Digital Currencies

An exploration into technology and money
Report to M. Bruno Le Maire, Minister of Economy
Jean-Pierre Landau with Alban Genais

June 2019
FOREWORD

This report has been prepared at the request of the Minister of Economy. It comprises two parts. The first part on “Crypto currencies” is a translation and adaptation of our report published in French in July 2018. The second part on “Public and private money in the digital world” is a development and extension of some preliminary conclusions and perspectives outlined in the July 2018 report.

Each part can be read separately.

Many people have contributed, through conversations and comments, to the content of this report. Our special gratitude goes to Philip Turner and Steven Saeger for their decisive contributions.
# Table of Contents

**EXECUTIVE SUMMARY** ............................................................................................................. 1  
**INTRODUCTION** ......................................................................................................................... 11  
**PART I: CRYPTO CURRENCIES** ............................................................................................... 13  
  I. Introduction ................................................................................................................................. 13  
  II. The Crypto Currency Ecosystem ............................................................................................ 14  
  III. The Fundamental Novelty of Crypto Currencies ..................................................................... 15  
  IV. The Problematic Economics of Crypto Currencies ................................................................. 28  
  V. Governance and Trust ................................................................................................................ 41  
  VI. The Regulation of Crypto Currencies ...................................................................................... 42  
**PART II: PRIVATE AND PUBLIC MONEY IN A DIGITAL WORLD** .......................................... 50  
  I. Digital Money and Payments .................................................................................................... 51  
  II. Policy Implications of Digitalization ......................................................................................... 62  
  III. New Private Currencies ......................................................................................................... 75  
**CONCLUSION** ............................................................................................................................. 83  
**REFERENCES** .............................................................................................................................. 84
This report is about technology and the future of money. Digitalization has changed everything in our lives: how we communicate, organize, interact, move, and trade. Increasingly, it is also changing how we pay, and potentially how we count, transfer and store value. In short, digitalization is changing money—certainly in its role as a medium of exchange and maybe as a store of value and unit of account as well.

Until recently, this transformation has been surprisingly slow. The internet has been around for more than thirty years, the smartphone is twelve years old, and electronic money (e-money) first appeared more than twenty years ago. Yet, digital money still represents only a small fraction of total money outstanding. That is now changing fast. Mobile technology and the internet are combining to produce a silent revolution in payments which together with the emergence of new forms of money has the potential to transform and disrupt financial intermediation more broadly.

This report examines those evolutions. It is composed of two parts that may be read separately. The first focuses on crypto currencies. The second looks more broadly at the digitalization of payments and money and the respective roles of public and private money in a digital environment.

In the midst of a fast and disruptive technological transformation, any assessment of the future is necessarily tentative. The report does not attempt to come to firm and specific conclusions. Rather, the objective is to explore possible paths this transformation could take and outline a research and policy agenda.

I. CRYPTO CURRENCIES

This report takes crypto currencies seriously. They are highly innovative and highly ambitious. They aim to transform money. At this point, however, they are far from fulfilling the ambitions of their creators. They may never do so in their current form. It looks impossible to run a fully decentralized monetary system efficiently and safely. However, other forms of digital currencies, combining innovations in different ways and based on different, more centralized, architectures, could prosper in the future.

The fundamental novelty of crypto currencies

Often presented as a “revolution,” crypto currencies can be more accurately described as an artful combination of three types of innovations: technological, monetary, and design. The precise mix is specific to each currency.

Crypto currencies make extensive use of ancient technologies that have been improved over time. They use encryption tools to securely transfer of messages and, most importantly, value in an open network. They are supported by Distributed Ledger Technology (DLT) in which secure registers are permanently synchronized between a large number of participants. Most function on a blockchain, a particular form of DLT where new entries are first bundled into “blocks” and then sequentially linked to each other, forming a chain. Because, each block incorporates a coded
summary of the entire preceding chain, the blockchain cannot be tampered with. It is immutable.

Crypto currencies are new monetary objects. They look similar to existing electronic money (or “e-money”). But they are different. They are private monies with no backing. They are not related to a bank account. They are not a claim on any natural or legal entity. They are denominated in specific units of account, unrelated to existing currencies. There is no historical precedent for this type of private money.

Most crypto currencies follow very strict rules of issuance with ceilings imposed on the total number of units (e.g., Bitcoin) or its growth rate (e.g., Ether). Others, such as Ripple are issued in a one-time allocation for a fixed number of units. There are differences in the allocation of newly created money units and the distribution of seignorage. For Bitcoin and Ether, seignorage is used to finance the functioning of the payment system. In other cases, seignorage is—partially or totally—appropriated by the creators or developers. This is less satisfactory as it opens the way to potential abuse and manipulation.

Most crypto currencies are decentralized. They are designed to function efficiently on an open network with no trust between participants. They dispense with any financial intermediary. Decentralization is attractive in theory but very challenging to implement in practice. A consensus must be found to validate payments between multiple actors with no time coordination and no mutual trust. It has been proved that such consensus is theoretically impossible (the so-called "Byzantine Generals theorem"). Bitcoin and similar protocols circumvent this problem by introducing economic incentives that push participants to converge spontaneously on an honest solution. This invention has proven robust and worked well over time. It may turn out to be the most important innovation associated with Bitcoin.

The problematic economics of crypto currencies

However, this achievement comes at a price. Bitcoin’s method for validating transactions, the so-called “proof of work,” forces participants to mobilize computing power and spend significant resources. It has been called “minting money with megawatts” because of Bitcoin's massive energy consumption and capital-intensive process. Contrary to its initial objectives, the production of Bitcoin has become increasingly concentrated, with “factories” of computing power located in a limited number of countries where electricity is cheap.

In contrast with existing payment systems, Bitcoin and Ether are not “scalable.” Because of the security constraints imposed on the system, they cannot easily absorb a growth in activity. This scalability problem is a major obstacle to the broad acceptance and use of crypto currencies. In fact, they are almost nonexistent as payment instruments. This handicap is structural. It does not result from technical limitations of the network. It comes from the impossibility to conciliate the three objectives of (1) security, (2) efficiency and (3) decentralization. Bitcoin and Ether sacrifice efficiency for the sake of security and decentralization. Other crypto currencies are based on different choices, often with more centralization to achieve speed. But the tradeoff seems unavoidable.
Today, crypto currencies are essentially promoted as stores of value. Because the supply is scarce, they are presented as the ultimate reserve asset, a sort of “digital gold”. However, even if abundance can erode value, scarcity is not sufficient to create it. There a must be some demand. With no present or expected usage value as means of payment, the demand for crypto currencies is fueled exclusively by its speculative component. The value can collapse at any time. Combined with a rigid supply, there is an intrinsic volatility in prices that also prevents crypto currencies’ use as a unit of account.

Despite all these handicaps, crypto currencies yield some significant benefits. They have made it much easier and cheaper to transfer small amounts of money between countries. They stimulate competition in cross-border retail payments, where inefficiencies are higher. It may not be a coincidence that a growing number of global initiatives to improve cross border payments have emerged in the last few years.

**Stable Coins**

Stable coins are a new category of virtual currencies that have recently gained attention. They are not strictly crypto currencies, despite using a digital token, and they have very different monetary underpinnings and issuance regimes. They come in three varieties:

- Some coins are backed one-for-one by an equivalent amount of official fiat currencies. In effect, they are different digital representations of fiat currencies or a new crypto version of e-money.

- Other are backed not by fiat currencies proper but by financial assets (e.g., securities) denominated in those currencies. The income from those securities is collected by the issuer as seignorage. This scheme involves some maturity and liquidity transformation and is similar in nature to a money market mutual fund. It also carries similar risks, including exposure to runs.

- Finally, some promoters of stable coins are working on projects where currency issuance would be regulated by a sophisticated algorithm. The objective would be to expand and contract the supply so as to maintain a stable price. While the idea is seductive, the implementation may be difficult. Ultimately, there is no alternative to holding real resources or financial assets denominated in official currencies as backing to support the value of a coin.

**Initial Coin Offerings**

Initial Coin Offerings (ICO) have appeared over the last three years as a byproduct of crypto currencies. Through ICOs, companies (most often startups) aim to raise funds by issuing digital tokens that are purchased with crypto currencies. The procedure is generally informal, with a simple document (a “White Paper”) describing the nature of the tokens being issued. ICO tokens are usually quoted on crypto currency exchanges shortly after they have been issued.
The tokens themselves come in different forms. It is customary to distinguish between (1) security tokens, that mimic equity shares, and (2) “utility tokens” that in principle confer a right of usage for future services. Utility tokens are often structured as special purpose payment instruments—or currencies—that can be used in the future to purchase services produced by the issuer.

After significant growth in 2017 and the first half of 2018, ICO issuance has fallen substantially since. This development closely follows the decline in the price of crypto currencies.

The regulation of crypto currencies

Regulators should give priority and urgency to implementing and strengthening international cooperation on anti-money laundering and combating the financing of terrorism in the crypto world. Apart from that, the report does not advocate any direct regulation of crypto currencies. At this stage, it appears neither necessary nor advisable. The risks posed by crypto currencies to financial stability are currently minimal and they can be allowed to develop in their own cyberspace. It is difficult for regulators to sort out the good from the bad in the middle of an innovation wave. In some cases, as with Bitcoin, the monetary and technological aspects of innovation are difficult to disentangle. It may be that legally defining and classifying those new objects would change economic incentives, impede innovation, or orient it towards regulatory avoidance.

However, the report strongly recommends that crypto currencies be kept separate from the “official” financial sector to avoid any contagion and any risk taking by retail or relatively uninformed investors. Regulators should prohibit or discourage banks from taking or financing exposures in crypto currencies. Asset management companies should not be authorized to create vehicles (such as exchange-traded funds (ETFs)) that would enable retail customers to invest in crypto currencies. Finally, regulators should prioritize reaching an international agreement on a minimum set of principles and rules applicable to crypto currency exchanges. Exchanges are the interface between crypto currency and the official financial system. They are also the “weak link” in the current crypto architecture, the places where criminal activities develop and where all “hacking” of crypto currencies takes place. In many cases, investors do not enjoy a basic degree of protection regarding the transparency of exchanges’ operations, the order book, or even the basic security of their holdings.

II. PUBLIC AND PRIVATE MONEY IN A DIGITAL WORLD

The second part of this report focuses on one key issue: the respective role of public and private money in a digitalized economy.

Today, private money, in the form of bank deposits, dominates as a medium of exchange. Public money, composed of cash and banks’ reserves at the Central Bank, provides the unit of account and the basis for legal tender. Crucially, the coincidence between the two functions—exchange and account—is guaranteed by the unconditional convertibility between the two types of money.
Technology could change that equilibrium in many ways. Mobile technology and the internet are combining to produce a new architecture of payments and the emergence of new forms of money. Together, they have the potential to disrupt financial intermediation and change the role of public money in our economies. The report looks at those evolutions, the policy questions they raise, and, finally the possible development of fully private “network” currencies.

**Tokens, networks, and platforms**

Technically, what is called "mobile money" is both an instrument—tokens stored on a mobile device—and an infrastructure—the network that transfers the information and the value. The current transformation involves both, in a symbiotic relationship, but they may be considered separately for analytical purposes.

*The tokenization of money*

Token money has always existed, albeit in physical form such as coins and banknotes. Today, it is possible to attach an identity to a digital representation of value that can be securely transferred. A new form of money is emerging. Digital tokens may turn out to be the true monetary innovation brought by technology.

The token form of money is specially adapted to transactions in a digital world. For the general public, a digital token stored on a mobile phone closely mimics the characteristics of cash. It can be securely exchanged on a peer-to-peer basis, with or without a financial intermediary. For corporates and financial institutions, “there is (now) a computer in the middle of each transaction.” Interactions between machines and algorithms will increasingly dominate business relations. Tokens offer the possibility to transfer value between computers in extremely short periods of time.

Importantly, from a user perspective, tokens can be complements or substitutes to a bank account. Tokens can simply mirror existing deposits, as in most wallet applications. Alternatively, in a pure e-money model, tokens are directly possessed by users on their mobile devices, with their phone number as sole identity. Tokenization, therefore, is compatible with a diversity of monetary architectures. In some of them, banks will keep direct relations with depositors; in others, money issuers will interpose themselves between banks and users.

*Networks and platforms*

Digitalization is also changing the shape of payment and money systems. It naturally favors the expansion of large networks and the structuring of economic activities around “platforms.”

The convergence between networks, platforms, and money is a dominant feature of the current transformation. It is increasingly apparent, especially in emerging economies where banking systems are less dominant or established.

Networks and money are closely linked. Network effects and externalities play an essential role in establishing and maintaining a currency. A currency supported by a digital network may be able to quickly achieve broad domestic and international
acceptance. Digital networks (whether social or e-commerce) are large and not technically bounded by national borders.

Money can also play an important role in the business model of platforms. Platforms are multi-sided markets or, in common parlance “ecosystems,” that aggregate a multiplicity of activities within which consumers, merchants, and service providers interact. The economic logic of platforms is to create and develop complementarities and links between those different activities. A shared (form of) currency strengthens those links; it keeps the platform growing and profitable.

The (potential) consequences are significant. Three are particularly emphasized in the report.

First, the financial system may become “payment centric.” In a platform / network architecture, the payment activity sits at the center of all interactions between users, merchants, and financial services providers. Customers enter the system through the payment platform. The payment functionality is what keeps the network valuable and growing. It dominates other activities. Payment providers enjoy an unparalleled access to data which they can use to develop other functions (e.g., credit scoring, lending, and asset management). Digitalization may therefore lead to an inversion in the current industrial organization of financial activities. At the moment, banks are the only point of contact with their borrowers and users. The preeminence of payments may challenge banks’ existing business models and reverse that implicit hierarchy. Other financial services, such as credit and asset management, could become de facto accessories to payments.

Second, on a different level, technology will push for a fragmentation of the monetary system.

A money network has an incentive and tendency to organize itself as a closed system. In some respects, such a network then becomes a currency area of a new kind: a digital currency area. It is not defined, as in the traditional literature on Optimum Currency Areas (OCA), by the commonality of macroeconomic shocks and the degree of factor mobility. It is based on digital interconnectedness. Because participants share the same form of money, payments inside the area are easier and trading frictions are lower than with outside. For people who use the same form of money, price transparency is greater, price discovery easier, and conversion to other payment instruments is less likely and sometimes technically impossible. This create an incentive to accumulate monetary balances in the forms of money used inside the network.

Third, such digital currency areas may not be circumscribed by territorial borders. Technology could serve as a powerful vehicle to internationalize some currencies as mediums of exchange. And symmetrically, some jurisdictions would be faced with more intense currency competition from foreign currencies through cross border payment networks. At the moment, most payment systems using digital money operate in national currencies even when the technology and the infrastructure are located abroad. However, in the future, the possibility of such “digital dollarization” should not be discarded.
Uniform currency and CBDC

Modern monetary systems rest on a subtle equilibrium. Authorities favor competition between different mediums of exchange. But they also want to preserve a “uniform currency.” They want multiple issuers, but one money. They want the different forms of money to be fully equivalent representations of the same unit of account. Maintaining that equivalence will become more challenging in a digital world.

Based on history, the report makes the case that full and unconditional convertibility at par between different forms of money is essential to a uniform currency. Effective convertibility cannot be taken for granted when technology changes and the forms of money diversify. There are two key requirements. First there must be convertibility between different private forms of money. Technically, the interoperability of systems and tokens may become a key issue. Second, and most important, there must be convertibility of all private monies into public money, issued by the Central Bank.

Today, cash is the only public money accessible to the general public. However, cash is vanishing in many countries and places, at least as a payment instrument and medium of exchange. The tendency toward cashless payments could accelerate as merchants and users interact to promote and use mobile payments in a mutually reinforcing feedback loop.

In a cashless society, bank deposits and e-money would not be convertible into cash, as there would nothing to convert them into. The general public would not have access to public money anymore. Without effective convertibility to public money, different forms of money would become imperfect substitutes, despite being denominated in the same unit of account. In effect, the monetary system would be transformed and behave more like the broader financial system where the creditworthiness of every single instrument is constantly re-assessed and priced. The likely result would be greater financial fragility, with the possibility of periodic runs on some forms of currencies if doubts emerge about their issuers’ solvency.

What would then happen to the unit of account is a matter of conjecture. There is no precedent in modern times for a situation where private money is the only one available to the public. It is generally assumed that social conventions and habits ensure the permanence of the unit of account. It is also assumed, however, that economic agents use the medium of exchange as the reference to set prices and denominate their contracts. It is therefore possible, though by no means certain, that new and diversified means of payments could progressively push economic agents to count, set prices, and contract in many different units.

In such scenarios, there is no doubt that sovereign authorities can assert their power and protect a currency’s role as the unit of account. They can decide which currency serves as legal tender and in which currency taxes have to be paid. They can impose the technical interoperability of systems. They can regulate e-money issuers to ensure full backing by Central Bank money if necessary. They can legally impose the acceptance of cash.

The key question is whether they can do those things without repressing technology and without limiting the free choice, by economic agents, of their instruments of
payment. They may want to find ways to relax this tradeoff. In addition to regulation, they can offer public money in a new form; adapted to technology and in line with the people’s preferences.

This is the main rationale for a Central Bank Digital Currency (CBDC): to maintain the availability of public money in a digital world.

There is currently an intense debate on the merits and dangers of CBDCs. It runs across two main dimensions. First, whether they would strengthen the transmission mechanism of monetary policy by allowing interest (including at negative rates), to be paid on the currency. Second, whether they would imperil financial stability by offering an attractive (riskless) substitute to bank deposits.

This report takes on a different line of argument. A CBDC would ensure that the general public keeps access to public money even when technology changes. It would maintain effective convertibility of private into public money. It would help to preserve the uniformity of the currency and its role as unit of account in a digitalized economy.

In addition, it could foster financial inclusion in places where mobile penetration is higher than banking intensity. In some countries, a CBDC may also provide protection against “digital dollarization,” i.e., increased currency competition from digital payment systems and currencies developed in foreign countries.

To meet those objectives and minimize its impact on financial stability, a CBDC should be designed as a complement, not a substitute, to bank deposits. It should be as close as possible to cash. It should be available in token form and not carry interest. Whether it should be anonymous is a fundamental societal choice on the nature of money. It goes beyond the scope of this report and would have to be properly debated.

Private network currencies

Finally, the report explores the possibility that private currencies could emerge, supported by a large network. Many projects are rumored to be under consideration. Some are “stable coins” denominated in existing currencies. For the purpose of this analysis, the report considers the most extreme hypothesis: a currency denominated in its own unit of account, therefore in direct competition to existing national monies.

While very speculative, several points can be made.

Private “network currencies” could emerge more easily today than in the past for three reasons.

First, they could rapidly gain broad acceptance if supported by large cross-border (social and commercial) networks that already connects tens or hundreds of millions of people.

Second, technology now makes it easier and less costly to switch from one currency to another. Switching costs are traditionally seen as a major obstacle to currency competition. But technology has helped lower these costs in a digital economy. There
are programs available on mobile devices that can be used to manage currency transformations. Existing and future applications should allow for easy and instant computation of relative prices and conversion of monetary balances from one currency to another as well as automatic arbitrage.

Third, technology may help to solve the problem of trust. All monies, public and private, face the same difficulty. People know that a currency issuer has an incentive over time to maximize its revenue by creating more money than is compatible with price stability. That perspective undermines trust in the currency and may lead to immediate loss of value. Modern governments have found ways to deal with this "dynamic consistency" problem through institutional arrangements (e.g., independent Central Banks). Private issuers do not have the same option. For that reason, private currencies are inherently fragile. However, if a private issuer could credibly submit itself to a rule, trust could be reestablished. The rule would be transparent, implemented by a protocol, with a very strict governance framework that would strictly limit or prohibit changes and human intervention. Subordinating monetary policy to a rule is an old remedy to the problem of dynamic inconsistency. Technology can give it a new relevance. With the development of artificial intelligence, it is conceivable that in the future, algorithms will be devised that reproduce, for a private currency, the complex process leading to monetary policy decisions.

Based on a large network, a private currency could therefore conceivably establish itself as a reliable medium of exchange. However, if successful, it may not avoid becoming also a store of value—especially if it is accessible to citizens of countries where the monetary regime is fragile.

