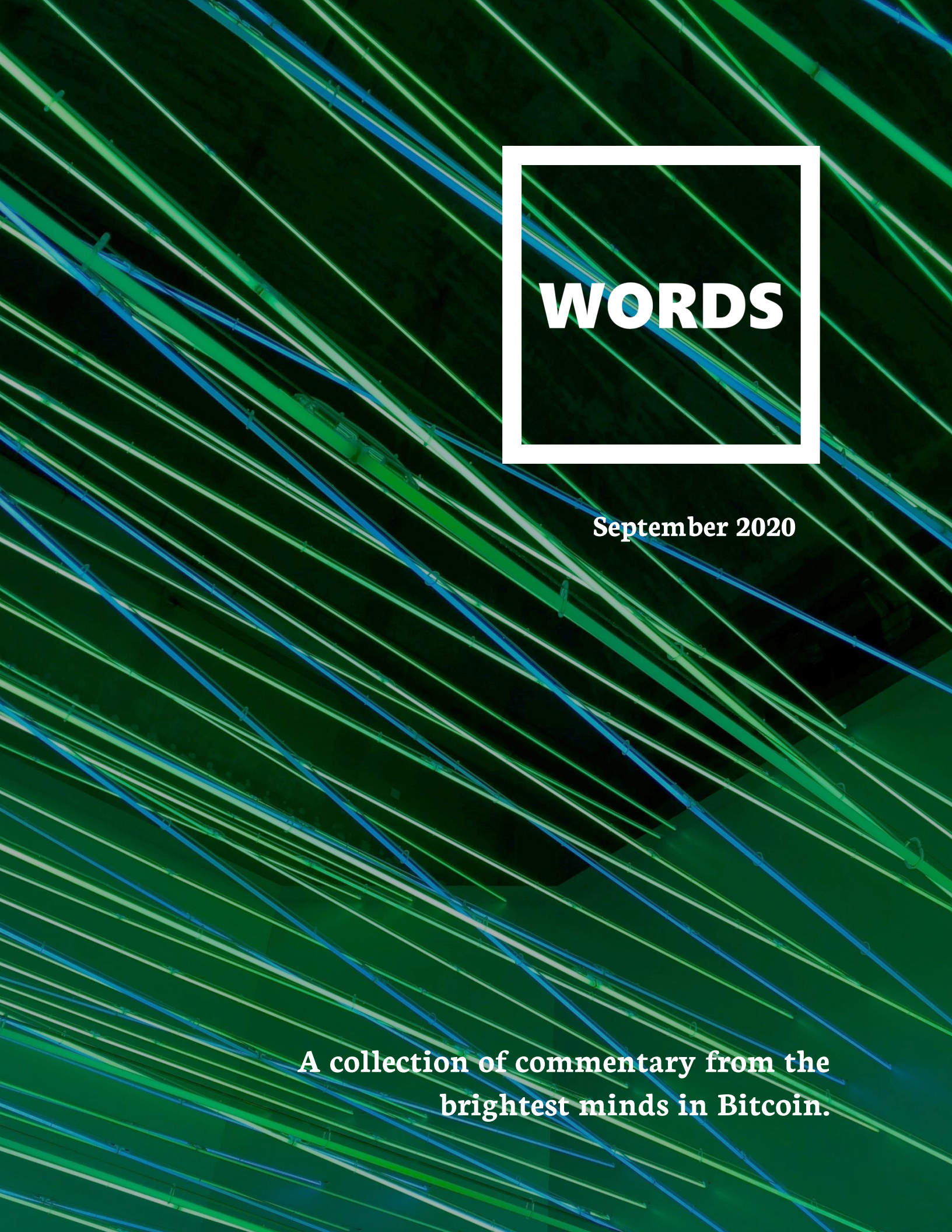


September 2020

A collection of commentary from the brightest minds in Bitcoin.

Contents

Goals and Scope

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

History

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

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

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

Support WORDS

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

Support WORDS

Spread the word

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

Follow us on social media

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

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

Twitter

Subscribe to our newsletter

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

Subscribe

Our pledge

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

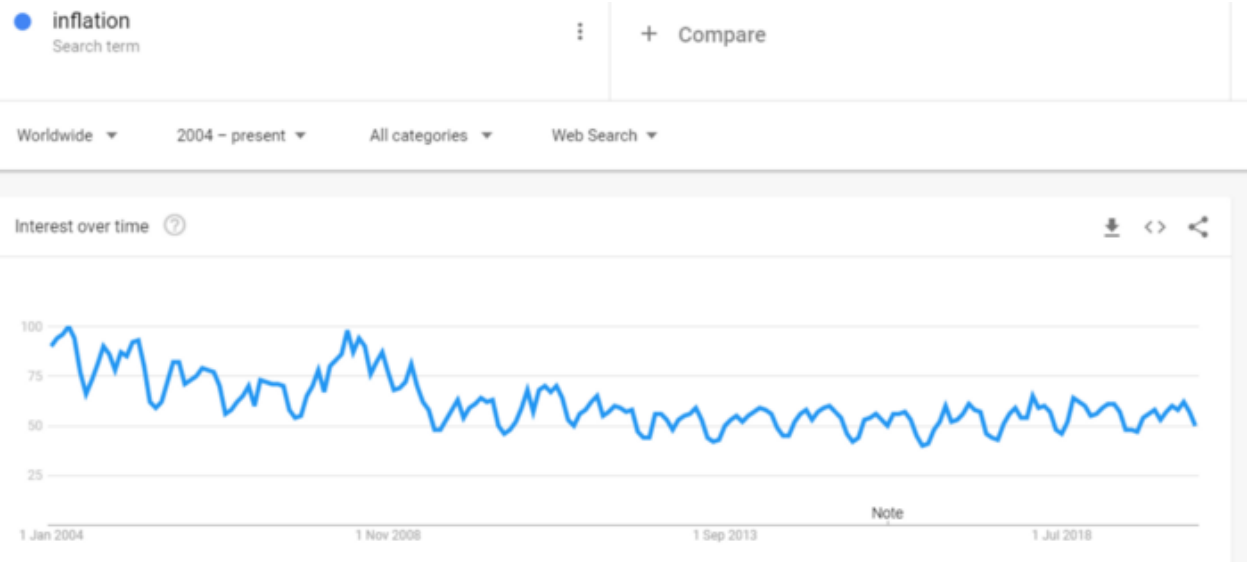
Once Inflation Starts, It Won't Be Contained

By Gael Sanchez Smith

Posted June 12, 2020

Introduction

The mainstream media has spent decades underplaying the risks of inflation, claiming that deflation is the most perilous thing that could ever happen in an economy. Amazingly, their propaganda has succeeded and most people have come to accept the ludicrous notion that falling prices of goods and services are an economic problem— for a detailed analysis of the fallacies of deflation see Jeff Booth's, The Price of Tomorrow. Even today, as central banks around the world implement ever more unorthodox monetary policies such as asset purchases and negative interest rates, the public remains largely oblivious of the risks of inflation.



Searches for Inflation Worldwide

This article isn't an attempt to forecast the exact set of circumstances that might give rise to inflation. Instead, it argues that the chief belief that gives fiat money value — namely, the expectation that central banks are capable and willing to preserve their currency's purchasing power — is unwarranted. In the event of inflation, central banks won't be able to preserve the value of fiat money for three reasons: The high level of private debt, the high level of public debt and the precariousness of central bank's balance sheet.

Markets are forward looking, hence, as people come to realize that central banks can't preserve the purchasing power of their currencies, we should

expect a repudiation of State liabilities — fiat money and government bonds — and a move towards hyperbitcoinization.

The Value of Fiat Money

Fiat currencies are financial assets, more specifically they are liabilities issued by a nation's central bank which we demand for three reasons:

- **Tax Demand:** The government mandates taxes be paid in the national currency. This is the smallest component of the total demand since it only exerts itself once a year.
- **Store of Value (SOV) Demand:** Fiat money is used as a highly liquid asset that promise to preserve its purchasing power — i.e. a store of value. This is the largest component of total demand and it is contingent upon the currency's price stability.
- **Transaction Demand:** We use fiat money as a medium of exchange to conduct commercial and private transactions. Transaction demand is closely tied to SOV demand; if the currency doesn't have stable purchasing power, merchants will apply a high discount rate or will demand a more stable currency.

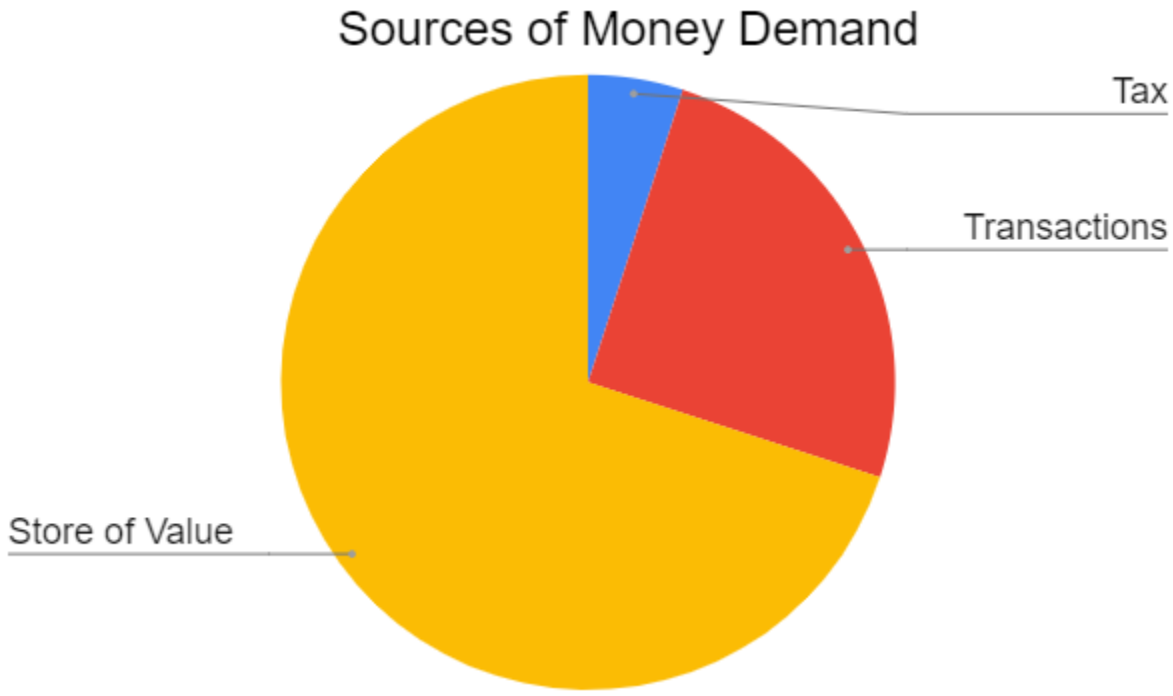


Illustration:Sources of Money Demand, Gael Sánchez Smith

Chartalists mistakenly believe that the obligation to pay taxes a alone makes fiat money valuable. Of course, there is always a minimum level of Tax Demand since failure to comply with tax laws results in imprisonment, but most of money's demand is derived from its use as a medium of exchange

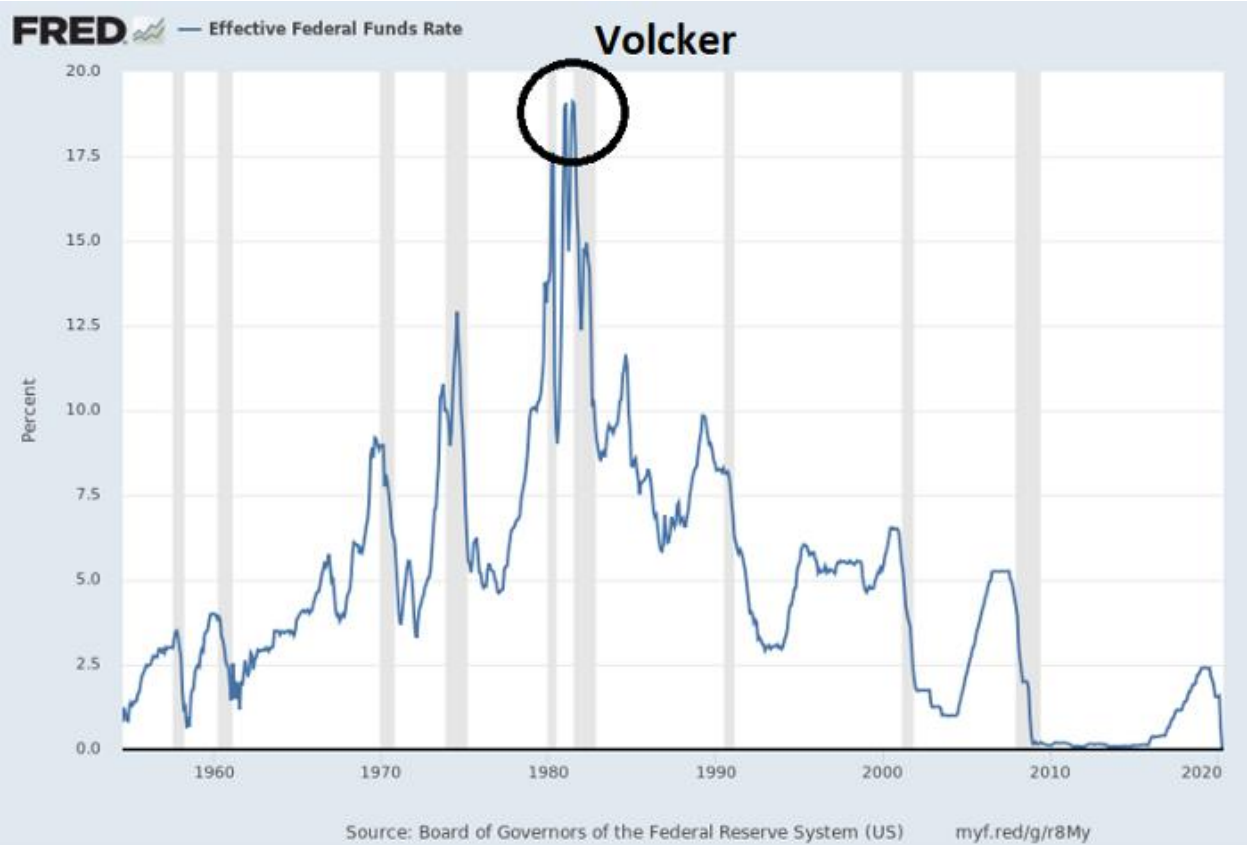
and a store of value. Consequently, the monetary powers of the State are much more limited than what Chartalists profess; a government can mandate taxes be paid in the national currency but it cannot impose its use as a store of value or a medium of exchange.

In other words, money is always and everywhere a market phenomenon. If a currency starts depreciating at a high rate, SOV demand will collapse and it won't be used as a medium of exchange regardless of what the State decrees. We can see this reality play out today in countries like Argentina or Venezuela where, even though taxes are collected in the national currency, most transactions are conducted in dollars and value is stored in dollars, Bicoin, or gold.

The value of fiat money, like any other asset, depends not only of its demand but also of its supply. Central banks are very aware that if the supply of money exceeds its demand significantly, the currency will depreciate and its SOV demand will disappear. Hence, they present themselves as independent institutions that are are committed to fighting inflation and divorcing the supply of money from the governments financial needs. In the real world, central banks target 2% inflation and often collude with the government, but functioning monetary territories like Europe, Japan, or the U.S. have until now, shown sufficient restraint from printing their currencies to oblivion.

Central banks influence the supply of money by manipulating the interest rate: When they wish to increase supply, they lower the interest rate and when they wish to reduce the supply, the interest rate is increased (Stefanie von Jan explains the process in further detail here). If the supply of money increases above its demand or if demand falls below its supply (for example due to a loss of trust in the issuer) the currency will depreciate, its discount rate will spike — e.g. workers will sell their labor for 20 $ instead of 10$ in anticipation of inflation — and the Store of Value demand will fall creating an inflationary spiral. In this scenario, it is imperative that the central bank intervenes in order to stabilize the value of the currency and recover its SOV demand. If the central bank were unable or chose not to intervene, the self enforcing depreciation would lead to a vicious cycle of high inflation that ends with the currency's repudiation.

The last time there was an inflationary cycle in the United States was after Nixon closed the gold window in 1971. After 10 years of rampant inflation, Fed Chairman Paul Volcker was forced to raise the interest rate to 20% in order to stabilize the dollar's purchasing power.



U.S. Effective Federal Funds Rate, Chart Source: FRED

In conclusion, the value of fiat money depends of changes in its ***supply and its demand***. The largest component of fiat currency's demand is the Store of Value function, if a currency stops acting as a store of value — it starts depreciating — demand falls further and the central bank must intervene in order to reduce the supply and stabilize the currency's purchasing power. In this regard, the ***expectation*** that the central bank will be willing and able to adjust the supply of money in the event of inflation is key to maintaining a currency's SOV demand. Markets are forward looking, if individuals anticipate the currency will depreciate, they will sell it today. In other words, in order for fiat money to maintain its value, the market must believe that in the event of inflation, central banks are capable and committed to preserving the purchasing power of their currency.

At present, the money supply in the U.S is increasing dramatically: M2 money supply — which includes money in the form of bank cash, bank deposits, and easily convertible near money — is growing at 24% per anum, its highest rate in recorded history, but inflation hasn't increased in a meaningful manner.

U.S. Yearly Percentage Change M2 Money Supply (blue) & Inflation (Red)

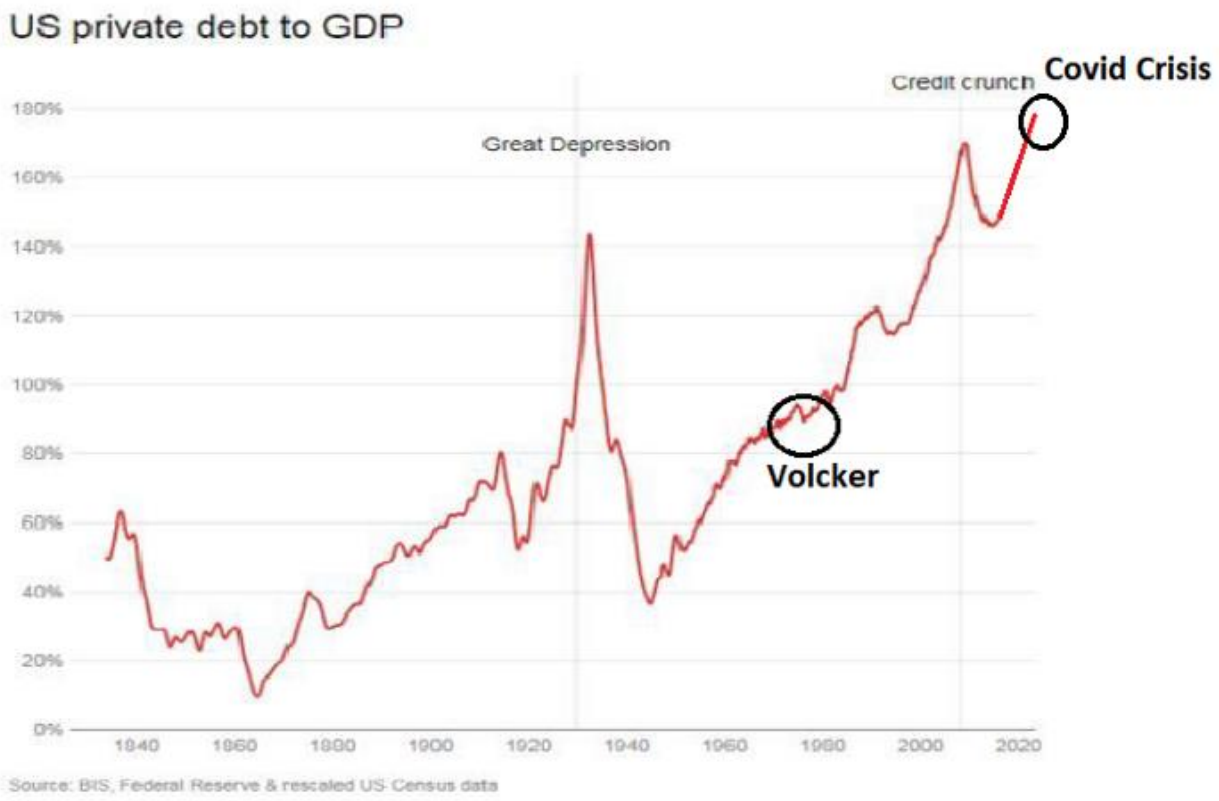
This can be explained because the increase in currency supply has gone hand-in-hand with higher demand for money due to social distancing, uncertainty surrounding the Covid-19 crisis and debt repayments. The absence of inflation also tells us the market is expecting that if in the future, the increase in the money supply leads to inflation, the Fed will be able to raise interest rates in order to stabilize the dollar's purchasing power.

In this article I argue that the market's expectations are misplaced; the belief that the Fed can preserve the value of the dollar in the event of rising inflation is unwarranted for three reasons: **Firstly, the high debt and leverage in the private sector** would make it impossible to raise interest rates without unleashing a depression and a financial crisis. **Secondly, balancing the budget in light of the high deficits and public sector debt** would require austerity which would lead to social and inter-generational conflicts. **Thirdly, the act of raising rates would render the Fed** insolvent due to its high leverage and iliquidity.

1- Private Debt

As was mentioned above, the last time there was a loss of faith in the U.S. dollar, Volcker was forced to raise rates to 20% in order to control inflation.

The Fed succeeded in stabilizing the value of the currency at the cost of the 1980–1982 recession, however, the economy recovered swiftly thereafter. Back in the 70's, private debt amounted to less than 100% of GDP but today, it is at an all time high considerably above Great Depression levels.



Total US Private Debt, Source: BIS

The extreme debt levels means rising rates would not simply cause a moderate recession but would lead to mass defaults in businesses, corporations and households and high unemployment. Austrian economists argue that this "cleansing" process is actually a desirable phenomenon since it corrects the misallocation of resources produced by the artificial credit expansion — See Ben Kaufman's article for a detailed outline of the Austrian Business Cycle Theory — , however, we are not concerned here with what central banks ***should do*** but with what they are ***likely to do***. In this regard, the high levels of unemployment and economic disruption that would result from higher interest rates makes it unlikely that the Fed would chose to go down that path.

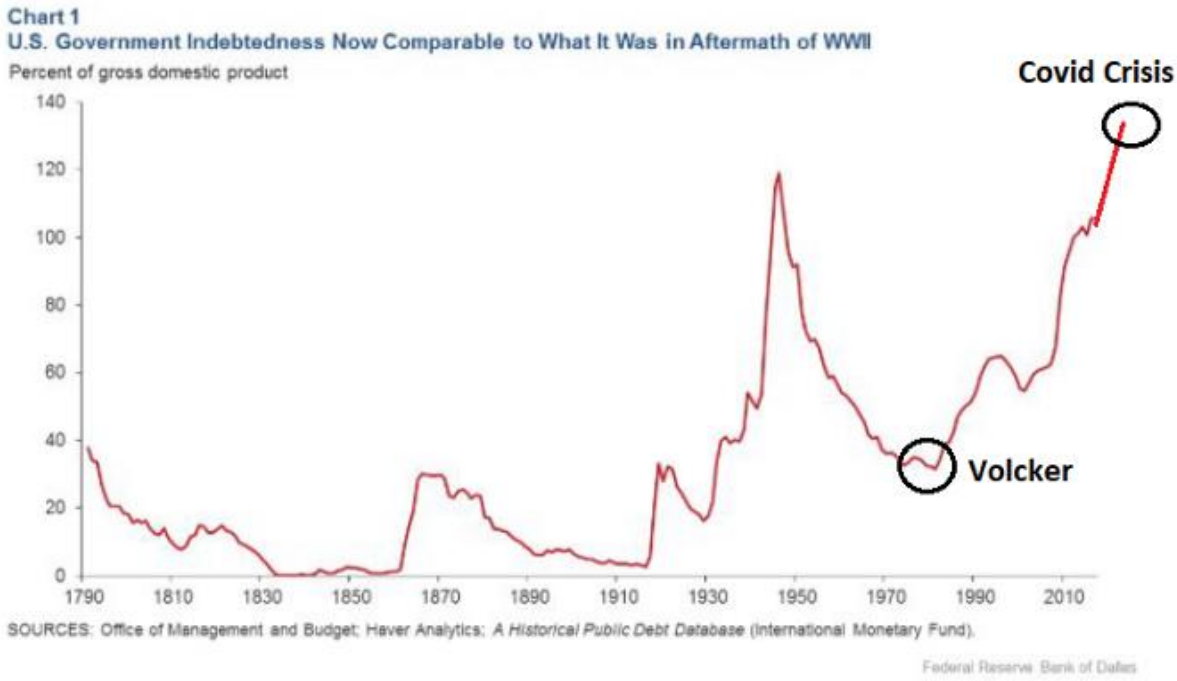
To make things worse, most of these loans are issued by commercial banks, and their writing off would result in a financial crisis and a need to — yet again — bailout the banking sector. Before the Great Recession, governments around the world had relatively low debt/GDP ratios which enabled them to recapitalize the banking sector by issuing new debt. Today public debt is at

its highest point in history, thus, the government's ability to bail-out private banks is limited. This would be specially the case in an environment of higher interest rates; since the Fed wouldn't be buying bonds in the open market, the treasury would have to pay higher interest rates in order to attract bond buyers, making it difficult to issue additional debt to bail-out private corporations. Instead, one should expect a mixture of bail-ins, depositor haircuts and nationalizations.

