

Bitcoin: Financial Innovation Burgeoning into a New Form of Stable and Convenient Money

Tom Sykora

I. Introduction

The ancient Chinese curse, “May you live in interesting times,” certainly seems to have been cast on the monetary and financial systems of the world, especially in the last 100 years. In that period, economies have experienced historic downturns such as the Great Depression and the recent financial crisis of 2007-09. Moreover, many monetary, fiscal and financial innovations have become widespread such as fiat currencies, fractional reserve banking, Keynesian business cycle smoothing and the use of derivatives. On the tail end of the most recent financial crisis, a new financial innovation has been created that represents a truly novel approach to the definition of money; namely, Bitcoin.

In this paper, I argue that Bitcoin has the potential to become a dominant electronic currency to facilitate international trade and payment. The arguments put forth cover the benefits of Bitcoin as well as its properties. First, I show that Bitcoin, as an electronic payment system, has distinct advantages over current payment systems such as bank wires, debit/credit cards, cheques, and to some degree, even cash. Second, as a result of Bitcoin’s inherent algorithm to stabilize the money supply, it is not prone to inflation, especially when compared to some hyperinflationary episodes within the last century. Third, I demonstrate that Bitcoin has the ability to satisfy the three properties of money. Finally, I discuss some potential risks associated with broad adoption of Bitcoin as a currency in the long run.

II. The Rise of a New Currency

Bitcoin is a recent technological innovation designed as a decentralized, cyber-crypto-currency. There is no central authority required to issue and maintain the currency, since the Bitcoin network itself, with its distributed nodes, performs the task of creating new Bitcoins (called “mining”) and verifying all transactions that have occurred. The Bitcoin Protocol was designed to prevent double spending without the use of a trusted third-party such as a central bank. Essentially, transactions are encrypted with a public-private key authentication system and verification is performed via “forced work”, meaning that a certain amount of computer CPU cycles must be performed in order to generate the correct hash (a numeric value) that is then broadcast to the entire network. Once a transaction is verified, it becomes part of the transaction ledger, called the block chain. The larger the block chain, the more certain the nodes are that the transactions contained within the chain are valid, and consequently, the same owner is prevented from

spending the same Bitcoins twice (Nakamoto 2008).

Bitcoin was developed as an open-source project so that a community of software developers would have the ability to closely monitor the source code. This monitoring greatly reduces the probability of covert insertion of malicious code, “Indeed, as cybercrime goes, Bitcoin may be safer than traditional financial institutions, which are often on the receiving end of such attacks”.¹ In addition to the availability of the project to all software developers, participation in the Bitcoin network is open to anybody with a computer, some software and an Internet connection. This represents a stark contrast to the system of debit and credit cards, which require authorization from a financial institution.

Since the first Bitcoins were mined in early 2009, the relative price of Bitcoins to U.S. dollars and the number of transactions have increased vastly (Figures 1 and 2 show the meteoric rise of both, respectively). Bitcoins are used as payment for online services such as Web development as well as real world commerce through venues such as restaurants.²

To use Bitcoins, a user requires a Bitcoin wallet, which is simply some software that runs on a user's computer or exists on some trusted service provider's servers. Each wallet can contain one or more unique addresses that are available to receive Bitcoins; superfluous addresses enhance a user's anonymity. After the wallet is funded,³ a user is then able to trade his Bitcoins for goods and services by sending his Bitcoins to a recipient's address. Once confirmed by the Bitcoin network, the Bitcoins will then exist in the recipient's wallet.

Above, I have described most of the rudimentary technical details of Bitcoin and its usage. Next, the focus shifts to an economic examination.

III. Bitcoin as a Major Electronic Currency

III.1 Superior Electronic Payment System

Modern financial transactions are settled in many ways. Today, the most common method in the developed world is electronic funds transfers that can take many forms including bank wires, debit and credit card transactions. Paper notes such as cheques, bank drafts and, of course, cash are another popular form of settlement. There are advantages and disadvantages involved with each of the aforementioned forms of payment. While all of these methods are distinct, they share one common attribute: issuance of the underlying currency by a central authority (most commonly a central bank). Moreover, once cash is in circulation, every one of these payment forms (aside

¹ “Virtual Currencies.” Last updated June 15, 2011.
<http://www.economist.com/blogs/babbage/2011/06/virtual-currency>

² For a listing of current locations accepting Bitcoin as payment see <https://en.bitcoin.it/wiki/Trade>.

