WORDS

February 2020

A collection of commentary from the brightest minds in the Bitcoin community.

Contents

Goals and Scope

WORDS is a journal of Bitcoin commentary, established February 13, 2019. Its purpose is to document and advance commentary and research in disciplines of particular interest to the Bitcoin community. The journal is broad in scope, publishing content from original research, essays, blog posts, and tweetstorms from a wide variety of fields, especially governance, technology, philosophy, politics, and economics, but also legal theory, history, criticism, and social or cultural analysis. Its broader mission is to capture the conversations and think pieces in the Bitcoin space for current and future researchers. *WORDS hopes to* continue and expand the tradition established by publications such as the *Journal of Libertarian Studies* and *Libertarian Papers*.

History

There exists a gap in Bitcoin publishing. For authors with commentary and scholarly papers on topic, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for Bitcoin research is in any event too small, as the number of Bitcoin thinkers continues to grow with every market cycle.

This generation of Bitcoin thinkers have limited places to submit thought pieces for publication. Content is scattered across the web, and in some cases behind paywalls which prevent the free flow of information. With the advent of the Twitter and blogging, authors also now have the option of self-publishing: they post the content to their own site or some private site, link it in a blog post, or post a working paper. But this is obviously not the best way to document and publish. What is needed is a journal that takes full advantage of the possibilities of the digital age as a go to resource for think pieces in the Bitcoin space.

Enter *WORDS*. Published independently, *WORDS* is a journal that welcomes submissions on a range of topics of interest to the Bitcoin community. In addition to conventional research articles, we welcome review essays blog posts, tweets as well as papers in other formats, such as distinguished lectures. Finally, wherever possible, content on this site is licensed under a Creative Commons Attribution 4.0 License. Authors retain ownership without restriction of all rights under copyright in their articles. *WORDS* is open access, and we encourage readers to "read, download, copy, distribute, print, search, or link to the full texts of these articles…or use them for any other lawful purpose." We want our ideas read, spread, and copied.

Support WORDS

The posts and journals published here have been carefully curated and crafted as a true labor of love. If you've found any of this content useful here's how to show your thanks and keep the project going.

Support WORDS

Spread the word

Have a website or use social networking sites like Twitter, Facebook, or LinkedIn? Please consider sharing the content found on *WORDS* or linking to https://bitcoinwords.github.io.

Follow us on social media

We post regularly on Twitter and use it as our main form of communication. — We don't rapid fire posts but add commentary where we see fit. Posts are typically links to our content and other things regarding development of this site.

If these sorts of things interest you, follow along on:

Twitter

Subscribe to our newsletter

We publish our journal monthly and share it via Twitter and via newsletter. Consider subscribing to the newsletter. If you're not on Twitter all day, it might make sense to subscribe so you never miss a publication.

Subscribe

Our pledge

- We will never sell you out.
- We will never shill you shitcoins.
- We will only deliver what is promised.

Money is about credibly representing value transactions

By acrual

Posted February 5, 2020

According to the Selfish Gene book, we only want to exchange value or cooperate with strangers when there is an inmediate exchange. If we postpone this exchange, we are very likely to cheat (and even in the case we are not strangers!).

We are some serious cheaters according to this fascinating book and I agree.

Unless you believe we prefer to satisfy everyone else's needs before our own, you must necessarily agree with this book, and this is important, because it explains money very well.

If you can't give me something I value right now (barter), I want you to prove to me that you have provided value to someone else in the past, that is, I need a prove from you that you have made a value transaction earlier.

You must, as a result, be able to represent a transaction credibly.

What would you do if you had to represent a transaction in the most "credible" way 20.000 years ago?

I suggest that if you want to cooperate with me, whenever you provide value, you get in return something that is universally very scarce, so that you can't tamper this representation easily. Otherwise I may have the feeling that you could be cheating me and again, you and I are very likely to do so.

But that something has to be easily recognizable by me, otherwise I won't accept it either. If you want me to accept it, you'd better get divisible items, so that you can pay me smaller values. And chances are you will only accept stuff that is cheap and easy to transport. (in Menger terms, saleable in space and scale)

If I were you, I'd only accept stuff that is extremely cheap to store, that deteriorates the least over time, because you have no idea when your needs will arise, and that could be a long time into the future. (saleable in time)

Transferring the property of this stone must not depend on third parties, because otherwise those third parties are likely to cheat as well!!

During the first transactions, you will have no way of knowing if you are representing that transaction with the right-sized stone. It may be too big or too small. You won't have any guarantees that the rest of humanity will accept this stone and as a result, you won't be able to size it properly until this item is universally accepted by the market so that you can compare it. You'll be gambling and speculating that you are sizing this transaction accurately. If it costs little to store, you will try to store as much as possible of it and as a result your gamble will have little cost.

Therefore that stone will be for you both a product you will use (a medium of exchange) and speculation too.

The market will slowly realize that by being data and software, Bitcoin is "the thing" that best solves each and everyone of these requirements.

The market should also understand that things that are valued are those which are stored, not those which are used because using them means buying and selling, so supply is kept high.

Storing means buying and keeping, limiting supply as a result. If Picassos were not kept, just seen in your home and then sold next day, then their value would tend to zero, but no, they are typically kept for decades.

Even if your shitcoin is designed to cure malaria, chances are that you will sell it inmediately after being used and as a result its value will tend to zero. With a value tending to zero, it is more likely that developers will end up curing malaria with Bitcoin than with your shitcoin.

For the n-th time, block, mute everyone speaking about shitcoins/blockchains, we have to be merciless with people that insist on being either ignorants or scammers.

Small note on Statism vs Libertarianism

I got into Bitcoin with a completely statist mindset, but understanding that we are programmed to cheat made me wonder if it does make any sense to pretend that Statism is the best way to organize ourselves.

It is also hard as a result for me to take seriously people that say they understand Bitcoin, and keep defending Statist views.

If we are programmed to cheat, and throughout history we have gone through the pain of using all sorts of monies in every single civilization as a way of solving it, does it make sense to spend each others resources in something named "common good"?

Tweetstorm Bitcoin as super-collateral

By Aaron (Fiat Minimalist)

Posted February 5, 2020

Bitcoin is quickly evolving into an asset that will become the ultimate form of collateral. Have been hearing more trad funds/groups willing to accept BTC as collateral in return for fiat loans at ~6-12% per annum

The latest I know of is a traditional global multi-family office that specializes in share-backed loans, and now have just branched out to BTC-backed loans.

Typical collateralized assets in today's markets are (1) real estate, (2) shares, (3) bonds

As bitcoin continues to capitalize, its vol will approach & fall in-line with these categories of assets + liquidity will exceed even the most liquid shares (and BTC loans will become the cheapest, fueling more demand for BTC as the highest quality collateral) -> reflexivity

With the exception of volatility, Bitcoin scores (or will soon score) better than all other assets in all "what makes a good collateral" dimensions such as liquidity/marketability, 24/7 availability, speed and ease of settlement, global acceptance, fungibility etc.

Unlike most assets, Bitcoin is a bearer asset so its clearly unencumbered. Once lender is holding on to the actual BTC they can be sure it hasn't been pledged to 10 other parties simultaneously

Also cheaper & more efficient than paying for title deed searches, lien enforcement

BTC can be liquidated 24/7 and almost immediately - unlike real estate which can sometimes take >1 year for resolution, or shares/bonds which only trades certain times during the day for which liquidity tends to dry up during periods of stress

Matter of time banks begin accepting Bitcoin as collateral, and they'll have to build out infrastructure to manage Bitcoin borrowing/lending

---

Lessons from the uneven distribution of capital

By Nic Carter

Posted February 8, 2020

What we can learn from distorted maps

As the crypto markets continue their transition from a retail-focused, unrestricted global altcoin casino, to a more constrained and regulated environment, it's worth zooming out and pondering what long-term allocative outcomes this market is likely to witness. Cryptocurrency purports to allow commerce and capital to flow freely, independent of artificial nation state boundaries. However, when securities are involved, the state tends to intervene.

There is a good reason for this: securities are high-stakes markets governing the allocation of productive capital, and for them to function, the state needs to enforce fairness, disclosure, and information symmetry. In fact, the best example in favor of securities laws I can think of is the anarchy and carnage exhibited in the Initial Coin Offering boom in 2017. If blockchain-lubricated capital markets mature from these early hiccups and some of these equity-like assets become viable, they will surely be indexed to their local jurisdictional rules. To the extent that tokenization and crypto-wrapped securities become investable, I'd venture that the U.S. is strongly positioned to compete for issuers — despite the globalized nature of the crypto industry.

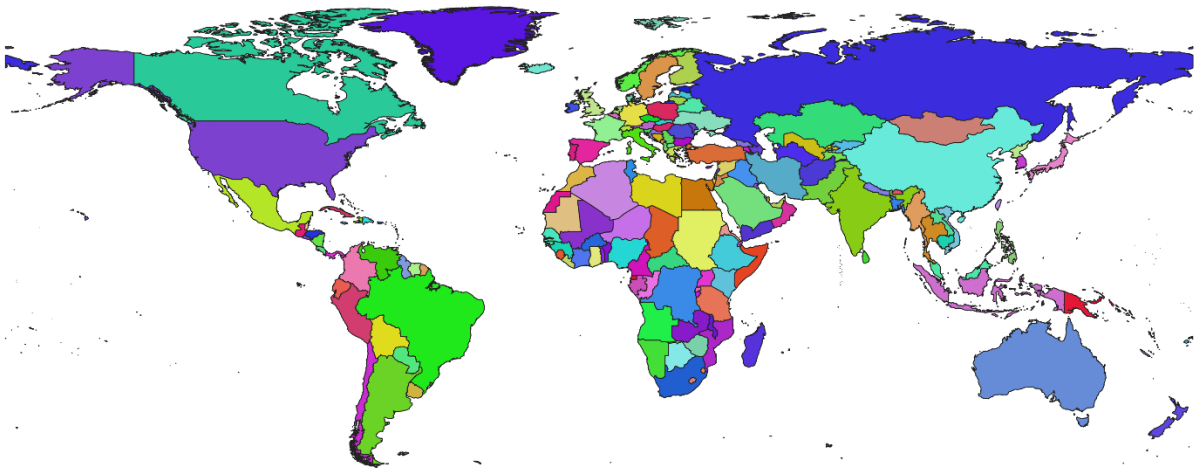
What distorted maps tell us about shareholder rights

It's often said that the SEC is "pushing innovation abroad" by cracking down on crypto projects, especially those that issue pseudo-equity in the form of a token. This may well be the case. It is also quite a reductive view. Capital clusters in jurisdictions where the rules are understood, where property rights are respected, and where legal systems appropriately apportion power between shareholders and directors. Thus, the enforcement of age-old rules which made the U.S. the most vibrant equity market on earth in a crypto context can be understood as either hostile to issuers, or accommodating to investors. The latter perspective is sorely neglected in the regulatory analysis.

In the issuance of equity, standardization is a godsend. If you work in startups, you will mostly likely have a strong understanding of the nuances of a Delaware C corp or the YC SAFE. When issuers select these instruments to raise capital, they are opting for a set of rules and a legal context which are mutually understood by founders, VCs, and law firms. This often entails cheaper diligence and less legal overhead. Indeed, some VC funds don't

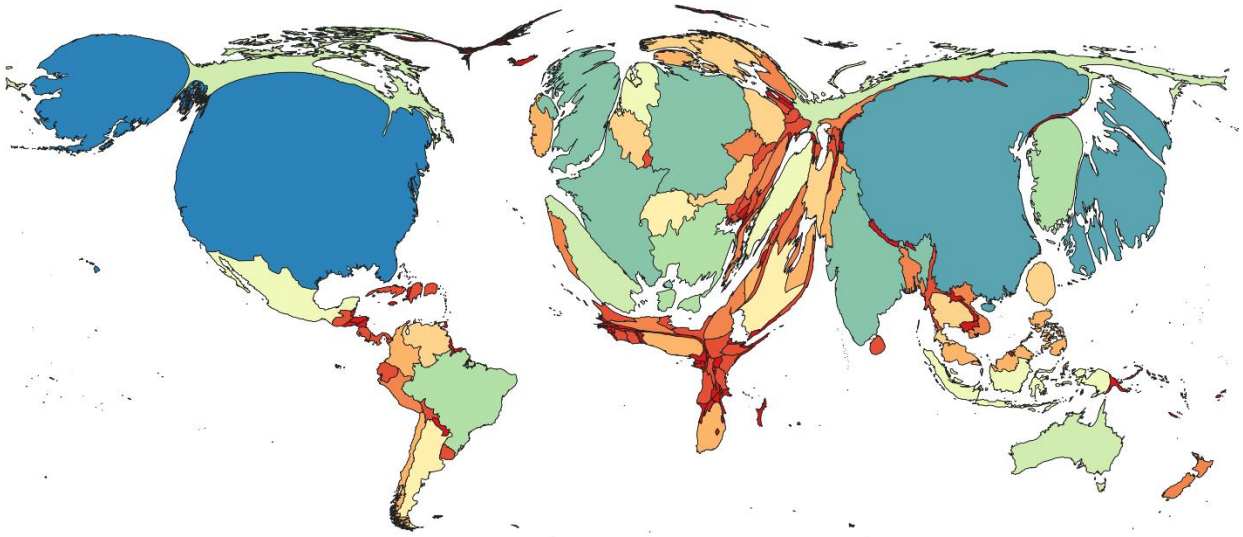
invest in anything other than Delaware C Corps. This is just one anecdote, but it hints at the bigger picture: investors like predictable and comprehensible structures. They like to know where they stand relative to founders, and what their recourse is if something goes wrong. At a global scale, small differences in jurisdictional predictability lead to wildly divergent outcomes.

You may be surprised to learn that the U.S. accounts for 26% of global GDP, but a staggering 40% of global public equity capitalization. This point is best made visually with a chart called a cartogram. What a cartogram does is weight land area by some variable while keeping shape intact (or at least attempting to). Let's start with a basic map projection. In this case I am using the Plate Carée projection, a variant of the equirectangular projection. This is what it looks like:



World countries shapefile courtesy of ArcGIS Hub (source)

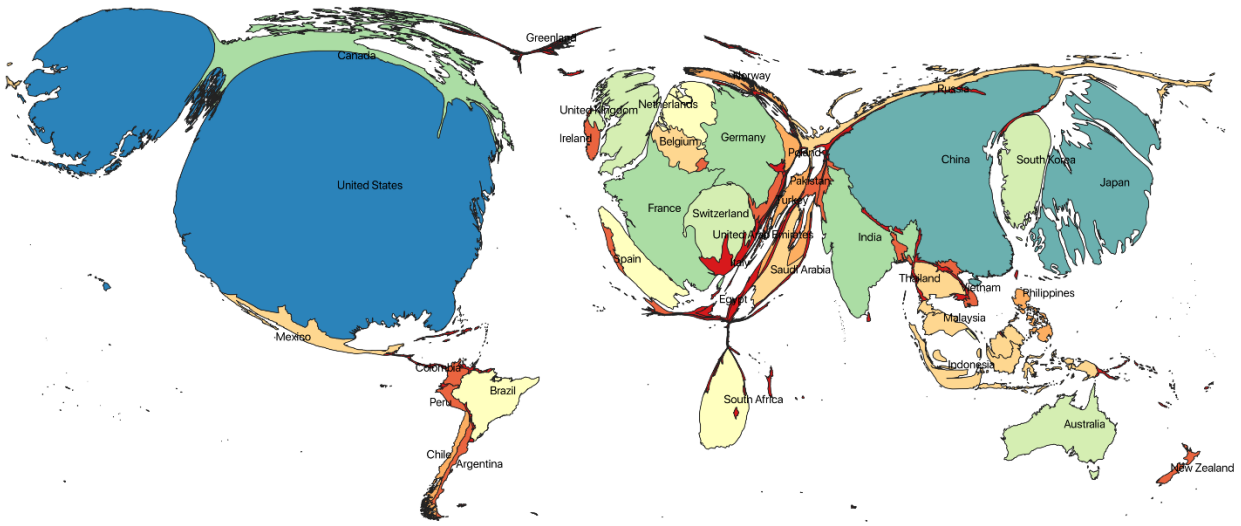
Now let's **weight countries by GDP** (2018) so you can get a general sense of the global income distribution. This means that certain more developed countries will swell up and less developed countries will shrink. But I'll do my best to retain the general shapes of the countries so the map is still intelligible.



Cartogram made with Scapetoad and visualized in QGIS3.4. Data is 2018 GDP in USD terms from the World Bank

I've bucketed countries into a few color coded categories so you can compare similar countries by GDP. For instance, with this chart, you can tell that France ($2.5T), Germany ($3.6T), and India ($2.9T) are in a similar range. Same with South Korea ($2T), Brazil ($2T), and Italy ($1.9T). You can also tell that Australia, Spain, Canada, and Russia have similar GDP — between $1.3 and $1.6 trillion. You get the point.

Now if I were to ask you what the same map with **domestic public equity capitalization** as the key variable might look like, you might imagine it would resemble the above. More GDP, more money to invest in the stock market, after all. Interestingly, this isn't quite the case. Here's the map weighted by the size of domestically listed equity markets:

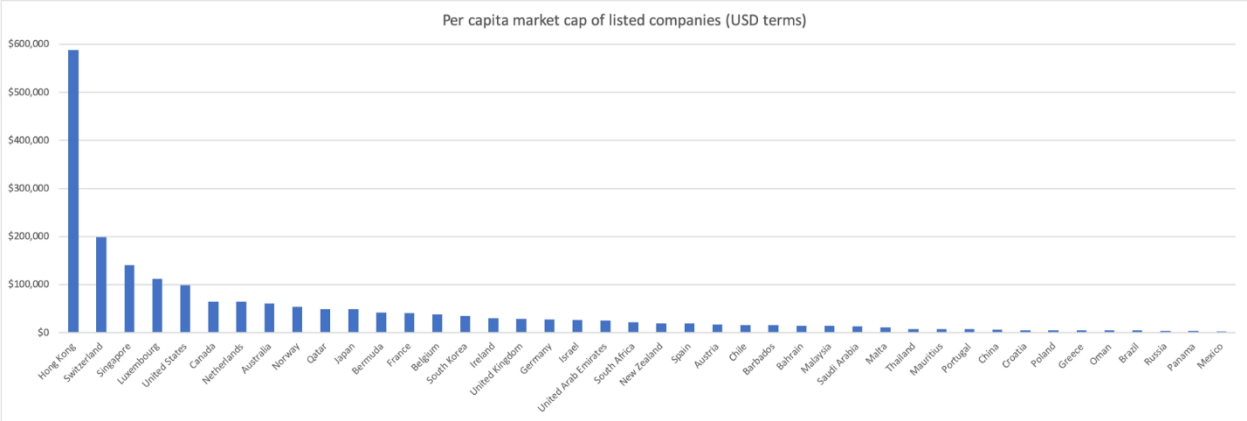


Cartogram weighted by market capitalization of domestically listed companies, 2018 data courtesy of the World Bank

Please note that Hong Kong isn't present on this map because it sadly wasn't included in the open source vector file I used to build the country shapes. Hong Kong would be about 50% the size of China on this map. Compare the Public Equity cartogram with the GDP cartogram and you notice a few things immediately:

- the U.S., even though generates a big chunk of global GDP, still punches above its weight in terms of domestically listed equity
- South America and Africa have under-developed capital markets, even relative to GDP
- Chinese equity markets are prominent, but small relative to their share of global GDP
- niche/haven jurisdictions like Hong Kong (not depicted), Luxembourg, Singapore, Switzerland, are overweighted
- Europe represents a significant fraction of equity markets but less than you might expect from their share of global GDP

Let's dig in to the data a bit more to find the biggest outliers when it comes to countries that punch above their weight from an equity market perspective.



Market capitalization of listed domestic companies (USD) divided by population, *World Bank data*

Amazingly, the per capita market cap of domestic equity in Hong Kong is US$588k. This is a bit of an exception, as many Chinese companies choose to list on the HKEX rather than in Shanghai or Shenzhen. This is partially a function of less onerous listing requirements in Hong Kong, partly a function of Hong Kong's financial hub status, and tighter relationships with western capital markets, and partially a function of the fact that Hong Kong's legislature, judiciary, and attitude towards property rights are influenced by its former status as a British colony.

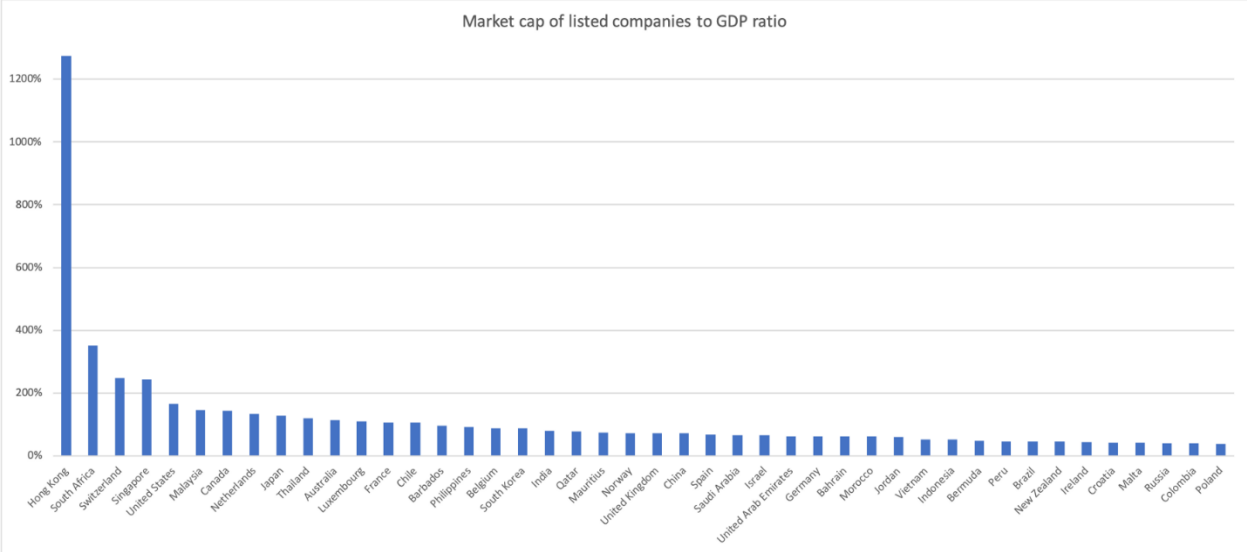
For a more detailed take on why Chinese firms are so fond of listing in Hong Kong, Fanpeng Meng's ***A History of Chinese Companies Listing in Hong Kong and Its Implications for the Future***provides additional context:

Specifically, there are some fundamental elements [present in Hong Kong]: a stable and sound legal system with strong respect of private property ownership, an absence of exchange rate control with the linked exchange rate, an efficient and sophisticated banking sector populated by some of the world's top banks, a simple and low-rate taxation regime in which there are no capital gains taxes and whereby income taxes are charged on a territoriality basis, and a relatively clean and transparent business environment intensively monitored by the government.

Listings in Hong Kong are quite significant relative to China, totaling about US$4.3T compared with China's US$8.7T.

Other states scoring highly on the per capita equity market cap figures include a smattering of haven states like Switzerland, Singapore, Bermuda, and Luxembourg, and developed nations like the U.S., Canada, the Netherlands, Norway, and Japan. Regional financial hubs like Qatar, the UAE, and South Africa also score well by this measure.

Another similar measure is the aggregate market cap to GDP ratio. This synthesizes the two cartograms depicted above, so you can find the biggest outliers without having to visually inspect the charts.



The ratio of the market capitalization of listed domestic companies (USD) to 2018 GDP, World Bank data

Compared with the per-capita metric, this one better selects for nations which have a lower overall standard of development but still have large equity markets relative to their economies. Again, Hong Kong is the stark outlier here. But it's joined in the list of unexpectedly large equity markets by places like South Africa, Malaysia, Thailand, and Chile.

South Africa is an interesting case study. In Africa, there are only three meaningfully developed local equity markets — Nigeria, South Africa, and Egypt. South Africa, a historically prosperous former British colony with the lingering presence of British institutions, is the largest of the three. Literature on equity development in Sub-Saharan Africa is sparse.

Political risk determinants from the International Country Risk Guide Methodology

POLITICAL RISK COMPONENTS		
Sequence	**Component**	**Points (max.)**
* A	Government Stability	12
* B	Socioeconomic Conditions	12
* C	Investment Profile	12
* D	Internal Conflict	12
* E	External Conflict	12
F	Corruption	6
G	Military in Politics	6
H	Religious Tensions	6
I	Law and Order	6
J	Ethnic Tensions	6
K	Democratic Accountability	6
L	Bureaucracy Quality	4
Total		100

Some answers can be found in an IMF working paper on the topic (Andrianaivo and Yartey 2009). The authors conclude from a cross sectional regression that the most important determinant of equity market development in Africa, aside from straightforward variables like domestic savings and per capita GDP, is political risk. This stands to reason: if a military junta takes over, or parliament is dissolved, or the country experiences armed insurrection, equity markets will not develop. I've inserted the political risk rubric that the authors used to give you an idea of the relevant criteria. Historically, South Africa has been relatively conflict free (their main post-independence conflicts were minor excursions in Namibia and Angola) and has benefited from stable rule under the ANC, although political conditions have deteriorated in recent years.

My main reaction from the data is to observe that the development of a vibrant equity market is somewhat of an aberration. There are a huge number of disqualifying features — and indeed, your typical state does ***not*** in fact have a liquid domestic equity market. So what explains the uneven development of public equity markets around the world?

Rules Make the Market

So why do some jurisdictions dominate when it comes to the issuance of public equity? As it turns out, there's an incredibly vibrant literature motivated by this specific question. The foundational, field-defining paper is **Law and Finance** by La Porta, Lopez-de-Silane, Shleifer, and Vishny.

Law and Finance NBER Working Paper №5661 Issued in July 1996 NBER Program(s):Corporate Finance Program This paper examines legal... www.nber.org

If you haven't read it, I strongly recommend a read. It's one of my favorite economics papers, because the methodology really is dead simple: the authors simply look at the variance in investor protections across a broad array of countries, and realize that legal traditions in those countries explain a significant fraction of that variance. In other words, the legal tradition employed on a country-by-country basis, which informs_ what it means to be a shareholder._

Specifically, the authors divide commercial legal traditions in 49 jurisdictions into civil law and common law, further subdividing civil law into German, French, and Scandinavian variants. Common law refers to the British tradition of allowing judges to shape the law through precedent, whereas in civil law, inherited from the Roman tradition, the law is generally created by the legislature, with case law (precedent-setting through court cases) being secondary.

As the authors (henceforth LLSV) note,

[Civil law] originates in Roman law, uses statutes and comprehensive codes as a primary means of ordering legal material, and relies heavily on legal scholars to ascertain and formulate its rules

More abstractly, you can think of common law as a bottom-up, adaptive approach, and civil law as a top-down, more rigid approach. The consequential differences between jurisdictions with diverging legal traditions are significant; indeed, it has been compellingly argued that Brexit primarily boils down to a dispute between legal traditions (in which the EU attempted to impose a civil law tradition on the common law UK, causing frictions). In the words of the Economist, "English lawyers take pride in the flexibility of their [common law] system, because it can quickly adapt to circumstance without the need for Parliament to enact legislation." In short, common law is considered to be faster moving and more adaptable — ideal for fast-changing capital markets.

A full 21 countries in the sample inherit France's civil law tradition, many of which were conquered by Napoleon. Others were added as part of France's colonial holdings in Africa and the Pacific. And French jurisprudence informed the structure of post-colonial regimes in the wake of Spanish and Portuguese empires in Latin America.

The British Empire led to the proliferation of English jurisprudence throughout the commonwealth. Strikingly, these colonial origins seem to have had long term effects on the future development of shareholder rights, hundreds of years later. As LLSV note:

[L]aws differ a great deal across countries: an investor in France has very different legal rights than she does in Britain or Taiwan. Moreover, a large part

of this variation is accounted for by differences in legal origin. Civil laws give investors weaker legal rights than common laws do. The most striking difference is between common law countries, which give both shareholders and creditors the — relatively speaking — strongest protections, and French civil law countries, which protect investors the least.

Mechanically, LLSV enumerate specific shareholder rights which speak to the extent to which shareholders are protected against directors. A selection are listed below:

- **One share one vote**: whether laws exist to tie shares to votes, as opposed to dual classes or nonvoting tranches of equity. The authors consider jurisdictions with these laws as more shareholder friendly
- **Proxy by mail**: whether or not shareholders are allowed to vote by mail (more hindrance in shareholder votes disempowers shareholders, especially smaller ones)
- **Oppressed minorities mechanism**: whether or not minority shareholders (owning 10% or less of share capital) have the ability to challenge the decisions of management or force a buyout of their shares in the case of certain changes like M&A activity
- **Preemptive rights:** whether shareholders have the right of first refusal over new equity issuance
- **Percent of capital required to call a shareholder's meeting:** the higher the required fraction, the less friendly the jurisdiction is to minority shareholders

Their conclusions, while simple from a statistical perspective, were revelatory in the corporate governance literature. LLSV found that:

[A]long a variety of dimensions, common-law countries afford the best legal protections to shareholders. They most frequently (39 percent) allow shareholders to vote by mail, they never block shares for shareholder meetings, they have the highest (94 percent) incidence of laws protecting oppressed minorities, and they generally require relatively little share capital (9 percent) to call an extraordinary shareholder meeting. The only dimension on which common-law countries are not especially protective is the preemptive right to new share issues (44 percent). Still, the common-law countries have the highest average antidirector rights score (4.00) of all legal families. Many of the differences between common-law and civil-law countries are statistically significant. **In short, relative to the rest of the world, common-law countries have a package of laws most protective of shareholders.**

Taking the analysis further, the same four authors followed their seminal paper with the 1997 Legal Determinants of External Finance, demonstrating

that not only do common law countries systematically offer better shareholder protections, but that these investor protections empirically manifest in larger and more robust capital markets.

The authors summarize the key finding:

[T]he legal environment — as described by both legal rules and their enforcement — matters for the size and extent of a country's capital markets. Because a good legal environment protects the potential financiers against expropriation by entrepreneurs, it raises their willingness to surrender funds in exchange for securities, and hence expands the scope of capital markets.

This might seem like a simple point — more investor assurances yield more capital deployed, but when you reflect on the fact that these assurances trace back to the legal philosophy undergirding the financial system, one becomes starkly aware of the path dependence in capital market outcomes. Put simply: institutional quality dictates allocative outcomes. The U.S. isn't just the largest hub of capital formation on earth, it's disproportionately large. This system creates extreme outliers like Hong Kong, Singapore, or Luxembourg.

A related conclusion can be found in Hernando de Soto's book, ***The Mystery of Capital***. De Soto evaluates the relationship between property rights and capitalism in a large number of countries worldwide, and concludes that for capitalism to function properly, it must rest atop the bedrock of strongly codified property rights. His reasoning is as follows: the main form of savings for individuals worldwide is through property (in particular, real estate). The main way that capital formation occurs on a small scale is through the monetization of that property, turning it from a purely instrumental asset (somewhere to live) into a capital asset. One example of this would be an individual borrowing against their house in order to set up a small business. If lots of savers can mobilize the capital that they naturally accumulate, capitalism can flourish.

However, as de Soto finds, a significant chunk of property, especially in the developing world, is poorly codified. That is to say, homeowners cannot prove that they hold the deed to their home (a deed may not exist), and they may not have a plausible path to formalizing their ownership. This inhibits their ability to monetize their property at all. Typically, this is due to a dysfunctional bureaucracy or a state apparatus which does not provide a means for incorporating black/grey markets into the formal economy. My takeaway from this remarkable book is that free market economies alone are not enough; they must be accompanied by a legal and bureaucratic apparatus which is flexible enough to enable property owners to make transition from ***de facto*** to ***de jure***, and these rights must be consistently respected. For a longer take on De Soto's conclusions as applied to Bitcoin, see Allen Farrington's essay on the topic.

Cryptocurrencies, perhaps more so than any asset, mitigate these institutional constraints. It's trivial to prove to a third party that you own some Bitcoin; it's trivial to self-custody this claim, and settlement is physical and almost immediately final. Cryptocurrencies are ***monetary institutions*** — the protocol lays out a set of rules for permitted behavior, and all participants must adhere to them. This is what gives cryptocurrencies such remarkable global penetration: users mutually understand where they stand relative to the system and the established ruleset, and trust that no well-connected lobbyists are able to exert local policy on system. This is what Nick Szabo refers to as social scalability — the idea that a system can only scale to serve millions of disparate users if it standardizes behavior in a narrow domain (say, rules for what transactions are valid) while minimizing idiosyncrasy and obscurity (which undermine the system's credibility).

Don't Count the U.S. Out

Within the crypto industry, the U.S. has a reputation for being extremely restrictive with regards to the issuance of new cryptoassets. Since 2017 with the infamous DAO report, the SEC has made it quite clear that ICOs are more often than not unregistered securities issuances, and that issuers should be held to the same standard as conventional issuers of securities. In the U.S., if you want to sell equity to the general public, this entails significant legal costs and a high standard of transparency.

In the crypto markets so far, virtually no issuers have met this conventional standard (one exception is Blockstack). Moreover, it's not even clear what information would be considered material for the issuance of a novel protocol or token. In their paper _What Should Be Disclosed in an Initial Coin Offering?, _Brummer, Kiviat, and Massari convincingly make the case that the various disclosure frameworks in the U.S. poorly fit the reality of token issuance, calling for a more appropriate model to be devised.

The significant amount of teeth-gnashing within the crypto industry belies the reality of these markets: the vast majority of tokens sold to the public were entirely meritless, and carried no investor protections whatsoever. Even in cases where tokens purportedly held benefits relative to conventional issuance, with touted features like algorithmically enforced vesting schedules, much of the time these soft provisions were not actually enforced. Hoffman's _Regulating Initial Coin Offerings _takes a careful look at the promises made by promoters which could have been algorithmically enforced. In a survey of the top 50 ICOs that raised significant capital in 2017, Hoffman evaluates the actual implementation in code of promises made to investors. These fall into three categories:

- Promises made about the restriction of supply

- Promises made about vesting schedules that team members were subject to and restrictions on transfers
- Promises about surrendering power to modify smart contracts once deployed (many issuers claimed they would ultimately give up this power)

Unsurprisingly, the authors, by examining the actual code written by issuers, find overwhelming noncompliance with these relatively weak restrictions. So not only were issuers providing extremely limited assurances to buyers; ***those issuers could not even adhere to their own, self-imposed standards***!

So we have a situation where the vast, vast majority of token offerings openly flouted the law. And _lex cryptographia _was an inferior substitute for the law: the few assurances which could indeed be encoded into a smart contract were only spottily upheld. In this context, U.S. policy towards token issuance seems downright reasonable. Assuming that the predominant legal analysis of token launches (in which a single issuer sells tokens to the public) as unregistered securities is correct, the fact that this issuance was happening through a new technological medium is irrelevant.