In conclusion, higher interest rates are unlikely to be pursued by the Central Bank since they would lead to mass insolvencies, a deep depression and a financial crisis.

2- High Deficit & Public Debt

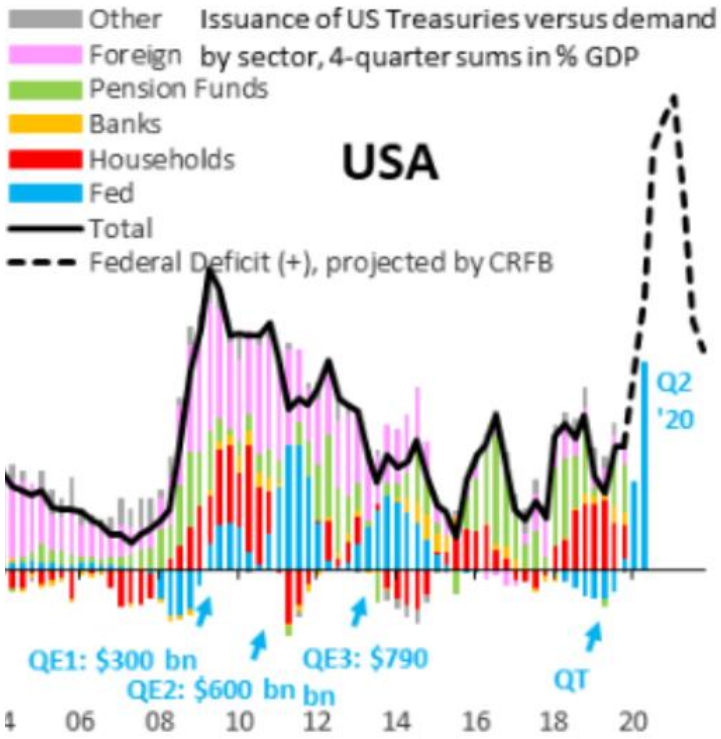
We have already touched upon the second reason why it is unlikely that the fed can keep its commitment to stabilizing the value of the dollar; the high level of public debt. During the 1980's, government debt only amounted to 35% of GDP compared with an expected all-time high of 140% of GDP post covid-19 crisis.



U.S. Total Government Debt, Source: IMF

Today, debt levels are so high and yields so low that investor apetite for treasury bonds has dwindled considerably. The following chart shows how foreign investors (pink area) have been purchasing less and less of the total bond issuance every year. Up until 2019, foreign demand was replaced by

Pension Funds, households and banks who are legally obliged to buy the Treasury's bond issuance as long as they can meet their capital requirements.



Source: Federal Reserve, Bloomberg

Lyn Alden has pointed out how how the infamous September 2019 spike in the repo market was due to primary dealers not holding sufficient reserves to absorb the Treasury's bond issuance and meet their post-Great Financial Crisis regulations — See Lyn's article for a full explanation. It was at this point that the Fed (blue area) was forced to resume quantitative easing, effectively monetizing the government's budget deficit which is expected to surpass a shocking 20% of GDP this year.

Having the Fed monetize the deficit allows the government to pursue infrastructure projects, pay extra unemployment benefits, tax cuts and other popular measures that the public is advocating in times of economic hardship and humanitarian distress. If the monetization of the deficit leads to higher inflation, and the Fed chose to raise interest rates in order to stabilize the value of the dollar, it would force the government to balance its budget which could lead to social and inter-generational conflicts. e.g. taxes would need to be raised on the younger segments of the population in order to repay bonds held by retirees.

An alternative strategy could be allowing inflation to run high for a prolonged period of time in an effort to reduce the real value of the debt — as prices go

up in nominal terms the real value of the debt falls — , and raise interest rates once debt levels as a percentage of GDP have fallen. As will be discussed later, this avenue is already being proposed by the Fed and would likely lead to a complete loss of faith and repudiation of fiat money and a complete adoption of Bitcoin.

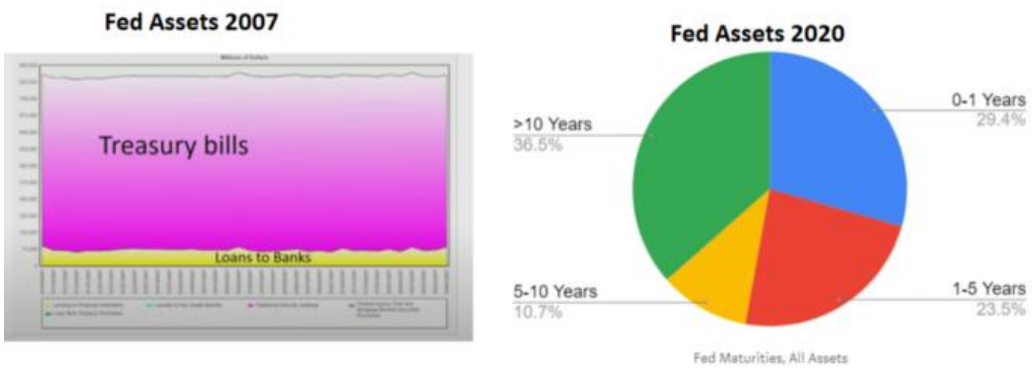
3- Precariousness of the Fed's Balance Sheet

Even if ones believes the Fed would obliterate the banking sector, unleash a depression and force austerity on the government in order to preserve the value of the dollar, there is a third reason why I believe the central bank would be unwilling to control inflation; doing so would make the central bank insolvent.

Looking at the Fed's balance sheet, two things stand out: Maturity mismatching and extreme leverage.

Maturity mismatching:

Prior to the Great Recession, monetary policy was limited to short term bills which enabled the central bank to raise rates by simply allowing its assets to mature. Today, the Fed's holdings are mostly in the form of long dated treasuries and mortgage backed securities with an average maturity above 5 years.



Fed Assets, Source: Federal Reserve

The long duration of the bonds in its portfolio make it impossible for the Fed to raise interest rates by allowing its assets to matures. Hence, if the central bank wanted to raise interest rates, it would need to either sell some of its holdings or increase the interest it pays on excess reserves (IOER). The low yield on its assets and its over-leverage makes it very difficult for the Fed to implement either of these measures effectively.

High leverage, assets= 150 x Capital

Fed Balance Sheet 8 April 2020			
Assets Yield 1.4%		Liabilities	
Treasuries	3,634,386	Currency	1,835,225
MBS	1,459,701	Reverse repurchase agre	334,488
NEt Unamortized premiums	221,982	Reserves	3,858,360
Repos	227,643	Other Liabilities	15,892
Loans	130,004	Capital	39,176
Liquidity Swaps	385,365		
Other	24,060		
Total	**6,083,141**	**Total Liabilities**	**6,043,965**

Assets= 150 x Capital

Fed Balance Sheet 8 April 2020, Source: Federal Reserve

At present, the Fed is extremely leveraged with assets just under 151 times capital, ironically, it fails spectacularly to meet the capital requirements it imposes on commercial banks. Furthermore, the average return on its assets has continuously diminished as each round of quantitative easing has pushed bond yields lower: The interest payments it receives on its holdings has dropped from 3% in 2010 to roughly 1,4% in 2019.

These factors make it impossible for the central bank to raise interest rates without revealing its insolvency:

- If it raised rates by selling some of its treasuries, the market would front run its selling resulting in loses which — due to its high leverage — would rapidly lead to negative equity. This already happened during the last unwinding of quantitative easing, when the FED piled billions in paper losses.
- If it chose to raise rates by increasing the interest paid on excess reserves (IOER), it would quickly find itself paying more for its liabilities than the interest payments it earns on its portfolio. Not all of the Fed's liabilities generate expenses, for example currency in circulation doesn't pay any interest. Of the total 6 Trillion $ liabilities, 3.9 Trillion (63.4%) are in the form of reserves that the FED would have to pay interest on. The average return on the FED's assets is circa 1,4%, which leaves them enough room to raise IOER to roughly 2,2 % before their expenditures are higher than their revenues. In today's ultra low rates environment, 2,2 % interest rates might seem quite high but in a potential scenario of 5 or 7 % inflation — which in light of the financial

> history of the U.S. doesn't appear at all outlandish — would lead to massive losses on its holdings.

Of course, the Fed already realizes that any "exit strategy" leads them down the road to insolvency, but what exactly does this mean for this unusual institution? At the end of the day, the Fed's liabilities (fiat currency) are non-interesting-bearing and irredeemable — having a $10 Federal Reserve note provides a claim on the Fed for $10 worth of Federal Reserve notes, possibly in different denominations, but nothing else. Thus, ***balance sheet insolvency*** (assets<liabilities) is a sign of incompetence and mismanagement but the central bank need not worry about a bank run.

Equitable insolvency (failure to pay obligations as they fall due) is more worrisome since the central bank would fail to pay its expenses such as rents, salaries, entertainment services etc. The Fed must rely on the interest it receives on its holdings to fund its operations, but in an environment of higher rates, it would have negative equity. Since the Fed cannot create reserves that are unbaked by assets, it would need to be recapitalized by the Treasury with real tax dollars or new debt issuance in order to pay for its expenses. This would be extremely ironic given that the Fed is currently engaged in Quantitative Easing in order to finance the government's deficit. It would also be politically unpalatable since the taxpayer would suffer additional austerity in order to recapitalize a central bank that has been used to bail out private corporations.

Conclusions

In the event of inflation, the high levels of public and private debt in the economy and the precariousness of the Fed's balance sheet would make it impossible for the central bank to preserve the value of the dollar without unleashing a socio-economic and political crisis. If it tried to restore trust in its currency by raising rates, like Volcker did in the 80's, it would cause household and corporate defaults that would result in a financial crisis and a depression. In parallel, the government would be forced to balance the budget, imposing severe austerity that would lead to inter-generational and social conflicts. Furthermore, in the process of raising rates, the Fed would become insolvent and would need to be recapitalized by the Treasury. This would result in social and political backlash, as well as undermining the central bank's alleged independence.[1]

Centrals banks were created for the benefit of the financial services industry and the State, hence, it is unlikely that they will chose a policy path that is directly opposed to the interests of their main constituents. Instead, they will likely allow inflation to run rampant, hoping to reduce the real value of public and private debt before they can safely raise rates again — since most debts

are fixed nominally, when the currency devalues significantly and prices/assets/wages go up in nominal terms, debts vs GDP goes down. This strategy is nothing new, the Fed already inflated away the debt after World War II and is openly proposing the same approach today — NBER working paper and Cleveland Fed.

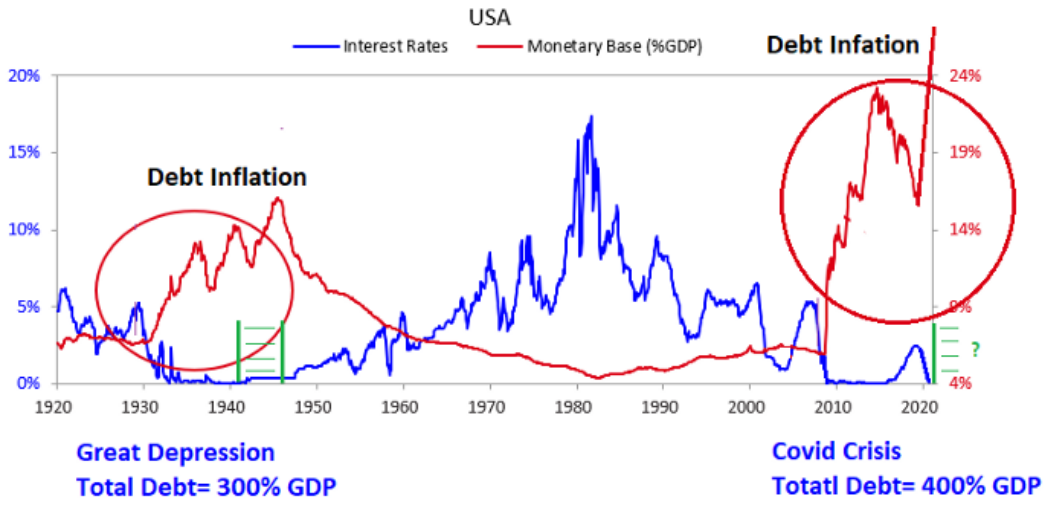


Chart Source: Bridgewater Associates, Ray Dalio, Updated by Lyn Alden, Annotated by Gael Sanchez

Back in the 40's, gold had been outlawed and investors didn't have a highly liquid store of value alternative, so they accepted the losses on their currency and bond holdings and demand for the dollar returned once Volcker stabilized its purchasing power.

We can think of fiat money today as somewhat of a Ponzi scheme, it only holds value for two reasons: Firstly, there is an expectation that in the event of inflation central banks will preserve its purchasing power via contractionary monetary policy and secondly, new buyers will demand it in the future. [2] As the market realizes these two conditions won't be met, one should expect a repudiation of State liabilities — government bonds and fiat currency — and a move towards hyperbitcoinization.[3] This outcome should come as no surprise as Austrian Economists have been warning about it for decades.

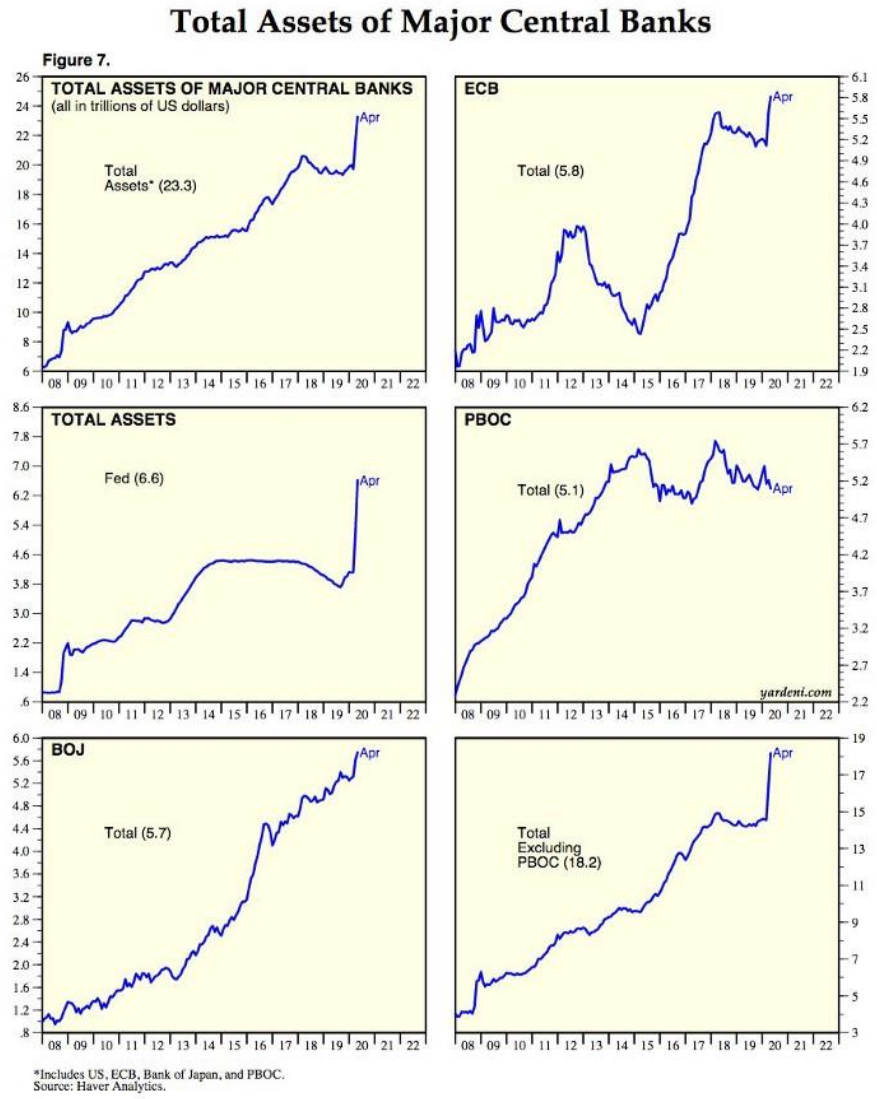
"There is no means of avoiding the final collapse of a boom brought about by credit expansion. The alternative is only whether the crisis should come sooner as the result of voluntary abandonment of further credit expansion, or later as a final and total catastrophe of the currency system involved."
Ludwig von Mises, _Human Action (_1949)

I believe Mises would agree that given today's unsustainable debt levels and the political and social incentives, the latter option is by far the most likely outcome.

Many thanks to Stefanie von Jan, Ben Kaufman and Emil Sandstedt for proofreading the text and for their very insightful comments.

Notes:

1. This article is not an argument against the U.S. dollar per se but against the sustainability of the fiat system as a whole. Major central banks around the world are going down the same road as the Fed and the analysis is aplicable to most jurisdictions . Moreover, given that the Dollar is the reserve currency, its demise would most likely breach the trust in the fiat system worldwide.



Source: Haver Analytics

2. Expectations are crucial; even if the growth of the money supply is halted, the demand for a depreciating currency needn't return instantaneously. Monetary authorities have breached the trust of investors so many times, that in my opinion, even a credible announcement by the Central Bank would not be enough to recover investors trust. They will likely need to buy and prove they hold Bitcoin in order to truly regain trust in their currencies. Of course, by that point, hyperbitcoinization will have run its course and bitcoin will already be the economy's medium of exchange, unit of account and store of value.

3. As individuals repudiate fiat currencies, governments might try to outlaw Bitcoin like they did with gold in 1933. Whether they succeed in doing this or not will depend largely on technological factors. If the decentralization of the network is preserved and anonymity tools are readily available, banning Bitcoin will be a practical impossibility. Furthermore, as is mentioned in the article, money is always a market phenomenon. Unless fiat money is stabilized, it won't be used as money regardless of what the State dictates. (we can see this reality today in Argentina and Venezuela)

Bitcoin as a Tool for Secession

By Yuri de Gaia

Posted Summer 2020

The Triumph of Civilization, 1793, Jacques Reattu

Bitcoin may be many things to many people, but one cannot ignore its primary effect on the mind - the realization of how much power is acquired by a simple act of holding private keys to censorship-resistant unconfiscatable property.

The hardest money on earth brings the concept of inalienable property rights back on its feet, and with it, an available opportunity for ***personal secession***.

Throughout history, protests, revolutions and civil wars proved to be ineffective against State tyranny.

The predictable result of any such event was the replacement of one tyrant with another. When the democratic way became the standard around the

world, it guaranteed that only bad men could rise to the top. Demagoguery, cunning and trickery were the tools that one had to master to be able to sway the public opinion in your favor. When at the top, all bets were off. The four short years of so-called “office”, turned the dangerous man’s high time preference into a frenzy of wealth redistribution, surveillance and wars. And if a rare good man managed to occupy the desired position, demonization or assassination was sure to follow.

But that was in the past.

Today We Have Bitcoin

The importance of the times we live in cannot be stressed enough. With ease, one can say that on January 3rd 2009, the timeline split into the pre-Bitcoin and Bitcoin eras. Property rights were restored, and personal secession became possible again.

Although the effect may not be immediate and seen by the majority, those in the know understand that what governments around the world took for granted for so many years, is now gone. Taxation and expropriation, the bread and butter of every State, have become nearly unenforceable. What is yours, is yours to keep. There is a key to your property, and you are the key master. Every ten minutes, with each block produced, your belief in the new system is justified and strengthened. There is no referendum or democratic vote that can change that.

The mob has lost.

With the newly restored property rights, you can focus on your work. Slowly but surely, the process of personal secession kicks in. First, it is a purely mental event: the ultimate red pill, the walk through the door. But as soon your stash grows to a sizeable amount, the wheels of secession in the physical realm are set in motion. Capital accumulation becomes a natural habit. And with capital, many more doors open.

Opt Out

Opting out of the oppressive system, disassociating from anyone who supports Leviathan, ignoring unjust rules whenever possible while building your own tools, joining communities of like-minded individuals, creating independent circular economies - this is what personal secession is about.

Replacing the flag of the usurping State with that of human dignity. Summoning the courage to escape the grotesque reality imposed by the Parasites, and step into the brave unknown. Relentlessly studying oneself and the world, cultivating higher aspirations, perfecting skills to become part of the new Natural Elite that will restart the engine of *civilization*.

The process of civilization is only possible under Natural Order, a state of affairs that adheres strictly to the foundational principles of the Universe. The modern State directs its energies to the defiance of natural laws, and thus must be considered the ultimate agent of ***decivilization***. By infringing on peaceful individuals' property rights, it degrades relationships among people and distorts the naturally occurring order. Now that it is possible to reclaim individual sovereignty, the unwinding of the global destructive machine has begun. Leviathan's demise may be slow but certain.

True progress does not always imply a move forward. Sometimes, a better state is achieved by ***taking a step back***. The laws of Nature are universal and eternal. Going against them, as we have done in the past century, is always a mistake. Therefore, to restore Natural Order, we must look back to when it was more prevalent and identify what it is that made it so. The answer is undoubtedly ***Family*** - the principal benefactor of property rights, the nucleus of society.

Status of Family Estate

In its traditional form, Family has been under a massive attack, especially in the Western world.

The process of individual atomization, devaluation of familial relationships and degradation of youth has been long, but in many cases successful. Spiking rates of singledom, divorce, single parenting, abortion, abuse and non-traditional sexual relationships are all the proof you need. One may argue that this process occurs naturally due to the general liberalization of society, but it is not so. There is someone who benefits from the disintegration of the most vital unit of civilization - the Parasite.

By encouraging atomic individualism, the parasitic element in our society wants to achieve its ultimate goal: total control and domination over people's lives.

For what is a better place to do that than in a household? Traditionally, the head of Family is responsible for the ultimate decision making. He is the procurer of goods, the protector of the estate, the reason and the muscle. Removing him from command is akin to relieving the captain of the ship of his duties and telling the sailors that they are now in charge all at the same time. Naturally, only chaos can ensue. And that is what we see. Men are told to be women, women are encouraged to become men, couples are brainwashed to forego having babies, children are incited to rebel against parents. Generational ties become ever weaker to the point where the concept of a family estate ceases to exist. There are only individuals, linked by their DNA, who feel nothing but disdain towards each other. Having no support from immediate family, but still needing it psychologically and often

financially, they turn to Leviathan for help. And he is there, waiting with open arms.

Managing people's political affiliations and professional lives is one thing. Affecting their decisions inside households is a whole new level. It is a crown achievement of the micromanaging State, a parasitic dream come true.

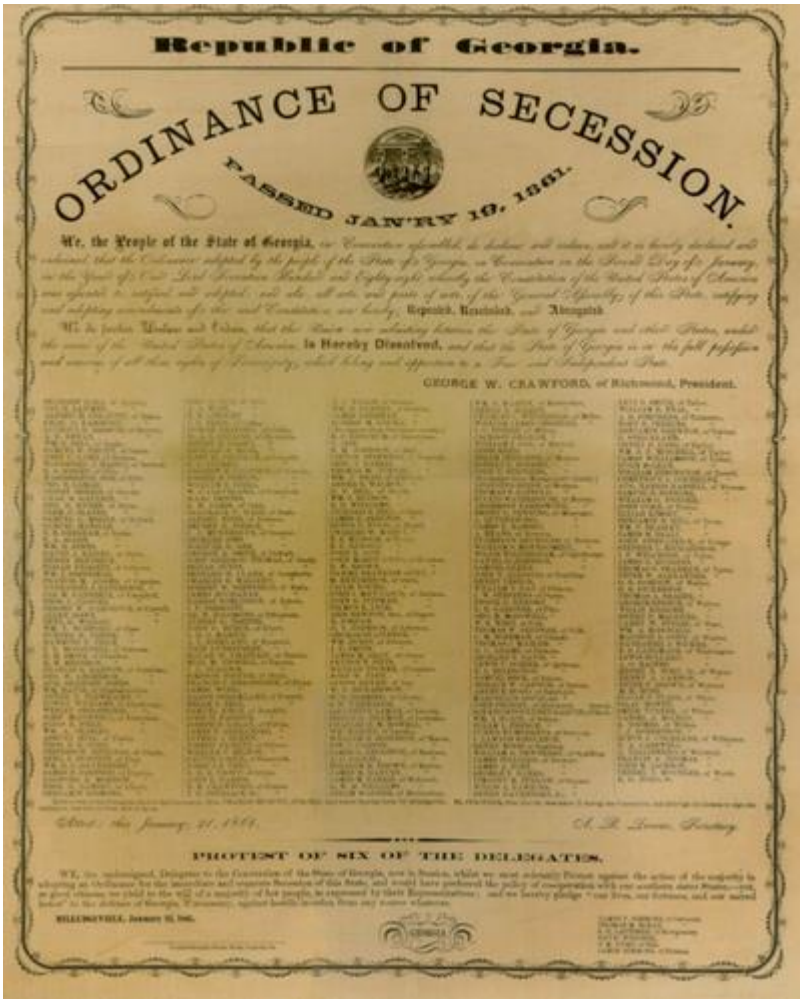
If one can be told how to behave in his own bedroom, then the last glimmer of personal liberty has disappeared.

