The Digital Currency Revolution

David Birch

CSFI
Centre for the Study of Financial Innovation

CSFI

The Centre for the Study of Financial Innovation is a non-profit think-tank, established in 1993 to look at future developments in the international financial field – particularly from the point of view of practitioners. Its goals include identifying new areas of business, flagging areas of danger and provoking a debate about key financial issues. The Centre has no ideological brief, beyond a belief in open markets.

This CSFI publication is available through our website www.csfi.org
or by calling the Centre on +44 (0) 20 7621 1056

Published by Centre for the Study of Financial Innovation (CSFI)

Email: info@csfi.org
Web: www.csfi.org

ISBN: 978-1-9997174-8-3

Printed in the United Kingdom by Heron Dawson & Sawyer

Contents

Foreword

These are difficult times. Dave Birch wrote this paper for the CSFI before the coronavirus hit, at a time when the possibility of a global depression was the last thing on almost anyone's mind.

Things have changed. But this too shall pass - and when it does, it may well be that opportunities for radical change will open up in areas that we might have felt were closed.

One such area - where radical change has long been theoretically possible, even desirable, but where it has been blocked by the power of incumbents - is payments. There is nothing new about the idea of digital cash (which goes back to Mondex) or a digital 'token' (which goes back to de Bono's 'IBM Dollar') or even central bank digital cash. But there has always been pushback - from central banks, from commercial banks and from the broader payments ecosystem that makes a healthy living from the existing arrangements (and from the inefficiencies therein).

But no castle is impregnable, and - as Mr Birch explains - the ramparts had already been breached by Mark Zuckerberg's 'Facebucks' initiative (ie Libra) and by the PBoC's announcement of an e-RMB. With the computing power that is now (and, we hope, in the future) available and with the ubiquitous smart phone in place of some fiddly dongle or card reader, we are ripe for a big leap forward.

And, as Mr Birch also points out, central banks shouldn't fight the change. True, there may be seignorage to lose, but - contrary to much of the mythology about smart ledgers - there is a big gain in terms of the authorities' ability to track transactions. And, in the end, this is as much about identity as it is about payments.

So, lift your eyes from our present problems, and look ahead to a bright new, digital world of currencies, tokens and alternative investment markets.

Andrew Hilton
Director
CSFI

CSFI

Number 134 April 2020

The Digital Currency Revolution

David Birch

Introduction

It is now a quarter of a century since a pamphlet that I picked up at the CSFI changed my world view. It was entitled *The IBM Dollar* and it was written by the noted lateral thinker Edward de Bono. His thesis on the future of money was that technological developments in computers, communications and cryptography would mean that the cost of creating money would fall to the point where it would make sense for private organisations to make their own. He suggested, in particular, that it would make economic sense for companies to issue their own currency, rather than use equity (hence the title). He went on to write that he looked forward to a time when "the successors to Bill Gates will have put the successors to Alan Greenspan out of business".

De Bono was arguing that companies could raise money just as governments do now, by printing it — and put forward the idea of private currency as a claim on products or services produced by the issuer, rather than as bank credit. In his formulation, IBM might issue 'IBM Dollars' that would be redeemable for IBM products and services, but also practically tradable for other companies' monies or for other assets. To make such a scheme work, IBM would have to learn to manage the supply of its money to ensure that (with too many vouchers chasing too few goods) inflation did not destroy the value of its creation. But companies should be able to manage that trick at least as easily as governments do, particularly as they have no voters to cope with.

This money would be rather like a corporate bond — a bearer instrument, with no interest, no clearing and no settlement.

The concept is expandable. A start-up launches, and instead of issuing equity or debt, it issues a security that is redeemable against some future service. So, for example, a wind farm start-up might offer money in the form of kilowatt hours that are redeemable five years from now. In the early days, this "money" would trade at a significant discount to take account of the risks inherent in the venture. But once the wind farm is up and running and producing electricity, then the value of the money will rise. There might even, in this case, be a surge in demand for renewable energy that drives its value higher than its original face value.

With millions of these currencies in circulation and constantly being traded on foreign exchange markets, the situation might appear unbearably complex for anyone trying to pay anyone else. However, as de Bono explained, in an "always-on" networked world, this complexity is no barrier to trade:

> *'Pre-agreed algorithms would determine which financial assets were sold by the purchaser of the good or service depending on the value of the transaction. And the supplier of that good or service would know that the incoming funds would be allocated to the appropriate combination of assets as prescribed by another pre-agreed algorithm. Eligible assets will be any financial assets for which there were market clearing prices in real time. The same system could match demands and supplies of financial assets, determine prices and make settlements.'*

Remember, de Bono was writing this before there was a Google — or even Netscape. In his vision, you send me an IBM Dollar and I put it in my wallet. Instead of bank accounts in conventional fiat currency, companies would hold a basket of such currencies. It is worth emphasising that de Bono also wrote that the key would be the ability "of computers to communicate in real time to permit instantaneous verification of the creditworthiness of counterparties" - simultaneously imagining both the always-on internet and the "ambient accountability" of the blockchain.

If that seems far-fetched, let me quote from a just-released white paper produced by the conservative Swiss payment organisation, SIX. In its analysis of "future of money" scenarios, it has one called "moneyless", in which:

> *'…the 'price' of any asset can be displayed in real-time in terms of any other asset. Algorithms scout the most liquid pairs of assets to form a chain of bilateral exchange rates linking the to-be-priced assets with the to-be- priced-in asset. Market makers furthermore provide liquid bilateral exchange rates between different pairs of assets.'*

This is de Bono's argument precisely, and it reminded me that the reason his CSFI pamphlet stopped me in my tracks was that I was already working on systems for decentralised and secure transactions. I immediately recognised that his was not idle speculation but a vision of an inevitable future. Now that the combination of mobile phones, social networks and strong authentication makes the necessary calculus cost-effective even for small transactions, the technology needed to deliver the IBM Dollar is in place. The world of digital money, digital cash and digital currency is upon us. In that world, we should no longer assume that currency will be provided by the nation-state through a central bank. The low cost and wide availability of relevant technologies mean that there is a wide range of public and private alternatives.

It seems to me now that the whole topic of digital currency needs to be explored further. In this paper, I will try to set out the economic and technological imperatives, discuss the potential impact on the international monetary and financial system and start to explore the likely repercussions — economic, social, and political.

I. What Is a Digital Currency?

The topic of digital currency is attracting a great deal of attention, but I find much of the conversation frustrating. I see frequent commentary that almost randomly switches between "virtual money", "cryptocurrency" and "digital fiat", to the point that the terms are essentially meaningless. So before we go any further, I think it might be useful to explore a framework for discussing the topic.

Kevin Werbach has already set out a useful taxonomy, suggesting that:

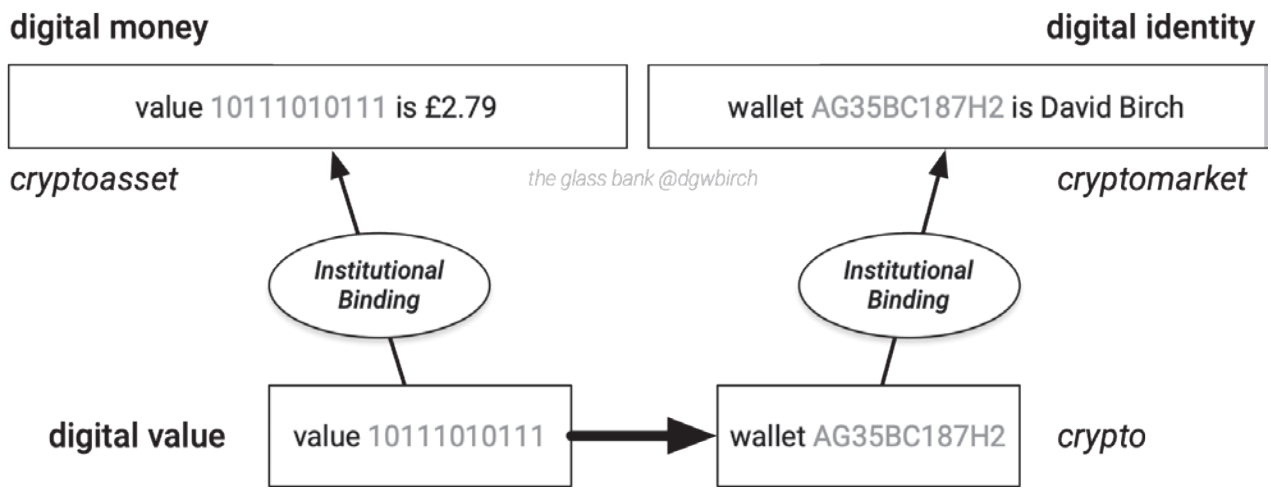
- There is cryptocurrency: the idea that networks can securely transfer value without central points of control;
- There is blockchain: the idea that networks can collectively reach consensus about information across trust boundaries; and
- There are cryptoassets: the idea that virtual currencies can be "financialized" into tradable assets.

I use a generalised approach as shown in Figure 1 below (because a blockchain is only one kind of shared ledger), but Kevin summarises the situation well. His perspective is that cryptocurrency is a revolutionary concept, but that the jury is still out on whether the revolution will succeed, whereas the shared ledger and the assets that might be managed using a shared ledger are game-changing. The idea of such assets, which I will label digital bearer instruments, goes back to the long-ago days of DigiCash and Mondex, but the idea of implementing them using technology that is (in principle) available to every single person on the planet is wholly new.

