12-16-2016

A Perspective on Electronic Alternatives to Traditional Currencies

Gabriele Camera
Chapman University, camera@chapman.edu

A Perspective on Electronic Alternatives to Traditional Currencies

Comments

Working Paper 16-32

A Perspective on Electronic Alternatives to Traditional Currencies

GABRIELE CAMERA*

Economic Science Institute, Chapman University

WWZ, University of Basel

16 December 2016

The institution of money is rapidly evolving thanks to developments in computer-based cryptography. Technological advances have made possible the creation of cost-effective electronic alternatives to banknotes and coins, which are the traditional physical currencies. This document aims to describe — based on scientific literature — the use and characteristics of money, some of the problems associated with issuing a new currency or a new payment instrument, and the possible comparative advantages of a central bank in leading the way relative to private issuers.

1 Introduction

Conducting retail transactions costs about 1% of GDP per year to the average European country (Schmiedel et al. (2012), Segendorf and Jansson (2012)).[1] Half of this cost comes from commercial banks, which have a prominent role in settling payments, especially now that the use of cash is rapidly diminishing in some countries (Segendorf and Wretman 2015).[2] Moreover, a significant portion of payments is typically executed by exchanging demand deposits, instruments that are risky and therefore costly to insure.

Technological innovation has recently enabled alternatives to traditional currency instruments. Thanks to new developments in cryptography and computing, it is now possible to develop digital alternatives to traditional currencies that are as peer-to-peer as cash, as convenient as a debit card, and potentially cheaper to use and safer than deposits. As a result, there is currently significant

* This overview, which has been prepared for Sveriges Riksbank, partly reflects content that has appeared in some of my own previous research, cited in this document. I thank, without implicating, Gabriela Guibourg, Erik Lenntorp, Jonas Milton, Kasper Roszbach, and, especially, Björn Segendorf at Sveriges Riksbank for many comments and stimulating conversations. The opinions expressed in this article should not be interpreted as reflecting the official views of Sveriges Riksbank.
Address: G. Camera, Chapman University, Economic Science Institute, One University Dr., Orange, CA 92866. E-mail: camera@chapman.edu

1 Defined as payments by cash, check debit and credit card, direct debit and credit transfer payments up to 50,000 Euros.

2 This decline is not common to all countries. For the US, Klee (2008) reports that cash captures 54% of all transactions collected from scanner data at 99 grocery stores. Survey data from Austria and Canada shows that more than 50% of all consumption purchases are paid for with cash (Huynh et al. (2013)).

interest—both from private and public financial institutions—in understanding whether or not there is scope for currency innovation.

Nowadays, the focus is on studying technologies that support the construction of cheap, safe and reliable *public ledgers*, essentially decentralized record-keeping systems that can be adopted to support the settlement of payments within large groups of traders who do not necessarily trust one another. Broadly speaking, such record-keeping systems can theoretically allow traders to accurately and quickly establish property rights over the instruments being traded, while, at the same time, eliminating or at least minimizing the traditional layer of services provided by trusted intermediaries, such as banks, in settling payments (Ali et al. (2014b), Barrdear and Kumhof (2016)).

A prominent candidate technology is “blockchain technology” or “distributed ledger” (Nakamoto (2008)), which was originally developed to support the Bitcoin network. This technology has spurred a number of private currency-like instruments, and is currently being tested for settlement of financial transactions (Bloomberg (2016a), The Economist (2015)). Importantly, this technological innovation is being studied for possible application in the emission of “all-digital” cash substitutes by central banks (Brainard (2016), Broadbent (2016), Fan (2016), Skingsley (2016)). Throughout this document, I will call this type of instrument *e-cash* because, on the one hand, it is as peer-to-peer as physical cash, and, on the other hand, it has a digital representation and is electronically exchanged and stored, in much the same way as the main forms of digital money in use today (commercial bank money and bank reserves at the central bank).

The possible economic consequences of bringing to the market an electronic substitute for cash have not been systematically studied. Many questions are still open. Even so, the scientific literature has addressed some of the fundamental, and closely related, questions. For example, what is the role of a currency in society, and what supports its stability and value in the long-run? Should we move away from traditional currency systems to embrace new technologies? What problems or market failures can we foresee that are associated with introducing an alternative payment instrument? Should central banks play an active role or should private issuers lead the way? This document aims to describe—based on scientific literature—uses and characteristics of money, some of the problems associated with issuing a new currency or a new payment instrument, and the possible comparative advantages of a central bank in leading the way relative to private issuers.

To summarize, moving away from traditional physical cash and into e-cash offers several potential benefits. An improved currency system could be constructed that greatly reduces the costly layers of the financial institutions that we currently use to process and settle electronic payments. E-cash may also allow significant changes in the way in which currency is managed, as it is now technically feasible to allow households direct access to the central bank balance sheet as Tobin suggested (Tobin (1985)). This could revolutionize the way in which monetary policy is conducted, affecting the monetary transmission channels, and the speed and efficacy of intervention. However, there are also risks in moving away from traditional currency systems, which depend on how a new currency system would be designed and operated. Granting deposits at the central bank could have profound consequences for banks, their financing, and their asset-transformation role, which could possibly adversely impact financial volatility during a crisis or during the transition period. Understanding these issues should be one of the priorities of a central bank.

The paper proceeds as follows. Section 2 develops some basic knowledge about money and the role it serves in a society. Section 3 offers a simple characterization of the main monetary instruments used nowadays. Section 4 discusses the problems and implications for central banks associated with the introduction of electronic alternatives to cash. Section 5 touches upon considerations about privacy and crime-related externalities, and Section 6 offers some final comments.

2 Currency, Money, and Cash

Currency identifies an object that widely circulates to facilitate payments. The term is commonly used as a synonym for money. Although economic textbooks do not typically tell us what money *is* — academics are still debating a possible answer[3] — there is consensus in the scientific literature about what money *does*. According to a view going back at least to Aristotle, money serves three basic functions. It facilitates trade by acting as a *means of payment* — e.g. we hand over banknotes for a coffee. It serves quantification purposes as a *unit of account* (or standard of value) — e.g. we choose our diet by comparing foods' prices. It is also a *store of value* — e.g. we hold a checking account balance to enable a future transaction or the repayment of financial and tax obligations. To perform these functions, societies have typically chosen currency instruments that are durable, highly portable, divisible, easy to authenticate and difficult to reproduce. Coins and banknotes — commonly referred to as *cash* — are tangible monetary instruments and the ones that the public is most familiar with.

The cash in use today is a sovereign *fiat* money, meaning that these tangible monetary instruments are issued by a state authority but neither have intrinsic value — coins are not made of precious metals, for example — nor are explicitly convertible into real assets such as precious metals (ECB (2015b), McLehay et al. (2014)). However, cash has generally a special status: in most countries it is "legal tender," meaning that tendering banknotes and coins legally discharges financial obligations.[4]

But money is much more than cash. In particular, it includes two kinds of intangible monetary instruments: banks' reserves with the central bank (sovereign money), and commercial bank deposits (instruments that are privately issued by commercial banks). The main difference between these two kinds of money, sovereign and private, is on whom they are a claim. Sovereign money is a claim on the central bank, and is often called "outside money" or "central bank money"; commercial bank money is a claim on private domestic debt and is often called "inside money."[5]

2.1 The nature of money

To understand the role and the value of currency and monetary systems, we must answer two questions. Why do societies use money? Which economic problems does money ultimately solve?

Money is first and foremost a *social convention*, which emerges to build trust among strangers in their economic transactions, both intertemporal and in spot markets. A convention of monetary exchange facilitates valuable intertemporal exchanges that would not occur otherwise.

According to this view, individuals who may neither know nor trust each other choose to settle their transactions by offering symbolic objects—bank deposits or banknotes for instance—in exchange for labor, goods and services because they find this trading arrangement superior to the available alternatives (Camera, Casari and Bigoni (2013)). Hence, symbolic objects spontaneously become money when individuals share the belief that those objects can be quickly and easily exchanged for labor, goods and services in the foreseeable future. If no-one can personally gain from acting differently—demanding payment of a different kind, for instance—then those

---

3 Krugman (2010) writes: "But here's an even more basic question: what is money, anyway? It's not a new question, but I think it has become even more pressing in recent years."

4 Legal tender is roughly interpreted as obliging the economic agents to accept the instrument as payment, but this interpretation is not always fitting. For example, in the U.S. "legal tender discharges all debts for which the payment of money is specified when tendered in the appropriate amount and in the proper manner" (Konvisser (1997)). In Sweden everyone is obliged to accept banknotes and coins as payment, but only if the contracting parties have not made a different agreement (Segendorf and Wilbe (2014)).