Unfortunately, in many parts of the world, we are very close to such a condition. But as things seemed to reach the bottom, when sinking further was almost impossible, and the process of moral degradation was near complete, a savior appeared.

Like Prometheus who gave mankind fire, a world-changing technology, Satoshi Nakamoto brought with him the gift of Bitcoin. And with it, a hope of restoring the civilizing force of Family.

As Bitcoin lowers one's time preference, gradually, the outlook on life starts to change. An existence filled with instant gratification is replaced with one of delayed consumption. Foresight, long-term plans and projects, personal restraint take hold. Man turns his attention to the future. He realizes that there is a moment in the coming years when he will have to pass and leave his legacy behind. But to whom? Who will care about his life achievements more than anyone else? Most certainly Family, a tribe of kinship. And so he starts planning for the ***ultimate long-term project***.

Not only does the act of accumulating Bitcoin strengthen one's material well-being, it also promotes higher aspirations in man. The focus shifts from short-lived superficial relationships, to the establishment of a family estate that will last generations. Man's children and grandchildren are raised in an environment that promotes farsightedness, culture and morals. In cooperation with like-minded neighbors, they work diligently to improve their surroundings. The process of civilization is set in motion once again.


Republic of Georgia.

ORDINANCE OF SECESSION.

PASSED JAN'RY 19, 1861.

We, the People of the State of Georgia, ... Is Hereby Dissolved, ...

GEORGE W. CRAWFORD, of Richmond, President.

PROTEST OF SIX OF THE DELEGATES.

Strong individuals create robust families. And strong families form resilient communities. When faced with the moral degeneration of the rest of the world, such outposts of civilization have no choice but to strive for segregation - physical, cultural and intellectual. What starts as personal secession turns into a collective movement for self-determination. ***This is not a violent global revolution*** but a peaceful exit of thousands of newly formed congregations into different ways of living that they decide for themselves.

The Parasites may stop one or two of them, but can they really crush a multitude of independent citadels?

Before Bitcoin, one could not help but wonder how far downhill we would go. It seemed like the end of civilization was near, and there was no way to prevent it. Now that we have the necessary tools to create new systems independent from the parasitic status quo, we can finally reverse the painful damage inflicted upon our spirit. The process of personal secession is the creation of a citadel of the mind, first and foremost. A fortress of light, impenetrable to the forces of darkness. Combined with the power of will, it

helps us mold the physical reality into what we want it to be. A world of Natural Order, a place of fairness and justice.

You can only change the world by changing yourself. Bitcoin may be the catalyst you were looking for.

Proclaim your independence.

Start a family.

Cultivate your community.

Secede.

Different bitcoins different prices

By JP Koning

Posted September 2, 2020

6	Bitstamp	BTC/USD	$11,290.77	0.15%	$4,870,629	$3,151,288	$142,866,906
8	Bitfinex	BTC/USD	$11,322.33	0.88%	$6,912,379	$6,581,688	$71,222,295
10	Indoex	BTC/USD	$11,345.08	0.12%	$3,891,319	$3,592,723	$55,768,942
16	Currency.com	BTC/USD	$11,304.84	0.1%	$3,447,105	$2,575,020	$2,475,455
17	B2BX	BTC/USD	$11,342.30	0.12%	$839,460	$5,220,432	$143,027
19	Gemini	BTC/USD	$11,302.86	0.11%	$2,914,524	$1,897,568	$34,515,381
24	Tokenize	BTC/USD	$11,317.50	0.12%	$2,984,267	$1,634,157	$1,715,700
32	Binance US	BTC/USD	$11,307.06	0.11%	$1,490,073	$1,712,004	$8,378,026
33	Coinbase Pro	BTC/USD	$11,306.60	0.1%	$386,007	$527,776	$215,832,695

Not all bitcoins are the same. If someone steals 100 bitcoins from a cryptocurrency exchange and tries to sell them, they'll have to price them at a discount to the market price in order to compensate the buyer for the risk of laundering them. Different bitcoins different prices.

This isn't just a bitcoin phenomenon. There are two wholesale markets for banknotes, too. The legitimate one is comprised of banks, retailers, and cash-in-transit companies like Brinks that exchange notes at par. And the illegitimate one is made up of mob lawyers, drug dealers, and note brokers exchanging dirty notes at 20 or 30 cents on the dollar. Different dollars different prices.

You can find this same fractionalization everywhere: in electronics or prescription medicine or used cars. There is a licit and illicit price in each market.

But the difference between dirty and clean prices isn't the dichotomy that interests me in this post. Could we see a two-tiered market develop for ***clean*** bitcoins? In other words, could a situation arise in which Jerry's 100% legitimate bitcoin's are worth more than Elaine's 100% legitimate bitcoins?

I'd argue that the precedent already exists in the gold market.

Last month I wrote a quick explainer on the **London Bullion Market Association**, or LBMA, for CoinDesk. The LBMA is a standards-setting body for the gold market. It defines what constitutes a London "good delivery" gold bar and what doesn't. These standards include physical details like purity, weight, height, and appearance. Increasingly, the LBMA's standards are being stretched to include details about sourcing. Has the miner extracted the

metal in an environmentally friendly and ethical way? Are they laundering money for Mexican drug lords?

Good delivery bars can only be stored in a handful of London-based vaults. A strict paper trail is maintained to ensure that nothing gets in (or out) of this walled-garden. The moment a bar is withdrawn from a London vault, it loses it's good delivery status.

This has the effect of creating a two-tiered ***licit*** gold market, one in which London gold is worth more than non-London gold.

Consider that the world's largest buyers congregate in London to trade gold. A 400-ounce gold bar fabricated by a refiner that doesn't have the LBMA's stamp of approval can't access the incredibly liquid London market. And so it won't be worth as much as an LBMA-approved 400-ounce bar. (No one wants to buy your metal if it can't be immediately on-sold in London.)

To be granted London "good delivery" status, an unapproved bar must go through a process of being anointed. That means bringing the bar to a refiner on the LBMA's approved refiner list. The refiner vets the bar owner to check for money laundering, much like a banker would. Only then can the bar be melted down and reformed into an entirely new and approved bar. But all of these steps are costly.

As my CoinDesk article suggests, we might one day see the same sort of fractionalization emerge in the bitcoin market. A core group of exchanges and custodians would begin to define what qualifies as a "good delivery" bitcoin. Standards would mostly apply to the provenance of bitcoins. Since the history of bitcoin transactions can be easily monitored, it is relatively easy to cast aspersions on certain flows of bitcoins, perhaps because they happen to pass through suspicious addresses or are mixed by coin tumblers. (As Izabella Kaminska suggested a while back, bitcoin has a lien problem. Tim Swanson has been writing about this for a while, for instance in A Kimberly Process for Cryptocurrency.)

Should a bitcoin be withdrawn from this "walled garden" of approved exchanges and custodians it would fall out of the ***Bitcoin Marketing Association's*** "chain of custody" and, as such, would no longer have access to core liquid markets. And so unapproved bitcoins would be forced to trade in lower quality venues with lax vetting standards, and less liquidity.

An online retailer might not want to take the risk of selling their products for unapproved bitcoins (i.e. ones that come from non-vetted personal wallets). Sure, it might be possible for the retailer to accept non-approved flows with the intention of re-depositing them into the Bitcoin Marketing Association's system in order to get the Bitcoin Marketing Association price. But there would always be the risk of an unexpected blockade or freeze of a customer's

unapproved bitcoins. And so retailers would ask their customers to only spend approved bitcoins straight from their Coinbase wallets.

By the way, the sort of LBMA-driven dichotomy that exists in gold (and could one day exist in bitcoin) does ***not*** exist in banknote markets. There is no such thing as a good & expensive $20 bill and a good but cheap $20 bill. Cash, as we say in the monetary biz, is pretty much fungible.

Why do we see a two-tiered gold market but just a single-tiered banknote market?

There are probably many reasons for this, but a big difference is the sorts of people that occupy each market. The gold market is populated by investors, the most dominant of which are large institutional investors and central banks. These big players do not want the risk of having their gold being tarnished in any way. They don't want their $50 million in gold bars to end up being fake, or subject to a court dispute, or frozen by law enforcement due to money laundering concerns. That's why the LBMA standards exist; to make gold safe for big institutional buyers.

But cash is different. Warren Buffett and Ray Dalio don't occupy this particular market. The market for coins and notes is dominated by regular people. Furthermore, banknotes are primarily used in small day-to-day retail purchases, not financial speculation. This sort of activity is not conducive to the emergence of a centralized marketing association. Cash transfers are done too quickly, and in small amounts, and by folks who don't have deep enough pockets to pay for verification.

The market for banknotes is literally everywhere (each corner store in town will accept them), whereas the market for gold tends to clump up in a certain specific physical locations. This centralization makes standardization easier.

Bitcoins are more like a gold bars than a banknotes. Let's face it, it's been ten years since bitcoin appeared on the scene and no one really use bitcoin it as money (just like they don't use gold as money). The majority of bitcoin demand is a demand to hoard the stuff for price exposure, much like the yellow metal. And like gold, the market for bitcoins has coagulated around exchanges. It's not an ***everywhere*** market, not like the market for banknotes.

So to sum up, the market for bitcoins is very much like that for gold. Given that a standardized gold market has evolved, I wouldn't be surprised to see the same happen to the bitcoin market, especially if big financial institutions start arriving.

Tweet Thread: What is an xpub?

By Danny Diekroeger

Posted August 30, 2020

~ What is an xpub? ~

An xpub (“extended public key”) along with an xprv (“extended private key”) allows you to generate a nearly endless number of bitcoin addresses without having to store and protect the individual private keys for every single one

👇 Time for a thread 👇

1/ To protect your privacy, it’s good practice to use a new bitcoin address for every transaction

But each new address requires its own private key...

Back in the old days (pre-2013), bitcoin wallets would generate and store a new private key for every new address

2/ Imagine running a popular exchange that uses millions of addresses...

You would be forced to store and protect millions of individual private keys

What a headache! There had to be a better way...

3/ In 2013 @pwuille authored BIP-32, which specified a standard for Hierarchical Deterministic Wallets

This type of wallet allows you to generate a ton of addresses using only a single seed

That single seed is called an xprv (“extended private key”)

bitcoin/bips Bitcoin Improvement Proposals. Contribute to bitcoin/bips development by creating an account on GitHub. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

4/ If the concepts of private keys and public keys are confusing, now would be a good time to check out my previous thread that goes into more detail:

Threads on Twitter

5/ Essentially an xprv is a private key, and an xpub is its public key, and each one is extended with additional data

This extra data (called the “chain code”) helps you generate a nearly endless number of additional keys

6/ All these additional keys are generated using a standard pattern, so they can be re-calculated at any time!

Why is this useful?

Say you had a wallet with millions of addresses in it, and tragically all the data got destroyed...

7/ As long as you still had your original seed (xprv), you would be able to re-generate all your addresses by following the standard pattern, and you’d be able to recover your whole wallet!

8/ So what is this special pattern that allows you to generate so many addresses from a single seed?

The math involves some hashing which I won’t go into detail about here...

But one concept you should be familiar with is a “Derivation Path”

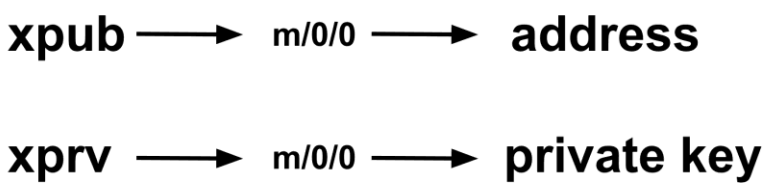
9/ Derivation Paths are like instructions that tell you how to generate an address, and they look something like this:

Derivation Path	Address
m/0/0	1991C5pxTyqLtjrJQxciLYtW5fMjSSLwAG
m/0/1	1MzREAev7KZBCRcqaZhF7uo2zDHNHoCpuE
m/0/2	1D8h7StBmnEy2ARbXAyYA1kiuFcSbSqgMF
m/0/3	1F77LcVWT52jeonWKugCPrcReDn4UKwsHJ
m/0/4	1BEPpYWejDQ5etCxcMeVta6wbEYVTZWpLk
m/0/5	1Q2fDd8xUt4NZDN6iJxDBBkkUSoWGLC7kL
m/0/6	1Lp75ZVzcUNxwZ4HzdsesWyKyX98RWKXuh

10/ Each Derivation Path provides all the instructions needed to calculate the address and its corresponding private key

By applying the Derivation Path to the xpub, you get the address

And by applying the Derivation Path to the xprv, you get the private key



11/ Note, I'm skipping over the concept of "Hardened Derivation", in which the xprv is also used to generate the addresses

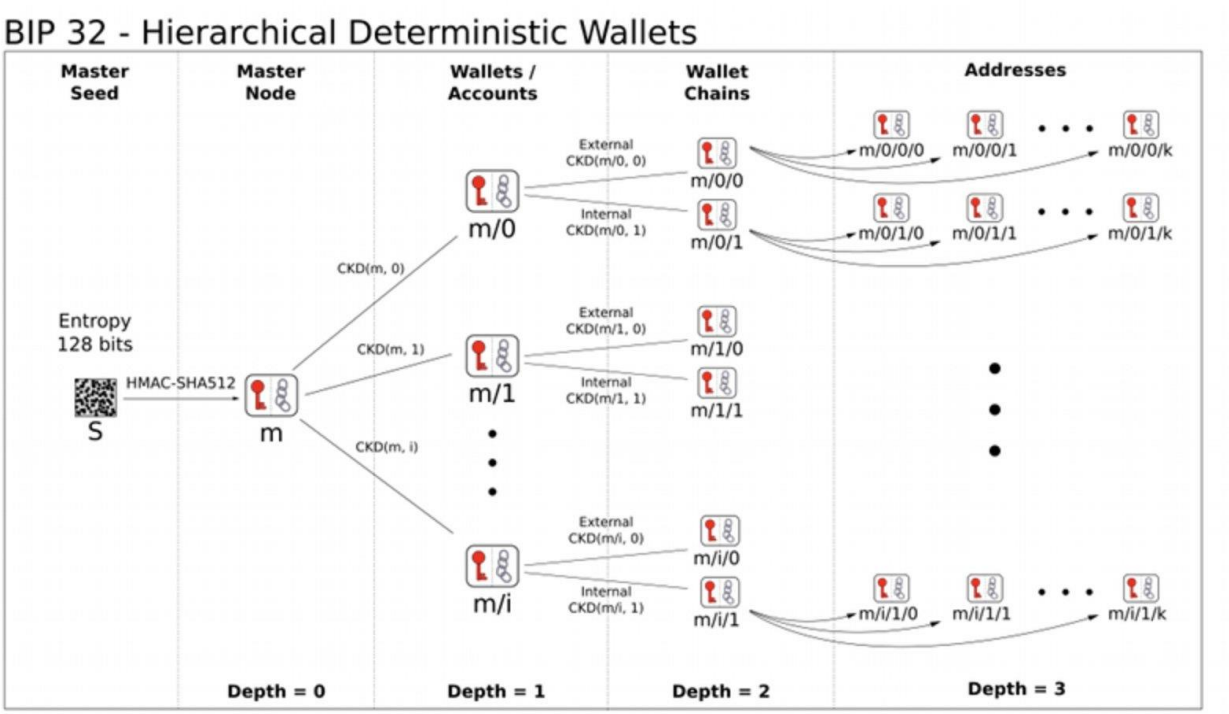
But let's keep it simple for now...

Just think:

- Xpub generates Addresses
- Xprv generates Private Keys

12/ Using HD wallets is a nice way to organize your addresses, as the different numbers in the Path allow you to organize your addresses in a tree-like structure...

A common use case is to put all Receiving addresses on one branch, and all Change addresses on another branch



13/ A note of caution though - it's a good idea to keep your xpub private!

If somebody has your xpub, and you're using normal derivation paths, then they'll be able to calculate all your addresses and see the entire contents of your wallet!

14/ This is why auditors might ask for your wallet's xpub

Without the xpub, they'd have no way of knowing that all your different addresses are connected (assuming you don't send transactions between them)

15/ So to recap:

- An xpub is public key with some additional data that lets you generate a ton of addresses
- An xprv is the private key that lets you generate a ton of private keys that correspond to these addresses

16/ And together they are the foundation for HD wallets, which are a neat way to organize your wallet without having to store a bunch of individual private keys

17/ Hope this was helpful! Shoutout to @PeterMcCormack for the original question

I hope that everyone feels comfortable asking questions, and I hope everyone can be more friendly about explaining complex topics to others

This stuff is complicated! 18/ For more educational threads on all the basic technical concepts behind Bitcoin, check out this mega-thread where I've linked all my previous ones:

18/ For more educational threads on all the basic technical concepts behind Bitcoin, check out this mega-thread where I've linked all my previous ones.

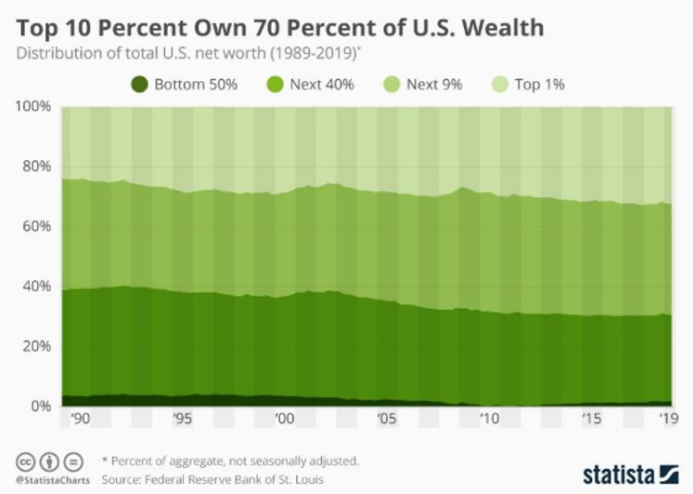
19/19 And check out my email list to stay connected with me

Bitcoin is One for All

By Parker Lewis on Unchained Capital Blog

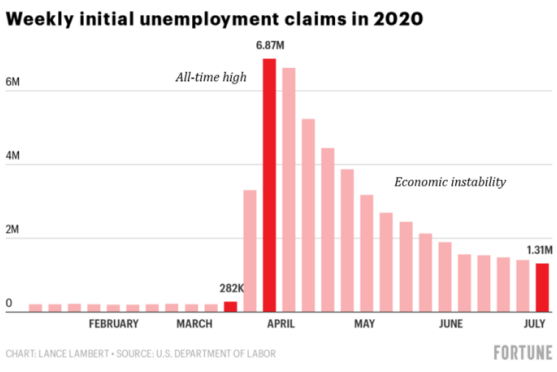
Posted August 27, 2020

At the Democratic National Convention (August 2020), Congresswoman Alexandria Ocasio-Cortez described the Bernie Sanders presidential campaign as, “a movement that realizes the unsustainable brutality of an economy that rewards explosive inequalities of wealth for the few at the expense of long-term stability for the many.” That the current economic system is working very well for a few at the expense of the many has become more widely recognized and accepted across both sides of the political aisle in recent years. While there is vehement disagreement on the appropriate solution, most everyone at least agrees that there is a problem. Fortunately or unfortunately, there is no political solution to a problem that is inherently of economic origin. It is unfortunate because politicians of all ideologies will make promises of grandeur while further dividing the nation as they hopelessly search for a political solution which does not exist. At the same time, it is fortunate that the solution is not political, as bridging partisan divides has historically proven to be a fool’s errand.



Without doubt, the economic structure is broken. Wealth gaps are only becoming wider, it is unsustainable, and economic instability is everywhere. The stock market and national average home values are back at all time highs while tens of millions of Americans are filing for unemployment and half of society has practically no savings. Economic equations do not add up. That is a hard-to-deny reality; it is suffocating many and it applies globally. Politicians simply are not the answer. The fundamental problem with the current economic structure lies not in politics, but in the currencies which

coordinate economic activity (e.g. the dollar, euro, yen, peso, bolivar, etc.). The chink in the armor is in the foundation. No politician can fix problems that stem from structural flaws inherent to modern money. Once the foundation is fixed, then solutions to higher order challenges can follow suit, but until then, any efforts will continue to prove ineffective.



A currency is the foundation of an economy because it coordinates all economic activity. If an economy is functionally breaking down, it would be more appropriate to say that the underlying currency is not effectively coordinating economic activity; the currency is the input and the economy is the output. In short, the fly in the ointment is the money. While many are focused on how to solve the problem of massive wealth inequality, very few connect that the greatest source of inequity lies in the tool that everyone is using to coordinate the entire orchestra. It is not just that the economy is not working for many; it is that the dollar (or euro, yen, etc) as the primary mechanism coordinating economic resources is failing for everyone. Economic imbalance and growing inequality is the new normal, but there is nothing natural about sustained economic imbalance. In fact, it is an economic oxymoron. Balance is critical to the functioning of any economy, and when functioning properly, an economy would naturally eliminate imbalance in its normal course. If an economy fails to do so, and instead allows imbalance to be sustained, that is evidence of a broken economic structure. But, the massive and growing economic imbalance which exists today is not the inevitable and unavoidable consequence of free market capitalism; instead, it is principally a result of central bank monetary policy, which allows economic imbalances to be sustained in ways that would otherwise not be possible.

Central bank monetary policy is the exogenous force creating massive economic distortion and extreme levels of inequality. The mere existence of economic inequality is not in itself an inequity; in fact, unequal outcomes are both natural and entirely consistent with economic balance. On the other hand, the inequality which has been created and exacerbated by a flawed monetary system ***is*** an inequity, and it is not natural to a free market

economy. It is exogenous. The structural flaw inherent to the dollar currency system (or any fiat currency system) is the force most responsible for sustained economic imbalance. Unsustainable and extreme wealth disparity follow from that imbalance. Every other distortive economic action or policy exists at higher orders than the issues created by the manipulation of the money itself. That is the root of all structural economic problems, and until it is fixed, the world will remain suspended in an increasingly fragile state. The legacy monetary system centralizes and consolidates wealth; that is the output of sustaining and exacerbating economic imbalance. It is a system that works for a few in the short-term but fails for all in the long run because the end game of monetary manipulation and an ever-growing economic imbalance is instability. The currency's ability to coordinate economic activity degrades gradually and eventually fails completely; everyone pays that inevitable price.

