Tyler Kadow

ECN 497

11-28-2013

Is Bitcoin money (or can it become money) and how will it affect the economy?

Cryptocurrencies are a new phenomenon that is generally overlooked by the media. Their impact on the global economy could be staggering, due to their pseudonimity, low transaction costs, and the fact that central governments cannot manipulate the supply of a given cryptocurrency. On the other hand, cryptocurrencies could be in an economic bubble and could prove to be worthless, since they are not directly redeemable for any asset, nor are they backed by a central government. But what exactly is a cryptocurrency? Are cryptocurrencies money, and if not, can they become money? How would a Bitcoin standard, to single out the most widely-used cryptocurrency, compare to a commodity standard or a fiat standard? Should Bitcoin be regulated or, given its decentralized nature, can it be regulated?

The characteristics and history of money

Money is commonly considered to have three characteristics. First, it is a commonly accepted medium of exchange, an intermediary used to avoid the double coincidence of wants problem in a barter economy. Money is also a unit of account, meaning that it is a standard unit of measurement of value. The third characteristic is that it is a store of value, meaning that it can be saved and spent in the future.

It is very important to understand how money came about historically. Textbooks often state the flaws of barter economics without stating how monetary exchange came about. But success or failure for new currencies may be predictable if one looks at the development of money.

Austrian economist Carl Menger formed the classical explanation of money's development. Menger saw that money came about through a series of events by self-seeking individuals. Special knowledge of economics by any one trader was not necessary to create money. Inventing money was a totally organic event by willing traders in a free market (White 3).

First, we have the barter economy. Players in the marketplace trade goods or services for other goods or services without any financial intermediaries. Trading in this manner often creates a double coincidence of wants, where player one wants a good or service from player two, but player two does not want the goods or services produced by player one.

Imagine a large barter system with many players. The odds of a player being able to trade their one good, call it "A," directly for a specific desired good, call it "B," is very small. But if a player notices that most sellers of "B" tend to desire good "C," then that player will trade "A" for "C," not because she or he wants to consume good "C," but because she or he would like to eventually trade "C" for "B."

Illustrated above is Menger's concept of differing degrees of marketability. Perceptive players in this barter economy will trade their goods for a more highly

marketable good, since this good is more easily exchangeable. The more marketable good can then be easily exchanged for the goods that the players desire.

Since this requires two trades, trading “A” for “C” and then “C” for “B,” good “C” is advantageous only if:

1. Good “C” is more widely used than good “A,” and
2. Costs associated with buying, holding and reselling “C” are relatively small

Once more players in the marketplace are engaging in this indirect exchange, these players can begin to converge and agree upon a common medium of exchange. Over time, one medium emerges as the sole medium of exchange and becomes money.

There are some implications of this theory:

1. Central, coercive legislation is not required for money to emerge.
2. Sellers are reluctant to accept goods which are less marketable than money. This is true even if the good would be better money for the economy, should it become the medium of exchange.
3. The role of money as a “unit of account” also arises spontaneously. Self-interested sellers will post their prices in terms of the medium of exchange, since it is widely used in a monetary economy.

Some have proposed monetary systems wherein the roles of “medium of exchange” and “unit of account” are separated. Monetary economists Robert Greenfield and Leland Yeager proposed such a system, with a multi-commodity unit of account

that keeps the price level more “stable” than a commodity-standard. The money, however, would be issued by private banks and redeemable for an indexed quantity of anything more convenient.

Greenfield and Yeager consider their proposal a “lassiez-faire” proposal. However, the separation of the unit of account from the medium of exchange is not a natural market phenomenon and it would require government intervention to initiate their proposal. Also, a commodity standard uses claims for a commodity that are directly redeemable for that commodity, which ties the value of commodity claims to the value of the underlying commodity. The Greenfield-Yeager proposal does no such thing. Nothing ties the value of bundle “claims” to the value of the assets in that bundle. In fact, Norbert Schnadt and John Whittaker (1993) demonstrate how this proposal could fall apart.

As opposed to returning to par, should the sum of the value of the goods in the bundle become inequal to the value of the claims, arbitrage could make the system fail. If the price of the bundle rises but the price of one asset in the bundle remains unchanged, then banks with bundle-denominated liabilities have to pay those liabilities with a higher percentage of that asset. This could make the value of that asset fall even further, since people will want to obtain that asset at the banks for a lower price than in the marketplace. Then, banks must adjust the redemption rates further, and the process continues *ad infinitum* (White 242-43).

Natural monetary regimes occur due to the mutual self-interests of players in the marketplace. Money also involves a combination of the “unit of account” with the “medium of exchange.” A new money regime, such as cryptocurrencies, clearly has an

uphill battle to fight. Money is difficult to replace with another good because the network effects with the old money are not present with the new good.

Austrian economist Murray Rothbard described the plausibility of competing against a commodity standard with a private fiat currency: “But issuance and acceptance are two very different matters. No one will accept new currency tickets, as they well might new postal organizations or new computers. These names will not be chosen as currencies precisely because they have not been used as money, or for any other purpose, before.” (Rothbard 3)

However, the development of the Bitcoin economy has, so far, flown in the face of this conventional wisdom regarding money. Despite the fact that Bitcoin was never before used as a currency, the number of businesses that accept Bitcoin has grown dramatically, along with the value of Bitcoins. In order to understand why this may be, we need to go in depth into what Bitcoin is.

