencies are struggling to uphold their creator's objectives, given that no existing cryptocurrency has been universally successful in fulfilling the role of 'money'. This is partly due to the failure in practice for a decentralized system to work in the presence of large mining consortiums, a lack of price stability, high transaction costs with large electricity consumption (with Proof of Work consensus protocols) and, potentially lower degrees of transparent governance. There also exists a general distrust of new currencies issued by new institutions. While central banks are not perfect, in most advanced economies they have built a trust premium compared to private sector companies, which makes them better candidates in the opinion of most citizens for issuing money and managing/regulating financial transactions.

These trust premiums and low levels of trust and understanding of cryptocurrencies are confirmed by the unique results from the IE Survey on the Future of Money. Specifically, residents of Argentina, Brazil, Mexico, France, Germany, Spain, the UK and USA all i) place significant premiums on money which is issued by a traditional authority (preferably central banks), ii) place a heavy discount on currencies which lack price stability, and, iii) place a high premium on money that is highly accepted. Based on these results and the technical challenges listed in Chapter 4, cryptocurrencies have a considerable amount of obstacles to overcome before gaining widespread acceptance by general public. The good news is that central banks are currently working diligently to investigate/establish Central Bank Digital Currencies (CBDCs) which would overcome some of the challenges associated with cash while still being managed by a trustworthy central authority in the case of advanced economies. Where central banks have poor records of money issuance and management or high degrees of exclusion abuse and mistrust, such countries could benefit in the short term from the introduction of a privately issued cryptocurrency, especially with the vast increase in worldwide Internet users and availability of secure servers.

In short, we can return to the conclusion from Lawson in Chapter 1: "The challenge, then, for those seeking to render a form(s) of cryptocurrency as money lies both in getting it positioned as a legitimate general means of payment (governed by relevant rights and obligations to ensure this) and so also trusted in the sense that if positioned as money it would serve as a store of liquid value."



List of Figures

List of Tables

References

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014) The Economics of Digital Currencies – BOE Quarterly Bulletin 2014 Q3

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014) Innovations in payment technologies and the emergence of digital currencies– BOE Quarterly Bulletin 2014 Q3

A. Gervais, G. O. Karame, V. Capkun and S. Capkun, "Is Bitcoin a Decentralized Currency?," in *IEEE Security & Privacy*, vol. 12, no. 3, pp. 54-60, May-June 2014.

Baran, *P. On Distributed Communications. Rand Corporation*, 1964.

Barrdear, J. and Kumhof, M. (2016). The macroeconomics of central bank issued digital currencies. BOE Staff Working Paper No. 605

Benes, J. and Kumhof, M. The Chicago Plan Revisited. IMF Working Paper WP 12/202.

Bernanke, B., & James, H. (1990). The Gold Standard, Deflation, and Financial Crisis in the Great Depression: An International Comparison. *NBER Working Paper* No. 3488.

Bordo, M. (1995). Is There a Good Case for a New Bretton Woods International Monetary System? *American Economic Review*.

Bordo, M. (2018). The imbalances of the Bretton Woods System 1965 to 1973: U.S. Inflation, The Elephant in the Room. *NBER Working Paper* No. 25409.

Bösl, S. M. (2019) Mehrheit der Deutschen skeptisch bei Facebooks Libra. https://www.finanzwende.de/presse/mehrheit-der-deutschen-skeptisch-bei-facebooks-libra/?L=0

Craig, B. (1996). Competing Currencies: Back to the Future? *Federal Reserve Bank of Cleveland Economic Commentary*.

Doidge, F. and Exton, J. (2018) Cracking the code on cryptocurrency. ING International Survey Mobile Banking – Cryptocurrency June 2018

du Toit, G., Bradley, K., Swinton, S., Burns, M. and de Gooyer,C. (2018) In Search of Customers Who Love Their Bank. Bain and Company Report, November 14, 2018

Eichengreen, B. (1986). The Bank of France and the sterilization of gold, 1926-1932. *Explorations in Economic History*.

Endres, A. (2009). Currency Competition: A Hayekian Perspective on International Monetary Integration. *Journal of Money, Credit and Banking*.

Exton, J. From cash to crypto: The Money Revolution. ING International Survey ING International Survey, New Technologies, September 2019 September 2019

Fisher, I. (1936). 100% Money and the Public Debt. *Economic Forum Spring Number, April-Jun*.

Friedman, B. (1999). The Future of Monetary Policy: teh Central Bank as an Army with only a Signal Corps? *International Finance*.

Hanke, S. and Kwok, A. (2009). "On the Measurement of Zimbabwe's Hyperinflation", Cato Journal, Vol. 29, No. 2 (Spring/Summer 2009).

Hayek, F. (1978a). *Choice in Currency*. Chicago University Press.

Hayek, F. (1978b). *The Denationalization of Money: An Analysis of the Theory and Practice of Concurrent Curriencies*. Chicago University Press.

Hoppe, H.-H. (1994). How is Fiat Money Possible? -- or the Devolution pf Money and Credit. *Review of Austrian Economics*.

Kaminska, I. What mobile money giveth, it also taketh away. FT Alphaville, November 23, 2015. https://ftalphaville.ft.com/2015/11/23/2145684/what-mobile-money-giveth-it-also-taketh-away/

Kaminska, I. (2015). Mpesa: the costs of evolving an independent central bank' FT Alphaville, July 2015. https://ftalphaville.ft.com/2015/07/15/2134081/the-collateral-velocity-and-sovereign-costs-of-mobile-money/

Kindlegerger, C. (1989). *Economic Laws and Economic History*. Cambridge University Press.

Lawson, Tony (2016) 'Social positioning and the nature of money', *Cambridge Journal of Economics*, 40(4): pp. 961–996.

Lawson, Tony (2018) 'Debt as money', Cambridge Journal of Economics, 42(4): pp. 1165-81.

Lawson, Tony (2019) *The Nature of Social Reality: issues in social ontology*, London and New York: Routledge.

Morgan Jamie, and Brendon Sheehan (2015) 'The Concept of Trust and the Political Economy of John Maynard Keynes, Illustrated Using Central Bank Forward Guidance and the Democratic Dilemma in Europe', *Review of Social Economy*, 73(1):113-137.

Nakamoto, Satoshi Bitcoin: A *Peer-to-Peer Electronic Cash System*, paper downloaded from https://bitcoin.org/bitcoin.pdf on 01/09/2018.

