Bits and Pieces: The Digital World of Bitcoin Currency

Gerald P. Dwyer, and Norbert J. Michel

September 16, 2015

Abstract

Bitcoin is the most prominent privately issued digital currency today. It is neither issued by a government nor backed by a physical commodity. Bitcoin's underlying technology also serves as the basis of an electronic payments network. Bitcoin is the first technology that allows people to reliably exchange funds on the Internet without relying on a third party, such as a bank or PayPal. A key aspect of the technology is the blockchain, a publicly available database that records every bitcoin transaction. Bitcoins are created by "miners," who expend resources to create new bitcoins, analogous to the physical process of mining gold. Unlike gold mining, the number of bitcoins to be produced is determined by a fixed schedule. Bitcoin is now accepted as payment by well-known companies, such as Dell, Papa John's, and Overstock.com, but it remains a very small part of global commerce. It is a technological innovation with the potential to benefit millions of people. Policymakers should prevent burdensome regulations that single out Bitcoin's development or drive it offshore.

Bitcoin is an electronic currency that is neither issued by a government nor backed by a physical commodity. Bitcoin's underlying technology allows users to transfer funds in an electronic payments network. Ultimately, the technology could have effects far beyond purchases of goods by, for example, improving processes that rely on time-stamped electronic records, such as digital passports or even stock trades. A key aspect of this technology is the blockchain, a

publicly available database that records every bitcoin transaction, and many digital currencies now use some version of it.

The blockchain is maintained by a decentralized computer network rather than by a central authority. A bitcoin transaction is not final until it is included in the blockchain, and no bitcoins exist outside the blockchain. This complete record is distinct from government-issued fiat currency transactions, for which there are no such records.[1] Bitcoin's process of authenticating each new transaction that is added to the blockchain, commonly referred to as mining, also creates new bitcoins. Every four years, the number of bitcoins produced is halved, until as many as 21 million bitcoins have been created. After those bitcoins have been created, which is expected to occur about 2041, mining will only authenticate transactions. The first bitcoin was created in 2009, and there were approximately 14.1 million bitcoins as of May 2014, as computed at the website bitcoincharts.com.

Bitcoin is still in the early stages of development, but bitcoins are already accepted as payment for goods and services by well-known companies, such as Dell, Papa John's, and Overstock.com, as well as many other vendors. Bitcoin transactions are still a small part of the global economy, and it is difficult to imagine Bitcoin replacing an established national currency, such as the U.S. dollar, as long as the Federal Reserve acts as a moderately good steward of the national currency. Nonetheless, the privately produced cryptocurrency Bitcoin is one example of a market innovation that allows people to choose their own mediums of exchange. Congress should prevent barriers that single out Bitcoin development and impede people from using their preferred medium of exchange.

What Is Bitcoin?

Bitcoin is a privately issued electronic irredeemable currency. Bitcoin is not issued by any government nor backed by any physical commodity. Bitcoin's underlying technology makes it possible to use bitcoins on an electronic payments network. One key part of this technology is the blockchain, and many digital currencies now use some version of it. The concepts discussed in this Backgrounder apply equally to Bitcoin and any similar digital currency based on a blockchain.

Bitcoins are digital and might be thought of as bits that represent money, but they are very different from, for example, a digital Microsoft Word file. Word bits represent a document that can be altered, copied, and sent to any number of people. Anyone who attaches a Word file to an e-mail can still send the original Word file to someone else or use it otherwise. Once a bitcoin is transferred to another person, the original owner can no longer send it to anyone else or use it for any purpose. One of the key reasons why Bitcoin became the first successful privately issued digital currency is precisely because individual bitcoins cannot be copied and re-used even though no central authority is running it.

If users could re-spend the same bitcoins—that is, "double spend" them—bitcoins would be useless as money. An infinite number of bitcoins could be created at virtually no cost and the value of bitcoins would be zero. Bitcoin's underlying technology avoids this problem by using a decentralized peer-to-peer computer network rather than a centralized authority to verify transactions. This decentralized network effectively maintains a database ledger that authenticates all bitcoin transactions.

