

Alternative Currencies

A Critical Approach

Louis Larue

First published 2025

ISBN: 978-1-032-87021-2 (hbk)

ISBN: 978-1-032-87022-9 (pbk)

ISBN: 978-1-003-53049-7 (ebk)

Chapter 5

The politics of alternative currencies

(CC-BY-NC-ND 4.0)

DOI: 10.4324/9781003530497-6

The funder of the Open Access version of this chapter is Aalborg University.



Routledge

Taylor & Francis Group

LONDON AND NEW YORK

5 The politics of alternative currencies

Introduction

Until now, this book has either examined alternative currencies in general (Chapters 1 and 2) or focused on arguments related to a limited group of them. Chapter 3 studied the case for bounded currencies, the use of which is limited in some way, and Chapter 4 analysed several arguments raised by the proponents of LETS and local currencies against the market. This chapter is concerned with two other specific currencies, namely Bitcoin and Central Bank Digital Currencies (CBDC), whose relatively recent emergence has brought about important changes to the way we think about money.

Relying on cryptography and peer-to-peer networks, cryptocurrencies such as Bitcoin do not rest on a central authority nor require any centralised management or system of payment. In the wake of criticism of the contemporary banking system following the 2007 financial crisis, they have gained in popularity and have been presented as an alternative to the current payment system.

Having inspired a great number of alternative cryptocurrencies such as Ripple, Dogecoin, and Ethereum, Bitcoin remains the most prominent cryptocurrency in terms of valuation and public recognition. I will therefore focus on Bitcoin, but the following discussion could also apply to other cryptocurrencies insofar as they share Bitcoin's aims and main characteristics.

Bitcoin has been the subject of much enthusiasm, billed by some as “the future of money”,¹ or presented as “challenging the global economic order”.² Its proponents are often highly critical of state regulations over money, sometimes conceived as inadmissible infringements on freedom, or as inefficient, insecure, and inflationary.

Naturally, Bitcoin has also attracted a fair amount of scepticism, some going as far as denying that Bitcoin really constitutes a form of money,³ or noting that the valuation of Bitcoin exhibits all the characteristics of a speculative bubble.⁴ Moreover, a substantial amount of commentary on Bitcoin focuses on its technical functioning, or on discussing the achievements and flaws of its underlying technology.⁵

Bitcoin has received much attention in the media and public debate in recent years. Increased public attention has also triggered reflection about the role of central banks and of monetary policy, and about possible reforms of traditional forms of money. While some see these new currencies as a potential threat to the stability of monetary systems, most commentators – including central bankers themselves – acknowledge that the technological innovations associated with cryptocurrencies can have interesting applications for monetary policy. In fact, several central banks are currently studying the possibility of issuing their own digital currencies, which have been dubbed “Central Bank Digital Currencies” (such as the e-krona in Sweden).⁶ In any case, while their exact form is still unclear, CBDC would allow firms and citizens access to (a new form of) digital money issued directly by central banks.

The research literature on CBDC is growing at a fast pace, and it will not be the purpose of this chapter to review it in its entirety. A significant part of the literature on CBDC is enthusiastic, arguing that it would provide central banks with new policy instruments that have the potential to challenge the influence of private financial institutions.⁷ The literature from central bankers themselves is more mixed and tends to concern technical details about the consequences of CBDC for monetary policy and financial stability.⁸

My aim in this chapter is to analyse and compare Bitcoin and CBDC. I will avoid dwelling too long on how the technology behind these currencies works, and I will only briefly consider the discussion as to whether they are a form of money.⁹ Rather, in this chapter, I want to take Bitcoin’s and CBDC’s proponents at their word: if we consider them as a form of money, are they appropriate for use as a currency? Each of them, though for quite different reasons, is often hailed for its supposed advantages over the conventional payment system. They have been praised for being more stable, safer, and more efficient than more conventional forms of money, or for allowing to dispense with the need of a central authority. They could also decrease the financial system’s reliance on the commercial banks. This chapter will inquire whether they can effectively meet these expectations, and at what cost.

The first half of this chapter will be concerned with analysing whether Bitcoin and CBDC can deliver on their promises.¹⁰ After a brief presentation of Bitcoin, I will delineate the main arguments in its favour, its main promises, and its ethical underpinnings. I will then show that Bitcoin has so far failed to deliver on these promises, and that we have strong reasons to think that it cannot in fact meet the expectations of its supporters. I will then turn to CBDC and show that it is more promising as a currency (or, in fact, as a means of payment, for, as we shall see, it would not be a new, independent, currency, but an additional payment option available to financial institutions and private individuals). Its main potential advantages fall into two categories: some are technical, having to do with the efficiency and stability of the payment system; others are political: CBDC could provide central banks with an additional monetary policy instrument, which could significantly reduce the influence of

the private financial system (mainly commercial banks) on monetary affairs. However, CBDC also has its own drawbacks. Its greatest potential problem, or so I will argue, is that it would give additional powers to already powerful (and to a large degree, undemocratic) institutions. Thanks to CBDC, central banks would gain additional tools to influence the economy. But without proper democratic checks and balances, this would further exacerbate the current imbalance of power at their advantage.

The proponents of Bitcoin and CBDC exhibit opposite views on the role of the state in monetary affairs. I shall discuss the political philosophy underpinning these different views of the state, and argue that, despite the fact that each has its problems, the view underpinning CBDC is more palatable than the one supporting Bitcoin. In the concluding section, I briefly discuss what place exactly the state must take in monetary affairs and consider the appropriate division of power between private and public financial actors.

What is Bitcoin?

As we have seen in Chapter 1, Bitcoin is not legal tender in any country (with the exception of El Salvador) and thus constitutes an alternative currency. Yet it differs in many respects from more “usual” examples of alternative currencies. In particular, contrary to LETS, local currencies, and Time Banks, Bitcoin is a universal currency, which can, in theory, be used to buy anything anywhere. Bitcoin also differs in important respects from official currencies, such as the euro or the dollar. These differences are at the centre of this chapter.

For the most part, in modern capitalist societies, money takes either of two forms: cash or bank deposits. Cash, that is, coins and notes, is usually emitted by the central bank of each monetary zone (the European Central Bank for the Eurozone, the US Federal Reserve for the dollar), while deposit money, which constitutes the vast majority of the money supply today, is made up of funds held in deposit accounts in commercial banks. Bitcoin differs both from cash and from deposit money. It is a decentralised cryptocurrency that rests on a distributed repository, protected and managed through the use of cryptographic protocols. Contrary to cash and deposits, it is, in theory at least, independent from any central authority.

First, Bitcoin is not backed by a state or by a central bank. Contrary to the euro or the dollar, where a central bank is in charge of ensuring price stability and financial stability through adequate monetary policy, there is no such central authority in the Bitcoin system. There is no lender of last resort either, that is, a state or a central bank that could bail out banks in the event of financial panic.

Second, Bitcoin’s payment system is entirely decentralised and rests on an open-source cryptographic protocol. This protocol originates from an article published in 2008 by a certain Satoshi Nakamoto (2008), whose identity remains mysterious.¹¹ The central innovation of Bitcoin, which puts together previous advances in cryptography, such as the proof of work technology, is

that it is based on a decentralised public ledger. In a conventional payment system, banks hold a record of transactions and ensure that no unit of money is used more than once by the same user (“double-spending” problem). With Bitcoin, this control system is decentralised through a public ledger system operated on a peer-to-peer network. This ledger has several important properties.¹² First, every user can verify and process transactions. Moreover, the Bitcoin protocol secures the ledger against falsifications, without resorting to any banking institution or any central authority. Finally, an important consequence of the public availability of this ledger is that Bitcoin can only preserve a “pseudo-anonymity” for its users: details of all transactions are logged on the public ledger, where the only indication of the identity of their parties is their Bitcoin address.¹³

A third crucial difference between Bitcoin and official currencies lies in its creation process. Every user can participate in the creation of new Bitcoins, by resolving a deliberately complicated series of algorithms (though in practice this “mining” process is mainly taken up by professional miners). The first Bitcoins were created from scratch and used by the first Bitcoins users. The first user of the protocol, assumed to be Nakamoto himself, mined the first 50 Bitcoins in 2009.¹⁴ The following Bitcoins are created when new transactions take place, as a reward going to those who successfully add a new block to the ledger. More precisely, miners, by solving puzzles, try to verify each transaction and to get the right to add it to a new “block” containing several transactions, appended in the Bitcoin ledger (also called the “Blockchain”, for that reason). This new block is accepted within the ledger if it contains a valid transaction and a new puzzle solution. Miners are all competing to verify each transaction in order to get the reward attached to the completion of a block. Along with this reward, miners may also set a fee for processing transactions, as a complementary revenue. Eventually, every time a block is verified, new Bitcoins are mint.¹⁵

However, the Bitcoin creation process has an algorithmic limit. The Bitcoin protocol has a marginally decreasing rate of Bitcoin creation per block. Therefore, the total supply of Bitcoins will asymptotically approach the amount of 21 million, which, according to some estimations, will be reached around the year 2040.¹⁶ The reward of miners is therefore set to decrease, being divided by two every 210.000 blocks, while the difficulty of mining is programmed to increase along with the network size. As we shall see in later sections of this chapter, the purpose of this limit is, according to its creator Satoshi Nakamoto, to make sure Bitcoin does not lose its value over time.

