KNUFF & CO.
YOUR FAMILY OFFICE

On Digital Currencies (Bitcoin Revisited)

By William G. Knuff, III

(Excerpted and republished from a report originally published in 2017)

"*There are two times in a man's life when he should not speculate: when he can't afford it, and when he can."* – Mark Twain

"Speculation is only a word covering the making of money out of the manipulation of prices, instead of supplying goods and services." – Henry Ford

"The problem with speculating is not that you can turn a quick profit at the expense of the last sucker; it's that you never know whether you are the last sucker." – Will Knuff

***

I first wrote about digital or "crypto" currencies, specifically Bitcoin, in 2014 (see *On Bitcoin*). Then, as now, I am no expert. Notwithstanding its explosive price appreciation since then and any bit of regret you (or I) might harbor for heeding my advice to avoid Bitcoin when it traded for a few hundred dollars, my advice has not changed. In fact, I wish to re-emphasize and supplement it to address rampant speculation in digital currencies today because it makes no sense to me that a rational person would happily exchange something of established value for something of no value. This behavior reminds me of people spending real U.S. dollars to purchase virtual cows in Zynga's game Farmville.

First, let me briefly explain blockchain technology and its role in digital currencies. Essentially, blockchain technology is to digital currencies what the Internet is to email. A blockchain is a continuous list of "blocks" linked together chronologically and secured by encrypted codes or cryptography. Each block contains unique information that links it to the previous block in the chain, including transaction-related data (e.g. price, terms, parties, etc.), an encrypted code, and a timestamp. Blockchain technology is considered to be a decentralized efficient way to self-validate and permanently record transactions between two parties. In this regard, it is a potentially powerful tool that could be used to facilitate myriad transactions, from simple ones (e.g. buying food or clothes) to complex ones (e.g. buying a house or a business).

Blockchain technology is often referred to as an open or public distributed ledger and, today, it is used primarily to validate and record the creation (*aka* "mining") and exchange of

digital currencies. In fact, digital currencies could not exist without blockchain technology's ability to validate their creation.

As I mentioned back in 2013, several essential traits must be present for a currency to be sustainably accepted and trusted. They include: (1) a reliable means of exchange; (2) a reliable store of value; (3) divisibility; (4) durability; (5) portability; (6) uniformity; and (7) a limited or controlled supply. Implicit in this list of traits are protections against excessive systemic frictions, like transaction costs, theft, counterfeiting, and policy manipulation (fiscal and monetary). To supplant an existing form of currency, a new form of currency must materially improve upon any weaknesses in the traits of an existing one. How are digital currencies fairing relative to these standards? Let's have a look.

As a reliable means of exchange, digital currencies are underperforming existing currencies. The three major digital currencies (Bitcoin, Etherium, and Litecoin) have exhibited average daily price volatility in excess of 7.0% relative to other currencies over the past five years. By comparison, the average daily price volatility of the U.S. dollar relative to other currencies and Gold has been approximately 0.9% over the same period. Digital currency prices have been at least 7x more volatile during this time, and volatility has increased over the past year – the opposite of what should happen over time.

As a reliable store of value, digital currencies have zero value and, despite what its proponents say, cannot be safely stored. I doubt it occurs to people that digital currencies are derivative instruments, meaning their values are based solely on the value of something else – in this case, the U.S. dollar. While neither has any material intrinsic value, at least fiat currencies like the U.S. dollar have other critical sources of value, such as: (a) being backed by the productive output of their base economies; (b) stability based on the price of a consistent basket of goods and services; (c) taxes can only be paid with them; and (d) network effects – e.g. being the only recognized "legal tender" accepted for the payment of debts. Since the first digital currency (Bitcoin) was created in 2009, there have been at least a dozen published instances of digital currency theft by computer hacking of digital currency exchanges and/or "digital wallets". The most recent theft occurred in January 2018 when hackers stole $530 million in digital currency. To date, approximately $15.9 billion in digital currency has been stolen from a market currently valued at $433.5 billion. The very first theft actually took advantage of a flaw in the Bitcoin code, which resulted in the thief stealing more Bitcoin than were ever supposed to exist. The thief stole 184 *billion* Bitcoin in a transaction validated by the blockchain when at most only 21 *million* Bitcoin could potentially exist. Bitcoin's engineers executed what is known as a "hard fork" to isolate this fraudulent transaction and essentially start anew, with a clean or legitimate blockchain ledger. Interestingly, these thefts represent 3.7% of the current market (the actual percentage is much higher given the growth in the market since 2009). Based upon data from the U.S. Federal Reserve System, less than 0.4% of U.S. dollars are stolen annually. Another point for the dollar!