The ledger is referred to as the blockchain, and all bitcoin transactions are checked against the blockchain to ensure that there is no double spending. This authentication process on the network allows people to make direct digital currency transactions with each other without relying on a third-party intermediary, such as a bank or PayPal. The authentication process is referred to as mining, and it also creates new bitcoins at a pre-determined rate.[2] People who make their computer resources available for authenticating the blockchain, referred to as bitcoin miners, are rewarded with some combination of new bitcoins and transaction fees.[3] Transactions are verified by miners working to solve a computer resource-intensive computational problem built into the underlying Bitcoin protocol.[4]

This mining process is designed to produce fewer bitcoins as time goes on, and no more than 21 million bitcoins will be created. This maximum number is expected to be reached by approximately 2041. It is easy to verify the exact number of bitcoins in existence at any moment, which ensures that the production of bitcoins follows this schedule. The use of resources to create new bitcoins mimics the extraction of a precious metal from the earth, which accounts for the use of the term "mining."[5] After the maximum number of bitcoins has been created, transaction fees higher than current fees will compensate miners, who are not employed by Bitcoin, for the resources used to authenticate transactions.[6]

How to Use Bitcoins

People can download Bitcoin client software if they want to use bitcoins. This program, called a "wallet," connects a user (by Internet) to the decentralized network of all Bitcoin users. The software also generates unique, mathematically linked keys, one public and one private. A user needs both the public and private keys to transfer bitcoins.[7] Once armed with these keys, anyone can obtain bitcoins by either accepting them as payment for a good or service, buying them from another person, or purchasing them on a bitcoin exchange. These public and private keys play an important part in finalizing transactions using cryptographic processes, and ensure that the transactions are valid. Because of this connection with cryptography, Bitcoin and similar currencies are often called "cryptocurrencies."

While not a necessary aspect of using or acquiring bitcoins, bitcoins can be purchased on exchanges. These bitcoin exchanges are similar in some ways to stock exchanges, with people purchasing bitcoins instead of stocks.[8] Similar to stocks on stock exchanges, people who own

bitcoins can sell them on an exchange for a preferred currency, such as dollars, other fiat monies, or other digital currencies. When they want bitcoins from the exchange, they can order the exchange to transfer the bitcoins to their wallet.

The wallet allows users to send and receive bitcoins, as well as to keep track of their transactions. Despite its name, the wallet does not store bitcoins. Instead, the wallet is more similar to a spreadsheet program that keeps track of a balance.[9] All evidence of bitcoin ownership is solely in the blockchain.[10]

The Blockchain

The blockchain is a publicly available database that records every bitcoin transaction. Every bitcoin is associated with an address. This address is derived from a public key in a public-key/private-key pairing. The blockchain records every trade of bitcoins from one address to another. A bitcoin transaction is not final until it is included in the blockchain, and no bitcoins exist independently of the blockchain. Each bitcoin is associated with a public key, and each bitcoin user has a private key, known only to the user associated with a specific public key.

Bitcoin's decentralized network creates transactions using public and private keys. When someone decides to send bitcoins to someone else, the user effectively creates an electronic message that can only be authenticated with the correct keys. For example, when Katie wants to transfer bitcoins to Hugh, she creates a message including her address from which she wants to transfer funds, and Hugh's address as the recipient. She signs the transaction with her private key; her public key can be used to verify that she signed it. She broadcasts this transaction to other nodes on the network. Miners then can verify that this address has the necessary funds and that the transaction is valid. The transaction can then be included in one "block" in the blockchain. Once the transaction is included in the blockchain, Katie can no longer spend those bitcoins associated with that address, and it is Hugh who can now spend them. Bitcoin's protocol ensures that the blockchain is accurate.[11]

If a Bitcoin user loses his private key, he permanently loses his bitcoins. If a thief obtains Katie's private key, the thief can transfer the bitcoins to his own address; there is no mechanism to transfer the bitcoins back. Katie would lose her bitcoins just as she would lose her paper currency if a thief steals her physical wallet. Losing a private key is, in this way, very similar to losing physical currency.[12] On the other hand, all bitcoin transactions can be traced by address. In other words, Katie, and anyone else, can easily discover the address to which her bitcoins were transferred. If the address can be associated with a particular person in the physical world, the thief can be identified. Moreover, all of the thief's transactions using that address can be determined.[13]

Open-Source Software and Bitcoin. Bitcoin and the blockchain were developed by programmers and released under open-source licenses.[14] Thus, while the original owners retain a copyright on Bitcoin, there are conditional, free licenses available to the public, and the source code is

open-access. Still, none of the software includes patented elements, and no attempt was made to patent the blockchain. Without paying anyone else anything, anyone can access and edit the Bitcoin network. Anyone can also simply copy the code and change it or use it for other purposes—even for starting another cryptocurrency. However, these volunteers must include a copy of the open-source license going forward, a limitation that might fail to encourage as much innovation as a traditional licensing scheme because it lacks the same profit motive. Nonetheless, it would be incorrect to say that no one leads development of software for bitcoin.