Is Bitcoin money?

Whether Bitcoin is money is a highly debated issue in the literature.¹⁷ In economics, it is often argued that what money is relates to what money does: something is money as long as it serves several functions, which, traditionally, are the following: means of exchange, store of value, unit of account. On the

basis of that theory, it has been argued that the currencies that fail to serve these functions well should not be conceived as money.

For instance, David Yermack argues that Bitcoin is not a real currency because it does not fulfil the traditional functions of money sufficiently well.¹⁸ Similarly, J.P. Smit and his co-authors claim that money is whatever is efficiently used as a means of exchange, that is, as a device to reduce transaction costs.¹⁹ Since Bitcoin is not largely and efficiently used as such, they argue that it is merely a financial asset.

I think that these claims are mistaken, though.²⁰ First, the definition of money is a controversial issue. Philosophers such as John Searle, anthropologists like David Graeber, and sociologists and economists like Nigel Dodd and Geoffrey Ingham have, for a variety of reasons, criticised the view that money is defined by its functions.²¹ Instead, money is sometimes conceived as a debt token, or as a social relation, among other examples. It is not at all clear, then, that the classic theory of money constitutes the right basis for assessing whether Bitcoin is money.

I think, however, that the main issue with the claim that Bitcoin is not money lies elsewhere. Let's assume that the classic theory of money is the right one and that money's functions are well defined. How well a currency fulfils them is difficult to assess in practice, though. In fact, no currency could be said to fulfil all functions well for everybody all of the time. Does that mean that no currency can properly be called money? Are we all wrong to call dollars "money" after the 2007 financial crisis? Certainly not. But then, how well should a currency function, and for how many people, in order to be counted as money? J. P. Smit and his co-authors argue that Bitcoin should not count as money because "at present, the vast majority of bitcoins are traded as a speculative investment, not as a means to lower transaction costs".²² I wonder why this would disqualify Bitcoin as money. Large quantities of dollars, euros, and pounds are also traded as assets, and speculation on currencies is a profitable business. Moreover, Bitcoins do serve as a means of payment, though maybe not the majority of them. Finally, as we have seen in Chapter 3, some currencies, such as local currencies, are used only in a very tiny geographical area. Yet, most of their users would say they are money.

I think that what money is should not be confused with how successful it is (whatever this means). Squeezing into the definition of money an account of its efficiency, or of its success in fulfilling certain functions, should be avoided.

This chapter will not postulate any theory of the nature of money. Rather, it will assume, for the sake of the argument, that Bitcoin is money. My goal is to take its proponents at their word, and therefore, to see whether it can be successful as a currency. Considering that Bitcoin is money, then, is a methodological assumption, not an ontological stance on the nature of money. I am open to the claim that Bitcoin is in fact not money (though not for the reasons advanced by David Yermack, J. P. Smit, and others), but this shall not matter for the purpose of the present inquiry.

The ethics of Bitcoin

Bitcoin's proponents do not form a homogeneous group, and different people may support Bitcoin's adoption for different reasons. However, the main recurring cases for Bitcoin may be summarised as follows:

- Bitcoin can constitute a more stable currency than conventional state-sponsored money, by taking monetary policy out of the government's hands.
- Bitcoin can provide a more secure and efficient payment system, compared to a system relying on trusted third parties.
- Bitcoin can dispense with the need of coercive institutions such as states and central banks, by achieving a decentralised securing of transactions through cryptographic proof.
- Bitcoin helps protect users' privacy against abuse of state power through government surveillance.

Let me analyse each of these claims in turn.

Is Bitcoin a stable currency?

First, Bitcoin is often hailed as a means to achieve a more stable monetary system.²³ As Satoshi Nakamoto stresses, with conventional currencies, "the central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust".²⁴ This criticism reminds the neoliberal critique that state monopoly in the issuance of money will necessarily lead to over-inflation, resulting in depressions and unemployment. Friedrich Hayek, perhaps the most vocal proponent of neoliberalism, argues that governments have a tendency to abuse their monopoly power over money by systematically creating too much money, hence fostering inflation.²⁵ Milton Friedman, the influential neoliberal economist, argued that monetary policy should "avoid wide swings" and proposed to tie the hands of the central bank by setting a fixed annual rate of growth of the money supply.²⁶ His argument is based on historical evidence, but also on his own theory, which, similar to Hayek's, predicts that excessive money creation is inflationary and cannot impact employment in the long run.

The Bitcoin protocol is designed in this spirit: since no central agencies can control the Bitcoin's supply, whose rate of growth is set to decrease steadily, it is immune from inflation. Actually, unless a majority of nodes decides collectively to modify the protocol itself, there is no procedure for altering the rate of Bitcoin creation.

It is not my purpose to discuss the economic merits of such a fixed or "algorithmic" monetary policy, an issue which is the subject of an extensive literature.²⁷ Leaving that theoretical issue aside, I will focus on the day-to-day workings of Bitcoin as a currency and examine whether it does in fact abide by its own promises. I will argue that, in practice, its high volatility compared to other currencies seriously undermines its quality both as a means of exchange and as a store of value.

Financial economists have studied Bitcoin's volatility in depth. Gerald Dwyer finds that Bitcoin's average volatility is always higher than that for gold or a set of foreign currencies.²⁸ Econometric analysis also shows that the price of Bitcoin exhibits speculative bubbles.²⁹ These studies show how, for many users, Bitcoin is mainly used as a speculative asset, which people buy and sell for the sake of rapid financial profit, explaining why, as a consequence, its value has varied sharply throughout time.

Why does volatility matter? First, a volatile asset is a less secure asset, from an investor's point of view. Contrary to gold or government bonds, it might yield a greater return but bears the risk of abruptly losing its value. Second, volatility means that one cannot predict the value of a commodity (labelled in Bitcoin) even in the very near future, because the valuation of the currency tends to fluctuate constantly and in a random way. This means that Bitcoin cannot be a stable unit of account as it is unable to represent adequately the value of goods and services. Volatility exacerbates uncertainty and undermines the possibility of contracting in Bitcoin, which cannot, therefore, constitute a reliable means of exchange and a secure store of value.

In sum, the empirical evidence from Bitcoin's financial records appears to contradict the claim that Bitcoin can provide a stable means of payment and store of value, and thus dashes the hope that it can function as a stable currency, in line with the theoretical prescriptions of Milton Friedman and Friedrich Hayek.

Does Bitcoin provide a secure payment system?

Bitcoin is often presented as the basis for a more secure and efficient payment system, which allows to dispense altogether with the need for a trusted third party.³⁰ According to James Angel and Douglas McCabe, Bitcoin "represents a technological solution that creates appropriate incentives for honesty without needing a government to enforce laws against dishonesty".³¹ This motivation originally comes from a distrust of banking institutions, which, in the context of the 2007–2008 global financial crisis, many consider as unsafe.³² Presenting Bitcoin in the aftermath of the crisis, Satoshi Nakamoto has some harsh words for our current banking system: "Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve".³³ Bitcoin's payment system is presented as safer, since it does not require trusting any particular payment intermediary. Moreover, Nakamoto also points to two other disadvantages of having to rely on a trusted third party: the transaction costs it induces and the possibility of fraud through reversal of transactions.³⁴ By providing "a system based on cryptographic proof instead of trust", Bitcoin purports to reduce transaction costs due to the absence of intermediary and to reduce opportunities for fraud by making transaction irreversible.³⁵

However, while Bitcoin's protocol itself has been remarkably secured against possible abuses or manipulations, this security is undercut by the difficulty for

users of securing their Bitcoins against fraud or loss. Indeed, Bitcoin users are faced with a dilemma between ensuring their own security and trusting intermediary services.