³ There are several ways to fund a wallet such as using an exchange provider that converts fiat currency into Bitcoins or by directly trading some labour in exchange for Bitcoins. (*Getting started with Bitcoin*. Accessed March 31, 2013. <https://www.weusecoins.com/getting-started.php>).

from the cash itself) requires a financial intermediary to perform settlement of payments via their networks and/or fiduciary instruments. For example, most major banks participate in the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, which accommodates bank wire transfers. Ultimately, any individual dealing with these financial institutions relies on trust as the mechanism for keeping his financial assets safe and for ensuring that his transactions are carried out securely and correctly. Unfortunately, history is replete with instances of banks failing and governments defaulting (Allen and Gale 2007, 1-24; Reinhart and Rogoff 2009, 49-98, 139-171). In addition, whether justified or not, there have been restrictions imposed on the movement of money such as through capital controls or sanctions (Quinn 2003; Bale 2012). These examples and other mishaps tend to spoil or completely destroy the trust that once existed and may leave the individual with limited access to his assets or even the inability to recover a portion of said assets. With Bitcoin, trust is not placed with a central authority or a financial intermediary, but in technology: specifically, cryptography and mathematics. Proven and well-defined encryption algorithms and brute-force mathematical hashes are the key to making Bitcoin trustworthy as a payment system. As long as the Internet is functioning⁴ and people continue to participate in the Bitcoin network, currency holders have the ability to access their Bitcoins and make unrestricted payments.

Another advantage of Bitcoin as a payment system is its cost, convenience and speed of processing payments. With many forms of electronic payment, such as credit card purchases, the fees charged to consumers and merchants can be substantial (Kelly 2013), and merchants can suffer from charge-backs and countermands that are sometimes associated with fraud. The usage of some instruments requires the physical presence of the user at a particular location to initiate the transaction or to obtain the instrument. In addition to the cost and convenience factors mentioned above, all of these forms, except for cash, require a fairly long settlement period by today's technological standards, lasting anywhere from one day to a week or more. Conversely, the Bitcoin network operates with voluntary fees and thus fees are low or zero.⁵ Moreover, the settlement process lasts, on average, ten minutes (Nakamoto 2008, 4) meaning a transaction is finalized much faster than with many of the other present forms of payment. Another benefit of Bitcoin is that transactions can be facilitated in several ways. First, users can log into an online wallet service⁶ and use the interface to make a transaction. Second, users can have a wallet running on their home computers, which allows them make payments without the need for a third-party service. Third, by running a Bitcoin application on their smart-phones, users can make payments anywhere that Internet access is available, often through mobile service providers' data access points. Bitcoin, therefore, allows for Web purchases as well as emulating in-person payments using a mobile device.

⁴ As is commonly known, the Internet was designed as a decentralized communication system to withstand large-scale wars, natural disasters and other catastrophes. If the Internet were to go off-line, Bitcoin would not be the only system affected. In such an event, the global economy would come to a grinding halt.

⁵ However, a sender can pay a small fee as an incentive for miners to process his transaction quicker (*Getting started with Bitcoin*. Accessed March 30, 2013. <https://www.weusecoins.com/getting-started.php>).

⁶ For example, Coinbase (<http://coinbase.com>).

Many people believe that their financial dealings should remain private. Presumably that is why cash transactions are still in favour today, albeit for small value transactions. Bitcoin can also provide a form of anonymity, however, unlike cash, Bitcoin addresses are not truly anonymous, but “pseudonymous”. That is, by design, all transactions are public so given the will, through data mining and network analysis, Bitcoin addresses can possibly reveal somebody's identity. Having said that, there are ways to strongly increase the level of a user's privacy to a degree that a user can effectively enjoy full anonymity.⁷ Furthermore, the ability to perform anonymous transactions removes many of the burdens associated with establishing and operating a bank account such as providing copious amounts of identification or being granted authorization for various transactions or their associated limits. Thus there is reasonable evidence to suggest that Bitcoin has the ability to make economic activity smoother and more accessible by removing potentially unnecessary encumbrances.

