

Meridian 180 Forum: Does Bitcoin Have a Future?

Katsuhito Iwai

“Bitcoin” is a digital payment system conceived in 2009 by an anonymous computer scientist with the Japanese pseudonym Satoshi Nakamoto. It was designed so that it needs no central authority or banks for its operation on the internet. At one point the total value of Bitcoin reached \$1 billion and attracted wide media coverage. Many, however, now debate its future because of the widely-publicized bankruptcy of Mt. Gox and other bitcoin exchanges this year.

There is nothing new about bitcoin from the standpoint of the theory of money. To explain why there is nothing new, we have to pose the question of “what is money.” Indeed, “money is money simply because it is accepted as money.” What this zen koan (philosophical riddle) like definition shows is that people accept money as money not because they want to use it as a “thing,” but because they expect others to also accept it as money. And the reason they expect others to accept it as money is only because they expect those others to also expect others to accept it as money. It is because money is a product of such “bootstrapping” expectations that we can circulate worthless pieces of metal or paper as hundred yen coins or ten dollar bills. [See, e.g. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1861952]

Theoretically, therefore, anything could be used as money. And historically shells, cows, leather, swords, salt and, in the case of the famous Yap Island, even large stones sunk deep in the sea were used as money. As time passed, gold, silver and other precious metals began to circulate in the form of bare metal, then coins minted from these metals gained currency for facility of counting and difficulty of counterfeiting, and eventually government bills, bank notes and various forms of private debts were accepted as paper money. And, the latest vintage of money is digital currency – a system of electronic “codes” used as money on the internet.

Though bitcoin prides itself on freedom from central control and national borders, there have been countless currencies in the past like this one. For example, the Maria Theresia Silver Coins issued by the Austro-Hungarian Empire during the 18th century were still in circulation in various parts of the world even after the empire collapsed. In fact, Ethiopians used those coins until the last quarter of the 20th century.

As I said anything could be used as money. There are in fact several technical problems that have to be solved before “codes” can circulate as money. The prevention of counterfeits is one of them, but the rapid development of cryptographic technology has already taken care of this. The most difficult problem arises from the very nature of “codes.” When a unit of money takes a physical form, that unit cannot be owned by more than one person at any given time. But, when a unit of money consists of a code, the payer might still remember that code even after he makes his payment to somebody else. This has turned out to also be solvable even without the intermediary of banks or governmental institutions at least theoretically -- I myself proposed a solution long before [see <http://iwai-k.com/HowToCirculateECash.pdf>]. However, Mr. Nakamoto came up with a mathematically beautiful and technologically simple solution. And I think it is that beauty and simplicity that captured the hearts of computer-savvy people who also hate any central authority. (By the way, I am not Satoshi Nakamoto.)

So, is bitcoin money? I don't think it is. For money to be money, it must be accepted as such by a large number of people. However, at least at the moment, a majority of bitcoin users are still those who own it as a mathematically beautiful gadget, or as a subject of financial speculation, or as a means for money laundering. So long as bitcoin is used in this way, it is not yet money. This does not however deny the possibility of bitcoin becoming money in the future, because theoretically anything could become money. If, for whatever reason, the number of people who expect others to accept bitcoin as money were to increase beyond a tipping point, the bootstrap mechanism would start up and the bitcoin might turn into a real money.

Yet, even if bitcoin were actually to circulate as money on the internet, I believe its future would will not be as bright as its advocates wish it to be. This is because the value of money is (at least potentially) fundamentally unstable. We have learned a hard lesson from recent history that bonds, stocks, asset-backed-securities, futures, options, and other financial derivatives fluctuate wildly in value. Nevertheless, they still retain a certain level of stability because they are backed by the issuing entities (corporations, governments, etc.) or founded on real assets (capital goods, real estates, actual commodities). Money, on the other hand, is not linked to any particular "thing." Money has its value as money only because we expect "other people to accept it as money." Once that bootstrapping expectation begins to falter and we begin to worry that others (not us) will not accept money as money, we will rush to markets to get rid of it by buying real goods and services, thereby self-realizing our own worries. This is hyperinflation, and money will no longer be accepted as money. Money loses its charm, turning back to mere pieces of metal or paper or electronic pulse.

Money is thus inherently unstable. Therefore, contrary to the teachings of laissez-faire economists or to the claims of libertarian politicians, money ultimately requires the oversight of a central bank in its role as the lender of last resort to stabilize its value. [See, e.g., http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1861949] This means that bitcoin contains an inherent contradiction because of its very design to be free from any central authority or banks. Even if bitcoin were to circulate as money in the future, it would inevitably carry with it the "fate of ultimate failure."

In closing, I would like to propose a few questions:

- (1) During the 1990s, digicash and other electronic money were very popular. However, they eventually disappeared. For all the talk about Bitcoins, is there anything "new" about this digital currency that makes it different from past digital currencies? And if so, what?
- (2) I claim bitcoin cannot be considered money yet. Do you think this understanding is correct?
- (3) Friedrich Hayek claimed that an ideal currency system was based on "free banking" – a system where even the issuance of currency is subject to competition by private issuers. One could say that bitcoin is part of the free banking movement. I respect Hayek as a historian of ideas. However, his "free banking" philosophy either misunderstands the inherent instability of the value of currency or is a logical fallacy. Of course, there are those who support "free banking." If you support "free banking," what are your logical justifications?
- (4) Does bitcoin have a future?

Comments

[Kaja Tretjak](#)

04/08/2014

Many thanks for the initial post, and for the opportunity to engage this issue.