Initially, Satoshi Nakamoto led the development of Bitcoin in the late 1990s—it was his proposal—and subsequently he suggested that Gavin Andresen lead development. This development occurs with other core developers and the assistance of anyone who wants to contribute. None of these people, though, owns the source code (the programs). Anyone who does not like a decision made by Andresen and the core developers can take the code and start his own cryptocurrency, but if most people agree with the developers' decision, there is little incentive to take such action. Some argue that this arrangement gives the core developers (or cliques within that group) de facto control of the Bitcoin network, even if only because people are predisposed to accept developers' suggestions.

The developers have made few major suggestions to test this theory, but two recent suggestions are illustrative: One recommendation was widely accepted, while the other has not been met with acceptance even among core developers. In 2013, core developers suggested that a software glitch should be fixed by reverting to an earlier version of the software. This solution was widely accepted even though it required anyone using Bitcoin 0.8 to switch back to version 0.7, and to resubmit trades conducted under version 0.8 so that they could be added to the blockchain based on version 0.7.[15]

More recently, Gavin Andresen proposed increasing the maximum block size from 1 MB to 20 MB, a suggestion that has sparked much debate among the core developers. While this issue is rather technical, it is one that needs to be resolved if the network is to facilitate increased traffic as Bitcoin use grows. Many developers disagree with Andresen because they feel that increasing the block size too much—or even too fast—could harm network decentralization and security. To date, no group of developers' view has taken hold, and the debate highlights that major changes to the network are not simply decreed by the core developers.[16] The debate also highlights the fact that any major aspect of the Bitcoin code could be changed in the future, a feature that has to be accepted if such currencies are to become more widespread.

One reason for the success of Bitcoin is that it is "open source," a feature that permits development to occur and for improvements suggested by many different programmers to appear in the sole source code.[17] While it is entirely possible to write copyrighted software for Bitcoin that incorporates none of the open-source software created so far, doing so could be counterproductive because core developers generally would be unaware of what that code contains, and might inadvertently make changes that conflict with the copyrighted code.[18]

More fundamentally, a major advantage of open-source code is the possible innovation that results from the collaboration of many people on the code, an advantage that could be lost by creating copyrighted software.[19]

Current Status of Bitcoin and the Blockchain. Bitcoin is not included in any measure of money today because it is not a generally accepted medium of exchange or a close substitute.[20] It is possible, though, that Bitcoin eventually will be widely accepted and included in standard measures of money. It is difficult to get precise data on the use of bitcoin in exchanges for goods and services, but many large companies such as Microsoft, Dell, DISH Network, and Overstock.com now accept bitcoins.[21] Furthermore, bitcoins can be used indirectly for retail purchases via gift cards at countless major retailers.

There were about 14.1 million bitcoins on May 9, 2014, as computed at the website bitcoincharts.com. At a price of $241 per bitcoin, this quantity indicates an approximate value of $3.4 billion. This amount, while certainly nontrivial, is much smaller than the value of U.S. dollars as measured by the Federal Reserve's M2 aggregate,[22] which was $11.8 trillion at of the end of April 2015. Another way of looking at the aggregate value of bitcoins is to compare their value to the value of reserves in the banking system.

This comparison is suggested by the possibility that bitcoins will be useful in finalizing transactions between other monies. Before the 2008 financial crisis, reserves in the U.S. banking system (primarily clearing balances maintained by banks) were $8.75 billion. The value of bitcoins in March 2014, therefore, represents approximately 39 percent of the value of reserves held by U.S. banks before the crisis. Given the newness of Bitcoin's technology, this figure seems quite large if the only role of bitcoins is to finalize transactions in dollars. However, bitcoins are not useful only in the United States, and an often repeated and recently explored use for bitcoins is in international remittances and transfers.

Bitcoin provides a potentially large advantage to individuals who transfer funds internationally, particularly by offering lower transaction costs for secure transactions.[23] Bitcoin has proven especially beneficial for foreign workers who send money to family and friends in their home country, transfers of funds known as remittances. According to the World Bank, total annual remittances are $430 billion globally, an amount three times greater than the aggregate global aid budget.[24] People in underdeveloped countries depend heavily on these funds. In some developing countries, for instance, Haiti, remittances are one-fifth or more the size of gross domestic product.[25]

Historically, remittance transfers have been expensive compared to domestic transfers, with a global average transaction cost estimated at 8 percent of the transfer amount.[26] Bitcoin can dramatically lower the cost and time to complete these transfers, and it allows—for the first time—people and businesses with no formal banking relationships to transfer funds easily. Traditionally, people have used wire service companies, such as Western Union, to send

remittances. With bitcoins, migrant workers can transfer their local funds into bitcoins, convert bitcoins into their home currency, and deliver money to their family members by one of many less-expensive domestic transfer options.[27]