Here's my take. We have a value transfer layer that may or may not be implemented using a blockchain. This makes for the secure transfer of digital values from one storage area ("wallet") to another. We then build a crypto-asset layer on top of that to link the digital values to something in the real world. Note, of course, that this crypto-asset layer could be null and the digital value itself be the value traded, as in the case of Bitcoin. Either way, we have some form of digital money. We then have a crypto-market layer to link the wallets to entities in the real world (eg, people or companies), giving us digital identity.

In this formulation, the transfer of value is between wallets and there is no clearing or settlement — so the

Figure 1. From Digital Value to Real-World Markets



digital money is a digital bearer instrument (whoever holds the cryptographic key holds the value, whether that value is a dollar, one-thousandth of the Mona Lisa or gold in a depository somewhere). Digital bearer instruments can be exchanged by what the blockchain fraternity insists on calling "smart contracts". The general term for these bearer assets is "tokens", and it is worth diverting for a moment to explain why so many people see the "tokenisation" of financial services as a likely path for the sector.

A. Token solutions

Tokenisation gives literally anybody the ability to deliver money into a global market. Unlike the underlying cryptocurrencies that have no reality beyond the consensus protocols of shared ledgers, tokens obtain their value by linking to assets in the 'real world'. Tokens took off with the ERC-20 standard back in 2015, which defined a way to create a standard form of token using smart contracts on the Ethereum blockchain. Think of them as a new kind of app that executes on shared ledgers. Tokens are a kind of data — fungible value exchanged between these apps; a practical implementation of digital bearer claims on assets with no clearing or settlement involved in their exchange.

Picture this: I want to license some IBM software for IBM$100, so I tell my smart contract to send this value to an IBM smart contract, and the IBM smart contract then creates a permission for me to use the software. Using these tokens, it is even possible to create the smart, programmable money of the future ('this money cannot be used before 1st January, 2030', and so on).
When the current craziness has passed and tokens have become a regulated digital asset — a cross between corporate paper and a loyalty scheme — there will be an opportunity to remake markets in a new and better way. With reputations established through an immutable history of participation in transactions, good behaviour will not be gamed and bad behaviour will be on display. Market participants will be able to assess and manage risk, and regulators will be able to look for patterns and connections. For instance, I will be able to see that your assets exceed your liabilities without necessarily being able to see what those assets or liabilities are. We will find ourselves in an era of "ambient accountability", where the technological architecture means continuous verification and validation.

This is because of the transparency obtained from using modern cryptography in interesting ways. As Salome Parulava and I wrote in *Ambient Accountability: Shared Ledgers, Glass Banks and Radical Transparency in Financial Services*, these technologies give us the possibility of "translucent transactions", where the technological architecture means continuous verification and validation instead of periodic auditing long after the trades and exchanges have taken place.

Billions of dollars flowed into the first generation of ICOs. A great many of them went to Zug (often referred to as "crypto-valley"), because the issuers used Swiss Foundation law to create the tokens. This is why the opinion of the Swiss Financial Market Supervisory Authority (FINMA) is very important. It examined all kinds of tokens, not only ICOs, and looks to regulate them as appropriate. In its guidelines, FINMA classified tokens into three categories: securities, utilities and payments. The US Securities and Exchange Commission (SEC) made a similar distinction, but while SEC chairman Jay Clayton acknowledged that ICOs "can be effective ways for entrepreneurs and others to raise funding", he also cautioned that neither payment nor utility tokens have a safe harbour if they function as securities.

How do these tokens implement de Bono's vision? Well, a start-up launches, and instead of issuing equity, it issues "money" that is redeemable against future services. So, for example, a distributed file storage start-up might offer money in the form of megabyte days that are redeemable five years from now. In the early days, this "money" would trade at a significant discount to take account of the risks inherent in the venture. But once the file system is up and running, then the value of the money should rise. With millions of such currencies in circulation, it might sound as if the "money" would be unusable because transactions would be unbearably complex. But that's not the world that we will be living in. This is not about transactions between people but transactions between what Jaron Lanier called "economic avatars". This is a world of transactions between my virtual me and your virtual

me, the virtual Waitrose and the virtual HMRC. This is my machine-learning AI supercomputer robo-advisor (or more likely my mobile phone front end to such) communicating with your machine-learning AI supercomputer robo-advisor.

These robo-advisors will be entirely capable of negotiating between themselves to work out the deal using algorithms, as de Bono foresaw. As tokens become a regulated (but wholly new) kind of digital asset, they will present an opportunity to remake markets in a new and better way. One might imagine a new version of London's Alternative Investment Market, where start-ups launch but instead of issuing money they create claims on their future in the form of tokens. The trading of these tokens would be indistinguishable from the trading of electronic cash (because they are bearer instruments with no clearing or settlement), but there will be additional transparency because aspects of the transactions are public. Market participants will be able to assess and manage risk; regulators will be able to look for patterns and connections.

This is a far more efficient way to manage a marketplace. There won't be some giant IMF database that manages the new kinds of money. In this market, company performance rewards private money holders by improving the exchange rate against other private monies. No coupons and dividends; no clearing and settlement; no hiding the number of tokens out there. The cost of trading these tokens will be a fraction of the cost of trading stocks and bonds, which is why liquidity will seep out of existing markets and into these new and more efficient structures. Stephen McKeon, a finance professor at the University of Oregon, summarises this imperative by saying that assets of all kinds will tokenise because they will lose the "liquidity premium" if they do not.

The worlds of Bitcoins and blockchains and tokens and ICOs all come together here in a new architecture for financial services. To recapitulate (and to emphasise the importance of this), I would point out that once digital identities can exchange digital money with each other in complete security, we have a functioning base layer for a new financial system based on digital bearer instruments that require no clearing or settlement — instead of the existing financial system based on electronic currency, accounts and fiat cash.

Table 1. Who might make digital currency? The 5Cs.

Who might issue money?	What kind of money?
Commercial Bank Credit under regulatory control.	*Bank Money.* What we have now, essentially: money is created by banks under central bank supervision.
Central Bank National money under political control.	*Fiat Money.* The money we have now (that critics see as being inflated away).
Cryptography There is no control beyond mathematics.	*Dosh ex Machina.* There is no issuer and no value beyond the market.
Companies Future money under commercial regulation. The new world of tokens.	*Private Money.* Currency to be redeemed against future products and services.
Communities Reputation money under regulatory control and in a competitive market.	*Local Money.* Bearing in mind that "local" means something different in the virtual and mundane cases.

1. There are detailed case studies on both of these schemes, so here I will simply note that both used cryptography with hardware at its core to protect the integrity of the system. In the case of Mondex, this was the now-familiar smart card that chip and PIN has propelled into every pocket and, in the case of M-PESA, it was the now familiar SIM card that the GSMA has propelled into every phone in every pocket. Mondex was decentralised; M-PESA was centralised. But both were managed by a central authority, and in both cases the electronic value in the chips was issued against a 100% reserve in fiat currency held in the banking system.

B. The 5Cs

Looking at this architecture inevitably leads on to the bigger question of who might use it. I have a "5Cs" framework for thinking about this that I set out in my book *Before Babylon, Beyond Bitcoin*, as shown in Table 1 below. Technology is not a barrier to any of these options, whether for central banks or for anyone else. The idea of a central bank running something like M-PESA, but for citizens, is hardly far-fetched. There are millions of M-PESA users in Kenya, and Facebook can manage well over a couple of billion accounts, so I'm sure that the Bank of England could download an app to run a few million accounts for post-Brexit Britain. There is a middle way though. The central bank could create the digital currency, but could still distribute it through commercial banks. The commercial banks would not be able to create money as they do now (only the central bank would be able to do this), but they could use their existing systems to manage it.

Those of you schooled in the history of digital money may well remember that the banks had a go at this sort of thing a couple of decades ago with Mondex and its ilk. Those efforts failed for a number of reasons, but primarily because of a lack of acceptance. It was easy to give people cards, but hard to give them terminals. A decade after Mondex, M-PESA didn't use cards or terminals; it used mobile phones to vault a non-bank through a regulatory gap and create something that transformed the lives of millions.[1] I'm sure that when future historians write about the evolution of money, they will see that the mobile phone, not the plastic card, was the nail in the coffin of cash.

C. The road to Central Bank Digital Currency

Let us begin by examining what the fundamental CBDC concepts are. Ben Dyson and Jack Meaning from the Bank of England set out a particular kind of central bank digital currency (what some would call "digital fiat") with quite specific characteristics. This seems to be to an excellent starting point. They describe a form of digital money that is:

- Universally accessible (anyone can hold it);
- Interest-bearing (with a variable rate of interest);
- Exchangeable for banknotes and central bank reserves at par (i.e. one-for-one);
- Based on accounts linked to real-world identities (not anonymous tokens); and
- Withdrawable from your bank accounts (in the same way that you can withdraw banknotes).

This seems to me to be a sensible definition. Central bank digital currency is digital fiat, which is one particular kind of digital money. Some years ago, David Andolfatto, Vice President of the Federal Reserve Bank of St Louis, said that it was "hard to see the downsides to central banks supplying digital currency". I agree, although I have long held that central banks will be only one of the providers of digital money. But how exactly will this digital fiat work?

