
SOUNDNESS

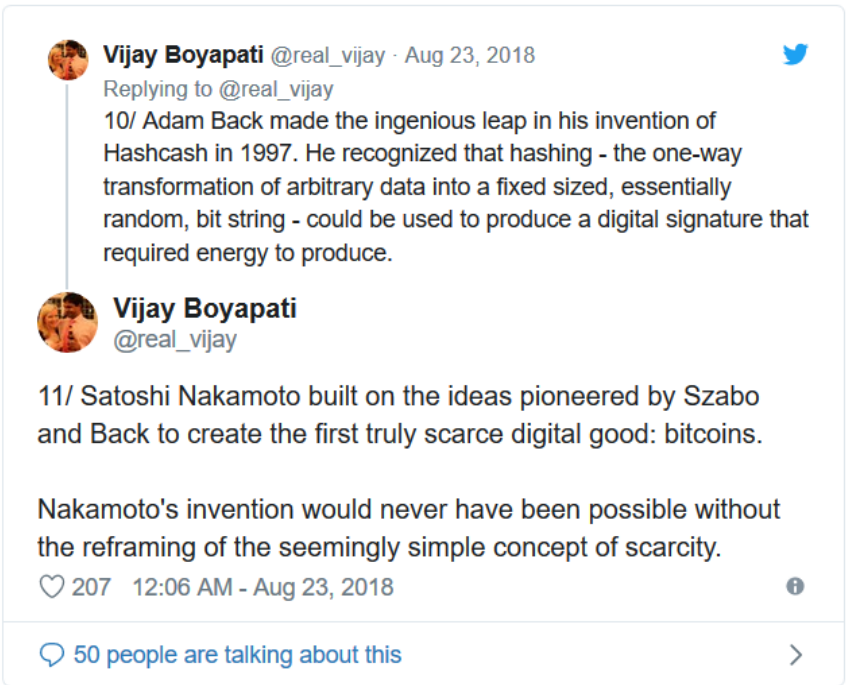
Contents

Tweetstorm: Bitcoin's 10 Year Anniversary as told by Vijay

By Vijay Boyapati

Posted January 2, 2019

1. 10 years ago today, in an unknown location, a mysterious figure whose identity is still unknown, tapped a key on his keyboard, spurring his CPU into action.
   In doing so, Satoshi reified his vision for a decentralized digital cash that he'd published 3 months earlier.
2. The fan in his computer began spinning to keep the CPU, burning from the burden of work it had been given, from overheating.
   The CPU in Satoshi's computer was searching for a special pattern, much like a digital needle in a haystack, that would secure #Bitcoin's first block.
3. Here is that needle:
   0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
   It is the hash of Bitcoin's "Genesis Block", which created the first 50 bitcoins ever to be mined (by a quirk of Bitcoin's protocol these 50 bitcoins can never be spent).
4. With a brilliant leap of imagination, Satoshi had done what no one else had been able to do, and which many thought impossible. He had ingeniously incorporated @adam3us's Hashcash design as a way of securing transactions on a network not controlled by anyone.
5. By burning energy in search of digital needles-in-haystacks, Satoshi's proof-of-work design allowed, for the first time ever, scarcity to be brought to the digital realm:



6. Since the creation of Bitcoin's genesis block on January 3rd, 2009 at 6:15pm (GMT), the Bitcoin network has seen the steady and remarkably reliable creation of blocks for a decade, allowing millions of people to store and transfer value without let or hindrance.
7. While many are obsessed with making price predictions about #Bitcoin in 2019, one thing we can actually predict with high certainty is that Bitcoin blocks will continue to be created approximately every 10 minutes with remarkable reliability.
8. As the Bitcoin network continues to function reliably well into the next decade, there will be near-universal confidence that it will be available forever, much as people believe the Internet is a permanent feature of the modern world.
9. Slowly but inexorably the world's population will come to recognize the benefit of opting out of the status quo monetary order and returning to a world of true individual financial sovereignty.
10. 10 years hence we will look back at the now 20 year old Genesis Block and recognize its creation as the beginning of a new monetary epoch.
    With the tap of a key on his keyboard Satoshi set in motion a sequence of events that set our world financially free.

Addendum: If you're interested in learning more about the genesis block I highly recommend the fantastic 2013 post by the brilliant @SDLerner.

A Primer on Bitcoin Investor Sentiment and Changes in Saving Behavior

By Tuur Demeester, Tamás Blummer, and Michiel Lescrauwaet

Posted on February 20, 2019

In our conversations with institutional investors, we often get asked the question "What is your model to value Bitcoin?". Investors want to know what the fundamental drivers are behind BTC price gyrations, and whether at a given time Bitcoin is overvalued, undervalued, or at fair value. The new measures we suggest here are tools to help with that judgement. We build on work that goes back to 2011, and use the Bitcoin blockchain to extract market information not generally available for traditional commodities.

We suggest two new ways to measure changes in Bitcoin saving behavior:

- **Relative Unrealized Profit/Loss Ratio** (≈investor sentiment)
- **HODLer Position Change** (≈insider buying/selling)

Also introduced is the **Liveliness** measure, which reflects the extent to which a cryptocurrency is meaningfully used by savers.

A History of Bitcoin Valuation Research

Here's an overview of the quantitative approaches we've seen Bitcoin investors take to help them decide what its fair value is at any given time.

- In 2010, Bitcoin users tried calculating the "value" of one Bitcoin by estimating the electricity cost of mining it. However, the usefulness of this was quickly dismissed, as the cost of mining goes up when investors bid up the price of Bitcoin.
- In 2011, early investors came up with the idea of calculating Bitcoin's market cap as a valuation tool, and with the concept of 'Bitcoin Days Destroyed'. The latter was dubbed an "indicator of market health and participation" and it was the first valuation metric that considered the age of addresses. There was also discussion about a "Price over Difficulty" ratio, to determine whether it was better to mine than to buy BTC, and forum threads emerged about how many lost coins there might be.
- In 2012, Trace Mayer suggested the 200 Daily Moving Average of Bitcoin's market capitalization as a value indicator, because it filters out the long-term secular uptrend.
- In 2013, various authors explored the idea that Bitcoin's price is in a long-term parabolic uptrend, and that deviation from that trend line is indicative of over- and under valuation.
- On January 1st, 2014, user gbianchi proposed "Network Value" as the ratio of Bitcoin's address growth and its market capitalization—similar analyses followed later that year.

- In November 2014, developer Jon Ratcliff published his analysis of the blockchain, showing the distribution of bitcoins based on age of last use, and commented "This graph shows … how many bitcoins are actively moving at any one time over time."
- In September 2017, Willy Woo and Chris Burniske published research around the NVT ratio, which was called a "PE Ratio for Bitcoin" as it focused on comparing Bitcoin's on-chain volume with its market cap.
- In March 2018, Dmitry Kalichkin suggested a variation on NVT which he dubbed the 90-day NVT ratio. Two months later introduced the Network Value to Metcalfe ratio (NVM) which was based on Daily Active Addresses.
- In April 2018, Dhruv Bansal updated Ratcliff's work on UTXO age distribution, and suggested the concept of HODL waves. He commented: "It is not possible to make charts such as the one above for traditional asset classes. It's only Bitcoin and other public blockchains that meticulously track these data throughout their whole histories. This enables post-hoc analyses of large-scale market behavior."
- In October 2018, inspired by Pierre Rochard, Nic Carter and Antoine Le Calvez created the Bitcoin "realized cap" which is the aggregate value of the UTXOs priced by their value when they last moved. Soon after, Bitcoin "thermocap" or "accumulated security spend" was suggested, which is the aggregated miner revenues over the entire history of Bitcoin.
- That same month, Murad Mahmudov and David Puell published work on the Bitcoin Market-Value-to-Realized-Value (MVRV).
- In December 2018, Tamás Blummer introduced the concept of Liveliness, which reflects how much a given blockchain is used for meaningful transaction settlement.

Goal: Measure Changes in Saving Behavior

Given that we view Bitcoin's primary use case as censorship resistant store of value (digital gold), and its utility as a payment mechanism as only secondary, our main goal in identifying the components of our valuation toolbox is to find data that specifically reflects changes in *saving* behavior.

Limitations and challenges of existing valuation methodologies

The Bitcoin blockchain records a lot of data, but not all data. It is blind to how many bitcoins are lost. It doesn't know whether a transaction represents a transition from one owner to another (sale), or whether it's simply the same owner moving coins to another address in his control. It also doesn't reflect off-chain transactions—for example it won't show balance transfers from one Bitfinex user to another, or Liquid Sidechain transactions, or Lightning Network transactions.

The limitations of blockchain-recorded information, as well as the commodity nature of cryptocurrencies themselves, have consequences for valuation methodologies:

- With cryptocurrencies, information about real circulating supply is opaque, exchange listing requirements are often extremely loose, and dilution schemes can

be stretched to extremes. Assigning a "**market cap**" to a cryptocurrency (mined coins × token price) doesn't at all create an objective comparison tool—a coin's "market cap" doesn't teach us anything about the commitment of coin holders. To illustrate: a centralized coin with a premined supply of 1 billion tokens and a single recorded sale of one token for $10 would yield a $10 billion market cap, identical to a decentralized coin with a large community of long-term savers. This "market cap" measure is also blind to lost coins, which stretches the comparison with the securities world where the assets are held by transfer agents, making loss a very rare phenomenon.

- The challenge with using the number of active addresses or transaction volumes (e.g. **NVT**, **NVM**) is that these data sources don't allow us to separate behavior that is long-term oriented from behavior that is short term oriented. These measures don't directly differentiate speculators from value investors, and can conceivably be gamed or inflated by moving a large amount of coins back and forth, or by creating a flurry of small on-chain transactions.

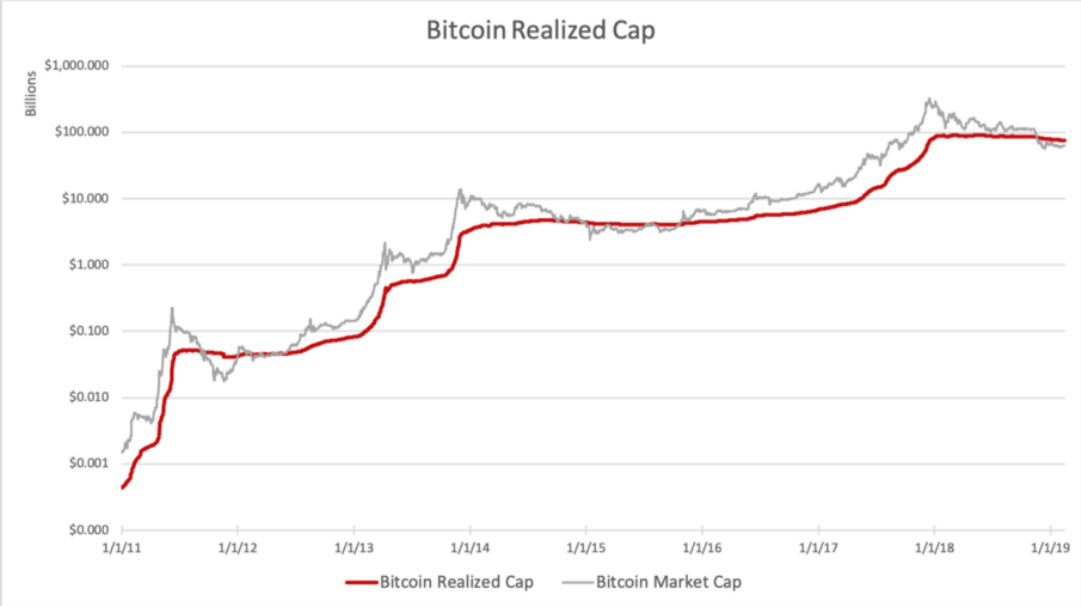
Solution

Our solution is to collect data that places each circulating quantity of Bitcoin *in its historical context*, in the tradition of previous work such as HODL Waves, Realized Cap, and MVRV. We focus on the data provided by *the Bitcoin blockchain*, as this is the ultimate (most secure and final) settlement layer for all its important transactions. By taking the Output Quantities of a block, and combining it with the Recorded Time of that block, we learn more about the behavior of Bitcoin savers.

Relative Unrealized P&L (≈investor sentiment)

Every time a bitcoin moves on the blockchain, its market value is realized. The owner was aware of its value and affirmed his control over it at the point of the move. It doesn't matter if the transaction represents the owner sending the coins to somebody else (a sale or gift), or if it is an act of self-dealing.

If we value every coin at the time it last moved and aggregate these values, we arrive at the "**Realized Capitalization**."



By subtracting the Realized Cap from the Market Cap, we calculate **Unrealized Profit/Loss (P&L)**:

We see that Bitcoin investors in aggregate currently face a significant unrealized loss, which is quite a change if compared with the 2017 huge unrealized profits.

The measure of Unrealized Profit also contains the unrealizable profit of **Lost Coins**. Some coins are certainly lost as they were associated with a provably un-spendable output script, but the majority of lost coins can only be guessed by setting a threshold of inactivity after we consider them Lost.

The measure of Unrealized P&L estimates the total dollar amount of paper profits/losses in Bitcoin, but it does not clearly filter out the relative change that accompanies it. By dividing Unrealized P&L by the Market Cap, we arrive at the **Relative Unrealized P&L**, which can be interpreted as an indicator of investor sentiment:

When a high percentage of Bitcoin's market cap consists of unrealized profits, it can be interpreted that investors are greedy. The ratio drops as prices decline and investors likely become more fearful. When the unrealized gains turn into unrealized losses, we enter the phase of capitulation and apathy. Here's a suggested illustration:

So why does the percentage of Relative Unrealized P&L go up in a bull market? What this indicates is that on average, investors are realizing profits at a slower rate than the growth in the market cap. For the time being, 20% of the market cap consists of 'underwater' holdings—coins that would generate losses if they were sold today.

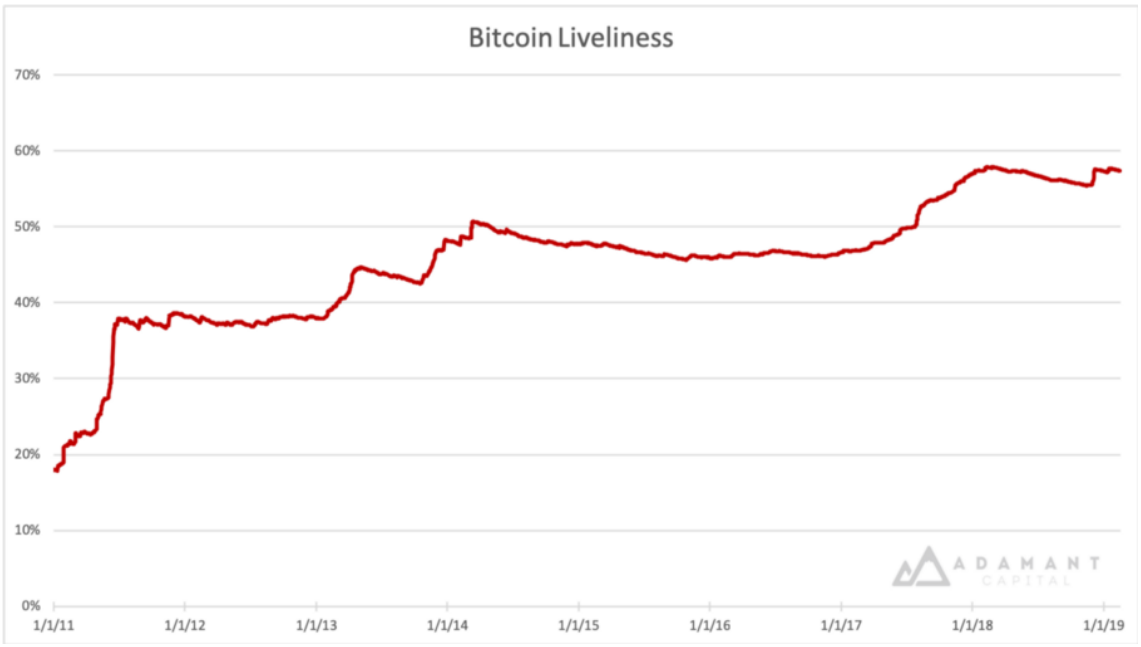
Before we move on to a new suggested valuation tool, **HODLer Net Position Change**, we first need to explain the measure of Bitcoin **Liveliness**.

Liveliness

The idea of old coins moving on the blockchain has always spoken to the imagination of Bitcoin enthusiasts and investors: "What are the 'Bitcoin whales' doing?", "What might Satoshi be up to?", etc. The analytical work mentioned in our historic overview provides investors with information on how Bitcoin savers move coins at any given time. However, the challenge with measures such as HODL waves is that they don't provide us with a clear signal or unambiguous utility. We instead propose *a single measure* that focuses on the coins that move relative to how long they were previously dormant.

What is Liveliness?

Liveliness is a new quantitative measure that gives insights to shifts in saving behavior. The higher the amount of meaningful transaction settlement a blockchain accommodates, the higher its Liveliness.



Liveliness can be defined as the ratio of the sum of Bitcoin Days Destroyed and the sum of all Bitcoin Days Ever Created. (See here for a more detailed breakdown.)

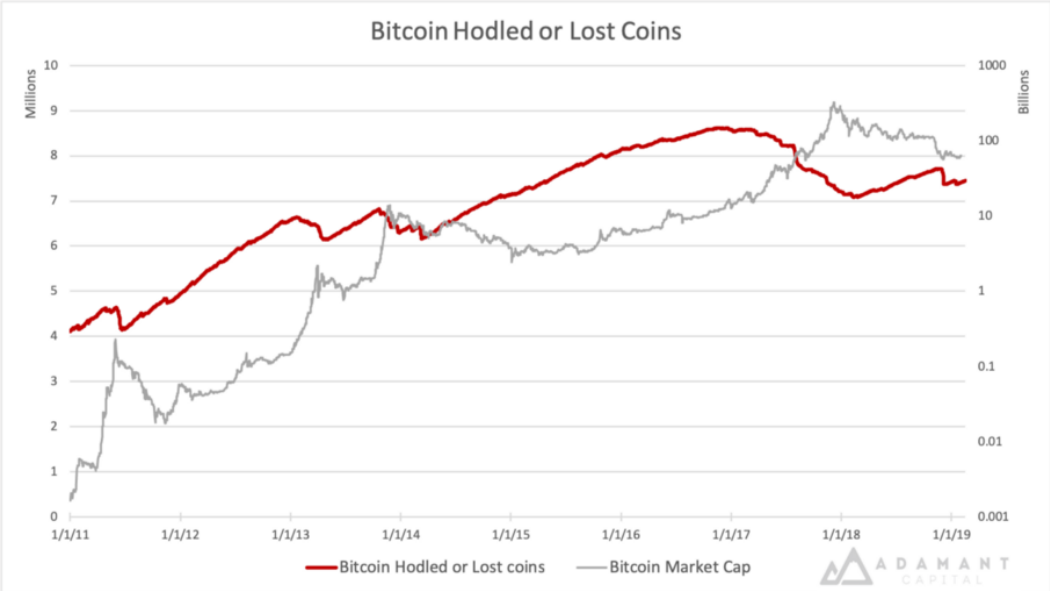
Let's illustrate with a few examples:

- A blockchain that during its lifetime has not yet seen a transaction other than issuance, has a Liveliness of 0%. Likewise, a blockchain where only one recent balance is systematically moved back and forth would produce a very low Liveliness—in other words, this measure is unforgiving for lack of meaningful transactions. Bitcoin has high Liveliness if it facilitates the transfer of large amounts of old coins on a regular basis.
- A blockchain where all the coins move within a single block has at that moment a Liveliness of 100%. A blockchain of two years old with no new block rewards, and where exactly one year ago all coins moved within a single block and no transactions moved since, would have a liveliness of 50%. In other words, the measure fluctuates relative to the total lifespan of the blockchain.
- The total circulating supply also impacts Liveliness: if in the previous example 20% more new coins were created in the year since all the coins were moved, then the Liveliness today would not be 50% but only 40%. So this measure also warns us about blockchains with high inflation/dilution.

Liveliness **can be used to weight market cap if comparing cryptocurrencies**, as it will be close to zero for currencies that have inflated market cap through pre-mined coins or wash trading of the same few units.

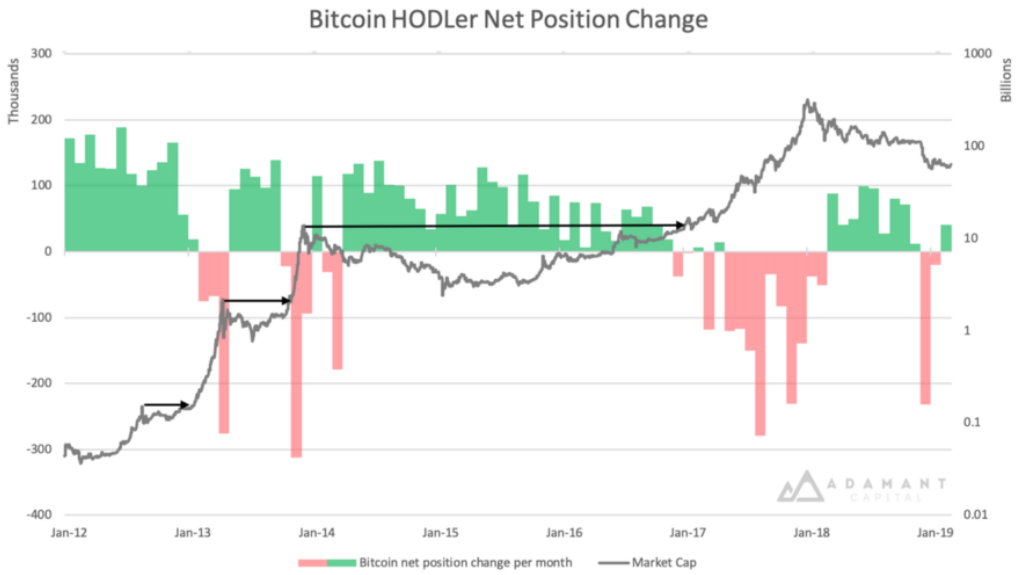
Besides this, Liveliness can also be used as a **foundational tool** from which to derive other insightful time series. One of these metrics is the aggregation of **Lost or HODLed Bitcoins**

and alerts us to moves of large and old stashes. For this purpose, subtract Liveliness from 1 and multiply with the circulating supply at the time.



HODLer Position Change (≈insider buying/selling)

Now that we know the approximate number of coins that are held as a long term investment or are lost, we can approximate the monthly position change among Bitcoin savers. We call this measure **HODLer Net Position Change**. Because it only measures actual moves of coins, our graph naturally excludes lost coins.



We see that significant quantities were cashed out during bull markets of Bitcoin, and net new positions were accumulated by HODLers in bear phases. Net buying seems to switch into net selling once the previous top is reached (cf. arrows on the graph above).

It's important to note that a significant amount of coins are held on Bitcoin exchanges and that mere administrative decisions on their behalf can have a significant impact on measures like HODLer Net Position Change. However, serious effort has been made to de-anonymize exchange addresses, so future analysis should be able to mitigate for "exchange bias."

For example, one anomaly in the graph is the **recent negative position change of meaningful Bitcoin savings** (Dec 2018). While at first sight this is worrisome, we found evidence suggesting that a significant part of the move stems from Coinbase reshuffling around 5% of all BTC in circulation.

Another notable negative position change is the **278,000 BTC net move in August 2017**. This is likely attributable to the Bitcoin Cash hard fork (BCH) of that same month. Every Bitcoin private key gave access to an equivalent amount of BCH as the BTC in that wallet. And so with BCH rallying strongly—at some point reaching over 20% of a BTC—Bitcoin HODLers were incentivized to split the two via on-chain transactions and either buy more BCH and sell their BTC, or vice versa. Given how strong the (flawed) narrative was at the time of BCH being "the real Bitcoin," it's conceivable that many old bitcoins were actually sold. More analysis is needed in this area.

Conclusion

By creating tools that measure changes in saving behavior on the Bitcoin settlement layer, we believe to have meaningfully contributed to the valuation debate. **Relative Unrealized Profit/Loss** in Bitcoin tells us about Mr. Market's emotional state, **HODLer Net Position Change** gives us information about how Bitcoin whales are moving their pieces on the chessboard, and **Liveliness** gives us a powerful tool to meaningfully compare long-term investor activity, as well as a platform for building new valuation measures in this space.

In a follow-up article we will share our take on what these and other measures tell us about Bitcoin's valuation today. Feel free to contact us with questions, or sign up here for future research updates.

Links

- https://bitcointalk.org/index.php?topic=98.20
- https://bitcointalk.org/index.php?topic=98.msg3568#msg3568
- https://bitcoin.stackexchange.com/questions/2047/market-capitalization-over-time
- https://bitcointalk.org/index.php?topic=6172.msg90789#msg90789
- https://bitcointalk.org/index.php?topic=7427.0
- https://bitcoin.stackexchange.com/questions/419/is-there-empirical-data-

about-a-relationship-between-bitcoin-price-and-difficult
- https://bitcointalk.org/index.php?topic=7253.0;all
- https://web.archive.org/web/20130328180243/http://www.runtogold.com/2012/12/during-2012-fiat-currencies-and-gold-collapse-against-bitcoin/
- https://altoidnerd.wordpress.com/2013/11/07/the-bitcoin-price-model-large-time-scale-calculations-of-the-bitcoin-price/
- https://www.reddit.com/r/Bitcoin/comments/21se5e/predictions_of_470_in_march_were_correct_now_btc/
- https://www.tradingview.com/chart/BTCUSD/oc3YX0JB-Bitcoin-Daily-Andrews-Pitchfork-Long-term-view/
- https://youtu.be/K7LQu-eIOO0?t=377
- https://bitcointalk.org/index.php?topic=831547.msg9293359#msg9293359
- https://bitcointalk.org/index.php?topic=394221.0;all
- https://bitcointalk.org/index.php?topic=655792.0
- https://www.reddit.com/r/Bitcoin/comments/21pujs/bitcoin_compared_with_metcalfes_and_zipfs_law/
- https://bitcointalk.org/index.php?topic=68655.msg9059346#msg9059346
- https://www.reddit.com/r/Bitcoin/comments/2n205b/an_area_chart_showing_the_distribution_of/
- https://www.forbes.com/sites/wwoo/2017/09/29/is-bitcoin-in-a-bubble-check-the-nvt-ratio/#40ef77fd6a23
- https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7
- http://charts.woobull.com/bitcoin-nvt-ratio/
- https://medium.com/cryptolab/https-medium-com-kalichkin-rethinking-nvt-ratio-2cf810df0ab0
- https://medium.com/cryptolab/network-value-to-metcalfe-nvm-ratio-fd59ca3add76
- https://blog.unchained-capital.com/bitcoin-data-science-pt-1-hodl-waves-7f3501d53f63
- https://bitcoin.org/en/glossary/unspent-transaction-output
- https://coinmetrics.io/realized-capitalization/
- https://medium.com/@RainDogDance/bitcoin-as-a-novel-market-institution-nic-carter-talk-at-baltic-honeybadger-2018-e085f163b213
- https://blog.goodaudience.com/bitcoin-market-value-to-realized-value-mvrv-ratio-3ebc914dbaee
- https://medium.com/@tamas.blummer/liveliness-of-bitcoin-174001d016da
- https://medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1
- https://blog.unchained-capital.com/bitcoin-data-science-pt-2-the-geology-of-lost-coins-79e5a0dc6d1
- https://coinmarketcap.com/
- https://bitcoin.stackexchange.com/questions/4301/what-is-an-unspent-output
- https://bitcoin.stackexchange.com/questions/7788/what-format-is-the-time-of-a-bitcoin-transaction-stored-in
- https://en.wikipedia.org/wiki/Hodl
- https://medium.com/@tamas.blummer/coinbase-cold-wallet-moves-possible-market-effect-68a09902feab
- https://bitcoinmagazine.com/articles/when-fork-forks-what-you-need-know-bitcoin-cash-goes-war/

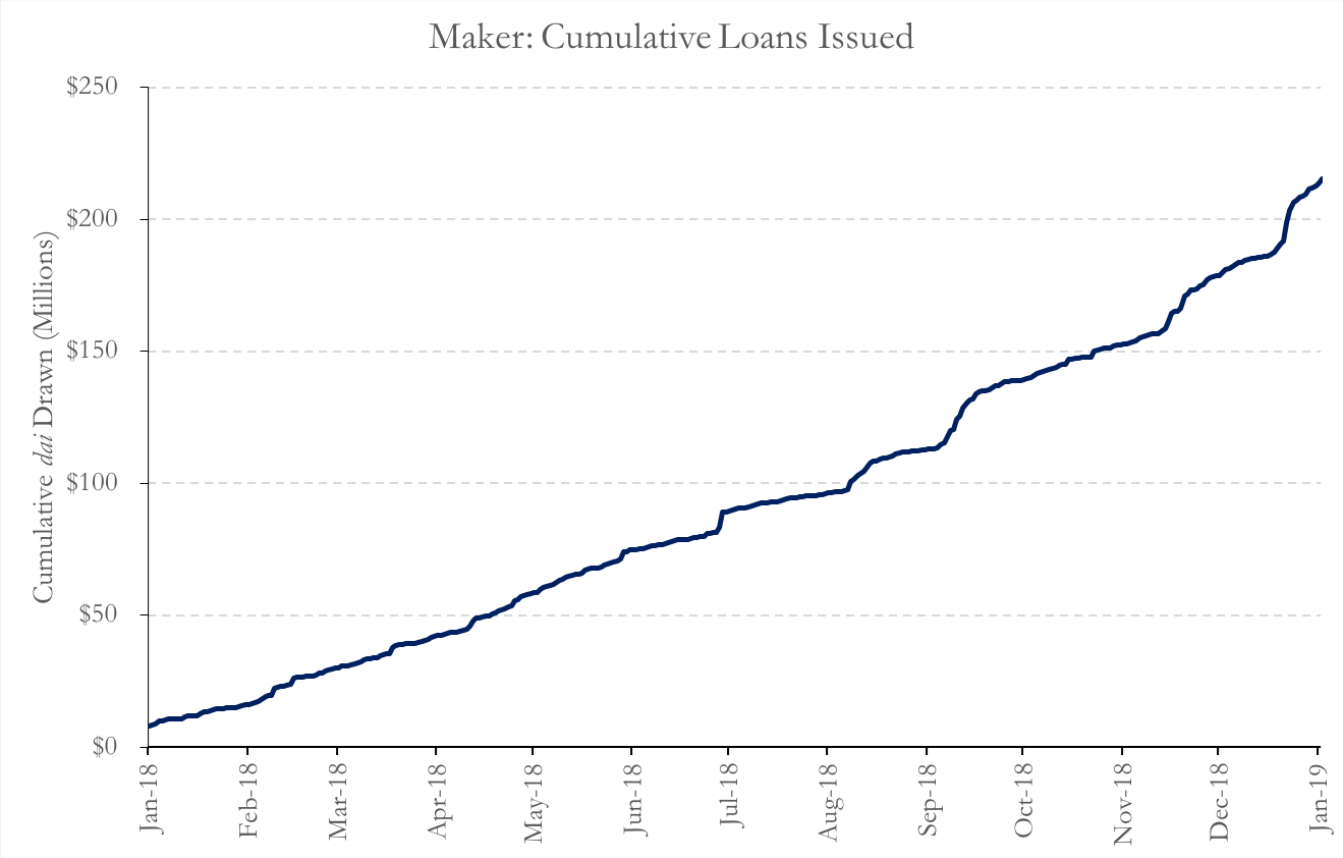
Maker Investment Thesis

By Chris Burniske and Joel Monegro

Posted January 23, 2019

Credit has greased economic wheels for millennia, and Maker is the world's first 100% software-based, community owned and operated credit facility. As a family of smart contracts operating on Ethereum, the system offers secured loans of equal cost to anyone in the world. The by-product of loan generation is *dai*, a stablecoin collateralized using on-chain rules and assets.

In its first year, Maker issued roughly $200 million in loans, with over $70 million currently outstanding (Figure 1). For some perspective, it took Lending Club five years to originate $250 million in loans [1].



Data from Digital Asset Research (DAR)

To get a loan, borrowers first lock ETH through an Ethereum transaction [2], creating a *collateralized debt position* (CDP). They are then able to issue themselves a dai-denominated loan against the posted collateral. The maximum amount of dai that users can issue themselves depends on the loan parameters set by MKR holders. Currently, the

loan must remain under 2/3 the value of the locked collateral (i.e., $3 of collateral allows for $2 of dai to be issued to the borrower). The newly-created dai can then be exchanged for any of the assets it trades against (including BTC, ETH, USDC and USDT), which can be used to purchase other goods and services.

If the borrower's collateral drops in value such that the loan outstanding becomes greater than 2/3 the value of the collateral (that is, if the loan becomes less than 150% collateralized [3]), then some of the borrower's collateral is automatically sold to repurchase dai and partially pay down the loan. Self-interested agents called *keepers* do the work of enforcing this *liquidation ratio*, and in some months have made $200-300K in nearly risk-free profit from their efforts. The supply of dai expands as users create loans, and contracts as loans are paid down or liquidated.

Having principal at risk incentivizes borrowers to be responsible about their debts. Proper risk management combined with a lean protocol as the facilitator, instead of a profit-seeking company, leads to a lower cost of credit for all. The cost of a loan has ranged from 0.5% - 2.5% per year (called a *stability fee*), placing Maker's credit facility at 1/10th the cost of secured loans offered by traditional financial institutions [4].

The stability fee must be paid with the second cryptoasset of the system, MKR, which is subsequently destroyed, making it a deflationary asset from its starting supply of 1,000,000 units. The more loans that are created and redeemed, the more MKR's supply will deflate. This burning mechanism helps create token value similar to how equity buy-back programs can drive share prices in traditional companies.

But MKR holders don't get something for nothing: they must govern the system by voting for the parameters around loans, such as collateralization ratios, types, and fees. While they stand to benefit from a MKR supply that deflates as loans are redeemed, they also stand to lose if any loan becomes undercollateralized. Should collateral values fall such that not enough value is left to cover the loan (i.e., the loan is less than 103% collateralized), then new MKR would automatically be created and sold in order to to buy back dai and pay down the toxic loan. MKR holders would then be diluted for having set parameters that allowed for such an event to occur.

The permissionless creation and circulation of dai positions it as an important unit of account within other decentralized finance applications. It is already being used by a rich ecosystem of centralized and decentralized applications, such as Ripio, Wyre, Compound and Nexo, with many more integrations in the works.

While there are valid concerns about the dangers of "permissionless credit creation," MakerDAO's *auditable code & collateral* and *direct consequences for operators* solves two principal-agent problems that have historically plagued the behavior of credit facilities.

First, credit facilities consistently run into trust issues due to the (relative) opacity of their operations and centrally held collateral. By contrast, if anyone is suspicious of Maker's integrity, they can inspect all code (operations) and collateral of the system, anytime,

anywhere. Transparency enables remediation before a crisis in confidence, making for a more resilient system.

Second, direct consequences for operators and holders of MKR disincentivize risky management. As we witnessed in the 2008 Financial Crisis, many of the actors that enabled an over-extension of credit were not directly punished for their actions, and many were even able to extract billions in bonuses from the government bailouts. In Maker, if the system fails, all capital holders are diluted equally, with no room to walk away enriched.

Maker's open, low-fee service provides fair access to credit for everyone. Today, such access is only available to those already in the best financial position, while the rest are subject to wealth-eroding, high fee loans. Maker's solution serves crypto-geeks and investors right now, but we believe is a critical step towards a more equal economic opportunity future.

Footnotes:

1. In a future report, we'll share a full set of stats on Maker adoption. Some may object to the LendingClub comparison, which we agree is not apples to apples, but we provide it for perspective nonetheless.
2. While ETH is currently the only collateral accepted, Maker is moving to a multi-collateral model soon.
3. Some will complain that a 150% collateralization requirement is capital inefficient and will impede Maker's broader adoption. As the volatility of cryptoassets drop, and more kinds of collateral can be used, the volatility of the value securing the loans will drop as well, allowing more capital efficient parameters to be set. Beyond these simple mechanics, the Maker team has a variety of other ideas for how to make the system more capital efficient over time. Right now, as one of the few venues where cryptoassets can be used as collateral for loans, Maker is not focused on optimizing, but instead enabling.
4. As mentioned in Footnote 3, Maker loans are currently over-collateralized, which is a cost due to the time value of money. The other cost to keep in mind is if a loan becomes under-collateralized, the liquidation process incurs a 13% liquidation penalty.

Links

- https://makerdao.com/en/
- https://coinmarketcap.com/currencies/dai/
- https://www.digitalassetresearch.com/
- https://coinmarketcap.com/currencies/maker/
- https://coinmarketcap.com/currencies/dai/#markets
- https://www.reddit.com/r/MakerDAO/comments/8efk5q/faq_possibly_everything_you_ever_wanted_to_know/
- https://medium.com/@mikeraymcdonald/single-collateral-dai-9-months-in-review-b9d9fbe45ab

- https://www.nerdwallet.com/blog/loans/secured-personal-loans-lenders/
- https://vote.makerdao.com/
- https://medium.com/makerdao/makerdao-partners-with-ripio-to-bring-dai-to-south-america-via-fiat-on-off-ramp-e22ac71a210d
- https://medium.com/makerdao/makerdao-and-wyre-give-businesses-immediate-access-to-dai-stablecoin-in-over-thirty-countries-4fe94957c730
- https://app.compound.finance/?fbclid=IwAR1yBqcpanBEP58-ZR-XVCw7Amp7W40xYfQSDB7IbIdRpCZBLNQba9xvdOs#Markets
- https://medium.com/nexo/earn-interest-and-protect-your-stablecoins-with-nexos-1-to-1-conversion-guarantee-dbdefa8a8152
- https://www.investopedia.com/terms/p/principal-agent-problem.asp
- https://www.nytimes.com/2009/07/31/business/31pay.html
- https://medium.com/makerdao/the-road-to-mainnet-release-21931d47f857

Tweetstorm: Power and Money

By Saifedean Ammous

Posted February 17, 2019

Fiat money allows wars with no real cost to governments, which makes detestable bloodthirsty chickenhawk scum like @MaxBoot & @BillKristol, who've never faced costs for their warmongering, the perfect "foreign policy experts".

> ***Why Are These Professional War Peddlers Still Around?*** *Pundits like Max Boot and Bill Kristol got everything after 9/11 wrong but are still considered "experts." https://www.theamericanconservative.com/articles/why-are-these-professional-war-peddlers-still-around-tucker-carlson-max-boot-bill-kristol/*

In 2003 Wolfowitz told Congress the Iraq war would be practically costless.
It turned out to cost more than $2Trillion.
With hard money Wolfowitz would have had to raise the $2T BEFORE war.
With easy money, he can get his carnage on & leave taxpayers footing the bill for decades

Wolfowitz was not alone. Richard Perle, Lawrence Lindsay, Kenneth Pollack, Glenn Hubbard, Ari Fleischer, Donald Rumsfeld, & Mitchell Daniels all lied about the expected cost of war. They all got paid handsomely for it; never had to pay back a dime.

> ***Who Said the War Would Pay for Itself? They Did!*** *Unwise words from the "experts" who promised a cost-free war. https://www.thenation.com/article/who-said-war-would-pay-itself-they-did/*

Modern "intellectuals", who are government propaganda parrots, think this is just how war works. I urge you to read Hoppe's Democracy The God That Failed for an explanation of how war functioned under governments forced to be responsible by hard money: riosmauricio.com/wp-content/upl…

Under hard money, governments had to finance their operations from their citizens, which made wars possible when necessary but bankrupted governments that engaged in unnecessary war. War was limited & contained to expensive armies kings were careful to not decimate needlessly.

Under hard money, governments fought till they ran out of their own money.
Under easy money, governments can fight until they completely consume the value of all the money held by their people.
This is why the century of central banking was the century of total war.

Whatever you think of the retarded Keynesian economics used to justify government control of money, you need to come to terms with the fact that the most horrific criminals of history have all operated with easy government-controlled money, as discussed in The Bitcoin Standard:

> It is no coincidence that when recounting the most horrific tyrants of history, one finds that every single one of them operated a system of government-issued money which was constantly inflated to finance government operation. There is a very good reason that Vladimir Lenin, Joseph Stalin, Mao Ze Dong, Adolf Hitler, Maximilien Robespierre, Pol Pot, Benito Mussolini, Kim Jong Il, and many other notorious criminals all ruled in periods of unsound government-issued money which they could print at will to finance their genocidal and totalitarian megalomania. It is the same reason that the same societies which birthed these mass murderers did not produce anyone close to their level of criminality when living under sound monetary systems which required governments to tax before they spent. None of these monsters ever repealed sound money in order to fund their mass murder. The destruction of sound money had come before, hailed with wonderful feel-good stories involving children, education, worker liberation, and national pride. But once sound money was destroyed, it became very easy for these criminals to take over power and take command of all of their society's resources by increasing the supply of unsound money.

This is why bitcoin matters, and this is of course the point that critics of bitcoin miss. What better technology do you have for castrating scum like Kristol & Wolfowitz & preventing their sociopathic minds from capturing government money & causing millions of deaths?

Bitcoin's real cost is in hardware & electricity needed to run the network. Fiat's real cost is the hundreds of millions of deaths financed by government made omnipotent by inflation. Which do you find more expensive? Which would you rather pay in the twenty-first century?

Bitcoin might end up consuming half the world's electricity, but if it prevents one war, that would be the best bargain humanity ever got.
Bitcoin might be the most important application of electricity. Can you think of a better use for electricity than neutering mass murderers?

Cryptocurrency: The Canary in the Coal Mine

What Crypto Can Tell Us About Macro Markets in 2019

By Jill Carlson

Posted January 1, 2019

Over the last quarter, the market has rejected risk assets across the board in a sudden reversal of the year's trend. The S&P 500 erased its 9% gain over a matter of weeks in October. The Nasdaq index retraced from an 18% gain to end the year down 5%.

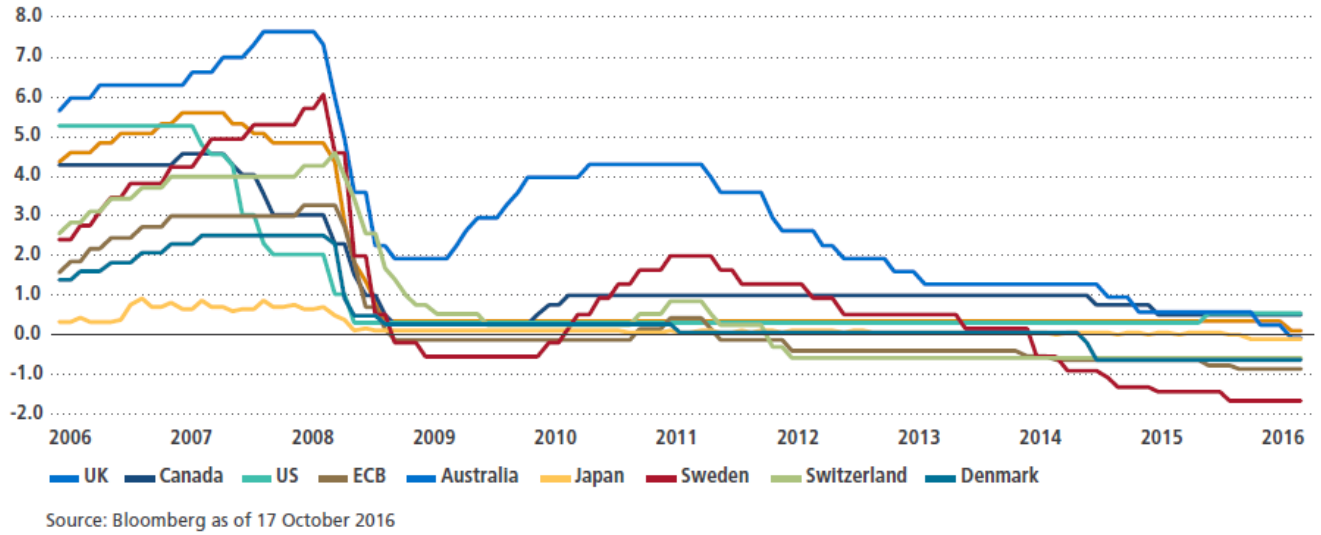
But no market has felt more pain recently than that of cryptocurrencies. The aggregate market cap of cryptocurrencies, which topped out at $830 billion last January, has since crumbled to $130 billion. Much of this unwind has occurred only in the last two months, with the crypto market as a whole getting marked down over 40% quarter-to-date.

The cryptocurrency market is admittedly miniscule relative to other asset classes. Cryptocurrency (no matter how big the drawdown) is unlikely to have any impact on broader markets any time soon. Bitcoin has demonstrated no substantial correlation to any other asset, whether equities or gold. Nonetheless, what has been happening with this nascent asset class over the last year may reveal some important macro trends.

Two years ago, at the end of 2016, the cryptocurrency market stood at $15 billion in value. Trading volumes across all cryptocurrencies hovered in the double-digit millions. What led to the asymptotic spike in prices over the course of 2017? While it may be possible to point to certain headlines and technology developments as catalysts, most would probably dismiss the phenomenon as a speculative bubble. They may not be wrong in this characterization, but they may also miss the macro context in which all of this occurred.

We have seen many search for yield trades play out over the last 8 years. With central banks around the world pumping liquidity into the economy, traditionally risky assets have seen their premiums sucked out of them. Emerging markets stocks, bonds, and currencies have benefited from this trend. High beta equities, most notably in the tech sector, have boomed with the FAANG stocks leading the way. This trend has also driven money further out along the risk spectrum into alternative asset classes, ranging from art to cars to venture capital.

FIGURE 1: GLOBAL CENTRAL BANK RATES



Source: Bloomberg as of 17 October 2016

With rates like these, who needs hedges? *Image from Pimco's 2016 Negative Interest Rate Report.* https://global.pimco.com/en-gbl/resources/education/investing-in-a-negative-interest-rate-world

The cryptocurrency boom of 2017 may have been the illogical conclusion of this global search for yield. It certainly followed this trend, starting as money poured into the relatively lower beta cryptocurrencies (like bitcoin and ethereum). Over time capital found its way into brand new assets as well, the products of initial coin offerings (ICOs) into which investors dumped an estimated $20 billion in the last year and a half, often with little in the way of investor rights or protections. Talk about "risk on"…

But the story has changed since then. If you bought bitcoin at the peak last December and sold today you would be realizing an 80+% loss. Many of bitcoin's brethren, including many ICOs, have performed far worse with some cryptocurrencies getting marked down 95+% this year. The last major legs lower of this correction in October and November have coincided with the broader market sell off.

Perhaps cryptocurrency, the last mover on the way up, is the leading indicator of a broader market fall. If the cryptocurrency boom of 2017 was partly the result of the longest expansionary period the economy has seen in a century, perhaps the bursting crypto bubble of 2018 is the canary in the coal mine that the search for yield has run its course.

The recent downturn across asset classes has been blamed on a global growth slowdown, rising interest rates, and continued political uncertainty. Whether this plays out in 2019 remains to be seen, but if it does, it will manifest first as capital leaves what it perceives to be the riskiest assets.

Quantum Narratives

The rise and fall of crypto narratives

By Dan Held

Posted January 22, 2019

Quantum Superposition

If you like audiobooks, I've done a voiceover of this article which is available to listen to on Soundcloud and YouTube.

In 1935, scientists wrote an article called "The EPR Paradox" which described the strange situation of quantum superpositions, in which systems can exist in multiple states corresponding to different outcomes simultaneously. In effect, the paper argued that there wasn't only one but in fact multiple "true" realities. Each of these realities would remain valid until they were interacted with or observed by the external world. At that time, the superposition collapses into one of the possible states.

To better visualize this idea, Austrian physicist Erwin Schrödinger proposed a thought experiment that would eventually become ingrained in our culture. Imagine a cat in a box with a flask of poison, a radioactive material, and a monitor that will smash the flask and release the poison if a single atom decays. After a while, quantum theory dictates that the cat is simultaneously dead and alive at the same time. It is only once we open the box to observe the cat to be either dead or alive that the multiple states cease to be simultaneously true. It is our actions that determine, ultimately, which reality prevails.

(The above and below section was largely borrowed from @nlw's article titled "Schrödinger's Securities: Regulation & The Quantum State Of Crypto")

Narratives

Nobody can know everything. The complexity of society is irreducible. We cling to mental models that satisfy our thirst for understanding a given phenomenon, and stick to groups who identify with similar narratives.

Beliefs are not only shaped by reality; narratives define it. In any social arena, there's a never-ending battle to tell what's happening, why is it happening, and what is happening next. Controlling narratives is particularly powerful. These narratives constitute the fabric of the world around us: government, religion, culture, and finance all exist simply because we believe in it (and provides value for those who believe in it).

Investors invest in or against narratives; builders build directionally towards narratives; commentators race to associate themselves with the dominant narratives or, alternatively, to be the contrarian positioning against the conventional wisdom.

Market narratives are marketing. The incentives to push a narrative can be financial, like an investor sharing a view of the world that would just so happen to benefit them if more people were to agree with them and invest accordingly. In this way, narratives are attempts at self-fulfilling prophecy. Incentives can also be even simpler, however, such as the desire for status and community relevance.

The fact that narratives are marketing is not a bad or malicious thing. Indeed, there is value in an emerging industry enabling a space where people can discuss narratives they see trending.

This is especially true in the crypto space, in which content from investors and builders today has an outsized influence on market sentiment relative to neutral third-party research firms or data-driven journalism. Again, this is not in and of itself a problem. It is a good thing to get live insights into how operators see things. Moreover, the independent, data-driven research/journalist side of the market is catching up quickly which is accelerating the critical analysis of these narratives.

Cambrian Explosion of Crypto Narratives

During the Cambrian explosion more than half a billion years ago, the variety of life on Earth burgeoned dramatically. While most species that came about eventually went extinct in a series of mass extinction events, we still have this relatively short period of profligate experimentation to thank for the variety of life we experience around us now. In other words, the truly bizarre creatures that roamed the planet then were side-effects of Nature showing off its capacity for variegated expression of lifeforms, before settling into a somewhat more sensible pattern.

In an analogous vein, the dotcom bubble was an extinction event that wiped out exuberant companies, but fundamentally sound ideas survived, a large variety of which are to be found today (ex: Amazon).

In the crypto world, we have WhopperCoins, Putincoins, Bitcoin Cash, Bitconnect, and a string of other tokens/cryptocurrencies that were created during the last bubble. In the long-run, many shall die out—much like the numerous species that kicked the bucket at the end of the Cambrian explosion. Only the fittest shall survive.

> "Jostling for narratives can be seen as an evolutionary battle to compose the doctrines most likely to attract the next wave of adherents. Coin prices amplify this mess. Market cycles–especially up-cycles–appear to pick winning narratives, leading to sudden increases in evangelism and waves of new adherents. And when the market swings the other way, a new narrative gains steam and steals adherents."—*Tony Sheng*

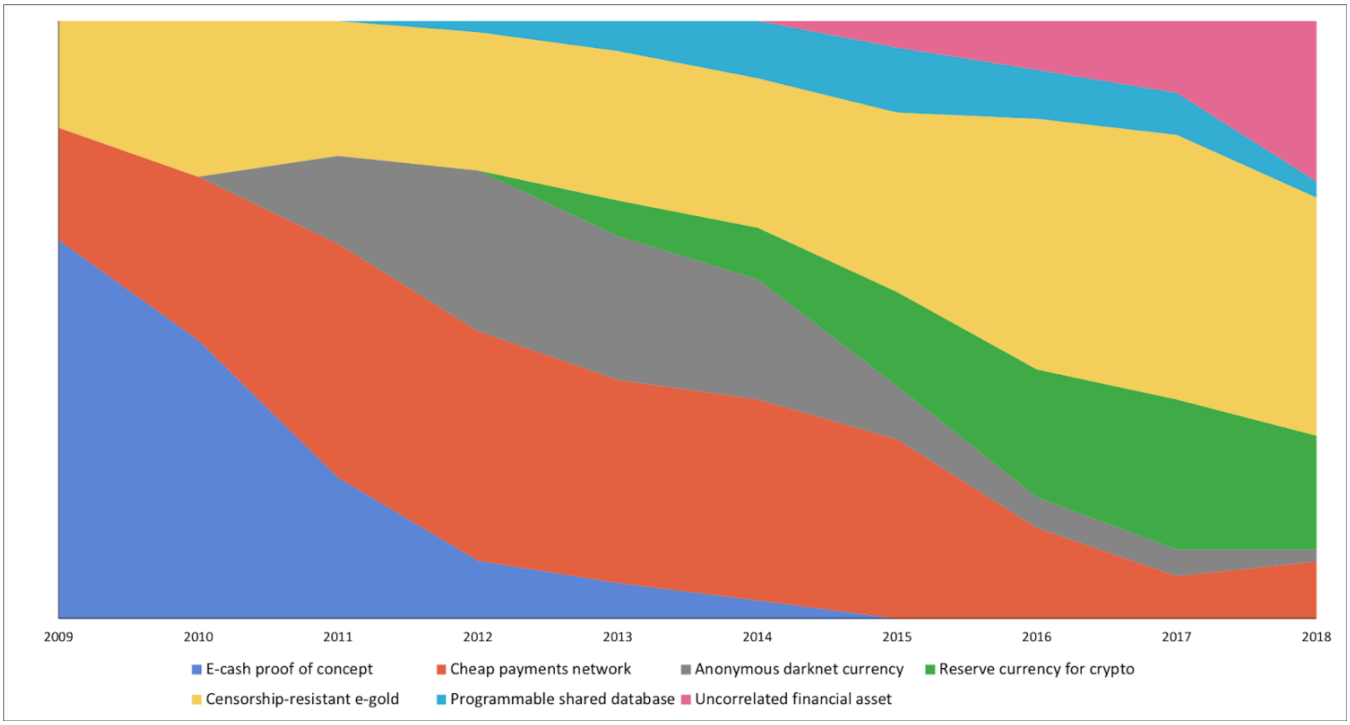
Which crypto narratives are gaining steam tomorrow? How will that change next month or year (or 10)? What are prospective catalysts that could change the dominant narratives of today? How does this differ globally?

Bitcoin and Ethereum, the two most popular cryptocurrencies, have had many narratives fade in and out of popularity over the years. In the below sections are two charts which visualize the ebb and flow of these different narratives for both cryptocurrencies.

Before you read further, I must note an important differentiation. Bitcoin's narrative of SoV/Gold 2.0 was present from day one, has Protocol Market Fit (PMF), has held off competing narratives, has been delivered on, and remains the dominant narrative today. There is persistence of the original intent.

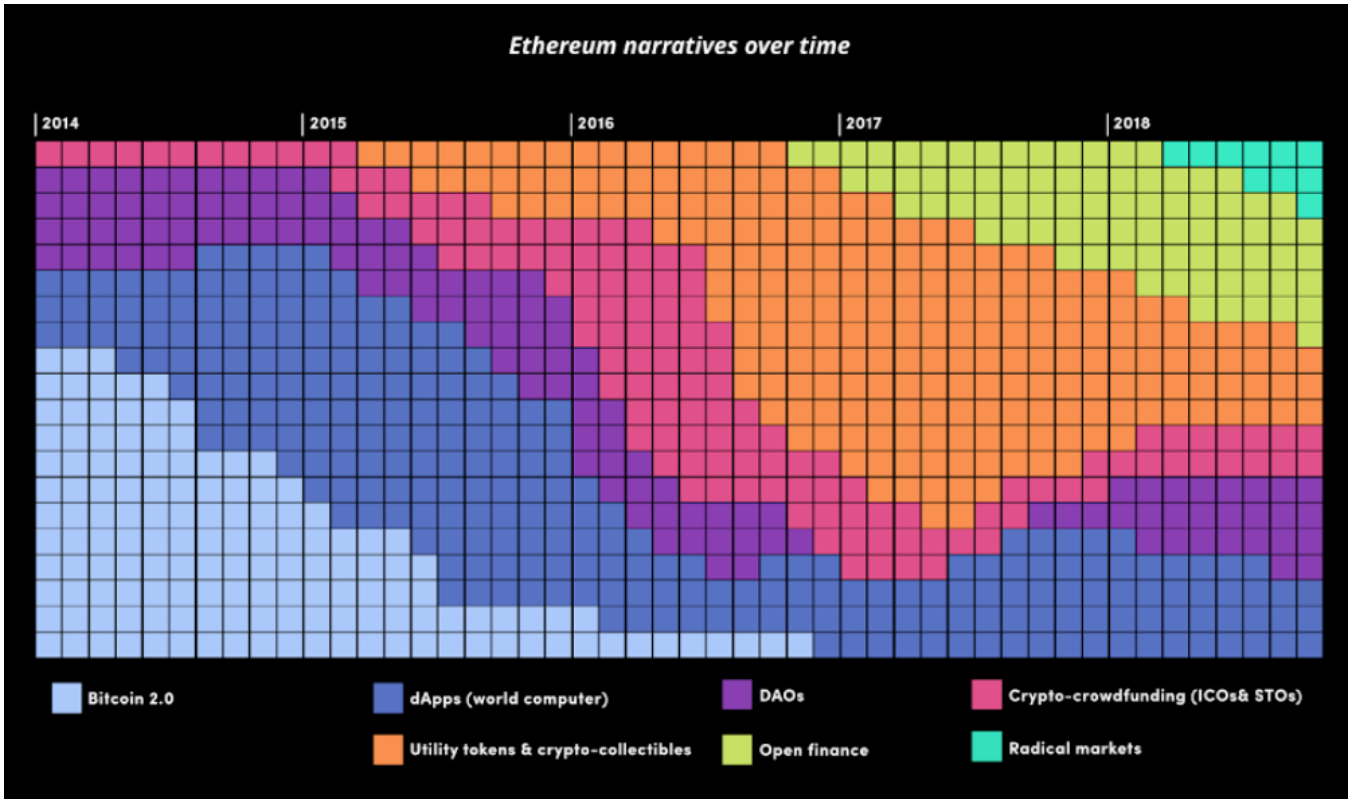
While the Ethereum community has endorsed radical changes/pivots, trying to find narrative fit (PMF), even so far as to recently claim a SoV narrative. The Ethereum leadership team is more willing to embrace alternations to the core objective of the protocol in their search for PMF (world computer, dapps, crowdfunding, nonfungibles, open finance, radical markets).

Bitcoin Narratives



https://medium.com/@nic__carter/visions-of-bitcoin-4b7b7cbcd24c

Ethereum Narratives



https://tokeneconomy.co/visions-of-ether-590858bf848e

Only the antifragile narratives will survive

When something is "antifragile" it gains strength as a result of volatility, stressors, or shocks (originally coined by Nassim Nicholas Taleb)

> "Every criticism Bitcoin survives makes it stronger." — Jimmy Song

Crypto-communities seek for newish narratives or adapt current ones as an exercise of collective strengthening. They also do so to combat critique by isolating some of its premises. **Since there is no objectively correct monetary premium, promoting the superior attributes of a monetary good is more effective than for regular goods, whose value is ultimately anchored to cash flow or use-demand**. The religious fervor of participants in the Bitcoin market can be observed in various online forums where owners actively promote the benefits of Bitcoin and the wealth that can be made by investing in it. In observing the Bitcoin market, Leigh Drogen comments:

> "You recognize this as a religion—a story we all tell each other and agree upon. Religion is the adoption curve we ought to be thinking about. It's almost perfect—as soon as someone gets in, they tell everyone and go out evangelizing. Then their friends get in and they start evangelizing.

> While the comparison to religion may give Bitcoin an aura of irrational faith, **it is entirely rational for the individual owner to evangelize for a superior monetary good and for society as a whole to standardize on it**. Money acts as the foundation for all trade and savings, so the adoption of a superior form of money has **tremendous multiplicative benefits to wealth creation for all members of a society**."

Fiat currency, similarly, is faith based. Per wikipedia:

> **"**Fiat money is a currency **without intrinsic value** that has been established as money, often by government regulation. Fiat money does not have use value, and has value only because a government maintains its value, or **because parties engaging in exchange agree on its value**."

US dollars reinforce the faith with "In God We Trust"

> "Gold's simplicity is a great feature. But Bitcoin is likewise the simplest cryptocurrency. You can explain the intuitions behind Bitcoin to any captive high schooler who has a basic grasp of probability and a moderate attention span. To the digital native of the future, Bitcoin wallets will probably seem more natural than vaults full of useless metals painstakingly drilled out of the earth." — Haseeb Qureshi

> "Stable ideologies allow communities to thrive. A simple example in religion is the Christian tenet that "there is one true god". This belief strengthens the religion because it weakens membership in competing religions. Communities with unstable ideologies will eventually collapse. **The very ideology that justifies the existence of Bitcoin Cash, also justifies the use of chain splits to settle any disagreements within the community. It's easy to see that this ideology, that a hard forked minority chain can be a legitimate successor to the original chain, is completely unstable.** It is thus reasonable to conclude that Bitcoin Cash will face a never-ending threat where its community members threaten to split off permanently from the main chain." — *Kay Kurokawa*

This was prophetic. Due to fragmented ideology, Bitcoin Cash (also known as the altcoin "bcash") ultimately split into two chains late last year and the price collapsed.

Wave Function Collapse

In quantum mechanics, "wave function collapse" occurs when the superposition of several states appears to reduce to a single state due to interaction with the external world; this is called an "observation." Narratives can persist in the multiple states for quite some time, until the moment when it comes under critical observation.

Narrative wave function collapses only when we believe that everyone else believes the critical observation (common knowledge). That's what changes behavior. And when that transition to common knowledge happens, behavior changes fast.

The classic example of this is the fable of The Emperor's New Clothes. Two weavers who promise an emperor a new suit of clothes that they say is invisible to those who are unfit for their positions, stupid, or incompetent—while in reality, they make no clothes at all, making everyone believe the clothes are invisible to them. When the emperor parades before his subjects in his new "clothes", no one dares to say that they do not see any suit of clothes on him for fear that they will be seen as stupid. The only thing that changes behavior is when the little girl announces the Emperor's nudity loudly enough so that the entire crowd believes that everyone else in the crowd heard the news. That's when behavior changes. There's a lot of ubiquitous private information about powerful ideas trapped in the crowd today, just waiting for a someone to release it as common knowledge.—Ben Hunt

What we are observing now in the crypto bear market is the collapse of the narrative wave function from critical observations making knowledge common, ultimately manifested as price.

Some narratives are unraveling. Narratives that conflict will reconcile (ex: utility vs SoV theory of money). Which ones will remain? Which ones will survive? As we've seen in previous crypto market cycles, only the most antifragile will endure.

Links

- https://en.wikipedia.org/wiki/EPR_paradox
- https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat
- https://hackernoon.com/schr%C3%B6dingers-securities-regulation-the-quantum-state-of-crypto-ffb4e5b7446
- https://www.econlib.org/library/Essays/hykKnw.html
- https://fs.blog/mental-models/
- https://tokeneconomy.co/market-narratives-are-marketing-introducing-the-crypto-narrative-index-deeeb49bc909
- https://www.nationalgeographic.com/science/phenomena/2013/02/18/weird-youth-animal-kingdom/
- https://blog.goodaudience.com/bitcoin-as-exit-bitcoin-as-voice-c3d4520e201e
- https://www.danheld.com/blog/2019/1/6/planting-bitcoinspecies-14
- https://www.tonysheng.com/mass-movement
- https://medium.com/u/be4506861043
- https://twitter.com/danheld/status/1084848063947071488
- https://github.com/ethereum/EIPs/issues/960
- https://medium.com/@nic__carter/visions-of-bitcoin-4b7b7cbcd24c
- https://tokeneconomy.co/visions-of-ether-590858bf848e

- https://medium.com/u/f138bf5466fe
- https://medium.com/u/4acb12744ff8
- https://www.cnbc.com/2017/10/19/josh-brown-goes-down-the-bitcoin-rabbit-hole-commentary.html
- https://www.youtube.com/watch?v=bBC-nXj3Ng4
- https://medium.com/u/8bc4e5f8b505
- https://medium.com/u/731e1423e587
- https://en.wikipedia.org/wiki/Emperor
- https://www.epsilontheory.com/harvey-weinstein-common-knowledge-game/

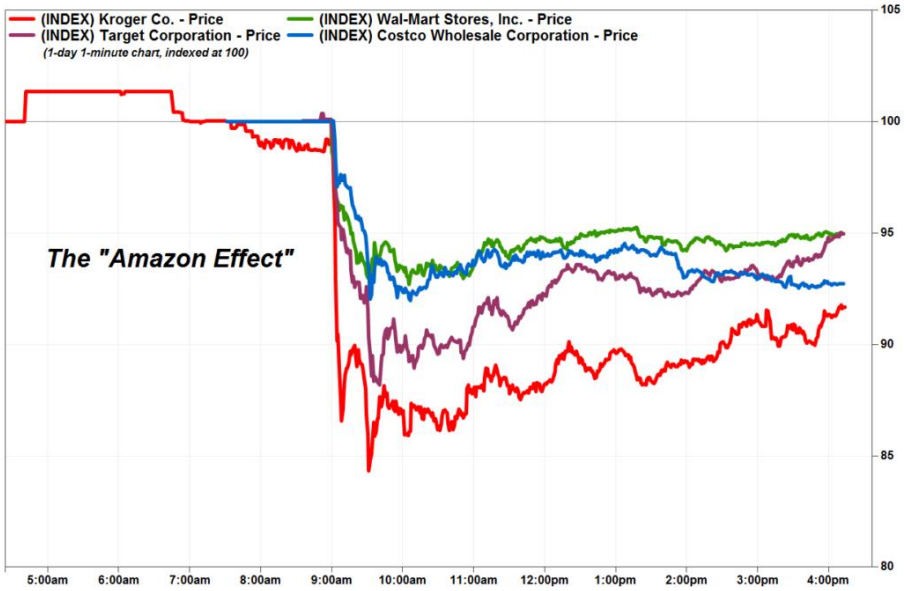
The Value Chain Constraint

By Ben Thompson

Posted on February 26, 2019

On June 16, 2017, minutes after Amazon announced it was buying Whole Foods Market Inc. for $13.7 billion, grocery store stocks fell through the floor; from MarketWatch (*emphasis mine*):

Shares of grocery stores took an unexpected hit Friday as investors reeled from the news that Amazon.com Inc. was moving into their space by acquiring Whole Foods Market Inc. After Amazon announced that it was buying Whole Foods in a $13.7 all-cash deal, shares of grocery store chain Kroger Co. slid to close down 9.2%, shares of Costco Wholesale Corp closed down 7.2%, Target Corp.'s stock closed down 5.2% and shares of Wal-Mart Stores Inc. closed down 4.6%…



Mark Hamrick, a senior economic analyst at Bankrate.com, said Amazon's technological innovation in traditional retail is a "earthquake" for the sector, which it may have hinted at with its recent launches of brick-and-mortar Amazon bookstores. "**We can only imagine the technological innovation that Amazon will bring to the purchasing experience for the consumer**," Hamrick said.

This is why I found Walmart's recent earnings so interesting: the company cited groceries as the biggest drivers of its ecommerce business, both last year and going forward — the company plans to expand grocery pickup to an additional 1,000 stores — because, as Walmart CEO Doug McMillon put it on the company's earnings call:

We strive to make every day easier for busy families as we increase convenience and save them money and time. Part of our strategy is to build on our existing strengths, such as having a broad assortment including fresh and perishable foods within 10 miles of 90% of the U.S. population.

Amazon, meanwhile, appears to be struggling; from Bloomberg:

The number of Amazon Prime members who shop for groceries at least once a month declined in 2018 compared with 2017, according to the results of an annual consumer survey released Wednesday by UBS analysts. The drop was surprising given the company's Whole Foods investment and expansion of two hour delivery service Prime Now, the analysts wrote in a note to investors.

A separate study by research firm Brick Meets Click found that households using grocery delivery and pickup services from physical retailers spend about $200 per month and place orders more frequently than Amazon grocery shoppers, who spend $74 a month.

So where is the promised technological innovation?

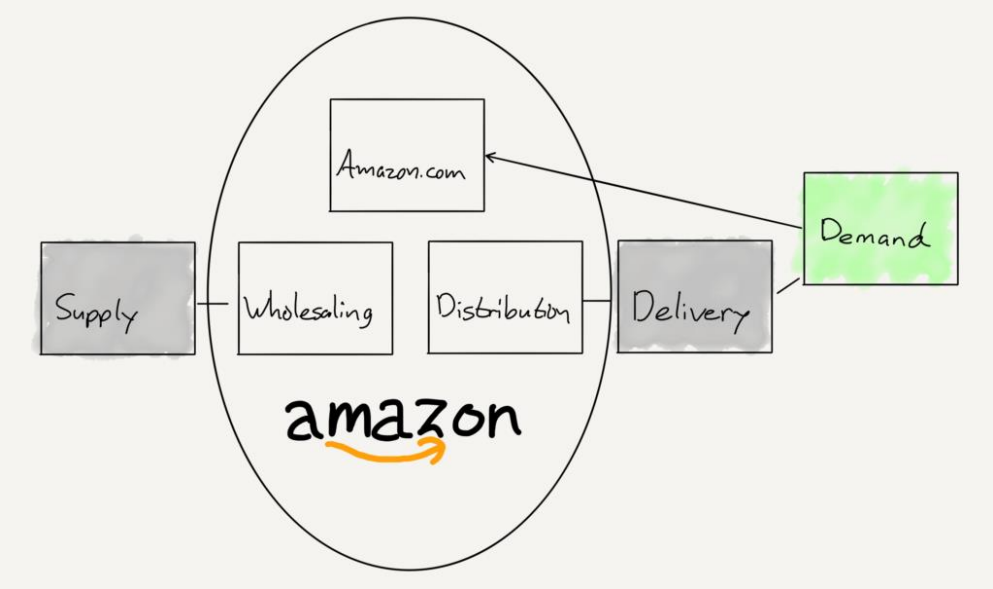
The Conservation of Groceries

I have written several times about the *Conservation of Attractive Profits*, most notably with regards to Netflix, Facebook and BuzzFeed, and Zillow. To put it in generic terms, profit in a value chain flows to whatever company is able to successfully integrate different component pieces of that value chain; the other parts of the value chain then modularize and are driven into commodity competition.

For example, this is what Walmart's traditional value chain looked like:

Walmart was able to integrate wholesale purchasing with an expansive network of stores; this provided a moat of sustainably lower prices for customer driven by purchasing power over suppliers.

Amazon, though, thanks to technological innovation — specifically, the Internet — was able to build a different integration in the value chain:



Amazon integrated wholesale purchasing and fulfillment centers with Amazon.com, relying on modularized delivery services for distribution; this provided a moat of superior selection and, at least at the beginning, lower prices, and with Prime, superior convenience, at least for non-perishable goods.

Walmart has worked for years to respond to Amazon's threat; the problem, though, as I explained in 2016's Walmart and the Multichannel Trap, is that an integration built around stores was fundamentally unsuited to offering the sort of selection and convenience that Amazon does. The company needed to build up an entirely new set of capabilities and integrations, even as Amazon was leveraging theirs to integrate forward into logistics, adding on a 3rd-party marketplace to expand selection even more, and integrating backwards into their own brands. The result is that Amazon has around 50% share in e-commerce while Walmart has less than 5%.

That, though, is precisely why groceries is worth examining: as I explained when Amazon bought Whole Foods, perishable goods are not well-suited to Amazon's value chain. Superior selection has diminishing returns, quality varies on an item-by-item basis within a single SKU, and, most importantly, the quality of items degrades with time and transport. In other words, they are a great fit for stores, not distribution centers.

In this view, Amazon's purchase of Whole Foods was an attempt to acquire a first best customer for its grocery delivery operation, one that would efficiently store and sell perishable goods that weren't suitable for Amazon's traditional e-commerce model. And, to be clear, this strategy may yet succeed, but only to the extent Amazon builds a completely new set of capabilities and integrations that will probably end up looking a lot like Walmart, which has a massive head start it is clearly taking advantage of.

In other words, what matters is not "technological innovation"; what matters is value chains and the point of integration on which a company's sustainable differentiation is built; stray too far and even the most fearsome companies become also-rans.

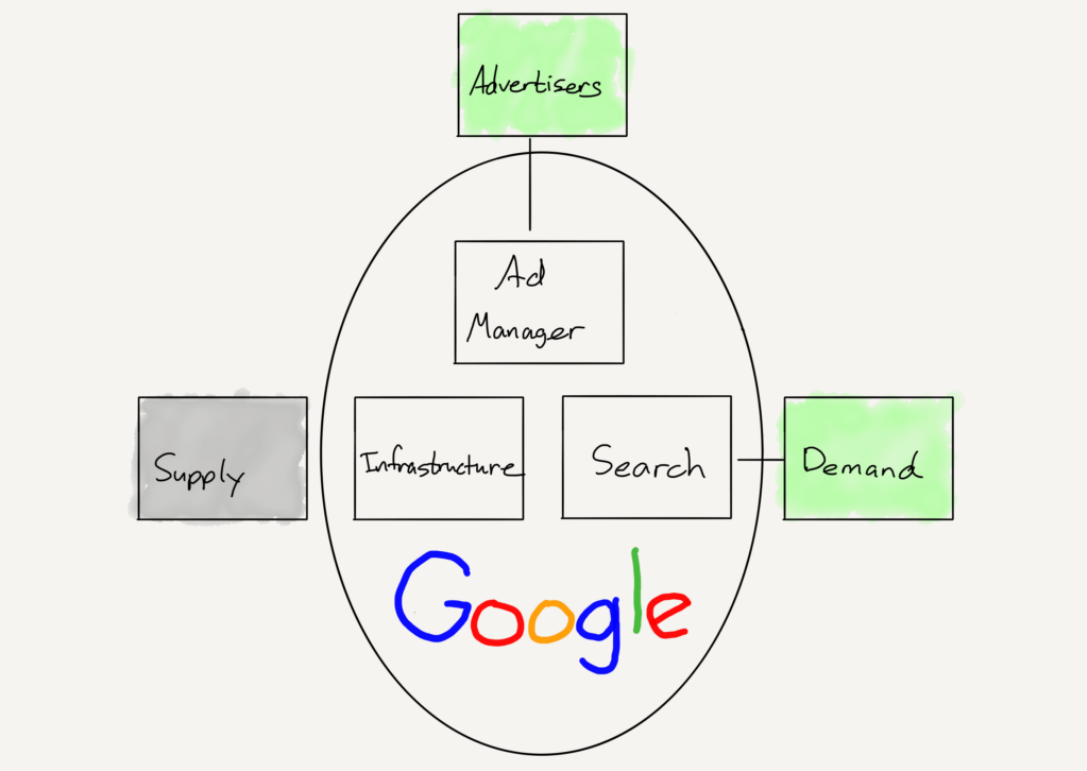
Google Cloud Struggles

Consider Google, a company that, more than any other, has been predicated on "technological innovation". This was possible because the company's core product — Internet search — entered a value chain with no integrations whatsoever. On the supply side there were countless websites and even more individual web pages, increasing exponentially, and on the demand side were a similarly increasing number of Internet users looking for specific content.

Crucially, all of the supply was easily accessible — just link to it — and all of the demand was capturable — they only needed to type in google.com. This meant that the best search engine — and by best, I mean the purest form of the word, i.e. best performing — could win, and so it did. Google was leaps and bounds better than the competition, thanks to its focus on understanding links — the fabric of the web — instead of simply pages, and consumers flocked to it.

This set off the positive cycle I have described in Aggregation Theory: owning demand gave Google increasing power over supply, which came onto Google's platform on the search engine's terms, first by optimizing their web pages and later by delivery content directly to Google's answer boxes, AMP program, etc., all of which increased demand, resulting in a virtuous cycle.

At the same time Google was building out two critical pieces of the value chain in integration with Search: the first was infrastructure — supporting that much demand required huge investments in servers, fiber optic cables, etc. — and the second was advertising. Ultimately the company's model looked like this:



Note how Google is so dramatically optimized on all three sides of this integration: users, suppliers, and advertisers interact with Google through their own volition, thanks to the infrastructure Google has built to facilitate that interaction, with almost no person-to-person contact with anyone from Google. It is a model that works very, very well — for search and digital advertising, anyways.

Things have not gone so well for Google Cloud. At first glance, selling infrastructure seems like an obvious opportunity for Google, and much ink has been spilled about how the company — any day now! — will threaten Amazon or Microsoft. After all, Google was building out worldwide infrastructure before anyone else, and the company remains at the forefront of technological innovation.

The problem, though, is that the company's value chain is completely wrong. The world of enterprise software is not a self-serve world (and to the extent it is, AWS dominates the space); what is necessary is an intermediary layer to interact with relatively centralized buyers with completely different expectations from consumers when it comes to product roadmap visibility, customer support, and pricing.

It has taken Google many years to learn this lesson: Google Cloud remains a distant third to AWS and Microsoft with a strategy that simply wasn't working. I wrote in a November Daily Update upon the occasion of Google Cloud changing CEOs:

A strategy predicated on being "better" on specific product attributes, though, may fit the culture of Google, but it doesn't necessarily lead to a winning enterprise strategy. To that end, Google Cloud faces three major problems:

- First, Google has not made an effective case about how specifically machine learning can benefit business that is appreciably different than traditional business analytics. That is not to say it can't, just that the company hasn't really made the case.
- Second, Google isn't competing with Lycos and Yahoo: AWS and Microsoft have machine learning offerings of their own, and Microsoft in particular is much more accomplished at productizing offerings in a way that are understandable and approachable to CIOs.
- Third, and most importantly, the technical attributes of a product are only one piece of what matters to success in the enterprise. Just as important are customization, support, and the ability to sell. Google is widely regarded as being the worst in all three areas.

In short, what Google Cloud needs is not a CEO that fits the culture, because the culture of Google is about making the best product technologically and waiting for customers to line-up. That may have worked for Search and for VMWare, but it's not going to work for Google Cloud. Instead the company needs to actually get out there and actually sell, develop the capability and willingness to tailor their offering to customers' needs, be willing to build features simply because they move the needle with CIOs, and actually offer real support.

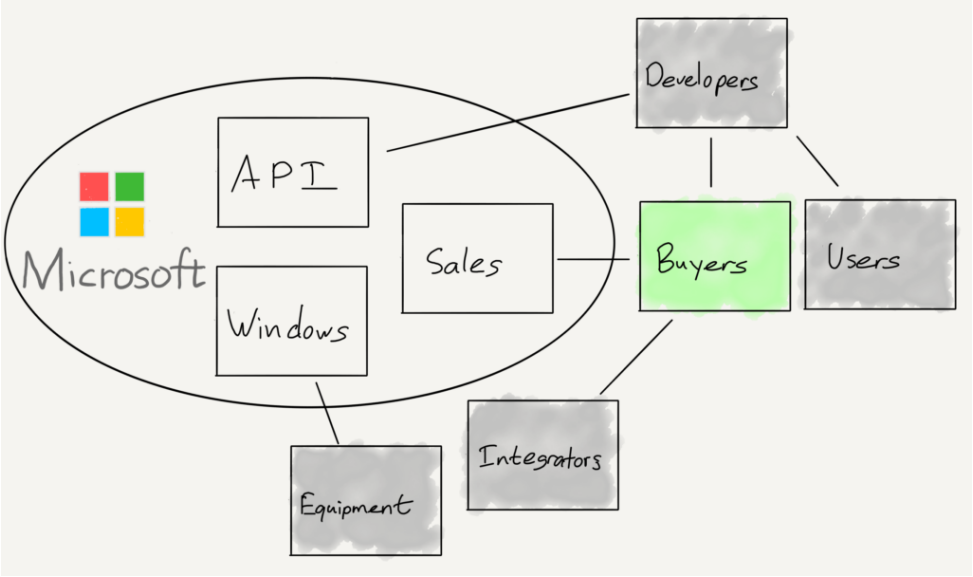
In short, Google Cloud is competing in a different value chain than is Google search, and it needs to build new integrations accordingly. To that end, note the strategy chosen by Thomas Kurian, Google Cloud's new CEO; from the Wall Street Journal:

The new leader of Google's cloud-computing business plans to dramatically expand its sales team, addressing one of the biggest challenges he faces as rivals Amazon.com Inc. and Microsoft Corp. race ahead in the market…While Google has long offered cloud technology, it has seen Amazon and Microsoft surge ahead to become the leaders in providing computing power and storage services for rent over the web. Those companies have robust sales and service staffs that large corporate customers demand to support their technology needs, an area where Google has trailed, analysts have said.

