Cryptocurrencies: Policy, economics and fairness*

Jon Danielsson
Systemic Risk Centre
London School of Economics

July 2019
Version 2.0

Abstract

Cryptocurrencies promise to replace fiat money with private money underpinned by algorithms, not government guarantees. While the technology is elegant, the success and failure of cryptocurrencies in the competition with fiat will not be determined by technology alone. It is more important to avoid serious economic and social consequences, and a cryptocurrency based monetary system would suffer from persistent price volatility and high systemic risk and would exasperate inequality.

JEL: G00, G01, E42

*Systemic Risk Centre Discussion Paper 86. I thank the Economic and Social Research Council (UK) [grants number ES/K002309/1 and ES/R009724/1] for support and Robert Macrae, Andreas Utheman and Jean-Pierre Zigrand for valuable comments. Updated versions of this paper can be downloaded from my website `www.riskresearch.org`.

1 Introduction

> "Money and religion have much in common. They both concern beliefs about eternity. The British put their faith in an infinite sequence: this pound note is a promise to pay the bearer on demand another pound note. Americans are more religious: on this dollar bill it says 'In God We Trust'. In case God defaults, it is countersigned by Larry Summers."
>
> John Moore's 2001 Claredon Lecture "Evil is the Root of All Money".

Are cryptocurrencies the future of money? The idea is to replace flawed publicly issued fiat money with private money underpinned by algorithms, not government guarantees. Cryptocurrencies are controversial. Advocates see them as better forms of money, providing freedom, useful economic functions, fabulous riches, and a hedge against bad government policies. The skeptics[1] reject these arguments, finding that cryptocurrencies lack economic rationale and hence are unable to deliver on their promises. While the technology is elegant, it will not alone determine the success and failure of cryptocurrencies in competition with fiat, and serious economic and social questions need to be addressed if cryptocurrencies are to play a significant role in society.

The central feature of money is trust. Most money in use today is fiat money, created by central banks which promise to keep the value of money stable. The most widely used currency in the world, the US dollar, is issued by the central bank of the United States, the Federal Reserve. For the US dollar to have value, we have to trust the government of the United States.

The record of central banks is checkered. They manipulate the supply of money for political purposes and find it hard to meet their target inflation rates. Some create hyperinflation like Venezuela and Zimbabwe, others peg the currency, only to let it sharply appreciate like Switzerland did in 2015. Quantitative easing taxes savers and subsidizes borrowers, as well as destabilizing financial markets. The central banks control the payment system and are not shy in using that power for political purposes.

If the central banks are political or incompetent, an algorithm might do better, if designed not to be political, incompetent, or corrupt. Cryptocurrency algorithms are transparent, so we will know what the supply of money will be in the future. Algorithms beyond anybody's control provide trust.

[1] Including Daníelsson (2018) and BIS (2018). Recent testimony to the US Senate by Roubini (2018) and Valkenburgh (2018) gives a useful expression of both positions.

Pure cryptocurrencies, such as the largest, Bitcoin, are created by private entities, but not controlled by them. Hybrids sit between fiat money and Bitcoin. Some are fiat money in new forms, such as Facebook's Libra and JP Morgan's JPM Coin, where corporations provide trust. Others, like the various stable coins underpinned by mining, promise one–to–one convertibility to fiat money, either with algorithms or full reserves.

Cryptocurrencies have the advantage when it comes to technology. Fiat money dates back at least 800 years, and complicated infrastructure of accounts has emerged to support transactions. To move money around, we have to deduct money from one account and deposit it in another, often several times. This infrastructure is complex, slow, error-prone, prone to abuse and hence heavily regulated, all of which gives insiders ample scope for rent seeking and abuse.

It is different with cryptocurrencies. They exist as tokens on a blockchain, where transactions involve an exchange of tokens, no accounts involved. A financial system based on token money should, in theory, be much more efficient than the fiat system of today. It is the threat of alternative payment systems, beyond the control of government authorities, that has forced central banks to respond with their own central bank digital currencies, CBDCs.

When the monetary system works well, we take it for granted. Payments made efficiently and securely, money stored with predictable value and the worst of crises mitigated. When things go wrong, the consequences are catastrophic: social disruption, deflation or hyperinflation, and systemic financial crises.

However compelling the trust and technological arguments in favor of cryptocurrencies, they are not sufficient. Money is the most fundamental part of the economic system, and the risk of getting it wrong when the monetary system is changed is serious. The criteria for crypto success are consequently much higher than for other technical innovations, and cryptocurrencies will need to deliver on their promises without creating new economic and financial stability risks.

The danger and benefit of a cryptocurrency financial system depend on what form it will take. In the simplest form, tokenized fiat money promises to improve the efficiency of the payment system while keeping central banks as the guardians of price and financial stability. The main disruption will happen if we go beyond that, displacing central bank managed fiat money with algorithm controlled cryptocurrencies, like Bitcoin.

No monetary system can guarantee price or financial stability — not fiat,

not gold, and not crypto. The advantage of fiat money is that it comes with a safety valve, the central banks can adjust the supply of money to best suit the economy, but only at a cost, as it is easy to abuse such a system. A gold or a cryptocurrency system with a fixed mining schedule like Bitcoin prevents the worst abuse but likely leads to price volatility and social strife, because it lacks adjustment mechanisms.

Systemic risk would be higher under a crypto monetary system than a well-managed fiat system because money wouldn't merely remain as tokens on a blockchain. Higher forms of money like crypto M1, M2, and traded IOUs will emerge. These will be claims on coins, and in times of crises, when confidence evaporates, that by itself leads to panic. We will doubt the solvency of the crypto banks and other institutions in the crypto ecosystem, and become alarmed by the absence of a financial authority able to provide liquidity assistance.

That by itself is a good reason for keeping the fiat system. But besides, a monetary system based on privately issued cryptocurrencies would be fundamentally unfair. The current market value of all cryptocurrencies is around $310 billion. The total value of M1 money in the G20 economies is $31 trillion. If we fully replace fiat money with cryptocurrencies, up to a $31 trillion profit will be transferred to a handful of crypto speculators, unacceptable to society and prevented by governments.

2 Types of money

We have used many assets as money, including silver, copper, seashells, and cigarettes. Graeber (2011) argues that before money, the exchange of goods took place via bilateral debt contracts and that money only became widespread when coinage was invented simultaneously in China, India, and Lydia around 600-500 BCE.

2.1 Old school money

The monetary system cryptocurrencies most resemble is the *gold standard*, the longest period of monetary stability the world has ever seen, see Schenk (2013). The stability of the gold standard was underpinned by the amount of gold in the world being fixed, and increasingly costly to mine so that the supply of gold was limited and hence the quantity of money. Of course, it isn't quite that simple as Karaman et al. (2018) show, even under the gold

standard there was plenty of room for manipulation of the currency.

The monetary system in almost every country in the world today is based on *fiat* money, from the Latin "let it be done", where the central bank creates money out of nothing, and the government guarantees the money retains value. Fiat money, in its base form, is historically created by printing, but nowadays refers to the central bank arbitrarily increasing the balance in commercial banks' accounts held at the central bank. It does not have to transfer money in or out. It just changes the numbers on the account.

Scrip money is privately issued, perhaps by companies in lieu of salaries to force employees to spend their income in company-owned stores. Other forms include vouchers, gift cards, IOUs and the like. Scrip money is sometimes valued with reference to fiat, but not necessarily, it can merely function as an alternative money.

E-money is denominated in fiat, but is kept in custodian accounts that provide transactions between electronic wallets on handheld devices, like AliPay, Bitt.com, M-Pesa, PayTM, and WePay.

2.2 Cryptocurrencies

Cryptocurrencies, first proposed by Nakamoto (2009) in his Bitcoin, are envisioned as a 21st century replacement for fiat money. It is not straightforward to define cryptocurrencies, as they have very different characteristics, but they generally have three distinguishing characteristics.

The first is that units of money are called a coin even though they have no physical representation. The second is that we keep track of coins on a blockchain, not as numbers in an account, where the blockchain can be permissionless, or permissioned.[2] The main difference between cryptocurrencies and base fiat money is how new money is created. With fiat, it is physical printing or arbitrary increases in reserve balances at the central bank, where the central bank owns the newly created money (technically, it is a debt obligation of the central banks). With cryptocurrencies, an algorithm generates new coins that are owned by private entities.