Future Uses for Bitcoin and the Blockchain. The blockchain is the major innovation in cryptocurrencies and has many possible future uses independent of any cryptocurrency. Some refer to the future evolution of this technology as Bitcoin 2.0, with a look forward to Bitcoin 3.0, analogous to the development of the World Wide Web and numbering systems used for it.[28] The more obvious possible uses center on the verification that information or a contract exists. For instance, the blockchain could help implement digital passports, copyright registration, or notarized records. It could also be used instead of escrow accounts in real estate transactions. One technology expert recently noted:

The engine that powers Bitcoin [the blockchain] can be used for a whole array of other applications.… Suppose you replaced the Internet's centralized Domain Name System [DNS] with a blockchain for Internet names (like Namecoin) such that every DNS request included some proof-of-work effort.… Or you built a new blockchain for crowdfunding. Or you replaced a centralized system which absolutely does need to be scrapped—that horrific barrel of worms known as TLS/SSL Certificate Authorities—with a blockchain-based solution powered at the browser level. Or you built a new distributed email service, with a blockchain for email addresses, and every time you checked your email you contributed to the network.[29]

Even leaving aside Bitcoin 2.0 or 3.0, there are other currencies based on blockchains. There is nothing to prevent these other cryptocurrencies from arising, and many have, such as Peercoin, Litecoin, and Freicoin.[30] For example, someone might start an alternative cryptocurrency because he does not like Bitcoin's rule for increasing supply over time, with an eventual upper limit of 21 million bitcoins. If Bitcoin is successful, a bitcoin's value will increase as the economy grows after 21 million have been created. This increase in a bitcoin's value is deflation in terms of prices of goods and services in bitcoins, which some regard as a bad thing.[31]

Bitcoin's rule for an eventually constant stock of coins is not a necessary part of a currency based on a blockchain. Cryptocurrencies can have alternative rules, such as a constant growth rate similar to Milton Friedman's proposed rule for the money supply in the United States.[32] For example, Peercoin[33] has an eventual growth rate of 1 percent, and Freicoin[34] has an annual fee of approximately 5 percent for holding freicoins. The Freicoin fee is similar in its effects to 5 percent inflation as far as holders of the currency are concerned. Virtually any rule for determining the quantity of a cryptocurrency is possible.[35] The major requirement is that adherence to the rule be exactly verifiable at virtually zero cost by anyone interested in using the cryptocurrency.[36] This requirement is important because it prevents creation of cryptocurrency in excess of the scheduled amount.

Some have suggested creating state-dependent rules for cryptocurrencies, in which the quantity of the currency increases more or less depending on the behavior of the economy. Leaving aside the problem of which economy is referred to—the U.S. economy, the world economy, or some other entity's—a major issue with any such rule is whether it would be verifiable. Some have suggested that a successful currency has to include countercyclical responses to be successful. Others have made more limited suggestions. For example, George Selgin, monetary and financial expert at the Cato Institute, recently suggested using the blockchain protocol to adjust mining rewards based on a feedback rule. The general idea is to produce a stable growth rate for the total value of cryptocurrency spending, or a constant rate of deflation or inflation.[37]

If successful, such a currency could offer a flexible supply without a discretionary central bank.[38] It is not obvious that this sort of rule is feasible even if it might be desirable, but the possibility of using the technology in this way is just one of the reasons why policymakers should resist regulations that stop further innovation. Unsuccessful currencies will affect a few people a little, whereas successful ones can affect many people a lot.

Possible Impediments to Widespread Bitcoin Use

A major deterrent to Bitcoin's widespread acceptance as a currency is its volatile value. Much like any currency, the market value of bitcoins fluctuates based on supply and demand in an international market.[39] This value can be measured in terms of the dollar, the euro, or any other currency. Compared to the dollar and other well-established national currencies, the value of bitcoins has been relatively volatile over time. For instance, the maximum price for a trade on Bitstamp, a U.K.-based exchange, was $1,163 on November 30, 2013. The price on Bitstamp on March 3, 2014, was $586, a decrease of 50 percent in about three months.[40] It also is true, though, that bitcoins were worth less than five cents in their first trade on an exchange in 2010.

Such high volatility makes Bitcoin's widespread use as a medium of exchange less likely, but Bitcoin is a new currency and uncertainty about its long-term value is hardly surprising. Over time, Bitcoin's volatility is likely to decline, though whether it subsides at positive prices for bitcoins or a price of zero is uncertain. The growth of the number of bitcoins at a pre-determined rate, one key benefit of the underlying technology, also contributes to Bitcoin's price volatility. In particular, a change in demand for bitcoins can change only its price because the quantity supplied cannot vary from the predetermined number of bitcoins. Other problems that will have to be sorted out over time include security, theft, and consumer fraud issues, such as the theft of 650,000 bitcoins from the Mt. Gox bitcoin exchange.[41] Ideally, policymakers will avoid the temptation to resolve apparent problems with regulatory fixes that go too far, thus preventing the further use and development of the bitcoin technology.

