CAPCO

Journal

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

Transformational

Strains of Digital Money

Ignacio Mas

APEX 2016 AWARD WINNER

FINANCIAL TECHNOLOGY

Download the full version of The Journal available at CAPCO.COM/INSTITUTE

#44
11.2016

Empowering the Financial World

FISGLOBAL.COM

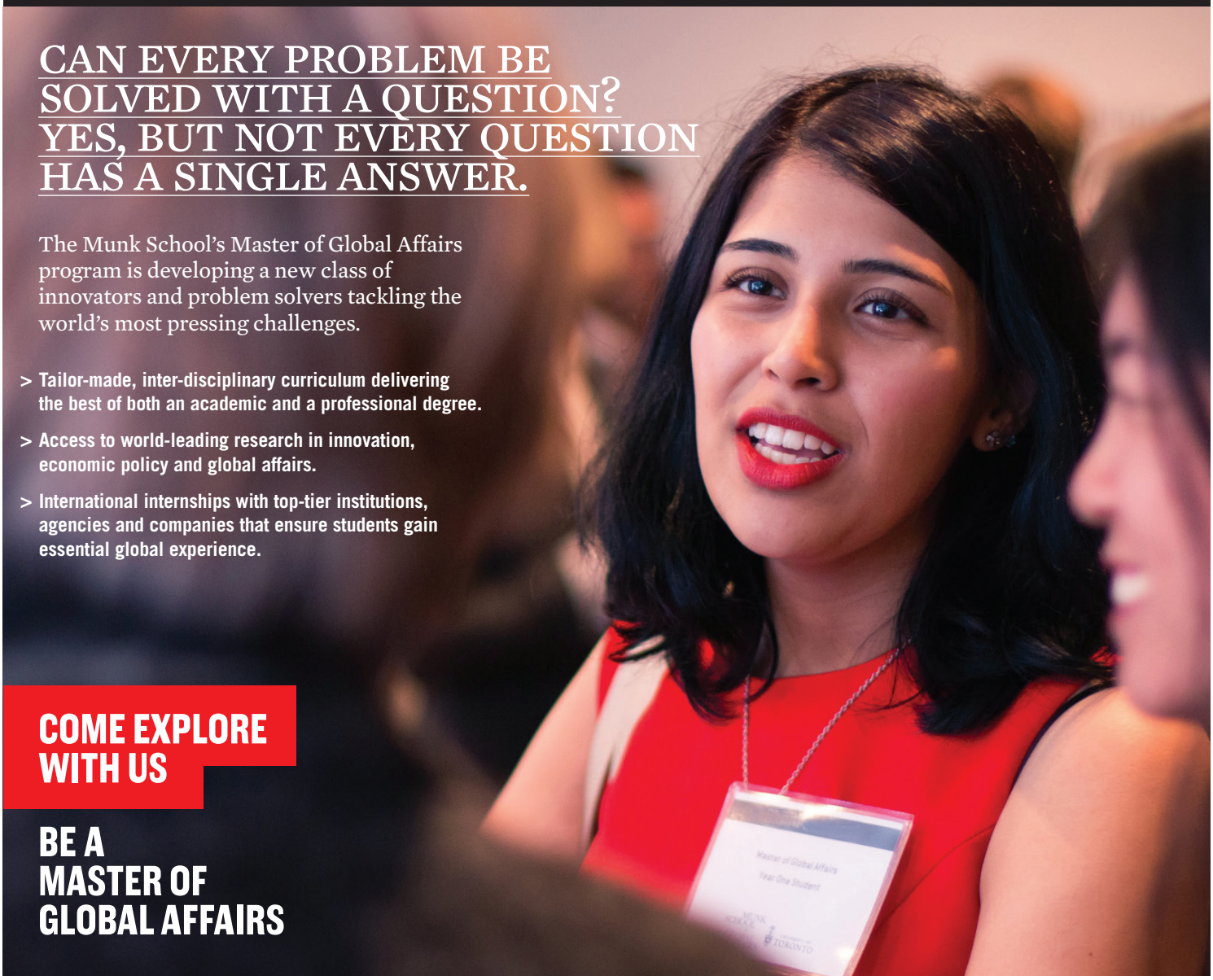
FIS

Journal

The Capco Institute Journal of Financial Transformation

Recipient of the Apex Award for Publication Excellence

WHAT ARE THE DRIVERS AND DISRUPTIONS THAT DETERMINE INNOVATION AND PROSPERITY?



CAN EVERY PROBLEM BE SOLVED WITH A QUESTION? YES, BUT NOT EVERY QUESTION HAS A SINGLE ANSWER.

The Munk School's Master of Global Affairs program is developing a new class of innovators and problem solvers tackling the world's most pressing challenges.

- > Tailor-made, inter-disciplinary curriculum delivering the best of both an academic and a professional degree.
- > Access to world-leading research in innovation, economic policy and global affairs.
- > International internships with top-tier institutions, agencies and companies that ensure students gain essential global experience.

COME EXPLORE WITH US

BE A MASTER OF GLOBAL AFFAIRS

MUNKSCHOOL.UTORONTO.CA
MGA@UTORONTO.CA

MUNK SCHOOL OF GLOBAL AFFAIRS
UNIVERSITY OF TORONTO

Financial Technology

Operational

Transformational

Strains of Digital Money

Ignacio Mas – Senior Fellow, Council on Emerging Market Enterprises, Fletcher School of Law and Diplomacy, Tufts University[1]

Abstract

This paper provides a basic framework that explains how the major types of known digital money solutions relate to each other, i.e., what the similarities and differences are, and hence the pros and cons of each. The broader purpose is to offer some perspectives on how digital money grids might evolve in the future, so as to make them safer, more convenient and user friendly, more contestable by different providers, and much cheaper than current systems.

1 I would like to thank Gabriela Andrade of the Inter-American Development Bank (IDB) for her encouragement and support for this project, and the IDB for funding the work.

INTRODUCTION

It is easy to feel overwhelmed these days by the sheer volume of innovations around digital money and payments. Some are promoted by existing players, and some are offered by new ones. Some tackle specific points of customer convenience, and some aim for greater safety and robustness. Some feel incremental, and some feel disruptive.

The specific purpose of this paper is to provide a basic framework that explains how the major types of known digital money solutions relate to each other, i.e., what the similarities and differences are, and hence the pros and cons of each. The broader purpose is to offer fresh new perspectives on how digital money grids[2] might be pieced together in the future, so as to make them: (i) safer, technologically and operationally; (ii) more convenient, user friendly, and useful by making them easier to integrate into broader digital solutions (i.e., more programmable); (iii) more contestable by different providers, creating more of a level playing field and stronger incentives to innovate; and (iv) much cheaper than current systems, especially for micro-transactions, which to this day remain unsupported by efficient payment mechanisms and yet constitute the vast majority of transactions in the mass market.

This paper first looks at the user side and examines what it means fundamentally to shift from physical money, which the majority of people are used to and engage with daily, to digital money, which has yet to be discovered by half the world's population. Where are the main customer tensions and anxieties likely to lie? This is the first sense in which the word "strains" is used in the title of this paper. The following two sections then look at the different varieties of digital money that have been deployed, which is the second – and main – sense in which the word is used. The concluding section reviews the major opportunities presented by the emergence of digital money, beyond simply replicating the characteristics of cash but without the hassle of requiring physical support.

Down the path of digital money there is much opportunity for efficiency as well as disruption, for integration and fragmentation, for inclusion and relegation. Those strains again.