In that situation, the issuer will have to decide whether to take responsibility for maintaining financial stability inside the system and for stabilizing the currency value—its exchange rate—vis à vis official currencies. The conventional wisdom would advocate ambiguity. The issuer should not take any commitment as to whether it will support the currency. But it could not either formally exclude any intervention forever. Uncertainty and ambiguity may be destabilizing, which could have a broader impact on the network’s value to its customers.

This raises the question of the currency’s backing. What resources would be available to a private issuer to support its currency? It could be argued that the largest corporate entities have balance sheets that are sufficiently strong to provide the necessary backing. However, the issuer would have to determine whether it is beneficial to commit, explicitly or implicitly, part of its balance sheet for the purpose of backing the currency. To do so would have implications for the financial strength of the company and perceptions of the firm’s creditworthiness among outside investors.

Overall, the business case might be very complex. Running a monetary balance sheet is very different from running an "ordinary" corporate balance sheet. The issuer of a private currency would expose itself to a very different set of risks and volatility factors than those faced by private corporations. Runs do not occur on industrial or service companies; they do, however, affect entities that issue liabilities that have a monetary character.
These constraints do not necessarily make the issuance of a private currency impossible, but they make it very demanding.

III. CONCLUSION

Overall, the digitalization of money creates the possibility of increased currency competition. Whether such competition materializes will depend on regulation and, more generally, the interaction between public policies, private attitudes, and technology.

Currency competition could develop across three dimensions:

- Between private mediums of exchange. This is already happening and may change the equilibrium between private and public forms of money.

- Between private and public units of accounts. This evolution is more uncertain and speculative but cannot be ruled out.

- Between different national currencies, due to the cross-border nature of networks. Not all countries are equally affected by current technological changes or equally exposed to such competition. Digitalization may serve as a vehicle for the internationalization of some currencies. It may help them to quickly gain international acceptance and status. And, symmetrically, other countries may be exposed to new forms of “digital dollarization,” depending on their monetary regimes, the openness of their capital account, and their regulation of payments and the internet.

Over time, as it transforms domestic monetary systems, technology may reshape international monetary relations and the international monetary system as well.
INTRODUCTION

...the internet is going to be one of the major forces for reducing the role of government. The one thing that's missing but that will soon be developed is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A, the way in which I can take a $20 bill and hand it over to you and there's no record of where it came from and you may get that without knowing who I am. That kind of thing will develop on the Internet and that will make it even easier for people to use the internet. Of course, it has a negative side. It means that the gangsters, the people who are engaged in illegal transactions will also have an easier way to carry on their business.

Milton Friedman (1999)

How will value be stored and transferred over the internet? With great prescience, Friedman foresaw that technology would create new needs and fuel new aspirations. He guessed that as people routinely exchange messages and information instantly and bilaterally, they would aspire to instant, peer-to-peer, and potentially anonymous ways of transferring value on the internet, including across borders. The smartphone has reinforced the ability and aspirations of individuals to manage their payments and their wealth directly and autonomously.

In response, existing payment systems are evolving and adapting. For the end-users, electronic money is becoming more like physical cash, with progress being made in contactless payments and the increasing use of smartphones as payment devices. Fast payments and instant payment schemes are being developed in many countries. They will be available at any time in the day and transfer funds to beneficiaries in a few seconds for a very low cost. It can be argued that these developing aspirations for high speed, peer-to-peer payments will be met fully with existing forms of money.

At the same time, however, it is also plausible that technology will provoke and necessitate more radical changes in payments and money. Digitalization has changed everything in our lives, including how we communicate, organize, interact, move, and trade. Increasingly, it is also changing how we pay and, potentially, how we count, transfer, and store value. In short, digitalization may be changing money—certainly in its role as a medium of exchange and maybe as a store of value and unit of account as well.

Until recently, this transformation has been surprisingly slow. The internet has been around for more thirty years, the smartphone is twelve years old, and electronic money (e-money) first appeared more than twenty years ago. Digital money still represents only a small fraction of total money outstanding. But that is now changing fast. Many innovations that appeared over the last several decades are suddenly being combined to produce a silent revolution in payments and money.

This report examines those evolutions. It is composed of two parts that can be read separately. The first focuses on crypto currencies. The second looks more broadly at
the digitalization of payments and money and the respective roles of public and private money in a digital environment.

Obviously, in the midst of a fast and disruptive technological transformation, any assessment of the future is necessarily tentative. There is no attempt to come to firm and specific conclusions. Rather, the objective is to explore possible paths this transformation could take and outline a research and policy agenda.
PART I: CRYPTO CURRENCIES

I. INTRODUCTION

As of May 2019, there are more than 2500 crypto currencies in circulation.\(^1\) During the first five months of 2019, their total market value has oscillated between 126 USD billion and 264 USD billion after reaching a peak of 830 USD billion in January 2018.\(^2\) By comparison, the global market capitalization of equities stands at 65 USD trillion, the global value of gold in private hands is around 8 trillion USD, and monetary aggregates for G20 countries amounts to 26.5 trillion USD.\(^3\)

As those numbers make clear, crypto currencies, in aggregate, do not currently play a significant role in the world economy and financial markets. Only three of them have a total value above 1 billion USD. At this stage, they do not pose any significant risk to the financial system. They currently attract attention primarily because of their design and ambition, as well as the bubble that formed in crypto currency prices during the course of 2017 and early 2018.

There is no commonly accepted definition of crypto currencies. Clearly, they have no material existence, which differentiates them from cash. However, most currencies today are also immaterial. Going one step further, one may see that all immaterial money that is used today exists as a deposit in a bank account. That is not the case for crypto currencies, and for this reason, they may be called “virtual.” Technically, they are digital “tokens,” a form of money that exists as an inscription of value on an electronic file. To own and transfer them, one has to use cryptographic techniques, hence their nomenclature. The graph below presents a summary classification of different types of money.\(^6\)

---


\(^6\) For a more precise and detailed taxonomy, see the “money flower” developed in M. Bech, and R. Garratt (2017).
Crypto currencies show a great diversity in design and functioning. Some are truly decentralized in their architecture and functioning, while others are not. Some are a simple mirror of existing bank accounts – the equivalent of e–money in cryptographic form. Others are essentially accessories to a messaging and payment system (e.g., Ripple, Stellar).

This report will primarily concentrate on issues related to the two most important crypto currencies, Bitcoin and Ether, which share many design and technical characteristics. As necessary, however, I will also discuss and analyze other crypto currencies such as so-called stable coins.

II. THE CRYPTO CURRENCY ECOSYSTEM

Crypto currencies do not exist in a vacuum. They prosper inside an open network of participants on the internet. Some participants are more active than others and take special responsibilities (and receive special rewards) to make the system work. In the case of Bitcoin, so-called “miners” solve the cryptographic puzzles necessary to add new transactions to the blockchain and receive new bitcoins as compensation.

Auxiliary activities such as wallet providers and exchanges are also part of the broader crypto currency ecosystem.

A crypto currency wallet is a software program used to store, send, and receive cryptocurrencies safely. Wallets also typically have an interface enabling users to track their balance in crypto currencies and automate some functions. A majority of wallet providers offer additional features, such as an integrated currency exchange service that lets users conveniently exchange crypto currencies from the same wallet interface.
Crypto currencies interact with the “official” financial system through so-called exchanges. These exchanges may have a physical presence or exist purely online. They have at least three functions (and may aggregate other activities). First, they are payment systems that can execute transfers of crypto currencies between addresses on the blockchain. Second, they are trading platforms for transactions between official and crypto currencies or between crypto currencies themselves. Finally, they serve as custodians by keeping crypto currencies in accounts for their customers and keeping and storing private cryptographic keys.

Other actors also play a significant role in the crypto currency ecosystem: merchants, payment facilitators (who allow merchants, mainly in e-commerce, to accept virtual currencies as a payment method), software developers (who develop user interfaces for trading and storing crypto currencies), and computer hardware manufacturers (who build equipment specifically for mining). From a financial investment perspective, there are also providers of investment vehicles and brokers that facilitate investment in start-up companies and design specific financial products. Another type of actor that has appeared are called “tumblers,” who provide services to increase the anonymity of the payer by making it more difficult to find out where the virtual currency transaction came from.

### III. THE FUNDAMENTAL NOVELTY OF CRYPTO CURRENCIES

Crypto currencies and the blockchain are commonly labelled as “revolutionary” and are sometimes described as a fundamental breakthrough or a one-time disruptive jump in technology. The reality is different, however. It would be more accurate to see crypto currencies as a bundle of multiple existing technologies, some of which are actually quite ancient. These technologies have been artfully combined into what is a truly audacious, and potentially problematic, monetary experiment.

The comedian John Oliver has described crypto currencies as “everything you don't understand about money combined with everything you don't understand about computers.” Indeed, what makes crypto currencies interesting and intriguing is the aggregation of three different types of innovations: (1) technological innovation based on novel uses of previously existing cryptographic tools and ledgers; (2) monetary innovation involving the creation of fully private digital currencies; and (3) design innovation enabling the operation of fully decentralized payment and monetary systems. The novelty of crypto currencies arises from this grouping of different ideas and advances, in proportions that may vary for different crypto currencies.

#### Technological innovation

Most existing crypto currencies rely on three major technological components:

---

• First, they make extensive use of encryption tools, such as public-private keys, electronic signatures, and hash functions. These are technologies that date back two or three decades but have been constantly improved since then. They now allow someone to securely transfer messages and, most importantly, value, in an open network.

• Second, crypto currencies are based on Distributed Ledger Technology (DLT). Distributed Ledgers are secure registers that are permanently synchronized between a great number participants. In effect, the same database is replicated in real time across a multiplicity of copies. Different architectures are possible depending on who has permission to read and write on the ledgers. A DLT naturally supports a decentralized system and is more resilient to cyber-attacks than a single register. That makes DLTs an attractive proposition for crypto currency developers given their sensitivity to cyber risks.

• Finally, the blockchain is a particular form of DLT where new entries are first aggregated into “blocks” (several entries at a time). These blocks are then sequentially linked to each other, forming a chain. Each new block of information is attached to a pre-existing blockchain through a validation process. An example of how this process works is illustrated in the figure.

---

**Figure 2**

Blockchain

---

Public-private key pairs work as a way to encrypt and decrypt data for a specific entity or individual. Simply put, data encrypted with one’s public key can only be decrypted by that person’s private key. Electronic signatures and hash functions are two types of cryptographic algorithms also used to encrypt data. A hash function takes in a string input, and outputs a unique fixed-size output that can be used for data authentication. An electronic signature acts as a digital proxy for a handwritten signature, in that it is uniquely identifiable, unreplicable and non-transferrable. A. Nananyan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016).
The link between the blocks is cryptographic. Each block incorporates a coded summary of the entire preceding chain. As a consequence, the chain cannot be retroactively altered without such changes being immediately visible to all participants. The existing blockchain is thus “immutable.” This immutability is a great advantage when there is a need for full integrity and transparency in record keeping. It can, however, also be a source of difficulties. When the blockchain is used to support a payment system, immutability means that errors cannot be corrected and fraudulent transactions cannot be rectified without tampering with the protocol.\footnote{11}

How can a blockchain be used to operate a payment system? To understand this, one has to abstract from the vision of a monetary system as a set of accounts, with deposits, balances, and money transferred between those accounts. There are no such things for crypto currencies. There are only messages. Those messages, once validated, are instructions to move money from one address to another. There is no single entity that keeps track of the balances. The protocol just checks that the money is there in the address from where it has to be moved. The blockchain keeps the whole history of the transfer messages. Holding bitcoin means that previous messages have brought sufficient amounts into one’s address to be able to operate transfers. One drawback, of course, is that keeping record of the whole history of transactions simultaneously on thousands of computers mobilizes enormous storage capacity.\footnote{12}

Finally, for more recently launched crypto currencies, including most prominently Ether, the same protocol that governs the payment system can also be used to offer other functionalities. Amongst these are so-called “smart contracts.” These are computer programs that automatically implement the terms of an agreement between parties when certain conditions are met. One example is that of a car lease: upon a missed payment, the car would automatically lock and control would return to the lender. In finance, smart contracts could be used to implement repo agreements by moving collateral and operating margin calls. Since execution of a smart contract does not involve a decision or an action by a human, it may be faster and safer and should minimize the number of mistakes. Although frequently associated with the blockchain in public debate and articles, smart contracts can be implemented in different infrastructures, including centralized ledgers.\footnote{13}

\textbf{Monetary innovation}

With the exception of cash, which represents only about 10% of the total money supply,\footnote{14} all money today is “digital.” It has no intrinsic value and exists only in electronic form. Payments are made by electronic transfers using different

\footnote{11} In contrast with other means of payment, such as credit cards, where fraudulent uses can be nullified ex post.

\footnote{12} Bank for International Settlements (“BIS”) (2018A).

\footnote{13} J. Gans and H. Halaburda (2013).

\footnote{14} Representing less than 10% of total monetary mass (10% in the Euro zone).
instruments: credit transfers, debit and credit cards, and, increasingly, applications on mobile phones.

Crypto currencies appear to be no different in this regard. The same type of instruments can also be used to move crypto currencies around; in particular, most payments in crypto currencies are made through mobile phone and QR code identification. For users, crypto currencies can thus look like a new category of e-money.

While there may seem to be a continuum between the different categories of electronic money, this impression is misleading. Crypto currencies are fundamentally different from all existing bank money and e-money. They are truly new monetary objects. To grasp their novelty, it is useful to briefly describe and characterize the existing forms of money.

**Bank money**

In modern economies, money held by the general public takes the form of bank deposits. Bank deposits are money, which banks create by making new loans. This “bank money” has several notable characteristics:

- Holding and using money requires a bank account.

- Any monetary transaction is a movement between bank accounts. It is identifiable and traceable and therefore can be monitored and regulated.

- Money is a legal claim on an identifiable entity: the bank. It is a liability of the bank. A bank deposit gives the holder legal rights on the bank, and an (indirect) claim on its assets.

- Bank customers have the right to convert their deposit into banknotes, which are legal tender. The Central Bank issues the currency serving as a “base” for the system, giving it its legal status.

- Bank money is a form of “private” money. It is therefore vulnerable to a loss of confidence in the issuing bank.

- Bank money nonetheless benefits in many ways from public backing through deposit insurance and/or access to Central Bank refinancing.

**E-money**

Most of those attributes extend to what is commonly called e-money. E-money, which often takes the form of money on prepaid cards or stored on mobile phones, is actually a representation of bank money. The outstanding amounts of e-money are covered by existing bank accounts, so that if a provider were to fail, the user could

---

15 With the exception of deposit insurance.
still recover the balance in their accounts. E-money, in its current forms, is simply a technology to access and move around money deposited in bank accounts. As such, e-money is not a new form of money, but is instead one of the modern forms that bank money takes.

In some e-money systems, holders are not (and cannot be) required to have their own personal bank account. Their banking identity boils down to their phone number. The e-money issuers, through their own bank accounts, interpose themselves between the banks and the consumers. This is a powerful instrument of financial inclusion, as consumers that previously could not access the formal financial system are able to do so. It is not surprising that these innovations are developing particularly in emerging countries with low banking intensity. But, whatever the technical architecture, a mobile phone with e-money always reflects a bank account.

**Crypto currencies**

Crypto currencies are fundamentally different than bank money or e-money. Like bank money, they have no intrinsic value, are privately created, and are totally dematerialized and digital. But each of their other characteristics are the opposite of those of existing currencies:

- They are purely private currencies, are not legal tender, and are not convertible at par\(^\text{18}\) in any legal currency.
- They are created and circulate independently of any bank; they are not connected to any bank account.
- They do not represent a claim on any person or legal entity. They are “outside money,” because they are created outside the banking system.\(^\text{19}\)
- They have no physical, financial, or legal backing of any kind.
- They are denominated in specific units of account, unrelated to existing currencies.

Beyond the apparent similarities with electronic currencies, there is no precedent for the type of money that cryptocurrencies represent. The forms and attributes of

\(^{16}\) Electronic money can be defined as “value stored electronically in a device such as a chip card…or a hard drive in a personal computer.” Committee on Payment and Settlement Systems (“CPSS”) (2002), p. 44. According to the GSM Association, the trade body that represents mobile money operators globally, “the total value of e-money is mirrored in (a) bank account(s), such that even if the provider…were to fail, users could recover 100% of the value stored in their accounts.” GSMA (2010), p. 2.

\(^{17}\) Some implications related to the role of e-money issuers are discussed in Part II of this paper.

\(^{18}\) Crypto currencies are convertible to legal currencies, but not at par.

\(^{19}\) It is common in economic analysis to distinguish between inside and outside money. Inside money is created inside the financial system by banks extending credit and is thus a claim on a financial intermediary. By contrast, “outside” money is not a claim on any private financial institution, and includes fiat money that the Central Bank issues.
money have constantly evolved throughout history, with changes in technology, institutions, and social conventions. However, a private money with no backing has never existed. All currencies that have been developed and used in market economies for the last three hundred years possessed one or more of the following attributes:

- They had an intrinsic value (e.g., coins and precious metal coins);
- They were a claim on a counterparty holding a physical or financial asset that was used to provide backing and value the currency. This is the case of the gold standard. This was also the case, in a different form, of banknotes issued in the United States by private banks during the free banking period, and whose value (which was variable) was secured by the assets and capital of the issuing banks; or,
- They had public support, based either on their status as legal tender or on refinancing by the Central Bank.

Crypto currencies have none of those attributes, but instead constitute a pure monetary experiment.

**Issuance regimes**

Economically, a currency is mainly defined by its issuance regime. From that perspective, crypto currencies fall into two main categories:

- Rules-Based Governing Protocols: Most existing crypto currencies follow very simple rules that are automatically implemented by their governing protocols. Many introduce a ceiling either in the absolute number of currency units issued or in the growth rate of units outstanding. For Bitcoin, the total number of units that will ever be issued is 21 million, a limit that will be reached in 2040. In the interim, the supply of bitcoin follows an asymptotic path, with the annual growth rate progressively reduced to zero. For Ether, the number of units issued is set to grow at a constant rhythm of 3% a year.

- One-Time Allocation: Other currencies (such as Ripple) are issued in a one-time allocation of a fixed number of units.

These are clearly very rigorous issuance regimes. The limits embedded in the governing algorithms protect the users against any future temptation to over issue the currency—a problem that has plagued many private monies in the past. Crypto currency promoters generally argue that such limits guarantee the future value of the currencies and ensure their stability. Whether a rationed supply is sufficient to preserve or increase the value of a currency is debatable, however, and will be discussed later on in this report.

A completely rigid supply of a crypto currency entails both benefits and costs. Should some crypto currencies gain broad acceptance and be used as a unit of account,

---

20 This period lasted between 1837 and 1864. D. Sanches (2016).
their issuance regime would impart a deflationary bias to the economy. A continuous decrease in the overall price level would be needed to accommodate growing transaction demand with a fully fixed supply. In turn, the expectation of future decreases in the overall price level (an increase in the value of the crypto currency) may encourage hoarding and prevent the currency from establishing itself as a medium of exchange in the first place. Finally, a completely rigid money supply creates volatility in the relative price (the “exchange rate”) with other currencies, crypto or otherwise.

**Seignorage**

Crypto currencies can also differ from one another on another key feature: the allocation of newly created money units and the related distribution of seignorage. Seignorage is the income derived from money issuance because the economic cost of producing a dollar bill or other monetary representation is much lower than its nominal value. Issuing money therefore is generally very profitable. Seignorage on public currencies is a significant source of revenue for Central Banks and, by extension, governments. The same is true for private currencies. The ability to earn seignorage sometimes appears to be an essential incentive for creating private crypto currencies. However, there are variety of modalities for how crypto currencies earn seignorage.

- Seignorage can be used to finance the functioning of the payment system. This is the case for bitcoin and ether. All newly-issued bitcoins and ethers are allocated to “miners,” who are the participants that take the responsibility for validating and executing the transactions. The attribution of seignorage in those crypto currencies is both logical from an economic perspective and fully transparent.

- By contrast, there are also cases where seignorage is de facto either partially or totally appropriated by the creators or developers of the crypto currency. For instance, for some of those crypto currencies that are issued in a single operation, part of the proceeds often are allocated to a “reserve” that is managed by the founders at their discretion. It is natural to expect that in this situation, the issuer will try and maximize its profits by releasing the reserve when the currency appreciates, thus “diluting” the other holders. The business model may consist in letting the crypto currency gain acceptance and value (through usage) and then “monetize” the reserve by conversion into other (official) currencies at the optimal moment. If the issuers retain discretionary power over those operations, they de facto control the value and price of the currency at any moment in time. There is no guarantee for other holders that stability objectives will prevail and that their interests will be taken into account. This uncertainty affects many crypto-currencies, and has the effect of undermining their viability and potentially compromising their integrity.