If you strip away the technobabble and the (generally spurious) claims of "decentralization" and "unstoppable applications," you are left with the straightforward issuance of pseudo-equity to the general public. That anyone, even the most devoted crypto stalwarts, imagined securities regulators would turn a blind eye to this practice in perpetuity is baffling. And gradually, the SEC has come to reckon with this market niche. By being relatively (but not overly) stern, U.S. regulators are positioning themselves for a middle path. Far from outright banning tokens and the industry surrounding them, regulators have meted out a mixture of punishments. The SEC has prosecuted the very worst ICOs and given amnesty to others. Some academics have even praised the much-maligned SEC strategy of selectively enforcing the law.

Reminding ourselves that the U.S. has a 40% share of public equity markets for a reason, the professed strategy of many industry participants to seek greener pastures elsewhere seems short-sighted. The fact that an inferior instrument (the public ICO) did not get a regulatory blessing does not mean that the U.S. is destined to lose its crown as the premier locale for capital formation. Indeed, many high profile securities regulators in other capital-friendly jurisdictions are falling into step with the U.S., as is customary. If crypto issuance is to evolve into something friendlier to buyers, with functional, germane disclosures, genuine algorithmically-enforced vesting and lockups, and perhaps other strongly codified investor protections, there's no reason that regulators wouldn't acknowledge this reality. That they

haven't given carte blanche to these issuances is a reflection on the poverty of the implementations we've seen so far, not the weakness of the idea.

Recall, given the above, why the U.S. hosts a disproportionate share of public equity capital. Not only has the U.S. been a hegemonic power for most of the last century, but it has been politically stable, has not seen violent conflicts on its shores, and it boasts an accommodating common law regime which has manifested in strong shareholder protections. Additionally, it has a large middle class for which investing in equities is as much as pastime as it is a necessity. This affinity for active consumer participation in capital markets has unsurprisingly spilled over into crypto as well. Coinbase, the largest crypto exchange/custodian in the world (by far!), is an American company. The largest financialized Bitcoin product is the Bitcoin Investment Trust, issued by the NY-based Grayscale. The first established global financial institution to take Bitcoin and digital assets seriously was the Boston-based Fidelity. To the extent that this industry is an ***asset class*** (to be clear, the jury is still out on this!)_, _jurisdictions with the financial plumbing and the consumer demand for exposure will naturally be the first to service it.

This perspective may strike you as anglocentric. However, consider it in context. Within the crypto industry, the U.S. is considered a pariah simply for enforcing its local laws (and even then, extremely permissively — see the Block.one settlement). The token frenzy has been chased overseas for now, but it's unlikely to develop into a functional securities market if it operates in an anarchic mode, dependent on the goodwill of marginal jurisdictions. The industry's best hope is to acknowledge that market oversight is what makes them function and embrace a regime which takes a commonsense view about shareholder/tokenholder protection.

When and if these markets do mature, and security tokens, or on-chain cashflow-wrapped instruments, or highly automated smart-contract-mediated equity do emerge as a meaningful segment of the securities industry, I would fully expect U.S. regulators to engage productively. At that time, issuers and market participants will benefit from taking part in the most dynamic capital markets on earth.

The Tortoise and The Hare

By Marty Bent

Posted February 10, 2020

“Trust me.”

“I want to be candid. This strategy will cost money, involve risk and take time. We will have to try things that we’ve never tried before. We will make mistakes. We will go through periods in which things get worse and progress is uneven or interrupted.” — Timothy Geithner

This is but one snippet of one iteration of the pitch newly appointed Treasury Secretary Timothy Geithner shilled to the public on February 10th, 2009.

At the time, he was frantically running across Washington D.C., from Capitol Hill to media appearance after media appearance in an attempt to convince his fellow citizens that $300 Billion of the remaining TARP funds he was about to spend on toxic assets was not a bad deal. The populace was wary that the banks he would be buying the toxic assets from would refuse to sell below market price. They had been through a lot at this point.

As Geithner was uttering the words quoted above, the computers running bitcoind v0.1.5 and below were racing to confirm the 3,768th block of the Bitcoin blockchain. Ordering their CPUs to go out and seek a SHA-256 hash below the difficulty target at the time so that they could collect 50 bitcoin block subsidy.

No one really noticed it then, but there were two solutions to the Great Recession running in parallel; the one put forth by Timothy Geithner, Ben Bernanke and crew, and another put forth by Satoshi Nakamoto.

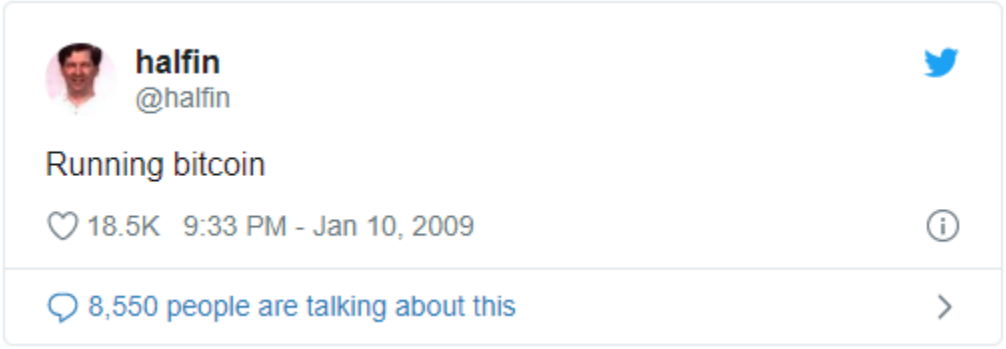
The powers that be in the US and across the globe - those attempting to put Humpty Dumpty back together again - were too busy to be cognizant of their competition in the aftermath of the financial crisis. They were rushing to make sure people would be able to get cash out of ATMs. Satoshi and the band of misfits who were drawn to the new open source protocol he launched were hyper aware of their competition. This is evidenced by the message that was etched into Bitcoin’s genesis block, “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”. A reference to a headline in that day’s issue of The Times of London.

This wasn't the only reference to the traditional monetary system that would be made by Bitcoin's creator. Coincidentally, on the day after Timothy Geithner was making quick iterations of his pitch to the American people Satoshi made a direct reference to the Central Banking system and its flaws in his eyes:

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust." — Satoshi Nakamoto

Over the course of the last eleven years, the two solutions have been going head to head in the market. The solution put forth by Geithner and crew - who have bequeathed control of the levers to the Fed presidents and Treasury secretaries who have followed - is more of the same; money printing. The accumulation of long-term debt in hopes that we can stoke production today. On the surface, it seems to be working. But can this type of monetary policy persist?

The solution put forth by Satoshi is in direct opposition to the one put forth by the banking elite; a sound digital money that cannot be debased or controlled by a select few. Bitcoin is controlled by everyone and no one at the same time.



The first man to ever receive a bitcoin transaction. RIP Hal.

The two competing solutions are engaged in a classic Tortoise v. The Hare scenario.

The Federal Reserve and other Central Banks around the world have sprinted out of the gate; increasing the size of their monetary bases by orders of magnitude in very short order as they tinker with interest rates on a whim.

The Bitcoin Network has been on a slow grind for the last eleven years. Consistently producing blocks roughly every ten minutes as those who would like to see it succeed meticulously fortify the system. Working to make it

more efficient, more scalable, more private and more robust one pull request at a time.

Most people don’t realize it, but we’re all watching a race to fix the money play out in real time. The money game is a long game. My sats are on the Tortoise.

Why Bitcoin is Not a Security

By Elisabeth Préfontaine

Posted February 10, 2020

Bitcoin is a broad topic and links together many disciplines such as cryptography, game theory, monetary theory, monetary history, economics, computer science, network dynamics, thermodynamics and information theory. This text shall be understood as a demonstration that Bitcoin, Bitcoin-related dealings, trading, and applications unequivocally sit outside the scope of the securities or derivatives legislation. This demonstration should make the case as to why the proposed framework for crypto-assets trading platform by the Consultation paper 21–402 and CSA Staff Notice 21–327 does not apply to Bitcoin.

1.1 Bitcoin Never was a Security

Here is a brief but straightforward explanation as to why Bitcoin was not a security from the start.

Monetary Capital

- No monetary capital was raised to develop Bitcoin.
- There was never a bitcoin Initial Coin Offering (ICO).
- There was no investment of capital from a founder.
- There was no premine (i.e. founders keeping a portion of the tokens for themselves).
- There is no bounty program, or free tokens offered to ''promoters''.
- No capital was spent to promote its launch.
- Growth was entirely organic.
- Bitcoin was born out of an 8-page idea and roughly 40 years of R&D.
- The early-stage was sustained by volunteers.
- Bitcoin is not debt; Bitcoin is not equity. Bitcoin is Bitcoin.

Value

- Bitcoin is a bearer instrument. It solves for the double spending problem in the digital world.
- Bitcoin is functional since its inception and has an up time of 99.9837111434% since then.
- Bitcoin has no financial statements.
- Bitcoin doesn't share security-like attributes such as a profit-sharing interest.

- The currency bitcoin has unique characteristics where individuals can express personal preference (see section 1.3)
- The market has spontaneously attributed value to it.
- The price is market driven. The value of one bitcoin is one bitcoin.
- The network effect of Bitcoin has value: its community, its users, its developers.
- The proof-of-work has value. It is an expensive monument of immutability.
- The stability at the base layer has value.
- The transparency and predictability of Bitcoin's monetary policy has value.
- The self-regulating mechanism embedded in bitcoin has value.
- Bitcoin is its own and we are still early in the discovery of its full potential.

Decentralization

- Bitcoin is not a common enterprise. It is a network.
- Bitcoin is a decentralized system recording a sequence of transactions with 80,000+ nodes
- Bitcoin is not a company. There is no authority in charge, no management team, no CEO, no head office, no sales team, no tech support line.
- It is not centrally planned in an effort to deliver an eventual product. Bitcoin exists.
- No one person (or entity) controls the network or the protocol or can change the rules.
- No2X is a specific event that proved, in real life, bitcoin's decentralization and uniqueness versus other centralized cryptocurrencies.

Unique Phenomenon

- A replica or a bitcoin 2.0 / 3.0 / 4.0 would inevitably be centrally planned.
- That central planning would most likely involve securities-like characteristics.
- Now that the path to creation is known a 51% attack could be successful in the early days

This section aimed to demonstrate that Bitcoin is not and never was a security. It is very possibly a one-time phenomenon and draws a line between bitcoin and the rest of so-called crypto-currencies.

We ended up with 2,000+ crypto-currencies because of the Blockchain bubble. A very sticky narrative has developed around the "technology underpinning bitcoin", as if it could be considered in isolation. The market created the name 'blockchain' which led to marketing narratives and fund-raising pitch decks being created. Much like the "snake-oil" claims of previous centuries, this new technology would solve almost any problem in the world (from lettuce tracking to identity management). This spurred the rise of blockchain projects raising capital through ICOs (initial coin offerings) in a tulip-bulb like mania.

We ended-up with 2000+ so-called crypto-currencies because very few took the time to first understand what, how and why bitcoin is. If organized true data without a central authority is not needed, then decentralization and open architecture are not needed. This would have helped contrast Bitcoin's network and infrastructure with Initial Coin Offerings (ICOs) which are essentially a global venture-capital crowdfunding mechanism.

Could there be networks that initially started as an ICO and now are too far advanced and can no longer be considered a security? Perhaps. This will be a definition question that securities regulators will need to answer. But Bitcoin did not start as an ICO.

Understanding the uniqueness of Bitcoin's conception and how it gave life to a digitally native scarce asset is perhaps the most direct way to comprehend what makes it different from a security-like instrument.

1.2 What is Bitcoin? Bitcoin is Text.

Bitcoin is surely different from anything we have seen before. Some argue that Bitcoin is a form of money, others argue it is a commodity and some simply don't see anything in Bitcoin. However, this does not matter. What matters is Bitcoin exists and its network and protocol do exactly what they are meant to do, for over ten years. Bitcoin is text, information, speech. It communicates.

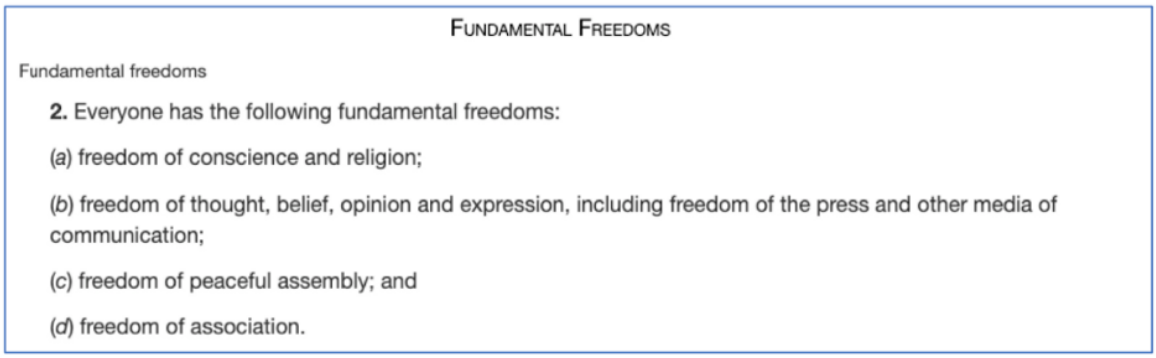
"Bitcoin is a distributed ledger system, maintained by a network of peers that monitors and regulates which entries are allocated to what Bitcoin addresses. This is done entirely by transmitting messages that are text, between the computers in the network (known as "nodes"), where cryptographic procedures are executed on these messages in text to verify their authenticity and the identity of the sender and recipient of the message and their position in the public ledger.

The messages sent between nodes in the Bitcoin network are human readable, and printable. There is no point in any Bitcoin transaction that Bitcoin ceases to be text.

It is all text, all the time.

The purpose of Bitcoin is to absolutely verify the ability of the owner a cryptographic key(which is a block of text) that can unlock a ledger entry in the global Bitcoin network." — Beautyon

There are deep implications to understanding Bitcoin in such a way as it has ramifications to the fundamental freedoms 2(b) of the Canadian Charter of Rights and Freedoms.



FUNDAMENTAL FREEDOMS

Fundamental freedoms

2. Everyone has the following fundamental freedoms:

(*a*) freedom of conscience and religion;

(*b*) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;

(*c*) freedom of peaceful assembly; and

(*d*) freedom of association.

Is IIROC, the national **self-regulatory** organization overseeing all investment dealers and trading activity on **debt and equity** marketplaces in Canada, and the CSA, aiming to challenge the Constitutional act of 1982 by trying to legislate software developments, text and messaging systems?

1.3 The General Understanding of Bitcoin is "Digital Gold"

The perception of value varies from one individual to the next. Individuals will purchase comic books, preserve them in their original sleeves without ever reading them. Others will purchase figurines, keep them in their original boxes and never play with them. Others will collect vintage cars knowing very well they can only drive one at a time. Other examples include watches, antique furniture, precious stones, paintings, sculptures, fine jewelry and wine.

The point here is their value is not tied to their use, but rather attached to the perceived value in the eyes of the owner. Gold has a valuation significantly above its industrial or ornamental usage. In today's world, it is unlikely anyone buys a pair of shoes with gold. As such, bitcoin doesn't need to be money (in the transactional definition of the term), but it can be valuable. What these examples have in common is scarcity. Some individuals will own them to store value, to brag, to seduce a mating partner or to speculate on the future price appreciation. Generally speaking, individuals will self-custody them.

I do not have the pretension to define something as complex and broad as bitcoin nor to define its full potential, for one reason: it is the free market that dictates what Bitcoin is. I invite the curious reader to consider these selected texts to realize the depth and uniqueness of the topic. For the first time in the history of mankind, a scarce digital asset exists. Bitcoin is not debt or equity; Bitcoin's infrastructure permits the first digitally native bearer instrument without a central authority. Bitcoin is its own.

The monetary policy of the Bitcoin protocol is crystal clear. Its predictability, its limited supply and its stability at the base layer are valuable attributes. Accordingly, bitcoin is often referred to as "digital gold" (1, 2, 3, 4, 5, 6, 7). Therefore, bitcoin can be viewed as a limited-supply consumer good.

It can be argued that bitcoin is;

- rarer than gold since technological innovation cannot increase its actual supply or the speed of production.
- more portable than gold as it can be used over the Internet, ham radio, satellite or paper.
- useful in a way that gold can't be, as bitcoin can be programmed.

The curious reader will probably enjoy _Shelling Out: The origins of Money _by Nick Szabo. A special consideration must be paid to the concept of unforgeable costliness in the context of the energy consumption as it anchors Bitcoin is the physical world. Proof-of-work (energy consumption), the difficulty adjustment and the monetary policy are important concepts to understand in order to draw parallels and grasp the comparison with digital gold and to unbundle bitcoin from other crypto-assets.

Some won't see any value and won't buy bitcoin. This is simply how a market operates (i.e. where conflicting views meet). It is by the same market mechanism that someone did not invest in Amazon +/- 20 years ago when it was trading in the low double digits. Some saw value beyond a simple online book store, some disagreed, some have been rewarded, some have not.

Bitcoin is neither a debt or an equity instrument and from the start never fit the definition of a security. It can rather be viewed as a consumer good or a commodity and its dealing, trading and marketplace activities sit outside IIROC and CSA's legislative scope.

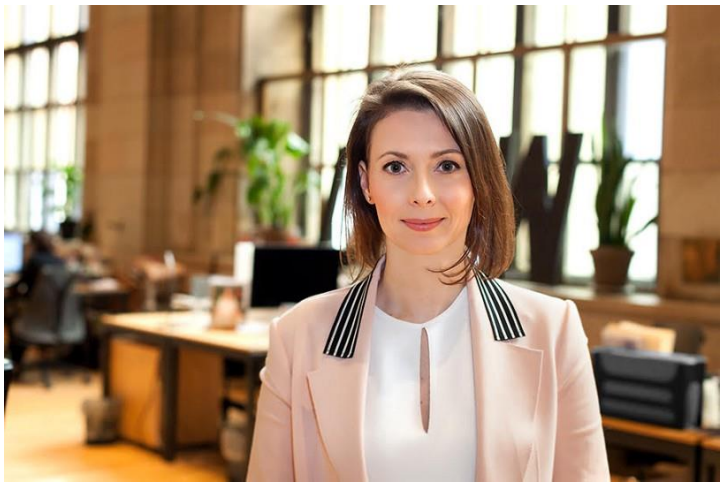
1.4 How are the U.S. SEC and the U.S. CFTC Treating Bitcoin?

The U.S. Securities and Exchange Commission (SEC) has stated that Bitcoin is not a security. Here is a video interview dated June 6th 2018, where the Chairman of the SEC, Jay Clayton is crystal clear:

"...Cryptocurrencies, these are replacements for sovereign currency, replace the Dollar, the Yen, the Euro with Bitcoin. That type of currency is not a security. Let me turn to what is a security (...)"

The U.S. Commodity Futures Trading Commission (CFTC) has also already stated that:

"Yes, virtual currencies, such as Bitcoin, have been determined to be commodities under the Commodity Exchange Act (CEA)"



Why is it that a year later, Canadian securities regulators are still not clearly expressing themselves on the matter? Vague language such as "may represent" is used abundantly in their communications.

Just like a collection of rare butterflies, Bitcoin falls outside the scope of the security regulatory regime. This is valid for, but not limited to, the butterfly catcher, the distributor, the servicer, the collector, the curator and the gatekeeper.

Elisabeth Préfontaine, MBA, CFA, CAIA

To support this work, you may donate BTC to :

15Zb5wRJ95i2o5Pw6xSpz2xrHt2oL9xLmj

Octonomics is an independent research and consulting firm dedicated to financial technologies. More specifically interested in the fast and evolving world of Bitcoin, its ecosystem and applications.

A weekly newsletter is available by registering here.

A World Without Bitcoin

By Alex Gladstein

Posted February 11, 2020

The year is 2040, and cash is gone. The money you use on a daily basis has fully transitioned into a tool of surveillance and control.

In midtown Manhattan, you tip sidewalk performers with a scan of your wearable, your face, or your fingerprint. Coins and dollar bills are now curiosities—fossils from a forgotten age.

In Beijing, the government-issued Yuan has long since been digitized into the ubiquitous DCEP. Holding old paper notes is illegal, all payments are touchless or biometric, and all transactions are natively linked to your full identification stack. Every time you buy something, your national digital profile simultaneously updates.

Transaction privacy was one of the last freedoms to be stripped away in China. Now, your communications, movements, and interactions with other citizens are tracked with billions of cameras, real-time surveillance streaming from your wearables, swarms of micro-drone recorders, and immensely powerful algorithms, linking everything together in a panopticon.

In Caracas, Venezuela, the recovering economy runs on digital dollars. There is some street bartering, of course, but greenbacks finally became obsolete a few years ago, and other bearer assets like gold remain incredibly rare. If you want to buy something, you have to do it electronically and the transaction will be tracked and linked to your citizen profile.

In Lagos, like in many African capitals, all commerce is carried out on the rails of Chinese fintech, and everyone communicates seamlessly with the latest version of WeChat. The Nigerian economy runs on DCEP and the government and its 300 million citizens basically act as a Chinese satellite state.

At some point in the 2030s, governments around the world made cash illegal. They initially accomplished this feat through a demonetization process where public officials announced a new digital economy that they claimed would not leave anyone behind, would increase stability, and would make it easy to catch criminals and money launderers. Most citizens believed them.

Even in countries where the majority never had a brick-and-mortar bank account, all citizens were encouraged, then forced, to create ID-linked digital currency accounts accessible through their wearables or biometrics. Then,

they were given a multi-year time window during which they could redeem their cash for a shrinking amount of digital credits. Almost everyone cashed in and went fully digital early on, when they could get the most credits. After the window expired, it became a punishable offense to carry paper or metal money.

Now, in 2040, there are two dominant currencies in the world: the digital dollar and China's DCEP. The world is roughly divided: North America, Europe, and some top U.S. allies use the digital dollar, while the rest of the world uses DCEP. Very few other currencies remain.

Some rogue states still produce their own currencies, but these don't last long and aren't worth much to anyone else. These regimes tend to inflate their money supply extremely quickly, severely devaluing their currency, and eventually forcing authorities to create new currencies. This cycle destroys trust between state and citizen. Eventually, such governments give up sovereignty in exchange for survival and turn to the digital dollar or DCEP. The common person effectively has no ability to store savings in a way that isn't controlled by either the American or Chinese government.

There hasn't been any meaningful innovation in savings technology. Most citizens simply just save up their digital credits, but the value of their credits depreciates against real goods relatively quickly. And then there is autotaxing. By now, taxes are automatically deducted from your credit balance and tax rates rise unpredictably and always, it seems, too fast.

As in previous decades, some poor and middle class citizens still buy things like cattle or sheet metal in an effort to save against inflation, but all (save the 1%) are locked out of premium assets like real estate, fine art, vintage wine, and other scarce items.

Financial privacy has virtually disappeared, and not just in China and the DCEP countries. Along with the rise of ubiquitous surveillance cameras in public places – all linked together with AI-powered insta-analysis – all transactions are immediately linked to individuals. With cash gone, it's extremely difficult to buy a burner phone or SIM card. Fines for trying to manipulate your credit wallets are harsh, and no one ever invented an alternative digital currency that was able to hold value.

Big data analysis wasn't always so powerful. But it is now. Of course, humans had credit cards for decades, but unlike those early days, now governments can sift through all financial data with the press of a button.

To get credits, you need to provide ID. To use credits, you need to be loyal. To get the best perks, you need to be a perfect patriot. Around the world, digital currencies give governments unprecedented abilities to control their citizens. If your digital profile doesn't have a top rating, you're locked out of many

public services and benefits. In dictatorships, if you dare to criticize the government, you immediately lose your financial abilities. Some say being in financial jail is worse than being in actual prison.

Corporations do create their own money. Libra was just the beginning. But all these credits are inevitably pegged to the digital dollar or DCEP, and therefore are surveillable, censorable, and confiscatable. They don't offer an escape.

There has also been a dramatic increase in the real-time sale of your data and behavior to third parties. There is practically no way to buy something without your government and a range of corporations knowing. Instantly upon purchase, you're met with a variety of advertisements. Many people have upgraded to smart visors and retinal implants, and they get advertisements there, too. Unless, of course, they can pay for the premium versions. In the DCEP countries, one can opt out of everything except government propaganda.

The public feared the rise of the Orwellian police state, and it came, but they also got the dystopia of Aldous Huxley. In this brave new world, a sophisticated constellation of carrots and sticks built into the financial system encourages and reinforces state-compliant behavior with impressive efficiency. Patriotism is addictive.

The Chinese social credit system, much mocked in the early 2020s, was finally implemented by governments worldwide in the ensuing decade, and with the transition into a fully digital economy, has become incredibly effective at stamping out dissent.

Governments ran sweeping campaigns to locate every single citizen within their borders and connect them to national identity systems. India's Aadhaar was the first of many, initially promoted as a miracle for the unbanked, vulnerable, and stateless. But later, it became clear that these ID networks were just surveillance and exploitation machines.

Things are more fair for some, but a tiny few control everyone else in a way not even previously imaginable. The benevolent idea of "compliance" has led ultimately to slavery. It is the digital banality of evil.

Even now, governments continue to innovate their surveillance tech. Some citizens are being offered valuable perks for agreeing to install their credit wallets into their wrists or retinas. They say it's the ultimate in touchless convenience. The program is popular. Some analysts say that by 2050, everyone will have one.

This could be our world.

But thankfully, this is a fantasy. In our world, we have an escape.

In 2009, a pseudonymous programmer by the name of Satoshi Nakamoto launched Bitcoin, a sovereign financial system.

Over the next few years, this decentralized money project grew. A global community made it strong, and grew a brilliant initial design into an unstoppable force. Over time, there were more nodes, more miners, more users, and more adoption.

By 2020, the separation of money from state had begun.

What was first a curiosity turned into a powerful global phenomenon. Once people understood they could digitally transact in a parallel economy that authorities didn't control, they wanted to learn more and get involved. Satoshi pioneered a way out of the panopticon with proof-of-work, creating a non-governmental financial system.

Our future 2040 is still a horribly imperfect place, but omniscient tracking and surveillance is much more difficult for governments to achieve, because Bitcoin has enabled the survival of a digital form of cash.

So let's rewind — let's describe the year 2040 again, but what it could look like not just with government issued digital currencies but also with Bitcoin.

In the Bitcoin future, privacy has actually improved in some areas. With technological improvements in the Bitcoin software, it actually becomes very difficult for governments or corporations to track the Bitcoin use of citizens who practice good operational security. Bitcoin was at one point hard to access and clunky to use – just like email in the early 1990s – but things got a lot easier in the 2020s.

Governments promised waves of crime and terror if citizens dared to use a currency outside of state control. But those waves never came. By 2040, crime rates are essentially the same as they were for the previous century. In the Bitcoin world, however, it's much more difficult for bankers to steal your money and for governments to devalue your savings.

Back in 2020, very few used Bitcoin, and even fewer understood its potential. A long hard road of education was to come. But later in the 2020s, universities began offering courses and degrees in Bitcoin. Eventually, one was able to get a bachelor's degree or even a PhD in Bitcoin Engineering at any top university.

By 2020, tax authorities began asking citizens how much Bitcoin they held or sold, further increasing awareness among the citizenry. But by 2030, most people were using Bitcoin without knowing much about how it works, just as

hundreds of millions of young people once adopted email without knowing how it worked.

Governments tried to prevent their citizens from using Bitcoin, but most measures and bans failed or were unenforceable. The permissionless nature of Bitcoin turned it into a virus that infected the surveillance state, preventing it from reaching its maximum potential.

Even in the most restrictive tyrannies, citizens figured out how to send Bitcoin back and forth in a way that was virtually impossible to effectively surveil at mass scale. Yes, governments are still able to police nations and communities, and investigators find most big criminals, but broad-based financial surveillance has been stopped in its tracks.

By this point, the Bitcoin network is protected by geopolitics. Part of Satoshi's genius was creating an asset that would increase in value due to scarcity. Even bad governments which subsist on authoritarianism got involved in Bitcoin initially because of their greed. But over time, their reliance on Bitcoin shifted their local economy towards it, which in turn hurt their ability to control the money supply and financial system and ended up eroding their control over the citizenry.

The more democratic governments adjusted to life with Bitcoin. For example, many democracies changed the way they taxed their citizens, veering away from an income-based approach. Sales tax, VAT, and "citizen" taxes all became more important. Just as in the 20th century, taxation and the financial relationship between citizen and state continued to evolve in the 21st.

In democracies, the people created laws to allow daily small purchases to be completely private. You can buy groceries, have a small medical procedure, or buy an e-book or podcast without disclosing your identity. Because of this, your digital footprint ended up being much smaller than it would have been had all these events been tracked. Governments still ensure that larger purchases like cars, weapons, and homes require that the seller ID their customer, but for most purchases, your transactions are not uploaded to a national database—just like how things were in the cash age.

Critically, Bitcoin has allowed dissent to survive in an increasingly digital era. Independent media organizations and NGOs are still able to receive funding from supporters, even in the most difficult environments. In mega-cities, one can pay for public transport with Bitcoin-based payments, preventing the authorities from knowing your every step.

Ubiquitous surveillance cameras and data collection from next-gen social media still make privacy in general very difficult to achieve, but at least payments are protected. And Bitcoin becomes a native payment rail for

pseudonymous social media platforms, where citizens can still enjoy avatars online, and practice digital freedom. Without a decentralized currency, all of this would be impossible.

I've painted two visions here.

On the one hand, an Orwellian dystopia.

On the other, an overly-optimistic techno-utopia. Neither will happen.

How close we get to a more positive and open financial future is dictated by what we do now with the Bitcoin ecosystem in 2020 and moving forward.

In this essay I propose six priority areas for you to consider getting involved with. There are of course more aspects of Bitcoin, but the ones I list here will be most crucial for us to tackle in the coming years.

A first priority area is global education. Only a tiny fraction of people on this planet use Bitcoin, and even fewer properly understand its power. The latest estimates put the total number of Bitcoin users at no more than 45 million people — roughly .058% of the world's population. I personally interact with many at the top of the wider cryptocurrency and blockchain industry, ranging from executives to journalists to investors. My best estimate is that, at most, 25% of them understand the underlying principles of how Bitcoin works and why digital scarcity is the key to its success. It's a back of the envelope estimate, for sure, but let's just say that even inside the industry, the number of people who understand the impact Bitcoin may have on the world is small. There aren't enough non-technical explainers; not enough university-level courses; not enough (or virtually no) journalists at mainstream media outlets who understand; few if any initiatives to try and bring this topic to the attention of policymakers, philanthropists, and public figures; and no good Bitcoin film or video content on platforms like Netflix. There is much work to do.

A second priority area is usability. Just as the mobile phone and email were hard to use at first, and only popular with the scientific or economic elite, Bitcoin has begun its life as a niche technology. We should try to break this bubble. In order for that to happen, the average user needs to be able to send and receive Bitcoin with a few clicks and a swipe. But this will take time, as all users should be able to easily control their own keys without relying on a third party. Bitcoin usage needs to be simplified without making critical tradeoffs with regard to decentralization, privacy, or sovereignty. Technical complexity needs to be minimized as well, as Bitcoin should be accessible to those who need it most around the world, who have the least powerful devices and least consistent internet access. Thankfully, things are moving in the right direction. Even in just the past two years, Bitcoin wallets have become much, much easier to use. Just as sending email transformed from a

complex task to a swipe on an iPad, Bitcoin will eventually simplify. Already, unnecessary details are being gradually hidden from the end user in the same way that Signal, for example, made private communications much easier and more widespread than previously possible with clunkier tools like PGP.

Which brings us to the third priority area: privacy. It is critical that privacy be encouraged, normalized, and baked into the Bitcoin ecosystem. Critically, we want Bitcoin on-ramps, wallets, and payment networks that are open source, decentralized, and relatively private. For example, BTCPay Server is perhaps one of the most important technologies in Bitcoin today. Originally a clone of Bitpay, today it allows anyone to set up their own hosted payment server, allowing them to receive donations or payments in Bitcoin, in a way that is much more privacy-protecting. Each transaction is done via a unique invoice, and can be dumped into a wallet that isn't attached to your ID. This will prove equally important for mom-and-pop corner stores as it will for non-profit organizations operating under authoritarian regimes. Other key innovations in this space include the upcoming Taproot upgrade, which will help reduce the amount of information Bitcoin transactions leak on the blockchain; innovations in mixing technology like CoinJoin that help camouflage users; and, of course, the Lightning Network, which takes transactions off the surveillable chain into a second layer.

This brings us to our fourth priority area: scaling. All base monies need to be scaled through secondary layers to have a global impact. Consider the gold-based economy, where we invented paper notes to help scale commerce. Or the dollar-based economy, where companies like Visa helped spark growth around the world. For Bitcoin, the most promising scaling solution is the Lightning Network: an open source, decentralized payment system. You can think of Lightning as digital cash to Bitcoin's digital gold. At the moment, the Bitcoin network can only support around 7 transactions per second. With Lightning, there is no technical upper barrier to how many transactions per second we can do with Bitcoin. This technology is still nascent, but arguably essential for Bitcoin to become usable by hundreds of millions of people in a non-custodial way. If we want to scale Bitcoin to the masses, without them having to trust a third party, Lightning seems to be the way forward. Companies as big as Square seem to agree: there, CEO Jack Dorsey has created Square Crypto, a research group that is building a Lightning toolkit for developers. This kind of scientific exploration is important for other companies and universities to emulate and expand on in the coming years.

A fifth priority area is liquidity. Once the average person can acquire Bitcoin, the following step, at least for the next few decades, is to ensure that it is easy for them to convert their BTC to local fiat currency when necessary. A world in which we pay for everything or even most things with a Bitcoin-based system

is far away, and may never come at all. For now, people in distressed or repressed places need an ability to shave off their Bitcoin into fiat to pay for daily expenses and bills. This, thankfully, is getting a lot easier. In most major urban areas on earth, there is some mixture of Bitcoin ATMs, peer-to-peer marketplaces, Bitcoin brokers, and brick-and-mortar exchange points. Expanding Bitcoin off ramps will be key to popularizing the technology in the future. The website UsefulTulips.org does a good job of analyzing Bitcoin's growing use around the world. More initiatives like this are necessary so we can learn how and why people are using Bitcoin.