1) [The Bitcoin system](#) is the first to solve the double spending problem in an entirely decentralized way. This protocol is also how bitcoins enter circulation. A primary argument for its superiority to fiat is that the fixed total amount guards against inflation. Eventual price deflation remains a ground for criticism. Further, one can only engage in exchange after first obtaining bitcoins through an earlier transaction, a key distinction from [mutual credit schemes](#).

2) According to the initial post's definition of money, bitcoin is indeed already money. Its [market cap has been substantially larger](#) than \$1 billion for some time. It was at around \$10 billion in Nov. 2013 and is currently between \$5 and \$6 billion. Bitcoin has millions of users, all of whom accept that it has value and are willing to pay for it. Most are willing to sell something other than dollars in exchange for it. Bitcoin is already bigger than many national currencies. The exponential rise in price since its first trades indicates that people are choosing bitcoins over dollars at an exponential rate; advocates maintain there is no built-in reason to expect an end to this process.

3) Inherent instability of money: Advocates would highlight that a currency could not hyperinflate on its own. For its price to drop, people must either be selling it for something else (switching to a superior currency), or devaluation via government action is so severe that people have no choice but to abandon it. Theoretically, a voluntary barter system could emerge spontaneously, but this is unlikely in light of its limitations. There further appears to be some conflation here between stability in terms of price, and stability in terms of a population's chosen means of exchange. These two are not necessarily related. Bitcoin's price (in dollars, which remains the unit of account) is increasing because it is becoming of interest to more people. The price volatility is a result of its high adoption rate. The price can (occasionally and temporarily) outpace the growth in its real prospects, but goods that rapidly increase in price in this way can be expected to experience shocks and manias because it is difficult to distinguish between a sustainable price increase and short-term speculation. While its price is extremely unstable, advocates would maintain that bitcoin is becoming more and more stable as a chosen means of exchange. As an aside, a currency's volatility here should be distinguished from liquidity (something bitcoin does indeed need).

4) I would suggest that, irrespective of the fate of this particular currency, the cryptographic protocol is significant for those who see the control of money and banking as a central mechanism for concentrating power and wealth, and interested in low-overhead, informal economies outside of the purview of the state. ["If Bitcoin isn't the Messiah of the darknet economy, at the very least it's John the Baptist preaching its immanent arrival."](#)

Looking forward to your thoughts!

Bill Maurer

04/08/2014

With my colleagues Lana Swartz, Taylor Nelms, and Scott Mainwaring I have been researching bitcoin since its inception. Three of us published a paper on what we call the bitcoin community's "[digital metallism](#)." Like Professor Iwai, we suggest that the ways bitcoin proponents frame the experiment echo other traditional ways of thinking about money generally. Yet while they prefer metallist or commodity language, we argue that in the very way users and developers have come together to talk, code, discuss and debate points toward credit theories of money, the chains of trust that Prof. Iwai also emphasizes.

We have seen a shift, or a debate, between people who view bitcoin as a currency and people who view it as a payment protocol or payment "rail." For the former, the idea that there can be a decentralized, peer-to-peer, quasi-anonymous currency holds great appeal, mainly for libertarian reasons. Indeed, I argue that it is very difficult to separate bitcoin in its current instantiation from the relatively right-wing and, in the US, racial politics of anti-federalist populism. My colleagues and I often find ourselves, as a result, in the [position of defending "the state" or "the public interest" when in bitcoin-sympathetic forums](#). This makes us a little uncomfortable for a number of reasons but one of them is that it also informs the bitcoin ideology—the originary link between the state and money as unit of account which bitcoin proponents seek to break. For the latter, however, those who talk about bitcoin as a "payment rail", the issue is one of providing an alternative to the electronic value transfer systems that have moved money – but are not themselves money – since BankAmericard if not Diners Club before it. The bitcoin system – or similar cryptographic block-chain based protocols like Ripple – does seem at least potentially to provide an alternative "rail" (and in the US and UK the railway metaphors are fascinating, again indexing a particular politics of cartelization, trust and anti-trust) to Visa, Mastercard or American Express.

As a payment rail, how does bitcoin or a similar system work? It works by creating a public record of all transactions, verified by a group of volunteers who offer their processing power to the algorithm running the bitcoin protocol. These are the so-called miners, who are rewarded for their effort in the form of new bitcoins. The first interesting thing to me about this is that it resonates with state theories of money that emphasize the unit of account function of money. Ironically, in fact, insofar as bitcoin is supposed to be decentralized, etc. But there is ONE ledger in bitcoin; it is NOT a distributed ledger, each node in the network holding a piece of it. Instead it is a massively replicated ledger, each node holding THE ENTIRE LEDGER, the miners reconciling ledgers against one another. [I have argued that in this it is very like old cuneiform tablets held in clay envelopes, the envelope containing an entire transcription of the information on the tablet within, as a means of preventing forgery or fraud.](#)

Sung-In Jun

04/09/2014

Bitcoin has some advantages and also its share of weaknesses. The most notable advantage is anonymity. It is an ultimate form of cash unless you have to visit Mt. Gox and convert it into other forms of more "real" currencies, thereby leaving footprints. Even the thief who stole Bitcoin can claim de-facto ownership. It is a fascinating means of making payment and storing value, especially for those who work underground.

Now the weaknesses. First, the whole scheme is easy to copy. If Bitcoin becomes widespread, other forms of money of a similar type, say "Bytecoin," may emerge. Since the inventor of money can enjoy the sweet taste of seigniorage, people will have an incentive to invent and circulate similar forms of money. So Bitcoin has to compete and win the battle before it can claim the title of real money. Currently, it is just an attractive (and risky) opportunity for financial investment.