5 This distinction was made by John Gurley and Edward Shaw in their book "Money in a Theory of Finance." Various measures of the money supply — typically, monetary base, M1 and M2 — account for the different components of the stocks of outside and inside money.

symbolic objects become money and support a currency system. The system is stable if everyone maintains their confidence in it.[6]

A monetary trading pattern resembles an intertemporal gift-giving scheme, where each gift is acknowledged by delivering a token. But, if tokens are intrinsically worthless, then why are they exchanged at all? The answer is that doing so resolves an underlying trust problem. Any transaction characterized by a mismatch between the timing of delivery of goods and of payment requires that counterparts trust each other. However, the most valuable trades involve specialized goods. This typically requires dealing with strangers, instead of trusted neighbors (Greif (2006)), which prevents reciprocity and makes contractual enforcement problematic (Milgrom et al. (1990)). Monetary exchange can overcome these contractual difficulties as long as traders are confident that others will accept money in the future. Public confidence in the currency is thus key ingredient in a monetary system.

This problem is conceptually represented in Figure 1. Assume there are many individuals in the background who alternate between being producers and consumers of a non-storable good. They meet each other at random in each period. The figure shown represents one such meeting. The consumer benefits from receiving a gift of a good from the producer. Maximum welfare can only be attained if individuals coordinate on a norm of mutual support, wherein every person makes a gift of a good when they are a producer. However, people cannot guarantee they will reciprocate a gift in the future because meetings are random. Markets, that is, are incomplete. This norm of mutual support thus requires *trusting* that a gift made today corresponds to a gift in the future. However, building this kind of trust is practically feasible only in small groups, where individuals know each other very well.

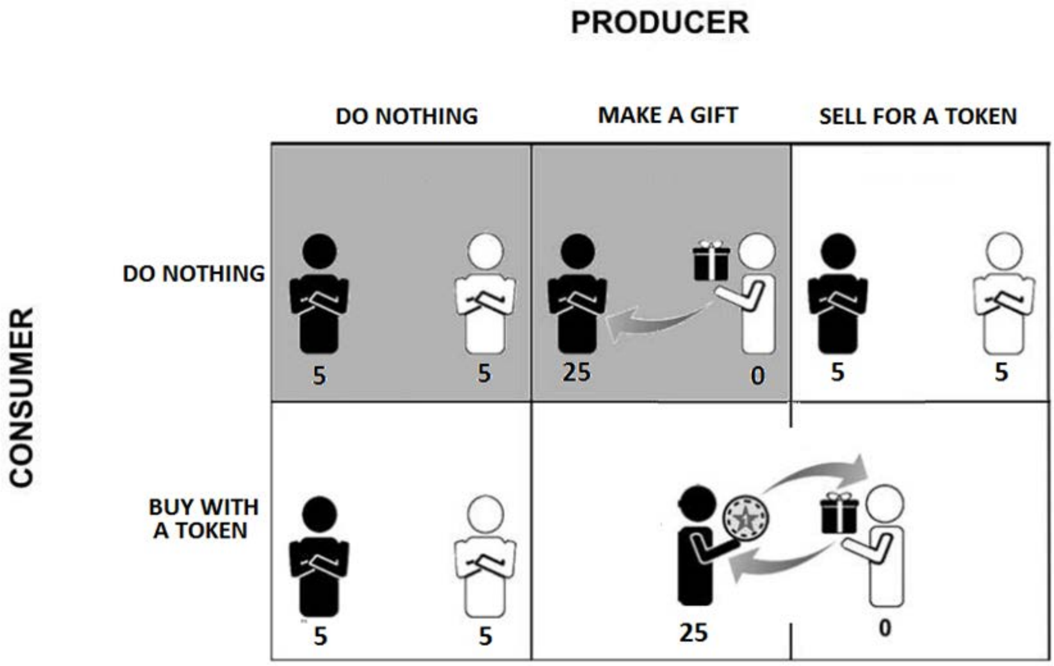
Introducing a stable supply of symbolic tokens can resolve this market failure if people trust that others will sell *only* in return for a token. In this case, the token becomes a currency. Public confidence in the monetary system is thus inextricably linked to confidence in the currency issuer—which is why central banks' conduct is key for the stability of a currency system. A monetary system can thus be viewed as a social convention that emerges to build the trust needed to support valuable economic interactions among strangers. In a way, confidence in the institution of money can shore up the lack of trust in other members of society. Laboratory research provides some empirical support for this view (Camera and Casari (2014)).

---

[6] In the language of economics, money emerges as the solution to a non-cooperative game — a *Nash equilibrium*. Shapley and Shubik (1977), among the first to apply non-cooperative game theory to the study of money, put it as follows: "Although a person may view, say, fiat money as being of dubious value as a store of wealth, he knows that most others will continue to use it for trade, and he may be in no position to do otherwise himself."

Figure 1. How monetary exchange resolves trust problems

Each cell reports the outcome from a combination of actions (producer on the right, consumer on the left, and payoffs listed below the human figures). The shaded cells refer to outcomes without a monetary system. The other cells depict the additional outcomes possible when a monetary system is in place. The figure is an adaptation from Camera, Casari and Bigoni (2013).



Do informationally sophisticated societies need money?

Some economists have compared money to an information technology—a record-keeping device (Ostroy (1973), Ostroy and Starr (1974), Townsend (1987)). Kocherlakota (1998) suggested that money is a rudimentary public monitoring system. According to this view, if it is difficult to write and enforce contracts, then revealing others' past conduct is sufficient to deter opportunistic behavior in a community. According to Kocherlakota (1998), all that is needed to ensure that counterparts keep their promises is the possibility to publicly reveal departures from agreed-upon plans, because this information can be used to trigger punishment by the entire community (Abreu et al. (1990), Kandori (1992)). Thus, the theory says, monetary exchange has a role to play only if monitoring past conduct is difficult. This is the sense in which money is simply a substitute for public monitoring systems. According to this view, currency systems should have no role to play in informationally sophisticated societies (Kahn et al., (2005), Corbae et al. (2007)). Laboratory evidence does not support this assertion. Individuals who can see others' past conduct do not, in fact, frequently cooperate (Bigoni et al. (2015)). This suggests that money is likely to remain a valuable institution even as societies become more interconnected and informationally sophisticated.

2.2 A monetary system is a public good

The discussion above suggests that currencies and monetary systems are a public good, much as clean air, national defense, or national parks. In its most basic form, a monetary system is non-excludable — single individuals can hardly be prevented from using banknotes and coins.[7] It is also non-rival because an individual's participation in the system does not impede another's use. In fact, it likely raises the value of the currency through network effects — a currency that is widely used is more valuable than one that is not, because it enables more trades. As is typical in public goods problems, self-interested individuals would rationally choose to free-ride by avoiding to privately contribute to this public good, reducing their input to building and maintaining "confidence in the currency." This socially inefficient provision would take the form of an *excessive* emission of currency instruments under a laissez-faire approach, which would reduce confidence in the currency, lowering the value of the currency up to the point where the monetary system would collapse because the future value of the currency would be too small (Ritter (1995)).[8] This public goods aspect of monetary systems is one of the factors justifying the central role of public institutions in the provision of currency instruments (Tobin (1985)) and, consequently, in playing an active role in currency innovation.

3 Modern monetary instruments: physical vs. digital

There are many ways to classify the monetary instruments in use today.[9] Table 1 adopts a conceptual classification based on two basic features: the denomination of the currency instrument — either a sovereign reference unit or not — and its type — physical or not. This is convenient because, on the one hand, modern currencies are typically sovereign but only in (small) part physical; on the other hand, the key technological innovation has been originally confined to instruments, such as Bitcoin, which are purely digital and are not denominated in sovereign reference units.

---

7 In fact, this is true for domestic as well as foreign users. The U.S. dollar supports trade in many countries and U.S. authorities cannot effectively prevent this from happening.

8 This is exactly what happened with Stockholms Banco, the first bank in Sweden. The bank was established in 1656 but folded in 1664 after the general public lost confidence in the banknotes it issued. The bank was then rescued by the Swedish parliament in 1668, and became the Riksbank. See http://www.riksbank.se/en/The-Riksbank/History/.

9 For example, the BIS identifies physical tokens, privately issued notes, cash, central bank deposits, commercial bank money, legally recognized e-money and digital currencies as being distinct types of assets (Bank for International Settlements (2015), Figure 1). Some are issued by a central bank, some are not. Some are centrally issued and some are not. Some are physical some are not.

Table 1. A basic classification of modern types of monetary instruments

	Type: Physical	Type: Digital
Denomination: Sovereign reference unit	**Notes and tokens** (central bank coins & banknotes)	**E-money** (central bank reserves, commercial bank money) **E-cash** (RSCoin concept)
Denomination: Other reference unit	**Notes and tokens** (Ithaca HOURS)[10]	**Abstract currencies** (Bitcoin, Ethereum)

The currencies in existence today are typically issued by a sovereign institution, such as a central bank or a national mint. This is especially true for physical currencies, coins and banknotes. But cash, which is synonymous for physical currency, is not the predominant form of money: for example, U.S. banknotes and coins comprise slightly more than 2/5 of M1, the smaller of the two money stock measures published by the Board of Governors and currently the narrowest monetary aggregate.[11] There is no consensus on the language used to describe the money component that lacks the physical structure of cash. I will use the term *digital currency*, to emphasize that the instrument is intangible, and is based on computer technology.