What are Bitcoins?

Bitcoin is a cryptocurrency, meaning that it is a decentralized, peer-to-peer digital currency. The peer-to-peer system is a network in which individuals act both as suppliers and consumers. Once a transaction is validated, it is permanently recorded in a public ledger known as the blockchain. New Bitcoins are issued to competing “miners.” The miners’ computers solve math problems that secure the system and the system rewards them with Bitcoins. Bitcoin uses a hash-based proof-of-work scheme to prevent double-spending of coins. To generate a block for the blockchain, Bitcoin peers

must find a nonce, an arbitrary number used only once in a cryptographic communication, that is less than a given target value when hashed with additional fields.

Bitcoin is not redeemable for another commodity and it is not backed by any government or legal entity. One of the first Bitcoin transactions ever was the purchasing of a pizza for 10000 BTC (Bitcoins) in 2010. As of October 30, 2013, at 5:06 GMT, the weighted average price for one Bitcoin was $211.86 at Mt. Gox, the largest Bitcoin exchange. The price rose to $885 as of November 27, 2013, at 4:16 am GMT.

The supply of Bitcoins increases at a decreasing rate, and will stop at 21 million. As of August 2013, approximately 11.5 million Bitcoins were in circulation. Bitcoins are divisible into eight decimal places. The smallest unit (0.00000001) is referred to as a Satoshi because Bitcoin was first introduced in 2009 by an unknown inventor who worked under the pseudonym “Satoshi Nakamoto,” which is a very common Japanese name.

Origins of Bitcoin

Nakamoto wrote a paper explaining how Bitcoin would work. In the introduction, he said, “Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. ... What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a

trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers" (Nakamoto 1). Nakamoto's goal with Bitcoin was to create an electronic payment system without any financial intermediaries necessary. Bitcoin was modeled after "b-money," a program proposed by Wei Dai, which had the explicit goal of allowing "untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts" (Dai).

Motivations behind Bitcoin and its Users

Wei Dai's paper often spoke of a concept called crypto-anarchism. Crypto-anarchism is the employment of cryptography to protect one's liberties, by evading the harassment and coercion of the government. Crypto-anarchists see political action to be futile in protecting themselves against government surveillance. Instead, they actively build counter economies and compete with the "white market." According to libertarian theorist Samuel E. Konkin, "The Counter-Economy is the sum of all non-aggressive Human Action which is forbidden by the State." Konkin's doctrine, called agorism, calls for a peaceful revolution by engaging in any nonaggressive action that one desires, even if the state forbids it.

Many anarchists, including Stefan Molyneux, Adam Kokesh, and Davi Barker, as well as many writers for the website "DailyAnarchist.com" have spoken or written positively about cryptocurrencies and their implications. Stefan Molyneux posted a video in which he stated "political power is money power. … It is the power to control money,

it is the power to print money, it is the power to issue I.O.U.'s, it is the power to sell bonds, [and] it is the power to have national debts. This is what political power fundamentally is these days. … Politicians have nothing to offer Bitcoin users. The only thing they can do is get in the way and make things difficult. … And so politicians aren't going to have anything to offer them. … Since political power is basically the control of money, political freedom is based on the liberty of money; is based on removing the power of money from the political classes. I would argue that, other than the internet, there's nothing more revolutionary, nothing with a greater capacity to enhance and expand human freedom than getting out of the pockets of the state, getting out of the currency of the state" (Molyneux). To Molyneux and other anarchists, Bitcoin is the key to freedom.

Kokesh and Molyneux accept donations for their podcasts in Bitcoins. Wikileaks, a nonprofit group, which publishes secret information, news leaks, and classified media from anonymous sources, also accepts Bitcoins for donations. Julian Assange, founder of Wikileaks, was on the cypherpunks mailing list, which desired to achieve libertarian ideals through cryptography. On December 3, 2010, PayPal issued a statement that they would no longer be processing donations for Wikileaks due to its "illegal activity" (Grinberg 162).

Recent Events Relating to Bitcoin

Bitcoin has a growing number of users. Since currencies are in a market with extreme network effects, the increased use of Bitcoin has caused its value to go up,

which has also encouraged more people to use Bitcoin, and so on. Far more people use Bitcoin than the crypto-anarchists of its origins.

The University of Nicosia, the largest private university in Cyprus with 5,000 students, has become the first accredited university to accept Bitcoin for payment of tuition and fees. UNic's Chief Financial Officer Dr. Christos Vlachos said, "We are acutely aware that digital currency is an inevitable technical development that will lead to significant innovation in online commerce, financial systems, international payments and remittances and global economic development" (Soper). Garrick Hileman, economic historian at the London School of Economics, commented on the move by UNic, stating, "The most fertile ground for Bitcoin is in places like Cyprus, Argentina, Iceland, China and other countries which have experienced significant financial disruptions and/or maintain strict financial controls" (Soper). Due to fairly recent events involving the 2007-2008 recession, the interests of the mainstream institutions in these countries fit well with what Bitcoin offers. UNic will likely see Bitcoin used by African students enrolled in online programs. A spokesperson for the university stated, "In certain countries, international payments are extremely cumbersome and given that certain students pay on a monthly installment plan, the transmission fees end up reaching 5-to-10 percent of their payments and being highly inconvenient" (Soper). Bitcoin alleviates this problem with its minimal transaction fees.

