

Myrmikan Research

October 26, 2017

Daniel Oliver
Myrmikan Capital, LLC
doliver@myrmikan.com
(646) 797-3134

The Bitcoin Bubble

Quis custodiet ipsos custodes? So asked the great Roman satirist Juvenal in the second century A.D.: *who will guard the guards?* The Latin word he actually used, *custodes*, is most appropriate when this question is pondered in the monetary realm. Indeed, it defines the flaw in every gold standard system.

Gold has served as base money in every advanced, civilized nation because of its liquidity profile. As Carl Menger pointed out in 1892, money serves to lubricate trade, and, therefore, the money market will gravitate naturally to that substance that entails the least transaction costs, which is another way of saying the one with the most liquidity. Menger divided liquidity into two qualities: spatial and temporal. Spatial liquidity refers to the direct costs of trading a commodity and is determined by the elements of recognizability, uniformity, divisibility, distribution, scarcity, and settlement costs. Temporal liquidity refers to the costs of holding a commodity over time, including rate of decay, storage costs, long-term stability, and short-term volatility.

Liquidity is an attribute completely distinct from value. A diamond may be very valuable, for example, but diamonds are very illiquid: their quality difficult to identify, non-uniform, divisible only at great expense and the pieces do not sum to the whole (and cannot be reassembled), trading entails huge settlement costs both in terms of transportation and commission costs. As a result, the spread between bid and ask is enormous. Moreover, diamonds may now be grown in laboratories, and their scarcity is not natural but an artifice enforced by a cartel, the longevity of which is uncertain. Diamonds make terrible money.

Gold, on the other hand, of all the elements, best participates in the elements of liquidity. As America's longest serving Treasury Secretary Albert Gallatin observed in 1831:

And when we see that nations, differing in language, religion, habits, and on almost every subject susceptible of doubt, have, during a period of near four thousand years, agreed in one respect; and that gold and silver have, uninterruptedly to this day, continued to be the universal currency of the commercial and civilized world, it may safely be inferred that they have also been found superior to any other substance in that permanency of value which is the most necessary attribute of a circulating medium, in its character of the standard that regulates the payment of debts and the performance of contracts.

NOTE: This material is for discussion purposes only. This is not an offer to buy or sell or subscribe or invest in securities. The information contained herein has been prepared for informational purposes using sources considered reliable and accurate, however, it is subject to change and we cannot guarantee the accurateness of the information.

But raw gold has its shortcomings. The coin was designed, as Aristotle noted: “in order to save the trouble of weighing, and this stamp became a sign of its value.” Yet coins can be sweated or clipped, wear out through use, or be debased, causing the market to distrust the stamp. Merchants as late as the sixteenth century used scales to measure not just the goods they were selling but also the gold coin being tendered.

The market eventually developed a more liquid way to exchange gold: paper money. Merchants would deposit their gold coin and bullion in a bank; the bank would weigh, assay, and custody it, and then issue bank notes that represented the precise amount of gold on deposit. The market greatly preferred these representations of gold to gold itself because the bank (and often the state as well) guaranteed that these receipts could be redeemed back into gold in the precise amount stated at any time, making the stamp once again an accurate representation of value. As a result, while claims on gold moved rapidly through the market, gold itself was rarely demanded.

Ah, but *Quis custodiet ipsos custodes?* All that gold sitting unmoving in the vault of the custodian over long periods of time has always proved a temptation too strong to resist. Either the bank begins lending out newly printed, unbacked notes at interest (which is little different from embezzling the gold since the profit extracted nearly always matches the eventual losses to depositors), or else in a crisis the state will confiscate some or all of it (see, e.g., Charles II and Franklin Roosevelt). History has not recorded the custodian that remained true to its charge, whether because of internal or external forces.

Thus the base problem in gold-based money: physical gold is far too illiquid to serve as the basis of commerce; representational gold systems require trust in a custodial system that has proven itself always faithless.