A characteristic of digital currencies is that — unlike banknotes and coins, settlement cannot be completed by a simple physical transfer of the instrument. A ledger — i.e. a record-keeping system — must be in place to establish property rights over the instrument.[12] As a result, users of digital currencies must rely on some trusted institution — an intermediary, a network of banks, or a group of fellow system participants — to help with the processing of transactions and the ledger updating. This is where innovation in cryptography and computing has recently made a big contribution, as I next explain.

---

[10] *Ithaca HOURS* is a privately issued fiat currency that has circulated in the city of Ithaca, New York, since 1991 when a local resident issued the first notes. It is accepted by local businesses and residents. One hour is worth $10 and its supply is currently valued at about $100,000; see http://www.paulglover.org/hours.html.

[11] It includes cash held by the public and transaction deposits at depository institutions. The figure is not that different if we consider the sum of the Federal Reserve's monetary liabilities and the Treasury's monetary liabilities (the monetary base or "high-power money"), where the share of cash is slightly less than 40%. In the U.S., M1 is currently the narrowest monetary aggregate, about 10% smaller than the monetary base.

[12] Roughly speaking, a ledger is needed when physical possession and transfer of an instrument is impossible or insufficient to establish property rights over the instrument.

3.1 Sovereign digital money: e-money

Most digital currencies are denominated in a sovereign unit, and issued by central banks as well as private institutions — such as commercial banks. I will define *electronic money*, or *e-money* for short, as an electronic representation of a physical sovereign currency.[13] As such, e-money has been around for a long time. The main forms of e-money are commercial bank reserves with the central bank and the money created by commercial banks when they make loans. E-money can generate revenue for the issuer, which roughly corresponds to the spread between the yields on securities bought and liabilities issued;[14] the owner of e-money has a claim on the issuer's funds, while e-money represents a liability for the issuer.

Though e-money does not necessarily imply a legal right to a physical currency, it has so far typically implied, or is taken to imply, that owners of e-money can exchange the instrument at par for the underlying physical currency without restriction (e.g. demand deposits). This characteristic is behaviorally important because it may boost confidence in the currency system in periods of uncertainty, since individuals can disintermediate their savings and independently store value by physically hoarding the instrument.[15]

Broadly speaking, every financial institution participates in partly maintaining the ledger associated with an e-money system. This ledger is not public. Settlement relies on several layers of trusted institutions (banks, courts, central banks, etc.) and is ultimately accomplished by adjusting the reserves of commercial banks with the central bank (Broadbent (2016)). In this sense, the system is centralized and likely more expensive compared to systems that grant some decentralization. *Blockchain* technology—which essentially is a kind of database that can be easily shared—has made possible the creation of secure bookkeeping systems called *distributed* (or *public*) *ledgers* that can be publicly shared. According to some observers, this database-sharing innovation has the potential to raise the speed of settlement while dramatically lowering settlement costs compared to traditional payments systems (UK Government Office for Science, (2016)).[16] I discuss this next.

3.2 Non-sovereign digital money: abstract currencies

The past ten years have seen the creation of a new class of digital instruments that are not issued by a sovereign institution or commercial bank, are not denominated in a sovereign unit, and do not have physical counterparts. Since these instruments may be used as a currency (though not everyone agrees, e.g., Krugman 2013, Rogoff (2014)), they are variously labeled "electronic cash," "digital currency," "virtual currency," "altcoins," or "cryptocurrencies."[17] What are these digital instruments, why have they been created, and how do they differ from e-money?

---

13 The CPMI's "A glossary of terms used in payments and settlement systems" defines e-money as "value stored electronically in a device such as a chip card or a hard drive in a personal computer" (Bank for International Settlements (2015)). The European Commission has a similar definition: "Electronic money is a digital equivalent of cash, stored on an electronic device or remotely at a server." (see http://ec.europa.eu/finance/payments/emoney/index_en.htm)

14 In the case of central bank money, this is called seigniorage. It roughly corresponds to the interest income earned from the assets on its balance sheet (Haslag (1998)). A way to empirically calculate it is to take the product between the yield on an appropriately chosen portfolio of securities (typically, government bonds) and base money deflated by the CPI. As the choice of portfolio is somewhat arbitrary, empirical work often measures seigniorage as the change in monetary base normalized by CPI or GDP (Klein and Neumann (1990)).

15 Ecuador's recently inaugurated *Sistema de Dinero Electrónico* is based on a mobile-phone electronic wallet denominated in US dollars. The Bank of Ecuador manages the system and backs it by holding 100% physical reserves of U.S. liquid assets (Ecuador Embassy in the US).

16 This cost-saving aspect is non-trivial. A recent study estimates that half of the social costs of retail payments — amounting to about 0.5% of GDP in the average European country — are incurred by banks (Schiedel at al., (2012)). Indeed, currently payments are settled by exchanging commercial banks' reserves, since these are the players who have sole access to the central bank's balance sheet.

17 The architect of Bitcoin called it "electronic cash" (Nakamoto (2008)). The European Banking Authority (2014) and European Central Bank (2015a) call the instruments based on blockchain technology "virtual currencies". Some prefer "digital currency" (Broadbent (2016), Ali et al. (2014), Bank for International Settlements (2015)). Others use the words "cryptocurrencies" or "altcoins" (Bitcoin Magazine (2016), Danezis and Meiklejohn (2016)).

The central innovation compared to traditional currencies and traditional digital payment instruments is most of them are based on a distributed ledger in order to avoid reliance on the traditional layers of formal institutions — such central banks, banking authorities, and commercial banks — to process transactions and update ledgers. I will collectively call this category of new currency instruments *abstract currencies*.[18] They are *currencies* in the sense that they can be exchanged peer-to-peer, much as cash. They are *abstract* in the sense that they neither exist in space nor refer to an existing instrument, physical or financial (for example, deposits). Simply put, they are representations of numbers, i.e., abstract objects.

An abstract currency system is a self-enforcing system of property rights over an abstract instrument, which gives its owners the freedom to use and the right to exclude others from using the instrument. Using the instrument solely consists of digitally hoarding it or transferring ownership to other system participants, according to the system's built-in rules.

Bitcoin

Bitcoin is the first abstract currency system ever created. It appeared on the 3rd of January 2009, when the open source computer code was made public and the first ten bitcoins were created. The system allows the transfer of property rights over abstract objects called "bitcoins" among network participants. The system is built around the blockchain-based distributed ledger framework discussed in Nakamoto (2008). The emission of bitcoins is regulated by a mathematical algorithm that ensures a bounded, predictable bitcoin supply.

Unlike a traditional currency, an abstract currency is not issued by a central authority, is not a claim on any issuer, and is not backed by any central authority (through legal tender status, for example). Being a fiat instrument, an abstract currency acquires value only if its users are confident that the instrument is a safe store of value and its ownership can be easily transferred to someone else in the foreseeable future, in exchange for labor, goods, services, or other stores of value (e.g. other currencies or financial instruments). Since the instrument cannot be physically possessed, this means that property rights over the instrument must be established through some ledger system. The crucial innovation lies in how property rights are established and managed compared to traditional e-money systems.

Nowadays, the exchange of e-money relies on designated trusted intermediaries—such as banks and central banks — to update electronic ledgers. Intuitively, this resolves a problem of trust. If counterparts have little or no trust in each other, then trade requires an intermediary that can be trusted *not* to falsify the ledger's records. In traditional currency systems, only specially designated intermediaries can access the ledger. Instead, the original idea behind an abstract currency system (Nakamoto (2008)) is to enable electronic payments *without* having to rely on designated intermediaries. The solution to this problem partly relies on making the history of all transactions completely public through the "blockchain database," also known as the "distributed ledger" ("distributed timestamp" in Nakamoto (2008)).

How the distributed ledger supports trade

Property rights over an instrument are established by making the history of all transactions public through the blockchain database. One can think of this public ledger as a system-wide database that is transparent and synchronized: every system participant locally stores the entire history of payments. A payment thus simply corresponds to a time-stamped change in record in the public ledger, which takes the form of an addition to the blockchain database. In a way, the blockchain records the ownership trajectory of each instrument over time, as if describing a long chain of events. A transaction is verified as having taken place if there is sufficient consensus among system participants that a proposed change in instrument's ownership does not conflict with the

[18] The term "abstract" uniquely differentiates these instruments from unrelated instruments. For example, stored-value cards are a form of currency that relies on cryptographic technology; commercial bank reserves represent currency in digital form. In the computer-based (i.e., virtual) reality called "Second Life" trades must be completed with Linden dollars; this "virtual currency" thus ends up being traded for US dollars. This is unlike Bitcoin, whose value is not tied to a virtual reality.

information stored in the database (“Nakamoto consensus”). All valid payments are peer-to-peer — as if exchanging physical cash — and are irreversible.