First, we have to fill in some blanks. For example, should it be centralised, distributed or decentralised? Given that, as *The Economist* noted in an article about giving access to central bank money to everybody, "administrative costs should be low, given the no-frills nature of the accounts", and given that a centralised system has the lowest cost, that would seem to point towards something like M-PESA, but run by the government.
There are, however, other arguments in favour of using more radical technology — not least, issues of privacy. Again, as *The Economist* notes, people might well be "uncomfortable with accounts that give governments detailed information about transactions, particularly if they hasten the decline of good old anonymous cash". However, I think there are ways to deliver appropriate levels of privacy; pseudonymity is an obvious way to do it efficiently, within a democratic framework.

D. Brit-PESA, BritCoin or Britdex?

Were we to decide to create a British CBDC issued and managed by commercial banks (let's call it Brit-PESA),

of course, we wouldn't use either the smart cards of the Mondex days or the basic SIM toolkit and SMS technology of M-PESA. We'd use smartphones and chatbots and AI and fingerprints and voice recognition, and all that jazz.

I don't think it would be that difficult to create a basic centralised CBDC: there would be a system shared by the commercial banks with the funds held in a central account. Whether digital fiat is the long-term future of money or not (and I think it isn't), there is no reason not to press ahead with CBDC, whether Brit-PESA or Brit-Ledger or Brit-Dex, and give everyone access to payment accounts without credit risk. Aside from reforging our financial system in the white heat of new technology, there's a very good reason for doing so. Bank of England Staff Working Paper No. 605 says (amongst other things) that:

> *'...we find that CBDC issuance of 30% of GDP, against government bonds, could permanently raise GDP by as much as 3%, due to reductions in real interest rates, distortionary taxes, and monetary transaction costs. Countercyclical CBDC price or quantity rules, as a second monetary policy instrument, could substantially improve the central bank's ability to stabilise the business cycle.'*

GDP growth aside, there is another excellent reason for taking this step, which is that cash has no Application Programming Interface (API). Writing in the Bank of England's *Bank Underground* blog, Simon Scorer from the Digital Currencies Division made some interesting points about the requirements for digital fiat. He remarked on the transition from dumb money to smart money, and the consequent potential for innovation, saying that "other possible areas of innovation relate to the potential programmability of payments; for instance, it might be possible to automate some tax payments (e.g. when buying a coffee, the net amount could be paid directly to the coffee shop, with a 20% VAT payment routed directly to HMRC), or parents may be able to set limits on their children's spending or restrict them to trusted stores or websites".

Simon's insight here suggests that it is not the shared ledger itself, but the shared ledger applications (or "smart contracts") that will become the nexus for radical innovation as they are used to implement new digital currencies.

II. Why Explore Digital Currency Now?

Of course, when techno-determinist commentators say that the future of money will break with the Bretton Woods structure, and that the decentralising nature of computers, communications and cryptography mean that there might be currency issuers other than central banks, this might be dismissed as cypherpunk-addled machine-head babble. It seems to me, however, that when sensible, knowledgeable and powerful players are beginning to talk about radical change, then stakeholders (ie, all of us) should take notice of what they are saying and start to think about the implications.

The reaction of regulators around the world to one such radical change, Facebook's proposed "Libra" digital currency (more on this later), seems to indicate that the incumbents are not going to give up without a fight. Indeed, that most conservative of institutions, the Bank for International Settlements, has already created a new unit (led by former ECB executive board member, Benoît Cœuré) to explore public alternatives to private digital currency initiatives such as Libra. The unit's first project will be to co-operate with the Swiss National Bank to create a digital currency (using, apparently, some form of shared ledger) for wholesale use between banks.

Note that this is in parallel with attempts to create a pan-European digital payment service at the retail level, which Cœuré has said is needed to take on the US payment schemes and Chinese wallets. The Pan-European Payment System Initiative, given the somewhat ironic acronym PEPSI, is under discussion with about 20 banks involved at the time of writing.

What has brought us to this state of affairs? While the prevailing winds were in the direction of change, there is no doubt that the storm that drove us here is cryptocurrency. There is definitely something serious happening. The noted cryptocurrency investor Brock Pierce was responsible for the first Initial Coin Offering (ICO) back in 2013, and he is an investor in many companies in the space via Blockchain Capital. He's a serial entrepreneur with a long track record, and he has said clearly that "I think what I've done is the end of all VC, all private equity... I think all the big VCs are done".

That sounds ridiculous. However, there is something in what he says. In his book *The Money Trap*, Robert Pringle writes that globalisation has already "reached the limits compatible with existing international monetary arrangements". There is pressure for change and while I don't think Bitcoin and other cryptocurrencies are the money of the future, this could mean a new kind of financial market along the lines envisaged by de Bono because cryptocurrencies have provided the technology to deliver the Facebook Florin (a much better name than Libra) and the Microsoft Dollar (ie. Bill's dollars, rather than dollar bills).

A. The stability requirement

There is an underlying assumption that any alternative currency unit would need to demonstrate stability in order to obtain wide acceptance. Hence the use of the term "stablecoin", bandied around Libra. But what does this actually mean? On the Bank of England's *Bank Underground* blog, there was a post that explained that there are generally two designs of stablecoin: those backed by assets, and those that are unbacked or "algorithmic"". That is right – but I think there are three kinds:

- Fiat currencies (aka Currency Boards), which are similar to asset-backed currencies, but where the assets backing the digital currency are fiat currencies only. There are several versions of these already: in Bulgaria, for example, where the local currency (the Lev) is backed by a 100% reserve of euros.

- Algorithmic currencies, in which algorithms manage supply and demand to maintain stability of the currency. This is what a stable cryptocurrency is: since a cryptocurrency is backed by nothing other

than mathematics, it is mathematics that manages the money supply to hold the value steady against some external benchmark.

- Asset currencies, in which an asset (or basket of assets) is used to back the digital currency. I don't know why people refer to these as stablecoins, since they are stable only against the specific assets that back them. An asset that is backed by, say, crude oil is stable against crude oil, but nothing else.

This last category is effectively what is currently defined as electronic money under existing EU directives, and therefore, is already regulated. Those cryptocoins backed by fiat currency (such as JPM Coin) simply provide a convenient way to transfer value around the internet without going through banking networks. This may well be an advantage in cost and convenience for some uses, but it is a long way from an algorithmic currency.

In November 2019, the head of FinCEN made it clear that, as US regulators are technology-neutral, transactions in any of these kinds of stablecoin are covered by the Bank Secrecy Act for AML/CFT purposes, and that the administrators of any such services will have to register as a Money Services Business (MSB). So will any or all of these catch on?

Predictions are of course difficult, but my general feeling is that it is the asset-backed currencies that are most interesting and most likely to succeed. Algorithmic and fiat "stablecoins" exist to serve a demand for value transfer, but this is already served well by conventional means. I notice, for example, that Transferwise can now send money from the UK to Hong Kong in 11 seconds, a feat made possible by its direct connection to the payments networks of both countries. Why would I use a fiat token when I can send fiat money faster and cheaper?

Of course, you might argue that a digital currency board might allow people who are excluded from the global financial system to hold and transfer value, but I am unconvinced. There are plenty of ways to hold and transfer electronic value (eg, M-PESA) without using bank accounts. Generally speaking, people around the world are excluded because of regulation (eg, KYC), and if we want to do something about inclusion we should probably start there. If you are going to require KYC for the electronic wallet needed to hold your digital currency, customers may as well open a bank account, right?

I suppose there are some people who think that the anonymity or pseudonymity of cryptocurrencies might make them an attractive alternative for criminals. But, if cryptocurrencies are used for crime on a large scale then efforts would be made to police them. Bitcoin, in particular, is not a good choice for criminals since it leaves a public and immutable record, and you can imagine a future in which the mere possession of an anonymous cryptocurrency becomes a *prima facie* case of money laundering.

Looking at the "stable" part of "stablecoins", I'll put my money on the middle way. There is a real logic to the trading of asset-backed currencies in the form of tokens, and I expect to see an explosion of different kinds. The competition will be between private asset-based currencies and public fiat-backed (or synthetic) currencies.

B. Rethinking money

The private asset-backed and public fiat-backed tokens won't only be issued by companies. It seems to me that tokens that implement the values of communities (and, because they are "smart", can enforce them) may come to dominate the transactional space (think of the Islamic e-Dinar and the London Groat).

One such "community" might well be the nation state. In fact, at least one nation state is already thinking along these lines. Kaspar Korjus, the director of Estonia's e-Residency program, has already floated the idea of issuing tokens instead of sovereign bonds.

Korjus has suggested that the money raised in such an offering could be used for a fund jointly managed by the government and outside private companies. This would then be used to invest in new technologies for the public sector, as well as to invest venture capital into Estonian companies founded by both natives and e-residents.

Eventually, Korjus sees the tokens holding value and being used as a payment method for public and private services both within the country and globally.

That Estonian example helps us to find an answer to the misleadingly simply question: "what is money". Money is something that you can pay your taxes with. If Estonia were to go ahead by merging its currency and bonds into a single, liquid, circulating digital asset, then we will have gone full circle back to the days when government tally sticks were circulating in England.

This, of course, moves us on to a bigger picture. Technologists are not, or at least should not be, the only people who are rethinking money in the light of new technology. Digital currency is a political issue as much as a technological issue. This was made plain when Mark Carney, than the Governor of the Bank of England, gave a speech at Jackson Hole, Wyoming, in which he said that a form of global digital currency could be "the answer to the destabilising dominance of the US dollar in today's global monetary system". The problem that he was alluding to is that the US dollar's global hegemony "made sense after World War II, when the U.S. accounted for 28% of global exports. Now, the figure is just 8.8%, according to the IMF. Yet the dollar still dominates international trade".