THE CONSEQUENCES OF DEMATERIALIZING CASH

The most salient characteristic of cash is, of course, its tangibility.[3] Notes and coins can be thought of as objects, albeit ones subjected to rather unusual legal rules and deep-seated social conventions. Digital money removes the physical support for individual lumps of money, which has profound consequences that go to the root of the concept of money. The more obvious consequence that is often drawn is that digital money requires users to engage in a higher level of abstraction when using it. The sensory experience with cash brings concreteness. The implication is that poor people, in particular, will require substantial accompaniment and education in order for them to become comfortable with even conceiving of dematerialized or virtualized money.

But, that view ignores several millennia of history, as well as everyday informal financial practices that we see everywhere today. The fact is that for most people who do not use digital money, a good proportion of their money already is, and has always been, virtual, in the form of the money that they are variously owed or that they could otherwise obtain from others in their community. Think of all the informal loans, reciprocal favors, income sharing entitlements, and outright gifts that form the social and financial fabric of traditional societies. Virtual money is in fact virtually ageless: that must be the case, because the first and most basic role of money, that of unit of account (the yardstick by which all debts can be measured and netted off), is necessarily an artificial concept, a result of social constructs and legal institutions (see Box 1).

The second major consequence of digitizing money is that using it in any way – whether to check the amount held or to pass it on to someone else – requires access to an infrastructure. Digital money cannot be understood narrowly as a virtual thing, it must be thought of as an entire acceptance system. Notes and coins, in contrast, can be counted and exchanged directly: they are discretized objects that work on an entirely stand-alone basis. It is not that physical cash requires no acceptance, but that it can be accepted visually. All you need to ascertain the value of notes and coins is contained within them; it does not require the help of any external device. The primary purpose of the paper on a note is to carry an increasing range of visual (and tactile) acceptance cues. In dismissing physical cash as an outdated relic, we often forget how much of a technological feat that represents (see Box 2).

The implication is that, unlike with physical money, the discussion of the properties of digital money cannot be separated from the configuration of the rails on which it runs. Digital money may not present a conceptual challenge to people as a unit of account, but it will be

2 The notion of a digital money grid is further developed in a companion piece, which explores various scenarios for getting there. See: Mas, I. and G. Andrade, 2015, "A digital money grid for modern citizenship: Latin American scenarios, 2015-25." Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1725103&download=yes

3 It is estimated that only 8% of the world's money exists as physical cash, the rest is in the form of bank deposits (source: Grabianowski, G., 2016, "Forms of currency: electronic," in How Money Works blog, accessed on September 14, http://bit.ly/1V2ztQY. But money in the bank is actually money in a computer, so it counts as a "strain" of digital money.

Monetary economists explain the rise of modern financial arrangements as a logical sequence: first barter, then currency, then credit systems, finally double-entry book-keeping – a natural evolution towards higher levels of abstraction and complexity in trading arrangements. A long lineage of anthropologists have disputed this, finding no evidence that human societies ever worked on barter. In the beginning there was debt, as people variously shared, gifted and loaned each other stuff. The fabled "coincidence of wants" problem that makes barter so impractical (the fact that at the market you and I can only transact if I want your chicken and you want my goats) was solved by separating transactions in time (now I take something from you, later you will take something from me), developing simple debt tracking devices (such as the tally stick), developing various moral codes to guide the sizing and fulfillment of these dues, and periodically netting out the various debts across people in the community.

As David Graeber puts it in his book "Debt: the first 500 years"; "abstract systems of accounting emerged long before the use of any particular token of exchange." The primary need was to create common notions of value, not necessarily to harmonize how value got stored or passed around. So in the beginning money only fulfilled a unit of value or accounting function; means of payment and storage of value came later, much later. The startling conclusion is that "there's nothing new about virtual money. Actually, this was the original form of money."

People everywhere seem to have no problem managing the "artistry" of gifting – an even more intangible and convoluted practice than exchanging digital money. You can see generosity and balanced reciprocity leading to mutual insurance. But you can equally see dependence and charity preserving hierarchy. In Graeber's eloquent words, gifts "are usually fraught with many layers of love, envy, pride, spite, community solidarity, or any of a dozen other things." There is nothing simple about that, but somehow people work out a proper response to gifts (whether they are an honor, a provocation, or a form of patronage) intuitively.

Hence, there is no reason to believe that dealing with abstract notions of digital money should, in itself, be a barrier for ordinary people who are used to informal debt and reciprocity arrangements. The real challenge will be the formalization of finance: making them accustomed to reducing financial arrangements to a bunch of numbers and financial relationships to impersonal arithmetic.

Removing the social context from transactions may obliterate much of the intuition and survival strategies people have developed around money matters for centuries. As Johnson et al (2012)[4] vividly explain, the social dimension of informal finance allows for much more open-ended negotiability of resources in case of exceptional need. And it is not all casual: reading the typologies of informal financial mechanisms documented by Rutherford (1996)[5], Wright (1999)[6] and others, one wonders at how inventive and recurring certain structures are. Those can only be the result of a natural evolutionary process based on variation (fed by the inherent flexibility of social arrangements) and selection (the disciplinary and insurance benefits they bring).

With formal finance, all that is replaced by binding credit limits, inflexible terms made up by someone, and an imposed moral requiring you to repay your debts on time (the "criminalization of debt [non-repayment]," to use Graeber's graphic if hyperbolic language). The core problem of digital finance for poor people is then not how intangible it is, but rather how explicit everything becomes. Being more discreet may be an advantage, but must it all become so discrete too? To end with Graeber: "When matters are too clear cut, that introduces its own sorts of problems."

Box 1 – Virtual money is virtually ageless[7]

rejected if it does not provide adequate mechanisms to access it as a store of value and as a means of payment.

It is not fruitful, then, to discuss digital money in the abstract, we can only talk meaningfully in the context of specific instances of digital money systems – how the rails are made and laid out. In comparing different digital money architectures, it is convenient to split the discussion into two parts: the rules and mechanisms around the creation (and destruction) or issuance of digital money, and the rules and mechanisms for acceptance (i.e., validation and exchange, of money outstanding.

4 Johnson, S., G. Brown, and C. Fouillet, 2012, "The search for inclusion in Kenya's financial landscape: the rift revealed summary report" FSD Kenya, March 1.
5 Rutherford, S., 1996, A critical typology of financial services for the poor, ActionAid
6 Wright, G. A. N., 1999, "A critical review of savings services in Africa and elsewhere," MicroSave
7 This box is drawn from Mas, I., 2013, "Virtual money is virtually ageless," in MicroSave Financial Inclusion in Action blog, August.

Hard cash certainly has its drawbacks. Poor people mired in a cash economy find it difficult, in times of need, to support or seek support from distant relatives and friends. The size of the market they can sell their products and wares into or source their inputs from is limited by how far they can easily and securely transport cash. They are captive to local financial organizations and moneylenders, because more distant financial institutions do not find it cost effective to go collect their saved-up cash and have no visibility of their prior cash-based financial histories on which they might otherwise grant credit.

All of these are good reasons to expect that people everywhere will embrace digital money, if only it is served up to them in a convenient, understandable, reliable, and secure way. Money is just information – how much I have, how much I owe – and the short history of the internet shows us that information wants to become free of physical impedances.

So will cash go the way of the compact disk, in a gradual wind-down towards oblivion? Must we, or even can we, go for an accelerated eradication of cash? Many hope so, but I do not think so. The CD is simply digital information bottled up for convenient transport. Once devices became ubiquitously connected, there was no longer any reason for musical information to be delivered through a physical distribution network rather than online. But cash is more than just bottled-up information on financial value: it is value that is readily and universally recognized and accepted on mere visual inspection. The physicality of banknotes makes it easy for people to make snap judgments on how much value it embodies and whether it is a real banknote or not. Cash is a visual acceptance instrument, in contrast to electronic money which requires electronic acceptance (an ATM, a point-of-sale terminal, a mobile phone) in order to be recognized and exchanged. Electronic acceptance introduces risks that when you want to pay with electronic money there may not be a device available, that it may not work properly, that it may be tampered with, or that the information on that payment will be passed on to third parties (including the taxman). It takes a long time to overcome these fears, which is why the shift to electronic money is so slow and gradual, even in the most developed countries.