UNic is also the first university to offer a Master's Degree in Digital Currency. The program will be online and will start spring 2014. UNic also states on its website that, "As part of this path breaking initiative, UNic will propose to the Cyprus Government and the relevant stakeholders that Cyprus initiate the creation of a comprehensive

framework for developing Cyprus into a hub for Bitcoin trading, processing and banking.” The university sees Cyprus potentially becoming the London of Bitcoin. According to CoinDesk, “The Bitcoin price saw a massive surge to $266 in April during the financial crisis in Cyprus.” (Bonney). During this crisis, one proposal by the government of Cyprus was to remove 10% of everyone’s savings to raise the 5.8 billion Euros necessary to fulfill the bailout conditions by the European Central Bank. A pseudononymous currency would be effective for safeguarding one’s savings from such a tax.

Vancouver, Canada is currently home to the world’s first (and only) Bitcoin ATM. The company responsible is ‘Robocoin,’ a firm in Nevada. As described by ABC News, “The Robocoin kiosk first verifies customers' identities by scanning their palm prints. Customers can then feed cash into the machine to deposit as bitcoins, or withdraw bitcoins from their electronic wallet and get physical cash. Instead of waiting around a couple of days, the process only takes a couple of minutes” (Chang). CEO Jordan Kelley opted for the ATM to be debuted in Canada instead of America because, "The United States requires more licensing to operate … The barrier to entry isn't as low as it is in Canada” (Chang). The transaction limit per customer per day is $3,000. The company issued a statement to ABC News, saying "over one-third of customers were Bitcoin newcomers" (Chang). Robocoin’s ATM brings Bitcoin out of the heterodox and into the mainstream. To put it in Mengerian terms, the players in the market can converge and agree upon Bitcoin as a common medium of exchange.

Comparison to “e-gold”

E-gold was a digital gold currency operated by Gold & Silver Reserve Inc. Their website allowed users to open an account on their website and make transfers with other users on their website. Two glaring contrasts emerge between e-gold and Bitcoin: First, Bitcoins are not backed by gold or any other asset. Second, and perhaps more importantly, the e-gold system relied on a central body, whereas Bitcoin is decentralized. If anything were to happen to e-gold’s central body, the system would fall apart and the e-gold currency would become worthless.

Oncologist Douglass Jackson and attorney Barry Downey founded e-gold in 1996. Jackson once wrote “Many a paper currency has spun out of orbit in a calamitous trajectory.” According to wired.com, “at E-Gold’s peak, the currency would be backed by 3.8 metric tons of gold, valued at more than $85 million.” Jackson’s dream of a commodity currency backed by gold seemed to becoming true.

However, the Secret Service launched a secret investigation against a website called “Shadowcrew” and found that Eastern European criminals were stealing users’ passwords and passed that information to their clients all around the world. After the Secret Service raided the offices of Gold and Silver Reserve Inc, Jackson found that many online criminal groups were using his dream as a tool for money laundering.

In April 2007, the Justice Department had finished its four-year investigation and decided to indict Jackson on federal charges of money laundering, conspiracy and operating an unlicensed money transmitting business. Although attempts are being

made by Jackson and his colleagues to reopen the business, e-gold is effectively shut down.

The major problem with the e-gold system is the centralist nature of the system. If the website's owners fail to safeguard their system against money launderers and criminals, then people will lose faith in that system. Compromising the central body compromises the entire currency. Meanwhile, Bitcoin is a decentralized system. The federal government can investigate and indict the owner of Mt. Gox, the largest Bitcoin exchange and the currency would still survive.

Weaknesses of Bitcoin

Network effects for money are so strong in a free market that eventually, according to Menger's analysis of the evolution of money, only one currency is used as the medium of exchange and unit of account. People in the market need not be "convinced" that a specific good should be used as money. Instead, people use a good as money because that good has been agreed upon by all players in the market as the sole medium of exchange. Because of these network effects, new currencies will not be able to compete with the current money unless they provide unbelievable benefits to its users, compared to the current money. A thorough analysis of the weaknesses of Bitcoin is necessary to see what could prevent Bitcoin from overcoming the network effects of current monies.

Karame, Androulaki and Capkun (2012) analyzed the security of using Bitcoin for fast payments, focusing on double-spending attacks. Double-spending attacks are when an attacker spends a Bitcoin twice. Bitcoin prevents double spending by verifying each

transaction added to ensure that coins being spent have not already been used. If the time between the transfer of Bitcoins and providing the good/service is short, (less than 10 minutes) then there is a serious problem.

Karame et al's study showed an average time for a Bitcoin transaction to be confirmed is 10 minutes with a standard deviation of 15 minutes (Karame, Androulaki, and Capkun 2). What if an attacker bought a good/service from a vendor and tried to double-spend a Bitcoin on with the vendor and a separate Bitcoin address that is used by the attacker? The Bitcoins used could be sent to the separate address owned by the attacker instead of the legitimate vendor. If the transaction time is large, then there is no worry. The Bitcoins would not be received by the vendor and the vendor would not deliver the good or service. But if the transaction time is small, then using Bitcoins would not be practical for that business. Supermarkets and fast food restaurants are examples of business where the time between payment and delivery is very small. Security threats such as this pose a serious threat for Bitcoin to become a mainstream form of money.