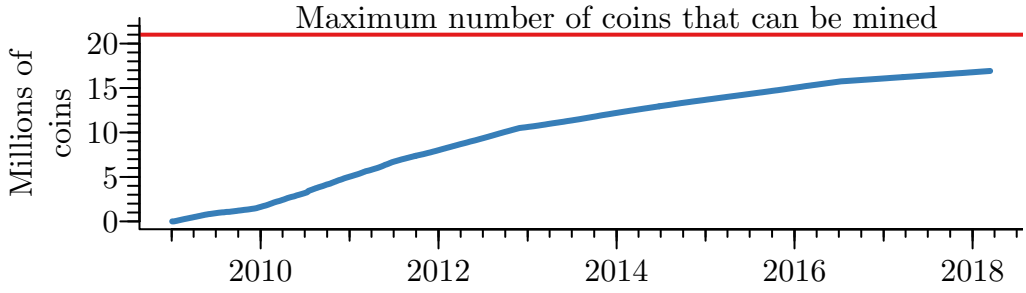
When it comes to the original cryptocurrency, Bitcoin, new coins are created by a computer algorithm using cryptography both for security and to create a deliberately difficult computational problem — mining. Mining each new

[2]Permissionless means that nobody needs permission to update the blockchain, instead, mining ensures the blockchain cannot be maliciously modified. Permissioned, by contrast, means that a trusted institution guarantees the blockchain is not maliciously updated

coin becomes progressively harder and harder as more coins are generated until a theoretical upper limit is reached, at almost 21 million coins, expected to be reached around the year 2140. We now have mined nearly 17 million Bitcoins or 81% of the total. Mining has two purposes: To limit the creation of new coins and to verify transactions, in particular, new transactions with existing coins can only be validated by mining new coins. That is a central feature of the trust model. Coins are kept on a permissionless blockchain, where all transfers of coins are recorded. And key to trust, the cost of maliciously manipulating the blockchain is higher than the profit from doing so.

The deliberately slow pace of mining means that transaction times with Bitcoin are similarly slow, 10 minutes at least. With Bitcoin all transactions are visible, a necessary feature to ensure trust. Figure 1 shows the supply until now.

Figure 1: Bitcoin supply, 2009-2018



Many other cryptocurrencies follow a similar setup, but often with two crucial differences. Some amount of coins is created at the outset out of nothing, just like with fiat money, a process called "pre-mining", a central feature of initial coin offerings (ICOs). Second, the mining schedule is often faster than with Bitcoin, which allows for faster transactions. Other currencies dispense with mining altogether, creating new coins when someone gives them fiat money or other cryptocurrencies.

Some cryptocurrencies aim to improve on Bitcoin as money, as it suffers from high transaction costs, slow speed, and lack of privacy. Bitcoin cash and Litecoin, improve efficiency while Monero promises anonymity and privacy. This comes at a cost since there are direct trust versus efficiency versus privacy trade-offs. The visible blockchain with slow updates is what guarantees Bitcoin's trust. Improving efficiency by speeding up transactions or removing visibility reduces that trust.

The second largest cryptocurrency after Bitcoin is Etherium, which aims

to be a globally distributed computer program to execute smart contracts. Ripple is number three, designed to be a new type of a fast payment system. To achieve this, it gives up on blockchain and its native technological trust, replacing it with trusted institutions.

The total number of coins outstanding is known as the cryptocurrency supply, and the product of the supply and price of coins denominated in fiat money is called "market capitalization". At the time of writing, each Bitcoin has a price of $11,162, a supply of 17,789,700 coins, so the market capitalization is almost $200 billion. Bitcoin retains the first-mover advantage as it is most valuable of all the cryptocurrencies. The second-highest market capitalization is with Ethereum, at $31 billion, while Ripple is third at $17 billion.

2.3 Central Bank digital currencies

Most central banks are actively studying digital and have even considered issuing their own, see the survey in Mancini-Griffoli et al. (2018). The main reason behind her interest appears to be their fear that private entities may create payment systems that are beyond government control. To forestall that, the central banks would prefer to create their own digital currency. These are not cryptocurrencies in the typical sense, because there is no mining and trust continues to be provided by the central bank. For a comprehensive dissuasion on the technical issues surrounding Central Bank digital currencies (CBDCs) see Kahn et al. (2018) and the macroeconomic issues Kumhof and Noone (2018).

The idea is that the central bank creates tokens out of thin air, with each token representing a unit of fiat money, and transactions with those tokens taking place on a blockchain permissioned by the central bank.

The system could be decentralized or centralized. A decentralized CBDC operates similarly to existing cryptocurrencies, so transactions are recorded on a distributed ledger like a blockchain. The downside to such an approach is that the distributed ledger technology of today is very slow, updating records is orders of magnitude slower than existing payment systems, implying that the distributed CBDC system would be unusable in practice without significant technological improvements.

That leaves a centralized token-based system where the central bank, or some trusted private company, keeps track of the transfer of tokens.

Why would a central bank want to move to a cryptocurrency based system?

There are four main arguments.

First, some countries are well on the way of getting rid of cash, like Sweden, and many others are seeing the emergence of nascent payment systems based on digital money. If those payment systems take off, the central banks may lose control of the payment system, and the regulators may not be able to enforce consumer protection, know your customers (KYC) or anti-money laundering (AML) criteria. The central banks can stay ahead of the competition by issuing their own digital money.

The second reason is that CBDCs might be more efficient generally than the existing system, allowing for more secure and faster payments. One example of this is Switzerland, where the central bank is considering issuing digital money for settlement on the stock exchange.

Third, cash is anonymous, but a CBDC is not, unless the central bank explicitly designs it to be, and then only if we can trust the central bank not to monitor. Therefore, CBDC gives the state direct surveillance powers over citizens, a major attraction for less democratic countries, but equally problematic for democracies.

The final reason is that a CDBC might make it easier for the central bank to control the money supply. In the current system, if the central bank wants to change the price level, it either has to do quantitative easing/open market operations, or adjust short-term interest rates, problematic if interest rates are already close to zero and it wants to lower them further. A CBDC gives the central bank the ability to directly increase or decrease the fiat value of coins, immediately and precisely affecting the supply of money.

There are, however, two reasons why a CDBC may not be such a good idea. The first is that if citizens are exchanging money on a central bank's blockchain, the central bank becomes a service provider, and will have to set up the necessary infrastructure, call centers and the like.

More important is the question of the allocation of credit. If the central bank, instead of commercial banks, is the recipient of people's money, then it also becomes responsible for lending out the money. That is not a role of the central banks will relish, nor one we would want them to have.

2.4 Corporate digital currencies

The final form of money is corporate digital currencies, such as Facebook's Libra and JP Morgan's JPM coin. These are related to the tokenized scrip

money of old and the account base e-money systems, discussed above. They cannot be considered cryptocurrencies because they exist on a permissioned blockchain, with trust provided by the corporate owners.

JPM coin is tokenized US dollars, with full reserve, designed to facilitate payments within the JP Morgan client base. As such, it is just more efficient database and payments infrastructure technology.

Information on Libra (2019) is limited at the time of writing. It involved tokenizing a basket of currencies on a permissioned blockchain under the control of the Libra consortium. Consumers use banks to buy the tokens and then can transact much more efficiently than they can do now. The target market seems to be developing countries that lack a well-functioning payment infrastructure. While similar to several proposals, Facebook's large client base distinguishes Libra from the alternative.

2.5 Can fiat money and cryptocurrencies coexist?

The world's monetary system was historically based on bimetallism, with both silver and gold used as money. While sensible when transportation links were problematic, and mining local, as globalism increased it was increasingly infeasible to use two metals, not the least because price stability depended on the ratio of the price between the two being constant. One problem with bimetallism was Gresham's law, "bad money drives out good". The cheaper metal (silver) was used in transactions, and the more expensive (gold) hoarded.