Storing one's wallet on one's computer is not much different than keeping one's money in a safe: unsecure password can be cracked, stolen through "phishing" scams, or simply forgotten. And because Bitcoin transactions are non-reversible, victims are left without recourse in case of theft.

Therefore, for many users, online wallet services and even Bitcoin exchanges can appear as safer alternatives for storing and trading one's Bitcoins, just as banks are considered safer than keeping one's money in safes. But if one resorts to such online intermediaries, Bitcoin is not any more secure than conventional currencies, where one has to rely on banking and payment intermediaries. It can be even less secure, as few of these services are (for the moment) regulated beyond the usual protection of general contract and insolvency law (the main focus of legislators having been the use of cryptocurrencies for money laundering).

Users of cryptocurrencies are therefore left without much protection against fraud or bankruptcy. As the European Banking Authority rightly highlighted shortly after the advent of Bitcoin, "no specific regulatory protections exist that would cover you for losses if a platform that exchanges or holds your virtual currencies fails or goes out of business".³⁶

On the contrary, centralised payment systems, such as the Euro system, are partly protected from such events. In Belgium, for instance, banking deposits are guaranteed by the state up to 100,000€ per person.³⁷ Of course, the protection of deposits differs from the protection of payments. However, the fact that deposits are protected is an indirect protection of payments: people are ensured that their money is safe (or a large part of it) and the continuity of payments is therefore guaranteed. Moreover, states usually play the role of lender of last resort. If banks go bankrupt, that is, if they cannot honour their debts anymore, states can usually bail them out to avoid a collapse of the economy.³⁸ These two kinds of protection are absent from the Bitcoin's payment system, which exposes users to frauds and to bankruptcies of exchange platforms.

Can Bitcoin avoid formal governance?

A third argument contends that Bitcoin may contribute to lessening the level of state coercion facing individuals, by putting money out of the control of government or any centralised institution. Indeed, another common objection to the exercise of monetary policy by states, besides stability, stems out of a libertarian concern for the protection of the rights and liberties of individuals.³⁹ Safeguarding these rights and liberties puts limits on what others can legitimately do to people without their consent. The state should keep only a marginal role, which basically consists of protecting property rights from theft or fraud.⁴⁰ Apart from that, state intervention in the economy encroaches on individual freedom (i.e., it amounts to coercion) and is therefore wrong.

This argument clearly rejects the possibility of the state's monopoly over money. In the words of Murray Rothbard, such a monopoly allows the state to act as a "legalized, monopoly counterfeiter" and use monetary creation as "a giant scheme of hidden taxation", thereby violating individual property rights.⁴¹ Similarly, for Friedrich Hayek, "legal tender is simply a legal device to force people to accept in fulfilment of a contract something they never intended".⁴² It thus violates their freedom to set voluntarily the terms of a contract.

Libertarianism constitutes an important philosophical root among Bitcoin proponents.⁴³ For libertarians such as Kevin Dowd, Bitcoin safeguards "the freedom of the individual to trade, and the freedom of the individual to accumulate, move and protect his or her financial wealth – in other words, financial freedom".⁴⁴ Because it supposedly allows to dispense with the need for any central institution, Bitcoin may significantly weaken the hold of coercive institutions over individuals' lives.

Whatever the merits of the underlying libertarian argument, it is dubious that Bitcoin can dispense altogether with any formal governance or trust in some privileged actors. While Bitcoin has indeed no formal governance (there is no constitution or founding principles setting decision-making procedures), a set of practices have emerged, in the interplay of three categories of actors: core developers, miners, and users.

Taking over from Nakamoto's initial drafting of the protocol, the core development team enjoys a sort of moral authority over the community, which entrusts it for technical decisions. As with many open-source development projects, Bitcoin follows an "autocratic-mechanistic" model, where anyone is free to contribute code, but a small group of co-opted developers (the core developers) can ultimately decide which changes get implemented in the software.⁴⁵

However, it is important to note that the Bitcoin core development team cannot impose any modifications to the existing Bitcoin protocol without the consent of at least a substantial number of miners or users. Since Bitcoin relies on an open-source software, any user could refuse to update its software and continue to use its older version or propose an alternative change to shift the software development in a different direction, thereby creating a "fork" (an alternative branch of a software development). In the case of Bitcoin, this can happen essentially through two mechanisms.

The first is called a "soft fork" and consists of adding stricter rules determining which blocks or transactions are valid. A soft fork can be imposed on the existing network with the collaboration of miners with a mere majority of hash-power, which can enforce the new rules by rejecting blocks or transactions that do not conform to the change. The second is called a "hard fork", which touches on the fundamental characteristics of the protocol such as block structure or difficulty rules. As it is not backward compatible, a hard fork requires all full nodes to upgrade, or the blockchain could split between users using the new updated version and those using the old version.

For a long time, these issues of governance were mostly ignored, due primarily to the idea that the developers' role was purely technical and unlikely to cause deep ideological divergence. In the last few years however, the Bitcoin block size controversy has brought to light the importance of governance and what Primavera de Filippi and Benjamin Loveluck call the "invisible politics" of Bitcoin.⁴⁶

A first risk of split occurred in 2015 when some Bitcoin core developers proposed a fork called "Bitcoin XT", aiming to increase its block size from 1 to 8 Mb. After much debate, the Bitcoin community stayed loyal to the original Bitcoin protocol (billed "Bitcoin Core"), thus avoiding a definite split. But the attempts by the reformists pursued, and during 2016 and 2017 various fork proposals have been made, either by consortiums of miners or by users. To succeed, these reform proposals generally require reaching a particular adoption rate of a qualified majority of miners or users before a given date. This process remains complex and risky for the integrity of Bitcoin's blockchain. And indeed, it already generated its first major split: in August 2017, after months of Bitcoin scaling controversy, a group of users successfully hard-forked Bitcoin, as well as its whole transaction history, into a new cryptocurrency with a block size of 8 Mb, named Bitcoin Cash. While the hard fork did not cause the rate of Bitcoin to crash, as some feared, it nonetheless showed that the risk of a Bitcoin schism was a very real possibility.

The risk of schisms is a huge problem for cryptocurrencies, where network effects are crucial: a currency can only function as such if enough people are willing to exchange it or accept it as a means of payment. Schisms could significantly weaken Bitcoin by diminishing its attractiveness as a medium of exchange. Admittedly, until now the existence of a great number of alternative cryptocurrencies has apparently not curbed user enthusiasm for Bitcoin. However, there is a significant risk that the ongoing multiplication of Bitcoin clones (such as "Bitcoin Cash", "Bitcoin Gold", and "Bitcoin Diamond") will constitute a factor of confusion for the broader public, thereby threatening its ability to be used as a mainstream medium of exchange.

Therefore, not only is Bitcoin not the self-governing, radically decentralised currency that some of its supporters would want it to be. Bitcoin's informal governance, plagued by the risk of schisms, also constitutes a significant threat to its sustainability as a currency.

Consequently, either the Bitcoin community retains its own libertarian form of "governance", with risks for its governability, user base, and security, or it recognises that some degree of formal central governance is inevitable. But that recognition leads to what Vili Lehdonvirta bills the "blockchain's governance paradox": if Bitcoin users address the problem of governance by trusting a central institution to make the rules, then why do they need a decentralised cryptocurrency anymore?⁴⁷

The prevailing scepticism against governance among the Bitcoin community has made any change in its algorithmic regulation very difficult and long to achieve and prevented putting in place any structural reforms. As a

consequence, Bitcoin's informal governance model cannot meet its promise to provide a reliable alternative to the allegedly flawed centralised banking system.

Can Bitcoin improve payment privacy?

