2016

Decentralized Banking: Monetary Technocracy in the Digital Age

Adam Hayes
University of Wisconsin-Madison, USA, ahayes8@wisc.edu

DECENTRALIZED BANKING: MONETARY TECHNOCRACY IN THE DIGITAL AGE

Completed Research

Hayes, Adam, University of Wisconsin-Madison, USA, ahayes8@wisc.edu

Abstract

Bitcoin has ushered in the age of blockchain-based digital currency systems. Secured by cryptography and computing power, and distributed across a decentralized network of anonymous nodes, these novel systems could potentially disrupt the way that monetary policy is administered – moving away from today's human-fallible central bankers and towards a technocratic, rules-based algorithmic approach. It can be argued that modern central banks have failed to stem macro-economic crises, and may have, in fact, exacerbated negative outcomes by incentivizing excessive risk-taking and moral hazard via unconventional monetary tools such as quantitative easing and negative interest rates. A central bank typically serves three primary functions: to issue and regulate the supply of money; to serve as clearinghouse for settlement of payments transactions; and to serve as lender of last resort. Could a digital currency system serve as a rational substitute for a central bank? This perspective paper examines that question, and then suggests that indeed it could be plausible. While Bitcoin in its current form will prove to be inadequate to function as monetary authority, I put forward what an operative case could resemble.

Keywords: Bitcoin, Digital currency, Blockchain, Monetary policy, Central banking

1 Introduction

1.1 Preamble

Fluid began to flow through plastic tubing, from one small tank to the next, as the hum of hydraulic pumps whirred in the background; the economists who had gathered at the London School of Economics quieted down. Graduate student Bill Phillips, who would later gain notoriety for describing the antithetical relationship between inflation and unemployment, stood at the controls of the six-and-a-half foot by five-foot analogue machine he had himself built. Phillips had arrived at the LSE from his home in New Zealand by way of Asia, where he was held prisoner in Java by the invading Japanese forces for three-and-a-half years. Now, in 1949, he adjusts the slider labeled 'tax rate,' sets various dials, and fiddles with the valve that will balance the budget; moments later The Phillips Machine gurgles and produces an estimate for the unemployment and interest rates, supposedly within a +/- 2% margin of error (Phillips & Leeson, 2000). Later dubbed MONIAC, it was an achievement in technology over fallible human minds in formulating monetary policy and informing central bankers to precisely what action to take upon observing the economy.

Since the Phillips Machine was first turned on, there has been a marked decline in the use of simple technocratic decision-making for monetary policy. Central banking has become much more nuanced, opaque, and complex as economies have grown larger and more intertwined. The nuance and complexity has also brought with it uncertainty regarding policy decisions, which manifests itself in financial markets in the form of volatility: Will the bank raise interest rates? By how much? When will they do it? Why was a specific word used in a statement by the Bank? Every last shade is scrutinized. Central bankers have shifted the conceptual basis of monetary affairs away from rules and standards such as gold or fixed exchange rates, and toward an evolving relationship with the public, rooted in sentiments and expectations (Holmes, 2009).

1.2 The Case for Following Rules: A Literature Review

The argument that central banks ought to be governed by rules, rather than by achieving a set of goals whatever way possible, has a great deal of support. If market participants incorrectly judge how interest rates will change, or if the central bank surprises the market by changing rates contrary to expectations, market fluctuations could increase. This applies to both how often rates are changed and by how much. In fact, empirical research has shown that too much tinkering with interest rates can produce negative economic outcomes (Kydland & Prescott, 1977).

In the United States, House Republicans have introduced a number bills that would require the Federal Reserve to follow a 'rule.' Recently, Congressman Jeb Hensarling (2014), who heads up the committee on finance which oversees the Federal Reserve, voiced concerns over the amount of leeway that exists in setting rates and the unanticipated consequences it can cause; he has urged central bankers to instead follow a simple set of explicit rules. On the campaign trail, Republican presidential candidate Ted Cruz has expressed his desire to implement an explicit monetary policy rule in a number of presidential debates in 2015 and 2016.

Political think-tanks have also voiced favor for a rules-based monetary policy. In February 2015, the Heritage Foundation commented that an explicit monetary policy rule will "greatly improve transparency and predictability," a belief echoed vociferously at the November 2015 monetary policy conference hosted by the Cato Institute.[1] From a policy perspective, a rules-based approach allows policymakers to evaluate the Bank's consistency with overt monetary policy or to other relevant legislation (Walsh, 2015). According to Walsh, this style may be contrasted with a looser "goals-based" approach, such as modern-day inflation targeting, whereby central bankers are evaluated on how well policy objectives are met, leaving much room for flexibility and creativity in achieving those goals.

Academics (*e.g*. Taylor & Williams, 2010) agree that simple rules-based decision-making is a robust method of implementing monetary policy, and point out evidence that historical experience has shown a set of simple rules works well in the real world. Taylor & Williams' studies show that relative macroeconomic performance has been *better* when central bank decisions were described by rules, and assert that such rules are not undermined by financial crises. Central bankers presently have quite a bit of discretion over how to set and implement policy. Problems tend to arise when the uncertainty surrounding these decisions (*e.g.* on setting interest rates) causes instability in financial markets (Deshmukh et al., 1983). If market participants incorrectly judge how and when interest rates will change, or if the central bank surprises the market by changing rates contrary to prevailing expectations, the potential for adverse volatility could increase. Kydland & Prescott (1977) suggest that a mandate to follow a strict set of rules could serve to reduce economic uncertainty.

An argument can be made that modern economies are too large and too complex for central banks to deviate from a basic set of rules (Walsh, 2015). How can central banks be expected to successfully manage economic stability via manipulations which can generate unpredictable results with unintended consequences? Prominent Austrian School economist Ludwig Von Mises (1953) argued that central banks actually cause economic instability by inducing an unsustainable expansion of bank credit. F.A. Hayek, a student of Mises, understood the need for central banks to regulate monetary policy as sort of a necessary evil lest a completely laissez-faire monetary system fall apart (White, 1999). More recently, former Federal Reserve Chairman Ben Bernanke (2000) has written extensively on how central bank policy exacerbated the

[1] http://www.heritage.org/research/reports/2015/02/why-congress-should-institute-rules-based-monetary-policy, http://www.cato.org/research/banking/rl-monetary-policy.html

Great Depression of 1929 by incorrectly raising interest rates instead of following the established rules, which would have caused them to act in the opposite manner.