To build consensus, some system participants must be willing to verify the validity of transactions — impartially and honestly — using computational methods that are made costly and lengthy *on purpose*. Those who choose to verify transactions are called ‘miners’ because they are compensated with newly created currency. Money creation is tied to settlement. Miners act as private third parties that compete among themselves to provide settlement services but, unlike banks, are unsupervised, unregulated, and face no counterparty risk. Computational burdens, database transparency and competition to verify prevent fraud in the form of double-spending.[19]

Abstract currency payments are not intermediated — although they take place over the internet, they are peer-to-peer like cash — they are settled as soon as enough system participants agree they are valid. A proposed change in the instrument’s ownership is valid when there is enough consensus that the change does not conflict with the information contained in the public record.[20] At that point, the transaction is made irreversible and is added to the public record in real time. Roughly speaking, the incentive to commit fraud — which simply means altering records to spend someone else’s asset (“double spending”) — is removed in two ways. First, validation work is randomly rewarded with a newly created instrument — thus promoting consensus-building through competition on validation. Second, the validation process is constrained to be computationally challenging — thus preventing record falsification by minority coalitions.

An advantage of an abstract currency is that transactions are peer-to-peer, thus avoiding the counterparty risk to which intermediaries are exposed in settling traditional payments. At the same time, an abstract currency grants the convenience of digital transactions with fast settlement[21] at a lower cost compared to the digital money currently in use in most countries. For example, the Automated Clearing House network used by U.S. depository institutions to make electronic transfers works through batch processing of transactions, and it only recently started to allow same day settlement (NACHA, (2016)).[22] However, it must be noted that this characteristic is not unique to blockchain-based payments. Some countries already operate real-time settlement systems that are very fast and the speed-cost advantages of blockchain technology are less clear. For example, Sweden’s cell phone-based “Swish” peer-to-peer payments service is supported by a real-time settlement system called BiR; that system could be possibly used for other payments services (Segendorf and Wretman (2015)).

There are also drawbacks in abstract currency systems like Bitcoin: (i) they can only generate a rigid currency supply, which is bounded above in the long-run,[23] (ii) they may not be easily “scalable” in the sense that they can only handle low transaction volumes (7 transactions per second for Bitcoin, vs several thousand for Visa, for example), (iii) they are highly volatile instruments, partly

---

[19] This does not mean that governance must necessarily be distributed. Bitcoin was intentionally designed so that a currency system could be operated without designing intermediaries that should be entrusted with record-keeping. If the incentives to perform validating services are adequate, then proper validation is self-enforcing and trust in the currency system is self-generating. However, problems with incentives for proper validation have recently emerged (Danezis and Meiklejohn (2015)). It is thus an open question whether or not introducing trusted record-keeping institutions could improve system governance—even, in this case, whether the structure of the intermediary’s incentives matters.

[20] A straight majority of system participants must recognize the transaction as valid. An accessible technical description of the distributed ledger technology can be found in the UK Government Office for Science (2016), Ali et al. (2014a), or Boehme et al. (2015).

[21] Bitcoin is neither particularly fast nor easily scalable. Transactions take several minutes to be confirmed and the system, in its current form, is unlikely to scale beyond 100 transactions per second (Decker and Wattenhofer (2015)). Moreover, Bitcoin transactions are typically considered final only after six confirmations, which creates a delay of about an hour before the transaction is validated (Boehme et al. (2015))

[22] The U.S. ACH system is a nationwide network through which depository institutions send each other batches of electronic credit and debit transfers (Board of Governors, (2016)). The Federal Reserve Banks and Electronic Payments Network are the two national ACH operators.

[23] The rule regulating the emission of bitcoins is built into the system and cannot be altered without reaching consensus among system participants. Roughly speaking, instruments are emitted every time a transaction is validated. The emission rate is designed to decline over time until all emission stops, at which point the supply of instruments can no longer increase.

because their value is not tied to a sovereign currency, and (iv) they tend to suffer from incentive problems as the network size increases. These practical considerations — as well as public confidence, coordination and stability challenges due to the lack of a central authority — partly motivate recent studies about the conceptual feasibility of sovereign digital currencies based on decentralized ledgers, as discussed below.

3.3 E-cash proposals between abstract currency and e-money

There is currently significant interest from academics and practitioners in the conceptual feasibility of sovereign digital currencies that could be issued by a central authority but that would exploit the flexibility of blockchain technology (Ali et al. (2014b), Barrdear and Kumhof (2016), Bank for International Settlements (2015), Danezis and Meiklejohn (2015)). We are starting to see some proof-of-concept currencies. One example is the Central Bank Digital Currency (CBDC) studied by the Bank of England (discussed below).

As in the case of banknotes and coins, the exchange of this new kind of currency from payer to payee would imply immediate settlement of the transaction. Unlike traditional currencies, and like abstract currencies, transactions would be broadcast to all system participants and would be validated through some consensus protocol. As a result, settlement would not require the exchange of bank reserves at the central bank.

Since these instruments are envisioned as a purely digital version of a coin or a banknote, I will use the terminology *electronic cash*, or *e-cash* for short, to differentiate them from both e-money and abstract currencies.

No e-cash system is yet in place, though some institutions are studying it. Examples include the Central Bank Digital Currency (CBDC) studied by the Bank of England (Broadbent (2016), Barrdear and Kumhof (2016)) and the proof of concept known as RSCoin (Danezis and Meiklejohn (2016)).

The RSCoin concept

The study in Danezis and Meiklejohn (2016) proposes an e-cash instrument, called RSCoin, to be issued by a trusted central institution (a central bank, for example). Unlike traditional e-monies, the transaction ledger would not be centrally maintained by the issuing institution. Instead, it would be partially distributed using blockchain technology. This, according to the authors, could allow high rates of transactions at low cost. To support the system, designated authorities called "mintettes" — basically, pre-existing intermediaries such as commercial banks — would be authorized to collect transactions and would ultimately be collectively responsible for producing a consistent, cross-referenced ledger. This ledger would then be sent back to the central institution for final validation. It is unclear if RSCoin would be exchangeable upon demand for physical sovereign currency.

The Bank of Canada is also studying a sovereign currency called CAD-COIN, which would adopt a distributed ledger based on blockchain technology. This instrument is being studied as a way to facilitate wholesale interbank payments, not for use by the general public, and its supply would be tied one-to-one to the amount of cash collateral pledged by system participants, and fully convertible into physical currency (Forbes (2016)). Bank of Tokyo-Mitsubishi is also studying a distributed ledger private currency fully backed by yen, as well as denominated in and convertible into yen (Reuters (2016)).

Recently, several central bankers have started to openly discuss the possibility and consequences of introducing an e-cash alternative to traditional physical currency. The Bank of England's deputy governor for monetary policy has noted that it is now conceptually and technically possible for a central bank to directly issue a new electronic currency in a manner that widens access to its balance sheet beyond commercial banks, not only to non-bank financial companies but even to individuals (Broadbent, (2016)). A deputy governor at the People's Bank of China wrote that central banks should take the lead in developing "digital legal tender of their own" (Fan (2016)). A Federal Reserve Board of Governors member remarked that the distributed ledger technology "may represent the most significant development in many years in payments, clearing, and settlement" (Brainard (2016)). In Sweden, the Riksbank is studying whether or not to meet the general public's need for central bank money by supplying it in some electronic form (Skingsley (2016)).

4 Electronic alternatives to cash: challenges and implications for central banks

Private issuers have readily exploited blockchain technology to offer electronic currencies of their own (collectively called "altcoins") such as *Ethereum*, and *Litecoin*,[24] partly to address some of the shortcomings identified with Bitcoin (Danezis and Meiklejohn (2016)). Given this, is there scope for a central bank to take a leading role in developing and issuing e-cash? This section helps form an answer by focusing on three classes of problem associated with issuing a new currency instrument—public confidence in the currency, avoiding coordination failures, and ensuring financial system stability—three problems that may give rise to market failures and create scope for a central bank-issued currency beyond the obvious benefit of obtaining seigniorage revenue.

4.1 Confidence

A currency system is self-sustaining when the public has trust in the feasibility of the underlying trading arrangement. In practice, this means that system participants must have confidence in the currency's future value and acceptability. Ultimately, this requires confidence in the issuer, so an essential characteristic of any currency is *on whom* it is a claim. Do private and public issuers have differential advantages in supporting confidence in a currency instrument?

Historically, public confidence in a currency largely referred to the quality of the coins that formed the basis of the currency. States had an obvious advantage in guaranteeing this quality over private issuers, not only because they could set and enforce quality standards more easily than private issuers, but also because states can internalize the long-run benefits of a stable currency, thus strengthening the incentive to avoid debasements (Goodhart (1998)).