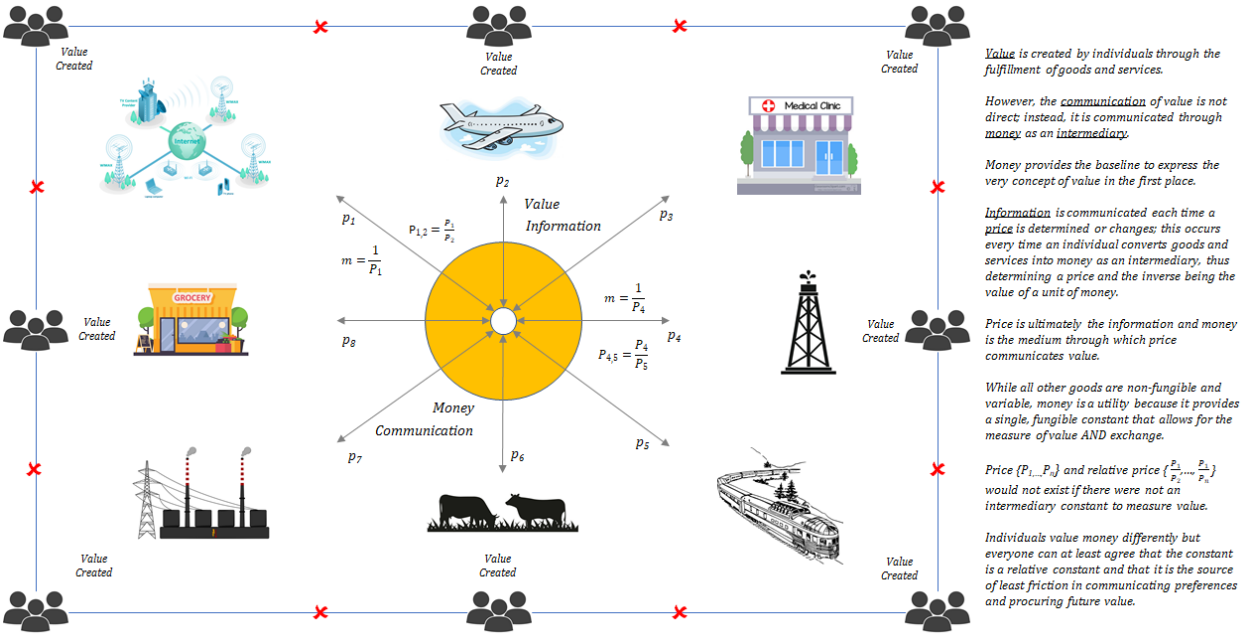
Bitcoin is the polar opposite. It is one currency that works for all, now and in the future. It eliminates imbalance as a natural function, wherever and as soon as it appears, because its supply cannot be manipulated. With a fixed supply capped at 21 million and an ever-increasing adoption curve, more and more people own bitcoin, and each person controls a smaller and smaller share of the same fixed pie. The ownership of the currency naturally becomes more distributed and less concentrated over time, which provides the foundation for greater balance. Bitcoin levels the playing field and ensures that the monetary system cannot itself be a source of extreme inequity. It does so by guaranteeing certain inalienable rights. Every holder of the currency is provided the assurance that more units of the currency will not be arbitrarily produced, and each unit of the currency is treated equally within the network. Bitcoin more effectively coordinates economic activity because its pricing mechanism cannot be distorted or manipulated by exogenous

forces, which is the fatal flaw of the legacy currency system. A fixed supply, equal protection, and true price signals deliver greater balance. Bitcoin fixes the economic foundation for everyone such that everything else can then begin to fix itself.

The Role of Money and the Price System

As a simplified construct, think about money as the coordination function within an economy. The utility of money is to intermediate a series of exchanges. Receive, hold, spend (h/t @pierrerochard), that simple. Money is the intermediary good used to both establish and trade value. As the market converges on a common form of money, a price system emerges, which allows for the subjective concept of value to be more objectively measured. Money is the pricing mechanism and the output is a pricing system. The price system communicates information; it aggregates individual preferences within an economy and communicates those preferences through local prices, as measured in a common monetary medium. Change in prices reflects changes in preferences.

Because preferences are ever changing, so too are prices. Within a developed economy, there are millions of goods, each with individual prices resulting in billions of relative price signals. Relative price signals ultimately communicate exchange ratios between various combinations of goods. While the value of any single good may be static for a period of time, certain prices are always changing within an economy, which dictates that relative prices are ever changing. An economy constantly works to find balance through the aggregate changes in price levels. Anyone and everyone within an economy reacts to the price signals most relevant to their own preferences, which naturally change and become dynamically influenced by changing prices themselves. Through the price system, individual market participants learn both what others value and what they need to produce to meet their own needs. As prices change, behaviors change, and everyone adapts. The price system is the ***visible*** hand which allows for balance to be achieved and for imbalance to be identified and eliminated. Long-term economic stability is achieved because variable information is constantly communicated through the price system. It is the fluctuation in prices inherent to undistorted markets that actively prevents large scale and systemic imbalances from forming.



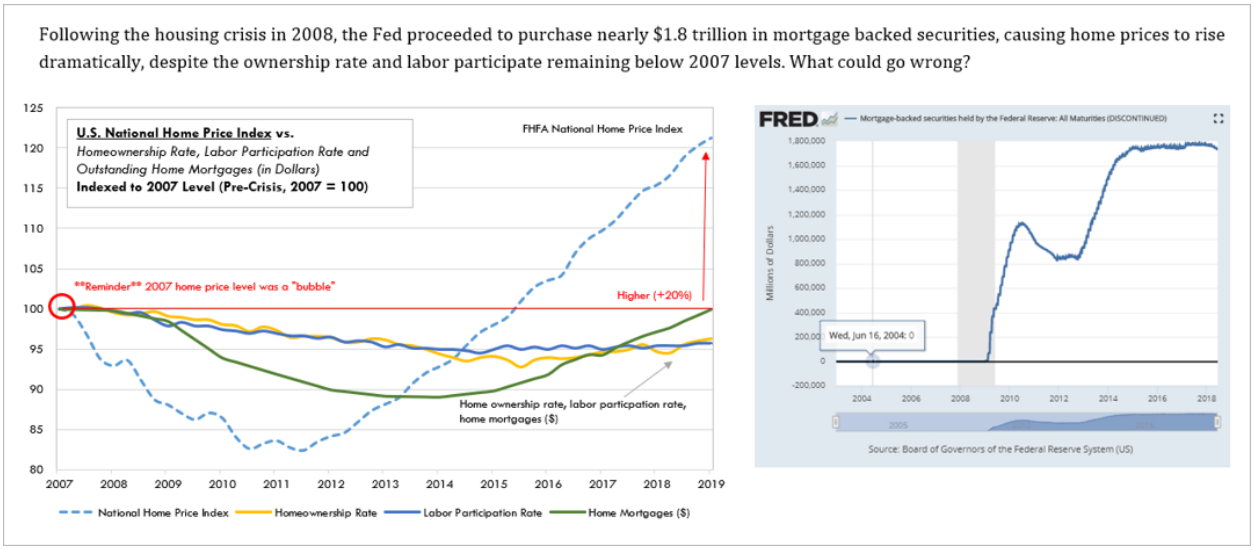
Flaws of the Central Bank Mandate

The foundation of the economy is broken because the money coordinating economic activity is actively manipulated. Most central banks, including the Fed, have the authority to create money arbitrarily at no cost and have a mandate to maintain stable prices (i.e. a price stability mandate). This combination is fatal to the functioning of any price mechanism and ultimately to the underlying economy. When a central bank targets the stability of any price level, it is actually working in opposition to the natural course of an economy, which seeks to find balance and to adapt to a change in preferences through the price system. Worse yet, the means by which a central bank works to achieve price stability is through the manipulation of the money supply, which distorts the entire pricing mechanism underpinning the economy. With every exogenous attempt to achieve price stability, the central bank actively allows imbalances to be sustained and distributes bad information to every person within the economy through false price signals, which in turn causes further imbalances to grow. Imagine this happening each time the economy tried to find balance. By sustaining imbalance, those that principally benefited from the existence of imbalance are continuously advantaged at the expense of everyone else.

Made worse, it actively impedes the ability of those on the lower end of the economic spectrum to contribute and to command a greater share of the resources within an economy. Artificially inflated asset prices create an uphill battle for those that do not own assets, and false signals induce poor economic decisions, disproportionately harming those lowest on the economic spectrum who can least afford errors and setbacks. False and

distorted economic signals, created through the manipulation of the money supply, are counterproductive for all in the long run, but in the short-term, benefit those to whom the imbalance is positively skewed.

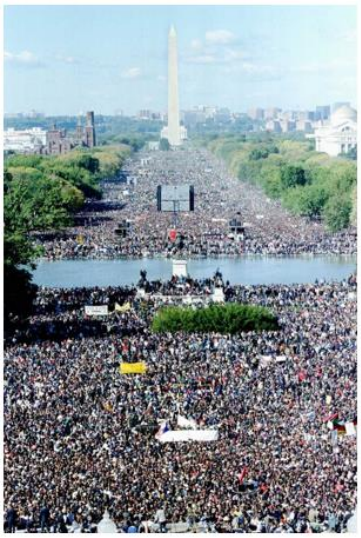
For example, when the value of real estate was declining during the 2008 financial crisis, the price mechanism of the economy was communicating that there was an imbalance. In aggregate, market participants were communicating an increasing demand for money relative to a decreasing demand to hold real estate. At that particular moment in time, the actual amount of money and the available supply of real estate were not rapidly changing. Instead, preferences within the economy were shifting as were relative price signals. Rather than allow the economy to find balance and eliminate imbalance, the Fed increased the supply of dollars in an effort to "stabilize" the dollar value of real estate. More literally, it created $1.7 trillion dollars and used those newly minted dollars to purchase mortgage-backed securities as a direct means to support the value of real estate. Those that owned real estate (e.g. housing) or operated businesses dealing in the production (or financing) of real estate benefited disproportionately at the expense of those that did not. The benefit skewed to the side of existing imbalance, as it always does when imbalance is being sustained artificially.



Not only did the Fed manipulate the value of real estate, it manipulated and distorted all price signals within the economy by significantly increasing the money supply. The market function to eliminate imbalance would have been for prices to change. The Fed's solution was the opposite. It devalued the money (by increasing its supply), such that the value of real estate (among other goods) as priced in dollars would change the least. Rather than eliminate imbalance, the Fed's actions allowed imbalances to be sustained and actually grow. Once one actually appreciates the fundamental role which money and the pricing mechanism play in coordinating economic activity, it

becomes clear as day that sustaining imbalance is precisely what occurs each time the Fed intervenes to stabilize price levels. Stability when achieved through manipulation merely suppresses volatility. It creates an unnatural rigidity in price, when price fluctuation is both a desired state and the natural function of a market communicating changes in preferences. When imbalances that would otherwise be eliminated are allowed to be sustained by artificial means and for extended periods of time, it ultimately creates greater volatility in the long run and critically impairs the ability of a monetary medium to coordinate economic activity, which is its singular utility. Each time and cumulatively, it advantages and further embeds the incumbents, just as the market is working to eliminate imbalance.

Rather than have a billion people that actually make up an economy set prices, a few number of people unilaterally change the whole game by clicking a few buttons on a computer screen; it distorts the entire value chain of the pricing mechanism.



By manipulating price levels, the Fed isn't just preventing smaller intermittent fires from naturally running their course while creating larger fires down the road. Instead, think of the Fed's actions as the arsonist that lights a fire, leaves through the back door in the middle of the night, and then is celebrated as the hero when it arrives through the front door to fight the fire with gasoline. A change in price levels, even if particularly volatile, is not a fire that needs putting out. Artificially preventing changes in price, aka a price stability mandate, is what lights the fire in the first place. The Fed coopts the entire value chain of the pricing mechanism. Change in price is actually desired and the central bank works in opposition to that change by manipulating the money supply. The formation of imbalance within an economy is natural; creating a centralized mechanism which prevents imbalances from being eliminated is the unnatural and damaging part. It also creates long-term economic instability by distorting price signals over decades and widens the wealth gap by constantly advantanging those on

the right side of imbalance. Predictably and unironically, the existence of the central bank's price stability mandate, combined with the power to print money, causes both long-term instability and sustained economic imbalances.

Hayek – The Pretense of Knowledge

> In fact, in the case discussed, the very measures which the dominant "macroeconomic" theory has recommended as a remedy for unemployment — namely, the increase of aggregate demand — have become a cause of a very extensive misallocation of resources which is likely to make later large-scale unemployment inevitable. The continuous injection of additional amounts of money at points of the economic system where it creates a temporary demand which must cease when the increase of the quantity of money stops or slows down, together with the expectation of a continuing rise of prices, draws labor and other resources into which can last only so long as the increase of the quantity of money continues at the same rate — or perhaps even only so long as it continues to accelerate at a given rate. What this policy has produced is not so much a level of employment that could not have been brought about in other ways, as a distribution of employment which cannot be indefinitely maintained and which after some time can be maintained only by a rate of inflation which would rapidly lead to a disorganization of all economic activity. The fact is that by a mistaken theoretical view we have been led into a precarious position in which we cannot prevent substantial unemployment from reappearing; not because, as this view is sometimes misrepresented, this unemployment is deliberately brought about as a means to combat inflation, but because it is now bound to occur as a deeply regrettable but inescapable consequence of the mistaken policies of the past as soon as inflation ceases to accelerate.

Most mainstream economics professors would readily agree that price fixing or setting quotas on certain economic goods naturally creates economic inefficiency and imbalance. However, the same cohort of experts would then turn around and avidly defend central bank monetary policy, not realizing the fundamental inconsistency. Economic manipulation is economic manipulation. Rigidity in price or quantity of any economic good driven by exogenous forces results in imbalance; variance allows for balance and equilibrium. Very logical and not controversial. Why then is the same not understood when applied to money? Imbalances are created when central banks target interest rates through the manipulation of the supply of money, just as imbalances are created when the Venezuelan government arbitrarily sets the price of a gallon of gas below its market value. Ironically, the manipulation of the money supply happens to be economically more destructive because it distorts all prices within an economy, and all relative price signals as individual price levels do not adjust ratably (in fact, far from it). When the Fed pursues its price stability mandate, it is actively sending false price signals throughout an economy and causing imbalances in supply and demand structures to be sustained. Price stability is price manipulation, and it is perfectly predictable that when the price of money is manipulated to

achieve any definition of stability, the very action causes a degree of economic distortion far worse than the manipulation of any single market.

Hayek – The Use of Knowledge in Society

> We must look at the price system as such a mechanism for communicating information if we want to understand its real function—a function which, of course, it fulfils less perfectly as prices grow more rigid. (Even when quoted prices have become quite rigid, however, the forces which would operate through changes in price still operate to a considerable extent through changes in the other terms of the contract.) The most significant fact about this system is the economy of knowledge with which it operates, or how little the individual participants need to know in order to be able to take the right action. In abbreviated form, by a kind of symbol, only the most essential information is passed on and passed on only to those concerned. It is more than a metaphor to describe the price system as a kind of machinery for registering change, or a system of telecommunications which enables individual producers to watch merely the movement of a few pointers, as an engineer might watch the hands of a few dials, in order to adjust their activities to changes of which they may never know more than is reflected in the price movement.

Consequences of Sustaining Imbalance

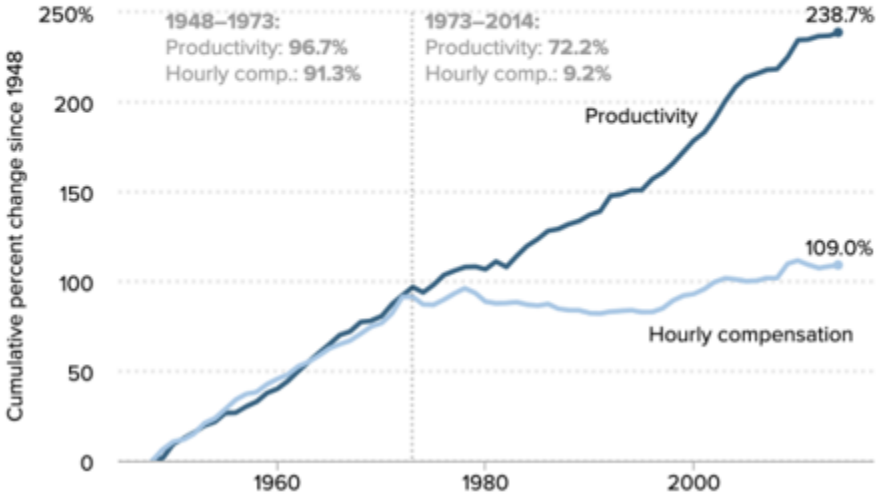
The effects of sustaining imbalance can be best understood and observed through the credit system because that is where the Fed directly intervenes and consequently where the greatest distortion and imbalance exists. As the economy slows and as price levels begin to change counter to the Fed's desired course, the Fed increases the supply of dollars in the financial system by purchasing debt instruments (typically government treasuries) and crediting the accounts of the sellers with newly minted dollars. At the onset, the credit system was just a tool to effect monetary policy; it was the mechanism through which the Fed pursued price stability. Increase the supply of dollars by purchasing credit instruments, reduce interest rates by that same mechanism, induce economic expansion via cheap credit and cause general price levels to stabilize. That was the theory and intent. However, predictably, this pattern caused imbalances to form and be sustained in the credit system itself. Now the tail is wagging the dog. Today, the credit system in the U.S. stands at $77.9 trillion system wide, whereas there are only $4.5 trillion actual dollars within the banking system. For every dollar that exists, approximately $17 dollars of dollar-denominated debt exists (debt-to-dollars of 17:1). Again, this is an imbalance only made possible and sustained as a function of the Fed. Each time the credit system attempts to contract, the Fed creates more dollars to help maintain the size of the credit system, such that it can further expand. Because the credit system is now orders of magnitude larger than the base money supply, economic activity today is largely coordinated by the allocation and expansion of credit rather

than by the base money itself. In aggregate, the credit system is the marginal price setter given its size relative to the base money supply. Because of its price stability mandate, the Fed has an implicit mandate to maintain the size of the credit system, and in order to do so, it must target asset prices that support existing debt levels. It has become circular. The Fed used the credit system as a tool to stabilize price levels but now it must maintain the size of the credit system in order to maintain stable prices.

This vicious cycle was only ever made possible because the Fed has unilateral control of the money supply. In 1971, President Nixon officially ended all convertibility of dollars to gold, and the U.S. government later decoupled the value of the dollar from gold altogether in 1976. While the creation of the Federal Reserve in 1913 was the beginning and President Roosevelt's executive order in 1933 banning private ownership of gold set the stage, the complete departure from gold as a monetary anchor in the 1970s removed constraints that otherwise prevented the true centralization of the money supply, and which ultimately enabled the great monetary inflation which Paul Tudor Jones recently wrote about. Once the final constraints were removed, it opened the door for the Fed to take a more central role in actively managing the economy via the money supply, which it ultimately effects through the credit system. As a direct consequence, the base money supply and the credit system have expanded in ways that would otherwise not have been possible, allowing imbalances to consistently grow over time and creating long-term economic distortions.

FIGURE A

Disconnect between productivity and a typical worker's compensation, 1948–2014

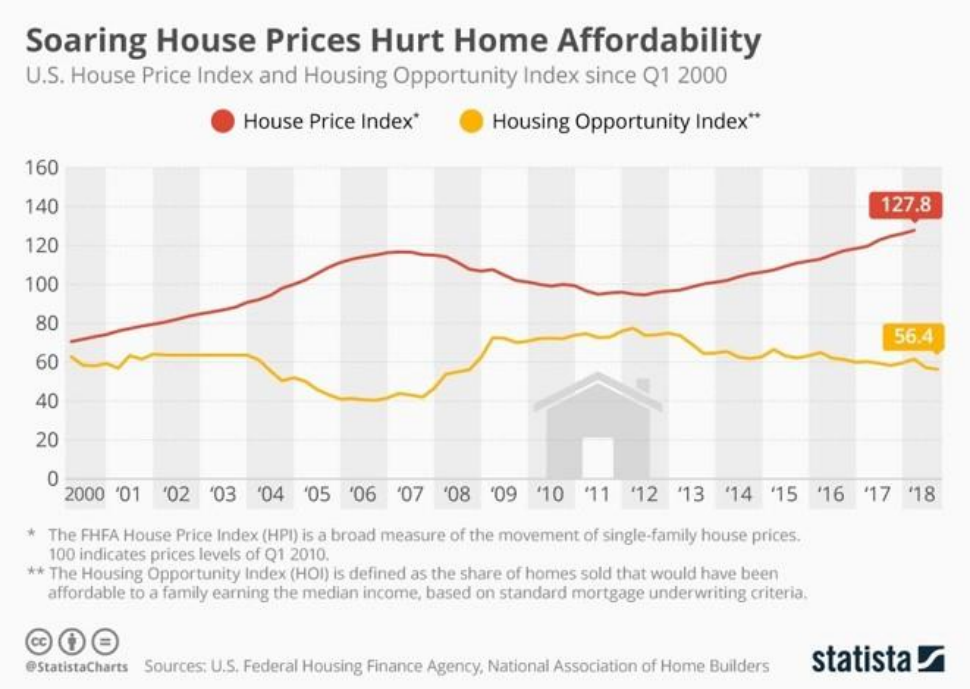


When imbalances emerge in the credit system (i.e. too much debt existing), the Fed supplies more dollars such that existing debt levels can be sustained. Rather than write off bad debt and reduce existing debt levels, imbalances are actively sustained rather than eliminated. This is the real reason why the banking sector and the function of credit has become as large as it has; it would not have been possible if the Fed were not able to print money to artificially sustain unsustainable levels of debt, all in the interest of "price stability." Effectively, each time the banking sector would otherwise contract, the Fed takes measures to actively prevent it. It sounds crazy because it is, but it exists the way it does because the credit system is the primary transmission mechanism of the Fed's monetary policy. The Fed needs the credit system to be maintained because it is through this vehicle that the Fed attempts to "manage" the economy. The Fed sees targeting asset prices to sustain debt levels as less disruptive than allowing debt to be restructured and written off. In the Fed's eyes, it's six one way, half a dozen the other; effectively the same, but with less disruption. In reality, one path is economic manipulation of the worst kind, and the other is the natural and organic balancing of an economy in imbalance. The Fed chooses the former, trading short-term stability for long-term instability and distortion.

While it should be obvious that asset price targeting advantages those with assets (wealthy) and is a regressive tax on those without assets (poor), the Fed has its price stability mandate. For those on the lower end of the economic spectrum with little to no savings, cash naturally represents most, if not all, of one's savings. On the other hand, those at the higher end of the economic spectrum typically hold cash in addition to equity in businesses, real estate and financial assets, such as stocks and bonds. Again, consider the 2008

financial crisis. There were imbalances in both the housing market and financial markets; prices within these markets were at unsustainable levels. As imbalance was being eliminated and as price levels were correcting, the Fed stepped in to “stabilize” asset prices. Imagine that you were someone just entering the economy, without any savings, or you could not afford to purchase a home and likely did not own stocks or bonds. Everyone who owned assets was bailed out at the expense of those who did not, all in the interest of price stability.

By increasing the supply of dollars to prop up asset prices, each dollar naturally becomes worth less. For those lowest on the economic spectrum, wages paid in dollars (labor) were devalued, and asset prices were directly manipulated higher. Inflation of most all consumer goods broadly followed. It is the equivalent of being hit from both sides. Wages purchase less and less day-to-day, and it becomes measurably more difficult to accumulate the amount of savings necessary to purchase assets. Initially, the effects are at best zero-sum. Those at the top benefit, those at the bottom suffer. In the end, everyone loses because the end game is economic instability. Notice the negative correlation below between housing prices and housing affordability, and then recognize that housing prices are actively manipulated by the Fed. Also recognize that housing prices are at an all-time high (above 2007 bubble levels), when nearly half the country has no savings. That equation only exists in a manipulated world, and it crushes those without savings.



Economists running the show and those that benefit the most will overwhelmingly agree it has to be done (every time); history is written by the winners but it is still all smoke and mirrors.

"Sure, it was a crazy experiment, but the Fed had no other choice. Just imagine all those on the lower end of the spectrum that would have lost their jobs if not for the Fed's actions. Without a job, the poorest on the economic spectrum would have been far worse off and would not have been able to afford a home."

At least, this is the common, predictable defense. The same line has certainly been used to defend the Fed's most recent actions in response to the global pandemic (printing $3 trillion with a T). While it may seem like logic, it is an anecdote that lacks any fundamental economic argument in defense of the manipulation of price levels. The narrative is caught in a vicious cycle that begins with economic imbalance as a starting point (and one created by decades of the same distortive monetary policy). Recall the role of arsonist hailed as a hero fighting the fire. You cannot dig yourself out of a hole by continuing to dig in the same direction. At a fundamental level, manipulating price levels allows imbalances that would otherwise course correct to be sustained. It disproportionately advantages those that contributed to, and benefited the most from, the very existence of imbalance – like having your cake and eating it too, or like getting a second bite at the apple. Those most directly bailed out took an inadvisable risk, and rather than be penalized, the world of imbalance is sustained. The advantages gained from manipulated incentive structures are allowed to continue in a way that would not be possible absent the Fed's policy decisions.

An Unmanipulated Economic Structure

While there is never perfect balance, the existence and fluctuation of price levels is how an economy works toward balance through trial and error. Every individual reacts to an ever-changing set of price signals. It is how people evaluate which businesses to create, which skillsets to acquire, and which jobs to pursue, all of which are interdependent on each individual's own interests and capabilities. Imbalances can naturally arise within an economy as individuals speculate and over-invest in certain segments based on imperfect expectations of consumer preferences. That is the nature of trial and error. Nobody knows or can predict the future; they use price signals to best guide decisions. A business or individual produces a good for X and attempts to sell it for Y, and if insufficient demand exists to make the activity profitable, that is the market communicating information to the producer. Better luck next time; build it for less or build something else that is of greater value or valued by more people. Imbalances are eliminated. Those that took the risk own the consequences, and it's back to the drawing board in a never-

ending game aimed at marrying individual ideas and skillsets with the preferences of other market participants.