There are solutions to this problem. One is to use a "listening period." Vendors can use a waiting period of a few seconds to see if the coins received are being double-spent in the system. However, the attacker can delay the false transmission by long enough for it to be unseen by the vendor. Then, the attacker still has a significant chance of pulling off the heist.

The vendor could insert a node into the Bitcoin network that she or he controls that relay to the vendor a double-spending attempt if either the vendor or the observer

receives the attacker's transaction. Karame et al's study also showed that around three observers would be necessary to ensure that at least one observer picks up a double-spending attempt.

Bitcoin users could develop an alert system to notify Bitcoin users of a double-spending attempt. This system would be unavoidable by the attacker and would also not incur more costs onto the vendor. The Bitcoin client is updated from time in case issues arise. Similar alert systems already exist with Bitcoin, but are not currently used. Significant changes to the Bitcoin client would not be necessary (Karame, Androulaki, and Capkun 11-12).

Set up with a decentralized network, Bitcoin cannot be completely taken down by the government, as e-gold was. Despite this inherent stability in the Bitcoin system, if the government attempts to crack down on Bitcoin users, then outsiders may be more reluctant to start using Bitcoin as money. Even if the system itself can withstand government blows, the value of Bitcoins could drop dramatically if Bitcoin is associated with criminality in the eyes of the public (Grinberg 177).

Bitcoin transactions are considered anonymous because nothing ties the addresses to the identities of the users. But people may post account numbers online in ways that connect them to their online identities. With some good statistical analysis and some identified accounts, the anonymity of the network could theoretically be undone. Much of Bitcoin's value comes from this perceived anonymity (referred to as pseudonymity) due to the philosophical beliefs of its core users. Compromising this feature could compromise most of Bitcoin's credibility as alternative money. Software

developers have proposed an extension to the Bitcoin payment network, called Zerocoin, which would add total anonymity to transaction, as opposed to pseudonymity. The extension would add zerocoins to the system, which would be redeemable for Bitcoins. This zerocoin/Bitcoin system would be designed in a way that it would be almost mathematically impossible to link where a Bitcoin began to where a Bitcoin ends.

Bitcoin vs Fiat Currencies, Commodity Currencies

Crypto-anarchists and other Bitcoin users are very skeptical of the benefits and long-term sustainability of fiat currencies. Ideologues in the Bitcoin community see fiat currencies as coercive, due to legal tender laws, and view inflation with a very negative connotation. Mainstream macroeconomists view steady inflation as necessary for the overall economy. Yet most Bitcoin users view inflation as theft, noting the combination of legal tender laws requiring people to accept the fiat currency with the loss of purchasing power due to inflation. Since fiat currencies are currently the norm, comparing the benefits of Bitcoin and fiat currency is essential. Comparing Bitcoins to commodity standards is also important, since there is plenty of history with commodity standards and only four years of Bitcoins.

Network effects in the market for money complicate this discussion. Even if Bitcoin is the superior currency for economic well-being, the network effects of fiat currencies may prove too strong. Also, Rothbard stated that people do not use money with names that have been not used as money before (Rothbard 3). Supposing the fiat currencies are unsustainable, governments can create a new fiat currency (or a commodity currency) with the same name as the old one and the market will (most

likely) accept the new currency as money. Rothbard made this statement to disprove the idea of privately competing fiat currencies issued centrally by a private bank. He had not envisioned a decentralized “fiat” currency, which may have different characteristics entirely that may overcome the network effects of current fiat currencies.

Resource Costs of Commodity Currency, Fiat Currency, and Cryptocurrency

Resource costs in currency include a stock and flow element. The stock cost is the cost of holding money and the flow costs are the costs of acquiring money. Lawrence White (1999) analyzed the resource costs of gold standards compared to fiat currency standards.

Milton Friedman (1953, 1960) estimated that the flow cost of a gold standard is 2.5 percent of GDP. This is a hefty sum, if it is accurate. He first derived this equation:

$$\Delta G \div Y = (\Delta G \div \Delta M) \times (\Delta M \div M) \times (M \div Y)$$

ΔG is the dollar value of the annual change in the stock of monetary gold, Y is the annual GDP, M denotes the M2 money stock, ΔM is the annual change in M2. Friedman used 0.625 for $(M \div Y)$ based off of information available in 1960. White found that number to be fairly accurate. White also found Friedman’s estimate of 4 percent for the ratio $(\Delta M \div M)$ to be accurate at the time (White 42-44).

The problem, however, lied in Friedman’s estimate of 100 percent for $(\Delta G \div \Delta M)$. This means that Friedman assumed banks would hold 100 of percent of gold against both demand liabilities and time deposits. Even proponents of 100 percent reserve gold standards, such as Murray Rothbard, limits the requirement for demand liabilities. White

calculated a more reasonable estimate for (ΔG ÷ ΔM) of 0.01914. This reduced the flow cost of gold standards to a 0.05 percent of GDP (White 46-47).

Rolnick and Weber (1994) found that annual inflation rates were 7 percent lower under a commodity standard than a fiat standard. “To put the same idea another way around, a fiat standard is not worth having … where it produces an inflation rate of 4 percent or more.” Four percent inflation puts the deadweight loss effects of a fiat standard above 0.05 percent of GDP. So, on average, fiat currency standards have higher resource costs than commodity standards (White 49).