III.2 Built-in Inflation Control

Milton Friedman famously said, “Inflation is always and everywhere a monetary phenomenon” (Friedman and The Council for Economic Education 1963, 17). A recent and extreme example of this notion is the hyperinflation experienced in Zimbabwe where, “Inflation is estimated to have peaked in September 2008 at about 500 billion (10 percent)” (Coomer and Gstraunthaler 2011, 21). Interestingly, as shown in Figure 3, during and after the financial crisis of 2007-2009, the U.S. money supply has seen explosive growth. Indeed, many developed countries have undertaken some form of quantitative easing in an attempt to jolt their economies into recovery or to provide liquidity. The world is still watching and waiting to see what, if any, inflation will result from these monetary expansions. Nonetheless, Fischer, Sahay and Vegh (2002) demonstrate that there is clear evidence, as shown in Figure 4, that a strong positive correlation exists between the growth of the money stock and price levels. In addition, today's monetary system is based on fiat money (most of which exists electronically) instead of commodity money. This allows for less effort to be exerted in the manipulation of the money supply by governments for various ends. In the name of repaying debts, boosting exports or funding military excursions, governments can dilute the value of their currency through money printing.

In light of this observation, Bitcoin was purposefully devised to mimic a steady and predictable growth in the stock of Bitcoins, somewhat akin to controlled mining of a commodity money, such as gold. This growth is to continue until the Bitcoin supply reaches its upper limit of 21 million around the year 2140 (Wallace 2011). Following this upper bound of available Bitcoins, a deflationary environment would undoubtedly prevail within the Bitcoin economy. That is, aggregate prices would begin to fall as each Bitcoin in existence gains in relative value. Bordo and Ellson (1985) argue if a gold money standard were to be adopted, eventually long-run deflation would take hold due to resource depletion and real economic growth. Thus, if their model were observed in practice, Bitcoin would experience the same outcome as the classical gold standard.

⁷ For a more detailed description on anonymity in Bitcoin and how to increase it see <https://en.bitcoin.it/wiki/Anonymity>.

The inflation versus deflation debate with respect to economic policy remains unresolved. Some Austrian economists are not averse to deflation: “[Murray] Rothbard takes a more favorable position toward deflation than most Austrian economists and, of course, than the mainstream economists” (Bagus 2003, 19). Ben Bernanke and others, however, caution against the risks of deflation: “Sustained deflation can be highly destructive to a modern economy and should be strongly resisted” (Bernanke 2002). In the face of this existing debate, this paper does not take a position on deflation, but considers that most, if not all, economists view high inflation as a condition that wreaks havoc on economies and people's lives. To the extent that high inflation can result from governments interfering with the money supply, Bitcoin can be viewed as a reliable deterrent. By its very nature, Bitcoin is anti-inflationary and therefore prevents or mitigates loss of purchasing power, uncertainty over expected prices, and monetary and fiscal dishonesty. Should the currencies of the world suffer from higher inflation in the years to come, Bitcoin's inherent deflationary property could entice the masses to adopt Bitcoin as a currency and participate in the Bitcoin economy.

III.3 Is it Money?

Before Bitcoin can become classified as a significant currency, it should pass, or have the potential to pass, the standard definition of money. The standard criteria that allow something to meet the definition of “money” are ability to act as: a medium of exchange, a store of value and a unit of account. Historically, the production of a particular form of money from gold coins to paper notes always remained within a nation-state, kingdom or region. For instance, even in the relatively free market era of coin minting, each mint was limited by a higher authority and by a specified location, “In England, for example, the mint system was directed by the crown, and all mints issued the same coin, whereas in France there existed a multitude of issuing authorities, coins and accounting systems, and Italy's largely autonomous cities all issued their own coins” (Eichengreen and Sussman 2000, 6). In this respect, Bitcoin deviates from the norm, since the production of Bitcoins exists across the entire Internet and the only authority is the mining protocol existing as code in software. The idea of an electronic, decentralized currency existing solely on the Internet represents a very unusual and novel interpretation of money and currency. In particular, when economists originally imagined the idea of money, they could never foresee the advent of the Internet and how it, in some ways, acts as its own nation, permeating physical geographies and national jurisdictions. What follows is a discussion of Bitcoin's ability to satisfy the three properties of money.

