HORIZON KINETICS

Cryptocurrency Musings
(February 26, 2018 - An Ongoing Series)

Cryptocurrency vs. Consensus Money: Technology vs. Credibility

It might astonish many people to learn that Venezuela has announced that it will soon establish a national cryptocurrency to be known as the Venezuelan petro. This name has been chosen because the units of petro issued will be backed by 5 billion barrels of petroleum reserves. A newly established government ministry, the Unique Registry of Digital Mining, is busily recruiting miners for the cryptocurrency.

Venezuela is not the first nation to launch a cryptocurrency. That distinction belongs to the city-state of Dubai, which launched emCash, a national cryptocurrency, in October 2017.

None of this has attracted much attention from the traditional media. The little commentary that exists focuses largely upon the fact that electronic payment media is less expensive and faster than conventional money payment, and that, consequently, cryptocurrency is yet another technological improvement, much like a smartphone. Following this logic, the “winner” in cryptocurrency will be that cryptocurrency that is the most technologically advanced.

Thus, the race has commenced to find the next technology champion. There are now about 1,511[1] cryptocurrencies, or tokens, as they are frequently called. Most of them are not operating as actual transactional media; they mostly operate only to the extent that one can purchase their coins—that is, they are not actually functioning as a system that is processing transactions. All of them have impressive white papers that buyers of the cryptocurrencies cannot possibly understand and generally do not take the trouble to read.

Some observers have commented that this is illustrative of classical bubble behavior. These observers are quite right. Thus, one might be easily tempted to include Venezuela and Dubai as two nations that have simply chosen to join the cryptocurrency madness. This might also be true.

However, even the truth can be misleading. For example, consider the many attempts to establish a search engine for the internet, most of which are now forgotten. Eventually, the claims many made that technological breakthroughs had been achieved resulted in the now-famous internet bubble. Yet, despite the failures and despite the bubble, today Alphabet Inc. (aka Google) exists with a $753.4 billion[2] market capitalization. The first-ever search engine was known as the Archie. Archie was invented in 1990. In 1991, the “Gopher protocol” was created, making the Veronica and Jughead search engines possible. In 1992, Sir Timothy Berners-Lee, essentially the founder of the internet, established the World Wide Web Virtual Library that still exists. There were many other search engines, like Infoseek and AltaVista. Despite these efforts, Google, launched in 1998, remains the most popular.

Many are aware of this history, and since humans reason by analogy, it seems to logically follow that the successful cryptocurrency—if one actually succeeds—will be the most technologically advanced. This is a

[1] Source: www.coinmarketcap.com, as of February 7, 2018.
[2] As of February 7, 2018

reasonable position, but it is not a defensible proposition if one reflects upon the matter and is given a little more information. The Venezuelan cryptocurrency effort will serve this purpose.

The socialist economy of Venezuela is completely mismanaged and is in a state of near-collapse with widespread shortages of food and medicine, among many other problems. Yet, it is still in a position to become a nation with a successful cryptocurrency. This is because there is no such thing as proprietary technology in the world of cryptocurrency. All of the code is open source. It can be seen by anyone and modified by anyone. Thus, if Venezuela manages to properly house and feed nothing other than a very small number of computer programmers, these few people can copy code and create a very technologically advanced cryptocurrency.

Merely as an illustration, what if the Venezuelan government were to apply this advanced technology to the bolívar. Further, assume that the Venezuelan government were to decree that forever there will be zero transaction fees. To illustrate the advanced technological capability, let us assume that the technology for this currency is fast and scalable, and it will be able to process 40,000 transactions per second. As a point of comparison, Visa has can process 4,000 transactions per second. And, of course, assume that this currency would have the capability of performing smart contracts.

One can state with absolute assurance that even if all this were true, the Venezuelan crypto-bolívar would be essentially worthless. In fact, not only would the currency be worthless, but the conditions would never develop to permit it to be fast, nor would it be scalable, it would not be able to execute smart contracts, and it might not even transact at all, even though we are assuming in this hypothetical instance that it would have the most advanced features imaginable.

The reason it would be worthless is because cryptocurrency is not about technology; it is about *trust* and *incentives*. As long as the Venezuelan government has the ability to create as many bolívars as it wishes, no one will trust the bolívar. There have been four devaluations of the bolívar since August 2012, and the currency has lost 99.99% of its purchasing power since that time. It might be worthwhile to mention in passing that since 2008, the bolívar has been known as the bolívar fuerte, or “strong bolívar.”