Pratten, Stephen (2017), 'Trust and the social positioning process', *Cambridge Journal of Economics*, Volume 41, Issue 5, 1 August 2017, pp. 1419–1436.

Minsky, H. P. (1992). The Financial Instability Hypothesis. *Levy Economics Institute Working Paper*.

Minsky, H.P. 1994. Financial instability and the decline (?) of banking: future policy implications. Working paper No. 127, October 1994. The Jerome Levy Research Institute of Bard College.

Mundell, R. (2000). A Reconsideration of the Twentieth Century. *American Economic Review*.

Rochemont, S. and Ward, O. (2019) Understanding Central Bank Digital Currencies (CBDCs). Institute and Faculty of Actuaries, March 2019.

Simons, H. (1946), "Debt Policy and Banking Policy", Review of Economic Statistics, 28(2), 85-89.

Temin, P. (1989). *Lessons from the Great Depression*. Cambridge University Press.

Tasca, Paolo and Tessone, Claudio, Taxonomy of Blockchain Technologies. Principles of Identification and Classification (March 31, 2018). Available at SSRN: https://ssrn.com/abstract=2977811 or http://dx.doi.org/10.2139/ssrn.2977811

Vanston, N (2012) Trust and Reputation in Financial Services. Driver Review DR30. Foresight, UK Government Office for Science

Weir, M. (2019) Boom in the Benjamins. IMF Finance & Development, June 2019, Vol. 156, No. 2

Wolf, M. (2014, April 24). Strip private banks of their power to create money. *Financial Times*.

Adrian, T. and Mancini-Griffoli, T. (2019). The Rise of Digital Money. IMF Fintech Notes, July 2019

Barker, J.; Clayton, E.; Dyson, B. and Meaning J. (2018) Broadening Narrow Money: Monetary Policy with a Central Bank Digital Currency. Bank of England Staff Working Paper No. 724.

Bech, M. L., Faruqui, U., Ougaard, F., & Picillo, C. (2018). Payments are a-changin but cash still rules. BIS Quarterly Review, March.

Berentsen, A., & Schar, F. (2018a). The case for central bank electronic money and the non-case for central bank cryptocurrencies.

Berentsen, A., & Schar, F. (2018b). A short introduction to the world of cryptocurrencies.

Bordo, M. D., & Levin, A. T. (2017). Central bank digital currency and the future of monetary policy (Tech. Rep.). National Bureau of Economic Research.

Broadbent, B. (2016). Central banks and digital currencies. Speech at London School of Economics.

Brunner, K. and Meltzer, A. H. (1971) The Uses of Money: Money in the Theory of an Exchange Economy. *The American Economic Review* Vol. 61, No. 5 (Dec., 1971), pp. 784-805

Carstens, A. (2019). The future of money and payments. Speech by General Manager of the BIS at the Central Bank of Ireland, Whitaker Lecture.

Coeur, B., & Loh, J. (2018). Central bank digital currencies. CPMI Papers.

Dyson, B., & Hodgson, G. (2016). Digital cash: why central banks should start issuing electronic money. Positive Money.

Engert, W., Fung, B., et al. (2017). Central bank digital currency: Motivations and implications. Bank of Canada.

Fisher, I. (1936). 100% money and the public debt.

Goodfriend, M. (2016). The case for unencumbering interest rate policy at the zero bound. In Federal reserve bank of kansas citys 40th economic policy symposium. Jackson Hole, wy. august (Vol. 26).

Gurtler, K., Nielsen, S. T., Rasmussen, K., & Spange, M. (2017). Central bank digital currency in denmark? Analysis.

Keynes, J. M. (1930). A Treaties on Money. Macmillan and Co. Ltd. St Martin's Street, London, 1930

Kumhof, M., & Noone, C. (2018). Central bank digital currencies-design principles and balance sheet implications.

Lagarde, C. (2018). Winds of change: The case for new digital currency. Delivery by IMF Managing Director, Singapore Fintech Festival.

Lowe, P. (2017). An eaud. Address to the 2017 Australian Payment Summit, Sydney, Australia, 13 December, 2017

Mersch, Y. (2017). Why europe still needs cash. Contribution by Yves Mersch, Member of the Executive Board of the ECB for Project Syndicate, 28 .

Raskin, M. and Yermack, D. Digital Currencies, Decentralized Ledgers, and the Future of Central Banking. NBER Working Paper No. 22238

Riksbank, S. (2017). The riksbanks e-krona project. Riksbank Studies, Report, 1 .

Rogoff, K. S. (2017). The curse of cash: How large-denomination bills aid crime and tax evasion and constrain monetary policy. Princeton University Press.

Sands, P., et al. (2016). Making it harder for the bad guys: the case for eliminating high denomination notes. Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government.

Skingsley, C. (2016). Should the riksbank issue e-krona? speech at FinTech Stockholm, 16 .

Smithin, J. (ed) (2000). What is Money? Routledge Press

Tobin, J. (1986). Financial innovation and deregulation in perspective. Cowles Foundation for Research in Economics at Yale University.

Woodford, M. (2000). Monetary policy in a world without money. International Finance, 3 (2), 229–260.

A. Laszka, B. J. (2015). When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools. *Workshop on Bitcoin Research*.

all cryptocurrencies. (2012). Retrieved from coinmarketcap: https://coinmarketcap.com

Androulaki, E. K. (2013). Evaluating user privacy in bitcoin. *International Conference on Financial Cryptography and Data Security* (pp. 34-51). Springer.

Bahack, L. (2013). *Theoretical Bitcoin Attacks with less than Half of the Computational Power*. Retrieved from arXiv preprint arXiv:1312.7013.

Barrera, C. &. (2018). SSRN . Retrieved from Blockchain upgrade as a coordination game.: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192208

Courtois, N. T. (2014). *On the longest chain rule and programmed self- destruction of crypto currencies*. Retrieved from arXiv preprint arXiv:1405.0534.

Gervais, A. K. (2014). Is bitcoin a decentralized currency? *IEEE security & privacy*, (pp. 54-60).

Herrera-Joancomartí, J. (2014). Research and challenges on bitcoin anonymity. *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* , 3-16.

J. Garay, A. K. (2014). T*he Bitcoin Backbone Protocol: Analysis and Applications*. Cryptology ePrint Archive, Report 2014/765.