First, as previously mentioned, Bitcoin is already being used as a medium of exchange in many online purchases and being accepted by a growing number of merchants. Some appropriate indicators of a medium of exchange are recognition, homogeneity, divisibility, durability, portability and resistance to counterfeiting. Both commodity⁸ and fiat⁹ money are good candidates with respect to recognition and homogeneity. Fiat money

⁸ Here I consider metallic coins such as gold and silver as commodity money since they both have a long history of serving as such.

⁹ This includes paper notes as well as coins minted with little intrinsic value (non-gold and non-silver

is quite adept at being divisible, but commodity money has some problems. Specifically, as Velde (1998) highlights, commodity money suffers from “The Big Problem of Small Change” and a solution for finding a way to keep large and small coins in circulation requires token coinage and a central authority. Thus, in the absence of the solution, purchases of vastly varying amounts become very difficult when only one denomination of a coin exists in circulation. On the other hand, commodity money is much more durable than fiat paper money. As for portability, commodity money suffers from weight and transportation issues for large purchases. Also associated with transportation, commodity and fiat money are prone to the prospect of theft. Lastly, counterfeiting has been a plague on both commodity and fiat currencies since their inception. In contrast, Bitcoin is recognizable in a virtual sense due to its adherence to the protocol. Bitcoin also satisfies homogeneity, as each Bitcoin exists simply as a computationally identifiable digital sequence of bits. Bitcoin excels in terms of divisibility since it can scale up or down to eight decimal places. Since Bitcoin is non-physical, it relies on the existence of the Internet and continued use of the Bitcoin network to ensure its divisibility, thus Bitcoin could, at least theoretically, exist indefinitely. Furthermore, while Bitcoins themselves are not portable, the virtual nature of Bitcoin and the use of mobile devices means that payments can be. Finally, Bitcoin is nearly impossible to counterfeit due to its inherent cryptographic and decentralized design. Therefore, Bitcoin sufficiently meets the stated measures that constitute a “medium of exchange”.

The second property of money, the store of value, perhaps requires the most faith on the part of currency holders. Expressly, to hope to realize future purchasing power, people must believe in their choice of savings vehicle. In the same vein, commodity money has, even to this day, proven itself as a reliable store of value, at least in a long-run sense and in real terms (Harmston 1998). Fiat money, alternatively, does not enjoy this degree of persistence. Globally, a fully fiat monetary system has only been in existence since 1971 with the termination of Bretton-Woods. In the last four decades, using fiat money as a store of value has retained *nominal* purchasing power. Of course, that is subject to time and space; for example, the German Deutsche Mark, though once strong, is no longer a recognized currency and thus a poor store of value. Bitcoin is still too young a currency to rate its success as a store of value, but the potential exists for the same reasons mentioned above: if the Internet and Bitcoin network continue to operate, there is no reason why Bitcoins cannot act as a good store of value. Furthermore, since Bitcoin leans toward a deflationary design, its real purchasing power, assuming economic growth, should increase.

Lastly, the unit of account property of money is important for an economy to conduct business. Having a standard numerical measure of value to relate prices allows for opportunity cost and tax payment calculations, and market clearing, among other things. Presently, most national economies operate under a fiat system as a unit of account within each jurisdiction. For international trade settlement, the U.S. dollar is typically the reserve currency. Though commodity money has historically been used as a unit of account, demonstrating its ability to fulfill the unit of account property, that is not the case today. Similarly, Bitcoin has the potential to be a unit of account, but has not yet been widely

coins), both of which are un-backed and derive their value by decree of a government.

adopted as such. There are, however, some merchants that are pricing in Bitcoin¹⁰ by converting the U.S. dollar equivalent to Bitcoins through the current exchange rate. As previously discussed, the nature of Bitcoin can be understood as the Internet, and thus one can imagine that any transactions conducted over the Internet can use Bitcoins as the numéraire. Just as exchange rate conversions are performed when an individual wants to purchase goods or services from a foreign jurisdiction, Bitcoin and the Internet could act as another foreign currency and jurisdiction, respectively.