Bitcoin will face a second challenge if it ever achieves widespread popularity. The challenge is the shortage of money. Bitcoin will have a hard time accommodating to an ever increasing volume of transactions with a more or less fixed money supply. Without banks capable of credit creation, there will simply not be enough Bitcoin around relative to the transaction volume. With banks? Well, in that case you will enter into a financial sector which is the most heavily regulated.

What will happen when Bitcoin becomes scarce relative to the transaction volume? The prices of goods in terms of Bitcoin will fall and the value of Bitcoin will rise. That is good news for Bitcoin as a financial investment opportunity. It is bad news for Bitcoin as money. Who would get rid of Bitcoin in exchange for commodities when its value is appreciating? From the perspective of the Gresham's law, it would be good money and good money doesn't get to circulate. The end of its life as money!

Jianguo WANG(王家国)

04/09/2014

Bitcoin speculation is destined to be a story of fraud – just like the dotcom bubbles in the 1990s, it will ultimately break down wildly. I believe bitcoin is like a rootless sprout. People, however, take it as a big sheltering tree.

In a strict sense, bitcoin is not money, nor is it paper currency, but just some mystic website codes and letters. The value of money and paper currency is protected by the state. Even in the case of gold in the Bretton Woods system, without state protection, gold was driven off the shrine and taken over by the US dollar.

The rise of bitcoin is not a result of its rarity, but rather of human-made disaster. To put this differently, it was caused by inflation and currency devaluation in the wake of the recent over-issuance of paper money by U.S. and other central banks. Faced with the flood of newly printed paper money, people's immediate concern has been to figure out how to maintain their money's value. During the economic recession, investment in the real economy could not produce stable profits. Therefore, people have all invested their money in "market speculation" –for example, in the Chinese real estate market, in the American stock market, or in bitcoin globally.

Therefore, the emergence of bitcoin is simply a unique abnormal offspring of a special time. When the tide fades away, bitcoin will disappear forever like evaporation. Even if people have lots of money to speculate on bitcoin, the ultimate result will be the same: a broken bubble.

Thus, central banks should be cautious about bitcoin, and investors should also keep their mind calm and sober. I hope people don't fall prey to this new form of Ponzi scheme of the virtual world.

[Christopher Ford](#)

04/09/2014

This is a topic well outside my expertise at this point, and I'm looking forward to learning (a lot) from the discussion on this string. ... I would, however, offer a quick quibble with Katsuhito Iwai's opening comments. Specifically, it's not obvious to me that "money ultimately requires the oversight of a central bank in its role as the lender of last resort to stabilize its value." Money has, of course, been around for a very long time, but central banks are a pretty modern phenomenon. Even if you restrict the data set to fairly modern, sophisticated economies -- which I'm willing to believe present qualitatively different challenges than more primitive institutions -- countries around the world clearly did have what was recognizably "money" well before they had central banks.

In the United States, we didn't get a central bank -- the First Bank of the United States -- until 1791, and after its dissolution in 1811 there was a gap before the Second Bank of the United States was chartered in 1816. After it, too, was wrapped up in 1836, we had a long period with no such central institution at all. Nevertheless, America's 19th-Century economy rather famously and successfully grew and expanded, becoming steadily larger and more sophisticated.

During this period of U.S. economic development, as I understand things -- and here I'll defer to anyone in this forum who has actually studied the history of the period -- "money" originated largely from private banks, which printed and issued small-denomination banknotes to borrowers, and this currency was redeemable in specie. (This banknote business was a major focus of private banking work for a while, before banks gradually moved out of the note issuance business into that of taking deposits.) Indeed, currency uniformity in the United States is said to be attributable not only to the policies of the Second Bank, but also to the growth of private interbank deposits designed to reduce the degree to which holders of privately-issued banknotes had to redeem them at a discount (or for specie) in dealings with banks distant from the bank of issue.

All this is just a minor footnote to Katsuhito Iwai's interesting comments, however, for it doesn't change his basic point: historically, in all sophisticated economies, "money" has been issued by some sort of accountable institution -- and bitcoin, by definition, isn't. I am looking forward to reading the developing discussion in this forum.

[Wataru Takahashi](#)

04/13/2014

The success and failure of bitcoin.

I appreciate this interesting and important initial post by Professor Iwai who is so well versed in the theory of money.

Bitcoin experienced success because it became a means of investment and because its transaction costs are low. It is well known that the value of bitcoin increased significantly since its inception. However, that's

not the only “success” bitcoin experienced. Convenience is important for currency. Bitcoin’s low transaction costs make it convenient not only for investment but also for international money transfer. Conventional banks charge high fees for currency exchange and international money transfers. Japanese banks charge 2 yen for service charges for foreign exchange transactions. International money transfer costs several thousand yen even if the transferred amount is small. These high service charges are “remnants” of the past when banks monopolized the international financial network. However, the development of the internet put an end to the banks’ monopoly. Bitcoin is one example where technological innovation such as the internet [brought about changes] in the field of finance.

Likewise, bitcoin also experienced failure because it is a means of investment and because it contains technological vulnerabilities. Bitcoin has been subject to speculation and its value has fluctuated. Assets that fluctuate widely in value such as this is not appropriate to be used as currency. Bitcoin grew precisely because it is a speculative asset. Ironically, however, this characteristic makes it unfit to be a currency.

Another problem is the technological vulnerability that allowing [some people have taken advantage of to] steal coins from servers. Central banks invest a lot great deal of energy to prevent counterfeit bank notes. Recognizing that the vast majority of today’s financial transactions take place electronically, central banks have also invested heavily in maintaining the safety of electronic transactions. However, this is a domain where technological innovation is occurring rapidly. There is no such thing as “absolute safety.” [Central banks] manage risks based on this chilling reality. Bitcoin is a product of such technological advancement, but there isit leaves much to be desired in terms of risk-management related to technology.