So, here you have the basic trade-off: electronic money is superior to physical cash in transport and storage (lower transaction costs), but cash has advantages over digital money in acceptance (immediacy, universality and privacy). Digital music, in contrast, requires electronic acceptance (i.e., translation of stored digital signals into sounds) whether it is delivered as a compact disk or online. The compact disk involves much transport pain and no acceptance gain. That is why it will end up going away, as have done the specialist stores that sell them.

Box 2 – Will hard cash go the way of the compact disk?[8]

A TAXONOMY OF DIGITAL MONEY ISSUANCE MECHANISMS

For money to retain its value, a key requirement is that it be a finite resource. The limitation on the supply side can come from a scarce underlying resource that the money is a claim on, outright promises made by the issuer within certain rules imposed by a legal code and governance structure, and (nowadays) the software code that implements the money management protocol. It, therefore, matters who the issuer is and under what parameters it determines the money supply. These are key determinants of the trust that economic agents will place on various strains of money.

The main mechanisms that money issuers have used to inject trust in their product are discussed below.

Fully backed (or reserved) money

Traditionally, money has represented a claim on a scarce physical resource, typically a naturally occurring, pure commodity such as gold or silver. Such metallic standards dominated international financial systems before World War II. The growth in the quantity of these assets is linked to the rate of discovery of the asset, which itself is a function of the sheer availability of the commodity in the ground and the amount of labor and cost incurred in finding, extracting, transporting, and refining it.[9] The assets can embody significant labor and skill to turn what may be an inherently unlimited asset such as limestone into a scarce commodity – for instance, in the form of heavy stone wheels used in the Island of Yap.[10]

8 This box is drawn from Mas, I., 2013, "Will hard cash go the way of the compact disc?" All about finance blog, World Bank, November.

9 Of course, in a commodity-linked standard, the money supply would also be affected by the demand for the commodity for uses other than as a monetary reserve, such as the gold used for jewelry or that hoarded as a private store of value.

10 These were thick, round stones of a diameter of 1-12 feet, with a hole in the middle to facilitate transportation with a pole. The limestone used to make them had to come from another island some 400 miles away from Yap. See Friedman, M., 1994, "The island of stone money," in Friedman. M. (ed.), Money mischief: episodes in monetary history, Harcourt Brace & Co.

		HOW IS THE MONEY SUPPLY DETERMINED?				
		Who is the issuer?	**Discretionarily, under broad policy and governance rules**	**Under explicit prudential ratios and standards**	**100% reserved**	**Pre-set under mathematical rule**
HOW IS THE MONEY DENOMINATED?	**In national currency**	Central bank			E-money accounts (Ecuador)	
		Licensed bank		Commercial bank deposits		
		Licensed non-bank			E-money accounts	
		Any, unlicensed	Store gift cards, cellular airtime			
	Private numeraire	Any, unlicensed	Frequent flyer miles & other loyalty point schemes			Crypto-currencies

Table 1 – Main issuance models for digital money

The backing for a national currency can also be in the form of other major currencies held as reserves by the central bank. Under a currency board system, the law requires that local currency in circulation must be 100% backed with international reserves.[11] Domestic non-bank money issuers (including payment system providers such as PayPal, prepaid card providers such as VISA-branded cards, and mobile money operators such as M-PESA) are also legally required to reserve the totality of the value of their money outstanding with safe and liquid assets, usually as deposits in prudentially regulated banks or in short-term government obligations. Of course, when a particular form of money is backed by other types of money held in reserve (as is the case with currency boards and non-bank issuers), the value of the issuer's obligations may be fully reserved, but the reserves they hold themselves may not be fully reserved by their issuer. This gives rise to a mixed trust system.

Prudentially managed money

Unlike non-bank prepaid card and payment service providers, licensed commercial banks are authorized to issue money that is not fully backed by safe, liquid assets. They create new money every time they give out a loan and create a deposit in the borrower's name with the corresponding amount.[12] These loans carry the specific risk of the borrower and are not immediately callable or even sellable if there is a need to fund an unexpected demand for depositor withdrawals. To mitigate these credit and liquidity risks, banks are typically subjected to strict prudential standards relating to the amount of capital and reserves they must hold, and the quality of the borrowers they can loan to or assets they can invest in, as well as certain governance and accounting rules. This turns the lack of backing for bank money into a calculated risk. Given the predominance of bank money within today's monetary system and the interdependence of banks to supply liquidity to each other in moments of need, this presents the risk of extended bank failures leading to potentially severe systemic risks. Commercial banks' activities tend to be heavily regulated to mitigate these risks.

Fiat (promise-based) money

For most national currencies today, the currency's value does not stem from its convertibility into other assets or the value of reserves held against it by the central bank, but from an inherent trust in the central bank not exploiting its money creation powers. Thus, the issuer retains substantial discretionary powers to fix the money supply arbitrarily. Though central banks generally must abide by some broad governance rules and policy mandates that curb its powers, these rules are generally not as specific as the kind of prudential rules that apply to commercial banks.

In the same way as reserve currencies (under a metallic standard or currency board) have shown a tendency to become fiat currencies, Milton Friedman explained how the stone money in the island of Yap could equally well become disengaged from the actual number of big stones available. He noted how Yap islanders started trusting that a defined number of big stones existed in the distant island where they came from, thereby saving the cost of having to transport them. At that point, if the large stones got wiped out, they could continue acting as if the stones existed, and nothing in people's behavior in Yap need change.

11 A long-standing currency board is that managed by the Hong Kong Monetary Authority. A notoriously failed currency board was that maintained by the Argentine Central Bank until 2002.

12 For a lucid account of how the process of money creation works, one that is a bit at odds with conventional wisdoms expressed in some standard textbooks, see McLeay, M., A. Radia, and R. Thomas, 2014, "Money creation in the modern economy," Bank of England Quarterly Bulletin Q1, 14-27

In the past, money has also been issued by private entities operating on an unlicensed and unregulated basis. This is now generally banned; private issuance tends to be allowed only for restricted-purpose money, such as store-value cards, and other forms of value that are not directly convertible to cash, such as loyalty points.

A fixed, pre-determined, rule (no discretion)

Monetarist economists have long argued that the growth rate of money supply should be fixed and pre-announced. They believe that unexpected variations in money supply (i.e., decisions imposed discretionarily by the central bank) are ineffective as a policy lever in the long term, and can produce disequilibria in the short term.

Present-day crypto-currencies are governed by an arbitrarily set, fixed money supply path that is coded into the currency's operating system. It is a fixed numerical rule that is enforced through technology rather than legally. In the case of bitcoin (BTC), the total supply is scheduled to grow at a diminishing rate until 2140, when the amount of BTCs stabilizes at 21 million and no new ones will be issued subsequently. In the case of Ripple (XRP), the supply was set at a fixed, invariant amount of 100 billion from the outset. However, in both these currencies, a substantial share of the currency outstanding is held by the early promoters of each system, and thus can be released at any time into public circulation at their discretion. Hence, the crypto-currency holding public is implicitly placing some trust in the actions of the currency promoters.[13]

The distinguishing characteristic of the issuance models

We can discern three critical dimensions that distinguish the various issuance models described above, as depicted in Table 1.[14] One critical distinction is the numeraire that is used. What is the currency in which the units of value are denominated: is the digital money linked to the national currency, or does it have its own, private denomination? Another key distinction is who the issuer is. This ranges from the national monetary authority (or central bank) issuing national currency at the top of the money food chain, through various categories of licensed financial institutions issuing money denominated in the national currency, to unlicensed entities issuing their own proprietary currencies. The third dimension, captured in the columns in Table 1, is the degree of discretion that the issuer has in determining or affecting the money supply. The scope for discretion may be limited by broad policy or governance rules, a more specific set of prudential standards and ratios (on capital, liquidity and reserve requirements), a mechanistic full reserving requirement, or a fixed mathematical rule.