IV. Risks

For any currency to be practical and meaningful, it must afford the people using it the ability to spend it and to save it. With that in mind, there are two main risks to Bitcoin's widespread adoption as a currency in the long run: (i) extreme price volatility and (ii) political risk.

Firstly, wild price fluctuations of Bitcoin could dissuade individuals¹¹ from acquiring and holding Bitcoin. Regardless of the currency, economic actors save whatever they do not spend. Presumably those people want to feel confident that the currency units they have saved will retain purchasing power in the future in real or nominal terms, in the case of an inflationary environment. Needless to say, when a currency experiences massive or frequent price volatility, confidence in its ability to act as a store of value is diminished or lost; Bitcoin is not immune to this phenomenon. Alas, Bitcoin has encountered some major price swings in its short lifespan. For example, in the spring/summer of 2011, the Bitcoin price in terms of U.S. dollars lost about 90 percent of its value (see Figure 1). As the latest data from *Bitcoin charts*¹² indicate, Bitcoin has experienced some more price swings lately, but not to the same degree, in percentage terms, as in its early years. Moreover, rather than any fundamental economic causes, most of the price volatility stems from highly publicized media events such as failures of various Bitcoin exchanges as well as incidents of illicit trade activities settling in Bitcoin. Therefore, in order to induce more people to save a portion of their wealth as well as make payments in Bitcoins, the Bitcoin price should be widely perceived as stable to an extent.

Secondly, and more importantly, political risk may be a substantial hurdle to Bitcoin's success. Since the very nature of the crypto-currency is a threat to central banking and, possibly, governmental capital controls and taxation, there exists the foreseeable risk that some of these institutions could implement countermeasures in an attempt to subvert Bitcoin's use. In particular, governments can enact laws banning the use of Bitcoins, though this, like online file sharing software, would be difficult to enforce. Another potential avenue would be to outlaw Bitcoin exchanges where people can trade Bitcoins for fiat currencies and vice versa. This measure may be effective within a jurisdiction, but

¹⁰ For example, see <http://giftsforcoins.com/store/> and <http://www.bitcoinin.com/>.

¹¹ This applies equally to merchants as they will be hesitant to accept Bitcoin as a form of payment lest they suffer exchange rate or purchasing power losses.

¹² *Bitcoin charts*. Accessed March 30, 2013.

<http://bitcoincharts.com/charts/mtgoxUSD#tgCzm1g10zm2g25>

more difficult globally. Furthermore, there exists little possibility to prevent individuals from exchanging Bitcoins using other methods such as face to face or through online forums. As mentioned previously, Bitcoin's distributed design makes it nearly as robust as the Internet itself. Akin to the hitherto unsuccessful War on Drugs, illegalization of Bitcoin is not likely to result in its eradication if sufficient demand for the crypto-currency persists.

V. Conclusion

As far as financial innovations are concerned, the idea of a currency existing solely on the Internet with no central authority to manage its supply and having a foundation predicated on mathematics and cryptography is truly revolutionary and unorthodox. Bitcoin is such an innovation. This paper has demonstrated that Bitcoin has the potential to flourish into a major currency for conducting international trade. It was shown that through the ease of joining the network, retaining privacy, enjoying lower transaction fees and higher convenience, and having transactions settle in minutes instead of days, Bitcoin demonstrates its remarkable ability as a rival payment system to the traditional forms such as bank wires and credit cards. In addition, Bitcoin's design for a controlled growth rate of the supply of Bitcoins prevents it from being exorbitantly inflated by careless governments or exogenous supply shocks. This offers better price stability when compared to the many historic and recent inflationary episodes experienced by national currencies. Finally, though Bitcoin is still aborning, it satisfies the three properties of money or at the very least, demonstrates its capacity to be money.

There exist risks in the form of extreme price volatility and political obstruction, which may undermine Bitcoin's widespread adoption and long run viability as a currency. Thus, it may be premature to make a definitive statement on Bitcoin's lifespan. However, the concept of a decentralized cyber-crypto-currency will be difficult to stuff back into Pandora's box.

