Fedcoin: A Central Bank-issued Cryptocurrency

JP Koning

November 15, 2016

Summary

A central bank-issued digital cash product, henceforth referred to as 'Fedcoin,' dates back to the original design goal of Bitcoin, the creation of a peer-to-peer electronic cash system. Bitcoin's creator envisioned an anonymous payments system without any central points of control. The removal of all central points of control over a currency has the effect of sacrificing price stability, since the absence of an independent entity to 'back' the bitcoins in circulation means that their price cannot be managed during periods of fluctuating demand. This price volatility in turn cripples any appeal bitcoins might have to a broader audience.

Fedcoin is one solution to the volatility problem. It reintroduces one central point of control to the monetary system by granting a central bank the ability to set the supply of tokens on a Fedcoin blockchain. This allows the central bank to guarantee the one-to-one equivalence between digital Fedcoin tokens and physical banknotes. Even though Fedcoin restores the 'backing' point of control over currency, other decentralized features of Bitcoin, such as permissionless validation, may continue to be implemented, the result being that Fedcoin could inherit some of the features of coins and banknotes that Bitcoin has managed to digitally replicate. These include a degree of anonymity, censorship resistance and reusability of tokens. Fedcoin also provides central banks with a monetary control feature not offered by banknotes or coins: negative interest rates.

While Fedcoin might seem like a novel concept, the entrance of government into the issuance of non-cash money for public usage isn't without precedent. A number of theoretical monetary systems have been sketched out over the years that include some form of government deposit money, including James Tobin's deposited currency accounts and the 1930s Chicago Plan. Nor is government participation in the issuance of non-cash money without precedent, the prevalence of postal savings banking systems in the 19th and 20th centuries being perhaps the best historical example.

I. The search for a stable cryptocurrency

Bitcoin: a wildly volatile technological marvel

With the arrival of Bitcoin in 2009, the world welcomed one of its first instances of digital cash (earlier examples such as DigiCash and CyberCash failed to make it out of the 1990s). Conceived under the pseudonym Satoshi Nakomoto, the Bitcoin protocol finds a unique approach to addressing a problem that has long bedevilled digital cash: how to prevent users from costlessly replicating cash tokens and spending the copies *ad infinitum*. One way to solve the problem is to have a third-party validator, say Visa or Mastercard, monitor transactions for double-spending. The Bitcoin protocol avoids the necessity of third party oversight by cross-referencing all new transactions against a shared historical record of previous transactions, the storage and maintenance of this historical record, or blockchain, being outsourced to a distributed network of competing nodes. To protect this record from tampering, these nodes engage in a costly process referred to as 'mining'. Using energy-intensive processing time, miners build blocks of legitimate transactions and submit their work to the network for verification, upon which the record is updated with the new transactions, the winning miner being rewarded with newly-created tokens.

Over the last seven years, the Bitcoin network's digital token (known as bitcoin) has been adopted by a small segment of the world's population as a store of value and medium of exchange. Its price has risen from nothing to as high as $1,000 and now trades (as of September 29) at $604. With 15,838,000 coins in existence, the total value of bitcoins in existence exceeds $9 billion, though on any given day this can change quite dramatically. By way of comparison, there are currently 64 billion Danish krone banknotes in circulation, or US$9.5 billion, which is dwarfed by the U.S. Federal Reserve's US$1.5 trillion in banknotes, although much of this circulates outside of the country.

Inspired by the emergence and staying power of bitcoin, discussion surrounding the idea of a central bank-issued cryptocurrency for broad public use, otherwise known as 'Fedcoin,' began in 2013 on a number of blogs and internet discussion boards.[1] This discussion has since migrated to more formal venues including the academic press and central banking publications. The Bank of England has been particularly vocal on the subject. In a March 2016 speech, Deputy Governor Ben Broadbent discussed the idea of a central bank digital currency involving a distributed Bitcoin-style blockchain containing reserve deposits issued by the Bank of England. Broadbent goes on to say that

> it seems likely that a distributed ledger would make that process easier, opening up the balance sheet to a wider variety of financial firms. One might go further, giving access to non-financial firms, or perhaps even individual households. In the limit, a distributed ledger might mean that we could all of us hold such balances.[2]

[1] See for instance Koning (2013), Motamedi (2014), Koning (2014), and Andolfatto (2015).
[2] The full speech can be read here.

A number of other central banks have introduced central bank digital currency pilots or research efforts including the Bank of Canada[3], the People's Bank of China[4], and the Dutch Central Bank[5].

The original impetus for thinking about Fedcoin was dissatisfaction with the wildly volatile price of Bitcoin which in 2013 had risen from just over $100 to $1000 only to fall back to $300 in 2014. In one tempestuous twenty-four hour period in April 2013, the price of bitcoin plunged from $260 to $50, or 81%. Bitcoin's volatility continues to exceed that of most major financial assets, including gold, the S&P 500, and the U.S. dollar index.[6]

While the typical bitcoin user, an affluent tech-savvy male aged 25-34, might be comfortable with that degree of volatility, most people need to be assured that the purchasing power of a financial instrument will stay relatively stable before they choose to adopt it as money.[7] David Andolfatto, who wrote an early blog post on the topic of central bank-issued cryptocurrency, highlights a pertinent quote from Bill Gates:

> Bitcoin is an exciting new technology. For our Foundation work we are doing digital currency to help the poor get banking services. We don't use bitcoin specifically for two reasons. One is that the poor shouldn't have a currency whose value goes up and down a lot compared to their local currency.[8]

Instead of using Bitcoin, the Gates Foundation prefers to work towards its goal of financial inclusion in undeveloped countries by promoting the use of mobile money; digital currency denominated in and backed by a given nation's unit of account that is issued by telecoms and/or banks and transferable by mobile phone. With volatility obscuring many of bitcoin's redeeming features—in particular its ability to uncannily replicate the properties of banknotes in digital form—the removal of its peaks and valleys in its price seemed imperative if cryptocurrency is to ever gain acceptance, especially in the face of competition with comparatively stable alternatives like mobile money.

Compounding the challenge faced by Bitcoin in gaining broader acceptance are the network effects enjoyed by existing exchange media like the U.S. dollar. Once everyone in a given community has adopted a certain instrument as a standard unit of account and medium of exchange, any single user who tries to defect from the standard by turning to a new unit faces the imposing cost that no one else in the community carries that unit in their wallet or expresses prices with it. Because transacting with a new currency is such a difficult and lonely task, desertion rates from incumbent currencies are very low. This lock-in effect, sometimes referred to as hysteresis, has been discussed in the literature on dollarization. Once a country has been dollarized or partially-dollarized, usually due to mismanagement of the local currency, it faces tremendous difficulties dedollarizing, even if the local currency has long since stabilized.[9]

---

[3] This is known as the CADCoin project.
[4] The People's Bank of China's project is described here.
[5] Otherwise known as DNBcoin.
[6] See the Bitcoin Volatility Index.
[7] See "New CoinDesk Report Reveals Who Really Uses Bitcoin" available here and The 2014 Bitcoin Community Survey available here.
[8] Quoted from Bill Gates's Reddit.
[9] See for instance Oomes, 2003.

Bitcoin payments providers like Coinbase may have some role to play in mitigating network effects and allowing users to cope with bitcoin volatility. For a fee, Coinbase allows retailers to post prices in Bitcoin and immediately receive payment in dollars, a popular feature because it shields them from volatility while expanding the usefulness of Bitcoin to consumers. Bitcoin holders, however, must still bear the instability of bitcoin.

A number of routes to creating a stable cryptocurrency exist, including: self-stabilization of bitcoin, privately-issued stablecoins, a central bank bitcoin peg, and flexibly-supplied Fedcoin. We'll discuss each one.

Self-stabilization of bitcoin

There is a widespread belief that bitcoin's extreme peaks and valleys in price will be ironed out over time as the Bitcoin ecosystem grows and matures, perhaps as new and better financial infrastructure is brought online and products such as derivatives are introduced. With increased usage of bitcoin as a medium of exchange, the effects of speculative behaviour on the price will be dampened, thus making it more competitive with traditional currencies.

That bitcoin volatility has declined over the last five years is not to be doubted. But the fact remains that bitcoin is an unusually volatile asset for its size, often demonstrating the volatility of a penny stock. Furthermore, bitcoin turnover continues to be quite low due to the tendency amongst users to hoard tokens as a means to gain exposure to potential price gains rather than for regular day-to-day trade.[10] To gain acceptance as a medium of exchange, bitcoin must become less volatile, but to become less volatile it must gain wider acceptance—this seems like an intractable problem. At best, bitcoin's fixed supply means that its volatility may one day resolve itself to the same level of fixed supply commodities like gold or oil, say Bolt and Van Oordt.[11] A system that locks the supply of coins lacks the gold feedback loop of mines opening and closing which is a critical supply-side feedback loop to reduce volatility. Due to the inelasticity of supply, bitcoin must be more volatile than gold and silver, other things being equal.[12] An instrument that exhibits volatility in excess of gold and silver implies it isn't sufficiently stable money for the great majority of individuals.

Privately issued stablecoins

Another solution to the volatility problem is to depart from the Bitcoin model and introduce private cryptocurrencies that are themselves pegged to the U.S. dollar.[13] As Luther points out, there is precedent for the private provision of tokens that trade at par with an official currency like the dollar. Bank deposits are the most obvious example, although Luther also cites the practice of private banks in Scotland and Northern Ireland issuing banknotes that exchange at par with the British pound.[14]

---

[10] See Tim Swanson, here and here.
[11] Bolt and van Oordt (2016) see bitcoin's extreme volatility as a symptom of early development. Over time, volatility should drop, although the fixed supply of bitcoin means that its volatility will reflect that of other commodities rather than traditional currencies.
[12] Robert Sams makes this point here.
[13] Buterin offers a number of ideas here.
[14] Luther, Theoretical Fedcoin Meet Operational Nubits, 2015.

Several examples of private pegged cryptocurrencies, or stablecoins, currently exist. Tether, for instance, operates very much like a modern currency board, maintaining a reserve of U.S. dollars in a bank account and issuing cryptocurrency units, known as Tethers, that are fully backed by those reserves. However, unlike cash and Bitcoin, Tether users must trust a centralized issuing body to hold sufficient reserves. BitUSD, a competing stablecoin protocol, avoids the centralization problem by keeping reserves on a distributed blockchain. More specifically, a network of users ensures that a sufficient quantity of bitShares, itself a cryptocurrency, are held on-chain as collateral for each bitUSD. When bitUSD falls below $1, say to 97 cent, then bitShares are used to repurchase bitUSD until the price of the latter has returned to par. bitUSD's peg to the dollar has remained in place since 2014.

This history of pegged private stablecoin is less than pristine, however. NuBits, a stablecoin that debuted in 2014, has several mechanisms for maintaining its peg. When demand for NuBits grows, the Nu protocol simply increases the supply of NuBits commensurately until upwards pressure on the peg is relieved. Maintaining the peg when demand falls is more complicated. The first line of defense is an offer to pay interest in the form of new NuBits to any NuBits owner who promises to "park," or withhold, their tokens from circulation, thus removing downward pressure on the peg. A second option involves having the administrators of NuBits sell off related tokens called NuShares, using the proceeds to support NuBits in the open market. Unlike NuBits, NuShares are not designed to be stable. Rather, they are digital tokens that offer owners a share in the profits accruing to the operations of NuBits as well as a voice in how the network is run.

