Forbes

Four Reasons Bitcoin Is Worth Studying

By: Timothy B. Lee – April 7, 2013

As Adam Ozimek points out Bitcoin has so far largely been greeted with eye-rolling by professional economists. One reason is that the cryptocurrency's most enthusiastic advocates tend to subscribe to a hard-money, end-the-Fed worldview that is unpopular among elites. That has caused the latter toreflexively take the opposite view, treating Bitcoin as primarily a monetary policy experiment and predicting its doom.

My sympathies are with the pros here. Fiat currency isn't perfect, but I think alternatives like the gold standard would be worse. But Bitcoin is a more than a gold standard for the Internet age. It's the world's first fully decentralized payment system, combining the irreversibility of cash with the convenience of electronic payment. There's never been anything quite like it before, and as a result it poses a number of interesting intellectual puzzles. Here are four examples.

Monetary economics

What gives money its value? One popular theory says that modern fiat currencies get their value by "government fiat": the government declares a currency to be the official one, requires that currency be used to compute and pay taxes, and thereby confers value on what would otherwise be worthless slips of paper.

Bitcoin is a clear challenge to that view. It has no "backing" from any government or other large institution, yet the stock of outstanding bitcoins is now worth more than $1 billion.

The conventional response is to dismiss Bitcoin as merely a bubble, with no intrinsic value at all. But that view makes it hard to explain the events of late 2011. The value of Bitcoins fell from $32 in June to $2 in November. Then the price started going up again, rising to $4 in December 2011 and to $7 in January.

That should surprise you. Even after watching the value of their previous investments decline by a factor of 16, a critical mass of Bitcoin enthusiasts was prepared to pour millions of dollars into the currency. It's possible, of course, that all those people were delusional. But it's at least possible they saw something the rest of the world didn't. Certainly, that was the conclusion I came to. I rethought my previous skepticism and bought some Bitcoins of my own in early 2012.

Even if you think the current value of of more than $140 is a bubble, it's clear that Bitcoin has *some* genuine applications. The number of daily Bitcoin transactions has soared from around 1000 at the beginning of 2011 to about 50,000 today. Figuring out the “fundamentals” that drive the currency’s long-term value seems like an interesting theoretical puzzle.

Political philosophy

The great technological feat of Bitcoin is its solution to the “double spending problem.” The cryptographic protocols needed for one currency holder to “sign over” his currency to another have been well-understood for decades. But no cryptographic operation can prove you haven’t given the same coins to someone else. Before Bitcoin, the only known way to address this issue was to have a centralized transaction register. Control over that list was inevitably a point of control for the currency as a whole.

Bitcoin uses a clever scheme to maintain a fully decentralized transaction register, preventing double-spending without giving anyone *de facto* control over the system. The global, shared register of Bitcoin transactions is called the blockchain, and it’s organized into “blocks.” One block is added approximately every 10 minutes. Each node in the Bitcoin network creates a candidate block and then races to solve a difficult mathematical puzzle that takes its block as an input. The winner of the race gets to add its block to the blockchain, and in that block it can credit itself a fixed number of new bitcoins (currently 25 BTC) as a reward for participating in this process. All bitcoins now in circulation were originally created by this process, which is known as mining.

When a new block is announced, the other nodes in the network confirm that the proposed block follows all of the rules of the Bitcoin protocol. If it doesn’t, the block is discarded and the other nodes continue working on their own candidate blocks.

A few weeks ago, a node that had upgraded to version 0.8 of the client softwaregenerated a block that nodes running version 0.7 and earlier didn’t recognize as valid. This produced a “fork” in the network, with each half generating blocks the other half viewed as illegitimate.

If this situation had continued unchecked, it would have led to chaos, because it would have allowed hackers to spend the same bitcoins twice: once in the 0.7 version of the blockchain and again in the 0.8 blockchain. Fortunately, the most influential members of the Bitcoin community moved quickly. They made a judgment call that it would be easier to get 0.8 nodes to downgrade than to get the older nodes to upgrade. They persuaded those who had upgraded to 0.8 to downgrade, abandoning the blocks they had created since the fork and accepting the 0.7 branch as the official one.