By the middle ages, multiple different currencies were circulation. Not surprisingly, the first modern financial center, the Netherlands, made harmonizing currencies a priority, which they did with the Amsterdamsche Wisselbank that operated between 1609 and 1795. Other countries followed, and by the 19^{th} century most of the world operated with a single currency, the gold standard. Even then, many countries had had parallel issuers of currency. Banknotes in the US were issued by private banks between 1786 to 1914, and jointly with government money until 1935, when the Federal Reserve gained a monopoly on note issue.

The historical lessons suggest that a single currency is preferred. Can cryptocurrencies coexist with fiat money? It is undoubtedly conceivable but has not yet been tested. The most widely used cryptocurrency, Bitcoin, sees very little transactional use outside the illegal, and the same applies to the others. People buy them at their own volition for reasons such as speculation

and macrohedging. Speculation and the resulting price volatility drive out transactional use as argued by Zimmerman (2019).

That could certainly change. The big hope of the cryptoenthusiasts is that the central banks will hold cryptocurrencies as reserves, and large retailers like Amazon accept cryptocurrencies for payments. Even that we begin to earn our salaries in cryptos.

Unlikely. As a practical matter, there are many hurdles before cryptocurrencies start circulating more widely. To begin with, we have the power of the incumbent fiat money. It is embedded in employment contracts and mortgages and lending and every aspect of the economy. I don't think many people would like to earn their salaries in dollars, pay rent in Bitcoin, buy groceries with Ethereum, and compensate the hairdresser in Ripple.

The main exception is the borrowing in foreign currency because it has lower interest rates than the domestic currency. Usually, that ends in tears. It works well in the short run because borrowing in foreign currency strengthens domestic money, but eventually, a currency crisis ensues causing widespread distress. Examples include the Asian crisis in 1998 and Poland and Iceland after the 2008 crisis.

Generally, we want to use a single currency, one that provides price predictability and ease of transactions. I want to know how large my monthly mortgage payment is, and will be, as a fraction of my salary.

Changing to a different type of money would be strongly resisted and very costly. For that to happen, the advantages of crypto have to be clear, and for most people, fiat money works quite well.

While most cryptoadvocates do not expect cryptocurrencies to displace fiat money anytime soon, like to point out that cryptos may see increasing use in the near future. They often to point to coexistence arising from niche applications, typically money transfers, the unbanked and those living with poorly managed currencies, and people looking to macrohedge. Both cases are discussed below.

3 Monetary systems

In a fiat system, money created by the central bank is known as the monetary base and consists of money held on account with the central bank plus the total amount of physical money: notes, and coins. In the eurozone in August 2018, base money was €3.2 trillion.

This is not equal to the amount of money in circulation because the eurozone is a *fractional reserve* system. If I deposit €100 euros into a bank account, the bank has to hold onto €1 (reserve requirement) and can lend out €99 euros. Then the borrower and I have together €199. The amount of physical money in circulation plus demand deposits is M1 (8.1 trillion euros), M2 (11.1 trillion euros) further adds savings deposits, and M3 (12.0 trillion euros) large time deposits, institutional money market funds, short-term repurchases and other liquid assets. The total amount of money in the system is much larger than M3, as economic agents create new money by lending and borrowing. That is the reason why it is hard to control inflation by managing the supply of base money.

The alternative is a *full reserve* system where banks hold 100% of depositors' money in cash, ready to be immediately withdrawn, implying banks can not lend out money deposited in current accounts. The advantage of a full reserve banking is more stability because depositors will feel their money is safe. The downside is that depositors earn no interest, and even have to pay for keeping money in an account, while the amount of credit is much lower than it would be in a fractional reserve system. Furthermore, such a system would likely not prevent the financial system from creating M1, M2, and M3 money, as people would simply deposit their funds into shadow banks, less regulated and transparent financial institutions.

The only form of money directly under the control of the central bank is the monetary base with the rest created by the financial system. Supposing we were to transfer to a crypto monetary system, what would the money supply be?

While some cryptoadvocates maintain that a cryptosystem would be a full reserve banking system, that is highly unlikely. Some owners of coins would inevitably want to lend them out, and others borrow. If the transaction is between two individuals, the amount of money is unaffected because money is coins on the blockchain. If the transaction happens via a financial institution operating under a full reserve system, the same applies.

If, however, claims on coins get traded or the financial institutions are not full reserve, we end up with crypto M1, M2, and M3, and higher forms of money. It is not possible to prevent such an eventuality with technical means because, by definition, transactions in coins are not controlled. As a result, we would get crypto reserve banks, crypto credit instruments, and crypto derivatives, just like we have with fiat.

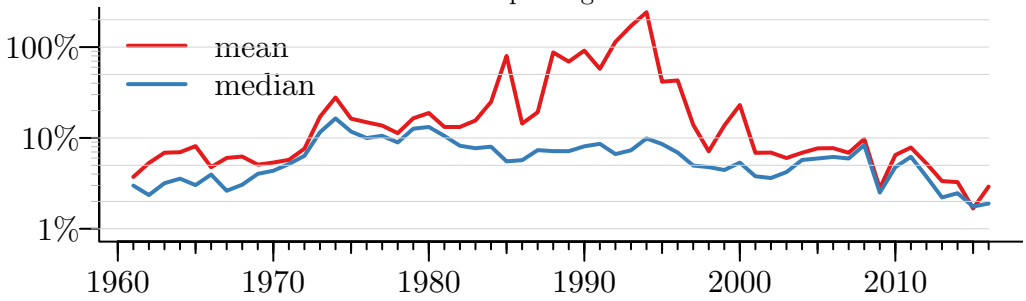
However, only one owner will be recorded on the blockchain, and the crypto M1, M2, and M3, and crypto derivatives would be claims on crypto, rather

than coins itself. That raises serious financial stability issues, as discussed in Section 3.2 below.

3.1 When things go wrong

The most crucial test for a monetary system is how it deals with adverse outcomes: inflation, deflation, and deleveraging. The most common is inflation, a persistent problem of fiat currencies as Figure 2 shows.

Figure 2: Global inflation. Log scale
Mean and median inflation across reporting countries. Data source: WDI



In the worst case, we get hyperinflation, typically when the government surrenders control of money creation because it is under some extreme imperative to raise revenue at all costs. In other cases, the hyperinflation may be deliberate, perhaps at instigation of an incoming communist regime. As Vladimir Lenin said: "The best way to destroy the capitalist system is to debauch the currency," as quoted by Keynes (1920). Table 1 shows the historically highest hyperinflations, and they happen either in the transition to a communist state, in civil wars or due to extreme economic mismanagement.

While many cryptoadvocates argue that the fixed supply of coins ensures price stability, it is not that simple. The reason is that the price level is determined by both the supply and the velocity of money, how frequently a unit of money is spent. An accounting entity describes the relationship between money, prices, and output:

$$\text{price level} = P = \frac{V \times M}{Q} = \frac{\text{velocity} \times \text{nominal amount of money}}{\text{economic output}} \qquad (1)$$

What frustrates monetary policy is that the components of (1) are not determined in isolation, but are jointly determined in equilibrium. If the monetary

Table 1: Highest monthly inflation rates in history

Data source: Hanke and Kwok (2009)

Country	Month with highest inflation rate	Highest monthly inflation rate	Equivalent daily inflation rate	Time required for prices to double
Hungary	Jul 1946	$4.19 \times 10^{16}\%$	207%	15.0 hours
Zimbabwe	Nov 2008	$7.96 \times 10^{10}\%$	98.00%	24.7 hours
Yugoslavia	Jan 1994	$3.13 \times 10^{8}\%$	64.60%	1.4 days
Germany	Oct 1923	29,500%	20.90%	3.7 days
Greece	Oct 1944	13,800%	17.90%	4.3 days
China	May 1949	2,178%	11.00%	6.7 days

authority changes M, the impact on prices is indeterminate, because both V and Q change.

This implies in practice that neither fiat, gold, nor a crypto monetary systems guarantee price stability, all can generate inflation and deflation.

A crypto monetary system with a slow and fixed mining schedule like Bitcoin is more likely to suffer from persistent deflation, that is, prices falling. The reason can be seen in (1). If the mining is slower than economic growth, unless velocity continually increases, P must fall.