Laurie, B. (2011). *An Efficient Distributed Currency*.

M. Babaioff, S. D. (2012). On Bitcoin and Red Balloons. *SIGecom Exchanges*, 56–73.

Meiklejohn, S. P. (2013). A fistful of bitcoins: characterizing payments among men with no names. *The 2013 conference on Internet measurement conference* (pp. 127-140). ACM.

N. T. Courtois, M. G. (2014). Optimizing sha256 in bitcoin mining. *Cryptography and Security Systems*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from http: // bitcoin.org/bitcoin.pdf

Sirer, I. E. (2014). Majority is not enough: Bitcoin mining is vulnerable. *In Financial Cryptography*.

T. Bamert, C. D. (2013). Have a snack, pay with Bitcoins. *IEEE P2P*.

ANNEX

Money and Trust: Country Profiles

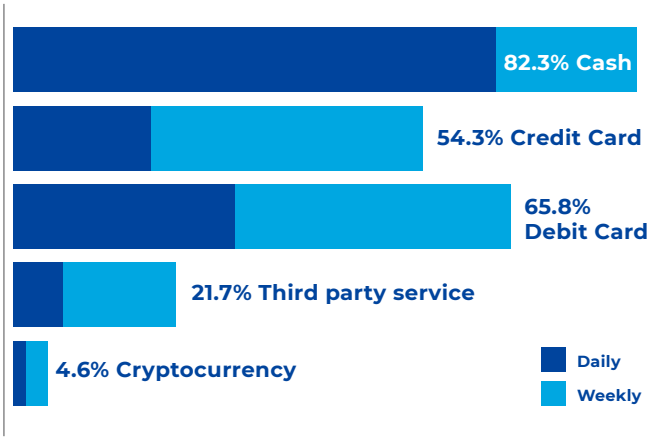
The Survey on Cryptocurrencies and the Future of Money conducted by the Center for the Governance of Change of IE University asked a representative sample of 8,000 citizens of the US, UK, Germany, France, Spain, Argentina, Brazil and Mexico about their use of different types of money, trust in institutions to create and manage money and their attitudes towards digital currencies, including Facebook's Libra. A summary of the results is shown in this Annex.

To get a better idea of citizens attitudes toward different types of money, the survey also presented each of the 1000 respondents with a variety of different hypothetical types of money (Conjoint Analysis of Preferences for Money). This gives a good measure of to what extent a premium or discount is placed on different attributes of money.

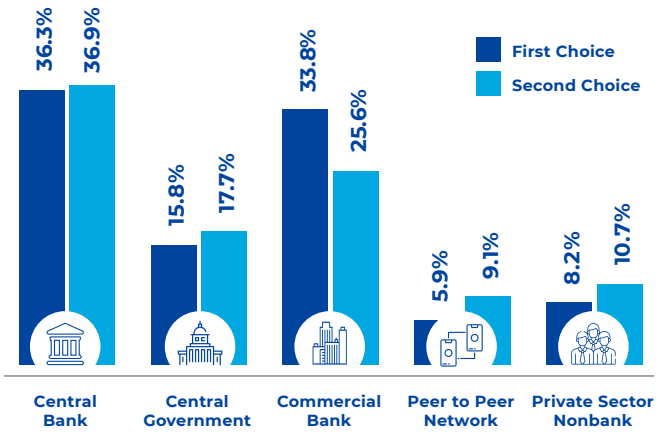
Money and Trust in Argentina

Argentinians appear to place a premium on central bank issued money and very high discount on money with high price volatility (inflation/deflation).

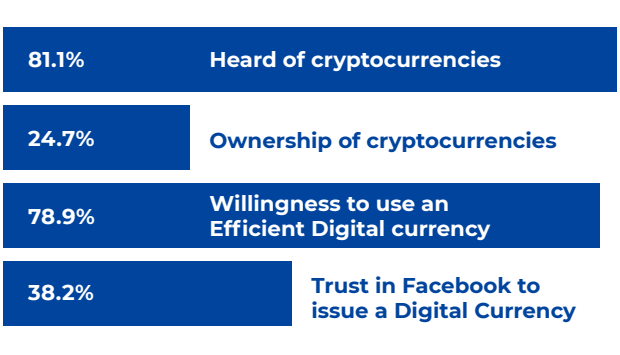
Use of Money in Argentina (Daily & Weekly)



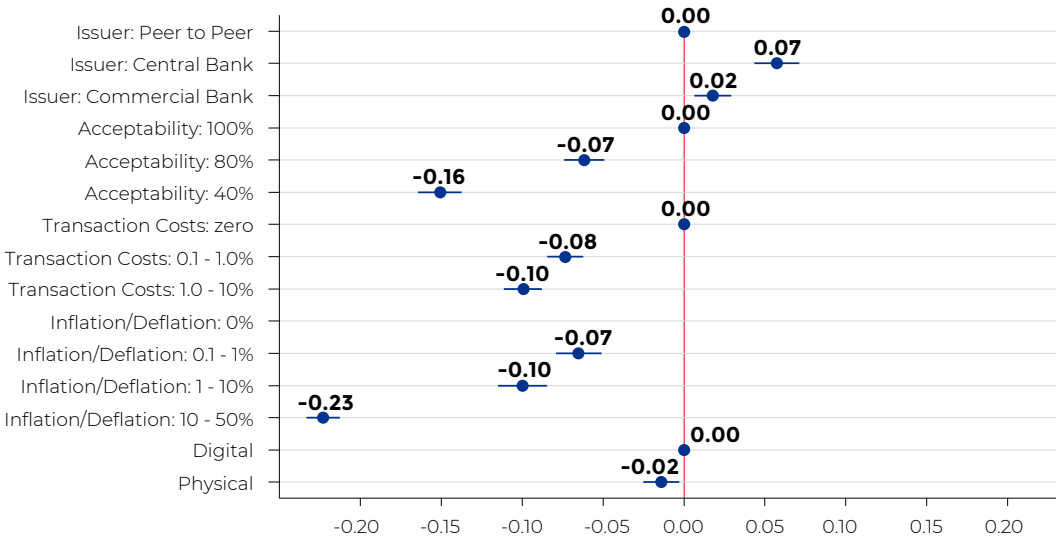
Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies



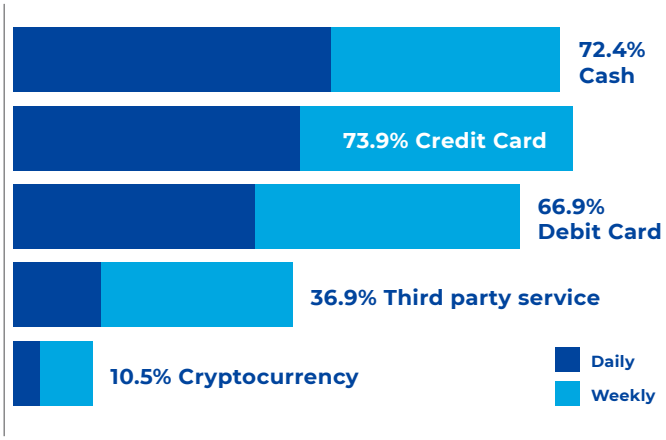
Conjoint Analysis of Preferences for Money in Argentina



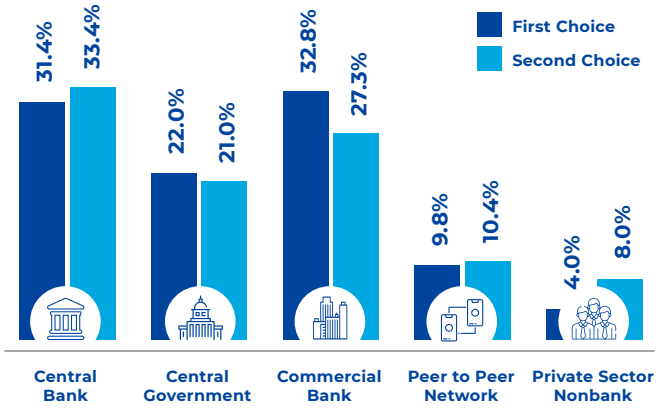
Money and Trust in Brazil

Brazilians appear to place a premium on central bank issued money and high discount on money with low levels of acceptability (40%).

Use of Money in Brazil (Daily & Weekly)

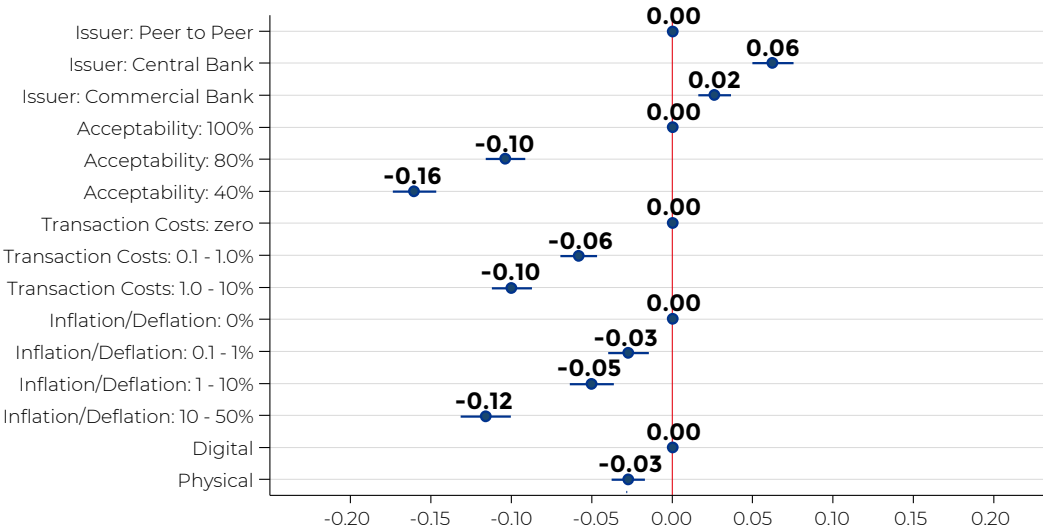


Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies

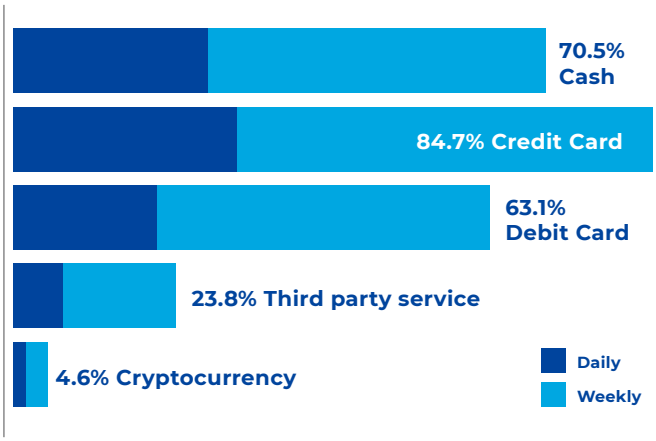
Conjoint Analysis of Preferences for Money in Brazil



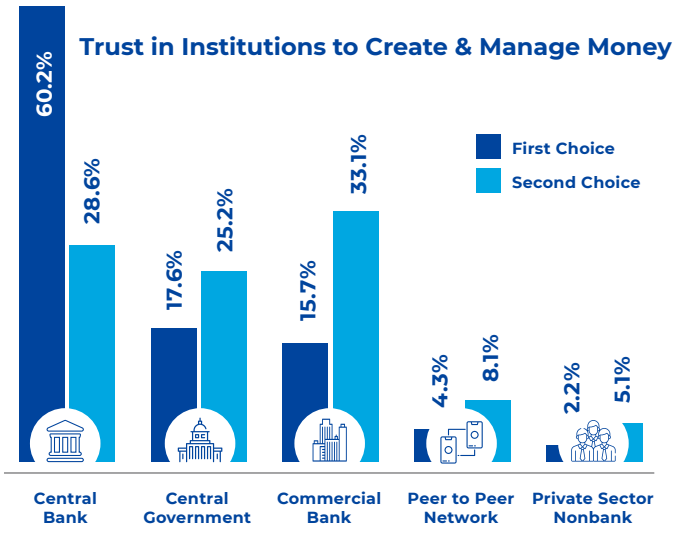
Money and Trust in France

French citizens appear to place a high premium on central bank issued money and high discount on money with high price volatility (inflation/deflation).