A sixth priority area, and one that might really move the needle, is minimum ID. There is a strong need for a platform like Twitter that still allows some level of pseudonymity to adopt a Bitcoin-based payment system that reveals an absolute minimum about the user. If avatars online are to exist in the future, we must be able to operate them securely without fear of our real life identities being leaked. So attaching a bank account or a credit card with our full ID stack on it to our social media account won't do us any good. We'll need to use digital assets that don't require Know Your Customer (KYC) or Anti Money Laundering (AML) compliance. Lightning seems well placed to serve this function. The less we reveal about ourselves in our transactions, the harder it is for Big Brother or surveillance capitalism to grow. There could very well be a future, even a near future, in which an individual can walk into a coffee shop, buy something online, send money to a friend, and make a donation to a cause all while giving up just a minimum amount of information about themselves.

If developers and investors can focus on these six areas; if consumer protection advocates can lobby for the space for them to grow in our societies; and if users can more easily engage with Bitcoin, then we are well on our way to a more private and free world.

In conclusion, let's revisit the impact Bitcoin could have on human rights communities if its technology ecosystem grows along the lines we've described.

First, consider independent journalists and NGOs operating in authoritarian environments who need to preserve financial independence. With Bitcoin, they are able to collect funds from around the world in a way that is difficult to surveil and impossible to stop. Then they can convert it into local fiat currency on an as-needed basis to pay for program expenses. This is already relevant in places like Russia and Hong Kong where the bank accounts of activists are frozen.

Second, consider the billions of refugees and stateless individuals, who cannot currently access the banking system. Today, you need to prove your identity to open a bank account or use any of the apps attached to the legacy

financial system. With Bitcoin, you don't need an ID or a passport. You just need, practically speaking, a smartphone and access to the internet. This is a great equalizer, giving anyone, no matter their class, education, background, or ethnicity, equality of opportunity.

Third, consider individuals who are dealing with high or hyperinflation. Many countries have been hit lately with double digit inflation, and some have suffered through hyperinflation. Ask any Argentine, Syrian, Turk, Iranian, Zimbabwean, or Venezuelan and they will tell you how rampant inflation can crush economies and vaporize the savings of the lower and middle class. With Bitcoin, anyone has access to a savings technology that requires no permission from a company, and cannot be devalued by a government that decides to print more money.

Fourth, consider the growing number of people who are falling under intense daily financial surveillance. Especially in China, hundreds of millions of citizens are increasingly being watched not just by hundreds of millions of surveillance cameras but also through their texts, calls, and social behavior. Transactions are a big part of this trend and will continue to be increasingly surveilled. Bitcoin provides the infrastructure for a parallel economy, one in which our financial transactions are not natively linked to our identities.

Fifth and finally, consider those who are victims of sanctions. The tragic fact is, individuals who live in sanctioned countries like North Korea and Iran didn't vote for their governments in free and fair elections and shouldn't reasonably be held responsible for their dictator's crimes. Through Bitcoin today, individuals inside Iran, for example, can earn income from abroad by working on open source software projects, or can receive money from their family abroad to pay for basic expenses or medical bills at home.

If the Bitcoin project falters or slows, then there won't be much hope for the billions of people in these situations around the world, especially as cash fades. Private payments will be practically impossible. All daily transactions will become increasing points of surveillance and control. The monetary substrate itself will be watching you, and controlling you—and you won't be able to do anything about it.

One more thing to keep in mind: the Davos elite who currently run the world are threatened by a technology that separates money from state and provides permissionless access to a premium savings technology. They are used to running things and want the game to be rigged. They want there to be obstacles and barriers to entry. Bitcoin will frustrate them because anyone can access it and use it, no matter who they are. In the progression of the global banking elite first ignoring Bitcoin, then laughing at Bitcoin, then fighting Bitcoin, and then giving up, we are nearing the end of the laughing phase. A big battle is on the horizon.

The good news is, there is excellent momentum for Bitcoin in the areas we've covered, and there is growing global adoption. Despite the obstacles, the path to freedom is clear.

In an age of increasing fear over how corporate and state technology will steal our rights and freedoms, we can be grateful to Satoshi that we won't ever have to live in a World Without Bitcoin.

Tweetstorm: The Pump

By Brendan Bernstein

Posted February 11, 2020

Most people think BTC is going to pump from a Zimbabwe esque hyperinflation.

But the opposite is going to happen

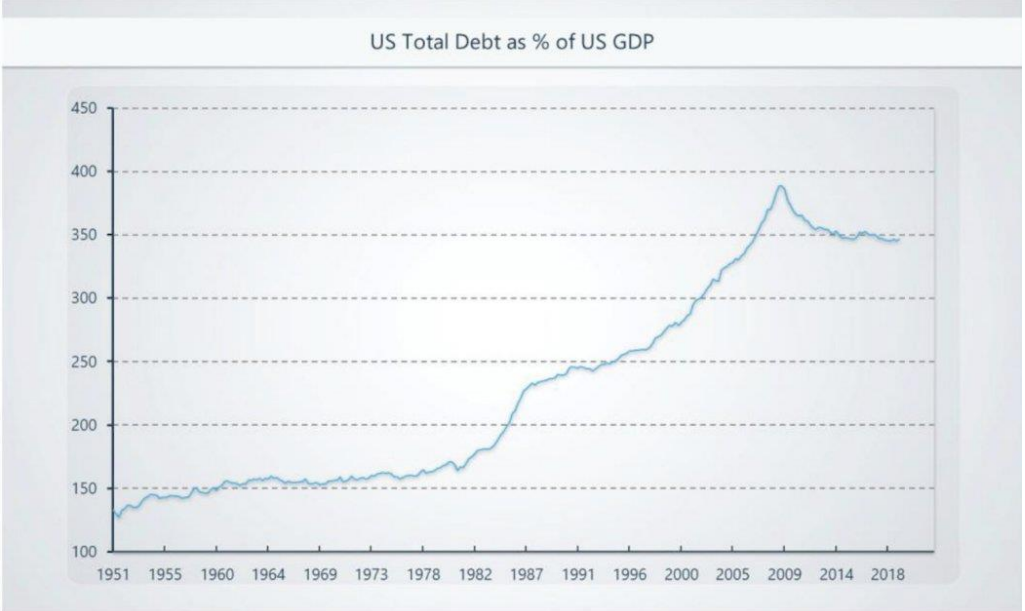
We're on the precipice of a deflationary crisis....and this is why BTC will pump

Here's why:

Debt has peaked and is beginning to turn.

As people deleverage, this suppresses inflation bc income goes to debt servicing instead of goods & services.

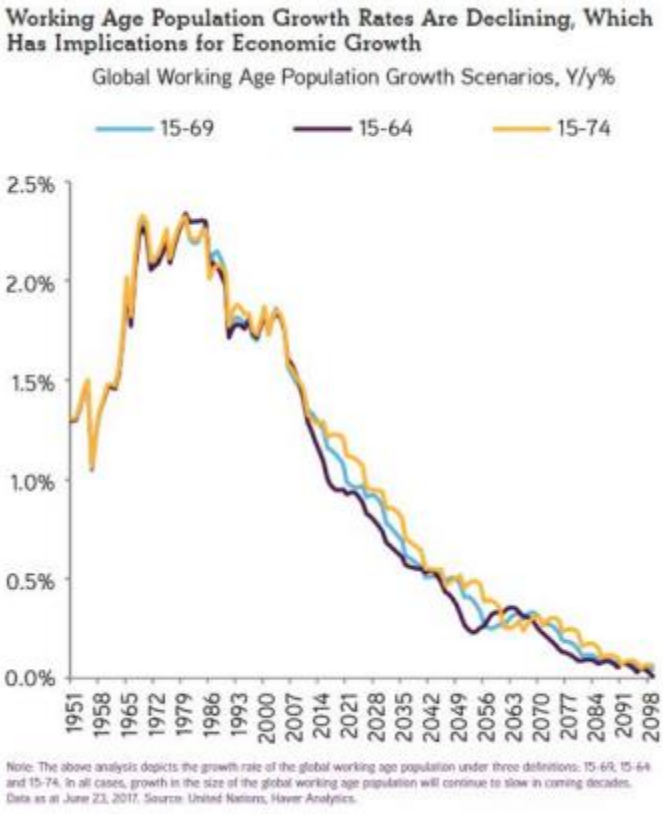
This is why the fed can pump $4tn into the economy and CPI doesn't budge.



Growth is also a product of demographics. Boomers are the largest demographic and their retirement is peaking in the next 5 years

Over the last 100 years, labor force grew 5x. Over the next 100, it will only grow 20%.

There will be less and less money to spend.



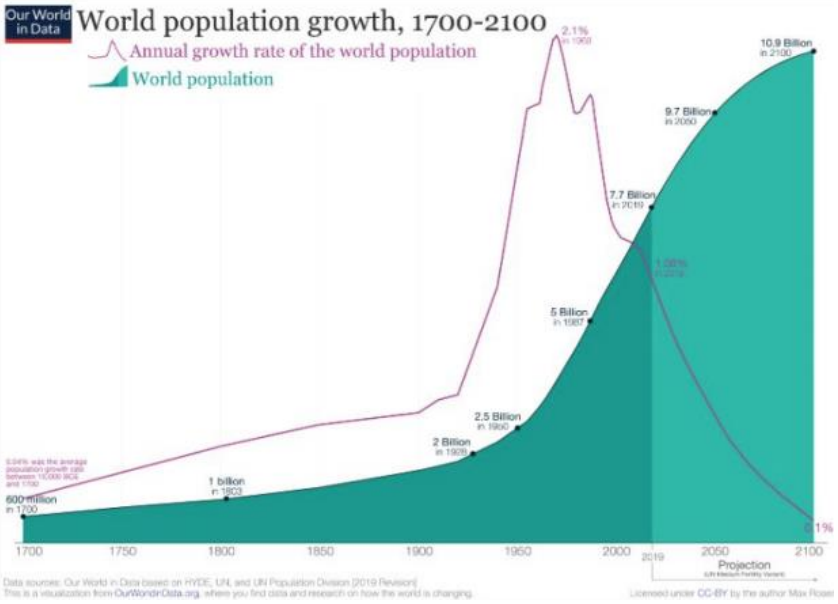
Additionally, GDP growth is directly tied to population growth.

Population growth peaked in the 1960s at 2.1% and will hit 0% in the next 100 years.

This massive tailwind is shifting to a headwind.

Population growth increases demand for goods, inflation and the stock market.

The success of our consumerist capitalist society may just be a product of labor and exponential population growth.



This is also why a $tn tax cut and $300m in fiscal spend led to almost no growth.

Boomers, which were a massive spending and stock market growth tailwind, are going to turn into a headwind this year.

The RMD law requires that they take cash out of the stock market.

As a result, up to $10tn in assets will be subject to mandatory withdrawals

Converging Elements

While the actual valuation of current RMD outflows and projections of future distributions are inexact in the absence of hard data, consider the following statistics:

- The value of retirement assets for all RMD-eligible plans currently totals an estimated $16.2 trillion.
- The current population of 50-69 year olds who will reach RMD status over the next 20 years will increase by more than 27 million individuals. By 2035, the total number of retirees taking RMDs could swell to 58.7 million individuals according to census projections.
- It is estimated that more than 65% of current traditional IRA investors (and their assets) will enter into the RMD strata in the coming 20-year period.[6] If these projections are correct, up to $10 trillion in assets will be subject to mandatory withdrawals over the next two decades.
- A first-year withdrawal, based on the current IRS formula, requires a distribution of 3.65% of eligible assets. What's more, the percentage grows as the retiree ages and jumps to 5.35% for that same individual at age 80. At age 90, the mandated withdrawal percentage leaps to 8.77% of the accountholder's balance.

The problem is that we are at peak debt and the stability of our society rests on an increasing stock market and increasing growth to service that debt.

Stock market declines are a national security concern.

And the fed will be forced to plug this hole.

This great chart from @RaoulGMI shows the US labor force participation rate overlaid with the fed balance sheet.

As more people leave the work force, the fed has been plugging the gap by expanding their balance sheet.

This trend is only accelerating and based on the upcoming boomer retirements, this correlation would predict a doubling of the fed balance sheet over the near term.

Many people assume Bitcoin is going to stave off a Zimbabwe-esque hyperinflation of the USD.

But because of the demographic, population growth and debt dynamics, it's much more likely the opposite occurs.

Extremely low growth and Japanification of the world

Long adult diapers

Negative rates will be the norm in this world.

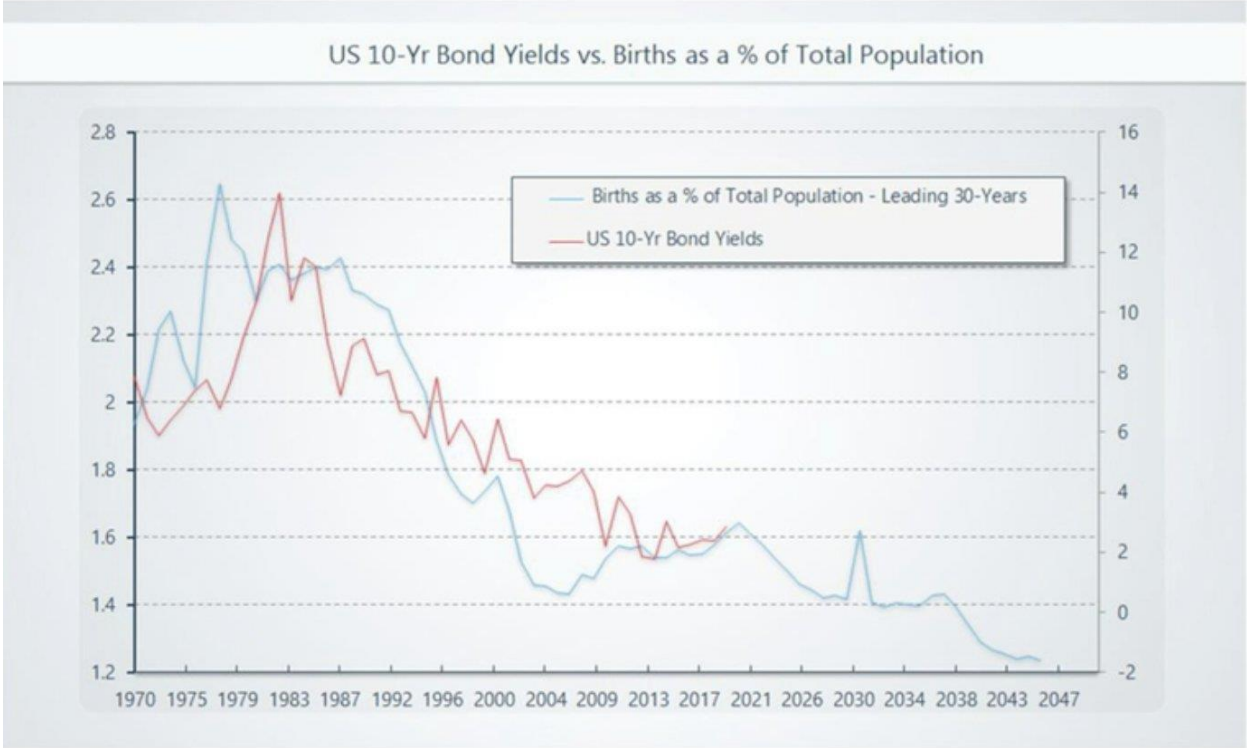
But because our system is predicated on growth, the fed is going to be forced to go to extreme measures to counter it.

It's not a question of if we get MMT, but when.

The best predictor of gold prices (and bitcoin prices too ultimately) is not the dollar or inflation...it's real yields.

The fed's hands are tied.

Over the next 50 years yields will be absolutely crushed.

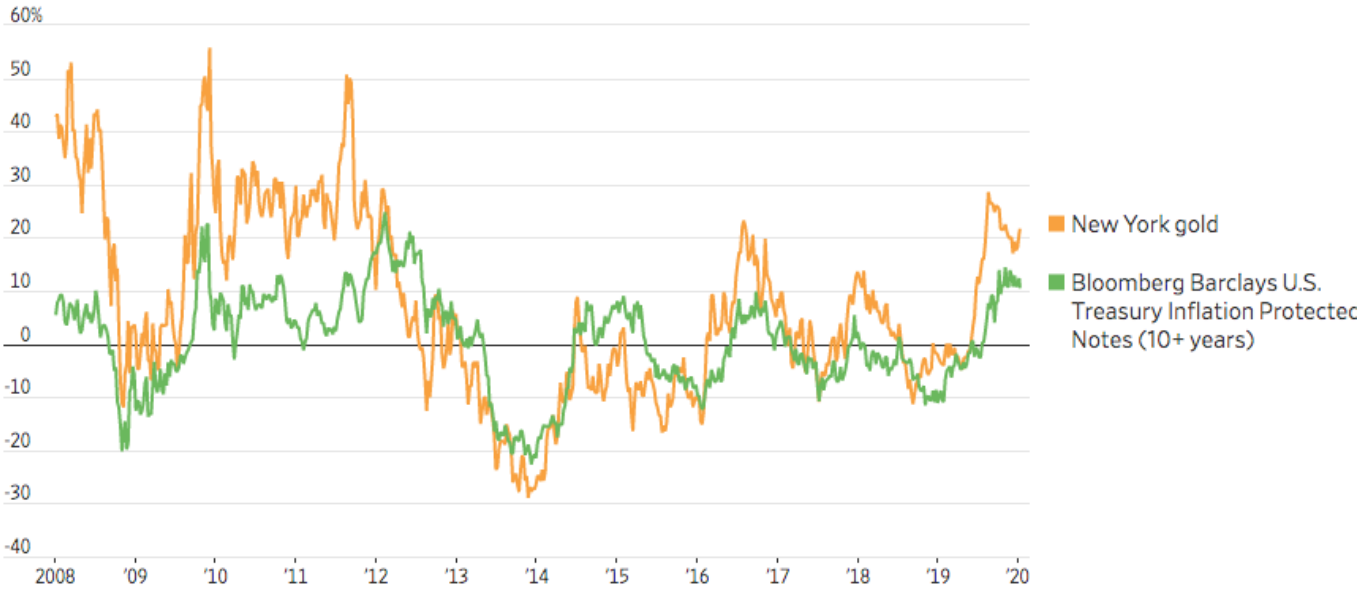


And there could be nothing better for scarce assets like bitcoin and gold as the Fed is forced to ramp up printing to attempt to counteract these trends.

Shine On

Gold tends to move in the same direction as inflation-linked bond prices, and in the opposite direction to their yields.

12-month change in price



Source: FactSet

FIGURE 1: GOLD PRICES ARE HEAVILY INFLUENCED BY 10-YEAR REAL YIELDS

Figure 1 shows the logarithm of the inflation-adjusted price of gold and the 10-year real yield from the Treasury Inflation-Protected Securities (TIPS) market. Using the logarithm makes the size of a given percent change constant over time (gold prices increased from $540 to more than $1,800 over this period, so a $100 move in 2006 is not the same percentage change as a $100 move in 2011). We also

There's a black hole in the pension system. Inequality is ramping up. Geopolitical instability is festering.

The fed is going to be forced to prop it up all up and anesthetize everything to death.

Sayonarah to any fiat purchasing power. Long scarce assets.

Over 75% of Bitcoin's On-Chain Volume Doesn't Change Hands

By Rafael Schultze-Kraft

Posted February 13, 2020

Assessing Bitcoin's True Transfer Volume

This article was originally published on Glassnode Insights.

Even though blockchain data is publicly accessible, it is a non–trivial challenge to make sense of it in a meaningful way.

On–chain data is without a doubt highly valuable — but in its raw form it's just not good enough.

It contains a substantial amount of noise, and careful preprocessing and contextualisation is required in order to distil useful information from it.

Consider **on–chain transaction volume**: *Figure 1* shows Bitcoin's raw daily on–chain transaction volume (USD value) for 2019.

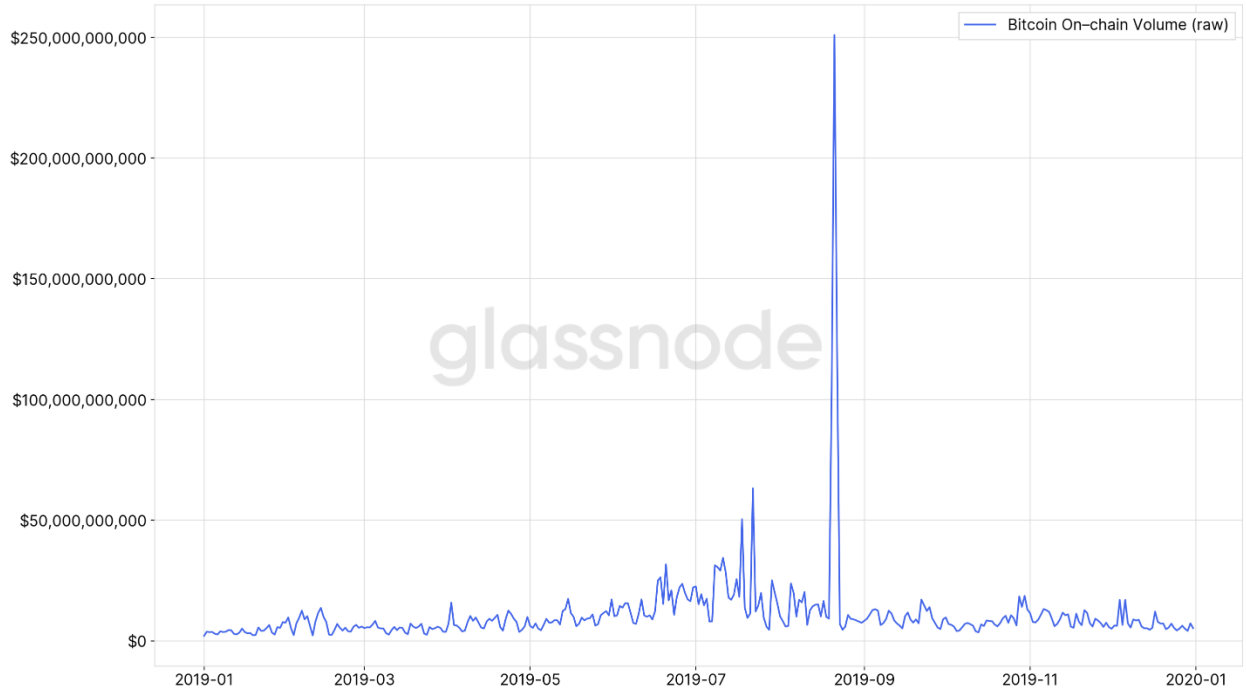


Figure 1 — Raw Bitcoin daily on–chain transaction volume for 2019.

On August 21st an enormous spike occurred, leading to a recorded on–chain volume of over $250 billion USD in a single day.

Without context, this might seem like a significant event.

However, this volume was simply caused by Bitcoin "change", associated to a crypto exchange creating new cold wallets and reshuffling their funds internally — no actual Bitcoins were transferred between different participants in the network.

Therefore, if we are interested in assessing the **value of bitcoin that is actually being transferred across different holders**, proper processing and sophisticated methods need to be applied to the raw blockchain data.

Change–Adjusted Volume

Adjusting for (obvious) change is a commonly applied heuristic to obtain a more accurate measure for on–chain volume.

This adjustment is applicable to transactions in which the sending address is present in both the inputs and the outputs of the transaction, i.e. a transaction output returns Satoshis back to an address of the sender (see _Figure 2 _for an example).

Figure 2 — Example of obvious change. An address with a balance of ~119,646 BTC sends 1,300 BTC to another address. The remaining amount is returned to the sending address. Source: blockchain.com

The change is considered "obvious" because the sender is re–using an existing sending address within the same transaction to receive the bitcoin change in return.

_Figure 3 _shows the daily change–adjusted on–chain volume for 2019.

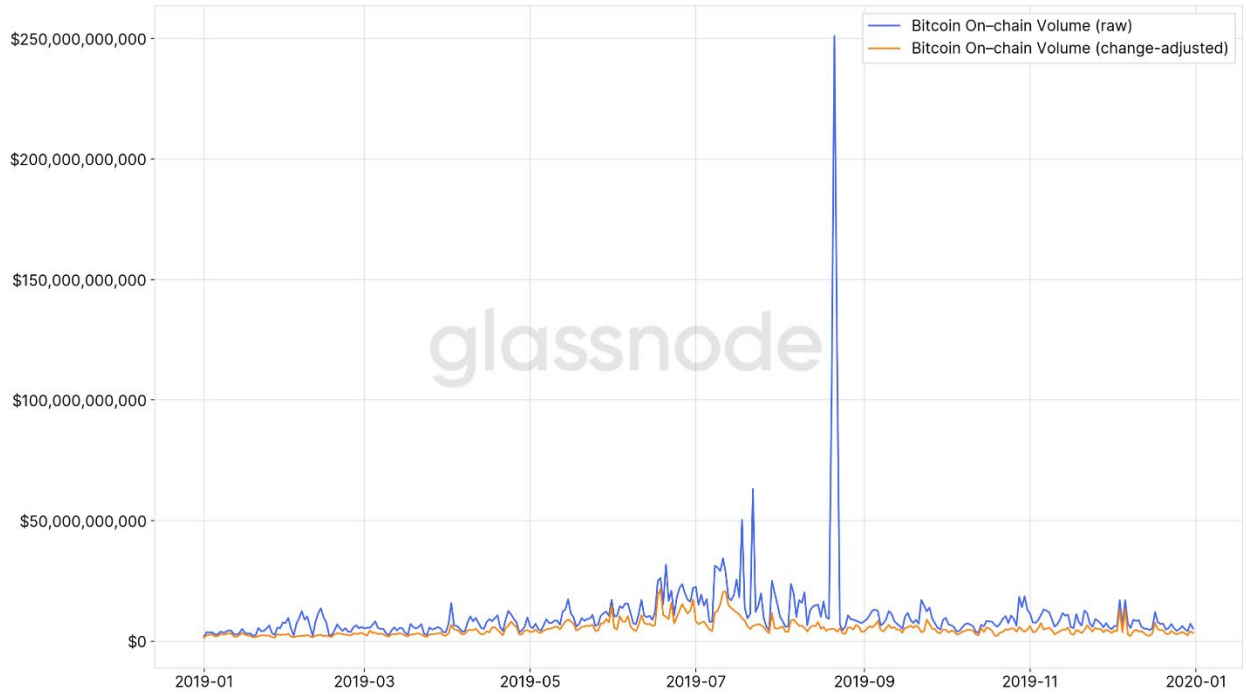


Figure 3 — Raw and change–adjusted Bitcoin daily on–chain transaction volume for 2019.

Note how the volume spike vanishes, and in addition change–adjusted volume is consistently lower compared to the raw volume.

In fact, within the denoted time period above, the daily **change–adjusted volume is, on average, 43% lower**.

A live chart comparing raw and change–adjusted Bitcoin volume can be found on Glassnode Studio **here**.

Beyond Change: Adjusting by Entities

The problem with the above heuristic is that it doesn't go far enough. There are other cases in which on–chain bitcoin volume does not represent actual transfer of Bitcoin between different holders.

For one, a single user can send bitcoin between different addresses that he/she controls. Furthermore, many wallets nowadays send change back to the spender using newly created addresses instead of re–using an existing one.

At Glassnode we use more advanced techniques and heuristics in order to estimate an upper bound for the "true" on–chain volume of Bitcoin — **volume that actually changes hands.**

To do so, we employ what we coin **entity–adjustment** and refine this methodology by accounting for so–called **relay addresses** as well.

Entity–Adjustment

In our previous article we introduced the concept of "entities" in the Bitcoin network: Clusters of addresses that are controlled by the same entity.

Entity–adjustment therefore makes use of this knowledge and discards volume moved between addresses that belong to the same entity cluster ("in–house volume"). This is volume that does not represent value transferred between distinct users in the network. Because one address belongs to a single entity, this adjustment entails, by definition, the aforementioned change–adjustment as well. (***Note: We ignore multisig addresses in this analysis).***

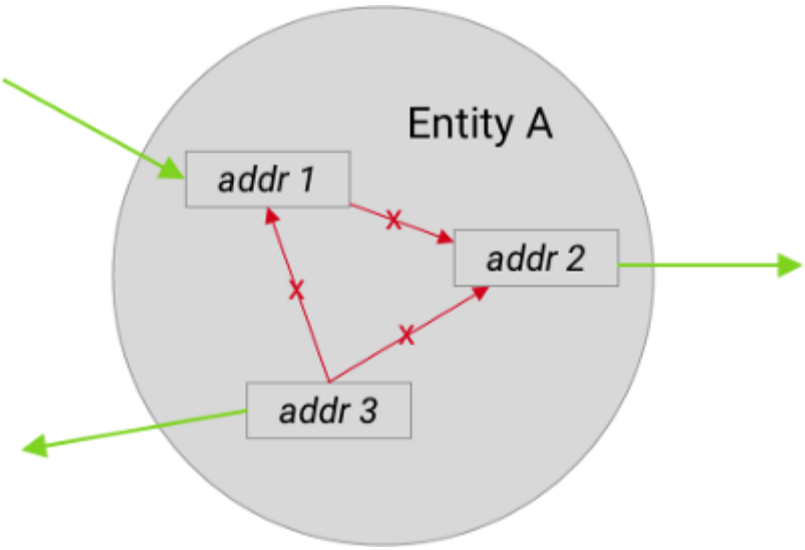


Figure 4 — Schematic example of entity-adjusted on-chain volume: Only volume that is moved into or out of an entity is counted (green). Transaction volume within addresses of the same entity ("in-house" transactions) are discarded (red).

Consider the example transaction in *Figure 2* above: While it contains obvious change, our algorithms actually detect that all input and output addresses are controlled by the same entity — therefore the whole transaction does not contribute to the true BTC transfer volume ***at all***.

Moreover, this implies that this transaction is discarded in the computation of entity–adjusted transaction **counts**, since it is a transaction that only transfers BTC internally.

Relay–Adjustment

In addition to adjusting for entities, we take into account so–called "relay addresses" as well. Relay addresses are addresses whose sole purpose is to forward (relay) funds to a subsequent address. Hence, the volume of relay addresses is usually double–counted: once moving into and once moving out of the relay address.

Through the identification of addresses with this behaviour, we are able to remove this added of noise in volume aggregates. To do so, we discard all outputs that are spent by relay addresses.

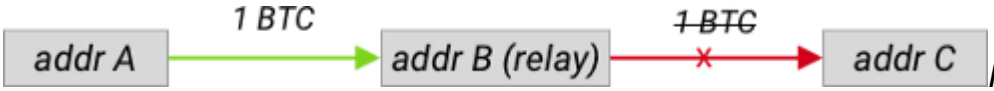


Figure 5 — Schematic example of relay addresses: In order to prevent double-counting on-chain volume, only transactions going into the relay addresses are considered. Outputs spent by relay addresses are discarded.

Technically, we define relay addresses as addresses whose ***mean spent output lifespan is less than 1 hour***, and whose current ***balance is zero (excluding UTXOs which were created within the last hour).***

Figures 6–8 show the difference between between our entity–adjusted volume (incl. relay–adjustment), change–adjusted volume, and raw volume for the the years 2016, 2017–2018, and 2019, respectively.

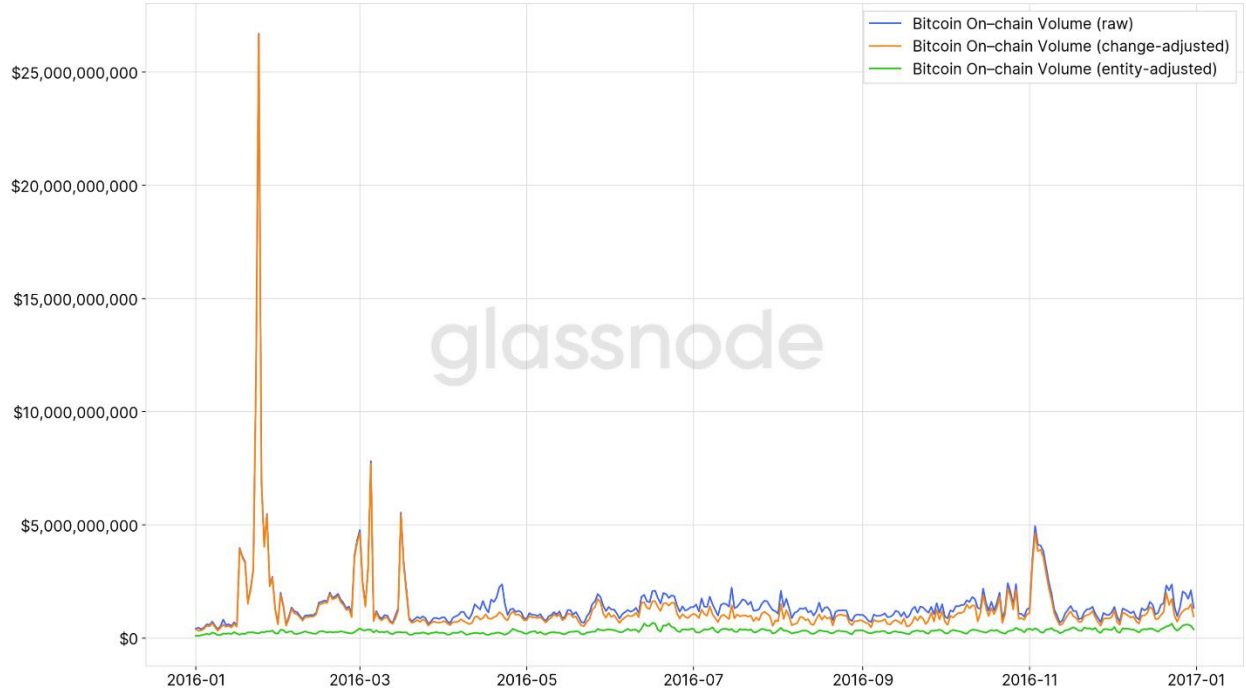


Figure 6 — Daily Bitcoin on–chain transaction volume for 2016.