The payment of interest in the form of new NuBits as a carrot for withdrawing NuBits from circulation, or parking, seems problematic – an excess supply of currency is being attacked by a mechanism that itself creates even more supply. The next level of support, the selling of NuShares, might require such large sales that NuShares falls to zero (or some very low number), the backing assets' worthlessness causing the peg to fail. A collapse in the peg is indeed what eventually happened when a large NuBits seller emerged in late May 2016, forcing the administrators of the Nu network to use scarce reserves to defend the peg. NuBits began to trade at 95 cents in late May and finally collapsed to below 50 cents in June.[15]

While the NuBits experiment has failed, it would be too hasty to pour cold water over the entire private stablecoin enterprise. BitUSD has succeeded in holding its peg to the U.S. dollar since September 2014 while Tether's newer, but tighter peg, is holding too. Maker DAO, built on the Ethereum network, may build on these successes.

A central bank bitcoin peg

The next solution is a pegged cryptocoin. Hypothetically, the most effective means of pegging a cryptocoin to a central bank-issued currency is to have the central bank itself underpin the entire scheme. One way to implement this scheme would be for the central bank to peg the price of an already-existing cryptocoin, such as bitcoin. The Bank of England, for instance, would offer to buy and sell unlimited amounts of bitcoin at $500.

[15] Koning, End of a Stablecoin, 2016.

However, a central bank cannot target two nominal variables—both an inflation target and the price of bitcoin—at the same time.[16] If the level at which it sets the bitcoin peg is not consistent with the inflation target of 1-3% a year, to reacquire its inflation target the Bank of England will have to give up on its bitcoin peg. If it decides instead to keep the bitcoin peg, the Bank of England will have to temporarily give up targeting inflation. Under a pure bitcoin peg, the nation would operate on something very similar to a gold standard with bitcoin in the place of gold. The British economy's price level would become hostage to the supply and demand for bitcoin, just like in previous centuries when the supply and demand for gold determined the economy-wide price level. If a central bank were to take a country onto the Bitcoin standard, economic theory states that the macroeconomic forces that might be set off could be disastrous.[17]

The second problem is that even though a central bank usually has more power to defend a peg than a private actor, the peg will never be impregnable. Should the market doubt its integrity, it will be attacked. If the attack goes on long enough, reserves will run out and the peg will have to be sacrificed. The best example of a failed government peg is the Bank of England's linkage of the pound to the Deutsche marks within a band that had as its midpoint a rate of 2.95 marks to the pound. The Bank was forced to give up on its peg in September 1992 when speculators led by George Soros began to bet against it, the pound subsequently falling to 2.40 marks by the end of October.

The third problem is that pegging the price of bitcoin would set a controversial precedent whereby early adopters of bitcoin, who bought when its price is low, are heavily rewarded by the central bank. This could result in a spate of cryptocurrency launches as others try convincing central banks to adopt them.

Flexibly-supplied Fedcoin

Satoshi Nakamoto designed Bitcoin to ensure that the quantity of bitcoins outstanding is controled by a protocol rather than a central actor. To begin with, there is a 21 million ceiling on the number of bitcoins. New tokens can only be created as a reward to miners for verifying bitcoin transactions.[18] Because bitcoins cannot be automatically uncreated, the quantity of bitcoins outstanding steadily marches higher thanks to the issuance of rewards until the year 2140 when the bitcoin supply will be fixed for the rest of time at 21 million. This lack of flexibility simply won't do if the goal is to create a monetary policy-friendly cryptocoin. Rather, the fixed quantity feature of the Bitcoin protocol must be modified in order to grant the central bank complete control over the supply of cryptocoin, thus removing any floor or ceiling to its quantity.

The creation and redemption mechanism for a monetary policy-friendly cryptocoin, or Fedcoin, would work as follows. To begin with, the central bank publishes the exchange rate

---

[16] This is Robert Mundell's impossible trinity, described in his Nobel Prize lecture.
[17] There is a broad literature explaining how the gold standard helped to either start or accelerate the economic forces leading to the Great Depression. Glasner, for instance, cites Cassel and Hawtrey who blame the Bank of France and the Federal Reserve for unwarranted gold purchases that breed the sudden and dangerous deflation that would set of the Great Depression.
[18] Every 210,000 blocks the coin supply creation rate divides in half, or roughly every four years. A hard fork could change this ceiling.

between Fedcoin and banknotes in circulation, i.e. $1 note = 1 Fedcoin. If the public wants to hold more Fedcoin at the published exchange rate, to get new tokens, people must turn over banknotes for new Fedcoin of the same nominal quantity (i.e. a five dollar bill for five Fedcoins). Those banknotes would in turn be cancelled by the central bank.

Where would the central bank get new Fedcoins? One possibility is that the protocol allows the central bank to create new Fedcoins for its account whenever it needs to meet cash-to-cryptocoin requests. If using Bitcoin technology, this would likely mean giving a single key the right to sign the first transaction in the block, creating a variable number of coins as freshly mint value, rather than leaving this open to the winning miner. This replicates the model for how central banks currently provide cash; whenever commercial banks need banknotes in order to meet customer requests they do so by redeeming central bank deposits, the central bank in turn printing this cash on demand. If the public wants less Fedcoin, the process works in reverse: the central bank simply redeems unwanted tokens and issues banknotes in their place. The protocol would allow the central bank to destroy unwanted coins, much like it shreds old currency.

An alternative way to create Fedcoin would be to "preallocate" the entire supply of tokens (say $100 trillion Fedcoin). This block would immediately be awarded to the central bank to be held in reserve until they are required.[19] Ripple set the precedent for a 100% preallocation. At its inception, the entire 100 billion supply of XRP (Ripple's native token) was created outright, much of it retained by Ripple Labs while the rest was auctioned off or given away.[20] As for a reduction in supply, the central bank can store surplus cryptocoins in its vaults, much as it does with deposited banknotes that are still fit for a second go around. Preallocating simplifies security requirements, as no one has the ability to issue Fedcoins; however, it is exceedingly difficult to change supply later if demand is underestimated. A new coin, say Fedcoin 2.0, would have to be issued in order to complement the exhausted supply of Fedcoin 1.0.

How does the central bank put those coins into the economy? It swaps Fedcoin for notes on demand at a fixed rate. By using a cash-in and cash-out mechanism for introducing Fedcoin, a central bank ensures that the combined quantity of banknotes and Fedcoin remains unaffected, and only the relative contribution of each one to the total changes. As Andolfatto describes it, this setup means that Fedcoin functions like just another currency denomination.[21] For example, if the Federal Reserve were to introduce a $200 bill, it would set a 2:1 peg between the $100 bill, a 4:1 peg with the $50, a 200:1 peg with the $1, etc. Should demand for converting $100 bills into $200 bills explode, the central bank can effortlessly maintain the peg by having as many $200s printed as necessary to satisfy demand while shredding $100s as they pour into Fed vaults. Likewise, under a Fedcoin scenario, the Federal Reserve would establish a 1:1 peg to the $1 bill, a 1:100 peg to the $100 bill, etc., these exchange rates being unassailable since the Federal Reserve can mint or cancel any quantity of Fedcoin.

Nor would there be any reason to worry about the effect of either the $200 bill or Fedcoin on monetary policy. A central bank's denomination structure—the spacing it chooses to set between its various denominations of bank notes—is irrelevant to the maintenance of an

[19] This idea was originally described by Szmigielski (2015).
[20] See here.
[21] Andolfatto, 2015.

inflation target. Thus we arrive at a stable cryptocoin without compromising the central bank's ability to follow an independent monetary policy.[22]

[22] Stability is only ensured if an attack on the network doesn't lead to a coping effort on the part of the central bank that involves unpegging or devaluing the Fedcoin-to-banknote rate. See "Undoing Fedcoin when it goes wrong."

II. To what degree should the public have access to central bank non-tangible money?

Having established that it is possible to issue a stable central bank-issued cryptocurrency for use by the public, should central banks spend time and effort on doing so?

Any discussion of Fedcoin brings into focus the current division of responsibility between government and the private sector on the supply of media of exchange. While the idea of Fedcoin seems quite modern, it is really just a narrow version of a much older and more general proposition: Should government be responsible for providing non-tangible money to the broad public or should the private sector be wholly responsible? Tangible money is comprised of banknotes and coin while non-tangible money is everything else, specifically tokens existing in book or digital form, of which Fedcoin is but one manifestation. Other types of non-tangible money include transferable deposit accounts, credit cards, or mobile money.

Under the modern paradigm, central banks do *not* offer any non-tangible money to the public.[23] In the next section we will investigate this paradigm more closely in order to get a better understanding of how alternative paradigms, both historical and imagined, find room for a potential Fedcoin.

The modern money-issuing paradigm

Of the two highly liquid financial instruments that central banks currently issue—tangible banknotes, or cash, and non-tangible demand deposits—the public is limited to owning cash. The maintenance of accounts at the central bank for payments purposes is confined to commercial banks, domestic and foreign governments, and other central banks. When members of the public, either individuals or non-financial corporations, want to make use of non-tangible money they can only do so by opening an account at a commercial bank.[24]

Another key feature of the modern paradigm is that private banks cannot themselves issue banknotes. Rather, the provision of paper money is the exclusive prerogative of the government. This wasn't always the case – in the 18th, 19th, and early 20th centuries, private banks enjoyed the power to print paper currency. As central banks increasingly took on the role of exercising monetary policy, government saw fit to pass legislation giving central banks a monopoly over the issuance of banknotes.[25] [26]

---

[23] The exception is Ecuador. See Section II.

[24] Individuals can also buy prepaid cards that are connected to banks but do not require a bank account. However, relative to deposits, prepaid cards account for a small number of transactions. In developing countries, mobile money providers have sprung up as a competing private alternative to commercial banks, the most iconic of which is the Kenyan-based mPesa brand.

[25] The only modern example of privately-issued banknotes is in Scotland where most circulating paper currency is issued by three private banks: the Bank of Scotland, the Royal Bank of Scotland, and the Clydesdale Bank.

[26] While this is the case in most parts of the world, the U.S. is different. The U.S. constitution vests in Congress the power to regulate money, but Congress has never explicitly defined what money is. While congress has given legal status to a variety of currencies issued under its authority, and has restrained specific currencies not under its authority, the legal means to drive out currencies other than Federal Reserve notes were

In most situations, non-tangible media of exchange such as deposits are a technically superior payments option to banknotes and coins. Deposits have a pecuniary advantage: unlike cash, they can earn interest, an advantage which is reversed when rates go negative. A number of physical characteristics separate the two media. Banknotes can only be safely transferred face-to-face whereas non-tangible money can securely cross vast distances, at little to no cost. And while banknotes can be easily damaged or stolen, deposits are highly secure. Deposits are perfectly divisible; cash is imperfectly divisible, especially if parties lack appropriate change. Lastly, cash is bulky. While a million U.S. dollars can be represented in digital form with just a few bits, it requires a small suitcase-sized container to store and transport that amount in banknotes.