In his speech, Carney went on to talk about the idea of a "synthetic hegemonic currency". This is a form of Artificial Currency Unit that has a long heritage. There are, broadly speaking, two kinds of ACUs: those created by official institutions primarily for official international transactions and those introduced at the initiative of private companies for commercial transactions. The pre-eminent example of the former is the IMF's Special Drawing Right (SDR).

The SDR was created as a supplementary international reserve asset. It was initially defined as equivalent to 0.888671 grams of fine gold — which, at the time, was also equivalent to one US dollar. After the collapse of the Bretton Woods system in 1973, the SDR was redefined as a basket of currencies.

The SDR is therefore neither a currency nor a claim on the IMF. Rather, it is a potential claim on the freely usable currencies of IMF members since SDRs can be exchanged for these currencies. It also serves as the unit of account for the IMF and a number of other international organisations (eg, the Asian Development Bank). It is also used in some international agreements. Just to give one example, the Convention on Limitation of Liability for Maritime Claims sets limits in SDRs.

There are other examples, both private and public. The ECU, the precursor to the euro, could have used the new digital money technologies to have become a "hard e-euro" for cross-border trade. I assume that Carney was thinking of these kinds of "official" ACUs when he said:

> *'We think Libra and other potential new payment solutions are shining a light on deficiencies in the system. And that is to be welcomed. They are trying to solve them. So domestic payments are still too slow and not distributed in real time. And cross-border payments are much worse. They cost a lot more and take a lot longer to execute. And that is just not necessary. It is a product of the old architecture. So coming up with new architecture and trying to solve it is a good thing.'*

An obvious example of the kind of ACU-as-SHC that Mr. Carney envisages, created by official institutions for international transactions, would be an electronic version of the SDR. In fact, World Bank officials have already asked the IMF to "develop a procedure for issuing and using market SDRs following currency board rules and backed 100% by official SDRs or by an appropriate mix of sovereign debt of the five basket currencies".

A virtual currency made from digital cash, denominated in a synthetic unit of account that is determined by a basket of currencies, does sound a little like Facebook's Libra, which is an example of an ACU for commercial transactions. We will look at Libra in some detail later on, but at this point it is sufficient to note that while Facebook may well have been the first "big tech" to try to establish a global digital currency, similar proposals will certainly follow. This is not bad. The historian Niall Ferguson has stated that "if America is smart, it will wake up and start competing for dominance in digital payments".

He is concerned about hegemony, and argues that a good way for America to rival Chinese initiatives such as Alibaba and Tencent is to support Libra. Right now, Alipay and WeChat wallets store RMB exchanged in and out of bank accounts, but as the People's Bank of China (PBoC) has made clear, these will soon store the "DC/EP" (digital currency and electronic payment) version, the Chinese digital currency.

This means that we now have two examples at hand to explore the dynamics of competition between private asset-backed and public fiat-backed digital currencies: Libra and the People's Bank of China. Let us look at the competing visions of Libra and the DC/EP to form an opinion on the future monetary system, and see if we can identify a path through the social, business and technical roadmap for digital currency.

III. A Private Synthetic Currency: Libra

A scheme to implement digital currency based on a shared ledger has already been put forward by Facebook. And because it is being put forward by Facebook, it is a big deal.

Mark Zuckerberg once observed that "in a lot of ways, Facebook is more like a government than a traditional company". Indeed it is, and perhaps it is about to become even more so by planning to have a currency of its own. The currency is Libra, and the media has been full of commentary about it, about the new blockchain that will support it (created by the Libra Network) and about the new wallets that it will be stored in (created by Calibra, a Facebook subsidiary). Put to one side whether it is a currency or not, a cryptocurrency or not, or a blockchain or not; the fact that it exists is nonetheless exceedingly interesting.

First, what would be the difference between holding Facebucks and holding eSDRs? Well, for one thing, the Facebuck currency board basket will not include renminbi. Its basket will apparently be based on the US dollar, the euro, the yen, sterling and the Singapore dollar as shown below.

Table 3. The Libra Basket.

Currency	Weight
US Dollar	50%
Euro	18%
Singapore Dollar	7%
Japanese Yen	14%
Pound Sterling	11%

The composition of the currency board aside, what is the purpose of this new payment system? Libra says that it hopes to offer services such as "paying bills with the push of a button, buying a cup of coffee with the scan of a code or riding your local public transit without needing to carry cash or a metro pass". But, as numerous internet commentators have pointed out, if you live in London or Nairobi or Beijing or Sydney, you can already do all of these things. It's only in San Francisco where such things appear an incredible vision of a future where people don't write cheques to pay their rent and can ride the bus without a pocket full of quarters.

From a payments perspective alone, it seems underwhelming. However, the ability to send money around on the internet is clearly useful, and there are all sorts of new products and services that it might support.

Still, currency has more far reaching implications. As J.P. Koning points out, "Libra is more than a means of exchange". It is not a digital fiat currency as previously described, but nonetheless could in theory (unlike cryptocurrencies such as Bitcoin) provide a reasonably stable currency for international trade.

This has significant implications. What if, for example, the inhabitants of some countries abandon their failing inflationary fiat currency and begin to use Libra instead? The ability of central banks to manage the economy would then be subverted, and this must have political implications. This has not gone unnoticed by the people who understand such things — an example again being Mark Carney saying that if Libra does become successful then "it would instantly become systemic and will have to be subject to the highest standards of regulation". Unsurprisingly, both the Financial Stability Board

and the UK's Financial Conduct Authority have said they will not allow the world's largest social network to launch its planned digital currency without "close scrutiny".

Global regulators in general have responded with varying degrees of scepticism, with some jurisdictions (eg, France) saying flat out that they will block it — although it is not clear to me how. As far as I understand, Libra is a form of electronic money already allowed in Europe under the provisions of existing Electronic Money Institution (ELMI) licences. While the Libra Association remains firm that the system will go live in 2020, many industry observers are already saying that it will never launch in its current form.

However, whether or not it will reach any of the goals set by its founders, there's something else interesting in Libra.

Let us look at the two institutional bindings needed to turn the cryptocurrency technology layer into a new financial system. These are, as noted earlier, the binding of cryptocurrency values to real-world assets and the binding of the wallets to real-word entities.

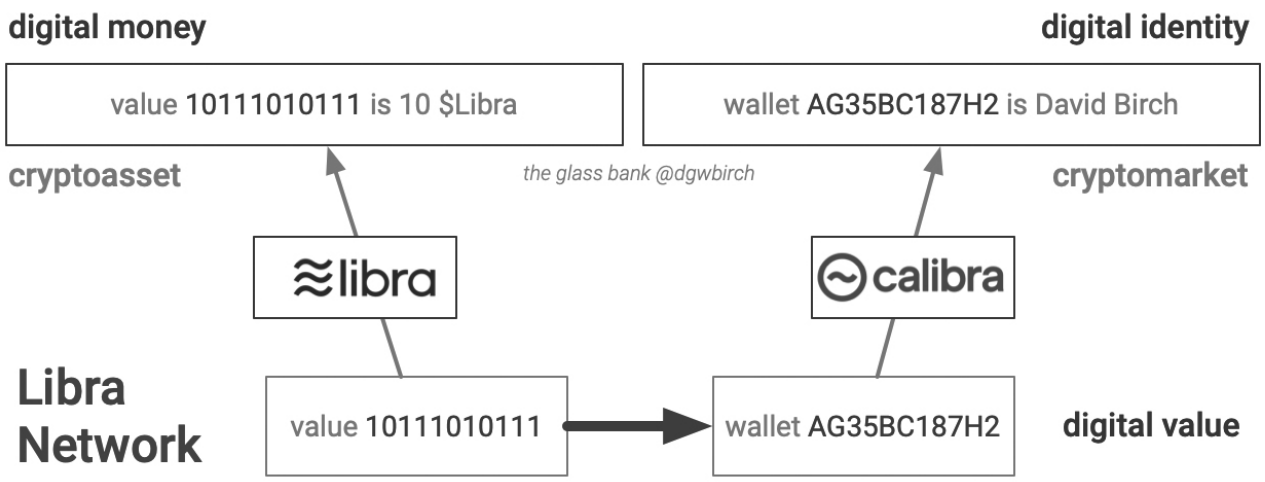
The binding of a wallet address to an actual person is difficult and costly. Calibra says that it will ensure compliance with AML/CFT requirements and best practices when it comes to identifying Calibra customers by taking the following steps:

- Require ID verification (documentary and non-documentary).
- Conduct due diligence on customers commensurate with their risk profile.
- Apply the latest technologies and techniques, such as machine learning, to enhance our KYC and AML/CFT program.
- Report suspicious activity to designated jurisdictional authorities.

I thought it was worth reproducing this list in full. If we put together what the Libra white paper says and what Calibra says about its wallet, you get a specific version of the model I set out earlier. I think it describes the overall generic proposition quite well:

The Libra Association formally launched in October 2019. It was noticeable that the membership did not include most of the payments organisations that had been identified in initial discussions (eg PayPal and Visa), but did include the organisations who are users of payments (eg, Uber and Spotify).

Figure 2. Libra and Calibra in Context.