Bitcoin was invented to solve this quandary. Bitcoins are at essence merely the unalterable electronic record that someone has done work, a bit like a unit of gold that can come into existence only through mining. The creation process is cunning: as Bitcoin transactions occur, every node running the software verifies each transaction and adds it sequentially to a “block” of new transactions. Completing and validating each new block requires solving a random mathematical puzzle, the complexity of which is altered continually by the software such that no matter how many nodes are competing to solve the puzzle, statistics dictate that there will be a winner every ten minutes. The more competitors there are, the more real resources are expended in the mining process in the form of electricity. The winner then transmits the solution to the puzzle to the network, and the other nodes verify both the winner’s record of transactions and its solution. Only if both check out do they accept the new block and add it to the file of previous blocks. In the case of alternate transactions being propagated, the majority of nodes determines which is correct. The first transaction in the new block is the creation of new bitcoin credited to the account of the winning node. The size of the reward shrinks over time such that there can never be more than 21 million bitcoins (see this link for a more thorough explanation: <https://tinyurl.com/yat8ffbn>).

Contrast the Bitcoin architecture with that of a bank: instead having tens of thousands of parallel, identical ledgers, each one maintained by a distinct entity, there is a single ledger on which the bank records all of its transactions. Customers must trust the bank to make an accurate record and risk not only errors and hackers but also that the state will forcibly alter the record in its favor (to assess tax penalties, for example). Bitcoin is immune from these threats.

It would have been relatively easy to create false Bitcoin transactions when the system was new, in fact, since the computing power spent verifying them was quite tiny. But, there was no reason to do so because at that time bitcoins had almost no value. Today, it remains conceptually easy to create false transactions, but Bitcoin nodes collectively wield processing power 50,000 times greater than the top 500 supercomputers combined, and a hacker would need to come up processing power at least double that amount. In a word: impossible.

Nor is Bitcoin vulnerable to competitors. As argued by Prof. Saifedean Ammous in his upcoming book *The Bitcoin Standard*, the numerous ICOs (Initial Coin Offerings) all contain a fundamental flaw: the entrepreneurs behind these projects raise huge amounts of capital to launch their new coins, but the promoters own most of the coins and control most of the associated computing power with which they can update and improve their systems. Improvement sounds good, but the effect is to reintroduce the custodian, the elimination of which is the very purpose of the blockchain technology. It is difficult to imagine another system evolving naturally the way Bitcoin did. Ammous adds that the large investments by big banks into blockchain technology is similarly flawed: the Bitcoin system accepts massive inefficiency in return for complete security; whereas banks constantly seek efficiencies (Visa alone can process 40,000 transactions per second)—how could it help a command and control system like a bank to have it maintain numerous, simultaneously updating ledgers of every transaction?

What Bitcoin has done is replace trust with verification, centralization with decentralization. There is no custodian, and the state is powerless to alter the blockchain record. The state may attack individual users of Bitcoin, arresting those involved in criminal transactions, for example. But Bitcoin is no more susceptible to this kind of interference than any other monetary medium, so this fact hardly acts as a mark against it. The only way to kill Bitcoin as a system would be to unplug the internet, and it seems unlikely that the populous would allow the government to send the economy back thirty years to contain a payment system.

Bitcoin's proponents argue the quantity commitment of never having more than 21 million units combined with the decentralized, unchangeable ledger makes Bitcoin superior to gold as a monetary element. Indeed, examining Menger's elements of liquidity, Bitcoin well exceeds that of gold on nearly every metric: it is perfectly recognizable, completely uniform, costlessly divisible, unalterably scarce, and transportation costs are zero; it cannot decay, and storage costs approach zero. The only flaw is its volatility, but, they argue, its increasing value is the just reward first-movers receive for risking their capital on a new currency architecture—and once Bitcoin is universally adopted, volatility will decline.

Let us assume this is correct—that Bitcoin's volatility will eventually match that of gold. If this were to happen, the implications are profound, for then Bitcoin would exceed gold in every measure of liquidity, and the market should, therefore, gravitate toward it as base money.

The reason Bitcoin must remain base money is that its blockchain system allows only 400,000 transactions per day, a pitiful amount when compared to global transactional demand (transaction fees will rise to constrain the number of transactions within that limit and will compensate for the loss of mining revenue). But recall that in the gold standard it was claims on gold that circulated; transactions in gold itself were limited and settlement was also somewhat expensive, involving transportation costs, insurance, etc.