Unredeemable currencies exhibit a similar confidence problem. In a fiat monetary system, the currency's value is a projection of its *expected* future acceptability and trading value. Confidence in a currency thus largely depends on expectations about the issuer's future actions. And here lies the central problem. Issuing currency generates a benefit for an issuer, through the interest income earned from the assets it acquires (seigniorage). There is thus a temptation to behave opportunistically and overissue currency. *Confidence* in a currency exists when the public believes that the issuer will not emit currency beyond the point where the currency's value will become unstable or rapidly decline. Lack of confidence in the issuer is a serious threat to a fiat currency. It can lead people to believe that the currency might no longer be accepted on some future date. If so, then we would witness a hyperinflationary spiral (Faust (1989)) or, at worst, the currency's value would immediately collapse (Cass and Shell (1980)).

Although current thinking in monetary theory pays little attention to the role of governments in establishing a currency,[25] some studies have emphasized that a credible public issuer might have a confidence advantage over private issuers.

First, currency systems are public goods and private issuers may not give sufficient weight to the externalities generated by money creation and so may end up oversupplying it. By contrast, governments can more easily internalize these externalities, and thus better mitigate the risk of a currency oversupply. If so, a sovereign currency system is less likely to suffer from confidence

---

[24] See https://coinmarketcap.com/ for a snapshot of current market capitalization of these altcoins. At the time of writing, more than 600 altcoins are being traded and the total market capitalization is $11.4 billion, 80% of which is associated with Bitcoin.

[25] Goodhart (2009) notes: "economists have tended to ignore historical reality, to establish formal mathematical models of how private agents (with no government), transacting among themselves, might jointly adopt an equilibrium in which they all settle on a common monetary instrument."

problems than a privately issued currency (Ritter (1995)). A related issue is enforcement of the quality of the currency. Governments typically control or operate the institutions that enforce the rules governing a society. Hence, there can be advantages from vertical integration of the two tasks of emitting currency and enforcing the currency emission rules. The design of Bitcoin reflects an attempt to resolve this crucial enforcement problem without relying on central institutions. In doing so, it creates other kinds of problems—for example, an inelastic currency supply and an inability to control illicit financial flows. This speaks in favor of a sovereign e-cash system.

Second, public monitoring of conduct is known to help mitigate temptations to behave opportunistically (Abreu, Pearce, and Stacchetti (1990)). The public can more easily monitor the actions taken by a central bank compared to those taken by a private issuer. This is likely to enhance the stability and value of the currency, because it allows a quick and coordinated response to socially undesirable policies, thus removing the incentives to stray from optimal policy in the first place.

Third, short planning horizons weaken the incentive to keep promises compared to having a long-run horizon (Friedman (1971)). Hence, the planning horizon affects the incentive to manipulate the currency supply. A currency issuer that is motivated by short-run objectives has stronger incentives to manipulate the currency supply to extract short-run rents compared to an issuer pursuing long-run objectives. Central banks tend to have longer planning horizons compared to private issuers. This allows central banks to internalize the social costs that monetary instability has in the long run. This long-run perspective is reinforced for central banks that are independent of the political authorities, as political authorities may be more easily tempted by the possibility of attaining short-term gains. Having a long-run view seems especially important in periods of uncertainty, to maintain confidence in the currency and avoid self-fulfilling currency collapses.

Self-fulfilling currency collapses

The value of a fiat currency is linked to *expectations* about its future acceptability as a means of payment. If confidence in an existing currency rapidly deteriorates, or if there is no sufficient confidence in a new currency, then the currency value will collapse to zero. To illustrate this, note we accept a currency in exchange for goods and services only if we believe that the currency can be easily spent. If we all think this way, then the currency is broadly accepted, thus confirming (or fulfilling) the initial belief in the currency's value. On the other hand, we will *not* accept a currency if we doubt that others want it. If we all share this view, then the currency will not be broadly accepted, thus confirming the initial belief. Here, the currency's value collapses to zero. This outcome is self-fulfilling because it is entirely driven by initial beliefs. Simply put, if the public *doubts* that others will want a currency instrument, then that instrument's value will quickly collapse.

Finally, in many countries, sovereign currencies have a well-established history of use and monetary authorities are trusted; this may prove to be an advantage for a national e-cash system over privately issued alternatives. In countries with trusted and well-functioning monetary institutions, a sovereign issuer could leverage the pre-existing trust to more easily build confidence in a new currency instrument, compared to private issuers.[26]

Overall, these considerations suggest that a sovereign issuer is in a unique position because it can more easily internalize the externalities associated with introducing a new currency, and can more easily build confidence in the instrument's stability compared to private issuers. However, additional research is needed on this topic. Empirical evidence would be especially valuable.

[26] This does not mean, of course, that states are necessarily trustworthy currency providers. The hyperinflationary experience in Zimbabwe in the first decade of this century, and the recent and sudden de-monetization in India come to mind.

4.2 Coordination problems

When more than one instrument exists that can serve the role of a currency, then the choice of instrument to use may become a problem. The reason is that there could be miscoordination resulting in partial adoption of multiple instruments instead of the common adoption of a single one. This fragmentation of payment methods is a source of inefficiency because it complicates settlement and raises its cost.

To understand this point, suppose two fiat currency instruments exist in fixed supply and only differ in their color. Individuals independently select which one to adopt. Here, one of the two instruments may be accepted by everyone, but it may also happen that none are wholly accepted (Kiyotaki and Wright (1993)). This second scenario is inefficient because the instruments' fragmented use may sometimes prevent trade from taking place. In this sense, money shares many similarities with language (Polanyi, (1957)). Coordinating on a single language is beneficial because the greater the number of people who speak a language, the more valuable it is to speak *that* language. The same holds true for money. These are known as "network effects" or "strategic complementarities," meaning that individuals benefit from making identical choices (Cooper and John (1988)).

Coordination problems as a two-person game

Eva and Isabella must independently choose one of two communication systems, A or B. Their joint choices determine if a communication system will be set up, and how they will share a prize V from setting it up:

Outcome	**Payoff**
AA	Eva earns 60 percent of V, and Isabella earns 40 percent
AB	No communication system is set up and no prize is won, so both earn 0
BA	No communication system is set up and no prize is won, so both earn 0
BB	Eva earns 40 percent of V, and Isabella earns 60 percent

Eva and Isabella want to coordinate on *some* common system to avoid a total failure. In the language of economics there is a positive network externality. But there is also strategic uncertainty because, though *AA* and *BB* are both equilibria, neither Eva nor Isabella is sure what the other will do. In fact, their interests are conflicting because Eva prefers *AA*, but Isabella prefers BB. If either *AB* or *BA* is realized, then we have a *coordination failure*. Having a third party acting as a coordinator may help.

Numerous studies have found that miscoordination commonly occurs in simple coordination games (van Huyck et al. (1990)) as well as in more complex tasks. For example, payment arrangements may be inefficiently selected (Camera et al. (2016)) and it is difficult to coordinate on a smooth transition from an "inferior" to a "superior" currency (Camera at al. (2003)). Habit can play an important role in leading to an inefficient selection of payment methods (van der Horst and Matthijsen (2013)).

These observations suggest there is scope for a public institution to serve as the sole issuer of the currency. A sovereign issuer can help resolve coordination problems by granting legal tender status to a newly issued instrument. A drawback of granting legal tender status to a new instrument is that it effectively imposes a constraint on the choice of payment instrument, which may itself be suboptimal. A government can also set a standard by requiring a new state-issued currency in payment for taxes—something known as the tax-foundation theory of money (Starr (1974), Goldberg (2012)).

4.3 Stability

A major open question is whether introducing a digital alternative to a traditional currency can induce instability in the monetary and financial system, and why this may happen. Here, I consider four aspects of this problem that have been discussed but that should be more carefully studied.[27]

4.3.1 Design of the instrument

Letting a central bank issue e-cash could induce instability by creating changes in the funding base of banks and would thereby alter the relation between banks and the central bank — possibly generating disintermediation in times of crisis. As an illustration, suppose that the central bank issues e-cash in a manner that gives direct access to its balance sheet to households — not only financial institutions. This could be as simple as a liquidity deposit, or could be more sophisticated. For example, central bank e-cash could pay some interest, thus coming into direct competition with the traditional role of commercial banks (Broadbent, (2016)). Either way, by design this instrument would be quickly and cheaply transferable from and to intermediaries. This might increase financial market volatility. In normal times, volatility could be induced by stochastic flows of deposits in and out of e-cash. In periods of uncertainty, households might seek the safety of the central bank, thus giving rise to rapid outflows of funds from commercial banks, as in a digital version of the classic bank run. This kind of volatility in funding liquidity would naturally have implications for the way banks fund their projects and for the cost of deposit insurance. On the other hand, interest-bearing e-cash could improve the stabilization of the business cycle (Barrdear and Kumhof (2016)).