A. The identity play

On page nine of the Libra white paper, Libra says that "an additional goal of the Association is to develop and promote an open identity standard. We believe that a decentralized and portable digital identity is a prerequisite to financial inclusion and competition".

It is clear what the wallet addresses in a transaction (as shown in the diagram above); a timestamp and the transaction amount will be public because they are on a shared ledger. But, as Facebook has made clear, any KYC/AML (ie, the binding shown in the diagram) will be stored by the wallet providers, including Calibra. Since the head of Libra, David Marcus, has repeatedly pointed out that Libra is open and anyone will be able to connect to the network and create a wallet, there could be many, many wallets. But you'd have to suspect that Facebook's own Calibra will be in pole position in the race for population scale. Hence Calibra's approach to identity is really important, and Calibra's global context as a competitor to (for example) Alipay becomes clear.

Now, if Calibra provides a standard way to convert a variety of government-issued IDs into a standard, interoperable ID, that will be of great value. Lots of other people (eg, banks) may well want to use the same standard. In the UK, for example, this would be a way to deliver the new Digital Identity Unit (DIU) goal set out by the then Minister for the Cabinet Office, Oliver Dowden, in a speech at London's *Identity Week* of "one login for your state pension and your savings account". But it isn't only the ID that needs interoperability, it's the credentials that go with it. This is how you build a reputation economy. Your Calibra wallet can store your IS_OVER_18 credential, your Uber rating and your airline loyalty card in such a way as to make them useful.

Equally, if you want to register for a dating side, you can log in using Calibra and it will automatically either present the relevant credential or tell you how to get it from a Libra partner (eg, MasterCard).

It seems to me that this may, in time, turn out to be the most important aspect of the "Facebucks" initiative. What if a Calibra wallet turns out to be a crucial asset for many of the world's people, not because it contains money but because it contains identity?

B. Government issue

Let us return for a moment to that point about government-issued ID. One of the things that governments do is issue passports as a form of formal identity. If I obtain a Calibra wallet by presenting my passport, that's fine. But suppose I live in a developing country and I have no passport or formal ID of any kind?

Well, I think Facebook can make a good argument that your Facebook profile is a more than adequate substitute, especially for the purposes of law enforcement. After all, Facebook knows whom I message, my WhatsApp address book, whom I hang out with, where I go... Facebook can tell real profiles from fake, and it kills off fake "identities" all the time. My guess is that if you have had a Facebook profile for (let's say) a year, then that identity is more than good enough to be able to open an account to hold Libra up to $10,000 or so – and, of course, it will be beneficial for society to get those transactions on to an immutable shared ledger.

Frankly, in large parts of the world, Know-Your-Customer (KYC) could be replaced by Known- by-Zuck (KYZ) to the benefit of society as a whole.

IV. A Public Digital Fiat Currency: DC/EP

As the centre of economic gravity shifts East (or, to take a less anglo-centric view of the world, returns to its historic centre), so the trajectory for digital money is likely to be different to what early pioneers might have imagined only a generation ago. Right now, there are some eighty countries that are part of China's "Belt and Road" initiative (BRI). These include not only Asian countries and many central Asian republics, but also countries of Africa, the Middle East, Eastern Europe, and the Caribbean. In other words, around two-thirds of the world's people, responsible for around a third of global GDP, are now living along the "new Silk Road".

Historian Peter Frankopan provides a valuable perspective on this new economic highway. As with the Silk Roads of the past, there is no specific geographical criterion to be part of this initiative; indeed, the maritime element of it is intended precisely to allow parameters of inclusion to be extended as far as the Eastern coast of Africa and beyond. Chinese President Xi has called it an initiative that could change the world, and many observers agree – although whether it will mean "mutual learning will replace clashes and coexistence will replace a sense of superiority" seems a tall order to me.

It seems logical to me, especially given my feeling that the currencies of the future will be more closely related to communities, that a new Silk Road will demand a new silk purse to keep a new silk money in.

If one obvious demand for cryptocurrencies will always come from the criminal fraternity, from money launderers and drug dealers, then the impact of digital currencies in general might be most important for states seeking to trade in the face of pressures (such as sanctions) in a world where the dominance of the US dollar makes large-scale trade in other currencies difficult and trade in cryptocurrencies too risky (if someone steals your Bitcoin, you are never getting it back).

This would seem logical for countries (such as Iran) that are, as Frankopan notes, "attuned to the fact that the world is changing". It is in nature of technological innovation, responding to the drivers for change discussed earlier, that some kind of global alternative will assemble itself.

With this perspective in mind, then, let us turn to what is, in my opinion, the most important current initiative in the world of digital fiat. This is in China — where, of course, fiat currency had its roots. When Kublai Khan became Emperor in the 13th century, he decided to replace copper, iron, commodity and specie cash with a paper currency. A paper currency! Imagine how crazy that must have sounded. Replacing physical, valuable stuff with bits of paper.

Just as Marco Polo and others returned along the Silk Road with astonishing tales of paper money, so commentators have been tumbling off flights from Beijing and Shanghai with equally astonishing tales of a land of mobile payments, where paper money is vanishing and consumers pay for everything with smartphones. China is well on the way to becoming a cashless society. Already, a significant proportion of the population relies wholly on mobile payments and carries no cash at all.

The People's Bank of China (PBoC) has been looking at digital currency strategy to replace cash for some years. It now looks as if Facebook's Libra initiative has accelerated this.

This is no knee-jerk reaction. Three years ago, the then-Governor of the PBoC, Zhou Xiaochuan, very clearly set out his thinking about digital currency, saying that "it is an irresistible trend that paper money will be replaced by new products and new technologies". He went on to say that, as legal tender, *digital currency should be issued by the central bank* and, after noting that it would take a decade or so for digital currency to completely replace cash, went on to state clearly that "he had plans for how to gradually phase out paper money".

What would be the impact of phasing out paper money? Yao Qian, from the PBOC's technology department, wrote back in 2017 that CBDC would have serious consequences for commercial banks, so that it might be better to keep

those banks as part of the new monetary system. He suggested what has been called a "two tier" approach. To offset the shock to the existing banking system posed by an independent digital currency (and to protect the investment made by banks in infrastructure), it should be possible to incorporate digital currency wallets into the existing commercial bank system "so that electronic currency and digital currency are managed under the same account".

I understand the rationale. The Chinese want the efficiencies that come from having a digital currency but also understand the implications of removing the "exorbitant privilege" of money creation from the commercial banks. If the banks cannot create money by creating credit, then they can only provide loans from their deposits. Imagine if Bitcoin were the only currency in the world: I'd still need to borrow a few of them to buy a new car, but since Barclays can't create Bitcoins, it can only lend me Bitcoins that it has taken in deposit from other people. Fair enough. But here, as in so many other things, China is a window into the future.

Whether you think CBDC is a good idea or not, it's a big step to take — and therefore one must understand the PBoC's position. There is a significant potential problem with digital currency created by a central bank. If commercial banks lose deposits and the privilege of creating money, then their role in the economy is much reduced. We already see this happening because Alipay and WeChat Wallet (and other Chinese third party payment platforms) use financial incentives to encourage users to take money out of their bank accounts and temporarily store it on the platform itself. It is my belief that the loss of interest income is a small inconvenience to the banks, compared with the much more serious loss of transactional data.

A. Digital cash is different

A couple of year ago, I wrote that the PBoC would not issue cryptocurrencies or digital currencies, at least in the foreseeable future. What I said they *might* do is allow commercial banks to create a digital currency under central bank control. And this is indeed what seems to be happening. The new Chinese digital currency will be centrally controlled by the PBoC, with commercial banks having to hold reserves at the central bank for assets valued in the digital yuan — exactly as Yao Quin said back in 2017.

How will this work? Well, you could have the central bank provide commercial banks with some sort of cryptographic doodah that would allow them swap electronic money for digital currency under the control of the central bank. Which, of course, reminds me of Mondex.

This "two tier" approach is how Mondex was structured 25 years ago. There was one big difference between Mondex and other electronic money schemes of the time, which was that Mondex would allow offline transfers, chip to chip, without bank (or central bank) intermediation. Would a central bank go for this today? Some form of digital cash that can be passed directly from person to person like Bitcoin, rather than some form of electronic money like M-PESA, using hardware rather than proof of work to prevent double spending? Well, it was being tried in Uruguay, where the central bank ran a six-month pilot scheme with 10,000 users to test the technology, but many observers thought it unlikely to operate in that mode at scale.

B. There is "Anonymous" and "anonymous"…

Ferguson's characterisation of Libra as "not a true blockchain cryptocurrency, but more like a digital currency in the Chinese style" is telling. The Chinese are serious. But, for all of the talk about a blockchain, they have no intention of launching their own official cryptocurrency. DC/EP will indeed implement the "two tier" architecture. Commercial banks will have accounts at the central bank and will buy the digital currency at par. Individuals and businesses will open digital wallets provided by commercial banks or other private companies (ie, Alipay and Tencent). This will, as Libra will, mean scale interoperability. The digital currency in my bank app and my Alipay app and my WeChat app will be freely exchangeable. I must be able to transfer value from my Alipay app to your WeChat app for it to be useful. If the PBoC cracks this, it will be on the way to one of the world's most efficient electronic payment infrastructures.

Given earlier points about anonymity and pseudonymity, I think there is something even more interesting in the PBoC's plans.