Rule following also confers, inherently, independence to a monetary authority, which is a virtue that almost all can agree on. Political influence or other external pressures cannot in any way sway the absoluteness of an emotionless algorithm. Elected officials often face incentives to favor policies that promote short-run gains in output and employment, and voters are likely to remember a recent period of economic growth rather than consider the damaging long-run inflation or instability that policies could bring in the future. A central bank needs to be willing and able to make unpopular decisions and take actions that a politician could not. For instance, a government may seek a policy of high inflation in order to achieve monetary financing of deficits. Such a policy has often been the harbinger of collapse for national economies, from Argentina and Zimbabwe to Weimar Germany and Hungary (Minsky, 2015). The incentives for paying off debt with inflation are enticing. If a government owes *e.g.* a million dollars a day in fixed interest payments to creditors, it would be much easier if that nominal one million dollars were made to represent significantly less purchasing power. Inflation causes the value of a currency to drop, and that would be an attractive fix for out-of-control government obligations. An independent central bank would not be swayed by the size of a national debt and may not agree with the attractiveness of devaluing the currency through inflation. An autonomous monetary authority with a mandate for a stable inflation target serves as a safety mechanism.

To be sure, the argument for independence is not a new one: one of the founding fathers of modern economics, David Ricardo (1849), accused the Bank of England, which was already well over a hundred years old at the time, of bending to the whims of the throne. Ricardo proposed that a central bank be independent from political pressure in three important ways: with the power to create money separated from the power to decide how to spend it; with preventing a central bank from financing the State's budget; and with external accountability for its decision-making. Drawing on Ricardo, article 130 of the Maastricht Treaty of 1992 established the current basis for central bank independence for Europe, and has since been copied in practice by much of the developed world (Lastra, 2012).

While pneumatic tubes and mechanical dials are relics, sophisticated algorithms built into silicon and traversing optical fibre have replaced them. In this digital age, can cutting edge technology allow monetary policy decisions to function in a rationally consistent manner – and bring with it the potential for macro-stability that some level of certainty brings to markets? Digital currency systems today are obvious examples of technology that could potentially function as technocratic monetary authority. These are known generically as a 'cryptocurrencies', owing the name to the process of encryption that facilitates them, with the most well-established and widely used being Bitcoin. [2,3]

For simplicity, I take the position that the technology of today – and specifically blockchain technology – can, indeed, produce such a result. At the same time, I am not advocating that a digital currency is the ideal protocol for implementing a rules-based central bank policy. Rather, I take the broader position that a technology-driven rules-based system can exist within the framework of a decentralized, blockchain-based digital currency system, *even if* such a framework proves to be inferior to traditional centralized fiat banking in terms of effectiveness in the real world. It should be made clear that technology, in and of itself, is most likely insufficient to promote stability given a set of explicit rules. Algorithmic (*a.k.a.* high-frequency) trading firms are largely thought to have contributed to recent spurts of market volatility including "flash

[2] For convention, 'B'itcoin with a capital 'B' refers to the protocol, network, and system. 'b'itcoin with a small 'b' refers to the currency and units of that currency.

[3] Cryptocurrencies today are based on a *blockchain* data structure, which is essentially a distributed ledger system. The technical details of Bitcoin, cryptocurrencies and blockchain technology are beyond the scope of this paper.

crashes" (Kirilenko, et al. 2015), and have caused the public to distrust some market participants (see Michael Lewis' *Flash Boys*). Alternatively, proponents of algorithmic trading cite evidence that technology actually increases market efficiency and liquidity (Boehmer, et al. 2014); more empirical work is needed to resolve this emerging discussion. Regardless, there are bound to be both positives and negatives for any technological intervention – including the use of cryptocurrencies – and reducing the potential negatives should be paramount. Of course, many of the algorithms employed in high-frequency trading are kept secret and proprietary, so it is unclear whether failures caused by such systems are the result of the technology itself or manmade flaws in the code. Any algorithmic approach to central banking must be both robust and transparent so that any technical errors can be easily identified and corrected. Most blockchain implementations are fortunate to rely on open-source software code and feature a fully visible and auditable ledger of transactions.

This paper is intended to provide perspective on how a blockchain-based digital currency system could function as an independent, rule-following monetary authority, taking up some of the roles now played by central banks. Bitcoin was designed to be a global currency system, and yet there is scant little literature on its use as such (Selgin, 2015). In fact, examination of a digital currency system as de facto central bank has been quite overlooked by the Academy, and the purpose of this paper is to provide some initial insights and perspectives on the issue. In this paper, I have already made the case that a rules-following monetary policy is desirable. I next summarize what traditionally central banks undertake, and then develop a practical as well as a theoretical framework for a viable "decentralized" central bank based on a digital currency system. The hope is that it will be able to spark further research, both qualitative and quantitative, in to the subject and inform both academia as well as practitioners of macroeconomics and monetary policy.

2 Contemporary Central Banking

Before examining digital currency systems such as Bitcoin, it is important to understand three core functions of modern central banks: to issue and regulate the supply of money; to serve as clearinghouse for settlement of payments transactions; and to serve as lender of last resort.[4] Only then can we examine if and how a digital currency system could potentially take over some or all of these tasks.

2.1 Central Bank as Monetary Authority

The most visible function of a modern central bank is that of monetary authority – creating and managing the supply of currency that exists in an economy. An effective monetary authority regulates the creation and destruction of money in such a way as to promote overall macroeconomic stability (*i.e.* low inflation and/or full employment). Controlling the money supply is achieved using a set of policy tools that either directly or indirectly influence the supply or demand for currency.