Does that matter? The empirical evidence, (see, e.g. Atkeson and Kehoe, 2004) finds that persistent deflation is not associated with poor economic performance, except in the Great Depression. That, however, only captures the macroeconomic consequences. Deflation has distributional consequences, and the social impact may be substantial.

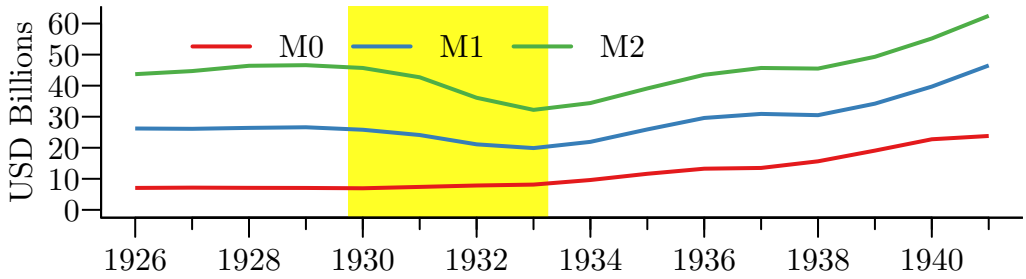
Deflation was persistent under the gold standard because the supply of money did not keep up with economic growth, causing prices to fall. The winners were owners of capital and the losers borrowers and employees. Nominal salaries had to fall continually, and labor market strife and social unrest resulted. The People's Party in the late 1800s in the US objected to gold being used as money because of a credit crunch causing widespread distress, unable to be resolved because of the fixed supply of gold.

Not surprisingly, the final nail in the coffin of the gold standard, at least in the United Kingdom, was universal suffrage, not of women, but the poorer social classes. They saw the gold standard benefitted property owners, and when they gained the vote, pushed the political system into abandoning it. This happened in the 1920s after World War I. In times of extreme stress, such

as during a war, governments will find a way to finance the war and almost inevitably will resort to debasing the currency. Once World War I started, most belligerent countries abandoned the gold standard, using inflation to finance the war. In the United Kingdom, Sterling depreciated by 40% during the war. In spite of that, Winston Churchill, at the advice of the governor of the Bank of England, decided in 1924 to return to the gold standard, at the prewar exchange rate. That meant the UK had a significantly overvalued currency, leading to persistent deflation and widespread social unrest until it abandoned the gold standard in 1931.

If the economy is growing rapidly, the supply of money needs to grow with it to prevent deflation. Many recessions are coupled with deleveraging when the supply of higher forms of money like M2 or M3 is falling, while M0 or M1 are still growing, rapidly increasing the supply of money prevents the worst economic outcomes. A good example of this is of the Great Depression when we saw a sharp fall in M2, while M1 moderately increased, signaling that people were deleveraging rapidly, as seen in Figure 3. This significantly slowed down the economy and was one of the two leading causes of the Great Depression, as argued by Friedman and Schwartz (1963).

Figure 3: The supply of money in the US in the Great Depression, 1929-1933



Neither fiat, gold nor a crypto monetary systems guarantee price stability. All can generate inflation and deflation. However, fiat systems have a built-in safety valve; the supply of money can be adjusted to best suit the economy. Consequently, a well-managed fiat system will result in more price stability than a cryptosystem, and the opposite holds when fiat is poorly managed, like in Zimbabwe and Venezuela.

3.2 Financial stability

Most observers do not find that cryptocurrencies pose much threat to financial stability, at least in the immediate future, (see e.g.

Financial Stability Board, 2018; den Haan et al., 2017). After all, an asset class that amounts to $309 billion is quite small compared to the overall asset markets, especially since cryptocurrencies are for the moment primarily held for speculative reasons and have a trivial economic use. If, however, cryptocurrencies were to take off, the picture changes, and severe financial stability concerns emerge.

A crypto monetary system is subject to the same financial stability challenges as fiat and gold systems. The mining process only controls the creation of base money, the number of coins, while the supply of money is crypto M1, M2, and M3, and just like with fiat and gold, the creation of such money is under nobody's control. In times of economic booms, such money might be rapidly created because of the growth of crypto credit, and conversely, during recessions, higher forms would be converted back into lower forms, a crypto credit crunch.

Many of the crises in the era of the gold standard show the fragility of a monetary system based on a commodity like gold or coins, like the Panic of 1893 in the US. At the time, we typically did not use gold directly in day-to-day transactions. Instead, the central bank created paper money and guaranteed it could be replaced by gold. In the case of the Bank of England in the mid-19$^{\text{th}}$ century, it held sufficient gold to cover 40% of printed money. Inevitably, such paper money was lent out, creating higher forms of money (M1, M2, etc.), and when the inevitable crises came along, people rushed to convert less liquid assets into gold.

It was the severe financial crisis of 1866, (Elliot, 2006) that show best the limitations of rigid gold monetary systems. When the largest bank of the era, Overend & Gurney, failed because of bad high-technology investments, most market participants did what people always do in times of crisis, convert their financial assets into the safest and most liquid, in this case, gold. The result was a very sharp reduction in the supply of money, a credit crunch, widespread bankruptcies and one of the most severe economic depressions of the 19$^{\text{th}}$ century. In response, the Bank of England was forced to create formal rules to relax the gold standard in times of crises, in their lending of last resort policy proposed by Bagehot (1873).

The same fundamental forces that caused the crisis of 1866 have been behind almost every financial crisis before or since, including 2008. Excessive amounts of endogenous risk (Danielsson and Shin, 2002) that is hidden until it is too late when a crisis is underway. All serious financial risk is endogenous, caused by the interaction of the human beings that make up the financial system. They are prone to act as a procyclical herd and are subject to a

variety of constraints and biases. In boom times, our behavior is more idiosyncratic than during crises when the self-preservation instincts kick in, the reason why prices go up by the escalator and down by the elevator. Booms built up slowly and deflate rapidly. During crises, we all want to avoid being burnt, and hence, all crowd the exits at the same time.

Endogenous risk is present in every monetary system, gold, fiat, and crypto, and the money supply under cryptocurrencies can be as procyclical as with gold or fiat. A cryptosystem is particularly vulnerable to endogenous systemic risk because of its very presumed stability. Minsky (1986, 1992) suggested that "stability is destabilizing". A financial system that creates an aura of stability encourages economic agents to take more and more risk. Investment projects, and hence loans to finance them, become increasingly risky, and it takes a smaller and smaller event to trigger a rapid reversal when the proverbial little boy yells "the Emperor has no clothes" as in HG Anderson's fairytale

The crypto specific systemic risk augments the standard types of systemic risk present in both gold and fiat systems. When economic agents get worried about the stability of their financial institutions, they run them. Crypto M1, M2, and M3 are only claims on coins, (at least under a Bitcoin style system) not like under gold where the central bank guarantees convertibility, or equivalent as with fiat. In times of crisis, when confidence evaporates, that can by itself leads to a cryptosystem panic since if economic agents start to worry their money is not equivalent to coins, they will run their financial institutions.

Just as under the gold standard, we can't resolve the crisis because we can't create new base money (coins), at least in a cryptosystem like Bitcoin with a fixed mining schedule.

While a fiat system is affected by the same fundamental crises forces, it does have a way out. Because it can create infinite amounts of liquidity on demand, the central bank can guarantee shock and awe. It can tell the financial markets that no matter what the demand for liquidity, it can meet it, keeping the economy going and preventing disastrous failures of the financial institutions without whom the economy cannot function. By itself, such a credible demonstration is stabilizing. Once the markets know the central bank will do what it takes, a crisis can be mitigated. We saw that in action with the ECB "we will do what it takes" announcement in 2012.

The failure of the Federal Reserve to do so during the Great Depression was the reason a financial crisis and economic recession became a depression. The globally coordinated liquidity creation of the financial authorities in the

autumn of 2008 is the reason why that crisis did not become a depression.

Ultimately this means that a cryptocurrency based monetary system would suffer from higher systemic risk than either the gold standard system or a well managed fiat system.

4 The ideological case for cryptocurrencies

Arguments in favor of cryptocurrencies are both ideological and technological, but for the most enthusiastic advocates, the ideological is more fundamental. Freedom from abusive and incompetent governments.