Had bitcoin been more prominent, banks might have lowered their service charges and improved convenience for their customers. However, even if bitcoin did not fail technologically, it would have met its demise sooner or later because speculative assets are not appropriate to be used as currency

Finally, I would like to try to respond to Professor Iwai’s questions although I’m not confident about [whether I can answer them well].

As I mentioned above, I think what’s new about bitcoin – as Professor Iwai asked in Q1 – is that it’s an “investment asset.” This is in contrast to digicash, which was not investable. Regarding Q2, the function of currency is a “question of degree.” Bitcoin’s “moneyness” was more widely accepted until the recent incident, but it seems to be in decline since. Regarding ...Q3, I want to point out the historical fact that private coinage served an important role in the history of Japan’s currency. The Muromachi period – Japan’s medieval period [running from approximately 1337 – 1573] – showed a wide circulation of coins imported from China. However, with the expansion of the currency economy in Japan and the reduction in the flow of imported coins from China, Japan faced a shortage of currency. To supplement this shortage, Japanese people began to privately mint coins that imitated Chinese coins. Some of those coins were called “red cents” and were treated as “low quality coins.” Nevertheless, the fact that those privately minted imitation coins resolved the currency shortage in Japan should be regarded in a positive light. If [people] refrain from using official currencies due to their high transaction costs, then private currencies should supplement them. “Red cents” are an example of this. As mentioned earlier, banks charge many fees for international money transfer. Just as “Line” became popular among [mobile] phone [users in Japan], even if bitcoin does not have a future, there is a high probability something similar will emerge. And that is my answer to Q4.

Katsuhito Iwai

04/16/2014

I appreciate the comments posted by Professor Tretjack, Maurer, Jun, Wang, Dr. Ford, and Takahashi in response to my initial post to the forum on Bitcoin.

1. As I mentioned in my initial post, the theory behind building a system that solves the double spending problem in a decentralized way has already been established. But as Professors Tretjak and Jun have pointed out, bitcoin is indeed new in that it actually puts the theory into practice. The reduction of transaction costs as a result of this is, as Professor Takahashi pointed out, a financial innovation, but I would like to discuss its significance at the end of this response.

2. Opinions seem to be split on whether bitcoin is a currency. Yes by Tretjak and Jun; No by Maurer and Wang. Indeed, the fact that opinions are split like this, in itself, is closely connected to the inherent nature of money. A “thing” is treated as money not because the “thing” itself has value (commodity theory of money) or because a state or a community designated it as a currency (chartal or state theory of money). (The error in the commodity theory is evident, whereas Professor Takahashi’s note about the imported coins and privately minted coins during medieval Japan points out one example of the error of the state theory. We should also keep in mind that most of M1 or M2, the statistical definition of money we use today, consists of not only cash but also deposits in private banks). In other words, money is the ultimate form of “functionalism,” and its existence is defined only by its function as money. Perhaps bitcoin functions as money among some circles. However, most of the world would not accept bitcoin as money because it would not be accepted as money by most of the world. How is this different from old stamps bought and sold among stamp collectors?

3. Free Banking theory and the instability of the value of money is what Professor Maurer and many others’ argument focused on. It is true that gold and silver have circulated [as money] in the past, and that their value was stable to some extent. However, that was only because of the collective illusion that gold and silver had some mystical value in themselves. And, there were multiple economic collapses during medieval times caused by over-issuance of coins by monarchs who held the right to coinage.

Professor Tretjack argued that bitcoin’s fixed total amount guards against inflation. However, money is a medium of exchanges whose quantity, by itself, means nothing from a long term perspective. One unit of bitcoin might be exchanged with one unit of goods or one million units. While the major cause behind hyperinflation is over-supply of money, it could also happen even under fixed supply if the confidence in the value of the currency is shaken. That said, changes in the quantity of money would significantly affect real economic activities during a short period of time when prices and wages are unlikely to change. (This is all about Keynesian economics.)

Dr. Ford has pointed out the fact that 18th and 19th century US economy grew significantly without central banks. Proponents of the free bank theory use this fact as a major basis for their argument. However, Chapter 11 of Kindleberger’s *Mania, Panic, and Crashes* depicts how the US Treasury served as the lender of last resort during that period in time. What is interesting is the history of the Bank of England. It was established as a private bank in 1694, but its size eventually led the Bank to recognize its public roles and spontaneously evolved into a “central bank” over the 18th and 19th centuries.

4. The future of bitcoin remains dark. But, if the present international monetary system with US dollar as key currency were to come to the end and a global central bank proposed by Keynes in Breton-Woods conference in 1944 would finally be established, the newly issued global currency might be a bitcoin-like system for its low transaction costs. This would be a nightmare to libertarians who dislike any kind of central authority but a blessing to the global economy as a whole. This new currency would, however, be called Bancor, not bitcoin.

