THE STAHL REPORT COMPENDIUM

April 2017

From the Readers

THE DISPUTE BETWEEN BITCOIN UNLIMITED AND BITCOIN CORE

Q: There is a dispute underway between the aficionados of Bitcoin Unlimited and Bitcoin Core. Would you please explain the dispute?

A: As I understand it, Bitcoin Unlimited is basically a way of reducing the block size so that blocks can be processed more rapidly. Without getting too technical, the same is true of Bitcoin Core, but it addresses the subject of block size with something called Segregated Witness. The idea is to shorten the time it takes to process a block on the bitcoin blockchain.

The market will decide which blockchain version is better. It is not for any one person to make that determination. Since the miners just want to make money; they will back whatever gets bitcoin's price to the highest level.

Several news articles have appeared addressing the possibility of a fight that could result in something called a "hard fork," meaning the bitcoin blockchain, or ledger, would split into two separate blockchains and bitcoin users will be forced to choose one. There are two kinds of hard forks. One occurs when there is unanimity, meaning that all the miners agree on the change. The problem arises in the other kind where there is no unanimity and the result is two different blockchain ledgers.

When the digital currency Ethereum faced a hard fork because there was no consensus on whether to stay with the original ledger (blockchain) or shifting to the new, Ethereum owners received one of each: one unit to be traced through the original ledger (Ethereum Classic) and one through the new ledger (Ethereum). Holders had the option to sell one and buy the other, or keep both. The Ethereum hard fork was event driven.

A certain smart contract called DAO had attracted over $100 million in funding. A hacker discovered and exploited a flaw in the DAO smart contract that would have drained $50 million from DAO investors if the hacker had been allowed to withdraw the funds after the mandatory 30-day waiting period. The hard fork was proposed as a way to stop the hacker from receiving the stolen money. A majority of the mining nodes "forked over" to the altered blockchain that thwarted the hacker, but about 20% maintained the original Ethereum blockchain, which allowed the hacker to withdraw the stolen funds. After the fork, holders of Ethereum had both Ethereum Classic and the new Ethereum. One could decide which to keep or whether to keep both. Based on the price of each, the market seems to prefer Ethereum over Ethereum Classic

It is uncertain whether there will be a hard fork in the bitcoin blockchain. Unlike the Ethereum hard fork, the bitcoin decision is not event driven. It is promoted as a way of speeding up the time it takes to process a block of transactions. I do not think it is an issue of concern. A major difference between Ethereum and bitcoin is that the number of bitcoin that will ever be created is capped at 21 million, all of which will be mined by the year 2140. Even if there is a hard fork in bitcoin, it will not affect the thesis that the finite number of bitcoin make it anti-inflationary.

Bitcoin is a completely voluntary project. Those who work on different ways of improving the bitcoin blockchain do it for free. They are willing to do this because their knowledge of the code in the new version of the blockchain would give them an advantage over other participants. A deep understanding of the code provides an advantage in making applications for the bitcoin blockchain code, just as those who have a deep understanding of the iPhone code have an edge when creating iPhone apps.

Ethereum does not work that way. For Ethereum, the issuance is unlimited. A number of Ethereum are issued every year. The base number increases every year for a target inflation rate of 2% in 153 years. Bitcoin already has a 3% inflation rate, but in two-plus years, it will have a 1.5% inflation rate. Then, in four years, it will have a 75 basis point inflation rate, with continued halving thereafter, such that the all-in inflation rate is 20 basis points a year. However, there is at least a one percent a year disappearance of bitcoins, called bitrot, that occurs because the private access keys are lost.

As a store of value, bitcoin is far superior. The question that one might ask is why the other currencies, like Ethereum, do not just move to a fixed issuance. The answer is that issuance is used by the Ethereum Foundation to subsidize itself. It gets a certain amount of the newly issued Ethereum, which it then uses to improve the system. Ethereum might turn out to be the currency with the best transaction system, because more money is spent on improving the software.

If Ethereum has a better system, there is no reason why one could not trade one's bitcoin on the Ethereum blockchain. If Ethereum is used to facilitate securities trading, there's no reason why bitcoin couldn't be traded on it as well.

In my estimation, bitcoin has an existence as a store of value complete and separate from the blockchain itself. The blockchain is interesting, and maybe the bitcoin blockchain will be better than the Ethereum blockchain, or maybe the other way around. It is unclear as yet which will be superior. However, one must distinguish between a currency that facilitates transactions and one that functions as a store of value. Most of the digital currencies subsidize themselves by having unlimited issuance. You might think of them as a kind of profitmaking enterprise.