In other words, Google Cloud needs to look a lot more like Microsoft.

Microsoft's Enterprise Value Chain

Microsoft, unlike Google, has always been first-and-foremost an enterprise company. That means its integration was between its operating system and the associated APIs on which enterprise apps were built:



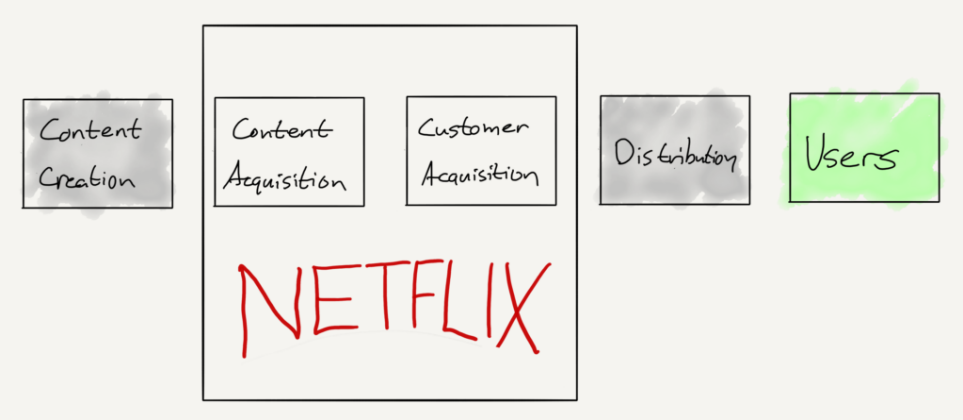
Note, though, that unlike Google's value chain, Microsoft is much further from the end-user: devices were built and sold by OEMs, sometimes to end users, but especially to enterprise IT departments by dedicated sales forces. Similarly, Microsoft developers were by-and-large enterprise software developers, working not for end users but for management.

This had obvious downsides in the consumer market: products in the Microsoft value chain were typically feature rich and user experience poor, exactly what you would expect from a world run by top-down purchase order, not individual consumer choice. To the extent Microsoft did succeed in the consumer space, the reason was a spillover from their dominance in enterprise; by the time pure consumer markets like the web or mobile came along, Microsoft was woefully unprepared to compete. They were basically the opposite of Google.

That, though, is also why Microsoft is succeeding with Azure even as Google struggles with Google Cloud: the company is used to value chains that include sales forces and top-down decision-making, and has the right business model and integrations to take advantage.

The Netflix Exception

Perhaps the most famous example of a prominent company "pivoting" and succeeding is Netflix, but that is very much the proverbial exception that proves the rule. Netflix built its initial customer base and IPO'd through a business model predicated on renting DVDs via mail. The value chain looked like this:



What was critical to making this value chain work was the first-sale doctrine: when a DVD was sold the rights of the copyright holder were exhausted; that means that Netflix could buy all of the DVDs it wanted and rent them to customers without copyright owners restricting them in any way. Critically, this meant that Netflix could integrate the customer relationship with content ownership.

Notice that that is the *exact same* integration that Netflix enjoys today: more and more of the company's content catalog — particularly the portions that attract new customers — is original content owned by Netflix. In other words, the point of integration — the customer relationship and content ownership — is the same as in the DVD days.

To be sure, it took time for Netflix to transition to this model, and the company was absolutely helped along by hapless studio executives more interested in bumping up their annual profit than in considering their long-term position in the content value chain. There are any number of points in the early days of streaming when Netflix — because it was, if only temporarily, in a vulnerable non-integrated position in its value-chain — could have been stopped. I suspect, though, those days have past, which is why Netflix Flexes.

More generally, from a value chain perspective, Netflix's transformation was less of a pivot than it might have first appeared: sure, the technology of DVDs by mail and streaming video are fundamentally different, but the value chain is the same. That is a far more viable transition than trying to leverage broadly similar technology into completely new markets and value chains.

The Solipsism Trap

It is understandable why the Internet giants in particular move into seemingly adjacent territories: the growth imperative is strong, both for financial and strategic reasons, and the technology seems easy enough, particularly given the resources these companies bring to bear. And yet, the truth is that those massive resources do not stem, at least in the long run, from technical excellence, but rather integration in specific value chains that produces positive feedback loops and outsize profits.

It follows, then, that without that integration, the positive feedback loops quickly disappear, along with the profits, which is the exact pattern we see again and again. Microsoft spent billions on phones and consumer Internet services, Amazon spent billions on Whole Foods, Google has spent billions on not just Google Cloud but a whole host of initiatives that have nothing to do with Search, Facebook has spent billions on Watch and VR, and now Apple is getting in the game with billions spent on Video, and the expected outcome of all these should be that they will fail.

To be sure, failure takes time: these companies do have nearly unlimited resources thanks to their core business models, and the reckless optimism bred by structural success. And, I suppose, sometimes they can actually push products across the line to profitability, kind of. Bing, for example is profitable — if you exclude traffic acquisition costs, which makes my point.

The reality is that technology has an amplification effect on business models: it has raised the Internet giants to unprecedented heights, and their positions in their relevant markets — or, more accurately, value chains — are nearly impregnable. At the same time, I suspect their ability to extend out horizontally into entirely different ways of doing business — new value chains — even if those businesses rely on similar technology, are more limited than they appear.

What does work are (1) forward and backwards integrations into the value chain and (2) acquisitions. This makes sense: further integrations simply absorb more of the value chain, while acquisitions acquire not simply technology but *businesses* that are built from the ground-up for different value chains. And, by extension, if society at large wants to limit just how large these companies can be, limiting these two strategies is the obvious place to start.

Links

- https://stratechery.com/author/stratechery/
- https://www.marketwatch.com/story/grocery-stocks-tank-as-amazon-effect-strikes-fear-in-investors-2017-06-16
- https://stratechery.com/2019/walmarts-earnings-walmarts-grocery-business-amazons-grocery-stumbles/
- https://seekingalpha.com/article/4242244-walmart-inc-wmt-ceo-doug-mcmillon-q4-2019-results-earnings-call-transcript?part=single
- https://www.bloomberg.com/news/articles/2018-12-20/amazon-s-grocery-push-keeps-stumbling-after-whole-foods-purchase
- https://stratechery.com/2015/netflix-and-the-conservation-of-attractive-profits/
- https://stratechery.com/2019/the-buzzfeed-lesson/
- https://stratechery.com/2018/zillow-aggregation-and-integration/
- https://stratechery.com/wp-content/uploads/2019/02/Paper.stratechery-Year-One-copy.391.png
- https://stratechery.com/wp-content/uploads/2019/02/Paper.stratechery-Year-One-copy.392.png
- https://stratechery.com/2013/amazons-dominant-strategy/
- https://stratechery.com/2016/walmart-and-the-multichannel-trap/
- https://stratechery.com/2017/amazons-new-customer/
- https://stratechery.com/2015/aggregation-theory/
- https://stratechery.com/wp-content/uploads/2019/02/Paper.stratechery-Year-One-copy.393.png
- https://stratechery.com/2018/google-cloud-changes-ceos-layers-of-surprise-or-not-the-vmware-analogy/
- https://www.wsj.com/articles/google-cloud-chiefs-plan-to-catch-amazon-and-microsoft-sales-reps-11550011137?mod=searchresults&page=1&pos=1
- https://stratechery.com/wp-content/uploads/2019/02/Paper.stratechery-Year-One-copy.394-2.png
- https://stratechery.com/wp-content/uploads/2019/02/Paper.stratechery-Year-One-copy.395.png
- https://en.wikipedia.org/wiki/First-sale_doctrine
- https://stratechery.com/2019/netflix-flexes/

Bitcoin Delta Capitalization

A New View of BTC Long-Term Valuation

By David Puell

Posted on February 14

Disclaimer: Nothing contained in this article should be considered as investment or trading advice.

As a follow-up to Willy Woo's recently-introduced Bitcoin Valuations live chart, this article aims to present delta cap with the goal of answering two of the most pressing questions in speculators' minds at the present moment:

Where is the bottom?

When is the next bull run coming along?

Something's Amiss

Two sets of items originated the search for what later became delta cap:

Awe and Wonder's studies on Bitcoin's logarithmic regression and Plan B's studies on Bitcoin's power regression (R^2 of 0.93 and 0.95 respectively), which seem to suggest that the BTC trend is increasing at a decreasing rate.

Murad Mahmudov's exploration of historical moving averages, expressing a dissatisfaction with any particular SMA or EMA as definitive enough to "catch the bottom" in every bear cycle.

This initiated the search for a metric that both adapted to Bitcoin's rapid, high-velocity parabolic moves and accounted for its overall trend decay over time. Two other valuation models seemed to provide a tentative answer: realized cap for the former and average cap for the latter.

Delta Capitalization

Delta cap is, as seen next, a hybrid of sorts—half "fundamental," half "technical." It is calculated through the following formula, measuring the difference between two long-term Bitcoin moving averages:

$$DeltaCap = RealizedCap - AverageCap$$

For the purposes of this piece, let's review these definitions:

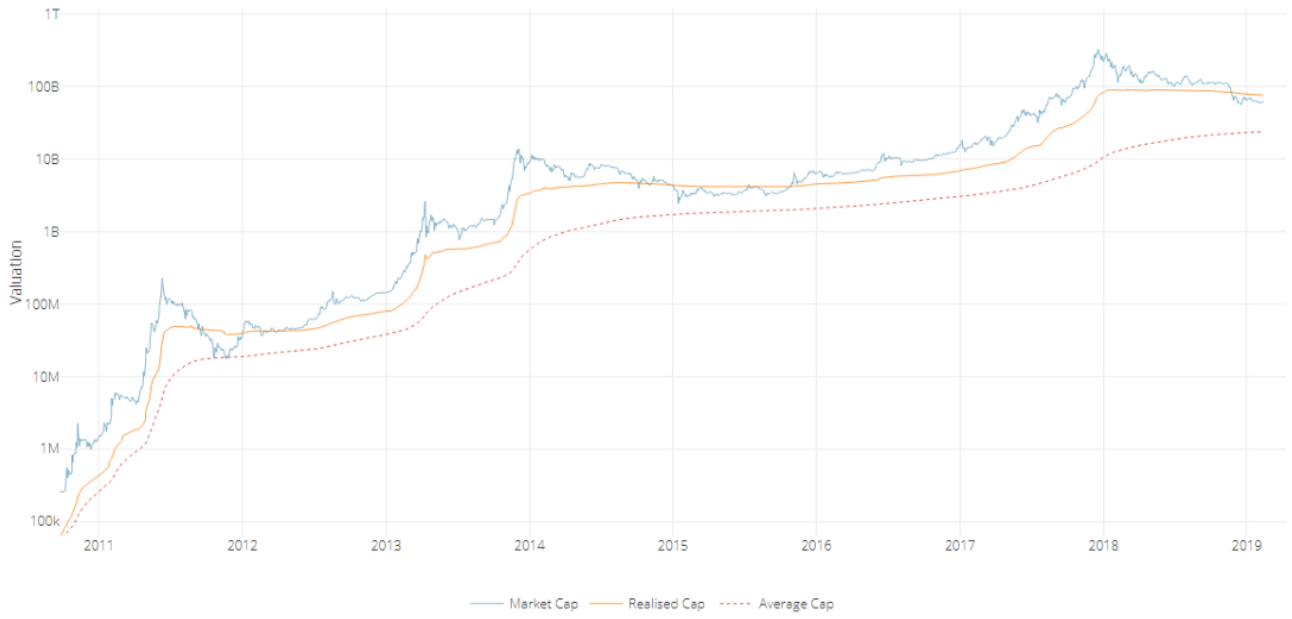
Realized capitalization

Invented and presented by the brilliant team at Coinmetrics, instead of counting all of the mined coins at current price, the coins are counted at the price when they last moved through the blockchain. This approximates the USD value paid for all the bitcoins in circulation. Best put by its co-creator Nic Carter, it can be described as an on-chain volume-weighted average price (VWAP) of BTC.

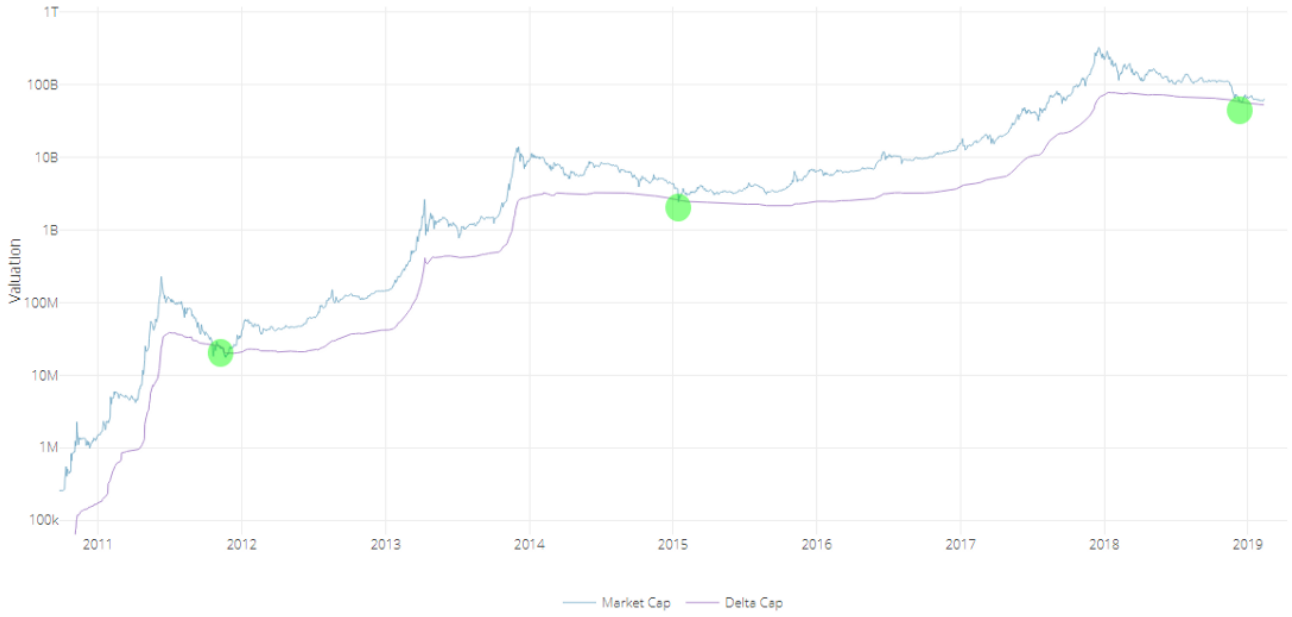
Average capitalization

Instead of setting a fixed period for calculating a moving average (e.g., a 200-day MA), this is a life-to-date, cumulative simple moving average that serves as the true mean of the whole history of market cap. Due to its "laggy" nature, it is the perfect mechanism to help decay the upward speed of delta cap over time. Shoutout to Renato Shirakashi for first pointing out this average.

Below, a view of both lines, courtesy of Willy Woo:



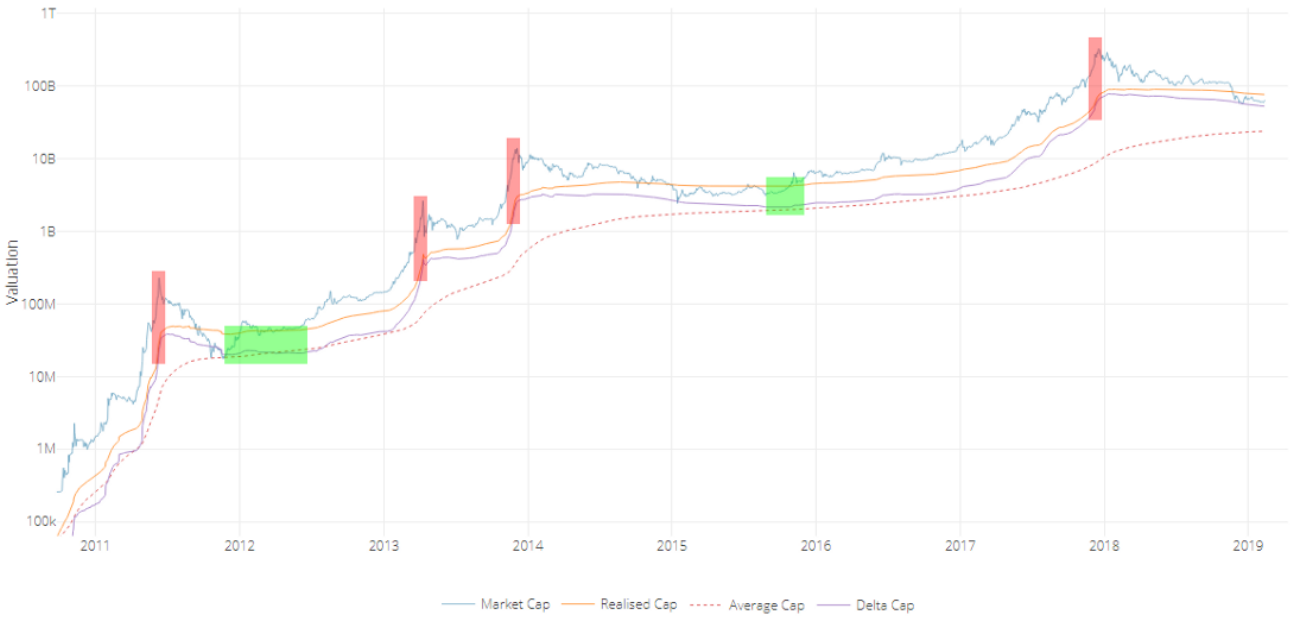
The aforementioned substraction of the two in turn provides the following delta cap line, both reactive locally and decaying globally:



As seen at first glance, delta cap provides an excellent framework for catching global bottoms—or at the very least bottoms near the floor of the bear cycle. Please see the caveats of this indicator below to have a more nuanced view of the current state of affairs, since *having just touched delta cap does not guarantee that we have bottomed.*

Time Analysis

Another interesting (and still experimental) exploration of delta cap emerges when comparing it to its parent inputs through a logarithmic view, as follows:



We can easily gauge periods were delta approaches realized cap during the bubble tops, and then evermore slowly descends to almost touching the average cap during the phases of breakout price behavior, signaling the inauguration of the new bull run.

The good news? If this pattern continues, people will have lots of time to buy up. The bad news? This bear-to-sideways market may last for an unprecedented while, going as far as projecting a post-accumulation breakout as late as Q2, 2020—the moment when it could be expected for delta cap to get nearest to average cap if the extension of these lines continues as-is. Bear in mind that this is all pending on the overall rate of drop of realized cap and the rate of rise of average cap—local price action, velocity, and dormancy are all in play. Time domain here is still a broad estimate.

It goes without saying that we lack enough bottom samples to claim this as a certainty, but long-term investors must stay mentally prepared for this possible delay. It is further evidence that suggests Bitcoin's cycles are elongating.

Yes, Another Ratio: MVDV

Since most will be curious about how the Market-Value-to-Delta-Value (MVDV) Ratio looks like, here it goes:

A few notes on it:

Just as seen on MVRV Ratio and the Mayer Multiple, MVDV seems to indicate that each of Bitcoin's blow-off tops is losing momentum. This is not necessarily bearish, as I believe it merely implies that each bubble is becoming less exuberant and getting closer to the mean.

Major bearish divergences seem to announce global tops (red circles) while differentiating them from previous local tops of the same cycle.

The bottoms seem to maintain a steadier horizontal longitudinal threshold at 1 (green line). If market cap were to revisit delta cap today at a lower low, the oscillator would present this event as a double bottom.

Caveats

Having touched delta cap recently does not imply a global bottom: One must remember that delta cap is currently sloping down—and it will continue to do so for several months—so the likelihood of market cap revisiting it is not out of the question. Add to that the fact that the NVT tools are still just slowly trending into normal historical conditions and velocity remains weak. Touching delta cap on a lower low in the following months is still a likely possibility. Every penetration of market cap into delta cap should be best used as one componet of an averaging-in strategy over a prolonged period of time.

Despite timeboxed halving days, the Bitcoin cycle seems to be elongating: This makes perfect sense, since larger bull runs require larger liquidity. The experiment here is to continue evaluating delta cap as a mean that keeps adjusting to Bitcoin's curved trend. That being said, the time analysis section of this article remains highly speculative, especially for signaling the breakout events, so let's take it one day at a time.

The market currently holds a major dissonance: That of delta cap providing a good "baseline" for a relatively optimistic market floor, versus the current state of velocity as seen on NVT Ratio, Network Momentum, and NVT Caps— on life support relative to price.

Delta cap remains experimental: Just as with most technical and on-chain tools, these indicators should be used with prudence and in the company of other trading mechanisms and a sound risk management strategy. Past events don't reflect future outcomes.

Acknowledgements

Many thanks to the following individuals:

Willy Woo, for the beautiful charts and valuable feedback.

Murad Mahmudov, Phil Bonello, Hans Hauge, PositiveCrypto, and Plan B, whose comments helped perfect this article.

Sources

Woobull.com: Charts and early market cap data archeology.

Coinmetrics.io: Realized cap data.

Blockchain.com: Market cap data.

Author

David Puell, Partner and Head of Research @ Adaptive Capital

Links

- https://medium.com/@kenoshaking?source=post_header_lockup
- https://medium.com/@kenoshaking
- https://twitter.com/woonomic
- https://twitter.com/woonomic/status/1096103959897489413
- https://twitter.com/Awe_andWonder/status/1053408719063707648
- https://twitter.com/100trillionUSD/status/1092771532231897088
- https://twitter.com/MustStopMurad/status/1090762552102084614
- https://coinmetrics.io/realized-capitalization/
- https://twitter.com/nic__carter
- https://twitter.com/renato_shira
- http://charts.woobull.com/bitcoin-mvrv-ratio/
- http://charts.woobull.com/bitcoin-mayer-multiple/
- http://charts.woobull.com/bitcoin-nvt-ratio/
- http://charts.woobull.com/bitcoin-network-momentum/
- http://charts.woobull.com/bitcoin-valuations/
- https://twitter.com/MustStopMurad
- https://twitter.com/PhilJBonello
- https://twitter.com/hansthered

- https://twitter.com/PositiveCrypto
- https://twitter.com/100trillionUSD
- http://charts.woobull.com/
- https://coinmetrics.io/charts/
- https://www.blockchain.com/en/charts/
- https://twitter.com/kenoshaking
- mailto:info@adaptivecapital.co

Against Szabo's Law, For A New Crypto Legal System

By Vlad Zamfir

Posted January 26, 2019

Earlier this week (on Sunday night, in fact), I came across a definition and understanding of "legal systems" that has really cleared up a lot of things that have been weighing heavily on my mind for a long time. Here it is:

Legal systems are protocols for the management of disputes.

This includes protocols for preventing disputes and for managing the whole lifecycle of disputes, from inception to resolution. It captures both descriptions of these protocols ("legal code") and their execution ("operation of law"). It might need to be refined, but it's useful enough as given here.

Disputes arise in blockchain governance. We follow protocols for managing them.

Ergo, crypto law exists.

The purpose of this writing is to 1) document some of today's crypto law, to 2) agitate for a change in crypto law; to convince the cryptocurrency community to abandon a crypto law (a law that I'm calling "Szabo's law"), and 3) to agitate for the inception of a new crypto legal system.

I am prepared to die on this hill.

Crypto Law, Today

I have identified a number of crypto laws, and believe that the following three crypto laws are the most important laws in cryptocurrency today, in the sense that they are the most operative in the day-to-day management of disputes in blockchain governance:

Crypto Law #1: Don't Break the Protocol.

The spirit of this law is simple and natural. Disputes in blockchain governance are not to ever be resolved by the introduction of known critical bugs into the blockchain protocol. Critical bugs can cause the bridge to collapse, and there are people on the bridge at all times. Systemic collapse and noticeable degradation in the system's quality always lead to disputes, and these disputes are to be avoided by preventing collapse.

It is the responsibility of developers, engineers, and architects to ensure that the software is maintained, that systemic failures don't occur, and that when they do (as will happen,

because of the sorry state of the software development industry), to remedy the situation as quickly as possible.

Anyone can halt a proposal to merge a change to the blockchain protocol by clearly pointing out that a critical bug is introduced by the proposal. This is crypto law (in fact, and not because I have just declared it to be the case).

How this law is interpreted, however, can get complicated. Blockchain core developers have precise and detailed pictures of what is considered a breaking change, and what is not. Their views are generally overlapping (for example, everyone agrees that the system crashing or having a consensus failure is breaking), however, but they also have disagreements (for example, backwards incompatible changes are considered to be breaking changes in more cases in Bitcoin governance than in Ethereum governance).

Crypto Law #2: Keep Crypto Law Legal.

This one came as a surprise to me, so it might come as a surprise to you, too. Or maybe not!

Crypto law operates inside many jurisdictions of many legal systems and is very much structured by attempts to avoid disputes with/in these legal systems. Developers and other crypto people structure their affairs in an effort to prevent disputes that might be brought to (and by) existing legal systems. As a result, crypto law operates legally in the jurisdictions of these legal systems. At least for now.

Devs make technical decisions in order to minimize their exposure to possible liability; they will choose a solution that involves assuming less liability over one that involves more, all else being equal. They will often cite their concerns that something might be illegal under some existing legal systems, or that they will be sued for their exercise of power, as motivations for their decisions.

I am not commenting on the effectiveness of efforts to keep crypto law legal, but I want us all to observe that the management of disputes in blockchain governance are very much structured by attempts to avoid disputes with existing legal systems.

The cryptocurrency community didn't come up with this law. That crypto law is structured by existing legal systems is a natural consequence of the fact that crypto law operates in the jurisdictions of existing legal systems. And while for some participants in blockchain governance it may be possible to remain anonymous or somehow else avoid structuring their affairs in accordance with the operation of law, most participants in blockchain governance are public people who make an effort to position themselves in a manner that doesn't get them in trouble with existing legal systems. Because of this reality, "keep crypto law legal" is crypto law. At least for now.

Crypto Law #3: Szabo's Law.

I'm naming this crypto law after Nick Szabo, since I am pretty convinced that he created it, popularized it, and brought it into crypto law. I'm sorry if I'm missing anyone else who deserves credit for it, but I'm just going to assume that Nick is responsible so I can keep my sentences short.

Szabo's law is simple: Do not implement changes to the blockchain protocol unless the changes are required for the purpose of technical maintenance.

It's called "blockchain governance minimization", but it can also justifiably be called "crypto law minimization", because of the following crypto legal consequence:

Crypto law does not (at least not crypto legally) manage disputes by making changes to the blockchain protocol, unless they are justified as needed tech maintenance.

It's a law that completely excludes other crypto legal processes from touching the blockchain protocol. Except as it is related to tech maintenance.

Nick Szabo has popularized (and legalized) his law in a few ways:

1. By popularizing autonomous software in the crypto legal form of smart contracts
2. By arguing that the minimization of responsibility for developers isolates them from legal risk
3. By arguing that crypto legal systems with Szabo's law are more socially scalable than systems with more legal and political power.

Nick's crypto law is responsible for a lot of the talk (and law) around the blockchain being immutable, and needing to remain immutable, and has justified decisions by developers to refuse to make changes to the blockchain protocol when they are engaged in blockchain governance disputes (for example in the Bitcoin block size debate). The DAO hard fork was a clear violation of Szabo's Law, and it offended Nick enough that he disowned Ethereum in favor of Ethereum Classic. But Szabo's law has been cited in Ethereum blockchain governance disputes after the DAO hard fork (specifically, in the still-unresolved stuck funds dispute). Indeed, Nick Szabo's law is often cited by core developers to justify their choices in blockchain governance disputes. Szabo's law is therefore crypto law.

In Awe of Nick Szabo's Crypto Legal Achievements

Before I dig in, I'm going to take the opportunity to express humility in light of the crypto legal work that Nick has managed to do, apparently working with only the power of his crypto legal mind, and his writings on blogs, mailing, and the like. It's an impressive—groundbreaking—achievement.

Nick Szabo forged a crypto law and popularized a legal theory that created software that is way more autonomous than society is capable of creating without the use of law.

In truly revolutionary cypher-legal-punk style, he created autonomous software with a crypto law and a legal theory that is profoundly and radically anti-legal and anti-political.

That the political and legal climate of the world was ready to embrace a legal theory and a law that is premised on the idea that legal and political processes are unworkable and need to be *ruthlessly minimized*, that software needs to be autonomous to be trusted is absolutely astonishing.

What a time to be alive!

Certainly Nick has vision and judgment—there is no way that the blockchain space could have gotten to where it is now, with crypto law the way it is, if people across the globe weren't jaded enough by the evolution of legal and political processes to be attracted to Szabo's law. Nick saw the opportunity and acted on it to create a truly global (crypto legal) revolution. It's really something remarkable. I am humbled by his insight, his foresight, and the effectiveness of his cypherpunk activist work.

And all things considered, it seems like cryptocurrency is going to remain more—or less—legal. At least for now!

So I take my hat off to you, Nick Szabo, in awe of your mindnumbingly brilliant and successful crypto legal activism! Thank you! No really—Thank you! Mad respect to you, sir!

But now—sorry Nick—I'm going to do my best to persuade the reader that we need to abandon Szabo's law as soon as possible.

Against Szabo's Law

Unfortunately for everyone, Szabo's radically anti-legal crypto law is too radically anti-legal to be part of a sensible crypto legal system. Szabo's law minimizes crypto law. It comes at the exclusion of all other crypto law that might be concerned with making changes to the blockchain protocol. Hopefully you already see how absurd this is, but I'm going to spell it out as clearly as I can, in the following four parts:

1. Szabo's Law breaks Crypto Law #2 (Keep Crypto Law Legal)
2. Szabo's Law is politically loaded, not politically minimal, apolitical or anti-political
3. Szabo's Law has an insecure and aggressive legal posture
4. Szabo's Law is not a part of the most socially scalable crypto legal system

Szabo's Law breaks Crypto Law #2 (Keep Crypto Law Legal)

Nick Szabo sold blockchain developers on the idea that the minimization of blockchain governance and of crypto law would minimize their exposure to legal risk, by requiring them to exercise only the minimum amount of crypto legal power and judgement possible.

Unfortunately for these developers who probably had no legal training of any kind, Nick's legal theory is actually very stupid, and based on a naive interpretation of how existing legal systems will interact with crypto legal systems.

If the response when a legal system brings a dispute to blockchain developer is "sorry, we can't do anything for you", as it will almost always be under Szabo's law, then it has two natural reactions (assuming that the legal system believes that the devs can't do anything). The first is for the legal system try to handle the disputes without any recourse through changes to the protocol. The second is to minimize the damage caused by unresolved or irremediable disputes by making the use and development of the blockchain protocol illegal.

Szabo's firm hypothesis is that legal systems will be satisfied with their ability to manage the disputes that arise in blockchain governance but which cannot be remedied by crypto law thanks to Szabo's law.

I can imagine lots of possible disputes that can't be resolved (and will be ongoing) without changes to the blockchain protocol, and so my hypothesis is that Szabo's law will make cryptocurrency illegal in many jurisdictions. Disputes that are not being adequately resolved by crypto law will be brought to existing legal systems, who in turn in some cases will not be properly able remedy the situation because they cannot change the blockchain protocol.

It should not be surprising, but a crypto legal system operating on principles as anti-legal as Szabo's law will naturally eventually become illegal. As a result, Szabo's law is in conflict with Crypto Law #2.

I'm not done arguing this point, I am going to come back to it after describing the legal posture of crypto legal systems that adopt Szabo's law.

Szabo's Law is politically loaded, not politically minimal, apolitical or anti-political

While Szabo's Law is sold on the principle that politics is to be minimized, its crypto legalization was a deeply politically motivated act. I don't know what Szabo's political goals actually are, but it is safe to assume that he believes that they can be brought closer to reality by legalizing autonomous software into existence.

Not only does the legalization of Szabo's law determine governance outcomes (always in favor of not intervening with the execution of software), it minimizes the space for political and legal conversations that question whether those outcomes are desirable.

It locks blockchain governance and crypto law on a collision course with the consequences of creating autonomous software. It's impossible to predict all of the ways that this can go wrong, impossible to predict all of the disputes that will arise if we go down this route, but it is the route that Szabo chose for us based on his worldview.

He imagines a world in which crypto political and legal processes are necessarily going to go against either his personal preferred political outcomes, or against the public good, and therefore must be minimized.

This positioning makes sense if Szabo wants to do something very politically unpopular or something very illegal. It also makes sense if Szabo is so radically jaded that he believes that crypto law and politics cannot be worth the effort, no matter what form the crypto legal system might take.

But in either case, Szabo's clear intention is to use crypto law to determine blockchain governance outcomes without participating in blockchain politics (which, conveniently, is to be minimized according to Szabo's law). The legalization of Szabo's law was therefore a highly politically charged crypto legal action.

Szabo's law is not anti-political. It is a law that is aimed at shutting down political debate in order to guarantee Nick's preferred political ends.

I regard this kind of anti-social behavior to be bad-faith participation in blockchain governance.

Szabo's law has an insecure and aggressive legal posture

I don't just mean that shutting down political debate is an insecure way to achieve your political goals.

Crypto law's current posture of "we don't deal with disputes that aren't related to maintenance" and "sorry, there's nothing we can do for you" is insecure and aggressive.

"**We don't deal with disputes that aren't related to tech maintenance" is insecure** in crypto law's ability to legitimately manage the disputes that might arise in blockchain governance.

"**There's nothing we can do for you" is an aggressive posture**, when someone has a legitimate dispute.

And why is crypto law insecure and aggressive?

Because of a radical law born of the view that politics and law are completely unworkable and not worth trying in any circumstance or configuration whatsoever. Because of Nick Szabo's insanely stupid crypto law.

Nick is insecure in his ability to participate in political and legal process, and in his ability to come up with legal systems that actively manage disputes, and his crypto law reflects it. He is very aggressive in his quest to create autonomous software, and his crypto law reflects it.

This legal posture is in direct conflict with Crypto Law #2. It invites conflict with existing legal systems. **Legal systems don't like to be involved in disputes with insecure, aggressive legal systems.**

Who does?

Nick's legal posture might be cool as a kind of radical cypherpunk crypto legal philosophy. Maybe. But it's not appropriate for blockchain governance, not today, and probably not ever.

Szabo's Law does not create the most socially scalable crypto legal systems

I don't think that Nick imagines that an aggressive and insecure legal posture is the most socially scalable legal posture. And it obviously isn't.

Nick believes that a crypto law that legalizes autonomous software will form a better basis for socially scalable society than is possible under any conceivable crypto legal system that is more political or legalistic.

I am very skeptical about his position, because I don't believe that autonomous software is at all safe, you know, for humans in society.

Nick knows that autonomous software isn't always going to be legal or politically popular, and he is determined to use crypto law to shut down any legal and political coordination that would undermine his mission. This antisocial behavior makes me question whether Nick is even concerned with the social scalability of public blockchains.

Assuming that Nick has good intentions, then I am absolutely certain that Nick Szabo is not the best legal thinker in the world. Someone can come up with crypto law that is more socially scalable than the crypto law Nick came up with so he could bring autonomous software into the world. *There's no doubt about it.*

Maybe enough people are as radically paranoid of legal and political processes as Nick that even a slightly more reasonable crypto legal system will be broadly seen as untrustworthy. I don't know. But I'm ready to have faith and to bet my life that we can do much, much better than the insecure, aggressive crypto law we have today.

A much more secure crypto legal posture is possible if we abandon Szabo's law

Crypto law doesn't have to be this way.

Legal realities do not warrant the posture of today's crypto law.

Cryptocurrency is more-or-less legal. We need to relax.

Szabo's law is anti-legal and anti-political. We need to abandon Szabo's law to adopt a more open and secure legal posture. One that acknowledges rather than shrugs off its responsibility to carefully manage disputes. One that does not write crypto law to push politically unpopular outcomes on society. We can't adopt a secure and open crypto legal posture without first abandoning Szabo's law.

But we don't need to know anything about the future of crypto law to assume a more secure posture, and benefit from the more comfortable position. **We can immediately embrace a much more correct position, one that does not change crypto law except by abandoning Szabo's law:**

Crypto Law is responsible for managing disputes in blockchain governance, and making sure that they are resolved via legal processes that don't break the protocol.

Crypto law is still nascent, and I have no clear picture where it will go in the future. But I don't need to know where it will go to see that it needs to abandon Szabo's law in order to develop in a healthy way.

We cannot foresee the nature of all of the blockchain governance disputes that will arise in the future, and need to retain the ability to remain flexible enough to adapt to changing circumstances, we cannot afford to blindly pledge our fates to a future with autonomous software.

We have crypto law because we have protocols for managing blockchain governance disputes. We need these protocols to be sensible, so that we don't create unnecessary headache and hardship when disputes arise. We need to believe in our ability to manage blockchain governance disputes based on sound crypto legal work—which means not breaking the protocol and keeping crypto law operations legal—at an absolute bare minimum.

We should admit that we need more legal principles, and more crypto law. We should admit that we need to come to a new understanding of how disputes in blockchain governance ought to be resolved.

We should admit that we collectively have an obligation to manage the disputes that will arise from the operation of global public blockchains to the best of our crypto legal

ability, so that as many people as possible can enjoy the benefits of global public blockchains.

This secure, open-minded posture is much more comfortable than the aggressive, insecure posture we have today.

I hope you're already feeling more comfortable!

If crypto law fails to tactfully manage disputes, the result is more plausibly going to be that blockchains (and the operation of crypto law) become illegal, than that blockchains remain legal and autonomous and become as widely adopted as Nick Szabo imagines they will. The only way the law-abiding public can have the most benefit from global public blockchains is with a new crypto legal system.

For A New Crypto Legal System

Nick Szabo took it upon himself to use crypto law to summon autonomous software.

In response, we must take it upon ourselves to use crypto law to conjure up a new crypto legal system, one that is able to keep Szabo's beast in check.

I am calling upon crypto law people to recognize that they uphold principles of law that are incompatible with Szabo's law.

I am calling upon crypto law people to strike down Szabo's law, and to establish a new crypto legal system in its wake.

No one should do this alone. Not me, not you, not Nick Szabo. It needs to be a global best effort that taps into the bests legal thought available, that is rigorously treated by the best legal minds on the planet, from as many legal traditions and schools of thought as possible. We can't afford to screw it up. And we have no idea how it's going to turn out.

We can't let Nick Szabo stop us from establishing a new crypto legal system. His paranoid conviction that legal systems are completely unworkable and are best ruthlessly minimized cannot be justified by impartial reasoning in legal or political analysis. The genius crypto legal footwork that Nick did to legalize Szabo's law is an impressive feat, and says a lot about our current legal and political climate, but his legal theories are not a sound basis for any system of crypto law.

His attempt to create autonomous software that is above any (other) law must be foiled by law people who are able to see through Nick's bogus legal theories.

But we must stand in awe of the astonishing success of Nick Szabo's law, and of Nick's evident ability to tap into the distrust that permeates the modern legal and political climate.

And we must pay due tribute to the legal and political climate that legalized Szabo's law.

Nick Szabo's crypto law does not do it justice!

If no one should be in charge, then how does Nick Szabo get to use crypto law to ban us from using crypto law?

Nick is insecure about his ability to participate in politics and law, and he wants to use the force of law to conjure up autonomous software, and he doesn't want us to have a say in the matter.

So why should we take tips from him about how we should handle disputes?

And why should *he* write *our* laws? How does he imagine that he can deny us our ability to create our own crypto law?

Nick Szabo's personal effort to minimize our use of crypto law is not a good crypto legal embodiment of the ethos of our sociopolitical movement today, and it never was.

We need to stop buying into his bullshit.

I don't trust Nick Szabo to write our laws, or to have sound, impartial judgment about how we should prevent and resolve disputes. And neither should you. Nick Szabo does not represent me, and I am sure that letting Nick dictate our future is not what decentralization is about at all.

Crypto law is a collection of protocols for handling and preventing disputes that arise in blockchain governance.

Nick Szabo has a narrow imagination for what crypto legal systems can be like, and doesn't even bother thinking about it too much because he categorically dismisses all non-minimized crypto legal systems.

Nick is a visionary cypherpunk activist, that's for sure, but the legal and political theories that he spreads do not reflect sound, impartial judgement. They reflect his insecure and aggressive crypto legal style.

I will not follow his lead.

Crypto law isn't decided. It isn't final. Law doesn't ever actually operate like that. It's an institution that humans use to coordinate the management of disputes. We can always coordinate politically to create new institutions, although it may not always be easy.

Crypto law doesn't need to be Szabo's law.

And I don't think anyone has the ability to defend Szabo's indefensible law.

Nick Szabo says that crypto law is decided and that it must be minimized. But Crypto law isn't decided, and it must not be minimized.

Nick Szabo wrote and decided on the "decided" crypto law himself, and he propagated legal theories in order to legalize it so that he could have autonomous software.

But crypto law doesn't need to be Szabo's law.

We need to be free to build a crypto legal system that embodies the ethos of the blockchain space, one that we can actually be proud of, as opposed to Nick's insecure and aggressive crypto law (that we should be ashamed of).

We cannot allow Nick Szabo to stop us from using crypto law.

Crypto law will become more secure when we let go of Szabo's law. Crypto law without Szabo's law doesn't suddenly become centralized, hierarchical, or captured by existing legal systems.

Even without Szabo's law, crypto law has technical and legal limitations, and it is up to crypto law people to have the judgement to make sure that crypto law operations are not in violation of Crypto Law #1 (Don't Break The Protocol) or Crypto Law #2 (Keep Crypto Law Legal).

But notwithstanding the technical and legal constraints that we cannot escape, crypto law can be almost anything we can imagine, and it can develop to match our changing circumstances.

The future of crypto law isn't set in stone. It depends on crypto legal actions taken by crypto law people.

For my part, I will start by attacking the legitimacy of Szabo's law.

And if the stars align and I have the opportunity, I will break Szabo's law.

Sue me. I don't care. I am prepared to die on this hill.

Links

- https://medium.com/@Vlad_Zamfir/how-to-participate-in-blockchain-governance-in-good-faith-and-with-good-manners-bd4e16846434
- https://medium.com/@VitalikButerin/i-replied-why-i-disagree-with-your-anti-immutability-position-not-the-same-as-disagreeing-with-93694b565e2b

In Defense of Szabo's Law, For a (Mostly) Non-Legal Crypto System

A Lawyer's Response to Vlad Zamfir's "Against Szabo's Law, For A New Crypto Legal System"

By Gabriel Shapiro

Posted January 26, 2019

Lawyers! Are you sick of devs holding all the power in blockchain-land? Do you wish you could go back to the good ol' days when devs came to you with questions about how their software comports with the law instead of you going to devs with questions about how the law comports with their software? Do you feel (or secretly suspect), like no-coiner crypto-lawyer Angela Walch, that it's puzzling to "act as if blockchains are all about math or science when they are really just about people deciding to work together…"?

Becalm thee! Rejoice! Vlad Zamfir, a leading Ethereum developer and sharding theorist, has announced the birth of "crypto-law." Now you can again feel relevant by helping define a new, bespoke legal order specifically applicable to the social governance of blockchain technology (& presumably agreed upon and enforced among some cross-section of devs, users, miners, exchanges, police forces and legislators? but query how that works…). Your job security is assured! Your social standing, restored!

Unless, like me, you think that "crypto-law" in Vlad's sense is something only a non-lawyer could dream-up, and while it may represent the kernel of a very interesting, creative and intelligent approach to blockchain, is in dire need of—well, for lack of a better word, some lawyering.

I'm trying to keep this brief and informal, so, without further ado, I'll just say I disagree with aspects of Vlad's proposal (though think he has the kernel of quite an interesting idea) and present a somewhat hastily hacked-together mix of criticisms and proposed alternatives in the three core proposals that follow:

1. ***We stick with REAL law about crypto rather than trying to invent "crypto law."***

What is "REAL law about crypto?" Well, it turns out a lot of it already exists, in the form of statutes and common law (including the common law of contracts, which allows for a high degree of private ordering), even though the vast majority those laws do not expressly mention (and were articulated long before the invention of) blockchain technologies.

Admittedly, some of this law suffers from either or both of two problems:

(a) Existing law can have gaps regarding blockchain tech, and these gaps should be filled—which can happen when legislators amend, or courts construe, old laws to cover new tech like blockchain. A great example of this can be found in Wyoming's pending

addendum to the Uniform Commercial Code, which attempts to gap-fill the UCC by defining different categories of blockchain tokens, tying them to the traditional UCC rules for a given category where reasonably possible, and creating new rules where necessary—for example, by creating a new concept of "control" for the perfection of security interests in blockchain tokens.

(b) Existing law can have bad (unintended?) consequences or innovation-stifling results when applied to blockchain. Again, this can only be solved by changing the law legislatively or judicially through normal political-legal processes. An example of this, in my personal opinion, are the U.S. federal securities laws, some of which make sense as applied to blockchain (anti-fraud, some disclosure requirements), and some of which don't (Sarbanes-Oxley anyone?)— but which the SEC largely seems to currently believe should apply to many blockchain tokens on a largely wholesale basis. The solution for such issues is to engage with regulators to the extent they have authority to grant waivers and modifications of existing law appropriate to blockchain, or, where that approach is insufficient, to prevail upon judges or legislators to modify the applicable law insofar as it pertains to blockchain.

Despite the limitations described above—which we would expect apply to ANY highly innovative and thus "disruptive" new technology—law is law: the vast majority of it already exists and has enjoyed centuries of testing, debugging and (mostly) conservative, incremental optimizing. Whatever changes need to be made to it to accommodate a new technology like blockchain (and of course, as described above, there are some) cannot be just decided by Vlad Zamfir and other denizens of the blockchain (chainizens? blockchainites? popolo chainos?), no matter how many of them there are or how broadly they agree on it. Rather, the most Vlad and other blockchain devs/users can do is one or both of the following:

→engage in the traditional law-making/influencing process by doing things like lobbying, writing influential thought pieces, voting for the politicians and judges they think will represent their interests when it comes time to legislating and adjudicating, etc; and/or

→enter into contracts (which to be contracts must comply with real contract law, not "crypto law") to agree among themselves to a certain set of governance rules as a matter of private ordering.

Note: The second possibility (private ordering via contracts) is actually really, really powerful, and is a path that could enable chainizens / blockchainites / popolo chainos to do more with law, more quickly, in sort-of-but-not-quite the way Vlad Zamfir might like, than creating a whole new "crypto legal system." I talk more about this possibility at the end of the article, but, for now, suffice it to say that's part of my recommended approach and ultimately means I don't disagree with Vlad nearly as violently as it might appear so far.

2. ***We Preserve Space for the Exploration of Szabo's Law by Letting the Communities Who Want to Use It Do So***

A. What is Szabo's Law?

Vlad describes "Szabo's law" thusly:

> *Szabo's law is simple: Do not implement changes to the blockchain protocol unless the changes are required for the purpose of technical maintenance.*

Most people may not notice it, but defining this as a law, as a law believed by Szabo, and as meaning exactly this "simple" thing are brilliant rhetorical maneuvers on Vlad's part that, if we let them slip by unquestioned, could win half the debate before it has begun. Therefore, we must not do that.

If you read Vlad's article closely it becomes clear that his critique is not restricted to this "law" of Szabo's (which, to my knowledge, Szabo has never defined, and certainly has never defined as a "law"), but rather to what one might more ordinarily and naturally refer to as an "approach," "philosophy" or "ethos" of Szabo's. For example, he repeatedly refers to Szabo as being "insecure" and to various ancillary behaviors of Szabo (described in a not terribly flattering light) that have supposedly bolstered the spread and acceptance of "Szabo's law." Thus, it is clear that Vlad has beef not only with the simple "law" or rule he calls "Szabo's law," but rather also the cluster of norms, assumptions and objectives associated with that "law."

Although I don't agree that the thing Vlad is criticizing is a "law" and think it is extremely confusing and counterproductive to refer to it as such, I ***do*** agree it is a very real cultural force in the blockchain world and is sufficiently discrete that it can be reified, held up, reviewed and criticized, lauded or built upon. Unlike Vlad, I don't refer this real thing as "Szabo's law," but rather as the "social-trust-minimization approach" to blockchain technology. While various people have described and advocated for this approach in various ways at various times, I think it is justly traced to the most articulate and famous expression it has received to date and a personal favorite of mine: Szabo's paper "Money, blockchains and social scalability." Thus, I do not disagree that Vlad is criticizing a real thing—the social trust minimization approach to blockchain—and that Nick Szabo is the poster-boy for that thing.

Nick Szabo and I have one thing in common: we're both lawyers (although in Nick's case he may not be practicing, he has a J.D. and is a very keen and longstanding student of the history of law, and that makes him a lawyer in my book). The similarities end there, since Nick is far more technically adept than I am and spent years developing revolutionary software, and I would venture to guess that I am more legally adept than Nick and spent eight years doing high-stakes deals for real high-stakes clients at real AMLAW10 law firms. But in this case, our similarity in both having a DEEP understanding of the law (rather than one developed mainly, by Vlad's own admission, by reading what I consider a very controversial, scatter-shot and uneven blockchain-focused legal blog) explains why we'd likely both see the merits of social-trust-minimization and arrive at similar conclusions on the issues Vlad raises in his article.

I invite anyone who doubts the merits of at least exploring where social-trust-minimization-via-blockchain can take us to do one simple thing: read Nick's article. I don't have much to add to that, beyond referring back to the gloss I gave it in my article "Tokenizing Corporate Capital Stock":

> *[F]rom a pure performance point of view, blockchains suck. Worse still, there is nothing that blockchain technology can do that* can't *be done on a network utilizing a so-called "client-server/master-slave architecture" …Worse worse still, since these "client-server/master-slave" architectures can rely on centralized coordination mechanisms to achieve byzantine fault tolerance and sybil resistance, they are faster, cheaper and easier to use [than blockchain technology]. Thus, blockchain technology's "unique selling point" (USP) for most applications is not "doing the same exact thing as centralized technologies, but materially faster, cheaper and more conveniently." …[Instead, t]he USP of blockchain technology …is that it furthers the values of individual asset sovereignty by creating the technological predicates necessary for ordinary persons to hold, manage and transact with assets in an environment that is [socially-]trust-minimized while also being secure.*

This is the ***real*** Szabo's law, and how it relates to blockchain, in a nutshell.

B. What is Zamfir's Law?

What does Vlad want instead of the Szaboist (Szabbic? Szaboean?) social-trust-minimization approach? Well, it's frankly a little hard to tell, but one way of interpreting him would be that he would like chainizens to come together and define their own "laws" (albeit not really "laws"—more like just a socially agreed ruleset) for how/when/where to fork blockchains/blockchain protocols, so that they could be forked relatively often, delivering swifter "justice" to the wronged, ensuring the enforcement of non-crypto-law and crypto-law on the blockchain, and facilitating blockchain innovation at a faster pace. So, what I surmise that he wants is a body of rules (including, presumably, meta-rules for how those rules can be amended or supplemented) that everyone agrees on after a long debates whereby, if, for example, Parity has lost funds due to a hack, Parity can submit the issue through some kind of social process (query what that is) and that process would work swiftly, decisively and legally to determine whether, how and in what amounts the funds should be returned to Parity via a fork.

Does this sound familiar at all? It should. IT'S BASICALLY THE CURRENT LEGAL DISPUTE MECHANISM PROCESS, BUT APPLIED TO BLOCKCHAIN UNDER A NEW QUASI-LEGAL SET OF RULES AND A NEW QUASI-LEGAL SET OF JUDGES/LEGISLATORS/REPRESENTATIVES AT THE BEHEST OF A NEW QUASI-BLOCKCHAIN-GOVERNMENT. Essentially what it appears Vlad would like to do is create an entire crypto legal system that runs parallel to, but outside of, without conflicting with or being in violation of, the traditional legal system. Vlad, if I have that wrong somehow, feel free to pipe up and correct me, but you have to admit that although you have been very clear about your critiques of immutability, you have not been very clear in the

alternative about how/when/where mutability decisions would be made under your vision—so, in fairness, I don't have a whole lot to work with on the latter score.

Let's call the law that such a system should exist and should govern blockchains "Zamfir's law".

While Zamfir's law represents an admirable/interesting goal, it is also arguably a very wasteful and implausible one. WE ALREADY HAVE A GREAT LEGAL SYSTEM, BUILT OVER CENTURIES. At least in the United States and other highly developed parts of the world, that is. It becomes a very reasonable and natural question to ask why we think "crypto law" patched together by a maybe motley (albeit maybe lovable) group of crypto enthusiasts is likely to do much better—at least at scale (again, see below under #3 for some contrary points re: private ordering).

C. A Hypo: Why Do Szabo's Law and Zamfir's Law Conflict?

To understand why/how Szabo's Law and Zamfir's law may conflict, and why Szabo's law (or, really, Szabo's social-trust-minimization approach) is something worth preserving/exploring, let's consider a variation on a hypo that personally has been very influential in exciting me about smart contracts on the blockchain and the potential value of social-trust-minimization as applied thereto.

1. You live India.
2. I live in the United States.
3. We meet on /r/mechmarket and I learn you have a fancy custom keyboard —brass weight, carbon fiber plate, HHKB layout, retooled vintage nixendorf switches, full RGB with hotlites, types like a dream—I'd like to buy.
4. We have the idea of entering into a contract where I agree to buy and you agree to sell your keyboard for $1,000.
5. For keyboard deals, payment in advance is customary, and, moreover, you are not willing to send me the keyboard unless I first pay you the funds.
6. But in doing my due diligence, I learn that India has a notoriously inefficient, byzantine legal system that is hard for even Indians (no less Americans like me) to navigate successfully—clearly, if I pay you, but you breach the contract by failing to deliver the keyboard, I am effectively going to have no remedy, since there is no way I am going to endure the time and expense of suing you in India—particularly since it's unlikely I'll get a satisfactory remedy even if I do.
7. I therefore consider doing the agreement under U.S. law, but then realize that even if I clearly, quickly and efficiently prove a breach of the contract under U.S. law, it will do me no good unless I can enforce the judgment in India where you and the keyboard reside—thus all the problems of the Indian legal system remain unavoidable.
8. But, I have an idea—"let's do the deal through a trusted intermediary!" "If we use PayPal," I say, "PayPal will effectively insure me against the possibility of your fraud. If I don't get the keyboard from you after paying for it, PayPal will refund me. While that's not as good as being able to get "specific performance" of the contract as a

remedy (i.e., a court forces you to deliver me the keyboard you agreed to sell) like I would be able to do if you were in the U.S., at least I will have *a* remedy, which is better than no remedy, and I think for the sake of being able to do a deal to get this dank-ass keyboard, that's a risk I'm willing to take."

9. You don't like that idea, though, you tell me, because PayPal places almost all the risk of a fraud claim on the seller. PayPal also charges the seller transaction fees, which is part of how it makes economic sense for PayPal to insure the risk of fraud in these types of transactions—in effect, me using PayPal means I am paying a lower price for the board as a discount reflecting my distrust in the Indian legal system. Finally, you note that it so happens you have been burned by PayPal before—you sent someone a keyboard bought through PayPal, and the buyer attempted the non-blockchain version of a "double-spend" by immediately filing a claim with PayPal for non-receipt, which resulted in the purchase price funds being held-up at PayPal for six months while PayPal investigated the claim. Even worse, PayPal got it wrong and decided against you, and thus you were out both your keyboard and your funds, with no effective remedy—since you were no more willing to wind your way through U.S. courts for a $1,000 claim than I would be willing to wind my way through Indian courts. You will never forgive PayPal, don't trust PayPal, and believe PayPal has a pro-American bias and will never give you a fair shake.
10. I don't trust India's legal system, and you don't trust my proposed intermediary (PayPal) that would enable me not to trust India's legal system. What do we do?
11. *The Arena Lights Dim*
12. *Metallica's "Enter the Sandman" Fades Up*
13. *Lights Start to Twinkle, Digital Coins Cascade on the JumboTron*
14. *Blockchain Enters the Arena, Strutting like Ric Flair in his Prime, to Thunderous Applause*
15. What about this? Let's say you know code, I know code, and we both have a strong confidence level about the way a particular blockchain and code on it works. What could we do then?
16. Although you don't trust PayPal, and I don't trust India's legal system, in general, any two people can find at least one other person they both trust. And in this case we have —/u/Ripster—a paragon of virtue, a hero, a legend in the mechanical keyboard community, who (we'll posit) conveniently happens to be located in the United States within driving distance of me.
17. Now, couldn't we do something like this?

→deploy a smart contract on Ethereum that we both feel we understand

→I deposit $1,000 worth of ETH there

→the smart contract gives Ripster's private key the sole authority to either send the $1k to you (upon successful delivery of the keyboard) or back to me (if keyboard isn't delivered by deadline x)

→you mail the keyboard to Ripster

→Ripster releases the ETH via a transfer command sent to the smart contract, signed by his private key (or first shows me the keyboard so I can inspect it and then releases the ETH)

→I take the keyboard from Ripster.

THIS IS MY (AND, I SUSPECT NICK SZABO'S) DREAM FOR BLOCKCHAIN. One can play with the details and probably imagine ways that social trust can be even further reduced, but the point is that this technology opens up massive, massive opportunities to enhance dealmaking through private ordering. Deals that wouldn't be done, or would only be done more expensively or with more problems and risks, can get done, or get done more cheaply or with less drama, leveraging blockchain than not. Or, at least, such is the dream—it is up to us to make it a reality.

However, you know what could really potentially limit the value of this dream? That's right , you guessed it— Zamfir's law could. Notice again #15 in my hypo. For this scheme to break our dealmaking logjam, it is critical that we eliminate all forms of trust other than the two forms of trust we happen to share—social trust in Ripster and mathematical/computational trust that such-and-such smart contract code deployed on such-and-such blockchain will lead to such-and-such predictable results. But if the blockchain can be changed through a socio-legal but extrajudicial "crypto-law" process, there is an additional piece of social trust we need beyond that of our shared trust in Ripster—trust in "crypto law" and the people that apply it. To me, this is a major problem and could drastically undercut the potential benefits of blockchain.

Of course, Vlad and critics like Angela Walch will point out that such trust is always needed—even Bitcoin, the most change-averse blockchain, *can* be changed, and thus in using Bitcoin I am "trusting" those who could change it adversely will not do so. But, as a general matter, what is easier to trust:

(a) a blockchain "governed" by a highly ingrained, time-honored and widely touted "Szabo's law" that both in theory and practice means the blockchain is almost never changed except for super important reasons that nearly any reasonable person would agree upon? or

(b) a highly complex Zamfir's law/"crypto law" that, in practice and by design, entrusts the decision of whether, when and how the blockchain is changed to a group of people, the complex principles they have agreed upon and the particular way that they might decide to apply those principles in a given case?

I would submit that, in general, the blockchain governed by Szabo's law is easier to trust, and thus in a certain sense helps "minimize trust," or minimize the amount or complexity of trust, that is needed to facilitate private ordering via blockchain, whereas Zamfir's law vastly increases such trust, and thus begs the question of why blockchain would even be preferable to existing alternatives that also require high amounts of social trust. ***After all, isn't it possible that you distrust "crypto law" and its administrators just as much as I***

distrust Indian law, and that therefore by using blockchain we would merely shift, rather than solve, the trust problems that led us to consider using blockchain in the first place?

On the other hand, here is what I will acknowledge: people can have very different preferences for what they place their trust in. Some people (presumably like Angela Walch) see everything as "ultimately being about people" and have little faith in or desire for automatic, mathematical decision-making. Others (like me and presmably Nick Szabo) think there is huge promise in being able to make deals while minimizing the number of people, social variables and social institutions that must be trusted to do so, and the degree of trust that must be placed in those things to whatever extent such trust is needed. It's a free world, and there's lots and lots of room to have different technologies, and even different blockchains, that cater to those varying preferences.

This brings me to my next point.

D. Why Are Szabo's Law and Zamfir's Law, Despite Conflicting, Not Mutually Exclusive?

I think Reluctant Raccoon put it well:

Long story short: there are different blockchains. Some can use Zamfir's law. Some can use Szabo's law. One can even fork a given blockchain that uses Zamfir's law or a given blockchain that uses Szabo's law, and try convincing people to instead apply Szabo's law to the forked version of the former or Zamfir's law to the forked version of the latter . We can let the market and history decide which approach is better (either absolutely for all

purposes or relatively for some purposes). There is no need to call for a repudiation of either, or to condemn either. Let the world experiment.

3. ***We Preserve Space for the Exploration of Zamfir's Law by Letting the Communities Who Want to Use It Do So—But Through Private Ordering (Contracts) Rather than "Law"***

As described above in point #1, in my opinion "crypto law" as Vlad seemingly conceives it (something voluntarily agreed upon by a cross-section of blockchain people) is neither a necessary nor viable alternative to what I'll somewhat comically call "legal law"—I mean real law, the law established by states and enforced by threat of coercion in the form of violence, imprisonment and/or deprivation of property. You know, "old-fashioned" law—your Dad's dad's dad's law.

HOWEVER, you know what Vlad's "crypto law" sounds like, aside from the ill-advised name for it? Oh, I don't know, how about "governance agreed to via contract in a system of enforceable private ordering"? I know that's a mouthful, but isn't that, at the end of the day, both what he is apparently really proposing and all he really needs? Corporations do this. LLCs do this. Private parties making deals do this. All the freaking time. And legal law, real law, helps them.

I don't really like/support EOS, but one interesting feature of EOS is that it combines blockchain tech with wet contract tech via a purported "constitution" written in natural language and inscribed to the EOS blockchain in a Ricardian fashion. I've been very critical of the particular way the EOS powers-that-be decided to implement that approach, and one can query whether their constitution is enforceable and quibble with the extra-legal manner in which it has been enforced. Also, in general I share Vlad's concerns about on-chain governance (and so really I just disagree with him, as I hope I'm elucidating here, about the extent to which blockchain governance (whether on-chain or off-chain) is necessary or advisable). ***However***, the core of the idea behind the EOS constitution—i.e., combining blockchain technology with a sort of contractal "terms of service" and potentially a "terms of forking" for its various users/maintainers—is very interesting and potentially powerful, and might be a great way to implement ideas like Vlad's within the framework of existing law.

For example, AFAIK there is nothing to stop Vlad from forking Ethereum, declaring that his version of Ethereum can only be used in, modified by, or participated in by people who sign (under whatever meaning of "sign"—might include a click-through agreement) a contract that agrees that all disputes regarding stuck funds, hacks, forks, whatever other issues will be decided by a "Council Of Vladdites" who follow "Crypto-Law"—as defined on Exhibit A thereto and as it may be amended or supplemented from time to time pursuant to Crypto Law #5 regarding amendments. That would seemingly achieve most of what Vlad wants to achieve by rejecting Szabo's law, but would not do so at the expense of eliminating the existence of systems that happen to like and/or just want to play with and explore the possibilities of Szabo's law.

I would humbly ask—what is wrong with this version of "crypto-law"? What is wrong with an approach that utilizes current truly legal contract law to allow a community of like-minded people to come together and have a sophisticated blockchain governance system for a particular blockchain, thus enabling it to fork often? I see nothing wrong with it. I'd even love to see it adopted and experimented with, and of course as a lawyer I would kill to be able to help advise what the contractually agreed "crypto law" should like. As a lawyer it'd be like advising on one of the coolest deals of all time—a deal to set up a platform for deal-making!

But I also do not see why this model should be universal or why it should be the ***only possible*** type of blockchain. And one question I have for Vlad is whether that is part of his position, or whether he just wants crypto-law to be one of many options for blockchain. One might argue (and I suspect, but am not sure, that Vlad would/will argue) that blockchains are "too dangerous without crypto law".

But why? "Legal law" still exists, no matter what we do, and legal law can regulate blockchain's dangers just fine. Maybe not ***perfectly***, but fine. And such law will continue to evolve, and get better, as we lawyers grapple with this fascinating new technology. Why presume in advance that it is unworkable and try to impose a parallel "crypto law" that essentially depends on the existence of a new "crypto state"? For all we know, the "cure" to blockchain's supposed dangers could end up being more corruptible and dangerous than the disease. And, if experience is any guide, when new governments/legal systems are set up from scratch, they usually suck, give power to weirdos, and end up as catastrophes. There is good reason to be cautious.

Conclusion

Vlad is quite a brilliant and interesting fellow, and I'm glad he's working on and publishing his ideas—including those about blockchain governance and "crypto law." That doesn't mean I can't criticize them. Just as if I were to write some screed about some aspect of coding, I would most likely badly mangle it in one way or another, but maybe also strike upon some interesting ideas, I analogously believe (truly without knee-jerk condescension) that Vlad is missing quite a few nuances about law and governance as he has ventured into legal terrain while being a non-lawyer. ***BUT,*** to Vlad's credit, there is nevertheless quite an interesting idea he has implicitly cottoned onto— namely, that of combining blockchain technology with the power of private ordering via legal contracts. I would humbly suggest that this (perhaps combined with some real legislative and regulatory lobbying), rather than proclamations about how blockchain governance should be, what "crypto laws" should be created, etc., would be a much more constructive frame within which to tackle the issues Vlad is, very very rightfully, concerned about regarding the maximization of blockchain's benefits and the minimization of its harms.

I would welcome further dialogue with Vlad or anyone else interested in these topics.

Links

- https://twitter.com/angela_walch/status/1083069503335002112
- https://medium.com/@Vlad_Zamfir/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827
- https://wyoleg.gov/Legislation/2019/SF0125
- https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html
- https://gabrielshapiro.wordpress.com/2018/10/28/2/
- https://twitter.com/ypical_
- https://github.com/EOSIO/eos/blob/5068823fbc8a8f7d29733309c0496438c339f7dc/constitution.md
- https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

Crypto Governance: The Startup vs. Nation-State Approach

By Jack Purdy

Posted February 25, 2019

Intro

Humans like to argue. It's in our nature.

Take any facet of human experience and you can find two people who disagree on it. Nowhere is this more prevalent than in the realm of governance, where we argue who should have power, who gets to make changes to the system, and how decisions are ultimately made. Given the magnitude of the impact governance has, it is easy to see how this became a highly controversial topic.

Now imagine a nascent industry full of highly intelligent people with strong opinions (and egos), where most of the debate occurs on globally accessible platforms. As you can imagine, there is no shortage of debates especially as it pertains to governing this industry. Welcome to crypto.

Crypto governance encapsulates the debates around how we coordinate to make decisions on changing the rules of a protocol. This could include anything from simple upgrades to changing the consensus mechanism to allocating block rewards. It involves many stakeholder groups such as node operators, network providers (miners), core developers, users, speculators, exchanges, and block explorers to name a few. These are diverse groups with varying incentives that frequently conflict with each other. For example, node operators want to keep block size low to reduce the costs of running a full node, while miners have incentives to increase the block size so each block includes more transactions and thus more transaction fees.

It is the interactions between these stakeholder groups that define what a blockchain is, its values and principles and how it evolves over time. This governance process shapes the imagined reality we create surrounding a network, and the value of a cryptoasset lies at this social layer.

Unsurprisingly, there has been a substantial amount of debate on the right way to govern cryptonetworks, which has created various thought-provoking theories. I believe much of the debate is misguided since 'crypto' is too general of a term to apply overarching ideas to. Jill Carlson explains it well:

> *Often investors attempt to apply the same priors and heuristics whether they are talking about bitcoin, petrocoin, or filecoin because they are all "crypto". This would be akin to applying the same fundamental analysis to gold markets, sanctioned Venezuelan debt markets, and the pre-IPO valuation of Dropbox circa 2008.*

In the same way we shouldn't apply the same fundamental analysis for these assets, we shouldn't analyze the governance of all cryptoassets in the same manner. We need to more accurately describe what is being governed in order to think about how it should be governed. In this analysis I'm going to delineate between base layer protocols from those further up the tech stack. The former should be governed like an established nation, while the latter an early stage startup.

The Startup Approach

> *"Moving fast enables us to build more things and learn faster. However, as most companies grow, they slow down too much because they're more afraid of making mistakes than they are of losing opportunities by moving too slowly. We have a saying: 'Move fast and break things.'The idea is that if you never break anything, you're probably not moving fast enough"—Mark Zuckerberg, IPO Prospectus 2012*

Zuck encapsulates this governance theory in the now famous mantra of "move fast and break things". When you are looking at early-stage, user facing applications, you need to be responsive to customer needs. This requires the ability to rapidly iterate in order to meet these changing needs. If you move too fast and there is a bug, it is not the end of the world since there is not a tremendous amount of value in the network. You fix it and move on. **The key is that the stakes are low so there aren't grave consequences if something goes wrong. Failure will not result in large personal losses or a complete loss in faith in the idea ever working again.**

Now what will this governance look like in crypto? It will likely operate like a well-oiled autonomous organization. A good example of a cryptonetwork that caters to this style of governance is Decred. (Note: Given Decred is aiming to be used as money, I am somewhat skeptical if this model makes sense for them, but regardless it is a general model I believe can be effective for more rapid improvements). Decred utilizes on-chain voting to allow DCR holders to participate in the governance process by staking tokens in order to obtain tickets. This lets stakeholders vote on matters such as how the treasury funds are spent to support development or whether consensus changes should be implemented via a hard fork. Placeholder summarized it best—"Decred's killer feature is good governance, and with good governance you can have any feature you want." **This thinking enables the necessary innovation needed to keep up with consumer needs and avoid a slow descent into irrelevance.**

"Move fast and break things" succeeded in turning Facebook from a scrappy startup to a unicorn, but once they reached scale and had data on 2 billion people, that mantra was no longer appropriate. With that many people at risk, breaking things is no longer the goal or even acceptable for that matter. Rather the goal should be keeping the system secure, and unfortunately Facebook failed at this exposing the data of millions.

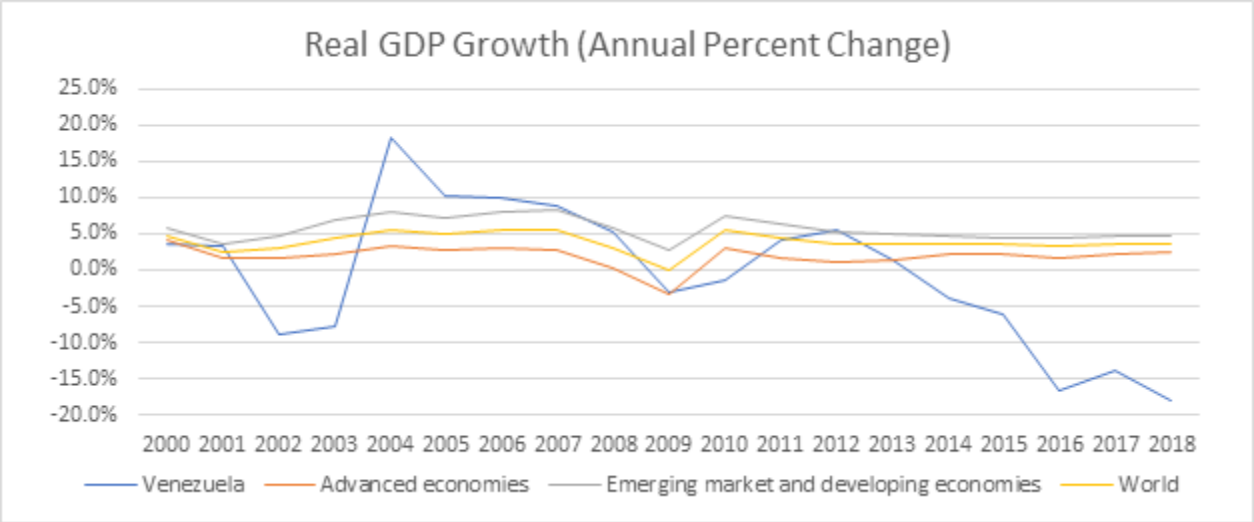
This brings us to our next approach that starkly contrasts with that of the early startup.

The Nation-State Approach

> *"We have to reinvent socialism. It can't be the kind of socialism that we saw in the Soviet Union, but it will emerge as we develop new systems that are built on cooperation, not competition."—Hugo Chavez to World Social Forum 2005*

In January 2005, Hugo Chavez was embarking on a mission to re-shape Venezuela. That month he passed land reform allowing the government to seize over 6 million acres of private property. Two years later the government took over the last privately run oil field, with the banks following shortly after. The drastic measures taken by no means stop there, and they continue to this day.

This example is not meant to make a political statement, but simply to demonstrate what can happen when a government attempts to make rapid changes that are unproven and largely experimental. This is a highly simplified illustration and there are a multitude of factors at play but that shouldn't distract from showing the risks of this type of governance. The results of these actions are widely known and evidenced by the graph below.



1 Source: IMF

When there are high stakes on the line to the underlying people, corporation, protocol etc. being governed, then the manner in which decisions and changes are made needs to optimize for the safety and security of those governed. No longer is the motive to innovate in order to outpace competitors because survival is the only way to win out.

Applying this to crypto, base layer protocols such as Bitcoin cannot afford to move fast at the detriment to security. When I refer to security here, I am talking about maintaining the well-being of bitcoin holders. This means not only ensuring the protocol doesn't break, but upholding the censorship resistance, trust-minimized features that keep these holders secure. **A 10x improvement in transaction speed or fees is not worth a 1% decline in security. If a critical bug is exploited or a users funds confiscated, it will be incredibly**

difficult to regain people's trust in not just Bitcoin but the entire story they tell themselves surrounding a decentralized money. This is because technology such as Bitcoin is prone to the Lindy Effect, where the future life expectancy is proportional to its current age. Therefore, the longer it survives, the longer it is predicted to survive. If it fails, it not only starts from where it began but behind since its competitors (namely fiat) are now even more Lindy.

While it can be easy to get frustrated with the slow process to upgrade Bitcoin, it should be noted that extreme caution needs to be taken in changing base layer protocols where significant value rests on top. **Valuable networks like Bitcoin need to be governed like national governments, where it is more important to reject unjust laws then to pass just laws**. The more active governance is in a cryptonetwork, the more one requires trust to interact with it and the whole raison d'être of a decentralized currency is to minimize trust in others. Bitcoin developer Matt Corallo states:

> *Of Bitcoin's many properties, trustlessness, or the ability to use Bitcoin without trusting anything but the open-source software you run, is, by far, king. More specifically, interest in Bitcoin appears to almost exclusively derive from a desire to avoid needing to trust some third party or combination of third parties.*

This applies to other base layer protocols where there are expected to be valuable dapps built on top of it. In the same way one would be hesitant to incorporate in a country where the laws governing its business are prone to change at anytime, one should be wary to build dapps on top of a protocol that requires trust that the rules wont change in a detrimental fashion. **While this is not an apples to apples comparison, I believe it is useful in highlighting the fact that high stakes situations where there is considerable value on the line necessitate a more ossified governance structure to mitigate risk for the governed.**

Conclusion

Often times in crypto, we like to believe were reinventing the wheel. Accordingly we come up with unique heuristics and terminology to describe things. While in some cases this is true, often times we're simply repurposing age old ideas to fit this new paradigm. I believe governance is one of these areas where we can learn from a lot from the past. For thousands of years humans have been organizing themselves in different groups to coordinate around shared goals in the form of nation-states, corporations and others social groups. Over time we have improved our standard of living as a result of organizing ourselves into these groups and evolving new ways to govern them. However, innovation in this front has been slow due to the difficulty in testing out alternate approaches (rightfully so) because of the high stakes on the line.

This is a big part of why I am so fascinated with cryptonetworks. They provide us a sandbox to try inventive new ways to organize human behavior by shifting how we incentivize participants. By carefully studying the failures and successes of different crypto

projects I believe we can learn more about governance and at a faster pace then has ever been possible. A great analogy is comparing them to petri dishes, where we can test out different ideas on smaller chains and based on the results begin to implement bits and pieces into more established chains.

This shouldn't be a black and white approach, but more of a spectrum based on the amount of value in the network and trust minimization required. **On one end you have Bitcoin that needs to iterate slowly, preserving security at all costs and at the other you have experimental petri dishes that can test the efficacy of new models and look to incorporate them gradually down the tech stack as they grow stronger via the Lindy Effect.**

To conclude, I believe instead of making overarching "laws" about crypto governance like Szabo's Law, we need to take a more nuanced approach. My hope here was to start separating the governance of mission critical base layer from protocols from more application specific crypto projects. I look forward to expanding my thoughts on the subject in order to further delineate the ways in which cryptonetworks should be governed.

Much of my thinking was influenced by prior work that includes:

- Bitcoin Governance
- The Crypto Governance Manifesto
- Blockchain Governance 101
- Blockchain Communities and their Emergent Governance
- Blockchain Governance: Programming Our Future
- On Governance: Coordination, Layers, and Structural Integrity
- Cryptonetworks and Cities: Analogies

Links

- https://medium.com/s/story/bitcoins-social-contract-1f8b05ee24a9
- https://medium.com/@jillcarlson
- https://medium.com/@jillcarlson/crypto-is-not-an-asset-class-dd28597951b3?ref=tokendaily
- https://multicoin.capital/2018/07/10/the-web3-stack/
- https://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm
- https://medium.com/@placeholdervc
- https://www.placeholder.vc/blog/2018/5/12/decred-investment-thesis
- https://www.bloomberg.com/news/articles/2018-04-04/facebook-says-data-on-87-million-people-may-have-been-shared
- https://www.nytimes.com/2005/01/30/world/americas/venezuela-land-reform-looks-to-seize-idle-farmland.html
- https://www.seattletimes.com/nation-world/chvez-finishes-nationalizing-venezuela-oil/
- https://worldview.stratfor.com/article/venezuela-bank-nationalizations

- https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEOWORLD/VEN
- https://medium.com/incerto/an-expert-called-lindy-fdb30f146eaf
- https://en.wikipedia.org/wiki/Raison_d%27%C3%AAtre
- https://medium.com/@TheBlueMatt
- https://medium.com/alpineintel/on-governance-futarchy-6a6fa2c012b
- https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827

Cryptonetwork Governance as Capital

By Joel Monegro

Posted February 19, 2019

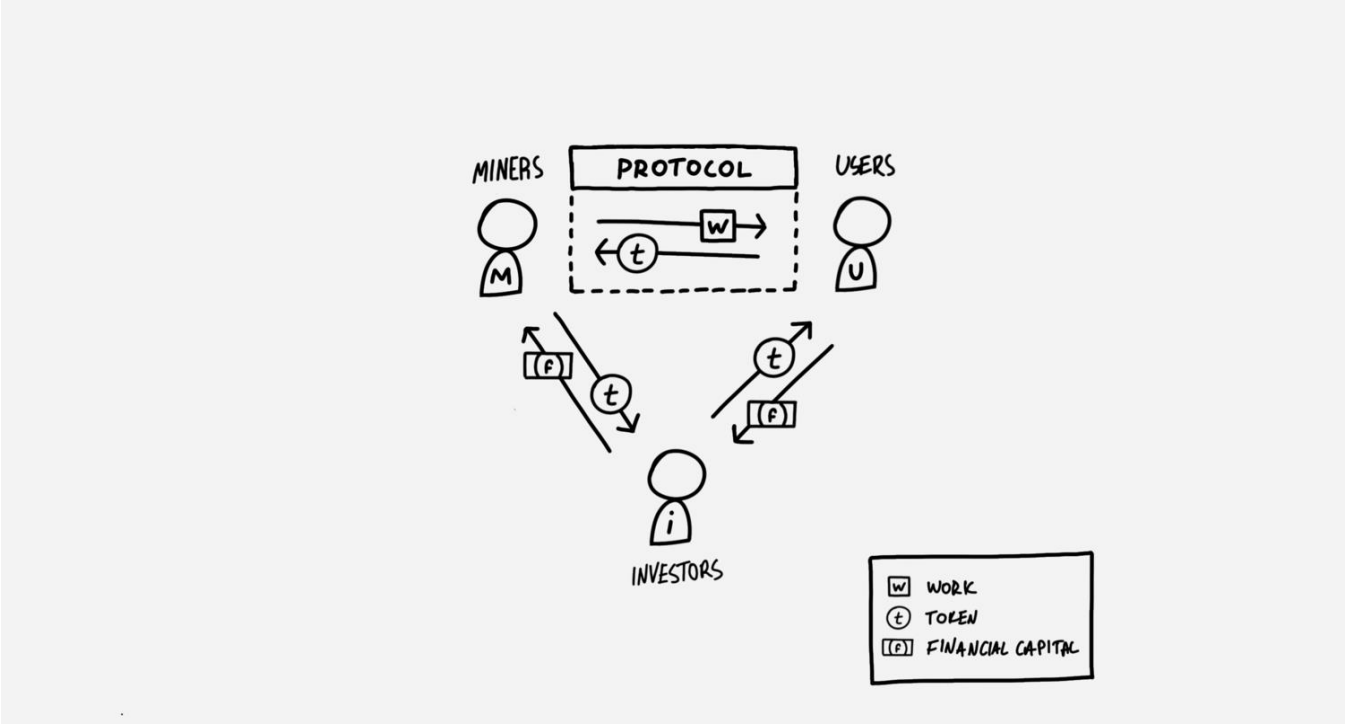
Capital is, in essence, *the power to organize the economic resources of a social system*, and its worth a function of how much of those resources can be directed to the holder's benefit. This understanding reveals the inherent value of *cryptonetwork governance as capital*, and helps us understand tokens with governance rights as new kinds of capital assets.

