Bitcoin, Currencies, and Bubbles

Nassim Nicholas Taleb*† ‡
*Flaneur
†Universa Investments
‡Tandon School of Engineering, New York University

INTRODUCTION/ABSTRACT

This discussion will apply quantitative finance concepts and economic arguments to cryptocurrencies in general and bitcoin in particular –as there are about 10,000 cryptocurrencies, we focus (unless otherwise specified) on the first crypto as per the original protocol [1] and the one with the largest market capitalization.

In its current version, in spite of the hype, bitcoin failed to satisfy the notion of "currency without government" (it proved to not even be a currency at all), can be neither a short or long term store of value (its expected value is no higher than 0), cannot operate as a reliable inflation hedge, and, worst of all, does not constitute, not even remotely, a tail protection vehicle for catastrophic episodes.

Furthermore, there appears to be an underlying conflation between the success of a payment mechanism (as decentralized mode of exchange), which so far has failed, and the speculative variations in the price of a zero-sum asset with massive negative externalities.

Going through monetary history, we also show how a true numeraire must be one of minimum variance with respect to an arbitrary basket of goods and services, how gold and silver lost their inflation hedge status during the Hunt brothers squeeze in the late 1970s and what would be required from a true inflation hedged store of value.

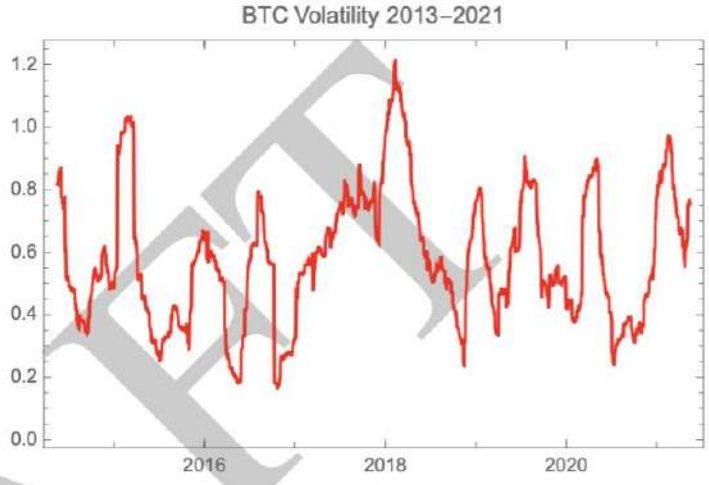

Fig. 1. BTC return, 3 months annualized volatility. It does not seem to drop over time.

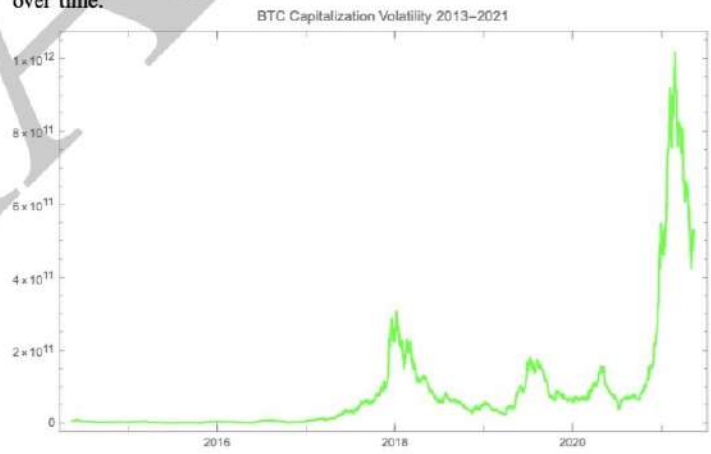

Fig. 2. Too volatile to fail? We show the volatility of the capitalization of BTC. At higher levels of capitalization, return volatility compounds. In 2021 a swing of half a trillion dollars in the capitalization of bitcoin took place.

THE BLOCKCHAIN

First, let us consider what cryptocurrencies do by examining the notion of blockchain and its intellectual and mathematical appeal.