Bitcoin's fourth alleged advantage flows from the previous one: because Bitcoin's payment system (supposedly) does not rely on trusted intermediaries, it would better protect the privacy of its users than conventional means of payments. For instance, Satoshi Nakamoto complains that "we have to trust [banks and payment intermediaries] for our privacy [and] trust them not to let identity thieves drain our accounts".⁴⁸ In the aftermath of the NSA surveillance scandals, which has shown that private intermediaries could rarely be trusted to protect the privacy of their customers against overreaching state authorities, privacy has often been viewed as one of Bitcoin's main appeal.

There are many good reasons why people might seek privacy in their transactions. They might wish to avoid mass data collection of their transaction history by private companies for targeted marketing, or they can be political opponents, fearing retribution from authoritarian regimes.

However, these privacy-protecting features are also what makes Bitcoin a particularly suitable tool for engaging in fraud, illegal business and tax evasion, which has been a recurrent concern for lawmakers. Yet is Bitcoin really protecting its users' privacy?

At the core of the Bitcoin protocol are two distinct features, which have opposite tendencies in terms of anonymity. On the one hand, Bitcoin's public ledger tends to make it more transparent, as all transactions are logged in a publicly accessible ledger. On the other hand, Bitcoin's peer-to-peer network tends to make it more anonymous (as it does not rely on the presence of financial intermediaries holding all the users' information).

As others have noted, Bitcoin only provides pseudo-anonymity, in that while a given transaction only lists the pseudo-anonymous Bitcoin address of the sender and receiver, details of all transactions are logged on the public ledger. Therefore, as Jason Luu and Edward Inwinkelried put it, "[i]f a Bitcoin address could somehow be associated with a specific identity, the pseudo-anonymity would be penetrated".⁴⁹ Parties to a transaction could be traced back to the holder of an exchange account, by using identification techniques such as traffic analysis and transaction graph analysis. State authorities could use such information to identify customers of cryptocurrency exchanges, provided that "Know Your Customer" obligations are imposed on these exchanges. In the EU, for instance, all payments and transactions in cryptocurrencies are subject to obligations for financial operators to report transactions suspected of being the proceeds of criminal activity or being related to money laundering or terrorist financing.⁵⁰

Therefore, until Bitcoin use becomes sufficiently widespread that an autonomous Bitcoin economy could be imaginable, the position of gatekeepers held by exchanges in the flow of Bitcoin appears to undercut the claim for Bitcoin

to be any more privacy-protecting than conventional currencies. Indeed, neither Bitcoin nor the euro or the dollar is entirely disintermediated; they are just relying on different sorts of financial intermediaries.

Of course, users could possibly resort to exchanges or mixing services based in lax or lawless jurisdiction, in order to minimise the risk that their data be handed over to the authorities by such services. They would however face an important issue of trust, as those unregulated mixing services are also likely to be the less reliable, with little guarantee of seeing one's money back in case of fraud. This apparently happened to Sarah Meiklejohn and her co-authors while studying these services. They note in their article that “[o]ne of these [mixing services], BitMix, simply stole our money”.⁵¹

The latter example illustrates how the decentralised (although not entirely disintermediated) nature of cryptocurrencies like Bitcoin comes with one important drawback for user privacy: without banks or other financial institutions, users are solely responsible for the privacy of their transaction. And any average – not particularly tech savvy – consumer will be more likely to commit some privacy oversight in its Bitcoin transactions. Therefore, paradoxically, the many flaws in Bitcoin's privacy protection mean that unsophisticated users might enjoy a lesser level of transaction privacy by using such a pseudo-anonymous cryptocurrency than by relying on traditional financial intermediaries.

Central Bank Digital Currencies

The previous section has shown that Bitcoin cannot deliver on its promises to constitute a stable, secure, and decentralised currency. Neither can Bitcoin effectively protect its users' privacy. Could public alternatives be more successful? CBDC provides a fitting example to answer this question.

As I already noted earlier, most money today consists of deposits on accounts in private banks or other financial institutions. A small share of the money supply is also constituted of cash (coins and notes), though the use of cash is slowly and consistently decreasing in many countries. Alongside cash and bank deposits, there is also a third form of money: central bank reserves. These are the deposits that the private banks hold at the central bank. Reserves are a digital form of money but underwritten by the central bank and mainly used to facilitate inter-bank payments.

How would CBDC fit into this picture? Despite its name, CBDC would not constitute a new currency but a new means of payment, labelled in a national official currency and available to all individuals and firms, alongside cash and bank deposits. CBDC could then take either of two shapes: it could be a form of digital coin or token, making it similar to cash, or it could be a form of digital account, making it similar to bank deposits and central bank reserves.⁵² In practice, virtually all CBDC proposals are “account-based”, as this option is easier to implement, safer, and under direct control of the central bank.⁵³ In essence, then, CBDC is an extension of the system of central bank reserves

to the general public. While only commercial banks (and a few financial arms of companies) are allowed to take part in that system today, CBDC would open it up to all citizens and firms.

People could have access to CBDC either directly from their central bank or indirectly through accredited commercial institutions. One option would be to give to everyone the possibility to hold an account at the central bank – like commercial banks today. Another would be to let commercial banks or specific agencies administrate a system of indirect accounts, labelled in CBDC. The possibility of the first scenario depends on the capacity of modern technology to reduce significantly the cost, for a single institution (which is currently unacquainted with this task), of managing millions of accounts. For example, J. P. Koning's "Fedcoin" proposal assumes that the Federal Reserve could create a digital currency whose circulation and emission would be managed through a "distributed ledger" technology, much like Bitcoin.⁵⁴ In this scenario, then, the Federal Reserve itself would manage the whole payment system. Alternatively, central banks could leave this task to commercial banks or specific non-bank intermediaries.⁵⁵ The money would then stay at the central bank, and be legally its money, but accredited financial intermediaries would provide access to these accounts to the public. These intermediaries would be the interface between firms or citizens and the central bank, and they could also deliver classical banking services labelled in CBDC.

How would CBDC be introduced into society? The most common scenario is that CBDC is introduced as a complement to other forms of money, at least in the initial phase. The role of the central bank could be either reactive or proactive. In the reactive scenario, CBDC is simply offered as a voluntary alternative. In the proactive scenario, the central bank takes active measures to increase the use of CBDC over time. These measures could in turn vary in strength: for example, the central bank could set a favourable exchange rate between bank deposits and CBDC to raise incentives. Alternatively, it could seek to inject CBDC directly into the economy.

There are several possible channels for the direct introduction of CBDC. For example, CBDC could be issued through exchanges against government bonds or other financial assets, which is the scenario imagined by John Barrdear and Michael Kumhof.⁵⁶ Another suggestion is that central banks should issue CBDC directly to people's accounts, which is sometimes called the "helicopter drops" proposal.⁵⁷

Would CBDC accounts function like normal bank accounts, for example, in accruing interest over time? Michael Bordo and Andrew Levin think that CBDC should be remunerated in a way similar to commercial bank accounts. They state that interest-bearing CBDC "could constitute a secure store of value" and that "the CBDC interest rate could serve as the main tool for conducting monetary policy".⁵⁸ An interesting feature is that remunerating CBDC would allow central banks to go beyond the Zero Lower Bound – that is, to set up a more pronounced negative interest rate. This is difficult in the current system as economic agents will prefer to hold cash (whose nominal yield

is zero) rather than deposits (whose nominal yield would be negative). Without cash as an alternative to CBDC, central banks could set a negative interest rate on reserves and CBDC to boost investments.⁵⁹ However, this will only work if all cash is substituted for CBDC, which seems somewhat unrealistic. Thus, Ben Dyson and Graham Hodgson argue for a purely cash-like and unremunerated version of CBDC.⁶⁰ They contend that remunerating CBDC would be difficult and may endanger the central bank's or the state's budget. Since the latter version seems less controversial in the debate, I will assume an unremunerated CBDC for the remainder of this chapter.

It is interesting to consider to what extent CBDC would be similar to Bitcoin and other cryptocurrencies. One of the main issues here is whether CBDC requires some form of centralised bookkeeping, as in the current system, or may rely on a “distributed ledger” technology, such as the one underlying Bitcoin.