4.1 Trust

The government controls fiat money and is not shy in using its power. Then, money outside of the control of the government becomes attractive. This is a long-running debate that predates cryptocurrencies, like in the 19^{th} century US, and the debate over the establishment of the Fed in 1913, and the free market monetary discussions in the 1970s. For those to whom this matters, cryptocurrencies make sense. This, however, is a tiny fraction of society. Even then, I question the freedom one gets.

A fundamental notion of cryptocurrencies is trust. Transactions with electronic fiat money go through several systems, including a payment processor, a bank on both ends, and a payment system in the middle. We have to trust that all these entities have our best interests at heart. We also have to trust the government not to confiscate or devalue our money.

Cryptocurrencies promise to replace all that with algorithms, transaction simply involve the movement of tokens on the blockchain, with trust provided by mining. As long as we trust the algorithm, we are safe. But the algorithm is only the mathematical middle part of the transaction, and a lot of practical implementation details erode trust. A tiny segment of the population is sufficiently technically adept at implementing the entire thing themselves and trusting their work. The rest of us have to rely on someone else for implementation. And then we are left with trusting unknown entities. Here is a small list of what can go wrong.

Abuse in the cryptocurrency market is rife, front-running, cornering, and pump and dump, all of which are legal and non-verifiable. Hacking of ex-

changes and trading platforms is pervasive. A recent report[3] showed that $927 million was stolen in hacking in the first three quarters of 2018. The best practice in transacting cryptocurrencies is to keep one's keys on an air-gapped laptop.

If something goes wrong, there is no recourse. No regulations, legal system, or police protect us. This is by design because the cryptocurrencies are meant to operate outside the state. But that means less protection and less trust.

It is not the same with fiat money. Internet banking and electronic fiat money transactions are quite safe, and multiple layers of security protect us. The chance of hacking is very low and, in the event of a problem, we have recourse. I am perfectly happy to do online banking without continually looking over my shoulders or resorting to air-gapped laptops.

4.2 Privacy

Some cryptocurrencies, like Monero, promise privacy. I can enter into a transaction without anybody knowing about it, except myself and the person I am dealing with. The most popular cryptocurrency, Bitcoin, does not offer this because the blockchain is, and has to be, visible. Transaction records are publicly searchable.

If we want purely anonymous transactions, trust has to give. If not provided by technology, it has to come from individuals and/or institutions. There is no such thing as 100% privacy when it comes to financial transactions. Fiat cash is entirely anonymous, except someone might be monitoring the transaction. If we move to electronic fiat money, we are subject to tracking, both by private companies and government authorities.

Same with even the most privacy-focused cryptocurrency; the starting point is the internet, which makes monitoring possible, and if the endpoint is a business, the government reserves the right to monitor the transaction. It is conceivable that two entities can conduct business by using only a privacy-based cryptocurrency, with correctly implemented end-to-end encryption and no monitoring of the exchange of goods. Even then, the transaction would have to be based on some goods that are outside of the standard economy — like illegal drugs, because the government can monitor all other economic transactions.

[3] https://uk.reuters.com/article/uk-crypto-currency-crime/cryptocurrency-theft-hits-nearly-1-billion-in-first-nine-months-report-idUKKCN1MK1JD

4.3 Decentralization and democracy

Cryptocurrencies are supposedly decentralized and democratic. We can approach centralization from two directions, IT and power. From an IT point of view, cryptocurrencies are designed to be decentralized. There is a large number of nodes and one vote per computer processor. Records are kept on multiple systems, ensuring robustness, so that they cannot be maliciously manipulated, except with a 51% attack.

That is the theory. In practice power matters. Mining is in the hands of a small number of cartels, with a constantly shifting group of individual miners, whose identities are opaque. The primary producer of Application Specific Integrated Circuit (ASIC) chips, the preferred way to mine, has 85% market share, and either directly owns or has majority share in the three largest mining pools, BTC.com, AntPool, and ViaBTC, with perhaps 50% of the world's mining ability.[4] More than half the miners are Chinese, and hence under the control of the Chinese Communist Party.

So, instead of one vote per processor, there is one vote per cartel. The miners are those who write history, so malicious manipulation is possible, perhaps via a 51% attack. The number of exchanges is small. This means that power is concentrated, non-transparent, and undemocratic.

It is different with fiat money. We have about 180 fiat currencies in circulation, with each a local monopoly. Some are well managed, and others not. There is, however, a central difference between decentralization in cryptocurrencies and fiat money, and that is democratic accountability.

With cryptocurrencies, power is concentrated in the hands of a small number of shadowy and uncountable entities beyond both legal and democratic control. An undemocratic elite making material decisions about other people. Central banks create fiat money, and are, in democracies, transparent and accountable to the citizenry.

4.4 Manipulation of supply

One of the most common argument advanced in favor of cryptocurrencies is that because the supply of cryptocurrencies is fixed (especially Bitcoin) just like gold, the government cannot manipulate the supply of money. These are old arguments, dating back to the gold standard and before. And for a

[4] https://www.forbes.com/sites/pamelaambler/2018/08/17/all-you-need-to-know-about-crypto-mining-phemon-bitmain

good reason. The central banks have frequently abused their privilege, with the stagflation of the 1970s, quantitative easing over the past ten years, and hyperinflation in countries like Venezuela, particularly problematic.

If we have a choice between a poorly managed fiat currency and a cryptocurrency underpinned by an algorithm, the latter should win out in the marketplace, following from Hayek (1997, 1999). For a modern analysis of Hayek's arguments in a cryptocurrencies context, see Fernandez-Villaverde and Sanches (2018).

While such arguments were convincing in the 1970s when inflation was out of control, monetary policy has improved considerably since then. So, does it make sense to use an asset in fixed supply, like gold, or a cryptocurrency as money instead of credible fiat money?

No. The cryptoadvocates often assume that money will be tokens on the blockchain, and because the supply of tokens is deterministic, so will prices. That is not true. The cryptomoney supply will not be the number of coins, because it is inevitable that someone will borrow or lend cryptocurrencies, we will end up with fractional reserve banks, credit markets, derivative markets, and all the other paraphernalia of financial markets. That implies crypto M1, M2, M3, and higher forms of money.

Prices and supply will fluctuate procyclically with economic fortunes, so if the supply of the monetary base is fixed, then there are no means to have a countercyclical monetary policy. We can expect more price level fluctuations in a cryptosystem than a well run fiat system.

Consequently, cryptocurrencies are not a good store of value, and even less so than fiat currencies. Figure 4 shows how many real goods one Bitcoin and 1,000 US dollars would have bought every year since Bitcoin started, 2009. The dollar has declined at a steady rate with inflation and lost 19% of its value over these ten years. Bitcoin has increased sharply, but at a very erratic rate, not providing anything resembling a stable store of value.

This result is supported by market risk analysis of Bitcoin. As Figure 5 shows, Bitcoin is over five times riskier than the FTSE, and 20 times riskier than GDP/EUR. Daily updates and more details can be seen on extremerisk.org.

The price fluctuations are not consistent with the store of value function. Some cryptocurrencies promise stability, most importantly Tether which has maintained an almost exact parity with the USD since its initiation in 2015. However, at best, this means that Tether is as good as the USD as a store of value. Furthermore, Tether has shown considerable volatility recently.