Regulatory Issues Surrounding Bitcoin. As with many financial regulatory matters, Bitcoin raises both state and federal jurisdictional questions.[42] Aside from taxes, most federal rules and regulations that apply to Bitcoin deal with money transmission and anti–money laundering

(AML) laws. Some of these rules have their genesis in the Bank Secrecy Act (BSA) of 1970, an Act originally aimed at deterring foreign banks from laundering criminal proceeds and helping people evade federal income taxes.[43] The BSA gave banks an affirmative duty to report (to the Department of the Treasury) cash transactions of more than $10,000, and it criminalized the failure to report such transactions.[44]

The BSA was little used until it was amended by the Money Laundering Control Act of 1986, an explicit component of the federal war on drugs and organized crime.[45] Finally, in the wake of 9/11, the USA PATRIOT Act levied new rules on an expanded list of financial institutions, and also imposed stricter due-diligence and AML requirements. While there is certainly anecdotal evidence of criminals who would have otherwise evaded justice being successfully targeted by anti–money laundering laws, there is, to date, no comprehensive study on the effectiveness of anti–money laundering laws.[46] Regardless, BSA/AML requirements apply to many firms besides banks, and businesses such as law firms, casinos, and car dealers are now required to report cash transactions of more than $10,000.[47]

These BSA/AML rules have surely contributed to existing firms' hesitancy to use the Bitcoin technology, as well as traditional banks' reluctance to work with Bitcoin-related companies.[48] Firms simply cannot legally transfer any type of funds without knowing their customer and having at least some idea of where the funds originated; Bitcoin transactions do not include the name or any other direct information about the person sending or receiving bitcoins. However, Bitcoin transactions are completed with an address, which is why Bitcoin is often referred to as pseudo-anonymous.

While legitimate businesses should not be penalized for failing to know that their customers might have engaged in criminal activity, prosecutors should prosecute criminals for their crimes irrespective of what kind of payment method they use.[49] Regardless of what the optimal AML regime may look like, all financial services companies currently have to adhere to these regulations. Most of the BSA/AML rules deal directly with federal rules for transferring money, and they are spread throughout several sections of the U.S. code.

Title 18 of the U.S. code, for instance, prohibits the operation of an unlicensed money-transmitting business, and also prohibits the knowing transfer of funds derived from (or intended for) criminal activity.[50] Title 18 considers a business unlicensed if it fails to comply with federal "money transmitting business registration requirements," or if it operates without a state license if one is required by the state. Additionally, Title 31 of the U.S. code requires money-transmitting businesses to register with the U.S. Secretary of the Treasury.[51] The Financial Crimes Enforcement Network (FinCEN) is the bureau within the Department of the Treasury that enforces most of these federal BSA/AML regulations.

Current federal policies related to transfers of bitcoins essentially treat cryptocurrency transmissions as electronic transfers of U.S. dollars or other national currencies. Current policy

ensures—for now, at least—that federal regulators will not treat individuals who transfer bitcoins to each other as money transmitters. FinCEN's official guidance states: "A person that creates units of … virtual currency and uses it to purchase real or virtual goods and services is a user of … virtual currency and not subject to regulation as a money transmitter."[52] Still, each U.S. state has the ability to create its own set of regulations for cryptocurrencies.[53] As Bitcoin becomes more widespread, states may choose to bring Bitcoin under the ambit of their current laws regarding other financial instruments.

To date, state regulations have not been overly burdensome for bitcoin users, because most states' cryptocurrency regulations treat bitcoin service providers as traditional money transmission businesses.[54] This approach might be considered a significant financial hurdle because many cryptocurrency businesses that want to operate on a nationwide level have to register separately in each state as money transmitters. Regardless of the optimal regulatory regime, the overall goal should be to regulate all currencies, even cryptocurrencies, in a neutral fashion. Furthermore, some regulators, such as those in New York and North Carolina, have regulated transmission of bitcoins more explicitly.