It was important to move quickly because the stakes were growing higher with every passing hour. Every few minutes another block was added to the blockchain, earning its creator about $1000. For many of the miners, abandoning the 0.8 branch meant giving up thousands of dollars in cold cash. The longer the fork had lasted, the bigger the financial hit they would have needed to take to heal the rift.

A core part of Bitcoin’s appeal is that it’s not under anyone’s control. Supposedly, nobody has the authority to change the Bitcoin money supply, cancel or reverse transactions, or otherwise change the attributes of the protocol. But in practice that’s not really true. In the wake of last month’s fork, the elites in the Bitcoin community effectively changed the rules in a matter of hours. In principle, there’s no reason those same elites couldn’t make other changes to the Bitcoin protocol.

There’s a direct parallel here to issues of political legitimacy in a nation state. In principle, most democratic nations have constitutions that bind the behavior of government officials. In practice, a cabal of elites can and regularly do change those rules with minimal input from the rank and file. Yet the discretion of elites is not unlimited. In the case of both Bitcoins and nation states, it’s easy to make changes that will be intuitively appealing to the broader public. But even a broad coalition of elites may not be able to make changes that are strongly opposed by rank and file members of the community.

Economies of scale and competition policy

When Bitcoin is described as a decentralized system, a key assumption is that no single party controls a majority of the network’s computing power. The randomized process for deciding who gets to create the next block effectively works on a “one CPU cycle, one vote” principle. If any single party gained 51 percent of the network’s computing power, it could effectively take control of the network, ignoring blocks produced by the other 49 percent of the nodes. A successful attacker could not only claim 100 percent of the mining profits for itself, it would also gain the power to block transactions it didn’t approve of by simply not including them in its blocks.

Early in Bitcoin’s life, this wasn’t a cause for concern because the barriers to entry was very low. Anyone could download the Bitcoin client onto his computer and run it. But a technological arms race has made Bitcoin mining an increasingly esoteric business. Today, the leading miners use custom-built Bitcoin mining gear that costs thousands of dollars. Indeed, this high-end hardware is so much more energy-efficient that conventional PCs are no longer energy-efficient enough to make Bitcoin mining profitable.

As a result of this and other factors, Bitcoin mining has become increasingly centralized. Bitcoin miners have organized themselves into “pools” that cooperate and share the spoils among their members in proportion to the computing power they contribute.
If this chart is to be believed, the top two pools control 53 percent of the Bitcoin network’s computing power.

In principle, these two pools might be able to join forces and execute a 51 percent (or 53 percent) attack on the rest of the network. But doing so might prove foolish in the long run, since that kind of power grab might undermine public confidence in the currency’s long-term viability, since a mining cartel might have the power to change the rules of the Bitcoin protocol in ways that benefit themselves at the expense of ordinary users.

Data

Imagine if Visa were to give researchers a complete record of every transaction it had ever processed. That database would provide the raw material for numerous studies on consumer spending patterns, the business cycle, and much more.

The decentralized nature of the Bitcoin protocol means that every transaction is automatically published to the world. To be sure, there are some limitations to its value for research purposes. Users can and often do make up new addresses for each transction, making it hard to tell which transactions were made by the same person. And the blockchain doesn’t include annotations on why each Bitcoin transaction was made.

Still, a clever researcher should be able to extract a significant amount of useful information. For example, many companies and individuals publish official addresses for receiving funds. Also, in many cases it will be possible to make inferences about which funds are related by observing when funds are combined and spent together. And at a minimum, you can study things like the volume of Bitcoin transactions over time, the average transaction size, the fraction of bitcoins that are in active circulation at any one point in time, and so forth.

Nothing quite like Bitcoin has ever existed before. Even if you think the current price of Bitcoin represents a ludicrous bubble (for what it's worth, I don't), it's still likely to be a fertile laboratory for testing our economic intuitions.

Disclosure: I own some Bitcoins.

Update: A friend who knows more about economics than me says that Kiyotaki and Wright's account is considered the standard account of fiat money's value in the profession.