Many observers have expressed some surprise that the PBoC would allow anonymous peer-to-peer transfers, despite the current deputy director of the PBoC's payments department saying that the proposed digital currency would have the ability "to be used without an internet connection and would also allow transactions to continue in situations in which communications have broken down, such as an earthquake". Talking about the DC/EP tool itself, he said that the functionality will be "exactly the same as paper money, but it is just a digital form", and went on to confirm that "as long as there is a DC/EP digital wallet on the mobile phone, no network is needed, and as long as the two mobile phones touch each other". He went on to say that "even Libra can't do this".

This would seem to mean that the system (as Mondex did) will allow offline transactions, which means that value can be transferred from one phone to another via local interfaces such as NFC or Bluetooth. To appreciate that Libra cannot do this, note that there are basically two ways to transfer value between devices and keep the system secure against double-spending. You can do it in hardware (ie, Mondex or the Bank of Canada's Mintchip) or you can do it in software. If you do it in software you either need a central database (eg DigiCash) or a decentralised alternative (eg, blockchain). But if you use either of these, you need to be online. I don't see how to get the offline functionality without hardware security.

If you do have hardware security and can go offline, then we are back to the question of fungibility. Here, the PBoCs principle is both clear and, to my mind, surprising. Its commitment is clear: "…the public has the need for anonymous payment, but today's payment tools are closely tied to the traditional bank account system... The central bank's digital currency can solve these problems. It can maintain the attributes and main value characteristics of cash and meet the demands of portability and anonymity."

It is important to note, however, that there are different kinds of anonymity, and what the PBoC means may be very different from what, for example, a ZCash user means by anonymity. It might be useful to categorise these different kinds of anonymity as unconditional, limited (or "controlled anonymity" as the PBoC calls it) or conditional anonymity where under normal circumstances the parties to a transaction remain hidden, but under certain conditions (eg, the double spending of value) algorithms will reveal information about counterparties.

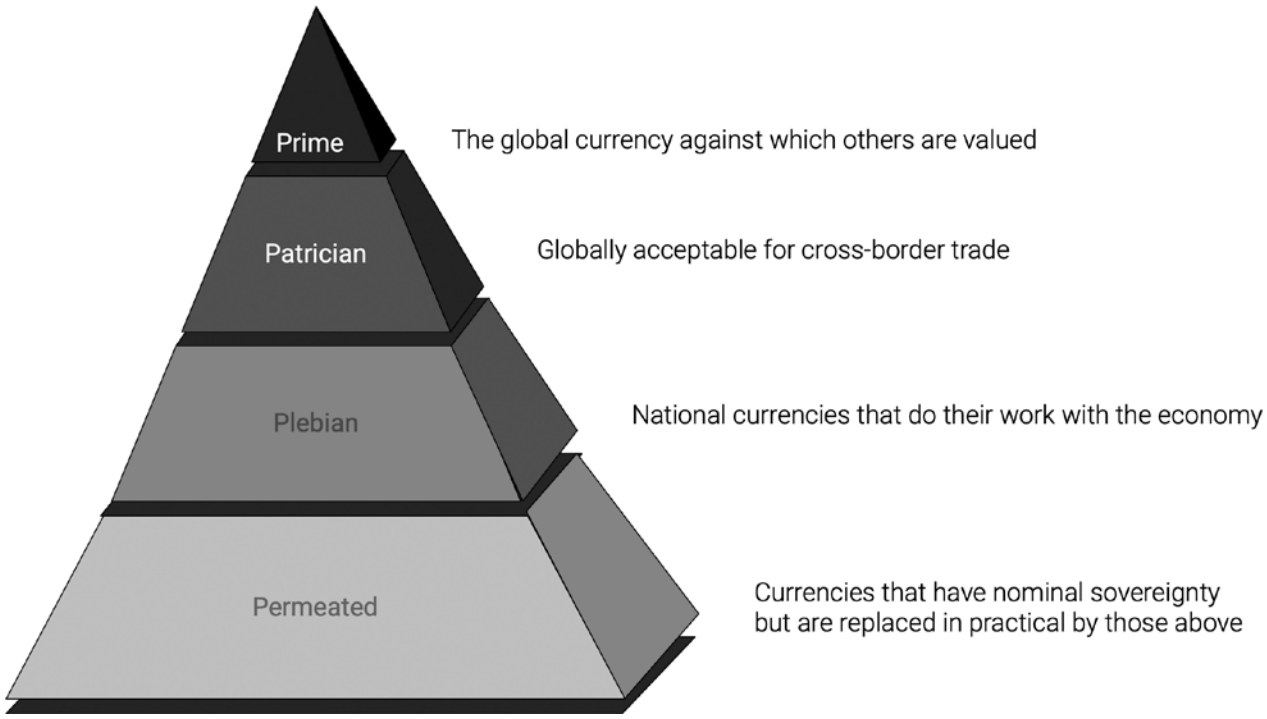
Unconditional anonymity means that no parties to a transaction nor any other observer can learn anything about the transaction counterparties from the transaction record. So, if I want to use my digital money to do something illegal, I can do so without concern because not even a government can throw enough computing power at the transaction system to find out who I am or whom I paid. Limited (or "1st party") anonymity means that the counterparties' identities are shielded from each other, but not from the operator of the system — and this is surely what the PBoC meant by "voluntary anonymity at front-end and real name at back-end".

As we will see in the next section, the anonymity or otherwise of a digital currency is central to the policy issues that arise from the use of digital currency.

V. The Cashless Cold War

In his 2015 book, *Currency and Power*, Benjamin Cohen set out a "currency pyramid" as a way of looking at international monetary arrangements. A simplified version of this pyramid (see Figure 4 below) categorises world currencies into four groups: the "prime" currency, the "patrician" currencies used for business and by the global elite, the "plebeian" currencies that work perfectly well within their currency areas but are little used beyond and, finally, the "permeated" currencies. I can illustrate the last category from personal anecdote: many years ago, I lived in a developing nation where all transactions of any significance were conducted in US dollars and the local currency was only used for day-to-day transactions such as shopping and transport. Anyone accumulating any reasonable amount of the local currency would change it to dollars. Thus, the local economy was "permeated" by dollar transactions.

Figure 4. The Currency Pyramid (after Cohen, 2015).



This pyramid is remarkably stable, and as Cohen notes, there is no sign of an emerging multipolarity in the global currency system. The US dollar is top dog, and the euro lags behind. There are some patricians (eg, sterling), but nothing much has changed for a generation or more.

That stability is taken for granted. The dollar's role as Prime Currency, global hegemonic currency or top money banana brings substantial benefits to the American economy and provides substantial support to American foreign policy. However, as Robert Kaplan, President of the Dallas Federal Reserve, said recently, discussions about cryptocurrency and digital currency reinforce the view that "the dollar may not be the world's reserve currency forever… if that changes, and you tack on 100 basis points to $20 trillion [that is] $200

billion a year and all of a sudden we've got a tremendous problem".

Apart from denomination rents, seigniorage and reduced transactions costs, these benefits include macroeconomic flexibility that is not available to nations further down the pyramid.

The US gets to exert both hard and soft power through the international monetary system, but this power might be seriously constrained were the currency pyramid to collapse.

A. Red vs. Blue

What could trigger this new "Cold War" — a currency conflict that Ferguson as a historian is alert to but politicians are seemingly not?

The IMF's former Chief Economist, Kenneth Rogoff, has said that competition to reduce the influence of the dollar will come from state-sponsored assets, and I think that at the global level he must be correct. I do, however, see a role for private currencies at both Patrician and Plebian levels, and they will undoubtedly have an impact on Permeated currencies also. It is important to note that this is not necessarily a bad thing. In a recent paper, Raskin, Salah and Yermack highlight "the potential for private digital currencies to improve welfare within an emerging market with a selfish government. In that setting, we demonstrate that a private digital currency not only improves citizen welfare but also encourages local investment and enhances government welfare".

Looking at the current situation, it is clear that the principal threat to the role of the dollar as Prime currency comes not from Facebook but from China. If the Alipay and WeChat wallets become widely used by a couple of billion people, starting with those along the "Belt and Road", they may well begin by using their own currencies but they will pretty soon shift to the digital renminbi if it does indeed offer speed, convenience and person-to-person transfers. A trader in Africa may soon find it more convenient to order goods from a Chinese partner via WeChat and settle via Alipay. And if he or she can settle instantly with a Chinese digital currency, then they will soon find themselves accepting the same in payment.

The real fear of some observers, then, is that in this new Cold War, it won't just be Calibra vs Alipay; it will be the RMB vs the US$. That's a pretty big deal because it means that a proportion of the world's financial transactions may well stop being dollar-denominated, meaning the demand for dollars will fall. I think the *Wall Street Journal* was right to characterise the future of digital currency as a "coming currency war" between digital money and the dollar, saying that "The U.S. dollar has been the world's dominant currency since the 1920s. But if national digital currencies allow for faster, cheaper money transfers across borders, viable alternatives to the U.S. dollar could emerge, embraced by nations and monetary officials concerned about the dollar's outsize influence on the global economy". Or, as the Chairman of the Federal Reserve, Jay Powell, wrote to Congressman French Hill in November 2019, "a digital national currency may not offer advantages to the U.S. that it may do to other nations".