Currency Essential #1: The Monetary Policy

It should be self-evident that the first requirement of either a cryptocurrency or a fiat currency should be a sound, noninflationary monetary policy. An associated requirement is that this policy should be objectively verifiable. Hence, the currency must be decentralized so that the central bank no longer has the power to create new currency. This is the original reason for the creation of the blockchain. It is a way of ensuring the noninflationary integrity of the system. Blockchain has many other highly useful faculties, such as accounting for inventory, property, securities, and even intellectual capital such as content or patents. These are not necessarily faculties of a sound monetary system. The comments in this connection are limited to consideration of a cryptocurrency as a monetary system and nothing more, while recognizing the desirable features of a functioning blockchain.

Currency Essential #2: An Effective Operator Incentive System

The next requirement of a functioning cryptocurrency system is that the operators of the system must be paid, and paid at a rate that provides incentive to maintain and operate the system. Many cryptocurrencies claim to have absolutely free transactions. One should be suspicious of such assertions. Obviously, the more feature-rich the blockchain becomes, the more transactions will be processed. This merely creates a more substantial blockchain in terms of size, since the blockchain—which is essentially a ledger of every transaction made—constantly accumulates new 'blocks' of approved transactions, and this clearly requires enhanced processing and storage capacity.

In the Bitcoin, Zcash and Litecoin systems, the bulk of the unit creation is designed to be paid to the operators of the system. In most other cryptocurrencies, the bulk of the unit creation is paid to the original creators of the system. Viewed from outside the system, many of these other currencies also have a fixed unit issuance. In other words, all units outstanding are created with the genesis block at system inception. This enables the creators to maintain that the system is noninflationary, but the way the units are allocated has profound implications.

In one allocation mode, for instance, there will be an "initial coin offering" (ICO), in which perhaps 20 percent or so of the coins are sold to the public at the "insider price." The creators assert that there will be absolutely no transaction costs once the system starts to operate, and they always produce a most impressive white paper. Unfortunately, the system will probably never operate, since no provision has been made to pay the system operators. For this type of ICO, one should also anticipate subsequent coin offerings as long as there is a market for coins and as long as the original creators happen to own coins.

Currency Essential #3: An Effective Operator *Disincentive* System

The last feature is that there must be a powerful disincentive for those who are operating the system to behave immorally or unethically. In cryptocurrency parlance, the operators are known as nodes. In the Bitcoin, Litecoin, and Zcash systems, nodes are "miners." Each node or miner competes for the privilege of validating a block by solving a very complex algorithm known as an elliptical function. Since huge banks of servers are simultaneously in competition to validate the block and earn the block reward, this requires substantial investment in equipment as well as a copious use of electric power.

Mining is a very lucrative activity, for reasons that will be discussed presently. This provides a powerful disincentive to behave improperly. A substantial fixed investment is required to bilk the system because of the presence of many honorable nodes. A successful cheat potentially destroys confidence in the entire system, which could make the currency worthless. It would also destroy the value of whatever fixed investment the cheater made in the mining equipment necessary to execute the improper activity, since the equipment is specifically designed to operate the cryptocurrency in question. Thus, if one were sufficiently clever to defeat the blockchain and steal 250,000 bitcoins, holders of bitcoin would quite rightly doubt the viability and integrity of the system and, therefore, the bitcoin would become worthless in a breathtakingly short period of time. To what end would one cleverly have stolen those 250,000 bitcoin?

In cryptocurrency terminology, this is frequently discussed as the "double-spend problem." What if I owned 100,000 bitcoin, and I could fool the system into allowing me to spend this amount twice? As a practical matter, I would have counterfeited 100,000 bitcoin. The same problem exists in fiat currency. What if more units can be improperly created? In reality, this happens frequently with fiat currency, but we simply have no way of assessing the magnitude. In the blockchain, however, the magnitude is instantly known, since all units in existence are tabulated, and each of the many thousands of nodes or servers running the blockchain always have the very same copy of the most recent ledger. The more nodes there are—the larger the network—the greater the security, since the attacker would have to identify all the nodes, then break the private keys of the many different servers all around the world and, moreover, accomplish this within the 10-minute window during which a new block is proved.