All forms of capital offer some kind of control over the distribution of economic resources across a group of people – in effect, *governance* over that pool of resources. Productive and human capital, for example, influence which goods and services are offered in the economy (and thus how income is ultimately distributed), financial capital determines the distribution of purchasing power, and equity capital presides over how a company's resources are used. Intangible forms of capital also exhibit this quality: political capital, for example, governs the rules of markets, and social capital drives human attention (and thus behavior).

This insight, that capital is governance (and vice versa) leads to the source of its intrinsic value: whoever has control over a pool of important resources also has the potential to direct some of those resources to their own benefit, so the value of a system's capital can be considered proportional to the value of the resources it governs.

This relationship is very clear in the case of corporate equity, where the value of a share of stock (which is essentially a voting instrument) is rooted in its right to a piece of the company's book and profits – its 'assets under power', so to speak. The relationship is less clear in the intangible realm, where capital does not take the form of tradable assets that can be priced by the market, but remains present nonetheless. For example, we might look at the global cost of corruption (about $3.6 trillion/year, or 5% of the economy) to assess part the value of political capital, even though "political capital" is not constructed to produce direct economic gains for its holders. Similarly, we might observe the ability of social media influencers to profit from their fame, even though having lots of followers does not by itself guarantee a right to financial benefit.

This relates to cryptonetworks insofar as they are a new form of social organization. It is useful to think about these ideas through the cryptoeconomic circle, pictured below:



The Cryptoeconomic Circle

The two pillars of trust of a cryptonetwork are its cryptoeconomic and governance models. The cryptoeconomic model defines 'the rules' of the system (what is the unit of work, how do users pay, how miners are compensated, the token supply model, etc.), while the governance model defines who has the *power* to change those rules, and under which conditions.

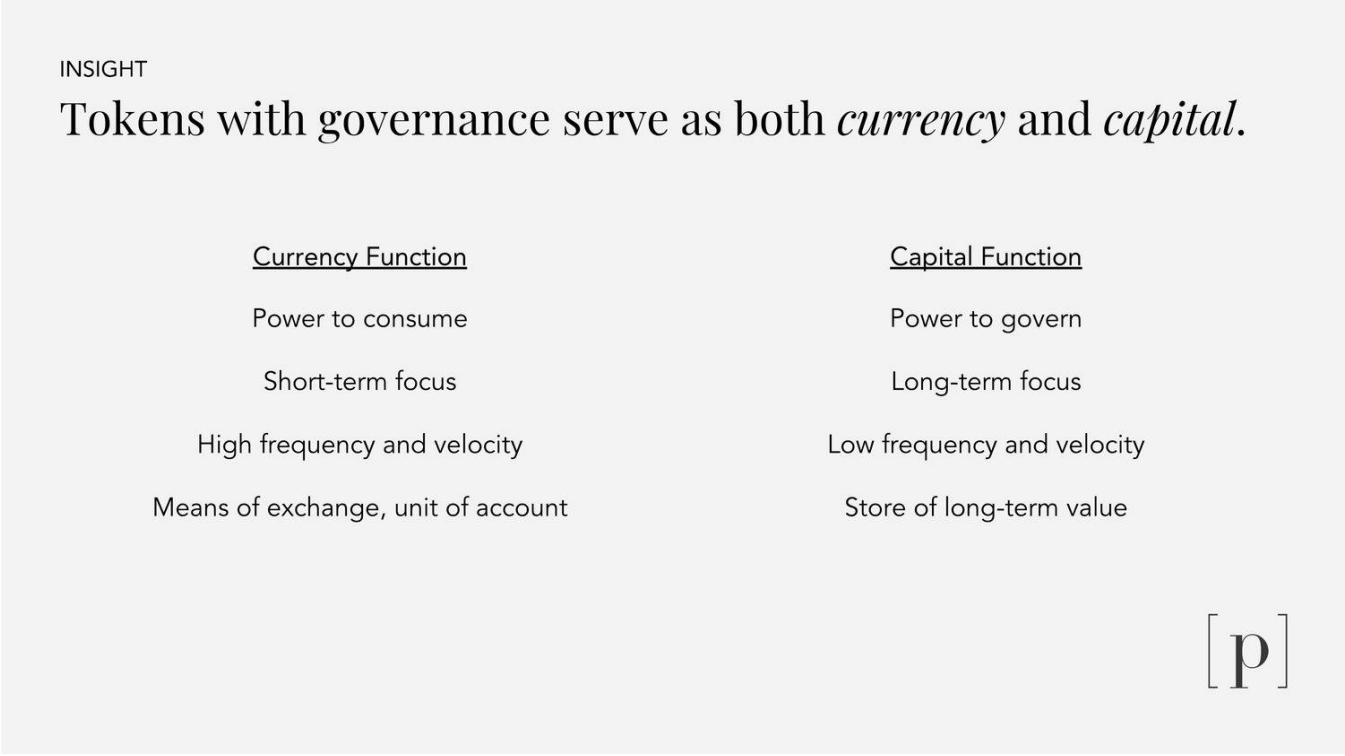
If capital is the power to organize economic resources, then the power to change the rules of a cryptonetwork forms its capital. And when that power takes the form of a token, it can be traded, priced and modeled by market. In this context, a network's 'assets under power' include (1) the token itself, which is controlled by the cryptoeconomic policy, (2) productive resources, as controlled by the definition of 'work' (e.g. the consensus protocol), and (3) flows of value, as controlled by regulating payment mechanics and other incentives for miners, users and investors. And as the value of these resources grows, so does the value of the capital which governs them.

Certain proof-of-stake systems are good examples of this idea. Here, miners are required to lock a certain amount of tokens in order to be allowed the right to work for the network. The value which flows from users to the supply side is then distributed to miners proportionally to their stake. This way, tokens that can be staked are a form of capital in that they represent the power to organize some of the economic resources of the network, such as production capacity and distribution of income. And ultimately this is a form of governance, in the sense that staking is a mechanism for deciding how income should be

allocated across miners. And so, as the value of that income grows with user demand, so does the value of stakeable tokens.

For example, in Decred, 30% of the block reward is reserved for users who participate in its proof-of-stake consensus layer, and that reward pool is divvied up in proportion to how much $DCR each participant has staked. Here, $DCR is a form of capital as it has power over how some of the block reward is distributed. But because Decred also allows the PoS layer to vote on the use of its community pool (which is funded with 10% of each block), as well as on protocol upgrades, the value of $DCR as a capital asset extends beyond what is connected to block-reward revenues. Such power is harder to quantify, and therefore difficult to price, but remains an important value driver that we might consider a kind of "governance premium".

I first presented the thesis that governance is capital (and thus the driver of long-term token value) at the Token Engineering meetup in New York in early 2018, where I showed the following slide which describes the features of what I now call ***power tokens***:



Slide from TokenEngineering talk *On The Price and Value of Governance*

The basic principle behind power tokens is that they fuse the features of "utility tokens" and "governance tokens", which really means the combination of currency and capital –

with the capital function being the driver of long-term value. We'll dive deeper into power tokens, the nuances, and why this combination is important in the next post in the cryptocapitalism series. But for now, the key insight is that what we're dealing with in the creation of these new assets is the creation of new forms of capital, *network capital*, that is natively digital, and cheap to distribute – and that's important.

Links

- https://www.un.org/press/en/2018/sc13493.doc.htm
- https://www.placeholder.vc/blog/2019/1/5/the-cryptoeconomic-circle
- https://decred.org/
- https://www.youtube.com/watch?v=Mwv4nnvTI5E
- https://youtu.be/Mwv4nnvTI5E?t=250

Politics, Power & Protocols

Insights from (available) on-chain governance data

By Meltem Demirors

Posted February 5, 2019

Ah, humans. What wonderful and mysterious beings we are. Millennia of human history have shown us that the systems we create, especially our systems of politics, are inherently fragile and often extremely flawed.

As you consider the following discourse—please remember:

1. We are complex creatures who are ***predictably irrational*** in our behavior; we often build rules to protect us, from us.
2. The pursuit of an ***optimal structure for governance has plagued every 'tribe'*** (society and organization) since human consciousness; and is ***still an unproven experiment (outcome TBD)***. Look no further than the fragility of our existing 'democratic structures' for evidence.
3. Governance occurs ***both within and between*** the institutions and entities that make up a system. Despite popular belief—***it is not a static and fixed process.*** It is ***largely dynamic and evolutionary;*** dependent on interactions of actors in systems.

Governance for the sake of this conversation, is broadly defined as the set of processes that comprise how a state, market or system 'makes rules'.

The familiar mechanisms of governance include: ***laws; cultural and social norms; language***.

Historically speaking, these are administered via both soft and hard expressions of power through ***violence, coercion, collusion*****;** and other more subtle mechanisms like ***social signaling*** and ***virtue signaling***, ***appeals to authority***, and the like.

Collectively, the whole of these make up the nebulous idea of "governance."

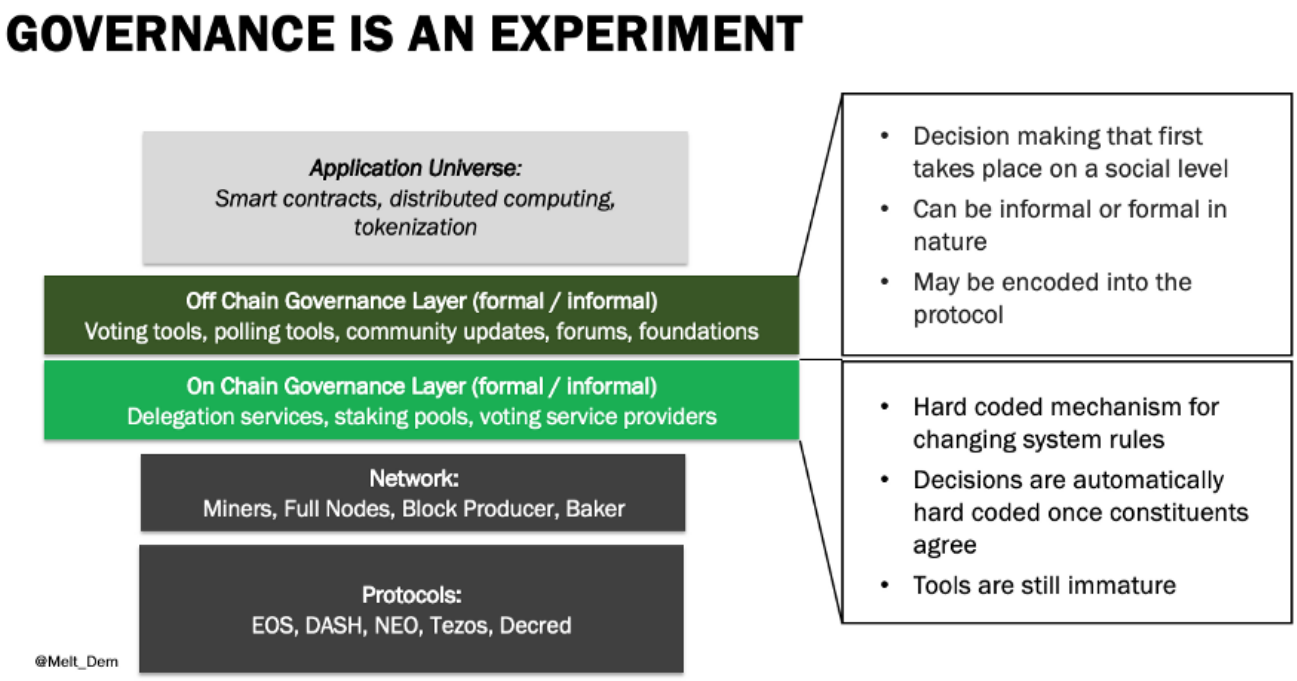
> ***Sidebar:*** Much pontification has been done about the nature of on-chain and off-chain governance, as well as formal and informal governance mechanisms. Instead of providing a thorough review of this literature here, I will simply state that there are as many opinions as there are individuals expressing these. As you'll likely agree, the optimal form of governance for each of us is that which serves our individual preferences and benefit, regardless of how deeply and ardently we justify and rationalize these arguments. I am frequently confronted with my own biases and rationalizations for these, and must confess, I often question my own incentives in engaging in these debates.

One of the pursuits of blockchain-based systems is the attempt to express governance at the 'protocol level' by codifying it into the function of the network itself—this post represents a summary of my current thinking on crypto governance experiments as they currently stand:

> …Remember, Governance of human systems, organizations, and networks is still an unproven experiment (outcome TBD). Look no further than the fragility of our existing 'democratic structures' for evidence…

It turns out that translating or iterating on these historical analogs in 'blockchain land' often leads to similar results.

Let's take a look—in my view, current expressions of blockchain governance look like this:



When the Aragon team asked me if I'd like to speak at their conference, it became a great forcing function to summarize my current thinking on crypto governance experiments as they currently stand…

I by no means believe my thoughts are unique or authoritative, and the process of informing my thinking by using data—as shared in the graphics that follow—was a hard fought battle indeed. More on this at the end.

Politics and power motivated my writing on Tezos over the summer—and this topic continues to fascinate me because the dynamics of most crypto protocols still revolve around quasi-political influencers who battle one another for influence and authority in the no-(wo)man's land known as 'Crypto Twitter.'

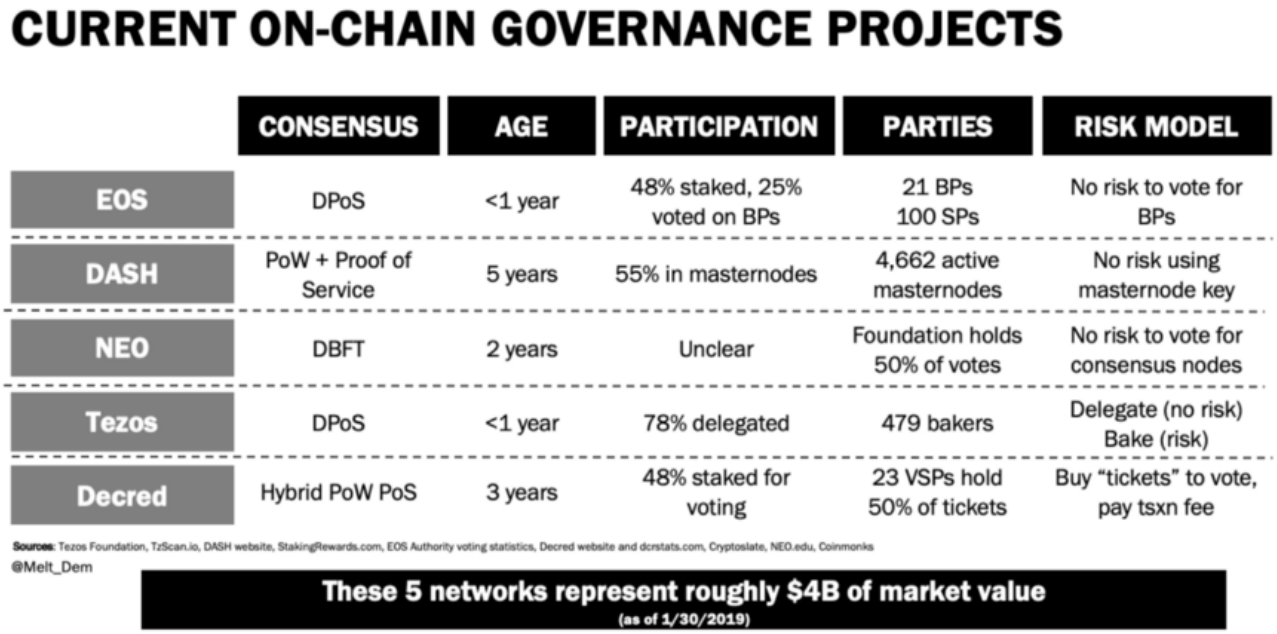
So, let's begin with the most basic question.

Who Has The Right to Govern?

For the purposes of this piece, I decided to focus on the five largest networks deploying on-chain governance today, since this would give us some empirical evidence, however imperfect.

Here is a brief summary of these five networks, who has the right to govern each, and how participation varies based on these dynamics.

> **One More Side bar (I promise):** I want to be careful not to conflate Proof of Stake, which is a consensus mechanism for securing the network, with governance—which is the process of decision making about changes to the network and how to utilize resources dedicated to the network. There is an emerging trend within protocols of using the same "Proof of Stake" tokens to vote, but there is a difference in function here, just using the same tokens (as opposed to systems like Aragon which have their own second, independent token dedicated to "voting.") For the purposes of this post, I am talking about using tokens for governance, not security and sybil-resistance.



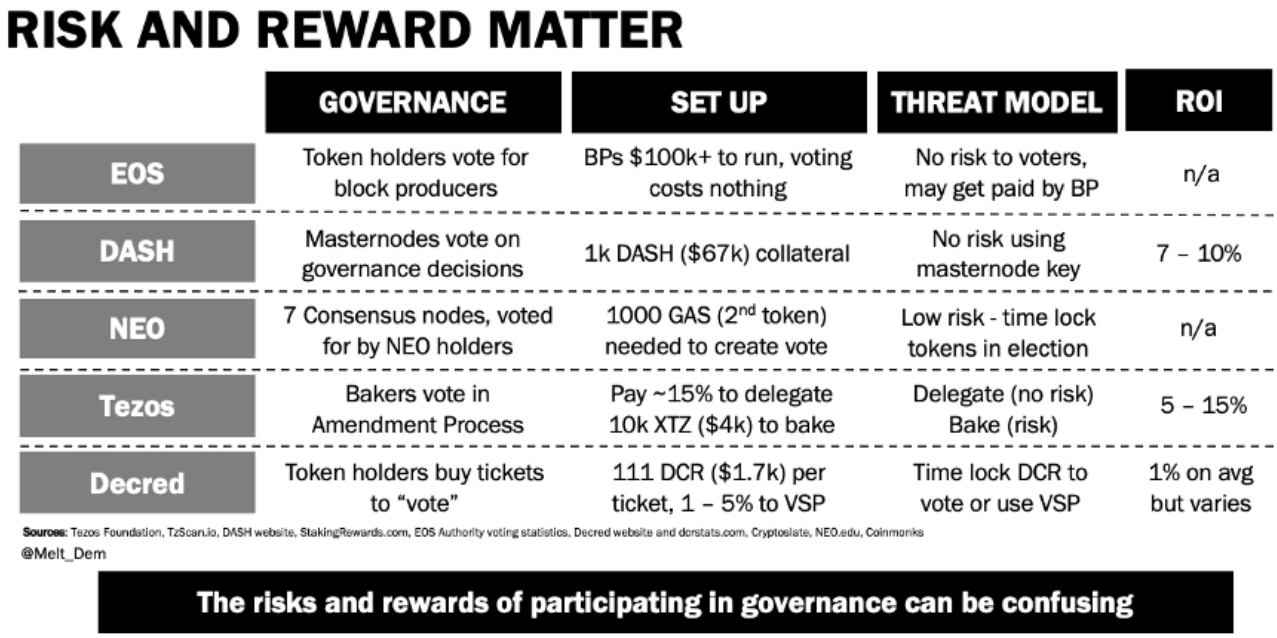
Disclosure: I participate in Tezos governance via Tezzigator, a baker and delegation service. You can see all of my investments and token holdings here.

Three takeaways from this grid —

1. Each network has its own, nuanced mechanism for governance and these slight nuances make "participating" in each network incredibly time consuming.

2. The risks associated with "participating" in governance in each of these networks is also vastly different, and therefore, any wise participant would carefully weigh the potential risk and reward of their participation in on-chain governance before proceeding.
3. There are a number of additional risks that are difficult to capture succinctly, but it suffices to say, in **all** of these networks, active participation in governance is time consuming and requires a non-negligible investment of time and energy.

So let's take a look at the risks (and rewards):



Looking at this very basic risk reward analysis, we can quickly start to determine where participation is profitable and where it is not, which might inform why we see certain networks gravitating toward more or less competitive dynamics in governance.

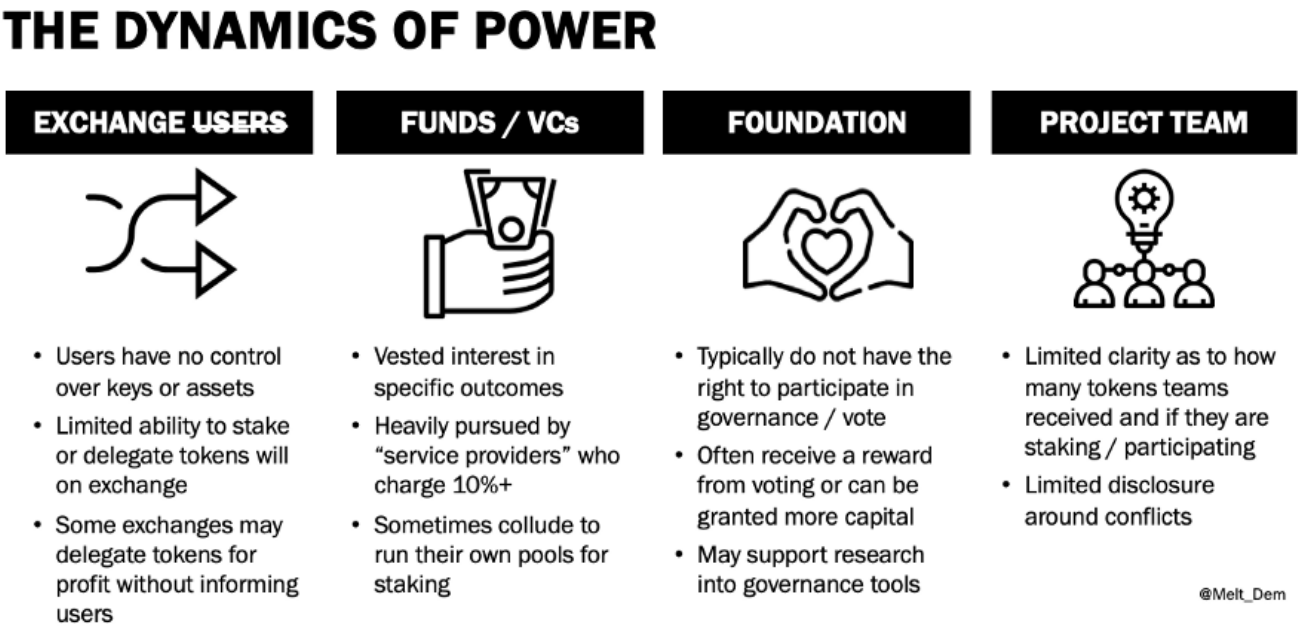
This leads me to my second, likely more accurate, question…

Who Has the Will to Govern?

Given that it's so time consuming to follow all of these protocols, to know the main actors and main influencers, to track development updates, to track network evolution and growth, and to track the flow of money—it's beginning to become clear that there are really two, perhaps three, key motivations for those who participate in governance.

1. Money
2. Power
3. Curiosity / Masochism / Insanity *(Perhaps)*

It's no real surprise that money and power dominate the conversation when it comes to governance. People were outraged when I suggested as much in my thinking around Tezos, but as more proof of stake protocols emerge, I imagine we'll start to see the beginnings of crusades and idealogical wars between the entities below.



Collusion, coercion, manipulation, lobbying, bribing, and gerrymandering are part and parcel to the processes of modern democracies.

> *It would be foolish to believe that crypto governance would be absent these forces, and many systems, while they may be technically robust, are susceptible to social engineering.*

We already see coercion and collusion for instance, in EOS, where there have been numerous accusations and in-depth investigations of collusion and cartel-like behavior amongst exchanges, investors, and the Block.one team.

DIFFICULT TO UNTANGLE INCENTIVES

	EXCHANGES	INVESTORS	FOUNDATION	TEAM
EOS	Bitfinex and others enable voting	>70% of EOS held by 100 addresses	Block.one controls 10% of voting power	Unknown how much EOS team owns
DASH	Must run own masternode	Most masternodes run by investors	Sell memberships, receive 10% of BR	Unknown
NEO	Unclear	Unclear	Foundation holds 50% of votes	Team holds 10% of foundation tokens
Tezos	Run own baker or delegate for users	Investors running own bakers	Foundations holds 10% of tokens	Founders got 8.5% of tokens
Decred	Must buy tickets outside exchange	Running staking operations	10% of tokens go to foundation for "dev"	8% dev subsidy, 9% dev pre-mine

Sources: Tezos Foundation, TzScan.io, DASH website, StakingRewards.com, EOS Authority voting statistics, Decred website and dcrstats.com, Cryptoslate, NEO.edu, Coinmonks

@Melt_Dem

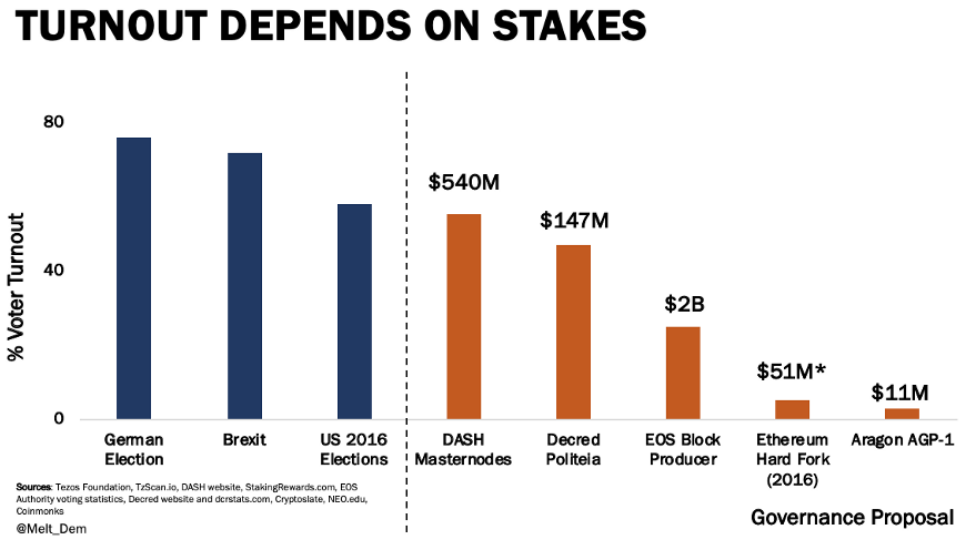
It's very difficult to find reliable information about stakeholders and their participation in formal, on-chain governance, as well as their motivations

In fact, as I was writing this, the Cosmos team merged a change to remove a cartel with 53% of voting power from "Game of Stakes"—their testnet.

Looking at the five protocols I analyzed, it's easy to see the balance of power amongst network participants.

How Is [Exertion of] Power Measured In This Model

Perhaps the best way to measure the ability for participants in a system to express their will is to look at the turnout rate for votes.



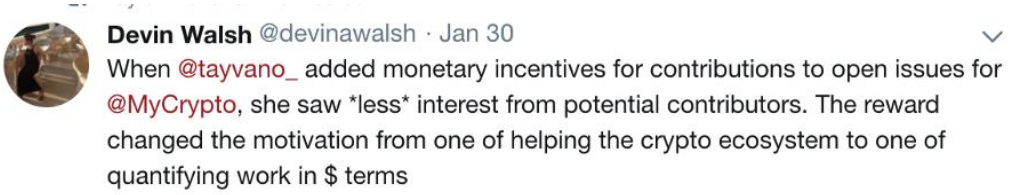
As we can see, participation is each protocol is challenging to measure, and I fully agree (with you, the reader yelling at the screen) that the above is an imperfect measure.

However, it's a starting point, and highlights a few key issues at play here:

- **Ease of Voting**: If voting is difficult, whether it be technically difficult (e.g. needing specialized hardware or specialized technical competence) or physically difficult (e.g. needing to travel somewhere or have robust connectivity to a network) turnout is likely to be lower. Today, most blockchain-based voting mechanisms feel clunky to users, and therefore casual users are unlikely to invest the time and energy to participate in voting if it requires using new software of paying for tickets, etc. This is why increasingly, funds with numerous token holdings are relying on staking-as-a-service providers to offer their specialized expertise, as these funds don't have the time to manage the mechanics of five, let alone fifty protocols. ***Specialization will inherently emerge as these systems grow in complexity.***
- **Importance of Voting Issue**: Depending on the issue at hand, voters may turn out in higher of lower numbers. I've attempted to capture the "magnitude" of each crypto governance vote in the graphic above, but again, the true stakes of these votes are difficult to identify. What we do see if when issues really matter, whether ideologically, socially, or financially, voters turn up. For example, very few EOS holders vote for block producers because they feel their vote doesn't really matter. Some EOS holders I polled said they feel the BP selection process is so heavily dominated by large EOS holders like exchanges, EOS founders, and early EOS investors, that it isn't worth their time and energy to participate. Perhaps these users feel the way a democratic voter feels in a republican state during US elections…
- **Risk of Voting:** If voting represents potential risks, either social (reputation damage or privacy loss); financial (capital loss); or physical (violence) then turnout is likely to be lower. In most current systems, voters are compensated for taking risk by putting their assets "on chain" or in escrow by getting a direct vote, while those who don't get little say. However, one of the aspects that hasn't been covered as widely is 'reputational risk' and privacy. For voting to be effective, privacy is tantamount. ***Should it be possible for participants to express unpopular opinions without feeling like they'll be ostracized*** by the hordes on crypto twitter? I believe yes, but others (see below) may not share that sentiment. We'll also cover this later under the topic of "ochlocracy" or rule by mob.

Source: Peter Todd's writing on the Ethereum hard fork (link)

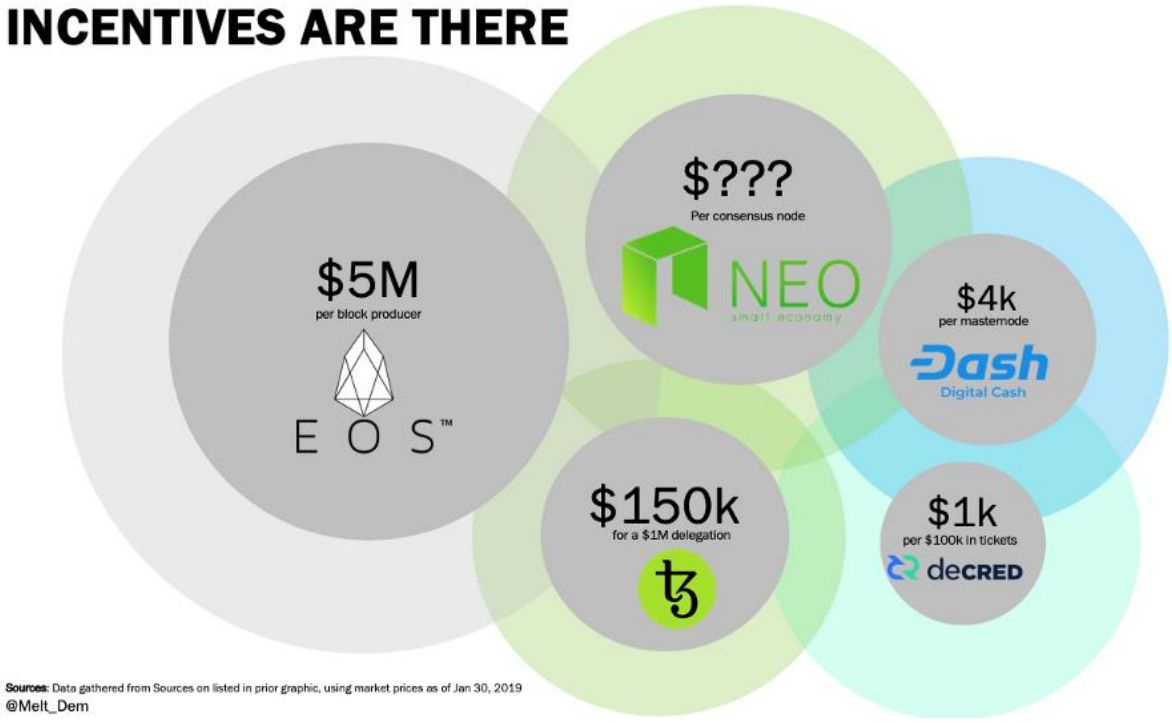
- **Personal Gain:** The most important factor of all is how much someone stands to gain by participating in governance via voting. ***In my view, what on-chain governance has done most effectively is put a price on network participation***. This is a rather contrarian view, but I believe networks that provide a financial reward for 'politicking' will become over-run with the types of people attracted to these schemes. As someone who spends most of her time in bitcoin, where there isn't a direct link between participation and compensation, and everyone is a volunteer, I wonder if we lose some of the magic of "community" when we 'financial-ize' participation.



Similar observations in [another conversation](#) at AraCon2019—by [Taylor Monahan](#) via [Devin Walsh](#)

A Rising Tide Lifts All Boats (Stakes)

The stakes in these games of governance will only continue to grow. The below graph represents the financial incentives at play in each of these protocols. The financial incentives will only grow as the value of these networks grow, and as the stakes continue to increase, I expect increasingly sophisticated players to enter the market for governance.



Not my best bubble chart, so don't come @ me—I know the sizes are not to scale :D

We also can't ignore the unquantifiable "path dependency" stakes in these protocols, which we saw play out in bitcoin's political landscape over the last three years.

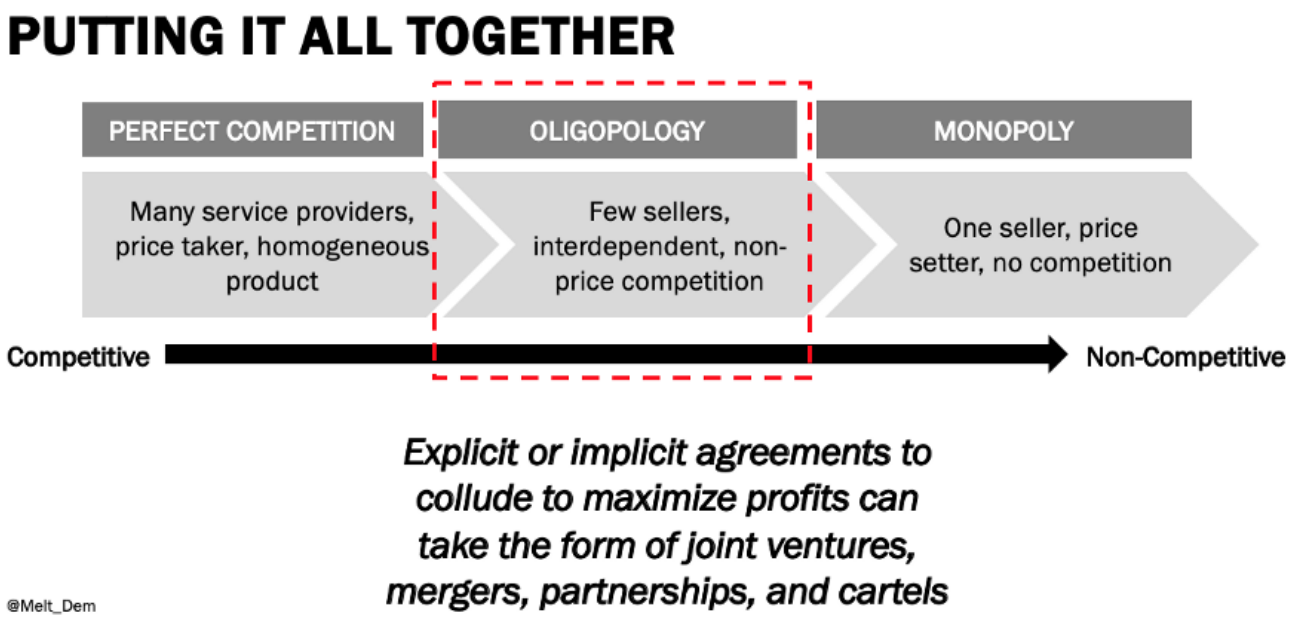
Many people building businesses on top of these networks are dependent on certain changes being implemented. Make no mistake, the ability to influence and control the future development of the network—what changes get merged, how governance itself evolves—in the right hands, can be priceless.

The Future of On-Chain Governance

So where does this leave us? While I'd love to imagine a world where governance is perfectly competitive and many service providers emerge to offer users practical tools, I believe the current state of on-chain governance is trending more towards oligopolies.

Each protocol has its own ruling party and its own oligarchs, some better known than others, and these parties will collaborate to maximize outcomes in their own favor.

Mind you, those outcomes might also happen to be optimal for all network participants; ***negative externalities do not have to manifest as a result.***



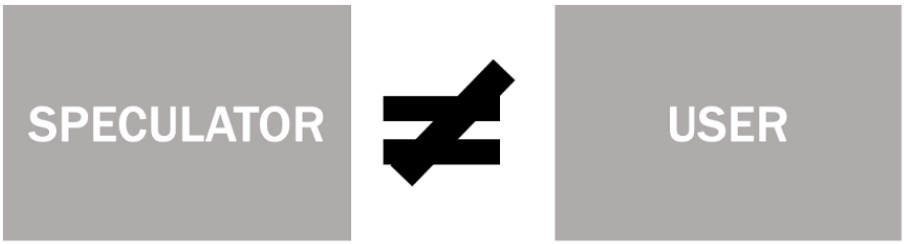
I do believe certain exchanges, investors and individuals will align themselves with specific protocols where they can "govern" or exert control more effectively; and play a more active role in shaping the future.

We already see this already, in the form of services like Staked and Battlestar Capital*, which support crypto funds by "compounding" their crypto and taking advantage of the opportunity to earn financial returns via staking.

It's odd to me that the politics of staking-as-a-service providers haven't been discussed, but it doesn't take a leap of the imagination to see that large service providers could effectively become "cartels-in-a-box" for large investors.

You may balk at the use of the word 'cartel,' as it brings to mind images of drug kingpins and oil-rich kleptocracies…calm your imagination… cartels have a rich history in emerging markets, particularly in new industries, where economics dictate that collusion is more profitable than no collusion, and consumers have few alternatives.

While to date, the incentives of investors (speculators) and networks have been largely aligned, I would not expect that to be the case in the future.



When will we learn?

I know I keep belaboring the point, but remember that speculators, i.e. investors with fiduciary obligations, are *not* users.

Therefore, I'm extremely wary of projects where speculative investors control more than 50% of the tokens, and therefore, 50% of the votes.

Some investors may convince you they are there to do what is best for the protocol, and I do believe that many investors provide positive contributions to the crypto community.

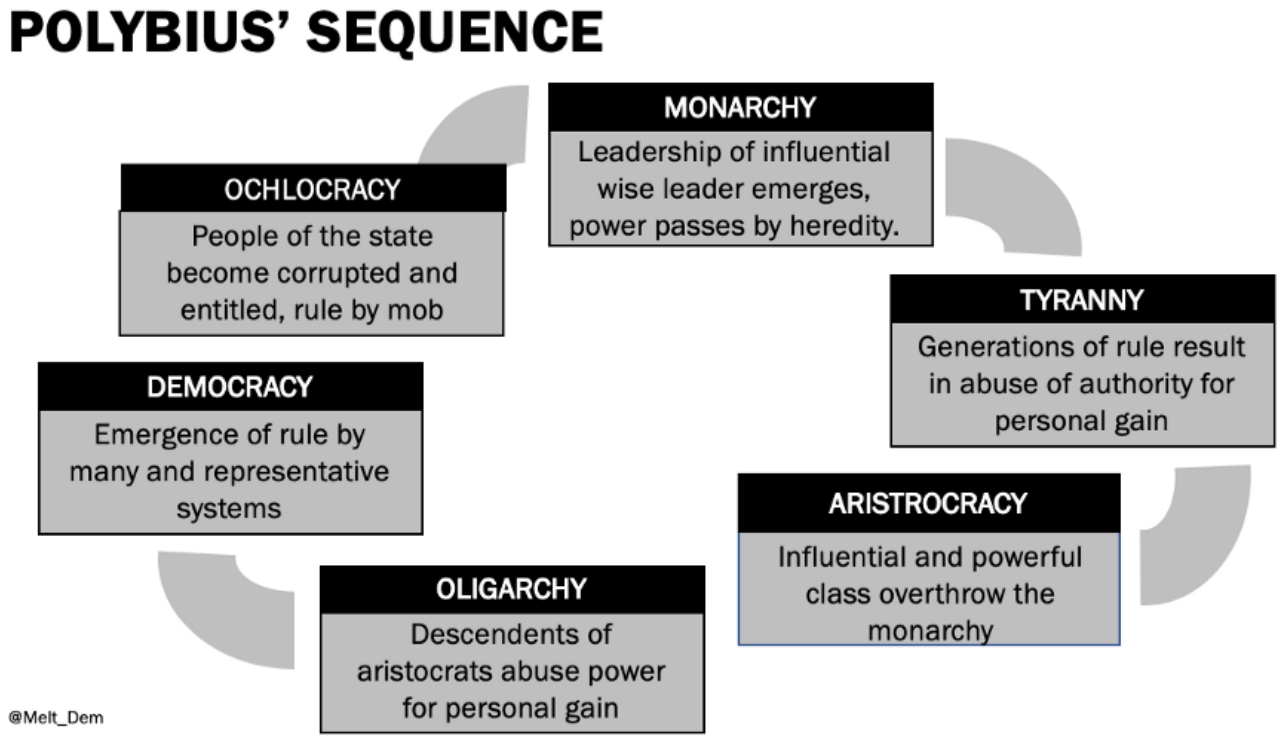
Of course, I am myself an investor, and therefore fall into this same camp. I have no illusions about the conflicts of interest here.

The "cartel of good intentions" (see this Foreign Policy article which helpfully introduces and defines the phrase) ultimately is all about charting a course which maximizes profit.

> *While we may all have the best of intentions, ultimately, tools are neither inherently good or bad, just or unjust. It is in their use, by humans, that these tools can take on this character.*

The phrase “absolute power corrupts absolutely” is perhaps a fitting reminder of what happens when we couple power with politics in protocols. Perhaps borrowing from history would be most appropriate here.

Most forms of governance begin as “benign” in nature—whether it be monarchy, aristocracy, or democracy. Over time, these benign and weak forms of governance are abused and become malignant, devolving into tyranny, oligarchy, and ochlocracy. Eventually, those subject to malignant rule overthrow it in favor of a more benign form of rule, and the cycle begins a new.



This pattern, called anacyclosis or Kyklos, features heavily in the writing of Aristotle and Plato

One needs only glance at the world of cryptocurrencies to see these patterns play out repeatedly:

Arguably, the emergence of governance oriented protocols was a direct response to the perceived tyranny of bitcoin. But as these protocols are implemented and their governance mechanisms activated, we see them, in turn, plagued by their own unique forms of dysfunction.

Perhaps the ultimate fate of many of these systems is rule by mob, where we all scream at one another on crypto twitter, until we see a wise ruler emerge (via Medium post, of course) who tames us all and decrees how it *shall* be going forward.

Perhaps, history can inform us as to the mistakes of the past and what has been learned from these. Again, Polybius, in his eternal wisdom, has some key lessons to impart (*which I've commented on in italics)*

- **Tenure of rulers must be kept short to prevent them becoming despots** (*Many networks rely on benevolent dictators, and I continue to believe one of the brilliant aspects of bitcoin's design is Satoshi's disappearance. Likewise, Charlie Lee stepping away from Litecoin and Ricardo Spagni (fluffypony) stepping away from Monero could be interpreted similarly.)*
- **External threats, whether real or imagined, preserve internal peace** (*We see this play out with many protocols, and its what makes the phrase "short the bankers, long bitcoin" and others like it so appealing. Rallying cries like these provide social unity and justify many forms of behavior in defense of a common good. See "The Banality of Evil" for further reading on this.)*
- **If any one individual gains too much power—whether it be monetary, political, or military—banish them** *(We have seen this play out, and perhaps the Bitcoin forks are a great example of people choosing to banish themselves.)*
- **Decision makers and governance bodies must never accept money to make decisions** (*This is in direct conflict with the idea of staking for return, and lobbying will inevitably become part of the industry as the size of these networks and the money and influence at stake continues to grow. Perhaps blockchains will change this, but I find it doubtful, because human nature, ya know.)*
- **The middle class must be large** (*This topic is controversial, but in my view, the initial distribution of wealth ie tokens matters greatly to future decision making. Balaji Srinivasan did some helpful writing on this topic, I discussed it at the World Economic Forum last year, and there is a lot of discussion around what is and isn't fair initial distribution, and whether or not it matters. Hopefully by this point, I've been able to demonstrate why in protocols with on-chain governance, initial asset distribution matters greatly.)*
- **If all citizens are aware of law, history, and constitution, they will endeavor to maintain "good" governance** (*Perhaps this is my greatest takeaway of all. Much of crypto governance tends to veer into the territory of ideas that have already been implemented or tried before, without an active acknowledgement of the failures and dangers of these designs. If nothing else, this post hopefully helps provide some context on how we might at least begin to understand our role in on-chain governance systems and what we may do to make them more likely to succeed at their stated intent.)*

Who knows how the future will unfold.

I have some ideas, some of which are shared above, but nothing is certain.

Part of the fun here is watching these ideas unfold in real time. As more and more Proof of Stake networks go live, it will be fascinating to see how these new networks evolve and grow to maneuver around the risks outlined above.

I am particularly intrigued by Cosmos, given its attempts to actively remove cartels from the system, and if and how that will prompt cries of "de-platforming" from those who happen to run these cartels. After all, the beauty of blockchain networks is their un-censorable nature, which means intent in design becomes all the more important. If abuse is possible in your design, then is it the fault of the abuser or the designer? Arguably, using the rules to play the game in a manner different than which it was designed for isn't a crime.

In the meantime, I continue to actively track the economics of staking, and to date, have chosen to focus primarily on Tezos to further my learning and my experimentation with proof of stake and on-chain governance. However, over time, this may change, and I look forward to sharing what I learn with the community.

A Few Final Comments

1. **Tracking the Data:** Gathering data for this piece was challenging, to say the least. A special thanks to TzScan, Eos Authority, DCR Stats, and StakingRewards.com, just to name a few of the sources I relied on heavily. I'd like to see protocol teams or foundations *themselves* also start to adopt, implement, and track more robust frameworks to track, analyze, and socialize key data points around their governance schemes. ***Maybe this is a gap Messari* will fill (cc: TwoBitIdiot)***
2. **Slides:** You can see and download the slides from this talk here Speakerdeck, and see other slides I've published here (not always up to date, but I try). Feel free to borrow and use as you like, but please attribute when and where appropriate.
3. **Notes and Disclosures:** *The Battlestar Capital team works out of our NY office, and we engage in a lot of lively debates around the economics and politics of staking, so it could be argued that I'm biased here. *I'm an investor in Messari.

Links

- https://www.youtube.com/watch?v=wfcro5iM5vw
- https://aracon.one/
- https://medium.com/@Melt_Dem/the-tezos-experiment-b97e124e5b38
- https://www.meltemdemirors.com/disclosure
- https://github.com/cosmos/game-of-stakes/pull/263
- https://petertodd.org/2016/ethereum-dao-bailout-vote
- https://twitter.com/devinawalsh/status/1090553366218969093
- https://medium.com/@tayvano
- https://medium.com/@devinwalsh
- https://staked.us/
- https://battlestarcap.com/
- https://foreignpolicy.com/2009/11/11/the-cartel-of-good-intentions/
- https://en.wikipedia.org/wiki/Anacyclosis
- https://news.earn.com/quantifying-decentralization-e39db233c28e
- https://www.youtube.com/watch?v=fQ0YkPCdxZ8
- https://tzscan.io/

- https://eosauthority.com/voting
- https://dcrstats.com/
- https://stakingrewards.com/
- https://messari.io/
- https://medium.com/@twobitidiot
- https://speakerdeck.com/meltdem/power-by-proxy-the-case-for-crypto-cartels
- https://www.meltemdemirors.com/content

There is no such thing as decentralised governance

Working toward the crypto trias politica

By Lawrence Lundy-Bryan

Posted on February 20, 2019

TL:DR

- The terms off-chain governance and decentralised governance are used with abandon in the 'crypto' space and without a full grounding in political philosophy.
- Decentralisation, or preventing the concentration of power and increasing individual liberty isn't a binary choice between centralisation and decentralisation, it's a spectrum.
- Different decisions and classes of decisions will need different levels of decentralisation and appropriate mechanisms for conflict resolution to balance efficiency versus diversity.
- Today, most crypto projects are governed by the open-source development tradition based predominantly on Linux and the foundation model instigated by Ethereum. These structures are not robust enough if we are to build inclusive equitable global public utilities.
- On-chain governance solutions are a step in the right direction but are liable to concentration of power in a technocratic elite with the time, knowledge and reputation to vote and decide on policy changes.
- The separation of powers (trias politica) model which forms the basis of almost all liberal democracies provides a more appropriate framework than traditional corporate governance or full on-chain governance. Crypto networks need an executive (implement law), a legislative (create law) and a judiciary (interpret law).
- Three network branches would formalise powers and act as necessary checks and balances on power consolidation. Regular voting and term limits would prevent power grabs by stakeholders, and formalised laws would build trust in the system by users that don't want to participate in governance directly. A separation of powers will form the foundation of a social contract between the network and users.
- We aren't just building businesses, so corporate governance won't work. We aren't just building economies, so economics alone won't work. We are building global communities, so I'm afraid we are going to need politics.

I. Political philosophy for the win

I love decentralised governance and on-chain governance as much as the next person but as with the word 'blockchain', we are suffering from a lack of clarity. What actually is 'on-chain governance'? And why are we doing it? Aragon are building amazing tools and

impressive projects like Cardano, Dash, Tezos, Decred, Dfinity, and Polkadot are live or going live with implementations. It all feels a bit 'blockchain 2017' and 'ICO 2018'. (And 'STOs' 2019 by the looks of things). There are some transformational ideas floating around, but it is all thrown together as 'governance'. Ideas of futarchy, quadratic voting, and liquid democracy are unmoored from the anchor of political philosophy. The question being asked isn't a new one: how can we best organise the society/community? We have reached the answer of 'full decentralisation' because that was the answer for a peer-to-peer electronic cash system. It seems like we have decided the answer before we understand the problem.

In thinking through the question of how best to organise, the tension is between self-interest and group interest. How do we create rules to ensure individuals can trust that acting in the group interest also serves their self-interest? In small scales like families, clans and tribes, trust is formed through reputational pressure. But at larger scales like companies and states, trust needs to be codified as less formal pressures are less effective between strangers. Trust is enshrined by institutions into rules, laws and regulations: essentially so that it can scale.

And then Bitcoin came along. A ledger that could be securely amended by all participants anonymously. So for the first time scaling trust without the need for an institution to enforce the rules. Rules would be enforced by cryptography, economic and game theory dynamics. This idea of the 'trust machine' and 'scaling trust' became a common narrative, but it is now clear that decision-making is more complex. The bitcoin network and other public networks using proof-of-work can successfully enforce rules in a collective way, but for rule creation, amendment, and conflict we lack equally effective mechanisms.

II. The crypto trias politica

One of the best ways to contextualise the challenges of decision-making is one that is pretty familiar. Inspiring the Constitution of the United States, the French philosopher Charles-Louis Montesquieu published The Spirit of the Laws in 1748 and coined the term the 'separation of powers'. The concept was to divide government responsibilities into three to reduce the potential for the concentration of power and provide for checks and balances. The executive branch would be responsible for implementing and administering the public policy, the legislative branch for enacting the laws, and the judicial branch for interpreting the laws and conflict-resolution. Certainly, the objectives of nation builders and crypto-network builders are similar: reduce the potential for concentration of power.

"A dependence on the people is, no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions." James Madison

The Executive (Development Team)

The framing is not perfect, but crypto-networks today are like the executive branch lacking a functioning legislative or judicial branch. The executive branch can be seen as the core

developers that invented and are tasked with developing the network. They are guiding the technical roadmap and pushing updates. In some cases the executive is formalised as a commercial entity, but in most cases, the executive is an ad hoc collective of individuals without any formal structure. Improvement proposals are an open process but in most cases, the accepted proposals are those from the core developers/executive branch. In the U.K. parliament for example, any member of parliament can propose a bill, but generally only high profile bills supported by well known members of parliament get support. Often proposals are accepted or rejected based on the different visions stakeholders have for the network. E.g. digital cash or digital gold with the Bitcoin network. In a national system of governance you could describe these differing visions for society or the network as political parties. However, unlike national systems with elections, crypto networks do not yet have a mechanism for changing the executive within the system, instead forking is the dominant expression of unhappiness. If crypto-networks are to be the digital communities of the future, it is imperative that a mechanism less destructive than forking is used to express the differing values of the community. Equally, it is unclear if eliminating the executive completely by dissolving the foundation and delegating all decision-making to the network users is an effective way to achieve network robustness and sustainability. A more pragmatic approach might be executive elections every four years acting as a limit to the concentration of power. The creation of a crypto legislative and judiciary would do the same.

Maybe the contours of an elected executive looks a little like the Collection Code Construction Contract (C4). But many projects are fearful of being see as 'centralised' or wielding too much power over the network. Indeed, as networks are still small consisting predominantly of pioneers and early adopters for which any form of centralisation is seen as anathema, this is a reasonable fear. But as networks grow and onboard the early majority, users will have different requirements. They will care about performance, ease-of-use, and innovative new features. An elected executive with a four-year mandate with budget to deliver could outcompete a network that has fully on-chain governance in which proposals are debated but consensus is hard to achieve.

The Legislative (The Foundation)

Very few projects have separated powers between an executive branch and a legislative branch. The legislative is tasked with the creation of laws and in most cases has the ability to allocate budget. The legislative is called a parliament, congress, and assembly depending on country. After the Ethereum Foundation set up in Switzerland, most crypto projects use a foundation structure primarily as a vehicle to raise capital rather than as a check on power. Tezos is an example of the difficulties in delegating budgetary responsibilities to a foundation. One popular approach is for money to be released by a foundation to the development team based on milestones. Blockstack and Aragon are compelling examples of this approach. This grant sign-off function of the foundation to the development team is similar to the process of budget sign-off by the legislative to the executive. However, there are few examples today of foundations acting more like a legislative and taking responsibility for lawmaking or network policy. (Edit: Sovrin's Trust Framework is an example). Network policy is in theory delegated to the users of the

network, but in reality, very few users are involved in network policy because of the time commitment and technical understanding required to contribute. On-chain governance approaches such as Dfinity, Tezos and Decred are experimenting with formally delegating some network policy responsibilities to the users of the network, which looks much more like direct democracy a la Switzerland than representative democracy.

The challenge will be in how to encourage participation in the creation and voting on network rules. Voter turnout in real-world elections can be close to 90% in Belgium or just 40% in Chile. And that is just for a single vote for a president or political party. How will on-chain governance projects limit voter fatigue? Or explain complex technical details that need to be voted on? Delegates or representatives are a good way to reflect the aggregate desires of a larger community. Innovation and experimentation should be around the size and structure of the legislative, rather than complete abolition. Vote for different representatives to take decisions on your behalf in areas for which they are experts. A cryptographer on security policy, an economist on budgetary policy, and a constitutional lawyer on constitution changes. With the appropriate rewards for representatives, a system can be designed that has powerful feedback loops between the actions of representative and the represented. It would be interesting to experiment with term limits to try and find an optimal term length to incentivise long-term thinking and high levels of performance. Every decision cannot be fully 'decentralised', in fact, a more robust system would be one in which a legislative body of elected domain-experts makes decisions on behalf of the electorate. You could even add a transaction fee to pay for such a body. Sounds a little bit like a taxation system….

The Judiciary (Miners?)

The third branch and the least developed in the crypto community is the judiciary. It has been argued, most prominently by Fred Ersham, that miners can be considered the judiciary in the sense that they 'enforce' rules. That isn't quite right because in a state the judiciary interprets the rules to resolve disputes. Miners don't really have any power to interpret. The community did also for a period suggest that "code is law" which did away with the need for a court system. With this line of logic, the judiciary is just an interpretive branch and therefore if new law was machine readable you could avoid disputes by well-designed laws. That is indeed a dream scenario, but the fact is, crypto projects will plug into real-world legal infrastructure for the foreseeable future. The SEC will see to that. Therefore dispute resolution will have to refer to existing legal structures a la Mattereum, Kleros, and Aragon take a different path trying to resolve as much as possible with a digital judiciary of jurors and game theory. Interestingly, Aragon throw a prediction market into the mix as a second appeal court. It's possible that with portable reputation and self-sovereign identity, reputation becomes so vital to an individual's ability to participate in the community that it acts as a sufficient deterrent to anti-social behaviours. Who needs prisons if the police could prevent Fortnight for a year? The Chinese social credit system spotted an opportunity early. For the foreseeable future though as real-world assets are on-boarded onto decentralised networks there will need to be an arbiter of conflicts. If we are to build trust in the system, there will need to an independent branch of the network that does not develop policy. The DAO bug and rolling back of the Ethereum network by

the executive branch showed that the network lacked a robust conflict-resolution mechanism resulting in a loss of trust and a fork.

What an independent judiciary will look like in crypto networks is an interesting question. Crypto-economics can only take you so far. As long as bugs exist in software and individuals interpret information differently there will be conflicts to be resolved. All conflicts cannot be automated away by perfectly written contracts. For the foreseeable future there will be a need to be humans in the loop. The exact structure of a digital court could be experimented on for lower-level conflicts. What is the optimal number of jurors to strike a balance between understanding a case and finding consensus? How are jurors selected in order to prevent bias? Are domain-experts chosen to rule on particular cases? Is there room for voting experimentation? For example, how would quadratic voting work for conflict resolution? More questions than answers at this point, but the key is to start asking questions. The more people on-boarded to crypto and the more activity that takes place on networks, high-quality conflict resolution could be key to building sustainable trusted networks.

III. End of corporate governance and toward network constitutions

Surely we just want to build technology and get users to use it? Lean startup style? Right? Wrong. As software has scaled to billions of users, many of the problems Facebook and Google face are those of nation states not corporations. Balancing free speech and censorship; individual privacy versus collective benefits of data aggregation; state-sponsored disinformation campaigns. You can make the case that Facebook in particular has managed these crises poorly, but I would argue that it is structurally not designed to manage these political problems. Corporate structures are designed to balance the needs of investors, management and to a limited extent employers. Users are not stakeholders in this structure.

Crypto projects are embarking on a vast experiment in inclusive governance. Users are a core stakeholder in decision-making and investors are not prioritised. There is an almighty tug-of-war between all stakeholders as you would expect, but it's clear that if the ambition is to build global digital infrastructure, a traditional corporate structure isn't going to cut it. So the race is on to understand and experiment with governance models which take the best from national governance in terms of limiting the concentration of power and mix it with the efficiency of corporate governance structures. The debate has been fixated on increasing the number of nodes that can validate transactions when referencing how 'decentralised' a network is. From a security perspective, I can understand why. But equally important is the concentration of network policy power and the concentration of conflict-resolution power. DAOs are part of the answer to automate budgetary responsibilities and projects like Moloch are pushing the envelope. But DAOs should be part of a broader constitutional framework.

I would advocate for the creation of a network constitution that outlines the values of the community. These are basic values for which users would opt into. These values will help

guide decision makers in the early days without precedents and when network preferences are hard to gauge. Decisions would be made in line with the values of the community not arbitrarily depending on the needs of the network or the development team at the time. E.g. data will always be owned by the user; all steps will be taken to protect user privacy; state level censorship-resistance will be prioritized; or 10% of all assets held in wallets will be redistributed to invest in charitable efforts. When all code and data is open-source, values are the only sustainable competitive advantage.

Once values have been articulated, the next steps are to formalize the structures for a network executive, network legislative and network judiciary. Checks and balances should be mapped out. And relationships between each body should be defined such as voting mechanisms. This work should be done in the open with the consultation of the network. The timing of this is a challenging question. The risk is slowing down decision-making to a crawl with multiple power-bases preventing decisions from being made e.g. the on and off again U.S. Government shutdown or Brexit deadlock. But equally, there is a risk that without the build-up of the different branches, the executive branch will consolidate power and lose the trust of the network stakeholders. Committing to abolishing the foundation as some crypto projects are planning is one strategy to prevent consolidation. The risk is that the network does not have the rules and processes in place to effectively make decisions. If this were easy, political science wouldn't exist.

The crypto trias politica

We aren't just building businesses, so corporate governance won't work. We aren't just building economies, so economics alone won't work. We are building global communities, so I'm afraid we are going to need politics. We can't just say 'decentralised governance' or 'on-chain governance' and get the network to vote on all decisions. We all want to meet the goals of inclusive, broad-based, diverse decision-making to limit the concentration of power. But we need to learn from the hundreds of real-world main-nets/nations operating today. These nations all have decision-making processes seeded from a single idea from 1748: the separation of powers. We now have the tools to improve governance and fix some of the misaligned incentives in national governance systems. But let's not throw the baby out with the bathwater. We need a crypto trias politica.

Links

- https://rfc.zeromq.org/spec:22/C4/
- https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74
- https://mattereum.com/
- https://kleros.io/
- https://blog.aragon.org/aragon-network-jurisdiction-part-1-decentralized-court-c8ab2a675e82/
- https://github.com/MolochVentures/moloch

Security Budget in the Long Run

By Paul Sztorc

Posted February 12, 2019

> *"A discussion of Bitcoin's ability to resist 51% attacks (ie, its "security budget"). Competition makes it difficult for one network to collect enough fees – instead, we should try to collect fees from all networks."*

This post is a somewhat more-empirical sequel to "Two Types of Blockspace Demand". And to my Building-on-Bitcoin talk.

1. The "Security Budget"

Bitcoin's "security budget" is the total amount of money we pay to miners (or, if you prefer, the total amount spent *on* mining – they are the same thing). When this value is low, 51% attacks are cheap. In 2018, BTC's security budget was about $7 million per day. So, the suppression of BTC (via a never-ending campaign of 51% attacks) would cost –at most– $2.6 billion per year.

$2.6 B is pretty low – by comparison, the 2017 annual US Military Budget was $590 billion, and the FED's annual operating expenses totaled $5.7 billion.

2. The Block Subsidy

Fortunately, we can expect the *block subsidy* to give us more security in the future. Even though it "halves" once every four years (effectively falling by a factor of 0.84 per year), it hits for full force no matter how high the BTC exchange rate climbs. As long as annual appreciation 19%+, it fully compensates for the PP lost to the halvening. Historically, the rate has been *much* higher than 19% (more like 70%+), and so the security budget has increased substantially over time, and will continue to do so for a while.

Of course, eventually the exchange rate must stop appreciating. Even if Bitcoin is outrageously successful, it will apparently reach a point where it simply cannot grow faster than 1.077 per year[1] , as this is apparently the growth in the nominal value of all the world's money.

Here I show the growth, and ultimate decline of the security budget:

Security Budget over next 40 yrs, if Fees are Zero							
Year	Subsidy	Exchange Rate (theoretical maximum)	Exchange Rate (market-imputed)	BTC Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio	
	from protocol	x_2017 = $11.22M, growth = 1.077	x_2016 = $700, growth = 1.6265; blended with maximum	= Subsidy * Exchange Rate (m.i.) * 6 * 24 * 365 * (1/1e9)	x_2015 = 637, growth = 1.047	Security B. / Defense B.	
2008	50	$2,725,960	$0	$0.00	$461.76	0.000	
2012	25	$3,671,828	$100	$0.13	$554.95	0.000	
2016	12.5	$4,945,897	$700	$0.46	$666.96	0.001	"Indifference" Epoch
2020	6.25	$6,662,050	$4,900	$1.61	$801.57	0.002	
2024	3.125	$8,973,683	$75,000	$12.32	$963.36	0.013	
2028	1.5625	$12,087,419	$800,000	$65.70	$1,157.79	0.057	
2032	0.78125	$16,281,574	$15,000,000	$615.94	$1,391.47	0.443	"Healthy" Epoch
2036	3.9E-01	$21,931,039	$21,931,039	$450.27	$1,672.32	0.269	
2040	2.0E-01	$29,540,785	$29,540,785	$303.25	$2,009.85	0.151	
2044	9.8E-02	$39,790,999	$39,790,999	$204.24	$2,415.50	0.085	
2048	4.9E-02	$53,597,887	$53,597,887	$137.55	$2,903.02	0.047	"Decline" Epoch
2052	2.4E-02	$72,195,560	$72,195,560	$92.64	$3,488.94	0.027	
2056	1.2E-02	$97,246,350	$97,246,350	$62.39	$4,193.13	0.015	

Above: Bitcoin's security budget over time. Each row refers to a different year. Theoretical max exchange rate from the Game and Watch paper. Imputed exchange rate is historical rates and growth factors, with some manual "blending in" so as to more rapidly approach the theoretical maximum. Defense budget extrapolated from wikipedia data. "Safety Ratio" is the percentage of military budget that would be needed to disable Bitcoin. All numbers are in nominal dollars.

The "indifference" epoch is one where Bitcoin is vulnerable, but few adversaries squander their opportunity to attack because they are not paying attention. The "healthy" epoch is one where BTC should be able to deter 51% attacks even from ultra-wealthy motivated adversaries. But the "decline" epoch shows us a bleak future, in which 51% attacks on Bitcoin are easy again.

3. Transaction Fees

i. The Desired "Fee Pressure"

As is commonly known, *transaction fees* are expected to come to the rescue. As Greg Maxwell remarked:

> *"fee pressure is an intentional part of the system design and to the best of the current understanding essential for the system's long term survival"*

He later famously wrote:

> *"Personally, I'm pulling out the champaign that market behaviour is indeed producing activity levels that can pay for security without inflation."*

This view, (of a needed "fee pressure"), is common. Roger Ver has compiled similar quotes from other Bitcoin intelligentsia. Roger did this in order to discredit them politically, but the quotes are nonetheless accurate.

ii. The Dual Nature

The **dual nature** of Bitcoin (as both a money-unit, and a payment-rail) has confused people since Bitcoin was first invented.

In general, monetary theorists and economics ignored the payment-rail (and dismissed Bitcoin as supposedly having "no intrinsic value"). Businessmen and bankers ignored the money-unit (and regarded purchases *of BTC* as hopelessly naive), and instead tried hopelessly to rip-off the "blockchain technology".

The confusion persists today in the "scaling debate", in the form of a discussion over whether or not the "medium of exchange" use-cases are more valuable than the "store of value" use-cases.

And I think it persists in long-run security budget analysis, as well. Consider the following table:

Revenue Source	**Block Subsidy (12.5 BTC)**	**Transaction Fees**
Market's Units	…of BTC	…of block space
Price Units	… $ (PPP) per BTC	$ (PPP) per byte
If BTC price = moon…	…SB Goes Up	…SB *Unaffected*
Meme	Store of Value	Medium of Exchange
Slogan	"Digital Gold"	"P2P Electronic Cash"

While the two are mixed into the same "security budget", the **block subsidy and txn-fees are utterly and completely different**. They are as different from each other, as "VISA's total profits in 2017" are from the "total increase in M2 in 2017".

VISA's profits are a function of how cost-effectively VISA provides value to its customers, relative to its competitors (MasterCard, ACH, WesternUnion, etc). Changes in M2 are a function of other things entirely, such as: election outcomes, public opinion, business cycles, and FED decisions. There is some sense in which M2 "competes" with the Japanese Yen, but there are really no senses in which it competes with MasterCard.

iii. Are fees truly paid "in BTC"?

Transaction fees are explicitly priced in BTC. But, unlike the block reward, they *do* react to changes in the exchange rate. As the exchange rate rises, a given satoshi/byte fee rate becomes more onerous, and people shy away from paying it.

And so tx-fees are not really "priced in BTC", despite the protocol's attempt to mislead us into thinking that they are. They are actually priced in purchasing power, which –these days (pre-hyper-bitcoinization)– is best expressed in US Dollars.

So, it is entirely appropriate to say, for example, that "in Dec 2017, BTC had tx-fees as high as *twenty-eight dollars*". And it would be inappropriate to say that the tx-fees were "as high as .0015,0000 BTC". For if the BTC price had been 10x higher[2], the tx-fees would have only reached .0001,5000 BTC.

iv. Stimulating Production

Whenever prices rise, entrepreneurs are induced to produce. (Owners are also induced to sell, but we are not interested in that right now.)

The supply of BTC is famously capped at 21 million. The *produced* supply (aka the "new" supply) is currently capped at 12.5 BTC per block, until the next halving.

The supply of a completely different good, "btc-block-bytes", is also capped. It was first (in)famously capped at 1 MB per block, and now is capped at something-like 2.3 MB per block.

As was just said: whenever blocks become more valuable, entrepreneurs search for ways to produce more of them.

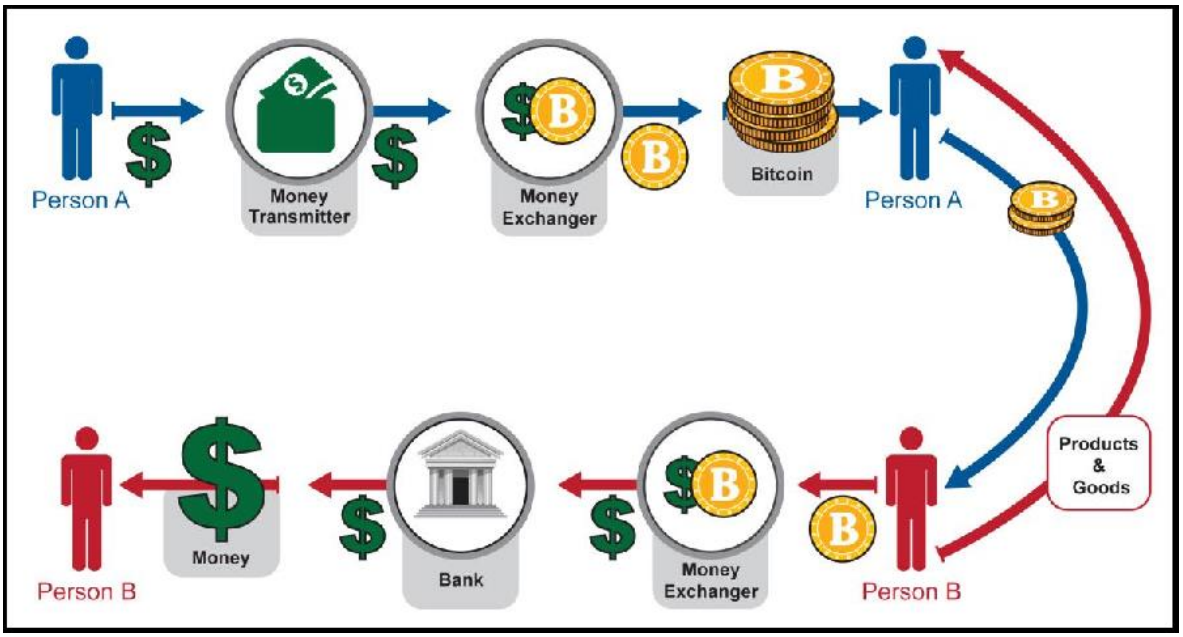
One way is to reactivate older, marginally unprofitable mining hardware. Production then hastens…temporarily. Of course, after the next difficulty adjustment, block-production will return to its equilibrium rate (of 1 block per 10 minutes).

Alternatively, entrepreneurs can create, and mine, Altcoins.

v. Altcoins as Substitute Goods

Alt-"coins" are *very poor* substitutes for Bit-"coins". Each form of money, is necessarily in competition with all other forms: money has strong network effects; the recognizability property has super-linear returns to scale; exchange rates are transaction frictions that are inconvenient; etc. What people wanted was a BTC. They wanted to *get rid of* all their other forms of money!

But it is the reverse when we consider transaction fees and "btc-block-bytes": Altcoin-blockspace is a pretty good substitute for Bitcoin-blockspace. Remember that this type of demand has *nothing to do* with obtaining BTC. Users merely wish to buy something using the Bitcoin payment-rail. This image from 2013 FINCEN Congressional testimony hopefully makes it clear:



Since the amount of coin sent in a blockchain payment is always configurable, it will always be possible to send someone "twenty dollars" worth of LTC; or "one BTC" worth of DOGE; or "one sandwich" worth of EOS. All of this is made much easier by the "exchangers" (ie: Coinbase, ShapeShift, SideShift, BitPay, LocalBitcoins, multi-currency wallets, CC ATMs, etc) which now take numerous forms and are easy to use.

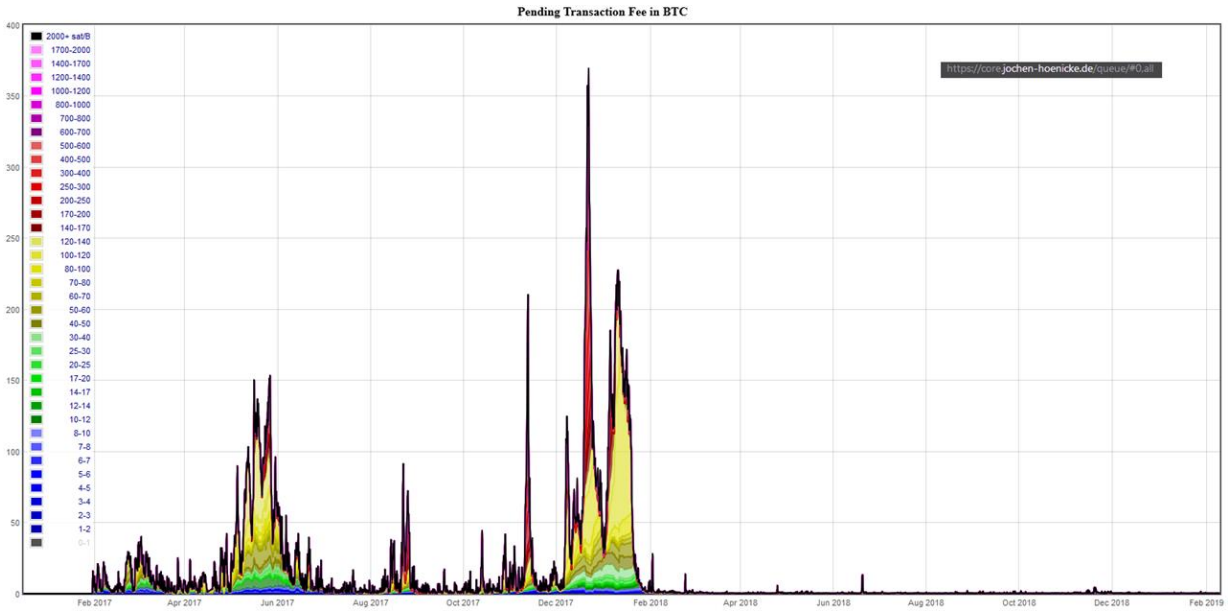
Furthermore, this (true) premise –that Altcoin-payments are indeed substitutes for Bitcoin-payments– is occasionally explicitly admitted[3], even by hardcore maximalists. Especially during the last fee run-up in late 2017:

- Samson Mao
- Francis Pouliot
- "The digital currency for payments"

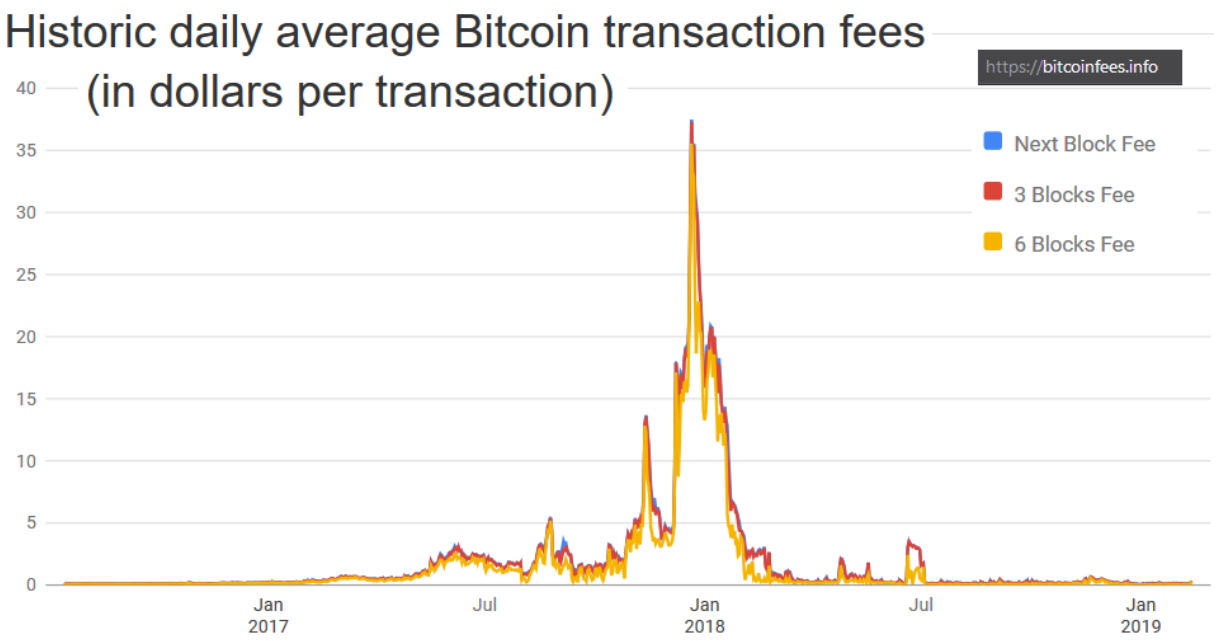
vi. Competitive Demand for the Payment Rail

The supposedly-essential "fee pressure" has, for the moment, deserted us.