Direct measures include open market operations (OMO), where the bank *creates* money by purchasing assets (typically high-quality domestic sovereign debt) in the open market using newly minted currency.[5] Unconventional monetary tools can also directly inject liquidity into markets. Quantitative easing (QE), credit easing, and asset stabilization are all examples of measures that have been tried for the first time since the Great Recession of 2008-2009. In QE, the central bank purchases riskier assets in the open market

[4] There are other functional roles of many central banks, such as custodian of cash or foreign currency reserves, and banker to the government that play a much smaller role from the perspective of a technocratic implementation using digital currency systems.

[5] Currency here refers to both physical or electronic funds.

such as mortgage-backed securities or corporate debt in exchange for new money. In November of 2008, the Federal Reserve initiated its first round of quantitative easing (QE1). The aim was to prop up the asset values of 'toxic' instruments in order to prevent a collapse of the financial system, which had massive exposure to what it mistakenly thought were high quality securities. Rated 'A' or similar by debt ratings agencies, investment banks and buy-side institutions alike found their balance sheets laden with mortgage backed securities, which became virtually worthless paper after the housing market collapsed and the financial markets crashed. The U.S. Federal Reserve Bank also did not stop at one round of quantitative easing. When $2.1 trillion worth of MBS purchases failed to keep asset prices aloft, QE2 was rolled out in November of 2010. And in December 2012, the Fed debuted QE3. To put all of this into perspective, in 2007, prior to the crisis, the Federal Reserve System held approximately $750 billion worth of Treasury securities on its balance sheet and virtually no privately issued assets (Joyce & Scott, 2012). By August, 2015, that number had swelled to nearly $2.5 trillion. Today, the Fed still maintains more than $1.7 trillion of mortgage securities on its books.[6]

Indirect measures for controlling the money supply involve mechanisms for fixing interest rates, and central bankers have great influence in using interest rates as a tool to accomplish their goals. Modern economies are intrinsically linked to interest rate levels, which affect everything from consumer spending and corporate investment to government debt levels and net exports. The 'risk-free' interest rate set by a central bank serves as the foundation upon which all other lending rates are built, and therefore it effectively dictates the cost of borrowing for all. In other words, interest rates help determine the 'price' of money (Woodford & Walsh, 2005).

High interest rate levels tend to discourage economic growth: when interest rates are high, loans become more costly and consumers will, in turn, buy less on credit. Some individual borrowers will be unable to service the higher cash flows needed to obtain a mortgage on a property that they could otherwise afford in a lower interest rate environment. Corporations may not issue bonds if they are uncertain that revenues generated from projects undertaken can sufficiently cover interest obligations, and thus risk default. Interest rates affect all financial markets in some way; equity, fixed income, derivatives, forex, and commodity markets are all highly dependent on this key figure.

Interest rate setting lends itself to a systematic approach (Clarida, Gali, & Gerler, 1998). The Taylor Rule, for example, informs central bankers how they should change nominal short-term interest rates in response to changes in inflation and GDP output. One version of the Rule is:

$$i_t = \pi_t + r_t^* + \alpha_\pi (\pi_t - \pi_t^*) + \alpha_y (y_t - y_t^*) \quad (1)$$

In this equation, i_t is the target short-term rate (e.g. the federal funds rate in the U.S.), π_t is the rate of inflation as measured by the GDP deflator, π_t^* is the target rate of inflation, r_t^* is the assumed equilibrium real interest rate (or neutral rate), y_t is the change in real GDP, and y_t^* is the change in potential GDP output, as determined by a linear trend. Taylor proposed that the sensitivities of each term (α) should be 0.50 (Orphanides & Wieland, 2008). Thus, given some macroeconomic data and observations, a certain lever of economic policy will be pulled to the specified setting.

Orphanides & Wieland (2008) find that, indeed, the Taylor Rule predominantly explains how the Federal Reserve Open Market Committee's (FOMC) decision-making has been characterized over the past few decades. *Even if* the individual decision makers or committees formulating monetary policy responses overtly deny that they are following such a hard and fast heuristic, the outcomes (incidentally or not) show

[6] http://www.federalreserve.gov/monetarypolicy/files/quarterly_balance_sheet_developments_report_201508.pdf

otherwise. As such, a viable digital currency system must be able to effectively create and regulate the supply of the monetary base in order to fulfill this purpose of a central bank.

2.2 Central Bank as Clearinghouse for Settlements

An often overlooked role of central banks, but one that is crucial for economic stability, is oversight of the payment system. Payment systems provide a vital piece of infrastructure in modern economies, allowing for the seamless buying and selling of both consumer and commercial goods and services. Faith that everyday transactions will settle and clear in a timely fashion underpins the value that people place on the usefulness of money. In other words, money is only useful in practice when there is a reliable and robust payments infrastructure with which to use it.

By virtue of its ability to regulate the money supply, the central bank stands at the center of this payment system infrastructure. That central place today often involves electronic interchange between various private payment systems and the central bank's own internal settlement account system. In the course of their own operations, central banks are usually users of payment systems and are accordingly exposed – both financially and practically – to glitches in their functioning.

Central banks have historically often been owners and operators of payment systems. In the United States, the Federal Reserve's automated clearinghouse (FedACH) is an electronic alternative to retail payments through cheques, and Fedwire is its wholesale securities and large value fund transfer service. In Europe, examples include the TARGET and TARGET2 systems (Trans-European Automated Real-time Gross Settlement Express Transfer System), which provide for the real-time payment and settlement of large value euro-denominated transactions, as well as debt settlement at central banks which is immediate and irreversible. In order for a digital currency platform to fulfill this function, it would need to integrate a mechanism to confirm and validate transactions and accommodate the volume of transactions generated in an economy.

2.3 Central Bank as Lender of Last Resort

When banks or other eligible institutions are experiencing financial difficulty, or are considered systematically risky or near collapse, the central bank can step in as lender of last resort to offer them loans when there is no other means of borrowing and whose failure to obtain credit would dramatically and negatively affect the economy. The lender of last resort functions not only to protect banking institutions, but also individuals who have funds deposited at those firms, preventing bank runs and stemming contagion if such a run were to take place.