Use of Money in France (Daily & Weekly)

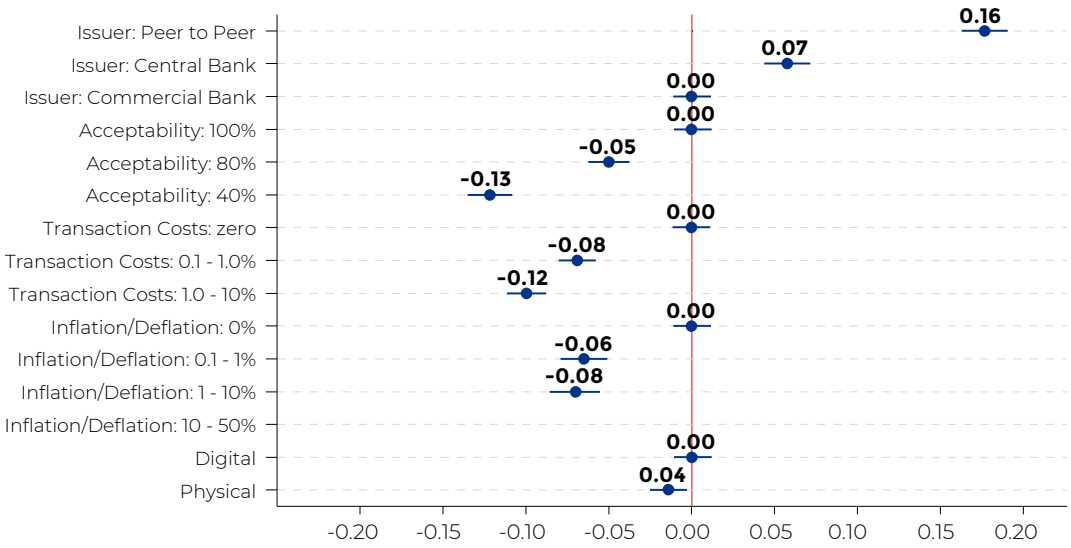


Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies

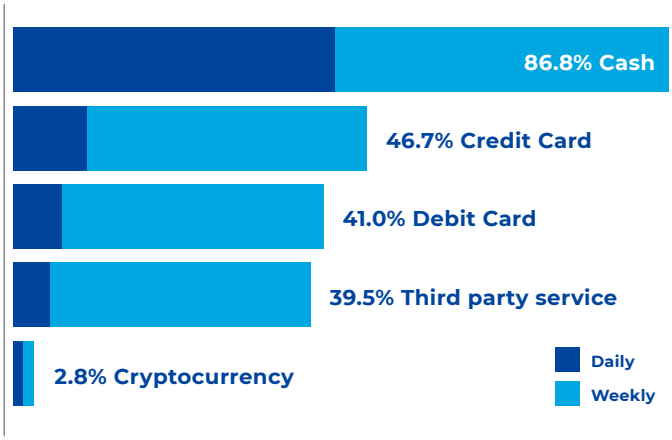
Conjoint Analysis of Preferences for Money in France



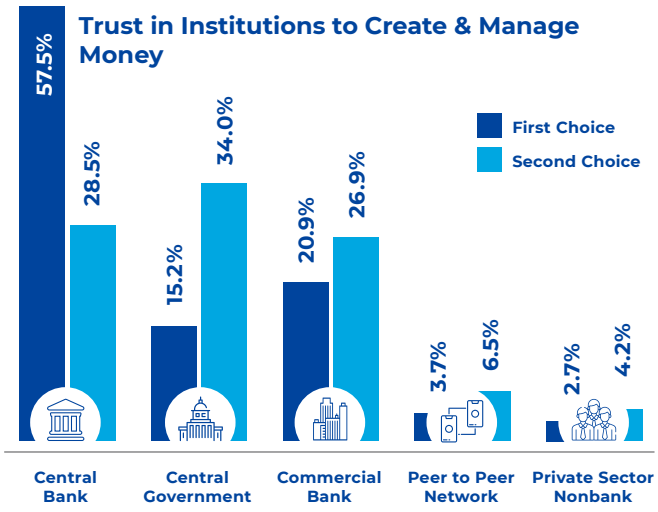
Money and Trust in Germany

Germans appear to place a high premium on central bank issued money and high discount on money with high price volatility (inflation/deflation).

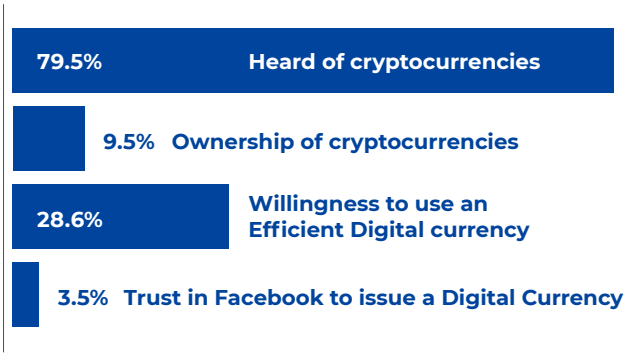
Use of Money in Germany (Daily & Weekly)



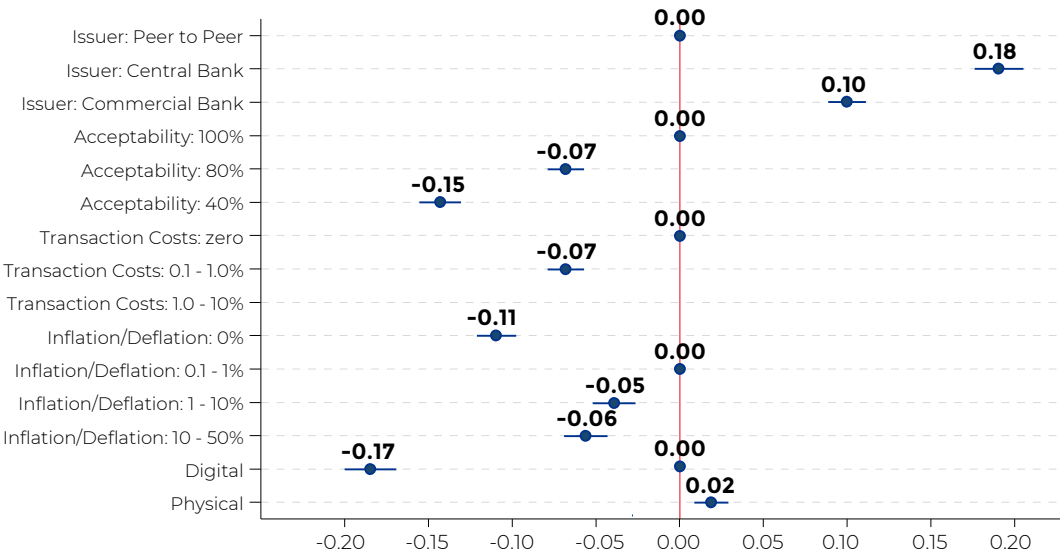
Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies



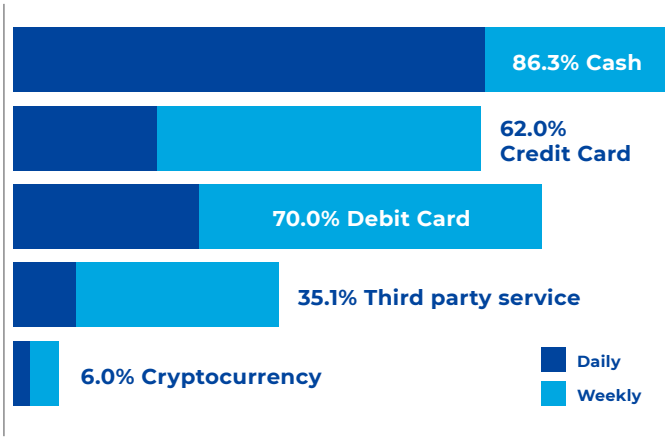
Conjoint Analysis of Preferences for Money in Germany



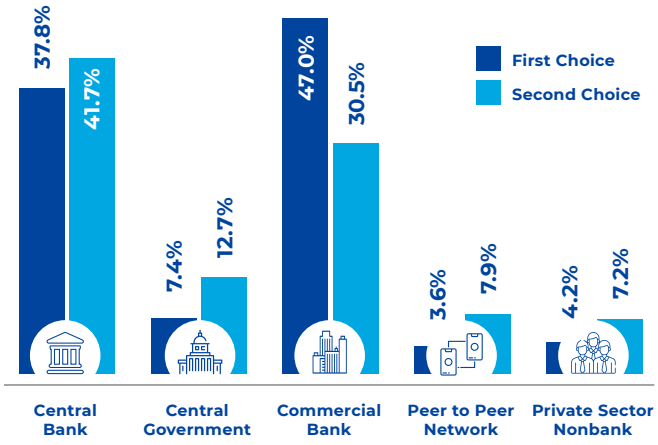
Money and Trust in Mexico

Mexicans appear to place a slight premium on central bank and commercial bank issued money and high discount on money with low levels of acceptability high price volatility (inflation/deflation).

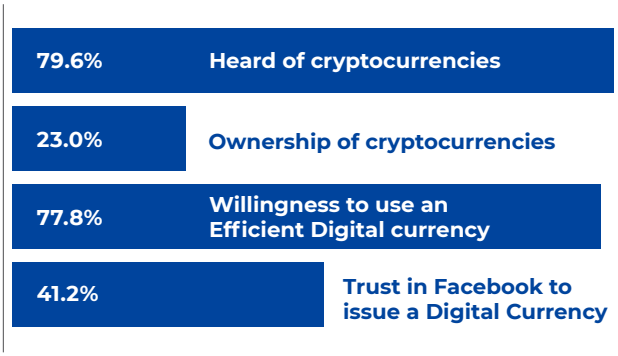
Use of Money in Mexico (Daily & Weekly)



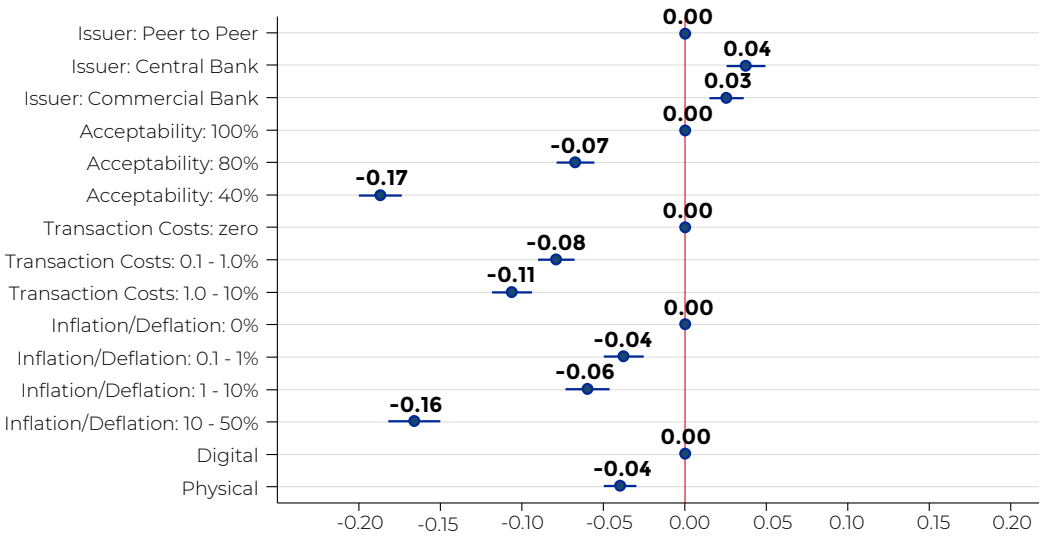
Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies



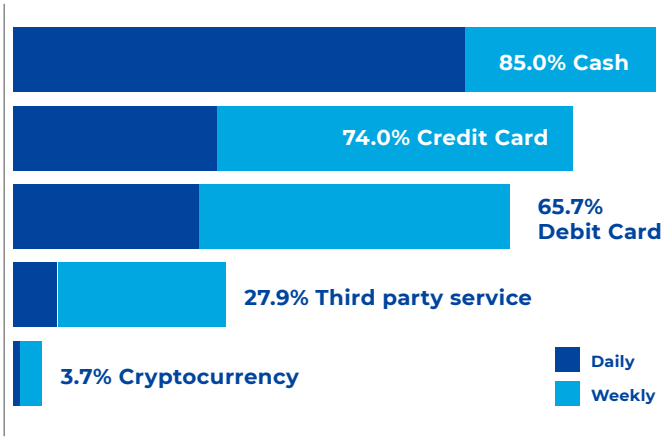
Conjoint Analysis of Preferences for Money in Mexico