[Leigh B. Bienen](#)

04/16/2014

Thank you for this very interesting series of posts. One intriguing aspect of Bitcoin is it forces us to ask fundamental questions about the role of banks, government and the huge financial institutions dominating our present, computer dominated society. I would like to see some figures on the percentage of financial transactions which taken place over the web now, in comparison to ten years ago or twenty years ago. These transactions occur in several different forms: as funds transferred over the internet from one financial institution to another, as credit card transactions (a similar, but is it the same kind of transaction?), as a transfers of representations of cash or currency, and as transfers of physical incarnations of wealth: pieces of real estate, cars, houses, etc. As was pointed out in an earlier post in the United States prior to the growth and dominance of the National Bank, individual banks issued their own currencies and backed them with their own assertions of solvency. People were understandably suspicious and held savings as cash. Consequently when a bank failed, the bank's currency failed, and hence the long lines for people to redeem deposits (usually without success). When banks became bankrupt, people holding their currencies lost everything. This raises another question: what is a currency or what is money without the backing of a national government? And what is a currency without the backing of a reliable government, or a solvent government. The images of German people carrying sacks of cash to purchase minor necessities between the war remains haunting and is not singular. So we are back at the beginning of the circle again. Indebted governments abound, borrowing without honest plans for repayment, and being carried along in a porous interlocking international financial system where all must float or sink together. I don't think, however, that Bitcoin is going to be the answer to this instability, nonetheless it is a noteworthy flag. The fact that it went as far as it did says much. Basically it is and was no different than a poker chip. Still, assets don't have intrinsic value whether they be gold, guns, bombs, food, gas, pearls, tulips, or cowrie shells, just what we as a society make them to be. When currencies look shaky, assets directly related to safety and sustenance increase in value. I hope economists and historian are noting what is now happening in Syria and Central Africa in this regard, and that they will tell us. I look forward to reading more on this topic.

[Minoru Aosaki](#)

04/20/2014

Though I'm not very knowledgeable about bitcoin, I would like to share my basic thoughts.

My first point is on the question posed by the forum "does bitcoin have a future?" I think our discussion would have developed differently had the question been "do cryptocurrencies or virtual currencies such as bitcoin have a future?" According to Wikipedia (English version), there are over 60 different cryptocurrencies that are, like bitcoin, circulating and being exchanged over the internet. Of course, the value of focusing on

bitcoin is that it allows us to have a more centered conversation. However, if we discuss cryptocurrencies more generally, we can focus our conversation on comparing cryptocurrencies with existing [conventional] currencies. This [focus] will also allow us to discuss how cryptocurrencies might evolve as information technology advances. To use another example, a discussion on whether “iPhones have a future?” would be very different from a conversation on whether “smartphones have a future?”

My second point is on another question posed by the forum of whether “people accept (bitcoin) as money.” I am interested in the social implications posed by how people – however small in number – conduct important transactions (in terms of either amount or nature) through bitcoin. If we define the word “money” by its continuity to its past, [that is, by how it has been perceived], then [our definition of “money”] might not be able to fully capture new developments. If bitcoin is used for money laundering, investment, or some backdoor trade, then it has already achieved social significance.

Finally, in terms of bitcoin’s future, I think there are two important factors to note. The first factor involves political and policy situations. My understanding is that the value of bitcoin rose sharply during the spring of 2013 when Cyprus was facing an economic crisis. [People fled to bitcoin because one of the] conditions proposed to Cyprus for receiving monetary support was to tax its bank deposits. Should [some other country] face a major financial crisis in the future and enforce similar policies, there is a possibility that there will be an increase in bitcoin users in that country. In at least that country, therefore, bitcoin may be perceived as money. The second factor is innovation. For example, the iPhone became very popular around the world very quickly because its interface [is so simple] that users do not need to read a manual. If cryptocurrencies experience this kind of innovation, making them more usable for the general population, then perhaps bitcoin will also have a future.

Bill Maurer

04/21/2014

I've appreciated the discussion on this forum so far - thank you to my colleagues!

Another interesting thing about bitcoin is that there is an upper limit to the number of bitcoins to be produced. For the bitcoin-as-money proponents, this provides the “scarcity” necessary for “value.” Leaving aside the digital bullionism here, what happens when all the bitcoins are mined? Well, the theory goes, the miners all turn themselves into payment processors, charging a fee to verify transactions. But there is something much less sexy about being a “payment processor” compared to being a “miner,” and also, becoming a payment processor opens the door to that which many bitcoin proponents most abhor—the “middleman”! The question, “does bitcoin have a future,” for me, really hinges on what happens when the upper limit of bitcoin production is reached. [This is to leave aside a technical issue that my cryptography colleagues in computer science and industry point out, which is that, the processing power required globally to run the bitcoin system as we approach the upper limit of coin to be “mined” becomes so intense that, as one engineer told me, “we’d need all the power of the sun, and all the tar sands of Canada, to make it work.” This is clearly not sustainable, in all senses of the term.]

Where does this leave us? In the US, bitcoin is simultaneously regulated by the Financial Crimes Enforcement Network (FinCEN) of the Dept. of Treasury in terms of “money transmission” regulations—

which, in a wonderful irony for the anti-federalists, are done state by state—and by the Internal Revenue Service as “property”—not as “money.” The State of California is pursuing new regulations to continue to permit the kind of innovation bitcoin has unleashed while ensuring there are clear lines of liability. Lots of startups are seeking to create products that make bitcoin or things like it more user-friendly, others are creating products modeled on bitcoin’s protocol, and others are seeking to “build out” what can be done with a block-chain protocol like bitcoins for the conveyance of other kinds of data that have similar qualities to money (qualities like the double-spending problem), notably, Ethereum, which may end up providing a way to do things like deeds and mortgages. Potentially interesting, but... a future for bitcoin? Perhaps not.

One has to wonder rather why bitcoin has captivated the imagination at this juncture. To me, that it has done so says more about the failure to imagine a future for the public interest or the state than the imagination of the future of money. This is where my colleagues and I are now beginning the next phase of our inquiry.

[Kaja Tretjak](#)

04/22/2014

Many thanks to all for the discussion so far!

On the inflation, value & related monetary arguments: As was pointed out with regard to Keynesianism, views here will be in large part informed by the underlying economic analyses and theories of value. Presently, some of the most vehement advocates of Bitcoin ground their perspectives in the Austrian school of economics, while rejecting the “inherent value” argument as traditionally formulated (and have thus found themselves expressly at odds with many of that tradition’s contemporary key figures, who remain advocates of gold/valuable metals as means of exchange – an interesting development in the history of that school in its own right). I simply intended to point out the inflation concern as one element of Bitcoin’s appeal for many in the current context rather than situate it as a broader significance of the protocol.