References:

- Allen, Franklin and Douglas Gale. 2007. *Understanding Financial Crises*. New York: Oxford University Press.
- Bagus, Philipp. 2003. "Deflation: When Austrians Become Interventionists." *The Quarterly Journal of Austrian Economics* 6 (4): 19-35.
- Bale, Simon. March 15, 2012. "SWIFT Instructed to Disconnect Sanctioned Iranian Banks Following EU Council Decision." In *Swift Press Releases*. Accessed March 30, 2013. http://www.swift.com/news/press_releases/SWIFT_disconnect_Iranian_banks/

- Bernanke, Ben S. November 21, 2002. "Deflation: Making Sure 'it' Doesn't Happen Here." Speech before the National Economists Club, Washington, D.C.
<http://www.federalreserve.gov/boarddocs/speeches/2002/20021121/>.
- Bordo, Michael David and Richard Wayne Ellson. 1985. "A Model of the Classical Gold Standard with Depletion." *Journal of Monetary Economics* 16 (1): 109-120.
- Coomer, Jayson and Thomas Gstraunthaler. 2011. "The Hyperinflation in Zimbabwe." *Quarterly Journal of Austrian Economics* 14 (3): 311- 346.
- Eichengreen, Barry and Nathan Sussman. March 2000. "The International Monetary System in the (Very) Long Run." Working Paper 00/43, International Monetary Fund.
- Fischer, Stanley, Ratna Sahay, and Carlos A. Vegh. 2002. "Modern Hyper-and High Inflations." *Journal of Economic Literature* XL 3: 837-880.
- Friedman, Milton and The Council for Economic Education. 1963. *Inflation: Causes and Consequences*. New York: Asia Publishing House.
- Harmston, Stephen. November 1998. *Gold as a Store of Value*. Research Study 22. World Gold Council.
- Kelly, Dan. April 1, 2013. "Credit Card Fees a Tax on Consumers, Small Business." *Financial Post*. Accessed April 2, 2013.
<http://business.financialpost.com/2013/04/01/credit-card-fees-a-tax-on-consumers-small-businesses/>
- Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."
<http://bitcoin.org/bitcoin.pdf>.
- Quinn, Dennis P. 2003. "Capital Account Liberalization and Financial Globalization, 1890-1999: A Synoptic View." *International Journal of Finance and Economics* 8 (3): 189-204.
- Reinhart, Carmen M. and Kenneth S. Rogoff . 2009. *This Time is Different: Eight Centuries of Financial Folly*. Princeton, N.J.: Princeton University Press.
- Velde, Francois R. 1998. "Lessons from the History of Money." *Economic Perspectives* 22 (1).
- Wallace, Benjamin. November 23, 2011. "The Rise and Fall of Bitcoin." *Wired*. Accessed March 25, 2013. http://www.wired.com/magazine/2011/11/mf_bitcoin/