In practice, when a financial company is forced to borrow from the central bank in such a manner, it signals to the market that an economic crisis may already be underway. As such, this facility, while crucial, is rarely invoked in everyday business.

Central banks, however, need not be the lender of last resort, and historically, private banks or syndicates have satisfied this duty. Before the Federal Reserve System was founded in the United States in 1913, private banks did indeed act as lender of last resort. For instance, The Suffolk Bank of Boston became lender of last resort during the financial panic of 1837-1839 (Rolnick, Smith and Weber 2000), staving off a more widespread depression. Later, during the panic of 1857 a policy committee of the New York Clearing House Association (NYCHA) allowed the issuance of clearing-house loan certificates, alleviating the crisis (Timberlake, 1984). Governments have also directly stepped in as "lender of last resort" on occasion by offering bailouts to the financial sector (among others), a recent example being the U.S. Treasury bailing out the banking (and automotive) sectors following the collapse of Lehman Brothers.

Critics have opposed the use of a lender of last resort altogether, claiming that it incentivizes excessive risk taking and moral hazard, since a bank knows it will be rescued in the event they collapse - they are more likely to perceive the potential consequences of risky actions to be less severe (Goodfriend & King 1988, Meltzer 2000, De Grauwe 2011).

Since it would be difficult for a digital currency system, as they exist today, to facilitate this particular role, I propose that if a blockchain-based monetary authority were to function, the job of lender of last resort would have to be either privatized or relegated to the state, or else eliminated entirely if the risk of moral hazard exceeds the risk of financial collapse.

3 Technocracy via "Decentralized Banking"

As described above, a central bank must effectively implement monetary policy, oversee settlement of transactions, and function as lender of last resort. I put forward that a digital currency system can, indeed, fulfill the first two roles, while allowing the third to be outsourced. A central bank may be able to leave the "every day" monetary policy in the hands of an automated set of rules governed by a digital currency regime and intervene hypothetically only if and when a crisis were to arise.

In the run-up to the latest episode of the Greek banking crisis, former finance minister Yanis Varoufakis surmised that his country could adopt Bitcoin (or some similar system) to function as a bridge currency to a new *drachma* if Greece did indeed leave the common euro currency (Mason, 2015). Quite correctly, Varoufakis has pointed out many shortcomings of Bitcoin itself as a practical long-run substitute for a nation's monetary system – such as its potential to be deflationary and its inability to react to external forces (Varoufakis, 2014). He has, however, gone on the record stating, "[a]lmost paradoxically, the technology of Bitcoin, if suitably adapted, can be employed profitably in the Eurozone as a weapon against deflation and a means of providing much needed leeway to fiscally stressed Eurozone member-states." The Phillips Machine is now consigned to a museum, but cutting edge information and communication technology (ICT) ought to allow an adherence to technocracy, free from human fallibility and corruptibility. Such a technology can be built upon a distributed network, such that no one individual or organization has sole control over the system, and yet it can still remain remarkably stable and robust without a single point of failure. While it will be made apparent that Bitcoin in its current form is likely a poor candidate to operate as an important global reserve currency, a system that builds off of its core technology – the *blockchain* – may in fact be a viable use case.

The Bank of England, Britain's central bank, has conducted research that finds clear macroeconomic benefits to implementing a central bank-backed digital currency (what they call a 'CBDC') based on blockchain technology (Barrdear & Kumhof, 2016). They find that such a currency based on distributed ledgers and that competes with bank deposits as a medium of exchange could permanently raise the GDP of a country by as much as 3% due to reductions in real interest rates, distortionary taxes, and transaction costs. They also suggest that a cryptocurrency monetary system crucially would contribute to the stabilization of the business cycle.

3.1 Bitcoin and its Inadequacies

The importance of Bitcoin as a proof-of-concept for blockchain technology and decentralized cryptocurrency systems cannot be understated. The advent of Bitcoin has shown that such a system can operate on a global scale, and has grown to command an aggregate value of more than $10.5 billion, with more than $150 million of notional value changing hands each day on its network.[7] Still, Bitcoin in its present form cannot function as a standalone monetary authority.

First, there is an ultimate limit of 21,000,000 bitcoins ever to be produced; once this amount has been mined, no new bitcoins will ever be created. Such an upper bound will likely create an artificial constraint that ultimately serves to make it an increasingly deflationary currency – each 'coin' will become progressively more valuable as demand for money increases and the supply cannot accommodate. To serve as an effective monetary authority, there cannot be an arbitrary limitation in place given the probability of increasing demand for money as an economy grows in population and in GDP. Of course, this technical limitation could be circumvented by using fractional amounts as the functional unit (say a nano-bitcoin) in everyday commerce, but having an unlimited potential supply is a more elegant solution. Empirical research has shown that granting *no* limit on ultimate supply seems to have no influence on a cryptocurrency's relative value (Hayes, 2015). Furthermore, cryptocurrencies do currently exist with no cap on the money supply, for example Peercoin, which has exhibited a fair amount of price stability despite its unlimited potential supply.

Second, Bitcoin's network cannot process more than approximately seven transactions per second (tps). While this may be sufficient to handle the amount of traffic that occurs on the Bitcoin economy internally, it pales in comparison to a nationwide economy. To put this in to perspective, VISA can handle upwards of fifty-six thousand transactions per second (although it averages only 2,000-4,000 tps on a typical day). PayPal, which is a much smaller network, could handle around 115 tps in 2014.[8] In order to handle the number of transactions actually occurring in an economy the system would need to handle many tens of thousands of tps on a consistent basis.

Third, and related to the problem with transactions per second, is the block size limitation. Currently, Bitcoin only allows for one megabyte of data to be stored in each block. The block size is already a matter of heated debate in the Bitcoin community, with little agreement between opposing sides. With an increase in transaction throughput, it would follow necessarily that the amount of data in each block would have to increase substantially (since each individual transaction carries with it some amount of data).