Figure 1: The Relative Quantities of Notes/Coins and Deposits in Developed Nations

	Notes and coin in circulation outside banks	Value of transferable deposits	Non-tangible to tangible ratio
Sweden	79.6	1945	24.4
United Kingdom	65.5	1437.6	21.9
Canada	69.42	699.48	10.1
South Korea	64439	521384	8.1
South Africa	94.19	678.8	7.2
Japan	88164	530561	6.0
Switzerland	62.69	329.1	5.2
Euro area	921.2	4828	5.2
Australia	61.75	257.4	4.2
United States	1254.1	1719.7	1.4
Average			9.4

Source: BIS, 2015, Statistics on payment, clearing and settlement systems in the CPMI countries

The public's preference for deposits over banknotes is best evidenced by the much larger quantity of the deposits in circulation than banknotes. As Figure 1 illustrates, data from a sample of developed countries shows that transferable deposits exceed the quantity of banknotes and coins in circulation by an average factor of 9.4. Sweden leads the pack with 24.4 krona worth of transferral deposits for each 1 krona banknote while the U.S. takes up last position with just $1.40 in deposits for each $1 in paper currency in circulation.[27]

Cash isn't without its own advantages. Unlike deposits, banknotes can be used without the buyer providing information about their identity. As a result, paper currency is a popular medium of exchange among those who desire anonymity. While this list includes criminals and tax evaders, the anonymity afforded by cash is also useful for less nefarious purposes. For instance, it shields consumers from potentially malicious sellers who might try to skim personal information in the case of a debit or credit transactions. When consumers wish to keep legal purchases secret from friends and family, cash is a better option than bank money.

Second, cash is *censorship-resistant*. This means that there is no way for the third party operating the payments mechanism to directly prevent anyone who wants to accept cash or spend cash from doing so. Contrast this to bank deposits, which is not censorship resistant; individuals can be prevented from opening bank accounts or, after having opened an account, may find that their ability to receive or make deposit payments impeded by a bank

repealed in the 1970s and 90s so that the private issue of notes is technically legal in the U.S. (See Schuler, 2001).

[27] The U.S.'s low ratio should be taken with a grain of salt, however, since U.S. banknotes are a popular medium of exchange in both dollarized and partially-dollarized nations, as well as a major form of transacting in international illicit trade

manager.[28] Third, cash is useful in areas where banking infrastructure has been slow to penetrate, or when electricity and other infrastructure has been temporarily disabled, such as during emergencies.[29] Fourth, cash is not always disadvantaged relative to deposits from a pecuniary perspective. It is difficult (but not impossible) for cash to be charged a negative interest rates, an advantage to its owner. Lastly, cash carries less credit risk than a bank deposit. A deposit provides its owner with a bank-issued claim on paper money whereas paper money is the actual thing, a feature that becomes relevant when it is too late to respond—during insolvency and bail-in.

That there is significant redemption risk inherent in deposits is due to the fact that the modern commercial banking system operates on a fractional reserve basis, that is, banks do not hold an equivalent-sized number of paper dollar reserves for each dollar of bank deposits they issue. Rather, apart from a thin sliver of paper money held in their vaults, banks maintain a portfolio of income-generating assets like securities and loans that must be liquidated in order to meet deposit redemption requests. Should those assets be impaired, the bank may not be able to acquire enough paper money to redeem all its deposits and will have to default on its promise.

This risk of default is partially mitigated by government deposit insurance which guarantees that depositor funds will be returned should a bank go bankrupt. However, many countries have not instituted deposit insurance schemes. Even when they have, deposits are typically covered up to a fixed amount with anything above the ceiling going unprotected. Bail-in, or the use of depositor funds, has been added as a legal remedy to many banking codes.[30] On top of all this, deposit insurance imposes an extra set of costs on society. It incentivizes banks to engage in riskier behaviour than they otherwise would since many depositors might not keep a watchful eye on the actions of their custodians.

In summary, the modern paradigm is one in which the world of publicly-available exchange media has been divided into two categories, tangible and non-tangible money, with government monopolizing the first and the private sector the second. Because anonymity and censorship-resistance are solely provided by cash, the government is essentially the lone provider of universally-available private transactions services. Despite these unique features, the qualities of non-tangible money (i.e. demand deposits) are far more preferred by the public (at least in the developed world). This preference arises despite the fact that, by outsourcing the provision of public non-tangible money to the private sector, all the convenience that non-tangible money provides to the public has been twinned with the burden of bearing credit risk, a risk that is somewhat mitigated by deposit insurance.

A government-issued cryptocurrency for public use would represent a sharp break with the modern paradigm. The public would be able to engage in an economic activity previously not available: the buying and selling of default-free electronic money. This money might be in the form of mobile money, a deposit account at the central bank, or Fedcoin. If the central

[28] For more on censorship resistance of cash, see Andolfatto (2015).
[29] Williamson (2015)
[30] In 2013, Cyriot deposits were frozen in preparation for a bail-in. The original formula envisioned that all those with 100,000 euros or less would face a haircut of 6.75%. Due to pushback, the plan was amended to only apply haircuts to those with more than 100,000 euros in their accounts.

bank were to enter the business of providing non-tangible money to the public, how far should its participation in this space go?

Alternatives to the modern paradigm

Two alternative money-issuing paradigms propose some degree of government involvement in the issuance of non-tangible money: 1) limited private issuance, and 2) a cashless world. The limited private issuance model attempts to rectify some of the modern paradigm's perceived deficiencies, specifically inadequate financial inclusiveness, a failure to provide the public with genuinely safe money, and the tendency for modern economies to exhibit destabilizing financial panics.

The second paradigm, a cashless world, sets out to rectify two different deficiencies in the modern paradigm. First, in a slow growth environment like the one we are currently experiencing, it may be necessary for governments to set deeply negative rates, for reasons to be explained later. Cash, which effectively yields 0%, prevents this from happening. Secondly, the existence of cash subsidizes a wide variety of welfare reducing behaviours including crime and tax evasion. Remove cash and the cost of criminality might rise, especially in low value and street crime. If the government were to use either of these two motivations to justify abolishing banknotes, the absence of cash could be made up by offering the public risk-free digital money like Fedcoin.

A. Limited private issuance

The various versions of limited private issuance try to inoculate the banking system, and therefore the economy, from destabilizing outbreaks of financial panic. The first version, the full reserve banking model, is the most radical option because the limit it imposes on banks would result in a complete remodelling of the banking landscape. [31]A less intrusive limit is to implement central bank-issued non-tangible money like Fedcoin while continuing to allow the private sector's ability to issue deposits, much as before.[32] This would provide the public with a safe payments medium heretofore lacking while also reducing some of the perverse effects of deposit insurance.

The other motive for limited private issuance paradigm is the role that government-issued non-tangible money can play in promoting financial inclusiveness. The argument here is that the profit motive that drives the private sector leads banks to underserve various segments of the population. The government can fill this gap by issuing a competing deposit option.

1. Full reserve banking

Because fractional reserve banks do not maintain a 1:1 correspondence between deposits and reserves, they may not be able to meet their promises. A bank run proceeds as depositors line up at the teller in an effort to get their money out of the bank before it is all gone. Should the panic spread to other banks, a financial crisis emerges that has broader macroeconomic implications such as deflation and the loss of jobs.

---

[31] Laina (2015) provides a full description of the many reserve banking models.
[32] For instance, a limited private issuance model is assumed in Barrdear and Kumhof (2016).

Bank runs and the ensuing financial chaos they create have always been endemic to capitalist systems. Adam Smith, the father of capitalism, was caught up in the failure of the Ayr Bank of Scotland, which embroiled Smith's patron the Duke of Buccleuch—one of the bank's largest shareholders—for a number of years.[33] One of the most common proposed solutions has been some version of full reserve model, where every deposit is backed by an equivalent amount of government money in the vault, thus making deposits risk-free. This remedy boasts a long intellectual pedigree going at least as far back as David Ricardo, the famous English economist, who advocated a policy whereby all English banknotes were to be 100% backed by gold.[34] The idea was in turn rekindled during the Great Depression by circulation of the so-called Chicago Plan in 1933 and the publication of Irving Fisher's 100% Money and the Public Debt in 1936.

The 2008 credit crisis has brought renewed interest in full reserve banking. In 2012 IMF economists Benes and Kumhof modelled the Chicago Plan using modern economic techniques, finding support for a number of claims put forth back in 1933.[35] Martin Wolf, chief economics commentator at the FT, came out in support of the idea in a 2014 editorial.[36] A number of similar schemes have been proposed including Andrew Jackson and Ben Dyson's PositiveMoney,[37] John Kay's Narrow Banking[38], Lawrence Kotlikoff's Limited Purpose Banking[39], and John Cochrane's run free financial system[40]. On the political front, a Swiss organization called the Vollgeld initiative managed to collect 100,000 Swiss signatures, enough to put the proposition of full reserve banking to a referendum sometime in 2017 or 2018.

The 1933 Chicago Plan, named after a group of University of Chicago economists who wanted to avoid a repeat of the Great Depression, proposed the creation of 'deposit banks.' These institutions would be required to keep a 100% reserve of dollars, ensuring that sudden redemption requests by depositors could always be met. As for the traditional practice of matching savers with lenders, the Chicago economists called for the establishment of 'investment trusts.' These specialized financial institutions were to fund themselves by issuing equity or debt, lending these funds out to businesses and individuals who needed to finance new projects. If the loans were to go bad, the market would react by rapidly marking down the price of the price of the firm's equity and bonds. This stands in contrast to fractional reserve banking scenario where, thanks to the fixed price of deposits, the market's dissatisfaction would quickly express itself in a long lineup outside the bank. In theory, the financial traumas arising from banks would become a thing of the past.

So where does Fedcoin fit into the full reserve banking model? If a government wants to implement a full reserve banking system, it isn't necessary for it to create risk-free non-tangible money like Fedcoin for public use. Rather, the government simply requires commercial banks, which already issue non-tangible money, to adopt its definition of what constitutes the legitimate form of non-tangible money. It is always possible that the private

[33] Murphy (2009), the Genesis of Macroeconomics
[34] See Laina.
[35] Benes and Kumhof (2012).
[36] Financial Times (2014).
[37] Positive Money (2014).
[38] Kay (2009).
[39] Kotlikoff (2012).
[40] Cochrane (2014).

sector opts out of the business of issuing 100% reserve money because it is not profitable, or does so at such a high price that large segments of the population go unbanked. This scenario isn't outlandish. As Lawrence White writes, history shows that when banking rules were relatively unregulated, full reserve banks have always been outcompeted by fractional reserve banks.[41] The Chicago Plan specified that any shortfall on the part of the private sector in providing the public with demand deposits was to be filled by government-provided deposits, the postal savings system put forth as one mechanism for doing so.[42] A more modern implementation of postal money could be Fedcoin.

The next five scenarios, three of them theoretical and two historical, motivate the founding of Fedcoin by imposing a much less dramatic limitation on private issuers than full reserves: having them compete directly with the government.

2. Deposit insurance and James Tobin's "deposited currency accounts"

Nobel Prize-winning economist James Tobin once described deposit insurance as the delegation to the private sector the "government's sovereign right to coin money." Devised in 1935 as a way to avoid bank runs, Tobin believed that deposit insurance made sense at the time, but he was worried about growing abuse of the system:

> Today, however, there appears to be a much greater component of imprudence and adventurism, even self-dealing, in the incidence of failure. Moral hazard is rampant; The sounder and luckier--it is not easy to distinguish--members of federal insurance corporations understandably balk at paying higher premiums to salvage the depositors of failed members. The taxpayers can be left holding the bag. Congress affirmed the government's ultimate guarantee just the other day.
>
> As has long been recognized, deposit insurance dulls the incentives of depositors to scrutinize the soundness of the depository's assets and the incentives of the institution itself to maintain liquidity and asset quality sufficient to limit to low probability the contingency that it will be unable to meet withdrawals.