Bitcoin could have a distinct advantage over both fiat and commodity standards in flow costs. Cryptocurrencies, unlike commodities or paper fiat currency, do not need to be maintained or replenished. Once all 21 million Bitcoins have been mined, no new Bitcoins can be mined and the flow costs of acquiring new Bitcoins will be zero.

Stock costs for Bitcoins are another story. Bitcoins do not have to be physically stored in a vault. But securing one’s Bitcoin wallet would be a must for maintaining a cryptocurrency economy. Low cost methods of securing one’s Bitcoins exist. Paper wallets include at least one public Bitcoin address and a corresponding private key which saves one’s Bitcoins from much of the risk of spyware, viruses and malware. These wallets can be generated online and printed for free. Thus, it appears that cryptocurrencies have an advantage over both fiat and commodity standards in resource costs.

Sustainability of Bitcoin, Fiat Currencies, Commodity Currencies

Fiat currencies are supported by government coercion and commodity standards are redeemable for commodities. Bitcoin is totally backed by the trust of its users. Which standards of currency are sustainable?

Americans began using dollars from the Federal Reserve in 1913. Some economists viewed the Federal Reserve as a necessary reaction to the Panic of 1907, in order to prevent bank runs. According to economist Hans-Hermann Hoppe, fractional reserve banking is responsible for bank runs. More specifically, allowing banks to hold less than 100 percent reserves will cause the money in circulation to increase without a withdraw in money substitutes from circulation (Hoppe 67). Credit expands, but this expansion of credit is fiduciary credit. Fiduciary credit is credit that "has been literally created out of thin air – without any corresponding sacrifice, in the form of non-consumed non-money goods, on the part of the creditor" (Hoppe 69). Fiduciary credit has disastrous consequences, according to Hoppe. "Misled by a lower interest rate, investors act as if savings had increased. They withdraw more of the presently available resources for investment projects, to be converted into future capital goods, than is warranted in light of actual savings" (Hoppe 69). This sets off a business cycle, where resources are misallocated, and leads to a recession. Inflation from fiat currencies also sets off this business cycle. Thus, whereas it was believed that the restrictive gold standard was responsible for the banking panics, it was in fact fiduciary credit from the legal impossibility of fractional reserve banking.

Voltaire once said "Paper money eventually returns to its intrinsic value - zero." Fiat money is a currency without redeemability in any asset. Fiat money is issued by government-run central banks and supported by government legislation, such as legal tender laws. Can governments who control fiat currencies be trusted to act independently of political pressures for the sake of monetary well-being?

The Reichsbank, the central bank of Germany, was politically independent in 1922 as a condition by the allies to allow temporary deferment of war reparation payments. By June 1922, the tax revenue to spending ratio had dramatically improved to 75 percent. In January 1923, the governments of France and Belgium had occupied the Ruhrgebiet in response to Germany's delinquency in its reparations payments. As explained by Thorsten Polleit, "The German government under chancellor Wilhelm Kuno called upon Ruhrgebiet workers to resist any orders from the invaders, promising the Reich would keep paying their wages. The Reichsbank began printing up new money by monetizing debt to keep the government liquid for making up tax-shortfalls and paying wages, social transfers, and subsidies" (Polleit).

The quantity of papermarks rose from 8.610 billion in May 1923 to 400 quintillion in November 1923. Unemployment would hit 28.2 percent in December of that year. By November 15, 1923, the rentemark was formed by the Reichsbank and the papermark was no more. Despite political independence, the central bank decided that inflating the currency was their most viable option.

It seems that gold standards are inherently stable monetary regimes and fiat currencies controlled by the government will eventually become worthless. But how

would a Bitcoin standard behave; like a commodity or a fiat standard? A conclusion drawn by Thorsten Polleit from the history of the papermark is, “Unbacked paper money is political money and as such it is a disruptive element in a system of free markets” (Polleit). There seems to be a vital nuance missing in Polleit’s conclusion. Namely, the unbacked paper currency in question was centrally controlled. One modern, real-world example existed in which an unbacked currency was relatively successful.

The Case of the Iraqi Swiss Dinar

The Iraqi Swiss Dinar was the currency of Iraq up until the 1990 Gulf War. It was “Swiss” because the printing plates were produced in Switzerland, and the currency was then printed in the United Kingdom. United Nations resolutions imposed sanctions on Iraq during the war, prohibiting importing of the “Swiss” dinar notes. Iraq then disowned the notes and began printing their own new currency. Kurdish regions in northern Iraq continued to use the Swiss notes, however (Grinberg 174).

Despite being unbacked by either a military or a commodity, the Swiss dinars maintained a stable trading value. Hussein’s central bank had begun massive inflationary policies with the new “Saddam” dinars. Counterfeiting was also a massive problem with the Saddam dinars, due to their primitive note-printing technology. Meanwhile, the Swiss dinars were more difficult to counterfeit due to the high-quality Swiss technology used to print the notes, even though no central authority existed to fight against counterfeiting the Swiss dinars. While the value of the Swiss dinars actually went up slightly, due to torn notes, Saddam dinars were undergoing a hyperinflationary period.