The concept behind such a chain is quite intuitive to early practitioners of quantitative finance. Consider that before efficient software for Monte Carlo simulations became widely available, some of us were using methods to generate pseudorandom variables via some forms of chained nonlinear transformations, in the spirit of Von Neumann's original idea [2]. Indexing sequences by $t = 1, 2, \dots n$, a seed at t, a variable x_t on the real line generates via nonlinear transformations $r : \mathbb{R} \to \mathbb{R}$, an output variable $r(x_t)$. This output variable can serve as a pseudorandom seed to generate another pseudorandom variable, $r(x_{t+1})$. For all t, knowledge of $r(X_t)$ allows knowledge of all subsequent variables $r(x_\tau)_{\tau>t}$, and replicate the entire sequence, thus probabilistically, mimicking the arrow of time. It is also crucial that the same seed produces exactly the same pseudorandom variable, allowing a verification of sequence, but disallowing easy reverse engineering.

What the blockchain added, thanks to the hash function, is the condition that $r(.)$ must be functionally and probabilistically bijective: no two seeds must produce the same output (or

NNT1@nyu.edu

The author thanks Gur Huberman, Mark Spitznagel, Brandon Yarkin, Trishank Karthik Kuppusamy, Jim Gatheral, Joe Norman, David Boxenhorn, and others for useful discussions.

should have a vanishingly low probability of that happening), what, in computer science terminology, is called *collision*.

This hard-wired attribute and absence of supervision of the blockchain thus allows the storage of activities on a public ledger to facilitate peer-to-peer commerce, transactions, and settlements. The blockchain concept also allows for serial record keeping. This is supposed to help create what the original white paper [1] described as:

> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

From that paper, bitcoin makes use of three recent technologies: 1) the hash function, 2) the Merkle tree (to chain blocks of transactions tagged by the hash function), and 3) the concept of proof of work (used to deter spam by forcing the agent to use computer time in order to qualify for a transaction). The idea provides a game theoretic approach to mitigate the effect absence of custodian and lack of trust between participants in the maintenance of a permanent shared public ledger – attenuating or circumventing the coordination quandary known as "Byzantine general problem".

The system established an adversarial collaboration between the so-called "miners" who validate transactions by getting them on a public ledger; these get coins as reward plus a fee from the underlying transactions, that is, transfers of coins between parties. The proof of work method has an adjustable degree of difficulty based on the speed of transactions, which aims, in theory, to keep the incentive sufficiently high for miners to keep operating the system. Such adjustments lead to an exponential increase in computer power, making at the time of writing onerous energy demands on the system –energy that can find substitutes in other computational and scientific uses.

Miners derive their compensation from both seignorage (the market value of a bitcoin minus its mining costs) and transaction fees upon validation –with the plan to switch to transaction fees as sole revenues upon the eventual depletion of the coins, which are limited to a fixed number. Note here that bitcoin depends on the existence of such miners for perpetuity.

Note that the entire ideological basis behind bitcoin is complete distrust of other operators –there are no partial custodians; the system is fully distributed.

Finally, note that bitcoins are zero-sum by virtue of the *numerus clausus*. As we will see, mathematical and combinatorial qualities do not necessarily translate into financial benefits at both an individual and systemic level.

VULNERABILITY OF REVENUE-FREE BUBBLES

Comment 1: Why BTC is worth exactly 0

Gold and other precious metals are largely maintenance free do not degrade over a historical horizon, and do not require maintenance to refresh their physical properties over time.

Cryptocurrencies require a sustained amount of interest in them.

A central result (even principle) in the rational expectations and securities pricing literature is that, thanks to the law of iterated expectations, if we *expect that we will expect* the price to vary, then by backward induction such a variation must be incorporated in the price now. When there are no dividends, as with growth companies, there is still an expectation of future earnings, and a future expected reward to stockholders –directly via dividends, or indirectly via reverse dilutions and buybacks.

Earnings-free assets are problematic.

The implication is that, owing to the absence of any dividend yield benefiting the holder of bitcoin, *if* we expect that, at any point in the future, the value will be zero when miners are extinct, the technology becomes obsolete, future generations get into other such "assets" and bitcoin loses its appeal to them, *then* the value must be zero *now*.

The comparison of bitcoin to gold is poor. We will see later how precious metals lost its quality as medium of exchange; gold and other dividend-free precious items (such as metals or stones) have held some financial status for more than $6,000$ years, and their physical status for several orders of magnitude longer (i.e., did not degrade or mutate into some other alloy or mineral). So one can expect one's gold or silver possessions to be around physically for at least the next millennium, on top of having some residual economic value then for the same reason, by iteration. Metals have ample industrial uses with demand elasticity (and substitution to other raw materials). Currently, half of gold production goes to jewelry, one tenth to industry, and a quarter to central bank reserves.