Appendix

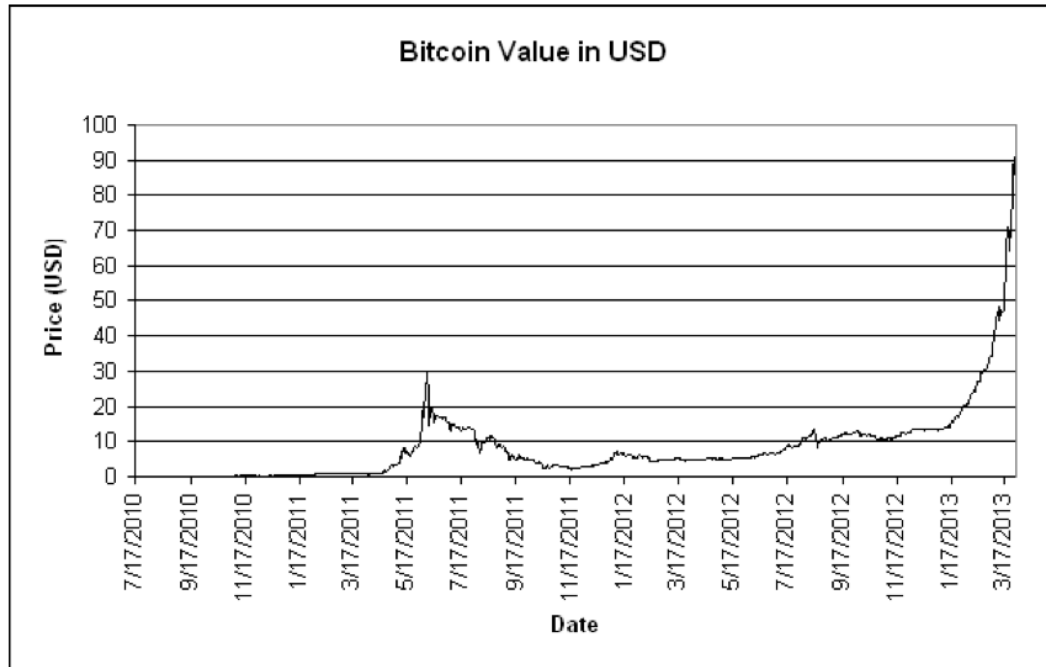


Figure 1: Bitcoin value in U.S. dollars (Source: *Bitcoin charts* 2013).

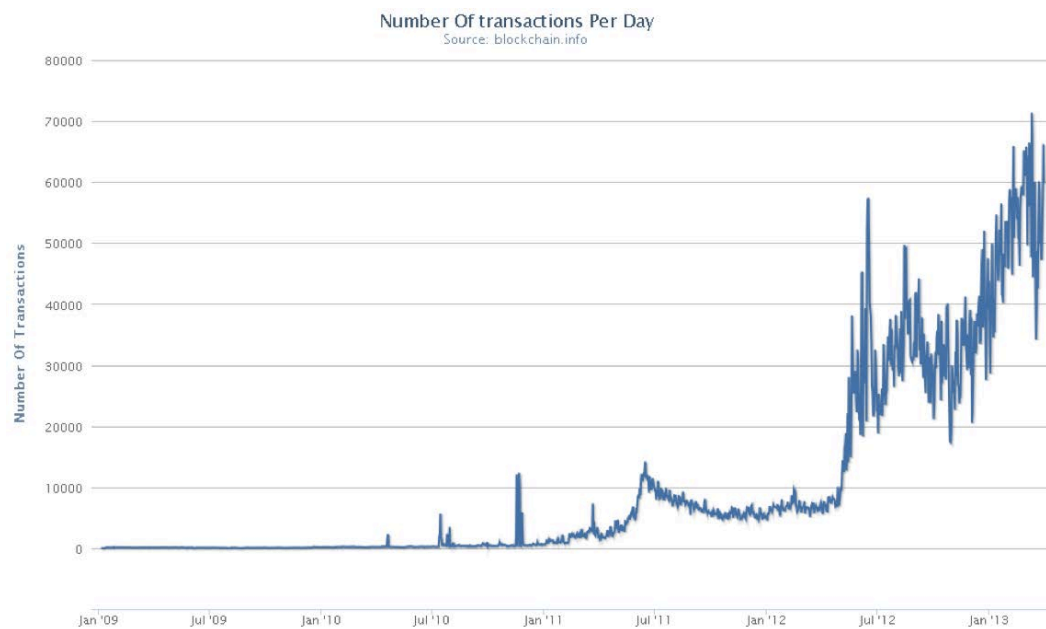


Figure 2: Estimated Bitcoin transactions per day.¹³

¹³ Blockchain. "Number of Bitcoins." Accessed March 30, 2013. http://www.chicagomanualofstyle.org/tools_citationguide.html