As we have seen, Bitcoin relies on a decentralised payment system, which records all transactions on a ledger that is distributed across an online network; “miners” compete to verify transactions, and the “winner” gets a reward for registering it on the ledger. This technology has several important properties. First, it is public. Every user can verify and process transactions. Second, cryptographic technologies secure the ledger against falsifications, without resorting to any financial institution or central authority. Finally, the fact that the ledger is publicly available means that Bitcoin can only preserve a “pseudo-anonymity” for its users, who can be identified by their Bitcoin address.

As things stand, some central banks are actively thinking about “decentralising” their payment system.⁶¹ A decentralised payment system would have several advantages. The main advantage would be a reduction of the costs of handling payments (for individuals) and verifying payments (for central banks) since decentralised payment systems would allow settlements directly between parties, without resorting to a central agency. It could also make settlements of cross-border transactions safer and more rapid. Finally, it could reduce the risk of technological failure of the payments system: as a larger number of payment providers will connect to the central bank, the bankruptcy or technological failure of any single actor would be less likely to threaten the overall system.⁶²

However, there are also disadvantages associated with a decentralised payment system. The cost-saving property may be exaggerated since making it work on a large scale could incur huge costs, as the case of Bitcoin illustrates. Bitcoin's proof-of-work mechanism entails that huge volumes of computing power are invested in “mining” facilities by private companies, which seek to get the reward associated with the validation of a transaction. The economic and environmental costs of mining cannot be underestimated and could seriously threaten the viability of a payment system such as CBDC, which would be implemented on a much bigger scale.⁶³ Finally, Bitcoin's payment system has also experienced several technical failures and serious security breaches during its short history – two prospects that would be a real nightmare for central banks.

Therefore, it seems that the most likely scenario is that CBDC would run on a centralised payment system, and hence not constitute a cryptocurrency but “merely” a digital currency. In other words, in technical terms, CBDC would actually be closer to the current system of central bank reserves than to Bitcoin or other private cryptocurrencies.

The ethics of Central Bank Digital Currencies

Apart from its promise to smooth the payment system, which was briefly discussed earlier, CBDC retains at least three other major potential benefits. First, it would provide central banks with an additional monetary policy option that can be used in economic downturns, namely to credit citizens’ accounts directly.⁶⁴ Second, CBDC has the potential to reinforce financial stability since it would provide a “safe haven” outside of the private financial sector.⁶⁵ Both of these promises rely on a third and more fundamental promise, namely CBDC’s ability to challenge the excessive level of power held by private financial institutions over our current monetary system.

Commercial banks retain both structural and infrastructural power in our current monetary and financial system. Commercial banks (collectively) wield structural power because of the central role they play in our economy, which relies heavily on bank intermediation for the provision of credit and the creation of money. Their structural power comes from the hard fact that modern capitalist economies, as they are currently designed, cannot do without them. Under the current system of fractional reserve banking, commercial banks provide the fuel of our economies, that is, credit. Because credit is so essential to the functioning of our economy, commercial banks have acquired a structurally dominant position within the financial system.

Moreover, the role of banks within the financial system gives them infrastructural power: they have (collectively) extensive powers over the transmission channels of the central bank’s monetary policy. Central banks have no direct access to the economic activities or accounts of citizens or firms. All they can do is to manipulate the interest rate on central bank reserves. Interest rate manipulations are then “transmitted” to the economy through commercial banks, which, it is hoped, will adapt their own rates in response to the change. Because of this, central banks can only steer the economy indirectly, through the financial infrastructure provided by commercial banks and the financial industry. Hence, commercial banks have acquired significant infrastructural power over their regulator.⁶⁶

It must be noted that these powers are collective: a single bank does not have any real structural or infrastructural power. But, together, commercial banks have significant powers. Moreover, these powers are the product of complex interactions among many actors. Commercial banks have not “robbed” these powers from the state or gained them by other means simply by their own will. They have acquired them through a long historic process and partly as the unintended consequence of past regulatory decisions by states, central banks, and regulators.⁶⁷

The main promise of CBDC is exactly that it could address these problems: it could deflate the structural and infrastructural powers of commercial banks – for two main reasons.

First, CBDC would decrease the structural power of banks, since the economic system would be less reliant on commercial banking. Namely, the introduction of CBDC would offer an alternative payment system that is not managed by the commercial banking sector. This would have several advantages. Individual and private firms would have more options available as to where to deposit their money. They would be able to hold their savings at the central bank, an option which, by definition, would be safer than a commercial bank account.⁶⁸ Moreover, by allowing people to bypass (at least to some degree) the banking system, CBDC would also reduce the “too-big-to-fail” problem.

This latter problem proves particularly acute during a financial crisis. Governments may be in a situation where not saving the banks that go bankrupt would hurt the economy, and, therefore, the prospects of the electorate, so much that letting them fail is not a viable policy option for politicians seeking re-election. They will bail out bankrupt commercial banks to save the economy (and their chance of re-election) – even if the behaviour of these banks was, by all standards, reckless. Commercial banks (or their governing bodies) anticipate this: they know that, whatever the risk they take, governments will bail them out. Commercial banks, given their structural power in the economy, and given the realistic assumption that governments will bail them out, thus have an incentive to take excessive risks, and, hence, precipitate the very crisis that government intervention is meant to avoid. The Too-Big-To-Fail problem, in other words, is a clear case of moral hazard, in which an actor (here, commercial banks) has an incentive to take excessive risks because it does not bear the full negative consequences of these risks.

CBDC would greatly reduce the TBTF problem, because government will have fewer incentives to bail out failing commercial banks, given the existence of a fall-back mechanism, that is, accounts at the central bank. Consequently, CBDC has the potential to reduce financial instability. CBDC’s success in these regards would, of course, depend on its rate of adoption among citizens and firms.

Second, CBDC could reduce the infrastructural power of banks and thereby help central banks regain control over their monetary policy. Since CBDC would provide central bankers with a direct monetary channel to reach households and firms, central bankers would no longer be dependent on commercial banks to transmit their monetary policy. Instead, CBDC could give central banks access to a new kind of monetary policy instrument, namely, to credit the accounts of both firms and citizens directly.

The latter possibility has been called the “helicopter money” proposal. It is not new, and, it must be noted, not necessarily linked to CBDC. Yet, CBDC would greatly help its implementation by allowing central banks to credit citizen’s accounts directly and efficiently. The helicopter money proposal was

originally a thought experiment of Milton Friedman in which he envisioned central banks “dropping” newly created cash directly into households’ accounts.⁶⁹ In the aftermath of the 2007–2008 financial crisis, NGOs and think tanks resurrected the proposal and called it “Quantitative Easing for the People”, arguing that it would allow central banks to support a broader range of policy goals, such as reducing inequality and promoting environmental sustainability.⁷⁰

Yet, policy reforms often come with unintended consequences, whose costs might outweigh the benefits. Despite its promises, the CBDC proposal may have (at least) two negative consequences. First, the introduction of CBDC may increase the risk of bank runs and thus threaten financial stability. Second, it may further expand the already great powers of central bankers, without proper democratic checks.

First, as argued earlier, CBDC would provide a “safe haven”, away from the traditional banking system. However, the existence of this safe haven may in fact threaten financial stability, rather than reducing it. The existence of CBDC may increase the likelihood of bank runs, that is, situations in which a large number of customers withdraw their money from a commercial bank at the same time.⁷¹ If a significant number of people decide to move their money away from banks onto their CBDC account, this would significantly threaten the stability and liquidity of commercial banks, which are nevertheless needed as providers of credit in a market economy. Another issue is linked to the fact that, due to increased competition from public institutions, private banks could lose access to safe assets to back their lending activities. Hence, CBDC could force commercial banks to rely on riskier sources of funding, which would make the whole financial system less stable.⁷²

These risks may be exaggerated, though, as current regulations protect consumers’ accounts against defaults.⁷³ Similarly, many central banks, such as the central bank of Sweden, which is seriously considering introducing CBDC, have made clear that this would not weaken their pledge to act as a lender of last resort in case of crisis.⁷⁴ But we may ask whether that pledge will be credible enough. CBDC puts a heavier weight on central banks to safeguard financial stability in all situations. This is a problem if, for example, the reputation of the central bank would come into question. CBDC may increase the risk of reputation loss due to conflict of interests, as central bankers would now be tasked with monetary policy, financial supervision, as well as providing banking services themselves (either directly or indirectly).