Figure 4: Bitcoin and fiat money store of value — to July 2019

Figure shows how Bitcoin and the USD have acted as a store of value

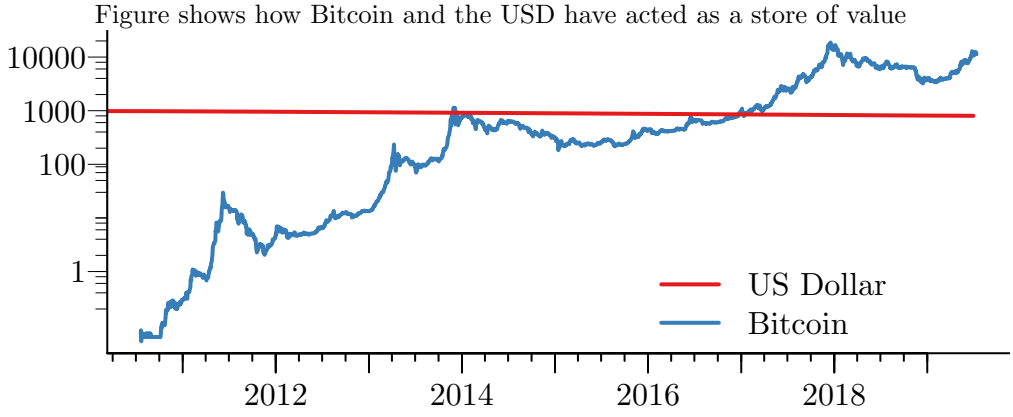
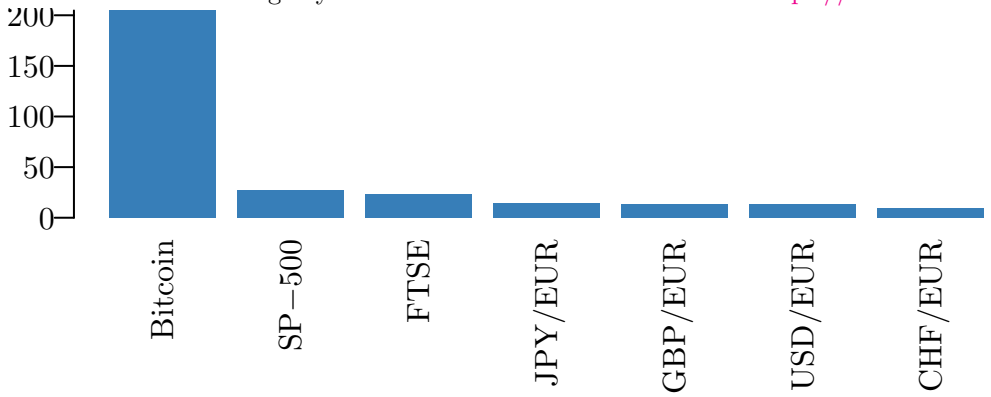


Figure 5: Bitcoin, stock market and fiat money risk

Risk is defined in the figure as the average Value-at-Risk over the six most commonly used risk methods, expressed in national currency units of a portfolio with a value of 1000. The forecasts are one trading day into the future. For more details see https://extremerisk.org.



4.5 Macrohedge

Many investors in cryptocurrencies see themselves as rational agents hedging against poor government policies, such as quantitative easing, political risk, macroprudential risk, and expropriation risk. All of these threats are real, and governments have not shown themselves to be credible long-term stewards of the monetary system, witness the 20% decline in the purchasing power of the dollar over the past ten years.

However, it is hard to see how cryptocurrencies can provide an effective hedge against government policies. For that to happen, we have to expect cryptocurrencies either to hold their value or increase in the future and that governments will not gain the power to confiscate crypto holdings.

The government has confiscated assets like gold. For example, in 1933, the US

government required all persons to deliver their gold to the Federal Reserve, in exchange for $20.67 an ounce and subsequently setting the price of gold at $35. Cryptocurrencies, at least those on a visible blockchain, are even easier to confiscate, as the government can monitor ownership and has the legal powers to compel owners to hand over the holdings to the government.

The question then is how well do cryptocurrencies compare to other forms of macrohedges, like gold, property, land, and art. We have considerable historical evidence for how these asset classes perform in times of extreme stress, and in expectation, cryptocurrencies will perform worse. The reason is that the cryptos will be subject to the same supply and demand issues as the other macrohedges, and if the cryptos retain value, should perform equally. However, unlike the other asset classes, unless one is willing to ascribe 100% probability of success to the cryptos, the product of the success probability and performance will be lower than the of the other macrohedges.

5 The technical case for cryptocurrencies

The ideological case for cryptocurrencies is often backed up by technical arguments. That cryptocurrencies provide handy economic functions that might not make them fully displace fiat money, at least facilitate coexistence.

5.1 Blockchains, databases, and ledgers

Instead of replacing fiat money, some cryptocurrencies aim to provide other economic functions, such as keeping track of assets on a blockchain. While conceptually appealing, the more ambitious applications have not been amenable to blockchain implementations, not the least because of blockchains' technical limitations, like the speed of updates and trust.

It all comes down to efficiency and trust. Mining guarantees the integrity of transactions on the Bitcoin blockchain. Integrity of the data on the blockchain is ensured both by the public visibility and distribution as well as it being costly (mining) to add new data. The very benefit that makes Bitcoin based blockchains attractive is also what makes them expensive and inefficient. There are many proposals for solving those issues, like the Lightning Network, Plasma, and thin wallets. So far, they remain proposals and generally rely on giving up trust and/or privacy.

That leaves straightforward ledger applications, involving blockchains but

dispensing with cryptocurrencies. The benefit of blockchains is that one can replace cumbersome legacy processes with simply tokens on a blockchain. Information the blockchain is immutable — can not be changed without a record of the change — and swapping tokens is much more efficient than moving money around in accounts. For example, the Swiss stock exchange, Six, is aiming to tokenize stocks and other assets on its blockchain, where trading will simply involve swapping tokenized central bank issued Swiss francs with tokens representing assets. Complicated settlement that now takes days will be eliminated. Similarly, procurement processes on a blockchain allow for a single place for keeping transparent and immutable information. The use case for corporate cryptocurrencies, like Libra and JPM Coin, also falls into this category.

While all of these make economic sense, they have nothing intrinsically in common with cryptocurrencies, except for the use of blockchains. The key difference is that the trust model of cryptocurrencies is replaced with trusted institutions, The Swiss stock exchange, Facebook, JP Morgan.

However, a private blockchain under the control of a single entity or a consortium of entities — permissioned — is indistinguishable from existing database implementations from the point of view of trust. Blockchains without cryptocurrencies are just a database technology, and blockchains with cryptocurrencies are much too inefficient to be useful in any real-world application.

5.2 Smart contracts

The idea behind smart contracts is that a contract between two or more counterparties can be written in a formal computerized logic that self-enforces and self-executes terms and conditions, typically on the Ethereum decentralized platform.

At least two reasons limit the usefulness of smart contracts. The first is that in most cases, it is impossible to map out all contingencies ex-ante, the reason we have courts of law. The second is that the law places direct limits on what can be agreed, as argued by Schuster (2018), so transactions need to be consistent with national law to be relevant. Smart contracts need to be in sync with the law and hence can only facilitate execution already done in the physical world, rather than replacing them with something new and magical. For smart contracts to surpass that, we would need bi-directional synchronization between the law and smart contracts, not a realistic prospect.

It does seem that the promise of smart contracts has been oversold, implicitly

recognized by the founder of Ethereum, Buterin (2018), on Twitter:

> "To be clear, at this point I quite regret adopting the term 'smart contracts.' I should have called them something more boring and technical, perhaps something like 'persistent scripts.'
> I do think that persistent scripts controlling assets compete with the legal system on some margins, but so do locks on doors. So IMO it's wrong to equate them with a specific philosophy of law privatization."

5.3 Money transfers

The transfer of money between users is the most frequently cited use case for cryptocurrencies. The transfer of blockchain-based cryptocurrencies like Bitcoin is inherently slow if we want to trust the transaction, taking at least 10 minutes, or even an hour. They are far from costless if one wants to have the transaction processed by a miner and confirmed by the Bitcoin network. Over the past year, the transaction costs for Bitcoin have ranged from $0.45 to $55. This is because someone has to be incentivized to continue mining to validate the transactions. That is costly, both financially and environmentally. Transaction costs can end up being much higher because a balance of, say 10 Bitcoins, does not mean we hold 10 Bitcoins in one lump, instead, we may hold a large number of much smaller pieces. One hundred millionth of a single bitcoin is known as a satoshi and is the smallest unit of Bitcoin recorded on the blockchain. A transaction may, therefore, involve the consolidation of multiple pieces on the blockchain, each subject to high transaction costs. Repeated transactions exasperate this fragmentation problem. If we want to speed this up or make it cheaper by switching to a different cryptocurrency, trust has to give. There are proposals for new cryptocurrencies aiming to improve on the transaction costs while retaining trust, but so far, they are only proposals.