Moral hazard emerges when the provision of deposit insurance changes the behaviour of those who receive the insurance in an undesirable way. As the public's cash holdings increase at the expense of insured deposits, the window for moral hazard window is closed. This window can only narrow so far, says Tobin, because the demand for cash will always be limited by its inconveniences including bulkiness and lack of a pecuniary return. This leads to an excessive reliance on the convenience of insured deposits, leaving the window open for the sorts of abuses that deposit insurance promote.

Tobin's idea was to remedy the physical defects of central bank money by having the Federal Reserve offer deposits directly to the public, known as *deposited currency accounts*. These deposits would be transferable by wire, check, or giro-type payments to other accounts within the system. Interest would be paid at a rate below that of Treasury bills. Deposited currency's uptake would be much larger than cash, thus widening that part of the financial system made secure without the help of deposit insurance and reducing the scope for moral hazard. Tobin specified that the wellbeing of two segments of the population would be improved by a

[41] White (2012).
[42] Phillips (1992). The 'Chicago Plan' and New Deal Banking Reform

deposited currency scheme: the poor, who tend to value safety over interest, and depositors who need safety in amounts that exceed deposit insurance ceilings.

Tobin devised his deposited currency scheme long before the rise of the internet, mobile phones and Bitcoin. There are many way of implementing Tobin's deposited currency plan, including adopting an Ecuadorian-style government mobile money scheme, discussed later in this report. Alternatively, it might be possible to implement a blockchain-based system whereby the public would buy Fedcoin tokens, and these would compete directly with private bank deposits.[43]

3. Gruen's Government Banking for All

To make banking cheaper and safer, Nick Gruen suggests that technological changes, specifically the internet, should be harnessed to introduce government-issued digital money for the public.[44] According to Gruen, before the internet the provision of banking services required physical branches. Central banks, which do not typically branch, evolved a model whereby they 'wholesaled' their core payments services to banks which would then offered those services to individuals and businesses via their branch networks. The internet now allows central banks to skip the middleman by wholesaling directly to a retail clientele.

Gruen's recommendation, which is focused on the U.K., is to modify the features of personal savings accounts held at National Savings and Investments (NS&I), a government-owned savings bank that descended from the Post Office Savings Bank, so as to allow online payments between accounts. NS&I lends directly to the government so that all deposits are secure. It should be noted that in proposing internet-based NS&I deposit accounts, Gruen does not support the establishment of a government-owned bank with a physical presence, only an online presence. The provision of services requiring bank branches should be left to the private sector which already does so competitively and competently.

According to Gruen, the scheme would provide the British government with lower interest costs while citizens would get the ability to hold as much risk-free money as they desire. By having the public sector take a greater role in facilitating retail payments, Gruen believes that more competitive pricing and better services would be induced from the private sector.

While Gruen's vision of a government-issued non-tangible money comes in the form of NS&I accounts, a Fedcoin-like product could also stand in its place.

4. Andolfatto's Treasury Direct

---

[43] Barder and Kumhof model a modern version of Tobin's deposited currency scheme involving a central bank-issued digital currency (CDBC): "By CBDC, we refer to a central bank granting universal, electronic, 24x7, national-currency-denominated and interest-bearing access to its balance sheet. We conceive of a world in which the majority of transaction balances would continue to be held as deposits with commercial banks and subject, where relevant, to existing deposit protection arrangements. Credit provision would remain the purview of existing intermediaries, and commercial banks would continue to be the creators of the marginal unit of money in the economy. In short, we imagine a world that implements Tobin's (1987) proposal for "deposited currency accounts"."

[44] Gruen (2014), Central Banking for All

David Andolfatto envisions a government-provided basic utility account. Focusing on the U.S., he suggests that the U.S. Treasury's *Treasury Direct* service, which offers online digital bond accounts to the public, be modified to allow for payments.[45] Andolfatto lists a number of advantages to implementing this sort of scheme including: 1) there would be no need for deposit insurance; 2) corporations could keep money at the central bank rather than putting it in the riskier shadow banking sector and 3) the cost of printing and maintaining banknotes would be eliminated.

To address concerns over lack of anonymity, Andolfatto has also proposed a related Fedcoin scheme.[46] The Federal Reserve would issue a cryptocurrency, or Fedcoin, at a fixed exchange rate where payments are made using what Andolfatto refers to as a "Bitcoin-inspired anonymous communal consensus algorithm."

5. Postal banking

In 2014, Mehrsa Baradaran published a paper calling for the United Postal Service (USPS) to offer banking services to Americans.[47] Baradaran's plea echoed that of the Office of the Inspector General of the USPS, which released a whitepaper earlier that year proposing that financial services offered by post offices would help reach millions of underbanked and unbanked citizens who, according to a 2011 FDIC survey, amount to 20% and 8% respectively of the U.S. population.[48] Low-income individuals and minorities are disproportionately represented in this group. Mobile transactions are one of the suggested product offerings in the USPS report, specifically a Postal Service branded open-loop reloadable prepaid card referred to as the Postal Card. Customers would load their cards by bringing cash to a Post office and would be able to cash out using ATMs located on the premises. Postal Cards would be integrated with online accounts that allow customers to digitally transfer funds and pay bills.

The provision of financial services via the postal system is not new. In 1911, the USPS-operated United States Postal Savings System was opened. Much like the U.S. Federal Reserve, which was established in 1913, the Postal Savings System was a direct reaction to the Panic of 1907, which brought down a number of banks including the Knickerbocker Trust Company. Carter Keene, the director of the Postal, described the role of the system as not just a means to a profit:

> "Its aim is infinitely higher and more important. Its mission is to encourage thrift and economy among all classes of citizens. It stands for good citizenship and tends to diminish crime. It places savings facilities at the very doors of those living in remote sections, and it also affords opportunity for safeguarding the savings of thousands who have absolute confidence in the Government and will trust no other institution."[49]

---

[45] Andolfatto (November 2015).
[46] Andolfatto (February 2015).
[47] Baradaran (2014), It's Time for Postal Banking.
[48] Office of Inspector General, United States Postal Service (2014). Providing Non-Bank Financial Services for the Underserved [link]
[49] New York Times (October 12, 1913)

The U.S. Postal Savings System was eventually closed in 1966 after a long period of declining usage. This decline can be blamed on uncompetitive interest rates on postal savings account, which lagged far behind private alternatives.

The U.S. is by no means unique in having provided banking services through the postal system. Great Britain began to provide postal savings products back in 1861 when it opened the Post Office Savings Bank. For much of the bank's existence these products were limited to savings accounts, government bonds, and lottery bonds. In 1968, however, it introduced National Giro, a payments option. According to Gruen, Girobank offered customers giro transfers[50] that cleared far quicker than bank-to-bank transfers as well as 'girocheques' that could be cashed in a bank or a post office.[51] Girobank was also the first to pay interest on chequing accounts.[52] Commercial banks were forced to adapt by offering matching interest payments, establishing their own credit transfer, or giro, services and by linking their ATMs to offer customers more accessibility. In 1989, Girobank was privatized by the Thatcher government, putting an end to 21-years of government-issued non-tangible money.

While many nations have adopted postal-based payments, the trend has been for governments to close or sell them to the private sector including: Canada in 1968, Netherlands in 1986, New Zealand in 1989, Germany in 1995 and Austria in 2000. Not all postal savings systems have ceased to exist, however. The longest-standing example of government-provided postal money can be found in Japan, which introduced a postal system in 1875 before adding giro services in 1907. Kuwayama claims that Japan Postal Banking accounts for just over half of all giro payments[53] and according to many commentators is the world's largest bank ranked by deposits.[54]

The lesson from postal banking is that far from being unusual, a government role in the provision of public non-tangible money has been quite common over the last 150 years or so. The motivations for this role have been numerous, but an important one appears to be the perceived value that a government can bring in providing a safe and trusted medium to the population. The adoption of financial technology appears to be another important motivator; postal banks brought giro payments to the masses decades before private banks, which continues to rely on the slower cheque-based payments model. Postal banks have also been justified as a way to reach those underserved by regular banks.

Postal savings accounts are of course only one way to meet these goals; some sort of government issued Fedcoin could also fill the same criteria. Indeed, the USPS recently trial-

[50] Giro transfers refer to direct payments to or from an account without requiring an intermediate exchange into cash or use of a cheque.
[51] Gruen, pg 24
[52] "Girobank brand laid to rest after 25 years", the Guardian, July 7, 2003 [link]
[53] Kuwayama (2000), Postal Banking in the United States and Japan.
[54] The postal banking system enjoyed a number of government-granted advantages over banks. According to Grimes (2001), all Japanese citizens could enjoy tax protection on one savings account up to a certain amount. Since postal banks were not required to closely track the identities of depositors, the ceiling could be evaded by opening multiple accounts at many different post offices. Banks were obligated to match identities with accounts and thus could not allow customers to exploit the same loophole.

ballooned the idea of something called Postcoin, a token that could be loaded at a local post office and used for transactions.[55]

6. Central bank accounts for the public

Since its founding in 1696 the Bank of England allowed members of the public to open accounts. Some of these depositors were quite famous. An interesting anecdote from the 1700s has Sarah, Duchess of Marlborough, asking her bankers at the Bank of England to provide her with a freebie, namely some pens because she 'could get none that were good.' [56]

Moving forward a century, we learn that, upon opening for business in 1855, the Bank of England's Western branch tended to attract small businessmen and private individuals "of modest means" as clients, including the accounts of the University of London, a Regent Street hatter, and a Sackville Street clothier—all on its first day of operations. Later that year the household of Queen Victoria left its private bank in order to do business with the Western branch. By all accounts, the Bank of England seems to have had excellent service:

> Staff were expected to recognize customers on sight and have a good, clear hand for writing up passbooks. Two porters were always on duty at the main entrance, clad in the pink livery of the Bank of England with silk top hats, and even the cashiers wore top hats when serving at the counter.[57]

The Bank of England kept up a retail presence well into the 1900s.[58] But as public service came to be regarded as the Bank's main role, the aggressiveness of its commercial and retail businesses was reduced and it transitioned into a purely bankers' bank. The Western branch would be sold in 1930 to the Royal Bank of Scotland.[59] By 1963 the Bank of England's services to the public were limited to a small number of accounts for existing customers. Presumably as they died, these accounts were closed. to the Bank continued the practice of allowing employees to keep accounts at the Bank, although it recently announced that it will be discontinuing these accounts.[60]

Perhaps the only modern example of central bank money for public consumption comes from Ecuador. In 2015 the Central Bank of Ecuador (CBE) began to offer Ecuadoreans a service called *Dinero electrónico*, a form of mobile money that, apart from its public ownership structure, is very similar to Kenya's privately-owned mPesa. Users with mobile phones can remotely open an electronic money account with their national identity card and begin receiving payments. Alternatively, they can visit a transaction centre and in return for a deposit of cash receive an equivalent quantity of mobile money tokens. Those same deposit centres also offer cash-outs.[61] The goal of the CBE's Dinero electrónico monopoly is to offer broad accessibility to basic payments services while avoiding some of the problems involved

---

[55] Office of Inspector General United States Postal Service (2016), Blockchain Technology: Possibilities for the U.S. Postal Service [Link]
[56] Bank of England: first report, session 1969-70.
[57] Western Branch of The Royal Bank of Scotland - The Story of a Bank and its Building (pdf)
[58] Other central banks that have offered retail deposits at some point in their history include the People's Bank of China and the Banco de Brazil.
[59] Branches of the Bank of England, 1963 (link)
[60] The Guardian (2016) "Bank of England Closing Personal Banking Service for Employees"
[61] Bank of Ecuador website [link]

with private mobile money schemes, namely their lack of interoperability, or the inability to transfer easily between one type of private mobile money and another.[62]

So, while issuing a central-bank issued non-tangible money like Fedcoin might seem a radical approach to dividing the provision of money to the public, the practice of allowing private individuals and non-financial businesses to directly hold central bank deposits is an established one. What further lessons can we take from these examples?