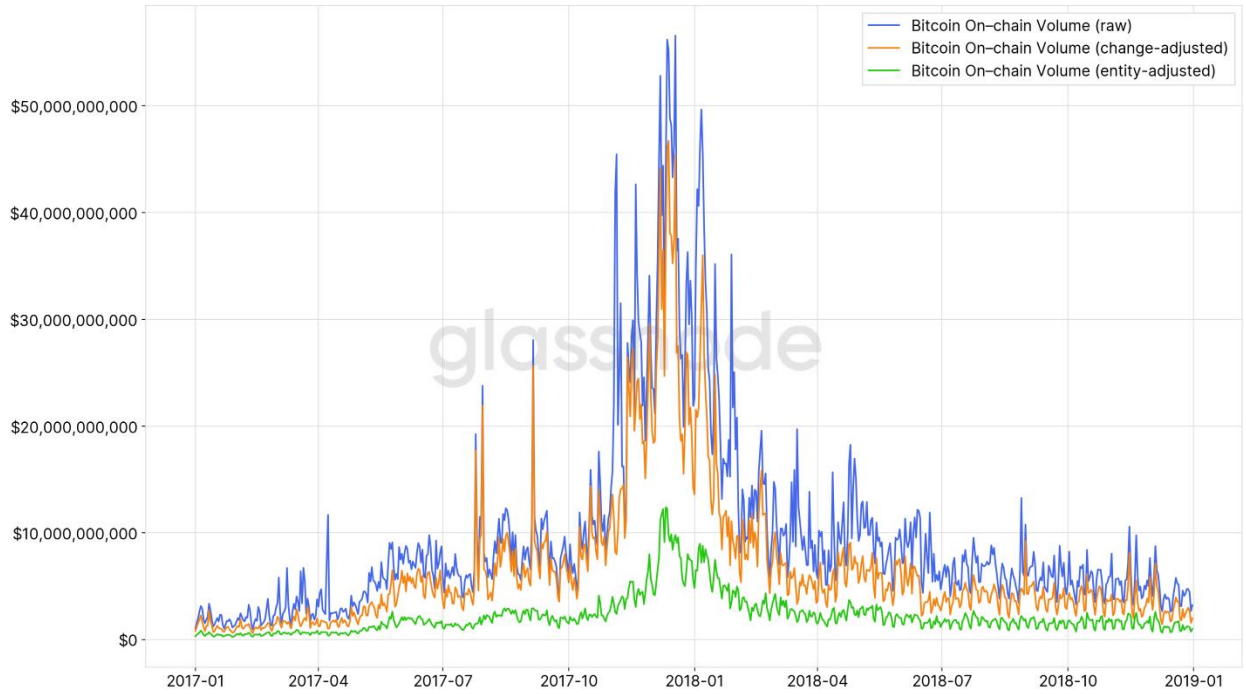


Figure 7— Daily Bitcoin on–chain transaction volume for 2017–2018.

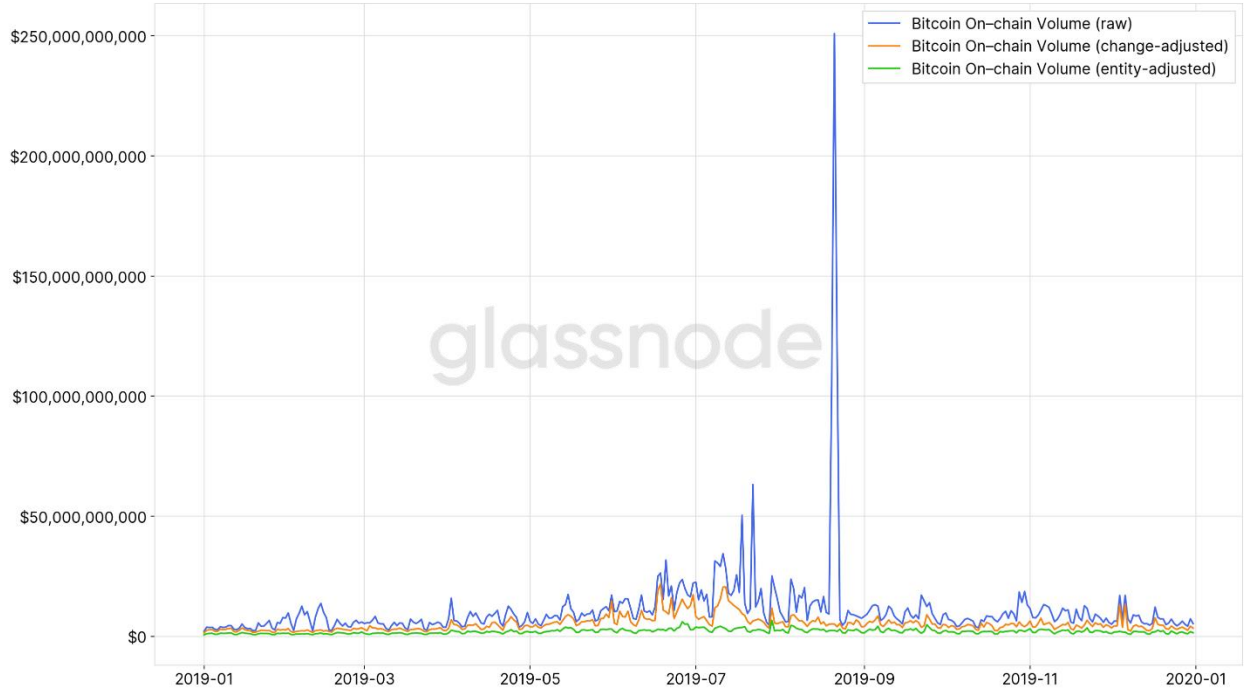


Figure 8— Daily Bitcoin on–chain transaction volume for 2019.

The results speak for themselves, and the differences are compelling.

The 2016 data illustrates the removal of significant volume spikes that are not accounted for by change–adjusted volume only. Similarly, volume during the

bull market in 2017 shows substantial discrepancies (5x) between entity–adjusted and raw/change–adjusted Bitcoin volume.

Over the period from 2016–2019 the daily on–chain transaction volume using our entity–adjusted methodology has been

- **75.5%** lower than the raw volume and
- **63%** lower than change–adjusted volume.

This means that less than 25% of Bitcoin volume that is recorded on–chain represents actual value transfers between network participants.

Our entity–adjusted metrics show that the true Bitcoin on–chain volume is on average only 25% of the raw volume recorded on the blockchain.

For a complete picture, *Figure 9* shows the ratio between raw volume and entity–adjusted (as well as change–adjusted) over time. The entity–adjusted ratio has been relatively stable fluctuating around 0.25 since 2016.

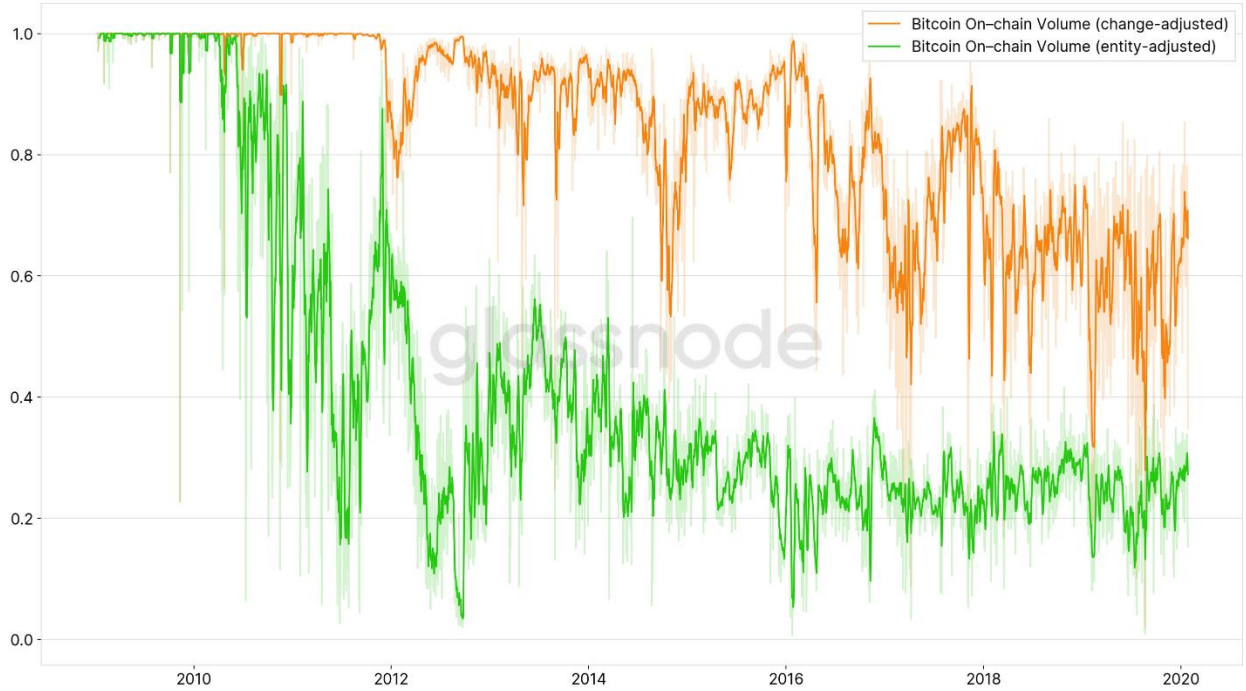


Figure 9 — Ratio of entity-adjusted/change-adjusted and raw Bitcoin on-chain volume.

Figure 10 depicts the monthly difference between raw and entity–adjusted (as well as change–adjusted) volume in USD. It shows that on a monthly basis our entity–adjusted volume is up to a compelling **$875 billion** and **$629 billion** lower compared to the raw volume and the change–adjusted volume, respectively.

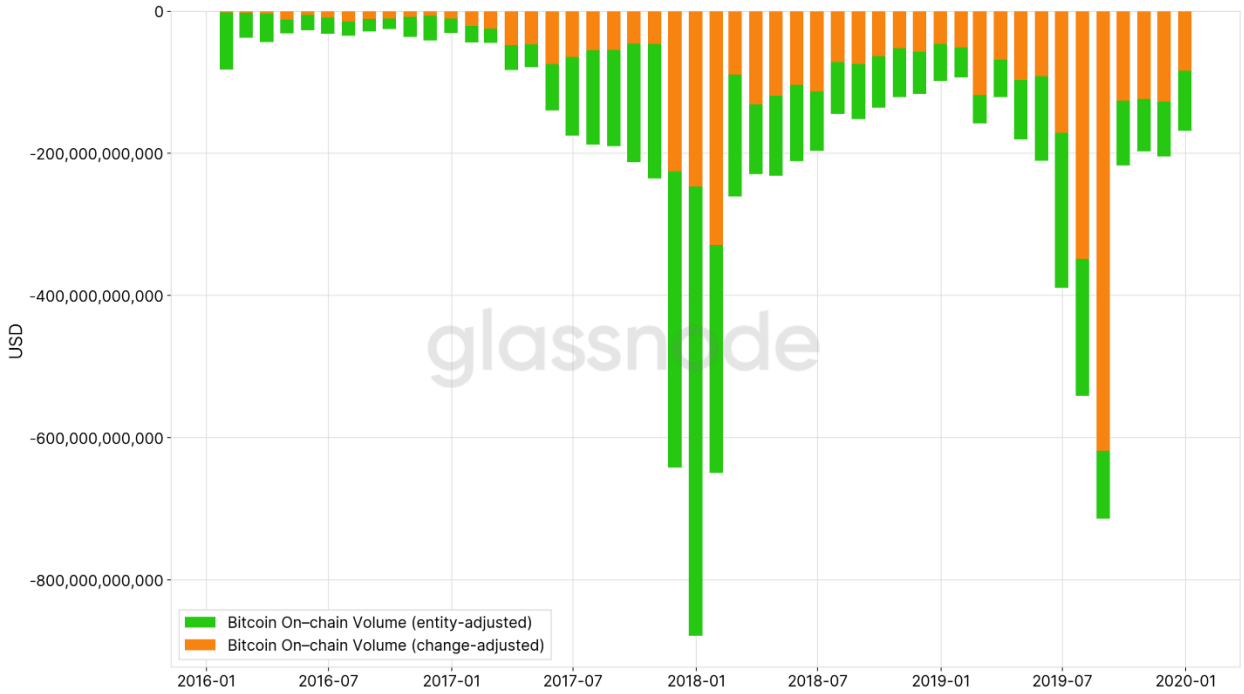


Figure 10 — Monthly difference between raw and entity-adjusted/change-adjusted volume in USD.

Conclusion

The data and analyses presented here are in no way intended to lessen Bitcoin's value proposition and should not be interpreted as such.

The purpose of this work is merely to signify that advanced methods are required to meaningfully make sense of on–chain data. In order to accurately understand the underlying state of the Bitcoin network and its events it is essential to contextualise and scrutinize this data properly.

Note the in the present work we exclusively refer to bitcoin moved on the blockchain. We don't account for BTC that is bought or sold on exchanges. Technically, on a network level, those bitcoin are still controlled by the same entity — the exchange itself.

In Bitcoin's economy the implications of moving funds within the same entity, and actually transferring ownership of bitcoin (and therefore value) across network participants, are very different — they represent very different things in terms of economic activity.

Any investor, trader, and researcher aiming to properly understand value and wealth transfers in Bitcoin's economy should be undoubtedly making use of these fundamental differences drawn from on–chain volume.

All metrics presented in this work are live on Glassnode Studio as of today:

- **Entity–adjusted Volume (Total)**
- **Entity–adjusted Volume (Mean)**
- **Entity–adjusted Volume (Median)**
- **Entity–adjusted Transaction Count**

For change–adjusted volume visit:

- **Change–adjusted Volume (Total)**
- **Change–adjusted Volume (Mean)**
- **Change–adjusted Volume (Median)**

glassnode insights

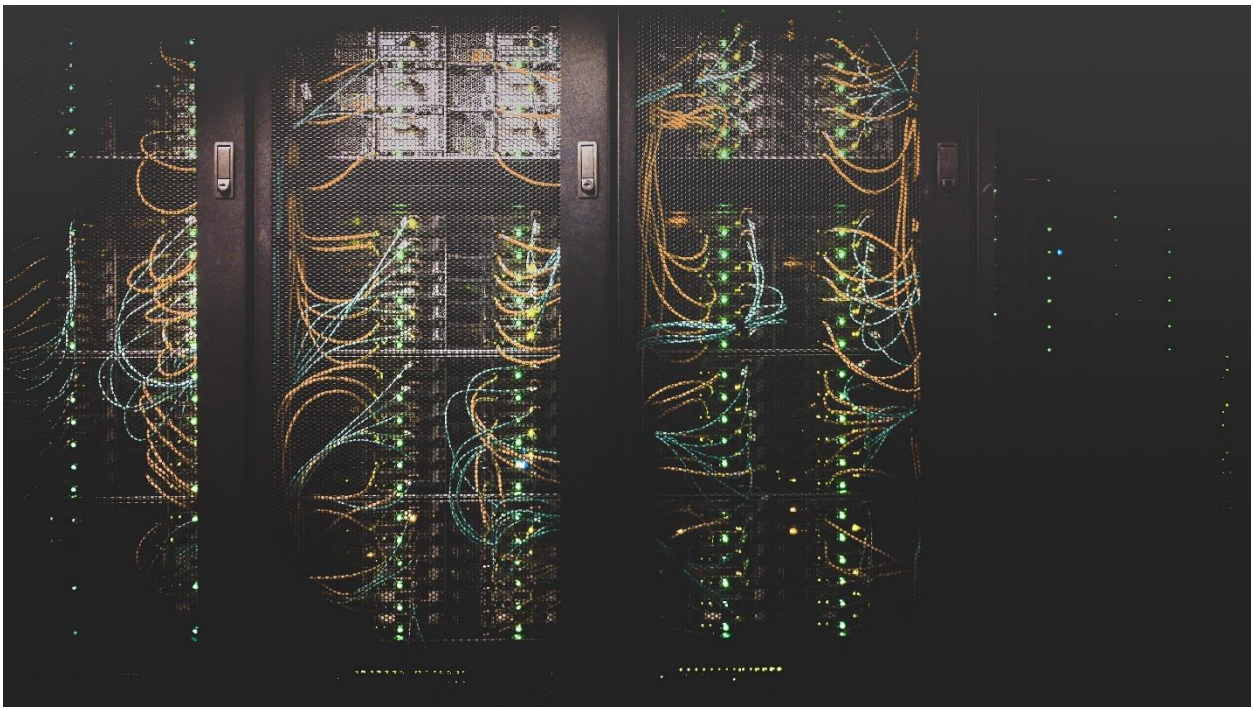
- Follow us and reach out on Twitter
- For on–chain metrics and activity graphs, visit Glassnode Studio
- For automated alerts on core on–chain metrics and activity on exchanges, visit our Glassnode Alerts Twitter

Disclaimer: This report does not provide any investment advice. All data is provided for information purposes only. No investment decision shall be based on the information provided here and you are solely responsible for your own investment decisions.

The Nature of Bitcoin

By Zane Pocock from Knox Custody

Posted February 13, 2020



(Photo by Taylor Vick on Unsplash

With the notion of Bitcoin as a security dispelled, including by American regulators themselves, the other common ways people attempt to wedge Bitcoin into legacy frameworks — and regulation — is as either a commodity, property, or the ultimate goal: money.

But Bitcoin is at odds with these concepts at a fundamental level. Because "bitcoins" don't exist.

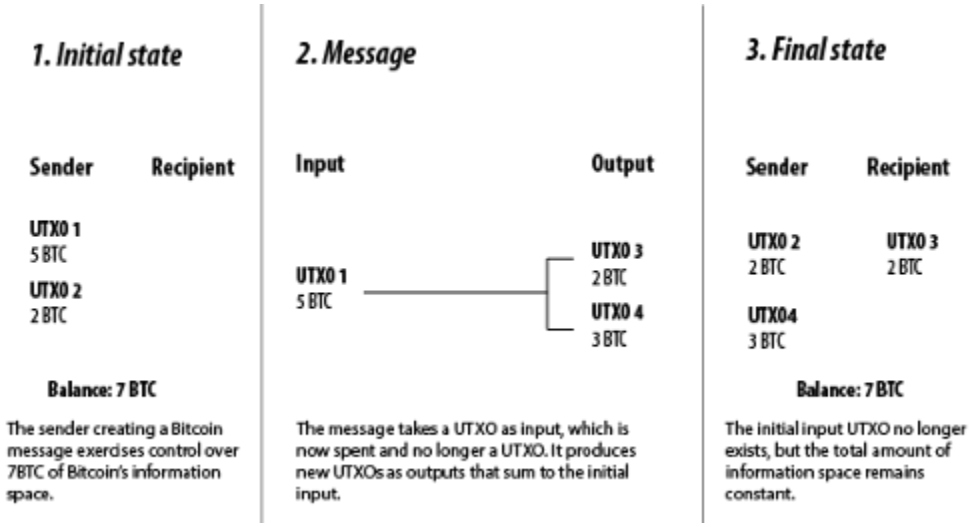
As Beautyon has popularized in his case that Bitcoin is speech protected by the first amendment, the definition of Bitcoin can be simplified to a distributed internet protocol that relays text messages between voluntary/free participants.

That's all Bitcoin is — a means of communication.

The unique value proposition of the Bitcoin communication protocol is that these messages can be used by participants to communicate an interpretation of *value*. How this works is through a mechanism called the

"unspent transaction output" (UTXO). UTXOs can be a little difficult to understand, but Investopedia describes it well:

"UTXO stands for the unspent output from bitcoin transactions. Each bitcoin transaction begins with coins used to balance the ledger. UTXOs are processed continuously and are responsible for beginning and ending each transaction. Confirmation of transaction results in the removal of spent coins from the UTXO database. But a record of the spent coins still exists on the ledger."



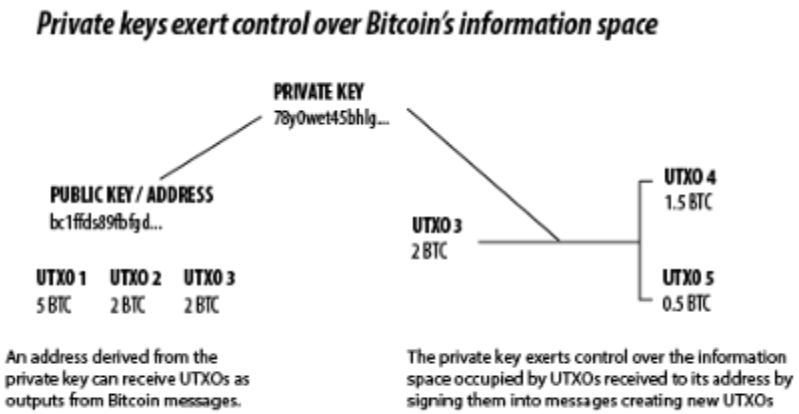
Bitcoin is a means of communication

It's these UTXOs that are measured in a unit called "bitcoin", but this is more akin to measuring how space is used on a hard drive than bars of gold in a vault. UTXOs are just the occupants of Bitcoin's information space.

One of Bitcoin's utilities is popularly described as "digital gold" because this information space comes in a limited quantity. The network-wide UTXO balance will only add up to a certain scarce amount with the current outstanding supply summing to 18.2M BTC out of the 21M BTC hard cap it will reach sometime next century. But this analogy — Bitcoin as digital gold — is not the actual definition of Bitcoin, only one subjective interpretation.

What controls these UTXOs?

Bitcoin private keys are another type of Bitcoin information. Through cryptographic processes outside the scope of this article, private keys can derive a corresponding public key that acts as an address for receiving UTXOs. The private key then exercises control over all the UTXOs it has received. UTXOs are transferred as inputs in messages when they are cryptographically signed by the private key with authority to do so.



Private keys exert control over Bitcoin's information space

Energy, Value and Settlement Assurances

Another viewpoint commonly employed to explain Bitcoin is to say that it is "backed by energy".

The reason why is that roughly every ten minutes, blocks of Bitcoin "messages" are confirmed by competing computers ("miners") employing a huge amount of energy to meet the rules set out by the protocol. These ten-minute blocks are Bitcoin's bandwidth. Only a certain amount of Bitcoin "messages" can be transmitted in each block, called the block-weight. Taken together, this process of adding message blocks to increment the "block height" by miners is called proof-of-work, and to simplify it gives the Bitcoin network some important features:

- The rules the miners follow to update the distributed network state require that UTXOs must be unspent (as the name suggests). This solves the so-called "double-spend" problem in the digital world where information had previously always been non-scarce. What value would a UTXO accrue if a user could reuse it? It means that absolute mathematical scarcity now exists for the first time, a discovery that can't be achieved again.
- These value-transfer messages are then effectively buried under each new block of messages: to undo them, an attacker would need to prove the same amount of work to the protocol as has been applied to each successive block — and from all the competing computers, not just the successful ones. This is a proxy for energy and means that expended energy is a key requirement to ensure transaction finality, or settlement assurances, as Nic Carter writes. It is a security feature that to attack Bitcoin, inordinate amounts of energy must be employed.

- The competition between miners, resulting in a distributed ledger that they all contribute to, means that this global value-transfer network does not rely on any trusted third party. Clearance and settlement happen according to strict rules on the Bitcoin protocol that tens of thousands of independent users verify for themselves.

Because expended energy is so core to Bitcoin's security and viability, the concept that "Bitcoin is backed by energy" has emerged as a useful concept for understanding why this communication protocol works at all. Taken to its literal conclusion, this line of thought has led some to argue that this energy creates Bitcoin's value and that Bitcoin is therefore a commodity — captured energy.

Rather, it is the energy expended for security in combination with Bitcoin's use of information space that is why the network accrues value. Put another way, if the information space occupied by Bitcoin UTXOs could be classified as a commodity, then space rented on Amazon's AWS servers would also be a commodity. Like the Bitcoin network, AWS relies on expending a lot of energy to function, and the computing resources rented by businesses and individuals represent information space in the virtual world. But it would be absurd to classify AWS as a commodity, and so it is with Bitcoin.

Indeed, it's the separation of value from commodities that makes the Bitcoin communication protocol so uniquely valuable. As Conner Brown has written, Bitcoin has no intrinsic value as a commodity — an observation often used as a criticism — but that is a feature, not a bug. A commodity-based value transfer system, such as the gold standard, not only finds its value subject to the market fluctuations caused by changes in supply and industrial demand, but it also inflates the price of the underlying commodity by increasing its demand. This monetary premium means that a commodity like gold is much more expensive than it otherwise would be, and this distortion in the price signal hampers its use in goods such as cheaper electronics.

The Most Tradable Information

Without needing to grasp for financial definitions, commerce enabled by the Bitcoin value-transfer protocol will still be commercial activity. If the distributed Bitcoin ledger helps to conduct commercial activity between a shop and a consumer, that shop is still going to file a tax return with profit based on the fiat value of goods sold.

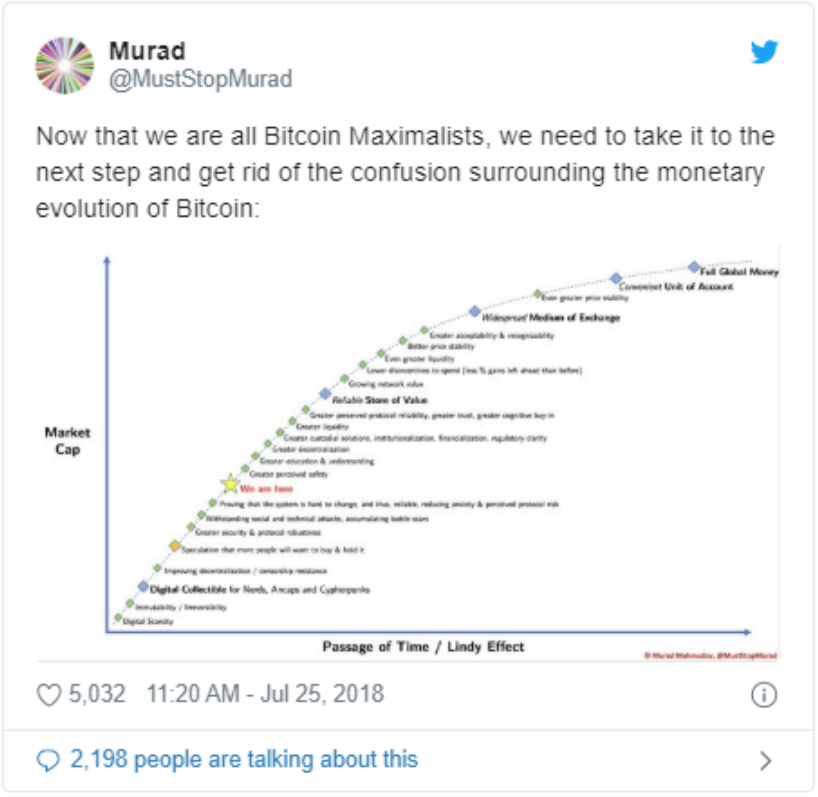
Monetary systems are savings technologies that ultimately serve to transfer value in time and space, a tool for the farmer selling his year's output in Fall to be able to purchase new shoes six months later when he has nothing to sell. Having lacked a logical system to keep track of everyone's market contributions until now, this value transfer role has traditionally fallen to the

economy's "most tradable good" — typically something exhibiting beneficial properties such as durability, portability, divisibility, and hardness (hard to produce more of it and debase it).

Monetary theorists such as Carl Menger, Nick Szabo and Saifedean Ammous argue that the emergence of a new money has historically gone through various stages. Starting as either a collectible (such as shells or family heirlooms) or a commodity (flint blades or gold), a monetary good first accrues value in the subjective eyes of an increasing number of people. Given enough time, this accrued value gains permanence, allowing the good to successively function as a store of value then as a medium of exchange when it reaches a certain level of liquidity and price equilibrium.

Similarly, Bitcoin's communication protocol and scarce information space have piqued the interest of human minds such that their uses and perceptions of it have gone through evolving narratives and led many to collect the scarcity of the information space into UTXOs only they have the authority to spend. These narratives have ranged from a crypto-anarchist collectible and "private" darknet currency, to current interpretations such as "digital gold". But just as price is an interpretation of value, these human narratives — Bitcoin as gold, Bitcoin as commodity — are an interpretation of the fundamental nature of Bitcoin: information.

If something becomes the most tradable good, it can function as money. Bitcoin is text, but its properties might allow it to fulfill a monetary role for those demanding scarce information space in the form of UTXOs. We can't say exactly where Bitcoin might be on its way to being used as a monetary system — that's for each individual market participant to decide for themselves — but early adopters are using it in that role already. With Bitcoin's help, the economy might just become a little more like entering a global barter system — a ledger system to keep track of everyone's



market contributions. Rather than being the world's most tradable good, Bitcoin is the world's most tradable information.

So, what of the other aspects of financialization? One of Trace Mayer's seven anticipated network effects of Bitcoin, it is becoming apparent that because Bitcoin's information space has accrued value, it can be used as the base value of financial instruments built around it. Control of UTXOs is being transferred as collateral against lines of credit, and Bitcoin key storage providers like KNØX are attaining insurance policies for the fiat value of the information space they guard. Even futures markets are being built, enabling participants to hedge and bet on fluctuations in the accrued value and energy costs of the network. These instruments — insurance, credit, futures — appear to be financial products. But again, the way the communication protocol is used does not define Bitcoin. An orange is an orange, but that doesn't stop the market trading on its future value from dealing in derivatives to hedge risk against orange production rate fluctuations.

Similarly, the properties of Bitcoin's communication protocol present opportunities to natively automate tasks with parallels to traditional financial services, but that doesn't make Bitcoin a financial service. For example, Bitcoin allows for unique audit solutions without the use of a third party audit. As an open communication protocol, the value transferred in each message is visible to all participants, meaning that scripts can be written to prove that a participant possesses the keys exerting control over particular UTXOs. This idea — that a custodian can demonstrate "proof of reserves" — is yet to gain wide adoption, but it has drawn much anticipation and demonstrates the power arising from Bitcoin's nature as a pure communication protocol.

Because Bitcoin is text, it fundamentally sits outside of existing financial definitions and regulations. But that doesn't preclude its information space from exhibiting monetary characteristics. In fact, it's in part because of all of this that Bitcoin _is _so valuable. And things that are valuable need to be protected.

How to Keep a Secret

At the protocol level, the nature of Bitcoin's information space means that private keys function like a digital bearer instrument: there is no inherent difference between possession, control and ownership.

Remember there are no bitcoins ***per se***; there are private keys that permit spending UTXOs via signed messages on the network. Bitcoin private keys are also information. You can write them down, speak them, print them, memorize them in your head. Thousands of people can hold the exact same key; if you have Andreas Antonopoulos' ***Mastering Bitcoin*** on your shelf then you share several Bitcoin private keys printed in its pages with all the other

thousands of people who have access to it. By US constitutional law, this means that creating, spending, or otherwise using Bitcoin private keys constitutes speech protected by the first amendment. But unlike the scarce information space occupied by UTXOs, when it comes to Bitcoin private keys we are dealing with non-scarce information.

Obviously, since Bitcoin's information space has accrued value, it is in the best interest of those who exercise control over a portion of it to keep the private key out of others' hands. To exercise exclusive control over replicable information requires competence at protecting a secret.

If the Bitcoin carnivores will excuse a fast food analogy, this is why KFC doesn't have a patent on its 11 secret herbs and spices, information that has accrued such value it contributed to the growth of a global fried chicken empire. Rather, they have a vault at their headquarters that very select individuals can access, inside of which is the only known certified copy of the recipe. They even have their own multisignature scheme, with two companies each responsible for supplying half of the ingredients.

This demonstrates the "not your keys, not your coins (UTXOs)" meme. Possession of the secret enables the bearer to exercise control over the valuable information space; at the protocol level, possession, control and ownership can not be separated. As Daskalov, CEO of KNØX, put it, "the Bitcoin protocol is necessarily amoral, governed by an uncompromising set of rules."

This is creating demand for an optional Bitcoin key storage layer that might allow businesses to delegate possession to a trusted key storage provider while maintaining unquestionable ownership in the legal sense, and control in the technical sense. Such is the burden of holding these secrets that exercising control over private key information is more a liability than an asset. Most companies holding Bitcoin keys are required to do so out of operational necessity but would rather offload that liability from their books, as they do not monetize it.

Private key storage is more like managing a password than anything else. When a hard drive is locked by ransomware, most people without an adequate backup are likely to pony up the ransom to retrieve access to their information. This digital information is not property in the legal sense, but it's certainly valuable to the individual who previously exercised possession and control over it.

Storing Bitcoin Keys Responsibly

Bitcoin is just information, so it is difficult to place it inside existing financial definitions and regulations. But with its information space being the first

example of truly scarce information, it has accrued substantial value thanks to evolving narratives.

If you want to learn about responsible Bitcoin private key custody for your fund, exchange, or other vehicles, have strict LP and risk management requirements, or otherwise appreciate a trust-minimized profile, we'd love to talk.

Please email us at custody@kn0x.io

Under no circumstances should any material on this post be construed as an offering of securities or investment advice. The reader should consult with their professional investment advisor regarding investments in securities referred to herein.

Services and products are offered through KNØX Industries Inc., headquartered in Montreal, Canada. KNØX Industries Inc. is not engaged in the offer, or sale of securities or bitcoins, and does not provide investment, tax or legal advice.

Investments and holdings of bitcoins are speculative and highly volatile, involving a substantial degree of risk, including the risk of complete financial loss.

Thanks to Thib.

The Perfect Storm: Why Bitcoin at $10,000 in 2020 is different from Bitcoin at $10,000 in 2017

By Marc van der Chijs

Posted February 13, 2020

Tonight I was walking along the Vancouver Sea Wall, something I do regularly these days. Just walking at a fast face (6-7 km/h) while watching the sea, the boats, the waves, and the occasional seal popping up, but mainly thinking through new ideas. I was feeling a bit anxious, which is unusual for me, so I tried to figure out why I was feeling that way. Suddenly I realized it is because of Bitcoin, not because of its recent performance (BTC is up 45% over the past 6 weeks) but because I realized we are finally at the point where Bitcoin is ready to break out. Let me explain.

Last Friday (6 days ago since I am writing this) Bitcoin broke through $10,000, an important psychological barrier for many investors. I was at a dinner party with friends while watching the Bitcoin price. During the beginning of the dinner I was more focused on the price than on the conversations (my bad…) and I actually managed to screen shot the exact moment when Bitcoin hit $10,000.

Of course the topic changed to Bitcoin right away (most of the people had some exposure to Bitcoin already) and I explained why this was an important moment for crypto. Not because Bitcoin would never go below $10K again (it actually dipped to $9850 a few days later), but because this was the first time that Bitcoin traded over $10K while I felt it was priced correctly. Breaking through $10K at the current fundamentals and at high volumes means $20K this year is suddenly very likely and my predictions of at least $100-200K per Bitcoin in a few years seem more and more likely.

During the past days I was more focused on non-crypto investments and new business ventures so I did not really take the time to put my thoughts on this together. But while walking I realized my mind had already done the work for me. So I am just going to type my thoughts into a blog post.

In 2017 BTC went up to an all time high of almost $20,000, but what people forget is that the ‘race’ from $10,000 to $20,000 lasted for just over a week and $14,000 to $20,000 happened in just 2 days. Hardly anybody bought or sold above the current price, meaning that today’s price of $10,000+ is actually quite similar to an all time high.

I remember that on December 6, 2017 we were on a Hut 8 road show on Wall Street and that we could not believe what was happening to Bitcoin when we checked our phones during investor presentations. Late afternoon after our presentations were finished, Mike Novogratz invited us to fly back to Toronto on his private jet and during the flight we mainly kept on checking our phones instead of enjoying the food and drinks. I think we hit $16,000 while in the air and I have to give it to Mike that he called the top at that point. He said it was time to start taking profits, something I was not so sure about yet at that point.