Path dependence is a problem. We cannot expect a book entry on a ledger that requires active maintenance by interested and incentivized people to keep its *physical* presence, a condition for monetary value, for any such period of time –and of course we are not sure of the interests, mindsets, and preferences of future generations. And once bitcoin drops below its level, it hits an absorbing barrier and stays at 0–on the other hand gold is not path dependent. As discussed by this author [3], technologies tend to be supplanted by other technologies with a vulnerability in proportion to their past survival duration (99% of the new is replaced by something newer), whereas items such as gold and silver have proved resistant to extinction[1].

Principle 1: Cumulative ruin

If any non-dividend yielding asset has the tiniest probability of hitting an absorbing barrier, then its present value must be 0.

We exclude collectibles from that category as they have an aesthetic utility, as if one were, in a way, renting them for an expense that maps to a dividend. The same applies to the jewelry side of gold: my gold necklace may be worth 0 in thirty years, but I would have been wearing it for six decades.

[1] It is also a reasoning error to claim that a new tool, bitcoin, can become the "new gold" *ab ovo*, when gold wasn't decided to be so by fiat; it became the reserve ex post, throughout centuries of competitive selection against other modes of storage, payment, and collectibles.

The difference between the current bitcoin bubble and past recent ones, such as the dot-com episode spanning the period over 1995-2000, is that shell companies were at least promising some type of future revenue stream. Bitcoin would escape such a valuation approach had it proven to be a medium of exchange or satisfied the condition for a numeraire off of which other goods would be priced. But currently it is not, as we will see next.

Success in wrong places

More generally, the fundamental flaw and contradiction at the base of most cryptocurrencies is that, as we saw, the originators, miners, and maintainers of the system currently make their money from the inflation of their currencies rather than *just* from the volume of underlying transactions in them. Hence the total failure of bitcoin in becoming a currency has been masked by the inflation of the currency value, generating (paper) profits for large enough a number of people to enter the discourse well ahead of its utility.

Comment 2: Success for a currency

There is a conflation between success for a "digital currency", which requires some stability and usability, and speculative price appreciation.

Transactions in bitcoin are considerably more expensive than wire transfers or other modes, or ones in other cryptocurrencies, and order of magnitudes slower than standard commercial systems used by credit card companies –anecdotally, while you can instantly buy a cup of coffee with your cell phone, you would need to wait ten minutes if you used bitcoin. Nor can the system outlined above –as per its very structure –accommodate a large volume of transactions –something central for an ambitious payment system.

To date, twelve years into its life, in spite of the fanfare, with the possible exception of the price tag of Salvadoran citizenship (3 bitcoins), there are currently no prices fixed in bitcoin, floating in fiat currencies in the economy.

Principles for a currency

First, let's discuss the demonetization of gold. In 1971, the U.S. government terminated the Bretton Woods Agreement, ending the convertibility of the U.S. dollar into gold. Gold stocks were growing at between 2% and 4% per annum, but, as mentioned earlier, much of it went to jewelry and industry – there was not enough gold to keep up with economic growth. Furthermore, there had been long debates over the hampering of monetary policy by sticking to metals, see Ricardo's 1811-1816 debates [4],[5], and commentary by Jevons [6]. It appears that developed economies have trouble hemming their currencies to a commodity.

In the early 1970s, the Hunt brothers started to hoard silver (when they started, U.S. citizens were banned from directly owning gold), and accelerated their hoarding in the late 1970s, turning it into a squeeze. It lead to a speculative explosion in the price of silver, as shown in Fig 3, leading by contagion to