Robert Sams has pointed out that, if individuals are allowed to directly own safe central bank deposits, there may be no reason for them to hold risky bank accounts.[63] This concern is echoed by Kenneth Rogoff, who writes that if a central bank were to issue a cryptocurrency of its own, "the potential impact on the financial system could be quite dramatic, significantly impinging on private banks' ability to engage in liquidity transformation."[64] Victoria Cleland, the cashier of the Bank of England, worries that central bank digital money could cause a "reduction in deposit funding available to commercial banks, undermining their ability to provide credit to consumers."[65]

History shows that the private sector can adapt to direct competition from central banks and other government monies. Postal banks, for instance, provided private banks with competition but were never capable of driving them into the ground. For central banks that are exploring the idea of issuing publicly-available digital money, historical examples of postal banking deserve more study. The history of English banking is another good example. Given the choice between keeping accounts at the safe Western branch of the Bank of England or a risky private bank, individuals did not collectively flock to the former. No doubt this was partly due to the two things: 1) the Bank of England's policy of charging for servicing unprofitable accounts; and 2) of not paying interest on deposits. Its private competitors, on the other hand, did pay interest. In essence, private banks had to retain customers by offering better services.

A further example of public-private competition in the provision of money, specifically in the business of banknotes, comes from Canada. Through the latter half of the 19th century and the early 20th century, government-issued Dominion notes circulated concurrently with banknotes issued by the Royal Bank of Canada, Bank of Montreal, and other private banks. Despite the superior safety of Dominion notes, privately-issued banknotes were able to hold their own against government equivalents. Private banknotes have long since ceased to circulate in Canada, but this isn't because they were competed out of existence; rather, private bankers faced legislation that reduced their ability to issue notes, beginning in 1870 when the government required banks to surrender the issuance of $1s and $2s, and next in 1880 when they were limited to only issuing notes in denominations of $5 or more, in multiples of five.[66] Banks lost all ability to print notes when the Bank of Canada, the nation's

[62] A 'Small Revolution' in Ecuador? (2015).
[63] Sams, 2015, Which Fedcoin?
[64] Rogoff, Curse of Cash, 2016
[65] Cleland, 2016.
[66] The reason for banishing banks from the issue of small notes goes all the way back to Adam Smith, who in the Wealth of Nations favored banning notes in denominations below £5. Small denominations were typically used by poorer classes whose ability to monitor notes for credit quality might be less than adequate.

central bank, opened for business in 1935.[67] If Canadian monetary history is any guide, it is possible for private banks to compete effectively with central bank-issued substitutes.

B. A world without cash

Having explored the limited private issuance paradigm as a potential landing point for a government issued cryptocoin, the second paradigm that will be visited is the cashless one. This scenario involves the government withdrawing from the business of providing cash to the public. The central bank becomes either a pure bankers' bank, offering deposit accounts exclusively to member commercial banks, or it continues to serve the public by introducing some sort of digital alternative to replace cash.

This is a purely hypothetical scenario; no society has ever phased out banknotes and coin.[68] There are two chief motivations a central bank might have for abolishing cash. Crime and tax evasion are often conducted with cash, so in theory the abolition of banknotes and coin should dramatically increase the costs of these unwanted activities. The second reason is motivated by the necessity of freeing monetary policy from barriers imposed by the availability of banknotes. Each of these will be investigated separately.

1. The criminality case for the abolition of cash

Advocates of an abolition of cash tend to prefer a staged abolition, beginning with high-denomination notes like the US$100, 1000 Swiss franc note, and €500, and ending several decades from now with low denomination ones. The general idea is that cash provides low cost anonymity to criminals and tax evaders. By killing off large bills like the $100, lawbreakers will have to rely on smaller denominations, like $10s. If criminals are forced to conduct trade with a few suitcases filled with $20 bills rather than one suitcase filled with $100 bills, the costs of buying anonymity increase as do the odds of detection and apprehension. At the same time, legitimate users of cash—most of whom either use small denominations anyways—still get to enjoy the anonymity services provided by banknotes.

There are a number of high profile advocates of high-denomination note removal. Early in 2016 *The New York Times* took up the torch for eliminating high value bank notes[69], echoing Larry Summers' earlier call to kill the $100 in order to reduce crime.[70] Summers editorial was in turn a follow up to a thought piece from Peter Sands, former CEO of Standard Chartered PLC.[71] More specifically, Summers says that "removing existing notes is a step too far. But a moratorium on printing new high denomination notes would make the world a better place." Not long after, the European Central Bank announced that it would stop producing €500 notes starting in 2018. The most consistent advocate of abolishing cash has

---

[67] Koning (2013), "Strange Money: Privately Issued $6 and $7 notes"
[68] Sweden is unique in demonstrating a contraction in banknote usage. See Enlund (2016) for details.
[69] New York Times (2016). "Getting Rid of Big Currency Notes Could Help Fight Crime" [link]
[70] Summers (2016), "It's Time to Kill the $100" in the Washington Post
[71] Sands (2016) "Making it Harder for the Bad Guys: The Case for Eliminating High Denomination Notes" [Link]

been Harvard's Kenneth Rogoff, who has been calling for abolition for over two decades and recently published a book on the topic, The Curse of Cash.

It is worth exploring the Rogoff plan more closely. Rogoff describes his immediate goal as a "less cash" society and his long-term goal as a "cashless" society.[72] He calls for an immediate withdrawal of large value notes, with notes in denominations below $20 staying in circulation for several decades. The reason for keeping small notes is that society requires some quantity of banknotes in order to mitigate concerns over the lack of privacy afforded by non-cash as well as for use during emergencies such as power outages. Low income households in particular, which are disproportionately unbanked, require cash in order to function. In the long run, Rogoff wants to convert the remaining small note denominations—in the case of the U.S. $1, $2s, $5s, and $10s—into heavy coins. These coins would make criminal usage of cash even more burdensome while offering non-criminals a tangible, albeit inconvenient, form of transactions media.

To further help out the unbanked, Rogoff's suggests providing free debit accounts to low-income households as well as free smartphones if necessary in order to make electronic currency a viable option for everyone. He proposes two ways to offer these accounts: require private banks to offer them, either at the bank's expense or via subsidies, or have the government do the job. Of the two he prefers the latter, specifically a government provider of subsidized debit cards, "designed to catch those people that the private sector will not service, even with subsidies."[73] These debit accounts might even have the property of providing anonymity, says Rogoff, thus compensating for the loss of banknotes. To make this guarantee of privacy credible, Rogoff would implement significant restrictions on the degree to which government can access and monitor payments data. This privilege of anonymity would only be extended to small individual accounts below a certain ceiling, thus limiting the use of anonymous currency in larger criminal transactions.[74]

Rogoff's free debit account scheme sets the stage for something like the introduction of postal banking, or even government-issued mobile money or a Fedcoin-style system. Interestingly, Rogoff proceeds to entertain the idea of "Bencoin," his chosen name for Fedcoin, named after Benjamin Franklin, in the last chapter of his book. Rogoff's Bencoin involves the government copying some of the technologies introduced by Bitcoin to create a superior clearing mechanism. He goes on to say:

> "For the moment, there are just too many uncertainties, but over a long enough time frame, it is not hard to imagining that this kind of idea, or perhaps a later generation approach to digital currencies, will make the case for a digital government currency compelling."[75]

2. Deconstructing the zero lower bound

The second motivation for abolishing currency is to allow central banks to set negative interest rates. When a sharp recession hits, central banks typically lean into the wind by

[72] "The Curse of Paper Currency: An Interview with Kenneth Rogoff" (2016), Princetion University Press [Link]
[73] Rogoff, Curse of Cash, pg 100
[74] Ibid, pg 102
[75] Ibid

reducing interest rates. If the policy rate is already near 0% and a recession hits, the central bank must soften the blow by pushing interest rates into negative territory. Arbitrage dictates that as central bank deposit rates are guided below zero, all other short term interest rates will follow along, including rates on government t-bills and insured bank deposits. However, one asset interferes with this adjustment: cash. Cash carries an implicit yield of 0%. If deposits are being penalized at a rate of 0.25% per year, there are significant incentives for everyone to convert these assets into zero-yielding paper equivalents in order to avoid the 0.25% penalty. Not only will commercial banks all convert their deposits at the central bank to cash, but the public will clear out their bank accounts in order to hold paper. The upshot is that a central banker can't pursue a monetary policy that involves the reduction of interest rates below 0% lest the entire country turn into a 100% cash economy. This line in the sand is referred to the zero lower bound (ZLB) by economists.

In practice, the lower bound to interest rates lies a little bit below zero due to storage costs of cash.[76] Since cash is bulky and easy to steal, individuals must rent vault space and buy insurance. Since this cost isn't trivial, the public will be willing to hold deposits even if their nominal yield has fallen to -0.75% or so.[77] While this offers central bankers some extra leeway to reduce nominal rates below 0%, economic rules of thumb including the Taylor rule specified that during the 2008 credit crisis, a short term policy interest rate of -6% was required.

According to Marvin Goodfriend, the most straightforward way to remove the lower bound to interest rates is abolish paper currency. He goes on to list some problems to this approach:

> However, the public would be deprived of the widely-used bundle of services that paper currency uniquely provides—a generally accepted paper medium of exchange providing transactions services especially for low-value transactions; a readily accessible, safe liability of the central bank; a store of value; a degree of privacy in financial management; and the option to hold money outside the banking system and to withdraw deposits at par as paper currency in times of financial stress. Hence, the public is likely to resist the abolition of paper currency until mobile access to bank deposits becomes cheaper and more easily available, ATM charges for access to paper currency become excessive, and/or electronic currency substitutes become widely available.[78]

Goodfriend proposes an alternative solution. Rather than abolishing cash, the central bank need only cease its policy of pegging the price of deposits and cash at 1:1. It can either float this rate, as suggested by Goodfriend, or set a managed peg, as Miles Kimball and Ruchir Agarwal have proposed.[79] Either way, cash is expected to fall in value over time relative to deposit money. This imposition of a capital loss on cash owners cancels out the pecuniary advantages of holding zero-percent yielding banknotes when nominal rates are deeply negative.

---

[76] Commodities like gold have an effective lower bound as well. See for instance Koning (2012).
[77] We know that the -0.75% does not constitute the effective lower bound because both Switzerland and Denmark have reduced their central bank policy rates to this level without facing a rush into cash.
[78] Goodfriend (2016). "The Case for Unencumbering Interest Rate Policy at the Zero Bound"
[79] Agarwal and Kimball (2015) ."Breaking Through the Zero Lower Bound"

Having paper money trade at a different rate to electronic money would be inconvenient. Goodfriend's next solution is to remove cash entirely and replace it with central bank electronic money. He suggests that a central bank issue currency cards, much like gift cards, that are linked to accounts kept at the central bank. Currency cards would provide all the services that paper currency currently provides: anonymity, divisibility, generalized purchasing power, portability, safety, and a store of value. However, because these cards access funds held at the central bank, the central bank is free to impose a negative interest rate on those funds.