"Prices and profits are all that most producers need to be able to serve the needs of men they do not know. They are tools for searching — just as, for the soldier or hunter or seaman, the telescope extends the range of vision."
— Friedrich Hayek

Money is the tool that is used to coordinate resources and to test the market by trial and error; it becomes the lifeblood of an economy because it is the foundation of a price system. It is how information is distributed to all participants. The better the money, the more reliable its price system. And the more reliable a price system, the greater the balance in an economy. Those within an economy that deliver the greatest value to the largest number of people are naturally rewarded with the most money, but money would be of little value to the producer if others were not producing goods that they themselves valued. The system would not sustain itself if balance did not exist; in order to purchase a good or service from another individual, one must have earned money in the first place. Acquiring money by voluntarily providing a service valued by others is a far better outcome for everyone in aggregate than if money were to be acquired through any other means. It is so because it's the only way for the cycle to be repeatable and symbiotic rather than one-off and zero-sum. What good is a customer that runs out of money or doesn't have any in the first place? In a balanced economy, every producer is a customer of someone else and vice versa.

"Give a man a fish and you feed him for a day; teach him how to fish and you feed him for a lifetime."

One need not be religious to understand the wisdom. Each individual benefits by having a larger number of people producing more goods or services, and everyone is incentivized to produce output valued by others within an economy. Everyone has a selfish interest in both delivering value to others and in helping others to contribute value in return. But, it is not just a naïve or hopeful economic view of the world; there are discernible benefits to trade, specialization and ultimately, in a broader range of choice for all individuals, which organically dictates a division of labor. Money coordinates the division of labor, and the form of money with the most reliable pricing mechanism will consistently deliver the greatest value with the greatest range of choice and balance. The pricing mechanism with the least distortion provides the clearest signals as to what other people value, and derivatively, provides the greatest assurance that the information communicated is not a false signal. The undistorted function of a monetary medium and its price system is what ensures imbalance is eliminated; it is the governor that allows for balance to be restored and for symbiotic relationships to continuously be discovered in a constant process of trial and error.

A Manipulated and Broken Economic Structure

The Fed's monetary policy actively prevents the economy from restructuring and from finding balance. Efforts to maintain price stability when imbalance exists equates to maintaining otherwise false price signals. Productive assets remain in the hands of a few, and the world remains suspended in a state of imbalance. Money that makes its way to those on the lower end of the spectrum eventually finds its way back to those that control the productive assets like a steel trap because structural imbalances are never fixed. Instead, the natural healing process is stymied when the Fed intervenes. The structure of the economy cannot sustainably cycle money in a symbiotic way because balance does not exist; skillsets and preferences of market participants are not aligned. The Fed pumping money into a structurally broken economy is akin to giving a man a fish and feeding him for a day, while at the same time preventing him from learning how to fish by sustaining false signals. The existence of imbalance signals that the composition of an economy is not meeting the needs of the participants that make up the market. Or rather, that the assets and individuals which capture the lion's share of wealth would not continue to do so if the economy was allowed to restructure.

The Fed's economic structure produces inequity by preventing imbalances from rebalancing. That is what the market attempts to do every time the Fed steps in to keep the dream alive. Giving all benefits of the doubt, the Fed believes it is helping. The starting point of the Fed's economic theory is that active management of the money supply is a positive driving force. That is in its DNA. It is not questioned or debated. It sees its activities as smoothing out market signals rather than manipulating them. The question for all those within the four walls of the Fed is how much and when to manipulate the money supply, not if. Would anyone expect the Fed to be an honest evaluator of its actions? It would be like grading your own test; no one would reasonably expect an objective assessment because there can be no objectivity. Certain false assumptions are encoded in their brains as true which prevents the possibility of objectivity. They look everywhere for answers but in the mirror, and try the same policies over and over again, always expecting a different result.

Economics

Powell's Fed Shift Allows for Higher Employment and Inflation

updated 2 hours ago

U.S. Jobless Claims Resume Decline But Report Comes With Caveats

Stocks Mixed, Yield Curve Steepens After Fed Pivot: Markets Wrap

A Warning Flashes for Record U.S. Stock Rally

(Bloomberg headline following speech by Chairman Powell on August 27, 2020; everything is under control)

"Inequality is something that has been with us increasingly for more than four decades, it's not really related to monetary policy. It's more related to [stutter] there are a lot of theories on what causes it, but it's been something that's more or less been going up consistently for more than four decades and there are a lot of different theories, one of which is just that globalization and technology call for rising levels of skills and aptitudes and education and that U.S. educational attainment flattened out, certainly relative to our peers, over that period[.]" Jay Powell, Chairman of Federal Reserve (June 2020)

Fed Chairman Powell recently provided this as a response to a question asking whether Fed policy contributes to increasing wealth inequality. Notice how the response is not an argument as to why central bank policy does not cause imbalance and inequality. It is more of a pronouncement followed by a "look over there" defense. Never believe the myths about globalization and technology driving wealth inequality. There is nothing about technology, innovation and globalization that causes sustained economic imbalance or a structurally expanding wealth gap within an economy. For innovation to be valuable, it by definition must solve problems for a range of people, but if those that valued it did not have money or means to afford the innovation, it wouldn't be valuable. Value becomes self-referencing in that sense. Economic balance is a governing input to value. In order to believe the tall tales of technology and globalization causing economic imbalance, one would have to be willfully blind to the impact of centralizing the money supply, which in turn caused banking to become the epicenter and lifeblood of the economy, and which made it possible for imbalance to actively be sustained over decades as a policy decision. There may be many theories, but the manipulation of every price signal within the economy is ground zero to economic imbalance and inequity; it is the structural flaw in the foundation which creates the unlevel playing field off of which all other contributing factors compound.

If A then B; if not A then not B

Money is the bedrock of economic systems. Understanding the fundamental and foundational role money plays in the economic engine establishes the logical connection between systemic economic issues of imbalance and the artificial manipulation of the money supply. Of course, there are other factors at play. The money supply is not the only way economic activity is manipulated. Tax policy, government spending and the regulatory apparatus all contribute. But, focusing there would be like trying to fix the windows on the 100th floor when the bottom ten stories are each being supported by a single Jenga block. That is the relationship between the issues inherent in the monetary system (the foundation) and all other economic issues (higher levels). The core problem that bitcoin solves is the foundation. If everyone were to display a little bit of humility, each would recognize that there is no silver bullet to solve the structural problem of a widening wealth gap and economic imbalance. There is no individual with a plan or piece of legislation that will make everything better. Imbalance created by central command does not get solved by central command. Quite the opposite. The only real hope is to first fix the foundation, such that everyone on net can get back to doing the desirable things without the need for conscious control. Balance will follow from there.

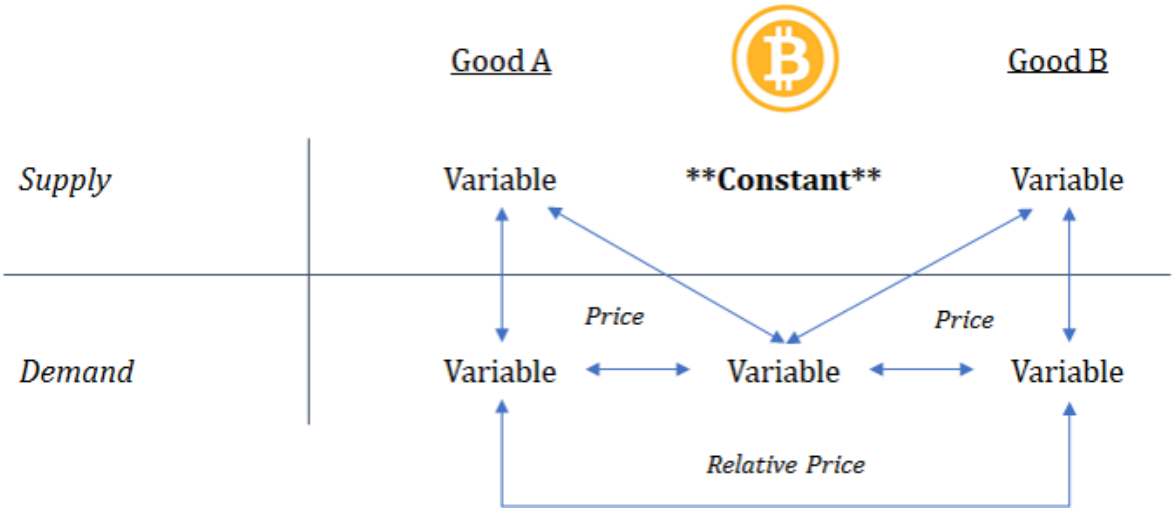
"But those who clamor for "conscious direction"—and who cannot believe that anything which has evolved without design (and even without our understanding it) should solve problems which we should not be able to solve consciously—should remember this: The problem is precisely how to extend the span of our utilization of resources beyond the span of the control of any one mind; and therefore, how to dispense with the need of conscious control, and how to provide inducements which will make the individuals do the desirable things without anyone having to tell them what to do." Hayek, Use of Knowledge in Society

With a fixed supply of 21 million, enforced on a decentralized basis and controlled by no one, bitcoin has taken away the ability to manipulate the monetary function entirely. If misbehaving children cannot find a way to share a toy and play nice, what do you do? You take the toy away and put the kids in the penalty box. That is kind of like the relationship between bitcoin and central banks. No human (or institution) can be trusted with control over the money supply, so the only practical solution is to take away the ability and temptation all together. The one constant in bitcoin is its fixed supply; there will only ever be 21 million bitcoin, and there is nothing anyone can do about it. Everything will change around bitcoin, but its supply as a constant will increasingly become the guidepost off of which all other activity is measured. It ensures a level playing field and represents a source of truth, which is absent in the existing economic structure. Because its supply cannot be

manipulated, neither can its price signal. Undistorted price signals communicate more perfect information. But never confuse more perfect information and a level playing field with price stability or the issue of volatility. If the value of bitcoin is $12,000 today and $10,000 tomorrow, that is the undistorted communication of information.

"Variation is information. When there is no variation, there is no information. [...] There is no freedom without noise—and no stability without volatility." — (Taleb & Blyth, Foreign Affairs, May/June 2011 Issue)

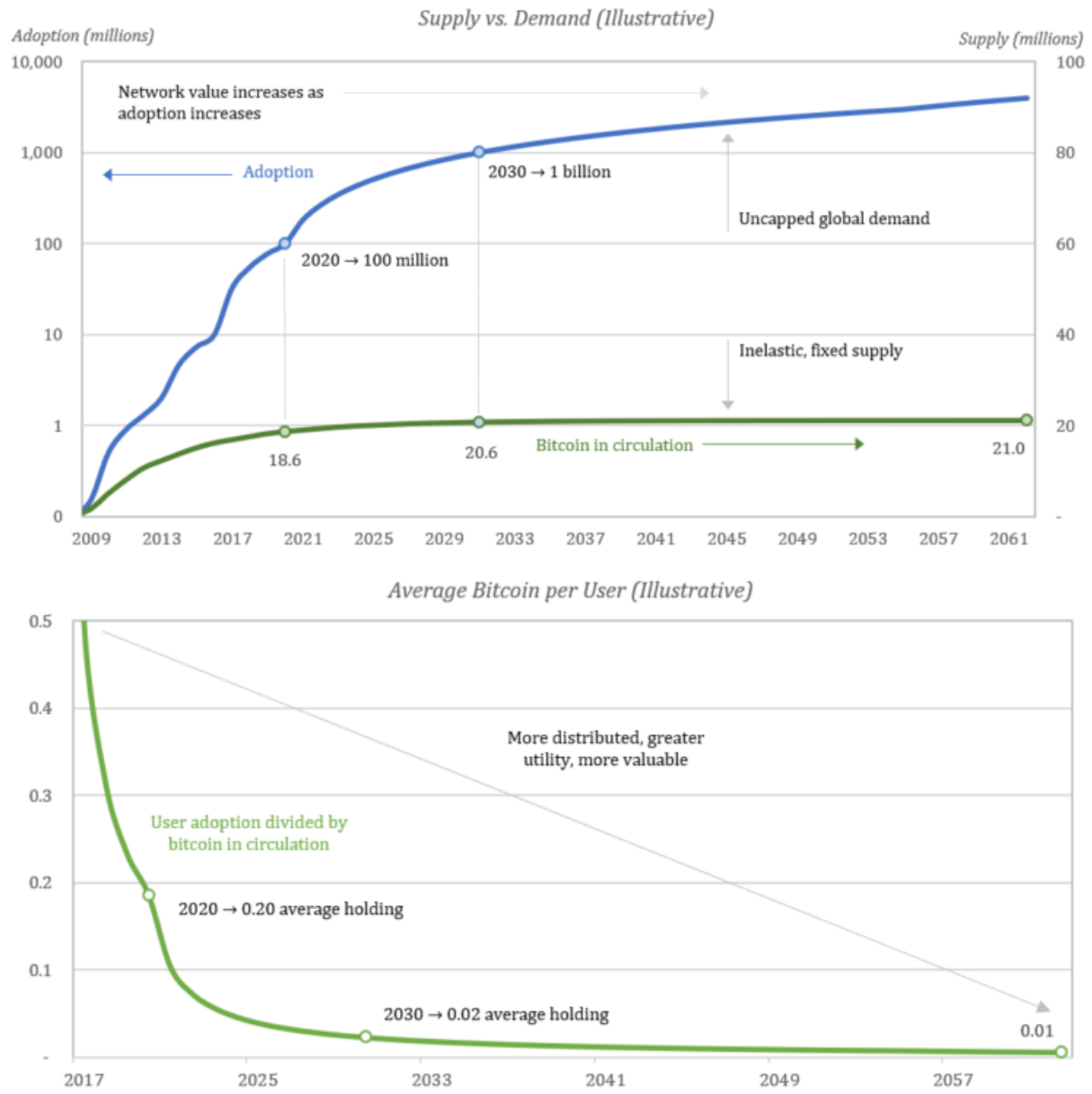
A fixed supply ensures that any change in price is exclusively driven by a change in demand rather than an artificial and unpredictable change in the supply of money (i.e. communicating a change in preferences to the entire economy). It eliminates an entire side of the equation, which heavily influences changes in prices today, and which distorts the communication of preferences. Imagine knowing with absolute certainty that every change in price were dictated by a change in consumer preferences rather than the effects of increases or decreases in the money supply. That is the difference between being able to consistently rely on true economic price signals and playing musical chairs knowing someone else is in control of the stereo. Today and into the future, the same principle will hold true. Everyone will be able to rely upon and trust that changes throughout bitcoin's price system will always be true and never be influenced by unpredictable changes in supply.



This fundamental difference between the existing monetary structure and bitcoin changes the entire game. False price signals vs. true price signals. False price signals are the equivalent to believing you have a cheat sheet for a test, training yourself based on that information and then showing up only to find out that the test was entirely different. Everyone believes they are responding to true price signals, not realizing that the information

communicated would be fundamentally different if the money had not been manipulated. Each time a violent shock occurs within the system, everyone gets a hint that price signals were communicating bad information, but then the Fed steps in to stabilize prices and everyone becomes reassured that it's ok to come back outside and play, relying on the same bad signals. The primary reason a violent shock to the system is even possible is because this process has occurred every time the economy has attempted to structurally rebalance over the past 50 years. Bad signals attempt to correct, only to be sustained and exacerbated by exogenous forces. With a fixed money supply, this wrong is permanently righted. It will no longer be possible to sustain imbalance. So long as bitcoin exists, the monetary medium will not be capable of distributing distorted price signals. There is a difference between right, wrong and true. True price signals merely ensure that the information being communicated is reflective of the individual and aggregate preferences of an economy. In that sense, there is no right or wrong, so long as the information can reasonably be relied upon as accurate and undistorted. No one has to trust or question whether bitcoin's price signals are true because its fixed supply will guarantee it.

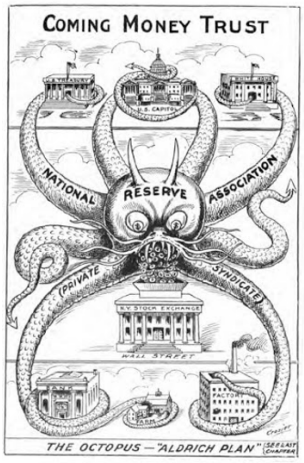
And no longer does anyone need to figure out how to play a rigged game because that game is ending. The days of monetary inequity will soon be past as bitcoin distributes throughout the world. It will shift the balance of power back to those that actually create value, as defined by true price signals, which are communicated by individuals that hold the currency. Setting aside taxes and regulatory capture for a moment, if one wants to acquire bitcoin, he or she will have to provide value in return, and bitcoin will become the arbiter of that value. Of 21 million, approximately 18.5 million bitcoin are already in circulation. The 18.5 million in circulation are all held by some individual or entity. In order to acquire any, bitcoin must be earned by delivering value to those that hold the currency. Even for those not yet circulating, every single bitcoin must be earned by contributing value. The same is not true of the current monetary system. In the current structure, dollars can either be earned by delivering value to others within the economy, or conversely, if the Fed decides to hand out more money. And this happens quite frequently. Of all the dollars that exist today, over 80% have been created and allocated by the Fed since 2008 (source link), rather than by the alternative – delivering value to others within the economy. Which system sounds more fair, balanced and conducive to aligning incentives throughout an economy over decades and generations?

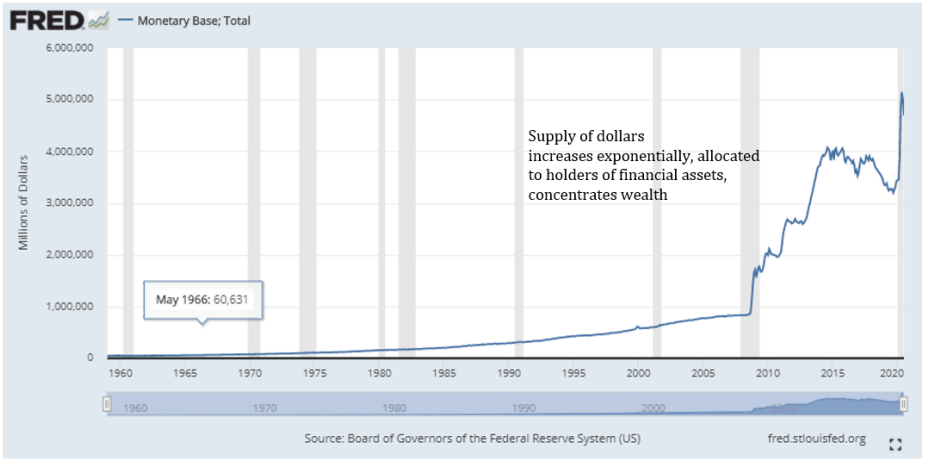


As more people adopt bitcoin, the currency is transferred from those that have to those that have not. By making the nominal amount of bitcoin zero-sum, it ensures that the economic system is non-zero sum. In order to join the economy, you must deliver value to someone within the network. No value leaks outside the system; no inefficiency can be introduced through the production of money. Whether new entrants are joining the network or trade occurs from within, value is always transferred, and through that transfer, value is actually created. Recall that the valuable function of money is to coordinate economic activity. The production of money, on the other hand, produces no value and only serves to distort and impair the ability of a monetary medium to properly function. The nominal amount of money is not

important. What is important is its ability to communicate accurate information to a broad set of economic participants.

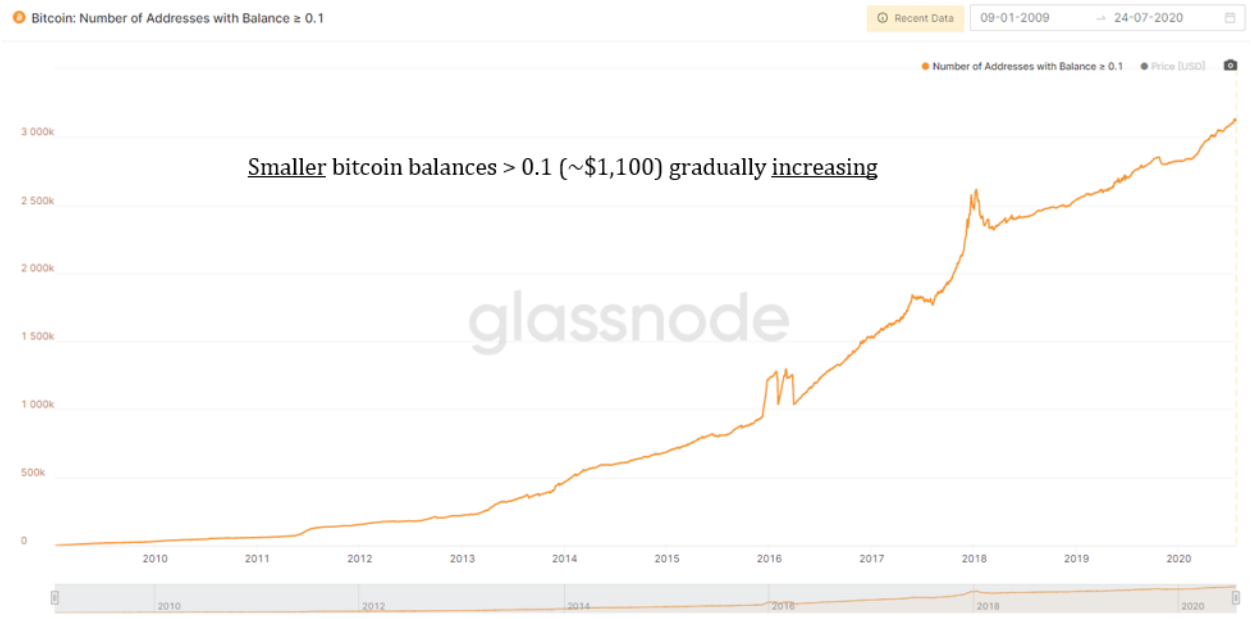
That is why people demand money, and with a terminal rate of change set at zero, each participant can use bitcoin to best understand the value of his or her own output relative to that of others and relative to the preferences of others, undistorted by any changes in the money supply. Each person can make better decisions (on average) in the pursuit of his or her own interest, while by definition delivering value to others as a means to that end. A fixed amount of currency plus more people valuing it equals greater distribution of the currency. With a fixed supply, no more than 21 million bitcoin can ever be saved and paradoxically, that change in the incentive structure will cause more people to save. By introducing an incentive to save (i.e. a fixed supply), more people will. And as more people save in a currency which has a fixed supply, it results in more and more people owning less and less but through that function of more people saving, it creates greater stability. Whereas the centralized control of the money supply and the ability to sustain imbalance causes wealth to consolidate, a fixed money supply naturally causes the currency to become further decentralized and more distributed, delivering greater balance.

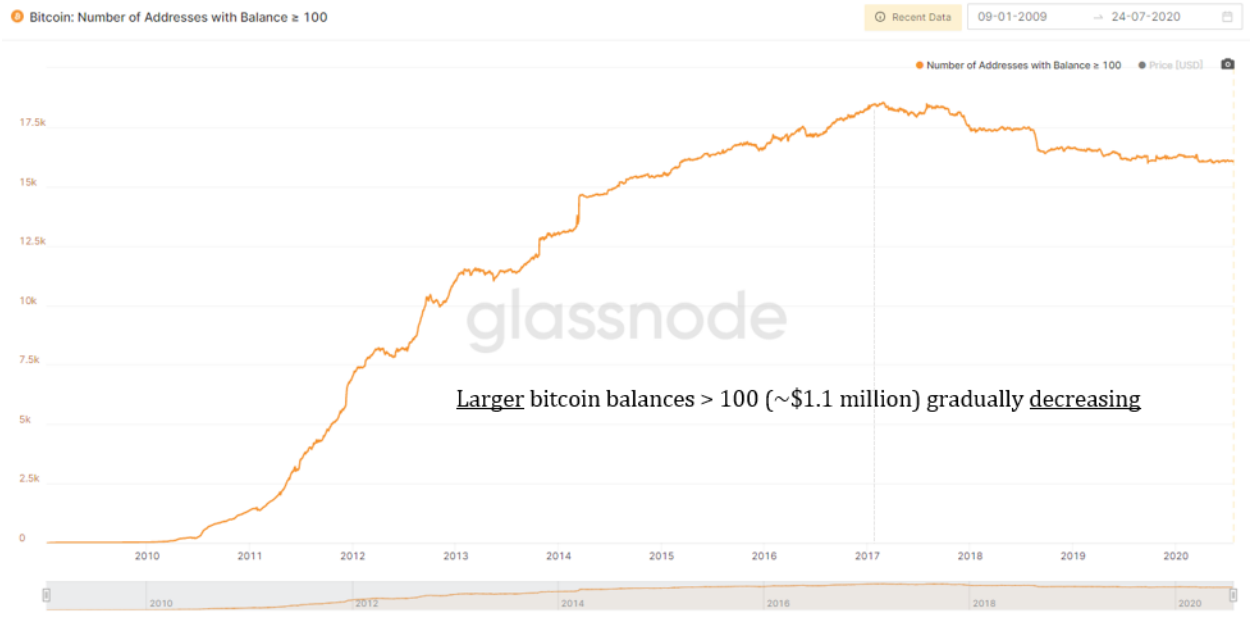




Centralized governance of the money supply allows the distribution to consolidate as new units of the currency are created and as imbalance is sustained; whereas, a decentralized governance model enforcing a fixed supply ensures that the distribution of the currency becomes greater and greater over time. The structure of the currency dictates the opposite effect, and the trend can be seen in actual data. Bitcoin held in smaller denominations continues to grow steadily, while bitcoin held in larger denominations continues to decline. As the currency and economic system grows, the currency becomes more widely distributed. Rather than consolidate, the currency distributes to more people, and the nominal amount held by each declines, while purchasing power increases. As more

people demand the currency, its value rises. However, there is a terminally fixed supply. As increases in demand naturally outpace ever diminishing increases in supply, there is one principal way to acquire bitcoin: by delivering value to an existing holder of the currency. The currency transfers from relatively few early holders to a more widely distributed base as a function of time. Everyone wins; the network utility increases as more participants voluntarily opt in and the distribution of the currency becomes less and less concentrated, ensuring greater balance and reducing systemic risks created by the existence of a few extremely large holders.