Most electronic money in circulation today is issued by licensed financial institutions, under a strict prudential regime if they are banks or under an even stricter full reservation regime if they are non-banks (such as e-money issuers, payment service providers, and mobile money operators). These types of money are denominated in the national currency, so they are in principle a close equivalent to, or substitute for, central bank-issued money. But still, these forms of money are not legally and economically identical to national currency, for two reasons:

Issuer risk: a dollar note issued by the central bank is only subject to country risk; the risk that the government may undermine the value of its own currency through inflationary policies, or outright repudiation or confiscation.[15] But money held in deposit at a commercial bank is, in addition, subject to the bank's idiosyncratic default risk, which may or may not be linked to country risk. Thus, bank money requires trust not only in the central bank as the keeper of the value of the national currency (to which the value of the deposit is pegged) and the national bank supervisor, but also in the management and board of the individual commercial bank. This distinction can be mitigated by the extension of deposit insurance on bank deposits, though that is generally capped.

Legal obligations to accept payment (legal tender): central bank-issued notes and coins generally are designated as legal tender, i.e., they are a form of payment that must be accepted in settlement of pre-existing debts. This is done to ensure that notes and coins are accepted universally within the country's territory. This designation is normally not extended to bank-issued money (deposits) because the state does not see a role in ensuring the tradability of the balances held at individual private banks, which may be subject to some idiosyncratic risks. With the growth of bank money, the notion of legal tender has become much less significant. Nowadays, governments typically place a cap on the transactions that must be accepted with notes and coins of different denominations (to avoid causing problems of procuring change), and many governments in fact cap the

13 In the case of Bitcoin, it is not known how many bitcoins have been kept by its anonymous founder(s) and the early group of miners. But well over half of all bitcoins are known to have never been traded. In the case of Ripple, 80% of all XRPs were gifted by their creator to Ripple Labs, which oversees the Ripple protocol and ecosystem. Ripple Labs has been releasing some of these, such that today 32% of all XRP are held by others. In the case of central banks, money that is printed but not in circulation is not counted within the money supply figures.

14 In this table and throughout the paper we refer to money in a broad, but not necessarily legal, sense. For instance, governments may choose whether to treat bitcoin legally as a commodity rather than as money. This legal distinction can have important consequences, one of which is that if it is treated as a commodity then fluctuations in its price may expose its holders to capital gains taxation.

15 If you think the scenario of a central bank repudiating its own currency is farfetched, you ought to know that there is a long history of just that. Repudiation of the currency amounts to a confiscation of the value of the currency outstanding. Usually it is done covertly, in the form of a currency reform. See: Mas, I., 1995, "Things governments do to money: a recent history of currency reform schemes and scams," Kyklos, October.

Mondex: is a smart card electronic cash system, implemented as a stored-value card and launched in December 1993. Initial public trials of the payment system were carried out from July 1995, and the system was subsequently sold to MasterCard International in 1996.

Mintchip: was a smartcard chip system launched in 2012 by the Royal Canadian Mint. The card stored electronic value, and the system allowed transfers of value across cards.

Octopus/Oyster card: the Octopus card was launched in 1997 as an electronic purse for public transportation in Hong Kong. The Oyster card was launched in London in 2003, also as a form of ticketing for mass transit. Subsequently the use of both cards was extended to other retail settings, beyond transit.

BTC: is a private currency as well as a peer-to-peer payment network that lets users transact directly without needing an intermediary. Transactions are verified by network nodes and recorded in a public distributed ledger called the blockchain. The system works without a central repository or single administrator.

Ripple: is a real-time gross settlement system (RTGS), currency exchange, and remittance network launched in 2012. It is built upon a distributed open source Internet protocol, consensus ledger and native currency called XRP (ripples). Ripple is the second-largest crypto-currency by market capitalization after BTC.

Box 3 – Digital money solutions mentioned in this article[20]

total size of payments that can be made just with cash (to avoid tax evasion and money laundering).[16]

While most forms of digital money are denominated in the national currency and aspire to become as close a substitute as possible for central bank-issued currency, the new breed of crypto-currencies, such as BTC and XRP, represent an alternative currency in their own right.[17] Their value is not pegged to the national currency, and thus must be converted from and into national currency at a floating exchange rate (determined at electronic exchanges). The value in exchange of these currencies is, of course, heavily affected by the credibility of how their supply is managed. Because this trust is not backed by any statutory limitations, they have taken the approach of eliminating all discretionary decision-making and pre-setting the money supply growth path for posterity. This tying-of-the-hands on the supply side in principle makes these currencies more inherently subject to price volatility because there is no way to accommodate demand-side shocks other than through the dynamic adjustment of its price at the exchanges.

The Central Bank of Ecuador has taken an unprecedented step in asserting the monetary authority's role in electronic money issuance by launching its own electronic money system. Others may follow Ecuador's lead. The governor of the central bank of Bangladesh has recently proposed replacing all cash with central bank-issued electronic money.[18] At the other extreme, Argentina is said to be one of the leading countries in terms of regular BTC use by ordinary people for real commercial transactions, perhaps due to its turbulent recent monetary history that has undermined the credibility of national authorities in handling money issuance responsibly.[19]

It should also be noted that these forms of money are often complements to each other, rather than substitutes. For instance, central bank notes and coins may fulfill the need for small-denomination transactions, whereas commercial bank deposits fulfill the need for larger-denomination transactions. E-money accounts may compete with bank accounts at the retail level, but their very existence relies on there being bank deposits that back the amount of e-money in circulation. Airtime balances (privately issued money denominated in national currency) can only be bought with an acceptable form of convertible money.

16 For instance, European Regulation EC 974/98 limits the number of coins that can be offered for payment to fifty. In Canada, a payment in coins is a legal tender for no more than $40 if the denomination is $2 or greater but does not exceed $10, no more than $25 if the denomination is $1, and so on. In Spain, payments in excess of €2,500 cannot be made with cash and must be made electronically; in France, the cash payment limit is €1,000. Source: Yoteasesoro (2014), posted online on March 15, http://bit.ly/2cppUxF.

17 Throughout this paper we refer to crypto-currencies as a form of money, but many governments do not legally accept them as a form of money because they ban private monies. Instead, some governments choose to interpret crypto-currencies as virtual commodities. This is not only a legal technicality, as it affects their tax treatment: holders of commodities – but not money – are required to pay income tax on any capital gains they obtain upon their sale.

18 The Ecuadorean mobile money system developed and managed by the Banco Central del Ecuador is described in its homepage http://www.dineroelectronico.ec/. See the statements made by Dr Atiul Rhaman of the Bank of Bangladesh in Islam, S., 2015, "BB governor for e-currency to fit in digital Bangladesh," Financial Express, February, 15, http://bit.ly/2cwLdch.

19 For a vivid description of the bitcoin scene in Buenos Aires, see Popper, N., 2015, "Can Bitcoin conquer Argentina?" The New York Times Magazine, 3 March.