See this graph (from this page) for BTC-priced fees:

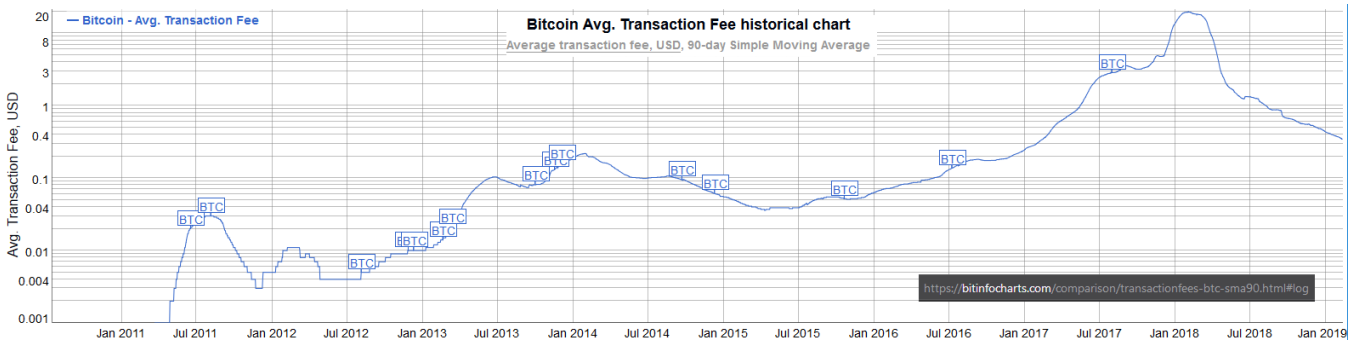


And this graph (from this page) for USD-priced fees:

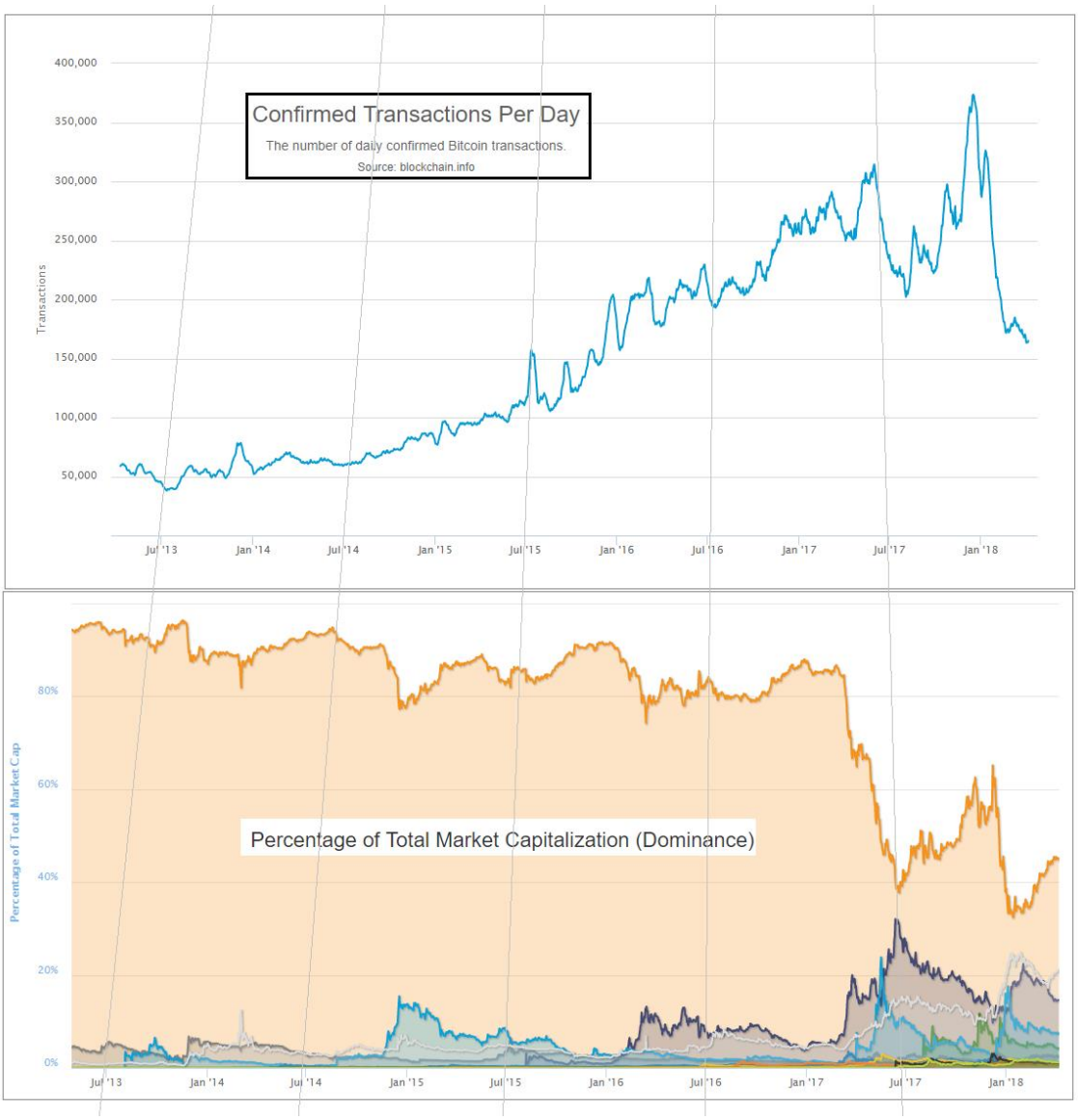


We see that fee pressure has crumbled. Today, a typical transaction will cost 30-40 cents – much cheaper than a VISA txn.

Compare the historical data, given in 90-day moving-average…



…to the two graphs below:



We see that BTC's crossing of the "1 USD per transaction line", in May of 2017, coincides with the rise of Altcoins. We also see that the "pressure" of late 2017 quickly canceled itself

out, and then some. Finally, we see that this release-of-pressure coincided with a sudden (and unprecedented) decline in BTC-transactions.

To me, this data refutes the theory that users will pay high BTC fees willingly. In fact, they seem to have only ever paid high fees *unwillingly* – during a brief "bubble" time (of relative panic and FOMO).

If that theory is indeed false, then total fees will not be any higher –in USD terms– than they are today.

According to blockchain.info, fees in the last 12 months totaled $70 million. (In the 12 months before *that*, they were $770 million).

Revisit the chart above, and you will see that this barely registers. After all, when $70 M is priced in the units of the chart (billions), it is just $0.07.

If the consumer is cost-conscious, and will only pay the lowest tx-fees, then how can we get those numbers up?

vii. Alternative Fee-Sources

a. Lightning Network

The Lightning Network (if successful) will allow very many "real-life transactions" to be fit into just two on-chain txns.

The immediate effect of this, is to *lower* on-chain transaction fees; but the ultimate effect is increase them. LN boosts on-chain fees by increasing the utility of each on-chain txn (by allowing each to do the work of many txns), and by therefore making high on-chain fees more tolerable to the end user.

Exactly how much will LN boost fees?

At this point – it is anyone's guess. But *my* guess is that they cannot realistically increase by more than two orders of magnitude.

First, on-chain txns are needed to create, and periodically maintain, the LN. So LN-users will still be paying on-chain fees; and will still prefer to minimize these costs. Meanwhile, Altcoins will have their own Lightning Network (they will copy LN, just as they've copied everything else). All of these LNs will compete with each other, the same way that different blockchains compete with each other.

Keep in mind, that the fees paid to LN-hubs[4] will, by definition, *not* be paid to miners. So, there is no sense in which LN-fees "accumulate" into one big on-chain txn-fee (in contrast to how *the economic effect* of each LN-txn *does* accumulate into a single net on-chain txn).

Second, the LN user-experience will probably always be worse than the on-chain user-experience. LN is *interactive*, meaning that users must be online, and do something [sign a transaction] in order to receive money. It also means that your LN-counterparties can inconvenience you (for example if they stop replying, or if their computers catch fire) or outright harass you. LN also comes with new risks – the LN-design is very clever at minimizing these risks, but they are still there and will still be annoying to users. Users will prefer not to put up with them. So they will tend to prefer an Altcoin on-chain-txn over a mainchain-LN-txn.

b. Merged Mining Sidechains

Merged-Mined Sidechains do whatever Altcoins can do, but without the need to purchase a new token. So they have infinitely lower exchange rate risk, and are more convenient for users.

On top of that, MM SCs send all txn-fees they collect to Bitcoin miners. Under Blind Merged Mining, they do this without requiring any users or miners to run the sidechain node software.

A set of largeblock sidechains could process very many transactions. In the next section, I will assume that the total Sidechain Network replaces VISA, (and VISA alone), and captures all of its transaction fee revenues. VISA is only a small percentage of the total payments market (which includes checks, WesternUnion, ApplePay, etc), but it is a good first look.

viii. VISA's Transaction Fee Revenues

Contrary to what I believed just moments before looking this up, VISA does not earn any money off of the interest that it charges its customers.

Observe page 40 of their most recent annual report:

> Our operating revenues are primarily generated from payments volume on Visa products for purchased goods and services, as well as the number of transactions processed on our network. We do not earn revenues from, or bear credit risk with respect to, interest or fees paid by account holders on Visa products.

Instead VISA's revenue comes from transaction fees. This perfectly facilitates our comparison.

Total revenues were 18,538 $M in 2017, up from 11,778 $M in 2013. This corresponds to quite an annual growth rate – 12% per year.

If we assume that current trends holds, we get the following:

Security Budget over next 40 yrs (assuming VISA-level fee-revenues)

Year	Subsidy	Exchange Rate (x_2017 = ...)	Exchange Rate (market-imputed)	Block Subsidy (billions per year)	VISA Tx-Fee Revenues (billions per year)	Total Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio	
	from protocol		x_2016 = $700, growth = 1.6265; blended with maximum	= Subsidy * Exchange Rate (m.i.) * 6 * 24 * 365 * (1/1e9)	x_2017 = 18.538, growth = 1.120	sum (block_subsidy + VISA_fees)	x_2015 = 637, growth = 1.047	Security B. / Defense B.	
2008	50	####	$0	$0.00	$6.68	$6.68	$461.76	0.014	
2012	25	####	$100	$0.13	$10.52	$10.65	$554.95	0.019	"Indifference" Epoch
2016	12.5	####	$700	$0.46	$16.55	$17.01	$666.96	0.026	
2020	6.25	####	$4,900	$1.61	$26.05	$27.66	$801.57	0.035	
2024	3.125	####	$75,000	$12.32	$41.00	$53.32	$963.36	0.055	
2028	1.5625	####	$800,000	$65.70	$64.53	$130.23	$1,157.79	0.112	
2032	0.78125	####	$15,000,000	$615.94	$101.57	$717.51	$1,391.47	0.516	
2036	3.9E-01	####	$21,931,039	$450.27	$159.87	$610.14	$1,672.32	0.365	
2040	2.0E-01	####	$29,540,785	$303.25	$251.63	$554.88	$2,009.85	0.276	"Healthy" Epoch
2044	9.8E-02	####	$39,790,999	$204.24	$396.05	$600.29	$2,415.50	0.249	
2048	4.9E-02	####	$53,597,887	$137.55	$623.37	$760.92	$2,903.02	0.262	
2052	2.4E-02	####	$72,195,560	$92.64	$981.15	$1,073.80	$3,488.94	0.308	
2056	1.2E-02	####	$97,246,350	$62.39	$1,544.29	$1,606.68	$4,193.13	0.383	

Link to Excel sheet.

Above: The 'security budget table' from earlier in this post, plus a new column: VISA transaction fees. These fees are added to the base block subsidy amounts, to get a new total security budget.

This security budget *does* seem to be much safer in the long run, and safer in general.

Conclusion

To deter 51% attacks, Bitcoin needs a high "security budget". Today's tx-fee revenues are not high enough; we must ensure that they are "boosted" in the future.

Higher prices (ie, higher satoshi/byte fee-rates) are one way of boosting revenue. Unfortunately, competition from rival chains acts to suppress the market-clearing fee-rate.

A better way, is to attempt to devour the entire payments market, and claim all of its fee revenues. This can be done using Merge Mined Sidechains, without any decentralization loss.

Footnotes

1. The math is that 1.077 = (25.94/5.85)^(1/20). And note that 1.077 is below the required "stasis rate" of 1.19. ↩
2. I mean that if the USD/BTC price had been 10x higher, throughout the "bubble" of late-2017. In other words, if Bitcoin had started Jan 2017 at around 9,000 USD/BTC and then risen to 190,000 USD/BTC. ↩
3. I do remember there being much more of this, but I could only find a few examples (before giving up). Please message me if you can find/remember any other

examples. I guess I will eventually remove this paragraph if I never find any more. ↩

4. By "fees paid to LN-hubs", I mean the fees that you would pay, (off chain), to any Lightning Node that your LN-payment routes through. ↩

Links

- http://www.truthcoin.info/blog/blockspace-demand/
- http://www.drivechain.info/literature/index.html#bob
- https://medium.com/coinmonks/bitcoin-security-in-one-chart-694ee3ed8c2d
- https://www.blockchain.com/charts/miners-revenue?timespan=2years&daysAverageString=7
- https://www.federalreserve.gov/publications/2017-ar-federal-system-budgets.htm
- https://coinjournal.net/research-paper-makes-case-5-8-million-bitcoin-price/
- http://www.truthcoin.info/blog/security-budget/#fn:1
- https://en.wikipedia.org/wiki/Military_budget_of_the_United_States
- https://web.archive.org/web/20171207201015/https://botbot.me/freenode/bitcoin-wizards/2016-01-17/?msg=58099943&page=1
- https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-December/015455.html
- https://www.docdroid.net/NG1sbVq/pantera-march-2017.pdf
- https://www.investopedia.com/terms/m/m2.asp
- http://www.truthcoin.info/images/true-money/
- https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html
- http://www.truthcoin.info/blog/security-budget/#fn:2
- https://en.bitcoinwiki.org/wiki/Block_weight#Conversion_to_real_sizes
- https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-0
- http://www.truthcoin.info/blog/security-budget/#fn:3
- https://twitter.com/Excellion/status/926908067521761280
- https://twitter.com/mikeinspace/status/1078546356476628992
- https://litecoin-foundation.org/product/understanding-litecoin-the-digital-currency-for-payments/
- https://core.jochen-hoenicke.de/queue/#0,all
- https://bitcoinfees.info/
- https://www.buybitcoinworldwide.com/fee-calculator/
- https://bitinfocharts.com/comparison/transactionfees-btc-sma90.html#log
- https://www.blockchain.com/charts/transaction-fees-usd?timespan=2years
- http://www.truthcoin.info/blog/security-budget/www.truthcoin.info/blog/security-budget#2-the-block-subsidy
- http://www.truthcoin.info/blog/security-budget/#fn:n
- http://www.truthcoin.info/blog/blind-merged-mining/
- http://www.truthcoin.info/blog/gigachain/
- http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_V_2017.pdf
- http://www.truthcoin.info/images/long-run-security-budget.xlsx

Why Monetary Maximalism could fall short of expectations

By Su Zhu and Hasu

Posted February 2, 2019

Monetary maximalism is the idea that in a free market for money one big winner will emerge and that the "soundest" money is in the best position to do so.

In a previous post I wrote that "every token competes in one massive power law distribution for the title of dominant non-sovereign monetary store of value. If it does not win this rat race (or comes to a close second or third place), its market share will, effectively, be zero."

The most popular argument for why that should be the case is that it already happened once – with gold.

There are two big assumptions baked into the grand narrative of monetary maximalism today. First, that the world will gravitate towards the soundest monetary-policy coin. And second, that gold-analogies are apt in describing Bitcoin.

We would argue that this is reasoning by analogy, and that the analogy is not self-evident even for many people inside crypto, let alone outside. We should steer clear of suggesting that we can use logic to determine how this will all play out.

Instead, we should realize that for Bitcoin to become what most of the community wishes it to be, there are multiple challenges to overcome that work as counterforces to the consolidation into one money. These counterforces are:

Misalignment of incentives with crypto companies

Crypto companies are funded with the goal to capture value – especially value that can weather both bull and bear markets. The result is a value capture layer on top of Bitcoin with actors that over time evolve their own opinions that ultimately become social attacks on Bitcoin.

Many of these companies would lose if bitcoin was to become a mature store-of-value tomorrow and since they respond to their shareholders and not the Bitcoin community, it's in their best interest to prevent that.

The biggest "attack" on Bitcoin is the existence of altcoins. Investors and VCs are incentivized to push for a multicoin future because they can be paid for finding the next Bitcoin. Monetary maximalism ascending necessarily implies that this paradigm of crypto-as-tech would come to an end.

Exchanges like Coinbase are also incentivized to push for a multicoin future, as they benefit from people trading back and forth between different assets. Consolidation into one money would mean a massive decline in cross-currency trading. As an exchange, they love drama and volatility in the markets to attract traders. Their support for past contentious Bitcoin forks as an attempt to shape the protocol to suit the needs of their business and later pushing for a world where Bitcoin is just one of many assets have been entirely rational.

Miners can also decide to attack Bitcoin, with Bitmain as a prominent example. When they disliked the direction protocol development was going, possibly because they were afraid that a layered scaling approach would hurt their bottom line, they launched a social attack in the form of Bitcoin Cash. Even though the attack ultimately failed, the fork diluted Bitcoin's supply in the eyes of the public as well as its brand value.

If we look at who is actually incentivized to help Bitcoin become a mature SoV, in terms of crypto businesses there are shockingly few. A mature Bitcoin would force many of them out of business. And yet we find that Bitcoiners are constantly surprised by the so-called impure behavior of companies in this space.

Culture clash between different currencies

Because of crypto's unique nature of a social layer and technical implementation reinforcing each other, all networks are highly cultural in nature.

All coins get their properties from the shared beliefs of their holders. A strong culture has to be enforced so they can retain these properties against change.

Image Source: Unpacking Bitcoin's Social Contract

Arjun Balaji and Yassine Elmandrja have recently laid out how almost all fundamental disagreements in crypto are not about details of implementation, but about the fundamental values that each project enshrines in their social layer.

The result is competing frameworks like "Vision of the Constrained vs Unconstrained", "Money crypto vs tech crypto" or "Autonomous vs Governed", proving that there is a lot to disagree about when it comes to culture.

Just as the world is unlikely to converge to a single culture, whether we are talking about politics, art, music, language or food, so too can crypto exist for a long time as a pluralistic collection of different cultures.

If we assume there are irreconcilable disagreements on the social layer between projects and that the value of each token is agreed upon at the social layer, then the logical conclusion is that people with different cultures will prefer – and hence monetize – different coins.

We claim Bitcoin is apolitical maximalist money, but in practice the political philosophy views of bitcoiners are homogenous, especially with regards to libertarianism, and distinct from other crypto communities (which your authors have previously argued is a dangerous mismatch).

Bitcoiners tend to be objectivists – they believe there is such a thing as objective moral truths. But let us not mistake strongly held opinions for provable truths. We can neither prove that global money will evolve through soft forks rather than hard forks, nor can we prove that a premine is worse than no premine.

We can only show that the tradeoffs are such that we believe certain approaches are more promising than others. But if people disagree with us and these projects don't actually implode as we predict, then this market can well stay fragmented forever.

Appealing to human biases

Beyond basic preferences that are the result of a different culture, there are some biases inherent to our thinking that can draw people away from Bitcoin's monetary maximalism and towards other forms of money.

The most familiar example is probably the unit bias. When faced with a selection of coins most people intuitively compare the price of one unit, without regard for the number of total units outstanding. As a result, they falsely assume the cheapest unit is underpriced relative to the others and buy it.

Then there are people who have a bias in favor of innovation and tend to promote the new over the old without really looking at its limitations or weaknesses. Pro-innovation bias could play a big role in Bitcoin's future as the incentives of this market (see earlier) are aligned in such a way that crypto companies and investors collectively benefit from a steady flow of new competitors.

The most important bias working against Bitcoin, however, might be the "anti-waste" or "anti-PoW" bias. Already today there are many who categorically refuse to use any currency that uses proof-of-work for security, claiming that it is extremely wasteful and hence dangerous to our environment.

You can expect Bitcoin competitors like Ethereum to lean even more on this bias once they have completed their switch to proof-of-stake.

It's hard to imagine that people with a strong ideological dislike for proof-of-work can be convinced by economic arguments to turn around and embrace it. We find it more likely that this particular bias will continue to appeal to many people in the same way that easy answers to hard questions have always appealed to humans throughout history.

Conclusion

While we don't fundamentally disagree with the idea that a big winner could emerge from the battle of monies in the ultra-long run, there are also significant counterforces at work to prevent Bitcoin from being that winner.

The counterforces presented today all assume that the market structure itself is uncompromised, i.e. a free market for money exists. In practice, this assumption is hopelessly optimistic. Governments will continue to shape our economic realities as people in the Liberal West will not risk their lives to use one money over another for ideological reasons.

Most Bitcoiners are gleefully unaware of how few companies in this space actually have an incentive to help Bitcoin succeed, especially those who own the customer relationship and onboard all the new people into this space.

Bitcoiners should stop expecting companies, miners, etc. to virtue signal to them and instead start taking ownership of the means of production by building their own exchanges, nodes, wallets, custody, and education.

All cryptos are highly cultural. They need to be because they derive their properties from the shared beliefs of all users. This is a major differentiation from gold. The idea of Bitcoin monetary maximalism would require Bitcoin to transcend culture itself if it wants to appeal to people versus other cryptocurrencies.

Many people are questioning the "top-down" analogies used by bitcoiners today. Even many Austrian economists are not buying into Bitcoin as sound money.

So instead of mapping the history of gold over the future of bitcoin, we should look where we are today, where we want to be tomorrow, and how we can get there.

Links

- https://uncommoncore.co/a-deductive-valuation-framework-for-cryptocurrencies/
- http://artodyssey1.blogspot.com/2011/09/vytautas-laisonas.html
- https://uncommoncore.co/unpacking-bitcoins-social-contract/
- https://medium.com/@yelmandjraark/a-conflict-of-crypto-visions-160dbfc33bfa
- https://www.tokendaily.co/blog/money-crypto-vs-tech-crypto
- http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html
- https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827
- https://uncommoncore.co/evangelizing-bitcoin/
- https://en.wikipedia.org/wiki/Objectivity_(philosophy)
- https://www.artstation.com/artwork/the-man-of-armadon-ebb515a7-7168-44da-a605-21baa34d1c71
- https://news.gallup.com/poll/240725/democrats-positive-socialism-capitalism.aspx
- https://www.artstation.com/artwork/k4Eqr2%EF%BB%BF
- https://en.wikipedia.org/wiki/Anarcho-communism
- https://mises.org/wire/why-cryptocurrencies-will-never-be-safe-havens

Bitcoin is a hedge against the cashless society

By Su Zhu and Hasu

Posted February 12, 2019

When cash is gone, where will you turn to transact with a basic level of privacy? What money do you hold when negative interest rates start eating away at your bank account?

The rise of digital payments and the move towards a cashless society are often seen as the same, but there is an important difference between them.

Digital payments like Paypal, Venmo, domestic-, and international bank transfers are convenient for people and businesses to transact with. They represent fintech innovation to consumers by the market. Faster, cheaper, and more efficient forms of digital payments are uncontroversial and largely an engineering and marketing challenge.

They don't however, remove every need for cash. Cash has unique properties that digital payments have not. As physical coins and notes, it can be exchanged peer-to-peer without a middleman. Its ownership is transferred simply by handing it over. The absence of an intermediary ensures that transfers are permissionless, censorship-resistant and, most importantly, private.

Digital payments solutions do not utilize physical cash but also do not prevent anyone from continuing to use cash if they want. It is an alternative payment method to cash but is not antithetical to it. Indeed, in almost all modern societies, there coexists both a large digital economy and a large cash economy.

We will argue that the elimination of cash, even if most payments are already digital, will make society more vulnerable to surveillance, financial control, and authoritarianism.

Why do countries go cashless?

In a cashless society, the government seeks to discourage or even criminalize the holding and using of cash itself. In Sweden, it happened largely without coercion. In India, the government demonetized the 500 and 1,000 Rupee denominations of notes.

Different countries can have different incentives to push for a cashless society. In China, digital payments are primarily a tool of social control and serve as a backbone for China's social credit system. And they are making progress on it: 96% of cash payments in 2012 have turned into only 15% in 2019.

Over in Europe, central bankers are enthralled by the idea of negative interest rates. A recent IMF report states that:

“Severe recessions have historically required 3–6 percentage points cut in policy rates. If another crisis happens, few countries would have that kind of room for monetary policy to respond.”

Negative interest rates were traditionally hard to implement because cash served as a lower bound. In a cashless society, this lower bound would disappear. In a severe recession, the CB could drop the policy rate to, say, -4% to make consumption and investment more attractive relative to saving.

Recently, central banks have started to brush everyone who prefers cash with the label of a criminal. They do that by separating the uses of cash into legitimate and illegitimate. People “abroad” can hold cash “legitimately” to replace an unstable or inflationary currency. Now domestically, the only beneficiaries of an anonymity-providing currency are

“those engaged in tax evasion, money laundering and the financing of terrorism, and those wishing to store the proceeds from crime and the means to commit further crimes.”

Indeed, the use of cash in larger denominations has become so stigmatized in the US and Europe that withdrawing or carrying above a certain amount requires explicit government permission.

Problems of the cashless society

A society without cash has no ability to transact value without the omnipresence of government actors. By going cashless, societies double down on the properties of digital payments but lose all access to the unique properties of cash.

If every payment is intermediated, it becomes impossible to pay someone for anything without there being a record somewhere. It eliminates privacy and places the government as the third party in every financial event.

Governments claim that a cashless society enables them to protect citizens from criminals. The specters of terrorism and organized crime are often cited at this point. But this makes the naive assumption that governments itself can never become evil.

Because all transactions require the consent of an intermediary, they can easily be censored and funds confiscated. It might not be happening right now, but a good monetary system should be robust to changes in political moods. A cashless monetary system is less resistant to both the tyranny of the majority and shifts towards authoritarianism.

Cash may not be the right tool for the majority of transactions, but the elimination of it removes an important choice, and safeguard against government abuse, for the people.

Bitcoin as a hedge against the cashless society

When cash is gone, where will you turn to transact with a basic level of privacy? What money do you hold when negative interest rates start eating away at your bank account?

Traditionally, it has been impossible for the private market to come up with solutions for these basic human demands. The state doesn't like competition to their own fiat currency and made sure to quickly shut down all attempts of other monies to enter the market.

Bitcoin could change that. Decentralized and digital in nature, it no longer has the central point of failure that made previous "private monies" vulnerable. And it is modeled to marry the two forms of money – physical cash and digital payments – into an entirely new breed: digital cash. It can be transacted peer-to-peer, is permissionless, does not censor people or transactions, and has a reasonable level of privacy (if one knows how to use it).

We are still early into the Bitcoin-experiment, but with the cashless society looming on the horizon, we more than ever need it to succeed. Its fixed monetary policy already makes it a hedge against high inflation (that is increasingly used in places with collapsing fiat currencies like Venezuela). But, equally importantly, Bitcoin is a hedge against the demonetization of cash and the rise of the cashless society.

Links

- https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf
- https://www.weforum.org/agenda/2018/11/sweden-cashless-society-is-no-longer-a-utopia/
- https://en.wikipedia.org/wiki/2016_Indian_banknote_demonetisation
- https://blogs.imf.org/2019/02/05/cashing-in-how-to-make-negative-interest-rates-work/
- https://www.nber.org/papers/w15118.pdf
- https://medium.com/@mattahlborg/nuanced-analysis-of-localbitcoins-data-suggests-bitcoin-is-working-as-satoshi-intended-d8b04d3ac7b2

A Conflict of Crypto Visions

Why do we fight? A framework suggests deeper reasons

By Yassine Elmandjra and Arjun Balaji

Posted January 29, 2019

Conflicts raging within "crypto" are endless. Heated debates take place on a wide spectrum of issues, with little attempt to devise compromises acceptable to both sides. Interestingly, it is the same people who consistently position themselves on opposite sides of these issues. From monetary maximalism and wealth distribution to governance and consensus algorithms, the issues vary tremendously while the formed groups of opposition remain the same. Naturally, this creates an unproductive habit of each side blindly talking past the other.

In *A Conflict of Visions* and *The Vision of the Anointed*, political economist and social theorist Thomas Sowell argues that this phenomenon comes from fundamental differences in people's assumptions about the nature of systems and their limitations. While seldom consciously recognized, these sets of assumptions are the largest drivers influencing people's opinions. Since visions are rarely examined but have profound impact, Sowell introduces the "conflict of visions" as a mechanism to think about these assumptions.

By highlighting how these assumptions play a fundamental role in shaping our views, we shed light on the "conflict of visions" and ideological battles raging within proponents of cryptocurrencies.

We begin our analysis by laying out the framework of conflicting visions. Using this framework, we proceed to explain the conflict of ***"crypto"*** visions. From an understanding of the conflict of crypto visions, we then comment on the structure of arguments taking place within crypto, before diving into the meat of our analysis: an exposition of four episodes exemplifying the conflict of crypto visions.

Setting The Scene

Episodes

Defining Visions

In order to understand the conflict of "crypto" visions, it is important to first establish *what a vision is* per Sowell's work. Simply, a vision is a gut feeling about how things *should* work—a set of assumptions about the limitations and nature of the world that enables someone to understand (or at least believe to understand) why things work the way they do. Sowell defines two opposing sets of assumptions and assigns them the terms "constrained" and "unconstrained."

Constrained Vision

At the core of each vision is some strong belief or recognition of limitations. Those with a constrained vision see certain realities as unalterable, "scarcity, self-interest, human fallibility, evil." [1] Under the constrained vision, the only way to improve is to understand the fundamental laws of nature and the only way to innovate is to remain consistent with the specific parameters set forth by these laws.

The constrained vision realizes that while A may be better than B, it does not matter if A simply cannot be done. For instance, while achieving flight by wishing away gravity or ending war by wishing away violence would be great, it is simply not within the realm of possibilities. Consistent with the constrained vision are concepts like Smith's Invisible Hand and Zhuangzi's Spontaneous Order, which recognize the limitations of man and prescribe ideas that transform these limitations into progress.

The constrained vision encourages decision making by identifying tradeoffs rather than solutions. Given the limited options available, the constrained vision attempts to make the best trade-offs with an understanding that "unmet needs" will necessarily remain. As such, "particular solutions to particular problems are far less important than having and maintaining the right processes for making trade-offs and correcting inevitable mistakes." [2]

Unconstrained Vision

Those with an *unconstrained* vision believe that the only limitation to achieving a desired outcome is our lack of imagination. Through this lens, the underlying problems in any system exist only because people are not wise, caring, imaginative, or bold enough: with the right mindset, scarcity can be eliminated, man's self-interest can be corrected, imperfections perfected, and all evil eradicated. Instead of building mechanisms to work around any fundamental limitations, the unconstrained vision sees it possible to re-engineer the world to eliminate its flaws. As such, "intractable problems with painful trade-offs are simply not part of the unconstrained vision." [3]

The questions posed under the unconstrained vision are centered around how to remove particular negative features in an existing situation to create a solution. By doing so, decision making boils down to choosing the perfect solution instead of identifying tradeoffs. With the right innovation in place, few, if any, sacrifices must be made to achieve a particular improvement. In the unconstrained vision, questions of feasibility are not of primary concern, as trade-offs merely reflect varying scales of preferences and circumstances among individuals.

In both cases, regardless of the assumptions held, the desired outcome remains the same. **The goal in both visions is to create the best possible outcome.** As these assumptions are so fundamental to decision making, very rarely is there agreement on how to achieve desired outcomes. Both visions acknowledge that the world has unlimited desires and believe there to be an optimal way to accommodate for these desires.

As the labels "constrained" and "unconstrained" suggest, one vision acknowledges that we cannot get everything we want (constrained) and the other affirms our potential to be limitless (unconstrained). It should therefore come as no surprise that each vision reaches opposite conclusions on how to accommodate for a desired outcome.

The Conflict of "Crypto" Visions

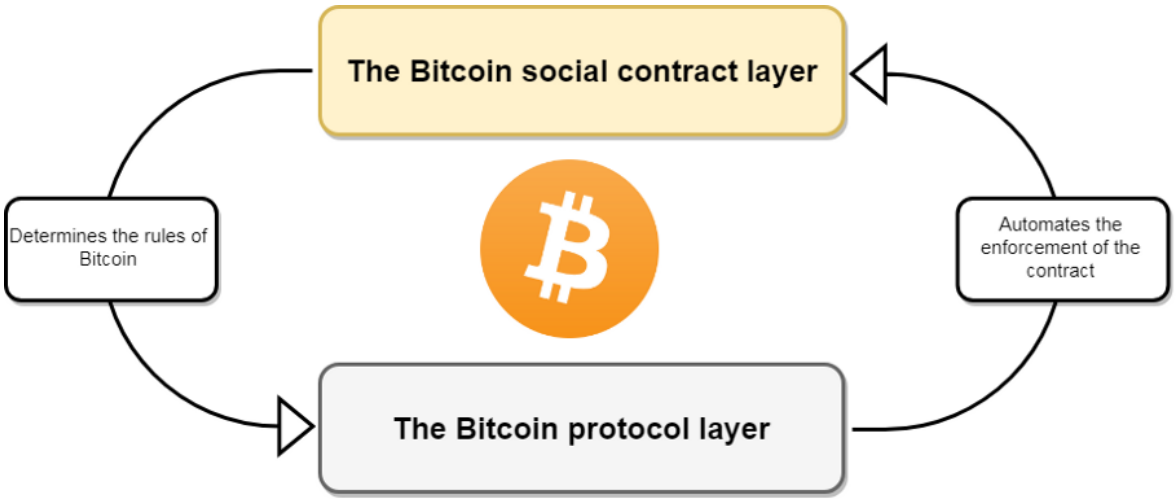
With this framing in mind, it is easy to begin to see how many of crypto's major intellectual fault lines lie along the constrained/unconstrained divide. The space is nascent: a large canvas with a massive surface area for experimentation and tens of thousands of participants, each with their own distinct end game.

In the absence of widespread adoption, participants fall back to narrative. When defining these narratives, we see intra-blockchain divides—is the end vision of "crypto" a hyper-capitalist Galt's Gulch or a radical markets-inspired disintermediated society (or both)? Even inter-blockchain narratives are inconsistent as we've seen narratives around Bitcoin and Ethereum transform over time.

This post builds on prior work from Nic Carter and Hasu exploring Bitcoin's evolving narratives (and Felipe Pereira's similar efforts with Ethereum). While researchers have focused on describing how narratives have evolved over time, less analysis has been done to frame these evolutions in context: are these evolutions simply opportunistic, the result of shifting commercial (and investment) opportunity in the cryptocurrency ecosystem, or do they reflect more fundamentally disjointed philosophical orientations?

The most salient distinction people have made, between "money crypto" and "tech crypto", is a good starting point but incomplete. In our view, these distinctions don't come down to "Silicon Valley" v. "cypherpunk"—many cypherpunks are not strong advocates of base-layer privacy and many SV entrepreneurs are wary of the "move fast and break things" culture of their peers—these distinctions are more foundational, reflective of constrained and unconstrained views of the future that technologies can help build.

The Structure of Arguments



Hasu's model of Bitcoin's social contract illustrates the dualistic relationship between the social contract and implementation details in public blockchains.

Virtually every debate about cryptocurrencies happens at the social layer. This is for good reason, given the nature of the network governance models many public blockchains follow, decisions around consensus often reinforce precedents for the future. As such, design is approached carefully and with thoughtful consideration in some major historical debates:

- Is it possible to have a sustainable long-term security model with a fixed money supply (v. mild or high inflation)?
- How important is programmability and expressiveness considering the increased attack surface and increased security cost?
- Is "absolute" base-layer privacy worthwhile if it increases the difficulty of verification of the money supply (or requires greater trust in the issuers or maintainers of the system)?
- Is increasing the block-size—lowering transaction fees and allowing full node cost to scale up linearly—a short-sighted decision given the uncertainty of future advancements?

These debates are rarely presented as such. Rather than presenting ideas as a question of tradeoffs, discourse—whether in a tiny Telegram chat or on stage at a conference—devolves into religious fervor and ad hominem. Cryptocurrency prices serve as a real-time scoreboard for winning narratives, with ownership creating bias as people "shill their bags" in the face of presenting debates with nuance.

Much of the debate ends up substituting opaque proclamation for arguments. Enthusiasts fall back to simple quips and vacuous rhetoric—technical features that are favored and already exist are "here to stay" while proposed features are "inevitable." Unpopular existing features are "obsolete" and unpopular, ambitious pitches are "unrealistic."

	Existing	Non-existing
Favored	“Here to Stay”	“Inevitable”
Opposed	“Obsolete”	“Unrealistic”

To see through this vacuous rhetoric, Sowell suggests applying general principles of common sense (which are nevertheless often ignored) illustrated below:

1. All statements are true, if you are free to redefine their terms
2. Any statistic can be extrapolated
3. A can always exceed B if not all of B is counted or if A is exaggerated
4. For every expert there is an equal and opposite expert, but for every fact there is not necessarily an equal and opposite fact.
5. Every policy is a success by sufficiently low standards and a failure by sufficiently high standards.
6. Most variables can show either an upward trend or a downward trend, depending on the base year chosen.
7. You can always create a fraction by putting one variable upstairs and another variable downstairs, but that does not establish any causal relationship between them, nor does the resulting quotient have any necessary relationship to anything in the real world

A careful examination of Sowell’s principles sheds light on the lack of thoughtful consideration that much of “crypto” debate is predicated upon.

Episode I: Monetary Maximalism vs. Multicoinery

First, we only had Bitcoin, released by Satoshi, who by all evidence was likely an outsider to the establishment. As Bitcoin was strictly focused on offering a new electronic cash system without the reliance of a trusted central mint, the utmost focus of enthusiasts and developers has always been security (of the codebase) and security again (of the monetary policy). Historically, changes to Bitcoin have been debated not just on their merits but in their second and third-order effects on security.

The original grassroots cypherpunk movement of Bitcoin was never focused on "blockchain technology". To this day, the majority of "Bitcoin maximalists" or "shitcoin minimalists" see Bitcoin's focus as a grassroots bottom-up effort in engineering in stark contrast to the more formal top-down efforts employed by projects like Ethereum, Tezos, and others.

Inspired by the view of Austrian economists, Bitcoiners have historically opted for a "simplistic" & "adversarial" view of the world, grounded in an understanding of monetary history: that the "killer app" is money and that Bitcoin, a potential global money competitor, has the largest potential TAM. In their view, other projects attempting to create a better Bitcoin and iterate on its "fundamental design limitations" misunderstand its intended use.

What Bitcoiners attack with historicism, multi-coiners defend with vision, often criticizing this limited, "simplistic" view held. The unconstrained vision believes it to be "a major failure of imagination (or really just plain observation, frankly) to think that crypto has nothing more to offer than a slow and volatile form of sound money."

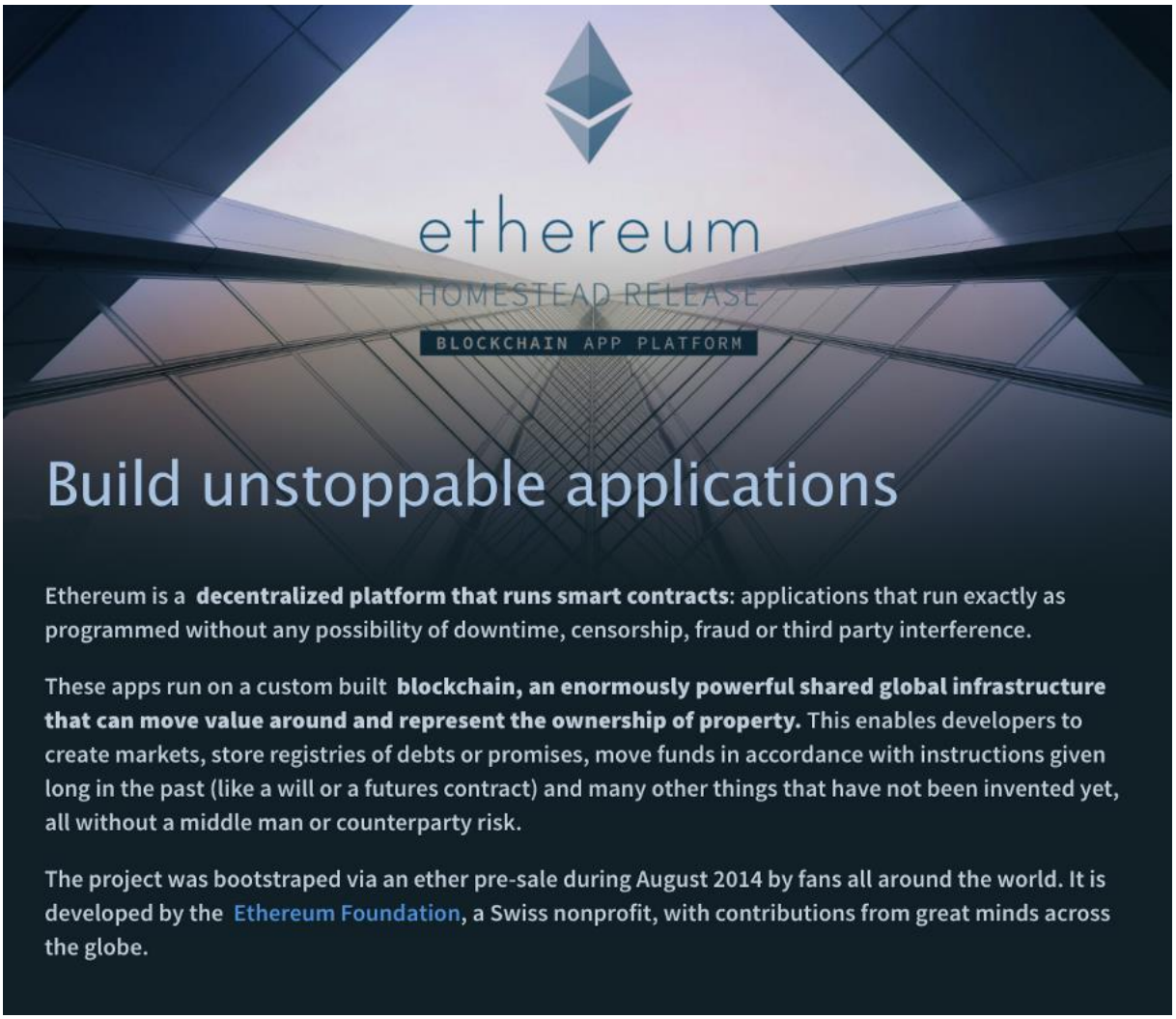
Under these sets of unconstrained assumptions, Bitcoin might instead be described as a part of the "calculator era" of cryptocurrencies, as recently explained by Andreessen Horowitz partner Jesse Walden:

> Many argue that that the most important property of a decentralized money system is security, not programmability, and that a limited scripting language is thus a feature, not a bug. Through that lens, we can view Bitcoin as more of a calculator than a computer (and that is intended as a positive remark!). **It is purpose built and good at its task, but for developers keen to tinker and build new applications an evolution to a new architecture was required.**

To people biased with an unconstrained view of the world, Bitcoin suffers from a lack of vision. As such, the same feature (e.g. complex programmability) might be viewed by the constrained vision as a bug and by the unconstrained vision as a feature. Sowell (135) clarifies this distinction:

> To those with the unconstrained the question is: What will remove particular negative features in the existing situation to create a solution? Those with the tragic vision ask: What must be sacrificed to achieve this particular improvement?

On the other hand, to the constrained vision **there are no solutions, only trade offs**. Bitcoin developers like Jimmy Song argue that blockchain technology comes with significant tradeoffs ranging from the high costs of development and maintenance, to the challenges of coordinating complex incentives across many parties. Bitcoiners view capital-b "Blockchain" and "tokenization" advocates as missing the point: with a distributed ledger hammer, every incentive problem looks like a nail.



Ethereum's marketing from late 2016 proposed "unstoppable applications", enabling developers to do lots of things, many of which have not been invented yet. While Turing Completeness may have its advantages, it does not come without significant tradeoffs.

Many Silicon Valley investors have historically thought of the killer app of blockchains as creating new markets, with Naval Ravikant famously notingthat blockchains can replace networks with markets. Pantera Capital CIO Joey Krug sees disintermediation of traditional companies as a core part of their "blockchain technology" thesis, suggesting that in their strongest form, blockchains can create marketplaces in industries far from financial services, massively up-ending traditional businesses in the process:

Blockchain tech is good for multi-sided marketplaces—particularly for finance. Other use cases, which really just converge with financial markets, include: file storage markets like Filecoin; computational markets; markets for items in video games; namespaces like Handshake; regular betting/gambling like FunFair; and sharing economy protocols like Origin. **These projects will fuel a classic disintermediation play: cut out the existing profit-seeking corporations and replace them with software. As software eats the world, software is eating software.**

Silicon Valley's bias for the unconstrained view is straight-forward. By defining networks like Bitcoin as software-first, the role of the technologist precedes that of a monetarist. As such, "blockchain" simply becomes one amongst a number of emergent platforms in the ever-evolving internet infrastructure (Web 3.0). In "What comes after open source?", Andreessen Horowitz's Denis Nazarov elegantly explains this view:

Years of state accumulated by innovative companies produced tremendously useful services (search, maps, social, commerce), but further combinatorial innovation is off-limits to outside developers and entrepreneurs. **Rebuilding services from scratch on the same terms and this late in the game is hopeless.**

As crypto networks evolve, they are likely to provide strong incentives to unlock further state and create open services in many areas dominated by closed ones today. **Open services powered by crypto networks will present unprecedented opportunity for a new generation of developers and entrepreneurs to innovate.**

The Use of Language

The technologist's articulation of the potential of blockchain technology rejects current constraints with a bias to technological progress. Not seeing this vision is often attributed to a lack of imagination on the part of the "doubters." Who could've seen the potential of the internet in 1995 given the nascent state of internet architecture or the explosion of mobile applications transforming the world given the limited capabilities of the first iPhone? Sowell clarifies:

Intractable problems with painful trade-offs are simply not part of the vision of the unconstrained. **Problems exist only because other people are not as wise or as caring, or not as imaginative and bold, as the unconstrained.**

This is visible even in the linguistic choices of the unconstrained view, with Sowell noting that "the vocabulary of the unconstrained is filled with words reflecting their rejection of incremental trade-offs and advocacy in categorical solutions."

More generally, the use of language becomes a strong reflection of an individual's views. The term "shitcoin minimalist", for instance, indicates a constrained view of the potential of blockchain-based solutions to human problems.

The term "Bitcoin maximalism" itself was a derogatory claim made by Vitalik Buterin, who started Ethereum after categorical rejection of his proposals to materially expand the

available feature set on Bitcoin. It has since been weaponized, with Vitalik noting that "I do wish ill on *bitcoin maximalism*, but only because bitcoin maximalism as an ideology seeks elimination of all non-bitcoin platforms." While the term has been co-opted by Bitcoiners to reflect a descriptive monetarist view rather than a prescriptive ideology, it is still a major point in the multi-coiners sieve to discount Bitcoiners' claims, with Vitalik clarifying his view, even going so far as to *use* the word "constrain":

Because **I view single-coin maximalism as an oligarchic rent-seeking ideology that seriously *constrains* the possibilities of cryptocurrency innovation** and makes it dependent on a political process (Bitcoin governance) rather than market competition?

Sowell preempts this conflict in his work, clarifying that "the anointed often place permanent labels on people, on the basis of transient circumstances" in order to more solidly position themselves as the underdog, fortifying "us v. them" dynamics. These labels aren't useful—the interests of a few "toxic" Bitcoiners don't reflect the views of most bitcoin holders, who are not even aware of the nuances of online cryptocurrency discourse.

Bitcoiners push back on this unconstrained view further, noting that they are largely divorced from science. Even the strongest proponents of the unconstrained view acknowledge the delta between the realities of today's technology and appeal to tomorrow's, with Walden further noting:

How exactly this will work is very much in the realm of open research. Proponents of "server era" architectures posit that a "cloud era" experience will emerge through standardization and abstraction of inter-blockchain communication among heterogeneous blockchains. Others, like Ethereum 2.0 (Serenity) and Dfinity, are converging on sharded versions of homogenous, turing-complete chains. And still others are researching entirely new architectures that move computation off-chain.

Through the lens of technological utopianism, or nirvana fallacy, feasibility is an after-thought to be attacked by a portfolio of diversified bets—the venture capital model—rather than an exploration of tradeoffs in an ever-exploding design space.

Episode II: The "fairness" of crypto distribution

Since the very beginning, debates about the "fairness" of various cryptocurrencies have sparked fiery conversation about what future wealth distribution should look like. This is expected—if cryptocurrencies actualize the full cypherpunk vision for the future, they represent one of the greatest wealth transfers of all time. With discussions of current income inequalities dominating global discourse, the potential for cryptocurrencies to exacerbate existing problems have been top of mind for many.

Over the years, there have been many attempts to quantify this disparity, including Balaji Srinivasan's work exploring different networks' Gini coefficients. These research efforts have sparked outrage from cryptocurrency enthusiasts and external critics alike, including:

Dogecoin creator Jackson Palmer:

Cryptocurrency analyst Ferdous Bhai:

Additionally, NYU professor and notorious cryptocurrency critic Nouriel Roubini remarks that "the inequality coefficient of BTC is worse than North Korea that has the worst inequality on earth."

This conflict is another example of the strain between bottom-up constrained views of Bitcoiners, who believe attempting to design "ideal" wealth distribution is futile, and critics, who believe that Bitcoiners are "unfairly" rewarded for their early adoption. Defenders of the constrained view maintain that Bitcoin's purpose is simply offering a non-sovereign money alternative—explicitly money that is designed *not* to be confiscated or debased—and that the distribution of bitcoins is perfectly calibrated by the free market to reward investors based on their place in the risk curve. Some further argue that given empirical suggestions that ownership concentration turns over with market cycles, concern over distribution is excessive—a problem solved by free markets.

Where holders of the unconstrained view project their desire for a certain wealth distribution in society, the constrained view clarifies that this is a violation of Bitcoin's single purpose: preventing forced wealth redistribution. Sowell, once again, thoughtfully comments on wealth disparities in practice:

> If one believes that income and wealth should not originate as they do now, but should instead be distributed as largess from some central point, then that argument should be made openly, plainly, and honestly. But to talk as if we currently have a certain distribution result A which should be changed to distribution result B is to misstate the issue and disguise a radical institutional change as simple adjustment of preferences. The word 'distribution' can of course be used in more than one sense.... **What is really being said is that numbers don't look right to the [unconstrained]–and that this is what matters, that all the myriad purposes of the millions of human beings who are transacting with one another in the marketplace must be subordinated to the goal of presenting a certain statistical tableau to [unconstrained] observers.**

Despite this, conflicting visions persist. More ambitious experiments than ever are being pushed, including attempts to create "UBI via mass airdrop" or Bitcoin-alternative money systems specifically designed to prevent long-time wealth hoarding. Subscribers to the constrained vision push back against these forms of idealism with practicality: despite having good intentions, early iterations of these systems are often naively designed and ignore the second or third-order effects of top-down incentive manipulation. In many cases, these policies could end up hurting those they purport to help by creating gamifiable or broken incentives that exacerbate existing inequalities.

Episode III: Governance

The meta-problem of open-source protocol governance has been a longstanding debate where a fault line can once again be identified along the constrained and unconstrained divide.

The constrained vision believes that optimal governance is achieved through a bottom-up approach that attempts to minimize subjectivity and maximize trustlessness, while the unconstrained vision believes optimal governance is achieved through a formalized on-chain approach that interfaces with existing, top-down legal frameworks.

Nick Szabo's mental model of wet code and dry further illustrates the nature of these conflicting visions. At the highest level, "wet code" is interpreted by humans, and "dry code" is interpreted by computers. Examples of wet code include law and traditional contracts. Examples of dry code include smart contracts, secure property titles, and the domain name system. Human language might be somewhere in between wet code and dry: if a computer program is able to translate text to multiple languages, for instance, human language may be considered dry.

The distinction between wet code and dry raises questions around the extent to which formalizing governance is possible without exposure to human subjectivity. If wet code is inherently human-readable and dry code computer-readable, the constrained vision would posit that transforming a wet code legal system into dry code would not only add additional complexity but also introduce elements of human subjectivity.

Because the specifics of law and governance are complex and unknowable, the constrained vision opposes fully formal on-chain governance: implementation of "law as code" becomes heavily subjective and unlikely to account for the unpredictable changes in the real world.

Since avoiding human subjectivity and maximizing a network's trustlessness is the constrained vision's top priority, "law as code" becomes unattractive. As Bitcoin Core developer Matt Corallo highlights, "trustlessness is the ability to use Bitcoin without trusting anything but the open-source software you run." The constrained vision posits that a formalized governance system, which adds unyielding subjectivity *to* the open-source software, would come at the cost of automated integrity and trustlessness.

Through formalized on chain governance, changes to dry code are completely arbitrary, a reality the constrained vision avoids by prioritizing and questioning the process first. As Sowell suggests:

> To those with the vision of the anointed, it is simply a question of choosing the best solution, while to those with the tragic vision the more fundamental question is: Who is to choose? And by what process, and with what consequences for being wrong?

A software's formal governance system is created from a dry code implementation of something that is inherently wet code. As a result, the control and trust of the software transfers to humans. Under the unconstrained vision, humans *should* be able to change a

network's implementation in an ongoing fashion, as humans are the final arbiters of truth. As such, the vision pushes back on the subjective claim that trust-minimization through software automation is optimal, refusing to accept such a claim as "law."

In practice, under the constrained vision, automated governance is limited to maintaining the set of verification rules, as seen in Bitcoin's governance model. In the case of a failure in a wet code process, such a system would resort to a fork, a change in the protocol influencing the validity of the set of rules. Since forks are seen as bugs to the unconstrained, the value proposition of an on-chain governance system is that it precisely avoi*ds* forks and encourages high upgradeability. However, by formalizing governance, the risks of undergoing a fork under what at the time would have been considered to be a perfect implementation may potentially speak to the subjective nature of the implementation. For the long term sustainability of the protocol, the constrained vision posits this to be detrimental.

Episode IV: Proof-of-work vs. Proof-of-stake

Bitcoin's proof-of-work is an embodiment of the constrained vision, a mechanism to work around fundamental limitations rather than re-engineer them. First explained by Nick Szabo in *Money, blockchains, and social scalability*, Bitcoin's proof-of-work accommodates our cognitive limitations and behavior tendencies by making a necessary and intentional tradeoff: **greatly sacrificing computational scalability to improve social scalability.**

A feature to the constrained, a bug to the unconstrained.

The ability to participate in an "institutional technology" is predicated on the technology motivating participation and protecting the system and its participants from malicious activity. By improving social scalability, which proof-of-work does so effectively, the number of people who can beneficially participate in the system is maximized. Therefore, the constrained, "proof-of-work" vision posits that Bitcoin's success should not be determined by its computational efficiency but by its ability to increase social scalability through trust minimization.

What the unconstrained vision deems computationally inefficient and unscalable, the constrained vision not only deems an intended tradeoff, but a fundamental feature: specialized, dedicated hardware *should* perform a function whose sole output is to prove that the computer *did* indeed execute a costly computation. As Nick Szabo highlights, "prolific resource consumption and poor computational scalability unlocks the security necessary for independent, seamlessly global, and automated integrity."

While an implementation of both computational and social scalability is optimal, the constrained vision acknowledges that it cannot be done without compromising security. Embedded in computer science is a fundamental understanding of tradeoffs in security and performance where inevitably, automating integrity requires high resource utilization. Even with breakthroughs in computer science, the constrained vision recognizes that total

integrity and absolute trustlessness is infeasible, making the delicacy of explicit and intentional tradeoffs all the more imperative. As such, the constrained vision fully accepts that such tradeoffs are unavoidable, and "it is probable no such big but integrity-preserving performance improvement is possible." [4]

To the unconstrained vision, the assumptions around proof-of-work are entirely different. Instead of asserting that proof-of-work sacrifices computational inefficiency for social scalability, the unconstrained vision asserts that proof-of-work unjustifiably consumes significantly more resources than it creates, making it a wasteful and archaic system in dire need of improvement.

A commonly used statistic the unconstrained vision employs to illustrate proof-of-work's "wastefulness" is a measurement of the amount of energy the system expends as a proportion of the total transaction volume the system processes. By employing such a statistic, it becomes obvious why under the unconstrained view, proof-of-work is so scandalously inefficient: "Bitcoin consumes five Hiroshima's worth of energy per day" only to process "a mere fraction of what a payment service like Visa processes."

The use of this argument to illustrate proof-of-work's wastefulness implies that trust minimization is not viewed as a necessary feature in the unconstrained vision. If it were, comparing Bitcoin to Visa would be futile: **Visa does not provide the same improvements in social scalability through trust minimization *precisely because* it is more "computationally efficient".** Such a comparison not only dismisses the existence of limitations, but attempts to associate two completely unrelated variables (i.e. energy expenditure and transaction volume are not functions of each other). As Sowell highlights, wrongful association of these variables leads to "statistical extrapolation without any analysis of the actual processes from which these numbers were generated." [5]

A costless alternative?

Deeming proof-of-work wasteful suggests a cheaper, more prudent alternative exists. To the unconstrained vision, the reason proof-of-work has not fully succumbed to an alternative may come from a lack of care for the environment or a lack of imagination of technological advancements as Emin Gun Sirer suggests:

> 100 years from now, future generations will talk about the PoW craze with the same bemused view we hold for other mass manias. The absurdity of wasting energy to make chicken scratch marks on an electronic ledger is going to become more obvious. We are going to look back the same way we look at the use of CFCs and leaded gasoline. We should replace it with systems that can do better.

As previously highlighted, the unconstrained view is to remove specific negative features in the existing situation to create a solution. In the context of proof-of-work, the question posed by the unconstrained is then: "how can we ***remove*** the computational inefficiency and energy wastefulness of proof-of-work to create a better sybil-control mechanism and consensus algorithm?"

Attempting to answer this question, mechanisms like proof-of-stake have emerged as the most popular solution, as Ethereum's Vitalik Buterin highlights:

"The philosophy of proof-of-stake is not 'security comes from burning energy', but rather 'security comes from putting up economic value-at-loss'.

In a proof-of-stake system, a blockchain appends and agrees on new blocks through a process in which anyone who holds coins inside of the system can participate and the influence an agent has is proportional to the number of coins (or 'stake') it holds. **This is a vastly more efficient alternative to proof-of-work 'mining' and enables blockchains to operate without mining's high hardware and electricity costs."**

Under the unconstrained view, proof-of-work is classified solely as a sybil-control mechanism. As such, there is greater justification for removing energy spend on coin production. Emin Gun Sirer explains:

Thus, the goal in the unconstrained vision is to implement an inherently costless system without leakage. In proof-of-stake, network participants are not required to use inordinate amounts of energy to maintain ledger immutability, significantly reducing labor intensity. A reduction in labor intensity would be more fair and help encourage community participation due to lower barriers to entry. Specifically, the unconstrained vision claims that taking mining out of the hands of entities with access to excessive amounts of low cost energy would help redistribute the work evenly and lead to a more democratized system. By removing the feature that secures value in a proof-of-work system, security in turn is derived from the value stored *within* the system itself. As David Yakira notes, "in a sense, a PoS system is recursive, augmenting the value it stores implies better security which further allows the value to increase and so on."

Under the constrained vision, however, defining proof-of-work as merely a sybil-control mechanism is non-exhaustive and trivializes its purpose. Proof-of-work is also seen as essential for maintaining unforgeable costliness "giving digital blocks real-world weight" and enforcing a predictable, meritocratic distribution mechanism.

Because the constrained vision believes there to be "no solutions, only tradeoffs," a costless mechanism without leakage would also be definitionally impossible, as Paul Sztorc notes:

"Switching the payout-trigger to a social or political dimension would merely transpose the work-expenditures correspondingly to the realms of bribery and propaganda.

If an object has value, people will spend effort to chase it, up to whatever the object is worth (MC=MR). This effort is also "work". [Thus], a stable solution to these problems is ***definitionally impossible***, as there is always an incentive to work until marginal cost equals marginal revenue."

The Future Remains To Be Built

As we've highlighted, these divisions between cryptocurrency enthusiasts, investors, and builders can be seen across the "unconstrained" and "constrained" axes, two conflicting ideologies that transcend geography, professional associations, or backgrounds.

We believe that the most likely outcome after the full possible actualizations of these visions is convergence in some form. While the future remains uncertain, a conflict of *visions* persists because in reality, visions are all we have to focus on ahead of a multi-decade roadmap of adoption and integration.

The dominant visions of the constrained view are not mutually exclusive with the more abstract unconstrained view. While on the surface, inter-currency battles persist, the final boss (third party disintermediation)—which unites everyone alike—is shared. Though differences emerge upon squinting, high-level goals are not divergent. Privacy-aware cypherpunks want to see the destruction of ad-driven technology monopolies and Bitcoin remains a useful tool against tyrants independent of political, social, or religious affiliation. While cryptocurrency adoption appears zero-sum, experimentation is at the core of open-source and expands the size of the pie in the short-to-medium term by bringing new entrants to the market with disparate views while concurrently validating existing implementations.

It may be that for creating a global money, only a tightly constrained, focused view can prevail as launching a system mimicking a Swiss bank in your pocket requires this level of carefulness. If indeed blockchains represent a major evolution in computing, those systems may follow an evolving philosophy closer to a traditional software release cycle with constantly iterated release cycles.

These debates will be reminisced upon like early internet debates about the ideal protocol standard or intranets and the Internet (earlier generations' blockchains v. bitcoin) or debates even further back about the viability of inferior monetary metals to gold. Ultimately, winners will emerge out of today's conflicting visions invoking "how did we not see that coming?" commentary in the process.

For now, the future remains to be built.

Links

- https://en.wikipedia.org/wiki/A_Conflict_of_Visions
- https://en.wikipedia.org/wiki/The_Vision_of_the_Anointed
- https://www.tsowell.com/
- https://en.wikipedia.org/wiki/Invisible_hand
- https://en.wikipedia.org/wiki/Spontaneous_order
- https://www.conservapedia.com/Galt%27s_Gulch
- http://radicalmarkets.com/
- https://medium.com/@nic__carter/visions-of-bitcoin-4b7b7cbcd24c
- https://tokeneconomy.co/visions-of-ether-590858bf848e
- https://www.tokendaily.co/blog/money-crypto-vs-tech-crypto

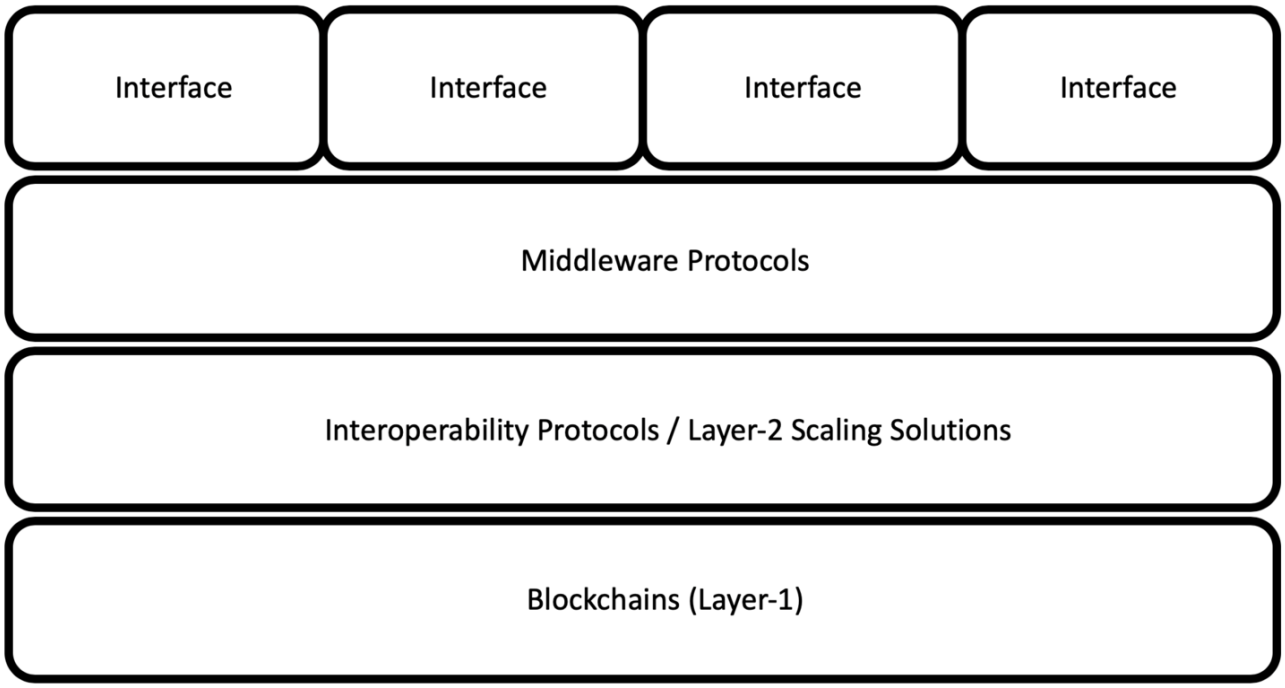
- https://medium.com/@hasufly/bitcoins-social-contract1f8b05ee24a9?sk=27e8cf65d45c46ffae1466ce2ac31b48
- https://medium.com/@pierre_rochard/bitcoin-governance-37e86299470f
- https://twitter.com/ali01/status/1073005172949843968
- https://jessewalden.com/4-eras-of-blockchain-computing-degrees-of-composability/
- https://medium.com/@jimmysong/why-blockchain-is-hard-60416ea4c5c
- https://twitter.com/naval/status/877467629308395521
- https://medium.com/@PanteraCapital/a-crypto-thesis-47eaacf861ca
- https://denisnazarov.com/what-comes-after-open-source/
- https://twitter.com/VitalikButerin/status/875191751752826880
- https://twitter.com/bitstein/status/993819747623096320
- https://twitter.com/VitalikButerin/status/993679744393732097
- https://en.m.wikipedia.org/wiki/Nirvana_fallacy
- https://news.earn.com/quantifying-decentralization-e39db233c28e
- https://twitter.com/ummjackson/status/1053122713848569857
- https://twitter.com/ferdousbhai/status/1087596119138287617
- https://twitter.com/Nouriel/status/1049092516233064451
- https://blog.picks.co/bitcoins-distribution-was-fair-e2ef7bbbc892
- http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html
- http://bluematt.bitcoin.ninja/2017/02/28/bitcoin-trustlessness/
- http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html
- https://twitter.com/el33th4xor/status/1055513144838238208
- https://twitter.com/martinvars/status/936654528736366594?lang=en
- https://twitter.com/el33th4xor/status/1045115535254540288
- https://twitter.com/el33th4xor/status/1046133563584909313
- https://medium.com/orbs-network/on-stake-and-consensus-a05e52daa496
- https://twitter.com/hugohanoi/status/1046100388133449728
- http://www.truthcoin.info/blog/pow-and-mining/
- https://twitter.com/naval/status/935878356507258880

The Defensibility of Middleware Protocols

By Chris Burniske

Posted February 14, 2019

Interoperability of state and value is likely to place downward price pressure on layer-1 blockchains that have no monetary premium, while enabling strong *middleware protocols* to achieve cross-chain, winner-takes-most dominance in their respective services. While not a perfect mapping to traditional use of the term *middleware,* these protocols can be thought of as anything sitting just below the interface layer (i.e., the applications the end user interacts with), but leveraging the lower-level functionality provided by layer-1 blockchains and interoperability protocols.



Others have called these service-layer protocols, as they focus on providing a specific service to the interface layer, be they financial, social, technological, etc. Financial services include things like exchange, lending, and risk-management; social services offer functionality like voting structures, arbitration, or legal-contract management; technological services include components like caching, storage, location, and maybe the granddaddy of them all, a unified OS for protocol services to be neatly bundled to the interface layer.

Financial-service protocols that Placeholder has invested in include 0x, Erasure, MakerDAO, and UMA, while Aragon is our main social-service protocol to date, and technological-service protocols that we work with include CacheCash, Filecoin, FOAM,

and Zeppelin. All of these protocols have originated on Ethereum, but we believe interoperability of state and value—the promise of a Cosmos, Polkadot, and Ethereum 2.0 future—will allow these protocols to become horizontally defensible starting from Ethereum's base.

Take MakerDAO, for example. Its token, MKR, can be thought of as an insurance pool for secured loans originated through the platform. The larger the overall value of MKR, the greater the insurance and therefore lower the risk for all users of the system. Let's say FakerDAO pops up on Tron, providing the exact same service, but with its own native governance asset, FKR. Right now, it would be hard for the Maker team to leverage the value in MKR to secure a parallel system on Tron, but with interoperability of state and value it would become considerably easier.

Assuming the Maker team can build out for Tron before FKR gets to a similar value as MKR, then they should be able to deploy on Tron and provide a lower risk service than FakerDAO can, insured by the much larger pool of value stored in MKR. With two communities driving utility through MakerDAO, MKR's pooled value is then likely to significantly outpace FKR's, further widening the risk and quality of service-gap (Whether MKR holders would want to underwrite the risk of operating on another chain like Tron is a separate question).

We believe similar dynamics will play out for many other middleware protocols, though in different ways depending on the cryptoeconomic [1] and governance design of the system. Protocols whose reliability, security, speed, liquidity, or coverage scales with the size of the asset base and nodes supporting it, stand to do well in an interoperable world.

Footnotes:

[1] Most middleware protocols are likely to employ some variant of a capital asset as their cryptoeconomic model, where supply-siders must stake the asset to provide the service, giving them access to value-flows for so doing.

Sidenote: After viewing what we hold, some have asked why ether isn't included. While we are fans of the Ethereum team, and think that people underestimate the soft-network effects of the system, we don't hold ether (or any layer-1 smart contract blockchain) in part for the above reasons. We believe the middleware protocols we've invested in give us upside exposure to ether (if ETH appreciates in fiat terms then the *quality* assets that ride atop it tend to also appreciate in fiat terms, holding their value relative to ETH), while also protecting us from the downside exposure should more dominant layer-1 smart contract blockchains, or interoperability protocols, start to steal from ether's value.

Links

- https://twitter.com/cburniske/status/1022140822165352448
- https://www.placeholder.vc/about
- https://www.placeholder.vc/blog/2019/1/23/maker-investment-thesis

Blockchain Privacy: Equal Parts Theory and Theater

Satoshi Has No Clothes

By Ian Miers

Posted February, 2019

The cryptocurrency community has done a poor job of evaluating privacy. We are even worse at explaining the tradeoffs of different implementations to regular users. Improvement is necessary and it needs to happen now. Many of these protocols aspire to be the future of payments — one of them may win. By the time that happens, it'll be too late to get the design right.

In 2011, when I started working on privacy in cryptocurrencies, it was commonly thought that Bitcoin was private. WikiLeaks solicited "anonymous Bitcoin donations" on Twitter, which is somewhat tragic; we can confidently guess that a few WikiLeaks donors were in sensitive positions, at least.

Now we're aware that Bitcoin is nowhere close to anonymous. A number of academic papers have shown that you can link pseudonymous transactions together and thereby track what someone is doing across a blockchain. In addition, companies like Chainalysis are in the business of discovering and surfacing such analytics.

Bitcoin is Twitter for your bank account. Anyone can see what you're doing. That includes your family members, friends, current and former romantic partners, business associates, competitors, all the way up to government agencies. Even people who are government decision-makers themselves should remember that other governments — the ones they don't like — will delve into the details of their finances.

It's common to say that "privacy is dead," suggesting that it's hopeless to protect your privacy. The idea is that someone — the government, Google, a mysterious bogeyman — will always know things about you. But there's a difference between one person knowing your deepest, darkest secrets, and everyone knowing them. Just because Google knows your browsing history doesn't mean that you want it to be public.

During the past seven or eight years, we've seen many proposals to add privacy to cryptocurrencies. The techniques range from simple things, like avoiding address reuse, to complex cryptographic protocols. Measuring the privacy afforded by a certain implementation is tricky.

Right now, we can't resort to empirical methods. It would be akin to evaluating internet privacy in 1992, when the only websites were ones at CERN. That was before targeted ads, and tracking cookies; Google AdWords didn't launch until 2000. Richard Stallman was

considered an alarmist crank. It was before we really used the web for anything where it would be worth tracking people.

In the current cryptocurrency ecosystem, you cannot look at people's usage and then produce an authoritative estimate of whether (or which!) privacy techniques are effective. The necessary data isn't there. Today nearly all transactions are speculative, which illustrates the privacy needs of risk-loving investors, but leaves aside everyone else.

We don't have the rich tapestry of structure that results when you pay for your train trip, walk to the local market to buy a sandwich, then mail a package at the post office, then buy something at the vending machine. That kind of behavior, and the data generated by it, is not evident among the vast majority of cryptocurrency users.

As a researcher, even if this data existed, I couldn't use it. I have limited access to data due to cost concerns, and I and other academic researchers have ethical limitations imposed by the Institutional Review Board. Our adversaries do not.

The upshot is that an empirical evaluation of future privacy is impossible. Instead of relying on data, we must resort to thought experiments. We need to think through the usage of our systems in the coming decades and consider how that will play out. One viable approach is to look at the problems in related domains.

Real-World Privacy Threats

The most common threat that people bring up is governments and law enforcement leveraging blockchain data. As with the privacy needs of speculators, that is one threat, but it's not the only one. Nor is it the threat most likely to affect the public at large. (That said, we should not dismiss the concerns of activists and dissidents.)

Looking beyond cryptocurrencies, we recently learned that Google has been collecting offline payment data from Visa and MasterCard and using it to build up profiles for targeted advertising. You may think that Google does a good job and institutes reasonable security controls, or you may not. Regardless, it's a worrying trend (and not a new one). If Google is doing it, so are people and entities that are less scrupulous. You've never heard of them and you have no idea how they're using information about your transactions.

Similarly, we know that companies want to build up rich profiles of their customers' behavior. There are numerous sources of data for them to compile — for example, usage of loyalty cards and coupons. Retailers can track and analyze this information, to the extent that they're able to guess when customers are pregnant, since pregnant customers exhibit certain purchasing patterns. Other medical conditions likely fall in the same boat.

News reports have indicated that retailers aim to discover these things before you even know yourself… or at least before the other people in your family know. In 2012, Charles Duhigg wrote a feature for the *New York Times Magazine* that contained this anecdote:

> *"About a year after [Target data scientist Andrew Pole] created his pregnancy-prediction model, a man walked into a Target outside Minneapolis and demanded to see the manager. He was clutching coupons that had been sent to his daughter, and he was angry, according to an employee who participated in the conversation. "My daughter got this in the mail!" he said. "She's still in high school, and you're sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?" The manager didn't have any idea what the man was talking about. He looked at the mailer. Sure enough, it was addressed to the man's daughter and contained advertisements for maternity clothing, nursery furniture and pictures of smiling infants. The manager apologized and then called a few days later to apologize again."*
>
> *"On the phone, though, the father was somewhat abashed. "I had a talk with my daughter," he said. "It turns out there's been some activities in my house I haven't been completely aware of. She's due in August. I owe you an apology." There are serious privacy problems with data about what people buy. It's plausible that sexual orientation could be targeted in the same way. These examples are more fine-grained than you might be able to extract from a blockchain, but nonetheless the issue manifests in a system like Bitcoin."*

A more on-the-nose example is Venmo. For those of you who don't know, Venmo is a service primarily used for payments between friends, to pay for a bar tab or split a restaurant check. By default, Venmo has a public feed of every transaction that its users make. It includes your name, the recipient's name, and a memo field describing why you paid them. That is pretty close to the data on the Bitcoin blockchain.

We've seen the failure cases of Venmo's public feed, including small-time pot dealers being arrested and supposedly lighthearted guides to stalking your ex-boyfriend. That's playful in theory, but actually no, it's creepy and abusive. People should not be okay with any system having these features.

Another threat that's more well-known to the cryptocurrency community, where issues are even cropping up today, is fungibility. We know that for certain cryptocurrencies, freshly mined coins sell for a premium. Exchanges sometimes block customers based on their transaction history; where they've sent their money in the past.

It's important to note that exchanges are powerful. We can't think of them as merely third-party observers. They know more about you than just the transaction graph. Frequently they conduct transactions on behalf of their users. The privacy problem here is akin to trying to maintain privacy from Google while using Gmail and Google Maps on an Android phone. At some level, you're embodying your adversary.

Remember, Bitcoin is Twitter for your bank account. And not the kind of Twitter where you choose what tweets to write and publish. Bitcoin is more like a creepy alternate-universe Twitter that automatically transmits all of your thoughts.

Defenses and Failures

What are the viable defenses?

In a world of massive data collection and machine learning, plausible deniability doesn't work. Typically when I talk about this, someone comes up to me and says, "What if I tell the police, 'Hey, you can't prove it's me!'" That is naivete, insufficient for the real world. The algorithms being deployed don't care about plausible deniability; they operate on probabilities. And when the probability is high enough, that holds up for law enforcement purposes as much as advertising.

Blockchain privacy is not intuitive. Typically people tend to think of passive third-party observers as the main threat. But it's crucial to consider active attackers who can send payments to you, receive payments from you, and interact with third parties. Obvious examples of such attacks are merchants or cartels of merchants who keep track of customers, people who try to identify a payment recipient's real identity, and exchanges that also want to track you. (I'll address these scenarios momentarily.)

The range of supposed solutions to privacy problems is huge, so I won't review all of them individually. However, we can look at the approaches broadly in terms of three different kinds of systems.

First, some systems look like vanilla Bitcoin, where you explicitly identify the origin of your payment. The only protection here is that there are no real names.The base layer doesn't even attempt to obfuscate transaction data, which is now widely understood in cryptocurrency circles. (The general public could still use education on the issue.) Another approach is what I'm going to call decoy-based systems, where you hide what's going on in a given transaction by selecting a certain number of possible payment origins. The strongest approaches are Zerocoin and Zerocash, where no origin at all is identified.

In decoy-based systems — CoinJoin, Monero's RingCT, and others — you are required to explicitly verify the source of your funds, but you try to hide it by including a handful of decoys that aren't your real source. Theoretically, anyone looking at the transaction cannot tell which is which. The actual origin is obfuscated by adding noise.

And again, in systems using the principles of Zerocash, you don't have any identifiers whatsoever.

My position is that we haven't properly examined the downsides of decoy-based systems. It is a significant oversight, because much of the cryptocurrency community is turning to decoys as a source of scalable privacy. Decoy-based systems do not provide the robust, attack-resistant privacy that people assume.

Decoy-Based Deanonymization

Let's say that you're sending a decoy-obfuscated transaction. The protocol identifies the possible source of the funds, along with a handful of decoys. Now an observer or attacker has access to a tree of possibly associated payments that go back in history. They can't pinpoint quite what happened, since it's like a fuzzy family tree, but they can extrapolate some notion of what's going on based on this single transaction. That family tree — what I will call a taint tree — also works going forward.

Overseer Attack

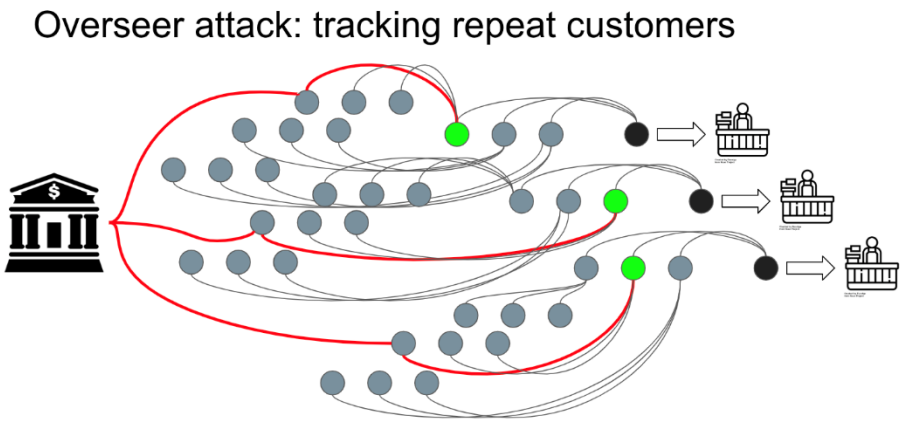
Let's say that your transaction was a payment to a merchant. Where does the money go next? Attackers cannot know precisely because of the systemic use of decoys. But they will be able to trace a finite number of possibilities in terms of where the money might have gone. Next, they can start a process of elimination.

The taint tree gives an attacker a lot of power, especially when tracking analysis is repeated over multiple transactions. One thing you can do if you're a merchant, or a set of colluding merchants, is track customers across repeated payments.

Hypothetically, I'm going into Target on a daily basis and making cash purchases. There should be no way of tracing me — beyond arduous methods like dusting for fingerprints or DNA, which requires already having those biometrics, or knowing in advance the serial numbers of the bills I'm going to use.

What if I start using a cryptocurrency to buy things at Target? (No, large retailers don't accept cryptocurrencies yet, but that's the endgame of these technologies.) Ideally I could make three separate purchases and there would be no way to link them together. A cryptocurrency with true privacy would achieve that.

If you look at decoy-based systems superficially, it seems like that do achieve that. None of these transactions appear to be linked together:



It gets worse. Again, let's consider multiple payments that I've made to one merchant. I don't want them to know that I'm the same person, but in a decoy-based system you have taint trees of possible ancestors. Well, what happens if they have a common origin? I went to Coinbase or whatever exchange, and I bought a bunch of cryptocurrency, then I loaded it onto the blockchain.

There's going to be one source of those funds. If you trace back the taint trees, you can look at the intersections and pinpoint the person making these transaction. That method works not just for one merchant, but also for groups of merchants — or other entities that receive payments. They can collude to figure out who you are, which is a problem when the goal is privacy.

Flashlight Attack

Let's suppose I want to accept payments online, anonymously. For example, I'm a dissident in an authoritarian country who needs to accept donations, but I cannot reveal my real identity; my life is at risk in the country where I do my activism. But I need to be able to fund my work. Of course, the government of that locale is trying to identify me. They have intel agencies and secret police at their disposal.

If I'm using a privacy-preserving cryptocurrency, it should be safe for me to deposit the donated funds at a local exchange. Even if that exchange is controlled by the government! Ideally the data that could be used to identify me — probabilistically or otherwise — is simply not available. I should be safe regardless of whether the exchange is hacked, corrupt, subpoenaed or otherwise infiltrated. What I'm describing is how it *should* work, not how it actually works.