Harvard's Institute of Politics recently ran a "wargame" simulation of a US crisis around digital currencies. The premise was that participants were members of the National Security Council convened to respond to the threat to the US after the roll out of the DC/EP. The scenario played out with the digital renminbi undermining the dollar's global dominance, with North Korea evading sanctions using the digital alternative to the global banking system to buy nuclear materials, and with a variety of malicious state and non-state actors looting from SWIFT.

However plausible this scenario might be, the virtual money debate is no longer about electronic money vs. digital cash, about hash tables vs. smart chips or about proof-of-work vs. proof-of-stake. This is all about global power. Being a historian, it is natural for Ferguson to remind us that countries that have led in financial innovation have led in other ways too. He cites Renaissance Italy, Imperial Spain, the Dutch republic and the British Empire, on to post-1930s America. He then goes on to note that should a country lose its financial leadership, it loses its place as global hegemon. And that has serious consequences. Whether you think

it might be a good thing or not, the dollar's dominance gives America the ability to use the international payments system as an arm of its foreign policy— a power that, as Ferguson puts it, other countries have found "increasingly irksome".

Now, while it is the case that for the renminbi to replace the dollar at the top of the pyramid there would have to be structural changes in the Chinese economy, there are other reasons why a Chinese digital currency might obtain a significant fraction of international transactions, and thus weaken the demand for dollars. Lower costs, because of the lack of clearing and settlement, might in themselves be sufficient. But so might a weakened ability for the West to track and monitor transactions.

Rae Deng, a founding partner of Du Capital in Singapore, talks about "digital migration" of the economy, which is a nice phrase, and observes that a Chinese digital currency could "further facilitate the internationalization of the yuan". He suggests that it could form a parallel ecosystem to run alongside SWIFT, carried around the world by the Belt-and-Road Initiative. Note the serious implication of replacing the existing financial infrastructure with a new infrastructure based on digital bearer instruments. No clearing and settlement means no transactions going through the international banking system, and no transactions going through the international banking system means that America's ability to deliver soft power through SWIFT disappears.

B. Never mind Star Wars

It is hardly for me to suggest a defence strategy for the dollar. But in the light of comments by various experts, I might make a few suggestions about how the West as whole might proceed:

First of all, **digital identity**. The UK (and, for that matter America and everywhere else) should take a leaf out of Facebook's book and create a global digital identity infrastructure for the always-on, connected world. We need a digital identity, not digitised identity.

Secondly, **digital money**. We need a global electronic money licence along the lines of the European Electronic Money Licence (ELMI), with passporting. We need vigorous competitors capable of challenging the incumbents to deliver innovation – and we won't get it if we require companies to obtain banking licences and state money transmitter licences in order to challenge Bank of America or Facebook.

Thirdly, we need to create an alternative to the existing vastly expensive KYC/AML regimes that serve to build a defensive moat around the incumbents. A new approach to **digital due diligence** is needed. We now have a world of AI and machine-learning and, it may work better for the purposes of law enforcement to stop using KYC to create financial exclusion and instead aim for financial inclusion while using modern technology to track and monitor transactions to look for the criminals and terrorists.

Finally, we need to take Mark Carney's idea seriously and use the digital identity, digital money and digital due diligence building blocks to create a new payments system, with one or more SHCs, designed with the goals of society and not only technologists in mind. The goal must be to satisfy the demand for an alternative to the dollar. If we (ie, the developed nations) don't do it, then someone else will and leave us out in the cold.

Acknowledgements

Sincere thanks are due to Jeremy Wilson for his helpful comments on an early draft of this paper.

Glossary

ACU. Alternative Currency Unit.

AEC. Anonymity-Enhanced Cryptocurrency.

AML. Anti-Money Laundering.

BSA. The US Bank Secrecy Act.

CBDC. Central Bank Digital Currency.

CTF. Counter-Terrorist Financing.

ELMI. Electronic Money Institution.

ICO. Intial Coin Offering.

IMFS. International Monetary and Financial System,

SHC. Synthetic Hegemonic Currency.

Bibliography

- Into the woods, in The Economist. 2019: London. p. 1.
- Eyers, J., ASIC's Greg Medcraft says that traditional bank accounts may be obsolete in a decade, in Australian Financial Review. 2017, Fairfax: Sydney.
- King, M., Heroes and Villains: The Role of Central Banks, in The End of Alchemy, 2016, Little, Brown: London. p. 156-210.
- Bono, E.D., The IBM Dollar, in The Money Changers, D. Boyle, Editor. 2002, Earthscan: London. p. 168-170.
- Birch, D., R. Brown, and S. Parulava, Towards ambient accountability in financial services: shared ledgers, translucent transactions and the legacy of the great financial crisis. Payment Strategy and Systems, 2016. 10: p. 118-131.
- Dahinden, D., et al., Future of Money. 2019, SIX: Zurich, Switzerland.
- Werbach, K. Why Blockchain Isn't a Revolution. Knowledge @ Wharton 2018 20th Jun. [cited 2018 24th Jun.]; Available from: http://knowledge.wharton.upenn.edu/article/blockchain-isnt-revolution/.
- Birch, D. and S. Parulava, Ambient Accountability, in Handbook of Blockchain, Digital Finance and Inclusion, D. Lee and R. Deng, Editors. 2017, Elsevier: London. p. 375-388.
- Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs). 2018. Bern, CH: FNMA.
- Birch, D., When anyone can be a money issuer, in Financial Times Alphaville. 2014, Pearson: London.
- Lanier, J., Financial Identity, in Who Owns The Future? 2013, Allen Lane: London, UK. p. 268-275.
- Dyson, B. and J. Meaning, Would a Central Bank Digital Currency disrupt monetary policy?, in Bank Underground. 2018: London.
- Andolfatto, D. Should the Fed issue its own Bitcoin? Newsweek 2015 31st Dec. [cited 2018 12th Jan. 2018]; Available from: http://europe.newsweek.com/fed-should-issue-its-own-bitcoin-lets-call-it-fedcoin-410289?rm=eu.
- Central banks should consider offering accounts to everyone, in The Economist. 2018: London.
- Barrdear, J. and M. Kumhof, The macroeconomics of central bank issued digital currencies. 2016, Bank of England: London. p. 92.
- Scorer, S., Beyond blockchain: what are the technology requirements for a Central Bank Digital Currency?, in Bank Undergound. 2017, Bank of England: London.
- Birch, D. and N. McEvoy, Downloadsamoney, in DEMOS Quarterly. 1996, DEMOS: London. p. 8.
- Kaminska, I. Central bank group BIS taps Benoit Cœuré to lead digital currency push. The Financial Times 2019 11th Nov. [cited 2019 11th Nov.]; Available from: https://www.ft.com/content/c7739de6-03e7-11ea-a984-fbbacad9e7dd.

- Blanco, K., Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium.
  2019, FinCEN: New York, NY.

- Giles, C., Mark Carney calls for global monetary system to replace the dollar, in Financial Times.
  2019: London.

- Michaels, D. and P. Vigna, The Coming Currency War: Digital Money vs. the Dollar, in The Wall Street Journal.
  2019: New York.

- Ascheim, J. and Y. Park, Artificial Currency Units: The Formation of Functional Currency Areas.
  1976, Princeton University International Finance Section Princeton, NJ. p. 33.

- Jeffery, C. and D. Hinge, Mark Carney on joined-up policy-making, forward guidance and Brexit, in Central Banking.
  2019: London.

- Coats, W., Proposal for an IMF Staff Executive Board Paper on Promoting Market SDRs, in The Bretton Woods Committee.
  2019.

- Petralia, K., et al., Banking Disrupted? Financial Intermediation in an Ero of Transformational Technology.
  2019, International Center for Monetary and Bankign Studies: London. p. 120.

- Ferguson, N., America's power is on a financial knife edge, in The Sunday Times.
  2019: London.

- Conway, E., Facebook currency will help it rule the world, in The Times.
  2019: London.

- Hinge, D., Facebook unveils new 'currency', in Central Banking.
  2019.

- Gerard, D., Facebook's New Currency Has Big Claims and Bad Ideas, in Foreign Policy.
  2019.

- Koning, J., Esperanto, money's interval of certainty, and how this applies to Facebook's Libra, in Moneyness.
  2019.

- Stacey, K. and C. Binham, Global regulators deal blow to Facebook's Libra currency plan, in Financial Times.
  2019: London.

- An Introduction to Libra.
  2019, Libra Association: Geneva. p. 12.

- Shuo, W., Z. Jiwei, and H. Kan, Zhuo Xiaochuan Interview, in Caxin Online.
  2016: Beijing.

- Knight, W., China's Central Bank Has Begun Cautiously Testing a Digital Currency, in MIT Technology Review.
  2017: Boston, MA.

- Leng, S., China appoints new digital currency head as race with Facebook's Libra heats up, in South China Morning Post.
  2019.

- Bergara, M. and J. Ponce, Central Bank Digital Currency: The Uruguayan e-Peso Case, in SUERF.
  2018, Larcier: Milan.

- Zhong, S., China's Digital Currency Debut, in Shanghai Securities News.
  2019: Shanghai.

- John, A. China's digital currency not seeking 'full control' of individuals' details: central bank official.
  2019 [cited 2019 20th Nov.]; Available from: https://www.reuters.com/article/us-china-markets-digital-currency/chinas-digital- currency-not-seeking-full-control-of-individuals-details-central-bank-official- idUSKBN1XM0H2.