When the incentives of a monetary medium align both individual and aggregate interests, non-zero sum outcomes become the default, as does balance. Bitcoin is accessible to anyone, and everyone that chooses to use it is afforded the same protections. Anyone that produces value and exchanges it for bitcoin is assured that their output will not be devalued in the future merely as a function of someone in a far-off land creating new units of money. Separately, everyone is assured the benefit of undistorted price signals. In bitcoin, rich and poor are provided these same protections equally. It is no guarantee that someone else will value the currency more or less, but it eliminates the possibility of an involuntary forced devaluation of labor and output stored in a monetary medium, which distorts economic activity and creates false price signals. When presented with that opportunity relative to a certainty of the worse outcome, it becomes a clear choice. Compared to the current economic structure in which the wealthiest better understand the effects of active monetary debasement and are best equipped to combat and exploit it, there is a reality that those on the lower end of the economic spectrum have more to gain by leveling the playing field. Even still, it is not about rich and poor. Everyone benefits from the elimination of money production and an economy that provides greater balance through the communication of more perfect information.

In a tweet from 2018, the founder of Ethereum (Vitalik Buterin) beautifully and ironically described the power of holding a currency with a fixed supply that could not be manipulated, while actually arguing for the opposite. He both made the precise argument which central bankers use to defend their actions while also articulating the power it would place in the holder of a currency with a fixed supply. While Buterin believes it to be oligarchic to have the immutable right to own a fixed percentage of all the world's money indefinitely, what if that right were extended to the poorest people on earth? What if it were applied equally to every single person on earth? That is the

power of bitcoin. If you are living in one of the poorest countries in the western hemisphere, such as Nicaragua, and choose to exchange your value for bitcoin, you now have an immutable right to own a fixed percentage of all the world's money indefinitely. Only you can decide when, how and to whom to transfer that for value received in the future. The poorest in Nicaragua suddenly are elevated to the exact same leveled playing field as a billionaire in New York like Paul Tudor Jones. Within the bitcoin network, there is no distinction. Equal rights are the default. That cannot and does not exist in the legacy financial system. It is infinitely more oligarchic to indiscriminately devalue someone's monetary savings by increasing the supply of money while at the same time determining to whom that new money should be "rewarded." There can be no comparison between that world and allowing those that earn money honestly by producing value for others to determine how best to allocate it for value returned in the future.

The idea that bitcoin could solve problems today for rich and poor alike stumps quite a few. Most consider bitcoin to be a speculative asset, and many will look at its volatility and believe it unfit for people without a level of savings that one could afford to lose. That view is fortunately flat wrong and economically unsupported. It is easy to look at an economic disaster like Venezuela, where the vast majority of people are struggling to have very basic needs fulfilled, and believe reliable access to food, water, power and healthcare is more important than "buying" bitcoin. However, it is harder to ignore that the economic collapse was caused by a deterioration in the money that previously coordinated economic activity and that the only long-term solution to build it back up is to use a form of money that better fulfills that coordination function. Reliable access to food, water, power and healthcare doesn't exist without the use of money to coordinate resources. In rebuilding an economy on top of a new monetary medium, someone has to go first, and just because it is hard to imagine, it does not change the reality that it's the only way out. One action triggers another. And another and another. Whether it's Venezuela, any other country suffering from rapid economic deterioration, or any poverty-stricken area in the developed world, the need for assistance is immediate, but there is no quick fix. Bitcoin can't remove a socialist dictator, it can't take the kleptocrats out of the kleptocracy, it can't reverse damaging tax policy or social programs, and it can't magically turn poor people into rich people or vice versa. It can, however, solve problems today for anyone that is determined enough to use it, regardless of poverty level or economic status.

There is no reason why a superior form of money would perform one function for some and not for others, regardless of wealth, income levels or any other reason. It is a vicious cycle to break, but the inception point of elevating any individual or society is finding a way to produce more value than is consumed or demanded of others. The best way to accomplish that goal is by using

money to exchange value and coordinate economic activity. Bitcoin isn't just a rich person tool that will become serviceable to poor people once enough rich people have it. That is nonsensical. It is the opposite; it is the best way anyone can level the playing field, regardless of whether the path may be harder for some than others. The demand for money is near universal, and over time, anyone using the form of money with the strongest foundation and the most true price signals will benefit. Whereas the dollar (and other fiat currencies) are one for a few in the short-term and all for none in the long-term, bitcoin is one for all, now and in the future, because it fixes the economic foundation for everyone.

"Whether in Rome, Constantinople, Florence, or Venice, history shows that a sound monetary standard is a necessary prerequisite for human flourishing, without which society stands on the precipice of barbarism and destruction." Saifedean Ammous, the Bitcoin Standard

Views presented are expressly my own and not those of Unchained Capital or my colleagues. Thanks to Phil Geiger, Will Cole and Robert Breedlove for reviewing and for providing valuable feedback.

The Patoshi Mining Machine

By Sergio Demian Lerner

Posted August 22, 2020

One of the topics that has been debated endlessly is what kind of hardware Satoshi used for mining. Some people argue he only needed a single computer using the latest generation of Intel processors available in 2009, using a CPU miner with SSE2-optimizations and multi-threading. Others argue that he had about 50 low-end networked computers. In this article, I will shed some light into this topic with some new discoveries.

But first, a disclaimer: all we know about how Satoshi mined blocks we know from the Patoshi pattern research and the relation between this pattern and Satoshi through some known public transactions between early Bitcoin devs and Satoshi. Because the relation is based on unsigned emails and not math, we'll never be sure. In this article, to sidestep that debate, we'll only talk about Patoshi.

Before we dive into the technical details, the reader has to accept that a single high-end server in 2009 could have mined all Patoshi blocks if running an optimized version of a Bitcoin CPU miner from 2010. We could debate if Patoshi was aware of these optimizations, but from the technical perspective, it's a solved issue. Some optimizations Patoshi could have easily spotted. For example, an optimized SHA256 hasher existed in cryptopp (an open-source and widely known cryptographic library) a year before Bitcoin was created. It would also need some other optimizations that appeared in the Bitcoin code months later of its launch, such as not recomputing the mid-state, and mining in multiple simultaneous threads. But both of them are pretty obvious. Mining multiple 4 nonces simultaneously with SSE2 instructions (also known as 4-way data-level parallelism or SIMD), would be not so easy to code, yet the idea is very old. The latest CPU miners used circa 2012 could scan 8 nonces simultaneously (8-way) with AVX instruction extension. But the AVX opcodes did not exist in 2009, but only SSE2 extensions existed in the latest Intel processors. If you take the Bitcoin source code from late 2010, all the optimizations combined represent a speedup of 10X compared to the public reference miner in Bitcoin v0.1 (approximately 1.5X from starting with mid-state, 4X from multi-threading, and 1.6X from SSE2). In 2010 it's well documented that a single computer from 2009 could mine all blocks at difficulty 1 to keep the network stable, using only 60% of the CPU.

Here I show the performances of a multi-threaded CPU-miner (4 threads), using SSE2 2-way, 4-way, and AVX 8-way instruction sets. All measurements were performed on the same machine (my intel core i5-4460S @ 2.90GHz).

	CPU (not SSE2)	4-WAY SSE2	8-WAY AVX
Avg. time per block [sec]	619	219	118

CPU Mining with multi-threading and different levels of optimizations

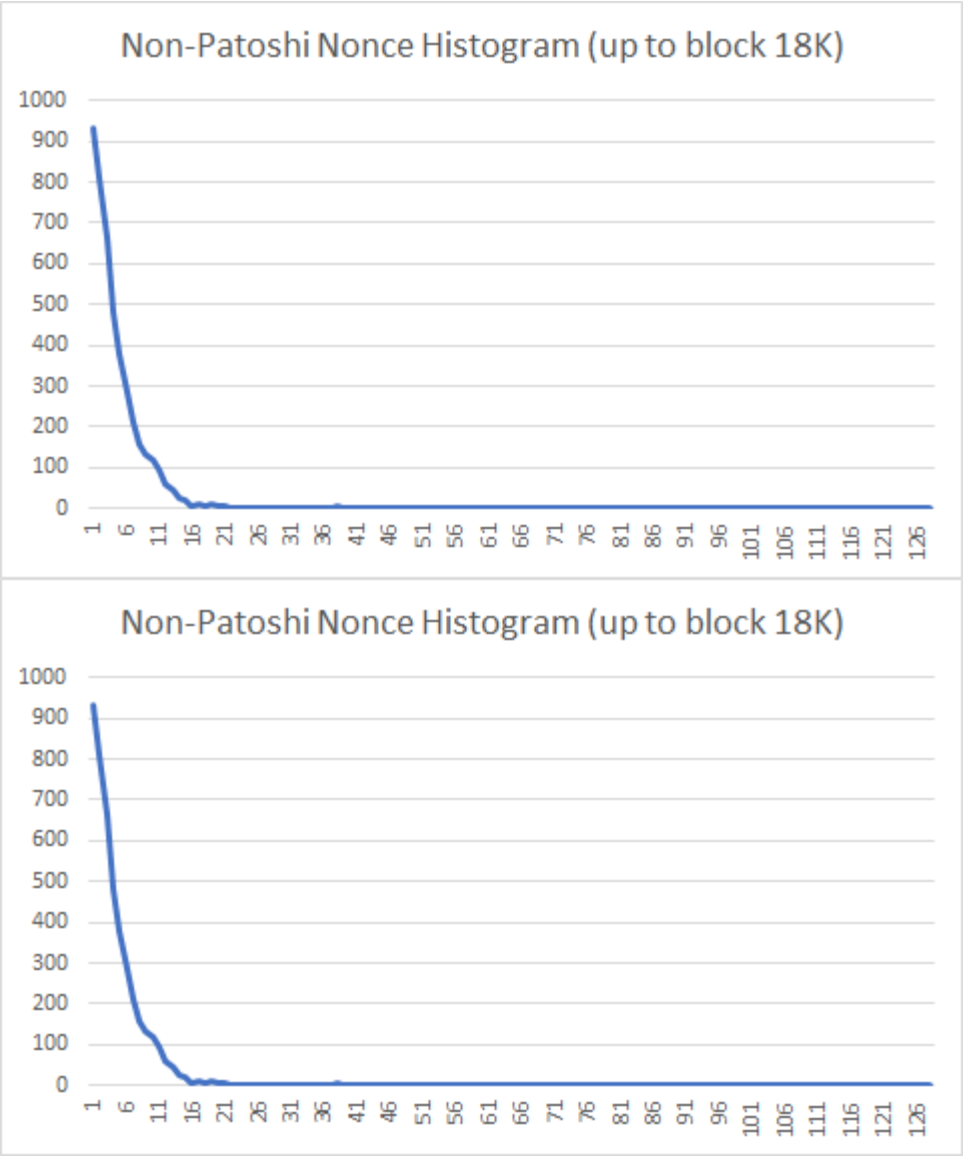
My computer, the Intel core i5-4460S, has a performance that is approximately the same as the Intel Core i7-965 Extreme chip, which was state-of-the-art in 2009. I did my own performance measurements to be sure that the Intel core i7 micro in 2009 could have mined steadily all blocks at difficulty 1. It could even have mined all blocks at difficulty 2.

Strangely, an implementation of SHA512 using SSE2 optimizations was present in the Bitcoin 0.1 codebase itself, but not one for SHA256. The SHA512 does not implement 4-WAY scan because SHA512 is not used for mining.

From Speculation to Evidence

Patoshi's pattern research revealed that Patoshi only scanned a subset of the nonces. We can describe this restriction as a reduction of a single sequential scan interval, the parallelization of 5 sequential intervals, or as the combination of a "selector byte" and a smaller 24-bit sequential scan space (the selector is positioned in the LSB of the nonce). The first two interpretations fit better with the idea of a single computer scanning the nonce space with one or multiple threads. The second interpretation, first proposed by user Eyal0, has given birth to other more sophisticated hypotheses, such as that Patoshi had many networked computers connected in a kind of mining pool. The explanation of the selector byte is also compatible with Patoshi using a rare single parallel computer, such as a TILE64 board, where each processor scans a reduced range. It's also compatible with using a GPU. To summarize, he could have used any of these machines, and speculation without evidence will lead us nowhere. That's why a month ago I decided to explore the blockchain to find a definitive answer.

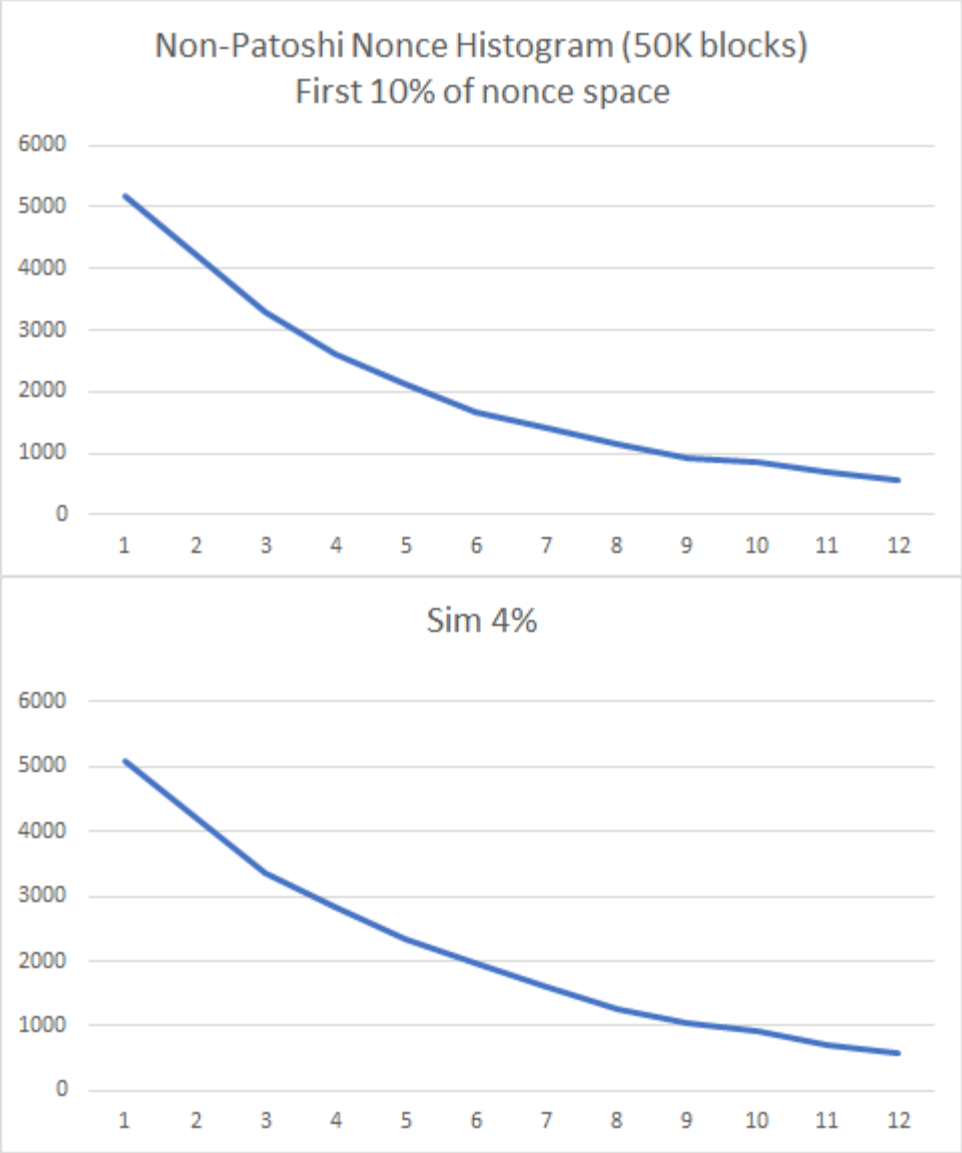
I started by analyzing nonce histograms of the first 18K blocks mined. I chose to analyze only the first 18K blocks because it's known that Patoshi used a fixed nonce distribution on those blocks. Afterward, Patoshi starts reducing his hashrate by removing parts of the nonce range scanned, and that would ruin the histograms. The following histograms show the nonce distribution of the 2^32 possible nonce values over 128 buckets for all non-Patoshi blocks in the first 18K blocks, and in the first 50K blocks.



You can see that the probability decays exponentially. The mining difficulty during this period was 1, which means that the whole network finds a block solution after testing 2^32 nonces on average. Why is it that most non-Patoshi miners, which mine much slower than Patoshi, find blocks so "quickly" that it seems that they are scanning 10% of the space? The explanation is simple: all individual miners, on average, find solutions after the same number of nonce tries. However, the histogram of non-Patoshi block nonces combines the output of several individual miners, and therefore the probability that any of them finds a block before reaching the average number of nonces is much greater than each one individually. Keep in mind that the nonce is reset for every new block. As an example, the average number of times you need to throw a dice to obtain the number one is 6, and if after getting a one you restart (a following "round"), then the average number of tries is still 6. But if you throw 3 dices simultaneously, then on

average you will be throwing each dice only 2.37 times per round until you find the number “one”.

The following two histograms show the real nonce distribution over in the first 10% of the nonce space, and the distribution obtained by a discrete-event simulation where each individual mining machine has only 4% of the network hashrate.

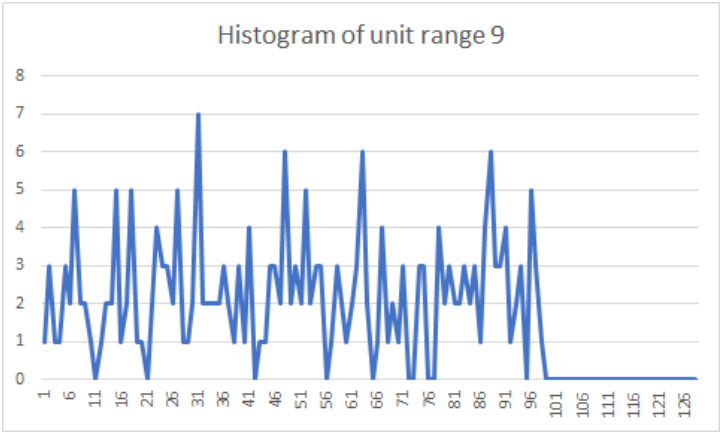


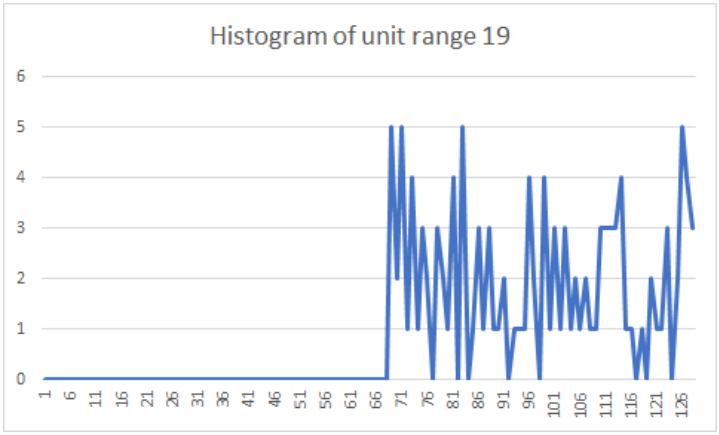
You can see that both distributions look alike. Can we do the same with Patoshi blocks? We know that Patoshi used one byte of the nonce in a strange way, either mining over a restricted range or mining in parallel over many ranges. Therefore we could ask how the nonce should be distributed if Patoshi scanned the space sequentially or used a selector byte and scanned

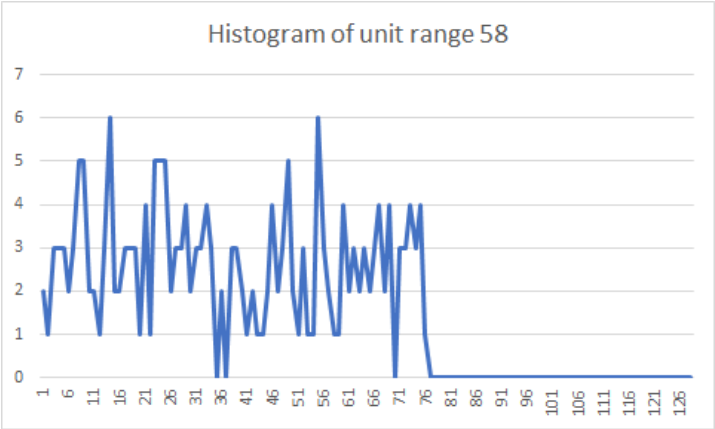
the remaining 24 bits, as an unsigned integer. Will any of these histograms show a clear decay in probability?

The Mysterious 19

In a recent article, user TechMix discusses the strange behavior of the value 19 in the Patoshi nonce range. Today we'll reveal this mystery. TechMix, along with user OrganOfCorti identified several subranges in the Patoshi range. These subranges are mined with the same hashrate. The subranges are: *[0..9],[19..28],[29..38],[39..48],_and _[49..58]*. Between 9 and 19 there is a nonce gap. We'll call each individual range of size 2^24 associated with a certain LSB byte a **unit range**, and therefore each subrange contains 10 unit ranges. The Patoshi subrange boundaries with the nonces outside the Patoshi range (9, 19 and 58) look diffuse in the histogram: the probability of mining on these unit ranges is lower than the rest of the subrange. TechMix was perplexed about the reason. Finding the answer requires abandoning the idea that the pattern comprises a selector byte and a unit range. Here I present the histograms of the nonce unit ranges 9, 19, and 58:





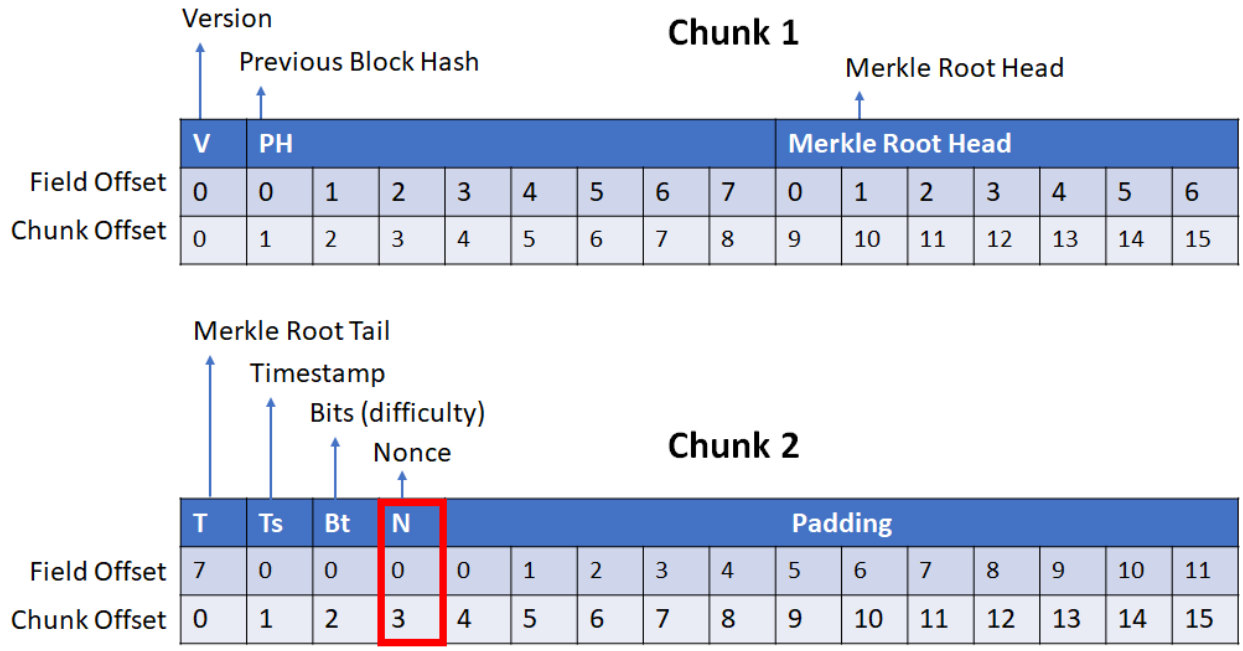


We see clearly that the reduction in probability is just that Patoshi didn't establish his ranges in terms of unit ranges. The exact positions of the subrange bounds are 163840000, 327680000, and 983040000. The size of the last contiguous range is 655360000. Of course, these are beautiful round numbers obtained by the formula N * 0x4000 * 10^4. To simplify our explanations, we can define a **punit** to be 0x4000 * 10^4. The punit range is slightly larger than the unit range. Each Patoshi subranges is composed of 10 punit ranges. For simplicity, we'll still name the subranges [0..9], [19..28] and so on, even if that naming convention is inexact.