If the government wants to identify me, they have my cryptocurrency addresses because I've exposed them in order to accept donations. Maybe my website is only accessible over Tor; maybe I even use a unique address per donation. And of course I'm relying on a decoy-based cryptocurrency.

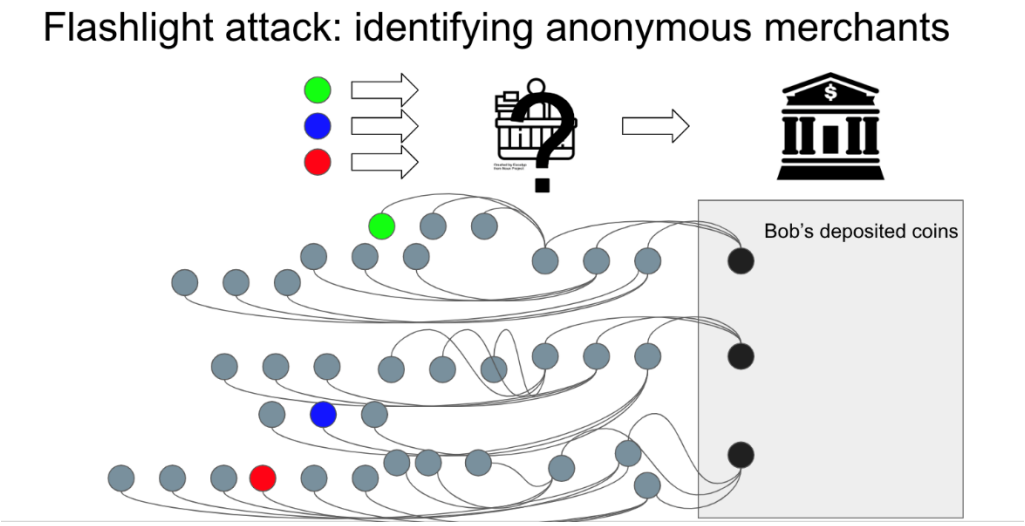
The government realizes that they can send tracking payments to an address of mine. Three of them, perhaps, or 20, or 100. The payments can be very small; size is irrelevant. At some point I'm going to deposit the funds from those payments.

Now I've got a big problem. Anybody who can access the exchange's records is now able to test whether the depositor is the same person as the democracy activist. They can examine the set of coins that I've deposited and reconstruct the taint tree, the possible sets of origins.

For any random person, it would be unremarkable that their deposits involved tainted payments. Decoys are picked at random, so by happenstance, one of the tainted payments could make its way into their deposits. On the other hand, the probability of that happening multiple times is quite low. It's vanishingly unlikely to happen with all of the funds from 100 tainted payments that were sent to this one democracy activist.

The government can look through all of my deposits, and see that my taint tree contains all of the tracking payments that they sent. That evidence links my legal identity to my democracy activism with overwhelming probability.

As you can see, taint trees are viable for deanonymization, and thus decoy-based systems violate people's notions of how privacy should (or does) work in cryptocurrencies. Taint trees allow privacy to be ripped apart in a way that would shock and concern many users.



This is probably the easiest to execute and most immediately troubling attack on decoy based systems.

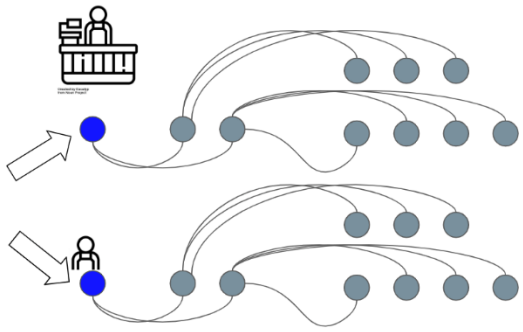
The takeaway is that repeated interactions with a malicious sender or recipient are dangerous. But it keeps getting worse!

Tainted Dust Attack

Remember when I mentioned that taint trees can be used to trace money going forward? After you make a payment, there's an uncertain cloud of possible transactions that could involve those funds. That can also be abused. For example, an attacker could find out where a friend — or family member, or ex-lover, or anyone else they know a bit about — is spending their money.

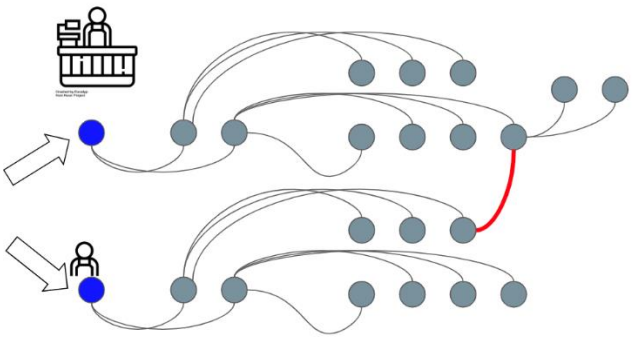
Let's say the attacker makes a small payment. It could even be a dust transaction. They make a payment to some merchant, and then to their victim. They keep watching as the taint tree grows out, as possible spends happen.

Tainted dust attack: seeing where money is spent



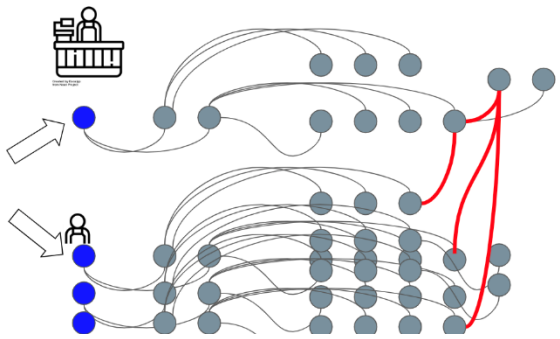
At some point, there's an interesting crossover. The attacker notices a transaction that seems to involve both the funds they sent to the merchant and the funds they sent to their victim.

Tainted dust attack: seeing where money is spent



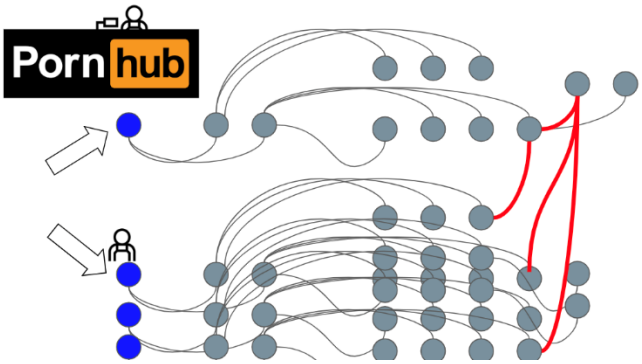
Many plausible explanations exist. The crossover could result from random decoys. Or perhaps the victim who received the attacker's transaction was spending money with the merchant in question. What the attacker now sees is the merchant moving funds out of a hot wallet, or spending them to pay bills, or whatever else. Again, any one instance is not definitive. But if the pattern repeats several times, then you have strong probabilistic evidence that your friend is making recurring payments to this merchant.

Tainted dust attack: seeing where money is spent



Law enforcement could use an analysis along these lines to validate that a particular person does indeed use a particular supplier. Or you could identify that your friend makes purchases on Pornhub. Which would be incredibly embarrassing for them, not because they're paying for porn, but because they're probably doing it using Verge.

Tainted dust attack: seeing where money is spent

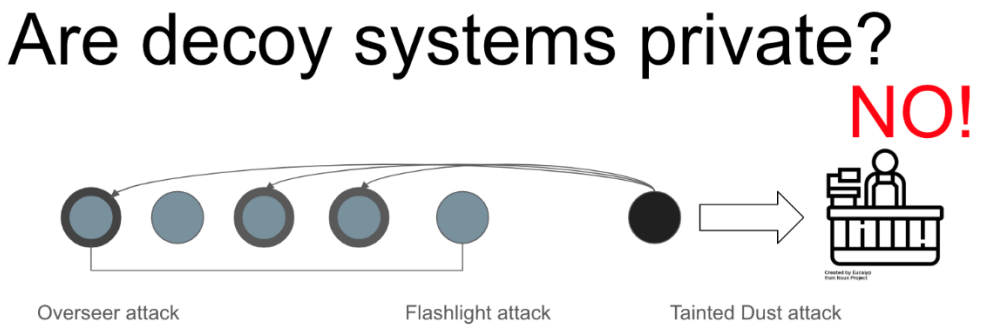


In summary, the limitations of decoy-based privacy systems are readily apparent once you threat model how attackers might approach them. You must consider what people can actively do, what they can't, and what goals they're likely to have. Various privacy proposals need this kind of rigorous evaluation or they can't be expected to stand up against clever adversaries (especially well-resourced ones). Cryptocurrency designers have to ask themselves, "If I were going to identify someone via this system, how would I go about it?"

The democracy activist taking donations over Tor might think, "I'm safe, I'm behind seven proxies!" But with a decoy-based system that isn't true. The moment someone can start

sending you tracking payments, and then get data from an exchange, you lose any and all privacy.

Solving Decoy Problems



The common perception of these various techniques seems to be, "Well, Bitcoin may not be private, but anything above-and-beyond Bitcoin will add meaningful privacy." The reality is that specific techniques and implementations matter. The details are crucial. Users need to understand the tradeoffs afforded by the specific system they're using. Buying modafinil has a different threat model from protesting an authoritarian regime.

I'm not saying that it's impossible for decoy-based systems to provide meaningful privacy. If your decoy set is very large — think five million possible origins to identify, rather than five — that changes the probabilistic evidence that attackers can uncover. On top of that, the decoy sets would have to substantially overlap across all recent transactions. Otherwise you will still see repeated common origins when making multiple purchases with a merchant and so on.

Finally, it's important to sample the decoys carefully. I won't go into it here, but a couple of papers have shown that the distribution from which Monero sampled their decoys didn't line up with the distribution of people's transactions. There was a gap. In previous versions of Monero — this is now somewhat fixed — the last transaction in the decoy set was actually the real transaction, with overwhelming probability, because of recency preferences.

Most decoy-based systems are intended to be practical. In order to get substantial decoy sets, you can't have systems that scale linearly in the number of decoys. Using Monero and bulletproofs as an example, each additional decoy costs you 1-2 kilobytes in transaction size. It should be very clear, with linear scaling, that you're not going to have a

transaction with 100 decoys in it, or 500, or a thousand. Proof generation and verification scale equivalently, which ruins the practicality.

What you need is logarithmic size. The transaction size should be logarithmic in your decoy set, and transaction generation and verification time should be at least logarithmic if not constant.

Zero-Knowledge Approach

I'm a little biased, but in my view the solution is a Zerocash-style protocol. Transaction outputs are commitments to the value in the recipient address, and you generate a Merkle tree over some fraction of the UTXO set, whatever you can afford computationally. A zero-knowledge proof is used to show that the origin of your payment exists in the UTXO Merkle tree. It can be verified without revealing the UTXO in question. This is where the privacy comes from. That's the basic approach of Zerocash, where the entire UTXO set is included in the Merkle tree.

How do you make that scalable? You have to pick a zk-proof technology that you like, and by "like" I mean: You think the cryptography is secure, you think that the assumptions are warranted, and the setup properties work for whatever operational requirements you have. It might be SNARKs, or STARKs, or bulletproofs. After choosing a zk-proof, you can tinker with scalability.

The scheme and parameters have been selected, so now you turn to efficiency. Start benchmarking. As the Merkle tree gets longer the transactions are going to get bigger and the verification times are going to slow down if your not using QAP-based zk-SNARKs like in Zcash.. The goal is finding a depth where efficiency meets your performance requirements. Maybe it's d=32, which Zcash Sapling uses. Maybe d=4, maybe 8, it doesn't really matter. Whatever you do, your decoy set is now 2^d, which exceeds most decoy-based approaches.

I should briefly note that the state of the art for these techniques is improving. With respect to zk-SNARKs, it's gone from taking ~40 seconds to like two seconds to generate a transaction. Huge amounts of memory used to be required, in excess of three gigabytes, and now it's 40 megabytes. Similarly, bulletproofs keep getting faster and faster.

Conclusion

We need to deeply consider our approaches to privacy. Cryptocurrencies should be built with robust, attack-resistance solutions for protecting financial information. That may happen on-chain, but it's not a given. The current mantra is that privacy will be ensured off-chain. That's fine and I hope it works, but it doesn't absolve you from assessing the default weaknesses of your system. Merely because it's off-chain doesn't mean that information doesn't leak.

It's been interesting to observe the reactions to my talks at Scaling Bitcoin and Devcon. Some projects care giving their users accurate expectations. For example, the Grin project has written up the state of its privacy protections. That's exactly what cryptocurrency developers should do, and the document is excellent. Grin's team took a very conservative position, talking about the privacy that is available now — not hypotheticals or privacy theater. My only concern is that Grin underplays the risks with leaking the transaction graph (what they call "inputs and outputs linking"). But all in all, the "Grin Privacy Primer" is very good, and I wish more groups would strive for equivalent clarity.

Unfortunately, many others have responded with the exact kind of privacy theater that I featured in my talk. It is irresponsible to claim that CT, stealth addresses, or Dandelion provide comprehensive or perfect privacy. None of those technologies address the issues that I've raised. None of them stop the flashlight attack that would allow governments to identify someone's legal identity by interacting with a dark-web site that accepts payments. It is a major concern for some users today, but privacy theater distracts from the real risks.

Finally, a number of people have noted that some of the attacks I mentioned may be hard to mount in practice, because of noise and large volumes of transactions. For the tainted dust attack, that's absolutely true. But it's not true at all for the flashlight attack or the overseer attack.

In general, the attacks that I described are thought experiments. The goal is to make you realize that many systems aren't as private as people think they are, and to guide explorations of the practical levels of privacy. It may be the case that with enough traffic and sufficiently large decoy set, you get viable privacy. However, barring an analysis proving that, we have to think about which implementations pass a basic smell test. Moreover, my examples are the basic attacks that come up when thinking through real-world cryptocurrency usage. Adversaries are clever, creative, and diligent.

Remember, passive third parties are not the only attackers. That's not the main threat that people face with existing technologies on the internet today. It's being tracked by companies, or malicious ex-lovers, or oppressive governments. Also remember that attacks only get better. We are in the early days of cryptocurrency functioning and usage. Compared to the internet or other older systems, we have very little experience with building or protecting cryptocurrencies.

By all means, choose to prioritize scaling over privacy. That is a reasonable choice to make as developers and as a community. But when you do that, understand what you're giving up in terms of privacy, and be transparent about it. Don't pick any random approach and say, "It adds some privacy, ergo the thing is completely private." That's not true; adding some privacy doesn't make a protocol private in totality, and users will still be vulnerable.

It took, what, 20 years for us to understand how bad the privacy problems with the internet were? Progress has accelerated, but a couple of years will not be enough. Five years, or 10, maybe. It's important to lay the groundwork for privacy now.

Tweetstorm: Bitcoin as SoV

By Dan Held

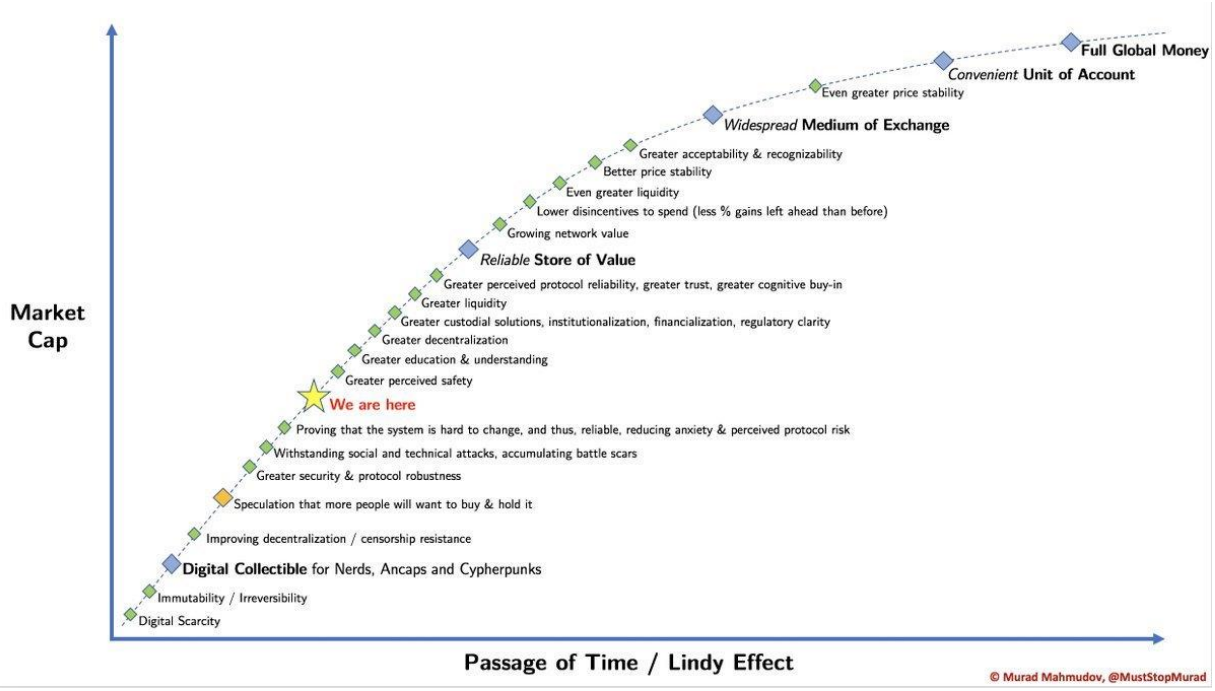
Posted January 14, 2019

1. Satoshi's Vision™ is a silly endeavor, as it doesn't matter what it was, we are where we are now. However, those pushing the "Bitcoin was first made for payments" narrative insist on cherry-picking sentences from the white paper and forum posts to champion their perspective.
2. The following tweetstorm is a categorical repudiation of this tired narrative. Bitcoin was purpose-built to first be a Store of Value (SoV), a thread:
3. How do we determine Satoshi's intention? We need to look at his ideology, description of functionality/architecture, timing, and audience. Let's start with how Satoshi describes the problem Bitcoin solves. In his first public comms after the whitepaper, in the first paragraph:
4. "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
5. He later expands on that Libertarian thought in his other writings:
   "[with Bitcoin] we can win a major battle in the arms race and gain a new territory of freedom for several years."—Satoshi Nakamoto
6. How does Satoshi describe Bitcoin? His forum posts provide insight through his consistent gold/metal analogy:
   "Bitcoin [is] more like a collectible or commodity." - Satoshi
7. *"In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases"* - Satoshi
8. *"As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties: [not useful/no utility]. And one special, magical property: can be transported over a communications channel"* - Satoshi
9. *"If there were nothing in the world with intrinsic value that could be used as money, only scarce but no intrinsic value, I think people would still take up something. (I'm using the word scarce here to only mean limited potential supply)"* - Satoshi
10. *"It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy."* - Satoshi
    Satoshi here clearly highlights that Bitcoin's scarcity gives it value… as a SoV. Limited supply is meaningless for VISA
11. So we now have an idea of Satoshi's motivations, and how he describes Bitcoin, but what does his timing tell us?
    Bitcoin's launch during the 08' financial crisis was not coincidental. Satoshi had been coding Bitcoin for the last 2 years. Let's look at the sequence of events

12. Jan - July: Fed tries to stop the housing bust: Fed bails out Bear Sterns. Paulson explains the need to bail out Fannie Mae, Freddie Mac the two agencies that held or guarantee 50% of the $12T in US mortgages.
13. Aug 18: Satoshi registers Bitcoin.org
    Sept 15: Lehman Brothers files for bankruptcy, the largest in U.S. history ($600B)
    Sept 17: Investors withdrew a record $144B from their money market accounts. During a typical week, only about $7B is withdrawn
14. Oct 3: Bitcoin whitepaper PDF likely created
    Oct 13: Treasury Secretary Paulson talks with 9 major bank CEOs. The total bailout package ~$2.25T
    Oct 21: Fed lends $540B to bail out money market funds
    Oct 31: Satoshi publishes the Bitcoin whitepaper
15. With the 2008 financial crisis, trust had been lost in a world that ran on trust. Bitcoin was launched in a time of absolute necessity, Satoshi planted the seed at precisely the right moment. The world didn't need a new VISA, they needed an alternative to banks.
16. So we now have an idea of Satoshi's motivations, how he describes Bitcoin, and his timing, what about this initial audience for the whitepaper? How did he market his message?
17. Satoshi crafted the whitepaper as a call to arms for his target audience: the Cypherpunks on the cryptography mailing list. Key components of their ideology are privacy and finality. His message needed to resonate with them as they would have to help him build it.
18. "Therefore, privacy in an open society requires anonymous transaction systems. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy." - A Cypherpunk's Manifesto
19. Many point to this in the whitepaper "peer-to-peer version of electronic cash would allow online payments" as proof that Satoshi meant for Bitcoin's main purpose is to disrupt VISA. However, "cash" represents a pseudonymous push payment in contrast to a credit-based system
20. Cash is a bearer asset. Let's look at the whitepaper with that in mind:
    "A purely peer-to-peer version of electronic [bearer assets] that would allow online payments to be sent directly from one party to another without going through a financial institution."
21. Note that the origin of the word "cash" is "caisse" (French) meaning money-box. So cash is by definition store-of-value. Other Cypherpunks had used the word cash in their whitepapers to reflect that functionality, like "HashCASH", "eCASH", etc"
22. In the other part of the whitepaper sentence the phrase "peer-to-peer" has been used as well against the SoV narrative. Charlie Lee has a great tweet storm that addresses this point of contention:
23. *"Bitcoin isn't "peer-to-peer." Payments are sent from sender to miners, who record it on a distributed ledger. The recipient receives the payment when it's recorded. BUT, this is facilitated by a p2p network where transactions are broadcasted."* @SatoshiLite

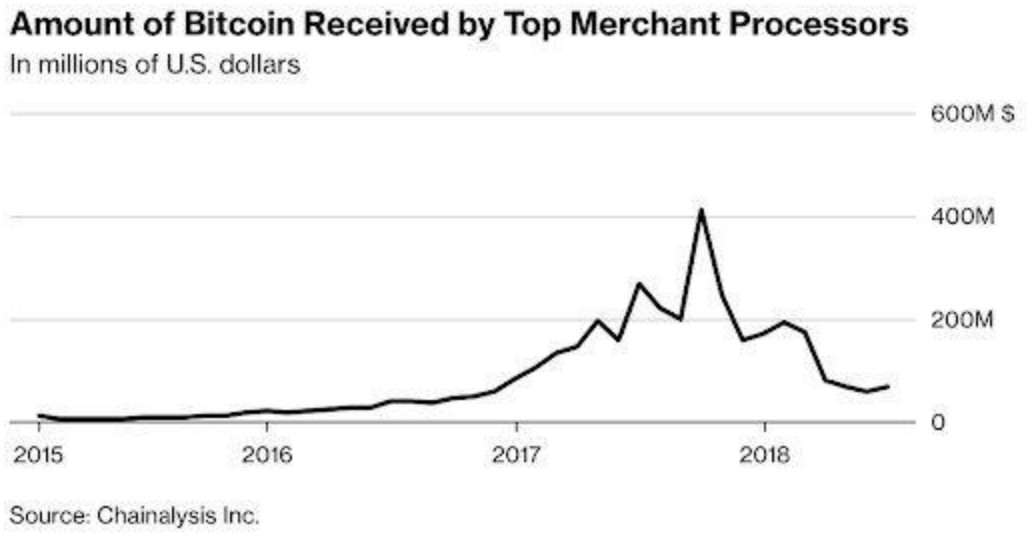
24. "*Lightning network payments, on the other hand, are p2p payments. They are sometimes direct p2p, sometimes indirect p2p. LN payments have to be sent from p2p to get from the sender to the recipient. Both have to be online, just like other p2p networks like BitTorrent"*
25. *"Bitcoin with Lightning Network more closely fits the Bitcoin whitepaper's title: "A Peer-to-Peer Electronic Cash System." This is Satoshi's Vision."* - @SatoshiLite
26. He wrote the paper to fit his target audience, but the source code implementation were his product specs. "If the Bitcoin Whitepaper is the Declaration of Independence, the Source Code is the Constitution" - @pierre_rochard
27. *"The functional details are not covered in the paper, but the sourcecode is coming soon."*— Satoshi Nakamoto
    Aka the whitepaper was marketing, the important details are coming.
28. In true Cypherpunk fashion, Satoshi's whitepaper was quickly followed by code release in January 2009. The notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list.
29. Just focusing on the whitepaper is a gross misinterpretation, here are the things not described in the whitepaper, but included in the source code or later defined by Satoshi: 21M hard cap, 10 minute blocks, 1 mb block caps.
30. If Satoshi wanted Bitcoin to first be used as a medium of exchange to purchase goods and services, he would have made it inflationary. People don't spend deflationary currencies when they can make the same purchase in infl. curr. There's even a name for It, Gresham's Law
31. Which is entirely intuitive. Why would any average consumer spend their Bitcoin with the perception that it will be worth more in the future when they can spend their fiat that they KNOW will be worth less?
32. So far that doesn't sound like he's trying to disrupt VISA now does it? And if that wasn't made perfectly clear, he permanently etched this message into the Genesis Block:
    "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"
33. To take it a step further, as a subtle jab to central banks, he chose his birthday as the date the US made gold ownership illegal through EO 6102 April 5th. He chose 1975 as his year of birth which is the year when the US citizens were allowed to own gold again
34. And finally, why did Satoshi choose to be anonymous if he were just disrupting payments?
    What he was trying to accomplish was clear, he wanted to build a new backbone for the financial system. Bitcoin isn't merely digital cash, but an alternative to banks.
35. And how does a new money get created? A new money comes into existence through stages: Collectible, SoV, MoE, and UoA.
    SoV and MoE aren't mutually exclusive. It's about where in the cycle of appreciation

we're in. At maturity, the payment use case finally makes sense.



36. Some may balk at the SoV terminology for Bitcoin since the price fluctuates. However, nothing in this life has a “stable” value, the longest running fiat currency, GBP, has lost 99% of its value since inception. Bitcoin has all the traits of a good SoV
37. Bitcoin is stable. The protocol has a 99.99989% uptime which is higher than USD. The “fluctuation” you see is the volatility of the world flowing into the stability of Bitcoin in ebbs and flows.
38. When applying “The Szaboian Theory of Money Origins” to Bitcoin, it is reasonable to conclude we just barely left the "collectible phase" and are now witnessing it's first steps into "Proto-money" @Willem_VdBergh @NickSzabo4
39. This phase, which is characterized by its primordial exploration of the SoV properties of the commodity, can easily take a decades to properly mature. Volatility is part of this maturing process.
40. People pushing the MoE narrative at this moment in time are counterproductive to adoption. By creating these expectations, which are unattainable at the moment, many people will get burned or disillusioned. This is a big loss for adoption and for

the affected individuals



41. *"Only by informing people correctly about the use case Bitcoin has *at this moment* can we maximize it's adoption and prevent a lot of people from making the biggest financial mistake of their life."* @Willem_VdBergh
42. So how did the payments narrative become a thing?
    A/ Satoshi used it to attract the cypherpunks
    B/ HODLing isn't good for business. In order to command higher valuations, startups latched onto narratives that VCs would fund. And in 2013-2016 that was "merchant processing."
43. Background on me: I was the first PM @Blockchain and @ChangeTip, both attempted to get people to use Bitcoin for payments. Consumers couldn't care less, which is entirely intuitive: right now it's not faster, cheaper, or easier to use for 99.99% of use cases.
44. After all of this do you really think Bitcoin was primarily built for payments at this stage in its lifecycle?
45. If you enjoyed this tweet storm, please sign up for an e-mail newsletter which will include more of my thoughts like these. (at a date far in the future when I have time)
46. Special thanks for the insight and inspiration:
    @real_vijay @nwoodfine @saifedean @NickSzabo4 @MustStopMurad @pierre_rochard @nic__carter @hugohanoi @MartyBent @francispouliot_ @TuurDemeester @arjunblj @jimmysong @hasufl @_prestwich @CremeDeLaCrypto @SatoshiLite @MrHodl

Planting Bitcoin—Species (1/4)

Sound Money (sanum pecuniam)

By Dan Held

Posted January 6, 2019

Foreword

I wrote this series, "Planting Bitcoin", to paint the origin story of Bitcoin leading up to the 10 year anniversary (10/31/2018). I felt that this story hadn't been told in a comprehensive and easy to read manner. I'd like to thank Jill Carlson for incepting this idea on the road trip back from Tahoe in early 2018.

Introduction

Bitcoin's origin is akin to planting a tree. It wasn't just Satoshi's selection of the species (code), but the season (timing), soil (distribution), and gardening (community) that were essential to its success. It had to grow to be strong, mighty, and huge. It had to survive droughts, storms, and predators. Its deep roots had to support the weight of becoming a new world reserve currency.

What is Money

Money is most easily defined as the medium in which value is transferred. But Money is not just paper in your hand; or numbers in your bank account, Money represents something much more fundamental:

- Money is a primitive form of memory or record-keeping. It is the collective memory of who has the ability to allocate wealth.
- Money, which is the representation of the work required to acquire goods and services, can also be viewed as stored energy.
- Money is the central information utility of the world economy. As a medium of exchange, store of value, and unit of account, money is the critical vessel of information about the conditions of markets.

The main functions of money are Store of Value (SoV), Medium of Exchange (MoE), and Unit of Account (UoA). No money starts by providing all three functions, each new species of money follows a distinct evolutionary path that we will cover later. Let's first start by identifying the newest species of money, Bitcoin.

Species

"These protocols can't be described comprehensively as static objective things. They're best thought of as live systems"—Ari Paul

Bitcoin is a new form of life, a new species of money called "cryptocurrency." More importantly, it is "sound money," or using proper taxonomy, "sanum pecuniam." Sound money is defined as money that has a purchasing power determined by markets, independent of governments and political parties which is essential for individual freedom.

"I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper."—Satoshi Nakamoto

The code of life is written into an organism at its inception. Satoshi carefully architected Bitcoin's DNA, or genetic code, to be the best sound money ever created. We can think of Bitcoin's genetic code as representing instructions that have been written to incentivize the organization and coordination of cellular function.

"I believe I've worked through all those little details over the last year and a half while coding it, and there were a lot of them"- Satoshi Nakamoto

Bitcoin's genetic code:

- Satoshi needed a way for the Bitcoin to spark itself into existence, so he coded in its DNA a fixed supply (21M Bitcoins). An increase in Bitcoin's price inevitably leads to a corresponding increase in participants (users), security (mining), and developers. This becomes a self-reinforcing feedback loop.
- Bitcoin's mining function, Proof of Work (PoW) is both its metabolism and defense mechanism. Bitcoin eats energy to generate new coins and build digital walls to protect the network. PoW also makes Bitcoin anti-fragile, or in other words, as it grows larger, it becomes more resistant to attack.
- A new Bitcoin block is found every 10 minutes, this genetic code enables Bitcoin's cells to effectively communicate and coordinate with each other despite enormous distances. It is the internal clock that sets the metabolic rate.

"It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because it is radically transparent: anyone can see its code and see exactly what it does. It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. It can't even be interrupted. If nuclear war destroyed half of our planet, it would continue to live, uncorrupted."—Ralph Merkle

Bitcoin's genetic code manifests itself via traits (characteristics of an organism) that may or may not be visible.

Traits

In biology, a trait or character is a feature of an organism. According to Charles Darwin's theory of evolution by natural selection, organisms that possess heritable traits that enable them to better adapt to their environment compared with other members of their species will be more likely to survive, reproduce, and pass more of their genes on to the next generation.

Money is no different. Money has traits that enable it to survive and thrive as a Store of Value (SoV), Medium of Exchange (MoE), and Unit of Account (UoA). Bitcoin is a new species that has vastly superior traits to its predecessors. Below we dive deeper into those traits between different species of money.

Traits of Money	Bitcoin	Gold	Fiat
Verifiable	High	Moderate	Moderate
Fungible	High	High	High
Portable	High	Low	High
Durable	Moderate	High	Low
Divisible	High	Low	Moderate
Scarce	High	Moderate	Low
Established History	Low	High	Low
Censorship resistant	High	Moderate	Low
Unforgeable Costliness	High	High	Low
***Openly Programmable**	High	Low	Low
***Decentralized**	High	Moderate	Low

**Bitcoin's birth introduced two new traits, "Openly programmable" and "Decentralized"*

(The sections below, on the attributes that make for a sound money, are largely borrowed from Vijay Boyapati's article "The Bullish Case for Bitcoin")

Verifiable

Fiat currencies and gold are fairly easy to verify for authenticity. However, despite providing features on their banknotes to prevent counterfeiting, nation-states and their

citizens still face the potential to be duped by counterfeit bills. Gold is also not immune from being counterfeited. Sophisticated criminals have used gold-plated tungsten as a way of fooling gold investors into paying for false gold. Bitcoins, on the other hand, can be verified with absolute mathematical certainty.

Fungible

Gold provides the standard for fungibility. When melted down, an ounce of gold is nearly indistinguishable from any other ounce. Fiat currencies, on the other hand, are only as fungible as the issuing institutions allow them to be. While it may be the case that a fiat banknote is usually treated like any other by merchants accepting them, there are instances where large-denomination notes have been treated differently to small ones. For instance, India's government, in an attempt to stamp out India's untaxed gray market, completely demonetized their 500 and 1000 rupee banknotes. Bitcoins are fungible at the network level, meaning that every bitcoin, when transmitted, is treated the same on the Bitcoin network. However, because bitcoins are traceable on the blockchain, a particular bitcoin may become tainted by its use in illicit trade and merchants or exchanges may be compelled not to accept such tainted bitcoins. Despite this, there is no alternative pricing for "tainted Bitcoins" so it remains highly fungible.

Portable

Bitcoins are the most portable store of value ever used by man. A single USB stick can contain a billion dollars, easily carried anywhere, transmitted near instantly. Fiat currencies, being fundamentally digital, are also highly portable. However, governments can control the free flow of capital. Cash can be used to avoid capital controls, but then the risk of storage and cost of transportation become significant. Gold, being physical in form and incredibly dense, is by far the least portable. When bullion is transferred between a buyer and a seller it is typically only the title to the gold that is transferred, not the physical bullion itself (It cost Germany $9.1 million to repatriate their gold).

Durable

Gold is the king of durability—the vast majority of gold that has ever been mined or minted, including the gold of the Pharaohs, remains today and will for near eternity (it can only be destroyed through nuclear transmutation). While fiat currency exists both in physical and digital forms, we will only consider the durability of its digital form… the durability of the institution that issues them. Many fiat issuing governments have come and gone over the centuries, and their currencies disappeared with them. If history is a guide, it would be folly to consider fiat currencies durable in the long term—the US dollar and British Pound are relative anomalies in this regard. Bitcoins, having no issuing authority, may be considered durable so long as the network that secures them remains in place. Given that Bitcoin is still in its infancy, it is too early to draw strong conclusions about its durability. However, there are encouraging signs that the network displays a remarkable degree of "anti-fragility."

Divisible

Bitcoins can be divided down to a hundred millionth of a bitcoin and transmitted at such infinitesimal amounts. Fiat currencies are typically divisible down to pocket change, which has little purchasing power, making fiat divisible enough in practice. Gold, while physically divisible, becomes difficult to use when divided into small enough quantities that it could be useful for lower-value day-to-day trade.

Scarce

The attribute that most clearly distinguishes Bitcoin from fiat currencies and gold is its predetermined absolute scarcity: only 21 million bitcoins can ever be created (the number of units is arbitrary, as Bitcoins can be subdivided into 210 quadrillion satoshis). This gives the owner of bitcoins a known percentage of the total possible supply. Gold, while remaining quite scarce through history, is not immune to increases in supply. If it were ever the case that a new method of mining or acquiring gold became economic, the supply of gold could rise dramatically (ex: sea-floor or asteroid mining). Finally, fiat currencies, while only a relatively recent invention of history, have proven to be prone to constant increases in supply. Nation-states have shown a persistent proclivity to inflate their money supply to solve short-term political problems.

Established history

No monetary good has a history as long and storied as gold, which has been valued for as long as human civilization has existed. Coins minted in the distant days of antiquity still maintain significant value today. The same cannot be said of fiat currencies, which are a relatively recent anomaly of history. From their inception, fiat currencies have had a near-universal tendency toward eventual worthlessness. The use of inflation as an insidious means of invisibly taxing a citizenry has been a temptation that no states in history have been able to resist. Bitcoin, despite its short existence, has weathered enough trials in the market that there is a high likelihood it will not vanish as a valued asset any time soon. Furthermore, the Lindy effect suggests that the longer Bitcoin remains in existence the greater society's confidence that it will continue to exist long into the future. The median age of a human is ~30 years old, which means Bitcoin has been around for nearly 33.3% of the average human life. If Bitcoin exists for 20 years, there will be near-universal confidence that it will be available forever, much as people believe the Internet is a permanent feature of the modern world.

Censorship resistant

One of the most significant sources of early demand for bitcoins was their use in the illicit drug trade. Silk Road was a testament to this resistance. The key attribute that makes Bitcoin valuable for proscribed activities is that it is "permissionless" at the network level. When bitcoins are transmitted on the Bitcoin network, there is no human intervention deciding whether the transaction should be allowed. As a distributed peer-to-peer

network, Bitcoin is, by its very nature, designed to be censorship-resistant. This is in stark contrast to the fiat banking system, where states regulate banks and the other gatekeepers of money transmission to report and prevent outlawed uses of monetary goods. A classic example of regulated money transmission is capital controls. A wealthy millionaire, for instance, may find it very hard to transfer their wealth to a new domicile if they wish to flee an oppressive regime (Russian assets in the UK being frozen). Although gold is not issued by states, its physical nature makes it difficult to transmit at distance, making it far more susceptible to state regulation than Bitcoin. India's Gold Control Act is an example of such regulation. If your mission is to disrupt central banks, you need to have sovereign level censorship resistance.

> *"Bitcoin's advantages lie not in its speed, convenience, or friendly user experience. Bitcoin's value comes from it having an immutable monetary policy precisely because nobody can easily change it"—Saifedean Ammous*

Unforgeable Costliness

Money that is costly to create. Due either to its original cost (gold mining) or the improbability of its history (art)—and that it is difficult to fake this costliness. Bitcoin's PoW ensures the cost to mine a Bitcoin is near equivalent to how much it would cost to purchase one on an exchange. The unforgeable costliness pattern includes the following basic steps:

> *"(1) find or create a class of objects that is highly improbable, takes much effort to make, or both,* and *such that the measure of their costliness can be verified by other parties.*
>
> *(2) use the objects to enable a protocol or institution to cross trust boundaries"*
> *- Nick Szabo*

Openly Programmable

Bitcoin is open-source; its design is public, it is usable by anyone/anywhere/anytime. Developers can freely program applications on top of the Bitcoin protocol without having to ask anyone for permission.

> *"It is dynamic, upgradable and extendable. It does not need throwing out and replacing with each new iteration, it will continuously improve."—Neil Woodfine*

Decentralized

In it's simplest definition, decentralization means a lack of centralized control. Or the degree to which an entity within the system can resist coercion and still function as part of the system. Coercion doesn't necessarily mean force, it means negative incentives to align with an authority. Decentralization is an important trait for money because any centralized

control could threaten any one of the other traits (especially scarcity and censorship resistance)

Decentralization is also important because it enables greater social scalability. The challenge is that natural systems inherently evolve towards centralization (hierarchies). We see this emergent property in cryptocurrencies as well. Hierarchy is an emergent property of networks. When we consider more complex systems, we must contend with more complex relationships between the layers. Quantifying decentralization is an especially thorny issue.

Decentralization is such a misunderstood concept, because people apply it to a whole system, when really it needs to be applied to multiple layers within the system: The Protocol, The Politics and The Practical. — Sarah Lewis

Evolution

For a species of money to survive, it needs to be competitive on every attribute and be exceptionally better on a few of them. Attributes don't sum, they multiply.

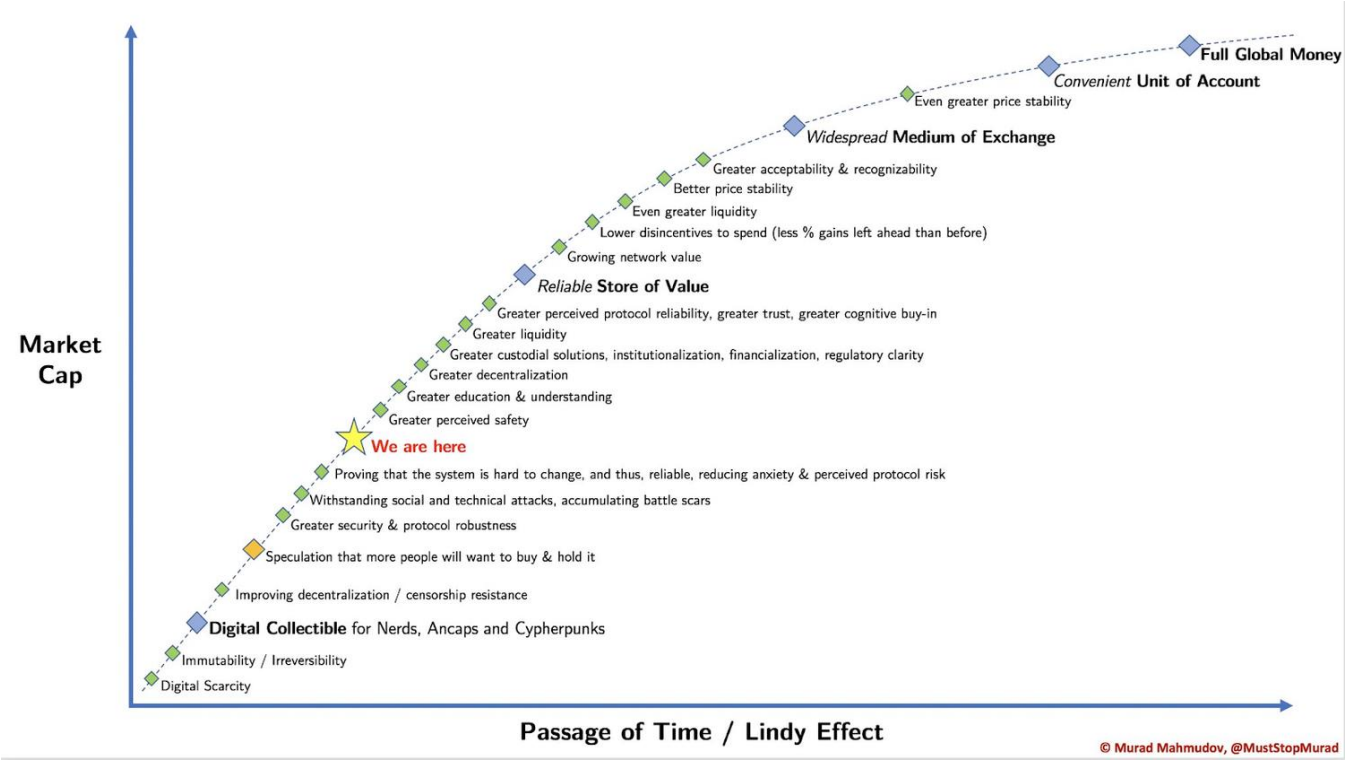
When Gold was first introduced, the bead makers (an example of a more primitive form of money) probably tried to convince the ignorant population that gold was no substitute for beads. But it turned out that gold had traits that were more advantageous. It did not matter what anyone thought. Gold was destined to be a more powerful currency than shells or beads.

The fact that gold has remained a valued commodity for thousands of years speaks to the importance of these specific traits. In fact, the combination of traits possessed by gold and other precious metals eventually provided the foundation for the next evolution in money, fiat currency. In money's next evolution of species, fiat currency fulfilled several critical traits to an even greater degree than gold. Paper was more portable and could be more easily transacted. That is not to say it was entirely superior. In many cases, fiat currencies lacked durability, and as we will see, would eventually become less and less scarce (due to inflation) The critical flaw: its supply was controlled by kings and governments and increasingly used as a tool to wield power and control. Upon every new iteration of species, they each evolve in the following four stages (taken from "The Bullish Case for Bitcoin"):

1. **Collectible**. In the very first stage of its evolution, money will be demanded solely based on its peculiar properties, usually becoming a whimsy of its possessor. Shells, beads and gold were all collectibles before later transitioning to the more familiar roles of money.
2. **Store of value**: Once it is demanded by enough people for its peculiarities, money will be recognized as a means of keeping and storing value over time. As a good becomes more widely recognized as a suitable store of value, its purchasing power will rise as more people demand it for this purpose. The purchasing power of a store

of value will eventually plateau when it is widely held and the influx of new people desiring it as a store of value dwindles.

3. **Medium of exchange**: When money is fully established as a store of value, its purchasing power will stabilize. Having stabilized in purchasing power, the opportunity cost of using money to complete trades will diminish to a level where it is suitable for use as a medium of exchange.
4. **Unit of account**. When money is widely used as a medium of exchange, goods will be priced in terms of it. I.e., the exchange ratio against money will be available for most goods.



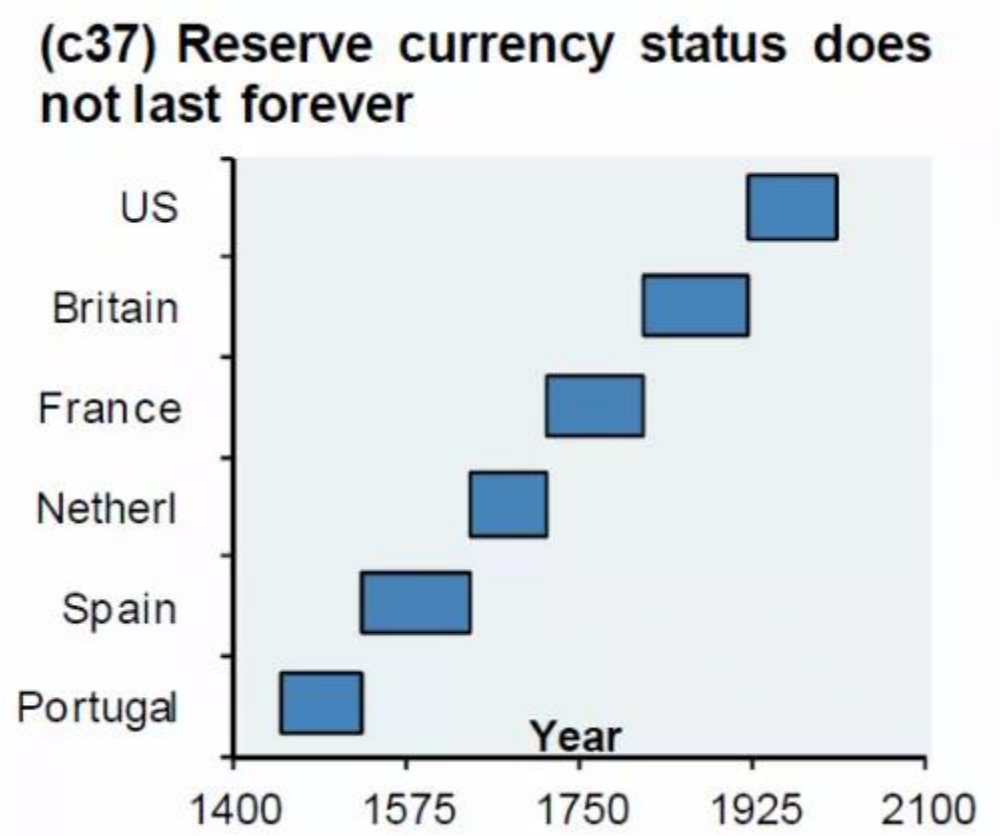
Bitcoin's stage in the evolutionary process is shown below, provided by Murad Mahmudov

Survival and Extinction

Extinction can most simply be described as the failure of a species to compete in an environment to such at a degree that it eventually ceases to exist. The inability to compete itself may be the result of two primary causes; increased competition from superior species or a dramatic change in environment.

"Charles Darwin's theory of natural selection originated to provide an evidence-based explanation of the past. We now leverage this theory to look forward and understand its implications on the future of currency. Given the ever-changing conditions of the future, will gold and fiat currencies continue to compete or go the way of the dinosaur?" —Ryan Walker "On the Origins of Money: Darwin and the Evolution of Cryptocurrency"

According to a study of 775 fiat currencies by DollarDaze.org the average life expectancy of a fiat currency is 27 years. The study also indicated the most common causes of any given currencies extinction are hyperinflation, monetary reform, war and independence. Looking towards the fittest of fiat currencies, those that become reserve currencies, we find that most last just under 100 years. (Note: US currency only starts from 1933 because USD was redeemable for gold prior to that)



JPM, Hong Kong Monetary Authority, December 2011

With fiat currencies being so susceptible to failure, gold has long served as an alternative as it is more scarce and durable. In terms of scarcity, fiat currencies can be printed and inflated at the will of their authorities.

"While Bitcoin is a new invention of the digital age, the problems it purports to solve—namely, providing a form of money that is under the full command of its owner and likely to hold its value in the long run—are as old as human society itself"—Saifedean Ammous

The currencies are in a state of hyper-evolution as they continue to take on a varied array of distinctive traits that set them apart from one another within their own competitive ecosystem (fiat/crypto).

Equally as threatening to traditional forms of money, the conditions of the environment in which currencies compete is in a constant state of change. Undertones of growing distrust in centralized entities encourage populations to consider alternative stores of value.

Sovereignty, once a trait that was necessary for the survival of a currency, may now be falling out of favor. Centralized failures such as the US financial crisis of 2008 or hyper-inflated fiat currencies such as Zimbabwe dollars or Argentinian pesos compound these sentiments. The most profound of these conditions is the growing awareness throughout the world that decentralized trust is possible.

Instead of becoming anti-fragile, which is the property of growing stronger in a volatile and stressful environment, central banks have removed danger and mortality from failure, which causes competition to stagnate or degrade.

Sometimes stressors are so strong that they are fatal for a species of money. While this is devastating for the money itself, the population comprised of those that survive are fitter on average. This isn't because any of the survivors grew stronger from the stress, but simply because the weaker monies were removed.

"We humans regularly underestimate high-impact, long-tail events. Careful consideration of long tail events is especially important in the design of a protocol that has the potential to become the backbone of the global economy" —Hugo Nguyen

It is interesting to imagine what Charles Darwin would make of the current state of money. History would have us believe that the existence and survival of any entity, be it plant, animal, corporation, or money is subject to the laws of natural selection.

With this understanding, it is hard to imagine Darwin contesting the opinion that Bitcoin possesses the necessary traits to become the dominant species of money.

Bitcoin has been perfectly honed for its environment through its exceptional genetic code and the manifestation of that code in the form of superior traits.

Bitcoin is the apex predator of money and is constantly evolving. None of the previous monetary life forms stand a chance.

Links

- http://pricesandmarkets.org/wp-content/uploads/2015/02/Luther-Olson-4.pdf
- https://blog.picks.co/pow-is-efficient-aa3d442754d3
- https://twitter.com/AriDavidPaul/status/1053007190552956928
- http://www.aei.org/publication/sound-money-vs-stable-money/
- https://satoshi.nakamotoinstitute.org/emails/cryptography/6/#selection-209.0-221.16
- https://satoshi.nakamotoinstitute.org/emails/cryptography/15/#selection-111.0-113.67
- http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562

- https://grisha.org/blog/2018/01/23/explaining-proof-of-work/
- https://mobile.twitter.com/SauceryCoin/status/1049184561974800384
- https://medium.com/u/9efdc740067f
- https://medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1
- http://www.cbc.ca/beta/news/canada/ottawa/fake-gold-wafer-rbc-canadian-mint-1.4368801
- https://en.wikipedia.org/wiki/Gold_fingerprinting
- https://www.dw.com/en/germany-repatriates-gold-reserves-ahead-of-schedule/a-40208045
- https://en.wikipedia.org/wiki/Antifragility
- https://news.nationalgeographic.com/2016/07/deep-sea-mining-five-facts/
- http://web.mit.edu/12.000/www/m2016/finalwebsite/solutions/asteroids.html
- https://en.wikipedia.org/wiki/Hoxne_Hoard
- https://en.wikipedia.org/wiki/Lindy_effect
- http://www.worldometers.info/world-population/
- https://en.wikipedia.org/wiki/The_Gold_%28Control%29_Act,_1968
- https://medium.com/u/becf6824fd89
- http://unenumerated.blogspot.com/2008/08/
- https://twitter.com/nwoodfine/status/981435332506906626
- https://inflationdata.com/Inflation/Inflation/Cumulative_Inflation_by_Decade.asp
- https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/sanctions-solutions/sanctions-screening
- http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html
- https://journals.plos.org/ploscompbiol/article/file?id=10.1371/journal.pcbi.1004829&type=printable
- https://twitter.com/SarahJamieLewis/status/1029217138601418753
- https://twitter.com/coindesk/status/1048786254245126144
- https://medium.com/u/e1c7b66721d6
- https://www.coindesk.com/origins-money-darwin-evolution-cryptocurrency/
- http://dollardaze.org/
- https://en.wikipedia.org/wiki/Long_tail
- https://medium.com/u/3efc6d31e61c

Planting Bitcoin - Season (2/4)

Central Banks and the 2008 Financial Crisis

By Dan Held

Posted January 6, 2019

> *"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. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."—Satoshi Nakamoto*

Introduction

In my last article, "Species," I covered why Satoshi's design of Bitcoin's genetic code made it the best species of money ever created.

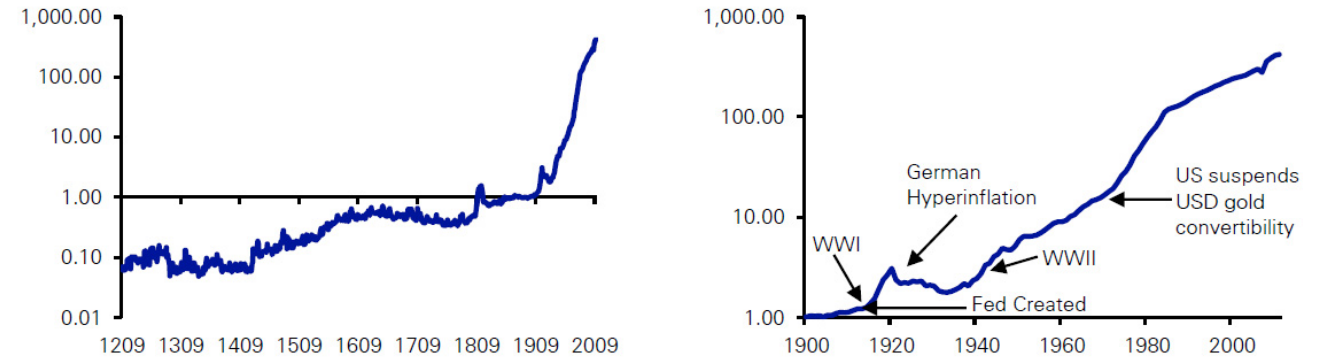
Satoshi had begun crafting Bitcoin's genetic code in 2007 but had waited for the right moment to plant the seed, the right moment in which the world would understand and embrace what he had created. In this article, I will dive into the moment in which Satoshi precisely chose to plant the Bitcoin seed.

Central Banks

From the founding of the Bank of England, central banks have been used as a means for states to fund their policies without risking the popular ire caused by direct taxation. When the capital provided by central banks is misallocated by either the state or in a market distorted by artificially low interest rates, an inevitable collapse occurs. The central bank is the root of these periodic market dislocations.

> *"I believe the root cause of every financial crisis, the root cause, is flawed government policies"—Henry Paulson (US Treasury Secretary during the 2008 financial crisis and former Goldman Sachs CEO)*

Figure 18: Global Median Inflation Series since 1209 (left) and 1900 (right)

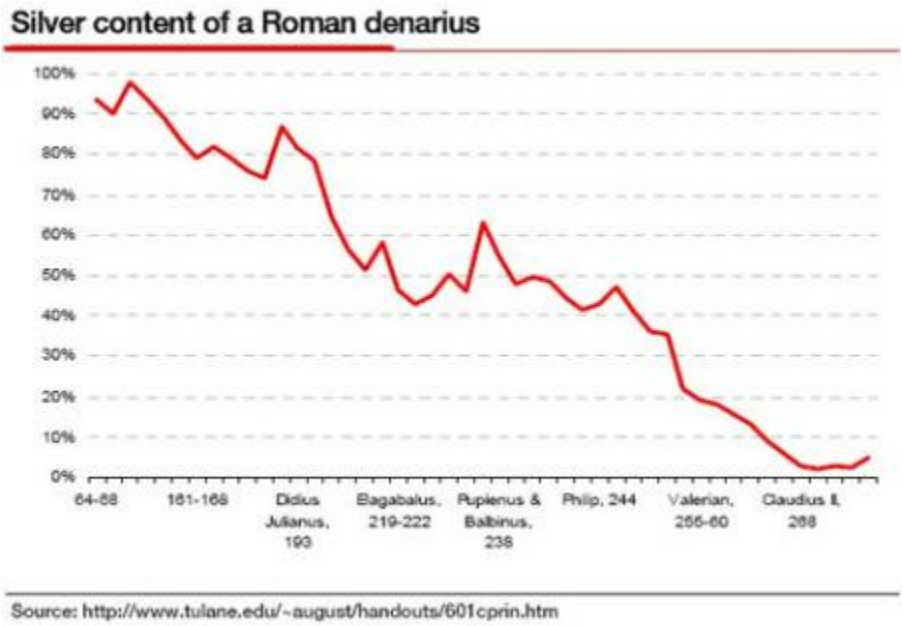


Source: Deutsche Bank, GFD

(There hasn't been a year of global deflation since 1933)

With the recent market dislocation, investors were bailed out. Unfortunately, you cannot subsidize irresponsibility and expect people to become more responsible. Prior to the 20th century, ordinary people could always flee to gold to save themselves from the effects of the failed, inflationist, policies of the central bank. This ended across much of the world in the 20th century as gold was outlawed. — Vijay Boyapati

"In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. There is no safe store of value." — Alan Greenspan
(Former Chairman of the Federal Reserve)



The standard Roman silver coin

Early 2007

Satoshi Nakamoto, after years and years of research, starts coding up Bitcoin.

2008 Financial Crisis

"The problem had grown so big that the end was bound to be cataclysmic and have big social and political consequences"—Michael Lewis (Big Short)

January

Fed tries to stop the housing bust

The Federal Market Open Committee began lowering the fed funds rate (to 3.0%). There were 57 percent more foreclosures than 12 months earlier

February

Bush signs tax rebate as home sales continue to plummet

February 13: President Bush signed a tax rebate bill to help the struggling housing market. The bill increased limits for FHA loans and allowed Freddie Mac to repurchase jumbo loans.

March

Fed begins bailouts

March 14: The Federal Reserve held its first emergency weekend meeting in 30 years.

March 17: The Federal Reserve announced it would guarantee Bear Stearns' bad loans.

March 18: The Federal Open Market Committee lowered the fed funds rate by 0.75 percent to 2.25 percent. It had halved the interest rate in six months. That same day, federal regulators agreed to let Fannie Mae and Freddie Mac take on another $200 billion in subprime mortgage debt.

April—June

The Fed buys more toxic bank debt

June 2: The Fed auctions totaled $1.2 trillion. In June, the Federal Reserve lent $225 billion through its Term Auction Facility.

July

IndyMac bank fails

July 11: The Office of Thrift Supervision closed IndyMac Bank. Los Angeles police warned angry IndyMac depositors to remain calm while they waited in line to withdraw funds from the failed bank.

July 23: Secretary Paulson made the Sunday talk show rounds. He explained the need for a bailout of Fannie Mae and Freddie Mac. The two agencies themselves held or guaranteed more than half of the $12 trillion of the nation's mortgages.

August

August 18: Satoshi registers Bitcoin.org through anonymousspeech.com

September *Global panic*

September 7: Treasury nationalizes Fannie and Freddie and will run the two until they are strong enough to return to independent management. The Fannie and Freddie bailout initially cost taxpayers $187 billion.

September 15: Lehman Brothers files for chapter 11 bankruptcy, the largest bankruptcy filing in U.S. history with over $600B in assets. The bankruptcy triggered a one-day drop in the Dow Jones Industrial Average of 4.5%, the largest decline since the September 11, 2001 attacks. Later that day, Bank of America officially announced it would purchase struggling Merrill Lynch for $50 billion.

> *"It's terrible. Death. Like a massive earthquake."—Kirsty McCluskey a Lehman trader in London*

September 16: Fed buys AIG for $85 Billion. The company had insured trillions of dollars of mortgages throughout the world. If it had fallen, so would the global banking system. On that same day, the Reserve Primary Fund "broke the buck." It didn't have enough cash on hand to pay out all the redemptions that were occurring.

> *"I asked my wife to please go to the ATM and take as much cash as she could. When she asked why, I said it was because I didn't know whether there was a chance that banks might not open."—Mohamed El-Erian (One of the most powerful economists/leaders in finance)*

September 17: Economy on the brink of collapse. Panic spreads. Investors withdrew a record $144.5 billion from their money market accounts. During a typical week, only about $7 billion is withdrawn. If it had continued, businesses couldn't get money to fund their day-to-day operations. In just a few weeks, shippers wouldn't have had the cash to deliver food to grocery stores.

October *Bailouts*

October 3: Bitcoin whitepaper PDF likely created (not the first time it was written, but the first time it was prepared for publishing)

The same day, the bank bailout bill allowed Treasury to buy shares of troubled banks. It was the fastest way to inject capital into the frozen financial system. Despite this, global stock markets continue to collapse.

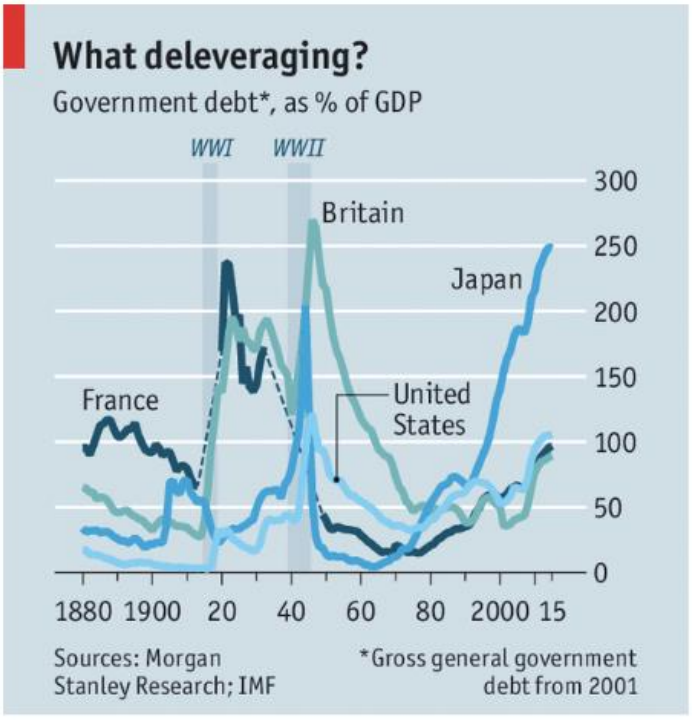
"Just as our politics are falling apart, our portfolios are falling apart, too."—Ben Hunt

October 7: The Federal Reserve agreed to issue short-term loans for businesses that couldn't get them elsewhere, to the tune of $1.7 Trillion.

October 13: Treasury Secretary Hank Paulson sits down with 9 major bank CEOs. The total bailout package looks more like $2.25 trillion, well more than the original $700 billion available.

"September and October of 2008 was the worst financial crisis in global history, including the Great Depression"—Ben Bernanke

October 14: The governments of the EU, Japan, and the United States again took unprecedented coordinated action. The EU committed to spending $1.8 trillion to guarantee bank financing, buy shares to prevent banks from failing, and take any other steps needed to get banks to lend to each other again. This was after the UK committed $88 billion to purchase shares in failing banks and $438 billion to guarantee loans. In a show of solidarity, the Bank of Japan agreed to lend unlimited dollars.



Debt/GDP ratios are at wartime highs. Central banks haven't unwound their 2008 trade

October 21—Fed lends $540 Billion to bail out money market funds which are continuing to meet a barrage of redemptions.

"People feel like nothing in the country is working—the president, Congress, corporations." (October 15, 2008) Reuters

October 31: **Satoshi publishes the Bitcoin whitepaper**

Walking on the street in a city Satoshi looks around and notices a businesswoman on her blackberry, hailing a cab. He passes a newspaper stand and sees Miley Cyrus' (known as Hannah Montana) controversial photos in Vanity Fair, she's 15.

George Bush's approval rating is at a record low of 21%, Congress is at 10%—just above its all-time low. Lehman Brothers had just collapsed a month prior.

> *"Is now the time? Is the world ready?" Satoshi thought to himself. He had spent the last few years coding up Bitcoin then writing the whitepaper. He had patiently waited to release it to the world, but the moment had to be right… there was only one shot at this. "Is the whitepaper easy enough to read? I want to make sure this resonates with the cypherpunks, I'm hoping* cash *will be most understandable to the other members on the mailing list who have previously created e-currencies."*

> *"When the moment is ripe, a fanatic leader galvanizes the ripe population and pushes it to a point of no return. The leader translates the ideals published by the "men of words [cypherpunks]" into doctrines [whitepaper] promising sudden and spectacular change."*—Eric Hoffer, author of "The True Believer" (via Tony Sheng)

He returned to his home and reviewed the whitepaper for any glaring mistakes the 47th time, he couldn't find any. He leaned back and stared at the wall. He realized this was the moment, it was time to plant the seed. He popped open his e-mail client, checked the draft e-mail to the cryptographer (cypherpunk) e-mailing list and pressed send. There was no going back.

> *"Indeed, Bitcoin rose like a phoenix from the ashes of the 2008 global financial catastrophe—a catastrophe that was precipitated by the policies of central banks like the Federal Reserve."—Vijay Boyapati*

With the 2008 financial crisis, trust had been lost in a world that ran on trust.

Bitcoin was launched in a time of absolute necessity, Satoshi planted the seed at precisely the right moment.

Links

- https://www.huffingtonpost.com/2013/08/27/hank-paulson-cause-of-financial-crisis_n_3822417.html
- https://mises.org/library/how-central-banking-increased-inequality
- https://medium.com/u/9efdc740067f
- https://en.wikipedia.org/wiki/Alan_Greenspan
- https://satoshi.nakamotoinstitute.org/emails/cryptography/15/
- http://www.realtor.org/rmodaily.nsf/pages/News2008022602
- https://www.thebalance.com/bush-economic-stimulus-package-3305782

- https://www.thebalance.com/fha-loan-basics-315656
- https://www.thebalance.com/what-is-freddie-mac-3305985
- https://www.thebalance.com/bearn-stearns-collapse-and-bailout-3305613
- http://www.washingtonpost.com/wp-dyn/content/article/2008/03/20/AR2008032003018.html
- https://www.stlouisfed.org/financial-crisis/full-timeline
- https://www.thebalance.com/what-was-the-fannie-mae-and-freddie-mac-bailout-3305658
- https://www.cnbc.com/id/25799253
- https://open.spotify.com/user/txdan2010/playlist/3X0JDW2W59uQ6Yx2J2X3XW?si=YpoSB0bLSSuaUoUhh7AClA
- https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12
- https://bitcointalk.org/index.php?topic=103369.msg1135218#msg1135218
- https://money.cnn.com/2008/09/07/news/companies/fannie_freddie/index.htm?eref=edition_business
- https://en.wikipedia.org/wiki/Chapter_11,_Title_11,_United_States_Code#Largest_cases
- https://www.cnbc.com/id/26708319
- https://www.thebalance.com/reserve-primary-fund-3305671
- https://www.businessinsider.com/tales-of-the-financial-crisis-2009-9
- https://www.gwern.net/docs/bitcoin/20081003-nakamoto-bitcoindraft.pdf
- https://www.thebalance.com/what-was-the-bank-bailout-bill-3305675
- https://www.thebalance.com/japan-s-economy-recession-effect-on-u-s-and-world-3306007
- https://www.theguardian.com/business/2008/oct/13/creditcrunch-marketturmoil1
- https://ftalphaville.ft.com/2008/10/15/17051/boj-offers-unlimited-dollars-to-banks/
- https://www.reuters.com/article/us-financial-usa-poll/u-s-mood-plummets-as-crisis-deepens-reuters-poll-idUSTRE49E3ML20081015
- https://www.cbsnews.com/news/top-pop-culture-moments-of-2008/
- https://www.tonysheng.com/mass-movement
- https://medium.com/u/be4506861043

Planting Bitcoin—Soil (3/4)

By Dan Held

Posted January 6, 2019

Introduction

In my last article, "Season," I covered the precise moment in which Satoshi planted Bitcoin, the 2008 Financial Crisis. In this article, I cover the Cypherpunks or the "Soil" in which he planted the Bitcoin seed giving it the best chance for survival.

Cypherpunks

Sending the Bitcoin whitepaper to the cryptography mailing list on October 31, 2008 was the obvious choice. This was the right group to gather feedback from, the right channel to engage with. The list was predominately populated by the Cypherpunks* who were activists advocating widespread use of strong cryptography, as a route to social and political change.

*"Cypherpunks" is a play on the word 'cipher' or 'cypher', for encryption; and cyberpunk a genre of sci-fi.

The group was originally comprised of Eric Hughes, Tim May, and John Gilmore. At first, the meetings were in-person meetings in the San Francisco Bay Area, but they decided to expand the group via the cryptographer mailing list which would allow them to reach other Cypherpunks. The mailing list was a place to exchange ideas freely through the use of encryption methods, such as PGP, to ensure complete privacy. The basic ideas behind this movement can be found in the Cypherpunk manifesto written by Eric Hughes in 1993. The key principle which underpins the manifesto is the importance of privacy and finality in transactions—PetriB

> *"Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system."—A Cypherpunk's Manifesto*

We want the ability to ensure that others cannot use the information in the history of our transactions against us. For example: a purchase indicating that someone is wealthy, an embarrassing purchase, or one that would make you subject to spam or harassment. We do not want our financial purchase to haunt us further down the road. We want an endpoint beyond which we do not have to worry about further contingencies. **In the world of payments, this is closely related to the concept of "finality"**—ideally we want to be able to state with certainty that at some point the payment has been made, the debt has been cleared, and the funds are secure. But recent developments have increased the ability for more powerful parties to clawback funds (via trusted third parties, legal funds, etc).

We hope that existing laws would provide protection against these difficulties. However, we can remove that moral hazard by not having to trust third parties or more powerful adversaries which can revert transactions solely based on their capabilities. This is what the Cypherpunks were fighting for with cryptography. They were the "Men of words," or anti-establishment intellectuals that laid the foundation for individuals like Satoshi to come along.

> *"The words of **anti-establishment intellectuals sow the seeds for revolution**. They present ideas and sometimes discredit the establishment, **paving the way for a charismatic leader to package their thinking into a movement**."—Tony Sheng*

Elliot Alderson, the "Cypherpunk" in the fictional show "Mr. Robot." He joins a group that aims to destroy all debt records by encrypting the financial data of the largest conglomerate in the world, E Corp.

Elliot Alderson, the "Cypherpunk" in the fictional show "Mr. Robot." He joins a group that aims to destroy all debt records by encrypting the financial data of the largest conglomerate in the world, E Corp.

The first attempts at making an anonymous transacting system were made by Cypherpunks on that cryptographer mailing list, including:

- Adam Back, the inventor of hashcash, the proof-of-work (PoW) system used by several anti-spam systems. A similar PoW system is used in bitcoin
- Nick Szabo, designed a mechanism for a decentralized digital currency he called "bit gold." Bit gold was never implemented, but has been called "a direct precursor to the Bitcoin architecture"
- Wei Dai, who published "b-money", an "anonymous, distributed electronic cash system"
- Hal Finny, who created the first reusable proof of work system before Bitcoin (And in January 2009 he became Bitcoin network's first transaction recipient). He was also a developer of the secure communication method known as Pretty Good Privacy (PGP)
- David Chaum, founded DigiCash (1989) as a form of centralized "electronic money" that deployed the same kinds of cryptographic protocols—public key cryptography—that support the nature of bitcoin transactions. It is often called "Chaumian eCash."

Satoshi cites many of these Cypherpunks in the Bitcoin whitepaper and references their influence on Bitcoin's development in public statements made post code launch.

> *"Bitcoin is an implementation of **Wei Dai's b-money** proposal… and **Nick Szabo's Bitgold** proposal"—Satoshi Nakamoto*

In fact, Satoshi thought he was late to cryptocurrency! While the Cypherpunks had attempted many times to genetically code a species of money that would survive, none had been successful.

> *"A lot of people **automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's**. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system."—Satoshi Nakamoto*

He had written the whitepaper to fit his target audience, the Cypherpunks. That's why he uses the words "electronic cash", "proof-of-work," etc. which was previously used terminology in the other Cypherpunk whitepapers. He uses an ecommerce example to make it easier for everyone to comprehend. He's crafting a narrative that will resonate with the Cypherpunks, to get them interested and involved. **Bitcoin was the holy grail—it had solved the problem of finality and provided a small measure of privacy.** The source code implementation was his product spec.

> *"The **functional details** are not covered in the paper, but the sourcecode is coming soon."—Satoshi Nakamoto*

The following things not described in the whitepaper, but are included in the source code: 21M hard cap, 10 minute blocks, 1 MB block caps. Those were incredibly important components of Bitcoin. The whitepaper was merely a teaser.

> *"If the Bitcoin Whitepaper is the **Declaration of Independence**, the Source Code is the **Constitution**"—Pierre Rochard*

In true Cypherpunk fashion, the publication of Satoshi's whitepaper (October 2008) was quickly followed by code release in January 2009. The notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list.

> *"**Cypherpunks write code**. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. **We publish our code so that our fellow Cypherpunks may practice and play with it**. Our code is free for all to use, worldwide…**We know that software can't be destroyed and that a widely dispersed system can't be shut down**."—A Cypherpunk's Manifesto*

Importantly, Satoshi didn't premine any Bitcoins. Satoshi gave the Cypherpunks a two month heads up before mining the Genesis block. To prove fairness, he included a proof of no premine timestamp in the Genesis Block of the Bitcoin blockchain. It carried a strong political message. What he was trying to accomplish was clear—they were building a new financial system. Bitcoin wasn't merely digital cash, it was an alternative to banks.

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"—Genesis Block

Links

- https://www.coindesk.com/the-rise-of-the-cypherpunks/
- https://www.activism.net/cypherpunk/manifesto.html
- https://medium.com/@Petri.basson
- https://research.stlouisfed.org/publications/review/2018/07/16/payment-systems-and-privacy
- https://www.tonysheng.com/mass-movement
- https://medium.com/@tonysheng
- https://en.wikipedia.org/wiki/Hashcash
- https://bitcointalk.org/index.php?topic=342.msg4508#msg4508
- http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493
- http://www.metzdowd.com/pipermail/cryptography/2008-November/014863.html
- https://medium.com/u/1206face71fc
- https://blog.picks.co/bitcoins-distribution-was-fair-e2ef7bbbc892
- https://en.bitcoin.it/wiki/Genesis_block

Planting Bitcoin - Gardening (4/4)

By Dan Held

Posted January 6, 2019

Introduction

In my last article, "Soil," I covered the Cypherpunks or the "Soil" in which he planted the Bitcoin seed giving it the best chance for survival.

Satoshi's design of Bitcoin's genetic code made it the best species of money ever created, he waited for exactly the right moment to plant the seed, and had planted it in the most fertile soil. Now it was time to nurture Bitcoin's development.

Early Development

> *"The project needs to grow gradually so the software can be strengthened along the way."—Satoshi Nakamoto*

Satoshi chose to be anonymous, which fit the ethos of the Cypherpunks. **People can project hopes and dreams on an anonymous individual, ensuring maximal narrative fit**. That's why a book is often better than the movie. His anonymity was a critical component of the founder story—dev worship is a dangerous thing for an open source project aiming for decentralization. Volunteers need to rely on trusting the objective reality of the code, rather than focusing on the merits of the project leader.

> *"It is high time for everyone involved in BTC to stop concerning themselves with the question of the identity of Nakamoto, and accept that **it does not matter to the operation of the technology, in the same way that the identity of the inventor of the wheel no longer matters**"- Saifedean Ammous*

As a subtle jab to central banks, and as a nod to his admiration of the gold standard, **he chose his birthday (on his p2p foundation website profile) as the date the US made gold ownership illegal** through Executive Order 6102, April 5th. And he chose 1975 as his year of birth which is the year when the US citizens were allowed to own gold again.

> *"[with Bitcoin] **we can win a major battle in the arms race** and gain a new territory of freedom for several years."—Satoshi Nakamoto*

In his public statements, he usually focused on ordinary, mainstream, users, with his tone sometimes even excited in suggesting many ways bitcoin could be made more convenient or useful for commerce or other things. Satoshi was practical, which made

interactions very easy and comfortable. He tended to avoid philosophical discussions and political arguments.

Additionally, Satoshi took steps to signal to the Cypherpunks, and future members, that Bitcoin wasn't a scam. The conservative deescalation of his mining contributions, never spending any of his coins, nor using his influence for any purpose, shows that he wanted the world to make up their own mind about his project and judge it on its own terms. **And unlike every other founder in history, Satoshi never cashed out.**

> *"Bitcoin benefited from an extremely rare set of circumstances. Because it launched in a world where digital cash had no established value, they circulated freely. That can't be recaptured today since everyone expects coins to have value. Not only was it fair, but it was historically unique in its fairness. The immaculate conception."* Nic Carter

Many of the early Cypherpunks became core developers in the Bitcoin protocol like Hal Finney and Adam Bach. The caliber of the early development team attracted talented (soon to be "core") developers.

> *"Gifted people tend to want to work with other top people and work on something that matters, that they believe in.* ***Motivation matters****. Protocol design and coding is partly an artistic, aesthetic endeavour; people do their best work on a mission: uncensorable global internet money"—Adam Bach*

The Gardener Leaves

Satoshi showed a great level of restraint and took a long-term perspective on issues, as when Satoshi resisted the calls for bitcoin to market itself as a funding mechanism for Wikileaks after PayPal famously froze its account. This, Satoshi argued, would only bring down legal and regulatory hammers that much faster. Satoshi recognized the need to carefully cultivate Bitcoin.

> *"I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and* ***the heat you would bring would likely destroy us at this stage****."—Satoshi Nakamoto*

The connection to Wikileaks at such an early stage, at the height of what could be called public resistance against the Iraq war, probably gave Bitcoin a very different dimension. So he did not mince his words nor hide his intention for leaving in what can be called the last public statement where he says the US government was headed towards Bitcoin.

> *"It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and* ***the swarm is headed towards us****."—Satoshi Nakamoto*

In April 2011, Gavin Andressen notified Satoshi that he was meeting with the CIA. **Any further involvement might give away his identity which would endanger the long-term success of the project**. Bitcoin now had enough support that he could walk away, and so he did.

> *"Satoshi left because he didn't want its influence to affect the protocol development creating a single point of failure. The very idea of "Satoshi Vision" itself is against Satoshi's vision for Bitcoin"—Frederico Tenga*

Social Scalability

Satoshi was able to walk away because Bitcoin had trust minimization baked into the protocol. This is what made it socially scalable.

> *"Power and scale breed conflict and corruption, that the purest part of any revolution is the beginning."—Dhruv Bansal*

It is easy to start with good intentions, however as things scale that becomes harder and harder to maintain. **Bitcoin was specially architected to be trust minimized**. Satoshi set it up so that there is no one person or group whose power can be coveted, usurped, or broken.

> "Bitcoin is a social breakthrough, not a technological one"—Alex Hardy

Bitcoin needed to be the universal language for money. You are communicating with strangers worldwide, which you neither know nor trust that agree you own an abstraction of value.

> *"Bitcoin is a distributed incentive structure we collectively engineer and freely opt-into. It's political technology, the first of its kind. This leaderless-ness is one part of what gives Bitcoin—in particular, beyond other cryptocurrencies today—such robustness."—Dhruv Bansal*

HODLing, the Hero's Journey

> "In the beginning of a change the patriot is a scarce man, and brave, and hated and scorned. When his cause succeeds, the timid join him, for then it costs nothing to be a patriot."—*Mark Twain*

Satoshi built Bitcoin for the believers in a new financial system, the HODLers, the revolutionaries. The ones who were disenfranchised with the existing financial system. The ones who would be attracted by the prospect of sudden and spectacular change in their life.

