Bitcoin: Problems and Prospects

George Selgin, Director
Center for Monetary and Financial Alternatives
The Cato Institute
Washington, DC 20005

November 12, 2014

Prepared for Hillsdale University's 2014 Free Market Forum, Indianapolis, Indiana, October 23-25.

Anita Folsom, in inviting me to take part in this year's Free Market Forum, originally suggested that I write about the problems of Bitcoin. Although I suppose I might have done so easily enough, I have chosen instead to review both Bitcoin's problems and its prospects. I've made this choice because, while I recognize Bitcoin's shortcomings, some of which are indeed serious, and while I even go so far as to wonder whether Bitcoins will still exist when this paper appears in print, I nevertheless consider them a wonderful development, and one that holds out som enticing possibilities for the future of money.

Problem: Bitcoins aren't money

Despite their name, Bitcoins aren't coins. They are, instead, a digital payment medium. So you must get out of your minds the image often published along with discussions of Bitcoin of metallic discs with "B"s instead of "$"s on them. Although there are such things, they are not Bitcoins but cute Bitcoin storage devices or "wallets." Apart from making this point I don't intend to go into the details concerning how Bitcoin works, as these have been addressed, and addressed more competently than I could address them, by this session's other panelists.

The fact that Bitcoins aren't actual coins isn't itself a problem. But the fact is that Bitcoins also aren't money of *any* sort, according to economists' standard definition of money as any *generally accepted* means of payment. Nor, for that matter, can the Bitcoin unit be said to serve as a unit of account—one of money's secondary functions—as it might were it both widely used in payments and reasonably stable in value. These facts certainly *do* constitute a problem for Bitcoin in so far as its enthusiasts wish to regard it as a potential rival to the dollar. Though we may not like them or the way in which they're managed, Federal Reserve dollars, unlike Bitcoin, are indisputably money, since they can be used for pretty much any purchase in the country, and even for plenty of purchases beyond it.

Carl Menger, the founder of the Austrian School of economics, explained how any ordinary good might spontaneously become money—meaning, again, a generally accepted medium of exchange.[1] But while Menger's theory, which requires no action by the government, might appear to offer encouragement to those who believe that Bitcoin also may become money, careful consideration suggests that, with regard to the possibility in question, Menger's theory supplies more grounds for pessimism than for optimism. Indeed, the theory suggests that it is highly unlikely, if not impossible, that something like Bitcoin should ever become employed, let alone generally, as a medium of exchange.

This conclusion follows from the fact that, according to Menger, money emerges from a state of barter, and does so as a result of individual traders' efforts to barter more effectively by trading what they have for something that seemse more likely to be wanted by those who have the the goods that the traders really want. As different traders experiement with different media of indirect exchange, a kind of a horse race gets going, with certain indirect exchange strategies involving certain goods succeeding more often than others. The goods that appear most "saleable" then become more widely adopted as exchange media, until eventually one good appears distinctly more saleable than all the others. At that point you no longer have barter: you've got money.

But consider: who, at the beginning of the process Menger describes, would be foolish enough to try trading whatever useful goods they have for something for which *no one* has any real use—that is, for something for which there's initially no demand at all? (Remember, at the start of Menger's process there is no demand for anything as a medium of exchange, the only demand for stuff thing being that of persons who ultimately wish to own or consume, rather than

[1] Karl Menger, "On the Origins of Money," trans. C.A. Foley, *The Economic Journal* 2 (1892), pp. 239–55.

to exchange, it.) So rational traders who opt to try indirect exchange will do so by looking out for things that are popular for reasons unconnected to their potential to serve as exchange media. These might include goods wanted for consumption, like tobacco, or as ornaments or jewelry, like cowrie shells and, of course, precious metals. Who, on the other hand, wants a bunch of digits that, *unless* they've somehow come to be adopted as exchange media, have no other obvious use at all? The answer would seem to be, no sensible person at all! So Menger's theory seems to suggest that Bitcoins, apart from not actually being money, couldn't possibly become money!

Nor is that all. Menger's theory also implies that, once you have enough people using something as a medium of exchange, more and more other people will want to use it for that purpose. A bandwagon is thus set going that ends up having everyone on board. But this means that, once some money is *already* established, it is extremely difficult for another to displace it, assuming that the other starts out as just another valued good. It follows that Bitcoins would be unlikely to displace dollars even if they were useful for something other than exchange. The inescapable conclusion seems to be that, when it comes their prospect of becoming money, Bitcoins are, not merely doomed to fail, but *doubly* doomed.