The impact of interest-bearing e-cash is, for natural reasons, still an open question. Empirically, there are reasons to be cautious. I am not aware of historical examples in which an interest-carrying currency has been at the heart of a stable currency system, widely circulating side-by-side, or instead of, a non interest-bearing currency.[28] On the other hand, the technical opportunity to issue such an instrument has not emerged until now. The uncertain consequences of an interest-bearing currency may be purely behavioral: individuals might attempt to hoard it and speculate on its value (Camera et al. (2003)). The public may also perceive different currency instruments as being only partially fungible, leading to an inefficient use, for example using interest-paying e-cash to store value but not as a currency, as per some form of “mental accounting” (Thaler (1999)).[29] These kinds of problems can presumably be minimized by letting the central bank offer individual deposit accounts that are a modern version of Tobin’s *deposited currency*: a plain, non-interest bearing cash-like instrument, 100% backed and payable on demand in cash (Tobin (1985)). Blockchain technology indeed seems to offer a cost-effective means to emit and manage this type of instrument.

4.3.2 Lack of explicit anchors

Letting private issuers provide e-cash may induce price instability, if price floors cannot be easily established. The experience with abstract currencies suggests that it may indeed be difficult to find price floors (a nominal anchor) with privately-issued electronic currencies. Bitcoin, for example, is very volatile and, for this reason, has been criticized for being an unstable store of value and, therefore, unsuitable as a currency (Krugman (2013)). Instability is a problem because it gets in the way of widespread adoption. One can apply evolutionary arguments to formalize this point by studying the stability of a fiat currency system when many individuals make independent adoption decisions. The system will collapse if the initial currency value has too low a price floor, as this negatively interferes with the dynamics of adoption and use (Camera et al. (2013)). Sovereign e-cash would reduce these risks, by providing explicit anchors such as making the new instrument legal tender, accepting it to discharge tax obligations, or accepting it in exchange for government

---

27 Barrdear and Kumhof (2016) discusses a wider variety of stability issues.

28 Arkansas offers one historical example where, for a couple of years during the Civil War, small denomination bonds circulated. But that happened only after they became receivable for taxes at par (Burdekin and Weidenmier (2008)).

29 According to this theory, different types of economic activities are uniquely assigned to special accounts, each with its own budget constraint. As a result, a dollar destined to be spent on a vacation is not perceived as being the same as a dollar to be spent on groceries.

debt. Central bank e-cash issued against government debt could also support financial stability (Barrdear and Kumhof (2016)).

4.3.3 The transition to a cashless society

Phasing out cash, to make space for e-cash, is another potential source of instability. Convertibility upon demand into banknotes or coins, or some other tangible store of value is important for traditional e-money, and it should remain an important element of competition between traditional and alternative currencies, especially in periods of financial instability. Cash is considered a "safe haven" in periods of crisis or negative interest rates. For example, some institutional investors are currently implementing physical cash-hoarding strategies and respectable fund managers are advocating storing physical currency to better diversity portfolios (Bloomberg (2016b), The Telegraph (2015)). However, if e-cash and cash coexist, then the tradeoff between e-cash and cash may create significant swings in currency flows in and out of depository institutions in periods of crisis. This concern may suggest a reason to gradually phase out physical currency, once an electronic alternative is made available. Another advantage of doing central banking without circulating coins and banknotes is that the liquidity would never leave the system. Depending on how the system is constructed, this might decrease vulnerability to bank runs. For example, Broadbent (2016) notes that, if the central bank engaged in deposit taking, then it might make deposits safer because "the central bank can't run out of cash and therefore can't suffer a 'run'." This would also affect other costs, as it would impact the way in which banks finance their lending activities. This is something that should be carefully studied.

Phasing out physical cash could also effectively remove the zero lower bound on interest rates — so central bank e-cash could easily support negative interest rates.[30] This is because current monetary models assume zero nominal interest rates as the lower bound of monetary policy. Below zero, there is an arbitrage opportunity available (Hicks (1935) and (1937)), as borrowing to buy cash is profitable and it is preferable to convert deposits into cash. Issuing e-cash while abolishing physical cash could thus — according to some observers — expand the set of monetary policy options. If policy is ineffective at the zero lower bound, then this could be an advantage in periods of crisis, as it would simplify the implementation of monetary policy. A caveat is that it is unclear whether the zero lower bound reduces the effectiveness of monetary policy (Swanson and Williams (2014)). Moreover, there already exists an array of non-standard policy instruments that offer opportunities for central banks to overcome zero lower bound constraints (Cœuré (2015)). Naturally, we do not yet know the consequences of charging rates below a negative value that accounts for the costs of storing and shipping cash for a prolonged period of time. Although some have noted this may create instability (Bech and Malkhozov (2016)),[31] this remains an important research question.

4.3.4 System security

Physical cash is subject to the problem of counterfeiting, but e-cash is unlikely to be immune from security problems either. An e-cash system would take the form of a network operating through internet connections. Governments have been known to purposefully shut down internet traffic on a regional or local scale to achieve political objectives.[32] Large scale internet disruptions can also occur that are entirely accidental, as happened in Algeria in 2015 when an undersea cable was cut, or could be intentional. Another problem is the possibility of distributed-denial-of-service attacks that shut down specific internet sites. Attacks of this type are becoming increasingly sophisticated and common against governments and private companies alike (NYT (2016)), which is a concern because blockchain-based instruments such as Bitcoin are typically managed and

[30] According to the deputy governor of the Bank of England: "[...] were a CBDC fully to displace paper currency, that would open the door to the possibility of materially negative interest rates […] But that would require explicitly abolishing cash, not just introducing an electronic alternative." (Broadbent (2016)).

[31] The demand for cash has so far remained stable in those countries with negative interest rates; Bech and Malkhozov (2016) note that "the fact that retail bank customers have so far been shielded from negative rates has probably played a key role in keeping the demand for cash stable."

[32] Recently, Bahrain shut down local internet access to thwart protests. https://bahrainwatch.org/blog/2016/08/03/bahrain-internet-curfew/

stored using website-based applications. The security of protocols to avoid "double spending" of the instrument is also something that should be thoroughly investigated. On the positive side, an e-cash system has the potential to be rapidly put to use nationwide during a crisis, when the only alternative would be transporting and distributing physical cash over a large area. From this perspective, an e-cash system could increase stability in times of crisis and boost the overall resilience of the payments system. Naturally, the e-cash system should be designed to ensure wide and easy access to liquidity across the whole of society, including vulnerable citizens such as elderly or disabled people.

5 Additional considerations

There are two additional issues that a central bank should consider in studying the possibility of issuing e-cash. One is the size of externalities associated with the use of physical currency in illicit and criminal activities. The other involves the implications that e-cash would have for the privacy of individuals.

5.1 Cash and crime

Some observers have asserted that cash and, in particular, large denomination notes are empirically integral to crime and tax evasion, and so should be eliminated. Rogoff (2014) asserts that the "major uses [of cash] seem to be buried in the world underground and illegal economy." Sands (2016) claims that "Illegal money flows pose a massive challenge to all societies, rich and poor." Summers (2016) calls for "a global agreement to stop issuing notes worth more than say $50 or $100."

This newfound interest in the connection between cash and crime is noteworthy and puzzling at the same time. First, it seems to imply causality, that cash ultimately causes crime, when, in fact, we should be talking about correlation. Even so, it is hard to quantify how massive the "challenge to all societies" stemming from the correlation between crime and cash is relative to, say, crime and fraudulent accounting practices (e.g., Enron or Parmalat frauds) or crime and commercial bank money (e.g. lending by Italy's BNL branch in Atlanta during the 80s). It is true that increasing the costs from using cash could decrease the amount of crime correlated with it. However, on the one hand, this might as well lead to instrument substitution not problem resolution (e.g. consider the questionable uses of Bitcoin) and, on the other hand, if cash exists to facilitate trade, then it is an empirical question how the inefficiency induced by removing cash would stack against the efficiency gain from reducing cash-related negative externalities (Camera (2001)).

Second, the view that removing large denomination notes is instrumental to fighting crime seems naïve. Large denomination banknotes are usually the dominant component in the sovereign currency supply. In the U.S., $100 bills represent about ¾ of the total currency supply. Prohibiting, or stigmatizing, possession of those notes would simply shift demand to the remaining ¼ of smaller-size banknote supply. This would surely increase the cost to criminals,[33] but would also create shortages and increased cash-management costs for everyone else. Finally, there does not seem to be much empirical evidence that removing large denomination notes is instrumental in fighting crime: in the U.S., large denomination notes have been removed over time — this has also happened in Sweden — but one could hardly make the case that this ultimately led to a general decrease in criminal activity. Additional empirical research in this area would be beneficial.

[33] One of the advantages of larger sizes is less onerous storage and transportation. One million dollars composed of $100 bills fits in a small backpack.

5.2 Privacy

One of the unique traits of cash transactions is that they help preserve privacy, which is a basic human right.[34] It has been argued that, since cash enhances privacy, then cash must be primarily used to hide misconduct and so it should be eliminated. This argument suffers from a basic fallacy (not all those who prize privacy commit crimes) and again implies causality (privacy ultimately causes misconduct) that has not been established as far as I know. Furthermore, privacy is an important element of many activities — such as research with patent application potential or strategic business decisions — where economic agents have nothing to hide from enforcement agencies or contractual counterparties (Solove (2011)). As a result, the privacy offered by currency-based transactions may be beneficial if information is likely to be misused by opportunistic counterparties (Kahn et al. (2005)). In summary, the tradeoff between advantages and disadvantages of a currency that cannot guarantee privacy is potentially difficult, and should be carefully considered in setting up an e-cash system.