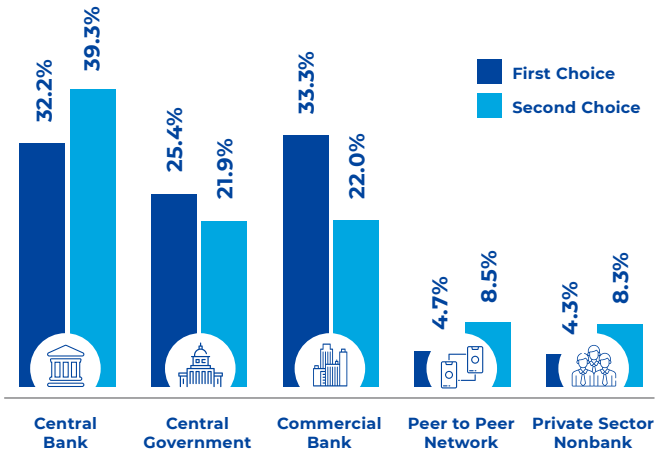
Money and Trust in Spain

Spanish citizens appear to place a high premium on central bank issued money and high discount on money with high price volatility (inflation/deflation).

Use of Money in Spain (Daily & Weekly)

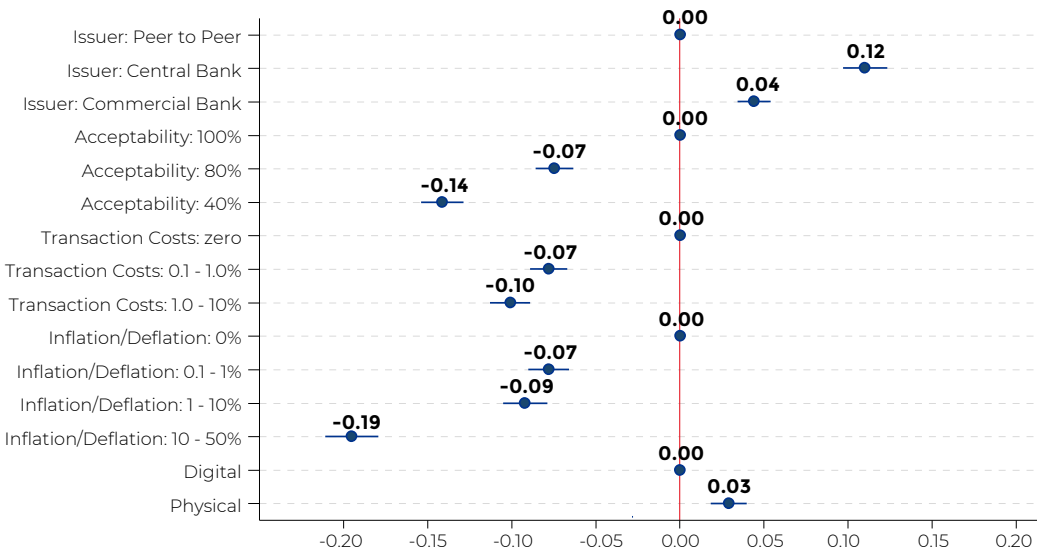


Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies

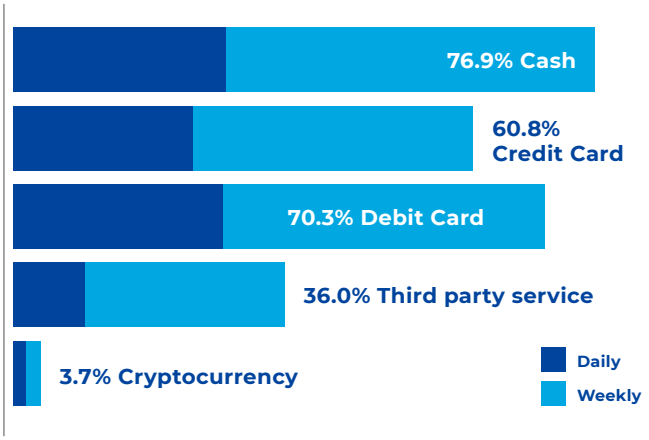
Conjoint Analysis of Preferences for Money in Spain



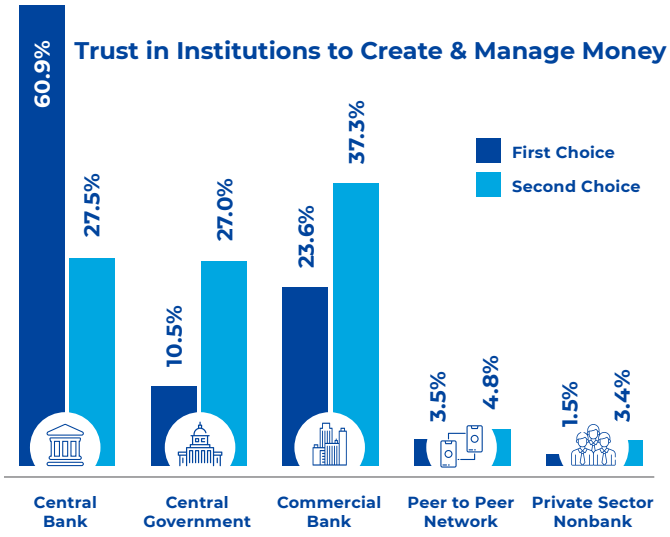
Money and Trust in UK

UK citizens appear to place a high premium on central bank issued money and high discount on money with low levels of acceptability high price volatility (inflation/deflation).