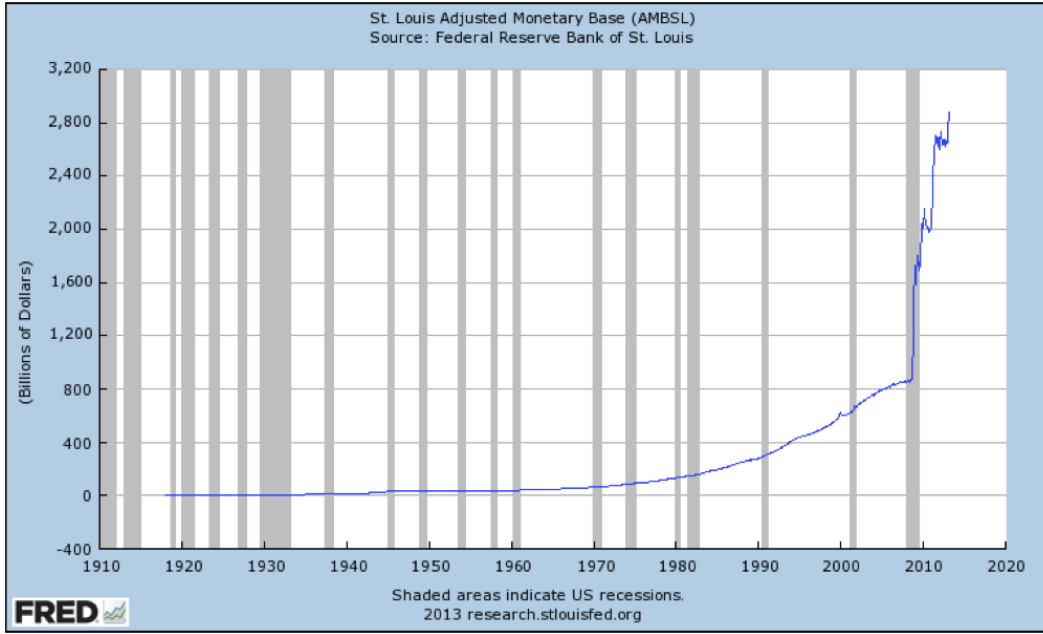


Figure 3: U.S. adjusted monetary base.¹⁴

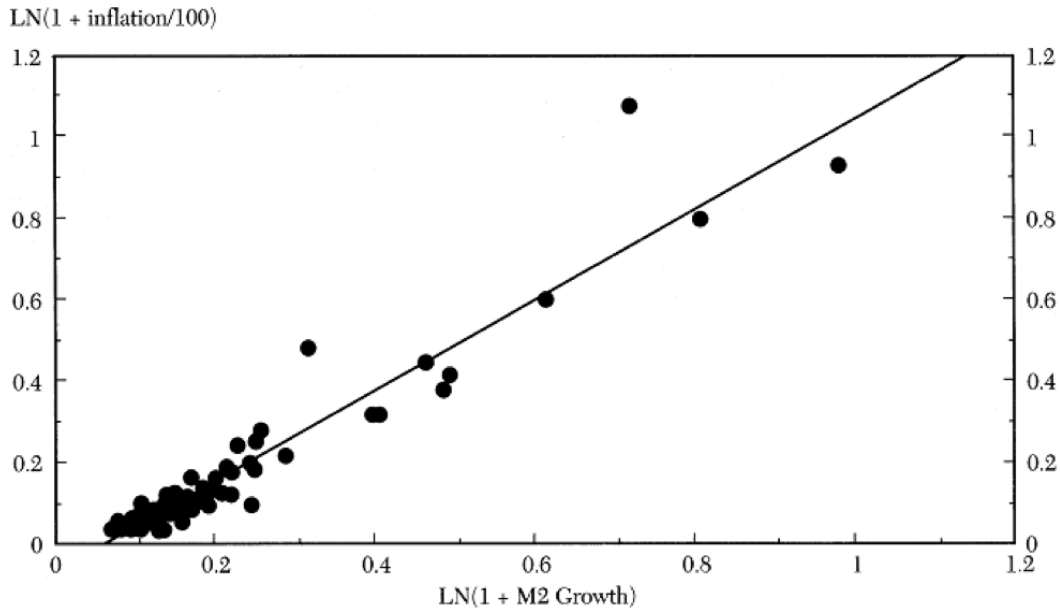


Figure 2. Inflation and Money (M2) Growth¹
1960-95 averages

¹ Slope of regression line is 1.115 with a t-statistic of 12.13; 94 countries in total, each with 10 or more observations.

Figure 4: Correlation between inflation and money supply growth (Source: Fischer, Sahay, and Vegh 2002, p. 848).

¹⁴ Federal Reserve Bank of St. Louis. "St. Louis Adjusted Monetary Base." Accessed April 4, 2013; page now discontinued. <http://research.stlouisfed.org/fred2/series/AMBSL>