The Gleason Report
www.gleasonreport.com

28 May 2017

An Analysis of Bitcoin’s Potential as a Digital Currency

Bitcoin Revisited

In a previous newsletter discussion I said that governments probably wouldn’t allow Bitcoin to operate independent of centralized control. Taxation, money laundering, and criminality are impediments to government acceptance of cryptocurrencies as lawful money. I wrote that text a few months ago. Since then I’ve immersed myself in studying blockchain technology and understanding its acceptance in the tiny and rapidly growing Bitcoin community.

Blockchain Technology and Money

For background, I have degrees in both Finance and IT technology. I worked for decades as a programmer building and maintaining both hierarchal and then relational databases. I also worked for years in the network security of large systems. Not nearly on the scale of Amazon but broad enough to understand the technology. Let’s begin by discussing blockchain.

Bitcoin is a digital payment system with transactions recorded in a blockchain ledger. The **blockchain ledger** is what IT people call a transaction database. It’s **distributed**. That’s a technical term meaning there’s more than one copy of the database. Distributed databases are a mature technology used worldwide for many applications. Bitcoin **Crypto** means the parties to a transaction have their identities encrypted using public key pairs. All databases can encrypt but public-private key encryption (*Diffie-Hellman encryption* from 1976) offers robust privacy between transacting peers. The blockchain is said to be **incorruptible**. That means once a transaction has been added to the database it is “read only”. It can’t be reversed or modified. Again, a common practice.

You could talk to programmers and network people and they’ll all understand the technology discussed to this point because they work with encryption, databases, disk mirroring, and some with distributed databases.

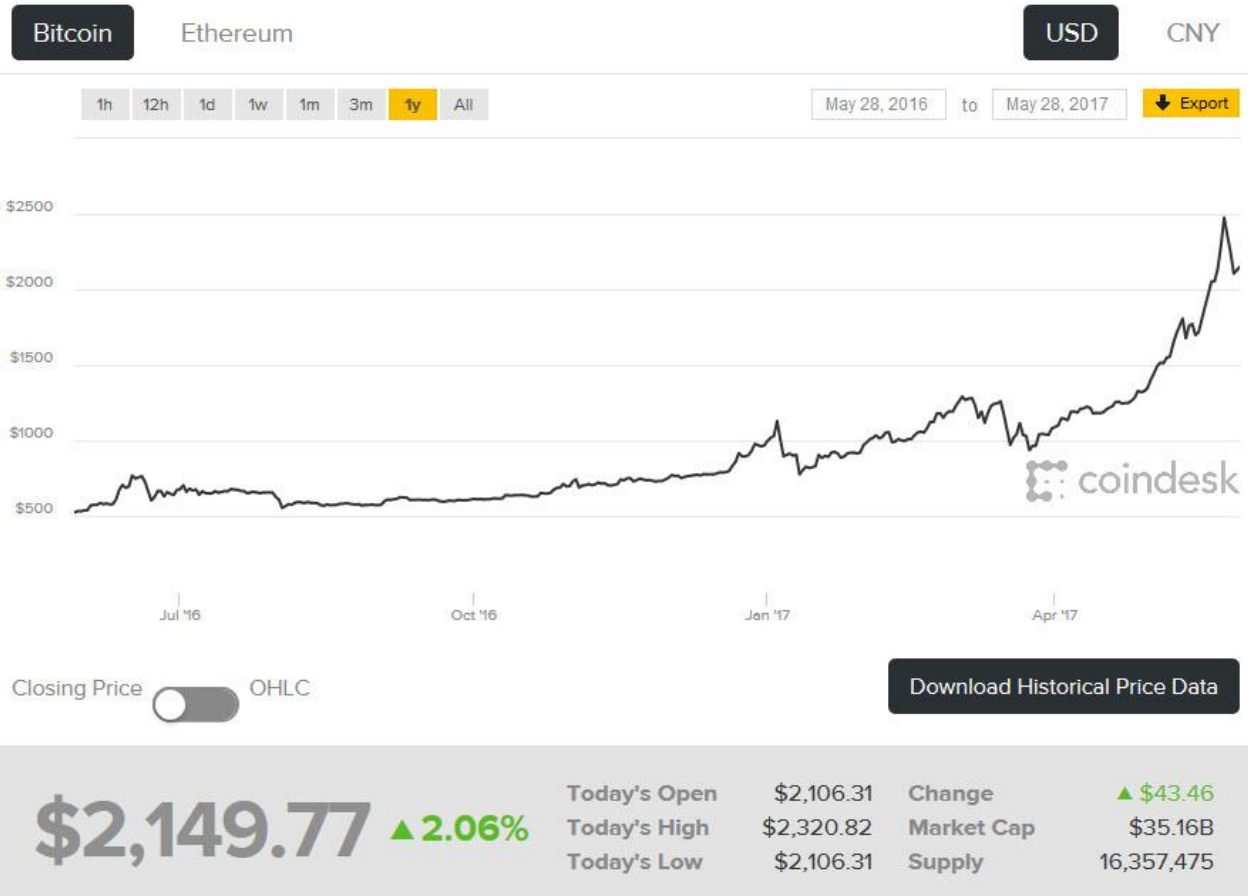
Data integrity of Bitcoin is maintained by numerous copies of the blockchain (database) dispersed across many servers. A certain number of them must confirm a new transaction before it's permanently added (appended) to the blockchain. Every Bitcoin transaction is linked to previous ones. This means there is a unique identifier or "key" that's created when you make a transaction that points back at the source of the Bitcoin. It's like a car with a VIN number. The VIN is the primary key that tracks the vehicle. Changes of ownership don't change the primary key just the name of the owner (the "foreign/secondary key"). Thus, there's a chain of encrypted numeric identifiers that point back to all the owners from when that Bitcoin was first "mined". This imposes what's called "referential integrity" on the system. None of this is new technology.