To prevent these accounts from being too popular relative to cash (and presumably hurting traditional banks) Goodfriend suggests some combination of a per-account ceilings, fixed costs of opening each account, and below market interest. Currency card accounts could be accessed through depository institutions as 100 percent reserve-backed pass through accounts at the central bank. This is of course just one way to implement a government non-tangible currency. It would be possible to substitute Goodfriend's currency card with a Fedcoin solution. Miles Kimball, a scholar who has been actively studying ways to skirt the lower bound, has advocated the idea of Fedcoin: "Governments should be creating their own version of Bitcoin. They should be ashamed they haven't."[80]

[80] Kimball (2013).

III. Further design questions about a potential Fedcoin

The first part of this paper described how to create a safe central bank-issued cryptocoin that allows the central bank to fix the price of cryptocoins to banknotes while preserving an independent monetary policy. The second section explored the larger concept of central bank non-tangible money, one form of which might be Fedcoin. This section refocuses back on Fedcoin and explores some of its potential design elements in more detail.

What distribution model should be adopted?

As explained in the first section, there are two methods for setting the supply of Fedcoin. A Fedcoin-issuing central bank can either have the ability to create and destroy Fedcoin, or the entire supply can be preallocated; the central bank would use this reserve to meet public demand while buying Fedcoin back when the public is oversupplied. The supply of Fedcoin in circulation grows as people bring existing banknotes to the central bank for new Fedcoins. A supply contraction begins when the public decides that it wants fewer Fedcoin and brings the coins to the central bank for conversion to an equivalent quantity of notes. The central bank, in turn, would destroy the Fedcoins or keep them in reserve for future issuance.

How can the public get its hands on Fedcoin? The easiest option would be for the central bank to set up an internet portal that allows individuals to buy Fedcoins directly from the central bank, either funding purchases with a bank transfer, or some other means.[81] As for banknote-to-Fedcoin transactions, the presence of a tangible medium, cash, means that a physical location is necessary to carry out this exchange. Central banks have offices where these sorts of exchanges could occur. The Federal Reserve, for instance, has twenty-four branches located across the U.S. While these branches might be repurposed to provide Fedcoin-in and cash-out services, this network would be too limited to provide a fully-inclusive financial product.

Central banks surely do not want to spend the time and effort building branches across the nation, which means they would probably want to partner with existing businesses that already have extensive physical networks. One potential partner would be commercial banks. Central banks have already built a partnership with the private banking system in order to provide the public with banknotes and coins. When an individual or business needs cash, they must visit a bank and convert deposits into underlying paper money. Banks, in turn, get this cash from the central bank by converting balances, which are held at the central bank, into currency. It might make sense to simply extend the model to include Fedcoin, or, in a Rogoff-style abolition of cash, have Fedcoin substitute for cash in the current private/public cash distribution model. If cash is to be kept in circulation along with a public digital money product, then banks would offer customers the option of depositing Fedcoin or cash in return for deposits and cashing out in either central bank product. It is conceivable that a bank would offer customers the ability to convert deposits into Fedcoin and vice versa, directly from the bank's website, without the necessity of visiting a branch.

---

[81] To see how this would affect the monetary base, consider that as individuals transfer funds to the internet portal to buy Fedcoin, the underlying settlement of these transfers requires that private banks transfer central bank settlement balances, or reserves, back to the central bank, which proceeds to cancel these balances. So on a balance, the monetary base stays constant since each increase in Fedcoin outstanding is matched by a decline in central bank reserves outstanding.

The post office would be an alternative or complimentary partner to banks. The advantage of the postal system as a distribution network is that it tends to be better represented in poorer neighbourhoods than banks. USPS seems open to the idea of distributing cryptocoin to Americans; it recently published a study that, among other things, suggested a USPS-branded cryptocoin called Postcoin that would be backed with a full reserve and offer a fixed exchange rate to paper currency.[82] If it became a distributor of Fedcoin rather than Postcoin, the USPS would not have to worry about maintaining a reserve and setting a peg as that would be the Federal Reserve's job.

The trade-offs between permissioned and permissionless blockchains

A blockchain is a way to coordinate activity without having to trust one central party. Thus, Bitcoin is often referred to as a *permissionless blockchain*. Anyone who wants to validate bitcoin transactions is welcome to do so and will be rewarded with bitcoin if they are successful in adding blocks to the chain. The network is said to be trustworthy because cryptographically-secured methods are used to append new information to the chain, and tampering is believed to be economically costly. However, this method of building trust comes at a cost: the mining process is relatively slow and energy intensive, requiring new bitcoin to be minted as a reward.

Permissionless blockchains were designed with the goal of enabling participants to transact without needing to link their real legal identities to accounts or transactions. On the other hand, *permissioned* blockchains have been designed to fulfill requirements such as the need to comply with regulations and allow for faster payments, transaction throughput and settlement speed.[83] Speed is important because a potential Fedcoin network needs to be capable of processing an incredibly large number of transactions each day. For example, the U.K.'s Faster Payment, a system for clearing and settling small value retail payments, processed 1.2 billion payments in 2015 (3.3 million per day) with over £1 trillion being transferred. Rather than allowing anyone to become a validating node, a permissioned blockchain vets nodes prior to granting them authority to update the ledger. Because all nodes are known and bound by legally binding contracts, the "mining" method of maintaining a blockchain is no longer necessary, thus reducing the costs of chain maintenance and paving the way for throughput speeds that are several orders of magnitude larger than what Bitcoin or Ethereum can offer today. [84]

The second advantage of vetting nodes and binding them to legal contracts is that permissioned chains allow for settlement finality; once a transaction is completed, there is

---

[82] Blockchain Technology: Possibilities for the U.S. Postal Service, Office of Inspector General United States Postal Service

[83] Swanson (2015) "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems"

[84] Meiklejohn and Danezis (2015) propose a permissioned central bank cryptocoin protocol called describe RSCoin which delegates authority for validating transactions to a number of other institutions, or mintettes. "Since mintettes are — unlike traditional cryptocurrency miners— known and may ultimately be held accountable for any misbehavior, RSCoin supports a simple and fast mechanism for double-spending detection," say Meiklejohn and Danezis. To solve for Bitcoin's lack of a monetary policy and volatile exchange rates, Meiklejohn and Danezis decouple the maintenance of the RScoin ledger, carried out by mintettes, from control over the money supply, which is outsourced to a central bank.

no way that the system can ever revert that transaction.[85] Bitcoin's settlement finality is much less certain. By assigning the task of updating the blockchain to anonymous nodes, a permissionless network, like Bitcoin, opens itself up to the possibility that a previously completed transaction can be undone, say by a 51% attack, whereby a miner gains enough control to alter and reorganize older blocks. Instead, bitcoin users must become comfortable with probabilistic finality, not absolute finality.[86] However, finality isn't attained without a tradeoff; permissioned blockchains sacrifice a degree of censorship resistance in order to achieve better finality. After all, if the real identities of the nodes are public knowledge, governments and other powerful actors can compel those nodes to censor transactions.[87]

While permissioned blockchains provide superior speed, oversight and finality, permissionless blockchains are better at recreating some of the unique qualities of coins and banknotes, particularly with their ability to provide anonymity and censorship resistance (these functions were discussed on p. 8). A central bank that wants to implement Fedcoin will have to evaluate each technology subject with whatever design goals it is trying to maximize.

How much interest to pay?

One of the economic advantages of Fedcoin is that it allows society to finally fulfill the goal of Milton Friedman's *optimum quantity of money*.[88] The idea here is that because it yields nothing, cash imposes significant "shoe leather" inefficiencies on society; people who are paid in cash must constantly walk to their bank to deposit the money for equivalent interest yielding deposits. If cash can be designed to pay interest, unproductive shoe leather costs can be avoided and society is made a little bit more efficient.

Modern central banks almost always pay interest to banks that hold central bank deposits overnight. This is referred to as the central bank's deposit rate, or the interest rate on reserves. To what degree should central banks provide the same level of compensation to private individuals who hold Fedcoin? The setting of the public deposit rate is important because whatever rate the government offers will in turn dictate the rate that banks can set on their customers' demand deposits. Should the central bank's rate be too high, depositors will redeem their deposits for Fedcoin. Banks in turn will be forced to jack up their own rates in order to attract deposits at the expense of their margins.

Historical examples of government-issued, non-tangible money may shed some light on the matter. The Bank of England paid no interest on deposits to the public; in fact, on unprofitable accounts it even charged a service fee, effectively setting negative interest rates on certain depositors. Sub-market rates were also a feature of the U.S. market for publicly-created money. When it was founded in 1911, the United States Postal Savings System was

[85] See Sams (2015) and Swanson (2016).
[86] See Buterin (2016); Also, see Bitfury (2015)
[87] See Sams (2015)
[88] Friedman (1969)

allowed to pay only 2% a year, below the approximately 3.5% that private banks were offering.[89] That 2% rate prevailed until 1934 when it was raised to 2.5%.[90]

The ability of government money providers to provide competitive, potentially superior rates is illustrated by Britain's Girobank, which was the first to pay interest on chequing accounts, thus forcing private banks to pay interest. According to Kuwayama, the Japanese postal savings system paid higher rates than banks on demand deposits, which may have given it an advantage over banks in attracting deposits for payments purposes.

On the other side of the equation, the ability to charge negative interest rates on Fedcoin balances is one of the key design features advocated by proponents of a cashless economy. When a central bank reduces rates below zero, by how much should this be passed on to Fedcoin owners? Rogoff suggests that the first $1000 or so deposited in government-subsidized or provided debit accounts be protected. If we relate this to a Fedcoin scheme, it is possible that a certain portion of each individual's Fedcoin holdings would also be excluded from negative rates, with everything above the ceiling facing the full penalty. However, if anonymity in the account opening process is permitted, it is possible to get around this ceiling by opening multiple accounts and splitting their holdings.

To what degree should Fedcoin offer anonymity and censorship resistance?

Because the blockchain reveals the number of bitcoins in each address, the Bitcoin protocol does not provide users with full anonymity. At best, it provides pseudonymity as the addresses themselves are not associated with the real persons of their owners. However, a number of bitcoin-inspired cryptocurrencies such as Dash, Monero and Zcash have modified their protocols in a way that reduces the traceability of transactions. The privacy this affords users is supplmented with price risk caused by cryptocoins' high volatility.

Bitcoin is also censorship-resistant. This means that any individual who wants to transfer bitcoin as payment cannot be prevented from doing so by the Bitcoin protocol.[91] This is different because most types of electronic money are not censorship-resistant; a bank must grant permission before a bank account can be opened or deposits moved from one account to another, giving rise to the possibility of being censored.

Banknotes and coin are unique in embedding both anonymity and censorship-resistance in a stable-valued medium. While this has its drawbacks, (fixed-price anonymity and censorship-resistance provide criminals a safe way to participate in a wide range of welfare reducing transactions) it also enables many worthwhile transactions that wouldn't otherwise be carried out with information-heavy payments media, such as debit or credit cards. Kahn, McAndrew, and Roberds argue that anonymity is particularly valuable in preventing situations in which one party may take advantage of the other by using

[89] Kuwayama, pg 8-9
[90] U.S. commercial banks didn't always have the interest rate advantage; in the 1930s and 40s bank deposits were paying well below the postal savings rate, leading to flight out of private deposits into postal deposits. This trend subsided in the 1950s.
[91] Garratt (2015) points out that this isn't necessarily the case. Miners might choose to exclude certain transactions from the blocks that they are processing. This happened in 2013 with Satoshi Dice transactions, an online gambling site.

transaction information. [92] The authors use identity theft as their example. Given that debit or credit cards provide information that might help a potential identity thief, cash is a useful form of protection that allows consumers to engage in transactions they would not otherwise feel safe making.