Fourth, and also similar to those above, Bitcoin transactions do not validate in real-time; rather they are confirmed only when a new block is mined, and that takes place by design once every ten minutes. Therefore, transactions will only be confirmed after a minimum of ten minutes, and likely more as many vendors prefer to have between three and six confirmations before accepting settlement. Having to wait for up to an hour is unacceptable for a large portion of daily financial transactions which must be confirmed and processed as immediately as possible. Distributed denial of service (DDoS) attacks on the network can also cause transaction speeds to drop below expectation, a problem not unique, however, to digital currency systems.

Fifth, Bitcoin addresses are *pseudonymous* rather than anonymous, meaning that the actual identities of those transacting on the network could be made known. This can be achieved by scraping data from the internet, or by analyzing transaction patterns of various address clusters on the blockchain (see, for example Tasca, Liu, & Hayes *forthcoming*). While certain regulations such as anti-money laundering (AML) laws and know-your-customer (KYC) are required of financial institutions, cash money is anonymous and should be so in order to protect the privacy of individuals.

Sixth, Bitcoin has a fixed rate of unit formation (one block every ten minutes), and a rule for arbitrarily reducing the amount of bitcoins found in each block approximately every four years.[9] Interestingly, a constant predetermined growth of the money supply does happen to have some theoretical

---

[7]blockchain.info/stats
[8] https://web.archive.org/web/20141226073503/https://www.paypal-media.com/about
[9] The current block reward is 12.5 BTC as over July 9, 2016

support. The so-called Friedman Rule (Friedman, 1948) proposes that the central bank should establish a fixed constant rate of growth for the money stock, and maintain that growth rate no matter what emerged from the state of the economy. Such a rule has some advantages: it is easy for the public to understand; the rate of inflation cannot take off toward plus (or minus) infinity; and, market-determined interest rates are free to fluctuate in response to changing economic conditions (Taylor, 1999). A fixed rule, however, critically ignores feedback from the economy and does not have the ability to adjust and smooth out the effects of macroeconomic changes.

There are other, less important factors that make Bitcoin inadequate to serve as “central bank,” such as the possibility of reversing transactions through a certain type of attack on the network (although the chances of this happening in reality are very remote).

3.2 Bitcoin and its Virtues

Despite its shortcomings Bitcoin has proven itself useful with respect to aspects of the concept of decentralized blockchain-based money. It has established that a conceptually digital money-form can be an acceptable store of value and a means of payment, both crucial features of any currency (Ingham, 1996) (Bamert, et al., 2013).

A currency needs to have societal trust in its security and fidelity. Bitcoin and related cryptocurrencies have exhibited recognition of so-called *trustless trust*. As a distributed network, Bitcoin transactions have *never* been compromised or hacked, and a bitcoin has *never* been forged or counterfeited.[10] A well-understood consensus mechanism amongst a network of anonymous and far-flung nodes has shown that a central authority or overseer is not a necessary requirement.

For a digital currency to operate as monetary authority, it must at the very least satisfy the requirements of being *money*. Aristotle, in ancient times, proposed four characteristics needed for something to be a “good form” of money (Smithin, 2002):[11]

1. *It must be durable*. Money must stand the test of time and the elements. It must not fade, corrode, or change through time.
2. *It must be portable*. Money must hold a high amount of 'worth' relative to its weight and size.
3. *It must be divisible.* Money should be relatively easy to separate and re-combine without affecting its fundamental characteristics, i.e. it should be 'fungible'.
4. *It must have intrinsic value.* This value of money should be independent of any other object and contained in the money itself.

Does Bitcoin fulfill these criteria? Taking Bitcoin as the general example, it is durable – its security is iron-clad and the existence of transactions is made permanent in the blockchain data structure without any degradation. It is portable – it can be accessed from any internet connected computer or mobile device. It is divisible – one bitcoin can be broken down to eight decimal places (the smallest such unit known as a *satoshi*), and it is fungible.

It *has* intrinsic value. This final point warrants some elaboration. Some have asserted that Bitcoin has no intrinsic value at all; that it has any market price is solely due to fleeting social popularity and the hope of speculators (Yermack 2013, Hanley 2013, Woo, et al. 2013, Polasik, et al. 2014). Hayes (2015a), however, has demonstrated that Bitcoin does in fact have some sort of intrinsic value, directly related to its cost of

10 Certain hacking events or theft have compromised services that use Bitcoin, such as the Mt. Gox exchange, but never Bitcoin itself.

[11] There are many alternative criteria with which to evaluate the ‘moneyness’ of something, but those arguments are beyond the scope of this essay and are unlikely to change the outcome of this analysis. To Aristotle, at least, a digital currency could reasonably satisfy all the requirements to be a “good” money.

production. In other words, its value behaves much like a commodity produced in a competitive market: electricity goes in and bitcoin comes out. If the average cost of production decreases, producers will offer their product in the market at lower and lower prices, in competition with each other, until marginal cost approaches marginal product (Hayes, 2015b). Therefore, it is appropriate to consider bitcoin more akin to a commodity form of money such as gold or silver than to fiat money. In fact, implementing Bitcoin as a national monetary system would be like a hard return to the gold standard in many ways.

In sum, Bitcoin has proven that it can function as a trusted form of money, and that its protocol can control its rate own rate of money supply – even if that controlled rate of supply is flawed from a practical perspective. And, it has shown that it can act as overseer and clearinghouse for its own transactions, even though its capacity is far too limited for everyday use. Those two features - to issue and regulate the supply of money and to serve as clearinghouse for payments – are two of the primary functions of an effective monetary authority that must be present for any viable alternative. That Bitcoin can serve these two roles, albeit inadequately, gives us a strong platform from which to build a more useful system.

3.3 A Workable "Decentralized Bank"

We have seen both the negatives and positives of Bitcoin, a truly decentralized, distributed system of digital currency. How can its protocol be improved upon to function as a true monetary authority for an economy; as a technocratic, rules-following "decentralized" central bank. First, I will address some fundamental macroeconomic issue such as using interest rates in a digital currency economy, then I will propose workable remedies to the limitations of Bitcoin.