Entrepreneurs are currently competing to develop systems that would allow long chains of claims on bitcoins to circulate rapidly with settlement occurring infrequently, the same way gold was liquefied by paper. The brilliance of some of these designs is that while they utilize competitive nodes that would charge vanishingly small transaction fees, the nodes never custody the customers' bitcoins, relying instead on encrypted, self-settling, contingent claims, thus preserving the main benefit of the system (see, for example, the video presentation of the Lightning Network here: <https://lightning.network/>).

This may sound complex, but it is structurally similar to the pre-banking real bills system of Medieval Europe: a miller, for example, would sell flour to a baker and bill the baker on thirty-day terms. The miller would then endorse his bill on the baker and use it to pay the farmer for more grain. The farmer would accept the bill because the endorsement meant that both the baker and the miller were fully liable, so default risk was minimal. Imagine that the farmer then uses this bill on the baker to purchase bread from him, and we can see how chains of claims on gold (silver in the Middle Ages) could circulate through the market liquefying commerce.

Note that while the bill matures into gold, it is not gold—it is an addition to the money supply. However, it is not inflationary since a bill may be created only by a merchant adding a new good to the market, in this case flour. Each chain would settle every thirty days—keeping the money supply in exact proportion to goods in the market—and gold would move only to the extent necessary to settle profits and losses, not gross transaction value. Banks evolved to act as clearinghouses for these commercial bills and to reduce the costs of settlement: depositor claims on gold could be adjusted on a ledger instead of having to move the physical gold itself.

The real promise of Bitcoin is not just that it could improve upon gold as a monetary standard, but that self-clearing Bitcoin-based payment chains could eliminate the need for banks both in the realm of commercial transactions and as custodians of savings. This is why the banks are so terrified of the technology, as should be the state. The imperialist, socialist nation states the dominate the globe depend upon the artificial credit creation of their banks to finance their deficits and ambitions. To the extent Bitcoin undermines the banking system, the state must suffer as well.

No doubt governments will resist the destruction of their banking systems, the source of their unnatural privilege, but, the argument goes, the decentralized nature of Bitcoin makes it hard to contain since, unlike with the gold standard, there are no custodians to attack. As the money market shifts toward Bitcoin, countries that resist will end up being be the monetary equivalents of North Korea. According to Prof. Ammous, as the flawed fiat currencies melt away, each bitcoin would need to have a value of \$4 million to replace entirely the current global monetary base, making the current price of \$6,000 seem a steal.

The vision presented above is powerful and non-frivolous. It is easy to see why Bitcoin has attracted the best technical talent and now also the innovative, young, libertarian thinkers (Prof. Ammous's book *The Bitcoin Standard* is available for pre-order on Amazon and does a thorough job of articulating the thesis presented above). But let us return to the assumption upon which the aspirations rest: falling volatility.

Gold acts a money par excellence not just because of its spatial liquidity, but mainly because prices are less volatile when using gold as a unit of account. The annual volatility of crude oil prices in dollar terms since July 1971 (when Nixon delinked the

dollar from gold) has been 64%. Pricing oil in terms of gold over the same time-period reduces volatility to 40%. Even in a fiat world, those in the oil industry who use gold as a unit of account have a clearer view of price and will thus prosper compared to those using dollars.

There is a good reason why commodities are stable in gold terms: gold mining. When gold becomes expensive in terms of industrial commodities, gold mining margins rise and marginal gold mines open, adding supply and constraining gold's increase. In addition, gold jewelry is melted down and converted to monetary gold. The opposite happens when gold's price is low: mines close and coins are melted into chalices and necklaces. The supply chain of every product and every structure begins with commodities, so stable commodity prices in terms of gold propagate down chains of production yielding stable consumer prices. Gold may *seem* volatile in a fiat world, but only because overlapping long-term contracts in supply chains and the expense of changing retail prices make consumer prices lag monetary developments, whereas gold reacts immediately (as do the spot prices of raw commodities).

It is gold's tie to the physical world added to its innate liquidity profile that keeps its value so stable and makes it such good money. There is no equivalent with Bitcoin: there is no non-monetary use whatsoever, and the pace of creation is fixed at a diminishing rate. Bitcoin has no anchor in the physical world. The solution proposed is that the world simply requires a certain value of base money and, since Bitcoin best fulfills the function of base money, the value of each Bitcoin will converge to this global, base money value divided by 21 million.

