HORIZON KINETICS

Consensus Currency Musings

THE ESSENTIAL INCENTIVE AND DISINCENTIVE SYSTEM OF AN EFFECTIVE OPERATIVE CRYPTOCURRENCY

When the colony of Virginia made tobacco legal tender, the first problem was that the incentive was created in order to increase production. The second problem was the creation of very low-grade tobacco that some people refused to accept as payment. The policy ultimately created low tobacco prices for farmers. In 1682, there were riots, and the tobacco crops of various farms were destroyed.

The non-uniformity of a currency (apart from paper) is a not a trivial problem. Throughout history, it has been a significant issue. In colonial Plymouth, Massachusetts, the Wampanoag Tribe's wampum was made legal tender at the rate of six white beads or three purple beads per penny. Unfortunately, the supply of beads was limited. It was hard for prices to rise in the sense that the bead, as an instrumentality, was not divisible.[1]

Historically, therefore, the government really needed to take over responsibility for coinage. That created another problem: How does one prevent the government from abusing its privilege by basically destroying the value of its currency by increasing issuance?

Enter Bitcoin. It is very hard to counterfeit, since all Bitcoin in existence are always visible in the Blockchain ledger. Supply of Bitcoin is fixed: it is hardwired in the code. This is a possible revolution in currency design. If nothing else, Bitcoin, in and of itself, is a new asset class.

It should be self-evident that the first requirement of either a cryptocurrency or a fiat currency is 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.

The next requirement of a functioning cryptocurrency is that the operators of the system must be paid, and paid at a rate that provides an 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

[1] Barry Eichengreen, *Exorbitant Privilege: The Rise and Fall of the Dollar and the Future of the International Monetary System* (New York: Oxford University Press, 2011), 9-10

capacity.

In the Bitcoin (and the forks), 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. On the surface, 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 insure 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, provisions to pay the blockchain's operators tend to be neglected. 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.

The last, but not least important, 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. Blockchain made it possible for private citizens to participate in the seignorage profit of currency creation.

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 in order 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 so as to defeat the blockchain and steal 250,000 bitcoin, bitcoin holders 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.

Ergo, 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 a 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 that of 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 could 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.

Because seigniorage is involved, the business of issuing money is now a real business that has to have profit and loss potential. This is in contradistinction to the United States government, or any government of the world, which could decide that it, as a matter of policy, wants to issue more money. It costs 5.4¢ to issue a dollar bill. But even a $5 cost to issue a dollar bill wouldn't stop the United States government from issuing them if it so desired.

In other words, the government is always in a position to inflate, because the cost is meaningless to it. But bitcoin, and many other cryptocurrencies for that matter, are not in a position to constantly inflate, because the bitcoin miners will only do so if there's a profit incentive. If mining becomes less profitable or unprofitable, then the resources will not be devoted to the dissemination of the currency: they will withdraw capital. The miners commit their capital and absorb the operating expense because they get compensated. In the world of cryptocurrency, trust and proper incentives easily defeat government regulations and even advanced technologies.

Important 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.

This material references cryptocurrencies, including bitcoin. Horizon Kinetics' subsidiaries manage products that seek to provide exposure to bitcoin and other cryptocurrencies. The value of bitcoins is determined by the supply of, and demand for, bitcoins in the global market for the trading of bitcoins, which consists of transactions on electronic bitcoin exchanges ("Bitcoin Exchanges"). Pricing on Bitcoin Exchanges and other venues can be volatile and can adversely affect the value of the bitcoin. Currently, there is a relatively small use of bitcoins in the retail and commercial marketplace in comparison to the relatively large use of bitcoins by speculators, thus contributing to price volatility that could adversely affect a portfolio's direct or indirect investments in bitcoin. Bitcoin transactions are irrevocable, and stolen or incorrectly transferred bitcoins may be irretrievable. As a result, any incorrectly executed bitcoin transactions could adversely affect the value of a portfolio's direct or indirect investment in bitcoin. Only investors who can appreciate the risks associated with this investment should invest in cryptocurrencies or products that offer cryptocurrency exposure. As with all investments, investors should consult with their investment, legal and tax professionals before investing, as you may lose money.

Horizon Kinetics Asset Management LLC ("HKAM"), a subsidiary of Horizon Kinetics, manages separate accounts and pooled products that may hold certain of the securities and cryptocurrencies mentioned herein, and Horizon Kinetics and each of its respective employees may have positions in the securities and cryptocurrencies mentioned herein. Horizon Kinetics is parent company to HKAM, a registered investment adviser. Past performance is not indicative of future returns and investors can lose money.

For more information on Horizon Kinetics, you may visit our website at www.horizonkinetics.com.