---


22 The crypto currency Ripple was issued in one allocation of 100 billion units when it was first introduced. The founders kept around 20 billion and a further 60 billion were placed into a reserve. After users expressed concerns were, Ripple agreed to put most of the reserve (55 billion units) into a
**Stable coins**

Stable coins are a new category of virtual currencies that have recently gained attention. Their issuance regimes are different. The main purpose is to ensure the stability of their value (or price) against official currencies. Stable coins currently come with three possible different designs, with different levels of intrinsic risk and likely long-term viability.

- Some coins are fully backed—one for one—by an equivalent amount of official fiat currencies. In effect, they are different (digital) representations of fiat currencies. Provided that the backing mechanism is robust (with official currencies effectively held and accessible to back the full amount of the stable coin outstanding) and the governance is transparent and accepted as appropriate by users, the value of those coins should be fully guaranteed. These coins can be considered to be a new (crypto) version of e-money. They may fulfil important functions by allowing official currencies to be used—and traded—in a digital form without need of a bank account. In some cases, the crypto currency can be designed as a “basket” of existing fiat currencies (duly backed by a mirror basket), thus allowing some existing (or new) unit of accounts to be effectively used as digital means of payments or stores of value.

- As a variant of the previous scheme, stable coins can be backed not by fiat currencies proper but by financial assets such as securities denominated in those currencies. The income from those securities is collected by the issuer as seignorage. This type of scheme involves some maturity and liquidity transformation. As such, it is similar to a money market (or mutual) fund and carries similar risks, including potential exposure to runs.

- Finally, some promoters of stable coins are working on projects where currency issuance would be regulated by a sophisticated algorithm. The objective would be to expand and contract the supply so as to maintain a stable price of the coin towards one of the major international currencies (its “exchange rate”). While the idea is seductive, the implementation may be problematic. While it is technically feasible to devise an algorithm that instantly adjusts the notional quantity of money when the price moves away from a defined objective, it is doubtful that this can be achieved without effective backing. The issuer can certainly increase the quantity of money if needed

---

23 This may not be always the case. Some “stable” crypto currencies such as Tether are issued and managed by a platform that also trades other currencies. Due to opacity regarding the dollars and accounts backing Tether, many rumors have undermined its standing and value. P. Tan (2018).

24 JP Morgan recently announced the launching of a prototype of JPM Coin, a token managed on a blockchain to help customers expedite money transfers between accounts (Reuters (2019)). In several countries, banks have considered using similar coins to support real time settlement in Central Bank money. J. Barrdear and M. Kumhof (2016).

25 See, for example, Saga, which was created in March 2018 and mirrors IMF Special Drawing Rights (SDRs). Saga Foundation (2018).
when demand is higher. However, the reverse is more difficult, as there is no easy way for a private issuer to engineer a contraction in the quantity of money when demand falls. Promoters of Basecoin have argued that they can mimic Central Banks and have the algorithms perform “open market” operations by purchasing coins in exchange for bonds. However, when Central Banks sell Government bonds, those bonds have an intrinsic value and are backed by future tax revenues. In this case, the “bonds” would simply be claims on the same stable coins whose demand is supposed to be falling at the same time. It is therefore questionable whether there would be demand for the bonds themselves and thus it is likely the mechanism would not work. Ultimately, there would appear to be no alternative to selling real resources or financial assets denominated in official currencies held as backing reserves.  

**Decentralization**

In all contemporary economies, monetary systems are centralized, with banks and Central Banks sitting at the center. These institutions are entrusted with the responsibility to “keep the records” and execute money transfers. The integrity of these payments depends on the trust placed in those agents, reinforced by legal guarantees and public supervision. Only banknotes do not depend on a trusted intermediary to be exchanged.

Crypto currencies are different. Their ambition is to function efficiently in the absence of any trust between participants and to dispense with any intermediary. In other words, they want to be a decentralized monetary system. A strong libertarian streak and distrust for existing institutions underpin this desire for decentralization. A decentralized system is also less vulnerable and more robust than a centralized one, as it cannot be paralyzed by an attack on one single unit.

**The problem of consensus**

In theory, decentralization has a number of attractive characteristics, but it also poses challenges. How can money be securely transferred inside a network where all participants are anonymous, where they can enter and exit freely, and must nevertheless come to an agreement on who owns what? Specifically, a decentralized system must meet several criteria:

- Decisions and transactions must be “honest.” For banknotes, honesty means they are not counterfeited. This is why significant resources are deployed by Governments to prevent fraud. For digital tokens, ensuring honesty is more difficult. Electronic files are much cheaper to create and duplicate than coins and notes. As a representation of value, they can easily be sent simultaneously to several recipients, a practice known as “double spending.” Double spending is unlikely when a central intermediary sits at the center of the system and can validate transactions or parties’ balances. In a

decentralized system, there must be a process to validate transactions and prevent double spending.

- A participant cannot be able to subvert the system through the decision-making process. One of the challenges of reaching consensus in a decentralized, digital network is that the usual ways of making decisions are not available. Voting, for instance, is not practicable when participants only exist as anonymous addresses. Because, there is no permanent and verifiable set of identities, the system can easily be rigged. As a result, it is possible for one participant to create multiple addresses and take control of the network, subverting the decision mechanism. This is called a “Sybil attack.”

- Finally, there must be a process for reaching consensus if conflicts arise due to asynchronous timing issues. The delays for message transmission are small, but not zero. That gives rise to a latency problem: not all participants have the same information at the same time. As a result, different parts of the network can honestly have different representations of its state and honestly come to different decisions when validating transactions. Specifically, different blockchains with different last blocks can exist simultaneously because each was validated in parallel in different parts of the network. There must be processes for determining which blockchain should be the “official” version going forward, with the others becoming “orphans.”

Overall, finding a consensus would be easy if all participants could come together to evaluate transactions simultaneously. It would also be easy if only one actor was delegated with this responsibility. But the combination of a network with variable configuration and an asynchronous process makes reaching consensus extremely complicated.

The theoretical impossibility of consensus

The problem of achieving consensus under these circumstances is known in cryptography as the “Byzantine Generals” problem, an allegory treated theoretically in a 1982 article:

“We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide...

28 Voting is nonetheless possible in certain circumstances, such as when the system is “permissioned” inside a private blockchain.
30 The temporary coexistence of several blockchains is most likely to occur when the delay between two blocks is short and notice of the validation of the last transaction has not had time to spread through the network. This is evident with ether, which has much shorter delays in validating transactions compared to bitcoin (a few seconds against 10 minutes on average), which results in more orphan blocks, called “uncles” in the language of ether users.
31 F. Velde (2013).
upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that A. All loyal generals decide upon the same plan of action .... [and] B. A small number of traitors cannot cause the loyal generals to adopt a bad plan."

"The Byzantine Generals Problem seems deceptively simple. Its difficulty is indicated by the surprising fact that if the generals can send only oral messages, then no solution will work unless more than two-thirds of the generals are loyal. In particular, with only three generals, no solution can work in the presence of a single traitor. An oral message is one whose contents are completely under the control of the sender, so a traitorous sender can transmit any possible message. Such a message corresponds to the type of message that computers normally send to one another." 33

So, without any other precautions, if one third of the "generals" in the network are failing to provide valid information, whether for technical or deliberate reasons, the system’s ability to reach consensus can be prevented or subverted. Honest consensus is impossible under these circumstances.

Reflecting this problem, developers often characterize network failures that may result from a diversity of causes, such as technical dysfunction, latency, or malfeasance, as "byzantine faults." In these systems, there will always be uncertainty as to the possible existence or origin of failures. There are no restrictions on how faulty actors might act; they may be actively malicious, trying to subvert agreement for the other participants in the system. Systems with the strongest safety properties assume that the actors in the system might be "Byzantine." Totally decentralized monetary systems must adopt such a stance to ensure safety within a payment system.

With varying technical assumptions, it has been shown that, even if all participants are honest, if latency on the network is indeterminate, even the slightest isolated technical failure is enough to prevent consensus from being reached. 35 Given these constraints, the general problem of consensus in a distributed system is impossible to solve. Another solution is required.

34 A. Tran (2017).
35 M. Fischer, N. Lynch, and M. Paterson (1985) ("In this paper, we show the surprising result that no completely asynchronous consensus protocol can tolerate even a single unannounced process death. We do not consider Byzantine failures, and we assume that the message system is reliable—it delivers all messages correctly and exactly once. Nevertheless, even with these assumptions, the stopping of a single process at an inopportune time can cause any distributed commit protocol to fail to reach agreement.").
**The Bitcoin solution**

Bitcoin and similar protocols circumvent the Byzantine General theorem through an ingenious solution to the problem of reaching consensus on a decentralized network. The idea is to introduce economic incentives which push participants to converge spontaneously on an honest solution. This protocol has proven robust over time and worked well and may turn out to be the most important innovation associated with Bitcoin. 36

The method Bitcoin created to reach consensus can be best described as a “rallying round.” Since no consensus decision will be reached given the characteristics of the decentralized system, the protocol must push participants to voluntarily agree on a solution—a list of transactions imbedded into a blockchain—that all accept. Because it is voluntary, there must be incentives to encourage agreement. In effect, the process is a “game” where participants—the miners—compete on an ongoing basis to build the longest possible blockchain accepted by others, and, if successful, receive a reward.

Each round of the “game” takes on average 10 minutes on Bitcoin (15 seconds on Ether) and can be described in several steps. All are automatically driven by algorithms inserted in the protocol or in participants’ wallets:

- First, those participants who want to make payments publicize the terms of their transaction on the network.
- Second, miners aggregate those transactions into blocks and propose those blocks for validation to other participants. Once a block is validated, it is added to the blockchain.

Mining is voluntary. In theory at least, the population of miners competing to add the transaction to the blockchain constantly varies with entries and exits.

For payments to be effective and safe, it is essential that this rallying round converges on a unique solution. It may not be easy. On a large network, there is some “latency”: messages take time to be transmitted. It will therefore happen regularly that several groups of miners, working independently, end up developing

![Figure 3: Blockchain Fork](image-url)

The protocol creates incentives to rally to the longer chain. If this happens, the shorter chain is “orphaned.”

36 While the Bitcoin protocol is robust in practice and has arrived at a solution, there is no theoretical proof that the process will converge on such an honest solution. A. Nananyan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016).
different and parallel blockchains. Such a situation is called a “fork.”

Forks may happen and last for some time. They should not be allowed to persist for too long, however, because they create uncertainty. During a fork, nobody knows exactly which transactions are valid. The protocol must ensure that any fork disappears quickly and only one chain subsists. This is where economic incentives matter.

**Proof of work**

The Bitcoin protocol functions on the following rules that define “proof of work”:

- At any moment of time the longest chain is the valid one. Suppose a long chain emerges in the network by random. Suppose further that some miners are working on a shorter chain. If they want this chain to survive, they must catch up and overtake the longest one, which means they quickly must validate several blocks in a row.

- But the protocol makes this endeavour extremely costly. To validate a block, miners must first spend significant resources. Those resources are lost if they do not succeed.

- However, if they do succeed, they get a reward. That reward must be given anonymously, which makes it impossible to use a bank. When a miner gets a block validated by the network, he/she is rewarded by the attribution of newly issued bitcoins.\(^\text{37}\) A clever idea in the Bitcoin protocol thus is to use seignorage to finance the functioning of the system. Because it depends on currency creation inside the system, the Bitcoin method of consensus cannot easily be transposed to other decentralized systems with no money creation.

- It is extremely risky for miners on the shorter chain to try and catch up with a longer chain, especially if they are behind by several blocks. The costs are significant and the reward uncertain. If a miner wants to make money and reap rewards, it is more rational to abandon the shorter chain, accept the longest, and then try to get transactions validated in subsequent blocks on that chain. If all miners behave rationally and follow their economic incentives, the process progressively converges on a single blockchain after a fork. But it may take some time.

How does “proof of work” manage to force miners to spend resources? In order to validate each block, miners must compete to be the first to solve a difficult cryptographic puzzle. The puzzle has several characteristics:

- The solution is very easy and costless to verify; once a miner has circulated its results on the network, all participants can instantly check that it is correct.

\(^{37}\) Each block proposed for validation includes the creation of bitcoin that are sent to the miner’s address. Once the block is validated, the reward is effective.
• The problem is very difficult and can only be solved through brute force, i.e., by trying successively a very large number of possibilities\(^{38}\). The key determinant of success in this competition is the amount of computing power that is used. To win, miners must be prepared to spend significant resources in computing time and electricity.

• The game is probabilistic. Over several rounds (several blocks), the probability of a miner succeeding (being the first to find the solution, validate a block, and pocket the reward) is roughly proportional to its share in the total computing power available on the network (the hash power in Bitcoin’s parlance).

IV. THE PROBLEMATIC ECONOMICS OF CRYPTO CURRENCIES

Proof of work has been very successful in securing transactions but also very problematic from an economic perspective. There are five major challenges:

1. Payments are settled with delays. Merchants who are paid in bitcoins, for instance, will wait to deliver their goods until they are certain that the block that includes their payments will not become “orphaned.” An orphan block is one that ultimately is discarded because it was in a chain that has been abandoned. In practice, goods paid in bitcoin are delivered online about one hour after having being paid. Merchants wait for approximately six blocks to be validated behind the one that contained their payment to be sure it will not become an orphan.

2. The system is plagued with inefficiencies. Significant resources are spent to validate orphan blocks, for no result. In addition, because they compete through sheer computing power, miners individually have an incentive to overinvest. Since all of them follow the same strategy, however, those efforts cancel each other. At the end, capital is spent with no effect.

3. Indeed, mining has become increasingly capital-intensive and, as a result, increasingly concentrated. In order to reach the critical size, many miners are grouping themselves into “pools” that share computing capabilities, costs, and profits. A very large fraction of the mining is now carried out by these pools. The production of bitcoin has become an industry in itself, with “factories” of computing power geographically concentrated in a limited number of countries where electricity is cheap. These developments mark a divergence from Bitcoin’s initial ambitions for decentralization and libertarianism.

4. With such inefficiency built into the system, it is no surprise that many indicators point to a very poor economic performance of crypto currencies. The most spectacular, and frequently mentioned, is the energy consumption. It is estimated that Bitcoin miners uses 40.64 TWh of energy to operate annually, slightly more than Hungary, the world’s 57th largest consumer of energy. This is also 75 times higher than the annual energy consumption of

---

\(^{38}\) Miners must find a number (the “nonce”) that, when combined in a hash function with the content of the block, will produce another number starting with a specified numbers of zeros—a result that can be instantly verified.
the centralized Visa network, which processed an average of 150 million transactions per day in 2016, compared to the 44 million transactions processed on the Bitcoin network for the whole of 2017.\footnote{L. Schilling, and H. Uhling (2018).}

Today, Bitcoin processes about 80 transactions per minute, while Ethereum, which is faster, can process 1,200. By comparison, Visa and MasterCard each process about 100,000/minute. According to a recent analysis performed in June 2018, Bitcoin and Ethereum can process 4 to 6 transactions per second operating at full capacity, while Visa is able to handle peaks at more than 20,000 transactions per second.\footnote{V. Buterin (2014).}

5. Finally, crypto currencies based on proof of work face a “scalability” problem. They cannot easily support the increase in activity that would be necessary for broader adoption. Contrary to all existing payment systems, Bitcoin does not normally benefit from economies of scale. On the contrary, the unit costs may actually increase with the intensity of payment traffic. The period from June to December 2017 illustrates this point in the figures below. As transaction volumes of Bitcoin increased during the second half of 2017, there was a concurrent upward movement in the price, the computing capacity (the so called “hash power “), and the unit cost per transaction.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure4.png}
\caption{Bitcoin Transactions per Day January 2017 - June 2018}
\end{figure}

\footnotesize
\textit{Source:} Blockchain Luxembourg S.A. "Total Number of Transactions Per Day." Available at :https://www.blockchain.com/Charts/n-transactions.
Figure 5
Bitcoin Cost per Transaction
January 2017 - June 2018

Source: Blockchain Luxembourg S.A. "Cost per Transaction." Available at: https://www.blockchain.com/charts/cost-per-transaction.

Figure 6
Bitcoin Hash Rate
January 2017 - June 2018

Source: Blockchain Luxembourg S.A. "Hash Rate." Available at: https://www.blockchain.com/charts/hash-rate.
For crypto currencies which seek to compete with “official” money and centralized payments systems, this cost structure is obviously a significant handicap. The problem of “scalability” has been recognized by developers and promoters as one major obstacle to the acceptance and further development of crypto currencies.

**Alternatives to proof of work**

The scalability problem has provoked crypto currency promoters to seek improvements or alternatives to the “proof of work” method of consensus. Possible solutions that are currently being explored can be grouped into three broad categories:

- Technical improvements to the existing protocol by shortening the delays between two blocks and/or increasing the size of the blocks. There is obviously a trade-off: shorter delays speed up transaction processing but also result in more “orphan” blocks, with potentially negative implications for security. This issue has proven to be contentious since larger blocks and shorter delays favor powerful miners. The debate triggered a hard fork in 2017 with the creation of Bitcoin Cash (whose blocks size is eighth times bigger than Bitcoin).\(^{41}\)

- Adoption of a different method of consensus. The main alternative to the “proof of work” process is the “proof of stake” consensus mechanism.

- Adoption of a different network architecture. Examples of the different network architectures that developers are exploring include the lightning project or partially centralized and two-tier networks

I will discuss these last two sets of alternatives below.

**Proof of stake**

In the proof of stake consensus method, potential miners or validators in effect post collateral by sequestering an amount of crypto currency in designated addresses. Those stakes are lost if the participants are proven to have behaved dishonestly. Participants also vote to validate transactions weighted by how much of a stake they hold. It is assumed that those holding the most currency have the greatest incentive to make the system work securely and efficiently.

Unlike proof of work, proof of stake does not require spending real computing resources to validate transactions. At least in principle, it therefore should not face the same scalability challenges. Ether is projected to switch from proof of work to proof of stake in the middle of 2019.\(^{42}\)

---

\(^{41}\) A hard fork is the deliberate and permanent scission of the blockchain (and the crypto currency) in two successor blockchains and currencies that share the same history but evolve separately in the future.

\(^{42}\) C. Kim (2019).
While proof of work has been tested over a longer time period, this is not the case for proof of stake. Thus far, it has only been tried over a short period for some smaller crypto currencies. It therefore is not clear yet that the method can overcome three different types of challenges that remain:

- **Effectiveness of incentives.** Participants stand to lose money if they misbehave, but the extent of this loss depends on the price of the currency itself. By contrast, in proof of work, the losses are in effect denominated in official currencies, since the main costs—mining electricity—are incurred in those currencies. Low crypto currency prices thus reduce the disincentives for engaging in dishonest behavior.

- **Security.** In effect, proof of stake may result in some re-centralization as the decision process allows for majority decision. It may be that attacks on the network are easier in this environment. These attacks would certainly be cheaper since they do not incur significant energy costs to produce. It is clear that it’s less costly to attempt to rig this system than with proof of work, where sunk costs have to be accepted ex ante and irreversibly.

- **General philosophy of proof of stake.** It is debatable whether the management of a monetary system should be entrusted to the major holders of the currency, as these parties’ incentives may not be aligned with those of other users. At the very least, there would appear to be a paradox in crypto currency advocates’ defiance towards Central Banks—who are public agents with a mandate—and rely upon a small group of agents whose motivations may change according to circumstances and are acting purely in their private interest.

**Lightning**

Lightning refers to one alternative solution that would work in conjunction with the Bitcoin blockchain by introducing a two-tier payment system in which small transactions would be concluded and paid “off-chain.”43 This should reduce congestion and allow for a scaling of activities. Participants operate specific “channels” that are in effect bilateral or multilateral exchange arrangements with means of payments earmarked and segregated in dedicated addresses. Only large or netting transactions would be directly settled on the blockchain using proof of work consensus.

In effect, lightning partially replicates the architecture of existing payment systems where different infrastructures are used depending on the size of payments. However, in contrast to recent improvements in existing payment systems, lightning requires the pre-payment to be held at specific addresses. The liquidity cost of such an approach may become significant if and when a currency becomes more widely demanded and rises in price.

