

October 2017

Cryptonite

“Fiat money is a currency without intrinsic value established as money by government regulation or law” –
Wikipedia

You may be familiar with the name Bitcoin. What you may not realize is that Bitcoin, and the technology behind it, are two massively disruptive forces that will fundamentally change the way we exchange goods and services and discover truth.*

Bitcoin is the grand-daddy (if you can attach this moniker to something that is only 8 years old) of a new class of payment systems called “cryptocurrencies”. I must admit, when Bitcoin came onto the scene in January of 2009 I yawned. Yet another fad somebody dreamed up that would eventually end up in bottom of the same drawer with the Beanie Babies collection and the Pet Rock. I was wrong.

What makes Bitcoin so potentially disruptive is that it is not controlled by any government or entity. It truly is the democratization of money. Bitcoins exist only in digital form (you can find some of the original coins that were minted in precious metals, but these are more conversation pieces than anything else). Of course, in order for this form of payment to be meaningful, buyers and sellers of goods must be willing to accept cryptocurrency as payment. A growing number of companies now accept Bitcoin as payment: Microsoft, Subway, Overstock.com and Virgin Galactic to name just a few. Just as, or maybe even more importantly, individuals are willing to trade with each other using Bitcoin.

What makes Bitcoin and other cryptocurrencies unique is that it eliminates the need for a “trusted third party”. Think about this for a moment (warning; the following may scare the heck out of you). When you use a bank, brokerage firm, or credit card, you rely on each entity to keep accurate and honest records of your cash, investments and/or payments. There is one ledger held by the institution that maintains your account (see, I told you). Instead of this imagine a world where there is not just one ledger, but thousands of identical, independent ledgers spread across the globe that verify each of your transactions and the balances in each account eliminating the need for the trusted third party. This technology, which is the foundation of all cryptocurrencies, is called “the blockchain” and represents major disrupter numéro deux.

Blockchain technology relies on a network of computers (nodes) creating a “chain”. Each node has an identical copy of a given ledger. In order for a transaction to be validated, all nodes must agree that the transaction is legit or it will not happen. If someone wants to transfer Bitcoin to another party, it is essential that there be an immutable record of that transaction so the same party can’t spend the same Bitcoin more than once. For this to happen, all nodes must agree on the validity of the transaction by reviewing their own copy of ledger to verify that the Bitcoin is “owned” by the party wishing to transfer it and is “received” by the other party. Each transaction is then time stamped and coded creating a “block”. Subsequent transactions add additional unalterable blocks to the ledger creating the blockchain.

So, where does all this disruption I speak of come in you ask (thank you for asking)? First, let's deal with Bitcoin and other digital currencies. As of this writing, there are over 900 different cryptocurrencies in existence with new ones being created daily. Clearly most of these will not survive. The market will determine which currencies will make it based on ease of use, reliability and acceptance by the masses. Now, if you are a central government that has gotten used to printing money at will in an effort to prop up your flagging economy (hmm...rings a bell), and no one is interested in using your money because they have discovered alternative "money" that can be used to exchange goods and services for value, you can't be happy. It is tantamount to digital kryptonite for profligate governments and central bankers.

Think about a currency that has no borders, needs not be exchanged into local currency, is widely accepted, and can be transferred while in your bathrobe, and you begin to see the potential unsettling capacity that digital currencies have.

One of the arguments that many government officials have made against digital currencies is that these transactions are anonymous. Although the ledgers are verified by thousands of computers, the parties to the transactions are only identified by a cryptic code. Some maintain that this will be a boon for illegal activity (it already has in the case of Bitcoin). I'm not sure that this represents a significant setback for digital currencies, but granted it is easier for bad guys to conduct business when they don't have to lug around suitcases full of cash. Governments really hate it because they can't control it.

Not only are these currencies useful in transactions, but they have intrinsic value due to their limited supply. Each digital currency has a finite number, established by the programmer that created it. The coins are put in circulation when they are "mined" by super computers that solve extremely complex calculations required to maintain and verify the transactions on the independent ledgers. The value of each unit of these currencies has fluctuated wildly. For example, when introduced in 2009, Bitcoin was essentially worthless. The first value attached to a Bitcoin was \$.033 in March of 2010 when the first Bitcoin exchange (now defunct) opened. As of this writing, a Bitcoin is now worth \$4337.75. Stories abound about guys trading tens or hundreds of shares to buy things like pizza (what was I thinking...). There is rampant speculation in Bitcoin and virtually every other digital currency. The problem is of course that most of these will end up worthless or useable only in very limited venues. Nevertheless, there are many who are buying Bitcoin and other digital currencies as a hedge to protect themselves from potential devaluation of their own home currency. A lot of money will be won and lost as these currencies fight for acceptance.

For me, the really exciting part of this technology is the blockchain. Although the current use is limited primarily to currencies, the practical application of this technology is far reaching. Think about protecting the title to property you own, or making sure that the organic apple you purchase is really organic by following it from seed to your table, or ensuring that your prescription medication is correct by tracking it from prescriber to manufacturer to pharmacy to your nightstand, or even using it to verify your identity, so that no one can steal it.

This technology is truly transformational. It creates unalterable chains of custody for all kinds of transactions. In fact, that fiat currency you currently hold in your wallet or purse may one day end up in a curio cabinet held down by your Pet Rock.



**For those that are so inclined, there is a fascinating documentary on Netflix called "Banking on Bitcoin" that describes the history and intrigue surrounding the development and use of Bitcoin.*