After the 2003 Gulf War, Swiss dinars were traded in for a new dinar note issued by Iraq's central bank at a rate of 150 new dinars for every one Swiss dinar. Only after military intervention by the U.S. and its allies did the Kurds trade in their unbacked currency. Although Polleit's conclusion still holds for the Saddam dinars, it does not necessarily hold for the Swiss dinars used in the northern Kurdish regions. Swiss dinars maintained their value in the eyes of the Iraqi Kurds because they were not, and could not be hyperinflated into oblivion, along with the already-existing network effects of the currency. Whether the Kurds would have continued to use the Swiss dinars is uncertain.

Bitcoin users should be encouraged by the fact that the Swiss dinar notes were valued by consumers despite, and partly due to, not being centrally controlled. Swiss dinars also proved to be more secure from counterfeiting than Saddam dinars. Bitcoins, can only be counterfeited if over 50 percent of the computing power of the Bitcoin network is controlled by a malevolent miner or group of miners. On August 15, over 184 billion Bitcoins were generated in a transaction. But the transaction was spotted within hours and erased from the transaction log. An updated version of the Bitcoin protocol was made to prevent counterfeiting from happening again. So far, no other attempt to generate Bitcoins has been successful.

The Philosophical Argument for Bitcoin (and Against Government Coercion in Money)

Philosophy seems out of place in an economics paper. However, one purpose of economics is to discover how to allocate resources such that utility is maximized. Utility is defined in economics as both an issue of usefulness and happiness. Therefore, when

comparing a currency used voluntarily to money used because of coercive legislation, philosophy may be important to explore.

Crypto-anarchism is a technological application of anarcho-capitalism. The foundation of the philosophy of anarcho-capitalism is the non-aggression principle; the assertion that aggression is inherently illegitimate. Any acts of force or fraud are illegitimate under NAP if committed against a non-aggressive individual. Non-aggression does not exclude violence used in self-defense or defense of others.

Disagreements exist amongst anarcho-capitalists as to how the NAP applies to abortion, intellectual property, and the treatment of non-humans. However, anarcho-capitalists view the government as immoral under the NAP. Taxation is an involuntary payment by citizens to fund the government. Unlike firms in a free market, where people have the choice to not purchase goods or services which they do not desire, government only maintains itself by the threat of force.

Some accept taxation because due to the free-rider problem, funds might not be obtainable in the voluntary free market for protection from aggression of a greater severity. This is, therefore, a utilitarian stance that as long as the force of taxation is used by the government to protect greater threats to property rights than the government imposes, it is an acceptable violation of NAP.

Problems arise with this argument. One is that it assumes perfect information exists that the economic consequences of the force of government is less than those consequences which the government prevents. Another problem with this argument is that the whole free-rider concept may be entirely wrong. Just because others receive

benefits from purchasing private defense does not mean that no one would purchase it. People purchase goods and services to the extent that it benefits them. Whether or not it benefits others indirectly does not change the fact that the purchaser receives a benefit from the good.

Americans began using dollars from the Federal Reserve for the same reason that northern Kurds in Iraq began using the new Iraqi dinars in 2003; government compulsion. Fiduciary credit, created both by fractional reserve banking and inflationary policies, sets off a business cycle, where resources are misallocated, and leads to a recession. Hoppe also notes that fractional reserve banking leads to a "legal impossibility" (Hoppe 67). It places the ownership of the same resource in the hands of both the time depositor and the borrower. But the key to private property is that it is excludable, meaning that fractional reserve banking is a form of fraud, which violates the non-aggression principle. Furthermore, a central bank creates fiduciary credit whenever it pursues an inflationary policy. So not only does a central bank not serve a utilitarian purpose, it is also contrary to NAP.

Legal Issues Regarding Bitcoin

Bitcoin's decentralized nature can protect it against government crackdowns. But not all of its users hold the same philosophies as the crypto-anarchists who developed and support Bitcoin. Many are reluctant to use Bitcoin because of its questionable legal status. On November 19, 2013, the United States Senate held a hearing called "The Present and Future Impact of Virtual Currency" to further understand Bitcoin and

cryptocurrencies in general. Lawmakers could bring Bitcoin into the mainstream by deciding how to define and regulate, or attempt to regulate, cryptocurrencies.

Two federal statutes limit citizens from creating private currencies: the Stamp Payments Act of 1862 and the federal counterfeiting statutes. Section 2 of the Stamp Payments Act says, “Whoever makes, issues, circulates, or pays out any note, check, memorandum, token, or other obligation for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States, shall be fined under this title or imprisoned not more than six months, or both.” (Grinberg 185). Multiple legal precedents have shown the act will not apply to a good that “(1) circulates in a limited area, (2) is redeemable only in goods, (3) does not resemble official U.S. currency and is otherwise unlikely to compete with small denominations of U.S. currency, or (4) is a commercial check (such as a customer might make out to a store to buy something worth less than $1)” (Grinberg 185).

Other virtual currencies like Linden Dollars and World of Warcraft Gold fall outside the Act since they are not intended to circulate as money and used in lieu of U.S. dollars. “Community currencies” also fall outside of the Act since they are intended to circulate only locally.