Digital money has value due to scarcity. There will only ever be 21 million Bitcoins; we're currently at 16 million. What does it mean to mine a Bitcoin? Mining a Bitcoin is done by solving a math problem to show proof of work. This ensures that new coins are added at a determined rate until the maximum number is reached. Once a mining computer solves a math problem, the computer receives payment in Bitcoin. At this time, the reward is 12.5 Bitcoin.

What's the math problem? A random number is generated and then repeatedly encrypted until the first X digits of the meaningless result show all zeroes. There are many solutions to the problem but only solutions with the required number of leading zeros will get you a Bitcoin. It's like throwing six dice. You win the game if all six die show the same number. There are six solutions to the game but the odds of winning on one throw are very low. $6*(1/6)^6$ = 6/46,656 = 1/7,776. Bitcoin mining is vastly more difficult than my die example. It's based on technology called HashCash first discussed in 1996.

What makes Digital Currencies like Bitcoin unique?

The developers solved the database problem of preventing the same Bitcoin from being spent twice - double spending. A new transaction goes through a vetting process where other copies of the database confirm that your Bitcoin hasn't previously been spent. It does this by checking the blockchain to look for any dated transactions that haven't been posted to the other databases. Once six databases confirm the transaction, it's considered for addition to the database. That's enough to verify that you're not double spending. The confirmation process across distributed databases is the Bitcoin innovation and a critical component that keeps the system honest. It accomplishes this at the cost of slow updating of the blockchain.



May 28, 2016 to May 28, 2017

$2,149.77 ▲2.06%

Today's Open	$2,106.31	Change	▲ $43.46
Today's High	$2,320.82	Market Cap	$35.16B
Today's Low	$2,106.31	Supply	16,357,475

Governments and Blockchain Technology

The blockchain is a bit like a virus. If the government shuts down or blocks access to one replicated database, Bitcoin can automatically check another database. No human intervention is required. Thus, it's a case of whack-a-mole for central banks and the NSA to kill it off. Could it be done? Yes, but realistically they can't do it because many millions of people and businesses would be affected and chaos would result. These people vote. People could also switch to one of the other 700 cryptocurrencies like my EndTheFedCoin (not yet available). Anybody can create one of these digital currencies using an automated platform.

Governments are no doubt alarmed and intrigued by this technology. They know they can't stop it and probably shouldn't. It's the market in action. What are the big issues for them?

- Bitcoin transactions are anonymous maybe. They'll only know what you transacted if they can get your private key to decrypt your transactions. US based coin wallets can be forced to give up your data. There are also difficult technical methods to break anonymity. "*How anonymous is bitcoin today? Average users should be aware that it is certainly less anonymous than cash. Meanwhile, dedicated users willing to go through extraordinary lengths can find ways to acquire and use bitcoin anonymously, but the* *open nature of the transaction ledger and other unknowns leave open the possibility that identities and activities once considered perfectly secure may be revealed at some point down the road.”* http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/

- Users can have multiple wallets and simply transfer Bitcoin to themselves. They can use mixers to exchange Bitcoins with others and break the tracking trail.
- Bitcoin bypasses the banking system, their credit card fees and the dossier on your financial activity.
- It is hard to tax the profit earned with a digital currency unless the government can break your anonymity.
- Bitcoin allows the cross-border transfer of money and bypasses currency controls. For example, the US government says you must declare more than $10,000 in cash or gold at border customs. Theoretically, you could do the transfer on the blockchain.
- Governments would love to have their own digital currency. It would be easy to collect taxes and mess with people.

Ed Snowden revealed to the world the scale of digital snooping into our personal affairs by the US government. These are grievously illegal acts according to the 4th amendment. The law is ignored. Government snooping spurred a huge adoption of encryption. Most commercial websites now use HTPPS security. The government responded by requiring ISPs to give them the keys. The market responded by adding Public Key Encryption to basic email. My Mozilla Thunderbird email client has the free Enigmail add-on which they can’t crack. This is the same technology used in the blockchain.

Government spy agencies have exploited security holes to spy on foreign governments and people they don’t like. Hackers found the holes and sold the knowledge to criminals who used it to create botnets of hacked computers to send ransomware. No doubt, foreign governments were aware of the security holes and created fake data (a honeypot) for the NSA/CIA to steal so as to mislead them.