Prospect: Bitcoins might become money after all.

And yet…despite what appear to be implications of Menger's theory, Bitcoins *are* being employed, if only to a very modest extent, as exchange media. That they've managed to gain a foothold against seemingly impossible odds is fascinating, so so let's talk about how it happened.

Though it is said to have been invented by "Satoshi Nakamoto," the name is a pseudonym that may in fact refer, not to any one computer geek (for all agree that "he" must be such), but to a bunch of them. Apparently these geeks were at first just enjoying themselves with

what was merely a fun (for computer geeks) game won by earning the most points for solving a math problem. In this game Bitcoins were nothing more than a sort of digital play-money used to keep score: the more problems one solved, the more Bitcoins one got. Usually play money just stays play money. But in this case it started to be perceived as having virtues that would make it usefu,l not just for keeping score among players but also for buying and selling stuff—and especially illegal stuff, like drugs—remotely and conveniently, yet still relatively anonymously. At first such dealings were presumably confined to a small circle beyond the original players themselves. But then the distinction between players and traders began to blur. Eventually people were trading for Bitcoin who had no interest in the original game at all, and who might not even have qualified as geeks, computer or otherwise.

According to Menger's theory, if something manages to get adopted at all as an exchange medium, it becomes more attractive for others to adopt it. So once Bitcoins' circle of users had widened enough, it started to widen faster and faster. Today more than 75,000 merchants in the U.S. alone, including some major ones, accept Bitcoins, and they are fast becoming the preferred medium for overseas workers' remittances. I recall pointing out, only two years ago or so, that the number of Bitcoin-accepting merchants then had reached about one-thousand, and that it was likely to reach ten thousand in another year. That gives you some sense of the acceleration.

In principle this acceleration could go very far: far enough, even, for Bitcoins to qualify as money. Certainly it has gone much further than we experts once thought possible. Bitcoins has taught us all a valuable lesson, which is that we must not be too quick to assume that something isn't useful enough to become money, simply because we can imagine no possible (non-monetary) use for it. Usefulness, like beauty, is in the eye of the beholder.

Problem: if Bitcoins do become money, they won't be a very good money.

So Bitcoins, though they still have a very long way to go, might yet become money. It's even conceivable, though still exceedingly unlikely, that they might come to be preferred to dollars, and so give rise to a Bitcoin economy. In that economy dollars would themselves be useless, either as convenient exchange media or as representatives of the unit of account, and we would no longer have to worry about the Fed mismanaging the money stock. Instead we'd have a Bitcoin supply that's strictly regulated—predetermined, in fact—with the supply rising at a gradually declining rate toward a limit of 21 million Bitcoins. Hyperinflation, or even inflation at more modest rates, would therefore be highly unlikely.

That's the good news. But there's bad news as well. Part of the bad news is that there's no reason to suppose that either the purchasing power of Bitcoins or the total volume of Bitcoin spending or "nominal income" would be stable. Today of course it's evident that the value of a Bitcoin fluctuates a great deal. But "value" here refers to the Bitcoin-dollar exchange rate. In a Bitcoin economy the only sort of stability that would matter would be that of Bitcoins' value relative to goods. In such an economy the real demand for Bitcoins would also be more stable than it is today, with speculative demand (as opposed to demand for making payments) playing a much less important role than it does now. For that reason Bitcoins' purchasing power in a fully "Bitcoined" economy would almost certainly be considerably less volatile than the present Bitcoin-dollar rate. So it's a mistake to assume that the instability of Bitcoin as money would mirror or resemble the instability that it has today as an aspiring money only.