Some believe Bitcoin is likely to fall under the Act. However, the Supreme Court made a purpose-based analysis of the Stamp Payments act in the case *Unites States v. Van Auken,* in which the court decided that the goal of the act was to “secure, as far as possible, the field for [official small currency], without competition from any quarter.” (Grinberg 184). The goal was preventing private competition with U.S. coins. It can be

said that Bitcoin mostly competes with credit cards and PayPal and checks, since it is rarely used face to face, like U.S. coins.

Another issue with Bitcoin falling under the Stamp Payments act is that the law is over 150 years old. Pragmatically, trying to cover digital currencies under the language of a law that was passed when telephones were an emerging technology may not prove fruitful, especially since “there has been no published court opinion interpreting the Act since 1899” (Grinberg 190).

Bernard von NotHaus, distributor of gold-backed Liberty Dollars, was indicted in 2009 and convicted in March 2011. NotHaus believed that his arrest was political in nature, a means of sending a message that competition with U.S. dollars will not be tolerated. However, the main focus of the trial was his attempt to spend Liberty Dollars into regular circulation. NotHaus was also selling metal currencies for a higher price than the value of their metal content (Grinberg 191-93). It seems clear that the issue here is one of fraud and counterfeiting, not a political witch-hunt to shun issuers of private currency. Since Bitcoin users make no such attempts to defraud people, and since Bitcoins are digital and cannot be made to look like U.S. coins or currency, Bitcoin also seems to be safe from the federal counterfeiting statutes.

Anti-Money laundering laws could be a legal Achilles heel for Bitcoin. The Bank Secrecy Act requires otherwise unregulated financial instruments to register with the government, report certain transactions, implement certain procedures, etc. And the Money Laundering Control Act of 1986 criminalizes money laundering. E-gold was found guilty of not properly monitoring for money laundering, which was a rampant

problem for the business. The BSA and MCLA may pose risks for anyone involved in the Bitcoin community, even individual miners. This legal gray area created by the BSA and the MLCA could hamper Bitcoin's legitimacy as money.

What Can the Government Do?

Cracking down on individual businesses is difficult enough for the government. Tracing the actions of money launderers, tax cheaters, and other criminals is no easy matter. If Bitcoin were to be more widely used, how could the government possibly trace the finances of all Americans, or even most? Collecting income taxes would become a nightmare. Tracing of banking information would no longer be possible if everyone began to store their money in Bitcoin on a digital wallet. Its pseudononymous nature means that Bitcoins are not connected to one's personal identity in any way.

Governments would then have a few options available:

1.) Shut down Bitcoin

Shutting down Bitcoin seems possible, since controlling over fifty percent of its computing power would give one total control over the currency. In the footnotes of Grinberg's paper on Bitcoin, he notes that the price tag to control the majority of the networks processing power is $600,000. However, this paper was written in 2011, and since the difficulty of the math problems for generating new Bitcoins continues to go up, the money needed is far higher by now.

Neil Fincham wrote a slightly more recent piece about the possibility of shutting down Bitcoin, "… for a small price of $20 million USD or so and an ongoing cost of

about $1 million per month … you could paralyze bitcoin. Note: You could also use the above equipment to mine about $50,000 USD a day or $1.5 million a month." This article was written in 2012, so these costs are also outdated and are much higher today. A humorous, yet important line in the article also points out problems with storage and other factors, "I am unsure of even where to start to estimate a place to put this all, internet connections or cooling cost but I am sure you can find something, perhaps an old nuclear reactor or something (Even better, inside a dormant volcano, you could have sharks with lasers on their heads)" (Fincham)

With the government taking in $2.8 trillion in revenue in 2013, the costs would not be insurmountable. However, it would likely not be politically feasible to spend millions of dollars to paralyze (not even shut down) an emerging technology with unknown positive capabilities. Furthermore, spending all this money just to paralyze one cryptocurrency, when there are more out in the market, would prove very futile.

2.) Make Bitcoin illegal under certain circumstances

Making cryptocurrencies illegal under certain circumstances may actually be more feasible than shutting them down. If governments forbade employers from paying employees in anything other than U.S. dollars, perhaps the threats imposed on the government's bottom line by Bitcoin would decrease. Income taxes would not be avoidable by using cryptocurrency. However, proving that people are paid in a currency which cannot be traced back to the original owner would probably be fruitless.

3.) Accept not being able to collect certain taxes anymore

As Stefan Molyneux stated before, the government does not have anything to offer Bitcoin users except further obstacles. One thing the government could do would be to accept that certain forms of taxation will no longer be viable. Tariffs will still be viable, since the goods have to physically arrive in the country. It still would not be difficult for governments to tax imports.

If the federal government was actually willing to relinquish income or sales taxes, then a major scaling back of government spending would be necessary to prevent budget deficits from exploding. Also, if more people use cryptocurrencies and less people use U.S. dollars; this could lower the value of the dollar. Consequently, potential creditors to the U.S. government could be reluctant to accept debt denominated in U.S. dollars due to its falling value.

Bitcoin's legal future remains uncertain. It is wise for the government to look into digital currencies. But the fact that it took them four years to assemble a hearing on new money technologies after Bitcoin was released into the market could be a troubling sign if one wants swift answers from the government. Inaction on their part to designate how it is to be regulated could hamper the credibility of the government. On the other hand, if the "Bitcoin community" begins to thrive without government action, the government's credibility could also be hampered.