For every stupid and illegal government action the market will respond with a countermeasure. Insiders hacked the CIA and stole the hacking tools and gave them to Wikileaks. This led to widespread security updates of routers and software. It’s pretty clear that we can’t trust the government to obey its own laws. Zero percent interest rates on savings and mistrust of government are behind the surge in Bitcoin. Interest rates below the inflation rate leads to speculations. Gold is temporarily capped by Fed market manipulation and cryptocurrencies are another way out of debased paper money.

Problems with Bitcoin

The first question to ask about Bitcoin is will the blockchain scale. By that I mean can it handle lots of transactions per second. The answer right now is a big no. Visa processes 20,000 transactions per second. As of May 2017, Bitcoin is processing 320,000 transactions per day or seven transactions per second. There are deep concerns about Bitcoin scaling among technical professionals. It takes a lot of network resources to keep distributed databases up to date.

Bitcoin requires frequent cross-database updates (replication) to maintain data integrity of the blockchain. Bitcoin is using the wrong database schema and I don't see how it can work with a high transaction volume. Updating the blockchain will always be slow because of all the network checks it must do with every transaction.

I don't know if the transaction confirmation process can be fixed. If Bitcoin can't scale vastly higher then it's a goner. Other digital currencies are designed with much faster transaction speeds but even those aren't even close to good enough at this time. That's the problem with the distributed database schema used by digital currencies. It takes far too long for transactions to process. A central server schema would be much faster but loses the positive attributes of the Bitcoin model. I'd be very cautious about putting much money into Bitcoin. Don't just assume it will all work out. I've seen conventional IT projects fail for this very reason. Bitcoin will have to change how it operates in order to scale upward and that means it won't look anything like today's Bitcoin. It might survive a reconstruction but that's not certain. https://due.com/blog/can-the-blockchain-scale/

It is foolish to use Bitcoin like a savings account. The wallet technology is rather primitive. I would use offline wallet storage on a thumb drive to be safe. Be very careful. If you lose your wallet/ private-key, you have lost your Bitcoin. There's no way to recover the money.

Cryptocurrencies can be manipulated by insiders trading among themselves.

Governments are testing Bitcoin for weakness. I have little doubt they can disrupt the network if they want. They will likely try to impose unmasking laws on wallet operators.

Bitcoin is a roach motel. You can put money in but good luck cashing out. Any cash-out sale of significant size and the price plummets. Volatility will continue until the user base expands. https://www.youtube.com/watch?v=91oot6hKbx4&t=40s

I hear people online saying Bitcoin will be $10,000 by year-end and over a million dollars within ten years. Listen to the Bitcoin believer in this video. There are many people who think like him. https://www.youtube.com/watch?v=EcKaHQhjOj0

Summary

All of today's money transfer systems are digital. All of them encrypt data over the Internet. The advantages of Bitcoin-like peer-to-peer payment systems are no bank fees, better anonymity, and the avoidance of government capital controls. The disadvantages are no fraud protection, extremely slow processing, and high price volatility.

PayPal offers free peer-to-peer money transfers and no anonymity. Buying products with PayPal or a credit card incurs a 2.9% fee. There's no anonymity but there's good fraud protection and fast transaction processing. Cash is excellent for face-to-face transactions. It's accepted everywhere and is private.

The real advantage to Bitcoin is anonymity if used properly. It's excellent for transacting in products and services deemed illegal by governments and for cross-border money transfers. Cashing out large amounts of Bitcoin is not easy.

The people using Bitcoin are first adopters. They like privacy from an intrusive government. That's the big positive I see in the product.

Its database commitment time is terrible. That's a huge technical problem that's not easily fixed. It's not ready to receive heavy traffic. To make transactions process faster will require core changes to Bitcoin. The most likely outcome is less dispersion of the blockchain. It will become more centralized.

A threat to Bitcoin comes from the Winkelvoss brothers and their proposed trading ETF. It was rejected at first but it's being resurrected. Bitcoin surged in price on the news. It shouldn't have. If the ETF is approved, the price will be manipulated. The Fed will do to Bitcoin exactly what they do to gold via GLD. This is the reason gold trades a bit over the mining cost despite serious dollar problems. It's called rigging.
http://www.cnbc.com/2017/04/26/bitcoin-price-sec-winklevoss-etf-review.html

Blockchain currencies are useful for low volume peer-to-peer transactions. It's the wrong methodology for doing high volume, point-of-sale transactions. It's in the proof of concept stage of development and not yet ready for robust transaction processing. We must not rule out new coin innovations that push aside today's problems but that will change the nature of digital currencies and today's market share leaders.

There's a huge buzz for Bitcoin as the price surges. More stores accept it and people are piling into it. It's my personal belief that Bitcoin will be a disappointment. I love the idea but hate the implementation. No doubt there's some people with millions of dollars in Bitcoin. They have a chance of successfully converting to gold/cash during the speculative expansion.

Best regards,

Tom Gleason
tom@gleasonreport.com