Scanning by incrementing the Inner or Outer Nonces

To fully understand how Bitcoin mining evolved we need to dig deeper into how SHA256 works and how Bitcoin v0.1, the first public release, was coded. The Satoshi client v0.1 was compiled first for Windows machines, and almost surely for an Intel x86 chip. The x86 architecture is little-endian. SHA256 is defined without a reference to a specific endianness, but making use of uint32 types. SHA256 can be implemented in C language without messing with machine endianness: constants are expressed as uint32 numbers, additions and even bit-shifting operations can be performed on full uint32 types, without ever casting a uint32 pointer to an unsigned char pointer. However, the input of SHA256, the Bitcoin header, is not a list of uint32 values, but an array of bytes. Therefore the SHA256 standard must specify how a list of bytes is converted into a list of uint32s, and how the last internal state of SHA256, which is a list of uint32 values, is converted back to a list of bytes. The SHA256 standard states that the input bytes are considered as if they were read unaltered by a big-endian machine, so the first byte of the Bitcoin header will be the highest significant byte of the first uint32. In a little-endian machine, the first byte is not the MSB of an uint32, so the first 4 bytes must be reversed prior to being processed by SHA256. The same happens for all groups of 4 bytes (20 uint32 in total). Because all fields in the Bitcoin header have sizes that are multiple of 4, one of these groups maps directly to the

nonce field. The following diagram shows how the different fields are mapped into uint32s.



The bitcoin header comprises two 64-byte chunks, split into 16 uint32s. The diagrams names these uint32s from 0 to 15. The Bitcoin client v0.1 incremented the nonce field as little-endian prior hashing, which means that just before hashing, the nonce (and all remaining uint32s) were reversed in memory. The following code in the Bitcoin client shows how it was performed:

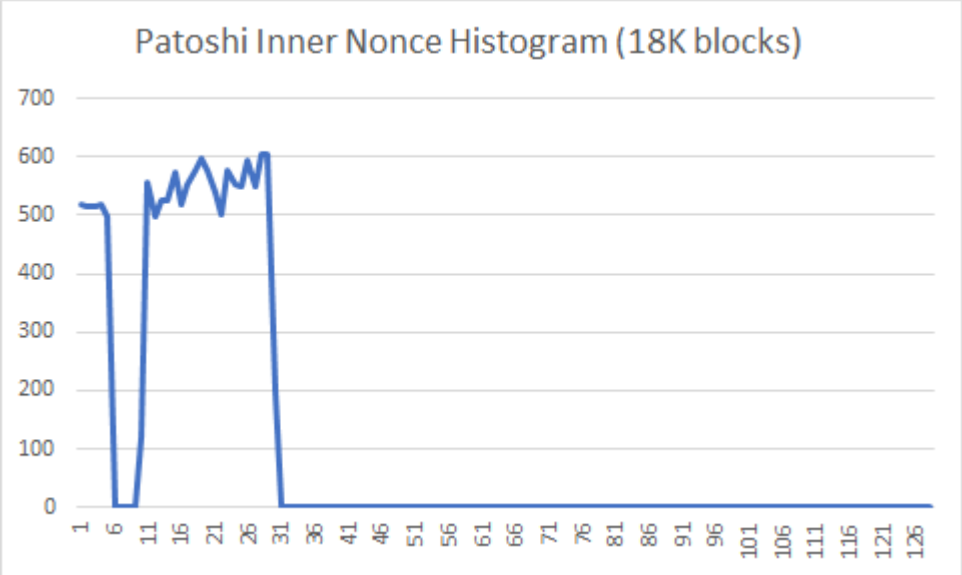
```
void BlockSHA256(const void* pin, unsigned int nBlocks, void* pout)
{
    unsigned int* pinput = (unsigned int*)pin;
    unsigned int* pstate = (unsigned int*)pout;

    CryptoPP::SHA256::InitState(pstate);

    if (*(char*)&detectlittleendian != 0)
    {
        for (int n = 0; n < nBlocks; n++)
        {
            unsigned int pbuf[16];
            for (int i = 0; i < 16; i++)
                pbuf[i] = ByteReverse(pinput[n * 16 + i]);
            CryptoPP::SHA256::Transform(pstate, pbuf);
        }
        for (int i = 0; i < 8; i++)
            pstate[i] = ByteReverse(pstate[i]);
```

Code that reverses each uint32 of the Bitcoin block header

Since mining consists mostly of incrementing the nonce and hashing twice repeatedly, it's clear that the continuous reversal of the nonce and the rest of the fields in the header is unnecessary, because almost all fields except the nonce do not change often. Regarding the nonce, Bitcoin is indifferent to the internal format of the nonce: you can increment it or decrement it, or even rotate it over all possible values using an 32-bit gray code. Therefore the miner can increment the nonce in little-endian or big-endian format and still cover the whole nonce space after 2^32 steps.

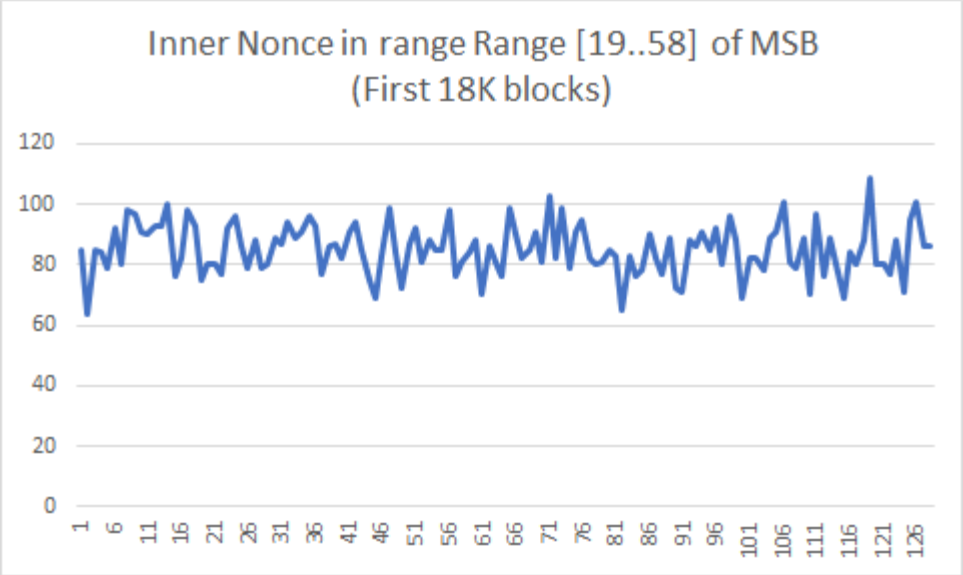
We'll say that the miner is mining with an **outer positive** (**OP**) algorithm, if it increments the nonce before reversal. We say the miner algorithm is **inner negative** (**IN**), if it decrements the nonce after reversal of the header fields. The other options are also possible (**outer negative** (**ON**) and **inner positive** (**IP**)). The first version of Bitcoin was outer positive, in version 0.3.22 (2010) the node adopted an inner positive algorithm to optimize mining.

Since Patoshi was mining with a special software different from the public version, we can hypothesize that he scanned the inner nonce. Under this assumption, we obtain the following histogram. The nonce is reversed and the outer nonce LSB now becomes the MSB of a 32 bit unsigned integer. Because we've analyzed the outer nonce LSB before, we already know how the inner nonce histogram would look like:

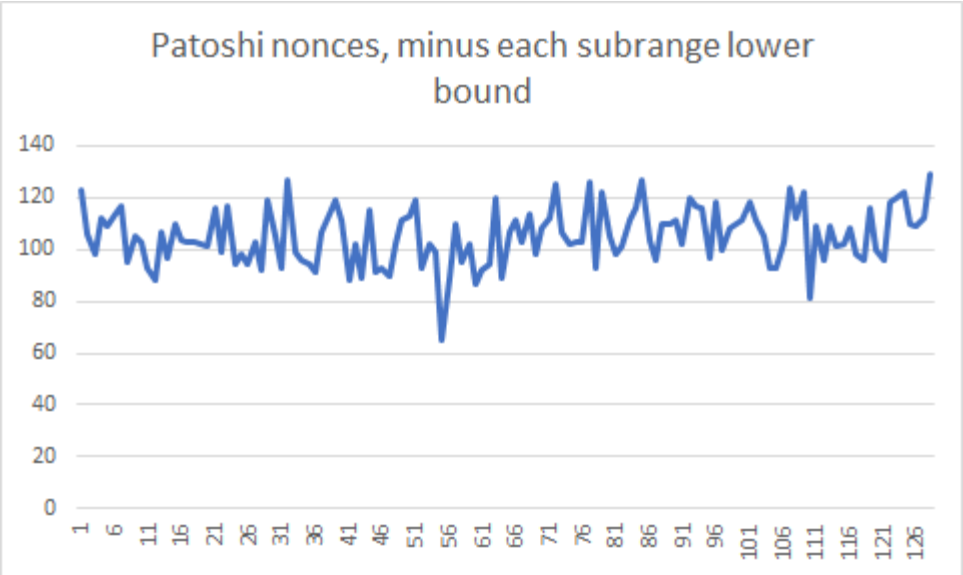


The histogram shows a slightly increased probability for higher nonces within the Patoshi range. There are two main continuous ranges, [0..9] and [19..58], but we'll assume that the second continuous range contains 4 subranges, as defined before. We'll assume that each of the five resulting subranges was scanned in parallel by Patoshi. To test this hypothesis, we show here the

nonce histogram of the range [19..58] expanded. Each bucket is only about 2^22 nonces:



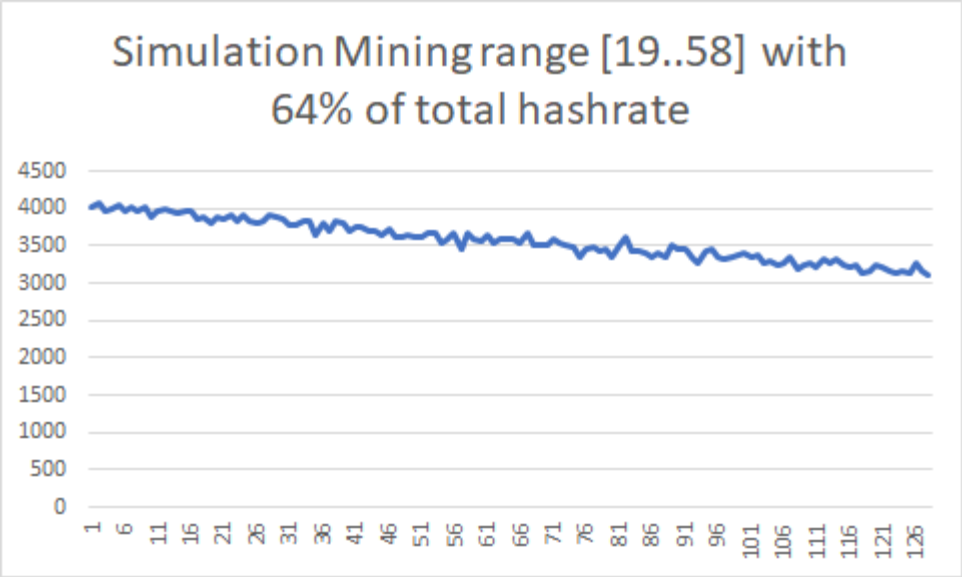
The Patoshi inner nonce histogram looked like there was a higher probability for higher nonces, but in this histogram of the range [19..58] I can't see a clear bias. This is compatible with our hypothesis of a parallel search. To test the hypothesis we can produce an histogram where we subtract to each nonce the lower bound of the subrange it belongs. This is the result:

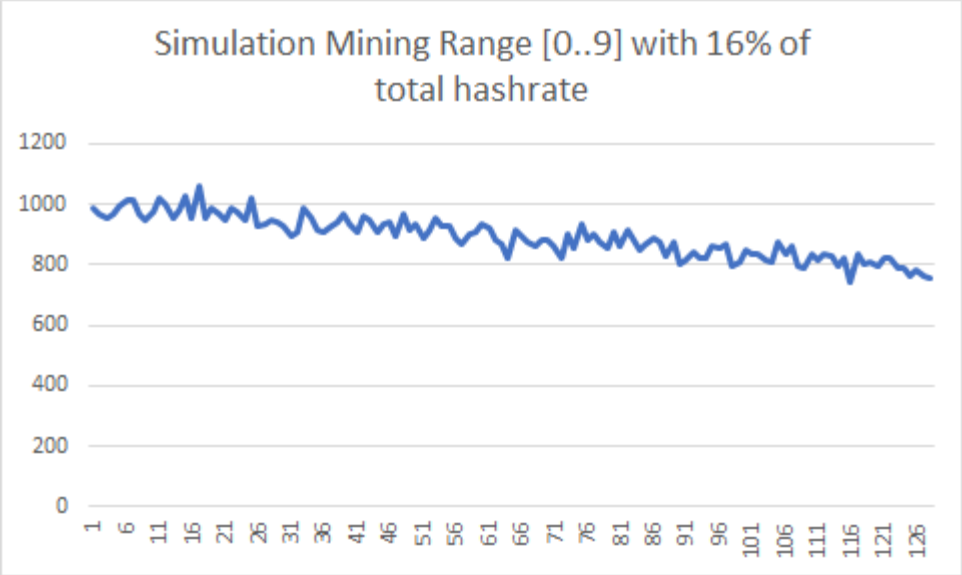


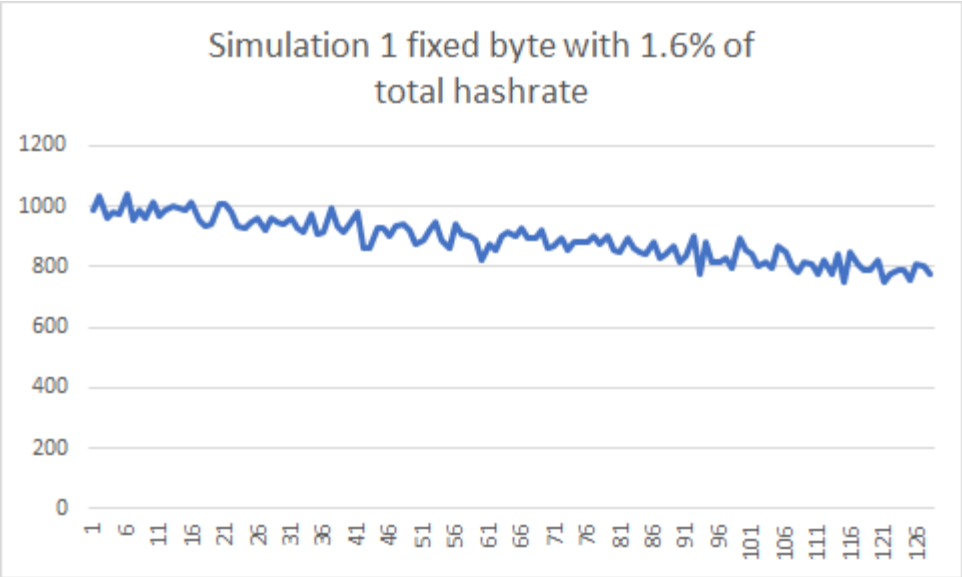
I can't see a clear tendency towards higher or lower probability for higher nonces. I needed to be sure what I should expect from this histogram, and therefore I decided to simulate Patoshi mining.

Simulating Mining

I simulated mining a large part of Patoshi nonce space scanning sequentially in the range [19..58] (assuming 64% of hashrate), a subrange [0..9] (assuming 16% of the hashrate), and finally a single unit or punit range (assuming 1.6% of the hashrate). In all cases the miner increments the inner nonce. These are the results of the simulations:







We can see in the first histogram that the last nonce has 25% less chance of being selected than the first nonce. In the second histogram the chances are reduced about 20%. For the unit range histogram, I increased the number of simulation events to get a more precise histogram. Again, the chance decayed 20% in the highest nonces. It seems that Patoshi was not resetting the nonce on new blocks. A new mystery? I needed a new method to analyze the histogram that was independent of the nonce starting point.

Re-Mining Comes to the Rescue

In 2014 I played with the concept of re-mining: searching for other solutions in the same space early miners found one. What can we learn from re-mining? Let's imagine we find two solutions for the same block header. Let's momentaneously assume that the miner does not update the block header timestamp nor the transactions contained in it until the blockchain grows by one more block and a new fresh header is created. We also assume that once the nonce hits zero or the maximum value, it wraps-around. When wrap-around happens, the extranonce is incremented and a new block header is built, producing a new nonce search space. The solution chosen by the miner, the one that exists in the blockchain, will be called the **real solution**. Let's assume that the real solution is always the one with lower nonce compared to any other solutions found by re-mining. Then that would be strong evidence that the miner scanned the nonce space by incrementing the nonce and that the nonce was reset to zero at every new block. If the nonce found was always the highest one, then that would indicate that the nonce space was scanned by decrementing the nonce. Under the assumption that the header is not periodically updated and that

we can find enough blocks with more than one solution to achieve statistical significance, it would be easy to detect the nonce scanning direction.

But the stated assumptions do not hold for the whole time required to scan the nonce space, but only for a short time, a short nonce range. This is because miners periodically increment the nTime field, which leads to the creation of a new block header. In the Bitcoin reference client version 0.1, the nTime field is updated every 0x40000 increments, as shown by the following code extract:

```
// Update nTime every few seconds
if ((++tmp.block.nNonce & 0x3ffff) == 0)
{
    CheckForShutdown(3);
    if (tmp.block.nNonce == 0)
        break;
    if (pindexPrev != pindexBest)
        break;
    if (nTransactionsUpdated != nTransactionsUpdatedLast &&
        GetTime() - nStart > 60)
        break;
    if (!fGenerateBitcoins)
        break;
    tmp.block.nTime = pblock->nTime = max(pindexPrev->GetMedianTimePast()+1,
                                          GetAdjustedTime());
}
```

Code that periodically updates the nTime field

Each nonce interval where the block header is unchanged will be called a “nTime slot”. When sampling many blocks with multiple solutions, and looking at a nonce histogram, the percentage of lower nonces picked by the miner vs higher nonces found in multi-solutions can give us information about the size of the nTime slot size. When two solutions lie on different subranges, the percentage can also give us information regarding the parallel sequential relation of the two subranges: a percentage too high or too low would indicate a sequential relation, while a percentage close to 50% indicates a parallel search.

Let’s say we collect a large sample of blocks (i.e. >1000) with multiple solutions, and then we count, for each consecutive pair of multi solutions, how many cases the one with lower nonce is the real solution. We then divide this number by the total number of multi-solution pairs to get a percentage. Let’s call this percentage L. We define H as (100-L). If L is close to 50%, then that indicates the nonce is neither being clearly incremented nor decremented on a single sequence. It may indicate that the nonce was scanned using a non-standard method, such as a pseudo-random order, or a parallel search from different starting points. If L has a noticeable bias towards 0% or towards 100%, then we have credible evidence of a certain type of mining direction. The closer is L to 0% or 100%, the larger the nTime

slot is. Note that if the nonce is never reset between blocks, so it restarts where it stopped, then L still provides the same information. This new method is invariant to the starting point!

We can make two assumptions regarding wrap-around-zero when scanning the Patoshi nonce range. If there is no wrap-around-zero, and a new header is created when the nonce reaches the subrange boundaries, then the block headers having a low nonce real solution have much higher probability to have an additional solution with higher nonce, while blocks having high nonce real solutions have much higher probability of having additional solutions with lower nonces. However, if the distribution of real nonces over the subrange is uniform, then these two cases would cancel each other and L would be unaltered by the boundary phenomenon. If L is biased towards 0% or 100%, then the boundary phenomenon will amplify the bias, because the bias close to the boundaries will not cancel out. Therefore L is a strong indicator of a sequential mining direction when there is one. If we assume Patoshi started mining at a random initial nonce, and only updated the header when he circularily reaches the starting point again after wrap-around a boundary,, then there is no bias amplification but still L is a good indicator of a sequential mining direction. If you're are anxious to know the experiment result, just stay one more paragraph with me.

Some Useful Definitions

We introduce some more definitions to be able to present the results. As previously stated, the **real solution** of a specific block header is defined as the nonce that exists in the Bitcoin blockchain for that block header. Any other nonce that makes the same block header pass the difficulty test will be defined as an **additional solution**. Now suppose that we identify all non-Patoshi blocks that have more than one solution for the same block header (at least two distinct nonces that result in hashes below the difficulty target). We define this event as a **multi-solution**. Because in Bitcoin v0.1 the slot size is small compared to the nonce space, it's highly probable that the solutions of a random multi-solution do not lie in the same nTime slot. If solutions lie on different slots, then there is no information we can extract from a multi-solution. For non-Patoshi blocks once every 16384 times (2^32/0x40000) an additional solution lies in the same slot of the real solution, and nTime will not be incremented in-between. Because a miner will on average scan half of a slot of the same block header, we can assure that, on average, a fraction of 1/(2*16384) of the nonce space of every block header does not contain an additional solution. Because in 2009 the block difficulty was 1, and because the number of solutions to be found is directly proportional to the number nonces tested, if we remine blocks scanning the full nonce space, we can expect to find an **additional solution** of any block with probability 32767/32768.

If we re-mine N blocks, we should find N * 32767/32768 additional solutions. For non-Patoshi blocks, it means that almost all blocks contain a second solution. Of course, some blocks will contain more than two, and some just one.

Here is the result of re-mining the first 18K blocks, and plotting the non-Patoshi multi-solutions found:

- Total non-Patoshi block: 1405
- Additional Solutions: 1176
- Multi-solutions: 793
- Lower nonce is real solution: **749** (H=**94%**)
- Higher nonce is real solution: 44 (L=5%)

These results confirm what the nonce histogram taught as: all non-Patoshi blocks are mined with an outer positive algorithm, such as the one existent in the Bitcoin public code. But what happens when we re-ming Patoshi blocks?

Surprise!

A month ago I started re-mining with a standard CPU. I don't have access to a GPU nor an ASIC right now. I re-mined all non-Patoshi blocks in the first 18K block only to check that the theory matched the reality (It does). But things became not so clear when I re-mined Patoshi blocks. These are the results I got when re-mining all Patoshi blocks in the first 13.2K blocks of the Bitcoin blockchain. I'm searching the whole Patoshi range [0..9] plus [19..58] to scan for additional solutions.

- Total Patoshi blocks : 10025
- Additional solutions: 1075

Results for inner nonce

- Lower nonce is real solution: 222 (L=21%)
- Higher nonce is real solution: **789** (H=**78%**)

Results for outer nonce

- Lower nonce is real solution: 526 (L=51%)
- Higher nonce is real solution: 499 (H=48%)

If nonces were mined uniformly on the Patoshi range, and Patoshi was scanning the inner nonce, we get L=21%, so there seems to be a clear bias towards picking the highest nonce. This implies Patoshi was using an IN (Inner negative) scanning algorithm. I don't have a sufficiently convincing

explanation which Patoshi was decrementing the nonce instead of incrementing it.

If Pasohi was in fact decrementing the nonce, then the bias towards high real solution would increase if I reduce the range that I'm searching around the real solution. In fact, our initial assumption was that Patoshi scanned the subranges in parallel. Here are the results obtained for the different subranges:

	[0..9]	[19..28]	[29..38] [39..48]	[49..58]	
H	97%	97%	94%	97%	95%

Number of cases the highest nonce is chosen by Patoshi within a subrange

Whenever I test a range which lies in the middle of the subrange boundaries (i.e. [25..34]), H moves towards 50%. It never reaches 50% because when two solutions lie in the same subrange, they are still dependent and show the preference for the highest nonce being the real one.

I also tested the cross-interval solution dependence between the range [0..9] and the range [19..28]. There are not so many multi-solution cases which have one solution in the upper range and another in the lower range (only 75). The result was L=38%, which indicates there could be certain dependence, but it's not sufficient due to the small sample size.