The problem with this thesis is twofold. First, it assumes a tautology: the value of Bitcoin will be stable only if it best fulfills the needs of base money; but it will be base money only if it is stable (and the latter is a condition precedent to the former). Second, the quantity theory of money upon which it relies is not just incorrect, it is incoherent: moneyness is an attribute not a distinct category. All goods participate in the qualities of liquidity at all times to greater and lesser degrees—"money" is just the colloquial term for the most liquid item. Even so, in most times and places there have been multiple monetary standards. The world operated on a bimetallic system for thousands of years, for example: gold coin is not very liquid for small, consumer purchases, the reason why retail sales were made in silver or even copper; whereas, silver is illiquid for large transactions, which is why gold has always been used for capital transactions not consumption. Similarly, U.S. dollars at present have the most spatial liquidity of any substance, but gold continues to have the most temporal liquidity.

In free markets, the market chooses the standards and itself creates liquidity in the exact amount required for commerce. In ancient times at harvest, for example, farmers would deposit their grain at granaries in return for redeemable receipts that would then circulate in the market as cash. The "money supply" soared, but prices were kept stable. The "money supply" would then shrink during the winter as the grain was consumed, yet prices would remain stable. Commercial bills provided the same mechanism for a manufacturing economy. As Paul Warburg pointed out in 1910:

If we compare the net results of the discount [of commercial bills] system with those of the bond-secured system [fixing quantity], we find that in Europe rates of interest fluctuate within comparatively small limits, while the outstanding circulation constantly contracts and

expands within wide ranges. With us it is the reverse: The outstanding circulation, once it is issued, remains fairly stationary, while the rates of interest fluctuate violently from 1 to 200 per cent.

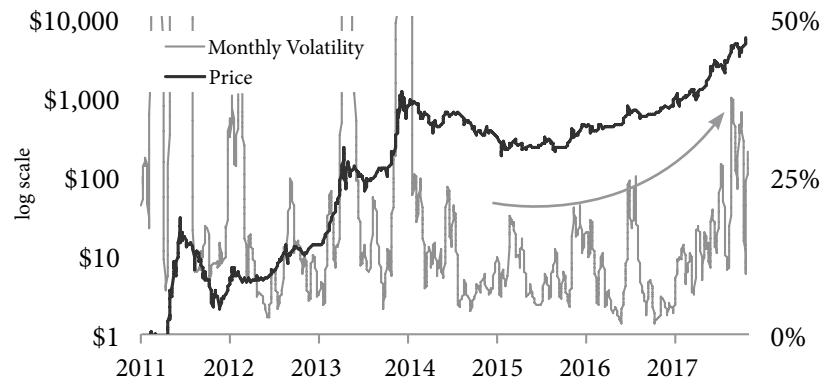
The proposed Bitcoin payment systems like the Lightning Network do not expand the supply of bitcoins since the contingent claim locks the claimee's bitcoins to prevent double-spending. Nor would a commercial bill issuance system alleviate Bitcoin's inflexibility: when the farmer agrees to accept the baker's thirty-day gold bill from the miller, he does so because he knows that he can pass it along endorsed with reduced entrepreneurial risk and also because it has stable value since it is ultimately a claim on gold. In other words, once gold had already proved its extreme stability, only then would merchants accept the risk of shifts of value to their working capital. This system, once in place, then stabilized gold's value still further. A Bitcoin commercial bills system cannot take hold until and unless bitcoins already have stable value. Commercial bill systems build on and enhance temporal liquidity; they cannot create it *ex nihilo*.

Bitcoin's shortcoming is fatal: its quantity commitment is in no way a quality commitment. It is rational to hold bitcoin only to the extent one thinks it is stable or rising in value. It clearly is not stable, and it will rise in value only to the extent that market participants either expect that it will one day be stable to fulfill its purpose as money or expect that someone else will pay a higher price for it—i.e., an expanding bubble.

Bubbles form only when there are easy monetary conditions and often around generally hard-to-value new technologies: the canal, the railroad, radio, the internet, and now blockchain technology. The parallels with blockchain and the internet bubble are manifest, in fact. Casting the mind back to 1996, few people knew what "an internet" was or why it was useful or how to get one. But there were already fortunes being made by young innovators. It wasn't long until wholesale money wanted in on the game and began funding all sorts of crazy internet start-ups. When these companies listed, Pets.com and theGlobe.com spring to mind, the public was able to join the growing bubble to drive it to insane heights before it was left holding the bag in the crash.