One hurdle to overcome is that it would be technically quite difficult for a cryptocurrency system to directly set a target interest rate *per se*. Interest rate setting has become a hallmark of modern monetary policy, but there are other ways to influence the "price of money" with similar effect: *a digital currency could still achieve monetary policy goals by manipulating the rate of change to new money formation to similar effect.* There is a theoretical basis that changing the rate of money supply formation is a logical equivalent to changing the interest rate (Tobin, 1969). Interest rates and the quantity of money are intrinsically linked, in that increasing interest rates makes money more "expensive"; decreasing the supply of new money would have similar effect.

As we have seen above, the Friedman rule provided a theoretical foundation for a fixed, constant rate of new money supply. I have reasoned that this falls short in terms of Bitcoin's controlled supply of money. Fortunately, McCallum (1988) and Meltzer (1969) have augmented the constant growth rate formula with quantity-based rules that yield a dynamically changing growth rate of the monetary base contingent on widely available economic indicators. Notably, the McCallum Rule has been proposed as an alternative to the Taylor Rule, and moreover it has been empirically shown to perform better during crises (Benchimol & Fourçans, 2012).

The McCallum Rule can be expressed as follows to give a target for the monetary base in the next quarter:

$$m_{t+1} = m_r - \Delta v^*_{t-16} + 1.5(\Delta p_D + \Delta q^*) - 0.5\Delta x_{t-1} \qquad (2)$$

Where: m_r is the natural logarithm of the M0 monetary base at time t (in quarters); Δv^*_{t-16} is the average quarterly change in the velocity of M0 over a four-year period; Δp_D is the targeted rate of inflation expressed as the natural logarithm of the quarterly change in the price level; Δq^* is the long-run average quarterly increase in the natural logarithm of the real GDP; and Δx_{t-1} is the quarterly change in the natural logarithm of the nominal GDP from time t-1 to t. The lagged change in the velocity of money (Δv^*_{t-16}) is included to reflect long-lasting, permanent changes in the demand for the monetary base that occur because of technological developments or regulatory changes, and is not intended to reflect cyclical conditions (McCallum, 2000).

Such a rule would be much easier to implement within a digital currency system as regulator of monetary supply, since there would be no target interest rate in the traditional sense. The McCallum rule determines the optimal change in the monetary base given changes in GDP, inflation and the velocity of money. It is also intended to reflect long-lasting, permanent changes in the demand for the monetary base that occur because of technological developments or regulatory changes, and not intended to reflect cyclical conditions (McCallum, 2000).

If we take a monetary policy with an explicit inflation target (say 2.5% annually), one could easily construct a McCallum-like rule for a digital currency to follow that will change the rate of monetary formation from one-time period to the next. This can be achieved by adjusting how many monetary units are produced when each block of digital currency is created, or by changing the interval in which blocks of currency are produced. For example, if the economy is growing too rapidly, the rate of money formation should be reduced over the next time period. This would have a similar effect to raising interest rates in that it would make money scarcer on the margin. In practice, to promote stricter monetary policy the number of currency units in each block would be reduced over some interval (for example from 25 to 10 'coins' per block), and/or the time between block formation can be made longer (for example from 10 to 15 minutes), while to promote expansionary monetary policy the reverse would take place.

A potential consequence is given that a digital currency system like the one described herein relies on publicly available, anybody can deduce its next move(s). Market participants, rationally motivated by profit maximization, will be incentivized to act on any perceived mispricings observed in the market which differ from how the digital currency mechanism is expected to behave as it reigns in or bolsters the rate of money formation. Under a fairly reasonable no-arbitrage assumption, this will serve to increase market efficiency as it will greatly reduce the asymmetry of information that people can trade on.

Another structural-economic issue is that in a fractional reserve banking system, like the one we have today in much of the developed world, the central bank regulates so-called "high powered" money, also known as the monetary base, or M0. This base supply is then amplified through the financial system via lending and credit mechanisms, through a money *multiplier*. A digital currency system cannot amplify itself via fractional reserve banking, but it can still work nevertheless. "Full-reserve banking" (Fisher, 1935) is a proposed alternative whereby banks are required to keep the full amount of each depositor's funds in cash – or in our case in digital currency. This 100% reserve system was offered as a theoretical solution for the causes of the Great Depression, although no country has yet implemented this policy. Since World War II, there has been an increasing focus on fractional banking, however a number of economists have advocated for it in the past few decades across various schools of thoughts ranging from the Monetarists to the Austrians (Kotlikoff, 2009). Proponents of full-reserve banking argue that not only could such a monetary system function, but that it would also eliminate the risk of bank-runs, bailouts of the financial sector, and increase macroeconomic stability (Rothbard, 1974). In the wake of the 2008 financial crisis the idea was again revived, finding favor with Martin Wolf, chief economics commentator of the Financial Times, who has called for stripping banks of their right to create credit money. His argument that allowing banks to create money by lending out deposited funds is what is responsible for creating destabilizing credit bubbles and busts has also been echoed by a number of well-respected economists (Cochrane 2014, Krugman 2014, Polleit 2010). A digital currency-based technocratic monetary authority would likely have to operate in a 100% reserve environment.

Accounting for interest rate setting and fractional reserve banking, a new digital currency system can be put in place that also obviates many of Bitcoin's weaknesses. The number of transactions per second needs to be ramped up to accommodate an economy's worth of transactions. The block size, in turn, must be increased to allow for that throughput. The money supply potential will be unlimited, with no cap. Transactions will be confirmed as close to real-time as possible, and users will remain wholly anonymous. These suggestions are not all pie-in-the-sky. Without a doubt, there are a number of alternative cryptocurrencies (known as "altcoins") which individually attempt to solve one or more of these issues. For example, Dash (formerly Darkcoin) enables entirely anonymous transactions on its blockchain, with almost instant confirmations, and has plans to increase its block size limit.[12]

Such a rule-following digital currency could operate completely independent from outside influence. It would only need to incorporate publicly available macroeconomic data into its function as feedback in order to adjust the rate of new money formation in the succeeding periods. Not only would such a currency system be independent, but it could be made completely decentralized with no single authority or regulator in place. Like Bitcoin and other cryptocurrencies today, it could even exist across a decentralized network, democratizing the money-creation and transaction validation process.