Second, it seems clear that CBDC could challenge the excessive power that commercial financial institutions have over our current monetary system. However, it seems equally clear that CBDC comes with a major drawback: the cost of reducing the power of commercial banks would be to increase the power of (unelected and independent) central bankers. In most developed economies, central banks are independent from political interference, and the extent of their prerogatives is generally defined in their mandate, which delineates the policy objectives and the monetary policy instruments available to

them. The introduction of CBDC gives rise to several difficult decision problems that are beyond the legitimate realm of central bankers. Consider, for example, the issues pertaining to financial inclusion. Who should be allowed to open CBDC accounts? Do you need a specific citizenship or visa to register? These questions become even more difficult if we factor in the “helicopter drops” proposal: What citizens or firms should receive the money? How much should they get? And should the amount vary according to wealth and income? These questions go far beyond the realm of competence and legitimacy of central bankers as we know them. In short, the introduction of CBDC would greatly extend the role and responsibility of central banks beyond their original contract of delegation as defined in their mandate.

In sum, the introduction of CBDC creates a dilemma: on the one hand, it would significantly reduce the structural and infrastructural power of commercial banks. On the other hand, it would give greater powers to already powerful institutions, and it could actually threaten financial stability. The political question at its core, then, concerns the adequate balance of power between commercial banks, central banks, and the state. I take up this task in the next section.

Concluding remarks: money and the state

What lessons can we draw from the critical discussion of Bitcoin and CBDC?

As we saw, it is dubious that Bitcoin, as it is now, can deliver on its promises. First, Bitcoin’s financial record detracts from any claim of being a stable currency: its highly volatile value makes it risky for merchants to accept, and inconvenient for consumers to use. Second, Bitcoin’s promise to provide a secure store of value or means of payment is not supported by evidence from its use. Third, Bitcoin’s pseudo-anonymous payment system provides a very limited layer of protection for the privacy of user transactions. Paradoxically, for the average user, Bitcoin might even provide a lesser level of transaction privacy than traditional financial intermediaries. And fourth, the promise of making Bitcoin a currency independent from central authorities has been largely a double-edged sword. Even if the Bitcoin protocol is an achievement of a currency run by a radically decentralised network, it is highly unlikely that it can act as a reliable and governable currency without some formal governance mechanisms, and without resorting to some financial intermediaries. Without formal governance mechanisms, Bitcoin ultimately relies on trusting the goodwill of its users – the very thing it purported to avoid!

The analysis of Bitcoin thus indicates that some form of central governance may still have some usefulness after all. First, the example of Bitcoin reminds us that, without guarantees from the state, there is a significant risk that money will not function as a stable means of payment and as a secure store of value. Of course, one cannot conclude, on the basis of this analysis, that money without state is always a failure. It would be a mistake to build a general theory of monetary policy based on the analysis of one quite peculiar currency. Yet, the

case of Bitcoin gives credit to the claim that state's involvement in monetary affairs is one way, certainly imperfect, to make sure that the payment system is safe and stable. Second, the example of Bitcoin makes clear that some central governance is necessary in monetary affairs. It does not tell, though, what exact sort of governance we need. The study of CBDC has been the occasion to raise that question and has given some insights as to which actor – the state, independent central banks, or the commercial financial sector – is best equipped to face the challenges of the governance of monetary affairs.

In this chapter, I have briefly investigated whether CBDC is a desirable addition to our current monetary system. I have highlighted both its promises and its perils in terms of circumventing financial power. On the one hand, the present state of the private financial sector is indefensible, and regulators cannot turn a blind eye towards the problems created by the structural and infrastructural power of financial institutions. In that context, CBDC has the potential to curb the structural and infrastructural power of commercial banks and may therefore constitute a valuable addition to the arsenal of central banks. On the other hand, implementing CBDC comes with risks of its own, such as that of creating a “Frankenstein scenario” where too much power is given to unelected technocrats.

This dilemma is related to the pivotal but difficult role of central banks. On the one hand, central banks must ensure a certain level of confidence in the monetary system: they need to control the channels of transmission of monetary policy and avoid creating situations of moral hazard when they intervene in the financial system. On the other hand, if they exert an excessive level of control over the production of money and the allowance of credit, they will go far beyond the remit of their mandates – and the confidence of both economic agents and the general public can also be undermined.

What, then, is to be done?

It may be worth looking at history for a brief moment. Many of the problems currently facing the financial sector stem from the several decades of financial deregulation that started with the policies of Ronald Reagan and Margaret Thatcher in the 1970s and 1980s.⁷⁵ It does not seem unreasonable, then, to seek remedies to the problems in some form of re-regulation of the commercial financial sector.

In the aftermath of the 2007–2008 financial crisis, there was indeed some political momentum for financial re-regulation. Several of the new regulations that came into place were designed to tackle exactly the problems of TBTF and financial instability. For example, the Dodd-Frank Wall Street Reform and Consumer Protection Act was passed in the US in 2010. Some of its main provisions were to separate banks' speculative activities from their retail operations (the so-called Volcker rule), restrict or regulate trade in very speculative investments (such as credit default swaps), create a new oversight council for financial stability, and increase the powers of various financial supervisory authorities. In a similar vein, European regulators introduced the Basel III framework in 2010. Some of its main provisions were to impose higher

liquidity ratios and stricter capital requirements on commercial banks. Moreover, the EU created the so-called Single Resolution Mechanism in 2014 in order to have an orderly process of bankruptcy for financial institutions (which they partly would have to pay for themselves).

While I cannot evaluate these policies here, their appeal lies in their potential of addressing the problems of TBTF and financial instability while avoiding the negative consequences associated with CBDC and Bitcoin. For example, challenging the structural power of commercial banks may not require ever more powerful central banks, but could instead be done through a re-regulation of the appropriate size and service mix of commercial banks. Similarly, safeguarding the stability of the financial system may not require the creation of a “safe haven” outside the private market, but could instead involve the imposition of appropriate levels of risk-taking, liquidity, and capital reserves on financial institutions. In short, as Sheila Dow argues, re-regulation measures taken at the national and international level would probably fare better than CBDC to regain control over financialised economies.⁷⁶

Obviously, one should not forget that, in practice, re-regulatory efforts have often been too mild. A case in point are the attempts of separating commercial banking from investment banking (such as the US Volcker rule and the UK Banking Act) which were weakened significantly during the legislative process and may therefore include too many loopholes to end the TBTF problem. The recent EU experience is a further case in point: the European Commission’s proposals on structural banking reforms were shelved in 2018 because of the lobbying efforts of large European banks.⁷⁷ In sum, despite partial regulatory improvements, the lack of stringent structural reforms after the crisis allowed a resurgence of risky financial activities and unsustainable business model in the banking industry.

If all other reforms to address the TBTF problems were doomed, CBDC could emerge as a desirable policy option, despite its shortcomings. If not, regulation of the financial sphere has to be preferred. The state, therefore, emerges from this discussion as an important player in monetary affairs: its role comprises securing the payment system against fraud, guaranteeing privacy, regulating financial activities to avoid (or minimise the risk of) instability and moral hazard, and, more demanding still, offering a democratic platform for the governance of monetary affairs.

Notes

- 1 Frisby (2014).
- 2 Vigna and Casey (2015).
- 3 Among them, see Dodd (2017), Glaser et al. (2014), Yermack (2015), and Smit, Buekens, and du Plessis (2016).
- 4 Dwyer (2015).
- 5 Böhme et al. (2015).
- 6 On this proposal, see Nessén and Söderström (2020).
- 7 Dyson and Hodgson (2016), and Bordo and Levin (2017).