The next day I was speaking at a GMP conference in Toronto and I was literally checking the price while I was on stage (and announcing to the audience that the price had gone up a $1000 to $18,0000 while I still on stage). Looking back I should have realized it was crazy and could not continue like this. It was indeed not sustainable and not long after that the Bitcoin price started to crash hard.

Today is very different though. 2017 was mainly a retail investor market, but most of these investors have left the market since. They did not really understand what they were investing in so they either sold at a loss or totally forgot about their investment. 2020 is different, I feel the current bull market is led by institutions and family offices. Well-informed investors that invest because they see Bitcoin as a potential store of value in volatile times. They were not in the market in late 2017 because they were either not allowed to be in it yet (e.g. there were no approved custodians) or because they did not know how to invest in Bitcoin. We have come a long way since then, but it's still not easy to buy and hold Bitoin (one reason why we are very far from a new top). The narrative has changed though and many people start to see Bitcoin as a real new asset class.

One important factor is that there is finally a model to value Bitcoin. When Sean and I did a roadshow all over Canada for the FBC Bitcoin Trust in September 2017 we always made the comparison to Gold, explaining that if Bitcoin would just become a store of value and its market cap would be just be 10% of Gold, the price would be $50,000-60,000 (this is based on today's BTC market cap of below $200B, while Gold is worth over $8 Trillion). I also explained the value of Bitcoin as a potential currency, and the value of the Bitcoin blockchain as the most secure database on earth, that would make Bitcoin even more valuable, but most people did not understand it. They wanted to see a model.

And now there is one, the stock to flow model, developed by fellow Dutchman Plan B (who wants to remain anonymous). The model is based on scarcity of Bitcoin and it can be used to calculate future Bitcoin prices. So far it hold up very well and it predicts a Bitcoin price of at least $50,000 next year

and possibly up to $100,000. From there it keeps on going up to $1 million by 2028-29. Wishful thinking? Maybe, but 7 years ago Bitcoin was a factor 100 lower than now, so it could easily go up another factor 100 in the next 7 years. Many people have been trying to falsify the model, but so far nobody has managed, which is a very strong signal for me.

The title of this post is The Perfect Storm because I believe the world is heading into the wrong direction at the same time that Bitcoin is becoming more prominent. First of all because of the Coronavirus (another topic I should write about soon). In 2017 it was not clear what BTC was going to be: a currency, a store of value or something else. Right now BTC has shown a couple of times that it seems to be mainly a store of value (it still might have other functions in the future as well). The Coronavirus might be the catalyst for a new crisis.

China has literally come to a complete stand still. People can't leave their homes (or don't want to, even if they can), most stores and restaurants are closed and the retail economy has come to a stand still. But even more important, factories are closed and will remain closed for the foreseeable future. This means that supply chains all over the world will be disrupted soon. Even if your product only has one small part sourced from China you won't be able to build your product. People in North America and Europe don't see the effects yet and it's actually hard to believe for me that it's still business as usual here. But I believe that will change fast and it may be the Black Swan event that will lead to a major stock market crash. When that happens it could lead people to invest in Bitcoin as a safe haven, meaning a potential huge spike in the Bitcoin price.

Even if the Coronavirus won't be as bad as I think it is, we still have the problem that many countries have so much debt that they will never be able to repay it. Whatever you call it or whatever it is, quantitative easing, repo short-term lending or simply printing money, the effects are all the same. This is not sustainable. The powers that be want the current state to last as long as possible, because they make tons of money. But it won't last. The corona virus could be the nail in the coffin that will lead the financial markets to collapse. But even if it is not, something else will happen soon that will push Bitcoin as a safe have investment.

In 2017 the crypto bull market was led by retail investors, but not many are still in the market. However, they are quickly coming back. I can see it on Twitter where I suddenly have a lot more Bitcoin conversations than just a few weeks ago. I can see it in the altcoin markets, where coins that in my opinion have zero value suddenly go up with double digit percentages. And the emails start coming in again from people that want to buy large amounts of BTC. Something is happening, I can feel it. And I guess that's where my

anxiousness came from. I want to be behind my laptop knowing what is happening in the markets and being part of it. But walking the Seawall is probably more healthy and a better use of my time for an hour per day.

During Bitcoin's past 7 years I have only felt twice like this. Once in October 2013 when I was a partner in a venture capital fund and I literally had no interest in looking at new companies simply because I believed putting money into BTC would lead to much better returns (too bad I did not follow my gut feeling, this was when Bitcoin just broke through $100, two months later it hit $1000). The next time was in early 2017 when Bitcoin started its new bull run from $1000 to almost $20,000 and I felt BTC was finally more or less de-risked.

Now it's February 2020, Bitcoin trades at just over $10,000 and it seems stronger than ever. The mining reward halving is coming up (which cuts supply by 50%, meaning a potential doubling of the BTC price), governments seem to be okay with Bitcoin and Bitcoin mining, and the Stock to Flow model predicts a 5-10X price increase before the end of 2021. The financial markets are at unsustainable all-time highs, a virus is threatening the world, and climate change is slowing but surely making the world a much worse place to live. It seems like a perfect storm to me and it may be time for Bitcoin to make its next big move.

Some conclusions after learning Bitcoin

By acrual

Posted February 15, 2020

1. There is no such thing as altruist cooperation with strangers, that's why we use money, ultimately a reputation system (Selfish gene)
2. If the system is not good enough, we need to trust 3rd parties for things like transportation, storage or property transmission of value to name a few.
3. Because of 1, 3rd parties will only work in their best interest, not in that of strangers, typically understanding strangers as those beyond the Dunbar number (around 150 people your neocortex is able to manage information from)
4. As a result socialism can't work. Socialism sells you the idea that by sharing things like language, some common historic achievements you will not be strangers, yet you likely are.
5. Socialism only explains either ignorance or willingness to gain power at the expense of strangers. Socialism looks after zero sum games and gets negative sums as a result. Cooperation is either positive or negative, it can't be neutral.
6. Disseminating pain among the many is an addictive drug, either via inflation, taxing, but the reputation system of money stops working. It is like soma to name Huxley's metaphor. Suddenly money, understood as the ultimate skin in the game, is not your skin in the game but somebody else's
7. Things become unfair as a result, understanding fairness not as equality of outcomes but as equality of opportunities. Those closest to the 3rd parties have more opportunities that those who are not
8. For 3rd parties, it was easier to pretend being indispensable when information was easy to control and censor but you can't control it any longer
9. Consequently people will increasingly challenge what they believed to be true and especially the need for those 3rd parties and close ones that behaved as rent-seekers
10. Trust as a result is moving somewhere else in fields such as education, health and financial advice.
11. And technology is also moving in the direction of empowering the individual in other areas such as security or energy, once economies of scale disappear
12. When both trust and technology move in the same direction, it is time for social techtonic shifts Bitcoin is the main driver of this transition, as

it reduces the main driver holding current 3rd parties' power together, which is the monopoly on violence

13. As I've said before, Bitcoin is in my opinion the coup de grace to the current social system because trust and technology are moving into a completely different direction to the current one

---

The Complex Markets Hypothesis

By Allen Farrington

Posted February 15, 2020

In which I hypothesise that markets are subjective, uncertain, complex, stochastic, adaptive, fractal, reflexive … — really any clever sounding adjective you like — just not efficient.

available as pdf **here**, if desired

photo by skeeze_, _via Pixabay

Around a month ago, Nic Carter asked me to have a look at a final draft of his article on the basics of the Efficient Markets Hypothesis. Dancing around the edges of Bitcoin Twitter as I am prone to do, I immediately grasped both the need for and the point of such an article; the question of whether the upcoming 'halving' is 'priced in' or not had "***become a source of great rancor and debate,***" as Nic wrote. For the uninitiated, 'the halving' is the reduction of the bitcoin block reward from 12.5 bitcoin to 6.25, expected around May 2020. Nic set himself the task of explaining the EMH more or less from scratch, in

such a way that the explanation would naturally lend itself towards insight on questions of Bitcoin's market behaviour.

[An Introduction to the Efficient Market Hypothesis for Bitcoiners, What the EMH does and does not say}(https://medium.com/@nic__carter/an-introduction-to-the-efficient-market-hypothesis-for-bitcoiners-ed7e90be7c0d)

I think he did a great job and the article is well worth reading. But I couldn't help thinking as I went through it that, basically, I didn't believe this stuff the first time around, and it all seemed strangely incongruous in a setting explicitly involving Bitcoin, what with the tendency of serious thinkers in this space to treat highly mathematised mainstream / neoclassical financial economics with something between suspicion and disdain.

To be completely clear, this is in no way a 'rebuttal' to Nic. He articulated the EMH very well, but didn't defend it. That wasn't the point of his article at all. He watered down the presentation at several points by saying (quite helpful) things like:

"I do not believe in the 'strong form' of the EMH. No finance professional I know does. It is generally a straw man,"

and,

"Interestingly, by caveating the EMH, we have stumbled on an alternative conception entirely. The model I have described here somewhat resembles Andrew Lo's adaptive market hypothesis. Indeed, while I am very happy to maintain that most (liquid) markets are efficient, most of the time, the adaptive market model far more closely captures my views on the markets than any of the generic EMH formulations."

One passage in particular stuck out to me:

"Referring to it as a model makes it very clear that it's just an abstraction of the world, a description of the way markets should (and generally do) work, but by no means an iron law. It's just a useful way to think about markets."

This is where I'm not so sure. Yes, it's an abstraction, and no, it's not an iron law. But I don't think it's a terribly good abstraction, and I think the reason is that it subtly contradicts and elides what ***are***, in fact, iron laws, or as close to iron laws as can be found in economics. It's a useful way to think about markets, to a point, but I want to explore what I think is a more useful way.

My argument will go through the following propositions, which serve as headings for their own sub-sections of discussion: value is subjective; uncertainty is not risk; economic complexity resists equilibria; markets aggregate prices, not information; and, markets tend to leverage efficiency.

I will conclude with some additional commentary on Andrew Lo's ***Adaptive Markets Hypothesis*** and Benoit Mandelbrot's interpretation of fractal geometry in financial markets, simply because, of all the reading around this topic that was thrown up by Nic's article, these two were by far the most intriguing. I didn't want to do either an injustice by bending their arguments too far to make them fit my own, but I think that they can be very fruitfully analysed with the conceptual tools we will have developed by the conclusion of the essay. I will also occasionally invoke the concepts of 'reflexivity', as articulated by George Soros in ***The Alchemy of Finance***, and several concepts popularised and articulated by Nassim Taleb, such as 'skin in the game' and 'robustness'.

This might seem like an excessive coverage list just to offer a counter to the claim that markets are 'efficient' — which seems pretty reasonable in and of itself. If it is at all reassuring to the reader before diving in, I don't think my thesis has five intimidating-sounding propositions, so much as one quite simple idea, from which many related propositions can be shown to follow. I think that, fundamentally, the efficient markets hypothesis is contradicted by the implications of value being subjective, and that some basic elements of complex systems are helpful, in places, to nudge the reasoning along. This essay is an attempt to tease these implications out.

Value is Subjective

You shouldn't compare apples and oranges, except that sometimes you have to, like when you are hungry. If apples and oranges are the same price, you need to make a decision that simply cannot be mathematised. You either like apples more than oranges, or vice versa. And actually, even this may not be true. Maybe you know full well you like oranges, but you just feel like an apple today, or you need apples for a pie recipe for which oranges would be ***très gauche***. This reasoning is readily extended in all directions; which is _objectively _better, a novel by Dickens or Austen? A hardback or an ebook by either, or anybody? And what about the higher order capital goods that go into producing apples, oranges, novels, Kindles, and the like? Clearly they are 'worth' only whatever their buyer subjectively assesses as likely to be a worthwhile investment given the (again) subjective valuations of others as to the worth of apples, oranges, novels, and whatnot …

This is all fine and dandy; readily understood since the marginal revolution of Menger, Jevons, and Walras in the 1870s rigorously refuted cost and labour theories of value. As Menger put it in his magisterial ***Principles of Economics,***

"Value is thus nothing inherent in goods, no property of them, nor an independent thing existing by itself. It is a judgment economizing men make about the importance of the goods at their disposal for the maintenance of

their lives and well-being. Hence value does not exist outside the consciousness of men."

Fair enough. But the first seductive trappings of the EMH come from the rarely articulated assumption that such essential subjectivity is erased in financial markets because the goods in the market are defined only in terms of cash flows. There may not be a scientific answer as to whether apples are better than oranges, but surely $10 is better than $5? And surely $10 now is better than $10 in the future? But what about $5 now or $10 in the future?

There are (at least) two reasons this reductionism is misleading. The first comes from the mainstream neoclassical treatment of temporal discounting, which is to assume that only exponential discounting can possibly be "optimal". The widespread prevalence of alternative approaches — hyperbolic discounting, for example — is then usually treated via behavioural economics, as a deviation from optimality that is evidence of irrational cognitive biases.

This has been challenged by a recently published preprint paper by Alex Adamou, Yonatan Berman, Diomides Mavroyiannis, and Ole Peters, entitled ***The Microfoundations of Discounting*** (arXiv link here) arguing that the single assumption of an individual aiming to optimise the growth rate of her wealth can generate different discounting regimes that are optimal relative to the conditions by which her wealth grows in the first place. This in turn rests on the relationship between her current wealth and the payments that may be received. Sometimes this the discounting that pops out is exponential, sometimes hyperbolic, sometimes something else entirely. It depends on her circumstances.

I would editorialise here that an underlying cause of confusion is that people value time itself, and, naturally, do so subjectively. It may be fair enough to say that they typically want to use their time as efficiently as possible — or grow their wealth the fastest — but this is rather vacuous in isolation. Padding it out with circumstantial information immediately runs into the fact that everybody's circumstances are different. As Adamou said on Twitter shortly after the paper's first release, ***not many 90-year olds play the stock market***. It's funny because it's true.

And it is easy to see how this result can be used as a wedge to pry open a conceptual can of worms. In financial markets, there are far more variables to compare than just the discount rate — and if we can't even assess an objective discount rate, we really are in trouble! In choosing between financial assets we are choosing between non-deterministic streams of future cash flows, as well as (maybe — who knows?) desiring to preserve some initial capital value.

Assume these cash flows are 'risky', in the sense that we can assign probabilities to their space of outcomes. In the following section, we will see that really the cash flows are not 'risky', but 'uncertain', which makes this problem even worse — but we can stick with 'risky' for now as it works well enough to make the point. There can be no objective answer because different market participants could easily have different risk preferences, exposure preferences, liquidity needs, timeframes, and so on.

Timeframes are worth dwelling on for a second longer (there's 'time' again) because this points to an ill-definition in my hasty setup of the problem: to what space of outcomes are we assigning probabilities, exactly? Financial markets do not have an end-point, so this makes no sense on the face of it. If we amend it by suggesting (obviously ludicrously) that the probabilities are well-defined for every interval's end-point, ***forever***, then we invite the obvious criticism that different participants may care about different sequences of intervals. Particularly if their different discount rates (which we admitted they must have) have a different effect on how far in the future cash flows have to come to be discounted back to a value that is negligible in the present. Once again, people value ***time itself subjectively.***

In the readily understood language employed just above, market participants almost certainly have different ***circumstances*** to one another, from which different subjective valuations will naturally emerge. What seems to you like a stupidly low price at which to sell an asset might be ideal for the seller because they are facing a margin call elsewhere in their portfolio (see Nic's cited example of what blew up LTCM despite it being a 'rational bet'), or because they hold too much of this asset for their liking and want to rebalance their exposure. Or perhaps some price might seem stupidly high to buy, but the buyer has a funding gap so large that they need to invest in something that has a non-zero probability of appreciating by that much. If you _need _to double your money, then the 'risk-free asset' is infinitely risky. There is no right answer, because value is subjective.

Uncertainty is not Risk

'Risk' characterises a nondeterministic system for which the space of possible outcomes can be assigned probabilities. Expected values are meaningful and hence prices, if they exist in such a system, lend themselves to effective hedging. 'Uncertainty' characterises a nondeterministic system for which probabilities _cannot _be assigned to the space of outcomes. Uncertain outcomes cannot be hedged. This distinction in economics is usually credited to Frank Knight and his wonderful 1921 book, ***Risk, Uncertainty, and Profit***. In the introduction, Knight writes,

"It will appear that a measurable uncertainty, or "risk" proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effect

an uncertainty at all. We shall accordingly restrict the term “uncertainty” to cases of the non-quantitive type. It is this “true” uncertainty, and not risk, as has been argued, which forms the basis of a valid theory of profit and accounts for the divergence between actual and theoretical competition.”

Keynes is often also credited an excellent exposition,

“By “uncertain” knowledge, let me explain, I do not mean merely to distinguish what is known for certain from what is only probable. The game of roulette is not subject, in this sense, to uncertainty… Or, again, the expectation of life is only slightly uncertain. Even the weather is only moderately uncertain. The sense in which I am using the term is that in which the prospect of a European war is uncertain, or the price of copper and the rate of interest twenty years hence, or the obsolescence of a new invention, or the position of private wealth owners in the social system in 1970. About these matters there is no scientific basis on which to form any calculable probability whatever. We simply do not know. Nevertheless, the necessity for action and for decision compels us as practical men to do our best to overlook this awkward fact and to behave exactly as we should if we had behind us a good Benthamite calculation of a series of prospective advantages and disadvantages, each multiplied by its appropriate probability, waiting to be summed.”

The conclusion of the Keynes passage is particularly insightful as it gets at why it is so important to be clear on the difference, which otherwise might seem like little more than semantics: people need to act. They will strive for a basis to treat uncertainty as if it were risk so as to tackle it more easily, but however successful they are or are not, they must act nonetheless.

The Knight extract hints at the direction of the book’s argument, which I will summarise here: that profit is the essence of competitive uncertainty. Were there no uncertainty, but merely quantifiable risk in patterns of production and consumption, competition would drive all prices to a stable and commoditised equilibrium. In financial vocabulary, we would say there would be no such thing as a sustainable competitive advantage. The cost of capital would be the risk-free rate, as would all returns on capital, meaning profit is minimised. In aggregate, profit would function merely as a kind of force pulling all economic activity to this precise point of strong attraction.

But of course, uncertainty is very real, as Keynes’ quote makes delightfully clear. I would argue, in fact, that in the economic realm it is a direct consequence of subjective value; in engaging in pursuing profit, you are guessing what others will value. As Knight later writes,

"With uncertainty present, doing things, the actual execution of activity, becomes in a real sense a secondary part of life; the primary problem or function is deciding what to do and how to do it."

So far I have danced around the key word and concept here, so as to try to let the reader arrive at it herself, but this 'deciding what to do and how to do it', and 'pursuing profit', we call ***entrepreneurship***. In a world with uncertainty, the role of the entrepreneur is to shoulder the uncertainty of untried combinations of capital, the success of which will ultimately be dependent on the subjective valuations of others. This is not something that can be calculated or mathematised, as any entrepreneur (or VC) will tell you. As Ross Emmett noted in his centennial review of ***Risk, Uncertainty, and Profit***, it is no coincidence that the word 'judgment' appears on average every two pages in the book.

There are two points about the ***process*** of entrepreneurship that I believe ought to be explored further, and which lead us to Soros and Taleb: you can't just _imagine _starting a business; you have to actually do it in order to learn anything. And, in order to do it, you have to expose yourself to your own successes and failures. Your experiment changes the system in which you are experimenting, and you will inevitably have a stake in the experiment's result.

This is fertile ground in which to plant Soros' theory of reflexivity. As briefly as possible, and certainly not doing it justice, Soros believes that financial markets are fundamentally resistant to truly scientific analysis because they can only be fully understood in such a way that acknowledges the fact that thinking about the system influences the system. He writes that the scientific method:

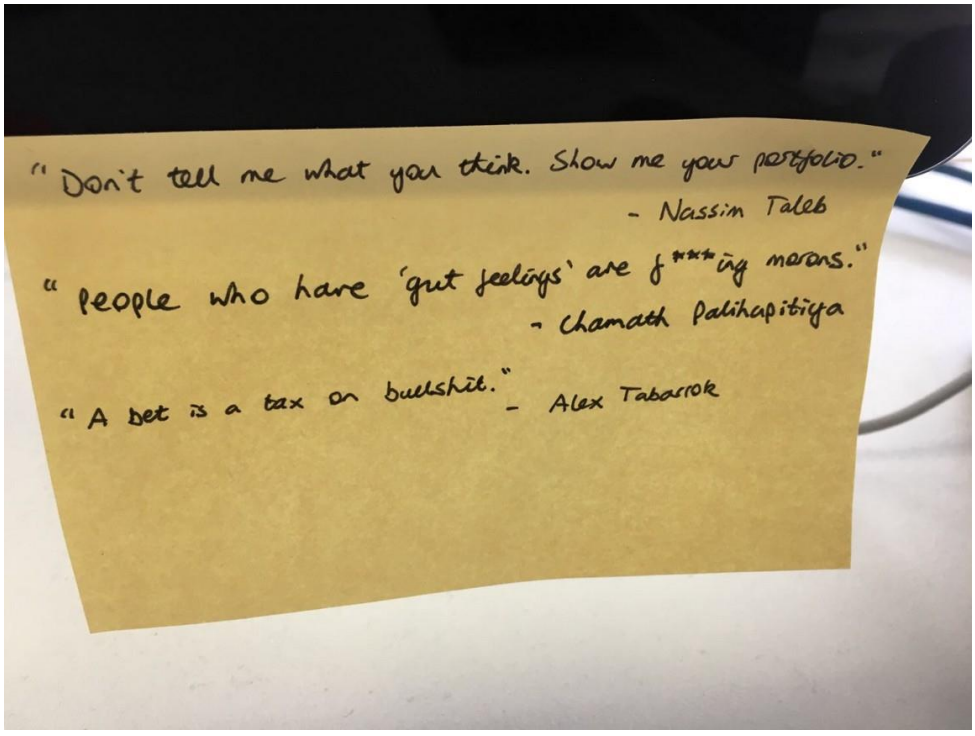
"is clearly not applicable to reflexive situations because even if all the observable facts are identical, the prevailing views of the participants are liable to be different when an experiment is repeated. The very fact that an experiment has been conducted is liable to change the perceptions of the participants. Yet, without testing, generalisations cannot be falsified."

All potential entrepreneurial activity is uncertain (by definition) but the fact of engaging in it crystallises the knowledge of its success or failure. The subjective valuations on which its success depends are revealed by the experiment, and you can't repeat the experiment pretending you don't now know this information. Alternatively, this can be conceived of in terms of the difference between thinking and acting, or talking and doing. In a reflexive environment, you can't say ***what would have happened had you done something***, because, had you done it, you would have changed the circumstances that lead to you now claiming you would have done it. As Yogi Berra (allegedly) said, "***in theory there is no difference between theory and practice, but in practice, there is,***" and as Amy Adams vigorously proclaims

in *Talladega Nights*, quite the treatise on risk and uncertainty by the way, and with a criminally underrated soundtrack, "***Ricky Bobby is not a thinker. Ricky Bobby is a driver.***"

We can also now invoke 'skin in the game', a phrase of dubious origin, but nowadays associated primarily with Nassim Taleb, and expounded in his 2017 book of the same name. Again, not doing it justice (he did write a whole book about this) Taleb believes that people ought to have equal exposure to the potential upsides and downsides of their decisions; 'ought to' in both a moral sense of deserving the outcome, but also in the sense of optimal system design, in that such an arrangement encourages people to behave the most prudently out of all possible incentive schemes. It readily applies here in that braving the wild uncertainties of entrepreneurship requires capital — it requires a stake on which the entrepreneur ***might _get the upside of profit, but _might _get the downside of loss. I say 'might' because you cannot possibly know the odds of such a wager. It relies not on risk, but on uncertainty. As Taleb writes, "_entrepreneurs are heroes in our society. They fail for the rest of us.***"

The combined appreciation of 'judgment' and 'skin in the game' is key to understanding what entrepreneurs are actually ***doing***. They do not merely throw capital into a combinatorial vacuum; they are intuiting the wants and needs of potential customers. And as I simply cannot resist the opportunity to employ, possibly my favourite quote from any economist, ever: as Alex Tabarrok says, ***a bet is a tax on bullshit.*** Or, ***don't talk; do.***



my desk at work. It's good to keep these things in mind.

That same Emmett review of Knight's book noted that the very concept of _Knightian uncertainty _re-emerged in the public consciousness around a decade ago due to two events: the role

ironically played by financial risk instruments in the financial crisis, which neoclassical economists had up until that point insisted would reduce uncertainty in markets (search for "Raghuram Rajan Jackson Hole" if unfamiliar); and Taleb publishing the bestseller ***The Black Swan.***

(Although, naturally, Taleb deplores the concept of 'Knightian Uncertainty'. What I believe Taleb truly objects to, however, is how the concept has come to be used, rather than anything Knight himself believed. Economists often invoke 'Knightian Uncertainty' as a sleight of hand to demarcate some corner of reality, and imply that everywhere else is merely 'risky' and can be modelled. This is nonsense. In real life, everything is uncertain, or, as Joseph Walker succinctly put, "***Taleb's problem with Knightian uncertainty is that there's no such thing as non-Knightian uncertainty***." I think Knight would almost certainly agree, as would anybody who has actually ***read _Knight, instead of employing his name in the course of _macro-bullshitting***, as Taleb would put it.)

Writes Emmett,

"Taleb did not suggest that uncertainty could be handled by risk markets. Instead, he made a very Knightian argument: since you cannot protect yourself entirely against uncertainty, you should build robustness into your personal life, your company, your economic theory, and even the institutions of your society, to withstand uncertainty and avoid tragic results. These actions imply costs that may limit other aspects of your business, and even your openness to new opportunity."

But enough about entrepreneurship, what about financial markets? Well, financial markets are readily understood as one degree removed from entrepreneurship. With adequate mental flexibility, you can think of them as markets for fractions of entrepreneurial activity. Entrepreneurship-by-proxy, we might say. If you want, you can use them to mimic the uncertainty profile of an entrepreneur: your 'portfolio' could be 100% the equity of the company you wish you founded. Or 200%, with leverage, if you are really gung-ho! But most people think precisely the opposite way: markets present the opportunity to tame the rabid uncertainty of entrepreneurship in isolation, and skim some portion of its aggregate benefit.

There is an additional complication. The fact of such markets usually being liquid enough to enable widespread ownership creates the incentive to think not about the underlying entrepreneurship at all, but only about the expectations of other market participants — to ignore the fundamentals and consider only the valuation. There are shades of Soros' reflexivity here. The market depends to some extent on the thinking of those participating in the market ***about _the market. This is sometimes called a Keynesian beauty contest, after Keynes' analogy of judging a beauty contest not on the basis***

of who you think is most beautiful, but on the basis of who you think others will think is the most beautiful. But if everybody is doing that, then you really need to judge on the basis of who you think others will think others will think is the most beautiful, and so on. Unlike the entrepreneur, who must only worry about the subjective valuation of his potential customers, participants in financial markets must worry, in addition, about the subjective valuation _of this subjective valuation _by other market participants. There is often grumbling at this point that this represents 'speculation' as opposed to 'investment', and I certainly buy the idea that over time periods long enough to reflect real economic activity allowed for by the investments, such concerns will make less and less of a difference. As Benjamin Graham famously said, "_in the short run, the market is a voting machine, but in the long run, it is a weighing machine". But the voting still happens. It is clearly real and needs to be accounted for. Risk is once again useless. Uncertainty abounds.

This range of possibilities is intriguing and points to a deeper understanding of what financial markets really ***are***: the aim of a great deal of finance is to grapple with the totality of uncertainty inherent in entrepreneurial activity — equally well understood as 'investment of capital', given the need for a 'stake' — by partitioning it into different exposures that can sensibly be described as _relatively _more or less 'risky'. The aim of doing so is generally to minimise the cost of capital going towards real investment by tailoring the packaging of uncertainty to the 'risk profiles' of those willing to invest, as balanced by escalating transaction costs if this process becomes too fine-grained.

This is the essence of a capital structure: the more senior the capital claim, the better defined the probability space of outcomes for that instrument. Uncertainty in aggregate cannot be altered, nor can its influence be completely removed from individual instruments, but exposure to uncertainty can be unevenly parcelled out amongst instruments.

This suggests a far more sophisticated understanding of 'the risk/reward trade-off' and 'the equity premium' than is generally accepted in the realm of modern portfolio theory, and, by extension, the EMH: bonds are likely to get a lower return than stocks not because they are less 'risky' (which in that context is even more questionably interpreted as 'less volatile') but because they are engineered to be less uncertain. The burden of uncertainty is deliberately shifted from debt to equity. You don't get a 'higher reward' for taking on the 'risk/volatility' of equities; you deliberately expose yourself to the uncertain _possibility _of a greater reward in exchange for accepting an uncertain possibility of a greater loss.

It is worth pondering for a second that this is arguably why the 'equity risk premium' even exists (and why neoclassical economists are so confused about it, while financial professionals are not in the slightest) — if there really

were no uncertainty in investment and every enterprise — and hence every financial instrument linked to it — had a calculable risk profile, then price discrepancies derivable from expectation values could be arbitraged away. There would be no equity risk premium — nor a risk premium of any kind on any asset. Everything would be priced correctly and volatility would be zero. That volatility is _never _zero clearly invalidates this idea. I suggest that the distinction between risk and uncertainty provides at least part of the explanation: unless, by remarkable coincidence, every market participant's opportunity costs (of exposure, liquidity, time, etc.) and perception of uncertainty (of fundamentals, other' perceptions of fundamentals, others' perception of others' perceptions, etc.) is all identical, and remains so over a period of time, price-altering trading will occur.

(I will note in passing that this commentary is merely intended to provide the intuition that something is amiss with the 'equity premium puzzle'. It is incomplete as an explanation. In the later section on leverage efficiency, I will cover Peters' and Adamou's more formal proof of the puzzle's non-puzzliness.)

An important concept to appreciate in the context of uncertainty is that of 'heuristics'. This is an important loose-end to tie up before moving on from uncertainty, along with one more, 'randomness and unpredictability', which I cover shortly. This is quite a simple idea that originates with Herbert Simon and has been taken up with force more recently by Gerd Gigerenzer of the Max Planck Institute for Human Development, and more obliquely by Taleb. Simon's framing began by assuming that individuals do not in fact have perfect information, nor the resources to compute perfectly optimal decisions. Given these constraints, Simon proposed that individuals demonstrate ***bounded rationality***; they will be as rational as they can given the information and resources they actually have. This probably sounds straightforward enough — perhaps tautological — but notice it flies in the face of behavioural economics, which tends to cover for neoclassical economics by saying, effectively, that since information and competition are perfect, risk is always defined and the optimal decision can always be calculated, but the reason people don't do so is that they are hopelessly irrational. I have always thought this is quite silly on the face of it, but it is clearly also seductive. Anybody reading the likes of ***Thinking, Fast and Slow*** immediately gets the intellectual rush of thinking everybody is stupid except him.

Bounded rationality encourages the development of 'heuristics', which the reader may recall behavioural economists railing against. A heuristic is effectively a rule of thumb for dealing with an uncertain environment that you are pretty sure will work even if you can't explain why, precisely. The classic example is that of a dog and a frisbee, or an outfielder in baseball

catching a flyball: the outfielder _could _solve enough differential equations to calculate the spot the ball will land, but the dog certainly can't. And it turns out that neither do: in real life, they adjust their running speed and direction such that the angle at which they see the frisbee or ball stays constant. And it works. No equations required. Yippee.

(Farrington's Heuristic is another good example, which I made up while editing a later version of this essay— if a writer is discussing risk, uncertainty, knowledge, and the like, if he refers to Gödel's Incompleteness Theorems, and if he is not obviously joking, then everything else he says can immediately be dismissed because he is a bullshitting charlatan enamoured by cargo cult math. This heuristic has only one binary parameter — 'is he joking?' — and so is highly robust. In case anybody cares, the theorems are NOT about 'knowledge': they are about provability within first order formal logical theories strong enough to model the arithmetic of the natural numbers. This is quite a specific mathematical thing that bears no relation whatsoever to epistemology or metaphysics. Also, there are two of them, which turns out to be important if you understand what the first one says.)

The implied simplicity of heuristics has subtle mathematical importance, also. A more technical way of specifying this is to say that they have very few parameters — discrete, independent information inputs to the decision procedure — ideally they could even have zero. In a purely risky environment (if such a thing exists, which, in real life, it almost certainly does not) a decision procedure ought to have *as many _parameters as are needed to capture the underlying probability distribution. But the more uncertainty you add to such an environment, the more dangerous this becomes, essentially because what you are doing is fine-tuning your model to an environment that simply no longer exists. Eventually you will get an unforeseen fluctuation so large that your overfitted model gives you a truly awful suggestion. Heuristics are _robust* to such circumstances in light of having very few parameters to begin with. Think back to the outfielder: imagine he solves all the necessary fluid dynamical equations, taking account of the fly ball's mass, velocity, and rotation, the air's viscosity, the turbulence generated, and so on. If there is then a gust of wind, he's screwed. His calculation will be completely wrong. But if he embraces the heuristic of _just looking at the damn ball _this won't matter!

Interested readers are encouraged to peruse Gigerenzer's recent(ish) work on the use of heuristics in finance, and their abuse in behavioural economics, which recently got a shout out in Bloomberg, or this video which is a great introduction to Gigerenzer's ideas, as well as their connection to Taleb's more informal thinking on the same topic. (also, note the number of times

Gigerenzer uses the word ‘complex’. It is no coincidence that this is ***a lot***, as we shall shortly see):

The video linked to is around an hour and a half, so the reader need not take such a detour now, but I would encourage it at some point, as both Gigerenzer and Taleb are excellent. My favourite excerpt comes around the 19-minute mark, when Gigerenzer recalls that Harry Markowitz — considered the founder of modern portfolio theory — didn’t actually use any Nobel-prize winning modern portfolio theory for his own retirement portfolio; he used the zero-parameter 1/n approach. If one were being especially mean-spirited, one might say that he didn’t want his own bullshit to be taxed. And as it turns out, in order for the Markowitz many-many-many parameter approach to investing to consistently outperform 1/n, you would need around 500 years of data to finetune the parameters. Of course, you also need the market to _not change at all _in that time. Good luck with that.

Since markets feature multitudes of interrelated uncertainties, it is reasonable to expect participants to interact with them not with the perfect rationality of provably optimal behaviour, but with the bounded rationality of heuristics, which are selected on the basis of judgment, intuition, creativity, etc. Basically, people mostly are not stupid. And if they are, they have skin in the game, so they get punished, and possibly wiped out.