6 Conclusion

Technological innovation has opened the door to cash-like instruments that are electronic and no longer require the costly layers of financial intermediaries we use nowadays to settle payments. Instruments with features of this kind — variously called digital, crypto, and virtual currencies — have so far been supplied by private issuers. But currency systems are public goods, and private currencies are more likely to be associated with risks and inefficiencies, such as credibility, instability and volatility, compared to sovereign currencies issued by countries with historically efficient institutions. This suggests there could be societal benefits from public players — such as a trusted central bank — playing a primary role in currency innovation.

A central bank with a track record of being independent is in a unique position to ensure continuity and confidence in the payment system by providing a clear framework and price anchors for the new currency instrument, something that is an issue in the volatile world of privately-issued abstract currencies such as Bitcoin. To further increase trust, the framework should explicitly discuss — through legally binding agreements — if e-cash is convertible into cash upon demand, and if there are limits to the central bank's ability to charge negative interest rates or charge fees on e-cash accounts, as a way to limit the perceived downside risk of e-cash. A clear operating framework is also behaviorally important to maximize use and adoption of an electronic alternative to cash.

How should a new e-cash system be organized? I do not see many advantages in adopting a strongly centralized structure, one in which the central bank issues the currency instrument and *also* provides services or products that have been traditionally offered by commercial banks on currency deposits. In fact, depending on how the system is set up, there may not be a clear distinction between e-cash and deposits (Broadbent (2016)). It is reasonable to leverage the comparative advantage of the financial sector in providing financial services and to develop products that suit individuals and businesses' needs. In this scenario, the central bank would take the primary role of issuing the new currency instrument, designing the architecture of the system, and setting the operating standards.

Many questions, theoretical and empirical, remain open. Future central bank research should be devoted to (i) narrowing down a set of possible operating frameworks to set up an e-cash system, (ii) assessing and quantifying the possible risks during the transition period, (iii) studying the consequences for the structure of banks and the monetary transmission channels, and (iv) identifying new tools and procedures to manage those risks.

One problem with providing answers to some of these questions is the lack of data. For example, how would the payment system function without traditional physical currency? And would it be

[34] Privacy is discussed in Article 12 of The Universal Declaration of Human Rights. http://www.un.org/en/universal-declaration-human-rights/index.html

optimal to simply remove all physical cash or could there be unintended repercussions for the stability of the monetary and financial system? Naturally, we have no field data that can shed empirical light on these kinds of questions. A viable solution would be for central banks to adopt the experimental methodology (Smith 1994) of collecting laboratory data to study a relevant theoretical operating principle, or to establish empirical regularities. For instance, if a theory suggests a given set of conditions under which phasing out physical cash is optimal, then laboratory experiments may help us validate that intuition, and determine if there are theoretically unforeseen aspects that should be taken into account.

The emergence of new currency-like instruments such as Bitcoin is a game-changer in our societies. It opens the door to transferring and storing value in ways that are simpler, faster and truly global. Many of the questions that revolve around this paradigm shift are still open, so the considerations I have made in this document should not be taken to be conclusive findings. My intention is to offer a perspective — at times speculative — which is based on existing theoretical and behavioral research in economics, which I hope can be helpful to those approaching the topic of currency innovation.

References

Abreu, D., D. Pierce and E. Stacchetti (1990), “Toward a Theory of Discounted Repeated Games with Imperfect Monitoring”, *Econometrica*, Vol. 58, pp. 1041-1063.

Ali, R, J. Barrdear, R. Clews and J. Southgate (2014a), “Innovations in payment technologies and the emergence of digital currencies“, *Bank of England Quarterly Bulletin*, Vol. 54, No. 3, pp. 262-275.

Ali, R, J. Barrdear, R. Clews and J. Southgate (2014b), “The economics of digital currencies”, *Bank of England Quarterly Bulletin*, Vol. 54, No. 3, pp. 276-286.

Alsterlind, Jan, Hanna Armelius, David Forsman, Björn Jönsson and Anna-Lena Wretman (2015), ”How far can the repo rate be cut?” *Sveriges Riksbank Economic Commentaries*, No. 11.

Bank for International Settlements (2015), *Digital currencies*, Committee on Payments and Market Infrastructures.

Barrdear, John and Michael Kumhof (2016), “The macroeconomics of central bank issued digital currencies”, *Staff Working Paper*, No. 605, Bank of England.

Bech, Morten and Aytek Malkhozov (2016), “How have central banks implemented negative policy rates?”, *Bank for International Settlements Quarterly Review*, pp. 31-44.

Bitcoin Magazine (2016), “Are Any Altcoins Currenty Useful? No, Says Monero Developer Riccardo Spagni”, March 23rd, 2016, available at https://bitcoinmagazine.com/articles/are-any-altcoins-currenty-useful-no-says-monero-developer-riccardo-spagni-1458743546

Bigoni, M., Camera, G. and M. Casari (2015) “Money is More than Memory”, *Economic Science Institute Working Paper*, No. 14-17, Chapman University, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2664134

Bloomberg (2016a), “Blythe Masters Firm Raises Cash, Wins Australian Contract”, January 21, 2016.

Bloomberg (2016b), “Cash in Vaults Tested by Munich Re”, available at www.bloomberg.com/news/articles/2016-03-16/munich-re-rebels-against-ecb-with-plan-to-store-cash-in-vaults

Board of Governors of the Federal Reserve System (2016), *Currency and Coin Services,* available at www.federalreserve.gov/paymentsystems/coin_about.htm

Boehme, Rainer, Nicolas Christin, Benjamin Edelman and Tyler Moore (2015), “Bitcoin: Economics, Technology, and Governance”, *Journal of Economic Perspectives*, Vol. 29, No. 2, pp. 213-238

Brainard, Lael (2016), “Distributed Ledger Technology: Implications for Payments, Clearing, and Settlement”, speech at Institute of International Finance Annual Meeting Panel on Blockchain.

Broadbent, B. (2016), “Central banks and digital currencies”, speech at London School of Economics on 2-3-2016, available at www.bankofengland.co.uk/publications/Pages/speeches/2016/886.aspx

Burdekin R. and M. Weidenmier (2008), “Can Interest-Bearing Money Circulate? A Small-Denomination Arkansan Experiment, 1861-63”, *Journal of Money, Credit and Banking*, Vol. 40, No. 1, pp. 233-241.

Camera, G. (2001), “Dirty money”, *Journal of Monetary Economics*, Vol. 47, No. 2, pp. 377–415.

Camera, G. and M. Casari (2009), “Cooperation among strangers under the shadow of the future”, *American Economic Review*, Vol. 99, No. 3, pp. 979-1005.

Camera, G. and M. Casari (2014), “The Coordination Value of Monetary Exchange: Experimental Evidence”, *American Economic Journal: Microeconomics*, Vol. 6, No. 1, pp. 290-314.

Camera, G., M. Casari and M. Bigoni (2012), “Cooperative strategies in anonymous economies: an experiment”, “*Games and Economic Behavior*, Vol. 75, pp. 570–586.

Camera, G., Casari, M. and M. Bigoni (2013), “Money and trust among strangers”, *proceedings of the National Academy of Sciences*, Vol. 110, No. 37 pp. 14889-14893.

Camera, G., Casari, M. and S. Bortolotti (2016), “An experiment on retail payments systems”, *Journal of Money, Credit and Banking*, Vol. 48, No. 2–3, pp. 363-392.

Camera, G., C. Noussair, and S. Tucker (2003), “Rate-of-return dominance and efficiency in an experimental economy”, *Economic Theory*, Vol. 22, No. 3, pp. 629–660.

Cass D. and K. Shell (1980), “In Defense of a Basic Approach”, in *Models of monetary economies*, pp. 251-260, Ed. by Kareken, J. and N. Wallace, Minneapolis: Federal Reserve Bank of Minneapolis.

Cœuré, Benoît (2015), “How binding is the zero lower bound?”, Conference speech, 18 May 2015, available at www.ecb.europa.eu/press/key/date/2015/html/sp150519.en.html

Cooper, Russell and Andrew John (1988), “Coordinating Coordination Failures in Keynesian Models”, *Quarterly Journal of Economics*, Vol. 103, No.3, pp. 441-463

Corbae, D, T. Temzelides and R. Wright (2003), “Directed matching and monetary exchange”, *Econometrica*, Vol. 71, No. 3, pp. 731-756.

Danezis, George and Sarah Meiklejohn (2016), “Centrally Banked Cryptocurrencies”, available at www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf

Decker, Christian and Roger Wattenhofer (2015), “A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels”, Stabilization, Safety, and Security of Distributed Systems, *Lecture Notes in Computer Science*, Vol. 9212, pp. 3-18. Springer International Publishing.