---

Other architectures and designs

Other crypto currencies have opted to take different approaches to consensus from the start. They operate systems where the decisions are delegated to a subset of participants ("validators" or "collectors"). This allows the crypto currency both to dispense with proof of work and adopt simplified voting procedures. In Ripple, for instance, the consensus is assessed to be robust with only 60% majority of the selected validators.

The scalability “trilemma”

Recent developments and experiments clearly show a general tendency of crypto currencies to become more centralized. Centralization may occur as a natural economic consequence of proof of work, which favors large players. It may also come by design, as developers seek alternatives to proof of work that partially sacrifice decentralization.

This evolution is not primarily the result of the technical limitations of the network. They instead derive from the constraints imposed on the systems to meet conflicting objectives. There is a natural tension between decentralization and security. Bitcoin does attempt to achieve both objectives, but at the price of very low efficiency. It appears difficult for a decentralized system, where each transaction must be validated simultaneously by a large number of participants, to be faster and cheaper than payment systems which rely upon a central intermediary. In turn, solutions to increase efficiency sacrifice either decentralization or, in some cases, security.
There are currently no examples of existing crypto currencies or projects that effectively achieve scalability while fulfilling the initial ambitions of crypto currencies combining decentralization and security. Based on the current state of technology, there seems to be a “triangle of incompatibility” inside which the three objectives of (1) security, (2) speed, and (3) decentralization cannot be attained simultaneously. As a result, there are unavoidable tradeoffs. This triangle of incompatibility is represented in the figure below, together with the position of major existing crypto currencies.

This “trilemma” will not be solved by future technical advances related to the speed of data transmission or efficiency in processing information. Should such advances occur—the possibilities of quantum computing are often mentioned by developers—they would benefit both centralized and decentralized systems and would not erase the competitive advantage of the former. Only a real revolution in consensus techniques or cryptography would give decentralized currencies the ability to effectively compete with official currencies and contemporary payment systems.

**Performance and value**

*The usage of crypto-currencies*

At this point in time, crypto currencies hardly exist as a medium of exchange. Holdings are highly concentrated, with 2.5% of bitcoin addresses holding more than
95% of the total amounts outstanding. An estimated 1,000 addresses account for 40% of total bitcoin holdings.

It is estimated that less than 2% of transactions in bitcoins are purchases of goods and services. Only a tiny minority of merchants currently accept crypto currencies as payment. These merchants are concentrated in certain regions and countries, especially South Korea, Europe, and the United States. Payment in bitcoin is often used as an advertising tool to target young audiences. Global payments in bitcoin (100 million USD per day) amount to less than 1% of the payments made by Visa and MasterCard in the United States on a daily basis (16.5 and 9.8 billion USD per day, respectively); in the euro area, bitcoin payments amount to less than 0.2% of the total.

Cross border payments

Despite their inefficiencies, some crypto currencies may be able to compete effectively with existing systems for cross border payments. In many cases, payments from one country to another remain difficult and costly for the general public, especially for small amounts. Payments from one “exotic” currency to another often will involve two foreign exchange transactions. In addition, there are also costs and frictions associated with correspondent banking.

In those cases, crypto currencies offer an attractive alternative. By using them as “bridge” currencies, it may be possible to transfer money from one country to another in a very short period of time, with limited volatility risk.

More broadly, by exerting competitive pressures on those parts of the traditional payment system that remain relatively inefficient, crypto currencies may help to accelerate transformative changes. It may not be a complete coincidence that a significant number of new cross border payment initiatives have been announced over the last two years.

The value of crypto currencies

If crypto currencies have no use as medium of exchange, people must hold them for other purposes.

---


46 As of the end of 2017, around 120,000 websites and 289 physical stores accepted bitcoin.


48 A. Alexandre (2019).
Indeed, the main “selling point” for crypto currencies is their function as a store of value. Their promoters commonly emphasize two major characteristics: they are scarce due to their very strict issuance rules and they are supported by a large network of participants. In sum, it is argued that the value of an immaterial currency can be fully dissociated from its effective usage in payments.

On the face of it, the scarcity argument looks very powerful. Crypto currencies are presented as a sort of “digital gold”—even better than gold. Gold is expensive to store, heavy to transport, and can only be handed over through an in-person interaction. The value proposition of cryptocurrencies is that they are a form of “teleportable” gold.

But is scarcity sufficient to create value? For a currency, a rigorous issuance regime certainly offers strong guarantees. It prevents the issuer from inflating away the value. However, if abundance can erode value, scarcity is not sufficient to create it. Looking at just the supply is not enough to determine the value of money. One must also consider demand. A good, a commodity, or a currency that nobody wants has no value.

Crypto currencies are immaterial and lack backing. For such currencies, the demand, and, therefore, the value, has two components. First, people might expect them to appreciate in the future, either in purchasing power (against goods) or in price (against other currencies). This is the “speculative” component in the demand for money. Today, this component is dominant for crypto currencies. Second, money can be used to make payments. It does a better job of fulfilling that function than any other economic object. It can be said that money brings transactional benefits to its holder and that these benefits give value to money.

These two sources of demand do not behave in the same way.

The speculative component is purely driven by expectations of future capital gains. Those expectations can sustain the value of a currency for (possibly very) long periods. Bubbles can form and develop. Those same expectations can also reduce the value to zero at virtually any time. Monies with no intrinsic value are especially vulnerable to such a collapse in speculative demand.

---

49 According to a survey conducted in November 2017 among crypto currency holders, investment purposes were the main reason for holding: out of 564 US citizens surveyed, only 8% acquired Bitcoins for transaction purposes. Between 2013 and 2016, more than half of the users of the Coinbase trading platform used Bitcoin for investments and not for transactions. J. Gitten (2017).

50 Money is usually valued either (1) in terms of the basket of goods that it can be used to purchase (the value of a money unit is the inverse of the price level); (2) through the opportunity cost of holding money rather than a bond (the nominal interest rate); or (3) by its “exchange rate” with other currencies. This last concept predominates the discussion on cryptocurrencies. It has a close relationship to the first definition in the long run under normal economic assumptions.


52 C.A. Sims (2013) (“It is easy to construct models of economies in which unbacked paper money can have value, but in such models it is generally also possible for money to be valueless, or to dwindle rapidly in value so that the economy approaches a barter equilibrium. In such models, introducing taxation either to pay interest on government liabilities or to contract the supply of non-
Demand for money to make payments also depends on expectations, but of a different nature. There must be coordination of beliefs, “trust” in common parlance. People hold money because they expect other people to accept it as payment in the future. In turn, those people also expect that other persons will accept it as payment. Each holder of money gives value to it, because she thinks others will do the same.

This second source of demand is more robust. Once a large number of people accept a currency as payment, it is unlikely that their collective expectations will suddenly shift (as long as they trust the issuance regime). When money is established as a medium of exchange, it has a usage value (even if its intrinsic value is zero). That usage value puts a “floor” (a lower bound) on its future price. It is unlikely that it will ever collapse to zero.

For “official” fiat currencies the value is further supported by legal tender and the obligation to use them to pay taxes. Those institutional constraints guarantee that they will be accepted as payment far in the future.\(^{53}\) That also gives them value today. Gold, for its part, has historical usage value as medium of exchange, but also for jewelry and industrial applications. Its value cannot fall to zero.

Crypto currencies, have no such institutional support or physical backing. Today, their usage as payment instruments is minimal. As long as that is the case and there is no realistic expectation that they can be used as a means of exchange in the future, crypto currencies’ value will rest solely upon their speculative component. They will remain vulnerable and directly exposed to a collapse of their price, even with a restricted supply.

The “support” of a large network—the second argument made by crypto currencies’ promoters—does not change that assessment. The network is necessary for transactions to take place on a broad scale. It is not sufficient. If payments are made difficult or impossible by technical frictions, the currency has no possible use as a medium of exchange and therefore no usage value.

Ultimately, it is the difficulty of operating a decentralized monetary system that deprives crypto currencies of any transactional value. It stymies their growth and makes it less likely that they will gain broad usage and acceptance in the future.\(^{54}\)

However, things might change. Some special purpose currencies may gain utility and value in more limited circumstances. Crypto currencies may develop as cross border payment instruments and acquire utility and be used as well as stores of value on this basis. In countries where monetary institutions are fragile, economic agents will turn to safe havens that even though imperfect are far superior to those offered by bearing liabilities (and thus, via deflation, create a real return) tends to resolve the indeterminacy and provide a uniquely determined price level.

\(^{53}\) Of course expectations on the precise value of the currency will be influenced, if not driven, by the issuance regime.

\(^{54}\) Since digital currencies lack any intrinsic demand (for use in production or for consumption) and no central authority stands behind them, an opinion about their future demand should largely rest on (i) a belief about their future use as media of exchange and (ii) a belief that they will continue to remain in demand even further into the future. J. Barrdear, and M. Kumhof (2016).
official institutions. The dollar fulfills this role in many countries. Crypto currencies may in some cases be more accessible and could play a similar role. Finally, currencies based on more centralized schemes and large cross-border networks could also gain broader acceptance in the future. This perspective is examined in Part II.\textsuperscript{55}

\textit{Crypto currencies as financial assets}

There is an ongoing debate on the role that crypto currencies (or assets derived from them) should play in the financial systems of many countries. In many cases, they have come to be viewed as an asset class for financial investment, driven by the interaction between their fixed supplies and increasing publicity.\textsuperscript{56}

To assess the potential roles and risks of crypto currencies as financial assets, one can consider two different angles:

- First, one may look at the asset's fundamental value, defined by its expected discounted cash flows. Those cash flows can be certain or probabilistic, conditional or not. The relationship between the asset value and the expected stream of cash flows can be complex, particularly in the case of derivatives, options, and structured products. But the underlying value conceptually always exists, based on a flow of future incomes. Fundamental value can be estimated, although different investors will reach different conclusions based on their assumptions about the economic environment and their risk appetite.

- Alternatively, the asset can be assessed through its observed and predicted behaviour in relation to other financial instruments. The asset is then characterized by identified patterns, correlations, or behavioral regularities that define its contribution to the risk and return profile of a portfolio.

Both approaches naturally complement each other in investment decisions. The second approach, based on empirical observations, can be self-referential, as observed patterns may self-validate once they are internalized by investors in their decisions.

In the present environment, only the second approach can apply to crypto currencies. As discussed above, they currently have no transactional usage value, nor do they generate and are not expected to generate any income.\textsuperscript{57} Some investors feel,

\textsuperscript{55} A. Stevens (2017), p. 82 (“However, recent theoretical model simulations by Bolt and van Oordt (2016) show that, in the long run, exchange rate risks are not likely to get in the way of widespread use of private digital currencies, because such risks would be mitigated as such currencies become more established. One interpretation is that the assessment of value is to a large extent based on subjective beliefs, which can evolve over time. For instance, if private digital currencies were to achieve increasing success as a medium of exchange, they would gain value in terms of practical utility. This source of value could render exchange rates less sensitive to the impact of shocks to speculators' beliefs. Financial stability risks would in any case be limited in this scenario, as widespread adoption of privately issued digital currencies would actually contain exchange rate volatility.”).

\textsuperscript{56} J. Barrdear and M. Kumhof (2016).

\textsuperscript{57} This is not true for ICOs.
however, that their pattern of behavior is such that they may help hedge some risks and, more broadly, improve the risk-return profile of specific investment portfolios.

One study, by JP. Morgan identified the main following characteristics:58

- Crypto-currencies have a correlation of close to zero on average with other asset classes over the last five years;
- A modest Bitcoin allocation in recent years would have improved the average efficiency of the securities portfolios;
- Crypto currencies are not, however, “safe haven assets.” They do not make it possible to offset portfolio losses during periods of acute stress on the equity or bond markets, such as during the “flash crashes” of August 2015 or during periods of turmoil in the capital markets of developing countries;
- Crypto-currencies have a limited level of liquidity, which can prevent their use in large portfolios.

Overall, there were over 700 specialized crypto currency funds as of the end of 2018, with more than 10 billion USD under management.59 These funds do not necessarily take long positions in crypto currencies, but are more likely to exploit price differences and arbitrage opportunities.60 In total, regulated financial institutions invest, trade and operate in cryptocurrencies or derivatives in at least eight jurisdictions. In 2017, the Commodity Futures Trading Commission (CFTC) authorized the trading of future contracts based on notional crypto currencies.61 Derivatives instruments offering exposure to crypto currencies were introduced on the Chicago Board Options Exchange (CBOE) and the Chicago Mercantile Exchange (CME) in December 2017, although the CBOE subsequently stopped trading new bitcoin futures contracts in March 2019 due to low volumes.62

While several Exchange Traded Funds (ETFs)63 investing in crypto currencies have applied for approval from the Securities and Exchange Commission (SEC) in the United States, none has been approved. ETFs would be more accessible to individual investors than most specialized funds currently available and are thus drawing a great deal of scrutiny from regulators.

---

63 ETF are index UCITS listed on regulated markets.
ICOs

Initial Coin Offerings (ICOs) have appeared over the last three years as a byproduct of crypto currencies. Through ICOs, companies (most often startups) aim to raise funds over the internet by issuing digital tokens that can be purchased with crypto currencies. ICOs aim to mimic the issuance of shares, without any of the formalities that are attached to IPOs. There is no prospectus for stock exchange authorities, but simply a document (a “white paper”) posted on the Internet. It does not legally bind the issuer. ICOs tokens are usually quoted on crypto currency exchanges shortly after they have been issued.

The tokens themselves come in different forms with a great variety of rights attached to them. It is customary to distinguish between (1) “security tokens” that mimic the economic and legal characteristics of equity shares; and (2) so called “utility tokens” that confer in principle a right of usage on future services to be provided by the issuers. The nature of rights an ICO confers is often very vague or unspecified. A few have legal rights of access attached to them. Most are actually special purpose payment instruments—or currencies—that can be used in the future to purchase services produced by the issuer.

After significant growth in 2017-2018, ICO issuance has fallen dramatically in the second half of 2018 and first half of 2019 (see graph). This evolution closely follows the price of crypto currencies.

![Graph of Initial Coin Offering Fundraising, May 2017 - May 2019](https://www.coinschedule.com/statsICO)

V. GOVERNANCE AND TRUST

In a decentralized monetary system, governance cannot be entrusted to a permanent institution “responsible” for the currency as such an institution does not exist. Where does trust therefore come from? Three sources of trust are commonly identified by promoters of crypto currencies:

- First, the protocols and algorithms that govern the issuance and circulation of crypto currencies. Provided that they are appropriate and cannot be tampered with, these protocols protect users against malfeasance such as double spending and any temptation to inflate the currency through over-issuance.

- Second, economic incentives. Participants, especially miners, are presumed to have a permanent stake in the long-run functioning of the system.

- Third, transparency. For those crypto currencies that operate on a blockchain, any single transaction is visible and traceable by everybody. Any misbehavior or malignant act would be quickly detected and, if not addressed by the community, would likely trigger a collapse of confidence in the currency, triggering a fall in value and depriving potential cheaters of any benefits.

The reality, however, is somewhat fuzzier. Protocols regulating cryptocurrencies are very frequently modified or amended. For the most part, these amendments are technical and are intended to correct or improve the operation of the network. Others, however, deeply transform the characteristics and operation of the crypto currency. They are not always consensual and, in the absence of decision rules, give rise to splits within the monetary systems, or “hard forks.” While such hard forks are infrequent, they nevertheless reflect the fragility inherent in informal arrangements lacking institutional backing.

For most crypto currencies there are no rules or established processes to modify the algorithms and protocols. Those decisions are taken informally by the community of developers, according to the traditional mode of open source protocol management. There are various modalities for these situations, including regular online forums, exceptional conferences, and more or less organized consultation procedures. In a number of exceptional cases, some currencies are “supported” by formal institutions. For Ether, a Swiss foundation that de facto assumes a coordination function by encouraging the necessary organizational decisions. Even then, however, its role is limited to organizing discussion and decision rules are not specified let alone formalized.

Informality naturally opens up the possibility of pressure and manipulation given the competing economic interests in the crypto currency ecosystem. The concentration of mining power makes conflicts between those interests more acute and visible. In a 2018 survey, more than 60% of minors acknowledged that they have an influence on the definition and characteristics of protocols.

Another potential source of fragility is that the incentive structure may not prove resilient over the long run. Rewards to miners are denominated in crypto currencies (as for Bitcoin) while the costs are in official currency. The profitability of mining
therefore depends on the price (exchange rate) of the crypto currency. Should a collapse in prices occur, mining would become a loss making activity, possibly leading to a “death spiral,” with the exit of miners, a paralysis of the network, and further falls in confidence and prices. In such a circumstance it would be hazardous to postulate that individual miners would coordinate and take a long-run perspective and keep operating the network at a loss, in anticipation of a return to normalcy.

In addition, for Bitcoin and Ether, the incentive structure is bound to change over time. As issuance of new units of crypto currency will stop (for Bitcoin) or stay at a constant growth rate (for Ether), the systems will increasingly rely upon transaction fees to reward mining and ensure the continuing operation of payments. It is not certain that users will accept the level of fees that would make mining profitable and significant uncertainty hangs over the long run viability of such an approach.64

Overall it may be Illusory to think that one can dispense with institutions in managing a currency. History, experience, and theory have provided many lessons on the effective governance of monetary systems. The functions of the currency, especially as a store of value, impose specific requirements: a very long-term horizon, a consideration of the public good (which may not always coincide with the interests of current holders), and an ability to react to changing circumstances and provide an “elastic supply” of money. Those lessons have led to the creation of Central Banks and, in the last thirty years, granting them operational independence. This institutional arrangement provides both stability in the long run and short-term flexibility in reacting to shocks. Strikingly, crypto currencies operate on diametrically opposed principles: great rigidity in short-term management (by algorithms and protocol) and significant uncertainty on the long run.

VI. THE REGULATION OF CRYPTO CURRENCIES65

Cross-Country Differences in Approaches

There is currently a great diversity of attitudes towards regulation of crypto currencies across jurisdictions. These differences stem not only from differences in the economic situations of countries, but also how they view innovation and the extent to which they want to foster it. These attitudes shape the policy and regulatory posture that countries are taking with respect to crypto currencies. Some are sensitive to the financial or cyber risks involved for investors or for public policy (e.g., crypto currencies may help circumvent capital controls). These countries, often emerging market economies, have imposed restrictions or banned any and all crypto currency activities. Others, while generally not recognizing cryptocurrencies as legal tender, seek to promote the technology and develop a friendly regulatory regime as a means to attract investment.


These divergences in attitude have not prevented governments, Central Banks, and financial regulators from warning about the pitfalls of investing in crypto currency markets.\textsuperscript{66} Such warnings generally aim to educate the users about the difference between actual currencies, which are issued and guaranteed by the state, and cryptocurrencies, which are not. Most warnings note the added risk resulting from the high volatility associated with crypto currencies and the fact that many of the organizations that facilitate such transactions are unregulated.\textsuperscript{67} Most also note that citizens who invest in crypto currencies do so at their own personal risk and have no legal recourse available to them in the event of loss.

**Defining crypto currencies for regulatory purposes**

In terms of applying regulation to crypto currencies, all countries face difficulties in simply defining relevant terminology and classifying crypto objects in a manner consistent with their regulatory frameworks given the diverse and original forms these objects take. Some of the terms used by countries to reference crypto currency include: digital currency, virtual commodity, crypto-token, payment token, cyber currency, electronic currency, and virtual asset.\textsuperscript{68} In the United States, the CFTC has designated crypto currencies as commodities subject to its regulation, whereas the SEC generally considers tokens from ICOs (many of which also serve as crypto currencies) as securities.

Defining and classifying crypto-assets is a natural first step to regulating them, as legislators and regulators naturally tend to deal with new objects by applying the models applicable to existing objects and categories. But there are limits to this approach when technological evolution is radical and quick paced. “Forcing” the classification of crypto currencies into pre-existing boxes may lead to mistakes and distort the evolution of the technology.

There are nonetheless certain circumstances where classification of crypto currencies is largely unavoidable:

- **Taxation.** When transactions occur and generate income for participants, tax authorities in that person’s home country must decide on the applicable tax regime. These differ widely across jurisdictions, with the United States treating crypto currencies as property similar to gold, while the European Union treats them as currencies.\textsuperscript{69} Courts are sometimes required to make a determination.

\textsuperscript{66} E. Kwok (2018).