It doesn't follow, however, that either Bitcoins' purchasing power or the volume of Bitcoin-denominated payments will be stable enough to make Bitcoins anyone's idea of a sound money. Because it makes no allowances for changes in the real demand for Bitcoins, whatever

their source, the strict "protocol" that regulates the supply of Bitcoins—a protocol that raises Bitcoin "mining" costs in response to changes in mining activity and technology, but without regard to Bitcoins' purchasing power—would allow fluctuations in the pure transactions demand for Bitcois to continue to influence their purchasing power. As the number approaches 21 million, mining costs will approach infinity, and Bitcoin output with cease once and for all. The transactions demand for Bitcoins will, in contrast, tend to go on increasing with economic growth. A Bitcoin standard would thus tend to result in a rate of deflation at least equal to the rate of economic growth, with occasional bouts of more severe deflation occusing with every cyclical increase in the demand for money. Although (as I've argued elsewhere) deflation needn't go hand-in-hand with recession or depression so long as the rate of deflation reflects an economy's (total factor) productivity growth rate, chances are that deflation in a Bitcoin economy would frequently exceed this safe limit.[2]

To put this consequence of a Bitcoin standrad in perspective, let's compare it, not just to the current dollar standard, which tends to be inflationary, but to the classical gold standard, which many regard as the best international monetary arrangement yet seen. Unlike a Bitcoin standard, the gold standard didn't involve a strictly fixed supply of basic money. Instead, that supply grew over time—and did so even despite widespread use of bank deposits and notes backed by fractional gold reserves as substitutes for actual gold coins. What's more, it tended to grow more rapidly as the purchasing power of gold increased, and vice versa. So while the gold standard also permitted some deflation, the deflation was—banking crises aside—not severe enough to impede economic growth. Moreover, it served to encourage more aggressive gold prospecting, as well as resort to previously uneconomical extraction methods, that in turn tended

[2] See George Selgin, *Less Than Zero: The Case for a Falling Price Level in a Growing Economy* (London: Institute of Economic Affairs, 1997).

to offset mildly inflationary stretches with mildly inflationary ones. Thus the t by equally mild inflation, which meant that the price level tended to be very stable over long periods—stable enough, in fact, to make it safe for people to deal in fixed-interest bonds of very long maturity.

In short, a Bitcoin standard is likely to be inferior to the classical gold standard which, though better than most other monetary arrangements, was itself far from perfect. What's more, it might even prove inferior to the dollar standard, if one allows that that standard, though inflationary, might not prove exceedingly so, and might at least avoid severe deflation except on rare occasions.

Prospect: a modified version of bitcoin could be very good money indeed.

Bitcoins are the only cybercurrency to achieve any relatively wdespread use thus far. But other such currencies, generally known as "Altcoins," also exist, and it is conceivable that one of them, or perhaps some yet to be invented cybermoney, might prove still more successul, while also having features that could in fact make it the best money ever.

To see how the technology upon which Bitcoin and similar cybercurrencies could serve as the basis for a truly superior monetary standard, we must first step back and have a look at the problems inherent in the non-cyber monies of the past. On the one hand there are fiat monies like the dollar, the quantities of which can be arbitrarily manipulated by a body of people making discretionary decisions. When such discretionary management goes awry, the results can be very bad news indeed. True, the dollar is in this respect better than many of the world's other fiat monies, but even it isn't particularly great. Fed officials insist, for starters, on treating two percent rate of inflation as rock bottom, even though that means cutting the dollars value in half every 36 years. In practice the Fed's stance means, that we can usually expect the dollar to loose

value even more rapidly than that, in addition to having to put up with booms and busts brought about at least in part by the Fed's tendency to stoke the former while mismanaging the latter.

But ordinary commodity monies, which have been the only alternatives to fiat money so far, are also imperfect, as the example of gold—perhaps the best of the lot—makes clear. Gold discoveries can cause it to depreciate, while a decline in the nonmonetary demand for gold owing, say, to a general switch from gold to silver fillings, can do the same.

To be fair, most critics of the gold standard who mention these possibilities exaggerate their historical importance. For example, although it involved a five-fold increase in European prices over the course of a century and a half, the so called "Price Revolution" that followed the Spanish conquest of New World gol and silver mines, translated into an average annual inflation rate below the Fed's present inflation *target*. It remains true nonetheless that the supply of any ordinary commodity money must be subject to the whims of mother nature in the same way that fiat money is subject to the whims of central bank governers.

Which brings us to the nifty thing about Bitcoin-type cybercurrencies. In principle, the same sort of people who came up with the Bitcoin supply protocol could also come up with a much more macroeconomically "smart" protocol that could be the basis for an exceptionally stable and well-behaved cybermoney. The new protocol might, for example, allows for long-run growth of the money stock, consistent with increased real output (or perhaps with increased labor and capital input), while also allowing for cyclical adjustments based upon feedback from transactions volume. The supply of such a "smart" cybercurrency would therefore remain beyond the power of anyone to manipulate, yet would also be "elastic" in a macro-economically desirable way. You really couldn't ask for anything much better.[3]

[3] For more on this topic see my article "Synthetic Commodity Money," forthcoming in the *Journal of Financial Stability.*

Problem: bad cybercurrency might drive out good cybercurrency.