The Economist (2015), “The great chain of being sure about things”, October 21st edition.

Ecuador Embassy in the US, “10 Things to Know about Ecuador's Electronic Payment System”, available at www.ecuador.org/blog/?p=4184

European Banking Authority (2014), *EBA opinion on ‘virtual currencies,* EBA/Op/2014/08.

European Central Bank (2015a), *Virtual currency schemes –a further analysis*, available at www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

European Central Bank (2015b), “What is money?”, available at www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html

Fan, Yifei (2016), “On Digital Currencies, Central Banks Should Lead”, *Bloomberg View*, September 1, available at www.bloomberg.com/view/articles/2016-09-01/on-digital-currencies-central-banks-should-lead

Faust, J. (1989), “Supernovas in monetary theory: Does the ultimate sunspot rule out money?” *American Economic Review*, Vol. 79, No. 4, pp. 872–881.

Friedman, James W. (1971), “A Non-Cooperative Equilibrium for Supergames”, *Review of Economic Studies*, Vol. 38, pp. 1-12.

Goldberg, D. (2012), “The tax-foundation theory of fiat money”, *Economic Theory*, Vol. 50, pp. 489-497

Goodhart, Charles A.E. (1998), “The two concepts of money: implications for the analysis of optimal currency areas”, *European Journal of Political Economy*, Vol. 14, pp. 407-432

Greif, Avner (2006), “The Birth of Impersonal Exchange: The Community Responsibility System and Impartial Justice”, *Journal of Economic Perspectives*, Vol. 20, No. 2, pp. 221-236.

Hancock, Diana and David B. Humphrey (1998), “Payment transactions, instruments, and systems: A survey”, *Journal of Banking & Finance*, Vol. 21, pp. 1573- 1624.

Haslag, Joseph H. (1998), “Seigniorage Revenue and Monetary Policy”, *Federal Reserve Bank of Dallas Economic Review*, pp. 10-20.

Hicks, J.R. (1935), “A Suggestion for Simplifying the Theory of Money”, *Economica*, Vol. 2, No. 5, pp. 1-19.

Hicks, J. R. (1937), “Mr. Keynes and the "Classics"; A Suggested Interpretation”, *Econometrica*, Vol. 5, No. 2, pp. 147–159.

Humphrey, David B, Moshe Kim and Bent Vale (2001), “Realizing the Gains from Electronic Payments: Costs, Pricing, and Payment Choice”, *Journal of Money, Credit and Banking*, Vol. 33, No. 2, pp. 216-34.

Humphrey, David B. (2010), “Retail payments: New contributions, empirical results, and unanswered questions”, *Journal of Banking and Finance*, Vol. 34, pp. 1729-1737

Huynh, Kim, Schmidt-Dengler, P., Stix, H. (2013), ”Whenever and Wherever: The Role of Card Acceptance in the Transaction Demand for Money”, unpublished manuscript, Bank of Canada.

Kahn, Charles M., James McAndrews and William Roberds (2005), “Money Is Privacy”, *International Economic Review,* Vol. 46, No. 2, pp. 377-399.

Kandori, M. (1992), “Social Norms and Community Enforcement”, *Review of Economic Studies*, Vol. 59, No. 1, pp. 63-80.

Klee, E. (2008), “How people pay: Evidence from grocery store data”, *Journal of Monetary Economics*, Vol. 55, pp. 526-541.

Klein, M. and M. Neumann (1990), “Seigniorage: what is it and who gets it?”, *Weltwirtschaftliches Archiv*, Vol. 126, 205-221.

Kocherlakota, Narayana R. (1998), “Money is memory”, *Journal of Economic Theory*, Vol. 81, No. 2, pp. 232–51.

Krugman, Paul (2010), “What Is Money?2, *New York Times*, December 15 edition

Krugman, Paul (2013), “Bitcoin is Evil”, *New York Times*, December 28 edition.

McLeay, Michael, Amar Radia and Ryland Thomas (2014), “Money in the modern economy: an introduction”, *Bank of England Quarterly Bulletin*, pp. 4-13.

Milgrom, Paul R., Douglass C. North, and Barry R. Weingast (1990), “The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs”, *Economics and Politics*, vol. 2, No. 1, pp. 1–23.

NACHA (2016), “What is ACH?: Quick Facts About the Automated Clearing House (ACH) Network”, available at www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network

Nakamoto, Satoshi (2008), “Bitcoin: A Peer-to-Peer Electronic Cash System”, available at https://bitcoin.org/bitcoin.pdf

New York Times (2016), “Australia's Controversial Census in Chaos After Possible Cyber Attack”, August 10.

Ostroy, Joseph M. (1973), “The Informational Efficiency of Monetary Exchange”, *American Economic Review*, vol. 63, No. 4, pp. 597-610.

Ostroy, Joseph M. and Ross M. Starr (1974), “Money and the Decentralization of Exchange”, *Econometrica*, Vol. 42, No. 6, pp. 1093-1113.

Ostroy, Joseph M., and Ross M. Starr (1990), “The Transactions Role of Money”, *Handbook of Monetary Economics*, Vol. 1, eds. Benjamin M. Friedman and Frank H. Hahn, pp. 3–62, Amsterdam: Elsevier.

Polanyi, Karl (1957), “The semantics of money uses”, reprinted in *Primitive, archaic and modern economies: essays of Karl Polanyi,* G. Dalton, ed. Garden City: Doubleday, pp.175-190.

Ritter, J. A. (1995), “The Transition from Barter to Fiat Money2, *American Economic Review*, Vol. 85, No. 1, pp. 134-149.

Rogoff, Kenneth S. (2014), “Costs and Benefits to Phasing Out Paper Currency”, *NBER Macroeconomics Annual*, Vol. 29, ed. Jonathan Parker and Michael Woodford. Chicago: University of Chicago Press. Forthcoming.

Sands, Peter (2016), “Making it Harder for the Bad Guys: The Case for Eliminating High Denomination Notes”, Harvard University, *M-RCBG Associate Working Paper Series*, No. 52.

Schmiedel, H., G. Kostova and W. Ruttenberg (2012), "The Social and Private Costs of Retail Payment Instruments—A European Perspective", *European Central Bank. Occasional Paper Series*, No. 137.

Segendorf, Björn and Thomas Jansson (2012), "The Cost of Consumer Payments in Sweden", *Sveriges Riksbank Working Paper Series,* No. 262.

Segendorf, Björn and Anna Wilbe (2014), "Does cash have any future as legal tender?", *Sveriges Riksbank Economic Commentaries*, No. 9.

Segendorf, Björn and Anna-Lena Wretman, (2015), "The Swedish payment market in transformation", *Sveriges Riksbank Economic Review*, No. 3.

Skingsley, Cecilia (2016), "Should the Riksbank issue e-krona?", Speech at FinTech Stockholm on 16-11-2016.

Solove, D. J. (2011), *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press.

Smith, Vernon L. (1994), "Economics in the Laboratory", *Journal of Economic Perspectives,* Vol. 8, No. 1, pp. 113-131

Starr, R.M. (1974), "The price of money in a pure exchange monetary economy with taxation", *Econometrica,* Vol. 42, pp. 45-54

Summers, Larry (2016), "It's time to kill the $100 bill", *The Washington Post*, February 16.

Swanson, Eric T. and John C. Williams (2014), "Measuring the Effect of the Zero Lower Bound on Medium- and Longer-Term Interest Rates", *American Economic Review* Vol. 104, pp. 3154-3185.

The Telegraph (2015), "It's time to hold physical cash,' says one of Britain's most senior fund managers.'' By A. Oxlade, 20 June 2015, available at www.telegraph.co.uk/finance/personalfinance/investing/11686199/Its-time-to-hold-physical-cash-says-one-of-Britains-most-senior-fund-managers.html

Townsend, R. (1987), "Economic Organization with Limited Communication", *American Economic Review*, Vol. 77, No. 5, pp. 954-971

Tobin, James (1985), "Financial Innovation and Deregulation in Perspective", *Bank of Japan Monetary and Economic Studies,* Vol. 3, No. 2, pp. 19-29. Reprinted in Y. Suzuki and H. Yomo, eds., *Financial Innovation and Monetary Policy: Asia and the West*, Tokyo: University of Tokyo Press (1986), pp. 31-42.

UK Government Office for Science (2016), "Distributed Ledger Technology: beyond block chain", UK Government Chief Scientific Adviser.

Van der Horst, Frank and Ester Matthijsen (2013), "The irrationality of payment behavior", DNB, *DNB Occasional Studies*, 11(4)

Van Huyk, J., R. Battalio, and R. Beil (1990), "Tacit Coordination Games, Strategic Uncertainty, and Coordination Failure", *American Economic Review*, Vol. pp. 80, 234-248.

World Bank (2011), "Payment Systems Worldwide: a Snapshot".