Rather, as several comments have noted, one element of the social significance of the protocol lies in its implications for further developments in both payment systems and related data transfer. For example, Bill Maurer refers to Ethereum – the [“smart contracts” wiki](#) is a nice starting point for further information. See also work on [distributed autonomous corporations](#).

I also find his observation regarding defending “the state” crucial. The appeal of these developments signals a broad-based cynicism toward and disenchantment with “state processes” and formal political institutions as a means toward promoting “the public interest.” I would caution against collapsing this dynamic with the US right, although there are surely overlaps. I am particularly interested in contemporary reconfigurations of the political “left” and “right” in the US context whereby we are witness to the resuscitation of various anti-statist lineages associated with what could roughly be termed the political left but not prominent in US politics since the 19th century. My dissertation on the present revival of US libertarianism, grounded in over two years of ethnographic fieldwork with various parts of the liberty movement, in part explores the journeys of young people from Ron Paul’s brand of libertarianism (which remains alive and well) to the building of liminal spaces drawing on the work of thinkers such as Proudhon, Benjamin Tucker, etc. ...In this sense the appeal of the Bitcoin protocol is one piece of a broader set of developments in how significant numbers of millennials in particular wrestle with and understand existing political economic arrangements.

Chris Gregory

04/29/2014

'Money has functions four: measure, medium, standard, store.' By these criteria the bitcoin is dysfunctional as money. As standard of value, for example, the price of money should be invariable and bitcoin fails spectacularly on this score. The bitcoin scores well on mathematical beauty and this, as Professor Iwai notes, has captured the hearts of the mathematically-inclined free-market anarchists who inhabit hyperspace. But the bitcoin's mathematical beauty cannot compare with that of Piero Sraffa's standard commodity which defines the conditions necessary for a medium of exchange to function as a perfect invariable standard of value. Sraffa's world is a free-market anarchist's paradise: commodities are produced by means of commodities free of the state intervention and without the need for banks. The standard commodity functions as a perfect measure, medium, standard and store because its price is invariant to changes in the distribution of incomes between capital and labour; it is the perfect numeraire because its price is always equal to one. But Sraffa's world is one where the economy is in a self-replacing state: output does not change and nor do the proportions in which different means of production are used by an industry. Such a world is the stuff of fantasy but it does mean that no commodity – be it gold, the US dollar or the bitcoin – can ever hope to fulfil money's functions four because no price is ever invariant. Monetary dysfunction, then, is the norm but some things function better as money than others. The gold bugs of yesteryear were the ultimate free-market anarchists and the relative stability of the gold-silver ratio of 12:1 underpinned their faith in the capacity of these two metals to function as money in a fourfold way. The stable 12:1 ratio – the greatest constant in economic history prior to the 1870s – was, after all, in line with their planetary analogues. Britain and USA as imperial states managed to turn their own currencies into a global standard by fixing the price of gold. But empires rise and fall: the supremacy of the UK pound is long gone and Nixon's decision to close the gold window in 1971 was the beginning of the end of the US dollar. The rise of China as an imperial power raises interesting questions about the future of a global standard of value because, unlike previous imperial powers, China's central bank holds a relatively small gold stock (1% of foreign reserves compared to 76% for USA and 70% for Germany). Currency wars between the US and China will define the meaning of money over the next decade or so. Mathematical solutions to the problem of money of the kind that Nakamoto has developed for his bitcoin will never solve the problem of money's functions four. Mathematical solutions will always be fantastic and will arise and pass away like the daily sun. Sraffa's fantastic standard commodity has the advantage that it will not pass away because it never arose and never will; its mathematical beauty and monetary perfection is a reminder that money is a political problem not a mathematical one. Bitcoin's future will be only assured if Nakamoto and his band of free-market anarchists can manage to seize world power.

Hirokazu Miyazaki

04/29/2014

The question of whether Bitcoin has a future may not turn on the question of whether Bitcoin is money. What if we thought of Bitcoin as a space of experimentation for computer programmers who are working out technical problems and generating ever more elegant solutions? One of my students, a computer programmer, is currently doing research on Altcoins and various technical innovations being made in these alternative cryptocurrencies. His research has reminded me of the old anthropological commitment (most powerfully articulated by Karl Polanyi and his students) to ethnographic investigations into what happens

around money rather than the question of what money is. The future of this experimental space may reside in those aspects of cryptocurrency that are only tangentially related to the problem of money.

[Chris Gregory](#)

04/30/2014

Hiro is right to note that the future of Bitcoin may not turn on the question of whether Bitcoin is money. But it will turn on the question of its price as a commodity. All money forms circulate as commodities but not all commodities function well as money. The reality is that Bitcoin circulates as a commodity with a price; it is also has served some monetary functions for some people. It is the former that matters. Its US dollar price was around \$100 in October 2013. It rose to over \$1100 in December and has been falling ever since. It is currently around \$400. Who knows what the future will bring but the graph of its price has all the classic signs of a speculative bubble.

Is it useful to think of Bitcoin as a space of experimentation for computer programmers? The Bitcoin as precious metal image comes to mind as I ponder this question. If Bitcoin has 'miners' is not this 'experimental space' analogous to the territory geologists cover in their search for new minerals? If Hiro's student can find a new commodity whose price rises from \$100 to \$1100 in the space of a few months it would certainly attract a lot of interest.