A kind of nice, conceptual corollary to ‘risk is not uncertainty’ is, ‘unpredictability is not randomness’. There can be unpredictable events that are not random, and randomness that is not unpredictable. The difference essentially comes down to ‘causation’. Think of Keynes’ example of the obsolescence of a new invention. This is ‘unpredictable’ not because it is subject to an extremely complicated probability density function, but because the path of causation that would lead to such a situation involves too much uncertainty to coherently grasp. Or think of the bitcoin mining process. The time series of the first non-zero character in the hash of every block is certifiably random, but it is not unpredictably random. It is the result of a highly coordinated and purposeful effort. It doesn’t spring forth from beta decay. Because we understand the causal process by which this time series emerges, we can predict this randomness very effectively.

A key building block of the EMH is the ‘random walk hypothesis’: the idea that you can ‘prove’ using statistical methods that stock prices follow ‘random walks’ — a kind of well-defined and genuinely random mathematical behaviour. But you can do no such thing. You can prove that they are _indistinguishable _from random walks, but that is really just saying you can use a statistical test to prove that some data can pass a statistical test. If you _understand _what _causes _price movements, you will arrive at no such nonsense as claiming that the moves are, themselves, random. They very probably _look _random because they are fundamentally unpredictable from

the data. And they are fundamentally unpredictable from the data because they derive from the incalculable interplay of millions of market participants' subjective assessments of the at-root uncertain process of entrepreneurship.

None of this is based on randomness, nor 'risk', nor 'luck'. It is based on the unknown and unknowable profit that results from intuiting the results of untried and unrepeatable experiments and backing one's intuition with skin in the game.

Before moving on, I think it is worth tying all of this to where it is more tangibly sensible, lest the reader not quite know what to do with it all. A big deal was made recently about Netflix being by far the best performing US mid-to-large-cap stock of the 2010s. Netflix is useful as an example because of the scale of its success, but note the following argument does not depend on scale at all. While you could craft an explanation as complicated as you like, I think saying, ***streaming is better than cable***, pretty much does it, once added to all the circumstantial factors to do with the competitive and technological environment. Now imagine an investor in 2010 whose thesis was that streaming is better than cable and would likely win in the long run, who surveyed the competitive environment, and decided Netflix would be a good investment. Is their outperformance over the next 10 years 'luck'? Was all the 'information' 'in the price' in 2010? Would the CAPM tell you what the price _should _have been? Did the stock go for a nice little random walk to the moon?

This is clearly an insane interpretation. Consider the alternative: The investor better intuited the subjective values of future consumers than did the average market participant. Very likely she justified this on the basis of a heuristic or two. She staked capital on this bet — which was not risky and random, but uncertain and unpredictable — and exposed herself to a payoff that turned out to be huge, ***because she was right***! To the peddlers of the EMH, rational expectations, perfect information, and the like, this obviously sensible interpretation is utterly heretical.

Economic Complexity Resists Equilibria

The link between profit and entrepreneurship can be tugged at ever-so-slightly further, and invites a brief detour into the basics of complex systems. The argument goes more or less as follows: the discussion on uncertainty needn't be interpreted as a call to abandon mathematical analysis altogether — just the sloppy mathematics of risk and randomness that has effectively no connection to the real world. There is an alternative mathematical approach, however, which directly addresses and contradicts the standard neoclassical formalism.

The starting point is Israel Kirzner, widely considered one of the foremost scholars of entrepreneurship, and his book, _Competition and Entrepreneurship. _One of Kirzner's theses is a positive argument that has roughly two parts, as follows: first, entrepreneurship is by its nature non-exclusionary. It is a price discrepancy between the costs of available factors of production and the revenues to be gained by employing them in a particular way — or, profit. In other words, it is perfectly competitive. It does not rely on any privileged position with respect to access to assets; The assets are presumed to be available on the market. They are just not yet employed in that way, but could be, with capital that is presumably homogeneous. Anybody could do so. The only barrier is that of the willingness to judge and stake on uncertainty. He writes,

"The entrepreneur's activity is essentially competitive. And thus competition is inherent in the nature of the entrepreneurial market process. Or, to put it the other way around, entrepreneurship is inherent in the competitive market process."

This notion of what 'competition' really means is highly antithetical to the neoclassical usage. In fact, it is more or less the exact opposite. Rather than meaning something like, _tending towards abnormal profit and hence away from equilibrium, _the neoclassicals mean, _tending towards equilibrium and hence away from abnormal profit. _Kirzner bemoans this,

"Clearly, if a state of affairs is to be labelled competitive, and if this label is to bear any relation to the layman's use of the term, the term must mean either a state of affairs from which competitive activity (in the layman's sense) is to be expected or a state of affairs that is the consequence of competitive activity … [Yet] competition, to the equilibrium price theorist, turned out to refer to a state of affairs into which so many competing participants have already entered that no room remains for additional entry (or other modification of existing market conditions). The most unfortunate aspect of this use of the term 'competition'; is of course that, by referring to the situation in which no room remains for further steps in the competitive market process, the word has come to be understood as the very opposite of the kind of activity of which that process consists. Thus, as we shall discover, any real-world departure from equilibrium conditions came to be stamped as the opposite of 'competitive' and hence, by simple extension, as actually 'monopolistic'."

I'd note in passing the delightful similarity in the concluding thought of this extract to the argument of Peter Thiel's ***Zero to One***, considered by many a kind of spiritual bible for — you guessed it — ***entrepreneurship***. Anyway …

Kirzner's second positive argument is that correcting this conceptual blunder leads one to realise that a realistic description of competitive markets would

be not as constantly at equilibrium, but rather as constantly ***out of equilibrium***. And that's really all we need to move on to complex systems.

Complex systems are commonly associated with the Santa Fe Institute, and popularised by W. Mitchell Waldrop's fantastic popular science book, ***Complexity***. Waldrop focuses, for the most part, on one of the SFI's first ever workshops, held between a group of physicists and economists in 1987. The proceedings of the workshop are fantastic, have aged very well, and seem to your author cheap relative to his subjective valuation of them at ~$70 in paperback or ~$140 in hardback. My thinking here comes from the very first paper of the workshop, W. Brian Arthur's now somewhat infamous work on increasing returns. To get a sense of what I mean by 'infamous', consider the following from Waldrop:

"Arthur had convinced himself that increasing returns pointed the way to the future for economics, a future in which he and his colleagues would work alongside the physicists and the biologists to understand the messiness, the upheaval, and the spontaneous self-organisation of the world. He'd convinced himself that increasing returns could be the foundation for a new and very different kind of economic science.

Unfortunately, however, he hadn't much luck convincing anybody else. Outside of his immediate circle at Stanford, most economists thought his ideas were — strange. Journal editors were telling him that this increasing-returns stuff 'wasn't economics.' In seminars, a good fraction of the audience reacted with outrage: how dare he suggest that the economy was not in equilibrium! "

Readers can probably sense where this is going.

Arthur's paper at the workshop, ***Self-Reinforcing Mechanisms in Economics***, is a breath of fresh air if you have ever slogged through the incessant cargo cult math of neoclassical financial economics (as I had to in researching this essay — thanks a lot, Nic!) It is frankly just all so sensible! Okay, so there are a few differential equations, but only after ten pages of things that are obviously true, and only to frame the obviously true observations in the absurd formalism of the mainstream.

To begin with, "***conventional economic theory is built largely on the assumption of diminishing returns on the margin (local negative feedbacks); and so it may seem that positive feedback, increasing-returns-on-the-margin mechanisms ought to be rare.***" Standard neoclassical theory assumes competition pushes all into equilibrium, from which a deviation is punished by the negative feedback of reduced profits. So far, so good.

"Self-reinforcement goes under different labels in these different parts of economics: increasing returns; cumulative causation; deviation-amplifying

mutual causal processes; virtuous and vicious circles; threshold effects; and non-convexity. The sources vary. But usually self-reinforcing mechanisms are variants of or derive from four generic sources: large set-up or fixed costs (which give the advantage of falling unit costs to increased output); learning effects (which act to improve products or lower their cost as their prevalence increases); coordination effects (which confer advantages to 'going along' with other economics agents taking similar action); and adaptive expectations (where increased prevalence on the market enhances beliefs of further prevalence)."

Now we are getting into the meat of it. An example or two wouldn't hurt before applying this to entrepreneurship and markets.

Arthur likes Betamax versus VHS — which is a particularly good example in hindsight because we know that VHS won despite being mildly technologically inferior. Point number 1: If a manufacturer of VHS tapes spends an enormous amount on the biggest VHS (or Betamax) factory in the world, then the marginal costs of producing VHS will be lower from that point on. Even if the factory as a whole is loss making, the costs are sunk, and so the incentive is to pump out VHS by the gallon. The fact that this can be done so cheaply makes consumers more likely to choose VHS over Betamax, which will in turn justify the initial expense and contribute positive feedback (via profit).

Point number 2: doing so may give the owner of the factory the experience to learn how to do so even more efficiently in the future. By the same eventual mechanism as above, this contributes positive feedback via lower prices. (interested readers are encouraged to look into 'Wright's Law', in particular a recent paper by Béla Nagy, Doyne Famer, Quan Bui, and Jessika Trancik, which basically says that Moore's Law happens for everything, just slower; or, we learn by doing)

Points number 3 and 4: if more people seem to be buying VHS tapes than Betamax, then producers of Betamax ***players _are incentivised to shift production towards VHS players instead. Cheaper VHS players incentivise consumers to buy more VHS _tapes***. The _appearance _of VHS winning this battle causes economic agents to adapt their behaviour in such a way that makes VHS more likely to _actually _win. In glancing over an early draft of this essay, Nic kindly pointed out to me that this represents the dominant philosophy behind growth VC from 2015 until WeWorkGate, as if a bunch of zealous, born-again Arthurians were playing a game of non-iterated prisoner's dilemma with other people's money. Anyway …

Arthur writes, "***if Betamax and its rival VHS compete, a small lead in market share gained by one of the technologies may enhance its competitive position and help it further increase its lead. There is positive feedback. If***

both systems start out at the same time, market shares may fluctuate at the outset, as external circumstances and 'luck' change, and as backers manoeuvre for advantage. And if the self-reinforcing mechanism is strong enough, eventually one of the two technologies may accumulate enough advantage to take 100% of the market. Notice however we cannot say in advance _which _one this will be."

While Arthur mostly considers realistic examples in economics which have discrete end-states that are then 'locked into', such as settling on VHS over Betamax, or Silicon Valley over Massachusetts Route 128, my contention would be that every one of these features describes a part of the process of entrepreneurial competition. The fact of staking capital at all towards an uncertain end represents a fixed cost which must be matched by competitors, and after which unit costs fall. As we have mentioned several times, entrepreneurs learn from the result of their experiments and improve their own processes. There is a clear coordination effect for customers in the default assumption of doing whatever other customers are doing. And adaptive expectations are likewise fairly straightforwardly applied: we tend to assume that businesses will continue to exist and that we can continue to act as their customers. Businesses tend to assume the same of their customers within reasonable bounds of caution. The specific positive feedback as a result of each individual effect is that of 'profit' — it is positive in the sense that it can be reinvested in the enterprise and allow it to grow.

Of course, it is possible that these effects would diminish and the marginal feedback become negative. But what we are more tangibly proposing here is that any once-existing competitive advantage has been completely eroded away. This only happens when the product itself becomes either obsolete in light of a superior competitor, or completely commoditised. The former is simply more of the same at the macro level, but the latter we can in turn explain by uncertainty becoming so minimal that we can more or less safely assume it is merely risk. Such circumstances are few and far between. Uncertainty is prevalent in all aspects of economic life, as we have discussed. My argument here is that, so, therefore, are increasing returns and positive feedback loops.

To bring in Arthur one last time:

"if self-reinforcement is not offset by countervailing forces, local positive feedbacks are present. In turn, these imply that deviations from certain states are amplified. These states are therefore unstable. If the vector-field associated with the system is smooth and if its critical points — its 'equilibria' — lie in the interior of some manifold, standard Poincaré-index topological arguments imply the existence of other critical points or cycles that are stable, or attractors. In this case multiple equilibria must occur. Of course, there is no reason that the number of these should be small. Schelling gives

the practical example of people seating themselves in an auditorium, each with the desire to sit beside others. Here the number of steady-states or 'equilibria' would be combinatorial."

Recall there is no way to know from the starting point which steady-state will be settled into. And of course, Arthur is only talking about specific economic circumstances, not the aggregate of all economic behaviour. The aggregate will likely have shades of evolution in a competitive environment (another concept we will soon encounter in more detail): many, many such interdependent sub-systems, always moving towards their own steady state, but almost all never getting there. And so, in summary, there is a solid mathematical basis to saying that economic behaviour in aggregate is wildly uncertain.

Before moving on, I just want to mention that Arthur should almost certainly be better known and respected in Bitcoin circles. Readers uninterested in the connection I am proposing between Bitcoin and complex systems (or unimpressed by my amateur passion for both) can skip ahead without missing anything. Arhur's 2013 paper, ***Complexity Economics***, is an excellent place to start. Likewise, a good argument can be made that complex systems researchers should be a lot more interested in Bitcoin. Readers may well have picked up on the essence of Arthur's analysis consisting of 'network effects'. I avoided using the term because Arthur himself doesn't use it. But he is considered the pioneer of their analysis in economics, and when you think about it, the concept of 'increasing returns' makes perfect sense in the context of a network. What greater competitive advantage can you have than everybody needing to use your product simply because enough people already use it? And what product do people need to use solely because others are using it more than 'money'?

Although I have eschewed the idea of 'lock-in' as helpful for the analysis above, Bitcoin surely has amongst the strongest interdependent network effects of any economic phenomenon in history? Is it not a naturally interdisciplinary complex adaptive system ***par excellence***? Is it not a form of artificial life, coevolved with economising humans in the ecology of the Internet? I mean, for goodness' sake, Andreas Antonopoulos claims to have put ants on the cover of ***Mastering Bitcoin***because,

"the highly intelligent and sophisticated behaviour exhibited by a multimillion-member ant colony is an emergent property form the interaction of the individuals in a social network. Nature demonstrates that decentralised systems can be resilient and can produce emergent complexity and incredible sophistication without the need for a central authority, hierarchy, or complex parts."

Back in the SFI workshop, Arthur writes,

"When a nonlinear physical system finds itself occupying a local minimum of a potential function, 'exit' to a neighbouring minimum requires sufficient influx of energy to overcome the 'potential barrier' that separates the minima. There are parallels to such phase-locking, and to the difficulties of exit, in self-reinforcing economic systems. Self-reinforcement, almost by definition, means that a particular equilibrium is locked in to a degree measurable by the minimum cost to effect changeover to an alternative equilibrium."

I'm not sure anybody can sensibly describe what such a 'minimum cost' would be. Particularly because Bitcoin is set up in such a way that any move away from lock-in by one metric causes a disproportionate pull back to lock-in by another. It's Schelling points all the way down.

Markets Aggregate Prices, Not Information

The most frustrating thing about the EMH for me is that even the framing is nonsensical. You don't really need to get into subjective value, uncertainty, complex systems, and so on, to realise that in reading the proposition, ***prices reflect all available information***, you have already been hoodwinked (***hoodwunk?***). What does 'reflect' mean?

Nic dramatically improved upon this by saying that markets ***aggregate information***. I noticed this is typical of many more enlightened critiques of EMH, and it serves as a far better starting point, in at least _suggesting _a mechanism by which the mysterious link between information and price might be instantiated. Unfortunately, I think the mechanism suggested is simply invalid. It is not realistic at all and it implicitly encourages a dramatic misunderstanding of what prices really are and where they come from.

In making sense of this we have to assume some kind of 'function' from the space of information to price. I think it's acceptable to mean this metaphorically, without implying the quasi-metaphysical existence of some such force. We might really mean something like_, the market behaves ***_as if __operating according to such and such a function***. Adam Smith's 'invisible hand' is an instructive comparison. For the time being, I will talk as if some such function 'exists'.

We can maybe imagine information as existing as a vector in an incredibly high-dimensional space, at least as compared to price, which is clearly one-dimensional. We could even account for the multitudes of uncertainty we have already learned to accept by suggesting that each individual's subjective understanding of all the relevant factors and/or ignorance of many of them constitutes a unique mapping of this space to itself, such that the 'true information vector' is transformed into something more personal for each market participant. Perhaps individuals then bring this personal information vector to the market, and what the market does

is *aggregate _all the vectors by finding the average. Finally, the market _projects _this n-dimensional average vector onto the single dimension of price. If you accept the metaphorical nature of all these functions, I can admit this model has some intuitive appeal, in the vein of James Surowiecki's _The Wisdom of Crowds_._*

The problem is that this is clearly not how anybody actually interacts with markets. You don't submit your n-dimensional information/intention-vector; you submit your one-dimensional price. That's it. The market aggregates these one-dimensional price submissions in real time by matching the flow of marginal bids and asks.

This understanding gets two birds stoned at once. First, it captures the mechanics of how we know price discovery in markets ***actually works***. There is no mysterious, market-wide canonical projection function — no inexplicable 'prices reflect information' — there are just prices, volumes, and the continuous move towards clearing.

Second, it implies a perfectly satisfactory and not at all mysterious source of the projection of information into price: individuals who make judgments and act. Any supposedly relevant 'information' is subject both to opportunity cost and uncertainty. Individuals alone know the importance of their opportunity costs, and individuals alone engage with uncertainty with heuristics, judgment, and staking. If individuals are wrong, they learn. If they are very wrong, they are wiped out. Effective heuristics live to fight another day.

I am genuinely surprised that this confusion continues to exist in the realm of the EMH, given that, as far as I am concerned, Hayek cleared it up in its entirety in ***The Use of Knowledge in Society***. A superficial reading of Hayek's ingenious essay might lead one to believe something like ***prices reflect information***. But, to anachronistically borrow our function metaphor once more, Hayek points out that the projection from the n-dimensions of information to the one dimension of price _destroys an enormous amount of information. _Which is the whole point! Individuals are incapable of understanding _the entirety of information in the world. _Even the entirety of individuals is incapable of this. Thanks to the existence of markets, nobody has to. They need only know about prices. 'Perfect information' is once again shown to be an absurdity. Of the 'man on the spot', whom we might hope would make a sensible decision about resource allocation,

"There is hardly anything that happens anywhere in the world that might not have an effect on the decision he ought to make. But he need not know of these events as such, nor of all their effects. It does not matter for him why at the particular moment more screws of one size than of another are wanted, why paper bags are more readily available than canvas bags, or why skilled labor, or particular machine tools, have for the moment become more

difficult to obtain. All that is significant for him is how much more or less difficult to procure they have become compared with other things with which he is also concerned, or how much more or less urgently wanted are the alternative things he produces or uses. It is always a question of the relative importance of the particular things with which he is concerned, and the causes which alter their relative importance are of no interest to him beyond the effect on those concrete things of his own environment."

Hayek proposes this be resolved by the price mechanism:

"Fundamentally, in a system in which the knowledge of the relevant facts is dispersed among many people, prices can act to coordinate the separate actions of different people in the same way as subjective values help the individual to coordinate the parts of his plan."

Perhaps ironically, this points to the only sensible way in which markets ***can _be called 'efficient'. They are efficient with respect to the information they manipulate and convey: as a one-dimensional price, it is the absolute minimum required for participants to interpret and sensibly respond. Markets have excellent*** *social scalability****; they are the original _distributed systems***, around long before anybody thought to coin that expression.

Interestingly, this meshes very nicely with the complex systems approach to economics associated with Arthur at SFI, and perhaps more specifically with John Holland. His paper at the aforementioned inaugural economics workshop, ***The Global Economy as an Adaptive Process***_, _at seven pages and zero equations, is well worth a read. Holland recounts many, now familiar, difficulties in mathematical analysis of economics that assume linearity, exclusively negative feedback loops, equilibria, and so on, before proposing that 'the economy' is best thought of as what he calls an 'adaptive nonlinear network'. Its features are worth exploring, even if they require some translation:

"Each rule in a classifier system is assigned a strength that reflects its usefulness in the context of other active rules. When a rule's conditions are satisfied, it competes with other satisfied rules for activation. The stronger the rule, the more likely it is to be activated. This procedure assures that a rule's influence is affected by both its relevance (the satisfied condition) and its confirmation (the strength). Usually many, but not all, of the rules satisfied will be activated. It is in this sense that a rule serves as a hypothesis competing with alternative hypotheses. Because of the competition there are no internal consistency requirements on the system; the system can tolerate a multitude of models with contradictory implications."

We could easily translate 'rule' as 'entrepreneurial plan' or something similar. Entrepreneurial plans can contradict one another, clearly — if they are bidding on the same resources for a novel combination — and can and do compete with one another. Clearly, such plans are hypotheses about the result of an experiment that hasn't been run yet. Holland then says,

"A rule's strength is supposed to reflect the extent to which it has been confirmed as a hypothesis. This, of course, it's a matter of experience, and subject to revision. In classifier systems, this revision of strength is carried out by the bucket-brigade credit assignment algorithm. Under the bucket-brigade algorithm, a rule actually bids a part of its strength in competing for activation. If the rule wins the competition, it must pay this bid to the rules sending the messages that satisfied its condition (its suppliers). It thus pays for the right to post its message. The rule will regain what it has paid only if there are other rules that in turn bid and pay for its message (its consumers). In effect, each rule is a middleman in a complex economy, and it will only increase its strength if it turns a profit."

Much of this does not need translating at all: we see Menger's higher orders of capital goods, and value of intermediate goods resting ultimately with the subjective value of consumers, who pass information up the chain of production. We see agents that learn from their experience. We see skin-in-the-game of staked capital in 'bidding part of its strength' and we see uncertain gain or reward ultimately realised by profit or loss. But most importantly — most ***Hayekily*** — we see agents who have no such fiction as 'perfect information', but rather responding solely to prices in their immediate environment, and whose reactions affect prices that are passed to other environments. In ***Complexity***, Waldrop quotes Holland's frustration with the neoclassical obsession with well-defined mathematical problems:

"'Evolution doesn't care whether problems are well-defined or not.' Adaptative agents are just responding to a reward, he pointed out. They don't have to make assumptions about where the reward is coming from. In fact, that was the whole point of his classifier systems. Algorithmically speaking, these systems were defined with all the rigor you could ask for. And yet they could operate in an environment that was not well defined at all. Since the classifier rules were only hypotheses about the world, not 'facts' they could be mutually contradictory. Moreover, because the system was always testing those hypotheses to find out which ones were useful and led to rewards, it could continue to learn even in the face of crummy, incomplete information — and even while the environment was changing in unexpected ways.

'But its behaviour isn't optimal!' the economists complain, having convinced themselves that a rational agent is one who optimises his 'utility function'.

'Optimal relative to what?' Holland replied. Talk about your ill-defined criterion: in any real environment, the space of possibilities is so huge that there is no way an agent can find the optimum — or even recognise it. and that's before you take into account the fact that the environment might be changing in unforeseen ways."

Hayek gives us the intuition of prices conveying only what market participants deem to be the most important information and actually destroying the rest, and Holland shows how this can be represented with the formalism of complex systems. But note that the EMH forces us to imagine that the information is somehow ***in the market itself***. It is honestly unclear to me whether the EMH even allows for honest or 'rational' disagreement given it implies that the price is 'correct', and all other trading is allegedly 'noise'. By my account (and Hayek's) people can clearly disagree. That's why they trade in the first place; they value the same thing differently. This is not at all mysterious if we realise that engaging with markets requires individuals to 'project' the n-dimensions of their information, heuristics, judgments, and stakes onto the single dimension of price, and that markets do not project the aggregates; they aggregate the projections.

Markets Tend to Leverage Efficiency

So we know that entrepreneurial efforts will tend towards positive feedback loops if successful, which is a fancy way of saying, they will 'grow'. And we know that the diversity of compounding uncertainty in markets for securities linked to these efforts will likely generate substantial volatility. But can we say anything more? Can we expect anything more precise?

It turns out that we can, and here we finally get to Alex Adamou, Ole Peters, and the ergodicity economics research program. It's about time! The goal of the program is to trace the repercussions of a conceptual and algebraic error regarding the proper treatment of 'time' in calculations of 'expectation value' that pervaded mainstream economics over the course of the twentieth century. Interested readers are encouraged to visit the program's website, check out this recent primer in Nature Physics, or just follow Ole and Alex on Twitter, which is where most of the action seems to happen anyway!

First, a down to earth example. Imagine you want a pair of shoes. You can either go to the same shoe store every day for a month, or you can do to every shoe store in town all in one trip. If it turns out there is no difference between these approaches, this system is 'ergodic'. If, as seems more likely, there is a difference, the system is 'non-ergodic'.

Now with more technical detail, the _conceptual and algebraic error _is as follows: imagine some variable that changes over time, subject to some well-defined randomness. Now imagine a system of many such variables, whose

'value' is just the sum of all the values of the variables. Now imagine you want to find the 'average' value of a variable in this system in some pure, undefined sense.

How do you make sense of an 'average' of a system that will be different every time you run it? Well, you could fix the period of time the system runs for, and take the limit of where individual variables get to attained by running the system over and over and over to infinity. Or, you could fix the number of systems (preferably at 'one' for minimal confusion) and take the limit of where individual variables get to attained by running the system further and further into the future, to infinity.

These are called, respectively, the 'ensemble average' and the 'time average', and are easily remembered as the average achieved by taking ***x*** to infinity. 'Ensemble average' is commonly known as 'the expectation' but Peters and Adamou resist this terminology because it has nothing whatsoever to do with the English word 'expectation'. You shouldn't necessarily _expect _the expectation.

Now these values might be the same. This means you can measure one of these even if what you really want is the other. If so, your system is called 'ergodic'. The concept first developed within nineteenth century physics when Ludwig Boltzmann wanted to justify using ensemble averages to model macroscopic quantities such as pressure and temperature in fluids, which are strictly speaking better understood as time averages over bajillions of classically mechanical collisions. If any regular readers of mine exist, they will remember me going through much of this in ***Cargo Cult Math***:

Cargo Cult Math

My point that time around was to go on to say that a great deal of financial modelling uses techniques — most notably expectation values — which would only be appropriate if the corresponding observables were ergodic. But they are not. Almost none of them are, to a degree that is both obvious and scary once you grasp it in its totality: clearly the numbers in finance are causally dependent on one another and take place in a world in which time has a direction.

My point this time around is more cheerful. I want to direct the reader's attention to another of Peters' and Adamou's papers on the topic: ***Leverage Efficiency*** (arXiv link here). This subsection is a whistle-stop tour of what that paper says. The usual disclaimer about not doing it justice absolutely applies. The reader is heartily encouraged to read the paper too.

Imagine a toy model of the price of a stock that obeys geometric Brownian motion with constant drift and with volatility that varies by random draws from a normal distribution. It turns out that the growth rate of the ensemble

average price — i.e. the price averaged over all possible parallel systems — is not the same as the time average growth rate of the price — i.e. the growth rate in a single system taken in the long time limit. Clearly what we care about is the time average, as we don't tend to hold stocks across multiple alternate universes, but rather across time in the actual universe. In particular, in turns out that the ensemble average growth rate is equal to the drift, while the time average growth rate is equal to the drift minus a correction term: the variance over 2.

This becomes very important when we introduce leverage via a riskless asset an investor can hold short. Let's call the model drift of the stock minus the stipulated drift of the non-volatile riskless asset 'the excess growth rate'. Then we can say that the ensemble average growth rate in situations with variable leverage is the growth rate of the riskless asset, plus the leverage multiplied by the excess growth rate. However, the time average has a linked correction, as above. As it is difficult at this point to continue the exposition in English, compare the formulae below:

$$g_e(l) = \mu_{riskless} + l * \mu_{excess}$$

$$g_t(l) = \mu_{riskless} + l * \mu_{excess} - \frac{(l * \sigma)^2}{2}$$

The relevance of the difference is that the latter formula is not monotonic in *l*. In other words, you don't increase your growth rate unboundedly by leveraging up more and more. This might seem intuitively obvious, and, in fact, the intuition likely strikes in exactly the right spot: in reality there is volatility. The more and more levered you are, the more susceptible you are to total wipeout for smaller and smaller swings. In fact, we can go further and observe that we can therefore maximise the growth rate as a function of leverage, implying an objectively optimal leverage for this toy stock:

$$l_{opt} = \frac{\mu_{excess}}{\sigma^2}$$

What might this optimal leverage be in practice? Well, Peters and Adamoupropose the tantalising alternative to the EMH: the ***stochastic markets hypothesis***. As opposed to the EMH's ***price efficiency***, they propose ***leverage efficiency***: it is impossible for a market participant without privileged information to beat the market by applying leverage. In other words, real markets self-organise such that the optimal leverage of 1 is an attractive point for their stochastic properties.

The paper continues in two directions: firstly, Peters and Adamou propose a theoretical argument for feedback systems that ought to be triggered over long enough periods of the theoretical value of optimal leverage in fact deviating from 1, which all ought to pull it back to 1. I will skip this as it is tangential to the point I am building towards, although obviously very interesting in its own right. Secondly, Peters and Adamou gather data from real markets to establish what the optimal leverage would, in fact, have been. I include some screenshots that strongly suggest this approach is quite fruitful:

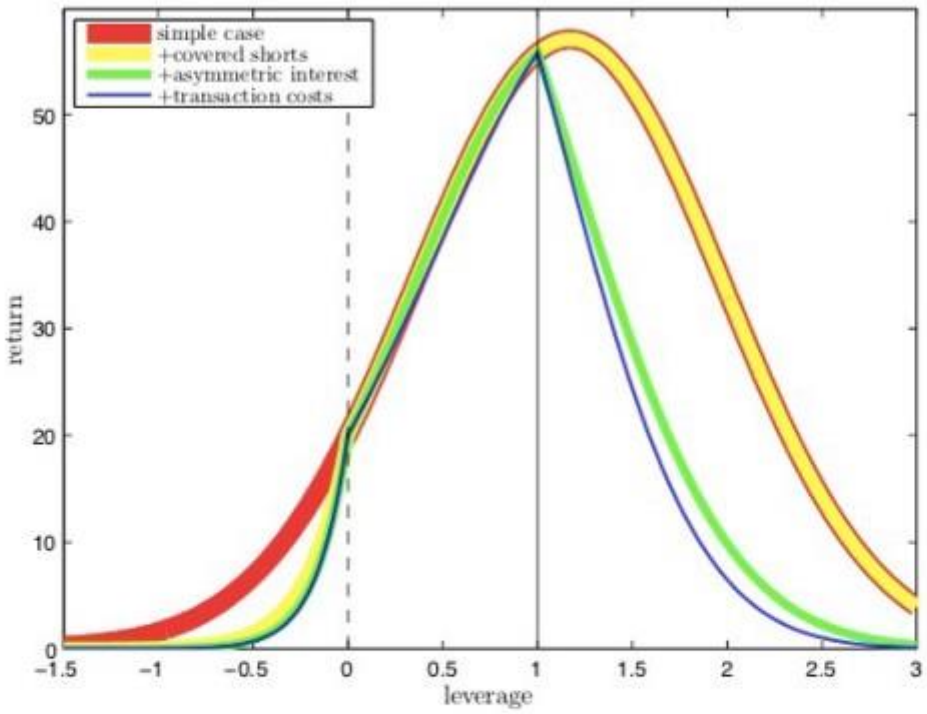
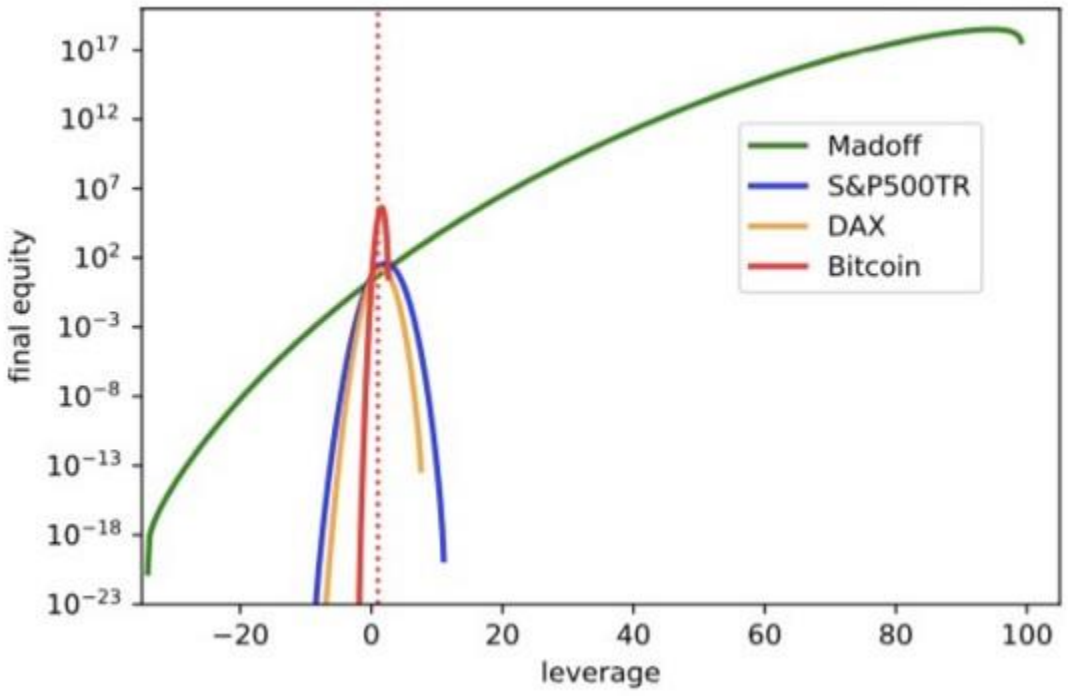


Figure 1: Return-leverage curves for the S&P500.
Total return from a constant-leverage investment in the S&P500, starting 4th August 1955 and ending 10th March 2017, as a function of leverage. Data analyses 1 (red), 2 (yellow), 3 (green), and 4 (blue). For descriptions of the computations, see text, section 4.2.



This chart probably deserves some explanation, but is very satisfying once grasped: as opposed to just the S&P500, above, both the German equity market (DAX) and Bitcoin show pretty much identical behaviours to the S&P500, which Peters and Adamou term "satisfying leverage efficiency". That the Madoff curve is so different, and seems to have no clear maximum, indicates it is likely too good to be true. This is a nice result given that we know Madoff's returns to be fraudulent!

However, what I really want to get to in all of this is a specific interpretation of the SMH; that markets self-organise such that optimal leverage tends to 1 in the long run. If we assume that the excess return of the stock price is generated by real economic activity (ultimately, the consistency of the stock's return on equity) in the long enough run, this would seem to suggest that a certain amount of volatility is actually natural. Were a stock to consistently generate an excess return above that of the riskless asset, investors would lever up to purchase it. This mass act would (reflexively!) cause its volatility to shoot up as the price shoots up, and in the inevitable case of a margin call on these levered investors, volatility would increase further as the stock price comes back down.

