CURRENCIES | HULBERT ON MARKETS

Why Bitcoin Will Never Replace Gold

By Mark Hulbert July 31, 2018 8:25 am ET

The more valuable bitcoin becomes, the more vulnerable its network will be, a recent study argues.
KMR Photography

Investors in gold need not fear that bitcoin will replace it as the preeminent global store of value.

That is the implication of a recent study by Eric Budish, a professor of economics at the University of Chicago. The National Bureau of Economic Research published the paper —"The Economic Limits of Bitcoin and the Blockchain"—in June.

Budish, in effect, argues that bitcoin is destined to play no more than a "bit" role in the global monetary system because, if it were to grow ever more significant, it would become increasingly vulnerable to an attack that could destroy much if not all of its value.

RELATED

Stiglitz, Roubini and Rogoff Lead Joint Attack on Bitcoin

Researcher: Manipulation Helped Bitcoin's 2017 Rally

How Blockchain Could Displace Facebook

Whether or not the fear of such an attack has played any role, however, there is no doubt that bitcoin is in a severe bear market. From a high near $20,000 late last year, the cryptocurrency fell to below $6,000 in late June—a drop of nearly 70%. Though bitcoin has recovered over the

Nevertheless, bitcoin devotees continue to enthusiastically predict that it will someday replace gold to become the global store of nongovernmental monetary value. That would represent a huge growth in the bitcoin market, since the total global stock of gold—around $7.5 trillion, according to the World Gold Council—is more than 50 times greater than bitcoin's total market value.

Why would a much larger bitcoin be more vulnerable? Budish, in an interview, answered that the incentives that currently protect bitcoin from an attack assume that the costs of maintaining the network are greater than the value of attacking it. If the relationship is reversed—if an attack is worth more and maintenance costs fall—bitcoin would be vulnerable.

It's helpful to review the costs required to maintain the bitcoin network. Its integrity depends on a large, anonymous, and decentralized collection of participants verifying all transactions, which in turn depends on those people having a huge amount of computing power and ample electricity (currently 0.3% of total global supply, by one estimate). Budish estimates it now costs $100,000 every 10 minutes to maintain the bitcoin network.

What is the value of attacking bitcoin? It depends on who is doing it. To a speculator with a large short position in bitcoin futures, the value of attacking is the profit he would realize if bitcoin's price were to plunge. In such a case, calculating whether bitcoin is vulnerable to attack is relatively straightforward.

To a saboteur aiming at monetary havoc—think North Korea or Iran—the value of attacking bitcoin is harder to quantify. A good estimate might be bitcoin's total market value, but even that might underestimate what an attack would be worth. Budish half-jokingly points out that the substantial cost of an attack would be "a lot cheaper than nukes."

So long as the cost of mounting an attack is bigger than the benefit someone would get from doing so, bitcoin should remain viable. This has been the case so far.

But the situation could very well change if bitcoin were, say, to grow so big as to supplant gold as the preferred global store of nongovernmental wealth, as some enthusiasts are predicting. Unless maintenance costs grew by a similar proportion—more than 50 times—the network would be vulnerable.

Another way of putting it: Bitcoin's continued viability requires that its maintenance costs grow just as fast as the value of attacking it. That's very expensive insurance. Budish uses the analogy of a home security system: If my house is worth 50 times more than yours, I probably will have a more elaborate security system than yours. But it's unlikely that it will cost 50 times more.

Budish's argument casts a different light on those who are envisioning the day when electricity becomes significantly cheaper and more plentiful, and when the cost of the computing necessary to mine and support bitcoin drops dramatically. These bitcoin

In any case, Budish reminds us, there are cheaper forms of data security than bitcoin's blockchain model—such as distributed databases or ledgers that depend on a trusted party. Bitcoin's devotees are purists who don't like to rely on any third party, however, no matter how trusted. Budish's argument in effect is that they are paying a very high price for their purity.

It's worth noting in this regard, however, that many gold bugs have reached their peace with reliance on a trusted party—which is saying something since they are a notoriously untrusting lot. I'm referring to the widespread popularity of the SPDR Gold Shares exchange-traded fund (ticker: GLD), the largest ETF benchmarked to the price of gold. It promises to own physical gold as full collateral against the shares it issues.

But, needless to say, most (if not all) of the investors who have bought the gold ETF—its market cap is now $32 billion—have not personally verified the existence of that physical gold collateral. That doesn't seem to pose a problem, since investors appear to be content taking the word of the outside firm that periodically attests to the existence of the requisite amount of gold.

That could very well be a model for us all.

Write to Mark Hulbert at mhulbert@marketwatch.com