A completely decentralized monetary system on a macro scale may seem wildly idealistic, but a digital currency can also exist across a distributed "permissioned" blockchain, where each node in the network is a known and trusted entity. Commercial banks and financial institutions could be obvious candidates to operate these nodes, and yet still operate with transparency with a well-understood consensus mechanism from the point of view of the population. Within a nation's borders, a permissioned blockchain is probably most appropriate as it can keep out foreign actors, can greatly reduce the need for expensive and resource consuming "mining" operations, and greatly increase the speed and capacity of transactions. An open blockchain, like Bitcoin, where all nodes are (for all intents and purposes) anonymous requires an energy-intensive consensus mechanism (mining, or proof-of-work) in order to prevent bad actors from undermining the system. Under a permissioned blockchain all nodes are vetted and known, making such an expensive and potentially limiting mechanism unnecessary. The system will need to have the capacity to handle the extremely large amount of transactions that are likely to occur each and every second across a nation's economy.

To sum up the above analysis, to provide the greatest chances for creating a viable digital currency system that could function as "central bank" it should: 1) have a potentially unlimited money supply; 2) be anonymous; 3) settle transactions in close to real-time; 4) follow rules based on dynamically adjusting the rate of new money formation; 5) have a mechanism to obtain feedback from the economy; 6) operate in a 100% reserve banking environment; and 7) operate as a permissioned blockchain with appropriate speed and capacity for all transactions in an economy.

4 Conclusion

Prof. Bennet T. McCallum has recently written a piece on Bitcoin which appeared in the journal for the Cato Institute (McCallum, 2015). In it, he acknowledges that Bitcoin in its present form could not satisfy the role of the monetary authority. For example, he reiterates that with a limit of 21 million bitcoins and an economy that grows each year, deflation will become a rampant problem. He does, however, generally propose the viability some alternative digital currency system, such as the one described in this paper, but he (perhaps ironically) fails to incorporate his own namesake Rule into his analysis.

With advances in blockchain technology now removed from the constraints of Bitcoin, it is possible

[12] https://www.dash.org/what-is-dash/

to encode *smart contracts*, algorithms that will act as a trusted enforcer of agreements. With deployable smart contracts, a blockchain-based monetary authority, which follows a McCallum-like rule for new money creation, might also engage freely in emergency measures such as open market operations to drastically increase or decrease the money supply when warranted. Such a crisis situation might be runaway inflation or deflation, a collapse in employment, or a period of recession. In these cases, the digital currency itself will act as a *decentralized autonomous organization* (DOA), making “decisions” on its own and interacting with real financial markets directly. Such a DOA Bank could feasibly buy up existing digital currency, and even destroy some of that money by sending it to unusable wallet addresses in order to quickly reduce the money supply outstanding. The DOA Bank could engage in purchases of foreign currencies in FOREX markets, as well as stabilize prices by purchasing bonds and equity in exchange for some of its stock of digital currency. Coupled with improvements in artificial intelligence and machine learning, an AI-enabled DOA Bank acting as monetary authority can truly be removed from government, central authorities, or the influence from policymakers and corporate lobbies.

Bitcoin has proven itself to be a fairly robust proof of concept use-case of blockchain technology in creating a global, decentralized digital currency and payments system. Bitcoin, however, is flawed in many ways if it is to be adopted as a true economic currency. Many of these issues can be rectified to make a more useful and dynamic digital currency, able to meet changes in supply and demand for money. If programmed as a decentralized autonomous organization, a blockchain-based monetary authority can even engage in its own emergency measures with effects similar to quantitative easing in order to stimulate a flagging economy or else halt rampant inflation. Doing so will enable a truly independent monetary authority to operate and perhaps even improve the prospects for economic stability and efficiency.

The conceptual framework outline above, I hope, will serve as a springboard for future analysis and research involving interdisciplinary collaboration in order to further the study of digital currency systems, blockchain technology, and its role as a viable, functional piece of the global macro-economy.

References

Bamert, Tobias, et al. "*Have a snack, pay with Bitcoins.*" Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on. IEEE, 2013.

Barrdear, John, and Michael Kumhof. *The macroeconomics of central bank issued digital currencies.* Bank of England Working Paper No. 605. London, England. 2016.

Benchimol, Jonathan, and André Fourçans. "*Money and risk in a DSGE framework: A Bayesian application to the Eurozone.*" Journal of Macroeconomics 34.1 (2012): 95-111.

Bernanke, Ben. *Essays on the Great Depression*. Princeton: Princeton University Press, 2000.

Boehmer, Ekkehart, Kingsley YL Fong, and Juan Julie Wu. "International evidence on algorithmic trading." AFA 2013 San Diego Meetings Paper. 2014.

Buiter, Willem H., and Nikolaos Panigirtzoglou. "*Overcoming the zero bound on nominal interest rates with negative interest on currency: gesell's solution*." The economic journal 113.490 (2003): 723-746.

Carlson, John, et al. "*Credit easing: a policy for a time of financial crisis.*" Economic Trends 11 (2009).

Clarida, Richard, Jordi Gali, and Mark Gertler. *Monetary policy rules and macroeconomic stability: evidence and some theory*. No. w6442. National Bureau of Economic Research, 1998.

Cochrane, John H. "*Toward a run-free financial system.*" Available at SSRN 2425883 (2014).

De Grauwe, P. (2011). "The European Central Bank: Lender of Last Resort in the Government Bond Markets?". *CESifo Working Paper Series* No. 3569: 11.

Deshmukh, S. D., Greenbaum, S. I., & Kanatas, G. (1983). Interest rate uncertainty and the financial intermediary's choice of exposure. *The Journal of Finance,* 38(1), 141-147.