This is a somewhat naïve explanation, but the gist is that the lack of volatility in the short run will tend to generate excess volatility in the medium run, such that a natural level is tended to in the long run. Or, markets are stochastically efficient. Readers familiar with the unsuspecting role that 'portfolio insurance' turned out to have played in 1987's Black Monday — the

single biggest daily stock market drop in modern history that seemed to follow no negative news whatsoever — will find all this eerily familiar. Taleb calls Black Monday a prototypical ***Black Swan*** that shaped his formative years as a Wall Street trader. Mandelbrot cites it as sure-fire evidence of power laws and wild randomness in financial markets. It ties together many themes of this essay because, evidently, the information was not in any of the prices. Not in the slightest. I leave it to the reader to mull over what all this implies if interventions in financial markets are targeted solely at reducing volatility as a worthwhile end in itself, the rationale of which makes no mention of growth or leverage. Once again, search for "Raghuram Rajan Jackson Hole" or read about the so-called ***Great Moderation***if unsure where to start. Volatility signals stability, in financial markets and likely well beyond …

All this has a final interesting implication that I teased earlier: the resolution of the so-called 'equity premium puzzle'; that, according to such-and-such behavioural models from the psychological literature, the excess return of equities 'should be' much lower than it really is. Cue the behavioural economists claims of irrational risk aversion, blah blah blah. Peters and Adamou provide an alternative with no reference to human behaviour at all. The difference between the growth rates of the risky (l=1) and riskless (l=0) assets is the excess return minus the volatility correction. If markets are attracted to the point at which leverage efficiency equals 1, then it follows by substituting the definition of the equity risk premium in terms of risky and riskless assets into the equation defining optimal leverage, that the equity premium ought to be attracted to the excess return over 2. Peters and Adamou delightfully write, "***our analysis reveals this to be a very accurate prediction … we regard the consistency of the observed equity premium with the leverage efficiency hypothesis to be a resolution of the equity premium puzzle.***" QED.

I'll note before wrapping up this sub-section that any readers triggered by such terms as ***geometric Brownian motion _and _normal distributions*** needn't be. Peters and Adamou acknowledge that GBM is not realistically either necessary or sufficient as a mechanism for stock price movements. But their argument really only depends on the characteristics of an upward drift and random volatility, both of which_ are_ reasonable to expect. They choose GBM because it is simple to handle, well understood, and prevalent in the literature they criticise, but they also write that,

"for any time-window that includes both positive and negative daily excess returns, regardless of their distribution, a well-defined optimal constant leverage exists in our computations …

Stability arguments, which do not depend on the specific distribution of returns and go beyond the model of geometric Brownian motion, led us to the quantitative prediction that on sufficiently long time scales real optimal

leverage is attracted to 0 ≤ lopt ≤ 1 (or, in the strong form of our hypothesis, to l-opt =1)."

We knew from previous sections that volatility is ***likely***. It will exist to some extent due to the teased-out implications of subjective values and omnipresent uncertainty. But now we know that it is _necessary. _It is not ***noise***, irrationality, panic, etc, around a correct price. It is, at least in part, inevitable reflexive rebalancing of leverage around whatever the price happens to be.

Incompleteness

You can't write ten thousand words on mathematical formalisms outlining the limits of human knowledge without mentioning Gödel's Incompleteness Theorems.

Adaptation and Fractals

As mentioned in the introduction, of all the dissenting work on the EMH, I most recommend, by far, Andrew Lo's ***Adaptive Markets Hypothesis*** — the original paper and the follow-up book- and the various thoughts of Benoit Mandelbrot on fractals in financial markets — strewn across numerous academic papers, but lucidly conveyed in the popular book, ***The (Mis)behaviour of Markets***. I assume familiarity with these works to avoid explaining everything from scratch, so if the reader is unfamiliar, I encourage jumping ahead to the next section.

My main critique of Lo is that he doesn't take uncertainty seriously enough. In covering the academic history surrounding the EMH, he only gives Simon a page or so, and Gigerenzer a paragraph. The key point of failure, in my view, is his treatment of the Ellsberg paradox. Or rather, the fact that he stops his rigorous discussion of uncertainty at this point.

The problem here is that the uncertainty in the Ellsberg paradox is confined to the odds, whereas we know from the previous discussion that the uncertainty in economics exists in the outcomes. This means that the odds aren't just uncertain, they are non-existent. By stopping here, Lo passes off the results of running the experiment that gives rise to the so-called paradox as simply indicating ambiguity aversion, which he presents as a kind of irrational bias — then a segue to behavioural economics. This prevents Lo from exploring the implications of Knightian uncertainty on entrepreneurship and competition, and ultimately gives him little ammunition to take on the EMH directly. In fact, he acknowledges that he never really does — he just proposes something he thinks is better.

That said, I agree that his model is better. Far better! Adaptation is a fascinating concept to employ here. As noted several times, it comes through

very naturally in the complex systems approach. I won't comment on it too much as its roots in evolutionary biology are outside my academic pedigree. But the basic intuition of changing circumstances and responding agents I find rather compelling. As do, it would seem, several thinkers I have already cited. Consider this passage from Kirzner,

"it is necessary to introduce the insight that men learn from their experiences in the market. It is necessary to postulate that out of the mistakes which led market participants to choose less-than-optimal courses of action yesterday, there can be expected to develop systematic changes in expectations concerning ends and means that can generate corresponding alterations in plans."

Also, there is a tradition of referring to heuristics as ***ecologically rational***, and the biological analogy is no coincidence. This passage from Waldrop's _Complexity _on John Holland's conversion to complex systems thinking in his study of genetics is striking in the almost simple obviousness of the comparison drawn to economics (again, not at all a coincidence):

"it bothered Holland that [R.A.] Fisher kept talking about evolution achieving a stable equilibrium — that state in which a given species has attained its optimum size, its optimum sharpness of tooth, its optimum fitness to survive and reproduce. Fisher's argument was essentially the same one that economist use to define economic equilibrium: once a species' fitness is at a maximum, he said, any mutation will lower the fitness … but that did not sound like evolution to me.

… to Holland, evolution and learning seemed much more like — well, a game. In both cases, trying to win enough of what it needed to keep going. In evolution that payoff is literally survival, and a chance for the agent to pass its genes on to the next generation. In learning, the payoff is a reward of some kind, such as food, a pleasant sensation, or emotional fulfilment, but either way, the payoff (or lack of it) gives agents the feedback they need to improve their performance: if they're going to be 'adaptive' at all, they somehow have to keep the strategies that pay off well, and let the others die out."

One thing I especially like about Lo's approach is his idea of 'evolution at the speed of thought', often rhetorical as much as anything else. I think this provides a useful conceptual tool to deal with what I deemed to be the only consistent deficiency in the material I covered on complex systems: Arthur, Holland, et al, seem to me so focused on the comparison to biological evolution, and on shifting the comparative conceptual framework from physics to biology as a whole, that they forget the role of purposeful human beings in all of this. Economic 'mutation' is not random, it is creative, intuitive, judgmental. It happens at the speed of thought because humans think ***on***

purpose. They do not cycle through the space of every thought that can possibly be had until they hit on one that happens to be a business plan.

To put this in a wider context and loop back to previously cited thinkers, I think Arthur is best read alongside Kirzner, and indeed Kirzner is best read alongside Arthur. Particularly in ***The Nature of Technology***, which is otherwise an excellent book, Arthur perfectly grasps ***how _change happens, but not _why***. In ***Competition and Entrepreneurship***, Kirzner perfectly grasps ***why _change happens, but not _how***. Both the why and the how rely, in part, on understanding economic evolution as an essentially human phenomenon, because genes mutate, but humans ***think***.

Mandelbrot's ideas on fractals in finance are iconoclastic, to say the least. Unlike Lo, I see nothing to disagree with, and much that probably went over my head. But given Mandelbrot sets himself the task of demolishing the EMH out of left field, and seemingly succeeds, it is definitely worth grappling with.

The mildly boring part of ***The (Mis)behaviour of Markets _is Mandelbrot showing that, empirically, financial data does not seem to fit the Brownian motion of the random walk hypothesis, and hence the EMH. The really juicy part is his explanation of _why***. To avoid getting into any really tricky mathematics and essentially rewriting his book, I will summarise his argument, again not doing it justice, as, ***this isn't random enough***. More suggestively, ***it is too predictably random***.

Mandelbrot thinks that prices in financial markets are, up to a certain granularity, fractals. If true, this has many fascinating implications, but the most relevant here is that the self-similarity this implies means that any randomness in their fluctuation must be irregular. It should not be possible to ascertain any regularity just by changing the timespan because they look the same on _every _timespan (look! there's 'time' again!) The randomness must itself be pretty random. And that randomness must be random, and so on. There are no genuinely normal distributions in finance, Mandelbrot believes, but rather they all tend towards Cauchy. We could be less hand-wavy about all this and point out instead that while a statistical test on some financial data might suggest the tail of a lognormal distribution, we are really looking at a power law. If parameterized to induce fat enough tails, such a distribution may not have a variance, and if fat enough, not even a mean. (And no, it doesn't have an 'infinite variance' or 'infinite mean' because that is meaningless, but nice try). As Taleb and Mandelbrot both wrote in Fortune,

"In bell-curve finance, the chance of big drops is vanishingly small and is thus ignored. The 1987 stock market crash was, according to such models, something that could happen only once in several billion billion years."

Black swans, amiright?

What does this have to do with 'complex' markets? Mandelbrot doesn't explore this idea, and I may be going out on a limb here, but I think this is almost exactly what you would expect if you thought markets were maximally uncertain, so to speak. If risk were predictable, then it could be hedged against. If it were unpredictable in and of itself, but were distributed predictably, then _that _could be hedged against. And so on and so forth. This all lends itself to a hand-wavy inductive proof by contradiction. We know that nothing can be perfectly hedged because it derives from uncertainty, and uncertainty on uncertainty, and uncertainty on _that _uncertainty, and so on. Financial markets can shift uncertainty around, and selectively parcel it into more and less risky instruments, but uncertainty itself cannot be removed.

Bitcoin

Oh goodness, I guess I have to say something about Bitcoin now, lest I be accused of rickrolling an angry twitter mob into a sermon on armchair economics. Is the halving priced in?

I have no idea. Which is sort of the moral of all of this. You can't predict the uncertain future, but you can bet on it. I'm not sure how you would bet on this exact hypothesis: perhaps a combination of options that pay off if and only if the price goes up (or doesn't go up) by whatever the stock-to-flow model predicts, within some bounds, when it predicts it, within some bounds? Obviously, you could just be long Bitcoin, but then you aren't isolating the essence of this claim, and you can benefit for all sorts of other reasons. If you do either, you'll move the price towards the outcome you are hoping for. But only by having put skin in the game. Also, you could believe something very specific about the halving, but have no way of testing it as you don't believe in stock-to-flow models, or any other valuation model, for that matter. That's the essence of my noncommittal answer above: I shouldn't tell you what I think, I should show you my portfolio, right? Well, I have no 'halving bet' in my portfolio, so I guess I think nothing. Which is what I said :)

Even so, we can still make a few interesting observations that draw on the above discussion. Clearly, the question relies on reflexivity, which is interesting in and of itself. It's only derivatively a question about the fundamentals, and more about the extent to which the market is a well-oiled beauty contest. I don't think I know enough about the actual workings of the Bitcoin market to comment on this. It strikes me that, relative to global equities markets, at least, the range of heuristics that market participants in Bitcoin are using vary wildly from one another. If it makes any sense to say so, they likely have pretty dramatic variance. At the same time, the market itself is probably highly illiquid, relative to what we might be used to. This might suggest the halving ***isn't*** priced in, in the sense that the change in marginal bids and asks at which the market clears that we know is going to happen

dwarfs the capital that is already deployed, including towards solely this essentially reflexive bet. But then again, maybe it doesn't.

Honestly, I just don't know. And if somebody does claim to know, tell them to show you their portfolio.

Conclusion

Value is subjective, which means uncertainty governs all economic phenomena. This creates a complexity that resists equilibria and is constantly changing besides. Within such a system, prices convey the minimal possible information necessary for economic agents to purposefully react. They do so with judgment and heuristics, not 'perfect information', which is nonsensical, as is 'perfect competition' and 'rational expectations'. Prices may pass statistical tests for randomness, but they are not themselves random (although it is plausible that their randomness is random, and that randomness is random, and so on) but rather are unpredictable on the basis of market data alone. They are, however, predictable to the extent that the predictor accurately assesses the future subjective valuations both of economic agents and fellow market participants, and backs up this prediction with staked capital. This act of staking changes the uncertainties at play, rendering any attempt at genuinely scientific analysis futile.
You ***can*** beat the market, it's just really hard, and it depends on understanding_ people_, not data. And it's meaningless if you do it in theory but not practice.

Markets have many characteristics. I suggest they are subjective, uncertain, complex, stochastic, adaptive, fractal, reflexive … — really any clever sounding adjective you like — just not efficient.

Thanks to Nic Carter, Robert Natzler, Alex Adamou, and Sacha Meyers, for edits and contributions.

follow me on Twitter @allenf32 and feel free to contribute to the Allen ideas fund: bc1q8utvneuvn3hf2lm5nvt3dreqenad6hh5sda2sa

Why is Bitcoin so hard for most people to understand?

By plasticman2011 - note - I cannot find this comment or user on YouTube anymore.

Posted February 17, 2020

h/t to nick-bravo on Reddit and Crypto Rothbard and Justin Hanneman for surfacing this post.

Why is Bitcoin so hard for most people to understand?

"The reason it's so hard for most people to understand is that most people don't really understand money. Money isn't wealth. It's an accounting system used to facilitate the exchange of wealth. (The paradox of money is that while everyone wants it, no one actually wants it - they want the stuff they can buy with it!) Many people are put off by the fact that Bitcoins are 'just data'. But that's what ALL money is, information! More precisely, money is a means for credibly conveying information about value given but not yet received (or at least not yet received in a form in which it can directly satisfy a person's wants or needs).

To put it yet another way, money is a ledger. With fiat currencies like the dollar, that ledger is centralized. And that gives the central authority responsible for maintaining that ledger tremendous power, power that history has proven will inevitably be abused. With Bitcoin, the ledger is decentralized. And that means that no one individual or entity has the power to arbitrarily create new units (thereby causing inflation), freeze (or seize) your account, or block a particular payment from being processed. We've had decentralized money before. After all, no one can simply print new gold into existence. And the 'ledger' of gold is distributed because the physical gold itself (the 'accounting entries' in the metaphor) is distributed. But with gold, that decentralization comes at a heavy price (literally). The physical nature of gold makes it hugely inefficient for global transactions.

And this is why bitcoin is important! It is the first currency in the world that is both decentralized and digital. It is more reliably scarce than gold and more private and transactionally efficient than "modern" digital banking. This is why people are excited about bitcoin, it has the potential to completely revolutionize money."

Tweetstorm My Bitcoin Forecast

By Charles Edwards

Posted February 16, 2020

My #Bitcoin Forecast

RocketBitcoin $100K within 5 years

Based on a conservative estimate of Bitcoin's Energy Value, it is likely that $BTC will **10X** within the next 5 years.

A thread forecasting Bitcoin's long-term price using Energy Value.

Approach

Bitcoin's Energy Value has tracked Bitcoin's price for the last 10 years.

Let's use it to forecast price.

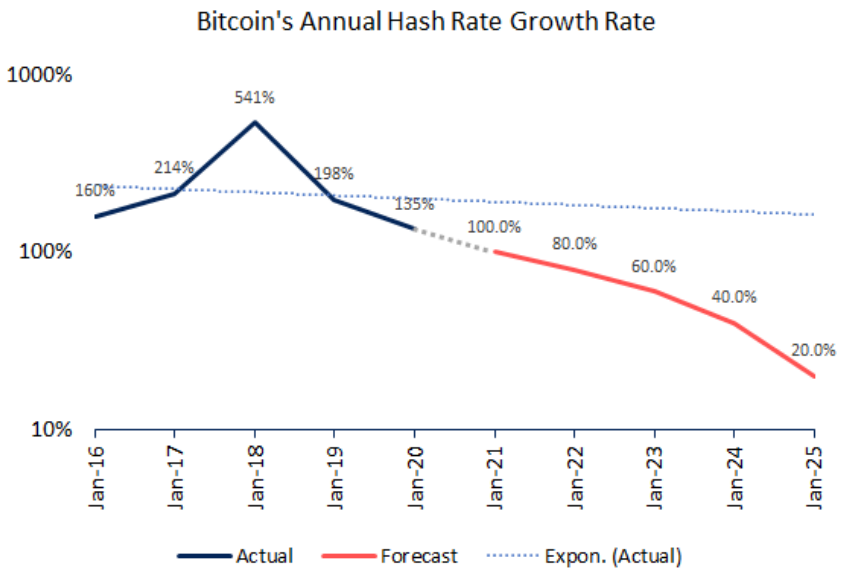
There are only two varying inputs in Energy Value: High voltage signHash Rate GearMining Hardware efficiency

We can forecast each of these to predict BTC's Price.

Hash Rate

Over the last 5yrs, Bitcoin's HR has grown exponentially (linear on a log scale).

Assuming this relationship holds, but allowing for some market saturation, we can estimate that the HR growth rate drops from ~135% p.a. today to ~20% p.a. in 2025.

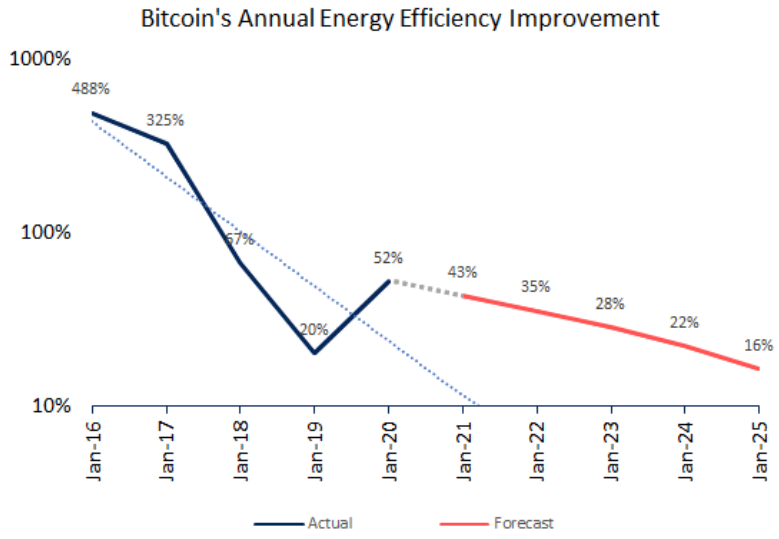


Mining Hardware Efficiency

Energy efficiency has also improved exponentially.

But the annual rate of improvement has fallen from over 400% in 2015 to 50% last year.

I expect this trend of declining improvement will continue.



The Forecast

Combining these estimates for HR and Efficiency, Bitcoin's Energy Value should reach $**100K** by 2025.

- Sanity check: $100K Bitcoin = 1.8T market cap.
- That's just 20% Gold's market cap

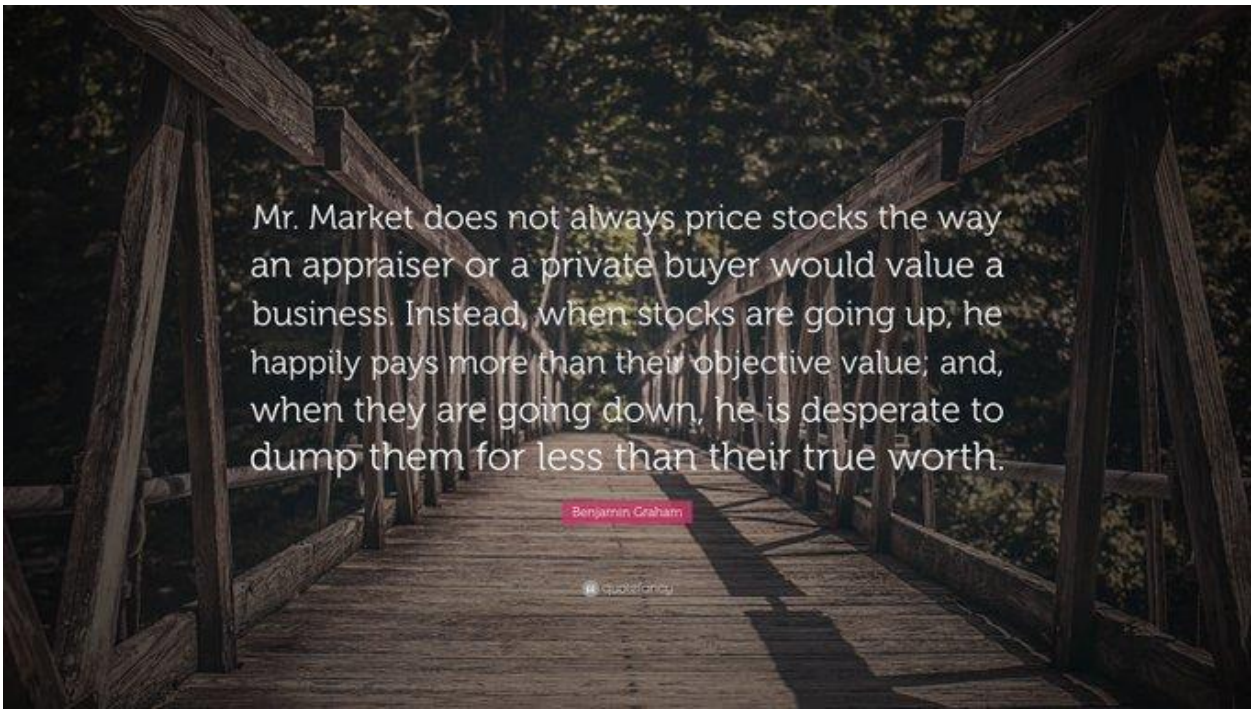
Mr. Market

So far, we have only looked at fair value.

As always, price fluctuates around value.

Bitcoin's Price has deviated to as low as -70% discount to Energy Value, to as high as a +600% premium.

If this cycle repeats, BTC could see prices as high as $600K+.



2X Fair Value?

While 6X fair value is a possibility, excessive swings will become more difficult with time due to the law of large numbers.

For the coming market cycle, I expect 2X fair value is definitely within the realm of possible.

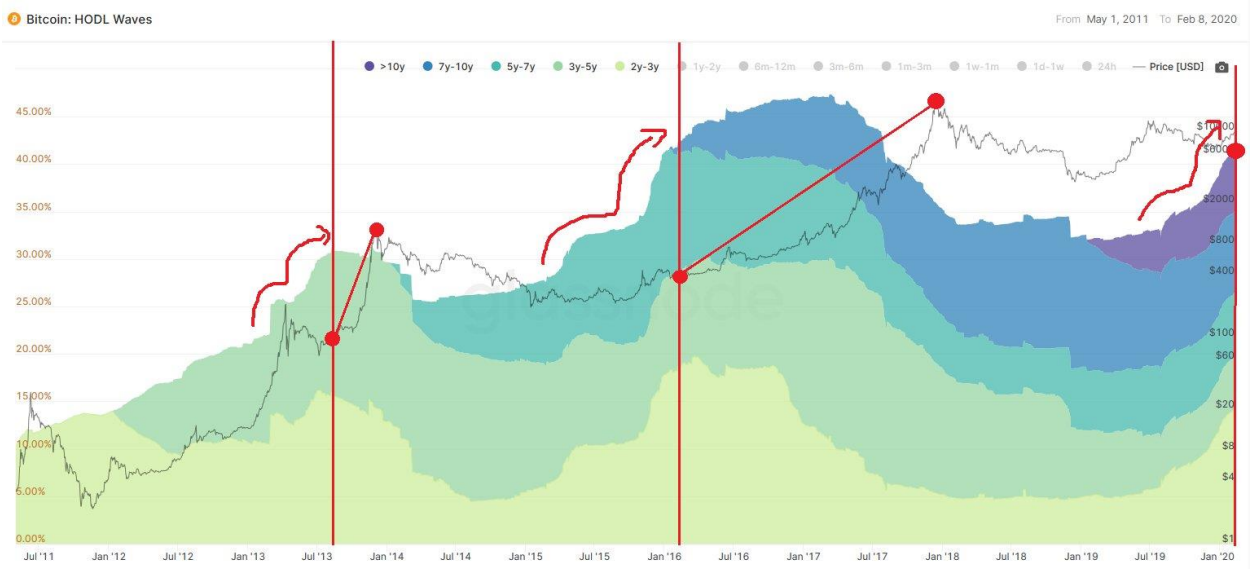
Where will this money come from?

Supply Falling:

- 40% of BTC is locked in wallets that have not moved their coin in >2 yrs.
- Bitcoin Inflation rate to halve in May & again in 4 years.

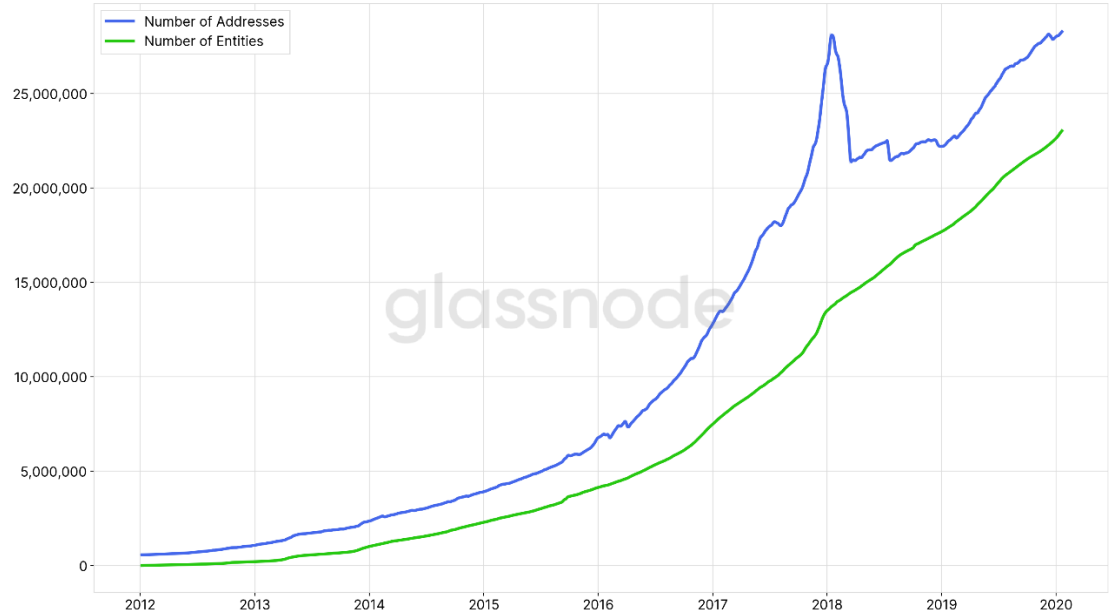
BTC will be the lowest inflation asset ever known to man

Note: HODL Wave patternEyes



Demand growing:

- @Glassnode number of entities ATH
- New onramps: VAR management now possible w/ options. Prev. Bitcoin's volatility blocked access to institutions
- Bitcoin up 100% in 2019, yet no growth in Google searches
- Number of 1+ BTC addresses ATH
- It's a QE hedge



What about electricity?

BTC uses ~0.3% of global elec.

With continued improvements in Energy Efficiency, $100K BTC will likely consume just 3X current energy.

A BTC market cap of $1.8T - 8T (=gold) could consume less than 1.5% of the world's power.

Note 1

Because the HR forecast is below the historic trendline, and the efficiency forecast is above the trendline, both forecasts can be considered historically conservative.

–> $100K Energy Value is conservative.

Note 2

The ASIC chips caused a step-change improvement in Energy Efficiency in 2013/14, dropping Bitcoin's Energy Value.

Should such an event occur again in the next 5 years (eg. Quantum computing), this would cause a 1-for-1 drop in predicted Energy Value.

Note 3

Perhaps the 2 most critical risks to Bitcoin's future are:

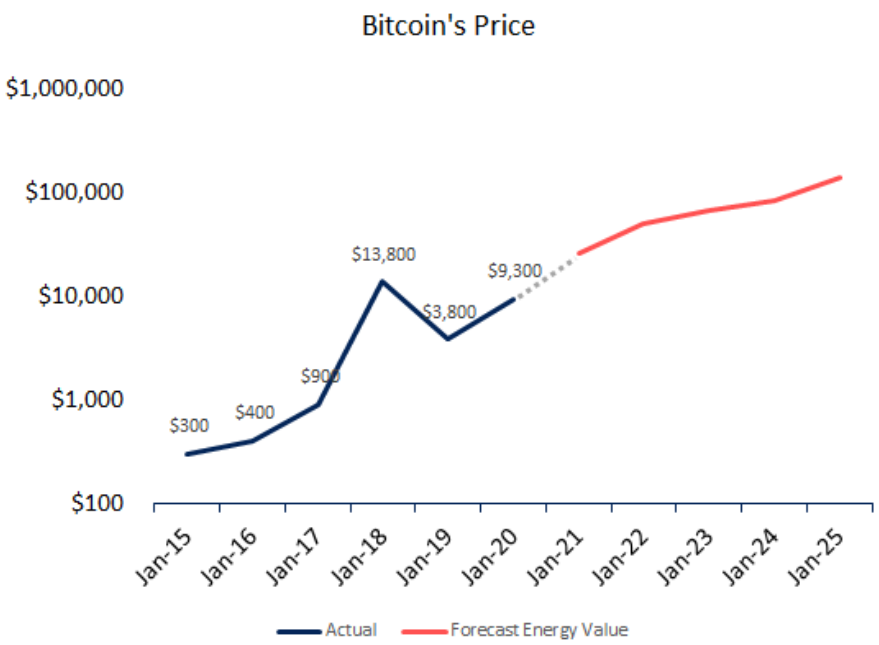
- Quantum Computing: breaking SHA-256 algorithm / accessing lost coins
- Government outlaw: while decreasing with time, major economic outlawing of BTC would curtail mass adoption and Energy Value

Conclusion

This forecast should be considered a "base case". All forecasts are wrong, some are useful.

I expect Bitcoin will hit at least $100,000 within 5yrs.

Based on historic BTC fundamentals, growth rates and market cycles this is a conservative estimate.



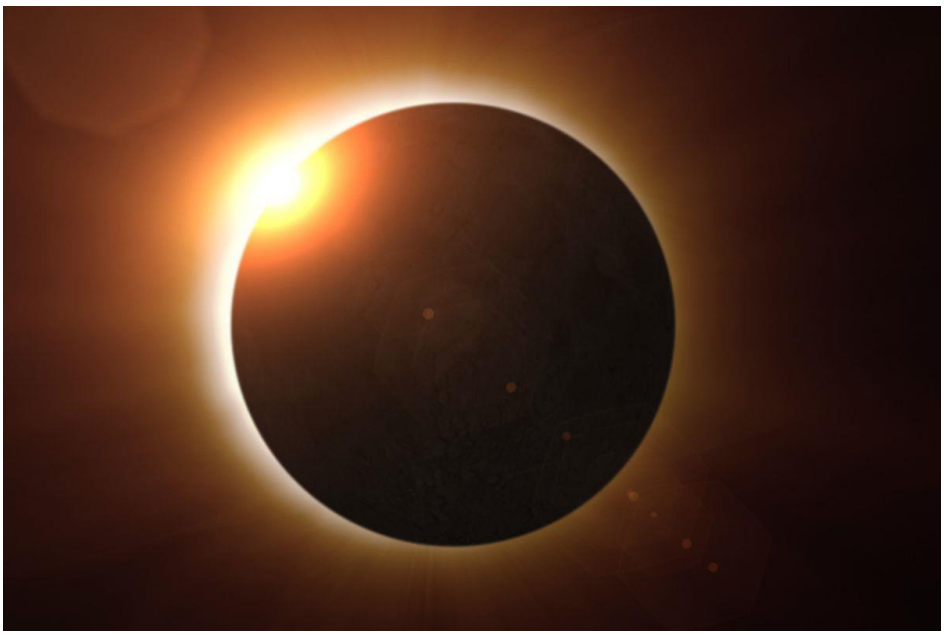
Final Thoughts

Risks considered, Bitcoin is an attractive investment.

Each generation has a “once in a lifetime” opportunity.

Bitcoin was the best performing asset of the last 10yrs.

There are plenty of reasons to think the next 5 will be no different.



Why Bitcoin's volatility can only decrease (but it will take a bit longer)

By acrual

Posted February 19, 2020

At an early stage, hodlers/bitcoin owners was a very small ratio

I know I suck at painting stuff, but I hope I can explain my point better within the next paragraphs.

In the image:

1. **Hodlers are represented by the orange color**. They are users because they understand Bitcoin's extremely low cost of storage / maintenance / deterioration / inflation. They are speculators, but in the very long run, and their speculation is based on the bet that they will hardly ever have to sell their coins.
2. **The green color is the (still) huge number of people who still don't get Bitcoin but own it only as short term speculators (STS)**. They have no problem with selling big amounts of their coins and turn them into fiat. **Hodlers+ STS= Bitcoin owners**
3. The white color is the even larger of people who still don't own Bitcoin (**nocoiners**)

My thesis is that information asymmetry is the result of STS guys speculating short term (typically buying at times of FOMO) and selling (typically at times

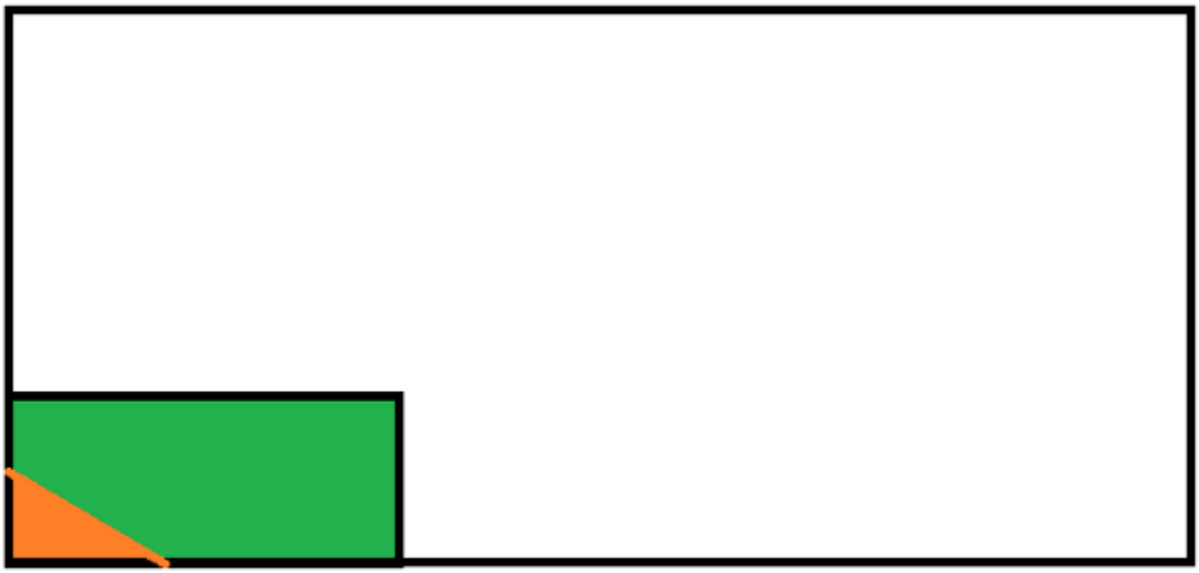
of panic), consequently increasing as such the supply, while hodlers keep their coins with themselves.