We must heed the call for a Hero's Journey (the HODLer) that is rooted in HODL. **It's not just a meme, it is representative of foundational values upon which stronger cultural memes are eventually developed**. This supports Bitcoin's cultural foundation.

"Over and over again, the financial system was, in some narrow way, discredited….The rebellion by American youth against the money culture never happened."—Big Short

The Hero at the beginning of their Journey has values that do not agree with the values that the Hero ends up with at Journey's end. That is the entire point of undertaking the Journey, but is also what makes it so frightening.**The Hero must let go of his/her former self in the pursuit of this transformed version of themselves.** The Journey's end is unknown, but what is known is that the Journey inspires the acquisition of new knowledge, the relinquishing of outdated paradigms and the abandoning of the familiar.The HODL Journey in Bitcoin sketches a map that becomes clearer with the acquisition of knowledge.

Satoshi needed to bootstrap the network with an incentive mechanism—the block reward which (a) controlled currency supply of Bitcoin and (b) created an incentive for people to participate in the network. **Each cycle brings aboard a new set of true believers; a new set of HODLers**. They, in their turn, become strong advocates for the adoption of Bitcoin as a store of value. Contagious Freedom. Vijay Boyapati

*"**Hodling bootstrapped Bitcoin into existence.** Hodling increases value, which increases demand, hash rate, and network security, which, in turn, attracts new hodlers and devs. This self-reinforcing feedback loop drives Bitcoin's network effects, security, and value."—@TobiasAHuber*

Satoshi had encoded in Bitcoin DNA a mechanism to incentivize the participants, through the shared belief in Bitcoin manifested via HODLing.

*"In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. I**t has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value.**"—Satoshi Nakamoto*

Early HODLers believed in Bitcoin despite overwhelming negativity and false information (ex: labeled as a currency for money launderers and drug dealers, price fluctuations). HODLers had stronger risk appetite to weather the volatility of being a first mover. They're practitioners of skin in the game.

In terms of the Hero's Journey, "HODL!" is the mentor's advice to the Hero in his Journey. Its roots are firmly based on the futility of trying to beat the market (Efficient Market Hypothesis and Hayekian Distributed information both dictate that the market can't be systematically outperformed).

The increase in Bitcoin's price has corresponding virality. And as it expands, HODLing becomes popular with people with a lower risk appetite, pulling in more and more network effect into the Bitcoin black hole—Dan McArdle

Via the Lindy Effect, the longer Bitcoin remains in existence the greater society's confidence that it will continue to exist long into the future. **It slowly seeps further into the psyche of those in charge.**

"Protocols die when they run out of believers."—Naval

The faith in a new financial system is what binds everything together. Bitcoin is not just a software project. It's a method of coordination for a large group of people who face powerful adversaries. Bitcoin isn't just a technological breakthrough, it's also a social one.

"When people are ripe for a mass movement, they are usually ripe for any effective movement, and not solely with a particular doctrine or program. All mass movements are competitive, and the gain of one in adherents is the loss of all the others….A stable and sustainable ideology must be the foundation of all cryptocurrencies. ***No amount of cryptography, or consensus protocol development will help a cryptocurrency with an unstable and bankrupt ideology. Stable ideologies allow communities to thrive****". Kay Kurokawa*

A simple example in religion is the Christian tenet that "there is one true god". This belief strengthens the religion because it weakens membership in competing religions. **Communities with unstable ideologies will eventually collapse.**

"Unlike Bitcoin, nobody needs to explain why gold is valuable. Gold is simple. Bitcoin is complicated. So in the long run, the argument goes, Bitcoin can never replace gold… It's true that the stories we tell matter, but those stories can change. ***Stories don't win over everything. Eventually, raw utility supplants tradition. Bitcoin is a serious improvement over gold and starts to displace its role, the market will respond and re-price accordingly****… To the digital native of the future, Bitcoin wallets will probably seem more natural than vaults full of useless metals painstakingly drilled out of the earth."—Haseeb Qureshi*

Money is a winner-take-all technology, driven by network effects. The crypto with the most HODLers, therefore, is the most demanded by consumers and will be the ultimate winner.

"Bitcoin is digital gold in the eyes of [HODLers]. To some extent this group already operates on a Bitcoin Standard: investments are evaluated on their ability to yield a return in Bitcoin." Tuur Demeester

HODL forces us to extend our gaze beyond the present. It forces our present selves to contend with an alternate reality. **HODL asks us to reconfigure our present set of preferences to permit the consideration of a future Bitcoin-based digital economy.**

HODL is a noble basis for a Journey. Through the sacrifice of current consumption, **HODLing is a net benefit for everyone as it increases every coin's purchasing power.**

"No Hero fights alone; All for one, one for all. Your call to HODL need not be the same as mine; indeed, they can be very different. Yet, in the end, they all redound to the benefit of each other."—Prateek Goorha

Bitcoin promises an alternative for citizens across the world to keep their savings in a form of money that can neither be confiscated nor diluted. If Bitcoin grows much larger, it may force governments to become a voluntary organization. **Through HODLing, we may finally be free.**

'The secret to happiness is freedom; the secret to freedom is courage'—Thucydides

Those who opt-in to Bitcoin, are trading something abundant for something scarce, **trading the past for the future, trading financial dependence for financial sovereignty.**

Conclusion

Satoshi architected the perfect genetic code necessary to a new species of money, Bitcoin. He then waited for the precise moment to plant the new species, the 2008 Financial Crisis. At that moment, he distributed the whitepaper to the only group that cared—the Cypherpunks. And finally, he nurtured Bitcoin to a stage where it no longer needed him.

Many digital cash systems came and went over the years before Bitcoin and after Bitcoin. Most were just whitepapers, some wrote and developed code, some even built a community, but it will be extremely difficult to repeat the success of Bitcoin's planting.

"Let the future tell the truth, and evaluate each one according to his work and accomplishments. The present is theirs; the future, for which I have really worked, is mine."—Nikola Tesla

Links

- https://bitcointalk.org/index.php?topic=1735.msg26999#msg26999
- https://medium.com/@saifedean
- http://p2pfoundation.ning.com/profile/SatoshiNakamoto
- http://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html
- https://medium.com/@nic__carter
- https://www.youtube.com/watch?v=dTILX-_JzTs
- https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280
- https://mobile.twitter.com/FedericoTenga/status/1019726734210555904
- https://medium.com/@shrubvandal
- https://medium.com/@vijayboyapati
- https://twitter.com/TobiasAHuber
- http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562

- https://medium.com/@robustus
- https://twitter.com/naval
- https://medium.com/@kaykurokawa
- https://hackernoon.com/we-already-know-blockchains-killer-apps-f2d443eba35
- https://medium.com/@tuurdemeester
- https://medium.com/@goorha

Money, Bitcoin and Time: Part 1 of 3

By Robert Breedlove

Posted January 20, 2019

A synthesis of perspectives from many prolific thinkers, this 3-part essay will cover the following topics in sequence:

· Money—its properties, story and evolutionary history

· Bitcoin—its nature and significance in the story of money (see PART 2)

· Time—perspectives on its value and how the story of money might play out (see PART 3)

This essay is guided, inspired and adapted from the literary works of many. Each section header will include a number [n] referencing relevant synthesized works at the end of each part. For those seeking further elucidation on any of the topics discussed herein, I highly encourage you to read these original works.

This essay is also available in .pdf form at: https://www.parallaxdigital.io/blog

Please feel free to send any questions or feedback to info@parallaxdigital.io

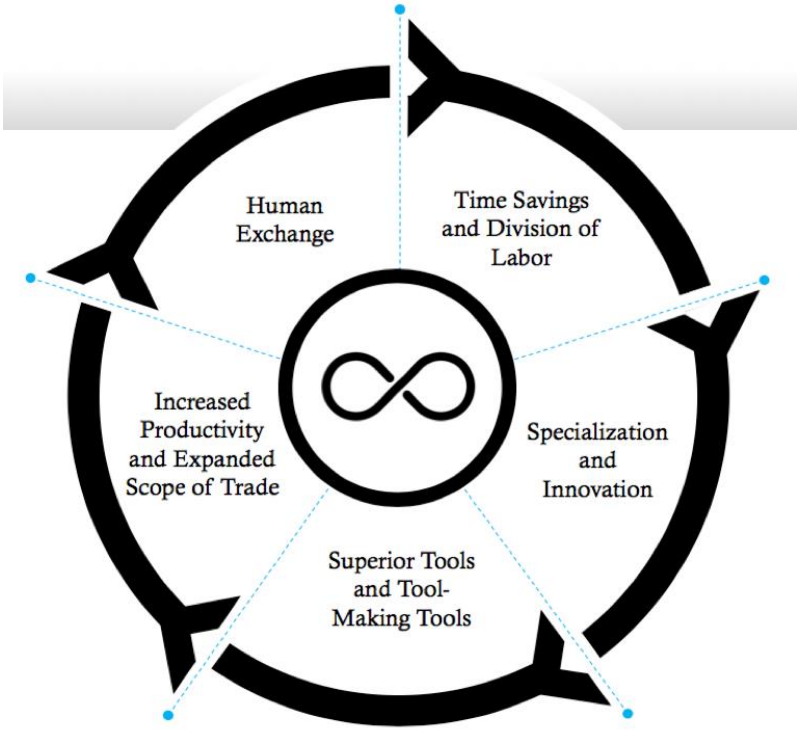
The Simple Truth about Money: Money is the most successful story ever told by humans. It is a reflexive narrative: meaning it has value only because everyone believes it, and everyone believes it because it has value. Money is a story that continues to be written…

Human Exchange [2,6]

Human beings are the networked species. Initially, these were small bands of hunters and gatherers numbering no more than 150 persons strong (Dunbar's number). When humans began to exchange with one another, they intuitively discovered the *division of labor* which allows people to focus on their relative advantages and concentrate on their chosen craft. The division of labor enables the *specialization* of productive efforts for mutual gain. If John makes axes faster than Steve, and Steve makes bows faster than John, then they both are better off by specializing and trading. Interestingly, this holds true even if John is faster than Steve at making axes and bows (up to a point) and, amazingly, this effect compounds.

Tools, or technologies, are mechanisms that increase *productivity* by amplifying the returns on human time directed at production. You can chop more wood per man hour using an axe than you can with your bare hands. As people made and exchanged more tools, time savings increased and specialization deepened. Specialization sparked innovation, because it encouraged the investment of time in tool-making tools, such as whetstones used for making sharper axes. This enabled people to create superior tools, which

increased productivity even further. That saved more time, which people used to specialize even further and expand their *scope of trade* by exchanging with an even greater number and variety of people, which increased the division of labor even further, and so on. This recursive dynamic persists to this day as a virtuous cycle with no known natural limit—modern markets in goods, services and ideas allow human beings to exchange and specialize honestly for the betterment of all. In this way, the act of exchange is the incipient force driving all human progress and *prosperity*. Prosperity is simply time saved, which is proportional to the division of labor:



Human exchange is the incipient force driving all human progress and prosperity. *Prosperity is simply time saved, which is proportional to the division of labor. This recursive dynamic persists to this day as a virtuous cycle with no known natural limit—modern markets in goods, services and ideas allow human beings to exchange and specialize honestly for the betterment of all.*

Human exchange is to cultural evolution what sex is to biological evolution. By exchanging and specializing, innovations come into existence and spread. At some point, human intelligence became collective and cumulative in a way that happened to no other animal. Language, and later writing, allowed us to pass our collective learnings to each successive generation. Written language allowed us to manifest and share our belief systems. As the only animal that can tell and believe stories, we learned to organize ourselves using abstractions such as money, mathematics, nations and corporations. Our unique ability to tell and believe stories—as free market capitalists, human rights activists, national citizens or whatever story we accord with—enables us to cooperate flexibly in large numbers and across genetic boundaries. This scale of collaboration, never attained by any other animal

before or since, is the reason mankind came to dominate the Earth. We are the networked species, fully interconnected by our acts of exchange. A spontaneous emergent property of these complex human interactions is money, which solved problems inherent to trade and accelerated the rate of human exchange and the division of labor. Money, as the vital lubricant for human exchange, was among the first stories we used to collectively organize ourselves.

Story of Money [1]

Let's begin with first principles and follow logic from there. The simplest form of human exchange is the direct trading of actual goods, say guns for boats, in a process known as *direct exchange* or barter. Direct exchange is only practical when few people are trading few goods. In larger groups of people, there are more opportunities for individuals to specialize in production and trade with more people, which increases the aggregate wealth for everyone. This simple fact, that exchange enables us to produce more goods per hour of human effort is the foundation of economics itself:

Economics is the social science of increasing production per unit of contribution.

Larger groups of people exchanging goods mean larger markets, but also creates a problem of *non-coincidence of wants*—what you are seeking to acquire by trade is produced by someone who doesn't want what you have to offer. This problem has three distinct dimensions:

- Non-coincidence in Scales—imagine trying to trade pencils for a house, you cannot acquire fractions of a house and the owner of the house may not need such a large amount of pencils
- Non-coincidence of Locations—imagine trying to trade a coal mine in one place for a factory in another location, unless by coincidence you are seeking a factory in that exact location and the counterparty you are dealing with is seeking a coal mine in that precise place, the deal will not be completed since factories and coal mines are not movable
- Non-coincidence in Time Frames—imagine trying to accumulate enough oranges to trade for a truck, since the oranges are perishable they would likely rot before the deal could be completed

The only way to resolve this three-dimensional problem is with *indirect exchange,* where you seek to find another person with a good desired by the counterparty and exchange your good for theirs only to, in turn, exchange it for the counterparty's good to complete the deal. The intermediary good used to complete the deal with the counterparty is called a *medium of exchange* – the first function of money. Over time, people tend to gradually converge on a single medium of exchange (or, at most, a few media of exchange) as it simplifies trade. A good that becomes widely accepted as a medium of exchange is commonly called money.

Money offers its users pure optionality, as it can be readily exchanged for any good available in the marketplace. In other words, money is the most liquid asset within a trade network. In this sense, money is said to have the highest *salability*, meaning the ease with which it can be sold on the market at any time with the least loss in price. Salability of a good is relatively determinable by how well it addresses the three dimensions of the non-coincidence of wants problem:

- Salability across Scales—a good that is easily subdivided into smaller units or grouped together in larger units, which allows the user to trade it in whatever quantity desired
- Salability across Space—a good that is easily transported or transmitted over distances
- Salability across Time—a good that can reliably hold its value into the future by being resistant to rot, corrosion, counterfeit, unpredictable increases in supply and other debasements of value

It is the third element, salability across time, that determines a good's utility as a *store of value*—the second function of money. Since the production of each new unit of a monetary good makes every other unit relatively less scarce, it dilutes the value of the existing units in a process known as *inflation*. Protecting value from confiscation via inflation is a critical feature of money, and money is critical to the existence of flourishing trade networks.

Hard Money [1]

Hard money is more trustworthy as a store of value precisely because it resists intentional debasements of its value by others and therefore maintains salability across time. The hardness of a monetary good, also known as its soundness, is determined by the stock of its existing supply and the flow of its new supply. The ratio which quantifies the hardness of money is called the *stock-to-flow* ratio:

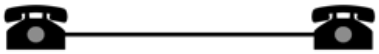
- 'Stock' is the existing supply of monetary units
- 'Flow' is the newly created supply over a specified time period, usually one year
- Dividing the stock of a monetary good by its flow equals its stock-to-flow ratio
- The higher the stock-to-flow ratio, the greater the hardness (or soundness) of money

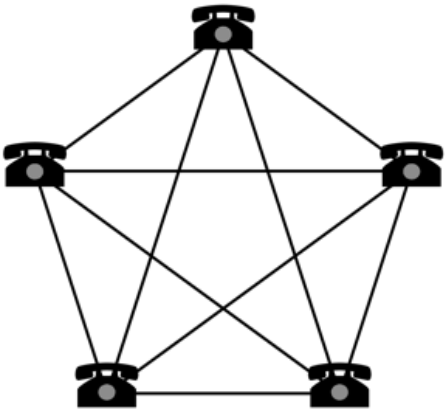
The higher the stock-to-flow ratio, the more resistant the money is to having its value compromised by inflation. There are no correct choices as to forms of money, however there are consequences to what form a market naturally selects. If people choose to store their wealth in a monetary good which exhibits less hardness, then the producers of this monetary good are incentivized to produce more monetary units, which expropriates the wealth of existing unit holders and destroys the monetary good's salability across time.

This is the fatal flaw of *soft money*: anything used as a store of value that can have its supply increased will have its supply increased, as producers seek to steal the value stored within the soft monetary units and store it in a harder form of money. As many historical examples in this essay will demonstrate, any monetary good which can have its supply cheaply and easily increased will rapidly destroy the wealth of those using it as a store of value.

For a good to assume a dominant monetary role within an economy, it must exhibit superior hardness with a higher stock-to-flow ratio than competing monetary goods. Otherwise, excessive unit production will destroy the wealth of savers and the incentives to use it as a store of value. Particular goods achieve monetary roles based on the interplay of people's decisions. It is from the chaos of complex human interactions that monetary orders emerge. Therefore, it is important to consider the social aspects of the spontaneous emergence of monetary orders.

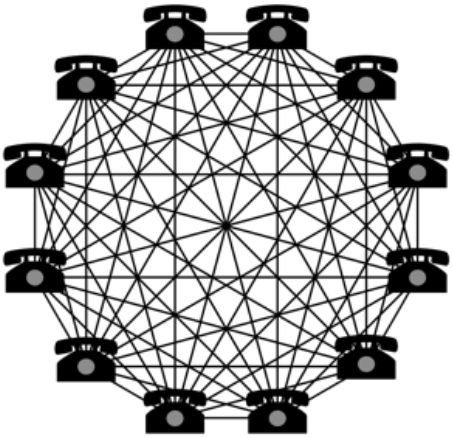
Money is a Social Network [1,4]





Money, as a value system which connects people across space and time, is the original and largest social network. The value of a network is a reflection of the total number of possible connections it allows. Similar to the telephone and modern social media platforms, a monetary network becomes exponentially more valuable as more people join it because the number of possible connections it allows is proportional to the square of the number of its total network participants, a relationship defined by *Metcalfe's Law*:

> *Network values are based on the number of possible connections they allow. Such values grow exponentially with the addition of each new constituent—a property commonly known as network effects.*



In a monetary network, more possible connections mean more salability and a broader scope of trade. Participants in a monetary network are connected by their use of a common form of money to express and store value. *Network effects*, defined as the incremental benefit attained by adding a new member to a network for all existing members in that same network, encourage people to adopt a single form of money. Intuitively, a monetary good that holds value across time (hard money) is always preferable to one that loses value (soft money). This causes people to naturally gravitate to the hardest form of money available to them. Further, since

human exchange is a singular communal phenomenon suffering from a three-dimensional non-coincidence of wants problem, any monetary good that can solve all three dimensions of this problem will win the entire (or vast majority) of the market. For these reasons, a free market for money exhibits a *winner take all* (or, at least, a winner take most) *dynamic*. Network effects accelerate people's natural coalescence around a single monetary technology since larger monetary networks support higher salability of the monetary good involved. However, the selection of a monetary good is limited by the technological realities of the markets selecting. This can impede the winner take all dynamic, since particular monetary goods each satisfy the desirable traits of money to greater or lesser extents.

Monetary Traits [1,4]

As we will see, markets have naturally and spontaneously selected for the monetary good which best satisfies a variety of desirable traits that determine how useful a particular monetary good is as a form of money:

- Hardness—resistance to unpredictable supply increases and debasements of value
- Fungibility—units are interchangeable and indistinguishable from one another
- Portability—ease of transporting or transmitting monetary units across distances
- Durability—resistance of monetary units to rot, corrosion or deterioration of value
- Divisibility—ease of subdividing or grouping monetary units
- Security—resistance to counterfeiting or forgery
- Sovereignty—the source of its value, trust factors and permissions necessary to transact with it (natural social consensus or artificial government decree)
- Government Issued—authorized as legal tender by a government

As discussed, hardness is the singular trait that takes primacy over all others in determining a good's suitability for playing a monetary role. Money, as an expression of value, has remained conceptually constant but has evolved to inhabit many different goods over time. Like language, which was first spoken, then written and now typed, the meaning expressed by money remains the same while its modality continually evolves. As the monetary technologies we use to express value change, so too do our preferences.

Prospects of Prosperity [1]

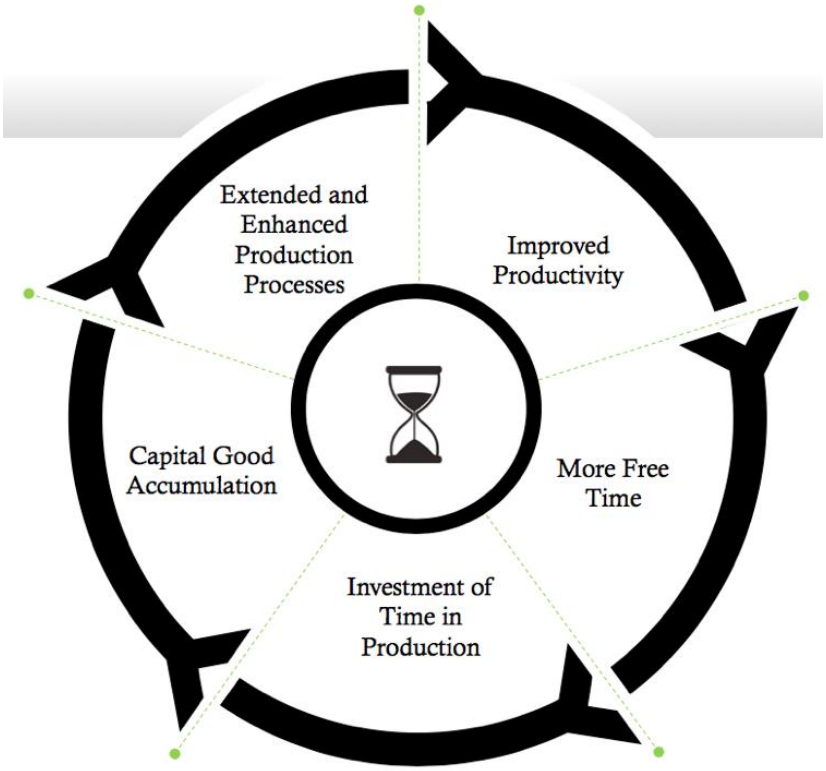
In economics, a critical aspect of human decision making is called *time preference*, which refers to the ratio at which an individual values the present relative to the future. Time preference is positive for all humans, as the future is uncertain, and the end could always be near. Therefore, all else being equal, we naturally prefer to receive value sooner rather than later. People who prefer to defer current consumption and instead invest for the future are said to have a lower time preference. The lowering of time preference is closely

related to the hardness of money and is also exactly what enables human civilization to advance and become more prosperous. In regard to time preference, hard money is important in three critical aspects:

- By providing a reliable way to protect value across time, hard money incentivizes people to think longer term and thus lowers their time preferences
- As a stable unit of measurement, hard money enables markets to grow ever-larger by reducing the costs and risks of free trade, which increases the incentives for long-term cooperation and lowers time preferences
- Self-sovereign money (like gold and Bitcoin) that cannot be manipulated by any single party reduces governmental intervention which encourages the growth of free markets, which increases their long-term stability and lowers time preferences

A lower time preference is an important part of what separates humans from other animals. By considering what is better for the future, we can curb our animalistic impulses and choose to act rationally and cooperate for the betterment of everyone involved. As humans lower their time preference, they develop a scope for carrying out tasks over longer time horizons. Instead of spending all our time producing goods for immediate consumption, we can choose to spend time creating superior goods that take longer to complete but benefit us more in the long run. Only by lowering time preference can humans produce goods that are not meant to be consumed themselves but are instead used in the production of other goods. Goods used exclusively for the production of other goods are called *capital goods*.

Only humans with a lower time preference can decide to forgo a few hours of fishing and opt to build a superior fishing pole, which cannot be eaten itself, but in the future will enable better results per hour of human effort spent fishing. This is the essence of *investment*: humans defer immediate gratification and invest their time producing capital goods which will, in turn, make the production process itself more sophisticated, extend it over a longer time horizon and yield superior results per hour of human effort. In this way, investment increases capital good stocks which increases productivity. Amazingly, this effect also transforms into a *positive feedback loop*. Also known as a virtuous cycle or the flywheel effect, a positive feedback loop is a process that is recursively energized (its outputs also serve as its inputs) and therefore creates compounding effects. Positive feedback loops play an important role in biology, chemistry, psychology, sociology, economics and cybernetics. In respect to investment, as more capital goods are accumulated, levels of productivity are increased even more and the time horizon of production is extended even further:



As people exhibit lower time preferences and spend their time wisely, they increase their capacity for investment and create more free time for themselves.

To understand this preference clearly, let's consider two hypothetical fishermen, Harold and Louis, who start out with nothing other than their bare hands. Harold has a higher time preference than Louis and chooses to spend his time catching fish with using just his bare hands. Using this approach, Harold spends about 8 hours per day to catch enough fish to feed himself for one day. Louis, on the other hand, spends just 6 hours per day catching fish, makes do with the smaller amount of fish and chooses to spend the other 2 hours building a fishing pole. Two weeks later, Louis has succeeded in building a fishing pole, which he can now use to catch twice as many fish per hour as Harold. Louis's investment in the fishing pole could allow him to only fish for 4 hours each day, eat the same amount of fish as Harold and spend his other 4 hours in leisure. However, since Louis has a lower time preference, he instead chooses to fish for 4 hours per day and spend the other 4 hours building a fishing boat.

One month later, Louis has succeeded in building a fishing boat, which he can now use to go further out to sea and catch fish that Harold has never even seen. Not only has Louis increased his productivity (fish caught per man hour) but he has also increased the quality of his production (a greater variety of fish from the deep sea). By using his fishing pole and boat, Louis now needs only 1 hour per day to catch a day's worth of food and spends his other 7 hours engaged in further capital accumulation—building better fishing poles, boats, nets, lures, etc.—which, in turn, further increases his productivity and quality of life.

Should Louis and his descendants continue to exhibit a lower time preference, the results will compound over time and across generations. As they accumulate more capital, their work efforts will be ever-further amplified by productivity gains and enable them to engage in ever-larger projects that take ever-longer to complete. These gains are amplified even further when Louis and his descendants begin trading with others that specialize in crafts in which they themselves do not—such as housing, wine making or farming. Successive layers of learning, productivity gains and flourishing trade networks are the foundational sediment upon which all human advancement in terms of knowledge, technology and culture is built. Human advancement is noticeable in the tools we make and the way we relate with one another.

From this perspective, it becomes clear that the most important economic decisions any individual faces are related to the trade-offs they face with their future self. Eat less fish today, build a fishing boat tomorrow. Eat clean today, be healthy tomorrow. Exercise today, be fit tomorrow. Read books today, be knowledgeable tomorrow. Invest money today, be wealthy tomorrow. We can all take solace that this compounding force of nature is always available to each and every one of us. No matter how bad the circumstances are for a man with a low time preference, he will likely find a way to keep compounding his present efforts and prioritizing his future self until he achieves his objectives. Contrarily, no matter how much fortune and wealth favors the man with a high time preference, he will likely find a way to continue squandering his wealth and shortchanging his future self. These individual relationships with our future selves is the microcosm of the societal macrocosm. As society develops a lower time preference, its prospects of prosperity improve in tandem.

Foundation of Economic Growth [1,4]

There are many factors beyond the scope of this essay which influence time preference. Most relevant to our discussion is the expected future value of money. As we have seen, hard money is superior at holding its value across time. Since its purchasing power tends to remain constant or grow over time, hard money incentivizes people to delay consumption and invest for the future, thereby lowering their time preference. On the other hand, soft money is subject to having its supply increased unexpectedly. Increasing the money supply is the same as lowering the *interest rate*, which is effectively the price of borrowing money and the incentive to save. By reducing the interest rate, the incentive to save and invest is diminished whereas the incentive to borrow is increased. So, soft money disincentivizes a favorable orientation towards the future. In other words, soft money systems raise society's time preference. For this reason, soft money, once it is sufficiently debased, tends to precede societal collapse (more on this later).

An ideal hard money would be one whose supply is absolutely scarce, meaning no one could produce more of it. The only noncriminal way to acquire money in such a society would be to produce something of value and exchange it for money. As everyone seeks to acquire more money, everyone would become ever-more productive which would encourage capital accumulation, productivity gains and a lowering of time preference.

Since the money supply is fixed, economic growth would cause the prices of real goods and services to drop over time, as a fixed quantity of monetary units chases an increasing quantity of goods. Since people could expect to be able to purchase more with the same amount of money in the future, such a world would discourage immediate consumption and encourage saving and investment for the future. Paradoxically, a world that consistently defers consumption will actually end up consuming more in the long run as its increased savings would increase investment and productivity, thus making its citizens wealthier in the future. This dynamic would spark a positive feedback loop—with present needs met and an ever-greater focus on the future, people naturally begin concentrating other aspects of life such as social, cultural and spiritual endeavors. This is the essence of free market capitalism: people choosing to lower their time preference, defer immediate gratification and invest in the future.

The foundation of all economic growth is delayed gratification, which leads to savings, which leads to investment, which extends the duration of the production cycle and increases productivity in a self-sustaining, virtuous cycle with no known natural limit.

Debt is the opposite of saving. As saving creates the possibility for capital accumulation and its associated benefits, debt is what can reverse it by reducing capital stocks, productivity and living standards across generations. As we will show later, when the gold standard was forcibly ended by governments, money not only became much softer, but it also fell under the command of politicians who are incentivized to operate with high time preferences as they strive for reelection every few years. This explains why politicians continue to mandate the use of soft government money, despite the long-term harm it causes to an economy, ensuring that it remains the dominant form of money in the world (we will cover soft government money's unnatural ascent to world domination later).

When a form of money becomes globally dominant, it finally serves the third function of money—*unit of account*. History shows us that this function is the final evolutionary stage in the natural ascendancy of monetary goods that achieve a dominant role—which are first a store of value, then a medium of exchange and finally a unit of account. As economist William Stanley Jevons explained:

> *"Historically speaking, gold seems to have served, firstly, as a commodity valuable for ornamental purposes; secondly, as stored wealth; thirdly, as a medium of exchange; and, lastly, as a measure of value."*

Today, the US Dollar is dominant and serves as the global unit of account as prices are most commonly expressed in its terms. This consistency of expression simplifies trade and enables a (somewhat) stable pricing structure for the global economy.

The Economic Nervous System [1]

Market prices are an essential communicative force in economics. As economic production moves from a primitive scale, it becomes harder for individuals to make production,

consumption and trade decisions without having a fixed frame of reference (unit of account) which to compare the value of different objects to one another.

In his paper 'The Use of Knowledge in Society' Friedrich Hayek elucidated the economic problem as not merely a matter of allocating human effort. More accurately, the economic problem is one of allocating human effort according to knowledge that is distributed in the minds of people that are each primarily concerned with their respective area in the broader economy. This distributed knowledge includes the:

- Conditions of production
- Availability of the factors of production
- Preferences of individuals

Knowledge, due to its dynamic and fluid nature, cannot be fully known by a single entity as it is constantly in flux and widely distributed within many minds. In a free market economic system prices capture this distributed knowledge, convert it into impartial information and disseminate it widely. *Price signals* are the coordinating force of free market systems. Each individual decision maker can faithfully rely on the prices of goods relevant to their production process, as the prices themselves are a distillation of all known market realities into a single, actionable variable. Each individual's buy and sell decisions, in turn, further shape prices which carry this altered information back out into the market. Price signals are to market participants what light is to the eye.

To understand this point, consider the 2010 earthquake which badly damaged an area in Chile responsible for a great deal of the world's copper production. This earthquake severely damaged copper mines and export infrastructure, which immediately reduced the flow of new supply to the world copper market and resulted in a 6.2% increase in its price. Anyone in the world whose business interfaces with the copper market will be affected by this, but they do not need any specific knowledge about the earthquake in Chile or market conditions to decide how to respond. All the relevant information they need to make effective decisions is contained within the price of copper itself. Immediately, all firms that demand copper are incentivized to demand less, delay purchases or find substitutes. On the other side of the market, all firms that produce copper are incentivized to produce more of it. With a natural shift in price, everyone in the world involved in the copper industry is incentivized to act in a way that alleviates the negative consequences of the earthquake. This is the power of a free market with accurate price signals.

The wisdom of the crowd is always superior to the wisdom of the board room. There is simply no way to recreate the adaptivity and collective intelligence of markets by installing a centralized planning authority. How would they decide who should increase production and by how much? How would they decide who should reduce consumption and by how much? How would they coordinate and enforce their decisions in real time on a global scale? In this sense, prices are the economic nervous system that disseminate knowledge across the world and help coordinate complex production processes by:

- Incentivizing supply and demand changes to match economic reality and restore market equilibriums quickly
- Efficiently matching buyers and sellers in the marketplace
- Compensating producers for their work efforts

Without accurate price signals, humans could not benefit from the division of labor and specialization beyond a small scale. Trade allows producers of goods to mutually increase their living standards by specializing in goods in which they have a relative or *comparative advantage*—goods they can produce relatively faster, cheaper or better. Accurate prices expressed in a common, stable medium of exchange help people identify their comparative advantage and specialize in it. Specialization, guided by reliable price signals, enables producers to improve their efficiency of production and accumulate capital specific to their craft. This is why the most productive allocation of human efforts is only determinable by an accurate pricing system within a free market. Also (as we will see later), this is exactly why capitalism prevailed over socialism, because socialism lacked an economic nervous system. But before diving into the economic aspects which underpinned this historic ideological struggle and seeing how it is still relevant today, we first need to understand the evolutionary forces that have shaped money throughout history.

Monetary Evolution [1]

Throughout history, money has taken many forms—seashells, salt, cattle, beads, stones, precious metals and government paper have all functioned as money at one or more points in history. Monetary roles are naturally determined by the technological realities of the societies shaping the salability of goods. Even today, forms of money still spontaneously emerge with things like prepaid mobile phone minutes in Africa or cigarettes in prisons being used as localized currencies. Different monetary technologies are in constant competition, like animals competing within an ecosystem. Although instead of competing for food and mates like animals, monetary goods compete for the belief and trust of people. Believability and trustworthiness form the basis of *social consensus*—the source of a particular monetary good's sovereignty from which it derives its market value along with the trust factors and permissions necessary to transact with it.

As these competitions continue to unfold in a free market, goods attain and lose monetary roles according to the traits which determine how believable or trustworthy they are and are expected to remain over time. As we will show, free market competition is ruthlessly effective at promulgating hard money as it only allows those who choose the hardest form available to maintain wealth over time. This *market-driven natural selection* causes new forms of money to come into existence and older forms to fade into extinction. Like biologically-driven natural selection, in which nature continuously favors the organisms which are best suited for success in their respective ecologies, this market-driven natural selection is a process in which people naturally and rationally favor the most believable and trustworthy monetary technologies available in their respective trade networks. Unlike ecological competition which can favor many dominant organisms, the marketplace for

money is driven by network effects and favors a winner take all (or, at least, a winner take most) dynamic as the non-coincidence of wants problem is universal and if a single hard money is capable of solving all three of its dimensions than it will become dominant (as discussed earlier in the social network aspects of money).

An example of this market-driven natural selection of money comes from the ancient Rai Stones system of Yap Island, located in what is today Micronesia. Rai Stones were large disks of various sizes with a hole in the middle that weighed up to eight thousand pounds each. These stones were mined in neighboring Palau or Guam and were not native to Yap. Acquiring these stones involved a labor-intensive process of quarrying and shipping. Procuring the largest Rai Stones required workforces numbering in the hundreds. Once the stones arrived in Yap, they were placed in a prominent location where everyone could see them. Owners of the stones could then use them as payment by announcing to the townsfolk the transfer of ownership to a new recipient. Everybody in the town would then record the transaction in their individual ledger, noting the new owner of the stone. There was no way to steal the stone because its ownership was recorded by everyone. In this way, the Rai Stones solved the three dimensions of the non-coincidence of wants problem for the Yapese by providing:

- Salability across scales as the stones were various in size and payments could be made in fractions of a stone
- Salability across space as the stones were accepted for payment everywhere on the island and did not have to be moved physically, just recorded by the townsfolks' individual ledgers (remarkably similar to Bitcoin's distributed ledger model, as we will see later)
- Salability across time due to the durability of stones and the difficulty of procuring new stones which meant that the existing supply of stones was always large relative to any new supply that could be created within a given time period (a high stock-to-flow ratio)

This monetary system worked well until 1871, when an Irish-American captain named David O'Keefe was found shipwrecked on the shores of Yap by the local islanders. Soon, O'Keefe identified a profit opportunity in buying coconuts from the Yapese and selling them to coconut oil producers. However, he could not transact with the locals because he was not a Rai Stone owner and the locals had no use for his foreign forms of money. Undeterred, O'Keefe sailed to Hong Kong and acquired some tools, a large boat and explosives to procure Rai Stones from neighboring Palau. Although he met resistance from them initially, he was eventually able to use his Rai Stones to purchase coconuts from the Yapese. Other opportunists followed O'Keefe's lead and soon the flow of Rai Stones increased dramatically. This sparked conflict on the island and disrupted economic activity. By using modern technologies to acquire Rai Stones more cheaply, foreigners were able to compromise the hardness of this ancient monetary good. The market naturally selected against Rai Stones because, as their stock-to-flow ratio declined, they became less reliable as a store of value and thus lost their salability across time, which ultimately led to the extinction of this ancient monetary system.

A similar story played out in western Africa which for centuries used aggry beads as money. These small glass beads were used in a region where glassmaking was an expensive craft, which gave them a high stock-to-flow ratio and made them salable across time. Since aggry beads were small and light they could easily be combined into necklaces or bracelets and transported easily, thus giving them salability across scales and space. In the 16th century, European explorers discovered the high value ascribed to these beads by the west Africans and began importing them in mass quantities; as European glassmaking technology made them extremely cheap to produce. Slowly but surely, the Europeans used these cheaply produced beads to acquire most of the precious resources of Africa. The net effect of this incursion into Africa was the transference its vast natural resource wealth to Europeans and the conversion of aggry beads from hard money to soft money. Again, the market naturally selected against a monetary good once its stock-to-flow ratio began to decline, as its store of value functionality and, therefore, its salability across time were compromised as a result. Although the details vary, this underlying dynamic of a declining stock-to-flow ratio presaging a good's loss of its monetary role has been the same for every form of money throughout history. Today, we are seeing a similar pattern cause the collapse of the Venezuelan bolivar, (where some Venezuelans are using Bitcoin to protect their wealth as the currency collapses).

As societies continued to evolve, they began to move away from artifact money like stones and glass beads and towards monetary metals. It was initially difficult to produce most metals which kept their supply flows low, thus giving them good salability across time. Gold in particular, with its extreme rarity in the Earth's crust and its virtual indestructibility, made it an extremely hard monetary technology. Gold mining was difficult, limiting supply increases relative to its existing supply, which itself could not be destroyed. Gold gave humans a way to store value across generations and develop a longer-term perspective on their actions (a lower time preference), which led to the proliferation of ancient civilizations:

The earliest coins are found mainly in the parts of modern Turkey that formed the ancient kingdom of Lydia. They are made from a naturally occurring mixture of gold and silver called electrum.

Monetary Metals [1]

The last dictator of the Roman Republic, Julius Caesar, issued a gold coin called the aureus coin which contained a standard 8 grams of gold. The aureus was traded widely

across Europe and the Mediterranean, alongside a silver coin called the denarius, which was used for its superior salability across scales. Used together, these coins provided a hard money system that increased the scope of trade and specialization in the Old World. The republic became more economically stable and integrated for 75 years until the infamous emperor Nero came into power.

Nero was the first to engage in the act of *coin clipping* in which he would periodically collect the coins of his citizenry, melt them down and mint them into newer versions with the same face value but less precious metal content, keeping the residual content to enrich himself. Similar to modern day inflation, this was a way of surreptitiously taxing the population by debasing its currency. Nero and successive emperors would continue the practice of coin clipping for several hundred years to finance government expenditures:

Isaac Newton is attributed with adding the small stripes along the edges of coins as a security measure against coin clipping. These stripes are still present on most coins today.

Citizens gradually wised up to this deceit and began hoarding the coins with higher precious metal content and spending the debased coins, as they were legally required to be accepted at face value in settlement of debts, one of the earliest instances of *legal tender* laws being implemented. This had the effect of driving up the price of coins with higher precious metal content and driving down the price of those with less—a dynamic that came to be known as *Gresham's Law*: bad money (soft money) drives good money (hard money) out of circulation. This is an important law to recall when we look at how modern-day hoarding of Bitcoin impacts its price.

Eventually, a new coin called the solidus was introduced which contained only 4.5 grams of gold, almost half the content of the original aureus coin. Pursuant to this decline in monetary value, a cycle familiar to many modern economies running on government money began to take hold—coin clipping reduced the money's real value, increased the money supply, gave the emperor the means to continue imprudent spending and eventually ended with rampant inflation and economic crisis. Analogous to central bank practices today, Swiss banker Ferdinand Lips summarized this era well:

> *"Although the emperors of Rome frantically tried to 'manage' their economies, they only succeeded in making matters worse. Price and wage controls and legal tender*

laws were passed, but it was like trying to hold back the tides. Rioting, corruption, lawlessness and a mindless mania for speculation and gambling engulfed the empire like a plague."

Amid the chaos of the crumbling Roman Republic, Constantine the Great took power. Intent on restoring the once great empire, Constantine began adopting responsible economic policies. He first committed to maintaining the solidus at 4.5 grams of gold, ended the practice of coin clipping and began minting massive quantities of these standardized gold coins. Constantine then moved east and established Constantinople in modern day Istanbul. This became the birthplace of the Eastern Roman Empire, which adopted the solidus as its monetary system.

Rome continued its soft money-induced cultural deterioration until it finally collapsed in 476 AD. Meanwhile, Constantinople flourished. The solidus, which eventually became known as the bezant, provided a hard money system with which Constantinople would remain prosperous and free for centuries to come. As with Rome before it, the fall of Constantinople happened only when its rulers began the debasing its currency around 1050 AD. As with Rome before it, the move away from hard money led to the fiscal and cultural decline of the Eastern Roman Empire. After suffering many successive crises, Constantinople was ultimately overtaken by the Ottomans in 1453. However, the bezant inspired another form of hard money that still circulates to this day, the Islamic dinar. People all over the world have used this coin for over seventeen centuries—which began as the solidus before changing its name to the bezant and finally becoming the Islamic dinar—for transactions, thus highlighting the superior salability of a hard money such as gold across time.

Following the collapse of the Roman Empire, Europe fell into the dark ages. It was the rise of the city-state (a new story mankind would begin organizing itself around) and its use of hard money systems that would pull Europe out of the Dark Ages and into the Renaissance. Beginning in Florence in 1252, the city minted the florin which was the first major European coinage issued since Julius Caesar's aureus. By the end of the 14th century more than 150 European cities and states had minted coins to the same specifications as the florin. By giving its citizenry the ability to accumulate wealth in a reliable store of value which could be traded freely across scales, space and time, this hard money system unlocked scientific, intellectual and cultural capital within the Italian city-states and eventually spread to the rest of Europe. Of course, the situation was far from perfect, as there were still many periods marked by various rulers choosing to debase their currencies to finance war or lavish expenditure.

Global Gold Standard [1,4]

When they were being used as physical means of settlement, gold and silver coins served complementary roles. Silver, having a stock-to-flow ratio second only to that of gold, had the advantage of being a more salable metal across scales, since its lower value per weight than gold made it ideal as a medium of exchange for smaller transactions. In this

way, gold and silver were complementary as gold could be used for large settlements and silver could be used for smaller payments. However, by the 19th century, with the development of modern custodial banking and advanced telecommunications, people were increasingly able to transact seamlessly across scales using bank notes or checks backed by gold:

The US Dollar was once redeemable for gold on demand.

With all of the critical salability characteristics gathered under a gold standard monetary system facilitated by paper bank notes, the superior salability across scales of physical silver lost relevance, setting it up to become demonetized (due to the winner take all dynamic discussed earlier). Ironically, the same banking industry that enabled a global gold standard would in later years see to its elimination (more on this later).

A brief aside on silver: This demonetization dynamic also explains why the silver bubble popped many times throughout history when facing off with gold and will pop again if it ever reflates. Since silver is not the hardest form of monetary good available, should any significant investment flow into silver, its producers will be incentivized to increase the flow of silver, and store any value expropriated from its increased production in the hardest form of money available to them (which, before Bitcoin, was only gold). This, of course, will bring the price of silver crashing back down, taking the wealth from the investment inflows with it. As a more recent historical example of this dynamic in action: In the 1970s, the affluent Hunt brothers attempted to remonetize silver by buying vast quantities of it in the market. This drove up the price initially, and the Hunt brothers believed they could continue driving up its price until they cornered the market. Their intent was to induce others to chase its appreciation and recreate a monetary demand for silver. As they kept buying and the price kept rising, silver holders and producers kept selling into the market. No matter how much the Hunt brothers purchased, the selling and flow of silver continued to outpace their buying, which decreased its stock-to-flow ratio and eventually led to a dramatic crash in the price of silver. The Hunt brothers lost over $1B (due to rampant inflation of government money since then, their losses equal $6.5B in 2019 dollars) in the ordeal, which is likely the highest price ever paid for learning the importance of hard money and its defining metric, the stock-to-flow ratio.

Driven by expanding telecommunication and trade networks, and with custodial banks enhancing its salability across scales by issuing gold-backed bank notes and checks, the gold standard spread quickly. More nations began switching to paper based monetary systems fully backed by and redeemable in gold. Network effects took hold as more nations moved onto the gold standard, giving gold deeper liquidity, more marketability and creating larger incentives for other nations to join.

Those nations which remained on a silver standard the longest before converting, like China and India, witnessed tremendous devaluations of their currencies in the intervening period. The demonetization of silver for China and India was an effect similar to the west Africans holding aggry beads when Europeans arrived. Foreigners who adopted the gold standard were able to gain control over vast quantities of the capital and resources in China and India. This drives home a key point: every time hard money encounters a softer form of money in a trade network, the softer money is ultimately outcompeted into extinction.

This dynamic has significant consequences for the holders of soft money and is an important lesson for anyone who believes their refusal of Bitcoin means they are protected from its economic impact. History shows us repeatedly that it is not possible to protect yourself from the consequences of others holding money that is harder than yours.

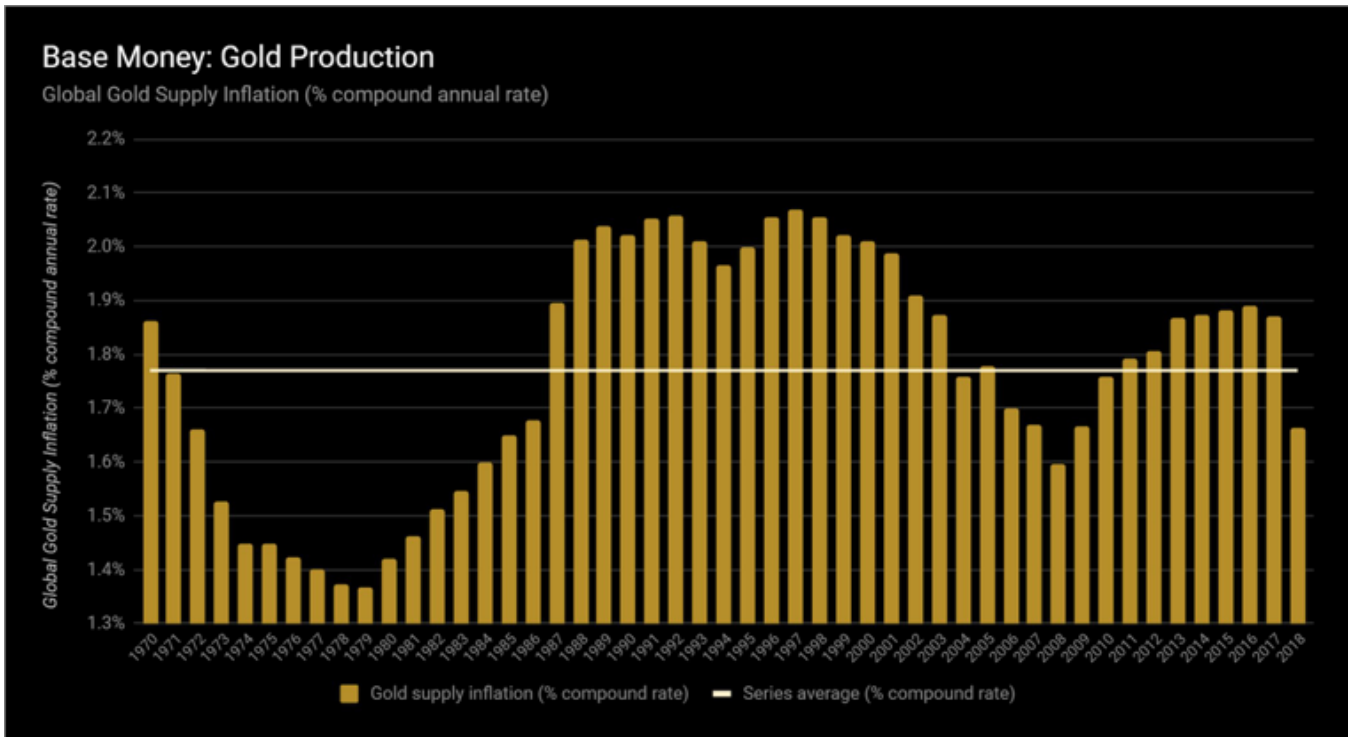
Finally, for the first time in history, the majority of the world economy began operating on a gold-based, hard money standard that was naturally selected for by the free-market.

Hardness of Gold [1,3]

By this point in history, virtually everyone had come to fully trust gold's superior stock-to-flow ratio and therefore believed they could use it to reliably store value across time. After thousands of years of mining this chemically stable element, virtually all the gold ever procured by humans is still a part of its extant supply. The stock of all the gold in the world fits into an Olympic-sized swimming pool today and is valued at almost $8T USD. Gold is rare in the Earth's crust and extraction is costly in terms of time and energy, which keeps its flow predictably low. It is impossible to synthesize gold by chemical means (as alchemy never panned out) and the only way to increase its supply is through mining.

The costliness of gold mining is the *skin in the game* necessary to increase its flow—the risk necessary to procure the reward. Skin in the game is a concept based on symmetry, a balance of incentives and disincentives: in addition to upside exposure, people should also be penalized if something for which they are responsible for goes wrong or hurts others. Skin in the game is the central pillar for properly functioning systems and is at the heart of hard money. For gold, its mining costs and risks form the disincentives which are balanced against the incentives of its market price. Unless consequential decisions are made by people who are exposed to the results of their decisions, the system is vulnerable to total collapse (an important consideration when we discuss soft government money later).

Every market-driven evolutionary step for money has naturally selected the form with the highest stock-to-flow ratio available to its population but stopped when the form lost this key property. With the highest stock-to-flow ratio of all the monetary metals, gold is the hardest physical form of money that has ever existed, which explains its success as hard money throughout history. Even with advances in mining techniques, gold still has a relatively low and predictable flow, as evidenced by its annual supply growth since 1970:



The rarity of gold in the Earth's crust ensures that its new supply flows are relatively low and predictable. Since gold is virtually indestructible, nearly every ounce that has ever been mined throughout history is still part of current supply stocks. The combination of these factors gives gold the highest stock-to-flow ratio of any monetary metal and is precisely the reason gold became a global hard money standard.

Gold mining, of course, only makes economic sense if the cost of producing an additional ounce of gold is less than gold's market price per ounce. Relatedly, when the price of gold increases, its mining becomes more profitable and draws new miners into the market and makes new methods of gold mining economically feasible. This, in turn, increases the flow of gold until supply and demand forces again reach equilibrium. So, although gold is the hardest form of physical money, it doesn't have perfect hardness as changes in demand for it elicit both a supply and price response, meaning:

- An increase in the demand for gold increases its price,
- An increase in the price of gold incentivizes gold miners to increase its flow,
- An increase in the flow of gold increases its supply
- An increase in the supply of gold puts downward pressure on its price

In this way, changes in demand for gold are expressed partially in its price and partially in its supply flow. This *price elasticity of supply* is true for all physical commodities. For all practical purposes, as we will see later, the Earth always has more natural resources to yield assuming the right amount of time and effort are directed towards their production (this will support an important point later when we look at the impact of changes in demand on Bitcoin's price).

Final Settlement [1]

Gold also has the advantage of being an instrument of *final settlement*. Whereas the use of government money requires trust in the monetary policy and creditworthiness of the issuing authority or payment intermediaries, known as *counterparty risk*, the act of physically possessing gold comprises all of the trust factors and permissions necessary to use it as money. This makes gold a self-sovereign form of money. This is best understood as an identity of the universal accounting equation: Assets = Liabilities + Owner's Equity

When you own gold free and clear, it is your asset and no one else's liability, meaning that your personal balance sheet includes a 100% gold asset matched by 0% liabilities and 100% owner's equity (since no one else has a claim on your gold asset). This makes gold a *bearer instrument*, meaning that any individual in physical possession of the asset is presumed to be its rightful owner. This timeless and trustless nature of gold is the reason why it still serves as the base money and final settlement system of central banks worldwide.

In the 19th century, the term *cash* referred to central bank gold reserves, which was the dominant self-sovereign monetary good at the time. Cash settlement referred the transfer of physical gold between central banks to execute final settlement. Central banks can only settle with finality in physical gold, and still do so periodically in the modern era, since it is the only form of money that requires no trust in any counterparty, is politically neutral and gives its holders full sovereignty over their money. This is why gold maintains its monetary role even today as only the delivery of a bearer instrument can truly be the final extinguisher of debt. In this original sense of the word cash, gold is the only form of dominant cash money that has ever existed (although Bitcoin is well-suited to serve a similar role in the digital age, more on this later). Unfortunately, the combination of gold's self-sovereignty and physicality would lead to the demise of the gold standard.

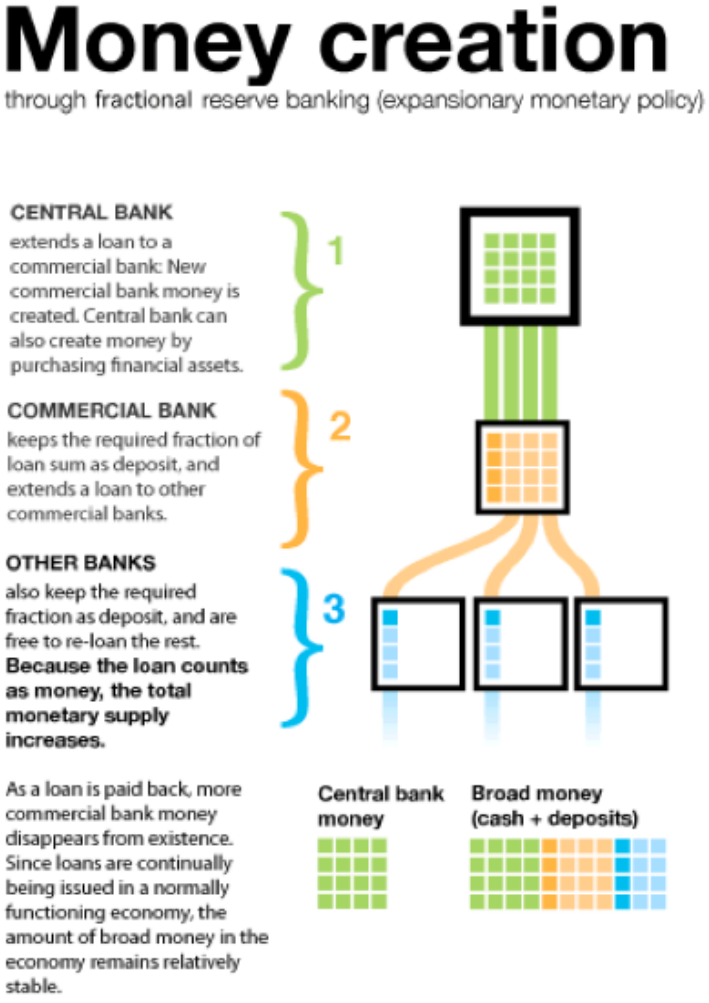
Centralization of Gold [1,4]

By the end of the 19th century, all the industrialized nations of the world were officially on the gold standard. By virtue of operating on a hard money basis, most of the world witnessed unprecedented levels of capital accumulation, free global trade, restrained government and improving living standards. Some of the most important achievements and inventions in human history were made during this era, which came to be known as *la belle époque* across Europe and *the Gilded Age* within the United States. This golden era enabled by the gold standard remains one of the greatest periods in human history:

"La Belle Époque was a period characterized by optimism, regional peace, economic prosperity, an apex of colonial empires, and technological, scientific, and cultural innovations. In the climate of the period, the arts flourished. Many masterpieces of literature, music, theater, and visual art gained recognition."

As multiple societies had now converged on gold as their universal store of value, they experienced significant decreases in trade costs and an attendant increase in free trade and capital accumulation. La Belle Époque was an era of unprecedented global prosperity. However, the hard money gold standard which catalyzed it suffered from a major flaw: settlement in physical gold cumbersome, expensive and insecure. This flaw is associated with the physical properties of gold, as it is dense, not deeply divisible and not easily transactable. Gold is expensive to store, protect and transport. It is also heavy per unit of volume which makes it difficult to use for day to day transactions. As discussed earlier, banks built their business model around solving these problems by providing secure custody for people's gold hoards. Soon after, banks began issuing paper bank notes that were fully redeemable in gold. Carrying and transacting with paper bank notes backed by gold was much easier than using actual gold. Offering superior utility and convenience, the use of bank notes flourished. This, along with government programs to confiscate gold from citizens (such as Executive Order 6102 in the United States), encouraged the centralization of gold supplies within bank vaults all over the world.

Incapable of resisting the temptation of wealth expropriation by tampering with the money supply, banks soon began issuing more notes than their gold reserves could justify, thus initiating the practice of *fractional reserve banking*. This banking model facilitated the creation of money without any skin in the game. Governments took notice and began to gradually take over the banking sector by forming central banks, as this model enabled them to engage in *seigniorage*, a method of profiting directly from the *money creation process*:



In fractional reserve banking artificial money and credit is created. For instance, assuming a reserve ratio of 10% and an initial deposit of $100 will soon turn into $190. By lending a 90% fraction of the newly created $90, there will soon be $271 in the economy. Then $343.90. The money supply is recursively increasing, since banks are literally lending money they don't have. In this way, banks magically transform $100 into over $1,000.

The ability to control this process was too tempting for governments to resist. Total control of over the money supply gave those in charge a mechanism to continually extract wealth from its citizenry. The virtually unlimited financial wealth the printing press provided gave those in power the means to silence dissent, finance propaganda and wage perpetual warfare. It is a fundamental economic reality that wealth cannot be generated by tampering with the money supply, it can only be manipulated and redistributed. Civilization itself relies on the integrity of the money supply to provide a solid economic foundation for free trade and capital accumulation. With a firm grip on the prevailing monetary order established, the next logical step for central banks was to begin moving away from the gold standard altogether.

Abolishing the Gold Standard [1]

By 1914, most of the major economies had begun printing money is excess of their gold reserves at the onset of World War I. Unsurprisingly, this had many negative consequences, some of which were immediate while others came on more slowly. Eliminating the gold standard immediately destabilized the unit of account by which all economic activity was assessed. Government currency exchange rates would now float against one another and become a source of economic imbalance and confusion. This distorted price signals, which would now be denominated in various government

currencies with rapidly fluctuating exchange rates. This made the task of economic planning as difficult as trying to build a house with an elastic measuring tape.

For a world that was becoming increasingly globalized and technologically sophisticated, freely floating currency exchange rates represented a significant step backwards and gave rise to what is commonly called a 'a system of partial barter'. For people to buy goods from other people who lived on the other side of any number of imaginary lines called national borders, they would now be required to use more than one medium of exchange (their own currency and the foreign currency) to complete the transaction. To an extent, this reignited the non-coincidence of wants problem which money was meant to solve in the first place. Today, over $5T ($5,000,000,000,000) of foreign currencies are exchanged daily, forming an annual market valued at over 12 times global GDP. This industry is purely parasitic—it enriches bankers and sucks real value out of society in the form of global trade frictions, market distortions and transaction fees. For this reason, it is excluded from GDP calculations and exist solely because of the inefficiencies caused by centrally controlled capital markets and the absence of a global, politically neutral hard money system. The resultant frictions to global trade fanned the flames of warfare.

Governments Take Control [1,3]

As 20th century wars raged, so did the printing presses. Governments and their central banks continued to grow more powerful with each new bank note printed as their citizens became poorer. The death stroke came when most governments, due to a unilateral decision of President Nixon in United States, finally severed the peg to gold entirely in the 1971. Which brings us to the modern form of dominant money: *government fiat money*. Fiat is a Latin word meaning decree, order or authorization. This is why government money is commonly referred to as fiat money, since its value exists solely because of government decree:

Today, the US Dollar is not redeemable for anything and its value is derived solely from government decree. Paradoxically, people were coerced into adopting soft government fiat money only because of their shared belief in gold as a hard monetary good.

This is an imperative point: it was possession of gold (self-sovereign, hard money) that gave governments the power to decree the value of their fiat money (soft money) in the first place. National governments were only able to achieve "sovereignty" because they drew this power from their possession of gold. Paradoxically, people were coerced into discarding the gold standard and adopting soft government fiat money only because of their belief in gold as a hard monetary good. This is proof that it is possible to create an artificial asset and endow it with monetary properties, whether by decree or by market-driven natural selection. Governments did so by stealing gold from citizens, which gave them the power to create fiat money and decree its value by force. As we will later see, Satoshi Nakamoto did so by creating Bitcoin and releasing it into the marketplace as a self-sovereign money free to compete for the trust and belief of the people based on its own merits.

Central banks also began engaging in propaganda campaigns declaring the end of gold's monetary role. However, their actions rang louder than their words as they continued to accumulate and hold gold, a practice they continue to this day. Gold remains the exclusive instrument of final settlement between central banks. Strategically, holding large gold reserves also makes sense for central banks since they can opt to sell reserves into the market should gold start to appreciate too quickly and threaten the value of fiat money. With their monopoly position protected and reinforced by legal tender laws, propagandists and sufficient control of the gold market central banks were free to print money at will. This exorbitant privilege gives central banks extraordinary power and made them extremely dangerous entities. In the words of former US President Andrew Jackson spoken at the Constitutional Convention in 1787:

> *"I believe that banking institutions are more dangerous to our liberties than standing armies. If the American people ever allow private banks to control the issue of their currency, first by inflation, then by deflation, the banks and corporations that will grow up around them will deprive the people of all property until their children wake up homeless on the continent their fathers conquered. The issuing power should be taken from the banks and restored to the people, to whom it properly belongs."*

Unlike to the flow restrictions associated with gold mining, there are practically no economic restraints preventing a government from printing more fiat money. Since there is virtually no cost associated with producing additional units (no skin in the game), government fiat money is the softest form of money in the history of the world. Predictably, money supplies grew quickly, especially in the heat of warfare. In the past, for societies operating with hard money systems, once the tide of war had shifted in favor of one belligerent over the other, treaties were quick to be negotiated as war is an extraordinarily expensive endeavor. The fiat money printing press, on the other hand, gave governments the ability to tap the aggregate wealth of entire populations to finance military operations by implicitly taxing them via inflation. This provided a more secretive, implicit method of funding warfare than explicit taxation or selling government wartime bonds. Wars began lasting much longer and became more violent. It is no coincidence that the century of total war coincided with the century of central banking:

Table 5.1 Conflicts steadily cost more in human lives

Period	Conflict-related deaths (millions)	World population, mid-century (millions)	Conflict-related deaths as share of world population (%)
Sixteenth century	1.6	493.3	0.32
Seventeenth century	6.1	579.1	1.05
Eighteenth century	7.0	757.4	0.92
Nineteenth century	19.4	1,172.9	1.65
Twentieth century	109.7	2,519.5	4.35

The ability to print unlimited quantities of money gives governments a means to finance military operations by implicitly taxing their citizens via inflation. This provides a more secretive method of funding warfare then explicit taxation or selling government wartime bonds. Resultantly, wars have grown in duration and violence.

As is to be expected, soft government money has an abysmal track record as a store of value. This becomes abundantly clear when we look at its inflationary effects on the price of gold. An ounce of gold in 1971 was worth $35 USD, and today is worth over $1,200 USD (a decrease of over 97% in the value of each dollar due entirely to inflation). Based on these figures, it is easy to see that gold continues to appreciate as its supply is increased less quickly than the supply of $USD (government fiat money). The constantly increasing supply of government money means its currency depreciates continuously, as wealth is stolen from the holders of the currency (or assets denominated in it) and transferred to those who print the currency or receive it earliest. This transfer of wealth is known as the *Cantillon Effect*: the primary beneficiaries from expansionary monetary policy are the first recipients of the new money, who are able to spend it before it has entered wider circulation and caused prices to rise. Generally, this is why inflation hurts the poorest and helps the bankers, who are closest to the spigot of liquidity (the government fiat money printing press) in the modern economy. A centrally planned market for money like this completely contradicts the principles of free market capitalism.

Free Market Capitalism versus Socialism [1]

In a socialist system, the government owns and controls all means of production. This ultimately makes the government the sole buyer and seller of all capital goods in its economy. Such centralization stifles market functions, like price signals, and makes decision making highly ineffective. Without accurate pricing of capital goods to signal their relative supply, demand and relevant market conditions, there is no rational way to determine the most productive allocation of capital. Further, there is no rational way to determine how much to produce of each capital good. Scarcity is the starting point of all economics and people's choices are meaningless without skin in the game in the form of

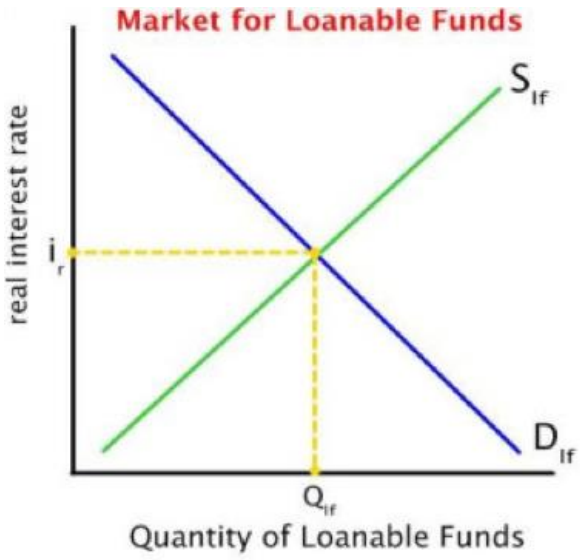
price or trade-offs. A survey without a price would find that everyone wants to own a private island but when price is included, very few can afford to own a private island. The point here is not to trumpet free market capitalism over socialism, but rather to clearly explicate the difference between the two ways of allocating resources and making production decisions:

- Free Market Capitalism places trust in Price Signals
- Socialism places trust in Centralized Planning

A free market is one in which buyers and sellers are free to transact on terms determined solely by them, where entry and exit into the market are free and no third parties can restrict or subsidize any market participants. Most countries today have well-functioning, relatively free markets. However, every country in the world today engages in centralized planning of the *market for money* (aka the market for financial capital) itself.

No country in the world today has a free market for money, which is the most important market in any economy.

In a modern economy, the market for money consists of the markets *loanable funds*. These markets match savers with borrowers using the interest rate as their price signal. In a free market for loanable funds, the supply of loanable funds rises as the interest rate rises, as more people are willing to loan their savings out at a higher price. Conversely, the demand for loanable funds decreases as the interest rate rises, as less people are inclined to borrow funds at a higher price:



In a free market for money, the interest rate (the price of money) is determined by natural supply and demand dynamics. Central banks attempt to "manage" these market forces and in doing so create recessions and the boom-and-bust business cycle which is now considered "normal" in the modern era.

Notice that the interest rate in a free market for capital is always positive because of people's naturally positive time preference, meaning that no one would part with money unless they could receive more of it in the future. These natural market forces are artificially manipulated in every market for money in the world. All markets for money in the world today are centrally planned by central banks, who are responsible for "managing" the market for loanable funds using monetary policy tools. Since banks today also engage in fractional reserve banking, they lend out not only customers' savings, but also their demand deposits (monies available to customers on demand, like checking accounts). By loaning out demand deposits to a borrower while simultaneously keeping them available to the depositor, banks can effectively create new, artificial money (a part of the money creation process from earlier). Central banks have the power to manipulate the market for financial capital and can artificially increase the money supply by:

- Reducing interest rates, which increases demand for borrowing and money creation by banks
- Lowering the required reserve ratios, allowing banks to lend more money out than their capital reserves justify
- Purchasing government debt or other financial assets with newly created money in the open market
- Relaxing lending eligibility criteria, allowing banks to increase lending activities and money creation

In a free market for money, the exact amount of savings equals the exact amount of loanable funds available to borrowers for the production of capital goods. This is why the availability of capital goods, as we saw with Harold and Louis, is inexorably linked to a reduction in consumption. Again, scarcity is the starting point of all economics, and its most important implication is the notion that all decisions involve tradeoffs.

In the free market for money, the opportunity cost of saving is foregone consumption, and the opportunity cost of consumption is foregone saving—an indisputable economic reality.

No amount of centralized planning can alter this fundamental economic reality. This is why centrally planned markets always suffer from distortions (aka bubbles, surpluses or shortages) as political agendas run up against the underlying free market forces. Undeterred, central banks continually attempt to "manage" these market forces to achieve politically established policy goals. Most often, central banks are trying to spur economic growth and consumption, so they will increase the supply of loanable funds and lower the interest rate. With the price of loanable funds (the interest rate) artificially suppressed, producers take on more debt to start projects than there are savings to finance these projects. These artificially low interest rates don't provide any benefit to the economy, rather they simply disseminate distorted price signals that encourage producers to embark on projects which cannot realistically be financed from actual savings. This creates a market distortion (in other words, blows up another bubble) in which the value of consumption deferred is less than the value of the savings borrowed. This distortion can

persist for some time but will inevitably unwind with disastrous consequences as economic reality cannot be fooled for long.

The excess supply of loanable funds, backed by no actual deferred consumption, initially encourages producers to borrow as they believe the funds will allow them to buy all the capital goods necessary for their project to succeed. As more producers borrow and bid for the same amount of capital goods, inflation sets in and prices begin to rise. At this point, the market manipulation is exposed since the projects become unprofitable after the rise in capital good prices (due to inflation) and suddenly begin to fail. Projects like these would not have been undertaken in the first place absent the distortions in the market for money created by central banks. An economy-wide simultaneous failure of overextended projects like this is called a *recession*. The boom and bust *business cycle* we have all grown accustomed to in the modern economy is an inevitable consequence of this centrally planned market manipulation. The United States and Europe saw a great illustration of this process when the dot-com bubble of the late 1990s was replaced by the housing bubble of the mid-2000s.

Free market capitalism cannot function without a free market for money.

As with all well-functioning markets, the price of money must emerge through the natural interactions of supply and demand. Healthy markets require functional nervous systems, as market participants must have accurate price signals to make decisions effectively. Basic economics shows us clearly that central bank meddling in the market for money is the root cause of all recessions and the business cycle. By imposing an artificial price, in this case the interest rate on loanable funds, central banks inhibit natural price signals which coordinate allocation decisions among savers and borrowers. Their market manipulation creates market distortions and recessions. Attempting to remedy a recession by injecting more artificial liquidity into the system will only exacerbate the distortions which caused the crisis in the first place and blow up new bubbles. Only central planning of a soft money supply and its pricing mechanism can cause widespread failures in an economy like this, as an economy based on hard money remains firmly rooted in economic reality and resists market distortions.

Alignment with natural market forces like supply, demand and the price signal is the principal reason free market capitalism prevailed over socialism.

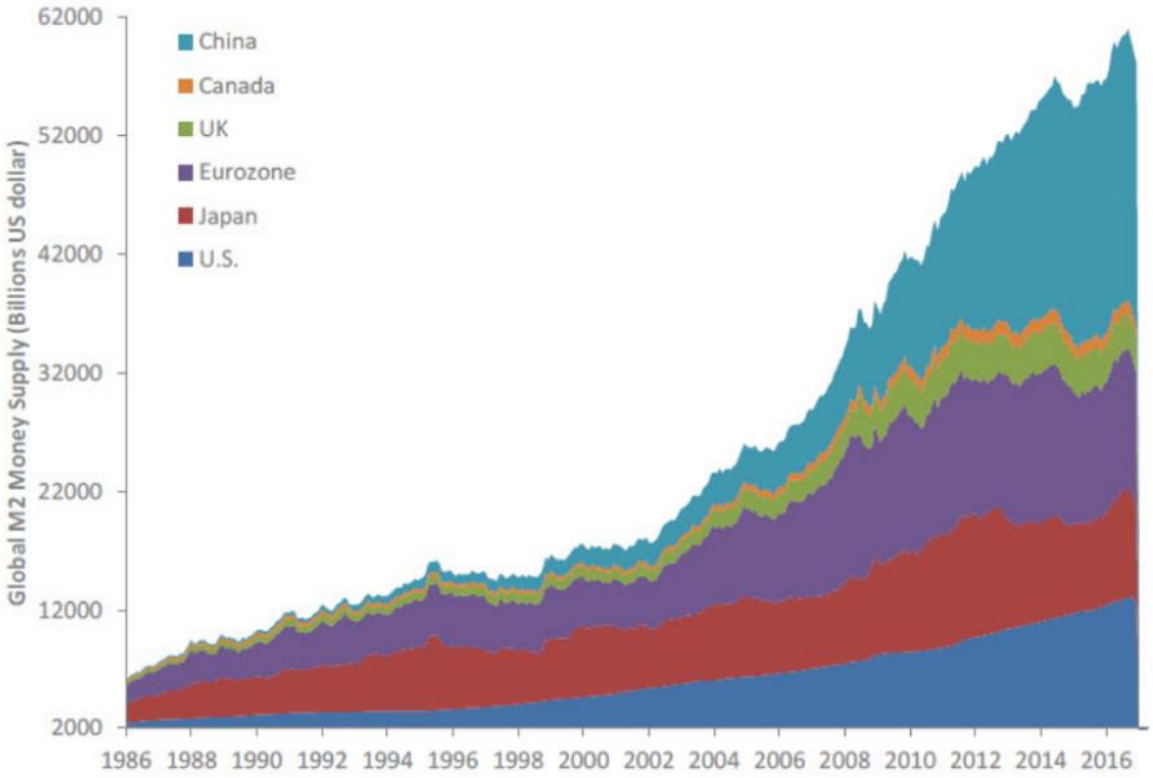
Failure of Government Fiat Money [1,3,4]

Seeing that governments have been forced to use coercive measures, such as confiscating gold and implementing legal tender laws, to enforce adoption of fiat money is a clear indication that soft money is inferior and doomed to fail in a free market. This severe inadequacy of government fiat money came to the forefront of global consciousness in the wake of the Great Recession that began in 2008. Due to gigantic market distortions driven by artificially low interest rates and credit ratings agencies with no skin in the game, US subprime real estate became the largest bubble in modern history.

When it bursts, its affects were globally systemic, and central banks all over the world (predictably) began increasing their money supplies in an attempt to reflate their broken economies.

Instead of calling it what really is, central banks now deceptively refer to the act of printing money as *quantitative easing.* As we have learned, increasing the money supply creates no real economic value, it only causes market distortions and furthers the misallocation of capital. Injecting liquidity into an economic system experiencing a recession only provides illusory, temporary relief. Printing money delays and exacerbates the inevitable correction, as economic reality cannot be deceived forever. Despite economic reality, central bank market manipulation is worse than ever.

Here we show the amount of government fiat money printed by the largest economies of the world since 1986:



Money supply growth by global central banks is accelerated after each recession. This artificial liquidity only provides illusory relief and further distorts the market signals which caused the distortions in the first place.

It was in the depths of the Great Recession that an anonymous individual named Satoshi Nakamoto introduced the open-source software project called Bitcoin to an online group of cryptographers. Many attempts at creating a digital cash had been made over the previous twenty years but none had succeeded. Initially, few in the group took Bitcoin

seriously. However, Nakamoto was eventually able to convince a few other cryptographers to join and the Bitcoin network was born.

After ten years of virtually perfect operation, the Bitcoin network has gone from $0 to $80B in value stored on its network and has cleared $1.38T in total transactions. It is clear that this monetary technology is now competing successfully in the marketplace and is being used by many for real world purposes.

Synthesized Works & Further Reading

- [1] *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] *The Rational Optimist* by Matt Ridley
- [3] *Skin in the Game* by Nassim Nicholas Taleb
- [4] *The Bullish Case for Bitcoin* by Vijay Boyapati
- [5] *The Age of Cryptocurrency* by Paul Vigna and Michael J. Casey
- [6] *Sapiens* by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism, Part 1 and Part 2* by Brandon Quittem
- [8] *PoW is Efficient* by Dan Held
- [9] *The Fifth Protocol* by Naval Ravikant
- [10] *Unpacking Bitcoin's Social Contract* by Hasu
- [11] *Antifragile* by Nassim Nicholas Taleb
- [12] *Letter to Jamie Dimon* by Adam Ludwin
- [13] *Placeholder VC Investment Thesis Summary* by Joel Monegro and Chris Burniske
- [14] *Diffusion of Innovations* by Everett M. Rogers
- [15] *Why America Can't Regulate Bitcoin* by Beautyon
- [16] *Hyperbitcoinization* by Daniel Krawisz

Money, Bitcoin and Time: Part 2 of 3

By Robert Breedlove

Posted January 26, 2019

The Simple Truth about Bitcoin: Bitcoin is the hardest form of money ever invented. It has successfully brought the advantages of physical cash money into the digital realm. Bitcoin is changing the way people organize themselves. The next chapter in the story of money is being written in a new language…

Grasping Bitcoin [7]

Bitcoin seems easy to understand at first (it's just magic internet money, right?), however truly grasping its significance is a formidable task. Once you think you have Bitcoin figured out, you'll see it from another perspective and realize how little you actually knew. This pursuit of understanding Bitcoin is like a mountain climber that continually encounters false peaks, which fool him into thinking he has reached the summit, only to realize it is higher still.

It has been said that you can judge the quality and importance of an idea by the vehemence of its opposition. Bitcoin has been called many things—digital gold, tulip mania 2.0, financial revolution, the MySpace of cryptocurrencies, environmental disaster, rat poison squared, libertarian idealism, apex predator of monetary technologies, the biggest bubble in history, the model-T of cryptocurrencies, a superior species of money—but it turns out that, in context of the history and nature of money, Bitcoin appears to be a distinct evolutionary leap forward. Bitcoin is not an internet application like MySpace, it is an internet protocol. Bitcoin is not the model-T of cryptocurrencies, it is a more like a global freeway system. Bitcoin is not like any type of gold coin, Bitcoin is more like the element gold. Its integrity is protected by the inviolable laws of mathematics. Human nature is one of its core components. It is a new form of social institution. Bitcoin is a living system unto itself that adapts to environmental changes.

This may sound mind blowing at first. Most innovations of this magnitude sound this way in the beginning as we struggle to communicate using outdated terms and analogies that cannot possibly convey their importance. However, history shows us that ignoring innovation is a terrible strategy. In light of its inherent complexity and novelty, we will view

Bitcoin from many different perspectives in an attempt to create a mosaic of understanding in the minds of our readers. First and foremost, Bitcoin is *digital cash money*.

Digital Cash Money [1]

As the global economy becomes increasingly digitized and interconnected, new technological realities are taking shape which will cause the market to naturally select for the most effective species of money native to this new digital terrain. Bitcoin is the first truly digital solution to the problem of money. It is the world's first digital cash (in the original sense of the word cash discussed earlier) meaning that it is under the full control of its owner and can be used for final settlement in the same way as gold is today. Put another way, Bitcoin is digital cash money, a self-sovereign asset that contains within it all the trust factors and permissions necessary to transact with it. Bitcoin is not the liability of any counterparty, hence its nickname—digital gold.