• Public offering of crypto assets. When a crypto asset is potentially made available to the general public, rules of protection have to be defined and applied. In the United States, the SEC has made clear that it determines whether an offering is a securities offering subject to its jurisdiction based on the “Howey test,” regardless of the technical labelling or form of the crypto asset. The SEC has been aggressive in its enforcement actions related to ICOs that it considers to be securities offerings in recent years.

• Anti-Money Laundering/Combatting Financing of Terrorism (AML/CFT). Given concerns about the use of crypto currencies for money laundering and terrorism financing, AML/CFT regulations have been a central focus of many countries’ regulatory efforts.

A general approach to regulation of crypto currencies

Is a more comprehensive and general framework necessary in designing and implementing a regulatory framework for crypto currencies? The landscape is constantly changing as authorities adapt to the rapidly evolving technology and local circumstances. Given the diversity of situations that countries face, is there a need for further harmonization and cooperation in terms of regulation? A useful framework for evaluating the regulation of crypto currencies was the seminal March 2018 speech by Mark Carney, then Chairman of the Financial Stability Board. He outlined three possible approaches to the regulation of crypto currencies that authorities could adopt: 1) isolate, 2) regulate, or 3) integrate crypto-assets and their associated activities.

This report advocates an “isolate” approach to regulation. Based on this approach, authorities should not at the present stage try to directly regulate crypto currencies except when unavoidable, as is the case with the cases described above. Authorities should allow crypto currencies and associated ventures to develop, experiment, and possibly grow in their own “cyber space.” But the authorities should contain these crypto-assets in that space and not allow interactions with the “official” financial system, except for informed and sophisticated investors or participants.

The rationale for “isolating” crypto currencies is twofold:

• First, regulating an emerging technology is hard, as a “technology neutral regulation” is difficult to achieve. It may be that defining and classifying new objects would change economic incentives, impede innovation, or distort business decisions by orienting it towards regulatory avoidance. It is delicate for regulators to sort out the good from the bad in the middle of an innovation wave. For instance, a common presumption amongst analysts and policy

---


makers is that bitcoin may be problematic, but the underlying blockchain technology is promising and should be supported. This sounds sensible, but there are complex interactions between the monetary and technological components of many blockchain applications. As discussed earlier, the existence of a native currency is often necessary for some specific decentralized, anonymous applications to work. As the saying goes “if there was no bitcoin, there would be no blockchain.” In effect, dissociating the blockchain from the monetary experiment means that only “permissioned” blockchains would be allowed to prosper.

- Second, according to the FSB, crypto currencies currently “do not pose a material risk to global financial stability” that could motivate regulation. Outstanding amounts of crypto currencies are minimal compared to the size of capital markets and financial systems as discussed earlier. Financial institutions do not have significant exposures, let alone the leveraged positions that might pose risks to financial stability. Total notional derivatives exposures are also very small. While confidence in the financial system could be adversely impacted if serious incidents were to occur and supervisors should stay vigilant, this does not appear to be a pressing concern at the moment.

The main financial risks associated with crypto currencies today relate to market integrity. These risks materialize primarily on the exchanges, at the interface between the crypto world and the official financial system. At the same time, regulators are currently faced with many requests to authorize the launch of new investment vehicles specifically dedicated to allowing the general public to take on exposure to crypto-assets. Should regulators give those authorizations, a new channel of transmission from crypto currencies to the financial system would open. Risks associated with crypto currencies would increase, and direct regulation of crypto currencies would become unavoidable. For those reasons, isolating the crypto system appears to be the preferable approach at this stage.

**Areas for international cooperation**

Due to the global nature of crypto currency ecosystems, interactions with the formal financial system necessarily are legally and physically located in numerous jurisdictions. An efficient “isolate” approach to regulation would therefore require at least some minimal degree of cooperation to define and implement appropriate rules and procedures. This coordination should be targeted at three different types of financial institutions: the banking system, the asset management industry, and the exchanges

**Banks**

Banks currently avoid taking proprietary exposures on crypto currencies and most of them would not grant credit to their clients in order to take such exposures. It would make sense for banking supervisors to agree to formalize this prohibition on a global basis, at least for a period of time.
Asset management and investment funds

The situation in asset management is more complex and urgent. There is currently a great deal of pressure on regulators to agree to the creation of investment vehicles aimed at the general public and dedicated to crypto assets.\textsuperscript{73} An “isolate” approach to regulation would directly conflict with these calls and militate against granting such authorizations. In my view, public policy should aim to prevent the general public from getting direct or indirect exposure to crypto currency risk at this juncture. There are three reasons it makes sense to wait and see before liberalizing access to crypto-assets.

From an investor protection perspective, crypto assets are extremely risky. The currencies themselves have limited usage value and their price is only supported by self-fulfilling expectations of appreciation. While crypto assets ultimately may find a role as hedging instruments given their lack of correlation with traditional financial assets, they generally should be reserved for well-informed, sophisticated investors with the appetite and ability to invest in high risk assets.

From a financial stability perspective, allowing retail investors to invest in crypto assets could potentially create a strong channel of transmission between the crypto ecosystem and the rest of the economy. Were crypto assets to gain “systemic” importance, they would thus pose important dilemmas for any efforts to regulate them.

Authorizing retail investment in crypto assets would result in a transfer of risk from current holders to future investors. As mentioned, holdings of crypto currencies are extremely concentrated and it is likely that the weak liquidity on crypto exchanges constrains many current holders from offloading their exposures. The creation of new investment vehicles would certainly bring additional liquidity to crypto currency markets; the benefits would be distributed in a highly asymmetric fashion, however. Current holders would be able to offload their exposures, particularly if market enthusiasm about the potential impact of these new investment vehicles help spur crypto currency prices higher. At the same time, new participants, many likely with limited experience investing in similarly volatile markets, would potentially be left bearing the risks of a market correction. Allowing retail investors to invest easily in crypto assets should only be contemplated when the technical and economic future of those assets is more assured.

These recommendations are predicated on the (currently valid) assumption that crypto currencies are not used as a medium of exchange. Consequently, their payoff is mainly driven by speculative demand. Should some existing or new forms of crypto assets gain broader acceptance and/or usage value, allowing retail investors to participate in the market would make more sense.

\textit{Crypto Currency Exchanges}

Crypto currency exchanges certainly constitute the “weak link” in the current crypto ecosystem architecture and represent the point where regulation is most urgently

\textsuperscript{73} Around 20 ETFs are pending on the SEC.
A significant number of crypto currency exchanges are completely unregulated, with only 30% to 50% of exchanges holding a formal government license or authorization.\textsuperscript{74} This activity also shows a high degree of regulatory competition and arbitrage, as shown by the movement of exchanges from one location to another.\textsuperscript{75}

In most markets, guarantees of market integrity are minimal. In some cases, investors do not enjoy the basic degree of protection regarding the transparency of operations, the order book, or even the basic security of their holdings. There is also evidence that some crypto exchanges also engage in proprietary trading, thus creating the prospect that they are trading against or taking advantage of their customers' trades.\textsuperscript{76} Some crypto trading platforms may also engage in wash trading where the same party trades with itself in order to create the appearance of greater liquidity or to manipulate prices.\textsuperscript{77}

Some exchanges hold accounts for their customers in both official and crypto currencies. These accounts are used for effecting transactions by transfers from one account to the other in a bank-like form of activity. However, there are currently no guarantees that the accounts held by exchanges are effectively backed by holdings of official currencies (if accounts are denominated as such) or addresses in the blockchain (for crypto currencies).

Unsurprisingly, exchanges appear to be the area of the crypto ecosystem where criminal activity is most prevalent and where "hacking" of crypto currencies take place. Since 2011, 19 severe incidents have occurred, with total losses reaching 1.93 billion USD.\textsuperscript{78} The frequent cause of these hacks is due to private key falsifications, followed by transaction malleability,\textsuperscript{79} and the introduction of malware. Some of these hacks occur because many users entrust their private keys to exchanges, thereby enabling them to manage their addresses and funds flows. If these private keys are kept in a public folder accessible on the internet, referred to as "hot storage," then the keys are vulnerable to hacks. Use of "cold storage," which is not connected to the internet, is much more secure, albeit less convenient to transact with and not supported by all crypto currencies.

For these reasons, authorities in all countries should consider agreeing on at least

\textsuperscript{74} This figure is only 15% for exchanges based in the Asia-Pacific. G. Hileman and M. Rauchs (2017).


\textsuperscript{76} J. Wilmoth (2018).

\textsuperscript{77} T. Massad (2019).

\textsuperscript{78} R. Rathi and Shivangi (2019).

\textsuperscript{79} Electronic signatures can change slightly while still being valid before being added to the blockchain, which makes it vulnerable to hacks attempting to modify it (to be compared with the falsification of a check signature for instance). Medium (2018). “How Does Blockchain Work in 7 Steps--A Clear and Simple Explanation,” https://blog.goodaudience.com/blockchain-for-beginners-what-is-blockchain-519db8c6677a, accessed on June 11, 2019.
some basic principles to guide the regulation of exchanges. Massad (2019) provides a useful framework for defining those principles. They should encompass:

- Governance standards
- Protection of customer assets
- Conflicts of interest (if the exchange fulfils several functions)
- Record keeping
- Transparency on quotes and trades
- Guarantees of best execution and settlement of transactions
- AML compliance

ICO tokens can cumulate several layers of risks. The informal issuing process offers no guarantee as to the final allocation of funds. In addition, holders of utility tokens are exposed to the ordinary business risk of the project itself and to a “monetary” risk. The issuer controls both the number of similar tokens that may be issued in the future and the price at which they will be accepted for payment. Strict regulation would be justified, especially for utility tokens.

On the other hand, ICOs and the successor technologies may be precursors of a profound transformation in the cross border issuance and trading of digitalized securities. It thus may appear appropriate to allow these innovative approaches to develop.

Regulators are facing this tradeoff with a diversity of approaches. The overriding objective of proper regulation is to make tokens safer for investors. Two mutually compatible approaches are being pursued. The first one aims at restricting the sphere of “utility” tokens by defining and enforcing strict tests that legally reclassify most tokens as “securities.” This is the approach taken most strongly by the SEC in the United States, where ICO tokens are treated as securities from a legal and regulatory perspective if and when (1) there is an investment contract (the so called “Howey test”) or (2) tokens are quoted on an exchange.

In France, recent legislation has introduced a mechanism of an “optional visa” that can be requested from the market regulator, the Autorité des Marchés Financiers. Authorities will check that the issuer is a legal entity established or registered in

---

80 T. Massad (2019).
82 See Article 26 of the PACTE bill.
France, funds collected during the ICO are monitored and safeguarded, and AML/CFT obligations are fulfilled during the ICO. The visa will offer investors substantial guarantees of integrity while preserving the flexibility inherent to the ICO process.
PART II: PRIVATE AND PUBLIC MONEY IN A DIGITAL WORLD

For all their imperfections and limited achievements, crypto currencies have brought a new perspective on the future of money. They force us to consider the impact of technological change on our payment and monetary systems.

This report focuses on one key issue: the respective role of public and private money in this new technological environment. In contemporary economies, private money dominates as a medium of exchange. Most of the money that circulates in the economy is privately issued and takes the form of bank deposits. Public money, composed of cash and bank reserves at the Central Bank, provides the unit of account and is the basis for legal tender. And, crucially, the coincidence between the two functions—exchange and account—is guaranteed by the unconditional convertibility between the two forms of money—private and public.

Technology could change that equilibrium in many ways.

It will certainly transform the forms of money in its role as a medium of exchange, with significant consequences for financial intermediation, the role of banks, and the uniformity of the currency. Part II of this report discusses the changes to the monetary system that can be expected as a result of mobile technology, the emergence of large payment networks, and the further development of e-money, as well as the possible consequences of the disappearance of cash and a technical fragmentation of the monetary system.

Although less certain and more speculative, technology may also enable new private currencies to compete with existing official ones as a unit of account. The report presents a preliminary analysis of possible scenarios.

These changes present many challenges for governments and monetary authorities. There is relatively little doubt that sovereign governments and Central Banks would ultimately prevail if they assert their power and authority in regulating and, if necessary, prohibiting those monetary innovations that they dislike. However, evolutions in technology present authorities with new trade-offs. On the one hand, Central Banks and regulatory bodies seek to promote efficiency and competition between payment systems and encourage the introduction of new technologies. On the other hand, they may be legitimately concerned about the risks and monetary implications of those same technologies. It will be easier to manage those trade-offs if Central Banks were to issue their own digital currency (a Central Bank Digital Currency or CBDC) in the future. A CBDC would guarantee that the general public

83 More precisely, the public currently holds two categories of money: the first, cash, has physical form, is transacted on a peer-to-peer basis, can be transacted anonymously, and is public (i.e., issued by the Central Bank); the second, bank deposits, is electronic in form, has account-based holdings and transactions, is not anonymous, and is private (i.e., is created by banks).

84 S.L. Schreft (1997), p. 60 (“…the concern for policymakers is not that electronic cash is electronic, but rather that private firms are issuing it.”).

85 Indeed, a number of countries, particularly emerging market economies, have started to do so.
could keep access to public money even as the underlying technology of money changes. It would also preserve the uniformity of the currency and its role as unit of account in a digitized economy.

I. DIGITAL MONEY AND PAYMENTS

A silent revolution is currently taking place in retail payments. For more than 20 years, e-money instruments have been available in most parts of the world. But they were hardly used. Still today, outstanding e-money in the euro (EU) area amounts to less than 1% of the total monetary aggregate.\(^{86}\)

That is about to change. The driver, of course, is mobile payments. Smartphones are making payments by e-money significantly more user friendly than previously available modes such as laptops and pre-paid cards. Technology has revealed a demand for instant, peer-to-peer, point of sale (POS) payments that mimic the use of cash in transactions as closely as possible. People have become more willing, and indeed may prefer, to make payments via the internet or mobile phones. Mobile payments are now reaching mass market penetration. The number of transactions by mobile payments worldwide were projected to more than double between 2015 and 2019 from 50 to 109 billion.\(^{87}\) Transaction volumes are projected to increase tenfold between 2016 and 2021.\(^{88}\)

This shift toward electronic retail payments is especially rapid and widespread amongst younger generations, as well as in countries where banks for various reasons have been unable to provide payment services to certain segments of the population.\(^{89}\) The rise is most spectacular in China, where 47% of the population used mobile wallets in 2018, compared to only 20% in Japan and 17% in US.\(^{90}\) This trend is intensifying in all advanced economies as well, however. This year, 20% of the US population are estimated to be using mobile payments.\(^{91}\) Penetration is greatest in the youngest part of the population (with 48% of people aged 18 to 34 having a mobile wallet compared to only 29% for those aged 55 to 64).

Payments are affecting money. The most visible sign in some countries is the displacement and increasing marginalization of cash, the only public money that is universally available.\(^{92}\) More broadly, mobile technology and the advent of “next


\(^{87}\) Capgemini and BNP Paribas (2017).


\(^{89}\) CPSS (2012).

\(^{90}\) M. Grothaus (2018).

\(^{91}\) R. Kats (2018).

\(^{92}\) This issue will be explored at greater length below.
generation” payments has the potential to reshape the architecture and organization of monetary systems in a profound way. The emergence of large payment operators and networks may challenge banks’ existing business models. Payments may become the core function in financial intermediation, emerging as the main or even exclusive contact point with customers, positioned at the center of a whole ecosystem of commercial and social interactions and aggregating valuable data about customer behavior. From a public policy perspective, this could lead to the technical, operational, and monetary segmentation of monetary systems. Managing such developments may require Central Banks to develop their own digital currencies.

Technically, mobile money is both an instrument—tokens stored on a mobile device—and an infrastructure—the network that transfers the information and the value. The current revolution involves both, in a symbiotic relationship. From an analytical perspective, it may be useful to first consider these developments separately in the following sections.

The tokenization of money

“Token” money has always existed in physical form. Coins and banknotes are physical tokens. Today, the possibility to securely attach an identity to a digital representation of value allows for the use of digital tokens. As a result, a new form of money is emerging. This may turn out to be the true monetary innovation brought by digitization.

The fundamental distinction between account-based and token-based money has resurfaced in analysis and policy debates.93,94 This distinction relates to how money moves and is exchanged between economic agents.

In account-based systems, money is a claim on a bank; payment is made by transfer of this claim between two bank accounts. By contrast, a token, when used as fiduciary money, is a digital file with the holder's name attached to it. Payment is made by changing the holder’s name, according to a process that is secure and whose authenticity is guaranteed by a designated authority.95

Fundamentally, a digital token96 mimics the characteristics of cash. Holding it (through cryptographic proofs) means that one possesses it. By changing the identity...

93 A. Stevens (2017).
96 The terminology around these issues is not yet fully accepted or consistent. Parts of the economic literature use the terms “value-based money” to designate the digital representation of value. For security experts, a token is a device that securely mirrors an identity to allow transactions on an open network. CryptoCurrency Facts. “What is a cryptocurrency token?,” https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-token/, accessed on June 10, 2019.
attached to the file, the representation of value can be transferred and a payment is made. A digital token can be exchanged on a peer-to-peer basis without any financial intermediary and, if necessary, without any need for a bank account.

Technically, there are two differences between token- and account-based money:

- The way finality in payment is achieved. With account-based money, a transfer reaches finality when the funds are debited from the account of the payer and credited to the account of the payee. The account keepers—the banks—are directly involved, as they register the transfer. Tokens are different: a transfer of cash is final when the payer hands the token over to the payee; while there must be a record of the transfer, the ledger holder does not take any responsibility for the finality of a payment.

- The security requirements that are attached to identification. The responsibility to verify the authenticity and validity of a token rests on its recipient. In an account-based system, the account keeper takes that responsibility.

Token-based money is specially adapted to transactions in a digital world. When money has to be stored on a mobile device and transferred by wireless networks, it is in tokenized form.

A system where tokens are directly exchanged between mobile devices either anonymously or without verifying the participants’ identification is potentially very different from one where payments are made by debiting and crediting identified bank accounts. Tokens allow users to dispense with having a bank account if a consumer either does not have access to one or does not want to have one.

Tokenization is, however, merely a form of money. It does not prejudge the underlying monetary architecture and is compatible with a diversity of monetary arrangements. Tokens can be used as a purely technical device that “mirrors” bank deposits and helps move the tokens around, as is the case with wallets and other applications available on mobile devices. Alternatively, tokens can also develop into a form of money fully detached from any bank account from a user perspective: in this case, an e-money provider issues tokens that can be exchanged without bank accounts.

A central question for the future is whether tokens will serve as a complement or substitute to bank deposits as money. Schematically three different models may exist:

---


98 E-money is generally described as “pre-paid.” This means that the token has been created through the deposit of cash by the holder or, more frequently, by transfer from its bank account to the issuer’s bank account.
• “Wallets” serve as complement to banking system. This first model is less disruptive for the customers and the banking system. Each individual retains their bank accounts, as is currently the case. They may choose to give “Payment Service Providers” (PSPs) technical access to their bank accounts and install Apps (“wallets”) on their mobile device to initiate their payments. This model has been actively promoted in some jurisdictions in order to increase competition in payment services, as is the case with the European Union’s recent PSD2 Directive. In this model, tokens play almost no monetary role.

• E-Money issuer plays more central role. In a second more disruptive model, customers do not need to have bank accounts anymore and instead can hold their money in the form of tokens stored on their mobile devices. The issuer of tokens holds some (large) settlement accounts at banks or the Central Bank but customers do not need to have a bank or financial ID other than, for instance, their phone number (see Figure 10 on next page). This model is spreading fast in some emerging economies (e.g., M-PESA in Kenya).

---

99 This is EU terminology.


101 So-called “stable coins” (see Part I of this report) in effect belong to this category.
There are four major differences compared to the first model: (1) the user holds tokens that are a new form of money that can be transferred via peer-to-peer exchanges; (2) the third party is no longer a simple service provider, but is instead an e-money issuer. It holds and manages a monetary balance sheet with monetary liabilities (the tokens) and assets in its own bank accounts; (3) the business model of banks has been altered as, instead of a multiplicity of small depositors, they may do business primarily with a small group of very large counterparties; and (4) new challenges arise for regulators on the supervision and regime of the new forms of money. Ultimately, the system remains “bank based” as settlements are made by transfers between bank (and Central Bank) accounts. But the underlying customer relationships and business models of banks are disrupted as the e-money issuer now plays the primary financial intermediation role with retail customers.