Use of Money in UK (Daily & Weekly)

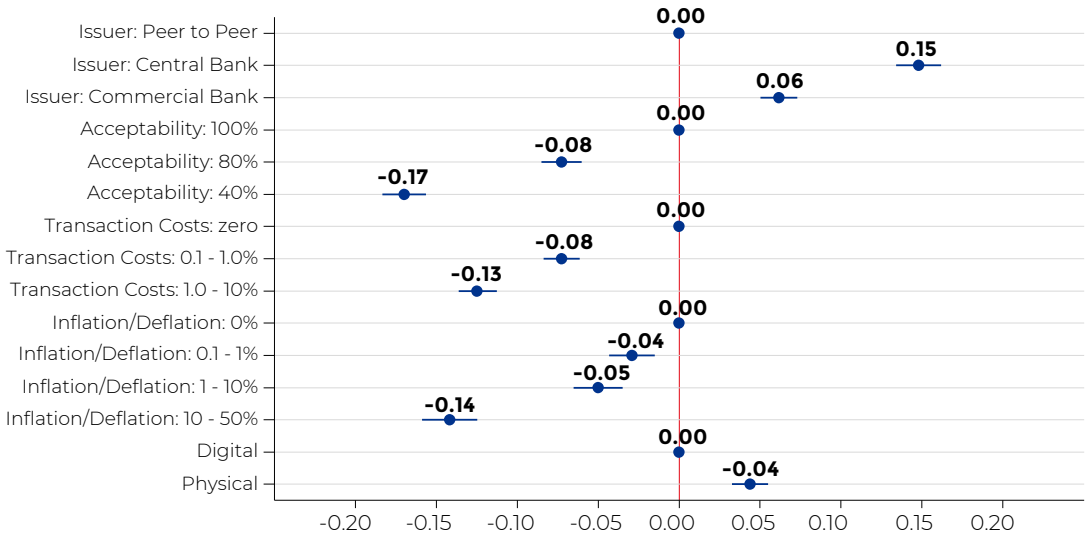


Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies

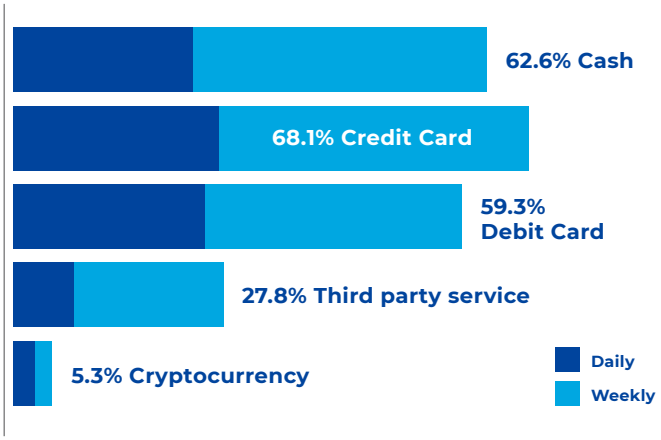
Conjoint Analysis of Preferences for Money in UK



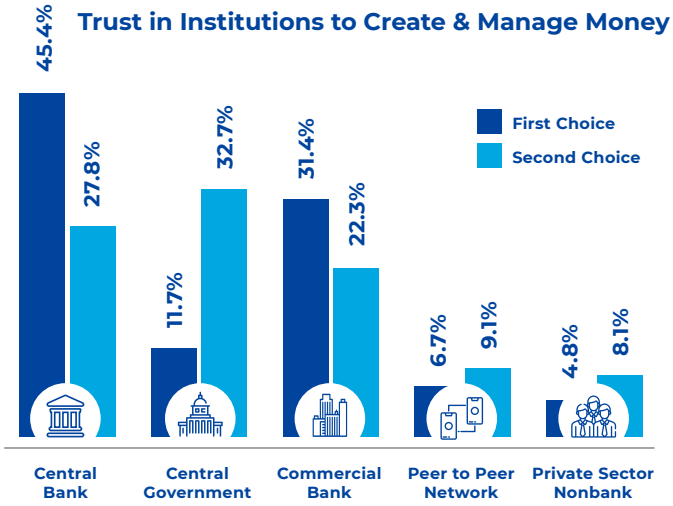
Money and Trust in USA

Americans appear to place a high premium on central bank issued money and very high discount on money with low levels of acceptability (40%).

Use of Money in USA (Daily & Weekly)

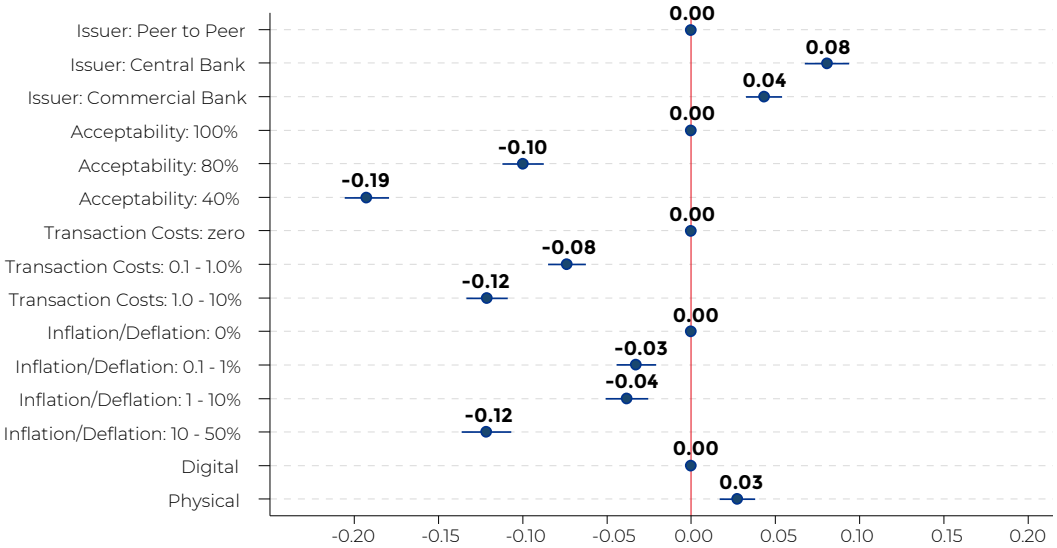


Trust in Institutions to Create & Manage Money



Attitudes Towards Digital Currencies

Conjoint Analysis of Preferences for Money in USA



Team of Researchers

DIRECTOR:
Dr. Mike Seiferling, UCL

RESEARCHERS:

— Mr. Thamin Ahmed, UCL Centre for Blockchain Technologies
— Dr. Abeer Yehia ElBahrawy, City, University of London
— Mr. Keith Chan, University of Cambridge
— Mr. Tales Padilha, Oxford University

RECOMMENDED CITATION:
CGC, *Cryptocurrencies and the Future of Money*.
Madrid: Center for the Governance of Change,
IE University, 2019.

www.cgc.ie.edu

CENTER FOR
THE GOVERNANCE
OF CHANGE