20 Some of the text in this box is taken from the respective Wikipedia entries.

A TAXONOMY OF DIGITAL MONEY ACCEPTANCE MECHANISMS

Once money has been issued, it must be handled as a uniquely held property claim: holders of legal monetary value must be able to establish command over accumulated balances, including the possibility of transferring balances to others or to exchange it into other forms of money. For the system to work well, there are three requirements: (i) no parties other than the issuer should be able to create new money (i.e., no counterfeit); (ii) no two parties should be able to establish claim to the same amount of money (i.e., unambiguous, rivalrous ownership); and (iii) no party should be able to use or pay out with the same money twice (i.e., no double-spend).

One's claim over money can be established in several ways:

As a bearer instrument (anonymous)
With physical forms of money, such as central bank-issued notes and coins, but also store coupons, the value is embedded within the monetary token itself. Money can, therefore, be handled entirely in bearer form, without requiring any identifying information or conducting any form of identity checks on the parties involved. Holders of notes and coins can pay out simply by handing out their physical money tokens, and all recipients need to do is to (visually, and maybe tactilely) check the integrity of the money tokens received.

For electronic money to be handled in this way, it is necessary for it to be embedded within and passed around through a physical device. This usually takes the form of stored-value card systems, where the value is stored within the card itself rather than in a remote server. Typically, smartcards with a chip are used as these have full digital read/write capabilities and hence the value on the card can be adjusted over time as it is used.

A high profile early example of such a system was Mondex, which was developed and trialed in the early 1990s. A more recent example is MintChip, launched by the Royal Canadian Mint in 2012. Both of these systems failed to take root, likely for two main reasons. First, these systems are costly to roll out because they require spreading new dedicated and expensive cards and new payment acceptance devices across the entire user base. Second, if cards are lost or stolen the value embedded within them is irrevocably foregone, so users tend to adopt them only for very specific, low-value purposes.[21]

More successful versions of stored value smartcard systems have tended to be restricted within specific usage domains. Smartcard systems have been successfully rolled out in mass-transit systems, starting with the Octopus card in Hong Kong and followed by the Oyster card in London. More recently, they are spreading as store value cards, such as the Starbucks card, offering convenient payment at the point of sale and a hook for loyalty programs. These restricted-use systems are easier to push into the market than general money schemes such as Mondex and MintChip because all acceptance points are controlled by the same company and hence can be converted overnight (e.g., equipping turn-styles at the subway to accept card payments). Moreover, because the value is only expected to trade at defined locations (such as at subway stations or at Starbucks stores), it is easier to ensure that all transaction points are online, establishing the possibility of backing up card values in central servers to recover stored value in case of loss or theft of the card.[22]

As a centralized account system (usually identity-based)
In most forms of digital money, the value is not stored primarily within devices held by users but rather in an account maintained by the provider. In other words, the information on who owns how much money is centralized.[23] User-held physical tokens such as cards may still be used, but their role is circumscribed to identifying the user and storing the account number details, but they do not in any way hold or represent monetary value by themselves.

More formally, customer identity information operates at three levels:[24]

- Each digital account – whether held at a bank, payment service provider, or mobile money operator – must be given a unique identifier, usually an account number. If only this identification level is used, the result is anonymous accounts, such as the Swiss numbered accounts of old where the only information one needed to present to gain access to an account was the secret account number.
- Additionally, digital account owners are typically assigned a set of unique authentication credentials (such as a card, the user's mobile phone number, a PIN, or a set of secret personal

21 This problem can be solved by maintaining a register of the value in all cards within servers in the network or cloud. This then requires that all transactions be conducted online, so that the server(s) can be updated in real time. Some intelligent systems, such as Net1's UEPS of South Africa, stores recent transaction histories in all cards (the payers' and the recipients'), so that balances can be reconstructed if some cards are lost even if they had done some recent transactions offline. Their system depends on cards synching their transaction history often enough, but not all the time.

22 For a detailed case study comparing the experiences of Mondex and the Octopus card, see Mas, I., and S. Rotman, 2008, "Going cashless at the point of sale: hits and misses in developed countries," CGAP Focus Note, No. 51, December. Available at: https://www.cgap.org/sites/default/files/CGAP-Focus-Note-Going-Cashless-at-the-Point-of%20Sale-Hits-and-Misses-in-Developed-Countries-Sep-2008.pdf

23 Of course, there is a fine line between this and the instances referred to earlier where money balances are held on the card and backed up into central servers. Technically, the distinction is which entity is presumed to have the right balance when there is a discrepancy between the account balance stored in the card and the balance held on the centralized server.

24 For a fuller treatment of the meaning of identity and common identification mechanisms, see Mas, I., and D. Porteous, 2015, "Minding the identity gaps," Innovations 10:1-2, 27-52.

questions) that they must use to establish their ownership over the account number, and hence to operate the account. By separating the account number from the user identification credentials, account numbers can now be shared publicly, for instance in order to solicit direct payment from others. Moreover, security is usually enhanced by requiring two distinct authentication factors, unlike the Swiss numbered accounts that operate on the single authentication factor represented by knowledge of the secret account number.

- In addition, the account issuer may link the account number and its associated authentication credentials to a verified legal identity. This is often a regulatory requirement imposed on licensed financial institutions, known as know your customer (KYC), though there may be exemptions for low-value accounts.

Thus, in contraposition to bearer systems, account-based systems are based on two distinct sets of capabilities: those relating to identity (being able to establish you are the rightful owner of the funds in your account, and to designate the intended recipient in a money transfer) and those relating to the accounting or ledger system (keeping track of balances held and owed, and authorizing transactions when there are sufficient funds per the account rules).

As a public, decentralized account system (pseudonymous)

Crypto-currencies have brought a disruptive new approach to the ledger system that supports the management of user accounts. Instead of having different institutions uniquely control their own ledgers, crypto-currencies work on the basis of a globally distributed ledger that is not controlled or managed by any single party. The ledger is decentralized in the dual sense that there is no central authority, and there are many instances of the ledger since any user (or node) in the network can gain access to a copy of the ledger. Ripple and Stellar are the two leading systems operating on this basis.[25]

A publicly available, decentralized global ledger has several advantages. First, it removes the power of individual organizations from imposing their access and pricing conditions; the market ought in principle to become more contestable and fair. Second, it automatically ensures interoperability across all players in the system since all are operating from the same global accounting system. The result ought to be stronger network effects and lower cost of providing transactional services.

But there are two major challenges associated with operating a public, decentralized ledger, that Ripple has had to design around:

- In a centralized account-based system, the account issuer is responsible for ensuring that all transactions are properly authorized and recorded in the system. Because there is no central authority in the Ripple system, this needs to be replaced by a system that creates consensus across all nodes on the system about which transactions are valid and hence should be used to irrevocably update all account balances. Ripple has created a complex algorithm under which all nodes vote on the validity of recent transactions they have become aware of. Transactions are deemed final once 80% of nodes vote them as being valid, and it may take several rounds of voting before this threshold is reached. This voting process is typically run and completed every five seconds or so.
- In a centralized account-based system, account balances are visible only to the account owner and the account issuer, and the issuer is duty-bound to maintain confidentiality. But on the Ripple system, anyone can query the global ledger, so the accounts cannot be directly linked to legal identities, as this would raise serious privacy concerns. Instead, users are identified by a pseudonym – technically, a private key that only they know and which they can use to sign transactions they wish to undertake from their account but without necessarily revealing their legal identity.