New York's newly finalized rules aim to regulate "business involving Virtual Currency," requiring that such firms obtain approval from the New York Department of Financial Services before starting their business in New York.[55] Furthermore, these firms "must obtain the superintendent's prior written approval for any plan or proposal to introduce or offer a new product, service or activity" or make material changes if New York or New York residents are involved. Bitcoin is an example of a virtual currency, and any business that, among other activities, transmits bitcoins, holds bitcoins for customers, provides exchange services, or administers virtual currency would qualify as a virtual currency business. Requiring such prior approval even for altering the provision of these services has the potential to drastically suppress the innovation of Bitcoin service providers, just as it prevents innovation in other money-transfer businesses. The most likely outcome of these types of rules will be to deny a given state's residents the benefits of money-transfer services.

Rather than using existing statutory authority to create new regulations, the North Carolina Commissioner of Banks has requested that the General Assembly pass a revised bill regulating money transmission businesses. Unsurprisingly, there is some controversy regarding North Carolina's legislation.[56] A large cryptocurrency money transmitter is in favor of it; apparently, smaller operations are opposed.[57] North Carolina's proposal deals only with money transmission, which currently is regulated, and does not single out cryptocurrency for special regulation. According to the Commissioner of Banks, the new plan clarifies the money transmissions covered by state law and "defines virtual currency consistently with federal financial regulation."[58]

Overall, the current approach has worked reasonably well, but there is little doubt that further developments in cryptocurrency regulation will follow. There might be differences between

traditional money-transmission businesses and decentralized cryptocurrencies, so a regulatory framework that properly addresses these differences could benefit both consumers and entrepreneurs. The nonprofit Coin Center has proposed such a framework that that might inform policymakers.[59]

At the very least, Coin Center's proposed definition of cryptocurrency transmission tries to address some of the key differences between traditional money transmitters and decentralized cryptocurrencies. Additionally, two principles should guide policymakers:

Regulations should focus on whether an intermediary can potentially "lose, misspend, immobilize, or fail to protect a customer's funds entrusted to them"[60] to the extent that current law does not address the issue.

Individuals should not be regulated like money transmitters if they only buy and sell on their own accounts.

These principles rely on the degree to which a third-party intermediary serves its customers in a positon of trust—in other words, the extent to which they serve a fiduciary role. While a single entity could produce a centrally issued cryptocurrency, no single person or entity controls bitcoin production. Hence, for person-to-person exchanges of bitcoins, no third party has a fiduciary role.[61] For this reason, regulations should not unduly interfere with the ability of individuals to transfer cryptocurrency directly to others. Not all bitcoin transactions are conducted without third-party involvement, such as in the case of some person-to-business payments, and appropriate regulations should apply to intermediaries that consumers trust to protect the value of their assets, whether U.S. dollars or cryptocurrency.

In the case of intermediaries, regulations should focus on intermediaries' activities instead of the technology. Consumer protection laws, for example, should encourage disclosure and protect consumers from fraud regardless of whether a third-party intermediary allows consumers to use bitcoins or MasterCard. Even in these cases, though, it is not clear that many new regulations are needed because bitcoin service providers do not operate outside the bounds of the legal system. Fraud is a civil and criminal offense, whether committed by a bitcoin service provider or by anyone else. Nonetheless, regulation could improve rather than hinder the development of Bitcoin if it provides a basic framework that helps consumers distinguish between reputable and fraudulent enterprises.[62]

The government should not require firms to receive permission for undertaking or ceasing activities or otherwise interfere with entrepreneurs' operations and innovations in the technology and its adoption. Just as some light-touch regulation has the potential to help Bitcoin technology develop further, regulation can have the unintended effect of moving cryptocurrency development and further innovations out of a state or out of the United States altogether. This negative effect is most likely if regulations focus on (1) controlling developments rather than

overseeing them to help consumers distinguish between reputable and fraudulent enterprises, or (2) protecting existing firms from competition.

Capital Gains Taxes. Taxes affect every aspect of the economy, and Bitcoin is no exception. In March 2014, the Internal Revenue Service (IRS) announced that it would treat cryptocurrencies as property for U.S. tax purposes, a decision that exposes bitcoin users to certain taxes.[63] In general, the income tax imposes a tax on capital gains when an asset is sold, and the amount of tax is a function of the applicable capital gains tax rate times the net capital gain. The net capital gain is generally the price realized when the asset is sold minus the cost of acquiring the asset, and the applicable tax rate depends on one's income bracket and whether the asset has been held for more than one year.[64] The tax rate is generally lower if the asset has been held for more than one year. (This case is called a long-term capital gain.)

Since the IRS treats (effectively all) alternative currencies as assets, every cryptocurrency transaction is a taxable event and is reportable on Schedule D of the taxpayers' Form 1040 (or, if a business, the analogous business tax form).[65] The price realized in dollars when the cryptocurrency is sold, less the cost in dollars of acquiring the cryptocurrency, will give rise to a capital gain or loss. This gain (or loss) may be long-term or short-term, depending on whether the cryptocurrency was acquired more than a year before. If the cryptocurrency is used to acquire a good, service, or asset, the measure of the price realized would be the fair market value in U.S. dollars of the good, service, or asset acquired.