Alas, I find I must I end with a problem, and hence on a negative note. The problem is that, although a very good cybercurrency can be created, it won't necessarily be the victor of open competition with inferior cybercurrencies. I say this, by the way, despite being a big fan of the general idea of currency competition, which I've spent much of my career defending, and despite the fact that I would nonetheless like to see Bitcoin and other such currencies compete freely against established fiat moneys. That is, I very much favor having a level currency playing field, with no laws serving to artificially raise the relative cost of using any particular type or brand of money, such as the recently-adopted IRS ruling classifying Bitcoins as a commodity and thereby subjecting their sellers to a capital-gains tax.

The problem is that, even with such a leval playing field, an ideal cybercurrency, assuming such a thing really does exit, would be unlikely to compete successfully on it. It would, first of all, have a hard time outcompeting the present U.S. dollar, or any other well-established fiat money, for reasons I've already explained. But the problem is more serious still, for even if the best possible cybercurrency only had to compete against rival cybercurrencies, including Bitcoins, there is no good reason for assuming it would win.

Here, too, part of the problem is that among cybercurrencies Bitcoins already enjoy a considerable first-mover advantage. But there's more to it than that. To see what the deeper problem is, we must consider Friedrick Hayek's theory of how currency competition might work, as given in *Denationalisation of* Money, the work that really got the private currency movement going.[4] Hayek's arguments in that book have proven prescient in many ways, and

[4]F.A. Hayek, *Denationalisation of Money: The Argument Refined* (London: Institute of Economic Affairs, 1978).

especially by anticipating the possibility of "private" fiat monies. Of course, as we've seen, and as Bitcoins demonstrate, the line between a commodity and a fiat money turns out to be a lot blurier than economists had realized; but in any event Bitcoins and Altcoins, allowing for their very limited success thus far, come very close to representing what Hayek had long ago imagined.

The rub, though, is that Hayek took for granted that competition among different "fiat" currency issuers would favor those offering currencies with the most purchasing power, while forcing others out of business. It all sounds reasonable if you're talking to economists because economists tend to treat stability of purchasing power as proof of a currency's soundness. The problem is that it doesn't at all follow that *consumers* of currency, that is, those actually deciding which currencies to accept in exchange and to hold among other assets, aren't inclined to adopt a similar, macroeconomic perspective. They will, first of all, favor (as has now been stressed many times) a currency with a wide network of users over one with a narrower network, *ceteris paribus*. They are also likely, other things equal, to favor, not a cybercurrency that has stable purchasing power, but one that appreciates, and the more rapidly the better, as it resides in their computers' memory or some other cyberwallet. Currency consumers, in other words, thinking only about what goes on in their own wallet and not about the economy as a whole, might select that currency which promises to bring about the most severe deflation![5]

[5] Hayek also imagined that fiat currency issuers could assure consumers of their currency's performance simply by pledging to maintain the currency's purchasing power—with loss of reputation sufficing to make them honor their pledges. In fact this argument seems mistaken, for it overlooks the possibility that by breaking their promises once and for all issuers might profit enough to feel more than adequantely compensated for the loss of their reputations. See Lawrence H. White, *The Theory of Monetary Institutions* (Oxford: Basil Blackwell, 1990), pp. 227-39. Bitcoin-type cybercurrencies address this problem of assuring their users against abuse using tamperproof quantity protocols instea of mere future purchasing-power pledges.

In short, although a very high quality cybercurrency is possible, it is not at all clear that such a cybercurrency would displace inferior rivals even if all competed on a leval playing field and (to mix metaphors) began the contest lined up at one starting gate. This means, ironically I suppose, that while fans of private cybercurrency may take pride in the possibility that they have discovered the means for building a better mousetrap than governments have ever come up with, they might have to depend on at least one of those governments to embrace their invention—and even rule out potential rivals—to see it prosper.

So, I end on a problem, and a rather dismal one at that. I hope that Anita will be satisfied. I, on the other hand, can't help feeling just a wee-bit depressed.