As a public chain of transactions (pseudonymous)

The BTC protocol, and particularly the blockchain technology it implements, has introduced a different mechanism for managing the validity of digital money claims, one that is neither embodied within a device nor account-based: through a historical record of its provenance. The closest analogy is the role that historical records proving the age, ownership transfers, and state of conservation of old art masterpieces play in attributing paintings to famous artists. The more complete the provenance, the stronger the attribution.[26] BTCs can be thought of as purely software-based tokens that represent control over a certain amount of money. These virtual tokens encode two crucial pieces of information, relating to the identity of the current owner of the money and its provenance. The identity part is done

25 Ripple Labs, the promoters of Ripple, are now positioning their platform as one that can power banks' business rather than bypassing them. Several banks, including Germany's Fidor and U.S.-based CBW and Cross River Bank, have embraced the Ripple platform. Source: Ferency, D., C. French, H. Tran, and S. Gibbs, 2015, "The internet of finance: unleashing the potential of blockchain technology," CMM Research Note, Institute for International Finance, April 16.

26 There is an interesting parallel between the stone money of Yap Island and bitcoin. When a transaction occurred, the big stones were not physically moved to the premises of the new owner nor were they marked in any way. Instead, the fact that they had changed hands was announced publicly and it became a matter of collective memory. The stones could all continue being housed together, and it was clear who was entitled to what stones. See: Ettinger, G., 2013, "The island of stone bitcoins," Lets Talk Bitcoin blog, September 15, http://bit.ly/2d28aHi.

through public key encryption, under which the token is "locked" with a public encryption key to which only the valid owner of the money has the corresponding private key. The provenance part is done by attaching a pointer to the previous virtual token where the value emanated from. The holder of a valid token (i.e., one to which they have the corresponding private key and that has a provenance that checks out fully in history all the way back to the moment of the money's creation) can effect a transaction by creating a new token, which contains the public key of the money's recipient and a pointer to the previous token. The previous token becomes spent, and hence no longer valid, because there is now a newer token that points to it. The new token is valid because it points to a previously valid token and no newer token points to it.

All these tokens – in effect, transaction histories – are collected in what is known as the blockchain. The blockchain must be freely searchable by anyone wishing to check the validity of any money they receive and hold. It is thus a public ledger, unlike the traditional account-based systems mentioned earlier, which are private ledgers controlled uniquely by individual financial institutions. Given this decentralized, public nature of the blockchain, there also needs to be a process for extending the blockchain as new transactions occur, one that drives a consensus among all parties as to which of the newly reported transactions are valid and should, therefore, enter the blockchain. The BTC protocol implements this through a process called mining, under which every ten minutes a specific entity (a miner) earns the right to append to the blockchain a new block of transactions they deem to be valid. Miners earn that right by being the first to solve a complex mathematical problem, so that miners who are willing to expend most computing resources are most likely to succeed.[27]

The BTC protocol is not account-based in the sense that the underlying value of each amount of BTC that you hold must be established independently, since each will have a different provenance. In account-based systems, on the other hand, once you prove ownership over the account, you gain control over the entire balance in it. However, most users are likely to experience BTC as an account because there is BTC wallet software that implements the BTC protocol in the background, thereby sheltering the user from directly having to manage disparate public/private keys and checking multiple BTC provenances.

As with Ripple, the BTC protocol is not based on anonymity because all BTCs need to be linked to a public key that their owner can use to claim the money. However, it is not identity-based in the sense that this public key cannot be directly linked back to a legal identity. The public key thus becomes a form of pseudonym for its owner. Anyone can see and trace all the transactions performed under the pseudonym, but the pseudonym itself is held anonymously. Thus, the system performs as if it were anonymous, only as long as users are able to hold their ownership of keys secret. As soon as public keys are linked to specific identities, their entire transaction history with that key becomes exposed.

		HOW IS OWNERSHIP ESTABLISHED?		
		Anonymous, with hardware token or device	Pseudonymous, software-based (using public key infrastructure)	Linked to identity, with mixed factor authentication
HOW IS VALIDITY ESTABLISHED?	Decentralized, directly from token	Stored-value smartcards		
	Checking public consensus ledger of past transactions		Ripple protocol	
	Checking public consensus ledger of current holdings		BTC protocol using public blockchain	
	Account issuers checking their private ledgers		Private blockchains on BTC protocol	Bank & e-money accounts

Table 2 – Main models for managing ownership rights over digital money

Based on the above discussion, there are two main differences between the various digital money systems, as shown in Table 2. The columns capture how the ownership over one's digital money is established: whether that comes with the possession of a physical device (analogously to how coins and notes work), access to encryption keys that work like a virtual or software token, or the use of multiple (generally two) factors of authentication that allow an account to be linked to an underlying identity. The rows capture how the validity of the money itself is established: whether it is done in an entirely decentralized fashion through direct manipulation of the tokens, in a distributed fashion by checking a public ledger that represents a consensus of past transactions or of current monetary holdings, or in a centralized fashion by requesting the account issuer to confirm the monetary value against their private ledger.

In the same way that various issuance models can complement each other, these various acceptance mechanisms can also work together and support each other. An example is the BTC protocol,

27 This is where it gets very technical, but the overall logic is that basing the mining rights on what is called a proof-of-work protocol (that combines the demonstration of raw computing power with some element of luck) ensures the stability of the blockchain itself. For more on how the bitcoin protocol works, see Box 4 and Mas, I., 2014, "Why you should care about bitcoin, even if you don't believe in it," mimeo, April. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1769124

The mining process implemented by BTC is designed to ensure that only valid transactions are captured in the blockchain, in the right sequence. The mining process runs every ten minutes or so, and results in a new block being appended to the blockchain that records the transactions that have been deemed valid during the last ten-minute interval. The blockchain has thus been growing since its inception many ten-minute intervals ago, such that at any point in time it represents the full record of all transactions that have ever been done using the BTC protocol. The blockchain is propagated to all nodes in the network, so that each node can reach the same conclusions as to whether certain BTCs that a user is proposing to use to pay someone else are valid or not.

Advocates of cryptocurrency systems such as Ripple and Bitcoin argue that they offer the possibility of much lower transaction costs than those we are accustomed to with our existing interbank infrastructure. First, these platforms can operate on generic internet infrastructure rather than on purpose-designed, proprietary systems. Second, by eliminating any central control over the ledgers, no player can exercise pricing control over the ensuing payment services. Third, the protocol enforces a standard so that all nodes in the network are interoperable; this lays the basis for reaping global network effects, in contraposition to traditional payment systems that are a patchwork of variously interconnected payment islands. On the other hand, critics argue that the system is not as cheap as it appears. First, the distributed, peer-to-peer nature of the ledger means that the same ledger information must be replicated, communicated and stored many times. It, therefore, ought to use up far more network resources in total than a centralized system that maintains at most a few instances of the ledger. Second, the mining process is extremely costly in terms of the computing power miners must expend, as well as in terms of the corresponding electric power that is used up in the process. Third, while per-transaction fees earned by miners is currently very low, this will change as the reward offered to miners is set to decrease over time and to disappear altogether eventually. In the meantime, the miners' reward acts as an inflation tax on existing holders of BTC, which is a form of hidden transaction tax.[28]

In addition, the operation of crypto-currency systems such as Ripple and Bitcoin raise a number of regulatory issues for central banks, beyond purely fiscal and monetary aspects: (i) there are systemic issues relating to the stability, integrity, and reliability of the crypto-currency protocol itself, i.e., the set of rules embedded in software which govern how the system works; (ii) there are operational, technological, and prudential issues relating to the firms offering digital currency services on top of the payment platform, such as hosted wallet providers, currency exchanges, and merchant payment processors; and (iii) there are conduct issues, particularly those relating to KYC and anti-money laundering (AML), given the pseudonymous nature of these services.