- 8 Bech and Garratt (2017), Engert and Fung (2017), Barontini and Holden (2019), and Boar, Holden, and Wadsworth (2020).
- 9 See the Introduction of this book, where I discuss the literature on the nature of money in greater detail, as well as Chapter 1.
- 10 This part of the chapter draws on my work in collaboration with Maxime Lambrecht, Clément Fontan, and Joakim Sandberg. See especially Larue (2016), Lambrecht and Larue (2018), Fontan and Larue (2021), and Larue et al. (2020).
- 11 Nakamoto (2008). On the mystery over Nakamoto's identity, see Davis (2011).
- 12 For a detailed presentation of the technicalities of Bitcoin, see Ali et al. (2014b).
- 13 I will discuss the issue of "pseudo-anonymity", as Luu and Imwinkelried puts it (2015), later in this chapter.
- 14 Wallace (2011).
- 15 For a detailed presentation of how transactions in Bitcoins works, see Ali et al. (2014a, 266–71). For an overview of Bitcoin's technicalities, see Böhme et al. (2015).
- 16 Ali et al. (2014a, 278).
- 17 For various takes on the question, see Bjerg (2016), Glaser et al. (2014), Urquhart (2016), Yermack (2015), and Smit, Buekens, and du Plessis (2016).
- 18 Yermack (2015).
- 19 Smit, Buekens and du Plessis (2016).
- 20 For a more thorough critique of why I think they are mistaken, see Larue (2024, 731–32).
- 21 I briefly review the theories of these authors in the Introduction of this book, under the section Money.
- 22 Smit et al. (2016, 333).
- 23 See, e.g., Ametrano (2016).
- 24 Nakamoto (2009).
- 25 See, for instance, Hayek ([1976] 1990, 28–32).
- 26 Friedman (1968, 16) argues for an annual growth rate comprised between 3% and 5%, but leaves the door open for a smaller rate still (around 2%). See also Friedman (1969, 90–91).
- 27 See Bordo (2008) for a review of the debates.
- 28 Dwyer (2015).
- 29 Cheah and Fry (2015) and Cheung, Roca, and Su (2015).
- 30 Ali et al. (2014a), and Angel and McCabe (2015).
- 31 Angel and McCabe (2015, 606).
- 32 Ali et al. (2014a, 267).
- 33 Nakamoto (2009).
- 34 See also Angel and McCabe (2015, 606).
- 35 Nakamoto (2008, 1).
- 36 European Banking Authority (2013, 1).
- 37 As described on the website of the Belgian Ministry of Finance: <http://fondsdegarantie.belgium.be/fr>.
- 38 I discuss the moral hazard problems that this may cause in the section on Central Bank Digital Currencies.
- 39 It is worth quoting Nozick's famous statement that "individuals have rights, and there are things no person or group may do to them (without violating their rights)" (Nozick [1974] 2012, ix).
- 40 Regarding the state, Nozick contends that "a minimal state, limited to the narrow functions of protection against force, theft, fraud, enforcement of contracts, and so on, is justified; (...) any more extensive state will violate persons' rights (...) and is unjustified" (Nozick [1974] 2012, ix).
- 41 Rothbard ([1995] 2024, 12).
- 42 Hayek ([1976] 1990, 39–40).
- 43 Golumbia (2016), Karlstrøm (2014), and Lakomski-Laguerre and Desmedt (2015).

- 44 Dowd (2014, 64).
- 45 This line of argument has been forcefully defended by de Filippi and Loveluck (2016), and de Filippi and Wright (2018).
- 46 de Filippi and Loveluck (2016).
- 47 Lehdonvirta (2016).
- 48 Nakamoto (2009).
- 49 Luu and Imwinkelried (2015, 10).
- 50 Directive 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, art. 1.
- 51 Meiklejohn et al. (2013, 130).
- 52 For this distinction, see Bordo and Levin (2017, 6–8).
- 53 Barrdear and Kumhof (2021).
- 54 Koning (2014).
- 55 As proposed by Dyson and Hodgson (2016), and Bordo and Levin (2017).
- 56 Barrdear and Michael Kumhof (2021).
- 57 Van Lerven (2016), see below for a discussion of that proposal.
- 58 Bordo and Levin (2017, 2).
- 59 On CBDC and the zero-lower bound, see Nabilou (2020).
- 60 Dyson and Graham Hodgson (2016, 31).
- 61 Fung and Alaburda (2016), and Engert and Fung (2017).
- 62 Dyson and Hodgson (2016, 10–11).
- 63 On the economic and environmental costs of Bitcoin, see Mora et al. (2018) and Krause and Tolaymat (2018).
- 64 Barrdear and Kumhof (2021, 12).
- 65 Dyson and Hodgson (2016, 9–10).
- 66 Braun (2020) was among the first social scientists to study and demonstrate that feature of modern financial systems. See also Fontan and Larue (2021, 159–161).
- 67 In particular, the slow development and current dominance of the Central Bank Independence framework has been decisive. On these points, see Fontan and Larue (2021, 156–158).
- 68 Dyson and Hodgson (2016, 9–10), and Engert and Fung (2017, 7).
- 69 Milton Friedman (1969).
- 70 Van Lerven (2016).
- 71 Camera (2017, 140), and Mancini-Griffoli et al. (2018, 21–22).
- 72 See Broadbent (2016, 3) and Raskin and Yermack (2018).
- 73 Niepelt (2020).
- 74 Sveriges Riksbank (2017).
- 75 Admati and Hellwig (2013).
- 76 Dow (2017, 2019).
- 77 Officially named the “Proposal for a regulation of the European parliament and of the Council on structural measures improving the resilience of EU credit institutions”, it was originally published on 29 January 2014 and officially withdrawn on 4 July 2018. See <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52014PC0043> [accessed on 21/10/2024].

References

- Admati, Anat, and Martin Hellwig. 2013. *The Bankers' New Clothes: What's Wrong with Banking and What to Do about It*. Princeton: Princeton University Press.
- Ali, Robleh, John Barrdear, Roger Clews, and James Southgate. 2014a. “Innovations in Payment Technologies and the Emergence of Digital Currencies.” *Bank of England Quarterly Bulletin*, Q3.

- Ali, Robleh, John Barrdear, Roger Clews, and James Southgate. 2014b. "The Economics of Digital Currencies." *Bank of England Quarterly Bulletin*, Q3.
- Ametrano, Ferdinando M. 2016. "Hayek Money: The Cryptocurrency Price Stability Solution." *SSRN Scholarly Paper ID 2425270*. Rochester, NY: Social Science Research Network.
- Angel, James J., and Douglas McCabe. 2015. "The Ethics of Payments: Paper, Plastic, or Bitcoin?" *Journal of Business Ethics* 132 (3): 603–611.
- Barontini, Christian, and Henry Holden. 2019. "Proceeding with Caution - a Survey on Central Bank Digital Currency." BIS papers 101. <https://www.bis.org/publ/bppdf/bispap101.htm>
- Barrdear, John, and Michael Kumhof. 2021. "The Macroeconomics of Central Bank Digital Currencies." *Journal of Economic Dynamics and Control* 142 (May):104148.
- Bech, Morten, and Rodney Garratt. 2017. "Central Bank Cryptocurrencies." *BIS Quarterly Review*, September, 55–70.
- Bjerg, Ole. 2016. "How Is Bitcoin Money?" *Theory, Culture & Society* 33 (1): 53–72.
- Boar, Codruta, Henry Holden, and Amber Wadsworth. 2020. "Impending Arrival – A Sequel to the Survey on Central Bank Digital Currency." *BIS Papers 107*. Basel: Bank for International Settlements.
- Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *The Journal of Economic Perspectives* 29 (2): 213–238.
- Bordo, Michael D. 2008. "History of Monetary Policy." In *The New Palgrave Dictionary of Economics*, edited by Steven N. Durlauf and Lawrence E. Blume, 2nd ed., 715–721. Basingstoke: Palgrave MacMillan.
- Bordo, Michael D., and Andrew T. Levin. 2017. "Central Bank Digital Currency and the Future of Monetary Policy." *Working Paper 23711*. Cambridge, MA: National Bureau of Economic Research.
- Braun, Benjamin. 2020. "Central Banking and the Infrastructural Power of Finance: The Case of ECB Support for Repo and Securitization Markets." *Socio-Economic Review* 18 (2): 395–418.
- Broadbent, Ben. 2016. "Central Banks and Digital Currencies." Speech, London. <http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech886.pdf>
- Camera, Gabriele. 2017. "A Perspective on Electronic Alternatives to Traditional Currencies." *Sveriges Riksbank Economic Review* 1:126–148.
- Cheah, E.-T., and J. Fry. 2015. "Speculative Bubbles in Bitcoin Markets? An Empirical Investigation into the Fundamental Value of Bitcoin." *Economics Letters* 130:32–36.
- Cheung, A.W.-K., E. Roca, and J.-J. Su. 2015. "Crypto-Currency Bubbles: An Application of the Phillips–Shi–Yu (2013) Methodology on Mt. Gox Bitcoin Prices." *Applied Economics* 47 (23): 2348–2358.
- Davis, Joshua. 2011. "The Crypto-Currency: Bitcoin and Its Mysterious Inventor." *The New Yorker*, October 10, 2011.
- De Filippi, Primavera, and Benjamin Loveluck. 2016. "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure." *Internet Policy Review* 5 (4).
- De Filippi, Primavera, and Aaron Wright. 2018. *Blockchain and the Law. The Rule of Code*. Cambridge, MA: Harvard University Press.
- Dodd, Nigel. 2017. "The Social Life of Bitcoin." *Theory, Culture and Society*, 35(3): 35–56.
- Dow, Sheila. 2017. "Central Banking in the Twenty-First Century." *Cambridge Journal of Economics* 41 (6): 1539–1557.
- Dow, Sheila. 2019. "Monetary Reform, Central Banks, and Digital Currencies." *International Journal of Political Economy* 48 (2): 153–173.