---

102 One frequently mentioned issue is the absence of deposit insurance on e-money.
• A third model is a mix of the two previous ones. Customers can transfer money from their bank accounts to a third party (i.e., an e-money issuer) and receive tokens to be stored and used on their mobile phones. But they still hold a bank account of their own. They are basically using two forms of money that are convertible into each other. In China, Tencent and AntFinancial manage huge payment systems on the basis of this model.

At the moment, for all their technical innovations and potentially disruptive effects, payment systems remain very traditional in their underlying monetary mechanisms. Most wallets are “pure” payment service providers. They do not (or only marginally) collect deposits or open accounts for their customers. They do not have a “monetary” balance sheet and are not regulated as banks. They use prepayments or get access to their clients’ existing bank accounts and move the money in and out according to instructions. They provide transaction services and act as “trusted intermediaries” for payments, ensuring speed and security. Customers still rely on banks to open accounts, to hold deposits, and ultimately to effect payments on their behalf. Payments are still made by reducing the balance in a customer’s account and increasing the balance in the recipient’s account by an equivalent amount—a process that has not changed since the 16th century. Bank deposits thus generally remain the means by which the general public makes most electronic payments.

Will that change as existing or new forms of e-money appear and develop? In the future, users likely will have a choice. They may still have accounts with both their bank and an e-money provider and can move money between them. But they could also dispense with having a bank account altogether and hold all their money in the form of tokens stored on their computers or mobile phones. Could the M-Pesa model be expanded or generalized to other emerging or advanced economies? If yes, it would mark a major shift in how money moves around the economy. The role of banks in payments would be limited to clearing and settlement purposes between e-money issuers.

As of today, there is little sign of such a revolution occurring. In part, this may reflect that there are not sufficient incentives for consumers to shift away from customer-based bank accounts. Banks are vigorously competing to improve their payment services and reduce their costs. At the same time, e-money issuers themselves may be reluctant to hold and manage a “monetary” balance sheet, with the attached responsibilities and increased supervision that would likely entail.

---

103 Examples include ApplePay, Tencent, and Alipay.

104 PayPal offers customers the option of opening an account in which value can be stored or instead just having the customer’s other (non-Paypal) accounts directly credited or debited to facilitate payments.

105 This process is encouraged in Europe by the new payment service directive referred to as PSD2. See Committee on Payments and Market Infrastructures (“CPMI”) (2014).

106 B. Dyson (2019).

107 Generally, e-money accounts do not benefit from deposit insurance.
In the medium run, several forces nonetheless could drive a shift from account-based to token-based money:

- **Consumer preferences.** Consumers may wish to not to be “banked” anymore once they get into the habit of making payments electronically. Smartphones may fuel a growing aspiration to treat and send money in the same way that people treat and send texts or e-mails. The recent financial crisis may also have contributed to consumer preferences to reduce reliance on the banking system.

- **Financial exclusion.** Token-based money offers an easy solution for the un-banked sectors of the economy. It helps address financial exclusion in advanced economies, and allows emerging and poor countries to leapfrog some stages of financial development.

- **Integration other financial assets.** New special purpose mobile applications (Apps) will allow people to directly manage their finances on their mobile devices without the assistance or intermediation of a bank. In addition to the potential logistical capabilities of these Apps (for example, reducing or eliminating the need for paperwork, providing access to account information) they could make it possible to instantly shift value back and forth between digital money and financial portfolios, offering the possibility of using money for payments without holding a bank account. This reflects a longstanding vision of many economists, as it would allow money to exist outside the banking system as a claim directly backed by a portfolio of financial assets. The tokenization of money makes this a realistic prospect.

- **Competition with card payments.** Finally, competition between mobile payments and debit/credit cards may intensify. Mobile and cards payments are two ways to make retail payments. Both are simultaneously available in growing parts of the world. They complement each other, as cards are frequently used to easily transfer money from a bank account to a wallet (for example, to put more money in a prepaid wallet). They can also compete with each other. Both allow for near field communication (NFC) payments as cards are increasingly equipped with that technology. However, there are two major differences between mobile and card payments. Mobile allows for peer-to-peer personal payments between individuals, independent of any purchase or exchange of goods. And

---

108 See, e.g., J. Cochrane (2014). (“With today’s technology, you could buy a cup of coffee by swiping a card or tapping a cell phone, selling two dollars and fifty cents of an S&P 500 fund, and crediting the coffee seller’s two dollars and fifty cents mortgage-backed security fund. If money (reserves) are involved at all—if the transaction is not simply netted among intermediaries—reserves are held for milliseconds… [These] electronic transactions can easily be made with Treasury-backed or floating-value money-market fund shares, in which the vast majority of transactions are simply netted by the intermediary.”) This transformation was aptly and precisely envisioned by C.A.E. Goodhart (2001), who noted that “the assumption that the means of payment will be an electronic transfer, a unit of ‘e’, Individuals, and companies, will hold personal accounts consisting (mostly, possibly entirely) of capital market assets…. A payment from X to Y would involve a pre-programmed, computerised sale of some set, or sub-set of financial assets, or increase in liabilities by X and an equivalent pre-programmed investment by Y, once the ‘e’ transfer had been received on her ‘e’ purse.”
mobile allows the user to dispense with a bank account. By contrast, a card needs a bank account (unless pre-paid). The competition between the two modes of payments will therefore have some impact on the forms of money that will be used in the future.

**Network money**

Networks and money are closely linked. Money derives its value and fulfils its role by allowing a very large number of economic agents to engage in transactions together. Network effects and externalities play an essential role in establishing and maintaining a currency: broad acceptance of a currency increases its utility and naturally attracts new users.

The expansion of digital networks will have significant monetary consequences. In a digital economy, networks are evolving in several key ways that affect the potential structure and operations of the payment and money infrastructure:

- Digitalization enables the ability to copy and transfer information at very low (or zero) cost. This allows networks to potentially grow and establish themselves in a very short period of time. A currency supported by a digital network may thus be able to quickly achieve broad acceptance.

- Digital networks are not bounded by national borders. Any currency associated with a digital network is thus in effect potentially a cross-border currency.

- Digital networks tend to be organized around platforms. Platforms are defined as multi-sided markets where goods and services are provided to several distinct groups for end-users. In ordinary language, platforms are "ecosystems" within which consumers, merchants, and service providers interact. The economic logic of platforms is to create and develop complementarities and links between different activities. Money can play an important role in the business model of platforms, as a shared (form of) currency could strengthen the network effects that keep a platform functioning.

The convergence between networks, platforms, and money likely will become increasingly apparent in the digital age. Social and e-commerce networks may find it useful to develop payment services, possibly incorporating their own internal medium of exchange, to facilitate the exchange of value inside the network. Most already offer wallet applications. At the same time, payment systems in some countries are attempting to expand their network effects by aggregating other activities in the domain of e-commerce, credit, or asset management.

---


112 For example: Apple Pay, Google Wallet, and payments made through Facebook Messenger.

113 For example, Worldpay, a global payments technology provider, recently partnered with Sage Partners, a cloud business management company, to expand the range of card payment solutions...
Indeed, some payment platforms have started to establish themselves as a main contact point between large populations of consumers and merchants. In this model, the payment platform serves as an aggregator of other financial services (for example, credit scoring and asset management) and eventually other types of economic activity such as trade in goods. This dynamic is leading to the emergence of what could be called *large payment conglomerates*.

This evolution is occurring most spectacularly in China, where fintech companies such as Antfinancial and Tencent have moved aggressively into payment services and e-money. They have developed state-of-the-art mobile payment systems while simultaneously aggregating many diverse activities. This model may also expand to other parts of the world; Facebook has recently applied for a Europe-wide e-money license, while Paypal and Alibaba have requested or obtained banking licenses in China.

Given the great diversity of services offered to users, the payment networks increasingly see themselves as complete and inclusive ecosystems and consumers appear to share this view. A recent article in *The Guardian* gives a sense of the strategy of these networks, as well as the depth of their reach into diverse consumer activities:

> Analysts say it is the ubiquity of Ant in the daily lives of Chinese consumers that underpins its valuation. … ‘You can think of Ant Financial as the water, electricity, and coal in your life. Ant Financial is everywhere in your life, from daily payments, to renting a house, to renting a bicycle.’

> ‘If Facebook started a bank, that’s kind of what it feels like’…

> The company sees itself more as a ‘lifestyle platform’ on which people conduct most of their life’s transactions. From ordering food, buying movie tickets, to paying utility bills. ‘The idea is...

---

114 Ant Financial is considered the largest fintech firm in the world. The company owns Alipay, a major online payments business with 870 million active users, as well as Yu’e Bao, a 1.5 trillion RMB (approximately 216.4 billion USD) money market fund. Ant Financial reportedly is planning to add two additional money market funds. Ant Financial also offers insurance and currently has 322 billion RMB (approximately 46.5 billion USD) outstanding in consumer loans. In addition, Ant issued 258.8 billion RMB (approximately 37.3 billion USD) in consumer loan asset-backed securities in 2017. S. Hsu (2018).

115 H. Roberts (2016).

people are living their lives through this platform,' an Ant Financial spokesperson said.\textsuperscript{117}

These developments are still in their infancy and geographically limited in scope thus far. But the underlying technology supports the potential for geographic expansion, and large payment networks are already expanding into neighboring countries.

\textbf{The pre-eminence of payments}

One defining characteristic of these payments networks is that payments are the core activity for these conglomerates. The payment functionality is what keeps the network valuable and growing:

\begin{itemize}
\item For consumers, adopting the forms and modalities of payments is a condition for easy access to and use of the resources and applications available on the platform.
\item For application developers and other service providers, the existence, performance, and resilience of the payment network creates the expectation of a strong and permanent consumer base, both in the present and for the future.
\item Most importantly, the payment network has unparalleled access to data. Data are subject to economies of scope. Benefits of data possession and processing are derived not only from the size of the database but also from its diversity. This is where the advantage of payments lies: they are the common link between a broad variety of economic activities. A payment platform allows access to data that no other, more specialized platform can provide. A bank can observe its customers' payment flows, their pattern and destination. Indeed, that information is essential to assessing the creditworthiness of borrowers. Data obtained by payment platforms are much richer, as they include the object of payment and identify the beneficiary. There is also a possibility to cross check with all other activities a user undertakes. It is no surprise that techniques and activities related to scoring the behaviour of individuals have blossomed on payment platforms.
\end{itemize}

This may lead to an inversion in the current industrial organization of financial activities. At the moment, although the payment function of banks is essential and central to the functioning of the financial system, customers get payment services as a natural complement, almost an accessory, of banks' deposit-taking and credit activities. Banks are the main contact point for the customers and manage the whole client relationship in an integrated way. In many countries, this extends to the provision of insurance or asset management services. The system is "bank centric" and, to some extent, "credit centric" as symbolized in the following graph:

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{bank_centric_model.png}
\caption{Bank-Centric Model}
\label{fig:bank_centric}
\end{figure}

\textsuperscript{117} L. Kuo (2018).
In a platform- and payment-dominated financial system, that implicit hierarchy may be reversed as payment services become the main point of entry for customers. Other types of financial services, such as credit and asset management, could then become de facto accessories to payments. In this new form of industrial organization that is emerging in some countries, banks, mutual funds, and asset management companies are subsidiaries of payment systems.

**Digital currency areas**

Once a payment system establishes itself as a platform used by tens or hundreds millions of persons for all their purchases and mutual payments, network externalities develop. One important step occurs when activities are not limited to purchases and e-commerce, but participants also use the network for bilateral payments and transfers with each other.\(^{118}\)

In some respects, such a system then becomes a currency area of a new kind, one based on digital interconnectedness.\(^{119}\) Obviously, a *digital currency area* is very different from the traditional concept of optimum currency areas (OCA).\(^{120}\) However,

---

\(^{118}\) J. Gans and H. Halaburda (2013).

\(^{119}\) In a recent presentation at the Bank for International Settlements, Holmstrom discussed this concept in the context of forms of “legal tender” inside the payments network. Holmstrom (2018).

\(^{120}\) Defined as a domain within which exchange rates are not needed for macroeconomic adjustment can be dispensed of. The OCA relates to macroeconomic stabilization and money’s function as a unit.
at a fundamental level, a currency area is defined by the proximity and “ease of trade and payments” between its participants. In the OCA literature, proximity is mainly defined according to the commonality of macroeconomic shocks and factor mobility. In a digital world, a different kind of proximity emerges. The links between economic agents derive from connections within the payment network, not primarily from their geographic closeness or economic structures. Payments inside the network are easier and trading frictions are lower between members of the network compared to trade with parties outside the network. The emergence of payment links of this type could result in monetary effects. Specifically:

• price transparency is increased and price discovery becomes easier inside the network than outside;
• the larger the network, the less likely a “conversion” would be necessary to effect a transaction within the network;
• finally, there are greater incentives for everyone (both merchants and consumers) to hold liquidity balances in the form of money used inside the network. This is especially the case if and when the network’s form of money serves as a store of value (potentially through its asset management services) accessible within the same payment infrastructure.

If such digital currency areas were to develop, they would have significant effects on the structure and workings of monetary systems. In particular:

• Inside domestic economies, they could fragment the monetary area in ways that could undermine the uniformity of the currency.
• Between national economies, they could establish cross-border links of a new kind that may lead to a form of “digital dollarization” in some countries.

Overall, the combined effect of tokenization and networks has important policy implications that are examined in the following section.

II. POLICY IMPLICATIONS OF DIGITALIZATION

Implementation of monetary policy

Concerns about the impact of technology on monetary policy are nothing new. Twenty years ago, when e-money was first developed, economists and policymakers worried that advances in information technology would render Central Banks obsolete and wondered whether they could “survive the IT revolution.” Central Banks primarily draw their powers from their monopoly in issuing “base” money. At that time, it was feared that the demand for such money would diminish or disappear, making this monopoly increasingly irrelevant. It would become difficult or impossible for a Central Bank to implement monetary policy effectively if this occurred, as it

of account. The question addressed by the theory is how far can a currency extend geographically without compromising macroeconomic stability

121 R. Mundell (1961).
would lose an effective transmission mechanism. Would Central Banks become “an army with only a signal corps” as Benjamin Friedman posited, with monetary policy implemented only through press conferences and public statements? In theory, there are four reasons why technology could reduce or eliminate the demand for Central Bank money:

- Digital money could partially or totally substitute for cash, whose usage would shrink or disappear. In that case, Central Bank money would be needed less in the economy.
- If large payment networks aggregating many activities dominate the economic landscape, most transactions would be settled within those networks, rather than between them, thus bypassing Central Banks. The need for clearing balances in Central Bank money would be minimal, limited to transactions between networks.
- From a more forward-looking perspective, progresses in IT could make financial intermediaries so well informed about each other that they would be more prepared to provide credit to each other and settle net claims, reducing or eliminating the comparative advantage of Central Bank money in providing payment finality.
- Finally, any settlement that remains necessary after multilateral clearing of balances between banks and financial intermediaries could be made by direct transfers of financial assets either held in accounts by a central depository or digitally created for that purpose. The possibility to

---

123 Concerns were sufficiently important to motivate the ECB to recommend that e-money issuers be subject to reserve requirements.

124 B. Friedman (2002).

125 C.A.E. Goodhart (1989), p. 32 (“If market information improves still further, so there is complete, or near complete, information of the standing and behavior of all participants, then there is no need even for bilateral clearing of debits and credits… transactions will give rise to credit and debit balances which can be settled multilaterally without the need for monetary assets as a means of payment.”).

126 Similarly, M. Woodford (2001) notes “Improvements in information technology may well reduce the demand for central-bank balances for clearing purposes as well. ... the demand for non-zero overnight clearing balances results from uncertainty about banks’ end-of-day positions in their clearing accounts that has not yet been resolved at the time of trading in the interbank market. But such uncertainty is entirely a function of imperfect communication; were banks to have better information sooner about their payment flows, and were the interbank market more efficient at allowing trading after the information about these flows has been fully revealed, aggregate demand for overnight clearing balances would be smaller.” See, also, Woodford, “Money Information,” (XXXX) (“... since the question of finality of settlement is ultimately a question of the quality of one’s information about the accounts of the parties with whom one transacts.”).

127 See C.A.E. Goodhart (2002) (“... Perhaps the simplest way to envisage this happening is that all agents (e.g. individuals and companies) hold their financial assets, i.e. claims on other agents, with a custodian, perhaps a computer company, not necessarily a bank. The custodian simply guarantees that the asset value is there. When a transfer is made, the custodian arranges the pre-programmed set of investment sales and purchases. The custodian would run the computerized settlement system but need neither issue liabilities nor make loans, i.e. it would neither be a bank nor a Central Bank, nor a financial intermediary.”).
digitalize or “tokenize” financial assets would make them divisible and fungible and facilitate their use as instruments for settlement.  

Thus far, none of these concerns have come to fruition. Far from vanishing, there has been increasing demand for Central Bank money for payment and liquidity needs:

- Most large-value payment systems settle in Central Bank money. In particular, real-time gross settlement systems (RTGS), have become widely adopted. In RTGS, substantially more Central Bank money is required to ensure smooth payment flows because each payment must be settled separately through a direct transfer. To enable this, most Central Banks provide intraday credit in significant quantities to banks participating in these systems.  
- Liquidity provision and asset purchases by Central Banks during and after the financial crisis led to an explosion of the ratio of Central Bank money to GDP. If anything, there may be an overabundance of Central Bank money and concerns are instead expressed about the size and possible implications of Central Banks' balance sheets. Related to this, banks are actually holding reserves far in excess of their settlement needs.

What about the future? With hindsight, most of the dire predictions about the demise of Central Bank money may have been based on a restrictive vision of its role. It was assumed that so-called “high powered money” derives its key role from Central Bank money's function as the ultimate medium of exchange, the final settlement asset between banks and other financial intermediaries. Technology was perceived as a threat to Central Banks' power because it was seen as reducing—or eliminating—the need for such settlements.

The financial crisis has shown that Central Bank money is much more than just a settlement instrument. It is also a store of value and the ultimate safe asset. Banks were happy, indeed anxious, to accumulate reserves at the Central Bank to cover any potential shortage in funding. In some countries, access to the Central Bank’s balance sheet had to be broadened to accommodate increasing demand for base money.

---

128 O. Issing (1999) (“However, an important feature of the new electronic payment and settlement infrastructure is its potential ability to compress the time delay for transactions to settle to effectively zero in economic time. This creates an essentially new circumstances which has the potential to obviate many, if not all, of the types of risk normally encountered in executing payments and their settlement. In principle, this would allow a much wider array of assets, especially marketable assets, to be mobilized as transaction media.”).


132 M. King (1999) (“Because base money is the ultimate medium of exchange and of final settlement, central banks have enormous leverage over the value of transactions in the economy.”).

133 M. King (1999) (“If financial intermediaries could settle with each other in real time, then the role of central banks in providing finality of settlement would disappear.”).
The store of value function provides a very strong basis to assert the power of Central Banks. By virtue of their ability to provide (and control the supply of) that specific safe asset, Central Banks control the risk-free interest rate, and, in effect, place a floor on the whole constellation of interest rates and financial conditions in the economy. They can do this even when there is little (or no) demand for Central Bank money for transaction purposes.

It may be—although it is by no means certain—that future technologies will reduce or eliminate the demand for Central Bank money for transaction purposes. However, this should not suppress the demand for a safe and liquid asset with an infinitely elastic supply, for which there is no substitute to Central Bank money. As long as Central Banks elastically provide the ultimate safe asset in the economy, they should be able to implement monetary policy efficiently even if private money becomes dominant in providing payment services.

**A uniform currency and the unit of account**

*Conditions for a uniform currency*

Diversity between forms of money is both natural and beneficial in a market economy. Different forms of money serve different purposes. For instance, metallic coins have for a long time been “specialized” in small payments. And, until recently, checks were primarily used for larger transactions. This diversity also fosters competition between payment systems that governments have encouraged because of expected gains in efficiency.

On the other hand, authorities want to operate a “uniform” currency, as they want the different forms of money to be absolutely equivalent representations of the same unit of account. The perception of the public must be such that it uses the various forms of money interchangeably so long as they are denominated in the same currency. That property has also been called the “singleness” of money.

For singleness to be achieved and permanently maintained, there must be a link or correspondence between the different forms of money. There must be a process that permanently guarantees their equivalence, their mutual substitutability. In practice, singleness of money is achieved if and when the different forms of money are always and everywhere convertible into each other, unconditionally and at par. In effect, the same money is circulating under a multiplicity of representations.