Box 4 – Benefits, costs, and risks of crypto-currencies

which can operate on a public, distributed blockchain as described above, but also on a private blockchain basis. Because the protocol is freely available on an open source basis, it can be implemented by private players on a closed network, centrally controlled basis. For instance, private blockchains could be used to cwonduct transactions among users served by the same wallet provider or in the same closed user group, leaving the public blockchain to record transactions between users of different providers or closed user groups. This might achieve a better tradeoff between efficiency (which generally favors centralization of information and authorizations) and universality (which generally favors decentralization).[29] On the other hand, the proliferation of private blockchains would introduce layers of opacity on the BTC system, hence potentially undermining its core objective of transparency.[30]

Most digital money in circulation today is managed in centralized fashion by licensed institutions that operate private account ledgers, and are linked to verified identities via authentication credentials that have been issued to each user. This is as far as it gets from physical cash, which is inherently anonymous and operates on an entirely decentralized fashion. We look at the implications of that below.

28 For an analysis of the sustainability of Bitcoin's low transaction fees, see: Ali, R., J. Barrdear, and R. Clews, "The economics of digital currencies," Bank of England Quarterly Bulletin 54:3, 276-286.

29 Moreover, the creation of private blockchains on top of the public blockchain might help address the scalability issues of the latter, which demands replication of the blockchain data at every node and broadcasting of transactions network-wide. Under a mixed model, only certain transactions (presumably larger ones, or those involving unconnected parties) would place a network burden, and the rest would be handled in centralized blockchains that need not be propagated to all nodes. See: Beikverdi, A., 2015, "How trustless off-blockchain transactions could solve the block size problem," op-ed, Cointelegraph.com, May 31, http://bit.ly/2cyZ041.

30 Private players offering off-blockchain transactions could in theory operate with less than full backing in terms of the volume of actual bitcoins they hold relative to the bitcoin exposure they absorb on behalf of their transacting customers. Off-blockchain operators could, therefore, have the effect of expanding BTC issuance on a fractional reserve basis. See: Carey, D., 2014, "Are off-block chain transactions bad for bitcoin?" Coindesk.com, May 14, http://bit.ly/1iMERPR.

Attributes of cash	Adaptation in digital money systems
Anonymity: no need for personal identification of sender	Most forms of digital money require the holder to present some form of credentials to gain access to the device, wallet application, account, or software tokens that holds the value. Moreover, because these credentials are likely to be persistent over multiple uses, all ledger-based systems, whether public or private, are in principle traceable: transactions can be linked to each other, if not back to the user's legal identity. Only stored-value systems implemented entirely in user devices can provide full anonymity.
Payment convenience: no need to specify identity or address of recipient	Digital money transfers must always entail addressing of money to the proper recipient. However, this can be hidden from users in proximity payment situations such as at a store if the payment instruments of sender and recipient can communicate directly. This can be done, for instance, by inserting cards into POS devices, bumping of mobile devices, or employing short radio communication interfaces such as NFC, Bluetooth, or infrared.
Universal technical acceptance: no need for specific acceptance technology	All forms of digital money require the use of electronic devices to request and confirm transactions. This introduces several potential problems. First, it creates the possibility of encountering situations where one cannot transact despite having enough digital money, if the device of either payer or recipient is malfunctioning or is not otherwise available. Second, it may create compatibility issues between senders and receivers, if they are not on the same digital money system. Their devices must be able to communicate and negotiate the transaction appropriately, and their providers need to agree to interoperate. Third, it creates large adoptions costs, as new systems and the evolution of existing ones require the upgrading of devices across the user base.
Universal legal acceptance: legal tender:	Digital money is usually not assigned legal tender status because it is generally issued by private entities and hence carry at least notional issuer default and fraud risk. This could change if central banks follow the lead of the central bank of Ecuador in issuing and managing its own form electronic money.
Instantaneous settlement: no counterparty risk	Payments using server-based digital money will usually imply at least some micro delays associated with network communications for issuing and confirming transactions, which creates at least the theoretical risk of an instantaneous counterparty risk while the transaction is being completed. These delays can be significant where network communications are poor.
Fixed denominations: available in standard amounts	Paying from a digital money account or wallet requires gaining access to the full digital money balance. It is hard to replicate the fixed-denomination feature of bank notes digitally, as this would require holding a number of sub-accounts, each with their unique numbers and credentials. The fixed-denomination feature of cash can be very useful in specific use cases where people want to cap how much money they carry with them. On the other hand, the ability to define the precise transaction amount makes the notion of giving change completely unnecessary in digital money transaction.

Table 3 – Cash versus digital money

BETTER THAN CASH?

So is digital money better than hard cash? The drawbacks of physical cash are clear: (i) transactions leave no record so they do not build up a financial history and balances cannot be regenerated in case of loss; (ii) cash transactions entail high transaction costs associated with the conveyance of cash, especially in remote payment situations, and present the problem of procuring change which may be scarce in some environments; and (iii) because of its more conspicuous nature, cash may be particularly subject to loss through theft, as well as the passing of counterfeit money.

But hard cash has some remarkable features that have stood the test of time. What do we lose when we transition to digital money systems? Table 3 describes some key attributes of cash and how those are dealt with (or not) in digital money systems, by way of summary of what has been stated previously.

But the emergence of digital money creates opportunities that go beyond simply replicating the characteristics of cash but without the drawbacks of handling a physical product. There are four major trends that digital money is likely to unleash. Each of these presents some exciting opportunities, though they may come with some hard-to-assess risks:

Decentralized and peer-to-peer money services

We are already seeing digital money spawning a new ecosystem of online price comparison sites, neutral peer-to-peer marketplaces, crowdfunding sites, online service aggregators, and specialized online financial service providers with innovative savings, credit, and international remittance models.[31] The new breed of crypto-currencies brings the concept of peer-to-peer services to the core function of money transfers – people being able to pass money to each other without involving any service provider. Many of these new models aim to disintermediate traditional players, who have long enjoyed a substantial degree of control over the market. All this serves to create more service options and choices for users. As a greater number and more diverse types of players vie for customers' attention, there are greater incentives to innovate and reduce prices.

However, managing risks, especially system-wide risks, may be harder in this more complex ecosystem. It may be harder to regulate and effectively supervise consumer protection risks, as the range of players involved and the complexity of their offerings increase. There may be much greater scope for regulatory arbitrage, as business models

31 For a categorization, analysis and leading case study of each of these new digital financial service models, see Mas, I., 2014, "Using broadband to enhance financial inclusion," IDB discussion paper no.: IDB-DP-427

morph and adapt to changing regulatory environments. It may be harder to quantify overindebtedness risks as product definitions and provider categories become blurred. And a rise in crypto-currencies may enable massive flight-to-safety flows out of financial institutions in case of a banking crisis, thereby aggravating systemic liquidity risks.

Programmable money

A particular source of innovation will likely be the embedding of money and transactions in software. Payments could be triggered automatically form any application, including social networking sites (such as Facebook or Twitter) and personal productivity tools (such as Google Calendar). Digital money could be earmarked for specific purposes only and special kinds of money could be tracked, creating a digital version of colored coins. Crypto-currency payments could be linked to the underlying asset purchased, thereby creating an automatic register of asset ownership right in the blockchain.

Bitcoin itself has an in-built scripting capability that allows some conditions to be placed on BTC payments, though it is quite limited in its programming power. Other crypto-currencies, such as Ethereum, have been designed with a much more flexible native application environment. In addition, there are services such as Codius that provide hosting environments for applications that implement smart contracts automatically on crypto-currencies.[32]

All these applications represent a major shift from finance as a service to finance as an application, much in the same way that Skype and other voice-over-IP applications turned the traditional voice service supplied by telecoms company into a downloadable application. Financial services will increasingly be conceived as apps directly downloadable by users onto their digital wallets, rather than as service upgrades offered by financial services providers.