[Bill Maurer](#)

05/01/2014

Nice comment, Hiro! I spent the whole day yesterday with a group of engineers and computer scientists from a major IT company that shall remain nameless, brainstorming on bitcoin. (There were also anthropologists, economists, and two payments lawyers). It was a 7-hour, intense discussion, so a lot happened. But two core questions were 1) what questions or element of popular consciousness does the btc phenomenon point to? and, separate from that, 2) what else can you do with a blockchain? There was the recognition that (1) does not equal (2). We got into a huge discussion about third parties and trusted intermediaries: are there currently "inefficient" processes requiring trusted third parties where the trade off between eliminating the third party and the protections a third party affords is outweighed by the efficiencies thereby created. And guess what the lawyer offered? He suggested that if there were a blockchain-like method for recording mortgages before the global financial crisis, the whole thing would have unfolded differently (he did not say it would never have happened). There are many cases now in the courts where "no one can locate the mortgage note - no one really knows who holds the note!" With a blockchain database you eliminate that problem, and you eliminate the intermediaries who are charged with tracking the note. This led to the "what ELSE could you do with the blockchain?" discussion. People offered: 1) enabling a personal data economy, where I have more control over my data's use by allowing the consensus model of the blockchain to validate use (among other ideas); 2) eliminate third parties (escrow was offered up for sacrifice!); 3) provide a platform for collaborations in which each party is only allowed access to a piece of a project, and the other parties' segments are hidden; 4) replace contract (!) and/or develop a new vision of social contract (with the consensus validation model of the blockchain). There was discussion of whether, given first-mover

advantage, btc achieves a position in the hierarchy of cryptocurrencies such that transactions among alt coins can continue until someone wants to convert "up" to fiat currencies, at which point btc makes the bridge - becomes the payment rail between alt coins and US dollars, say. At this point, one of the engineers pointed out the heavy computational and energy needs of btc -- as he had said to me earlier, "you'd need all the energy of the sun!" It was a fascinating day, and showed exactly what Hiro is suggesting: at least some of the engineers and computer scientists involved are already "beyond" the money question, and on to experimentation "around" money, seeing what else btc provokes. I should add: for those who are interested, I'm teaching a class on bitcoin, wholly online, this summer at UC Irvine -- all-comers are welcome (<https://summer.uci.edu/courses/sectiondetail.aspx?serialid=70095&session=S2> - for a fee, and note that it actually begins in June - there's still an error on the website - oh, all the ironies here! But please pass it on to your students!)

[Douglas R. Holmes](#)

05/04/2014

I fully agree with every aspect of Bill Maurer's post of April 21. He and his colleague are doing superb work on central bank payment systems and related issues such as bitcoin.

I have a brief aside regarding the last paragraph of his April 21 comment.

J. M. Keynes noted somewhere (unfortunately, I don't have the [citation](#)) that as the fierce debates on the gold standard unfolded in the late nineteenth and early twentieth centuries; few people recognized a revolution in finance taking place literally at their fingertips. The increasingly widespread use of personal checks during this period meant that people could with a few pen strokes create money.

Bill's comment is compelling and apposite. As he suggests, what is worrisome about bitcoin, like gold, is that it might distract us from what are the profound transformations of money and monetary affairs of our time.

[Alberto Corsin-Jimenez](#)

04/30/2014

This has been a most suggestive discussion, for which I would like to thank all contributors. So suggestive, in fact, that I want to make a brief intercession myself.

I am no expert on money or Bitcoin, so I hope I am not stating the obvious. I have been working for over four years now with open-source hardware hackers (architects, for the most part). They seem themselves as belonging to a global peer-to-peer (P2P) and open-source community -- where discussions about Bitcoin have become part of our daily digest.

Briefly, I thought I'd say that it seems to me that the discussion has conflated two separate and rather different questions: "Is Bitcoin money?" and "Does Bitcoin have a future?".

Most of the conversation thus far has centred on whether Bitcoin is or is not money – and the discussion about its future has been taken from here. Thus, the question about Bitcoin’s future has actually been posed as a question about the future of Bitcoin as *money*.

But of course Bitcoin can have a future as something other than money. And in fact most of the hackers that I work with talk excitedly about Bitcoin not in terms of its innovation as a currency, but as a cryptographic system. Everyone is excited about the possibilities that Bitcoin’s cryptographic developments open up.

I think this is interesting because (for some members of the P2P community at least) it displaces the question about currency and value to a question about communication, transaction networks and anonymity. These dimensions of Bitcoin can be seen as looking glasses to rethink theories of money but they can also be used to rethink other forms of communication and exchange.

In the long term, then, perhaps Bitcoin’s future is secured to the extent that it offers new ways to thinking about what a digital signature, a digital certificate or, more broadly, a digital identity is. These may or may not map neatly onto existing social and political categories. My guess is that they won’t. So it is perhaps in this guise that Bitcoin will double back and return in the future as a challenge to how we think about money.

[Meridian 180 Team](#)

05/06/2014

Thank you so much for posting these wonderful comments. Just a quick reminder that this forum is scheduled to close on Friday, May 9. We will be accepting comments until 5 pm that day. We look forward to hearing from more members in the remaining time!

[Daromir Rudnycky](#)

05/07/2014

This has been a great discussion. Thanks to all as I’ve learned a great deal about bitcoin and, more importantly, ways to think about it. One way to address the question of whether bitcoin is money is to consider the governance dimension. If money is a technology of government, both of the self and others, we might ask what kind of governance bitcoin entails?

Earlier on in the discussion Chris Gregory noted that bitcoin was especially popular among self-styled “free-market anarchists” who populate the internet, which sounds right to me. Recently I watched this short [video](#) by the Guardian on bitcoin.