The STS (green) guys get in and out very quickly. They completely destabilize the price.

A small number of STS have been becoming over time hodlers (orange), very slowly at first, people that understand that Bitcoin is a long term storage of value. They don't put their coins for sale easily and as a result stabilize the price creating the floor prices we all know and love.

So how do we create the first FOMO and therefore turn nocoiners into STS?

That is the role of halvings, and happens every four years.



Fast forward a few years and Bitcoin understanding grew. The proportion of hodlers among Bitcoin owners is higher.

After the first halving, I think that what we are seeing is a very variable green area that creates the volatility, grows very fast at times of FOMO and decreases very fast at times of panic.

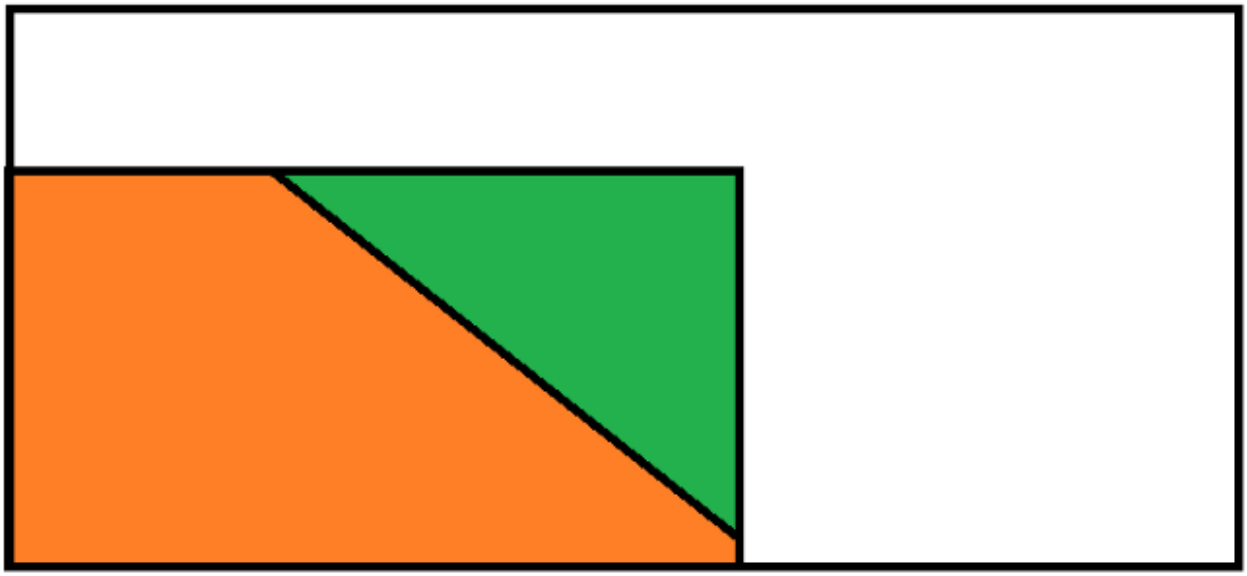
Hodlers on the other hand, grow very slowly, at their own rhythm as Bitcoin understanding grows.

We live in the information age and nowadays good information is way more widespread so I expect soon that the orange area will grow faster than it used to, even if the green one grows very fast too with the next FOMO.

Consequently, with a faster growing orange area of hodlers, I expect the next floor in the price to be way higher than many anticipate, especially given that

the next bull run is going to be way more mainstream than any other in the past.

And if this thesis is confirmed, I believe that we are likely to see a situation like this during the next halving of 2024:



After the next halving of 2024, I expect the proportion of hodlers within the total of Bitcoin owners to be way higher. Volatility should decrease drammatically as a result

My point is, Bitcoin understanding can only grow and Bitcoin understanding can only grow FASTER. FOMO is at some point going to be unbelievable and probably difficult to manage for many. That's why I say that the role of Bitcoin educators is wildly underrated.

Mine are not the prettiest articles (and pictures) but I appreciate a good discussion and your opinions. Please let me know what you think here or in my twitter account :)

No, Concentration Among Miners Isn't Going to Break Bitcoin

By Hasu

Posted February 20, 2020

Part 1

A recent TokenAnalyst report claims a single entity could be in control of around 50 percent of bitcoin's hashrate. The observation is based on the fact that five large mining pools have launched a new cloud mining service as a joint venture.

"In 2020, bitcoin has [...] become a highly centralized system that places an increasing amount of trust in a small number of large entities. Any centralization of bitcoin network hash power should be of concern as it erodes the trustless model of the network," TokenAnalyst, a cryptocurrency research firm, says.

Its strong language is consistent with the folk theorem that bitcoin (BTC) relies on the decentralization of hash power to be secure. But is it also correct?

Concentration is inevitable

It is certainly true that one miner with 100 percent of the hash power would have more control over the network than miners with 10 percent hash power. A majority miner can reorganize the blockchain to double-spend his own transactions or even block any unwanted transactions from making it into the blockchain.

If a majority miner can misbehave and hurt users, does that mean users should try whatever they can to prevent centralization in hash power?

Former Bitcoin Core developer Greg Maxwell sees that as a futile task, given that "[an attack] doesn't even depend on a single person having too much of the hash power. The attack would work just as well if there were 100 people each with an equal amount and a majority of them colluded to dishonestly override the result."

This insight is important because it shows we can not rule out concentration, ever. Miners can always collude with each other and act as a single entity. It would be ludicrous to trust a system that can collapse after a single

conference call – that's all it would take to coordinate the behavior of the largest mining pools. And if miners could make more money by colluding with each other, we should expect that they will.

RATIONALITY MEANS AGENTS DO WHAT IS BEST FOR THEM, EVEN IF THAT MEANS COLLUDING WITH OTHER MINERS TO ATTACK THE SYSTEM.

And – according to Maxwell – this problem might not have a solution because "any mechanism that would let you prevent one party (much less secret collusion) from having too much authority would almost certainly let you just replace mining entirely."

So if the concentration of hash power in proof-of-work (PoW), or of stake in proof-of-stake, is inevitable, why am I not worried?

Concentration is harmless

The answer is that bitcoin's design doesn't assume mining power is widely distributed. It's simply not a requirement. Instead, it only assumes miners are rational, which is something completely different. Rationality means agents do what is best for them, even if that means colluding with other miners to attack the system.

Satoshi addressed this matter directly in the white paper:

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

Let's unpack this a bit. It is the incentive in the form of new coins and transaction fees that motivate the majority to "stay honest." Satoshi realized the only way to prevent a "greedy attacker" from taking over is to make it more profitable to play by the rules than to attack the system.

This is the key to bitcoin's assurances and at the same time the most widely misunderstood aspect of bitcoin's design.

Economist Paul Sztorc even says he is "most comfortable just assuming that everyone is always in perfect collusion with everyone else. Specifically, that all of the hash power is actually owned and operated by one guy, whom we might call 'Mr. Greed.' [...] Why doesn't Mr. Greed double spend, you ask? (He can reorganize the chain at any time.) Well, Mr. Greed prefers to keep all of

the new coins for himself, rather than undermine the system (and the validity of his own wealth)."

I must admit, I was not comfortable with what I perceived bitcoin's security model to be initially. If bitcoin were vulnerable the moment a group of colluding miners obtains 51 percent of hash power, how could we possibly monitor – let alone prevent – this? Moreover, why are smaller forks like [bitcoin cash] BCH and [bitcoin SV] BSV not constantly under attack, given that several individual mining pools in BTC control more hash power than their entire networks?

The dissonance disappeared when I realized that hash power concentration doesn't actually matter. Bitcoin is secure not because it is impossible to attack, but because it is costly to attack.

The real cost of attack

The cost of an attack is directly related to how much hash power the attacker owns. That is the key finding of a paper I released with Curtis and Prestwich in 2019. In a simplified model, we estimated the present value of all mining operations in bitcoin at around 658,800 BTC or $6 billion at current bitcoin prices. (Consequently, 60 percent of hash power is worth around 395,000 BTC or $3.6 billion, and so on.)

The present value of these miners depends on the value of the network because their future profit is exclusively from block rewards. They are priced in bitcoin's native token, BTC. If something happened to bitcoin that would make users lose trust in the system, these 658,800 BTC could lose their value in real terms, incurring a large opportunity cost.

Let's say an attacker with 60 percent hash power decided to attack the network. If the attack depresses the price of bitcoin by only 10 percent, a rather conservative guess, he would lose $360 million in future profit. This is the opportunity cost of his attack.

This number – also called security margin – gives us an idea of how much an attacker has to be able to gain just to break even with his attack. And it does not yet include the ability for the other 40 percent of hash power to push back, or the ability of users to respond with their own nuclear option of changing the PoW algorithm.

The same logic has been replicated in the recent paper "Too Big to Cheat: Mining Pools' Incentives to Double Spend in Blockchain Based Cryptocurrencies" by Savolainen and Soria. The authors conclude that "the historically observed pool concentration does not indicate a higher risk of

double-spending attacks. […] This result demonstrates the well-known economic insight that feasibility does not imply desirability."

Takeaways

Mining concentration is inevitable. Mining concentration is also harmless as attacks on bitcoin incur an opportunity cost that scales with the amount of hash power an attacker controls. An attacker with a lot of hash power would incur a large cost.

As a result, the system ensures miners with more control have a stronger vested interest in its protection as well.

Thanks to their feedback to Su Zhu, Nic Carter, Eric Wall, Mike Co and Loomdart.

Part 2 No, Concentration Among Miners Isn't Going to Break Bitcoin – Part 2

Yesterday I published an op-ed for CoinDesk arguing that *concentration of hashpower is not going to break Bitcoin***. The reason is that miners who have more power in the network also have more to lose in terms of opportunity cost if they destroy the network or otherwise mess with its operations. (The same argument applies to stakers in PoS).** The article spawned many vivid discussions on Twitter, and I went back and forth talking to different people about it all day. Thanks so much for engaging with the article, it's really the best thing a writer can hope for. In this follow-up post, I want to take the time and respond to some excellent questions and counterpoints.

Wouldn't it be better if hashpower was more distributed?

Absolutely. I regret not making that more clear in the article itself, but widely distributed hashpower is strictly better than concentrated hashpower. **Concentrated hashpower just doesn't break the system**. That's a big difference. You can think of Bitcoin having different layers of security guarantees, and as you peel them off, the security of the system degrades but doesn't fall apart immediately. Imagine there are ten miners, each of whom controls ten percent of the hashpower and who never collude with each other, then most attacks are fundamentally impossible. Any attacker would race with a chain that outpaces his own nine to one – a huge uphill battle. That is the best possible scenario for the network. But even if a miner

controlled more hashpower than that, Bitcoin has the nice property that the amount of value a miner has at stake scales linearly with his power in the network. So there is still an incentive to be honest because misbehavior is met with a steep penalty. At least as long as the block reward is sufficiently high. Nic Carter summed that up better than I did:

*"Bitcoin consensus is protected, effectively, by two layers of defense. **#1** it's hard to obtain control at the network level **#2** even if you have control, it's not in your interest to interfere with the network"*

Many people are not aware the #2 layer even exists, and I want to change that. Folk wisdom still says that a network becomes insecure the moment a single party controls >50% hashpower. Of course, we would prefer that hashpower is widely distributed, but there's only so much we can do in that regard without moving away from the idea of a permissionless system.

If hashpower concentration doesn't break Bitcoin, why have smaller systems been attacked?

Ethereum Classic and Bitcoin Gold are two examples from the top 50 of crypto assets that have been attacked before, and more than once respectively. The intuitive reaction may be to blame it on the size difference (Bitcoin is 175x larger than ETC and 985x larger than BTG). In my opinion that is not the primary reason these systems are insecure, but their **lack of forced commitment from miners**. It's no coincidence both systems subscribe to a fallacy called ASIC resistance. The goal behind **ASIC resistance** is to keep mining competitive for hobbyists, which they achieve by using memory-hard hashing algorithms. But the perceived benefits for fairness come with significant downsides for system security. Bitcoin ASICs are so specialized, they are not useful for much else other than mining bitcoin. If Bitcoin ever went away, their market value would drop to zero. Miners in Bitcoin need to own a lot of Bitcoin ASICs, so their balance sheet is **necessarily** tied to the health of the Bitcoin network. GPU miners, on the other hand, are available to hobbyists because they are **not** specialized. Most people have one in their gaming PC and can continue to use them for gaming or mining other GPU coins (or sell them to other gamers or GPU miners). So their value is not tied to the value of a particular coin. Further, because many use cases require GPUs (e.g. machine learning or video processing) there are compute-marketplaces where such general-purpose hardware can be rented. The attacks on ETC and BTG have been executed with such rented hardware, allowing a miner to acquire temporary power over a network without forcing them to enter a long-term commitment to the particular network. So the reason that some smaller coins (but not others) are at risk, is that **miners incur no financial penalty from attacking them** – largely due to the fallacy

of ASIC resistance. (Thanks to Amrit Kumar for this question.) So Bitcoin miners are financially bound to the network, and attacking the network would be self-destructive. But this leaves wiggle room for a third party to force miners to attack the network against their will, or simply confiscate their equipment in a large-scale operation and use it to attack.

By coercing miners, couldn't the Chinese government attack Bitcoin for free?

In practice, I think this is not true because countries, similar to the private sector, **incur an opportunity cost** from attacking Bitcoin. By driving out a profitable industry such as mining, they would **sacrifice future tax revenue**. Bitcoin mining is great for countries with a lot of cheap energy but no way to use it domestically. Previously, aluminum refining has been used for the purpose of de-facto exporting electricity from low-cost countries to high-cost countries. Depending on how a mining crackdown happens, it can also **disrupt faith in local property rights and the rule of law**, which are important drivers of economic prosperity and foreign investment. Finally, no system is secure against an attacker who's willing to incur an unlimited opportunity cost. If the US or China set their mind to destroying Bitcoin, no matter the cost, then there's nothing that can be done about it. We can, however, **make it as painful as possible to destroy Bitcoin** by driving up that cost. That is the strongest deterrent we have. Concentration of hashpower may be inevitable unless we start vetting miners (effectively turning the system into a permissioned one), but this raises the question how Bitcoin with a single miner even differs from a centralized company like Paypal.

Does this "more power, more to lose" argument not equally apply to centralized systems?

Before we start, let me point to the very first answer. We don't want hashpower to be concentrated, it's simply not possible to disprove that concentration exists. Don't assume something you can't prove, at least directionally! The way mining works, any moment now existing miners could reveal that they have been colluding on a secret chain. And the same applies to an entirely new miner, of course. Models that don't consider collusion by miners by capping their maximum hashpower are simply not realistic and offer strictly worse security guarantees than models that do. Though I understand that may not necessarily convince you that the huge amounts of electricity we spend on PoW are "worth it" under that assumption. So let me try a different explanation. I will argue that, even as all hashpower is currently controlled by a single miner, Bitcoin still differs significantly from a system

like Paypal or a commercial bank. So the worst case is not actually as bad as it may seem.

- **Bitcoin is fully auditable with no trust required**. Users can validate that the central miner follows the rules of the network. These validity rules apply to a 100% miner the same way they apply to ten 10% miners. Users can also transparently evaluate the work of that miner. If the miner double-spends or censors transactions, users will be aware of that.
- **Users can exit more easily**. Building on the previous idea, if users are unhappy with the work of the current miner, they can simply fire him by collectively forking to a different PoW algorithm. This is significantly easier to coordinate than collectively switching to a Paypal competitor – which may not even exist. All users have read access to the shared state – the UTXO set – making it really easy to take that state and leave if the need arises. If Paypal failed, and someone starts a new one, you would not get your Paypal balance back.

Governments have less leverage on miners. Now you might respond that in capitalism, it is rarely the companies itself that hurt users – it's usually a result of government intervention, whether via direct regulation or indirect pressure to cut off certain people. And I agree that nation-states are the biggest threat for Bitcoin, as they, in turn, see it as a threat to their monetary and fiscal sovereignty. But nation-states have very different leverage over Paypal or a commercial bank than they have over miners. Let's dissect why:

- **Leverage is inversely correlated to mobility**. Someone who can pick up and walk away can not be coerced. This applies to miners! If miners expect the local policy to turn to worse, they can move to a different country with minimal effort. As a result, their leverage over local policy may actually be bigger than vice versa. We see evidence of that with the rise of "special economic zones" for mining in some countries.
- **The miner can be replaced**. If the local government "disappeared" the miner, that's when the free entry to mining matters, as miners in other countries can simply come online and pick up the slacks. So the government must be aware that any shenanigans it can do by confiscating mining hardware, and possibly using it to attack, can only be done once. Finally, a miner can always be disrupted in an organic way by another miner who makes more profit. For example, if the old miner does not process some transactions (censorship), he creates an

incentive for a new miner to step in a make more money by processing them.

(Thanks to Raphael Auer, figo, and latetot for asking this question.)

Issue #678: The fee market + Jevons Paradox

By Marty Bent

Posted February 20, 2020

Bitcoin is a bold affront to the conventional thinking on monetary policy that has consumed the world for quite some time now.

Yesterday morning, I wrote a Twitter thread on the falling bitcoin subsidy, the fee market, and Jevons Paradox as it pertains to Bitcoin. Below is the first tweet in the thread. I'm going to reproduce the rest of the thread in the body of this issue and elaborate a bit on my thoughts.

Yes, Bitcoin's fee market may be paltry at the moment due to better use of the blockchain as individuals and businesses learn how to use block space more efficiently. I will concede this. However, one needs to look to where the puck is going.

Bitcoin isn't on top of the public's mind like it was in the Fall/Winter of 2017. If number continues to go up like it has consistently done for the last 11 years, this should stoke activity in the fee market as more people are dragged into Bitcoin's gravitational pull.

This is pure demand for block space driven by speculation. Only one aspect that will contribute to the fee market and Bitcoin's long-term security as the block subsidy falls. This is where Jevons Paradox comes into play.

Jevons Paradox "occurs when technological progress increases the efficiency with which a resource is used, but the rate of consumption of that resource rises due to increasing demand."

As the Bitcoin protocol continues to advance technologically (SegWit, Schnorr, Taproot, OpCTV, DLCs, assumeutxo, Erlay, etc.), individuals will be able to do more creative things with their UTXOs, which should stoke demand for UTXOs, driving up fees.

We're only talking about technological innovations at the protocol level at this point. We haven't even mentioned second layer tech like the Lightning Network and Liquid, which also increase the utility of UTXOs.

As these particular second layer solutions mature and become more useful to bitcoin users, this will also stoke demand for UTXOs that can be locked up and leveraged in more unique ways, driving up fees.

On top of this, it would be incredibly naive to think that these will be the only second layer technologies that come to market over time. One needs to factor in solutions that haven't even been thought up yet into their long-term Bitcoin security models.

We haven't even touched on the future dynamics of mining, which provides the long-term security that people are so worried about.

As oil and gas companies continue to wake up and realize they can use all of the FREE gas they are currently wasting on their fields to mine bitcoin, this will severely reduce the price at which your average miner can mine profitably. An externality that many are blind to at the moment.

When you combine all of this, it is incredibly stupid to claim with any sense of authority that Bitcoin's long-term security is at risk. The number of things one can do with a UTXO is increasing at an incredible rate. This utility will drive demand, and create a fee market.

Don't let the haters try to convince you otherwise. These people don't have any vision and lack an understanding of economics. Particularly, Jevons Paradox. Number go up. Bitcoin fixes this. Get over it.

This thread was inspired by the constant nagging and prodding from those outside of Bitcoin, mainly confused Ethereum enthusiasts, who believe Bitcoin's monetary policy is flawed because its security will depend on a healthy fee market one day. Their argument revolves around a perceived

need for a “minimum viable issuance” [read: constant inflation rate] to incentivize miners to mine the chain in lieu of a sufficient block subsidy. This is some very high quality concern trolling that aims to position Ethereum as having a “superior monetary policy” because no one can truly know what will happen once the block subsidy falls below a certain point.

Newsflash, bitcoin was invented to provide the world with a scarce information space that can be used as a sound monetary good. A “minimum viable issuance rate” is against the whole ethos of the protocol and the fight for sound money in the Digital Age. Bitcoin is a bold affront to the conventional thinking on monetary policy that has consumed the world for quite some time now. Those who think constant inflation is necessary are thinking anachronistically. The times are changing, freaks. And this is a good thing.

Uncle Marty will admit it, we don’t have any certainty in regards to what will happen once the block subsidy falls below a certain threshold, and the history of Bitcoin’s fee market is nothing that imbues too much confidence outside of a few days during extreme mania phases.

However, again, this backwards thinking is very short sighted when one takes into consideration all of the technological developments that are being produced that will give UTXOs much more utility (driving up demand and eventually fees) and the fact that Bitcoin is still in its nascent stages. There aren’t enough people in the world who truly understand Bitcoin or the benefits it provides for this fee market to properly mature at the moment. We’re in the “that little mark with the ‘a’ and the ring around” phase of all of this. Probably even earlier.

As the central bankers and politicians of the world continue to erode the confidence of the populaces they rule over, more people will come to value the utility that Bitcoin provides. This will cause more people to use bitcoin and the nature of bitcoin’s scarce information space will force a healthy fee market to develop.

Obviously, this is certainly not a foregone conclusion. Your Uncle Marty does not own a crystal ball that can predict the future. But, this line of reasoning seems very logical to me. The thought of bastardizing the goals Satoshi set out to achieve before a material percentage of the global population is using the network is nauseating to ya boy. Especially when the ideas are being pushed hardest by script kiddies who have failed to deliver on almost every promise they’ve made since the launch of their protocol. Bitcoin works as intended and has done so almost flawlessly for eleven years. I could be wrong, but my gut says this is something we will look back on and laugh at in a few decades.

If the powers that be mess up the system to a certain extent, individuals will seek alternatives. If you build it (Bitcoin), they will come... and a fee market will come with them.

Tweetstorm: On 51% Attacks from a Miner

By Steve Barbour

Posted February 22, 2020

Bitcoin's security properties are amazing. For example, one really great aspect of proof-of-work consensus is that if a 51% attacker decides to orphan blocks from honest miners then the difficulty will adjust downward up to 50%.

This results in a decrease in the cost for honest miners to find blocks, so the honest hashpower that was priced out before is now incentivized to come online, increasing the difficulty for the attacker to maintain 50%+ of total hashpower.

And as soon as the dishonest attacker yields to honest miners the difficulty increases up to 2x, increasing the cost to attack and driving expensive hashpower offline again.

In parallel, if the dishonest attacker also chooses not to include certain transactions in his blocks then fees increase as a result and honest miners who accept the transaction in their block are paid more than the attacker, driving up honest hashpower.

Further, since 50%+ of hashpower gives the majority miner 100% of rewards, then any extra capital spent on maintaining their hashpower beyond 50% is wasted.

And then, of course, there are many incentives for an attacker to play nice rather than censor other miners or merchants. Bitcoin really is beautifully engineered system.

Tweetstorm on Deflation

By Per Bylund

Posted January 26, 2020

Will #deflation be the end for business? Hardly. Deflation is only a problem for businesses in an inflationary economy. Sounds contradictory, but the point is that business is properly operated aimed toward (meeting or creating) the future–not to repeat but to ***leverage*** the past. Entrepreneurs and managers continuously forecast and try to position their businesses with respect to the future market situation. In today's heavily distorted, #inflation-suffering markets, businesses have learned to anticipate that prices will continue to rise: buying (factor, input) prices as well as selling (output) prices. This is more than simply relying on experience, which is a shaky foundation for predicting the future. In present markets, government through central planning of national currencies ***promise*** to ***enforce*** inflation. The policy is to always inflate the currency, and this is the context for business. Thus, should deflation occur, ***despite*** government's attempts to go in the opposite direction, businesses are unprepared to handle it. Because they have not and also should not have considered deflation. Deflation will consequently be hardest on businesses in an inflationary economy. But this is not an argument against deflation per se. Any unhampered market is always deflationary: the purchasing power of wage earners' salaries increases over time while prices fall as a result of competition and innovation. This does not lead to overall failure, as macro-'economists' would have us believe. Instead, businesses learn to deal with this just like they learned to deal with a politically controlled and constantly inflated currency. The problem lies in the government's promise to cause inflation through policy (which is really a hidden tax and makes us all poorer). And the costly uncertainty caused by the monetary and fiscal policy where this promise fails (which also makes us poorer). Without these, business would thrive.

Ladies, Gentlemen, Welcome to Bitcoin Club — Here Are the Rules

By Sylvain Saurel

Posted February 27, 2020

Bitcoin from the Fight Club perspective.

Released in 1999 in cinemas, the film Fight Club marked a whole generation. During the course of the film, the two main characters played by Edward Norton and Brad Pitt create a Fight Club that should allow men to regain their true place in society by allowing them to express their virility which has been scorned for years.

At the launch of the club, Tyler Durden, played by Brad Pitt, reveals to the other participants the 8 rules of the Fight Club.

Being a big fan of this film, I had fun drawing a parallel between it and Bitcoin by defining the essential rules of what constitutes the Bitcoin Club.

Less macho than Fight Club, Bitcoin Club is as open to women as it is to men since the real opponent is the current monetary and financial system we all live under. That is why the first sentence to the newcomers will be :

Ladies, Gentlemen, Welcome to Bitcoin Club. Here are the rules.

Rule #1: You Do Not Reveal What You Own in Bitcoin

Some people love to tell everyone how much money they make. They even go so far as to reveal all the details of what they have in their bank account.

People who flaunt their wealth in front of everyone justify themselves by saying that they have nothing to hide because they earn that money by working hard.

There is nothing wrong with being proud of what one earns. However, this is clearly not the mentality you need to have if you want to be a member of the Bitcoin Club.

To be a member of the Bitcoin Club, you need to embrace its first essential rule, and apply it no matter what:

You must never reveal what you own in Bitcoin to anyone.

Being a true Bitcoiner requires humility in order to be willing to learn more and more about Bitcoin, and money in general.

The humility you develop will cause you to be discreet about what you own in Bitcoin.

Rule #2: You Do Not Reveal What You Own in Bitcoin

By joining the Bitcoin Club, some take the first rule lightly. They get tricked into answering questions about how many Bitcoins they own. This is an unforgivable mistake for any Bitcoin Club member.

Never revealing to anyone what you own in Bitcoin is also a matter of security.

From the moment you reveal what you own in Bitcoin, you can jeopardize your own security.

Bitcoin price is set to rise sharply in the years to come. So it will be tempting for ill-intentioned people trying to steal your Bitcoins.

It would be a shame if you were to miss out on the Bitcoin revolution in the future for breaking these first two Bitcoin Club rules.

In the future, if someone asks you what you own in Bitcoin, you will only have to answer that you are forbidden to say. This is part of the Bitcoin Club rules.

In fact, that is my answer to those who frequently ask me this question when I publish stories online. They take it as a joke and ask me again, but my answer is always the same: I never break these two golden rules of the Bitcoin Club.

I would advise you to do the same.

Rule #3: Someone Yells “Dump”, Stay Cool, Then Say “I HODL”

Bitcoin is relatively young, with only eleven years of existence behind it. Its price is therefore naturally very volatile. It is very common for Bitcoin price to rise or fall by almost 10% in the space of 24 hours.

So you should never panic then letting your emotions take precedence over your behavior with Bitcoin.

When Bitcoin price drops, everyone will start screaming “Dump” on social networks. A FOMO (Fear of Missing Out) feeling can quickly develop. It will

push some people to sell their Bitcoin without even realizing that there is nothing rational about this decision.

You should be aware that Bitcoin price varies greatly over short periods of time. In order to avoid these variations, you need to think long term with Bitcoin.

Bitcoin is here to stay. Its revolution will take time, and it is more interesting to rely on its fundamentals which are excellent rather than frantically looking at its price every 5 minutes.

Whenever the market gets excited and Bitcoin price drops sharply, the best thing to do is to keep a cool head.

Then, all you have to do is say to people who are panicking: “I HODL Bitcoin”.

You should even see these drops in Bitcoin price as an opportunity to buy new Bitcoins that you will HODL for the long run.

Rule #4: Just Bitcoin in Your Portfolio

Joining the Bitcoin Club requires sacrifice. In order to be admitted to this demanding club that wants to accompany the Bitcoin revolution in the best possible way, you will need to have only Bitcoin in your cryptocurrencies portfolio

99 percent of all cryptocurrencies will tend towards zero in the future.

Bitcoin is clearly a hegemonic king, and the cryptocurrency that has the most potential for the future. By focusing on Bitcoin alone, you will take fewer risks.

Many Bitcoin Club members even go so far as to say that other cryptocurrencies are just Sh*t coins. These members are the Bitcoin Maximalists.

I confess that I have already broken this rule by owning other cryptocurrencies, especially Ethereum.

BAT tokens are also often paid to me by people thanking me for the content I publish online. I believe in the Basic Attention Token innovative model, and especially in its Brave Browser which is an excellent alternative to Chrome.

The goal here is always to preserve my online privacy as much as possible by reducing my digital footprint.

Nevertheless, being a member of the Bitcoin Club requires sacrifices as I said before. To remain a full member, you have to make choices.

I’m willing to do these sacrifices because I strongly believe in the Bitcoin revolution.

Rule #5: One Buy After Another

I meet with some people who tell me they are interested in buying Bitcoin but find that buying a whole Bitcoin is too high for their investment budget. My answer is simple:

Bitcoin is divisible up to 8 decimal places. You must take advantage of this.

The current goal is to get 1 BTC in full.

However, if you can't afford it, you have no reason to give up Bitcoin. Quite the contrary!

Many people choose to buy Bitcoin on a regular basis in order to smooth out their costs.

This is a great strategy, and you can follow it by starting to buy just $100 in Bitcoin. Then, little by little, you will increase what you own in Bitcoin as you continue to buy.

With Bitcoin, another essential rule is to be consistent by focusing each time only on your next buy.

By moving forward one buy after another, you will accumulate more and more Bitcoins, which you will take care to keep safe, allowing you to show your faith in Bitcoin by declaring to its opponents: "I HODL Bitcoin".

Rule #6: Not Your Keys, Not Your Bitcoins

People who join the Bitcoin Club are delighted to regain control over what they own by buying Bitcoins. However, they should keep in mind that they only own their Bitcoins as long as they are in possession of the associated private keys.

So rule number 6 of the Bitcoin Club is easy to remember:

"No Your Keys, Not Your Bitcoins"

In the traditional banking system, the bank guarantees the amount you have in fiat money in your account. Your bank is responsible for what you have in fiat money.

If your bank gets hacked and loses millions of dollars, you will get your funds back because the bank is insured against this type of risk.

With Bitcoin, things are totally different from traditional banking system.

First of all, you need to understand that the expression “own Bitcoins” is a shortcut. No one actually owns Bitcoins.

In reality, you own the cryptographic keys to part of the Bitcoin Blockchain. This subtlety is essential to understand what is to come.

If you buy Bitcoins via a trading platform, and then leave your Bitcoins on that trading platform, then the trading platform will have the private keys to your Bitcoins.

The trading platform will then own your Bitcoins.

You will have the same risk of censorship as with the current monetary and financial system.

To really take care of your Bitcoins, you must transfer them immediately to a hardware wallet where you will be able to control the private keys of your Bitcoins.

Therefore, rule number 6 was created primarily to protect the wealth of Bitcoin Club members.

Rule #7: You Will Continue to Buy Bitcoin As Long as You Have To

Like all great disruptive technological revolutions, Bitcoin will take time to fully take hold and achieve its goals. Great successes don’t happen overnight.

You must accompany the progression of Bitcoin like a missionary.

To do so, you must be convinced that Bitcoin will triumph. You must have an unshakeable faith in Bitcoin, and the revolution Bitcoin is building day after day.

If you have true confidence in Bitcoin, you will be able to support it by continuing to buy Bitcoin on a regular basis for as long as it is needed.

Then you will need to HODL Bitcoin for the long term.

This “Buy Bitcoin, Then HODL” strategy will not only support Bitcoin by making it even scarcer, but also by supporting its price, which will attract new entrants to discover this totally revolutionary system.

Rule #8: If This Is Your First Time at Bitcoin Club, You Have to Buy Bitcoins

Within the Bitcoin Club, there is no place for people who say they are interested in Bitcoin, but that don’t make the effort to buy some Bitcoins. If you come to the Bitcoin Club for the first time, you have to buy some Bitcoins.

Don't be one of those people who are going to have regrets 10 years from now saying: "And if I had bought Bitcoin 10 years ago, my life would be different."

The best way to change your future life is to take action now.

If after discovering Bitcoin, you're convinced by its fundamentals and the paradigm shift it brings, you should buy some Bitcoins. This will allow you to put into practice what you have discovered.

This first buy of Bitcoins can even be small: $10 or $100 for example.

The important thing is to get into the Bitcoin system, so that you are familiar with how Bitcoin works. Little by little, you will be able to increase what you own in Bitcoin.

In any case, you should take care to buy Bitcoins only with money you can afford to lose. The goal is to support the Bitcoin revolution in a sustainable way, not to put you in a dangerous financial situation.

Conclusion

Within the Bitcoin Club, the opponent is the current monetary and financial system that has taken control of what the people own. In fact, unlike the Fight Club, the Bitcoin Club welcomes men and women.

Apart from this exception, the rules of Bitcoin Club are similar to those of Fight Club in the sense that to be a member you must have complete faith in Bitcoin, and not let a golden opportunity to change your future life pass you by.

The Bitcoin Club pushes you to take action in order to accompanying Bitcoin. Your main objective is to be among the first beneficiaries of the fairer and freer future world for all that Bitcoin is building.

Disclaimer:

WORDS

Please note that this Journal is provided on the basis that the person who is reading it accepts the following conditions relating to the provision of the same (including on behalf of their respective organization). This Journal does not contain or purport to be, financial promotion(s) of any kind.

This Journal does not contain reference to any of the investment products or services currently offered by the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

Share this journal early and often. Engage the authors and tell them what you think. We sharpen our position through discourse and debate.

DYOR | BTFD | HODL

I hope you enjoy this project. I'm on a mission to archive the great works of Bitcoin thinkers. Onward!

Read **WORDS**

- @_joerodgers