Furthermore, a person using an alternative currency to acquire an asset, good, or service may be deemed as engaging in a barter transaction as part of a barter exchange, particularly if he regularly serves as a "middleman" or buys and sells via an "organization of members providing property or services who jointly contract to trade or barter such property or services."[66] In this case, a bitcoin user would be required to file a Form 1099-B (Proceeds from Broker and Barter Exchange Transactions) for each transaction, providing the name, tax number, and address of the seller as well as transaction information. Failure to report these transactions is subject to a penalty of $50 per transaction not reported ($100 if the failure was intentional). Those who pay wages or salaries in bitcoins or pay independent contractors in bitcoins would be subject to the same reporting requirements as if they paid in dollars.

The current tax treatment creates a major barrier to the widespread use of cryptocurrencies (as well as other alternative currencies), and there are at least two possible solutions. To resolve these issues, Congress could adopt a fundamental tax reform plan in which financial transactions are irrelevant to determining the tax base or one in which capital gains are not taxed. The Hall–Rabushka Flat Tax on incomes or a national value-added tax, such as the Fair Tax, in the place of an income tax would accomplish this goal.[67] As a more likely near-term solution, Congress could amend the Internal Revenue Code to make gains or losses nontaxable when they are attributable to the purchase or sale of cryptocurrencies or other alternative currencies.[68] Either

way, Congress should remove this tax barrier to the widespread use of bitcoins and other cryptocurrencies, as well as other alternative currencies.

Why Shouldn't People Be Allowed to Use Bitcoin?

Mutually beneficial exchange is the central element of economic freedom; this centrality extends to the right to choose a preferred medium of exchange. Many people, even many economists, now assume that economic progress requires government provision of money. Economic theory and a wealth of experience indicate otherwise. It is easily forgotten, but money often developed in private markets and was monopolized later by government authorities who wanted the revenue from creating money.[69] Even today, seigniorage (the profit that government makes from printing money) is a significant means of financing, and is used by the federal government to reduce what it must borrow from the public to fund its debt. The fact that cryptocurrencies are not legal tender in most countries tells us nothing about whether people will use them.[70]

Government coins have a long history, going back to ancient Athens. Private coins and later private currencies have a long history as well. Many monies were common tender before they were legal tender, and legal tender laws then generally protected government monopolies.[71] The international prevalence of government money monopolies reveals more about the desire of government authorities for revenue than about the preferences of people who use money.[72] At this stage, though, it would be very difficult for any privately produced money to replace an established national currency.

People prefer to have their receipts and expenses in the same currency, and there are advantages of using the same currency as used by others.[73] It is hard to imagine Bitcoin replacing an established national currency such as the U.S. dollar if the Federal Reserve acts as even a moderately good steward of the national currency. On the other hand, people might prefer to use bitcoins rather than a currency such as the Zimbabwean dollar, which eventually included bills in the amount of 100 trillion in 2008. Countries with capital controls have found it expedient to attempt to restrict citizens' use of bitcoins because bitcoins can be used to evade such controls. There is no other obvious economic-policy rationale for restricting use of bitcoins besides shielding the government's production of money from competition. Monetary policy is likely to be worse when shielded from competition, and better when competing against alternative monies.

As with any privately produced good or service, no inferior form of money would be expected to replace an economy's preferred medium of exchange.[74]Allowing people to hold and use the money they prefer will not solve all economic problems, but neither will legal restrictions and government monopoly. Policymakers should apply this perspective to the theoretical case for privately produced money as well as to the history of successful competitively issued money regimes.[75] More than 60 episodes of competitive private note issue have been identified, with well-studied episodes in Scotland, the U.S., Canada, Sweden, Switzerland, and Chile.[76] Even

in the United States, a federal government monopoly of currency issuance did not exist before 1863.

Although competitive note issue in the United States often receives most of the blame for the country's monetary instability prior to the 1900s, that aspect of the banking system actually worked reasonably well. Government regulations were major causes of monetary difficulties in the U.S.[77] In fact, before the Federal Reserve was created, private clearing houses (and sometimes banks) issued emergency currencies that successfully stemmed several banking panics caused by such shortages.[78]

In some countries, privately produced money sometimes rivaled government money when the central authority failed to provide an adequate supply. For instance, during the early stages of the industrial revolution in Great Britain, private companies minted coins that were rapidly accepted and ultimately served as a preferred medium of exchange for nearly 40 years, until the government stopped the practice.[79]Aside from the typical metallic and paper money inside a nation's banking system, there are also many examples of spontaneously developed private monies.