The conditions for full and unconditional convertibility between the different forms of money can be quite demanding. This means that there should never be any friction in shifting from one form of money to another. Different forms of money should always exchange at par in unlimited quantities and there should be no gains to arbitrage from one to the other. One important implication is that there must be an infinitely elastic supply of each form of currency to accommodate any shift in relative demands.

---

134 Short-term government bonds in some countries are considered as safe as Central Bank money; however, their supply may not be as perfectly elastic.

135 Also referred to as a “uniform currency.” CPSS (2003)
Singleness, therefore, theoretically implies three different conditions:

- First, that each and every type of private money is convertible into the others;
- second, that all of them are convertible into the public money; and
- third, by extension, that all economic agents have access to public money, in one form or another.

In practice, it may not be realistic to expect that all forms of digital money will be mutually convertible into each other in unlimited quantities. All, however, should be exchangeable into public money. Ultimately, convertibility into public money is what keeps the monetary system uniform in contemporary economies.

**Technology and the risks to uniform currency**

Technology presents two main challenges to a uniform currency. First, if cash were to disappear or be marginalized, it would eliminate universal access to public money and effectively suppress the convertibility of bank deposits. Second, technological innovation has enabled the creation of a multiplicity of special purpose tokens and the creation of large payment networks that, together, could lead to a fragmentation of the monetary system.

**Marginalization or Disappearance of cash?**

A full digitalization of retail payments is today technically feasible. In addition to technology, the reduction in the role of cash is further encouraged by two forces: first, governments are adopting and implementing regulations aiming at combatting financial crime, money laundering, and the financing of terrorism; and second, the elimination of cash is a central and explicit component in the business models of large payment operators and wallet providers. Both Apple and Alibaba CEOs have made virtually identical statements to that effect in the last year, vowing to eliminate cash, which is presented as an obsolete and inefficient tool for effecting payments in a modern economy.

Cash demand varies considerably across countries according, to traditions and social habits. In some European countries such as Sweden and Denmark, electronic payments have started crowding out the use of cash. By contrast, the growth in demand for banknotes in the euro area has by far exceeded that of economic output in recent years.

---

136 This will require at least a minimal level of regulation. Today, in most (but not all) jurisdictions, it is a legal requirement for e-money issuers to redeem instantly and unconditionally in cash; in order to do so, they must hold sufficient public money to provide backing.

137 Some academics have been advocating for the elimination of cash as well; the most prominent of these is Ken Rogoff. See, e.g., K. Rogoff and D. Reisinger (2016), R. Guy (2017), and K. Rogoff (2014).

138 Data and developments taken from BIS (2018B).

139 Y. Mersch (2017).
Yet, despite continuing digitalization, cash still plays a significant, in fact increasing, role in most countries. Even as its use as a means of payment is declining, cash is increasingly becoming a store of value. The total amount of cash in circulation continues to rise in proportion of national GDPs. Over the last decade, the demand for large-denomination notes has outpaced that for smaller denominations (although this varies greatly across countries). Looking at data, therefore, “reports of the death of cash seem greatly exaggerated.”

On the other hand, the penetration of mobile money is only starting. In many countries, a dynamic is developing where consumers’ tastes interact with merchants’ incentives to reduce or eliminate cash payments. Such developments tend to be mutually reinforcing and accelerate over time, with possible snowball effects or sudden shifts and discontinuities. Existing data and trends thus may not be good predictors of the future.

The perspective of a cashless society is not a fiction anymore. In parts of the world, both emerging and advanced, it has become increasingly difficult for the public to pay in cash or even obtain cash from banks. China has moved increasingly toward being a cashless society. Many bank branches in Sweden have become cashless.

This evolution has prompted reactions from authorities in different parts of the world. In July 2018, the People’s Bank of China warned against the dangers of a cashless society. More recently, the City of Philadelphia has announced a policy sanctioning merchants for refusing to accept payments in cash.

If cash were to disappear, it would truly be an “historic event” with many consequences, as the Swedish Riksbank has stated. It is useful, therefore, to consider the hypothetical case of an economy without cash and the consequences that would result. Some of those effects would materialize even in the case where cash subsists with a very limited and reduced role.

First, the general public would be completely dependent on a third party to effect any payment. This would have important consequences for the structure of the payment system and issues such as the fight against cyber-crime. The need for emergency backups (with associated costs) also would have to be thoroughly explored, especially in the case of natural catastrophes. In some countries exposed to recurrent natural disasters, citizens are advised by authorities to always keep a certain amount of cash on hand in case payment services are disrupted for a long time. In the absence of appropriate emergency backups, a cashless society would be

---

140 It is likely that low interest rates are a temporary factor that reduce the opportunity cost of holding cash.
143 M. Savage (2019).
144 A. Lee (2018).
exposed to significant operational risks, with potential economic and social costs if a disaster were to occur.

Second, direct peer-to-peer payments would disappear as long as money remains account based, even for very small, day-to-day payments and expenses. Anonymity would also disappear in such a system. Anonymity, of course, is often associated with tax evasion or other criminal activity. But anonymity also guarantees some privacy. The shift to fully digitalized payments therefore may not be neutral from a societal perspective. More broadly, payments users may value their freedom of choice; this is consistent with the current diversity of payment instruments and their and coexistence over long periods, as well as different payment habits in different countries.

Third, in many countries a significant share of the overall population remains “unbanked,” even in advanced economies. That population would find itself almost excluded from all economic and social activities in a cashless society.

Finally, and most relevant to the focus of this report, citizens would no longer have access to public money directly backed by the authorities. They will not be able to hold Central Bank money, which is the only form of public money they currently can use. Access to Central Bank money would exist only in the form of banks’ reserves, crucial but invisible and inaccessible to individuals. There would in effect no longer be a functional legal tender, with the operation of the monetary system turned over to private entities. It is worth exploring the implications of this change in more depth.

One implication of this change is that money would no longer be a physical manifestation of sovereign authority, which may have some political and economic consequences. Citizens would no longer have any visible symbol linking money to the authorities and to the Central Bank. Symbols are important for money, as illustrated by the debates around the Euro banknotes when the single currency was created. Connecting the Central Bank to money might be important for the effectiveness of Central Bank’s communication. Even crypto currencies, the most dematerialized of all, feel the need for some visual representation and have their own logos in the form of what are essentially circular coins.

A second implication is more fundamental. Without Central Bank-issued currency, the general public would no longer be able to convert private money into public money, because there would be nothing to convert into. Bank (deposit) money, although private, is generally stable because it is convertible into public money and

---


148 See, for example, J. Nicolaisen (2017B) (“We may not be entirely comfortable with the thought that every purchase we make is recorded. It may be too reminiscent of the society described in George Orwell’s 70-year-old novel 1984.”); and C.A.E Goodhart (2002), p. 15 (“The one circumstance where one might, indeed, expect information technology to bring an end to the use of national currency would be when an (authoritarian) government might prescribe that all transactions must go through an electronic device. It is not hard to imagine the advantages that a government might envisage from being able to record (electronically) every payment that every agent in that country made. This is a perfectly feasible Orwellian nightmare.”).

this convertibility is frequently supported by deposit insurance. It is impossible to predict how the monetary system would behave over the long run if private money were no longer convertible into public money given that it can no longer be converted into cash.

A fragmentation of the monetary system?

Technology has the potential to segment domestic monetary systems across both technical and economic dimensions.

Technical fragmentation could de facto prevail if different payment systems (and associated tokens) are not fully interoperable. This is the current situation in China between the two main e-money networks.

Technology could lead to fragmentation in many other ways. There is great interest on the part of financial institutions and other corporates in dedicated payment systems working with special purpose tokens. For instance, participants in the interbank market in some countries are exploring transactions involving tokens that represent reserves at the Central Bank. This may be the beginning of a trend. In a digitalized economy, “there is now a computer in the middle of each transaction.”¹⁵⁰ Many computer-mediated transactions involve the transfer of value. The token form of money allows for instant settlement, with no counterparty risk. It is especially well-suited when exchange and payments take place between machines and are regulated by algorithms, when “real time” may be measured in milliseconds. Depending on their business needs, participants may wish to use special forms of tokens, possibly denominated in specific unit of accounts.

Consequences of a fragmented monetary system

In a fragmented monetary system, different types of currency become imperfect substitutes, despite being denominated in the same unit of account. Because frictionless arbitrage would not be possible between different forms of money, each would carry a specific and idiosyncratic risk that would necessarily be reflected in the price at which they trade. As a result, “exchange rates” would arise between different types of domestic money.¹⁵¹ In effect, the monetary system would be transformed and behave more like the broader financial system where the creditworthiness of every single instrument is constantly re-assessed and priced. The likely result would be greater fragility, with the possibility of liquidity crises and periodic runs on some forms of currencies if doubts about their issuers emerge.

These effects would be compounded if cash were to disappear with no clear replacement. Modern deposit money, while private, is generally stable because it is convertible into public money (and this convertibility is frequently supported by deposit insurance). Once private money ceases to be unconditionally convertible into public money, it becomes something different: a liquid but less safe claim whose

value ultimately depends on the issuer’s creditworthiness. The monetary system in effect becomes fragmented between different categories of issuers.

The unit of account

In a fragmented monetary system, money may be destabilized in its role as a unit of account.\textsuperscript{152} This was a real source of concern when e-money was introduced. Friedman and Schwartz (1986) raised whether:

\[\text{In the absence of legal obstacles, can, should, and would the unit of account be separated in practice from the medium of exchange function in the belief that financial innovation will render outside money unnecessary and obsolete.}\]

Issing (1999) raised this concern more precisely:

\[\text{Central Banks and governments will be confronted with a very specific problem of pivotal significance: can the unit of account be separated from the means of payment, while still remaining a viable unit of account and playing the crucial role of providing the common money language for the whole economy?}\]

The underlying fear was that form would drive the substance, as a new means of payments would progressively push economic agents to count and price in different units. Whether this would happen is largely a matter of conjecture. As noted by Buiter (2014), there is no accepted theory on what determines the unit of account in a market economy. Economic theory generally assumes that social behaviours are such that the unit of account emerges naturally from the medium of exchange. Historical examples of divergence between the medium of exchange and unit of account have been very localized or temporary.

Authorities have many ways to impose or consolidate the unit of account by deciding which currency serves as legal tender and in which currency taxes have to be paid and public contracts will be denominated. Ultimately, however, the authorities cannot prevent economic agents from contracting in the unit of account of their choice, at

\textsuperscript{152} “Singleness” seems to be a necessary (but not by itself sufficient) condition for a currency to effectively become “the” measure of economic value, or the unit of account, shared by members of a modern economy, with the associated advantages of efficiency and safety in trade. See CPSS (2003).
their own risk. However, how those agents would behave in a technologically different environment without singleness of money is a matter of some uncertainty.

However, if the unit of account is “weak,” it may be progressively displaced in agents’ calculations and behaviour, depending on the strength of social conventions and habits. These may be abruptly shaken by a technology shock or a generational change. The effects of such a shock could be amplified if there was a major change in the monetary architecture such as the reduction or elimination of all forms of public money in the hands of the general public.

Cross border effects also may be significant. Within large networks, the same digital instruments of payments may easily be used in several jurisdictions. If so, they may have the effect of promoting the use of a specific unit of account outside of the country where it has legal tender.

Given the fragmentation risks that would result from the multiplication in the digital forms of money, the rise of payment networks, and the disappearance of cash, it makes sense for Central Banks and governments to think about possible alternatives in the digital era. Could a CBDC be issued and serve as a public money generally available in the long run if and when the risks of monetary fragmentation materialize?

**CBDC as “digital cash”**

The case for a CBDC can be stated in very simple terms: in a highly digitalized economy, a CBDC is necessary to preserve and guarantee universal access to public money, which in turn may be essential to protect the uniformity of the currency and its role as a unit of account.

Depending on countries and circumstances, CBDC also offers other potential benefits. It helps financial inclusion if a part of the population is unbanked. For some

---

153 According to W. Buiter (2014), “[t]he unit of account that matters for private decision makers and is used to record transactions among private parties is decided by them alone. Nothing in the primitive assumptions of conventional (unboundedly rational) optimising economic theory (preferences, information, technology, endowments) implies that the private unit of account—the unit of account used for private calculation and computation and for recording contracts between private parties—be defined in terms of the liabilities of the central bank or in terms of the media of exchange or means of payment widely used in the economy.”

154 L.H. White (1984), p. 703, notes that “[i]t remains to be considered whether economic agents in an unregulated world without a central auctioneer would be likely to converge on use of a unit of account that is not a unit of outside currency.”

155 K. Rogoff (2014), p. 8, argues that “it is important to acknowledge that there is a least an outside risk that if the government is too abrupt is abandoning a century-old social convention, it will destabilize inflation expectations, introduce a risk premium into bond pricing, and generally induce unexpected macroeconomic instabilities.”

156 An interesting albeit more theoretical question relates to the pricing of government bonds in a cashless world. They cannot be, as today, redeemable into public money, because there is no such money available to the general public in a cashless society. They can only be redeemed against other public or private bonds, or in private money, creating some circularity and risk in the pricing. “This clearly would make bond pricing much more difficult than it is in our world.” L. H. White (1984), p. 710.
countries, it constitutes a defense against digital monetary competition from abroad. Overall, it provides the public with a form of money in line with their preferences, which is generally considered as part of Central Banks' missions.

While the case seems simple, the debate surrounding CBDC has been complicated by the introduction of a set of three interrelated arguments.

**Monetary Policy Implications**

“Economists for centuries have dreamed of interest paying money.” The electronic form of CBDC makes it technically feasible to pay interest on the currency, including a negative interest rate. This could enhance the transmission mechanism of monetary policy and increase its efficiency. The benefits would be especially important if and when monetary policy was to hit the zero lower bound, a scenario that is more likely if equilibrium interest rates are projected to stay low for a long period of time. The gains, in terms of absorbing shocks and stabilizing the economic cycle could be substantial.

However, such a change would raise questions of political acceptability. It would likely be controversial for Central Banks to take advantage of technological evolution to change the nature of money in a way that the general public might find objectionable. The success of such a policy also would depend on the total disappearance of cash. Otherwise, the same arbitrage toward physical currency that currently prevents negative interest rates on money would still take place.

**Financial Stability**

A CBDC would provide the public with an attractive alternative to bank deposits, especially if it carried interest. In ordinary times, the possibility of instant arbitrage towards the CBDC may force banks to pay more interest on their deposits. This could destabilize their funding structure which, in turn, could impede credit in the long run. In times of banking system stress, a CBDC would make it much easier to run from deposits into Central Bank money. Overall, a CBDC could thus contribute to the disintermediation of banks, which would have a major, potentially negative, impact on the functioning of the financial system.

It is true that a CBDC technically would make runs easier and this argument deserves careful consideration. However, it should not prevent the creation of CBDCs. While runs might occur more easily, that does not necessarily mean that they would be more frequent. Some runs are specific to a bank, as depositors shift their money from one account to another at a different bank, which is increasingly done online. That type of run would not be affected by a CBDC. Another type of run affects all banks, when there is a general loss of confidence in the banking system. In that case, CBDC would offer the natural exit. But what is the alternative in a digitized monetary system? Without CBDC and without cash, people would have nowhere to

---

159 B. Coeuré (2019).
run. In effect, the convertibility of deposits would have been suspended. If the Central Bank wants to maintain convertibility, runs must be allowed to occur. While the system must be constructed in such a way that runs are unlikely, it should not make them technically impossible.\textsuperscript{160}

\textit{Narrow Banking}

Finally, a third and related strand of argument supports the creation of a CBDC precisely because it would disintermediate banks. Proponents of “narrow banking” and the “Chicago Plan” from the 1930s view the power of private banks to create deposit money as a major source of financial instability and the cause of many crises.\textsuperscript{161} In addition, the dominant role of banks in payments creates an obligation for Central Banks or other supervisory authorities to rescue them when they are in trouble. From this perspective, a CBDC that would force banks to look for alternative sources of funding, get them out of payments, and submit them to market discipline would result in a very positive transformation.\textsuperscript{162} While motivated by different reasons, proponents of “Sovereign money” also advocate a monetary system where private bank deposits would disappear as a form of money and payment instruments would be issued by the State or fully backed by government bonds.\textsuperscript{163}

\textit{CBDC as a form of digital cash}

Once all these arguments and considerations are factored in, the debate regarding the introduction of a CBDC becomes extremely complicated. However, these complexities are primarily driven by issues that only appear when a CBDC is conceived and constructed as a perfect substitute for bank deposits that (1) pays interest and (2) is account based.\textsuperscript{164}

But this need not be the case. CBDC can be designed differently, as “digital cash” with the objective of mimicking almost all the characteristics of cash and serving not as a substitute but as a complement to bank deposits. Such a CDBC would have two main attributes: first, it would not pay interest under any circumstances; and second, it would not be account based but would come in tokenized form (or according to

\textsuperscript{160} It should be also noted that the impact on banks of any shift from deposits to CBDC can be compensated by additional refinancing from the Central Bank. A permanent increase in reliance on Central Bank funding would not, however, be a positive development.

\textsuperscript{161} J. Benes and M. Kumhof (2012).

\textsuperscript{162} For a recent exposition of this view, see R. Moghadam (2018) (“a system where a central bank provides payment services while banks focus on credit is more stable. It removes banks’ capacity to fund loans simply by issuing deposits and relying on borrowing to cover unexpected outflows. This should reduce the incidence of bank crises and taxpayer-funded bailouts in the name of rescuing the payments system.”).

\textsuperscript{163} B. Dyson, G. Hodgson, and F. van Lerven (2016).

\textsuperscript{164} Opening and holding accounts for the general public would generally not be considered a core competency for most Central Banks, as retail banking is not their normal habitat. They have no comparative advantage in managing account relationships with individuals. As a result, this could expose them to some compliance and reputational risk should they open accounts to individual citizens. See CPMI (2018).
terminology that is occasionally used, be “value based”). It would also be provided elastically so as to be permanently convertible into deposits and vice versa at a rate of 1 to 1. While the technology for issuing such a currency is not fully available today and the general public would need to have electronic wallets, the hurdles to such an approach seem relatively low compared to other possible models for CBDC.

The introduction of CBDC may become necessary to preserve a uniform currency if cash is marginalized and/or special purpose electronic money develops. Central Banks should therefore prepare for the possibility of issuing CBDC and ensure that doing so is technologically feasible. From this perspective, CBDC should be as neutral as possible in terms of any broader objectives. It should not seek to change monetary policy, nor aim to overhaul financial intermediation and move to narrow banking. It may be that greater fluidity between private and public money would change the business environment of banks and make runs easier (though not necessarily more frequent). Some of these effects can be dealt with by adjusting liquidity provision mechanisms.

**Anonymity and CBDC**

Important choices would have to be made on broader societal issues relating to traceability and anonymity of CBDC. A cash payment is not traceable and fully anonymous. A digital payment is always traceable—the tokens must be recorded in a ledger. The same would be true for any CDBC. However, traceability and anonymity are different concepts. Transactions with a CBDC could be made anonymous through appropriate technical safeguards and robust governance systems.

Should access to public money in the digital age be conditional on losing anonymity? These are major policy choices and are deeply political in nature: How should a society balance privacy rights with the extent to which the information in a CBDC could be used to fight terrorism and economic crime? Such choices, of course, are not specific to money. The use of data and the protection of privacy raise difficult trade-offs in a great number of activities. However, they have a specific resonance for money. On the one hand, contrary to many other activities, the use of money cannot be avoided. On the other hand, the negative externalities of anonymity in money—money laundering, tax evasion, and financing of terrorism—are large and well-defined.

---

165 See Y. Mersch (2017).

166 C.M. Kahn (2018) indicates that a specific token could be created for each transaction, with the identity of the owner attached to it and destroyed when a payment is made, with a new token then being created with a new identity.

167 See, e.g., F. Panetta (2018), p. 9 (“Just who should decide on the degree of anonymity associated with the use of a CBDC? Clearly, this is more than just a technical issue, and as such, the choice does not belong to central banks alone but also to the political sphere. We need to think carefully, right now, about how to make the introduction of a CBDC fully compatible with the rights of individuals and about how to square the increasing availability of information on the private lives of each one of us in relation to our political views, state of health, or sexual orientation, with the protection of our personal freedom and with the rules that govern the functioning of a modern liberal democracy.”).