Blockchain technology is just entering the second stage of the bubble. Most people still don't understand the technology, yet Coinmarketcap.com lists 1,180 different cryptocurrencies worth collectively \$174 billion. Much of this value is owned by young computer programmers and libertarian philosophers. That is a *lot* of value. On cue, hardly a day goes by without the report of a senior, wholesale money player backing a hedge fund, or a listing, or miner, or a team of young software engineers. We haven't even reached the crazy part yet when the retail investors arrive.

It is a good bet that Bitcoin will go a lot higher before it crashes: the \$4 million price target not only serves as a huge incentive for pikers to take a stab, but restrains early adopters from selling. Indeed, the public record of transactions suggests that most bitcoins do not trade. Combine the small amount of bitcoin actually available on the market with trading platforms, such as BitMex.com, that offer 100 *times* leverage on Bitcoin trades (25X on Monero and 50X on Ethereum), and the potential for rank gambling becomes clear. No wonder volatility, having settled down from inception spikes, is once again on the rise.



There is a big difference between 2017 and 1997, however. Twenty years ago the Federal Reserve was on the cusp of lowering rates to bail out the banks in the wake of the collapse of Long-Term Capital Management, which drove the NASDAQ to its crazy peak. The Federal Reserve currently is in tightening mode, suggesting that the time left for this bubble is limited (unless some crisis prompts the Fed to change course yet is minor enough to avoid puncturing the bubble).

That Bitcoin is a bubble in no way disparages the underlying technology. It may well be, as Prof. Ammous argues, that blockchain can never allow for a second Bitcoin, but one can imagine applications where decentralization adds value. There is a company, for example, that wants to defeat rampant fraud in academic degrees through a blockchain system. No university wants to trust its degree verification process to a third party, but in a blockchain system each university could maintain control of its own block creation process, and only the degree verification process would be decentralized. Even though each university acts as a trusted party, in this case (unlike with money), neither the state nor the trusted parties have an incentive to create false records. Medical and insurance records might also be candidates for a process that elevates accuracy and decentralization over efficiency and is uneconomical to hack or to cheat.

Worryingly, central banks are also looking at the technology and threaten to do to blockchain what big companies did to the internet—what began as a libertarian dream of decentralization resulted in a centralized oligarchy: Amazon dominates sales, Google dominates information, Facebook dominates opinion, and 90% of entertainment is controlled by just six companies. The only application of blockchain that has “worked” so far is Bitcoin, but several Federal Reserve officials and various papers have proposed Fedcoin, a blockchain currency redeemable at the Federal Reserve into U.S. dollars (see, for example: <https://tinyurl.com/y9bn2wzg>). Fedcoin blockchain integrity would be enforced not democratically like Bitcoin but by nodes controlled by big banks, which would charge fees for their service. No wonder the banks are pouring hundreds of millions of dollars into the technology: the threat is disaggregation, and the prize is having ATM-like fees on every single transaction, not just on cash withdrawals and credit card transactions.

For those who want to ban cash, like Harvard professor Kenneth Rogoff (because only criminals and terrorists use cash), Fedcoin would allow the central bank to impose negative interest rates, the ultimate Keynesian dream that Keynes himself blessed:

Thus those reformers, who look for a remedy by creating artificial carrying-costs for money through the device of requiring legal tender currency to be periodically stamped at a prescribed cost in order to retain its quality as money, or in analogous ways, have been on the right track; and the practical value of their proposals deserves consideration.

Even better for the statist, the technology makes every transaction public, and Federal Reserve would require that each user register, allowing the state to track literally every payment between every person. Vladimir Lenin's ghost would celebrate:

Without the big banks Socialism could not be realised. The big banks are that "state apparatus" which we *need* for the realisation of Socialism and which we *take ready-made* from capitalism. . . . One state bank as huge as possible, with branches in every *township*, in every factory—this is already nine-tenths of the *Socialist* apparatus. This is general state *accounting*, general state *accounting* of production and distribution of goods, this is, so to speak, something in the nature of the *skeleton* of Socialist society.

The state may well coopt blockchain technology with terrifying results, but it can be only a fleeting victory. If history teaches anything, it is that the "knowledge problem" dooms every command and control economic system to disintegration. In the wreckage, gold will reemerge as *de facto* money, as it has after every other economic collapse in history, and likely in the form of a "bitgold" that would fuse the spatial liquidity benefits of blockchain technology to the temporal liquidity of gold.