In the United States, Canada, and Mexico, for instance, thousands of companies created private types of money referred to as scrip. The scrip—very similar to a basic IOU—was intended for use by employees in company-owned stores, had no connection to a bank of any kind, and did not depend on redeemability in a national currency.[80] In the United States, scrip circulated as recently as 1958, and it was sometimes accepted at independent stores.[81] During the 1970s, several Las Vegas casinos produced their own token slot coins intended for use in their respective casinos, but they soon circulated well beyond these locations. Eventually, rival casinos accepted the coins, and various local businesses even accepted them for retail purchases.

On a much larger scale, private markets began producing money-substitutes in response to the high inflation and related dislocations in the 1970s.[82] The eurodollar market (dollar deposits in European banks), for instance, developed into a wholesale market on which banks, nonbank financial firms, and nonfinancial corporations still rely to borrow and hold deposits. During this same time period, the success of money market mutual funds and negotiable order of withdrawal accounts ultimately forced federal regulators to relax interest rate controls on bank deposits. Even though U.S. regulators gave up trying to limit interest rates on deposits in banks, the U.S. government maintained its monopoly control over currency issue.[83]

What Congress Should Do

Bitcoin is a privately produced cryptocurrency that is neither issued by a government nor backed by a physical commodity. Bitcoin's underlying technology is the blockchain, and it could ultimately prove beneficial to any endeavor that relies on time-stamped electronic records. Bitcoin's success should motivate policymakers to resist burdensome regulations that single out Bitcoin's development. In particular, Congress should:

Focus on general rules concerning contracts, disclosure, and fraud prevention. Regulations run the real risk of doing nothing but conferring advantages on incumbent money-transmission firms. Many, perhaps most, bitcoin service providers do not undertake a fiduciary role for their customers. Regulations should be guided by the level of control a firm has over customer funds. Government should focus regulatory efforts on general rules concerning contracts, disclosure, and fraud.

Remove barriers to entry in the market for money. The privately produced cryptocurrency bitcoin is just one example of a market innovation that allows people to choose their own mediums of exchange. The following barriers should be addressed.

Modify Capital Gains Tax Laws. Although it would be preferable for Congress to adopt a fundamental tax reform plan that determines the tax base without regard to financial transactions or leaves capital gains untaxed,[84] Congress should at least amend the Internal Revenue Code to provide that gains or losses attributable to the purchase or sale of alternative currencies are not taxable.

Modify statutes concerning coinage to make clear that they do not prohibit honestly making alternative coinage and using it in private transactions. To protect coins issued as U.S. currency by the federal government and to protect those who use them, federal statutes prohibit making counterfeit U.S.-minted coins or otherwise passing off non-U.S.-minted coins as if they were genuine U.S.-minted coins.[85] From their text, the statutes appear intended to prevent any pretense (either by appearance or use) that a non-government coin is a government coin. The statutes do not appear designed to prohibit private contracts in which the parties to the contract choose to accept in exchange for goods or services non-government coins that are clearly identified and understood by all parties to be non-government coins (that is, there is no counterfeiting or deceit involved). However, a recent court case has led to some misunderstanding concerning the permissibility of private minting of, and private use of, non-government coins.[86] Congress should modify federal coinage laws to make clear that such laws permit private minting and use in private contracting of coins in situations that do not involve counterfeiting or deceit. Such modifications would both fully protect the government's interest in the minting and use of its own coins and the liberty of contract among private parties who wish to use privately minted coins, that are clearly identified as such and understood by all parties to be such, in their commercial transactions.

Address bank secrecy and anti–money laundering laws. Cryptocurrencies should not be held to higher or lower standards than traditional financial companies. Legitimate businesses should not be penalized for failing to know that their customers might have engaged in criminal activity. Prosecutors should prosecute criminals for their crimes irrespective of what kind of payment method they use. Congress should also examine the possibility of creating a federal plan for licensing money transmitters so that firms can avail themselves of either the federal plan or states' plans, just as banks can obtain federal or state charters.

Modify legal tender laws to respect freedom of private contracting. Legal tender laws allow courts to force people to accept a certain amount of U.S. currency to satisfy debts even if they contracted for delivery of something else. If people want to transact in cryptocurrencies, gold, or, for that matter, beaver pelts, they should be allowed to do so. Congress should modify legal tender laws to provide for enforcement of the methods of payment for which private contracts provide. Such a modification would protect the freedom of contract among private parties and would not affect the status of U.S. currency as legal tender for payment of taxes.