> In short, in an economy without theft and with a frictionless system of credit, money would be superfluous. When theft is present, it would be welfare-improving to introduce money into a world with frictionless credit, as money introduces the possibility of anonymous, theft-free transactions.[93]

If it is incumbent on society to find a "sweet spot," as Kenneth Rogoff refers to it,[94] so that there is enough anonymity-providing exchange media for regular consumers but not enough for criminals, then something similar to a fully anonymous and censorship-resistant Fedcoin may be part of the solution. If we were to suppose that society settles on Tobin's deposited currency accounts or Rogoff's vision of a world with low denomination banknotes, then introducing a Fedcoin that is anonymous and censorship-resistant could be complementary to the services provided by already-circulating cash. For those without smartphones, cash (perhaps in low denominations), would provide universal access to a fixed value privacy-preserving payments option. Those with smartphones could get those same services by using Fedcoin, likely at a cheaper rate, since the costs of operating the Fedcoin network would be far lower than printing and maintaining the banknote and coin circulation. At the same time, Fedcoin would improve on the range of transactions services that cash provides, namely by offering a fixed-price anonymous transaction option that doesn't require a face-to-face meeting.

If, on the other hand, a full cashless scenario is to be adopted, a substitute form of anonymity and censorship-resistance will be needed to reach the sweet spot described by Rogoff. Kocherlakota suggests that in a cashless world, private alternatives like Zcash, Monero and Dash might fit the bill.[95] However, if anonymity and censorship-resistance are, to some degree, an essential service, it may be detrimental to outsource their provisions to assets that act like penny stocks.[96] As for stablecoins, their record is too spotty. A fixed price government alternative like Fedcoin may be the best way to provide the very unique services provided by cash.

Any decision to find the so-called sweet spot by implementing a fully anonymous and censorship resistant Fedcoin has implications for the sort of blockchain design that best meets these goals. A Bitcoin-style permissionless blockchain is one way to achieve censorship resistance, while a protocol like Zcash can offer anonymity. If censorship resistance and anonymity are less important than speed and compliance, then a permissioned blockchain or even FedPesa (see later) might be the better ways to implement government digital money.

Should there be deposit limits and a rationed form of anonymity?

---

[92] Kahn, McAndrews, and Roberds (2004). "Money is Privacy"
[93] Note that by "money," the authors mean coins and banknotes.
[94] See here.
[95] Kocherlakota (2016), "The Zero Lower Bound and Anonymity: A Monetary Mystery Tour"
[96] Koning, 2016 "Kocherlakota on Cash"

To limit what is often viewed as unfair competition with private banks, government-issued money schemes have typically faced certain size limitations. In his currency card scheme, for instance, Goodfriend suggests that deposits be capped in order to impose friction on the ease of accessing electronic currency. British NS&I accounts have always faced quantity constraints, notes Gruen, although he advocates the removal of such constraints. In the U.S., the United States Postal Savings System was originally obligated to limit deposits to $500 to reduce competition with commercial banks, although this was increased to $1000 in 1916 and $2500 in 1918.[97] Likewise, it might make sense to limit individual Fedcoin balances.

The discussion of deposit limits is intimately intertwined with that of anonymity and censorship-resistance. For the sake of preserving the privacy of those operating in the legal economy, Rogoff has suggested that the cancellation of large denomination notes be accompanied by the continuing circulation of small bills and the creation of debit accounts, the latter possibly offering privacy up to a fixed nominal amount. These secured accounts should not only offer shielding from inquisitive spouses, parents, and friends, but also be secret from the government, "say up to a few hundred dollars."[98] Furthermore, Rogoff is open to the idea of designing a regulatory regime for cryptocurrencies that allows for relatively small anonymous transactions.[99]

Is it possible to embed Rogoff's idea of limited anonymity into Fedcoin? Limiting cash denominations to small sizes is an elegant way to throttle, or slowdown, the use of anonymous payments. An analogous method applied to Fedcoin might involve a protocol design that is capable of limiting balance sizes or throttling transactions over a certain size. There is an inherent contradiction here since the anonymity provided by the protocol may conflict with the ability to set account and transaction limits. A criminal that hits his or her account limits would simply recieve a different address, for instance, or split one large transaction into many small ones. Nevertheless, the technical challenge of designing a limited anonymity Fedcoin is certainly worth solving, as it checks a large number of boxes. 1) the population would get a safe form of fixed-price electronic money that is pegged to the existing unit of account 2) the central bank maintains an independent monetary policy with negative rates as a tool 3) cash, an old technology, is replaced (or complimented) by a cheaper and faster form of fixed-price payment that can be used over long distances 4) and society continues to enjoy a form of anonymous and censorship-resistance payments. The caveat of a form of anonymous and censorship-resistant payments is that the quantity provided is limited (so as to prevent socially-detrimental use by criminals).

Fedcoin and not FedPesa?

Why should a central bank-issued digital currency for public use be implemented with a blockchain instead of a more conventional relational database? Consider that this database could even be run in a distributed fashion; similar to how Netflix and Facebook store data in many locations at once, a terrorist attack or natural disaster could not disable the database, like a blockchain. David Birch has described this choice as one between a Fedcoin and FedPesa, or in Britain's case BritCoin and BritPesa, where the -pesa qualifier is a reference to Kenya's MPesa mobile money system, a battle-tested public payments network that does

[97] Kuwayama, pg 8
[98] Rogoff, pg 93
[99] Ibid, pg 214

not use a blockchain.[100] Ecuador's Dineiro Electronico is perhaps a better example of government provided bank accounts, since unlike Mpesa, it is government owned.

It is undisputed that a permissionless blockchain is an expensive way to run a payments network. Mining is slow and the significant outlays of time and energy must be paid for with new coin issuance. A permissioned blockchain speeds things by placing a degree of trust in the nodes that have been selected to maintain the ledger. However, if it is possible to trust just a few known nodes, why not take the next step and trust just one node, the central bank, to be a good steward of a non-tangible money scheme? This is the FedPesa option. With only one node, resource-consuming processes for reaching consensus are no longer necessary and more transactions can be processed.

However, if it is desirable for a central bank digital currency to be designed in a way that replicates the anonymity and censorship-resistance of cash in the best way possible, if only for small transactions, then FedPesa runs into credibility problem. This is captured quite well by Rogoff:

> "In theory, a government could itself offer debit accounts that were guaranteed to be private. Unfortunately, that promise would not be worth the paper it was written on, so to speak. Given governments' past behaviour, who could take such a promise seriously?"[101]

Take, for instance, the example of Ecuador. To open a Dineiro Electronico account, the Central Bank of Ecuador requires users to submit their national identity numbers. It might be possible, as Birch suggests, to forgo identification requirements. But since the central bank is to be tasked with maintaining the FedPesa database, it would be able to see the amounts held in each account and trace activity back to the phones or computers that initiated them. This means that FedPesa would be pseudonymous (at best) rather than anonymous.[102] It is also difficult to see how the second feature of cash, censorship-resistance, can be recreated by FedPesa since the central bank would have the technical means to close accounts and halt transactions. It might be possible to set up a system of checks and balances that limits the ability of the central bank to scan the FedPesa database for information, perhaps by establishing a privacy watchdog, or some other system of oversight. However, this imposes an extra set of challenges and associated costs.

In sum, the more cashlike a government digital currency is to be, the stronger are the arguments for implementing a blockchain solution. On the other hand, if the attributes of low denomination cash are not deemed worth replicating, a potential government-issued electronic currency might be best implemented as centralized FedPesa solution.

Why not Chaumian cash?

---

[100] Birch (2016) "Britcoin or Brit-PESA?"
[101] Rogoff, pg 102
[102] This is very similar to Bitcoin. Utilities such as Chainalysis and Blockseer have produced software that can trace and monitor bitcoin transactions, providing anyone with concerns over the provenance of bitcoin with a useful tool for picking the good from the dirty.

If anonymity is a design goal that the architects of government digital money wish to pursue, a better alternative to Fedcoin might be some version of Chaumian eCash. In the 1990s, David Chaum patented an anonymous payment technology that could be used with the existing banking system. A client of a bank must first convert funds in a regular bank account into eCash. The client goes to the bank and asks the bank manager to debit his or her account and then signs a numbered digital coin for, say, $10. Thanks to a novel approach called blind signatures, the bank knows neither the serial number that the client has chosen nor can they match her identity with the coin. This allows the client to enjoy anonymity. When the client spends this $10, the merchant who is proffered the coin immediately notifies the bank of the coin's serial number. From there, the bank checks a list of used digital coins to ensure that the coin in question had not already been spent. This cross-checking process solves the double spending problem.

Like eCash, Fedcoin would provide a fixed-price anonymous payment medium for public consumption. Given its reliance on a single node to issue and verify notes, eCash would probably operate faster than a distributed blockchain.[103] A drawback of eCash is that it does not replicate the universal reusability of cash. Bitcoin, Fedcoin and cash do not require the creation of accounts or installation of special hardware, so anyone can accept these media in payment and on-spend them. A banknote, bitcoin or Fedcoin is potentially capable of partaking in millions of transactions. eCash is only capable of being used by consumers with existing bank accounts and accepted by merchants with bank-provided eCash accounts and hardware. Rather than spending received eCash, merchants must return the coins to the bank for cancellation.

What about settlement finality?

Settlement finality is a property of a payments system that guarantees that once a transaction is complete, a subsequent event, such as the insolvency of the payor, cannot result in the reversal of the transaction. Finality is important because it removes settlement risk, freeing up counterparties to focus on minimizing more relevant business risks. Central banks are important providers of settlement finality to the private sector through large value clearing and settlement systems, say Fedwire in the U.S., Target2 in Europe, or CHAPS in the U.K. Payments Canada, for instance, ensures finality by requiring all member banks to submit collateral to the system. Over the course of the day, members will incur debts and credits to each other. Payments Canada guarantees that any bank that becomes a creditor has effectively received an irrevocable and final payment in real-time, even though the actual settlement of debts and credits does not occur till the end of the day. A member bank knows this guarantee of real-time finality is credible because if one of the Payments Canada members becomes insolvent over the course of the day, the collateral of that member will be seized in order to force end of day settlement. Should that collateral be insufficient, all surviving member banks have already provided permission that their collateral can be used in order to make the system whole. In the event that this is insufficient, the Bank of Canada itself will guarantee the system settles, presumably by having the Canadian tax payer step up to the plate.

As mentioned on page 21, permissionless blockchains cannot provide settlement finality because there is no guarantee that blockchain users won't be left out of pocket by malicious

[103] Sharding is one proposed method to increase transactional capacity of blockchains. See here.

block reorganizations. Rather, users of permissionless blockchains must be content with probabilistic finality. If central banks wish to offer settlement finality to the public, then something similar to a fully-centralized FedPesa or a permissioned blockchain would be the best implementation. In the case of FedPesa, citizens holding FedPesa accounts would be directly transferring central bank book entries among each other; in the case of a permissioned blockchain, nodes would be held legally accountable for any block reorganization attempt.

However, it is possible that a central bank may be content with designing a public digital currency that offers only probabilistic finality. This would not be without some precedent, since existing publicly-available money products (coin and banknotes) do not offer 100% finality. Under a 'banknote protocol,' possession of a *100% genuine* banknote in the buyer's hand provides a potential seller with enough information to be sure that, should they engage in trade, they will be getting full and irrevocable value in return.[104] Settlement risk is introduced because because the determination of the genuineness of a banknote is difficult if counterfeit banknotes can be created.