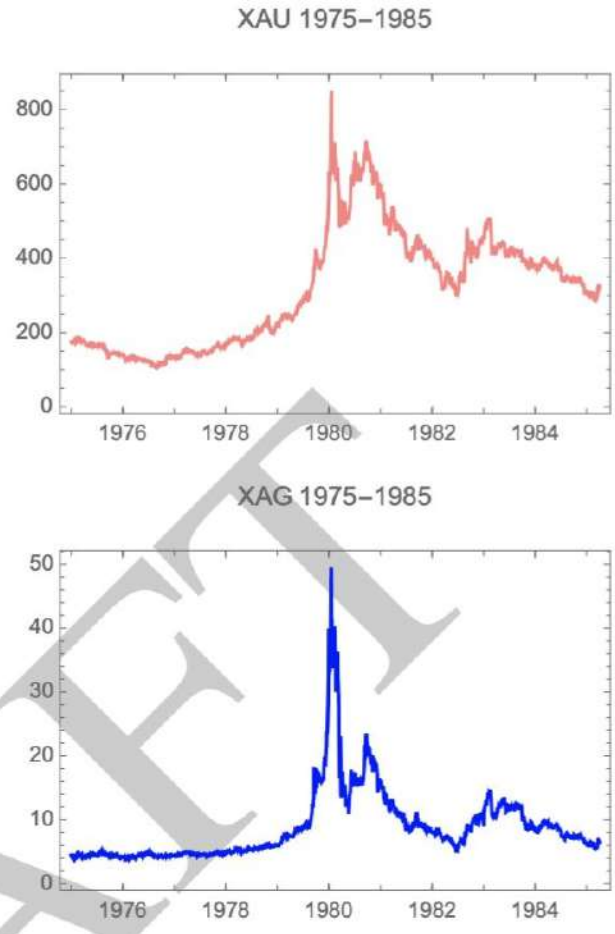

Fig. 3. The rise and fall of metals during the Hunt squeeze of silver and, indirectly, gold.

between a fivefold and tenfold increase in the price of precious metals. Then, upon the deflation of the bubble, metals gave back more than half of their gains and languished for more than two decades. At the time of writing, 41 years later, neither gold nor silver have, inflation adjusted, reached their previous peak. The same effect took place in 2008-2009 in the wake of the banking crisis: gold and silver jumped upwards between 80 and 120 % then lost most of the value back. I can include a graph of the rise and fall if there is space

Gold and silver proved that they could neither be a reliable numeraire, nor an inflation hedge. The world had gotten too sophisticated for precious metals. If we consider the most effective numeraire, it must be the one in which the bulk of salaries are paid, as we will show in the next section.

Comment 3: Payment system

There is a conflation of "accepting bitcoin for payments" and pricing goods in bitcoin. For that the price in bitcoin must be fixed, with the conversion into fiat floating, rather than the reverse.

Let us go deeper into how a currency can come about. No transaction is analytically pairwise in an open economy. The root of the confusion lies in the prevalent naïve-libertarian

illusion that a transaction between two consenting adults, when devoid of coercion, is effectively just a transaction between two consenting adults and can be isolated and discussed as such, pairwise[2]. One must consider the ensemble of transactions and the interactions between agents: people happen to engage in contractual agreements with others; for them a given transaction is just a piece. To be able to regularly buy goods denominated in bitcoin (that is, fixed in bitcoin, floating in U.S.$ or some other fiat currency), one must have an income that is fixed in bitcoin. Such an income must come from somewhere, say, an employer. For an employer to pay a salary fixed in bitcoin, she or he must be getting revenues fixed in bitcoin. Furthermore, for the vendor to offer a can of beer in fixed bitcoins, she or he must be paying for the raw material, and have the overhead fixed in bitcoin. The same with a mismatch of assets and obligations on a balance sheet. All this requires a parity bitcoin-USD of low enough volatility to be tolerable and for variations to remain inconsequential.

There are also arbitrage bounds present in any sufficiently efficient economy with relatively free markets.

If someone prices goods in bitcoin, and the value fluctuates from the initial fixing, the price will be directly or indirectly arbitraged: when the conversion rate to fiat is favorable, customers will buy from the bitcoiner; when unfavorable they will either buy elsewhere (indirect arbitrage), or if possible, return previous goods (direct arbitrage). For the price to not be arbitrageable requires the good to be unique and unavailable elsewhere at a fixed price in another currency –in this case it becomes, simply, a proxy to bitcoin. The only items that currently appear to be somewhat priced in bitcoin are other cryptocurrencies, even then.

Bimetalism did not last long [7], nor could commodities last as currencies in developed economies[8].