That leaves the transfer of tokenized fiat money. One can write a contract specifying the exchange of tokenized US dollars for tokenized euros at the prevailing midmarket exchange rate, paid for in Ethereum Gas. That transaction is almost instantaneous, at a fair exchange rate and very cheap. We are today able to use regulated fintech companies to do precisely that.

Transactions using a single fiat money are cheap, secure, and faster than with any of the cryptocurrencies in most of the world. Here in Europe, I can transfer any amount out of my bank account to someone else instantaneously

in the same currency at no cost, using a mobile phone. The same happens in many countries via e-money, like M-Pesa.

It is not the same if the transfer involves the exchange of currencies. A transfer of money via banks is costly, can be slow, is subject to KYC and AML restrictions, and requires one to have formal bank accounts.

The high cost of international transfers of money are especially egregious when the amounts are small and recipients in developing countries. The World Bank (2018) notes that the transfer cost of remittances is very high, the global average cost of sending $200 is 7.1% and 9.4% in sub-Saharan Africa. It sites bank de-risking and exclusive partnerships between national post office systems and money transfer operators as the main obstacles, which hinder the adoption of more efficient technologies, including cryptocurrencies.

There is certainly scope for improving the efficiency of international transfers. In much of the world, that problem has been solved by various fintech companies, like Transerwise. In other countries, political or government restrictions get in the way, channeling transfers via legacy banks.

5.4 The unbanked and bad currencies

Many cryptoadvocates argue that, while there may be little reason to move to cryptocurrencies for those living in developed countries with credible central banks and governments, that does not apply to all. Some countries have unstable governments or have large unbanked segments of the population, and cryptocurrencies may be of help to citizens in those countries. Often-cited examples include places like Zimbabwe. Venezuela has even created its own cryptocurrency, the Petro.

The most cited use case is indeed Venezuela, as that may be the only country where cryptocurrencies are used for daily transactions. The reason is rather prosaic. The Venezuelan government restricts the use of US dollars, but not cryptocurrencies, so the legal alternative is Bitcoin.

In countries with high inflation, people usually seek out other currencies, typically the US dollar. Transactions might be made entirely in dollars, or prices may be quoted in dollars while transactions take place in the local currency at the spot rate. This is called dollarization, or currency substitution. While not perfect, the presence of a credible fiat currency does make dollarization a useful hedge against bad government policies.

It is hard to see how cryptocurrencies would serve any better than fiat cur-

rencies. At least, in the latter case, we have a tried and tested technology. It would seem that the problems of the unbanked in those living in countries with poor monetary policy can be solved by financial technology, such as banking via mobile phones and the like, perhaps M-Pesa. Such solutions are currency agnostic, and one can plug in any currency.

6 Profit and fairness

6.1 There is money to be made

Cryptocurrencies have been a fabulous investment for early investors. A Bitcoin was worth $0.04 in 2009, and $11,538 now, a 29 million percent return. Does it make sense to invest in cryptocurrencies today? It depends.

Any asset can get into a bubble state. People buy it because they expect others to pay a higher price in the future, creating a positive feedback between buying and prices. Someone who invests early and sells in time makes money, just like an early investor in a Ponzi scheme profits, provided she gets out early.

This leaves two questions:

1. What sort of investments are cryptocurrencies?
2. Does it make sense to invest in them?

The price of stocks and bonds follows from expectations of future income. Other assets have value only because we hope others will buy them at a higher price in the future.

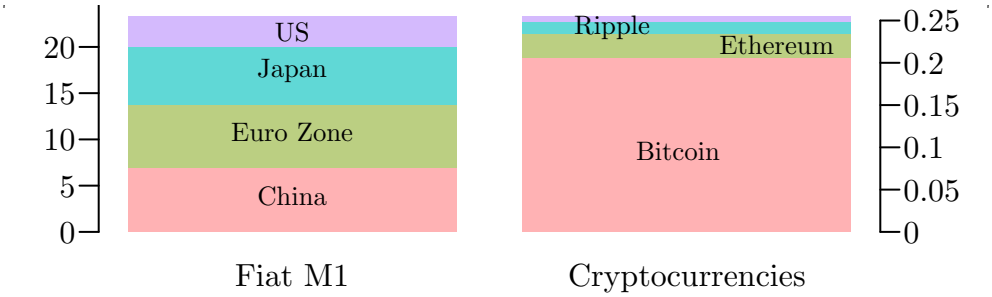
Collectables are in the latter category. The Wall Street Journal ran an interesting story on the risk of investing in collectibles in early 2018, "Sorry, Collectors, Nobody Wants Your Beanie Babies Anymore: Over two decades after the great Beanie Baby craze, speculators are back, hoping someone will finally buy their floppy collectibles". It is the same with art and stamps. Collectible stamps have a scarcity value, with some costing more than $200k.

Money is in the latter category. Fiat money, such as dollars, yen, and euros, the form of currency used in almost every country, only holds value because the issuing central banks and governments are expected to manage them properly.

Most cryptocurrencies — like the most popular, Bitcoin — are envisioned as a new form of money. The best case for cryptocurrencies, then, is a full replacement of fiat money. So how much would that be worth?

It depends on what we mean by money. Suppose it is M1, printed money, and demand deposits. The total value of M1 in the G20 economies is $31 trillion, with the four largest seen in Figure 6. The aggregate market value of all cryptocurrencies is $308 billion, of which Bitcoin is the largest at $206 billion.

Figure 6: The volume of money in the four economies compared to the four largest cryptocurrencies, July 2019



So what is the value proposition of cryptocurrencies? Their market value is today about 1% of M1, but over the past year has been double or half that at times. While we can debate the specifics, a 1 to 100 ratio provides a useful guide to scale.

There are three possible scenarios.

1. cryptocurrencies will fully displace fiat money;
2. cryptocurrencies will partially replace fiat money; or
3. cryptocurrencies will not usurp fiat money.

Under the first scenario, cryptocurrencies might increase 100 times in price. Under the last scenario, cryptocurrencies only have a logical terminal price, zero, unless some use is found for them that does not involve displacing fiat money. The zero and 100 times returns are therefore sensible lower and upper bounds on the profits a long-term investor can expect.

Sticking to my back of the envelope calculation for the extremes, a long-term, risk-neutral investor will hold cryptocurrencies if she expects the chance of them entirely replacing M1 to be higher than 1%. If not, she should either

not hold or consider selling short, provided the cost of doing so is sufficiently low.

That leaves the case of coexistence. As discussed above in Section 2.5, I think that is highly unlikely. Displacement would either be full or not happen.

6.2 Fairness

If cryptocurrencies become real competitors to fiat money, someone is going to make a profit. While I think the displacement of fiat to crypto will either be full (100%) or more likely not happen at all (0%), such a binary outcome is controversial, and it might be somewhere between 100% and 0%.

Under 100% displacement, $31 trillion will be transferred to a handful of crypto speculators. $31 trillion is almost the annual GDP of the US and China combined (at $34.5 trillion).

Such privatization of a public good, fiat money, dwarfs the largest expropriations of public goods we have ever seen. Some examples are the Inclosure Acts in England and Wales when 2,800,000 hectares of common land was transferred to private ownership and the Highland Clearances in Scotland. Similarly, the confiscation of Native American land in the US and Aboriginal land in Australia and the more recent Russian and Chinese privatizations.

Would the $31 trillion (or any amount significantly higher than the current $309 billion) switchover from M1 to cryptocurrencies be of the same nature? The transfers in the examples above happen at the instigation of the sovereign, which deliberately enriched some citizens and impoverished others. By contrast, current transfers to crypto speculators are entirely voluntary. I buy Bitcoin at my own volition.

However, for cryptocurrencies to displace fiat money, the sovereign has to acquiesce. Make the deliberate decision that Bitcoin is to be used instead of dollars. The reason is that fiat money is legal tender and for cryptocurrencies to replace fiat in any significant about, the sovereign has to permit it.

Consequently, the transfer of $31 trillion to a handful of private speculators would dwarf any historical antecedents, be the largest expropriation of a public good in human history.

This is strongly disputed by cryptocurrencies advocates, with many finding such notions Marxist. That it does not recognize the just return to an entrepreneur taking risk. Such counterarguments miss the point. There is widespread support for the idea that the entrepreneur should benefit from

the fruits of their labor, accomplished in a competitive marketplace, not by expropriation.