What struck me in the [video](#) was that the main problem that bitcoin solved was in structuring a payment system without an intermediary authority to vouch for those making payments within the system: what the video labels the “double spending problem.” In other words, the role of banks in dominant payment systems is to ensure the veracity of one’s credit. If the banks are removed, then how can anyone trust anyone else? Thus, the authority of banks is their role as guarantors of commercial trust.

Nakamoto's intervention was to usurp the role of banks in guaranteeing commercial trust by designing a system in which "all of the users would record all of the transactions at the same time." Essentially bitcoin devolves the sovereign power to mediate credit from banks to the individual users who participate in the system, each one monitoring the financial responsibility of all the others through the internet.

What is interesting is that these "free-market anarchists" promoting bitcoin are in fact devolving the government of others to the individual members who participate in the system. If this is correct then, contrary to their claims and self-representations, bitcoin appears a whole lot less like anarchy and much more like a liberalism with we have much deeper familiarity

[Katsuhito Iwai](#)

05/12/2014

When I wrote the initial post for this forum, I did not expect to receive so many interesting responses from such diverse academic backgrounds. I would like to thank all of the contributors for their efforts to keep this forum going. Some of the contributors have succeeded in expanding the scope of the forum to think about larger issues such as, to borrow Miyazaki's nicely put phrase, bitcoin as a space of experimentation on libertarianism, cryptography, etc. I would like to follow up on these new developments.

1. I remarked in my previous posts that people accept money as money simply because they expect others to also accept it as money. It is "the others' wants," not my wants, that give money its value as money. The value of money is thus intrinsically "social." But, as fundamental as this proposition may be, if we stopped here, we would miss the essential difference between commodities (goods and services, including financial instruments) and money. This is because it is also "the others' wants" that give any commodity its value as a commodity. Grocers treat an apple in their stores as a valuable commodity not because they themselves want to eat it but because they expect others (buyers) to want it. The value of any commodity is also intrinsically "social." The decisive difference between commodities and money emerges only when we ask those who have bought an apple and those who have accepted money respectively why they have done so. The former would answer "because I want to eat it," unless they are confectioneries or gift-givers. The latter would, however, answer "because I also expect others to accept it as money," and if we would repeat the same question to those others, those others' others and so on, the same answer would come back indefinitely.

One reason I have reiterated this point (sorry for my penchant for repetition) is to emphasize again that the mere spread of transactions does not necessarily turn bitcoin into money, as some commentators seem to believe. It has so far only made bitcoin a commodity, albeit a very valuable commodity currently worth 400 dollars per unit.

Another more important reason is to note that Mmoney may – but only "may" – evolve spontaneously without any communal decree or state sanction if by some chance many people simultaneously start to accept the same thing in exchange for other things merely because they expect others to accept it in exchange for other things. Carl Menger, the founding father of the Austrian school, indeed claimed in his 1892 paper that money is "the spontaneous outcome, the unpremeditated resultant, of particular, individual efforts of the

members of a society.” His “invisible-hand” account of the evolution of money is probably the most influential source of the libertarian theory of money, including that of Hayek.

Yet, the third reason is that... this bootstrapping nature of money also allows money to dissolve spontaneously, in the form of hyperinflation, bank runs, liquidity crisis, etc. The value of money, even in the case of gold and silver, necessarily exceeds its value as a thing, for otherwise people would use it as a piece of ornament or a cap on tooth, never parting with it as money in exchange for other things worth only its monetary value. It thus has no “real” foundation to support itself. Whenever people begin to worry that many people may not accept money as money, it soon loses its value as money and returns to a mere thing with little value of its own. In order for money to keep its status as money in the long-run it needs a state or a central bank as the regulator of its value or at least as the lender of last resort at a time of crisis. It is to this stability problem that neoclassical economics, especially its Austrian School branch, has been persistently blind. (Hence, our last economic crisis.)

Bitcoin advocates are certainly right to insist that money does not necessarily require any authorization by a state or a central bank for its evolution. But like laissez-faire economists, they are also blind to the fact that money necessarily requires the regulation of a state and/or the intervention of a central bank for its long-run stability. These two propositions appear contradictory on the surface. But, they are merely two sides of the same coin! -- the coin whose inscription is “money is money simply because it is accepted as money.”

As recent comments by professors Bienen, Mauer, Tretjack, Gregory, Holmes, and Rudnycky have all pointed out cogently, one of the intriguing aspects of bitcoin phenomena is it forces us to ask once again fundamental questions about the role of states, central banks, and other public organizations in our computerized global society that are rapidly eroding any kind of “public” authority.

This is all the more intriguing, because many of us believed (naively in hindsight, as Tretjack’s comment has reminded me) that the last global economic crisis (still not completely behind us) spelled the end of laissez-faire economics and libertarian philosophy during the last global economic crisis (which is not however completely behind us). I did not expect them [the libertarians] to reemerge so strongly in the guise of a computer program under the name of bitcoin.

2. I am grateful to professors Aosaki, Miyazaki, Corsin-Jimenez, Gregory and Mauer for having guided us to the world of computer programmers experimenting not only on various forms of crypt-currencies but also on the problems “around” and “beyond” money questions.

The stake is high in their experimentation, because all the unscrupulous programmers in the world craving huge wealth would devote all their talents to cracking those crypt-currencies’ encryption. Perhaps the future of our computerized global society hinges critically on the development of crypt-graphic technologies through competition between good programmers and bad programmers, which may eventually force us to rethink the meanings of individual identity, anonymity, exchanges, networks, and even society itself. Bitcoin may not have a future, but it has the potential to open up a brave new future for our global world, though I am a bit uncertain at this moment if it is for better or for worse.