Regarding divisibility, digital currencies are infinitely divisible whereas physical currencies are not. However, the infinite divisibility of digital currencies renders them impractical for daily use in small transactions. For example, by design there are supposedly only 21 million Bitcoins that can be created or "mined", ever. Assuming this is true (if it's not, it is subject to

monetary policy manipulation just like existing currencies) and the global population is currently an estimated 7.6 billion people, if Bitcoin was evenly distributed to just one-quarter of the world's population in exchange for their proportionate share of global currency ($9.2T), one Bitcoin would be worth around $438,095 and each lucky recipient would have 0.00001 of a Bitcoin worth about $4,840. Aside from the psychological impact of staring at a monthly bank statement or digital wallet containing infinitesimally small balances, how do you pay for a coffee at Starbucks without relying on a computer system? And, looking at next month's statement, how would you know how much you paid or whether the amount was correct?

Regarding durability and portability, digital currency can be erased from a portable storage device with a small magnet. Digital currencies are not portable because they are not physical; they only exist in the ether. When proponents tout the portability of digital currencies, they are actually touting its ease of access from anywhere in the world, not that you can take it with you anywhere, anytime. You are portable. Physical cash and credit cards are portable. Digital currencies are not. Further, there are no monthly bank or account statements to prove you own any digital currencies because there is no bank or financial intermediary. Digital currency owners rely entirely on the blockchain (which you now know can be altered or hacked) to verify what they own. Who do you talk to when there's something wrong? How do you prove and correct it? If you're digital wallet is hacked, who fixes the problem, insures you against loss, and/or has the financial ability to replenish your account?

As for a limited or controlled supply, proponents claim that digital currencies are superior to existing currencies because their supply is mathematically limited and cannot be manipulated and, therefore, inflation and deflation are no longer issues. Not true. Digital currency supplies can be manipulated just like existing fiat currencies; the only difference between them is who is doing the manipulating, a government entity or a private entity. Regardless of type of currency, digital or physical, the practical bounds on manipulation or control are civil unrest and currency acceptance. Further, digital currency supply is unlimited because there are no barriers to entry and most digital currencies, like initial coin offerings ("ICOs"), are not mathematically limited. Just like arcade tokens or casino chips, their supply (as well as value and redemption) is controlled by the issuer. With digital currencies, especially ICOs, there is greater risk of widespread fraud due to supply manipulation than when market manipulators Daniel Drew, Jay Gould, and James Fisk issued fake Erie Railroad stock certificates in an attempt to wrest control of the company from Cornelius Vanderbilt. Moreover, you could start you our own digital currency anytime. Eastman Kodak did. Looking back at a bit of banking history, before the establishment of the U.S. Federal Reserve as a central bank, state-chartered and unchartered "free banks" issued their own currency, resulting in dozens of different currencies, arbitrary values and exchange rates, and a fragmented, unregulated, and uninsured monetary system. Consider this: what do you suppose would happen to the prices of digital currencies if a government like the U.S. started its own digital currency as an alternative or supplement to dollars? Believe it or not, for desperate reasons, Venezuela is trying.

Lastly, regarding systemic friction from transaction costs, operating an economy with a physical money supply has its costs and leakages – manufacturing, printing, distribution, processing, transferring, theft, counterfeiting, etc. While digital currencies mitigate some of these

frictions, particularly transaction fees charged by intermediaries like banks, they do not eliminate them. It can take days or even weeks to process a single digital currency transaction because of the time it takes the decentralized ledger system to validate and complete the transaction. Time is money. The costs to manufacture or "mine" Bitcoin are substantial and depend on equipment and electricity costs. At present, there are two methods for validating transactions in a digital currency blockchain, proof-of-stake ("PoS") and proof-of-work ("PoW"). The PoS method is a cheaper process where owners of a digital currency are chosen hierarchically based on the amount of digital currency they already own (i.e. the more you own, the more likely you are to be chosen) to validate one or more transactions. This method may be effective but it sure sounds a lot like a pyramid scheme or a manipulative fiscal policy that redistributes wealth from the many to the advantaged few – something thought to be anathema to the digital currency crowd. The PoW method is a more expensive process where "miners' with powerful computers compete against one another to be the first to solve complex math problems. These math problems are derived from the cryptography designed to protect transactions from potential thieves. The first miner to solve the particular math problem "earns" a "block reward" and gets paid in digital currency…for doing nothing that contributes to the productive capacity of our society. Depending on where you live, the electricity costs to mine a single digital coin can range from $500 to $25,000 or more. At current digital currency prices, the electricity costs alone exceed the price of the digital currency. In this respect, the virtual mining of digital coins appears to be just as environmentally irresponsible as the physical mining of coal. By comparison, according to the Board of Governors of the Federal Reserve, it costs, on average across all denominations, 0.05% of a dollar or about $1/20^{th}$ of a penny to produce a dollar. Winner, winner, (dollar) chicken dinner!

I can't say when but this digital currency party is going to end badly for most, but not all, participants. If you want to speculate, then speculate. But, at least be well informed and don't try to convince yourself that buying or participating in the creation of a currency is a form of investing. By the way, should you manage to become one of the few fortunate speculators, I suggest you quickly convert your virtual windfall to a tangible, productive asset.