Unlike entrepreneurial wealth, the crypto fortunes would be created by inclosing a public good. It would be fundamentally unfair to transfer those $31 trillion to crypto speculators.

If we transit from a fiat monetary system to a crypto-based one, the only just way would be for all created coins to be under public ownership from the outset.

7 The desire and power of governments

Governments will resist any displacement of fiat with privately created crypto. Their objections are based on the reluctance to give up seigniorage, the lack of fairness in transferring $31 trillion to crypto speculators, inability to manage the supply of money to suit economic and political demands, both routinely and with lending of last resort.

Meanwhile, even if cryptocurrencies continue to gain traction, they will increasingly be subject to government scrutiny. With all the cryptoprofits, governments want people to pay taxes on those profits. They will also want to enforce microprudential regulations designed to protect consumers and monitor transactions to prevent terrorists and criminals from receiving funds.

Cryptoadvocates might retort that none of these matters since the opinion of the government is irrelevant. Cryptocurrencies live in cyberspace, outside existing economic and financial structures, away from the long arm of the law. A libertarian paradise. Nonsense. Governments have the power to ensure money controlled by them remains legal tender, and they will undoubtedly do so.

Any transaction involving fiat money is monitored and controlled by the government. If it is US dollars, transactions go through the US payment system in the New York Fed, in euros via Target 2. Any entity that refuses to cooperate can be denied access to the payment system, and hence unable to transfer fiat money to or from cryptocurrencies. The US government has not been reticent in taking advantage of its reserve currency powers in the past and. Surely it will not be shy if it perceives cryptocurrencies as a severe threat in the future. Governments can and do ensure company accounts are in the legal tender and that all transactions involving the government are also in the legal tender.

As long as the money stays within the cryptouniverse, that is not all that relevant. However, the point of having money is to spend it. Most of our money is spent within a small radius of our house: real estate, schools, hospitals, grocery stores, hairdressers, etc. All of these are directly monitored and controlled by the government. Merchants can be (and are) required to report any transaction, and can easily be prohibited from accepting payment in cryptocurrencies.

There is a reason why fiat money is also called 'legal tender' and for governments to insist on having a monopoly on printing money.

8 Conclusion

The technologies underpinning cryptocurrencies are quite elegant. That misses the point. An elegant technology does not imply usefulness in the real world. Knowing all the technical detail does not mean understanding its economic or social function. Take, as an example, human beings. I can know all the physics and chemistry and physiology, understand how molecules and organs operate, yet still not know the first thing about an individual.

Arguments in favor of cryptocurrencies, be they technological, economic, or based on freedom miss out on the practical issues. We do have a well functioning incumbent technology and any replacement of the incumbent not only has to be shown is better, but it also has to demonstrate that the benefits overcome the costs of switching.

Cryptoadvocates would be well advised to keep the words of John Maynard Keynes in his 1936 General Theory, in mind:

> "Practical men who believe themselves to be quite exempt from any intellectual influence, are usually the slaves of some defunct economist. Madmen in authority, who hear voices in the air, are distilling their frenzy from some academic scribbler of a few years back."

References

Atkeson, A. and P. J. Kehoe (2004). Deflation and depression: Is there an empirical link? *American Economic Review 94*(2), 99–103.

Bagehot, W. (1873). *Lombard Street*. London: H.S. King.

BIS (2018). Cryptocurrencies: looking beyond the hype. Technical report, BIS. www.bis.org/publ/arpdf/ar2018e5.pdf.

Buterin, V. (2018). twitter.com/VitalikButerin.

Daníelsson, J. (2018). Cryptocurrencies don't make sense. *VoxEU.org*.

Danielsson, J. and H. S. Shin (2002). Endogenous risk. In *Modern Risk Management — A History*. Risk Books. http://www.RiskResearch.org.

den Haan, W., M. Ellison, E. Ilzetzki, M. McMahon, and R. Reis (2017). Economists relaxed about bitcoin: New cfm-cepr expert survey on cryptocurrencies, the financial system, and economic policy. *VoxEU.org*. voxeu.org/article/cryptocurrencies-dont-make-sense.

Elliot, G. (2006). *Overend & Gurney, A Financial Scandal In Victorian London*. Methuen Publishing Ltd.

Fernandez-Villaverde, J. and D. Sanches (2018). Can currency competition work? www.sas.upenn.edu/~jesusfv/currency_competition.pdf.

Financial Stability Board (2018). Crypto asset markets. potential channels for future financial stability implications. Technical report, Financial Stability Board. www.fsb.org/wp-content/uploads/P101018.pdf.

Friedman, M. and A. Schwartz (1963). *A monetary history of the United States : 1867-1960*. Princeton Univ. Press.

Graeber, D. (2011). *Debt: The First 5,000 Years*. Melville House Publishing.

Hanke, S. H. and A. K. F. Kwok (2009). On the measurement of Zimbabwe's hyperinflation. *Cato Journal 29(2)*.

Hayek, F. A. (1997). Free-market monetary system. A lecture delivered at the Gold and Monetary Conference.

Hayek, F. A. (1999). The denationalization of money: An analysis of the theory and practice of concurrent currencies. In S. Kresge (Ed.), *The Collected Works of F.A. Hayek, Good Money, Part 2*. The University of Chicago Press.

Kahn, C. M., F. Rivadeneyra, and T.-N. Wong (2018). Should the central bank issue e-money? sites.google.com/site/rivadeneyr/e-money.pdf.

Karaman, K. K., S. Pamuk, and S. Yldrm-Karaman (2018). Money and monetary stability in Europe, 1300-1914. *VoxEU.org*. voxeu.org/article/money-and-monetary-stability-europe-1300-1914.

Keynes, J. M. (1920). *The Economic Consequences of the Peace*. Harcourt Brace.

Keynes, J. M. (1936). *The General Theory of Interest, Employment and Money*. London: Macmillan.

Kiyotaki, N. and J. Moore (2001). Evil is the root of all money. Clarendon Lecture, www.princeton.edu/~kiyotaki/papers/Evilistherootofallmoney.pdf.

Kumhof, M. and C. Noone (2018). Central bank digital currencies — Design principles and balance sheet implications. Technical report, Bank of England. Working Paper No. 725. ssrn.com/abstract=3180713.

Libra (2019). Libra white paper. https://libra.org/en-US/white-paper/.

Mancini-Griffoli, T., M. S. M. Peria, I. Agur, A. Ari, J. Kiff, A. Popescu, and C. Rochon (2018). Casting light on central bank digital currency. *IMF Staff Discussion Notes*. www.imf.org//~media/Files/Publications/SDN/2018/SDN1808.ashx.

Minsky, H. (1986). *Stabilizing an Unstable Economy*. Yale University Press.

Minsky, H. (1992). The financial instability hypothesis. Working Paper.

Morgan, J. (2019). J.P. Morgan creates digital coin for payments. https://www.jpmorgan.com/global/news/digital-coin-payments.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. bitcoin.org/bitcoin.pdf.

Roubini, N. (2018). Crypto is the mother of all scams and (now busted) bubbles while blockchain is the most over-hyped technology ever, no better than a spreadsheet/database. Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs On "Exploring the Crypto currency and Blockchain Ecosystem", www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf.

Schenk, C. R. (2013). The global gold market and the international monetary system. In S. Bott (Ed.), *The Global Gold Market and the International Monetary System from the late 19th Century to the Present Actors, Networks, Power*.

Schuster, E. (2018). The empty promise of cryptoassets and smart contracts. Presentation at personal.lse.ac.uk/schustee/crypto.html.

Valkenburgh, P. V. (2018). Testimony. Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs On "Exploring the Crypto currency and Blockchain Ecosystem" www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf.

Wall Street Journal (2018). Sorry, collectors, nobody wants your beanie babies anymore: Over two decades after the great beanie baby craze, speculators are back, hoping someone will finally buy their floppy collectibles.

World Bank (2018). Migration and development brief. Technical Report 29, World Bank. www.knomad.org/publication/migration-and-development-brief-29.

Zimmerman, P. (2019). Blockchain structure and cryptocurrency prices. https://sites.google.com/view/peter-zimmerman/research.