Like gold, Bitcoin is a supranational form of money, meaning that no government needs to decree its value or permit its use, nor can it be eliminated unilaterally by regulation. The hardness of Bitcoin is superior to all forms of money, including gold, and its stock-to-flow ratio will eventually reach infinity. As a digital asset, Bitcoin has unprecedented levels of salability across scales, space and time. It is resistant to confiscation, censorship, inflation and counterfeit. Meritoriously, Bitcoin's value is attained entirely from the social consensus it earns by competing freely in the marketplace.

As one perspective of its monetary significance, Bitcoin can be understood as the successful fusion of the advantages associated with physical cash payments with the efficiencies and certainties enabled by digital technology. Cash payments have the advantage of being immediate, final and requiring no trust from either counterparty in each other nor any other intermediary. The drawback of cash payments was the need for parties to be present in the same space and time, which increases risks associated with physical custody, especially for larger transactions. As more business is conducted remotely, thanks to ever-advancing telecommunications technologies like the internet, physical cash transactions become increasingly impractical.

Since the inception of computers, the nature of all digital objects is that they were infinitely replicable. This meant that no digital object could be provably limited in quantity. For instance, when you "send" and email, you are actually sending a copy, as you still have the email in your sent folder. Before Bitcoin, there was no way to send a digital good that could not also be resent elsewhere at a later time. This presented an intractable issue for direct digital payments known as the *double-spend problem*. Without a trusted third-party intermediary to verify the payer was not double spending, digital payments were not possible. Using intermediated digital payments (like Venmo or PayPal) exposed parties to additional transaction costs, risk of censorship, fraud and transaction disputes.

The nature of digital objects also meant creating a digital cash was impossible, since its monetary units could be reproduced endlessly and would therefore suffer from unlimited

inflation. Before Bitcoin, people had to rely on physical laws (rarity and chemistry, in the case of gold) or jurisdictional laws (government and central bank monopolies) to regulate money supplies. Innovatively, Bitcoin relies on mathematical laws to protect its monetary policy. Building on top of decades of innovative trial and error by other programmers and combining a wide range of proven technologies, Nakamoto successfully made Bitcoins the first digital objects that were verifiably scarce. As the world's first instance of *digital scarcity*, Bitcoin was able to solve the double-spend problem and become the world's first functional digital cash.

"That in order to make a person covet a thing, it is only necessary to make the thing difficult to attain."

— Mark Twain

In this way, Bitcoin would bring the desirous advantages of physical cash to the digital realm and combine them with an immutable monetary policy to inoculate its holders from all unexpected inflation. Drawing on lessons learned by other programmers during two decades of attempts at this innovative breakthrough, Nakamoto finally achieved digital cash money by combining four key technologies:

- Proof-of-Work—mathematical puzzles which require energy expenditure to be solved, solutions are rewarded with newly issued Bitcoin and user transaction fees, functions as the skin in the game necessary to keep Bitcoin's distributed ledger truthful and maintain its monetary hardness
- Distributed peer-to-peer network—a record of Bitcoin's entire transaction history is maintained by each network participant (known as a node) who mathematically verify each other's work, making the entire system resistant to censorship and manipulation
- Hashing—a method of computer cryptography that transforms any stream of data into dataset of fixed size (known as a hash), this transformation is irreversible and is the foundation of trustless verification within the Bitcoin network
- Digital Signatures—a method of authentication that relies on a set of mathematically related elements called the private key, the public key and signatures—the private key (which must be kept secret) allows its holder to control the Bitcoin associated with it, meaning that the private key is a bearer instrument (holding Bitcoin is holding its private key, which makes it a self-sovereign monetary good like gold)

In the same way a monetary assessment of gold would not delve too deep into its chemical properties, this essay will not delve too deep into the technological properties of Bitcoin. We will instead focus on its monetary properties and its relevance in the story of money. However, some basic technical knowledge of Bitcoin is warranted to fully appreciate the importance of the innovation that is digital cash money.

Technological Properties [1]

Bitcoin is *open-source software*, meaning its source code can be inspected by anyone. This makes Bitcoin a language, its source code and transaction history are universally transparent and can even be printed onto paper (interestingly, this makes it protected under the First Amendment in the United States, more on this later). As an open-source software project, Bitcoin is supported by a global network of volunteer programmers. These programmers are self-interested in the sense that they are almost always Bitcoin owners as they are aligned with its purpose philosophically, and therefore stand to gain financially from its expanding network. Their work over the years has greatly enhanced the functionality of the Bitcoin network. However, these programmers are unable to change the rules of Bitcoin (as we will see when we discuss Bitcoin's social contract).

To become a Bitcoin network member, known as a *node*, all that is necessary is to download and run the software on a computer. Once downloaded, the software will enable you to store Bitcoin and transact it with any other node in the world. Also, by becoming a node, the entire Bitcoin transaction history will be recorded on your machine and updated in perpetuity, just as it is on every other node in the world. This is the essence of Bitcoin's *decentralized architecture*. The Bitcoin network, similar to the internet, lives *everywhere and nowhere*.

Owning a Bitcoin means owning the private key that can authorize it to be used in a transaction. The private key is purely informational, meaning that it is just a string of alphanumeric characters. This makes it a self-sovereign form of money, giving its holder the presumption of rightful ownership, which makes Bitcoin an instrument of final settlement (like gold). Bitcoin is the world's first global, digital final settlement system.

Bitcoin is entirely reliant on verification, which allows its users to completely eliminate any need for trust. All Bitcoin transactions are recorded by every node on the network so that they all share one common ledger of balances and transactions (remarkably similar to the Rai Stone system used by the Yap Islanders). Transactions are grouped together approximately every ten minutes in what is known as a *block*. Each block is then added to the previous block of transactions, forming a chronological chain of inextricably linked blocks that stretches all the way back to the genesis block mined by Nakamoto himself exactly 10 years ago today. This is commonly called the Bitcoin *blockchain*. The blockchain is the common ledger of which each node maintains its own copy (commonly known as the distributed ledger). Each node verifies the accuracy of every other node's transaction inputs and truth is established by consensus. In this way, the Bitcoin network relies 100% on verification and 0% on trust. This gives Bitcoin the unique property of *trustlessness*, meaning it is able to operate successfully without the need to trust any counterparty or intermediary whatsoever.

Blockchain, Energy and Mining [1,3,8,11]

Economic incentives and disincentives are used to maintain truthful records in the blockchain, it what is an ingenious application of the skin in the game concept. Nodes compete to solve complex mathematical puzzles in a process called *proof-of-work*. Nodes are incentivized to perform this computing task because the first one to solve the proof-of-work is awarded a batch of newly issued Bitcoin and the transaction fees generated within the latest block of transactions—called the *block reward*. A block is sealed approximately every ten minutes, which triggers the opening of the next block and proof-of-work competition. Nodes expend processing power (in the form of electricity) to solve these complicated mathematical problems, although considerably less and much more efficiently than the systems that support gold and government money today:

	Annual Cost ($USD)	Energy Consumption (GJ)	$USD per GJ
Gold Mining	$ 105,000,000,000	475,000,000	$ 221
Gold Recycling	$ 40,000,000,000	25,000,000	$ 1,600
Government Fiat Money Production	$ 28,000,000,000	39,000,000	$ 718
Banking System	$ 1,870,000,000,000	2,340,000,000	$ 799
Governments	$ 27,600,000,000,000	5,861,000,000	$ 4,709
Bitcoin Mining	$ 4,500,000,000	183,000,000	$ 25

Bitcoin mining is exceptionally energy efficient relative to other monetary systems and their institutions.

Proof-of-work energy expenditure is the thermodynamic bridge from the physical to the digital world. It transmutes the fundamental commodity of the universe, energy, into digital gold. This energy expenditure is essential to the functioning of the Bitcoin network, as it disincentivizes node dishonesty. If a node attempted to include a fraudulent transaction in a block, other nodes would reject it and it would incur the cost of processing power without the prospect of earning the block reward. This process is commonly referred to as *mining* and the competing nodes are called miners (or mining nodes). Mining is a truly capitalistic voting mechanism where energy expended equals hashes, which are votes for the proof-of-work solution, generated. The name mining is an ode to the arduous process of mining of gold. As we have learned, the costs and risks related to the mining of this monetary metal is necessary for it to maintain its hardness (skin in the game). Similarly, mining using proof-of-work is the only known method of creating digital cash money.

Money, which is the representation of the work required to generate goods, can also be considered a form of stored energy. In the early 20th century, free market proponents like Henry Ford and Thomas Edison were interested in replacing gold or the US dollar with an energy money. Showing great prescience, they foresaw the day when the world may exhaust its non-renewable energy sources and be forced to switch to alternatives. Convicted in their free market beliefs, they shared this idea and assumed a great deal of reputational risk in the process, as their views ran contrary to the established economic order. The concept of energy money was popular due to its hard money characteristics, as

energy is costly to produce. However, energy money was technologically well before its time, as energy could not be transmitted or stored easily using technologies of the day. In championing a novel idea with the greater good at heart, Ford and Edison were exhibiting *soul in the game*, or the exposure to downside risks on behalf of others. As Edison said in 1931:

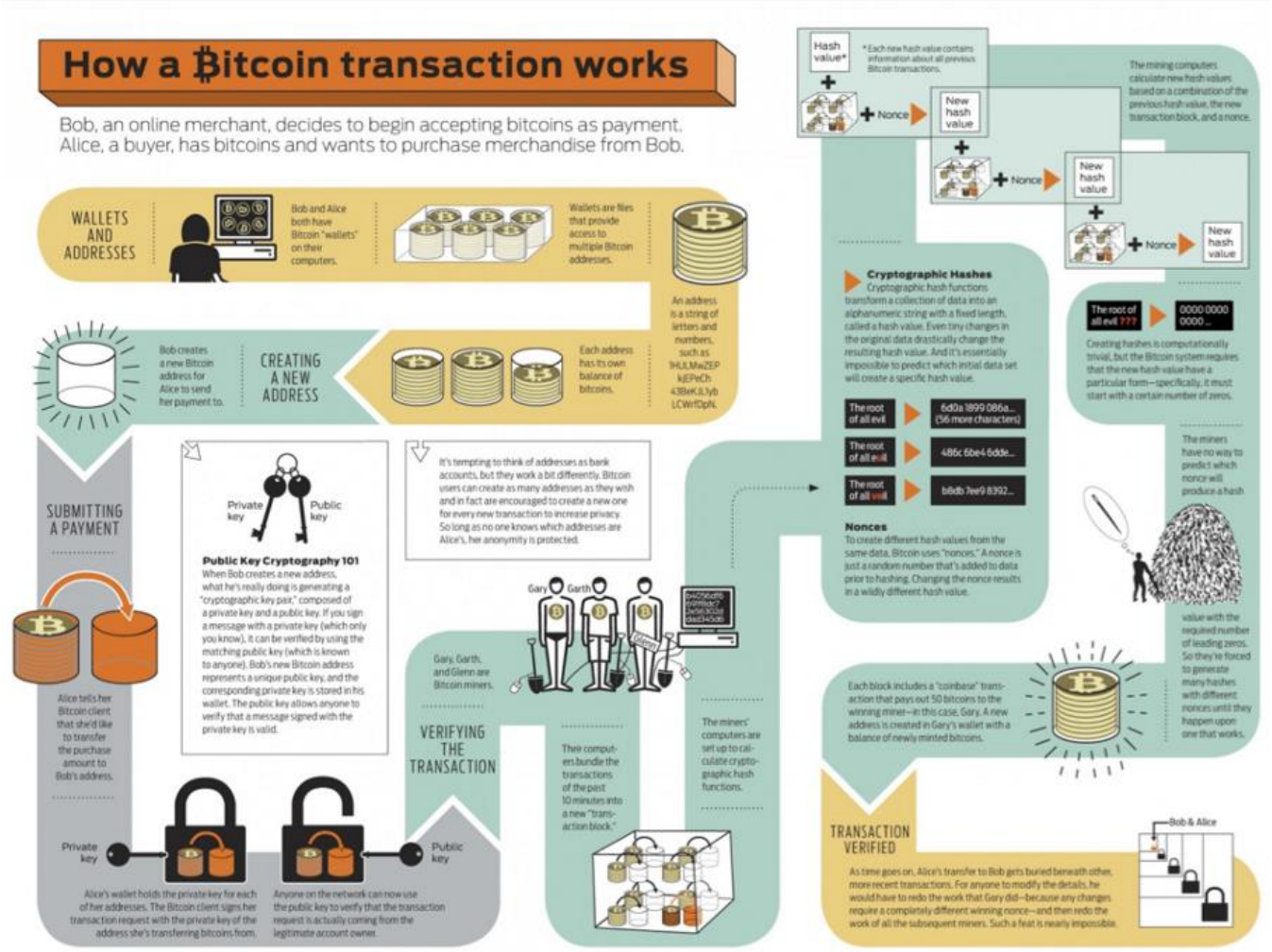
> *"I'd put my money on the sun and solar energy. What a source of power! I hope we don't have to wait until oil and coal run out before we tackle that."*

By using proof-of-work, which was originally invented as a measure to mitigate email spam, Bitcoin became the world's first functional energy money. With physical monetary goods, we were required to build walls to safeguard our money. With the Bitcoin network, we are required to expend energy to preserve the sanctity of its ledger, secure its network and enforce the immutability of its money supply. Proof-of-work is essential for Bitcoin to function as hard, digital cash money and enables it to serve as the buyer of last resort for electricity worldwide. The Bitcoin network provides a perpetual economic incentive for everyone in the world to invent more efficient methods of harnessing energy. This global incentive will increase the rate of innovation in energy technologies. As Bitcoin expert Nic Carter puts it:

> *"The Bitcoin network is a global energy net that liberates stranded assets and makes new ones viable. Imagine a 3D topographic map of the world with cheap energy hotspots being lower and expensive energy being higher. I imagine Bitcoin mining being akin to a glass of water poured over the surface, settling in the nooks and crannies, and smoothing it out."*

As more nodes compete to solve the proof-of-work puzzle, the difficulty automatically increases so that new blocks are added on average once every ten minutes. This automatic algorithmic change is called the *difficulty adjustment* and is perhaps the most ingenious aspect of Bitcoin. It is the most reliable engineering solution for making and keeping money maximally hard and gives Bitcoin the unique ability to adapt its network security as it grows. As we have seen, when a form of money appreciates, people are immediately incentivized to increase its new supply flow, which reduces its stock-to-flow ratio and compromises its hardness. With Bitcoin, an increase in its price does not lead to the production of more Bitcoin beyond its transparent and predictable supply schedule. Instead, it simply leads to an increase in processing power committed by miners which in turn makes the network more secure and difficult to compromise. Like a vault that becomes harder to crack the more money that is stored within it, Bitcoin offers people an incredibly effective means of value storage.

Next, we depict the entire process of a Bitcoin transaction:



The Internet of Value [9]

"The internet of value" is a popular moniker to describe Bitcoin. In reality, the Bitcoin *protocol* can be considered an integral and newly evolved layer of the commercial internet. In computer science, a protocol is a ruleset that governs the transmission of data. The internet as we know it is an integration of four successive layers of open-source protocols, called the Internet Protocol Suite, that maintain constant communication with one another:

- The Link Layer puts data packets on the wire
- The Internet Layer routes data packets across networks
- The Transport Layer persists communication across any given conversation
- The Application Layer delivers software files and applications

In this context, Bitcoin can be considered the fifth layer of the internet protocol suite:

- The Value Layer allocates scarce resources across networks

In the same way the internet is a set of open-source protocols for exchanging data, Bitcoin is an open-source protocol for exchanging value. It is trustless, as any machine can accept it from any other securely and at virtually zero cost. Bitcoin is also global and *permissionless*, meaning that any machine can speak its language and no central bank is required to authorize its use. This means that transactions on its network are essentially unstoppable as all trust factors and permissions necessary to transact with it are intrinsic to the act of holding a Bitcoin private key. Software protocol developments are being implemented that will make Bitcoin transactions even faster, cheaper, anonymous and capable of authentication. These can expand the utility of Bitcoin to enable the allocation of scarce network resources like computing power, verification of contracts or tracking identity and reputation.

Although Bitcoin is the fifth layer of the internet protocol suite, it is the base layer protocol for the value layer itself. This means that second and other higher order protocol layers may be built on top of it. A second layer protocol to Bitcoin, called the Lightning Network, is currently being implemented and is designed to sacrifice some degree of trustlessness to achieve higher transaction throughput, allowing Bitcoin to be used more effectively as a medium of exchange. The Lightning Network is an open-source protocol and functions by establishing trust channels among parties for faster, cheaper transactions that are then settled periodically to the Bitcoin blockchain. Higher order protocol development and integration is one of the many ways Bitcoin adapts to changes in its environment (more on this later).

In the same way that money is an emergent property of complex human interactions, Bitcoin is an emergent property of complex interactions occurring between people, machines and markets. Even if Nakamoto and Bitcoin never existed, it would still be necessary for us to invent the concept of cryptoassets to enable machines to exchange value to facilitate digital economies, use smart contracts and provide the substrate necessary for the 'internet of things' to come into existence. Not only is Bitcoin a prerequisite innovation to the digital economy, it is also the hardest monetary technology ever invented.

The Infinite Hardness of Bitcoin [1]

Bitcoin is the hardest form of money in existence. Its money supply is enforced mathematically and, like the other rules of Bitcoin, cannot be broken or changed. Only 21 million Bitcoins can and will ever exist:

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

The monetary policy of Bitcoin is set in (mathematical) stone.

This strictly limited supply makes it the first monetary technology exhibiting *absolute scarcity*. Unlike gold and other monetary metals, no matter how much demand for Bitcoin increases there will never be any units produced in excess of its fully transparent, predictable and unchangeable monetary policy.

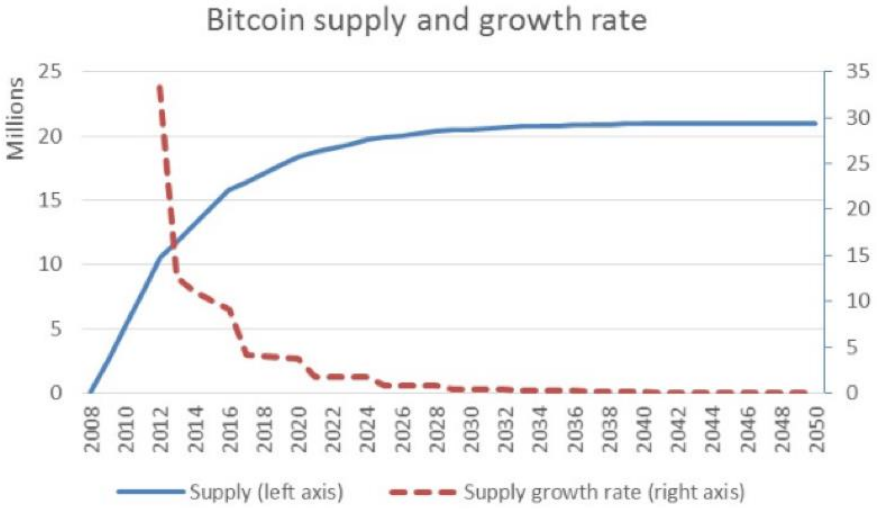
Before Bitcoin, only time itself had achieved the property of absolute scarcity.

Since increased demand for Bitcoin cannot affect its supply, it can only be expressed in its price. Bitcoin has perfect *price inelasticity of supply*, meaning that it has zero supply-side response to increases in its price. Unlike gold and all other physical commodities, where an increase in demand will inevitably lead to larger supplies being produced over time, Bitcoin can only express an increase in demand by becoming more expensive (and a more secure network). A perfect price inelasticity of supply no doubt contributes to the notorious price volatility of Bitcoin it is exhibiting at the earliest stages of its growth we are witnessing today.

Absolute scarcity greatly exacerbates Bitcoin's price volatility. As its network continues to grow, the value of Bitcoin as an unstoppable payments channel and uninflatable money is steadily increasing over time while its price is constantly attempting to find it, dramatically overshooting and undershooting along the way. With a totally inflexible supply schedule, as long as Bitcoin is growing quickly, its price will behave like that of a startup company stock undergoing meteoric growth. Should Bitcoin achieve sufficient market penetration that its growth slows down, it would stop attracting high-risk investment flows and become a stable monetary asset expected to appreciate slightly each year as demand increases due to productivity and population growth—like any mature hard money should. As expected, over the long-run we are already seeing a decrease in Bitcoin's price volatility:

As expected, the price volatility of Bitcoin is gradually declining as its network value grows.

Bitcoin's immutable monetary policy ensures that its supply will continue to grow at a decreasing rate and will reach its maximum of 21 million units sometime in the year 2140. To maintain salability across scales, Nakamoto designed each Bitcoin to be further divisible into 100 million units, which are now commonly called Satoshis in his honor. Once the last Bitcoin is mined, its stock-to-flow ratio will become infinite as its flow will completely and irreversibly cease. Beyond this point, miners will be compensated exclusively by transaction fees. Bitcoin's decreasing growth rate means that the first 20 million coins will be mined by the year 2025, leaving the last 1 million to be mined over the subsequent 115 years:

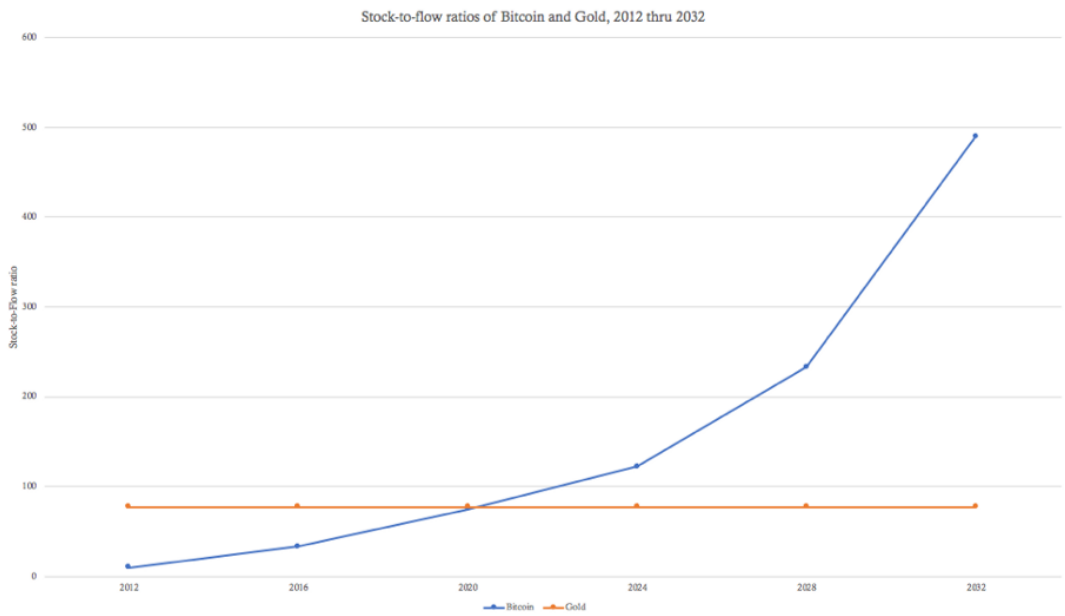


Due to its decreasing supply growth rate, over 95% of all Bitcoins will be mined by the year 2025.

This predictable, transparent and immutable supply schedule gives Bitcoin a significant advantage as it competes for the trust of the people to become a reliable store of value. Unlike government money or even gold, people know with absolute certainty that Bitcoin will never have its salability across time compromised by unexpected supply increases.

Bitcoin is uninflatable money in a world where wealth is continuously stolen via inflation.

As is the case with its other immutable laws, Bitcoin's monetary policy is enforced by the inviolable laws of mathematics. Inevitably, Bitcoin will surpass gold around the year 2020 to become the hardest form of money in history:



As sure as 1+1=2, Bitcoin will soon surpass gold to become the hardest form of money in history.

By virtue of its natively digital nature, Bitcoin is (critically) highly resistant to centralization. As we have learned, it was the centralization of gold that led to government money backed by gold, which made gold more salable across scales and encouraged a gold standard to flourish throughout most of the world. However, as the temptation to expand money supplies seems to be irresistible for humans, governments soon took control of the banking sector, printed money in excess of its gold reserves, eventually severed their currencies peg to gold and thereby destroyed the hardness of government money completely.

Historically, people who adopted hard money systems flourished—such as the Romans under Caesar, The Byzantines under Constantine and the Europeans under the gold standard—and people who had the hardness of their money compromised suffered enormous consequences—such as the Yap Islanders, West Africans using glass beads and the Chinese under a silver standard in the 19th century. Moving a society away from a hard money system has been a harbinger of economic crisis and societal decay, an outcome that can be explained as a social contract rescission.

Bitcoin's Social Contract [10]

Social contract theory starts with an assumed hypothetical state of nature full of violence that is unbearable for people to live in. Driven by a desire to improve their circumstances, people come together and collectively agree to sacrifice some of their freedoms to establish a *social contract* and empower an institution to protect them. Government is the result of a social contract: people sacrifice some of their freedoms to give the state control over the monetary system and armed forces. The state, in turn, uses that power to manage

the economy, redistribute wealth and fight crime. In the United States, our current social contract grants the government monopoly control of money (via the Federal Reserve) and violence (via the Police and Military).

Similarly, money itself can be thought of as a social contract. If enough people are unhappy with a barter economy, they can collectively agree to use money instead. This social contract entails sacrificing certainty (requiring trust that dollars will maintain their value over time) in exchange for convenience (using dollars as a medium of exchange). The social contract for money, as we have seen, emerges and evolves spontaneously based on market-driven natural selection. Each person continuously decides which outcomes they prefer and how best to achieve them. If enough people seek the same outcome, we call the result a social contract.

Throughout history, almost every government (a form of social contract) put in charge of the monetary system (another, often interrelated, form of social contract) has abused its power by forcibly confiscating assets, censoring private transactions and printing money to steal wealth via inflation. Using the virtually unlimited financial means provided by control over money supplies, these governmental social contracts grew in successive bureaucratic layers. The larger and more valuable these social contracts became; the more freedoms were forfeited and the more others sought control over them. This led to many instances of conflict (warfare or social revolution) in which old social contracts (dictatorships or tyrannical regimes) were rescinded in favor of new ones (new laws, treaties or governments). The principal point here is that people can agree they are in a terrible situation and come together to change it, but the resultant social contract is only as strong as its credibility and enforceability.

The invention of Bitcoin can be regarded as a new implementation of the social contract for money. Nakamoto settled on the following rules for this new implementation:

- Only the owner of a Bitcoin can produce the digital signature to spend it (confiscation resistance)
- Anyone can transact and store value in Bitcoins without permission (censorship resistance)
- There will only be 21 million Bitcoins, issued on a predictable schedule (inflation resistance)
- Anyone will always be able to verify all the rules of Bitcoin (counterfeit resistance)

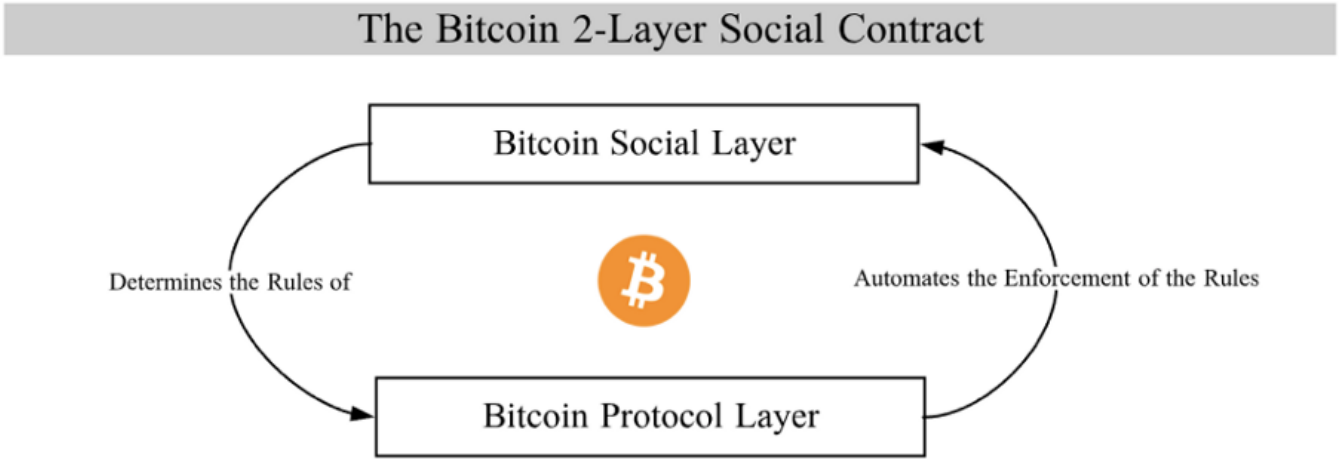
Historically, social contracts intended to protect people, such as governments and their central banks, eventually became controlling and ultimately turned abusive. When a social contract loses sufficient trust of the people, it falls apart or is overthrown, by ballot or by bullet. This dynamic has resulted in a continuous cycle of rising and falling social contracts throughout history. Bitcoin is intended to break this cycle in two ways:

- Instead of seeking security from a powerful central entity (like a government or central bank) that can be corrupted or overthrown, Bitcoin creates a

hypercompetitive market for its own protection. It turns security into a commodity and the security providers (miners) into harmless commodity producers.

- By requiring its security market participants (miners) to incur real world costs to generate their economic reward (skin in the game), Bitcoin incentivizes the market to reach consensus over who owns what at any given point in time.

In this sense, the Bitcoin social contract is composed of two distinct, self-reinforcing layers: the social layer and the protocol layer. The social layer is the social consensus itself, which determines the rules of Bitcoin and establishes its value. The protocol layer simply automates the enforcement of the rules set by the social layer:



In this sense, Bitcoin is more than just a technology. Indeed, it is a new institutional form. Viewing it in this way, we are better able to answer some of the more existential questions about Bitcoin:

Who Can Change the Rules of Bitcoin?

Since the rules of the Bitcoin social contract are decided at its social layer and enforced at its protocol layer, who can actually change its rules? Bitcoin, as computer network, comes into existence when people run implementations that follow the same ruleset (think of these rulesets as speaking the same language). You remain in the network by following the same rules as everyone else. If you decided to change the ruleset on your local computer, you would simply be evicted from the network (you no longer speak the same language as everyone else). Your unilateral decision to change the rules would not impact the actual Bitcoin network in any way whatsoever.

The only way to change the rules of the Bitcoin social contract is to convince people to voluntarily accept your proposed rule changes at the social layer. As each network member is self-interested, they will only adopt rules that benefit them. Seeing as its current rules are already optimal for Bitcoin holders (resistance to confiscation, censorship, inflation and counterfeit) it would be extremely difficult to convince a majority of the

approximately 30 million network participants to change rulesets. This asymmetrical governance dynamic virtually rules out any contentious changes from succeeding, as they would never get broad social consensus. Therefore, the Bitcoin network can be upgraded in ways that align with the collective best interests of its members and is at the same time highly resilient to changes that contradict these interests.

Can a Software Bug Kill Bitcoin?

In September 2018, a software bug arose in the main implementation of Bitcoin that opened up two potential attack vectors which theoretically could have been exploited to circumvent its counterfeit and inflation resistance properties. Bitcoin developers quickly fixed the bug before either vector was exploited, however this event left many people wondering what would have happened had the vulnerabilities not been discovered in time.

Any time the social layer and protocol layer diverge in the Bitcoin social contract, the protocol layer is always wrong. Again, all rules are set at the social layer whereas the protocol layer is only responsible for automating their enforcement. Had the software bug not been discovered in time, Bitcoin's blockchain would have undergone a *fork*—meaning its protocol layer would have been split it into two networks, one with the bug and one without it. Every Bitcoin holder would then have an equal number of coins in each network, but the value of these coins would be determined solely by the free market. This is true for all forms of money, as social consensus determines the value of money. At the social layer, each Bitcoin owner would then choose either the implementation with or without the bug. To protect the value of their Bitcoin, holders would rationally choose to migrate to the mended network and its blockchain would continue without interruption.

When the Bitcoin protocol layer successfully automates the enforcement of the rules determined at its social layer, the two layers are in sync. If they diverge for any reason, the social layer supersedes, and the protocol layer is mended to reflect the economic reality of the social consensus surrounding Bitcoin. Software bugs are inevitable, and Bitcoin's 2-layer social contract construction ensures that it can withstand them.

Can Forks Compromise the Immutability of Bitcoin's Rules?

Since Bitcoin is open-source software, anyone in the world can copy its code, change it and launch their own version. This is also a chain fork which, as established earlier, affects only the protocol layer of the Bitcoin social contract. Without changing the rules at the social layer first, a protocol layer fork only evicts you from the true Bitcoin network. To successfully change the rules of Bitcoin, you must successfully fork its social layer first. To accomplish this, you would need to convince as many people as possible that your proposed ruleset is meaningfully better for them, so that they take the risk of adopting your proposed software changes. Forks like these are difficult to pull off in reality because they require buy-in from thousands of people to be successful. This asymmetry between the cost of campaigning for ruleset changes and their potential benefit to network participants makes the Bitcoin network exhibit an extremely strong status quo bias when it comes to governance.

The key to understanding this is that the value of any form of money is purely a social construct or, in other words, is derived from social consensus. Individual Bitcoins, like US dollars or any other currency, receive their value exclusively from the shared belief of their users. Forking Bitcoin's protocol layer is worthless without forking the social layer from which it derives its value. In the rare cases that the social layer itself splits, as was the case with the Bitcoin Cash fork, the result is two weaker social contracts, each agreed upon by fewer people than before. The complete failure of the Bitcoin Cash fork (its price has declined from 0.21 to 0.04 Bitcoin over the past year) is yet another battle scar for Bitcoin that pays testament to its governance model and exemplifies the winner take all dynamics inherent to monetary competition.

So long as Bitcoin network participants continue to act in accordance with their own individual self-interest, the rules of Bitcoin (resistance to confiscation, censorship, inflation and counterfeit) are immutable and, therefore, as reliable as the laws of mathematics. It's clear from this perspective that Bitcoin is more than just a technological innovation. Although Bitcoin as a network and monetary technology is groundbreaking in many respects, its social contract implementation is revolutionary. Bitcoin is the first technology that incorporates human nature as one of its core moving parts.

In essence, by believing that mathematics and individual self-interest will persist, we can reliably believe in Bitcoin's value proposition and its ongoing successful operation.

Over the past 10 years, by inventively aligning human self-interest with its own self-interest, the Bitcoin network has managed to grow organically from $0 to $80B in value.

A New Form of Life [1]

Although Bitcoin is intended to be a monetary technology, it is a totally unique compared to other forms of money. Ralph Merkle, famous cryptographer and inventor of the Merkle tree data structure, has a remarkable way of describing Bitcoin:

> *"Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because if any one copy is corrupted it is discarded, quickly and without any fuss or muss. It lives because it is radically transparent: anyone can see its code and see exactly what it does.*
>
> *It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. It can't even be interrupted.*
>
> *If nuclear war destroyed half of our planet, it would continue to live, uncorrupted. It would continue to offer its services. It would continue to pay people to keep it alive.*

The only way to shut it down is to kill every server that hosts it. Which is hard, because a lot of servers host it, in a lot of countries, and a lot of people want to use it.

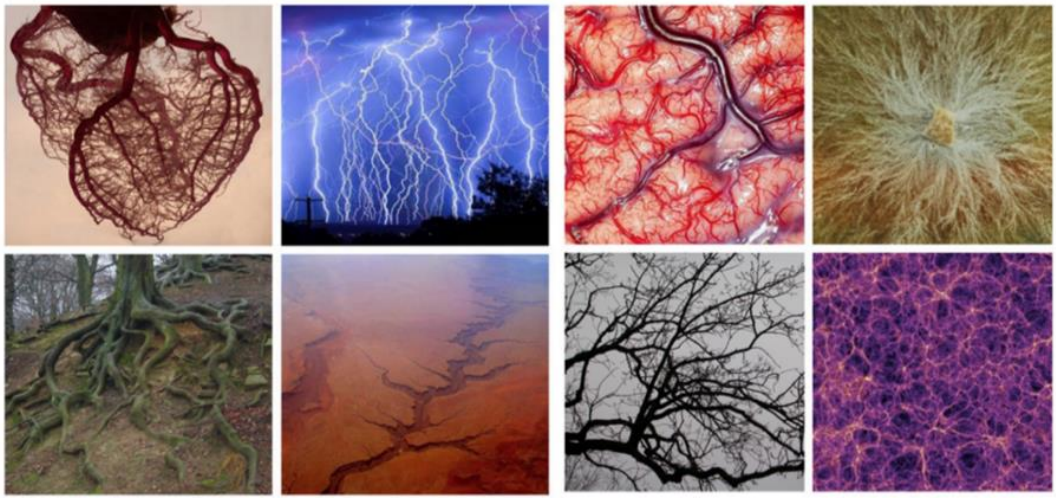
Realistically, the only way to kill it is to make the service it offers so useless and obsolete that no one wants to use it. So obsolete that no one wants to pay for it, no one wants to host it. Then it will have no money to pay anyone. Then it will starve to death.

But as long as there are people who want to use it, it's very hard to kill, or corrupt, or stop, or interrupt."

Bitcoin is a technology, like the hammer or the wheel, that survives for the same reason any other technology survives: it provides benefits to those who use it. It can be understood as a spontaneously emergent protocol that serves as a new form of uninflatable money and an unstoppable payments channel. Structurally, the Bitcoin network reflects a quintessential manifestation commonly found in nature.

The Decentralized Network Archetype [7]

The Bitcoin network mirrors one of the most successful evolutionary structures found in nature, the *decentralized network archetype*:



Clockwise from the top left: the human heart, lightning, the human brain, a fungal mycelium network, roots from a tree, an aerial view of the Grand Canyon, branches from a tree and a cosmic web of galactic superclusters in the deep Universe (which is the largest observable structure in the known Universe at over 1 billion lightyears across).

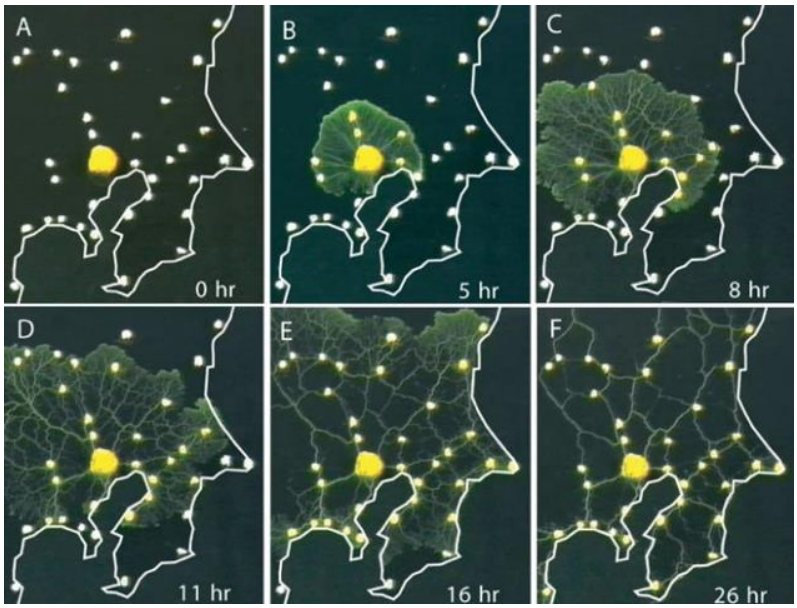
The decentralized network archetype is prevalent in nature because it is one of the most energy efficient structures possible. Energy is the fundamental commodity of the universe and nature always optimizes for its utilization. Atoms, bubbles and stars (in a state of

equilibrium) always form spherical shapes, which is the most energy efficient form for minimizing surface area, precisely because they are energy conservation structures. Minimal surface area output per unit of energy input ensures that these structures optimally expend the finite energy of which they are composed. Spheres are figures of equilibrium with equal distribution their own inherent energy.

Conversely, decentralized networks always form in these tendrilled, circuitous and redundant shapes, which is the most energy efficient form of maximizing surface area, precisely because they are energy exchange structures. Maximal surface area output per unit of energy input ensures that these structures achieve the highest degree of spatial exposure to optimize the likelihood of successful exchange—whether their purpose is pumping blood, imbibing groundwater or seeking sunlight. Spheres and decentralized networks are antithetical in purpose and archetype. Decentralized networks are figures of disequilibrium which both disperse and gather energy within their environments. A decentralized form in organic systems confers advantages such as distributed intelligence, invulnerability to singular attack vectors and accelerated adaptivity.

The decentralized network archetype found in nature is the antecedent to paradigm shifting innovations throughout history such as the railroad system, the telegraph, the telephone, the power distribution grid, the internet, social media and now Bitcoin.

To illustrate the power of this natural archetype, let's consider the story behind the design of the Tokyo subway system. Scientists conducted an experiment where an ancient fungus, the slime mold, was incentivized to recreate the Tokyo subway system. Each subway stop (node) was marked with oat flakes, the favorite food of the slime mold. In a single day, the slime mold grew to connect all the subway stops in a more energetically efficient design than that proposed by the central planning committee of engineers who spent many months at great expense to the Japanese government in the design process:



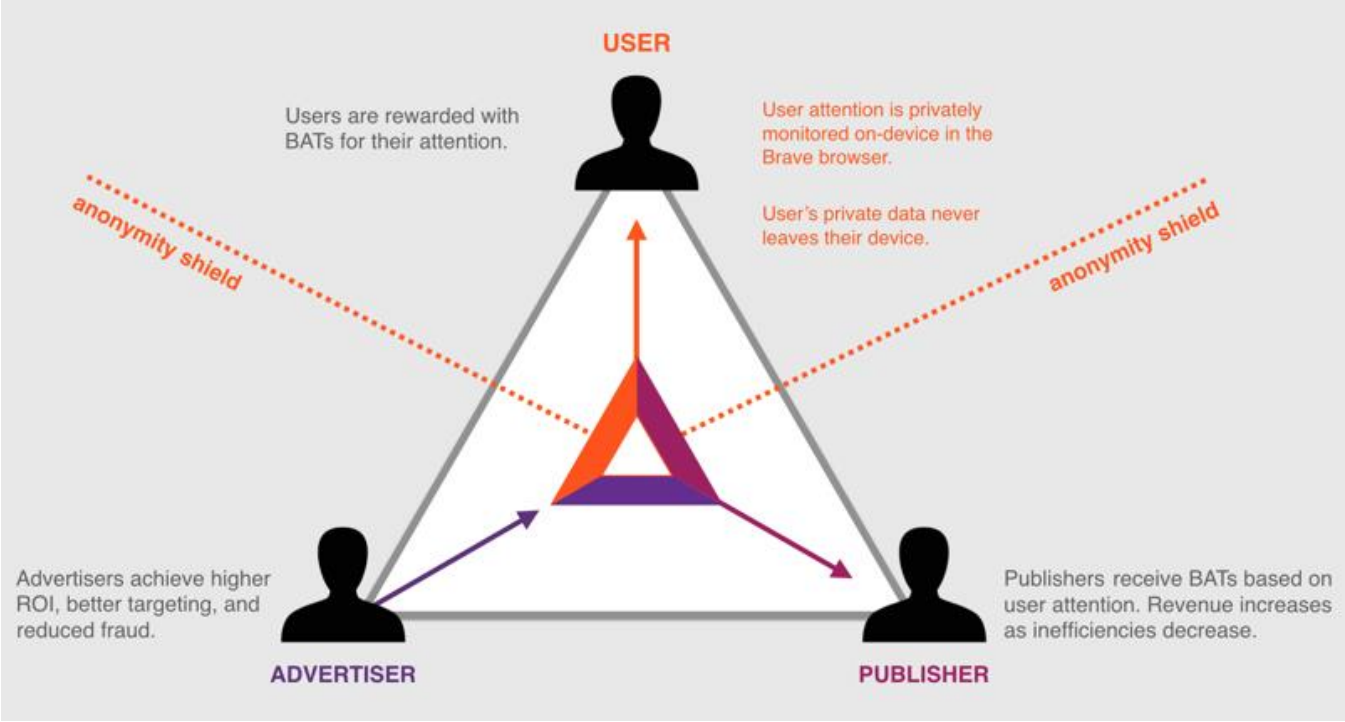
As the Scientists later reported:

> *"Transport networks are ubiquitous in both social and biological systems.* ***Robust network performance involves a complex trade-off involving cost, transport efficiency, and fault tolerance. Biological networks have been honed by many cycles of evolutionary selection pressure and are likely to yield reasonable solutions to such combinatorial optimization problems. Furthermore, they develop without centralized control and may represent a readily scalable solution for growing networks in general.*** *We show that the slime mold Physarum polycephalum forms networks with comparable efficiency, fault tolerance, and cost to those of real-world infrastructure networks—in this case, the Tokyo rail system. The core mechanisms needed for adaptive network formation can be captured in a biologically inspired mathematical model that may be useful to guide network construction in other domains."*

In a similar vein, Bitcoin and its network participants receive signals from the market to create features that satisfy unmet demands or improve the functionality of its network. When block space demand exceeds capacity, as it did it late 2017, transaction fees spike and encouraged the development of a second layer protocol to increase transaction throughout (the Lightning network discussed earlier). As rent-seeking businesses, like Western Union, continue charging exorbitant fees for international remittances, market demand shifts to Bitcoin's much more cost effective and permissionless payment channel. When governments crack down on Bitcoin exchanges, trading volume on peer-to-peer exchanges like LocalBitcoins.com flourishes. To enhance Bitcoin network accessibility, Blockstream launches satellites that provide global coverage for node synchronization. The Bitcoin network is constantly adapting to optimize for its own expansion and the interconnectedness of its participants. Perhaps Bitcoin is less so digital gold, and more so digital slime mold (just kidding, or am I?).

In most forms of life, genes are only passed from parent to offspring in a process called *vertical gene transfer*. Certain fungal networks, which are modeled after the decentralized network archetype, are able to steal competitive advantages directly from physical contact with other similar organisms in a process called *horizontal gene transfer*. These fungal networks can grow to gargantuan sizes—indeed, the largest organism on Earth, at nearly 4 kilometers across, is a honey fungus in Oregon that is slowly consuming an entire forest. Fungal networks live in constant competition as they fight off predators, pests and pollutants. This environmental stress causes them to naturally synthesize a variety of enzymatic and chemical countermeasures and, when one of these measures is successful, it is stored in the distributed mind of the entire fungal network. The next time it encounters a menace for which it has even once synthesized an effective countermeasure, the fungal network will use it to neutralize the threat, no matter where the latest encounter occurs. Amazingly, these fungal networks are capable of absorbing countermeasures created by competitors in the same ecosystem purely from physical contact. Such organisms exhibit distributed intelligence, meaning they learn at the edges and distribute the lessons throughout their vast networks.

There is a common misconception that an alternative cryptoasset could develop a superior feature that will eventually outcompete Bitcoin. Similar to certain fungal networks, Bitcoin is able to subsume features that have been proven in the marketplace from cryptoasset competitors. For example, an alternative cryptoasset called Basic Attention Token (BAT) is designed to power an internet browser called Brave that allows users to shield themselves from advertisements:



BAT is a cryptoasset designed to allow web browser users to monetize their own attention. Using a set of open-source software extensions, today you can perform browser-based microtransactions similar to BAT but using Bitcoin instead. This effectively eliminates the need for a cryptoasset like BAT. The capacity of Bitcoin to subsume market-proven features from competitive cryptoassets fortifies it from disruption.

Brave users are then given the option to open their browsing sessions up to advertisements and are paid in BAT for their attention. This blockchain-based digital advertising solution is intended to allow users to monetize their own attention, whereas in most browsers advertising revenues are allocated mostly to the content publishers. Given Bitcoin's open-source nature, it is able to absorb competitive features like this in a process similar to horizontal gene transfer. Today, by using the Lightning Joule browser extension and running a full Bitcoin node, you can perform browser-based microtransactions similar to BAT but using Bitcoin instead. This effectively eliminates the need for a cryptoasset like BAT. Further, the technologies combined to make Bitcoin all came from previous attempts at digital cash, reiterating the point that open-source software is amenable to feature absorption. This ability accelerates the adaptivity of the Bitcoin network and insulates it from competitive disruption which further reinforces its position as the market leader.

Antifragility [1,11]

Seeing the ubiquity of the decentralized network archetype throughout nature in this way makes the invention of decentralized digital money seem less novel and more inevitable. An open and decentralized nature also enables Bitcoin to benefit from adversity. In light of its track record, Bitcoin is an excellent incarnation of Nassim Taleb's concept of *Antifragility*:

> *"Wind extinguishes a candle and energizes fire… Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder and stressors and love adventure, risk and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile. This property is behind everything that has changed with time: evolution, culture, ideas, revolutions, political systems, technological innovation, cultural and economic success, corporate survival, good recipes, the rise of cities, legal systems, equatorial forests, bacterial resistance… even our own existence as a species on this planet."*

Fragility can be defined as sensitivity to disorder, whereas robustness is insensitivity to disorder. Antifragility is a property of anything that benefits from disorder, stress or adversity. The many failed attempts at killing Bitcoin thus far have only made it stronger by drawing attention to attack vectors or vulnerabilities that its global team of self-interested, volunteer programmers can then fix. These improvements have only increased the network's operational efficiency. Also, each time it withstands an external attack or a chain fork (as we are witnessing with the abject failure of Bitcoin Cash), its reputation for network security and immutability is strengthened. The resiliency of Bitcoin is hardened by hostility.

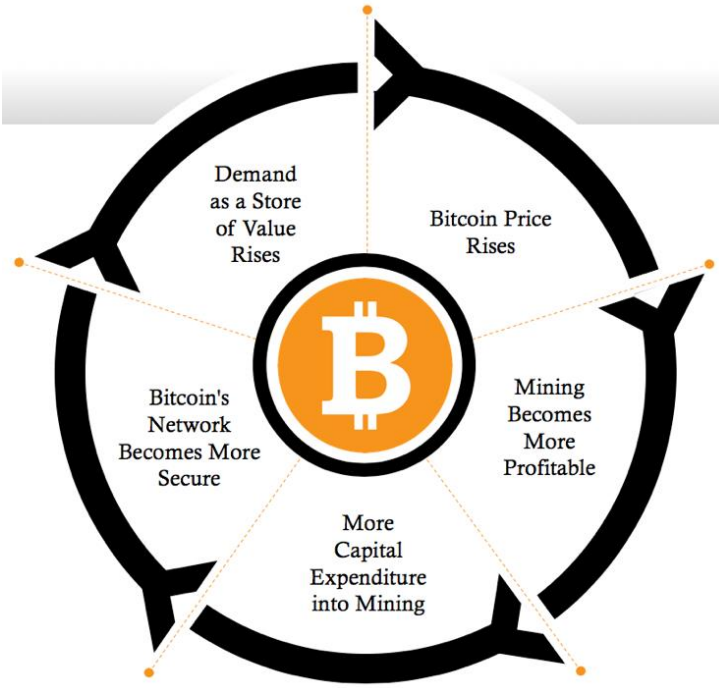
As Bitcoin has fluctuated wildly in price over the years, each new crash has triggered widespread declarations of its demise. Over 330 prominent articles declaring the death of Bitcoin, known as Bitcoin obituaries, have been written over the past 10 years. These publicity attacks on Bitcoin brought it to the attention of ever-wider audiences. As obituaries intensified, Bitcoin's network processing power, transaction volume and market capitalization all continued to ascend relentlessly—a confirmatory example of the saying 'all publicity is good publicity'.

When China took a heavy-handed approach to regulation by shutting down Bitcoin exchanges in 2017, we witnessed several informal exchanges and OTC markets appear following the demise of each centralized exchange. Although the liquidity for Bitcoin was negatively impacted initially, soon transactions started happening off exchange in China, with volume on websites like localbitcoins.com exploding. The regulatory attack also encouraged people to hold Bitcoin for longer periods, as evidenced by a steep decline in sell volumes, which only reduced the amount of Bitcoin being traded and put upward pressure on its price. Also, these regulatory actions backfired by triggering the *Streisand Effect*, which is a phenomenon whereby an attempt to hide, remove or censor information has the unintended consequence of publicizing the information more widely, usually

facilitated by the internet. As the world watched the situation in China unfold, both the Bitcoin price and global internet searches for the term Bitcoin reached new all-time highs.

Bitcoin's Positive Feedback Loop [1,4]

All of the adversity Bitcoin has faced so far has only fed its growth. Absent any top-down authority, Bitcoin is organic in the sense that it has grown from the bottom-up based solely on its own merits as money. Bitcoin perpetuates the expansion of its network and maintains truthful records by relying on asymmetric economic incentives that make fraud far costlier than its potential rewards. Network participants are all rewarded economically for their interactions with Bitcoin, which creates a flywheel effect on its price and network security:



Bitcoin autonomously proliferates its network by economically rewarding everyone who interacts with it.

As the Bitcoin network adapts to better meet the demands of its constituents, it in turn recruits more network participants. This positive feedback loop promotes the sustained growth of its network and fuels powerful, multi-sided network effects.

Bitcoin's Network Effects [1,4,5]

Bitcoin's meteoric growth has been both supported and protected by its unique multi-sided network effects. The basic example of a powerful 1-sided network effect is a social network (or a telephone network, as outlined earlier). The more people on a social network, the more valuable it is for others to be on it, as there are exponentially more

possible connections. It can, however, be disrupted by a competitor that provides a more valuable service to its single customer cohort, the users, who might then transition to the new service (as happened when Facebook disrupted MySpace).

Successful 2-sided markets (like eBay or Craigslist) are significantly more difficult to disrupt. Consumers want to be there because merchants are there, and merchants want to be there because consumers are there. To disrupt a 2-sided network, you have to simultaneously introduce a superior value proposition for both parties, otherwise nobody moves. That is why Craigslist, despite its limited innovation over the years, has been able to leverage its early 2-sided lead and is still a dominant website today.

Bitcoin has a unique 4-sided network effect that insulates it from disruption and supports its growth. These are the four constituencies that participate in expanding the value of Bitcoin as a result of their own self-interested interaction with its network:

- Consumers who pay with Bitcoin
- Merchants who accept Bitcoin
- Nodes that maintain the distributed ledger
- Developers and entrepreneurs who are building onto and on top of Bitcoin

This 4-sided network effect makes Bitcoin's first mover advantage seemingly indomitable. As an adaptive monetary technology, its network effects encompass the liquidity of its market, the number of network participants, the community of software developers who support it and Bitcoin's brand awareness. Large investors will always seek the most liquid market for ease of entry and exit. Consumers, merchants and developers tend to join the largest of each of their respective Bitcoin communities, which only reinforces their social interconnectivity and cohesion. Brand awareness is innately self-reinforcing, as any cryptoasset competitor will inevitably be mentioned in comparison to Bitcoin.

An aside on Bitcoin's brand awareness: As we have learned, the value of any money is derived from its social consensus, or the mutual beliefs of its users. The notion of a "believer" has religious connotations, as the notion of one having an epiphany once the "truth" is revealed. Such religious undertones are prevalent in most forms of money (In God We Trust on the US Dollar) and they are also part of Bitcoin's aura (The Genesis Block, Bitcoin Evangelists). The most important of these quasi-religious ideas is the mythological bedrock Nakamoto laid with his enigmatic appearance in 2008 and then with his mysterious disappearance 3 years later. Whoever he/she/they were, Nakamoto gave Bitcoin its *creation myth*. As market strategist Nicolas Colas said:

> *"In business, creation stories reinforce the role of the individual as a societal agent of change and speak to a core audience of customers. They are the bedrock for what marketers call a brand and the source waters for Wall Street's shareholder value."*

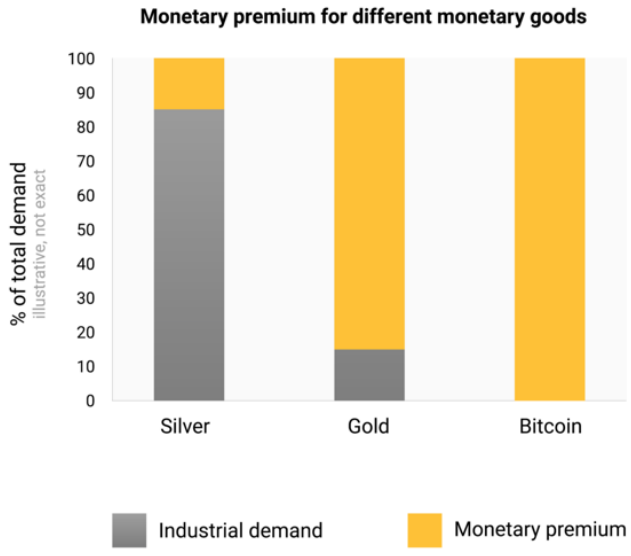
Assuming Nakamoto was a lone wolf, it is arguable that his disappearance transformed him from a person into a mythological figure. This mystery fuels the brand awareness of Bitcoin and reinforces its quality of decentralization, as there is no single individual to vilify,

denigrate or otherwise target in an attempt tarnish Bitcoin's symbolism. Like a super hero with a secret identity, all we have is the icon of Nakamoto as a cryptic genius—the godhead of Bitcoin.

As we have learned, the value of a network is a reflection of the total number of possible connections it allows. Therefore, each new Bitcoin owner increases the value of the Bitcoin network, which benefits all existing owners. This new owner is then incentivized to evangelize the benefits of Bitcoin to others, creating the next wave of new owners, and the cycle continues. As the price increases, so too do the incentives to secure the network which draws in more capital expenditure from miners, making Bitcoin's network effects even stronger and self-reinforcing as price appreciation reflexively energizes Bitcoin's positive feedback loop outlined earlier.

Since money is a social network, the price of a monetary good is a reflection of how widely adopted it has become or is expected to become. The price of a monetary good in excess of its industrial demand is its *monetary premium*. This is the only rational basis for the common criticism that Bitcoin is a bubble, as it is purely a monetary technology and has no industrial demand whatsoever. However, this premium is the defining characteristic of all forms of money, as all monetary value is based on the optionality it gives its user for exchange across scales, space and time.

Actual bubbles occur when price exceeds fair value, such as the market distortions created by central bank monetary manipulation. However, some mistake monetary premia for bubbles since they cause prices of monetary goods to exceed their underlying industrial values. If monetary premia are bubbles, then money is the bubble that never pops. Paradoxically, in this sense a monetary technology can presently be both a bubble and significantly undervalued if it later achieves widespread adoption:



As a pure bred monetary technology, Bitcoin derives none of its value from alternative uses.

Although there is no established price pattern for a digital good that is becoming monetized, Bitcoin's price appears to follow a fractal (a recursive, self-similar shape) wave pattern of increasing magnitude commensurate with its level of user adoption. The volatility of this price pattern is exacerbated by Bitcoin's perfect price inelasticity of supply (as discussed earlier). Each iteration of the *fractal wave pattern* appears to match the standard shape of the *Gartner hype cycle*, which provides a graphical and conceptual representation of emerging technologies undergoing five phases of maturation:

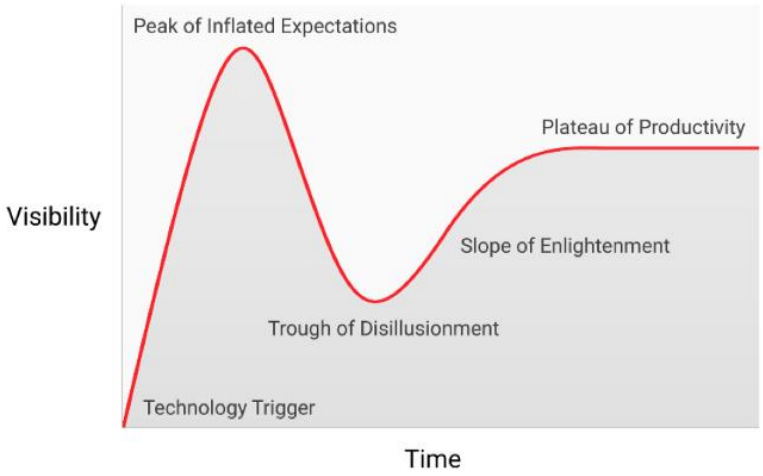


Figure 2 Bitcoin's price appears to follow a fractal wave pattern based on the archetypal Gartner hype cycle.

Bitcoin's growth, in terms of price and transactions, has been dramatic to say the least. Indeed, it is the fastest growing asset in history. Its price has gone from $0.000994 on October 5, 2009, in its first recorded transaction, to about $4,000 today—a total increase of over 400,000,000% in 10 years. By its 10th birthday, Bitcoin had processed about $1.38T USD worth of transactions, with USD value calculated at the time of each transaction. Here we show Bitcoin's entire price history, from a logarithmic perspective, with the Gartner hype cycle fractal wave pattern iterations located inside boxes:

Figure 3Bitcoin is the fastest growing and most volatile asset in history, although both are leveling off as it grows.

These extreme price cycles draw in new Bitcoin owners as each fractal wave crests. Some of these new owners buy in near the peak, only to be crushed in the trough. Most will capitulate, but those who remain because of their long-term conviction in Bitcoin (typically the most studious of history and monetary evolution among them) become the newest *hodlers of last resort*. Hodl, which began as a chat room typo in the early days of Bitcoin, has morphed into a memetic phrase that denotes "hodling" Bitcoin long term without regard to its price volatility. Layers of these stubborn hodlers have been added throughout each of Bitcoin's four major price cycles. A good proxy for the depth of these layers is the lowest price Bitcoin hits each year, which indicates the rising collective obstinacy of these hodlers:

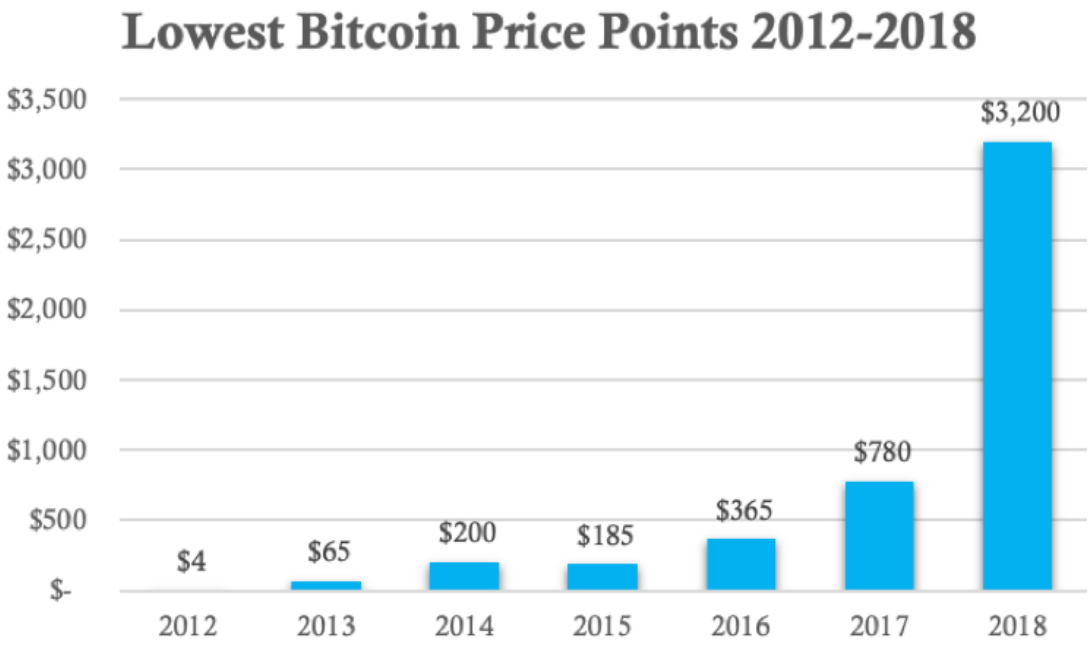


Figure 4The annual low prices of Bitcoin provide an effective proxy for the collective intransigence of its hodlers.

These layers form the base for the next iteration of each fractal wave pattern. As more observers recognize the survivability of Bitcoin following each price crash, they realize that investing in it may not be as risky as they once thought. This larger base of believers sets the stage for the next iteration of the fractal wave pattern which will support a much larger set of newcomers at a far greater magnitude of peak price. Few people are able to accurately predict how high prices will go in each fractal wave cycle, and they usually reach levels that would seem absurd to most investors at the earliest stages of the cycle. The best proxy for the timing of these fractal wave patterns has been the quadrennial Bitcoin inflation rate adjustment, when the amount of new Bitcoin rewarded at the close of each block is reduced by half, an event commonly known as the *halving.* Historically, Bitcoin achieves a new all-time high price within 18 months of its last halving. The next halving will occur in May 2020:

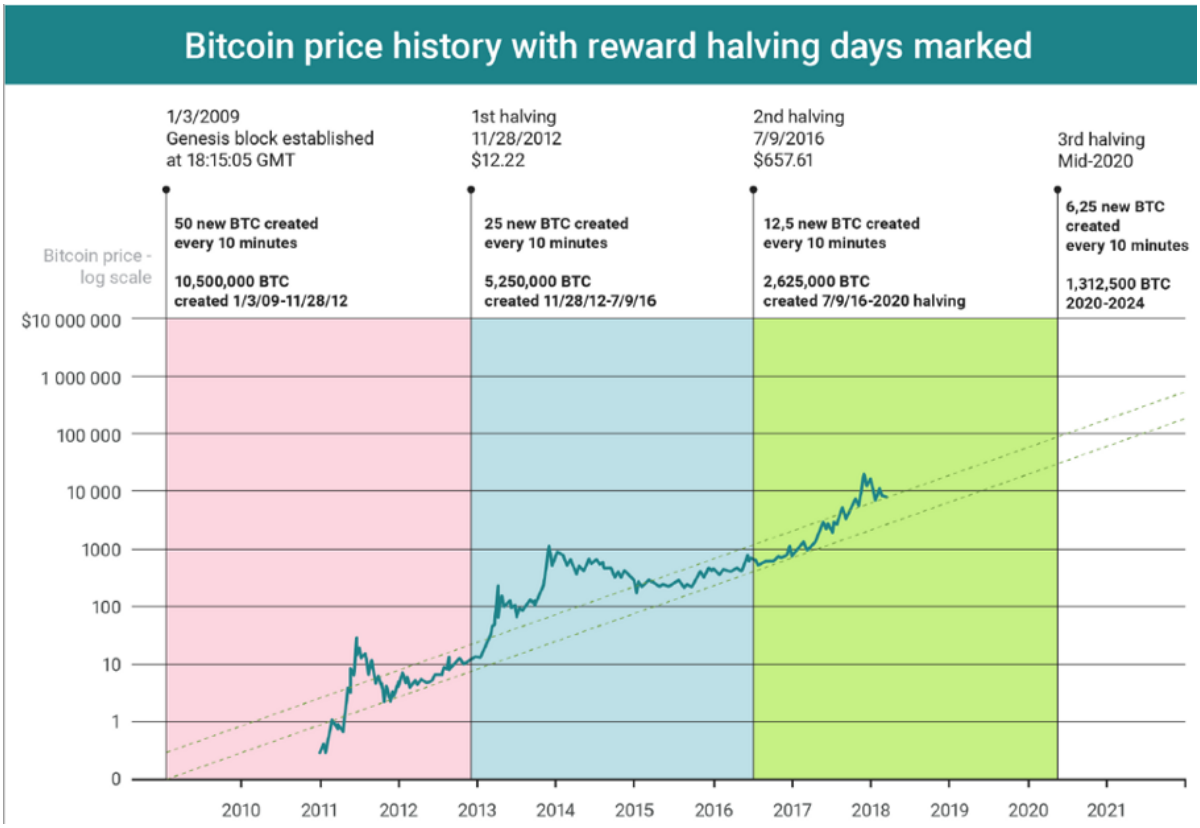


Figure 5Every four years, the Bitcoin supply growth rate is cut in half. Each halving also cuts the Bitcoin sell pressure from miners in half and creates upward pressure on its price. Historically, this quadrennial event is the best proxy for the timing of Bitcoin price fractal wave patterns.

The fractal wave patterns inevitably crescendo and begin to crash, usually attributed to myriad factors by mainstream media. However, the Gartner Hype cycle is an archetypal market pricing pattern that is driven entirely by human psychology, game theory and the ultimate exhaustion of market participants reachable in each iteration. The magnitude of each cycle is exacerbated by Bitcoin's absolutely fixed supply schedule, as increases in demand are expressed exclusively through its price, which historically leads to market frenzies at each peak. The long game for Bitcoin, and its final fractal wave pattern, will begin when and if central banks begin accumulating it as a reserve asset (more on this later). In this way, the bedrock of the Bitcoin network's expansion is the intransigency of its hodlers of last resort. Although they constitute a small minority of the whole, these stubborn hodlers will contribute to ongoing Bitcoin adoption in a meaningful way.

Minority Rule [3]

When it comes to group preferences, certain types of minorities—those who stubbornly insist on a particular preference—that constitute even a small level of the total population (often less than 4%) can cause the majority to submit to their preferences. Another clever concept from Nassim Taleb, called the *minority rule*, is the result of complex system dynamics, like those inherent to human interaction.

The nature of complex systems (society) is that the collective behaves in a way not predicted by its individual constituents (people). The interactions between its constituents matter more than their individual natures. Studying individual ants will never give us an idea on how the ant colony operates. For that, one needs to understand an ant colony as an ant colony, not just a collection of ants. This is called an emergent property of the whole. In other words, the whole is more than the sum of its parts because what matters is the interactions between the parts. These interactions, while complex, can obey simple rules, like the minority rule (or the rule that barter economies settle on a medium of exchange or that the hardest form of money always outcompetes). Many domains are impacted by the minority rule such as:

- Markets—Market prices are not the consensus of market participants, but instead reflect the activities of the most motivated buyers and sellers. In 2008, a single $50B order, less than 0.2% of the stock market's total value of about $30T, caused the market to drop by almost 10%, causing losses of around $3T. The order was activated by the Parisian Bank Société Générale who discovered a hidden trade by a rogue trader and wanted to reverse the purchase. The market reacted disproportionately because there was only a desire to sell and no way to change the stubborn seller's mind.
- Science—Similar to markets, science is not the consensus of scientists, it is the minority body of knowledge remaining after removing disproven hypotheses.
- Law—A law abiding citizen will never commit criminal acts but a criminal will readily engage in legal acts, and criminal behavior has been shown to be contagious within certain social groups.
- Imports—In the United Kingdom, where the (practicing) Muslim population is only around 4%, a very high proportion of the meat we find is halal (or Kosher). Close to 70% of lamb imports from New Zealand are halal. The same population and import proportions hold true in South Africa (the case of imports is closely related to the example below).

Today, in the United States and Europe, companies are selling more and more non-GMO food precisely because of the minority rule. Given the possibility of food containing GMOs, food not bearing the label "non-GMO" may be assumed by some to contain GMOs which, according to the minority, contain unknown risks. People who eat GMO food will readily eat non-GMO food, but not the reverse. Assuming the price and distribution costs differences between GMO and non-GMO are sufficiently small and the intransigent minority is distributed somewhat evenly throughout the population, this will have the effect of disproportionately increasing the demand for non-GMO food in the long run. This dynamic of scale can be explained quantitatively. In mathematical physics, renormalization groups are an apparatus that allow us to see how things scale up or down.

Here we show how the minority rule can renormalize the preferences of the majority.

Our graphic depicts:

· Three vertically-stacked large boxes, each representing one sequential step in the minority rule renormalization process
· Four medium boxes in each step, each representing a family of four
· Four smaller boxes contained within each medium box, each representing an individual member within each family of four

Assume that in Step 1, the daughter in the family of four is the intransigent minority (the small pink box) who eats only non-GMO food. As we move to Step 2, the group renormalizes as the stubborn daughter manages to impose her rule on her three family members (who are now all pink) as they are flexible on the matter and consistency simplifies their grocery shopping and administrative process. In Step 3, the family of four goes to a backyard barbecue attended by three other families. As their family is known for their strict eating habits, the host will only serve non-GMO food as the other families are flexible and consistency simplifies the food preparation process, thereby making all four families (which are now all pink) adopt the minority rule originally set by the intransigent daughter in Step 1.

This minority rule will continue imposing and proliferating itself as these families attend other social events, which gradually shifts customer preferences in the neighborhood and eventually causes the local grocery store to switch to non-GMO foods to simplify its procurement processes, which impacts the local wholesaler, and so on up the supply chain. The real world result of this dynamic is the preferences of 4% of a population (practicing Muslims) driving the market preferences of 70% of their respective populations (in the UK, New Zealand and South Africa). As we can see, the minority rule spreads by interaction and renormalizes the entire group to conform with its preferences. Its proliferation is accelerated if there are incentives to switch, low switching costs or anticipated future benefits from switching (as superiorly hard digital cash money, Bitcoin offers all three). In this example, a minority constituting 6.3% of the total population imposed its rules on the majority using pure intransigence. In reality, the minority rule often takes effect when minorities become 4% or less of the total population.

Languages also often adhere to the minority rule. For instance, French was originally intended to be the language of diplomacy as civil servants from aristocratic backgrounds used it, while English was reserved for those engaged in commerce. In the rivalry between the two languages, which are still considered two of the international languages (a third, Spanish, was added later because of its widespread use), English won as commerce came to dominate modern life. This gives us some intuition as to how the emergence of *Lingua Franca* languages, those commonly spoken across cultures, can come from minority rules. As Taleb puts it:

"Aramaic is a Semitic language which succeeded Canaanite (that is, Phoenician-Hebrew) in the Levant and resembles Arabic; it was the language Jesus Christ spoke. The reason it came to dominate the Levant and Egypt isn't because of any particular imperial Semitic power or the fact that they have interesting noses. It was the Persians –who speak an Indo-European language –who spread Aramaic, the language of Assyria, Syria, and Babylon. Persians taught Egyptians a language that was not their own. Simply, when the Persians invaded Babylon they found an administration with scribes who could only use Aramaic and didn't know Persian, so Aramaic became the state language. If your secretary can only take dictation in Aramaic, Aramaic is what you will use. This led to the oddity of Aramaic being used in Mongolia, as records were maintained in the Syriac alphabet (Syriac is the Eastern dialect of Aramaic). And centuries later, the story would repeat itself in reverse, with the Arabs using Greek in their early administration in the seventh and eighth's centuries. For during the Hellenistic era, Greek replaced Aramaic as the lingua franca in the Levant, and the scribes of Damascus maintained their records in Greek. But it was not the Greeks who spread Greek around the Mediterranean—Alexander (himself not Greek but Macedonian and spoke a different dialect of Greek) did not lead to an immediate deep cultural Hellenization. It was the Romans who accelerated the spreading of Greek, as they used it in their administration across the Eastern empire."

There is an asymmetry that those who do not have English as their first language usually know basic English, but native English speakers knowing other languages is less likely. If a meeting is taking place in an international office in say, Istanbul, among twenty executives from a sufficiently international corporation and one of the attendees does not speak Turkish, then the entire meeting will be run in English (the commercial Lingua Franca). This is the minority rule in action.

Money is an emergent property, as it is an expected result of complex human interactions within a barter economy. Similar to language, it is a means of expression, only it is used to express value instead of information or emotion. The US Dollar is the Lingua Franca of money today, as it belongs to one of the world's largest economies (an economy which also happens to effectively control the global banking system).

As the digital age matures and the world becomes increasingly interconnected, ever-more commerce and administration will be conducted over the internet. Also, fully interconnected trade networks will level the terrain of commerce and increase free market competition among different forms of money. Considering the significant market lead already enjoyed by Bitcoin, its superior hardness, its multi-sided network effects, the impotency of capital controls on digital cash and the winner take all dynamic inherent to monetary competition; it's likely that Bitcoin will continue to outcompete and its adoption rate will increase. By considering the application of the minority rule to adoption of Bitcoin in the digital age, we can reasonably expect the following:

- Once a sufficient minority of the world's population, say 4% or less, have realized the advantages of hard money and digital cash money, their

intransigent hoarding of Bitcoin will drive its price upward (Gresham's Law) and begin imposing itself economically on all other holders of money in the world. This will put downward price pressure on government fiat money, further accelerate Bitcoin's adoption rate and drastically improve Bitcoin's chances for global acceptance over the long run.

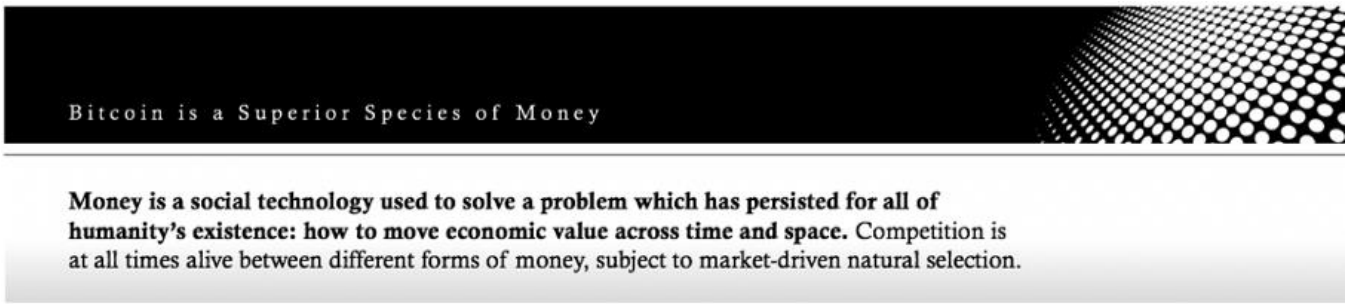
- As the first natively digital form of cash money, Bitcoin will become the Lingua Franca of digital commerce and the dominant value exchange protocol, thereby capturing nearly all the value transacted online (e-commerce alone is estimated to be nearly $5T annually by the year 2021) over the long run.
- Bitcoin may also become the base layer for other tools of cryptographic certainty in commerce, such as smart contracts and TrustNet applications (more on these later).

The minority rule is based on a fundamental asymmetry between the intransigence of the minority and the flexibility of the majority. The minority rule shows us that a small number of unyielding people with skin or soul in the game can change the shape of the majority. Bitcoin already has the advantage of being the hardest form of money ever invented, and its rules are immutable, which is the highest form of intransigency possible. It also has unrivaled brand awareness, fed by the mystery of its creation myth, and the support of free market fanatics all over the world. Once its obstinate minority reaches a certain size, the unbreakable rules of Bitcoin will begin to stubbornly impose themselves on the established economic order. In the words of Margaret Mead:

> *"Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it's the only thing that ever has."*

A Superior Species of Money [1,4,12]

Bitcoin also introduces three new traits of money never before seen—censorship resistance, adaptivity and programmability. Censorship resistance means that no group or individual in the world can stop payments made on its network. Bitcoin gains censorship resistance by virtue of its decentralized architecture. Adaptivity refers to the ability for Bitcoin's network to become more secure as it stores more value, its open-source nature which aligns the incentives of its global team of volunteer programmers with its own to ensure it is always up to date with state-of-the-art software enhancements and its ability to subsume features from competitors that have been proven in the marketplace. Programmability refers to the digital nature of Bitcoin and its ability to interface with smart contracts and other decentralized applications. As we have learned, the free market for money is a competitive environment that is shaped by continuous market-driven natural selection; as a competitor in this domain Bitcoin is a superior species:



Traits of Money	Gold	Government Money	Bitcoin
Fungibility (interchangeable units)	High	Medium	High
Hardness (stock-to-flow ratio)	Medium	Low	High
Portability	Medium	High	High
Durability	High	Medium	High
Divisibility	Low	Medium	High
Security (cannot be counterfeited)	Medium	Medium	High
Easily Transactable	Low	High	High
Scarcity (predictable supply)	Medium	Low	High
Self-Sovereign (permissionless)	High	Low	High
Government Issued	Low	High	Low
Decentralized (censorship resistant)	Low	Low	High
Smart (adaptive & programmable)	Low	Low	High

The technology that is enabling Bitcoin to compete effectively in the market for money is also being applied to create new markets or disintermediate other existing markets. In technical parlance, the Bitcoin network is the world's first decentralized application. A decentralized application is a service that no single entity owns or operates. It is a new form of software and human organization that eliminates single points of failure, resists external attacks and reduces the need for intermediaries. Decentralized applications are enabled by cryptoassets. In the same way corporate equities serve companies and government bonds serve nations, cryptoassets serve decentralized applications. Owning a cryptoasset (like Bitcoin) is the only way to own a piece of a decentralized application (like the Bitcoin network). Technically, a cryptoasset is a cryptographically protected digital token representing rights within an economic network. A cryptoasset is to a decentralized application what oil is to an engine; it provides functionality and liquidity for the network and its constituents. A defining feature of cryptoassets and decentralized applications, and arguably their most alluring, is their organic nature; they are not centrally owned, governed or developed—making them highly resistant against censorship and manipulation.