Enabling true micropayments

Digital money, and especially crypto-currency protocols that run on standard internet infrastructure in peer-to-peer fashion (hence without necessitating dedicated servers and intermediary institutions), have the potential for massively reducing unit transaction costs, down to vanishingly small levels. It may become possible to charge for very small transactions, below the $1 threshold, which today cannot be efficiently charged for electronically.

This can uncover a new nano-economy, including dynamic usage-based pricing on roads and public transport, and supply of products and services on a much more granular piece-work basis. Most importantly, widespread access to micropayments would likely unleash a creative explosion in digital services, as it would open up new paths for content and app developers to monetize their services. This would permit highly fine-tuned charging models for code, pay-per-view models for consumption of small-format online content such as press articles, and small rewards for answers to questions posted on online discussion.

However, there are questions as to how scalable the Bitcoin protocol is, and hence how capable it is of handling the explosion of transactions that would come with micropayments. One solution might be to handle micropayments through private blockchains, as private services offered by micropayment wallet providers working on specific transaction types, communities, or ecosystems. These transactions would be handled and authorized by centralized ledgers controlled by each provider, and would not need to be broadcast, mined, or stored individually within the public blockchain.[33] This amounts to using BTCs as a unit of account, but without using the BTC system (blockchain) as a payments system.

Digital currencies as legal tender

So far, central banks have not been inclined to issue currency in digital format to complement the physical currency formats (notes and coins) we are all familiar with.[34] Central banks have typically delegated the digitization of money at the retail level to licensed institutions, such as commercial banks and e-money issuers. Only central bank-issued currency constitutes legal tender, which means that in practice there is no notion of legal tender for larger transactions. Larger transactions must be settled in forms of money that embody some element of idiosyncratic counterparty risk since they are necessarily liabilities of some entity other than the central bank.

In future, central banks may choose to issue digital currency directly. A digital currency could be used as a settlement system for large-value payment systems, if its use was restricted to larger eligible economic actors. Alternatively, it may function as a retail

32 Smart contracts are programs that formally encode certain conditions and outcomes which have been agreed in advance between certain parties. The code is then faithfully executed by a disinterested, neutral system, such as Codius, based on whether the agreed conditions were met or not. See: Thomas, S., and E. Schwartz, 2014, "Smart oracles: a simple, powerful approach to smart contracts," Codius white paper, July 17, http://bit.ly/1rH2aEo.

33 The natural players for implementing off-blockchain micropayments are hosted BTC wallet providers, since they can validate the BTC holdings of their customers and hence directly clear payments between them. An example is Coinbase, which is said to enable transactions as small as 0.00000001 BTC (equivalent to roughly 5 millionths of a U.S. dollar). See: Gilson, D., 2015, "Coinbase implements zero-fee microtransactions off the block chain," Coinbase, June 18, http://bit.ly/2cLpbTV.

34 There are two narrow exceptions to the statement that central banks do not issue digital currencies. First, it could be argued that commercial banks' excess reserve deposits at the central bank are a form of digital currency, since they are liquid liabilities of the central bank and maintained by servers managed by the central bank. However, this is a highly restricted form of currency since only deposit-taking banks have access to it. Second, as we saw earlier, the central bank of Ecuador has taken the extra step of becoming the national issuer of e-money, which it has designated as legal tender.

payment system if it is made available to everyone, regardless of transaction size, thereby enabling individuals to use it to settle debts between each other directly.

Against these potential benefits, a digital currency may be rejected by people if they fear that the government might use its control over the digital currency systems and protocols as a tool for mass surveillance. There are already reports in Ecuador that such fears are limiting the take up of the central bank's new e-money.

The architecture for such a national digital currency could replicate today's centralized systems with servers controlled by the central bank keeping track of money outstanding and a hierarchy private entities reselling the currency to their customers (akin to the Ecuadorean system). Alternatively, it could be based on a decentralized ledger under a cryptographic payment protocol controlled by the central bank.[35]

CONCLUSION

The rise of information and communication technologies (ICT) over the last twenty years has spawned a tremendous boom of financial service innovations – including all kinds of structured products, derivatives, and risk syndications. This has opened up substantial funding and risk management opportunities for many, but along with that has come a level of complexity and opacity that has been at least partially responsible for the global financial crisis. As the power of ICT continues to unfold, we can expect the innovations to spill from financial services into the nature of money itself. The opportunities as well as the risks may be even more profound.

35 Imagine a bitcoin-like system, except that the BTCs are denominated in U.S. dollars and proclaimed to be legal tender. IBM is reportedly developing such a solution. See: Chavez-Dreyfuss, G., "IBM looking at adopting bitcoin technology for major currencies," Reuters, March 12, http://reut.rs/1QVWfq8.

FINANCIAL COMPUTING & ANALYTICS

STUDENTSHIPS

Four-Year Masters & PhD

for Final Year Undergraduates and Masters Students

As leading banks and funds become more scientific, the demand for excellent PhD students in **computer science, mathematics, statistics, economics, finance** and **physics** is soaring.

In the first major collaboration between the financial services industry and academia, **University College London, London School of Economics,** and **Imperial College London** have established a national PhD training centre in Financial Computing & Analytics with £8m backing from the UK Government and support from twenty leading financial institutions. The Centre covers financial IT, computational finance, financial engineering and business analytics.

The PhD programme is four years with each student following a masters programme in the first year. During years two to four students work on applied research, with support from industry advisors. Financial computing and analytics encompasses a wide range of research areas including mathematical modeling in finance, computational finance, financial IT, quantitative risk management and financial engineering. PhD research areas include stochastic processes, quantitative risk models, financial econometrics, software engineering for financial applications, computational statistics and machine learning, network, high performance computing and statistical signal processing.

The PhD Centre can provide full or fees-only scholarships for UK/EU students, and will endeavour to assist non-UK students in obtaining financial support.

UCL LSE Imperial College London

financialcomputing.org

INDUSTRY PARTNERS

Financial:

Barclays
Bank of America
Bank of England
BNP Paribas
Citi
Credit Suisse
Deutsche Bank
HSBC
LloydsTSB
Merrill Lynch
Morgan Stanley
Nomura
RBS
Thomson Reuters
UBS

Analytics:

BUPA
dunnhumby
SAS
Tesco

MORE INFORMATION

Prof. Philip Treleaven
Centre Director
p.treleaven@ucl.ac.uk

Yonita Carter
Centre Manager
y.carter@ucl.ac.uk

+44 20 7679 0359

Layout, production and coordination: Cypres – Daniel Brandt, Kris Van de Vijver and Pieter Vereertbrugghen

Imperial College Business School | Centre for Global Finance and Technology

Centre for Global Finance and Technology

The Centre for Global Finance and Technology at Imperial College Business School will serve as a hub for multidisciplinary research, business education and global outreach, bringing together leading academics to investigate the impact of technology on finance, business and society.

This interdisciplinary, quantitative research will then feed into new courses and executive education programmes at the Business School and help foster a new generation of fintech experts as well as re-educate existing talent in new financial technologies.

The Centre will also work on providing intellectual guidance to key policymakers and regulators.

"I look forward to the ground-breaking research we will undertake at this new centre, and the challenges and opportunities posed by this new area of research." – Andrei Kirilenko, Director of the Centre for Global Finance and Technology

Find out more here:
imperial.ac.uk/business-school/research/finance/centre-for-global-finance-and-technology/

CAPCO

BANGALORE
BRATISLAVA
BRUSSELS
CHICAGO
DALLAS
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
KUALA LUMPUR
LONDON
NEW YORK
ORLANDO
PARIS
SINGAPORE
TORONTO
VIENNA
ZÜRICH