The ultimate arbiter of whether a banknote is genuine or not is the central bank. After receiving cash over the course of the day from customers, retailers deposit the proceeds with their bank in the evening and banks credit their accounts. Banks, in turn, ship these notes to the central bank, which scans each note to determine whether it is legitimate prior to crediting the bank's account for the amount. A bank that is caught depositing counterfeit notes will not have their accounts at the central bank credited, nor will the central bank provide them with any form of compensation. The bank now finds itself out of hand. The prior trade it had engaged in (the exchange of the retailer's banknotes for bank deposits) was fictitious. The counterfeiting of banknotes in a banknote protocol is thus analogous to the double spending of bitcoins in the Bitcoin protocol; both activities reduce the ability of the respective protocols to provide finality. Instead, bitcoin and banknote users must accept probabilistic settlement.

The ability to unwind the chain of transactions in which a counterfeit note has participated is limited to the last completed transaction in which said note has participated. While a bank caught depositing counterfeit notes at the central bank no longer gets full value out of the prior transaction with the retailer, the bank cannot turn around and make a claim on the retailer for reimbursement. To reduce the risk of being the dupe, the entire chain of transactors (from customer to retailer to bank) partners with the central bank in the process of arbitrating the legitimacy of banknotes. Arbitration may be as low-tech as flicking a bill through one's fingers to make sure it feels right, or as sophisticated as running it through a machine.[105] But even in the role of junior arbiter, there is always some risk that a trade involving cash is not for full and irrevocable value. After all, it is impossible to fully replicate the note detection capabilities of a central bank.

Authoritative record of ownership

[104] Banknotes and coins are unique in being exempt from the principle governing property, *nemo dat quod non habet*. See footnote 99.

[105] In a sense, we can think of a banknote protocol's distributed arbitration mechanism as being akin to bitcoin's distributed mining process.

Permissionless blockchains may include blocks generated by a thief (malicious miner) who has removed legitimate transactional history with different entries. In other words, the blockchain may not represent the "right" distribution of resources. Nor does a permissionless blockchain provide a method for systematically correcting or rolling back theft. Because the law will not recognize a record that enshrines fraudulent property transactions, a permissionless blockchain can never be legally authoritative.

However, the law treats money differently from all other property. Because the legal authorities allow a string of transactions consummated with counterfeit banknotes to stay intact (except for the last transaction), a banknote protocol allows for some degree of fraud to stay "written into the system." Stolen banknotes are treated in a similar way to counterfeits. When a stolen note is spent, the law does not require any of the recipients involved in the ensuing chain of transactions to be held liable for returning said note to its original owner.[106] In practice, this means that if a note residing in a retailer's cash register is proven to be stolen, but the retailer received it innocently from the crook, the retailer has no obligation to compensate the victim by unwinding the transaction involving the stolen note.[107]

Because the law already accommodates the banknote protocol by allowing any distribution of resources attained by a chain of fraudulent transactions to stay intact, the law could grant this same recognition to a permissionless Fedcoin protocol. The Fedcoin blockchain could thus be filled with theft and counterfeiting while still being legally authoritative.

Undoing Fedcoin when it goes wrong

If Fedcoin is a program initiated by government, but not controlled by it, what if things go wrong and the government wants to unwind the scheme? Can it initiate a controlled retreat, or is this out of its hands? An exit would work in the exact same way that a central bank pulls the plug on banknotes, by simply calling Fedcoins in to be redeemed for a new type of exchange medium. A central bank would start by setting a window of time over which users are to bring Fedcoin to banks or post offices for redemption for an equivalent quantity of banknotes or deposits. After the window has passed, the central banks will cease accepting Fedcoins as their liability and remove their status as legal tender. If there are any Fedcoin tokens still in existence, their price will begin to float against central bank banknotes, turning Fedcoin into something like a Monero or Zcash: a volatile-priced anonymity product.

In the case of a banknote cancellation, if there are any legacy banknotes still in use as a medium of exchange after the window has closed, then those notes will steadily degrade thanks to wear and tear. This will make counterfeiting much easier, eventually pushing the

---

[106] As long as they accept the note in good faith.

[107] We can imagine the problems that would be created if retailers were responsible for stolen banknotes. To protect themselves, they would have to check each banknote against a list of serial numbers of confirmed stolen notes. This would be a time-consuming and expensive process, throwing a wrench into the gears of trade. Instead, society as settled on the legal principle that cash cannot be followed, or an exemption from the principle of *nemo dat quod non habet*. The latter principle, which applies to property in general, stipulates that "no one can give away that which they do not have." Thanks to their exemption, cash payments from a crook to a series of innocent counterparties (except the last one in the case of counterfeiting) are recognized by the law as being final.

price of the stranded notes down to the point of irrelevance.[108] A central bank can even facilitate the process of driving the value of notes to zero by printing large quantities and spending them, much like how during times of war various parties have tried to sabotage their enemy's note issues by dropping in counterfeit notes.

In the case of Fedcoin, as long as validators continue to function, the integrity of the Fedcoin ledger will be maintained and an analogous wear and tear problem cannot arise. However, it is conceivable that competing products would start to steal market share, especially now that Fedcoin no longer offers price stability, driving the value of Fedcoin down to zero. If it wishes, the central bank could also sabotage the issue of legacy Fedcoin by creating an infinite supply and spending it until Fedcoin is valueless, or spending all of its preallocated Fedcoins. The upshot is that in most situations, the central bank can unwind Fedcoin.

Another potentially dangerous scenario is a Fedcoin hard fork. Say a large number of mining nodes agree to install a new version of the Fedcoin protocol while others choose to stay with the legacy protocol.[109] The Fedcoin blockchain would bifurcate so that there are now two chains. A good example of this is the 2016 hard fork of the Ethereum protocol, which resulted in a sizable minority of miners continuing to use the legacy protocol so that Ethereum effectively split into what are known as Ethereum Classic and Ethereum.[110] This could be particularly problematic in the case of Fedcoin because the digital money supply would effectively be doubled; all those who previously held $x worth of Fedcoin would now hold not only $x of legacy Fedcoins but also $x of the updated Fedcoins. A sudden surge in aggregate demand would emerge as Fedcoin users spend their excess Fedcoins in order to restore their desired holdings of money. To ensure that it hits it's inflation target, the central bank would have to expend significant resources to sterilize the effects of the hard fork, specifically open market sales, to mop up excess Fedcoins. However, if the central bank lacks enough assets to engage in its mop up attempt, it would have to depend on the taxpayer to provide funds.

To prevent the emergence of two versions of the Fedcoin blockchain (and the worst case scenario, of a taxpayer bailout) the central bank need only publicize that it will limit 1:1 Fedcoin-to-banknote conversion to those Fedcoins that reside on the central bank-recognized blockchain. Having been severed from the peg, the price of legacy Fedcoins will fall to zero. So, when the central bank needs to upgrade the protocol, it can nudge all the nodes towards that protocol by threatening inconvertibility of legacy Fedcoins into banknotes. Likewise, if malicious miners try to upgrade the Fedcoin protocol but the central bank wants everyone to stay on the legacy protocol, it can threaten owners of new Fedcoins with inconvertibility, thus preventing malicious hard forks from arising in the first place.

The bigger risk is to those who, in the event of a hard fork, might accept "legacy" coins which are essentially valueless. To reduce the potential confusion of hard forks, the private sector would have to develop techniques to ensure that they are always up to date. When central

[108] Something like this occurred with the Somali shilling, which continued to circulate long after the Somali central bank had disappeared. See White and Luther.
[109] We can imagine that the central bank initiates the hard fork but many nodes do not wish to go along with the protocol change, say for ideological reasons. Alternatively, a number of nodes initiate a hard fork that has not been approved by the central bank, say for monetary motives, while other nodes wish to stay with the central bank-approved protocol.
[110] For more on the Ethereum hard fork see here.

banks upgrade their banknotes and declare the old issue invalid, for instance, the private sector quickly adopts the change.

What if the legacy coin does not fall to zero when the central bank removes its promise to redeem it at a fixed rate? This is unlikely. Whenever a central bank has demonetized a given denomination of notes they have ceased to circulate, their value is dictated only by their attractiveness as a collectible. The case of the Swiss dinar is an interesting counterexample.[111] Even after Iraq's central bank demonetized its issue of Swiss-printed banknotes, they continued to circulate. Likewise, it is possible to imagine that Fedcoins on the unapproved and henceforth non-convertible blockchain might fall in value and then float, relative to the price of Fedcoins on the approved convertible blockchain.

If so, monetary exchange would become a much more complicated affair. Fedcoins would no longer be fungible. Merchants could no longer set prices in terms of the general Fedcoin unit of account, but would have to specify which one they are using: the central bank-approved unit or the renegade unit. Rather than accepting all Fedcoins at face value, merchants would be forced to screen Fedcoins to ensure they are getting full value. Cash registers would have to be reprogrammed with the ability to calculate the appropriate discount to apply to payments made with the unapproved chain or the premium to apply to payments made with the approved chain. Alternatively, retailers may simply not accept coins on the renegade chain at all.

While the immediate effects of a Fedcoin blockchain bifurcation would be disruptive, in the medium- to long-term the government would be able to guide the economy towards use of the approved Fedcoin as a unit of account and medium of exchange, say by insisting that taxes are paid in the approved unit and posting prices of government services in that same unit. It could also lever legal tender laws to limit the privilege of legal tender to those Fedcoins residing on the government-approved Fedcoin blockchain. The government could also require banks to only redeem deposits with approved Fedcoins, not unapproved ones. This would push the unapproved Fedcoin chain so far into the background that it ceases to cause monetary chaos.

Conclusion

Over the last year, the technology underpinning Bitcoin and the blockchain has inspired a number of central banks to pursue research on the topic of central bank digital currency. While Bitcoin shows some promise as a digital currency, its volatility makes it inaccessible to the majority of consumers. A central bank digital currency might rectify this problem by allowing consumers to own a safe form of fixed-price electronic money that, like cash (but unlike Bitcoin), is denominated in the existing unit of account. At the same time, unlike cash (and like Bitcoin) this digital currency would be capable of being used over long distances.

[111] An example of this occurred in Iraq in 1993 when Saddam Hussein cancelled Swiss-printed Iraqi dinar banknotes. Even after the conversion window closed, Swiss dinars continued to circulate in Kurdistan as their own currency, despite having been disavowed by the Iraqi central bank. See King (2014).

For monetary policy makers, the replacement of physical cash by digital cash means that the issuing central bank would be able to implement negative interest rates, a useful tool when a recession hits in an environment when nominal interest rates are already low or at the zero lower bound.

The effect that a central bank digital currency has on the existing banking system is a complicated question. As the history of economic ideas and systems shows, there is some precedent for a government-issued non-tangible currency for public consumption. For central bank researchers who are interested in central bank digital cash, episodes such as postal banking deserve more research to help determine the merits of the government entering into competition with the private sector for the provision of a publicly-available medium of exchange. These episodes tend to show that government competition does not cripple the private banking sector, although a more careful examination of the historical data is necessary in order to determine the magnitude of these effects.

There are many ways to implement government digital currency. If replicating the unique features of banknotes and coins is considered important, then something like Fedcoin deserves study. Fedcoin could provide cash-like levels of anonymity and censorship-resistance, perhaps with a built-in mechanism that limits usage to small value payments so as to reduce participation by criminals and tax dodgers.