Bitcoin (the OG cryptoasset) is superior in the market for money because it possesses all the ideal features of digital cash money and enjoys a market dominant position by virtue of its serendipitous first mover advantage which is fortified from disruption by its open-source design and multi-sided network effects. With the invention of Bitcoin, the world

finally has a synthetic form of money with a stock-to-flow ratio that is guaranteed to increase (until it reaches infinity) and an unstoppable, permissionless payments channel. Its digital nature makes it salable across space in a way never before seen, as it can be stored in the human mind and transmitted at the speed of light. The deep divisibility of each Bitcoin into 100 million Satoshis makes them supremely salable across scales. Its informational and nonperishable nature, when considered in combination with its superior hardness, gives Bitcoin unprecedented salability across time. This design makes it an impeccable store of value. Finally, by eliminating all intermediary control (which is inherent to government money) Bitcoin resists debasement, censorship and confiscation. It removes the central banks, macroeconomists, politicians, presidents, dictators and military leaders from monetary policy and payments authorization once and for all. The masterful book (from which much of this essay adapted) titled "The Bitcoin Standard" by Saifedean Ammous sums up Bitcoin's historical relevance nicely:

> *"If the modern world is ancient Rome, suffering the economic consequences of monetary collapse, with the dollar our aureus, then Satoshi Nakamoto is our Constantine, Bitcoin is his solidus, and the Internet is our Constantinople. Bitcoin serves as a monetary lifeboat for people forced to transact and save in monetary media constantly debased by governments… the real advantage of Bitcoin lies in it being a reliable long term store of value, and a sovereign form of money that allows individuals to conduct permissionless transactions."*

Bitcoin is a tool for freedom. As the most accessible asymmetric bet in history, Bitcoin is also a unique investment opportunity.

Investing in Bitcoin [1,5,13]

Investing is all about taking intelligent risks. As Daniel Kahneman, a Nobel Prize-winning psychologist, describes it:

> *"Intelligent risks are based on wide and voracious data gathering checked against gut instinct; while dumb decisions are built from too narrow a base on inputs."*

Bitcoin is often referred to as digital gold, in reference to its hardness, self-sovereignty and as an instrument for final settlement. Following this analogy, there will only be one digital equivalent to gold (due to winner take all dynamics inherent to the free market for money), and if you were going to bet on which one will succeed you'd want to bet heaviest on the biggest (due to its deep liquidity and multi-sided network effects), most renowned (due to the minority rule) and the longest lived (due to the Lindy Effect, more on this later). As people tend to think by analogy, this comparison to gold mostly works well, although it is incomplete.

As we have seen, Bitcoin is a far superior monetary technology to the golden inert metal. Technologically, Bitcoin needs little to no protocol improvement to continue to compete effectively in the market for money. There are no unsolved computer science problems

standing between Bitcoin and its widespread adoption. Therefore, its primary aim is to remain extant as digital cash money, hence its minimal level of protocol functionality and the status quo bias it exhibits in relation to governance. By merely existing, Bitcoin provides a gateway for people to opt out of the prevailing inflationary monetary order. As long as it continues to operate successfully in its current form, Bitcoin will function healthily as the stateless base money protocol for the digital age—which makes it a viable contender in the $100T market for global money:

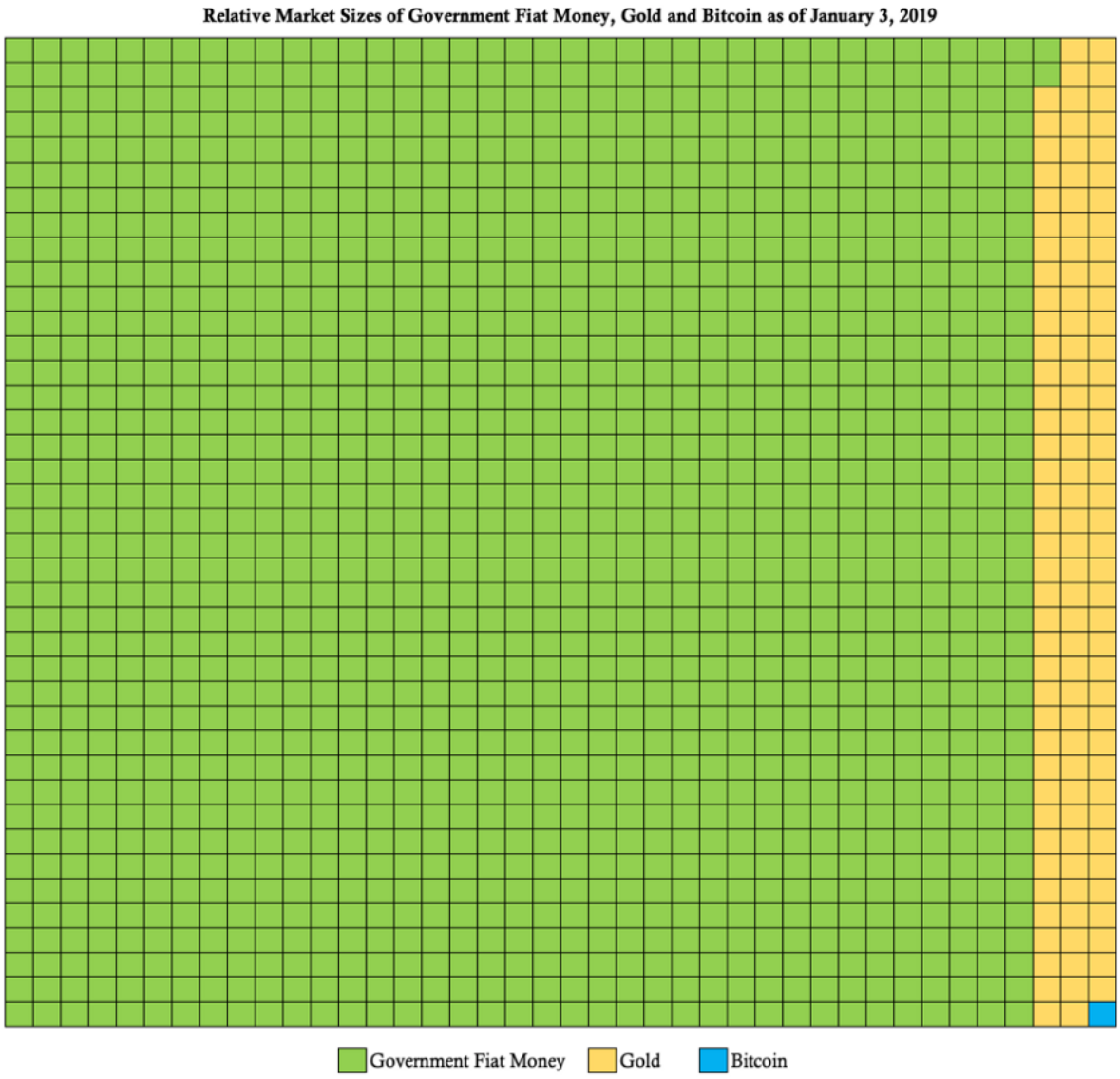


Figure 6 Bitcoin is competitively superior to both gold and government fiat money, and has plenty of room to grow.

Since it is still extremely small relative to its total addressable market, which consists mostly of gold and government fiat money, Bitcoin still has room to grow by orders of magnitude in both its network size and price. Like a call option, a bet on Bitcoin is asymmetric, meaning that an investor's downside is limited to 1x whereas their potential upside is 100x or more. Should Bitcoin achieve a majority share of the global market for

money, its level of demand will become far more predictable and steady, leading to a stabilization in its price.

Investing in Bitcoin can be considered a bet on its adoption as an uninflatable, politically neutral store of value and as an unstoppable, permissionless payments channel.

Bitcoin may also become part of a much bigger wave of innovation. Although the Bitcoin network and the decentralized applications it has inspired are poorly understood by most today (similar to the internet in the early 1990s) we believe that the world will gradually awaken to the paradigmatic shift that is underway for money and markets in general. The greatest wealth is created by being an early investor in innovation. Making such investments requires believing in something before the majority of people understand it — which also often entails enduring mockery, ridicule and criticism for your non-consensus perspective. As Mark Yusko, one of my favorite hedge fund managers, describes the coming crypto era:

> *"Technology follows 14-year innovation cycles. These began with the Mainframe in 1954, then the Microchip in 1968, the Personal Computer in 1982, the Internet in 1996 and most recently the Mobilenet in 2010. As a result of the innovations introduced by Bitcoin, soon we will christen 2024 as the dawn of the Trustnet."*

The *TrustNet* can be thought of as the dawn of trustworthy computing. In theory, it will enable new technologies such as the internet of things, decentralized autonomous organizations, self-owning commercial assets, decentralized internet provisioning, decentralization of energy distribution, reputation markets, computing power markets, stateless identity, immutable media, AI-run organizations, token curated registries, prediction markets and circles of trust. This anticipated innovation wave is consistent with a multi-decade cycle of information technology expansion, consolidation and commoditization:

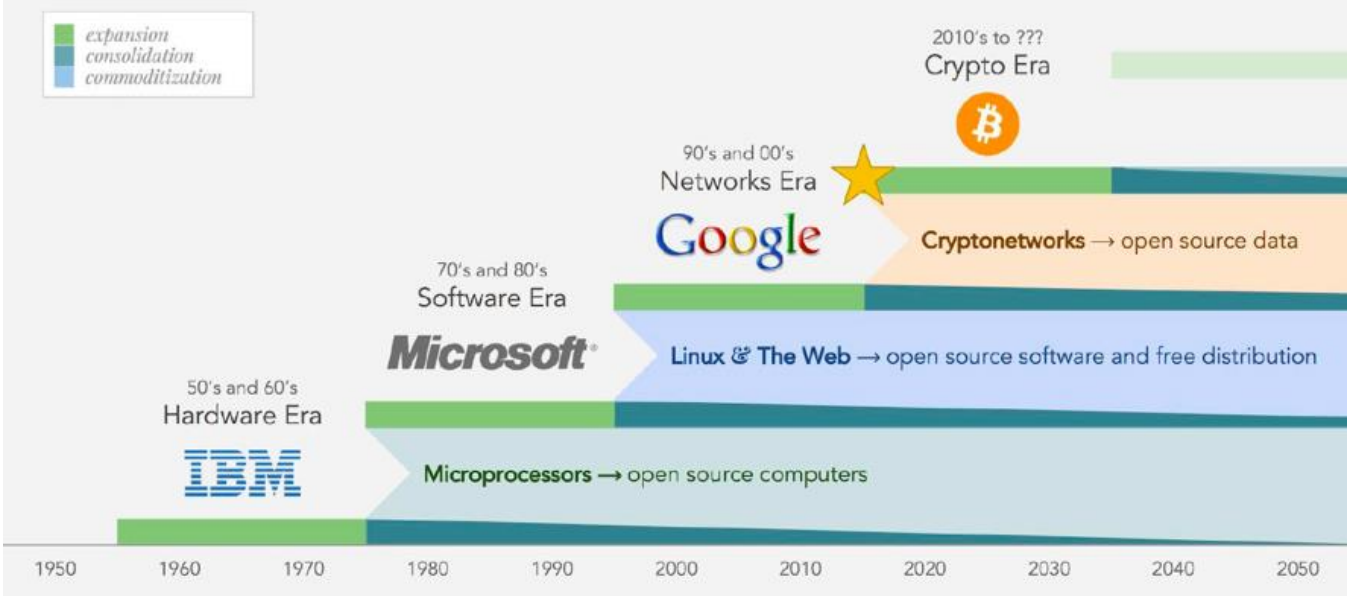


Figure 7 As innovations in information technology age, they inevitably become commoditized and create the bedrock upon which future waves of innovation are built.

Bitcoin, as the original and driving force of this innovation expansion cycle, will likely function as the systemic core and base money system of the Trustnet. During this cycle, all markets that are enabled by this technology will likely rely on the Bitcoin blockchain as a common value system, final settlement mechanism and temporal anchor point.

A Momentous Innovation [1,4,5,7,8,10]

Bitcoin is a momentous innovation of the digital age. As such, it has many unique characteristics, properties and capabilities never before seen in a monetary technology:

- Immutable Monetary Policy—Predictable, transparent and unchangeable money supply schedule. The most critical aspect to outcompeting in the free market for money, as people will naturally come to favor the hardest form of money available to them (uninflatable money).
- Digital Scarcity—Necessary to solve the double-spend problem and bring the speed and finality of physical cash settlement into the digital realm.
- Absolute Scarcity—The only asset in the world which has an absolutely finite supply, like time itself.
- Global Final Settlement System—A permissionless, unstoppable payments system with zero counterparty risk (like gold, only digital) that can be used to quickly and efficiently provide finality of settlement across scales and space.
- Self-Sovereign Network—A self-sovereign monetary good (an informational bearer instrument) whose network operates autonomously in full accordance with its own immutable rules as reliably as the laws of mathematics.
- Stateless Money—The first globally connected payments system that is politically neutral. Possible catalyst for the separation of money and state over the long run.

- Revolutionary Social Contract Implementation—A unique 2-layer social contract implementation that decentralizes power among its constituents and creates a hypercompetitive market for its own network security. A new form of social institution.
- Global Consensus—Perhaps the only truly objective set of facts in world history, its distributed ledger is created by converting processing power into indisputable truth.
- Global Energy Buyer of Last Resort—Enables anyone in the world to convert excess electricity into digital gold on demand. A perpetual incentive for everyone in the world to develop more energy efficient innovations.
- A New Form of Life—Feeds on human self-interest and electricity to provide uninflatable money, an unstoppable payments channel and immutable governance.
- Adaptive Security—By virtue of the mining difficulty adjustment, as more value is stored on its network, the network adapts to become more secure.
- Adaptive Functionality—As an open-source software project, programmers around the world are constantly improving Bitcoin's codebase, however it is up to the users to adopt these changes, which creates a governance equilibrium in which only those changes that are in the collective best interests of users will be adopted. Enables Bitcoin to subsume superior features from competitors that are market-proven, making it highly resilient to disruption.
- Programmability—As a digitally native form of money, it can be used as a form of payment, collateral or fuel for a variety of smart contracts (self-executing software or commercial agreements). Can interface with other decentralized applications. Could function as the core value system for the TrustNet, the anticipated wave of innovation triggered by the emergence of Bitcoin.

Bitcoin has made a major impact in the world in its 10 years of existence, and it still holds a great deal of promise for the future. All in good time. Given its inextricable relationship with money and Bitcoin, the concept of time is worth exploring more deeply. It turns out that time's role in our lives, individually and collectively, is the key to understanding prosperity and the ways in which Bitcoin could play a key role.

Synthesized Works & Further Reading

- [1] *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] *The Rational Optimist* by Matt Ridley
- [3] *Skin in the Game* by Nassim Nicholas Taleb
- [4] *The Bullish Case for Bitcoin* by Vijay Boyapati
- [5] *The Age of Cryptocurrency* by Paul Vigna and Michael J. Casey
- [6] *Sapiens* by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism, Part 1 and Part 2* by Brandon Quittem
- [8] *PoW is Efficient* by Dan Held
- [9] *The Fifth Protocol* by Naval Ravikant
- [10] *Unpacking Bitcoin's Social Contract* by Hasu
- [11] *Antifragile* by Nassim Nicholas Taleb

- [12] *Letter to Jamie Dimon* by Adam Ludwin
- [13] *Placeholder VC Investment Thesis Summary* by Joel Monegro and Chris Burniske
- [14] *Diffusion of Innovations* by Everett M. Rogers
- [15] *Why America Can't Regulate Bitcoin* by Beautyon
- [16] *Hyperbitcoinization* by Daniel Krawisz

Money, Bitcoin and Time: Part 3 of 3

By Robert Breedlove

Posted January 26, 2019

8 The Simple Truth about Time: Time is the ultimate resource. Its absolute scarcity bounds the entirety our stories, both as individuals and societies. With economics, we strive to use it more effectively. As the destroyer of all things and the healer of

The Ultimate Resource [1]

Scarcity is the starting point of all economics. It is commonly believed that natural resources are inherently scarce, which is true in a sense, as there is only so much gold within the Earth, for instance. However, this finite quantity of gold in the Earth is still too large for humans to even measure and in no way constitutes an actual limit to the amount we can conceivably mine. We have literally 'just scratched the surface', as our mining efforts haven't even taken us half way into the Earth's crust, its thinnest and outermost layer. Driven by need, humans have always found a way to explore farther and dig deeper to uncover ever-more natural resources. Therefore, the actual practical limit to the quantity of any natural resource is always and only the amount of human time, effort and ingenuity devoted to its production. For human beings then, the only truly scarce resource is time.

Individually, the only scarcity we face is our limited time on Earth. As a society, the only scarcity we deal with is the total amount of human time, effort and ingenuity available to be directed at the production of goods. This scarce resource, which we will call *human time*, is the ultimate societal means of production. Humans have never fully exhausted any single natural resource. The price of all natural resources, in terms of human time, has always decreased steadily over the long-run as our technological advancements have dramatically increased our productivity. Not only have we not depleted any natural resource, but the proven reserves (the amount of natural resources still within the Earth) continue to increase despite our increasing rates of production, as new technologies enable us to discover and excavate ever-more natural resources.

Oil, the lifeblood of the industrial economy, is a great example of this concept. Even as oil production has increased every year, its proven reserves increase at an even faster rate. According to data from BP's statistical review, annual oil production increased 50% from

1980 to 2015. Oil reserves, on the other hand, have increased 148% during the same 35 year period, around triple the increase in oil production. Similar statistics exist for all natural resources prevalent in the Earth's crust. Some are more common (iron, copper) and some are rare (gold, silver) but the limit of how much we can produce of any particular natural resource is always and only the amount of human time directed at its production. The best evidence of this simple fact is gold: if the annual production of the one of the rarest metals in the Earth's crust goes up every year, then it makes no sense to consider any other natural resource being scarce in any practical sense. Echoing back to the fundamental market realities related to deferred consumption and investment—the real cost of anything is always its opportunity cost in terms of goods forgone to produce it. In terms of natural resources, only human time is truly scarce, which makes time the ultimate resource.

Frozen Time [1]

As more humans exist, there is more human time to direct towards the extraction and production of natural resources. As we have learned, productive output per unit of human time (productivity) can be amplified by leveraging technological solutions to problems (tools). In economics, a tool or technology is considered to be both:

- A non-excludable good—once one person invents something, all others can copy it and benefit from it
- A non-rival good—a person benefiting from an invention does not reduce the utility that accrues to the others who use it

For example, once one person invented the wheel, everyone else could copy its design and make their own, and their use of this design would in no way reduce others' ability to benefit from it. Innovations like this spread and their benefits compound over time, leading to ever-higher productivity and division of labor. Like the candle whose flame burns undiminished even after igniting a thousand others, the benefits of innovation ultimately accrue to everyone without detracting from the innovator in any way.

Natural resources and innovation are always and only the product of human time. Therefore, in terms of production, human time is the ultimate resource and essence of value. To keep score, people needed a way to reliably store the value they produce with their time, so that they can exchange it in the future for other peoples' time, effort and ingenuity. Conceptually then, money is frozen time. It is earned by sacrificing human time and can be traded for commensurate sacrifices from others. The age-old problem faced by people is collectively deciding which monetary technology can best serve this purpose.

Technologically, money is a spontaneous emergent property that humans ascribe to a particular good. People, acting in self-interest, live within technological and economic realities that shape their decisions and provide them incentives to persist, adapt, change or innovate. It is from the countless collisions of these complex human interactions that spontaneous monetary orders have emerged and decayed. History has shown us myriad

cases of a good being subjected to market-driven natural selection, achieving a monetary role and subsequently having its role taken by a superior technology.

Whatever monetary media people chose as a store of value was always subject to being produced in greater quantity, so the producers could acquire the value stored in it. The Yapese witnessed this play out when O'Keefe produced Rai Stones using explosives. West Africans had their wealth confiscated by Europeans who shipped in boat loads of cheaply produced glass beads. Citizens in modern economies continuously have their wealth usurped as central banks gradually or quickly erode the value of government fiat money. Gold came close to solving this problem as it is indestructible, expensive to mine and its flow is relatively predictable. However, gold's physicality led to its centralization within bank vaults and its compulsory replacement with soft government money.

Until the invention of Bitcoin, all forms of money were subject to having their value stolen by producers of the monetary good. This made all monetary technologies before Bitcoin imperfect in their ability to store value across time. Bitcoin's finite supply makes it the best medium to store the value produced by finite human time. In other words, Bitcoin is the best store of value humanity has ever invented, as it is the only monetary technology that cannot be debased over time. The informational, intangible and purely digital nature of Bitcoin enables it to achieve absolute scarcity, a property that was previously exclusive to time itself.

The absolute scarcity of Bitcoin makes it the perfect modality for freezing and transacting the only other absolutely scarce resource—time.

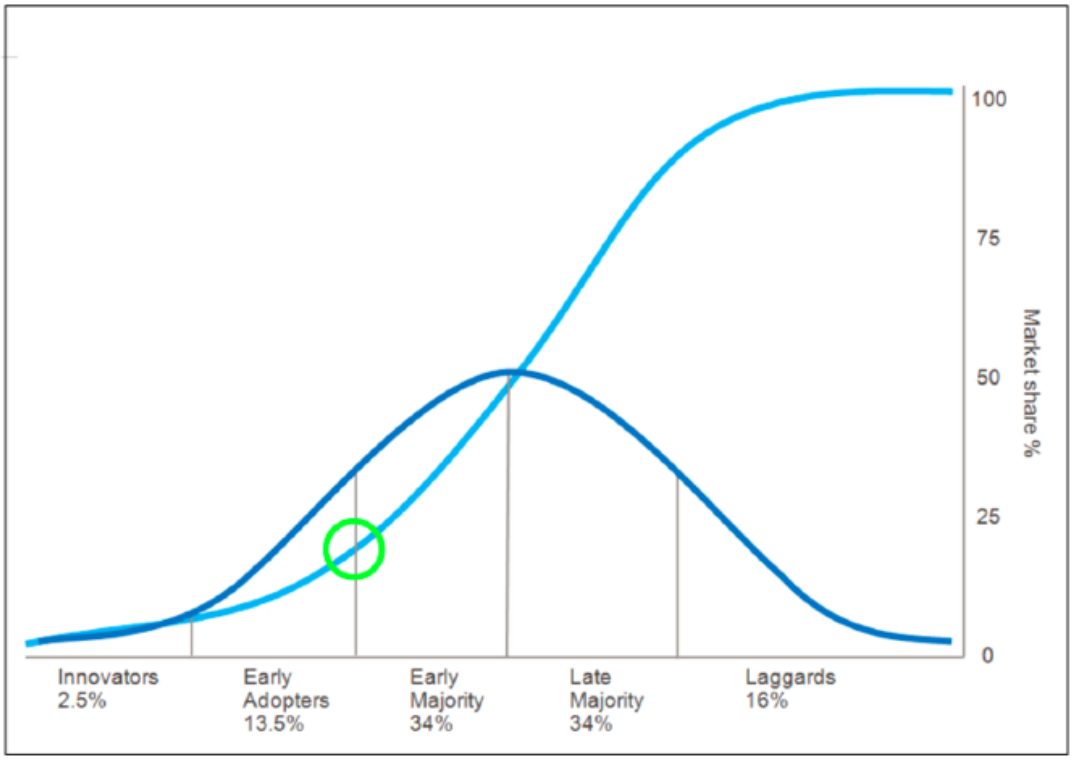
No matter how many people use the network, how advanced mining equipment becomes or how much its price increases, there can only ever be 21 million Bitcoins in existence. In time, it is likely that Bitcoin will be regarded as the best technology for saving ever invented.

Time Arbitrage [2,13,14]

Innovations of this magnitude are virtually impossible to predict; however, they do follow a familiar adoption pattern. The book titled 'Diffusion of Innovations' lays out a framework that seeks to explain how, why and at what rate new ideas and technologies spread. Diffusion is the process by which an innovation is communicated and adopted by participants in a social system over time. There are four main elements that influence the spread of the new idea:

- The nature of the innovation
- Communication channels
- Time elapsed since ideation
- The social systems under which it is adopted

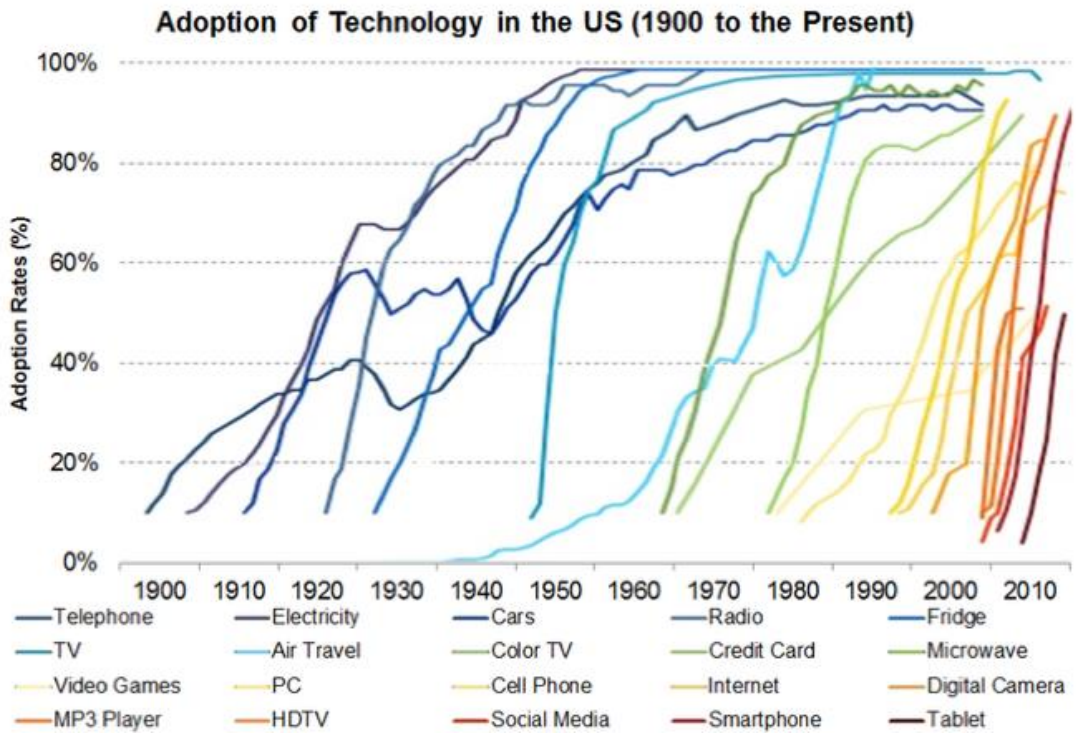
Once a certain rate of adoption is achieved, the innovation reaches a tipping point and its continuous spread becomes practically unstoppable (a concept of preferences closely related to the minority rule discussed earlier) as people naturally prefer superior technology solutions. Such an adoption curve is especially true of, and often completed faster for, network-based technologies such as the internet and Bitcoin; as their general acceptance is driven harder and faster by network effects. Based on its estimated number of users, we are just beginning to enter the early adopter phase for Bitcoin:



The S-curve of adoption. As succesive groups adopt a new technology or idea market share rises. The tipping point (green circle) marks an inflection point and leads to rapid growth in adoption.

In investing, the concept of *time arbitrage* refers to an asset becoming oversold based on a short-term or emotional market sentiment despite its long-term outlook or investment fundamentals remaining unchanged or even improving. Time arbitrage is essentially another form of the old investment adage "Buy on bad news, sell on good news". Times such as these present savvy investors with an opportunity to enter a position with the same or improved value fundamentals at a lower price point.

All ubiquitous technologies today, beginning as fledgling innovations themselves, have traversed this path to mainstream adoption. Here we show some of the most impactful innovations since the year 1900 and the rapidity with which they were adopted:



9As telecommunication networks have become more advanced and ubiquitous, the user adoption rates of new innovations have accelerated dramatically.

As we can see, advances in telecommunications and distribution methods have accelerated the pace with which new innovations are adopted. Today, the internet causes breakthrough innovations to spread like a wildfire throughout the minds of people all over the world. Since it is a nascent monetary technology that is not fully understood by the vast majority of the world, Bitcoin still has low levels of adoption and therefore significant upside prospects. Also, owning a piece of the Bitcoin network today is over 80% cheaper than about a year ago even though its utility in terms of throughput, transaction fee efficiency and network security have all improved substantially over the same period. This confluence of factors indicates that now is an opportune time to take advantage of time arbitrage and invest in the Bitcoin network. Also, as a technology, the Bitcoin network's value will continue to grow with every passing day that it successfully operates.

Lindy Effect [4,11]

Things in this world fall into one of two general categories: perishable and nonperishable. The distinction between the perishable (humans, single items) and the nonperishable is that the latter does not have a natural, unavoidable expiration date. The perishable is typically physical in nature, meaning it is subject to physical degradation, whereas the nonperishable is typically informational in nature. A single car is perishable, but the automobile as a technology has survived for a century and can be reasonably expected to persist for at least another one. An individual man will die, but his genes (which are digital)

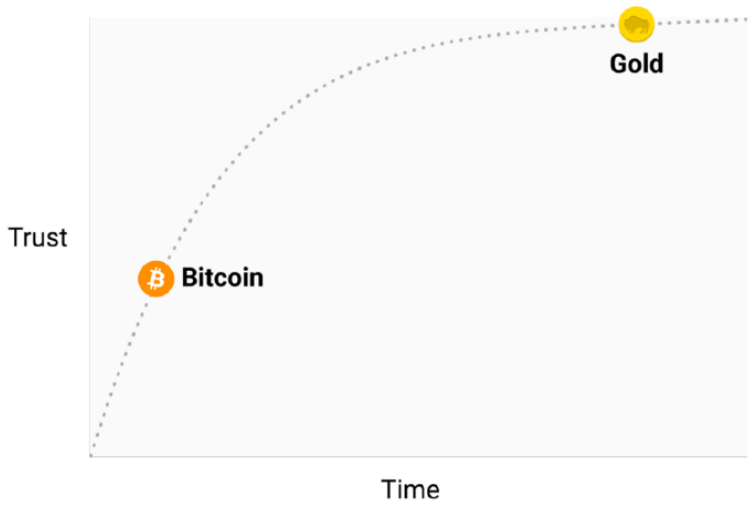
can be passed on for innumerable generations. This heuristic from Nassim Taleb, known as the *Lindy Effect*, can be summarized as follows:

- For the perishable, every additional day of life translates into a shorter additional life expectancy.
- For the nonperishable, every additional day of life may imply a longer life expectancy.

The only effective judge of things is time, as time is the ultimate destroyer of all things. The Lindy Effect is closely related to antifragility, as the ravages of time are a potent form of adversity. Anything that gains from temporally-driven increases in disorder is antifragile and benefits from the Lindy Effect. Using arbitrary math for simplicity, if a book is still in print after 50 years, it can be expected to remain in print for another 50 years. If it's still in print for another 50 years after that, then perhaps it can then be expected to remain in print for at least an additional 120 years. At some point, the Lindy Effect may imply an unlimited life expectancy. A book like the Bible, which has been in print for thousands of years, can be reasonably expected to remain in print for the rest of human history.

If you had conducted a survey in 1995 and asked people whether they believed the internet would be a permanent feature of their lives, you would have probably received mixed responses. If you conducted the same survey today, people would resoundingly agree that the internet is here to stay. A technology, being informational rather than physical in nature, does not age in the same way humans do. A technology like the wheel is not "old" in the sense of experiencing degradation, it is a technological design that has persisted for millennia and can be reasonably expected to persist for many more.

So, the longer a technology lives, the longer it can be expected to live. Since Bitcoin is a technology, every day that it continues to successfully operate increases its life expectancy. Further, as we have learned, the core moving parts of Bitcoin are mathematics and human nature—two concepts which are very "Lindy" and can be reasonably expected to persist for the rest of human history. Bitcoin's ever-growing life expectancy increases its perceived trustworthiness and eventually it will be regarded as a permanent feature of our modern lives in the same way the internet is today. This heuristic helps explain why gold will likely continue to be regarded as a monetary metal for many years to come, whereas Bitcoin is still in the process earning people's trust:



10 Hard monetary technologies become more trusted over time as they offer peace of mind to their users.

The Lindy Effect is universally applicable across time. The same competitive dynamics that caused the ascent of gold into a dominant monetary role are now driving Bitcoin adoption. In this sense, the future is in the past. As the Arabic proverb says: *he who does not have a past has no future.* Notwithstanding the past century of central bank coercion, hard money is the norm of human history and we are witnessing its reemergence with the rise of Bitcoin. As Bitcoin continues to persist, knowledge of its fundamental nature and functional capabilities will continue to spread. Threatened by its continued growth, incumbents will ratchet up their efforts to prevent Bitcoin's ascent and protect the monopoly on money they have enjoyed over the past century.

Future of Regulation [1,4,5,15]

There is a good reason why the gold standard was forcibly ended and no good store of value has yet risen to fill the void. To preserve seigniorage profits governments must enforce an inflationary monetary policy. Otherwise, if a sound store of value existed that was accessible to its citizenry, their business model would be jeopardized as people would exit depreciating fiat currencies to shield their wealth from further confiscation. As Alan Greenspan, former Chairman of the Federal Reserve (the central bank of the United States) said in 1966:

> ***"In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. There is no safe store of value. If there were, the government would have to make its holding illegal, as was done in the case of gold.*** *If everyone decided, for example, to convert all his bank deposits to silver or copper or any other good, and thereafter declined to accept checks as payment for goods, bank deposits would lose their purchasing power and government-created bank credit would be worthless as a claim on goods.* ***The financial policy of the welfare state requires that there be no way for the owners of wealth to protect themselves."***

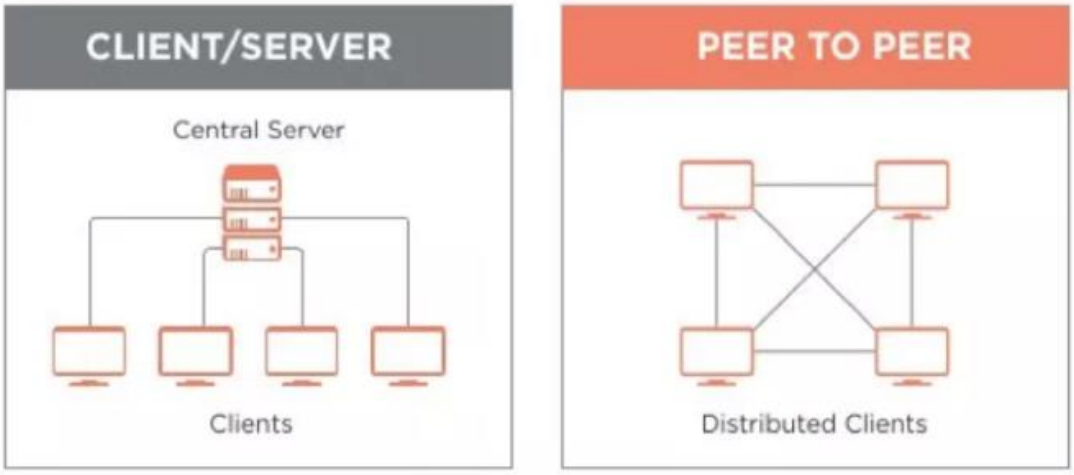
Clearly, central banks are aware that free market competition against hard money poses significant risk to the continuity of their socialistic business model. To protect central bank monopoly positions, governments have resorted to passing onerous laws against their citizens. Governments seek to insulate their national currencies from free market competition employing legal measures such as:

- Capital Controls—which prohibit the movement of money into or out of a country
- Confiscatory Orders—forceful seizure of assets, like Executive Order 6102 in 1933 which outlawed private ownership of gold in the United States
- Legal Tender laws—which create artificial demand for government fiat money by requiring that it be accepted in settlement of debts

With Bitcoin, regulators face a unique dilemma. Bitcoin exists orthogonally to the law, and there is virtually nothing that any authority (or anyone for that matter) can do to affect its operation. Regulations were designed to govern people and entities and are not equipped to deal with a decentralized network that autonomously proliferates itself. Regulators are really good at targeting centralized marks, like an individual business or its CEO, and enforcing laws against them. However, regulations have proven to be largely impotent against decentralized services.

To understand this point, consider the case of BitTorrent, a decentralized peer-to-peer file sharing service. In the earlier days of the internet, file sharing platforms like Napster and Kazaa had become an extremely popular way for users to share movies, music and other media directly with one another. With these free services, users would upload media to and download media from the companies' computer servers. This client-server file sharing directly threatened media monopoly profits, as it completely circumvented copyright law. Incumbent organizations quickly responded with heavy litigation. Since services like Napster and Kazaa were hosted by centralized companies complete with a headquarters, executive team and computer servers, they were vulnerable to being shut down. Filing a lawsuit, knocking on some doors, levying some fines and decommissioning some computer servers was all it took to shut down these services and protect media industry monopolists.

The introduction of BitTorrent, an open-source decentralized protocol for peer-to-peer file sharing, was a game changer. Once installed on a computer, BitTorrent enables user nodes to upload and download movies, music and other media directly from one another using encrypted communication channels. Since files on its network do not come from a single source, BitTorrent was also able to offer superior download speeds by fragmenting the media files and pulling from multiple nodes simultaneously. Unlike the failed client-server models of centralized platforms, the BitTorrent protocol never holds any of the media files, it only facilitates the transfer of files between individual users:



11 Like the proven model of BitTorrent, Bitcoin sports a decentralized architecture that makes it highly resistant to external attack and censorship.

Architecturally, the entire software codebase of the protocol exists on every user machine that downloads it, making it virtually impossible for a regulator to target and shutdown as there is no single point of vulnerability (censorship resistance). The BitTorrent protocol exists everywhere and nowhere by virtue of its decentralized network architecture, a model that would be later employed by Bitcoin. Indeed, without a centralized target to shut down, regulators were incapable of stopping BitTorrent and the other protocols it inspired. By 2009, peer-to-peer file sharing using decentralized protocols like BitTorrent accounted for up to 70% of internet traffic worldwide.

Bitcoin has already exhibited similar properties to BitTorrent as regulators have been incapable of containing the expansion of its network or shutting it down. It cannot be contained by capital controls, as it exists entirely outside the legacy financial system. Confiscation of Bitcoin, unlike that of gold, is extremely difficult given its informational nature. This leaves legal tender laws, which are still enforceable and could therefore require Bitcoin users to convert some of their holdings into government fiat money to pay their taxes. So, the exchanges and OTC markets where Bitcoin is traded are the only viable targets for regulators. As such, these financial gateways that connect Bitcoin to the traditional financial system are likely to see continuous intensification of regulatory scrutiny and enforcement actions. However, as we saw in China, escalated efforts will likely only highlight the need for Bitcoin, expand its brand awareness and spawn off exchange transactions (Streisand Effect).

In essence, open-source software projects like Bitcoin are just information—software written in a computer language called code. Since it is just code, Bitcoin can be printed out, written down, spoken or memorized. Bitcoin is also a form of money, so it makes money and information the same thing. This concept was summed up nicely by Naval Ravikant in 2017:

"This is one of the crazy things about this concept because money and speech turned out to be the same thing—money, information and math—they're the same thing. In a Bitcoin world, I can literally write down my Bitcoin address and keys on a piece of paper and put it in a safety deposit box. It's basically in cold storage, I could even put it in my head. I can memorize the key phrases and I could cross national borders with $1 billion in my brain. It's a very powerful but literally mind bending concept in that sense."

The First amendment of the United States Constitution guarantees that all Americans have the power to exercise their right to publish and distribute anything they like, without restriction or prior restraint—which includes software code like that which constitutes Bitcoin. Established legal precedent in the United States explicitly protects software code under the First Amendment. Consider the case of PGP:

"In 1995, the US Government had on the statute books, laws that restrict the export of encryption software products from America without a license. These goods are classified as 'munitions'. The first versions of the breakthrough Public Key Encryption software "Pretty Good Privacy" or "PGP", written by Philip Zimmerman had already escaped the USA via Bulletin Board Systems from the moment it was first distributed, but all copies of PGP outside of the United States were "illegal". In order to fix the problem of all copies of PGP outside of America being encumbered by this perception, an ingenious plan was put into motion, using the first Amendment as the means of making it happen legally. The source code for PGP was printed out. It's as simple as that. Once the source code for PGP was printed in book form, it instantly and more importantly, unambiguously, fell under the protection of the First Amendment."

Bitcoin unambiguously falls under the Freedom of Speech Protections offered by the First Amendment to the United States Constitution.

For these reasons, it is unlikely that any major government would attempt to ban Bitcoin outright as, not only would it contradict freedom of speech laws, it would also create a tidal wave of publicity (again, Streisand Effect). Central banks have acknowledged this reality. Former chairwoman of the Federal Reserve Janet Yellen confirmed:

"The Federal Reserve simply does not have the authority to supervise or regulate Bitcoin in any way."

So, Bitcoin can't be shut down, is virtually immune to regulation and leverages economic incentives to grow relentlessly. Its very existence is a game changer for almost everyone in this world, especially central banks who now face an existential threat to their business model.

The Long Game [1,4,16]

Money is how we keep score in the game of life. *Game theory* explores how rational people make strategic decisions in different scenarios. It is based in purely mathematical terms and has applications in any domain where people must choose whether to cooperate or compete with each other. The standard game analyzed by game theory is the Prisoner's Dilemma:

Two members of a criminal gang, Alex and Bobby, are arrested and imprisoned. Each prisoner is in solitary confinement with no means of communicating with the other. The prosecutors lack sufficient evidence to convict the pair on the principal charge, but they have enough to convict both on a lesser charge. Simultaneously, the prosecutors offer each prisoner a bargain. Each prisoner is given the opportunity either to betray the other by testifying against them, or to cooperate with the other by remaining silent. The possible decisions and outcomes are:

- *If Alex and Bobby both betray each other, each of them serves 2 years in prison*
- *If Alex betrays Bobby but Bobby remains silent, Alex will be set free and Bobby will serve 3 years in prison*
- *If Bobby betrays Alex but Alex remains silent, Bobby will be set free and Alex will serve 3 years in prison*
- *If Alex and Bobby both remain silent, both of them will only serve 1 year in prison (on the lesser charge)*

This game decisions and its outcomes are summarized in this table:

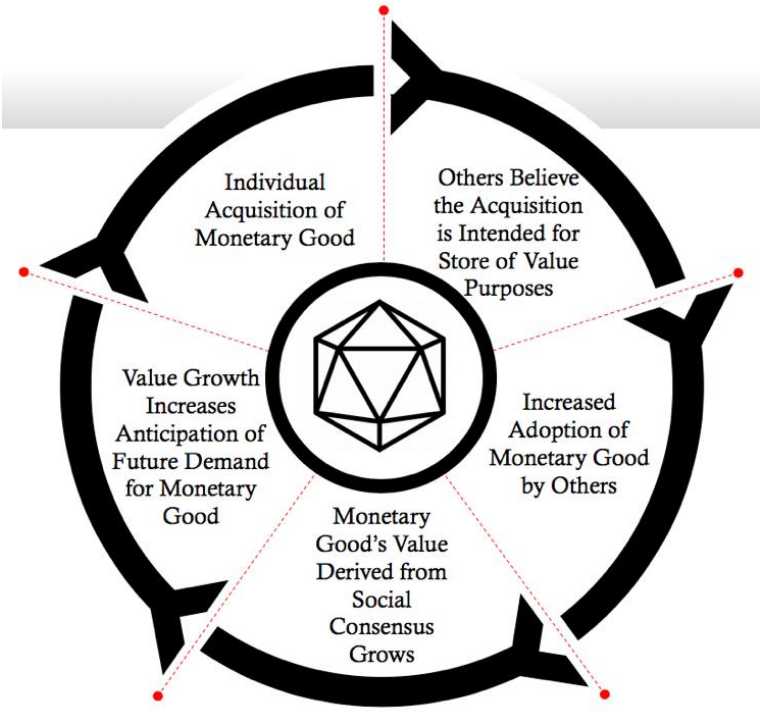
		Bobby's decisions	
		Bobby stays silent (cooperates)	Bobby testifies (betrays)
Alex's Decisions	Alex stays silent (cooperates)	Alex and Bobby each serve 1 year	Alex serves 3 years, Bobby goes free
	Alex testifies (betrays)	Alex goes free, Bobby serves 3 years	Alex and Bobby each serve 2 years

12 Game theory shows us that adversaries will often behave contrary to their mutual best interests.

This Prisoner's Dilemma game converges on a *Schelling Point*, which is a solution that people will tend towards in the absence of communication or definitive trust (in other words, in an adversarial environment). The Schelling Point in the Prisoner's Dilemma is that Alex and Bobby both choose to betray each other, as each would risk 3 years in prison if one chose to remain silent and the other testified. Since both have an incentive to testify, the optimal strategy for this game is that they both betray, despite their mutual silence offering the best outcome for them both.

Since money is an adversarial game (there are winners and losers) express communications between players cannot always be trusted. Therefore, the Schelling Point of monetary competition is to choose the available good which exhibits the highest hardness, because people (potential adversaries) must be restrained from creating new monetary units to steal the value stored within them. This is exactly the reason market-driven natural selection is so ruthlessly effective at promulgating hard money, as people are constantly seeking to acquire value and store it in the most reliably hard monetary technology available.

Monetary goods, like Bitcoin, are valued based on their game theoretic qualities—meaning each market participant values a monetary good based on their appraisal of whether and how much other participants will value it (in the same way that prisoners Alex and Bobby must anticipate each other's decisions to make effective decisions of their own). The earlier one is able to anticipate the future demand for a monetary good, the greater the advantage conferred to the prognosticator; as it can be acquired more cheaply than when it becomes widely demanded at a later time. Further, when one acquires a good expecting that it will be demanded as a future store of value, it actually hastens the adoption of the good by others for that particular purpose, as their selection of a store of value is partly influenced by their perception of your intentions which drove you to acquire the monetary good in the first place. This seeming circularity is another positive feedback loop that drives societies to converge on a single store of value (another aspect of the winner take all dynamic):



13 The game theoretic properties of the monetization process encourage people to converge on a singular money

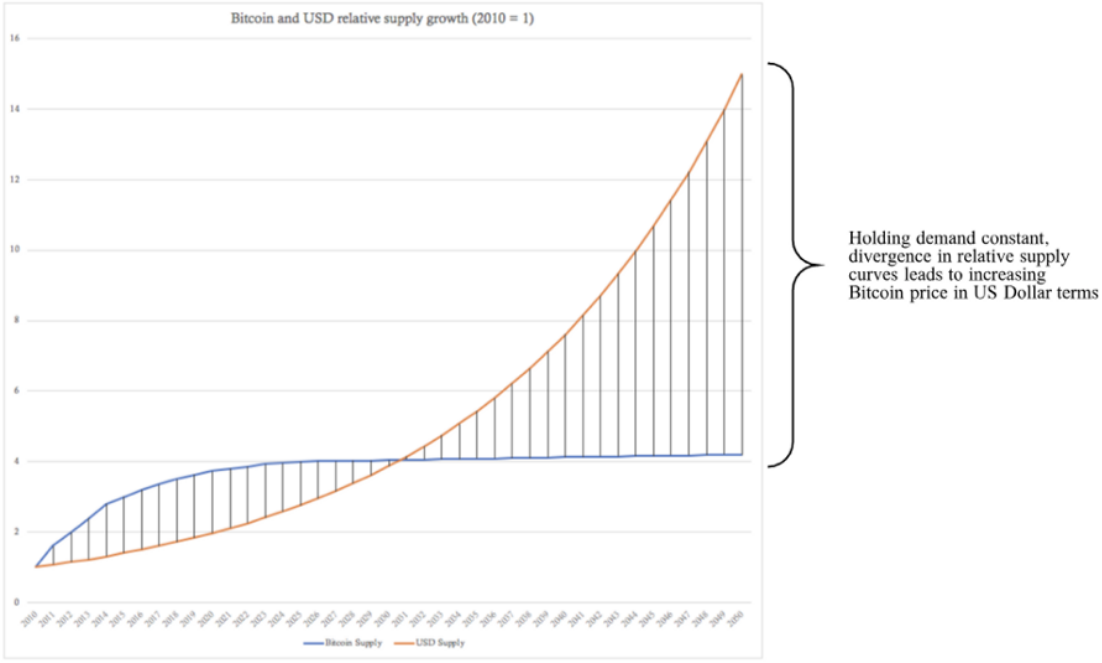
.

In game theoretic terms, total market dominance by a single store of value with a superior stock-to-flow ratio is known as a *Nash Equilibrium*—a game state where no player has an incentive to deviate from his chosen strategy after anticipating the most likely choices of all his opponents. Throughout all human history, societal convergence on a single form of superiorly hard money is the Nash Equilibrium of monetary competition. As we saw with gold in the 19th century, when multiple societies converge on a single store of value, they see a substantial decrease in trade costs and an attendant increase in free trade and capital accumulation (La Belle Époque). Only the past century, dominated by government fiat money, is anomalous in this respect.

Hard money is the norm of human history, and we are seeing its reemergence with Bitcoin.

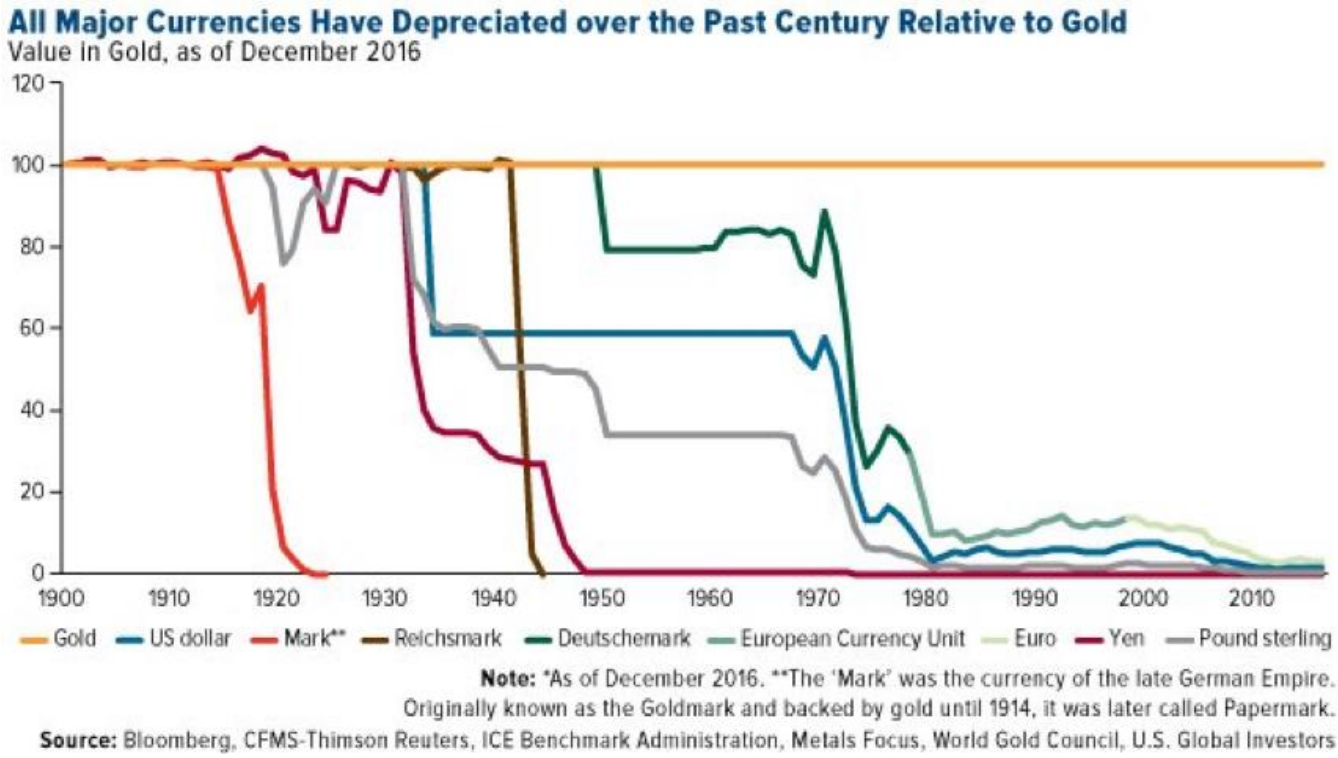
The monetization process, as we saw with gold and are now seeing with Bitcoin, is game theoretic. People must decide individually how best to store the value created by their time spent in production. This decision is based on the anticipated beliefs, decisions and actions of others in relation to the monetary technologies available to them. The complex interaction of these decision dynamics is how people spontaneously ascribe a good the role of money and why the hardest money always wins. In this way, hard money is an emergent property of indirect exchange just like money is an emergent property of direct exchange.

This emergent property perspective is exactly why value stored in softer forms of money is totally absorbed by hard money every time they interact within an economic network. Existing amid the expansionary monetary policies being practiced by every central bank in the world today, Bitcoin's price will continue to increase as the ratio of government fiat money in circulation to Bitcoin units in circulation diverges ever-further:



This graphic, which is strictly illustrative, simply shows that divergence in supply curves of Bitcoin and US Dollars will lead to the appreciation of Bitcoin in US Dollar terms, even without any increase in the demand for Bitcoin (as we have seen, demand for Bitcoin has been surging). The same dynamic is applicable to all modern government monies, as every central bank in the world is engaged in aggressive expansionary monetary policy. In the game of international government fiat monetary competition, the Nash Equilibrium is all currencies inflated into worthlessness. On this race to the bottom, those with easiest access to freshly printed money will expropriate as much value as possible (via the Cantillon Effect) and use it to acquire real estate, gold or other inflation resistant assets (such as Bitcoin). This game theoretic perspective clearly explains why virtually all soft government fiat currencies have trended towards eventual worthlessness.

Next, we show how all major fiat currencies have depreciated almost completely against gold since 1900 (notice the steep decline in 1971 when the peg to gold was completely severed):



As we have seen throughout history, every time hard money encounters soft money in a trade network, it has outcompeted it into extinction. We saw earlier how gold, possessing superior hardness, demonetized silver with dire economic consequences for those societies that remained on a silver standard the longest, such as China and India. Now it is gold that faces a monetary competitor with superior hardness, and it is likely that it will gradually become demonetized as people convert to Bitcoin for its unparalleled store of value properties. This will happen slowly, and gold may indeed maintain some of its monetary use case given the vast holdings of central banks, mankind's deep history with

the monetary metal (Lindy Effect), its relatively high and predictable stock-to-flow ratio and the fact that some people may always prefer a tangible store of value over a digital alternative. For government money, the competitive situation is much more dire.

The Event Horizon [1,4,16]

Hyperinflation is a particular type of demonetization, unique to government fiat money, that did not exist under the gold standard. Hyperinflation occurs when a government produces new monetary units at an accelerating pace to finance expenditures or service debt burdens, which pushes the value of its currency down at the same accelerating rate. The value of a hyperinflating currency collapses against the most liquid goods available to the society first (like gold or the US dollar) and then, depending on relative availability, against real goods such as real estate and commodities. This sequence is caused by individual's attempting to maximize their exchange optionality as they escape their failing currency and prepare to navigate highly uncertain economic conditions. When hyperinflation intensifies, currencies begin falling against perishable goods. It is common to see grocery stores completely emptied out in societies suffering from the late stages of hyperinflation. Eventually, the society will either devolve to a barter economy or adopt a new medium of exchange, as we saw in Zimbabwe when its failing dollar was ultimately replaced by the US dollar. This process is arduous as the replacement currency is often scarce as foreign banking institutions are either reluctant to or restricted from providing liquidity.

As Bitcoin is the hardest form of money in existence, it will continue to appreciate against a backdrop of hyperinflating, soft government fiat currencies even without any increase in demand for Bitcoin (as illustrated in the above graphic). Eventually, this will lead to an inflection point in some economies where users rush to exit from their failing currency to get into Bitcoin to protect their wealth from further confiscation. This transition will have similar dynamics to other demonetization and hyperinflation events, however it will also be different given Bitcoin's unique properties as a monetary technology. A Bitcoin-induced currency demonetization is called a *hyperbitcoinization event* and is different from hyperinflation in two critical respects.

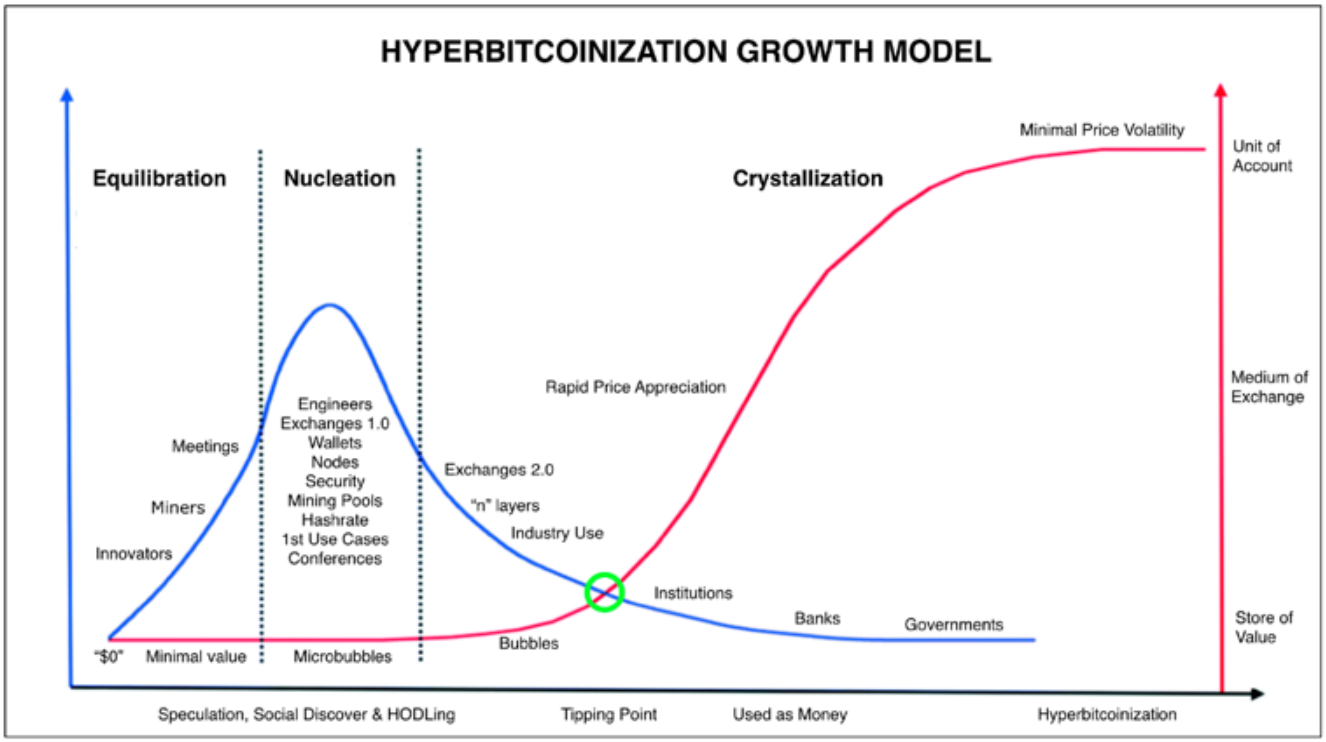
First, hyperinflation occurs with restricted competition with other fiat currencies, since a government can easily enforce capital controls that selectively prohibit inflows or outflows of government money, whereas hyperbitcoinization occurs because of direct competition with Bitcoin, which can easily cross borders as it is immune to capital controls. This will cause hyperbitcoinization to happen much faster than a hyperinflation event, since governments will have great difficulty preventing Bitcoin trading within their borders due to its purely informational nature. Given governments' inability to shield their local currencies from direct competition with Bitcoin and the high opportunity cost of holding a depreciating form of money, once a hyperbitcoinization event reaches a critical mass it will happen quickly.

Second, in hyperinflation, the governments expand money supplies in an attempt to outpace people's inflation expectations. As governments forms a habit of inflating money supplies, people form a habit of anticipating rising prices and seek alternative stores of value. Governments, in turn, must print incrementally more money to stay ahead of inflation expectations and generate the same economic effect with each new monetary unit produced. With no alternative monetary media in which to escape, prices surge until a breaking point is reached. Hyperinflation is extremely disruptive to an economy as it forces people to switch from the worst form of government fiat money available to them to some other soft government fiat money (at best) or ends in total economic collapse (at worst). In hyperbitcoinization, users have a supranational monetary media in which to escape centrally planned economies. Therefore, a hyperbitcoinization event should be much less disruptive to the economy, as people will be trading in an inferior form of money for a superior one. Seeing as hyperbitcoinization should happen fast, people will quickly become accustomed to dealing in Bitcoin, which will protect deteriorating wealth and stabilize economic conditions.

Hyperbitcoinization will likely be a confusing, potentially chaotic, time for many people. Initially, it will probably occur at the periphery, with the countries inflating their currencies the fastest experiencing it first. Stories of this will spread quickly in the digital age and add to the believability of Bitcoin, all while it continues to benefit from the resultant increases in demand, network effects and the Lindy Effect. As more people wake up to the reality of hard money, we would expect the pace of this global transition to accelerate until all soft money is outcompeted into extinction. Fortunately, it will happen relatively quickly, since Bitcoin is immune to capital controls, and act as a stabilizing force for the world economy going forward (since hard money resists market distortions and remains firmly rooted in economic reality).

Like a star orbiting a black hole, any established monetary order that goes beyond the event horizon of hyperbitcoinization will inevitably collapse into Bitcoin's singularity.

Next, we show how a hyperbitcoinization event is likely to unfold:



Once Bitcoin's ecosystem is seeded a crystallization process begins. Growth becomes exponential and self-reinforcing. In this model, the tipping point (green circle) represents a dramatic change at which point many people and oganizations adopt Bitcoin.

The estimates of how valuable Bitcoin would become after global hyperbitcoinization vary based on what weighting is included for different stores of value (gold, government money, real estate, stocks, bonds, art, oil and other commodities are all used for this purpose today) but, using simple math for our directional analysis, if Bitcoin demonetizes just gold it would be valued at about $400K per coin ($8T/20M coins in 2025). If it demonetizes government money as well, it would be valued at about $5M per coin ($100T/20M coins in 2025). As awareness of Bitcoin and its potential impact spread, the long game becomes even more interesting. Considering Bitcoin represents an existential threat to government fiat money and central banks, we must also consider their decisions from a game theoretic perspective.

Reverse Bank Run [1,4,5]

Although it is still considered magic internet money by most people today, its continued existence and appreciation will attract more attention from high-net-worth individuals, institutional investors and then, possibly, central banks. As we have learned, central banks still rely on gold as a means of final settlement, as it was (before Bitcoin) the only monetary medium entirely free of counterparty risk (cash money). However, transporting and securing gold is an extremely expensive process fraught with operational risk. These costs and risks are the reason final settlements between banks occur very infrequently.

With the transaction throughput available on the Bitcoin network today, the global group of 850 central banks can perform daily final settlement with one another. With each central bank serving an average of 10 million customers, this would more than cover the entire world's population. In a world in which central banks adopted a Bitcoin standard, governments would no longer have the ability to increase the money supply and banks would begin to compete freely with one another by offering various physical and digital Bitcoin-backed monetary instruments and payment solutions. By using the technologies introduced by Bitcoin, cryptographic digital certainty can be applied to bank accounting and help expose those that engage in fractional reserve banking. This may lead to Bitcoin realizing its ultimate use case: the fastest and most efficient system for global final settlement across long distances and national borders. Despite the clear advantages of a system such as this, central banks are unlikely to give up their monopoly control over the existing monetary order willingly.

As people begin to voluntarily exit fiat currencies into Bitcoin to protect their wealth, as is already taking place in countries like Venezuela today, it will likely grab even more attention from central banks. As central banks are effectively losing customers, they will need to hedge the *going concern risk* posed to their business model. Central banks today hold reserves mainly in US Dollars, Euros, British Pounds, IMF Standard Drawing Rights and gold. These reserves are used to settle accounts and defend the market price of their respective currencies. Should Bitcoin remain on its current trajectory, and considering its superiority as a final settlement layer, it is possible that at least one central bank somewhere in the world will add Bitcoin to its reserves, if for no other reason than to defend the market price of its government fiat money, as is consistent with their strategy for gold.

The most likely scenario is that a central bank will seek to own part of the Bitcoin network as an insurance policy against it succeeding. Strategically, it makes sense for a central bank to spend a small amount acquiring some of Bitcoin's supply today. For example, consider that the authorities of a central bank today judge that, although chances of a hyperbitcoinization event are extremely remote, it would represent an extinction-level event for their business. Mathematically, using Bitcoin's approximate price today of $4K and its expected post-hyperbitcoinization price of $5M, unless the central bank is more than 99.92% certain that this event will NOT happen then it is prudent to allocate at least 0.08% of their assets into Bitcoin as a perfect hedge against its success (since price growth from $4K to $5M is a 1250x increase, an allocation of 0.08% of assets would keep a central bank at even-money should a hyperbitcoinization event play out).

Game theory tells us that the first central bank to buy Bitcoin will trigger a reverse bank run, as its decision will alert the rest of the central banks who will be compelled by self-interest to follow suit. The first purchase by a central bank will cause the price of Bitcoin to rise significantly, causing others to move in based on their anticipation of future demand and compounding the effect as more central banks enter the market; making it progressively more expensive for later entrants. As central banks keep trying to anticipate the moves and strategies of one another, a game theoretic positive feedback loop will ensue that converges on a hard money Schelling point similar to that of free market

monetary competition, thus triggering a global competition among central banks for maximal Bitcoin accumulation. A smart play for a central bank under the circumstances would be for it be the first to buy a small share of the Bitcoin network. An even smarter play would be for a central bank to purchase Bitcoin without announcing it, allowing it to begin accumulation at lower prices.

Similar to the transition to the gold standard in the 19th century, network effects would eventually take hold as more central banks bought some Bitcoin, increasing its liquidity and making it more marketable, thus creating ever-larger incentives for other central banks to join. After a sufficient minority of central banks have purchased part of the Bitcoin network, the minority rule will reach its final step and begin imposing the immutable rules of Bitcoin on the established monetary order. Once this reverse bank run on Bitcoin became public knowledge (as tends to happen easily in the digital age), it would be the ultimate seal of legitimacy for Bitcoin adoption and would add even more force to its ascent in the marketplace as this global game of Bitcoin accumulation would reach a fever pitch. Even at the largest scales of the financial system, Bitcoin converts individual self-interest into the growth of its network.

You may find this prospect hard to believe. About 25 years ago, handheld touchscreen supercomputers with wireless global interconnectivity were hard to believe too. Change keeps happening faster and faster. Remember, each central bank will value Bitcoin based on its appraisal of whether and how much other central banks will ultimately value it. As they will all be conducting the same strategic analyses, they will undoubtedly realize the dilemma they face—either ignore Bitcoin and watch it continue to outcompete and accelerate the failure rate of fiat currencies thereby loosening their control over the established economic order or choose to adopt Bitcoin as a reserve asset and trigger a game of accumulation against other central banks and legitimize it as an asset which will culminate in the loss of their monopoly position in the market for money. Operating in an adversarial environment, game theory tells us that so long as Bitcoin continues to operate in its current form, central banks (like the prisoners Alex and Bobby) will eventually be faced with strategic choices such as these to protect their own interests. At some point, the substantial advantage imparted to the central bank that moves first will become an overwhelming incentive to at least one, causing it to be the first to make its move, thereby triggering the reverse bank run on Bitcoin.

A Path to Prosperity [1–16]

Making predictions is risky business, wrong answers are innumerable, and the right answer is singular. Accurate predictions are rare. By weaving together historical knowledge and awareness of current trends, one can develop a perspective on what technological innovations are possible. The biggest mistakes people make when making such predictions are:

- Forming an opinion on the innovative potential without considering it deeply (Blockbuster quickly reaching a decision to pass on buying Netflix for $50M)

- Disregarding an innovation because it contradicts a closely held worldview (Kodak refusing to accept the disruptive potential of digital photography as they spent 100 years building a business model centered on chemical film)
- Overlooking an innovation because it is too small or threatens a position of power (major newspapers refusing to develop an online presence early on)

Practicing a beginner's mindset and reasoning from first principles is critical for effective foresight. Pulling together everything we have discussed in this paper, we will now propose a potential path forward for Bitcoin based on the historical competitive dynamics of money, current macroeconomic trends and game theory. We will start from the inception of Bitcoin:

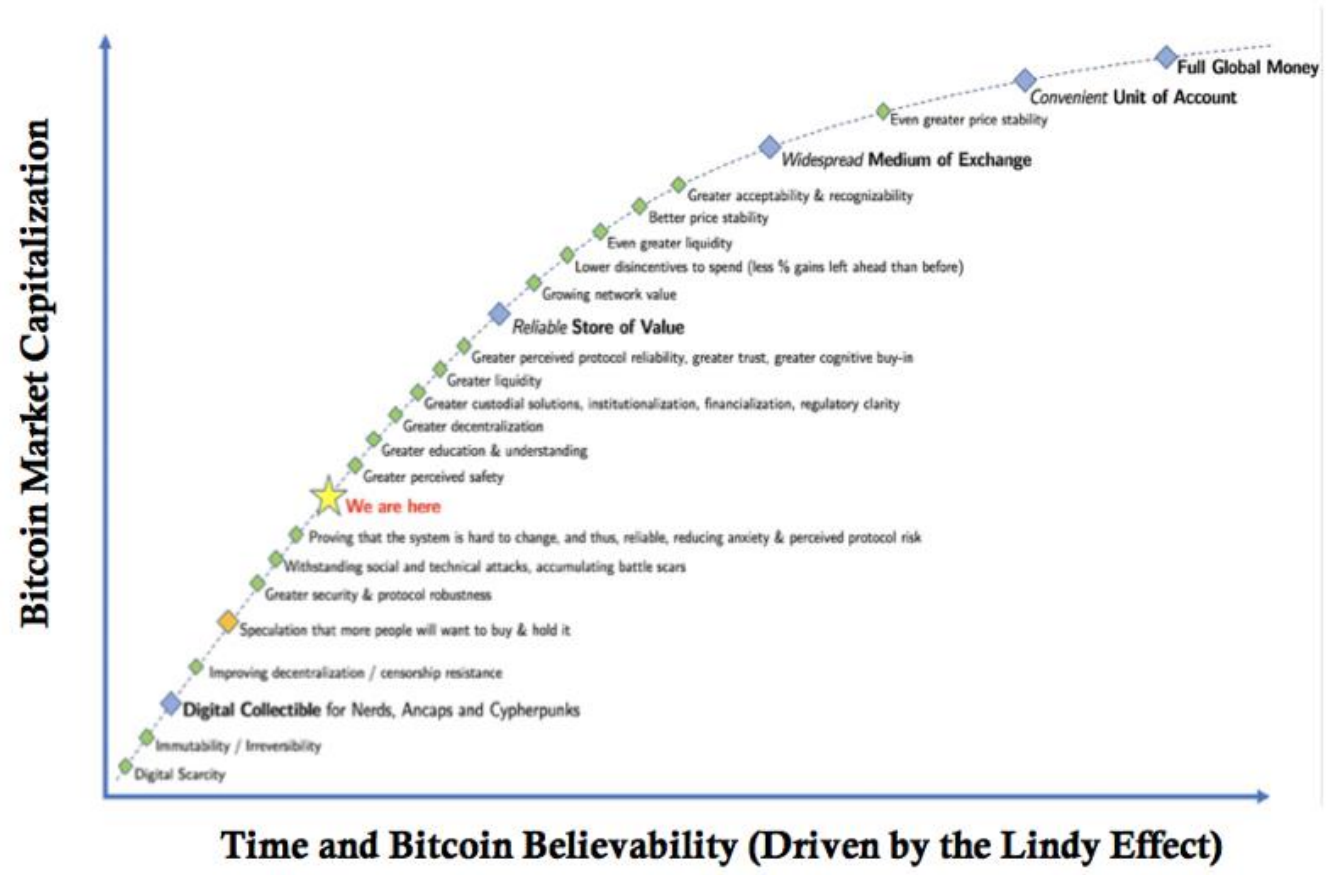
1. *Bitcoin is first perceived as an internet toy for cryptographers (Minority Rule—Step 1)*
2. *Its rapid price increase makes a small group of people rich, engages free market fanatics and brings media attention. Its hyper-volatile price presents itself early (Hodlers of Last Resort—Layer 1).*
3. *The media, financial and tech establishments—having failed to buy Bitcoin early and benefit from its meteoric rise—denounce it as a Ponzi scheme, the MySpace of Cryptocurrencies and the greatest bubble of all time (Streisand Effect).*
4. *A large number of scammers jump onto the Bitcoin hype-train and create their own cryptocurrencies claiming to be superior though lacking critical qualities including decentralization, security and immutable governance. Bitcoin's serendipitous first mover advantage, multi-sided network effects and its brand awareness fueled by the Nakamoto creation myth preserves its market dominant position.*
5. *Retail investors, venture capitalists and hedge funds—lacking understanding of monetary economics and applying inappropriate valuation models—invest into other cryptocurrencies, creating more noise and confusion as the prices of these altcoins increase at a rate higher than Bitcoin.*
6. *Well-connected venture capitalists and hedge funds are given discounts on the investments only to then dump much of what they bought onto retail investors.*
7. *Given their high correlation to Bitcoin and lacking utility, the world watches as the bear markets continue to wipe out more and more alternative cryptoassets as most fail to deliver any useful product, although some succeed in other market spaces. Features that are proven in the market by other cryptoassets are subsumed by Bitcoin (Decentralized Network Archetype). Bitcoin price volatility persists but annual low prices continue to ascend relentlessly (Holders of Last Resort—Layer 2).*
8. *Trust in Bitcoin increases over time (Lindy Effect) and its market price continues its upward yet volatile trajectory (Fractal Wave Patterns).*
9. *People, burned in the altcoin craze, witness and learn about Bitcoin's undisputed superiority across all monetary characteristics, especially its hardness (Holders of Last Resort—Layer 3).*
10. *On the eve of and during the next bull markets, Bitcoin's absolute scarcity and antifragile characteristics exacerbate investor FOMO (Game Theoretic Positive Feedback Loop). Some investors are inevitably caught in the subsequent Bitcoin price crash (Fractal Wave Pattern)(Hodlers of Last Resort—Layer 4).*
11. *Hyperinflating fiat currencies are further contributing to the adoption of Bitcoin as it becomes the only means of preserving wealth for many people, making Bitcoin a legitimate store of*

value. Governments scramble to try and enforce capital controls and create propaganda against Bitcoin, just like they did to gold in the 20th century. Capital controls prove to be impotent and the propaganda against Bitcoin incites internet and media narratives that regard it as a tool for freedom (Antifragility). Government dissent highlights the need for Bitcoin in the first place (Streisand Effect).

12. *Investors and high net-worth individuals are convinced to allocate a small portion of their assets into Bitcoin to capture further growth, hedge against inflation and increase the risk adjusted returns of their traditional portfolios (Minority Rule—Step 2)*
13. *Increases in demand for Bitcoin necessarily involve a reduction in demand for fiat currencies, causing even higher inflation rates (Gresham's Law). At great expense and effort, governments messily issue their own cryptocurrencies but fail to relinquish control over monetary policy, which makes them uncompetitive against Bitcoin (Market-Driven Natural Selection). Governments covertly attempt to attack the Bitcoin network, which only strengthens it (Antifragility). Media coverage about Bitcoin shifts towards its use as hard money (Skin in the Game) and its importance for prosperity (Hodlers of Last Resort—Layer 5).*
14. *Activists share the message that soft money creates social inequality (Soul in the Game) by disproportionately taxing the poorest via inflation (Cantillon Effect). This message spreads fast in a world of ever-more crashing fiat currencies and people rush to exit their local currencies for the safety of Bitcoin, triggering the first hyperbitcoinization events (Hodlers of Last Resort—Layer 6). Bitcoin mining hardware becomes commoditized and many citizens join mining pools (Decentralized Network Archetype)(Skin in the Game).*
15. *Central banks, in an attempt to adapt to the new conditions and hedge going concern risks, quietly start to accumulate Bitcoin as a reserve asset, consistent with their gold strategy. A former central bank employee leaks a confidential strategy document regarding Bitcoin (Soul in the Game) which triggers other central banks to begin purchasing Bitcoin, causing its price and perceived legitimacy to increase at an accelerating rate (Game Theoretic Positive Feedback Loop)(Final Fractal Wave Pattern)(Hodlers of Last Resort—Layer 7).*
16. *Bitcoin's market capitalization reaches tens of trillions in US Dollar terms. Bitcoin's volatility subsides as both its market capitalization and liquidity are larger than ever (Mature Hard Money).*
17. *Early Bitcoin investors are now sitting on significant unrealized gains and are willing to part with some of their Bitcoin to pay for their purchases. With its purchasing power stabilized, the opportunity cost of transacting with Bitcoin is diminished and its use as a Medium of Exchange increases.*
18. *With the world more digitized than ever before, people increasingly demand to be paid in Bitcoin now that it has proven to be a good store of value given its disinflationary, and later deflationary, monetary policy (Schelling Point)(Hodlers of Last Resort—Layer 8).*
19. *With the addition of highly performant transaction layers, Bitcoin's use as a Medium of Exchange becomes a widespread. Bitcoin, functioning as the core of a new innovation wave called the TrustNet, is christened as a momentous innovation.*
20. *As more consumers and merchants become accustomed to transacting in Bitcoin, it gradually becomes used as a Unit of Account.*
21. *Due to the emergence of a superior, uninflatable monetary standard, people increasingly store their wealth in Bitcoin rather than fiat currencies (Minority Rule—Step 3)(Hodlers of Last Resort—Layer 9).*

22. *Central bank monopolies on money are described by historians as a relic of the past. Bitcoin is regarded as the catalytic innovation behind the separation of money and state. A free market for money is now the defining feature of free market capitalism (Nash Equilibrium).*

This path to full global money will take Bitcoin through many stages:



Time Will Tell

All time beyond the present is unknown. All predictions should always be taken with a grain of salt. The future is uncertain, and the end can always be near. Anyone who claims they can tell you what is going to happen in the future is wrong. All we can do is study the patterns of the past and use them as our map to navigate the ever-advancing territory of the future.

In a free market, hard money has always outcompeted soft money into extinction. Hard money has been the norm throughout all of human history, except for the past 100 years in which we have been coerced into using soft government fiat money. Societies operating on hard money systems optimize for the allocation of the ultimate resource, human time, which increases prosperity for everyone.

In the digital age, markets are increasingly interconnected. Bitcoin is digital cash money. It is a new social institution that lives in accordance with its own laws. Its core components are human self-interest and mathematics. Bitcoin is the hardest monetary technology in history. Will it continue to outcompete and win the throne of full global money?

Only time will tell.

Synthesized Works & Further Reading

- [1] *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] *The Rational Optimist* by Matt Ridley
- [3] *Skin in the Game* by Nassim Nicholas Taleb
- [4] *The Bullish Case for Bitcoin* by Vijay Boyapati
- [5] *The Age of Cryptocurrency* by Paul Vigna and Michael J. Casey
- [6] *Sapiens* by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism, Part 1 and Part 2* by Brandon Quittem
- [8] *PoW is Efficient* by Dan Held
- [9] *The Fifth Protocol* by Naval Ravikant
- [10] *Unpacking Bitcoin's Social Contract* by Hasu
- [11] *Antifragile* by Nassim Nicholas Taleb
- [12] *Letter to Jamie Dimon* by Adam Ludwin
- [13] *Placeholder VC Investment Thesis Summary* by Joel Monegro and Chris Burniske
- [14] *Diffusion of Innovations* by Everett M. Rogers
- [15] *Why America Can't Regulate Bitcoin* by Beautyon
- [16] *Hyperbitcoinization* by Daniel Krawisz

Disclaimer:

THIS CONTENT IS STOLEN.

TIP THE CREATORS.

This is inspired by @NLW. You are the champion of great content and we salute you.

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 members of the any specific business, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile, Don't fuck around with this stuff because you might get burned.

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.

This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same.

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.

DYOR