Fisher, Irving. "100% money." (1935).

Friedman, Milton. "*A monetary and fiscal framework for economic stability*." The American Economic Review (1948): 245-264.

Goodfriend, M.; King, R. (May–June 1988). "Financial Deregulation, Monetary policy, and Central Banking". *Economic Review* 74 (3): 3–22.

Hanley, Brian P. T*he false premises and promises of Bitcoin*. ArXiv preprint arXiv:1312.2048 (2013)

Hayes, Adam. "What factors give cryptocurrencies their value: An empirical analysis." Available at SSRN 2579445 (2015).

Hayes, Adam S. "Cryptocurrency Value Formation: An empirical study leading to a cost of production model for valuing Bitcoin." *Telematics and Informatics* (2016).

Holmes, Douglas R. "*Economy of words.*" Cultural Anthropology 24.3 (2009): 381-419.

Ingham, Geffrey. "*Money is a social relation*." Review of Social Economy 54.4 (1996): 507-529.

Jones, Sarah. *Central Banks Load Up on Equities.* Bloomberg. April 25, 2013. http://www.bloomberg.com/news/articles/2013-04-24/central-banks-load-up-on-equities-as-low-rates-kill-bond-yields. Accessed August 4th, 2015.

Joyce, Michael, et al. "*Quantitative Easing and Unconventional Monetary Policy–an Introduction.*" The Economic Journal 122.564 (2012): F271-F288.

Kirilenko, Andrei A., et al. "The flash crash: The impact of high frequency trading on an electronic market." Available at SSRN 1686004 (2015).

Kotlikoff, Laurence J.; Leamer, Edward (April 23, 2009), "*A Banking System We Can Trust*" (PDF), Forbes.com

Krugman, Paul (April 26, 2014). "*Is A Banking Ban The Answer?*". New York Times.

Kydland, F. E., & Prescott, E. C. (1977). Rules rather than discretion: The inconsistency of optimal plans. *The Journal of Political Economy*, 473-491.

Lastra, R. M. (2012). The Evolution of the European Central Bank. *Fordham International Law Journal*, Spring.

McCallum, Bennet T. "*Robustness properties of a rule for monetary policy.*" Carnegie-Rochester conference series on public policy. Vol. 29. North-Holland, 1988.

McCallum, Bennett T. *Alternative monetary policy rules: a comparison with historical settings for the United States, the United Kingdom, and Japan*. No. w7725. National Bureau of Economic Research, 2000.

McCallum, Bennett T. "*The Bitcoin Revolution*." Cato Journal 35.2 (2015).

Meltzer, Allan H. "*Appropriate Indicators of Monetary Policy.*" (1969).

Meltzer; et al. (2000). "Report of the International Financial Institution Advisory Commission". *International Financial Institution Advisory commission*: 33.

Mishkin, Frederic S. *Is monetary policy effective during financial crises?*. No. w14678. National Bureau of Economic Research, 2009.

Orphanides, Athanasios, and Volker, Wieland. *"Economic projections and rules-of-thumb for monetary policy."* Vol (2008). Available at SSRN: http://ssrn.com/abstract=1141653

Phillips, Alban William Housego, and Robert Leeson. *AWH Phillips: Collected Works in Contemporary Perspective*. Cambridge University Press, 2000.

Polasik, Michal, et al. "*Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry*." Available at SSRN 2516754 (2014).

Polleit, Thorstein, "*The Faults of Fractional-Reserve Banking.",* Mises Daily, 2010. https://mises.org/library/faults-fractional-reserve-banking

Ricardo, David (1824), *Plan for the Establishment of a National Bank*, John Murray, London.

Rolnick, Arthur J., Bruce D. Smith, and Warren E. Weber. "The Suffolk Bank and the panic of 1837." *Federal Reserve Bank of Minneapolis. Quarterly Review-Federal Reserve Bank of Minneapolis*

24.2 (2000): 3.
Rothbard, Murray Newton. "*The case for a 100 percent gold dollar.*" Libertarian Review Press, 1974.
Selgin, George. "Synthetic commodity money." *Journal of Financial Stability* 17 (2015): 92-99.
Smaghi, Lorenzo Bini. "*Conventional and unconventional monetary policy.*" Speech at the Center for Monetary and Banking Studies, Geneva 28 (2009).
Smithin, John, ed. *What is money?.* Routledge, 2002.
Taylor, John B., and John C. Williams. *Simple and robust rules for monetary policy*. No. w15908. National Bureau of Economic Research, 2010.
Taylor, John B. "*A historical analysis of monetary policy rules."* Monetary policy rules. University of Chicago Press, 1999. 319-348.
Timberlake, R. (1984). "The Central Banking Role of Clearinghouse Associations". *Journal of Money, Credit and Banking*
Tobin, James. *"A general equilibrium approach to monetary theory*." Journal of money, credit and banking 1.1 (1969): 15-29.
Tobin, James. "*Keynesian models of recession and depression*." The American Economic Review (1975): 195-202.
Varoufakis, Yanis. *BITCOIN: A flawed currency blueprint with a potentially useful application for the Eurozone.* February 15, 2014. http://yanisvaroufakis.eu/2014/02/15/bitcoin-a-flawed-currency-blueprint-with-a-potentially-useful-application-for-the-eurozone/, Accessed August 5th, 2015.
Von Mises, Ludwig. *The theory of money and credit*. Ludwig von Mises Institute, 1953.
White, Lawrence H. "*Why Didn't Hayek Favor Laissez Faire in Banking?*." History of Political Economy 31.4; WIN (1999): 753-769.
Walsh, C. E. (2015). Goals and rules in central bank design (No. 5293). *CESifo Group Munich*.
Woo, David, et al. *Bitcoin: a first assessment*. FX and Rates (2013).
Woodford, Michael, and Carl E. Walsh. "*Interest and prices: Foundations of a theory of monetary policy*." (2005): 462-468.
Yermack, David. *Is Bitcoin a real currency? An economic appraisal.* No. w19747. National Bureau of Economic Research, 2013.