- Cohen, B., International Currency, in Currency Power—Understanding Monetary Policy. 2015, Princeton University Press: Princeton, NI. p. 8-27.
- Cohen, B. and T. Benney, What does the international currency system really look like? Review of International Political Economy, 2014. 21(5): p. 1017-1041.
- Cohen, B., The Dollar: Power Undiminished, in Currency Power—Understanding Monetary Policy. 2015, Princeton University Press: Princeton, NI. p. 160-184.
- Keoun, B. Top Fed Official Says US Central Bank 'Actively' Debating Digital Dollar. Yahoo! Finance 2019 16th Oct. 2019 [cited 2019 16th Oct.]; Available from: https://finance.yahoo.com/news/top-fed-official-says-us-213014241.html.
- Raskin, M., F. Saleh, and D. Yermack, How Do Private Digital Currencies Affect Government Policy? 2019, SSRN. p. 22.
- Derby, M., Powell Says Fed Has No Plans to Create Digital Currency, in The Wall Street Journal. 2019.
- De, N. In Wargaming Exercise, a Digital Yuan Neuters US Sanctions and North Korea Buys Nukes. 2019 20th Nov. 2019 [cited 2019 20th Nov.]; Available from: https://finance.yahoo.com/news/wargaming-exercise-digital-yuan-neuters- 193507677.html?guccounter=1.
- Ferguson, N., Understretch: The Limits of Economic Power, in The Cash Nexus. 2001, Allen Lane: New York. p. 387-416.
- Greenwald, M., What a Chinese Digital Currency Means for the Dollar's Future, in Belfer Center for Science and International Affairs. 2019, Harvard Kennedy School: Boston, MA.
- Chen, Q., The good, the bad and the ugly of a Chinese state-backed digital currency, in CNBC. 2019, CNBC.
- Kobrin, S., Electronic Cash and the End of National Markets, in Foreign Policy. 1997, FP Group: Washington, DC. p. 3.

About the author

David G W Birch is (in his own words) "an author, advisor and commentator on digital financial services - and a few other things besides." He is a prolific author, his most recent book, *Before Babylon, Beyond Bitcoin* was published in 2017; his next, *The Coming Currency Cold Wars* is scheduled for June 2020. He blogs and tweets extensively, and is a regular contributor to *Wired*.

CSFI Publications

134.	**"The Digital Currency Revolution"** By David Birch. April 2020 ISBN 978-1-9997174-8-3	Free
133.	**"It's not magic: Weighing the risks of AI in financial services"** By Keyur Patel and Marshall Lincoln. November 2019 ISBN 978-1-9997174-7-6	£25/$45/€35
132.	**"Insurance Banana Skins 2019: The CSFI survey of the risks facing insurers"** By David Lascelles and Keyur Patel. June 2019 ISBN 978-1-9997174-7-6	Free
131.	**"Making the Audit Market Work: the case for liberalising ownership"** By Paul Boyle. April 2019 ISBN 978-1-9997174-6-9	£25/$45/€35
130.	**"The Last-Time Buyer: housing and finance for an ageing society"** By Les Mayhew. February 2019 ISBN 978-1-9997174-5-2	£25/$45/€35
129.	**"Finance for All: Wedded to fintech, for better or worse"** By Keyur Patel and David Lascelles. August 2018 ISBN 978-1-9997174-4-5	Free
128.	**"The Dependency Trap – are we fit enough to face the future?"** By Les Mayhew. January 2018 ISBN 978-1-9997174-3-8	£25/$45/€35
127.	**"A Level Playing Field for Investment Research? Challenges facing the buy-side, sell-side and independents"** By Jane Fuller. October 2017. ISBN 978-1-9997174-2-1	£25/$45/€35
126.	**"Insurance Banana Skins 2017: The CSFI survey of the risks facing insurers"** By David Lascelles and Keyur Patel. May 2017. ISBN 978-1-9997174-1-4	£25/$45/€35
125.	**"From Peer2here: How new-model finance is changing the game for small businesses, investors and regulators"** By Andy Davis. May 2017. ISBN 978-1-9997174-0-7.	£25/$45/€35
124.	**"Reaching The Poor: The intractable nature of financial exclusion in the UK"** A CSFI Report. December 2016. ISBN 978-0-9926329-8-4.	£25/$45/€35
123.	**"Getting Brussels Right: "Best Practice" for City firms in a post-referendum EU"** A CSFI Report. December 2016. ISBN 978-0-9926329-7-7.	£25/$45/€35
122.	**"Financial Services For All: A CSFI 'Banana Skins' survey of the risks in financial inclusion"** By David Lascelles and Keyur Patel. July 2016. ISBN 978-0-9926329-6-0.	Free
121.	**"Banking Banana Skins 2015: The CSFI survey of bank risk"** By David Lascelles and Keyur Patel. December 2015. ISBN 978-0-9926329-8-4.	£25/$45/€35
120.	**"The Death Of Retirement: A CSFI report on innovations in work-based pensions"** By Jane Fuller. July 2015. ISBN 978-0-9926329-9-1.	£25/$45/€35
119.	**"Insurance Banana Skins 2015: the CSFI survey of the risks facing insurers"** By David Lascelles and Keyur Patel. July 2015. ISBN 978-0-9926329-5-3.	£25/$45/€35
118.	**"The City And Brexit: A CSFI survey of the financial services sector's views on Britain and the EU"** April 2015. ISBN 978-0-9926329-4-6.	£25/$45/€35
117.	**"Setting Standards: professional bodies and the financial services sector"** By Keyur Patel. December 2014. ISBN 978-0-9926329-3-9.	£25/$45/€35
116.	**"Financial Innovation: good thing, bad thing? The CSFI at 21"** November 2014.	Free
115.	**"New Directions For Insurance: Implications for financial stability"** By Paul Wright. October 2014. ISBN 978-0-9926329-2-2.	£25/$45/€35
114.	**"Microfinance Banana Skins 2014: Facing reality"** By David Lascelles, Sam Mendelson and Daniel Rozas. July 2014. ISBN 978-0-9926329-1-5.	Free
113.	**"Banking Banana Skins 2014: inching towards recovery"** By David Lascelles and Keyur Patel. May 2014. ISBN 978-0-9926329-0-8.	£25/$45/€35
112.	**"Insurance Banana Skins 2013: the CSFI survey of the risks facing insurers"** By David Lascelles and Keyur Patel. July 2013. ISBN 978-0-9570895-9-4.	£25/$45/€35
111.	**"China's Banks In London"** By He Ying. July 2013. ISBN 978-0-9570895-8-7.	£10/$15/€15
110.	**"Batting For The City: Do The Trade Associations Get It Right?** By Keyur Patel. June 2013. ISBN 978-0-9570895-7-0.	£25/$45/€35
109.	**"Independent Research: because they're worth it?"** By Vince Heaney. November 2012. ISBN 978-0-9570895-6-3.	£25/$45/€35
108.	**"Combining Safety, Efficiency and Competition in Europe's Post-Trade Market"** By Peter Norman. October 2012. ISBN 978-0-9570895-5-6.	£25/$45/€35
107.	**"Seeds Of Change: Emerging sources of non-bank funding for Britain's SMEs"** By Andy Davis. July 2012. ISBN 978-0-9570895-3-2.	£25/$45/€35

Supporters

The CSFI is an educational charity. It has no endowment income. It receives financial and other support from a wide range of public and private bodies, as well as from individuals. Among the institutions that have provided the Centre with financial support are:

Accenture
Arbuthnot
Citi
City of London
Deloitte
HSBC
JPMorgan

ACCA
Association of British Insurers
Aviva
Bank of Italy
Brunswick Group
Building Societies Association
Euroclear
Eversheds Sunderland
Financial Conduct Authority
Gate One
Hermes
ICMA
IHS Markit
Investment Association
Link Scheme Holdings Ltd

3 Lines of Defence Consulting
Absolute Strategy
AFME
Association of Corporate Treasurers
Bank of Japan
Brigade Electronics
Chartered Banker Institute
C. Hoare & Co.
CISI
CMS
Cognito Media
EBRD
Embassy of Switzerland
Endava
ETF Securities
Euro IRP
EVIA
Fairbanking Foundation
Farrer & Co
Finance & Leasing Association
London Stock Exchange Group

Moody's
PwC
Royal Bank of Scotland
Ruffer
Swiss Re
Tradeweb

Jersey Finance
Legal & General
LendInvest
Lloyds Banking Group
Meiji Yasuda
Morgan Stanley
Nomura Institute
Orrick
Oxera Consulting
PIMFA
Record Currency Management
Schroders
Triple Point
UK Finance
Wipro
World Federation of Exchanges

Greentarget
Hardman & Co.
HM Treasury
Intrinsic Value Investors
Ipsos MORI
Kreab Gavin Anderson
MacDougall Auctions
Meritus Consultants
Money Advice Service
NM Rothschild
Nutmeg
OMFIF
Raines & Co
Sapience Communications
Skadden, Arps, Slate Meagher & Flom
Taiwan Financial Supervisory Commission
TheCityUK
Zopa
Z/Yen

The CSFI has also received support in kind from, *inter alia*

Allen & Overy
Burges Salmon
Charles Russell Speechlys
Clifford Chance
Dentons
DLA Piper

Financial Times
The London Institute of Banking & Finance
Kemp Little
Linklaters
Norton Rose Fulbright

CSFI
Registered Charity Number 1017352
Registered Office: North House, 198 High Street, Tonbridge, Kent TN9 1BE
Registered in England and Wales limited by guarantee. Number 2788116