III. NEW PRIVATE CURRENCIES

As early as 2012, analysts and commentators raised the possibility that an existing global network could decide to create its own money, denominated in its own unit of account, and thus effectively compete with existing official currencies. In 2010, after Facebook introduced the Facebook Credit, one analyst asked “[c]ould a gigantic non sovereign like Facebook someday launch a real currency to compete with the dollar, euro, yen and the like?”\textsuperscript{169} Another analyst noted that “[i]n some countries (especially those with national debts that are greater than their GDPs) Facebook Credits could become a safer currency than the national currency.”\textsuperscript{170} As discussed in Part I of this report, it is also possible that some crypto currencies could adopt more functional architectures and improved governance, and thus emerge as more viable competitors to official currencies.

This section of the report discusses the possibility of such scenarios, the reasons why currency competition could happen, and the challenges this could pose for the issuers.

\textit{Currency competition}

Economists have long been divided on the benefits and costs of currency competition. Some of them, in the tradition of Hayek, want to “denationalize” money and establish a monetary system based on the permanent competition of several private currencies that would discipline governments in the issuance of money. Many current advocates of crypto currencies belong to this school of thought.

Most economists, however, doubt the micro- and macroeconomic benefits of competition in the currency domain. On the micro level, currency competition would complicate price discovery. The coexistence of several units of accounts would increase the transaction and information costs associated with price comparisons. The final outcome of the competition process would be uncertain, as network externalities would make switching between currencies costly, create advantages for the incumbent, and act as a brake on effective competition.\textsuperscript{171} In the end, competition in the unit of account could lead to the emergence of a single issuer who would face a similar incentive structure to a government monopoly, although it would potentially be acting for its own benefit, rather than for the benefit of a country’s citizens.\textsuperscript{172}

On the macro level, it is often argued that money is a public good, where the unit of account is the common language of economic agents.\textsuperscript{173} Given that the provision of money is fraught with peculiar market failures, this has led to the argument that the government should have a monopoly in the supply and control of the stock of circulating currency.\textsuperscript{174} Whether this balance between the costs and benefits of

\textsuperscript{169} M. Yglesias (2012).
\textsuperscript{171} O. Issing (1999).
\textsuperscript{172} S. Schmitz (2001).
\textsuperscript{173} O. Issing (1999).
\textsuperscript{174} M. Friedman and A. Schwartz (1986).
currency competition would shift with technological change is certainly a matter for further research. For example, it is possible that price discovery will continue to become easier with Apps, making currency competition easier as well.

**Platform currencies?**

Regardless of the theoretical debate, the emergence of some form of new private digital currency has become a real possibility.\(^{175}\) One can think of several possible scenarios. Crypto currencies could evolve into different, more centralized, architectures. Or existing payments instruments or special purpose currencies could transition towards new, fully fledged currencies. Special purpose payment instruments have existed for many years (for instance, the Oyster card for London public transit). They have made episodic or lasting appearances in some parts of the digital economy, starting with video games but also for dedicated applications.

Up to now, “platform currencies,”\(^{176}\) as well as those developed for games are deliberately limited in their usage and are not convertible into official monies (at any price).\(^{177}\) They can only be used to effect purchases of goods and services available inside the network, but not to execute payments and transfers between persons in the network. Sometimes there is an explicit prohibition on trading the currency outside the game or the platform. This has not, however, prevented a black market from arising. There are cases when these platform currencies have in fact served to settle bilateral balances and have already been used as means of payment outside their own platforms. This the logic of the development of a new money. As it is increasingly used for certain payments, it gains “value” and begins to be perceived as a store of value and ultimately is used as a medium of exchange.

If existing limitations on the platform currencies’ use were removed, some could develop into fully-fledged private digital currencies. The real shift would come when they are not only used to make purchases on the platform but also to effect transfers and payments between members, including for settling transactions that took place outside the network. That movement outside the platform may, or may not, result from issuers’ decisions. While that could occur if an issuer removes existing limitations on the use of its platform currency, one cannot exclude the possibility that a special purpose currency involuntarily could gain status as a fully-fledged store of value and unit of account, at least in some jurisdictions.

The central banking community is aware of the possibility of such a scenario occurring. For example, the Committee for Payments and Market Infrastructure (CPMI) of the Bank for International Settlements (BIS) noted:

---

\(^{175}\) For the sake of reasoning, it is assumed that no regulatory action is taken to prevent or help the development. It is obvious that most, if not all, Sovereigns could impose and enforce a regulation and prohibition of private currencies in their jurisdictions (at the cost, maybe, of intrusive measures, such as capital controls).

\(^{176}\) Examples of such platform currencies are Amazon Coins or Facebook Credits. This term was coined by J. Gans and H. Halaburda (2013).

\(^{177}\) The exception to this is the Linden Dollar.
Social networks and online gaming have created various new payment needs, often for use within a limited ecosystem. Traditional payment products may not efficiently meet these payment needs, leading to the development of new products such as Amazon Coin, Facebook Credit (now discontinued) and the Linden Dollar. While the use of such products is currently still restricted to their respective ecosystems, it is conceivable that some of them may develop into more widely used payment services, as PayPal did. Moreover, non-proprietary forms of such alternative payment products have appeared, notably Bitcoin.\footnote{CPMI (2014), p. 16.}

Similarly, a European Central Bank working paper discussed the emergence of a platform currency:

A major internet company could decide to issue a centralised [virtual currency scheme or] VCS to facilitate payments on its platform or “community.” These could be payments for digital content, e.g. a newly released song, an exclusive video, a high-quality media article, a new level within a game, etc. Once a couple of hundred million users keep a small balance of VCS units, they could also start using these for payments for real goods and services or for person-to-person payments.\footnote{ECB (2015), p. 44.}

**Network and currency acceptance**

Private currencies could emerge on networks today more easily than in the past for two main reasons.

First, they could rapidly gain broad acceptance if supported by large cross-border (social and commercial) networks, which connect hundreds of millions of people. Historically, gaining acceptance has been a major challenge for new currencies. Prior to electronic communication and the Internet, geographical distances were powerful obstacles to the diffusion of any new currency. This not the case anymore. Network effects and externalities will take effect in full force with no delay. Inside an existing social or commercial network, any user of a new monetary unit would have instant access to tens of millions of potential counterparties, a population the size of many economies.

Second, technology makes it easier and less costly to switch from one currency to another. Switching costs were traditionally seen as a major obstacle to currency competition.\footnote{ECB (2015), p. 44.} For that reason, new private currencies in the past could only emerge if existing public money were very poorly managed. Switching would only occur “in cases of profound distrust of authorities and deeply compromised sovereign
currencies... When currency substitution has occurred naturally it's almost always done so only after the incumbent currency has been debauched by hyperinflation.\footnote{Switches do very occasionally happen: degrade a currency sufficiently, via hyperinflation and collapse of the banking system, and people will eventually look for alternatives.\footnote{See, B. Broadbent (2016), p. 3.}} Even in that case, rather than flee to entirely new currencies, most people would try and switch to other existing and trusted forms of money, such as foreign sovereign currencies. This behaviour underpins the “dollarization” phenomenon that has occurred frequently in countries where the currency suffers from insufficient credibility.

However, current technological conditions may change the reasoning.

Switching costs are lower in a digital economy. Programs will help manage the currency transformation and risks from a mobile device. Existing and future applications will allow for easy and instant computation of relative prices and conversion of monetary balances from one currency to another as well as automatic arbitrage. This will eliminate some of the frictions that arise from having different units of account. As a result, the coordination effects of a single unit of account may be less important.

The incentives to switch may also be stronger given technological change. In the future, competition between currencies may not be solely driven by their performance as a store of value. Other elements might be dominant, such as the convenience gained by participation in a comprehensive ecosystem of trade and exchange with easy access to what seems to be an infinite number and variety of goods, services and people.

The remainder of this section will discuss two major challenges facing private issuers of new monies: first, over issuance, which may prove easier to solve than in the past due to technological progress; and second, the question of backing, which may prove more difficult.

**The “over-issuance” problem**\footnote{Should a large social or e-commerce network decide to issue its own money, it has to set a procedure to allocate any newly created money units between participants. In contemporary fiat systems, money is created through bank credit and therefore is initially allocated to the beneficiaries of loans. In a network, allocation could take the form of “bonuses” or “gifts” to the participants, winnings in games, or regular allocations for those active in the network (like miles for frequent flier programs for airline companies). The network currency could also be made available through conversion from official currencies. The exchange rate for this conversion, whether fixed or floating, would determine how much currency is issued.\footnote{Crypto currencies using a proof of work protocol are an exception.}}

A second, fundamental characteristic of currencies is their issuance regime.

Money has value and is (almost) costless to produce, especially if it is in a dematerialized form.\footnote{Money has value and is (almost) costless to produce, especially if it is in a dematerialized form. It generates seignorage. There is thus a natural incentive for both public and private issuers to produce more of it. One may think that the issuer would take a long-term perspective} Issuing currency is therefore profitable. It generates seignorage. There is thus a natural incentive for both public and private issuers to produce more of it. One may think that the issuer would take a long-term perspective
and maximize its profits over a long horizon. That would imply restricting itself to moderate issuance in order to ensure the acceptance of the currency. But once a currency is established and accepted, the issuer may always be tempted to produce an “inflation surprise” and reap an instant benefit from a sudden surge in issuance. However, people are rational and will expect this to happen. When those expectations form, nobody wants to hold the currency anymore and its value diminishes, or even collapses to zero. All issuers of fiat currencies face this “over-issuance” problem driven by dynamic inconsistency between an issuer’s incentives over time.\(^\text{184}\)

Governments have ways to deal with the problem. They can induce or force the general public to use the currency if it is legal tender or through various instruments of financial repression. Alternatively, they can ensure the credibility of the issuance regime by establishing institutions or rules that constrain issuance.

Private issuers in particular face specific challenges in this regard. They have an incentive to issue currency in greater quantities than appropriate and, because people are aware of this, it is very difficult for a private currency to establish credible issuance regimes. For that reason, private currencies are inherently fragile and unstable.

In the future, technology may help to alleviate this dilemma and solve the over issuance problem for private currencies. Stability can be established if the private issuer can credibly submit itself to a transparent rule, implemented by an algorithm.

Submitting monetary policy to a rule has for long been considered an effective way to establish credibility. It is still frequently advocated as the best solution to the problem of dynamic inconsistency in the context of monetary policy. The strongest objection to a rule-based monetary policy is that it is too rigid, as it seems impossible to fit the complexity of decision making in the real world. Indeed, most of the rules that have been proposed or considered are very simple in nature. For example, the Friedman rule prescribes a constant growth rate of the money supply, while the Taylor rule determines the policy interest rate as a simple function of the output and inflation gaps.\(^\text{185}\)

With the development of artificial intelligence, it is conceivable that algorithms can be devised in the not too distant future that would reproduce the complex process leading to a monetary policy decision for a private currency. Credibility then could be ensured by making the program open, transparent, and public, as well as adopting governance rules that would strictly limit or prohibit changes and human intervention. This institutional setting would guarantee the public that the issuer would not attempt to over issue the currency with the objective to maximize seignorage.

It should be easier for some private issuers to constrain their behavior, at least initially, because maximizing profit from money issuance may not be their primary

\(^{184}\) Indeed, the essential argument of Hayek in promoting currency competition is that it would penalize over issuance (by private or public entities).

\(^{185}\) Simplicity is considered to be an advantage by promoters of these rules as it helps to anchor expectations.
business objective. The function of a native currency in the business model of a large network is mainly to enhance the attractiveness of other activities, reinforce their complementarities, and cement the cohesiveness and inclusiveness of the ecosystem that develops around the platform.

**The question of backing**

Based on a large network and limited to its payment function, a private currency could conceivably establish itself as a reliable alternative to official monies. However, the evolution might and will not stop there. A fully developed currency is not restricted to payments. If successful, it will also become a store of value—especially if it is accessible to citizens of countries where the monetary regime is fragile. It may be equally difficult to prevent the deployment of credit and maturity transformation inside its own monetary system. Credit already exists, in many forms, for some crypto currencies.

Once those evolutions take place, the issuing entity would be confronted with a host of new challenges and difficulties. If a dematerialized currency is used for purposes other than transactions, demand for the currency will be driven by very different motives and dynamics. Depending on their expectations and risk appetite, people may want to hold more or less money as a store of value. They may also want to exchange it for other currencies (or the reverse). This “speculative” motive becomes important in driving the value of the currency. This creates the possibility of many different equilibria emerging: some where there is confidence in the currency and some where there is not. How those changes in demand are accommodated will determine the behavior of the currency. It may not be sufficient to have a stable and predictable issuance regime. The issuer instead will be facing two very difficult and interrelated choices: will it take (explicit or implicit) responsibility for maintaining some level of financial stability inside the system? And will it take (explicit or implicit) responsibility for stabilizing the value of the currency—its exchange rate—vis à vis official currencies?

The conventional wisdom would advocate ambiguity, which in most circumstances would imply that the market for the currency would be left to find its own equilibrium. Most issuers will likely let the exchange rate float with the hope that volatility will be limited if there is wide acceptance of the private currency and mitigated by easy conversion back and forth with the official currency.

However, self-fulfilling expectations about the future value of money can create instability. Too much volatility may compromise the use and role of the currency as medium of exchange, especially, if participants in the network have their income, assets, and debts denominated in other (official) currencies.

For those reasons, issuers cannot exclude intervention under any circumstances, as this could lead to a higher and permanent level of volatility. Even, if an issuer makes

---

186 In the following paragraphs, it is assumed that “private network” money is token based, with no accounts in the name of holders, and no claim on the issuing entity; it is therefore considered “outside money.”

187 Assuming that, by then, the authorities have not stepped in to impose regulatory oversight.
no firm and specific commitment to stabilize the market, it will want to keep the option to provide and withdraw liquidity and/or support the exchange rate. For this to be an option, there has to be an elastic supply of the currency—with the consequence that the issuer has to be able to exchange money for other real or financial resources. This raises the question of backing.

“Backing” means that the currency must be redeemable, at least in some proportion, into real or financial assets. In the case of a private currency, those assets must obviously be denominated in another money. Backing is necessary to withdraw money (by selling other assets through so called open market operations). It is also is necessary to stabilize the exchange rate (by selling official currencies if necessary). Because it is vulnerable to episodes of depreciation and crises of confidence, the stabilization of any immaterial currency may require some commitment of real resources.

For sovereign currencies, fiscal backing is generally assumed to exist in some way. The government has the power to tax and therefore to mobilize real resources in the future, should redemption become necessary. Economists have long been interested in how much fiscal backing was necessary to stabilize a currency and prevent a collapse in confidence. In two important articles, Obstfeld and Rogoff present a model where an (infinitely) small backing is sufficient to ensure that demand for a currency will be maintained and a run that would lead to a collapse of the currency’s value to zero is excluded. As long as a currency unit can be redeemed for an (arbitrarily) small amount of real resources, households will keep using and holding it for its transaction utility. The argument assumes that households are rational enough to see that the currency can never collapse in the future; as a result, they have no motive to stop using it today, taking into account its benefits for trade. Importantly, the model also assumes the currency is legal tender. Recent research refines this analysis by showing that the government does not have to commit to any specific course of action: backing is credible as long as fiscal policy keeps sufficient flexibility for the future.

Overall, the perspective and efficacy of fiscal backing remains uncertain. But that ambiguity plays into the hands of the Sovereign: together with legal tender, fiscal backing helps to anchor expectations, eliminate multiple equilibria, and stabilize the currency.

For a private issuer, the reverse may be true, as uncertainty and ambiguity may be destabilizing. A private issuer has no power to tax or designate currency as legal tender beyond its use in its network. The amount of backing that it could potentially

---

188 In those situations, management by algorithm may not be possible anymore.
189 The concept refers either to the necessity for fiscal policy to be broadly consistent with monetary policy or, more narrowly, for the fiscal authority to stand ready to redeem the fiat currency. We refer here to this second interpretation.
191 M. Obstfeld and K. Rogoff (2017) note “the implausibility of a sudden rejection of a widely used – and backed – currency for no reason whatsoever.”
mobilize would be assessed in relation to its own resources. It could be argued that large corporations have balance sheets that are sufficiently strong to provide backing. Indeed, some potential issuers have net assets that are higher—by an order of magnitude—than the resources available to many small- and medium-size countries (as measured, for instance, by the discounted value of their expected tax revenues). One might therefore think that these companies could easily provide backing.

However, the issuer would have to determine whether it is beneficial to commit part of its balance sheet, explicitly or implicitly, for the purpose of backing the currency. If the issuer does so, backing would affect their own solvency or, at least, the perception of this solvency by outside investors.

Overall, the business case for or against backing a currency might be very complex:

- On the plus side, there are benefits in creating strong complementarities and externalities with existing lines of business and perhaps reaping some form of seignorage.
- On the negative side, the perceived necessity of backing would transform part of the money issued into a liability of the company. The question then becomes the assessment of the underlying commitment. If it is limited ex ante, there will always be a possibility of a run on the currency (based on the same logic as a run on a country's foreign exchange reserves when they are perceived as limited). If there is ambiguity, equity and debt markets will assess the potential impact of the implicit backing on the issuer’s net worth. Depending on that assessment (what proportion is considered as liability) equity values could be negatively affected. It is not difficult to imagine the possibility of strong feedback loops, either positive or negative, between the sentiment about the currency, its exchange rate, and the issuer’s stock price.

Running a monetary balance sheet is very different from running an “ordinary” corporate balance sheet. Irrespective of (almost certain) regulatory and supervisory intrusion, the issuer of a private currency would expose itself to a very different set of risks and volatility factors than those faced by other private corporations. Runs do not occur on industrial or service companies, but do occur on entities which, one way or another, issue liabilities that have a monetary character. These constraints do not necessarily make the issuance of a private currency impossible, but they do make it very demanding.

---

193 An analogy can be made with defined benefits pension funds, as underfunding, if any, is generally considered as a potential liability of the company.
CONCLUSION

Over the last eighteen months, numerous policy makers, including major Central Bankers, have given speeches on “the future of money.” This contrasts with the previous three decades, when “as economics has become more and more sophisticated, it has had less and less to say about money.”

Technology is responsible for this shift in interest and emphasis. It is hard to say, at this stage of the transition towards digital money, whether it will lead to a reassessment of some tenets of monetary theory and policy. It certainly confronts Central Banks and, more generally, public authorities, with new challenges. They will have to decide on the extent to which they want to adapt to or regulate new forms of money.

From a payment perspective, the process is fast and most likely will be disruptive for the business models of banks and the structure of financial intermediation and services.

From a monetary perspective, digitalization creates the possibility of increased currency competition. Whether such competition materializes will depend on regulation and, more generally, the interaction between public policy, private attitudes, and technology. Currency competition could develop across three dimensions:

- Between private mediums of exchange. This is already happening and may change the equilibrium between private and public forms of money.

- Between private and public units of accounts. This evolution is more uncertain and speculative but cannot be ruled out.

- Between different national currencies, due to the cross-border nature of networks. Not all countries are equally affected by current technological changes or equally exposed to such competition. Digitalization may serve as a vehicle for the internationalization of some currencies. It may help them to quickly gain international acceptance and status. And, symmetrically, other countries may be exposed to new forms of “digital dollarization,” depending on their monetary regimes, the openness of their capital account, and their regulation of payments and the internet.

Over time, as it transforms domestic monetary systems, technology may reshape international monetary relations and the international monetary system as well.

---

REFERENCES


International Center for Monetary and Banking Studies: Geneva Reports on the World Economy.


CryptoCurrency Facts. “What is a Cryptocurrency Token?,” Available at: https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-token/

Crypto Fund Research (2019). “Despite Record Year, Crypto Funds Finally Fall Back to Earth.” Available at: https://cryptofundresearch.com/despite-record-year-crypto-funds-finally-fall-back-to-earth/


Friedman, M. (1999). “Interview with National Taxpayers Union Foundation.” Available at: https://www.youtube.com/watch?v=mlwxdyLnMXM.


Last Week Tonight with John Oliver (2018). “Cryptocurrency.” Available at: https://www.youtube.com/watch?v=g6iDZspbRMg.


SwissBorg SA. (2018). “Terms of CHSB Token Sale,” Available at: https://uploads-ssl.webflow.com/5c0e70439a14797357f10649/5c6169d988b898f5451febb0_swissborg-token-sale.pdf.


TwoBitIdiot, (2018). “WTF is XRP?,” *Medium.* Available at: https://medium.com/tbids-weekly-bits/i-see-you-xrp-fcf151feb96d.