More generally, the reasons multiple currencies exist (in the absence of pegs) is because there is not enough globalization and markets are not entirely free between currency zones. And some goods and services, "such as haircuts and auto repair cannot be traded internationally"[9] ; they are not, to use the language of quantitative finance, arbitrageable.

In 2021, the governments (central and local) share of GDP in Western economies is around 30-60%, one order of magnitude higher than it was in the 1900s. Government employees get salaries in fiat; taxes are collected in fiat. To displace fiat one must come up with a currency that is of low volatility.

Finally, while within a currency zone a bimetallic style dual currency cannot easily exist, the same limitations exist between currency zones; parity between currencies tend to be subjected to volatility bounds. An observation we currency option traders made while doing cross-currency volatility arbitrages is that the volatility of a currency pair is proportional to what trade is taking place between the two currency zones –countries heavy into trade such as Hong Kong, Saudi Arabia, the UAE, and Singapore (at some point) have maintained explicit pegs to the U.S. dollar or some basket. There could an interactive relationship between trade and volatility: one can argue that the stability of a currency-pair (adjusted for yield curve) encourages trade and trade in turn brings stability to the pair[3].

We note here that quantitative finance operates along the lines of neoclassical economic theory in that both share a central principle: absence of arbitrage, which maps to the law of one price –the former broadened to asset valuation a concept initially aimed for goods and services [10]. When we apply the law of one price to currencies, we realize using basic arbitrage arguments that the recent globalization does not allow for different currencies to coexist in the same markets: one must win. Bimetallism failed many times in history because it is hard to maintain the parity silver-gold. As transaction costs drop, so does currency volatility.

Note that bitcoin, as seen in Fig. 1 maintained an extremely high volatility throughout its life (between 60% and 100% annualized) and, what is worse, at higher prices, which makes its capitalization considerably more volatile, rising in price as shown in Fig. 2 –is it too volatile to fail?

THE DIFFICULTY WITH INFLATION HEDGES

This does not mean that a cryptocurrency cannot displace fiat –it is indeed desirable to have a *real* currency without a government. But the new currency just needs to be more appealing as a store of value by tracking a weighted basket of goods and services with minimum error.

Displacing fiat is not easy, and has been done locally – though no single item has proved to be permanent and the difficulty is best represented in the following example. For instance, during the 1970s, the Italian national telephone tokens, the *gettoni*, were considered acceptable tender, almost always accepted as payment. The price of the espresso in lira varied, but it remained sticky to the *gettone*. And while the gettoni worked for daily purchases such as the espresso, it is doubtful it could have been used as payment for an Alfa Romeo.[11] For a while the *gettone* proved closest think in tracking the Fisher Index across 12 communes[12][4] .

But the problem is that, owing to technological changes, in the long term, no single item, such a telephone call, will permanently track inflation indices and act as a store of value: consider that communications got cheaper over time and the notion of a telephone call is today, in the Zoom days, obsolete. Even categories have their weights naturally revised over time: the share of food and housing declined tenfold as a share of the Western consumer since the great recession.

Thus we can look at the inflation hedge as the analog of a minimum variance numeraire:

> *Let us assume that an efficient inflation hedge for period $[t_0, T]$, and for an index methodology, the one in which the index, constantly revised, is most stable when expressed using it as a numeraire.*

[2] www.libertarianism.org

[3] Currency pairs often show fake volatility as the spot price can be fluctuating but forward contracts less so, owing to interest rate adjustments in the weak currency: interest rates rise to compensate holders for the devaluation.

[4] Likewise, The M-Pesa mobile currency used as tender in Africa was born out of transferable airtime minutes.[13]

By its very nature, bitcoin is open for all to see. The idea of hiding one's assets from the government with a public blockchain easily triangularizable at endpoints and not just read by the FBI but by people in their living room also requires a certain lack of financial seasoning and statistical understanding – perhaps even simple common sense. For instance some were able to statistically detect and triangularize "anonymous" ransom payments made by Colonial Pipeline on May 8 in 2021 [16] –and it did not take long for the FBI to hack the account and restitute the funds.

Government structures and computational power will remain stronger to those of distributed operators who, while distrusting one another, fall prey to simple hoaxes.

In the cyber world, connections are with people one has never met in real life; infiltration by government agents are extremely easy. One never knows the degree of governmental surveillance and real capabilities.