Conclusion

Money was not an invention of the state. Rather, certain goods with higher degrees of marketability were traded in the marketplace until one good emerged to be the medium of exchange in the market. Due to the extreme network effects in the market for money, the current medium of exchange is difficult to replace, even if a new good would be more useful as money. Murray Rothbard suggested that if legal tender laws were lifted, new monies would not catch on, due to players in the market being unfamiliar with the new money. However, Rothbard wrote this in a time before the concept of a totally decentralized electronic currency.

Now in our current world, a certain currency may be the sole source of money in one nation's market. But there are actually dozens of monies in our current world market. Technically, the world has yet to converge onto one currency as the world's medium of exchange. Bitcoin has the technological capabilities to become that world medium of exchange.

Flaws still exist in the Bitcoin protocol that makes it inconvenient to use in fast transactions, but the protocol can be easily adjusted to remedy this problem and alert merchants of potential double-spending threats.

From Bitcoin ATM's to Master's degrees in digital currency, cryptocurrency is slowly making its way into the mainstream of finance. But will Bitcoin be considered money, or will it be used as a meta-currency, solely for quick transfers between different currencies?

Having no backing by commodities or government decree does not necessarily mean that Bitcoin has no potential to become money. In fact, the monies that function best throughout history have been those most free from government intervention. One example, the Iraqi Swiss Dinar, also shows that people will accept notes without government or commodity backing as money.

Cryptocurrencies operate in a legal gray zone, with no certainty as to how Bitcoin is to be treated by lawmakers, or under what circumstances anti-money laundering laws apply to individual users. Many articles (including this one) discuss how government decrees and regulation can bring Bitcoin into the mainstream of finance. But if we truly want Bitcoin to reach its full potential, as money, the last thing this technology needs is government regulation. Nonetheless, acknowledgement by lawmakers as to what kind of financial instrument Bitcoin is will make businesses less reluctant to adopt it.

One thing seems certain; even if the government finds Bitcoins and their pseudonimity to be a threat to law and order, lawmakers may be incapable of bringing Bitcoin to its knees without incurring serious costs. Bitcoin wallet addresses are not connected to the identity of the wallet holder in any way.

More than its political or economic impacts may be the philosophical impacts of Bitcoin. With a quick, digital pseudononymous money to use, buyers and sellers who were once unable to act in their own interests due to government coercion may finally be able to break their chains. Thus, a new world wherein all peoples are allowed to act in their own nonaggressive interests may be possible, if not inevitable.

Bibliography

Grinberg, Reuben. "Bitcoin: An Innovative Alternative Digital Currency." (2011): n. Web. 27 Nov. 2013. <http://www.meansofexchange.com/wp-content/uploads/2013/07/Bitcoin-Innovative-Alternative.pdf>.

Rothbard, Murray. "The Case for a Genuine Gold Dollar." (1992): Print. <http://mises.org/rothbard/genuine.pdf>.

Hoppe, Hans-Hermann. "How is Fiat Money Possible? - or, The Devolution of Money and Credit." Review of Austrian Economics. 7.2 (1994): 49-74. Print.

Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin." International Association for Cryptologic Research. (2012): 1-17. Print. <http://eprint.iacr.org/2012/248.pdf>.

White, Lawrence H. The Theory of Monetary Institutions. Malden: Blackwell Publishers Inc., 1999. Print.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." (2009): n. page. Print. <http://bitcoin.org/bitcoin.pdf>.

Zetter, Kim. "Bullion and Bandits: The Improbable Rise and Fall of E-Gold." Wired. (2009): n. page. Print. <http://www.wired.com/threatlevel/2009/06/e-gold/>.

Demand for Money: Theoretical Studies: by Bennett T. McCallum and Marvin S. Goodfriend

Fincham, Neil. "Want to destroy bitcoin? I am going to tell you how.." MineForeman (2012): n.pag. Web. 27 Nov 2013. <http://mineforeman.com/2012/12/10/want-to-destroy-bitcoin-i-am-going-to-tell-you-how/>.

Polleit, Thorsten. "90 Years Ago: The End of German Hyperinflation." Ludwig von Mises Institute (2013): n.pag. Web. 27 Nov 2013. <http://mises.org/daily/6588/90-Years-Ago-The-End-of-German-Hyperinflation>.

Dai, Wei. n. page. Print. <http://www.weidai.com/bmoney.txt>.

Molyneux, Stefan, auth. "The Truth About Bitcoin." Freedomain Radio, 27 Sep 2013. web. 27 Nov 2013. <http://www.youtube.com/watch?v=w4HGVJjqDVk>.

Soper, Taylor. "This university is the first in the world to accept Bitcoin for tuition." Geek Wire. (2013): n. page. Print. <http://www.geekwire.com/2013/cyprusbased-school-university-accept-bitcoin-tuition/>.

Bonney, Jeremy. "University of Nicosia in Cyprus Becomes First in the World to Accept Bitcoin." CoinDesk. 21 Nov 2013: n. page. Print. <http://www.coindesk.com/university-cyprus-first-accept-bitcoin/>.

Chang, John M. "First Bitcoin ATM Installed in Vancouver Coffee Shop." ABC News. (2013): n. page. Print. <http://abcnews.go.com/Technology/bitcoin-atm-conducts-10000-worth-transactions-day/story?id=20730762>.