There is an entity known as Room 39, which is one of the unofficial names of The Central Committee Bureau 39 of the Worker's Party of North Korea. Room 39 has a long history of counterfeiting U.S. $100 bills, but its technology is now such that their counterfeit dollars are known as super dollars, because they are essentially indistinguishable from U.S. currency. North Korea has a powerful incentive to print dollars and Chinese Yuan. We simply do not know the extent of the problem. If Room 39 successfully made the same effort in cryptocurrency, though, it would succeed only once, provided that their cryptocurrency were sold almost instantly. The most significant problem with fiat currency is not counterfeiting; it is the ability of the governments to legally create discretionary currency and, thereby, reduce the value of the existing currency.

As noted previously, there is a powerful disincentive for miners to behave improperly, since mining is very profitable. In ordinary business, excessive profit is eventually eliminated, because that enticement draws more efficient enterprises into the system. The most efficient enterprise lowers prices and forces the least efficient producers to leave the system because they cannot earn profit at the new, lower prices. Ultimately, the business becomes an oligopoly dominated by the few most efficient firms.

In the cryptocurrency world, if there were to be an oligopoly of nodes, a distributed ledger would cease to exist; the security of the system resides in part on the size of the network. Even if the oligopoly did not take advantage of the system, a circumstance would arise like Visa and MasterCard whereby those firms could impose large transaction fees. Visa and MasterCard have no incentive to collaborate with each other, so the system would return to a single point of failure, whereby a single successful hack can subvert the system. If there is a single point of failure, there can be no blockchain, and if there is no blockchain, there would be no distributed system. Therefore, the power would be brought back to the central provider.

In a blockchain, the nodes must collaborate in order for the system to exist. Thus, the most efficient node cannot force the least efficient node into unprofitability. The system must provide sufficient profit for the least efficient node to prosper and, hence, maintain a viable blockchain. The conventional profit system of computation entails that the most efficient company establishes the rate of return ceiling, and each market participant owns a lower rate of return. In a collaborative venture such as a blockchain, the least efficient participant establishes a rate of return floor and every other participant earns a higher rate of return. The system is designed to encourage participation, since the blockchain becomes more robust as the number of participants increases.

One may rest assured that the socialist government of Venezuela did not wish to create a cryptocurrency and surrender the prerogatives of the state. To some degree, this move was a response to sanctions imposed on the country. However, it was necessary to a large extent because the people of Venezuela do not trust the government. In the world of cryptocurrency, trust and proper incentives easily defeat government regulations and even advanced technologies.

On that note, if you're interested in learning about what the U.S. government – that is to say, the U.S. regulators – *really* thinks, we took the liberty to abridge the testimony presented this very month to the Senate Banking Committee by the Chairman of the CFTC about this very topic. While plenty of words were removed from this comprehensive, carefully researched and well-articulated 14-page document, no words were added or rearranged. It is unofficially wagered that most Americans and most professional investors would be quite surprised at the message.

Government Suppression and Consensus Money: What the Government *Really* Thinks

http://horizonkinetics.com/wp-content/uploads/CFTC-Testimony_Feb-2018_Final.pdf

Disclosures:

This information should not be used as a general guide to investing or as a source of any specific investment recommendations. This is not an offer to sell or a solicitation to invest. Opinions and estimates offered constitute the judgment of Horizon Kinetics LLC ("Horizon Kinetics") and are subject to change without notice, as are statements of financial market trends, which are based on current market conditions. Under no circumstances does the information contained within represent a recommendation to buy, hold or sell any security, and it should not be assumed that the securities transactions or holdings discussed were or will prove to be profitable.

Subsidiaries of Horizon Kinetics manage separate accounts and pooled products that may hold certain of the securities mentioned herein and Horizon Kinetics and each of their respective employees may have positions in securities mentioned herein. For more information on Horizon Kinetics, you may visit our website at www.horizonkinetics.com. No part of the research analysts' compensation was, is, or will be, directly or indirectly, related to the specific recommendations or views expressed by the research analysts in the research report.

All material presented is compiled from sources believed to be reliable, but no guarantee is given as to its accuracy. No part of this material may be: a) copied, photocopied, or duplicated in any form, by any means; or b) redistributed without Horizon Kinetics' prior written consent.