- Dowd, Kevin. 2014. *New Private Monies: A Bit-Part Player?* Hobart Paper 174. London: Institute of Economic Affairs.
- Dwyer, Gerald P. 2015. "The Economics of Bitcoin and Similar Private Digital Currencies." *Journal of Financial Stability*, 17:81–91.
- Dyson, Ben, and Graham Hodgson. 2016. *Digital Cash: Why Central Banks Should Start Issuing Electronic Money*. London: Positive Money.
- Engert, Walter, and Ben Fung. 2017. "Central Bank Digital Currency: Motivations and Implications." *Staff Discussion Paper 2017–16*, Toronto: Bank of Canada. <https://www.bankofcanada.ca/2017/11/staff-discussion-paper-2017-16/>
- European Banking Authority. 2013. "Warning to Consumers on Virtual Currencies." Statement EBA/WRG/2013/01.
- Fontan, Clément, and Louis Larue. 2021. "Central Banking." In *Routledge Handbook of Critical Finance Studies*, edited by Christian Borch and Robert Wosnitzer, 154–172. Abingdon: Routledge.
- Friedman, Milton. 1968. "The Role of Monetary Policy." *American Economic Review* 58:1–17.
- Friedman, Milton. 1969. "The Optimum Quantity of Money." In *The Optimum Quantity of Money and Other Essays*, by Milton Friedman, 1–50. Chicago, IL: Aldine.
- Frisby, Dominic. 2014. *Bitcoin: The Future of Money?* London: Unbound.
- Fung, Ben, and Hanna Alaburda. 2016. "Central Bank Digital Currencies: A Framework for Assessing Why and How." *Staff Discussion Paper 2016–22*. Toronto: Canada. <https://www.bankofcanada.ca/2016/11/staff-discussion-paper-2016-22/>
- Glaser, Florian, Kai Zimmermann, Martin Haferkorn, Moritz Christian Weber, and Michael Siering. 2014. "Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions." In *Proceedings of the 22nd European Conference on Information Systems*. Tel Aviv, Israel.
- Golumbia, David. 2016. *The Politics of Bitcoin*. Minneapolis, MN: University of Minnesota Press.
- Hayek, Friedrich A. (1976) 1990. *Denationalisation of Money: The Argument Refined*. 3rd ed. London: Institute of Economic Affairs.
- Karlstrøm, Henrik. 2014. "Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin." *Distinktion: Scandinavian Journal of Social Theory* 15 (1): 23–36.
- Koning, J. P. 2014. "Fedcoin." October 19, 2014. <http://jpkoning.blogspot.be/2014/10/fedcoin.html>
- Krause, Max J., and Thabet Tolaymat. 2018. "Quantification of Energy and Carbon Costs for Mining Cryptocurrencies." *Nature Sustainability* 1 (11): 711–718.
- Lakowski-Laguerre, Odile, and Ludovic Desmedt. 2015. "L'alternative monétaire Bitcoin: une perspective institutionnaliste." In *Revue de la régulation*, edited by Pépita Ould-Ahmed and Jean-François Ponsot. Capitalisme, institutions, pouvoirs, 18 (October), 1–19.
- Lambrecht, Maxime, and Louis Larue. 2018. "After the (Virtual) Gold Rush: Is Bitcoin More than a Speculative Bubble?" *Internet Policy Review* 7 (4).
- Larue, Louis. 2016. "Le bitcoin: évaluation d'une innovation monétaire." *Regards Économiques* 127 (September):1–10.
- Larue, Louis. 2024. "John Searle's Ontology of Money, and Its Critics." In *Palgrave Handbook of Philosophy and Money. Volume 2: Modern Thought*, edited by Joseph Tinguely, 721–741. Basingstoke: Palgrave MacMillan.
- Larue, Louis, Clément Fontan, and Joakim Sandberg. 2020. "The Promises and Perils of Central Bank Digital Currencies." In *Revue de La Régulation. Capitalisme, Institutions, Pouvoirs*, 28 (December).
- Lehdonvirta, Vili. 2016. "The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy." Oxford: Oxford Internet

- Institute. <https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/>
- Luu, Jason, and Edward J. Imwinkelried. 2015. *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics*. UC Davis Legal Studies Research Paper Series 462.
- Mancini-Griffoli, Tommaso Mancini, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu, and Celine Rochon. 2018. "Casting Light on Central Bank Digital Currencies." IMF Staff Discussion Note. Washington: International Monetary Fund.
- Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. 2013. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names." In *Proceedings of the ACM SIGCOMM Internet Measurement Conference*, 127–139.
- Mora, Camilo, Randi L. Rollins, Katie Taladay, Michael B. Kantar, Mason K. Chock, Mio Shimada, and Erik C. Franklin. 2018. "Bitcoin Emissions Alone Could Push Global Warming above 2°C." *Nature Climate Change* 8 (11): 931–933.
- Nabilou, Hossein. 2020. "Testing the Waters of the Rubicon: The European Central Bank and Central Bank Digital Currencies." *Journal of Banking Regulation* 21 (4): 299–314.
- Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." <http://www.bitcoin.org/bitcoin.pdf>
- Nakamoto, Satoshi. 2009. "Bitcoin Open Source Implementation of P2P Currency." <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>
- Nessén, Marianne, and Ulf Söderström, eds. 2020. "Special Issue E-Krona 2." *Sveriges Riksbank Economic Review* 2020 (2).
- Niepert, Dirk. 2020. "Reserves for All? Central Bank Digital Currency, Deposits, and Their (Non)-Equivalence." *International Journal of Central Banking* 16 (3): 211–238.
- Nozick, Robert. (1974) 2012. *Anarchy, State, and Utopia*. New York: Basic Books.
- Raskin, Max, and David Yermack. 2018. "Digital Currencies, Decentralized Ledgers, and the Future of Central Banking." In *Research Handbook on Central Banking*, edited by Peter Conti-Brown and Rosa María Lastra, 474–486. Edward Elgar Publishing.
- Rothbard, Murray N. (1995) 2024. *Taking Back Our Money*. Originally published as a three-part Series in *The Freeman*, September–November 1995. Auburn, AL: Mises Institute.
- Smit, J. P., Filip Buekens, and Stan du Plessis. 2016. "Cigarettes, Dollars and Bitcoins – an Essay on the Ontology of Money." *Journal of Institutional Economics* 12 (2): 327–347.
- Sveriges Riksbank. 2017. "The Riksbank's e-Krona Project." Stockholm: Riksbank. https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/handlingsplan_ekrona_171221_eng.pdf
- Urquhart, Andrew. 2016. "The Inefficiency of Bitcoin." *Economics Letters* 148:80–82.
- Van Lerven, Frank. 2016. "Quantitative Easing in the Eurozone: A One-Year Assessment." *Intereconomics* 51 (4): 237–242.
- Vigna, Paul, and Michael J. Casey. 2015. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York: St. Martin's Press.
- Wallace, Benjamin. 2011. "The Rise and Fall of Bitcoin." *Wired Magazine*, November 23, 2011.
- Yermack, David. 2015. "Is Bitcoin a Real Currency? An Economic Appraisal." In *Handbook of Digital Currency*, edited by David Lee Kuo Chuen, 31–43. San Diego: Academic Press.