There are companies like Goldmoney that already allow users to deposit, redeem, and transfer gold holdings electronically to other users. As with a checking account of a gold standard bank, the company must maintain a record of every transaction. Bitgold would be the equivalent of redeemable bank notes: the custodian would have no knowledge of their location after issuance until they arrive back for deposit or redemption.

It is true that any such system must involve a trusted party and the problems of custodianship. But the market can solve this problem. In a world devoid of hegemonies, competitive sovereignty directs rulers toward (classical) liberal economic policies. Writing in 1757, Turgot described the process of rehabilitation after the fall of Rome as an example:

[W]hen the whole of Europe was groaning under the manifold shackles of feudal government—when each village was, as it were, an independent and sovereign state, when the lords enclosed in their castles envisaged commerce only as an opportunity of increasing their revenue by subjecting all those who were forced of necessity to cross their territory to a tax or to an exorbitant toll—there is no doubt that those who were the first to be sufficiently enlightened to feel that, in slightly relaxing the severity of their duties, they would be more than compensated by the increase of commerce and consumption soon observed the enrichment, the growth, and the improvement of their places of residence.

Classical liberalism maintained itself as long as the system of distributed sovereignty continued, for reasons identified by Edward Gibbon:

The division of Europe into a number of independent states, connected, however, with each other, by the general resemblance of religion, language, and manners, is productive of the most beneficial consequences to the liberty of mankind. A modern tyrant, who should find no resistance either in his own breast or in his people, would soon experience a gentle restraint from the example of his equals, the dread of present censure, the advice of his allies, and the apprehension of his enemies.

Currently the world is in the grip of the opposite dynamic. America is the hegemon, and other countries obey the dictates of IRS, the SEC, and Treasury Department out of fear or greed. Switzerland, for example, recently betrayed its multi-century custodial reputation so that a few bankers at UBS and Credit Suisse could get rich exploiting the U.S. market. The EU, Russia, and China all aspire to regional dominance to exploit the same advantages regionally that the U.S. does globally, squelching any movement towards free markets, especially in the monetary realm.

After the mega-bubble in which the world resides collapses, however—and collapse it shall—it is possible that a geopolitical orientation could reestablish itself in which sovereignties would again compete to be good custodians, the best custodians becoming the wealthiest.

Bitcoin proponents hope that sound money will undermine the current socialist order to revive classical liberalism, but Bitcoin's goal to save man from his own folly reaches too far. History shows that money reflects societies; it does not shape them. Rome did not become great because the denarius lost only 13 percent of its silver content over 250 years. It became great because the Romans were the sort of people who faced upright whatever unpleasant realities the scales revealed and stood by contracts and commitments whatever the consequences. The stability of their money was merely a symptom of that steadfastness. So, too, the Byzantine Empire, which kept its money stable for seven hundred years, England, which maintained its gold standard for two centuries, and the United States, which maintain the dollar (excepting the greenback period) with little change from 1792 to 1933, all confirming Biblical wisdom: *But thou shalt have a perfect and just weight, a perfect and just measure shalt thou have: that thy days may be lengthened in the land which the LORD thy God giveth thee.* And vice versa.

True, the monetary standard is distinct from custodial fidelity, but the two concepts are related. The Bank of England lasted many lifetimes under the gold standard with only a few, temporary aberrations to its duty, whereas the absence of standards makes it difficult to judge custodial integrity, greatly magnifying the propensity to fraud (the reason modern bankers are so rich).

Juvenal's question illustrates an innate flaw in human society: when the custodians defect, nations collapse. Fortunately, gold's value as the most liquid substance survives the rise and fall of empires. Gold in physical form may not be very spatially liquid, but it retains supreme temporal liquidity and without relying on a custodian. Gold allows individuals a method of preserving their capital through monetary and political chaos, and it is the gold of individuals that will fund the depositories when the world again becomes receptive to free markets.

NOTE: This material is for discussion purposes only. This is not an offer to buy or sell or subscribe or invest in securities. The information contained herein has been prepared for informational purposes using sources considered reliable and accurate, however, it is subject to change and we cannot guarantee the accurateness of the information.