Because the bias towards picking the highest nonce is significant, we can conclude there is a high dependency in multi-solutions. This suggest two things:

- Patoshi updated the nTime field infrequently during mining (as infrequent as once a minute).
- Patoshi scanned each subrange in parallel, but within each subrange, he scanned each subrange sequentially.

The theory that Satoshi had 50 networked seems to contradict the results.

While it's possible to use the multi-solution distribution to estimate Patoshi nTime slot size or even try to guess the number of sequential ranges scanned, I leave that research for a future article.

Since reversing the header fields in software takes very little time compared to double hashing the header, I suspect Patoshi had optimized the miner a lot more than previously thought. You would only perform the nonce increment close to the SHA256 assembly code if it provides a meaningful advantage. Another reason may be that the scanning was performed on special programmable hardware, such as an FPGA, so wasting gates to

reverse the nonce is pointless, and those gates can be used to add more hashers. However, the hashers must have been mining consecutive block nonces ("pipelining" like CPU-miners do with SSE2) and not scanning multiple intervals in parallel. This theory is plausible since SHA256 implementations for FPGAs have been available since 2005. In my opinion, it's plausible that Patoshi had already performed other more evident optimizations, such as removing the hashing of the first chunk (which stays constant) and start mining from the SHA256 mid-state, and parallelizing the hashing with multiple-threads or SSE2 pipelining.

Flawed Estimations

I missed the opportunity to test re-mining in 2014. My conclusion in 2014 was that I could learn very little from re-mining because the nTime would be changing too fast to expect more than one solution belonging to the same nTime slot. But it turned out I was wrong, for two reasons. First, I knew that Patoshi mined with a different software than the reference code but I was still assuming his code would be using an nTime slot of size of 0x40000. He was clearly not. Second, I didn't take into account that even if the nTime were to be updated in sub-second intervals, the resolution of the nTime is just 1 second, so sometimes the updated value would be the same value that existed before.

Summary

In this article I solved the mystery of the Patoshi range boundaries, showing that the boundaries are not aligned with powers of 2, but with multiples of 0x4000 * 10^4. I presented several histograms that do not show a clear exponentially decaying (or exponentially increasing) probability of nonces in Patoshi blocks. I simulated different standard nonce scanning algorithms and realized that all of them produce certain imbalance in the nonce histograms, yet the real Patoshi nonces do not present a clear imbalance. The reason for this mismatch could be that Patoshi's mining machine did not reset the nonce between blocks, spreading the solutions more uniformly over his mining range, but I couldn't find evidence of this property. Finally I executed a new experiment: I re-mined Patoshi blocks in order to find additional solutions. I had proposed this experiment in 2014, but I wrongly disregarded it as ineffective. However, it turned out that re-mining reveals a strong tendency of the Patoshi mining algorithm to choose higher nonces when scanning the inner nonce. This tendency suggests the nonce was being decremented, which is the opposite that the Satoshi client version 0.1 does. Since the nonce imbalance decreases when analyzing two subranges together, this suggests Patoshi was scanning the 5 subranges in parallel, but each subrange internally sequentially. This contradicts a theory that Patoshi deployed the first mining farm of 50 independent computers (or any other

highly decoupled system) and supports the theory that Patoshi was simply multi-threading in a high-end CPU.

Special thanks to Raul Laprida for helping me with the article.

Edit: Kim Nilsson found the real Patoshi boundary before me. He sent me an email in January stating that “Patoshi’s nonce is a big-endian number partitioned into ranges of 163840000 values, where only certain partitions are searched while mining.”. Sadly I didn’t pay enough attention that 163840000 was not exactly 2^24*10, nor I understood what he meant by big-endian, and so I had to spent time coding and researching myself ☹. I wish I had understood.
Thanks Kim Nilsson for letting me know and I apologize for not citing your work before!

Tweet Thread: PUELL'S 21 LAWS OF BITCOIN

By David Puell

Posted September 9, 2020

1. Any sufficiently asymptotic money supply targeting is indistiguishable from the Moon.
2. When central banks become the market makers, sound data becomes the currency standard.
3. Despite appearances, Bitcoin is more crucial than risky, more localist than global, and more fun than complex.
4. Gridlock is good (gridlock is good (gridlock is good)).
5. MoE = log(SoV).
6. For Bitcoin, the more power you have, the greater the rate at which your enemies will own it.
7. It is easier to destroy your position than to create it—or, it is easier to liquidate or lose your sats than to buy or mine them.
8. "Bitcoin for all, but, unavoidably, more for few," just as, "Bitcoin for few, but, honestly, more for me."
9. Short exuberance (in spirit) and long asymmetry (in actuality).
10. The Bitcoin Caveat: Whether security, liquidity, or development, the network's growth will always be dictated by the aspect most in demand and least in supply at any given time.
11. The most ineffective network actors are systematically moved to the place where they can do the least damage: non-ownership.
12. A skeptic's call for a top shall be 10x'ed within four years.
13. You are the Beauty; Bitcoin the Beast.
14. Bitcoin should be the solution to your panic in the long term, not the cause of it in the short term.
15. Rochard's Dictum: At a ratio of 1:1, proof-of-work and skin in the game.
16. Unlike amnesia, in Bitcoin, the oldest memories are the most affected.
17. There Ain't No Index (TANI).
18. The more sober you are, the more important HODLing becomes.
19. Timechain will tell...
20. The earliest adopter will always out-own the largest insitution.
21. Follower count is directly proportional to price.

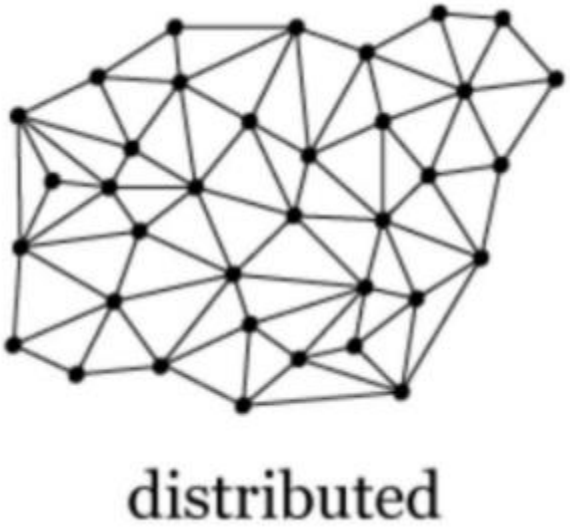
Map of the Bitcoin Network

By Gloria Zhao

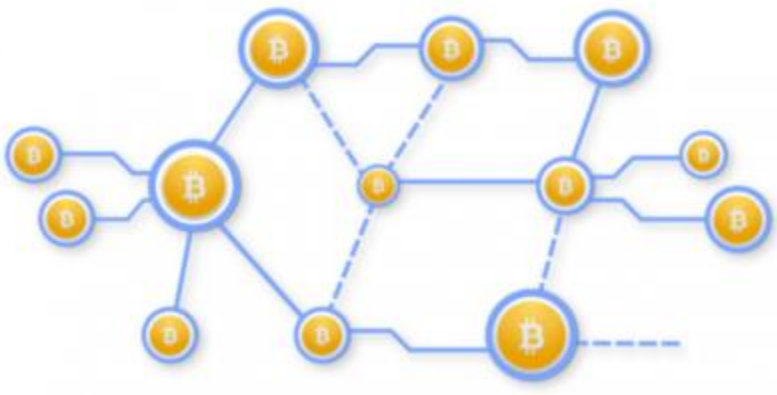
Posted July 22, 2020

A beginner-friendly “map” to help you navigate through the wide variety of nodes, software, and participants in the Bitcoin Network.

The Bitcoin network is often described as peer-to-peer (P2P), distributed, or decentralized. It’s often drawn as a homogeneous graph:



Or something similarly structured that suggests variation in the types of vertices and edges:



But what is a node, and what does it do? Is it a server or can it be a client… or both? Given the myriad of Bitcoin software, what “counts” as a node? How do all the participants in Bitcoin — users, miners, nodes, wallets — interact with one another?

This article draws a map of the Bitcoin network that clarifies these definitions and encapsulates some of the complexity. We'll start by classifying the different types of nodes based on their server/client functionality and describing the P2P connections formed between them. Instead of providing statistics on the entire network, this article is primarily interested in enumerating the diverse set of possibilities in the network.

The Short Answer

Primarily, the vertices are nodes in the P2P network and the edges are their P2P connections. There are many different types of nodes that can be categorized based on their ability to serve other peers and clients; nodes can act as a server, client, or both at any given point in time.

Node = a participant on the P2P Network that implements the Bitcoin P2P protocol. A node isn't required to run any specific software as long as it follows this protocol.

P2P Connection = a network connection directly established between two nodes communicating using the Bitcoin P2P protocol. We often use "peer" to refer to other nodes with which a node has a P2P connection.

Types of Nodes:

In the broadest sense, nodes fall into one of four categories based on how much state they maintain and what services they can provide.

Full Node (Fully Validating Node) = a node that is capable of validating transactions and blocks. Instead of searching through the blocks database every time, full nodes keep some state, i.e. a UTXO (unspent transaction output or "coins") set.

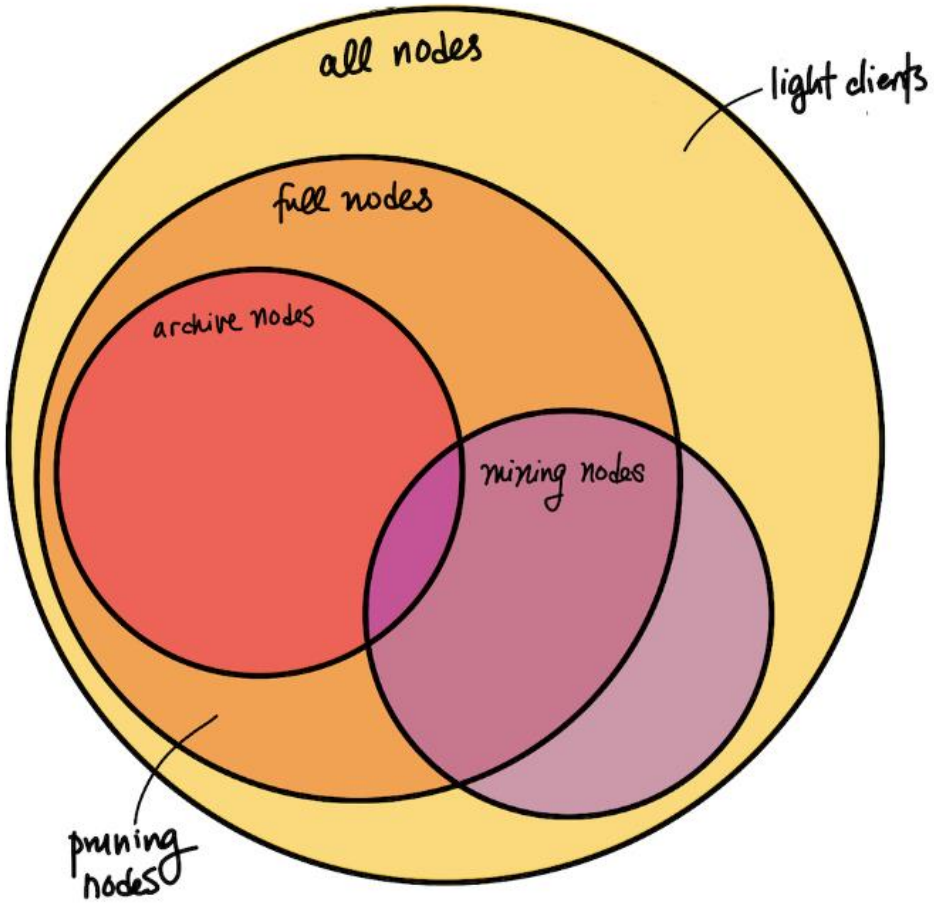
Thus, Bitcoin nodes don't necessarily need a complete copy of the blockchain in order to validate, as long as they maintain some block metadata and an up-to-date UTXO set. **Pruning Nodes** implement this exact behavior: they download and process blocks to build the necessary databases for validation, then discard the old blocks to save disk space. Since they have all of the information and can validate all new blocks and transactions, they are full nodes.

Archive Node = a node that has a copy of the entire history of the blockchain. These nodes are capable of validating incoming transactions and blocks, as well as querying block and transaction data from any point in history, including those that are no longer relevant to validation (hence the naming "archive"). It's crucial that archive nodes exist, as new nodes need to catch up on the entire history in order to become full nodes. They can only do so by downloading the history, one block at a time, from archive nodes.

Mining Node = a node that produces new blocks. This involves keeping a mempool of unconfirmed transactions, validating new transactions, and solving the Proof-of-Work hash puzzle (i.e. finding the nonce) to construct a block. Mining nodes often use extra hardware to assist them in solving the hash puzzle (e.g. ASICs) or participate in mining pools. Technically, there are also non-full nodes that join a mining pool, connect to a full node that manages the pool, and help solve PoW on a block without doing any validation (so there are mining but non-full nodes).

Light Clients = generic term for a node that doesn't keep the full state necessary for full validation and instead trusts other full nodes to do so. A light client may keep a limited amount of data in order to verify its own transactions, but not fully validate all blocks. Within Bitcoin Core, "light client" is often used synonymously with **Simplified Payment Verification (SPV) Nodes,** and not to be confused with **Pruning Nodes.** In some contexts, these aren't called "nodes" because they don't do most of the things [full] nodes usually do.

Here is an illustration of how these categories overlap:



Other Concepts for Nodes:

Nodes may also have additional characteristics that impact their participation on the network, but are not mutually exclusive with each other or any of the above four categories. Due to the decentralized nature and focus on accessibility in the Bitcoin ecosystem, **as long as a node implements the P2P protocol and obeys consensus rules**, implementation details and the decision to adopt features are within the node operator's discretion.

Initial Block Download (IBD): a temporary state in which the node is not yet caught up to the current block height and is in the process of downloading the blockchain. A full node signaling that it keeps a full copy of the blockchain history may still be in IBD and thus be limited in the services it can provide (i.e. won't be able to tell you about transactions that they haven't seen yet). The getblockchaininfo RPC returns whether a node is in IBD.

Blocks Only Mode: a non-temporary mode in which the full node only validates blocks and the transactions in them. It does not validate any unconfirmed transactions (apart from its own), doesn't keep a mempool, and asks its peers not to relay transactions to it.

Bitcoin Core: running the open-source software originally authored by Satoshi Nakamoto and currently maintained by various contributors, found at bitcoincore.org or from source. We know that Bitcoin Core isn't the only software that exists in the Bitcoin P2P Network; some nodes run custom patches that implement specific behaviors, and some might use older versions of Bitcoin Core that don't understand newly introduced protocol messages. It's important to be cognizant of what new features require full network cooperation, not expect nodes to behave correctly or honestly, and account for node operators being hesitant or slow to upgrade their software.

Malicious: any type of behavior that intentionally harms the network (not including bugs, networking complications or other unintentional behavior). Bitcoin assumes a highly adversarial environment including the possibility of Denial of Service attacks, sybil/eclipse-attacks intended to double-spend, spy nodes trying to deanonymize addresses, etc.

Node as a Server

We've seen that each singular node is *dependent* on its peers to send the information it needs. Also, nodes typically *serve* a number of users and client software through non-P2P interfaces such as RPC, HTTP/REST, and a GUI.

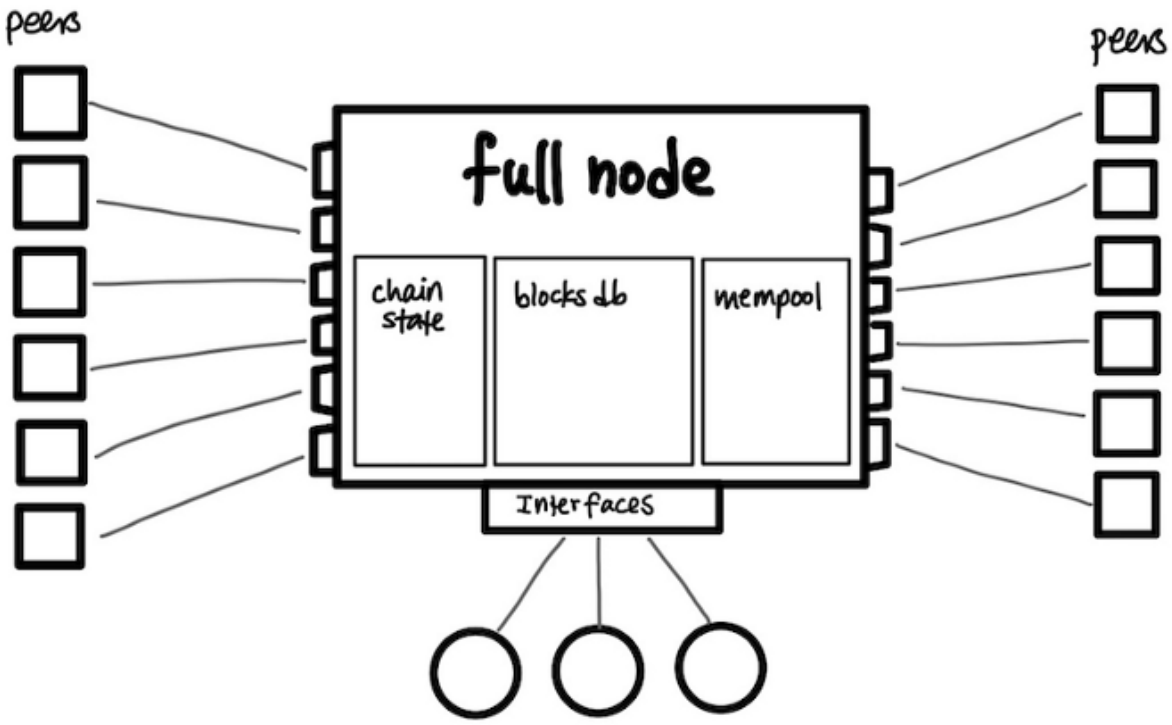
Some examples of non-node clients that may use a node as a server:

- **Users** running a node to send and receive bitcoins.

- **Wallets** which manage keys, create transactions, and maybe keep some UTXO state associated with those keys but don't have a copy of the blockchain and instead rely on a node to get up-to-date information.
- **User-Facing Software Services and Applications** such as block explorers, exchanges, and merchants that query full nodes for information and display them on a webpage or application.
- **Developers** creating nodes in regtest mode to test functionality or the interfaces themselves.
- **Developer-Facing Software** such as SDKs, APIs, and other interfaces. For example, the Bitcoin Core CLI (bitcoin-cli) uses the RPC interface to implement a command-line interface.

While these connections are not seen by a node's peers on the P2P Network, they make up a significant portion of Bitcoin functionality. Bitcoin Core developers heavily consider these participants when developing new features or deciding what features to support.

Now that we understand the node as both a server and a client, here's what an individual node looks like at a high level:



Simplified view of a node

Types of P2P connections:

P2P connections in Bitcoin all "speak the same language" in that they all use the P2P protocol to communicate, but are diverse in their conversation contents. The Bitcoin Core implementation attempts to balance stability (which prefers static connections) and accessibility (which encourages accepting connections from new nodes) through facilitating peer discovery and managing connections carefully. Bitcoin Core distinguishes between three main types of connections based on how they are initiated, which often informs the nature of the peer-to-peer relationship.

Outbound = automatic connection that your node initiated through peer discovery. Node discovery involves getting a list of IP addresses of established nodes to start out with, then a continuous and dynamic process of advertising your own address and attempting to connect to addresses you hear about. Depending on what your node needs (e.g. in IBD), it may prioritize connections that are able to provide specific services (e.g. serving past blocks and transactions).

Inbound = automatic connection that your peer initiated (to your peer, this connection is outbound). For security, inbound traffic is disabled by default and you need to configure some network and firewall settings to enable it.

Manual = connection that was made manually (e.g. through CLI or RPC) instead of automatically. You might create a manual connection because there's a particular node operated by someone you trust or you're testing the software and need to have control over the connections.

Other Concepts for P2P Connections:

Diversity in Outbound Connections

Outbound connections can be broken down into further categories based on the information received and duration of the connection.

Full-Relay outbound connections expect to communicate everything, including blocks, transactions, and addrs (used to find peers, similar to IP addresses, and not to be confused with wallet addresses used in transactions). **Block-Only-Relay** outbound connections only expect to receive blocks. Not to be confused with blocks-only mode; it is entirely normal for full nodes to establish Block-Only-Relay connections to 1–2 peers and Full-Relay connections to everyone else.

One-Shot and Feelers are temporary outbound connections used in node discovery. One-Shot connections are used to solicit a list of addrs that can be used to find new peers. Feelers are used to verify whether an addr corresponds to a real node.

Individual Differences

As we have seen, each node may provide different services and be looking for specific information from its peers. Every connection starts with a version handshake in which the nodes send information about themselves (e.g. best block height) and negotiate what to talk about (e.g. only interested in blocks). Connections may also change through subsequent messages, such as a fee filter message to communicate that they're only interested in being relayed transactions with a minimum fee rate.

Discouragement, Disconnection, and Banning

Bitcoin Core nodes keep track of which peers behave in a way that indicates they may be malicious or running malfunctioning software. In response to such behavior, a node might choose to discourage (mark its misbehavior and perhaps disconnect in favor of new peers), disconnect, or ban the peer.

Permissions and Whitelist

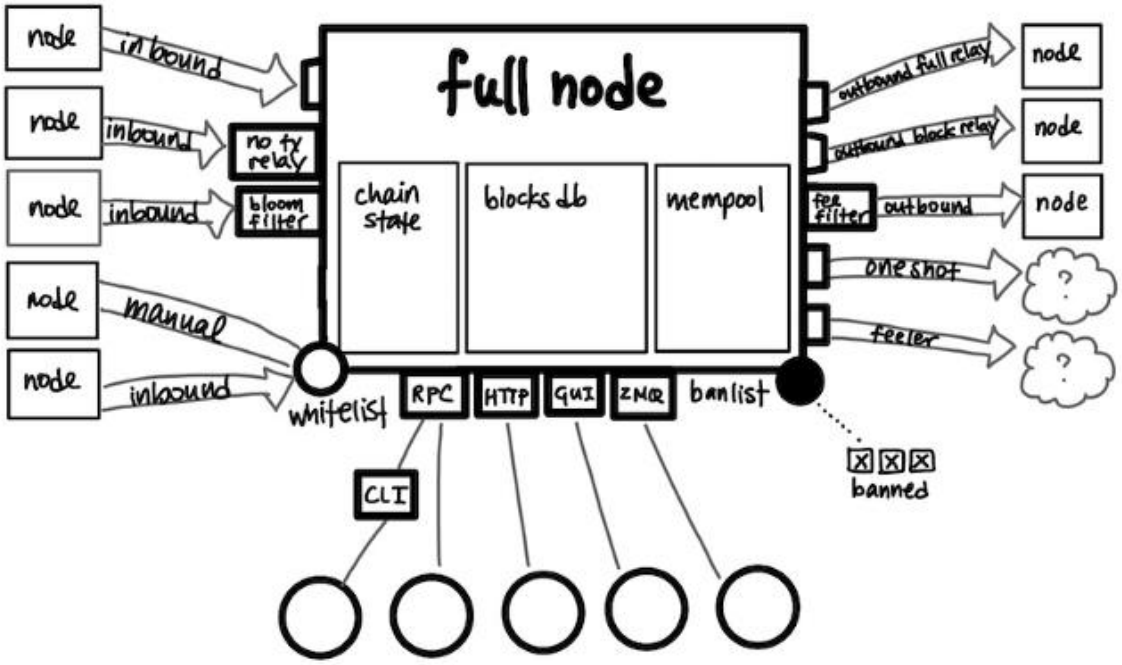
Nodes also keep a list of permissions that each peer has, such as particular services it's allowed to request or tolerance for misbehavior that would normally be penalized. Services are negotiated for every connection during the version handshake. Allowing misbehavior is often manually added for custom, personal light clients and nodes operated by people that trust each other. Related, nodes can also whitelist particular IP addresses.

Importance of Asymmetry

Note that each individual connection is bidirectional but **asymmetric**: the initiating peer may understand the connection to be a [full-relay] outbound, block-only-relay, feeler, or one-shot, but the receiving peer just sees an inbound connection with some established rules. This hides information through ambiguity about whether a node's behavior reveals its internal mechanics or merely reflects the nature of the connection.

For example, if a node knows that its peer is in blocksonly mode (i.e. rejects all incoming transaction messages), it is obvious that all transactions sent from that peer correspond to its own wallet addresses. Instead, the receiving node just sees an inbound connection with transaction relay turned off. This could mean blocksonly mode, block-relay-only connection, or an idiosyncrasy of the connection.

A more detailed view of an individual node could look like this (note that the arrows' directions just indicate which node initiates, not that the communication isn't bidirectional):



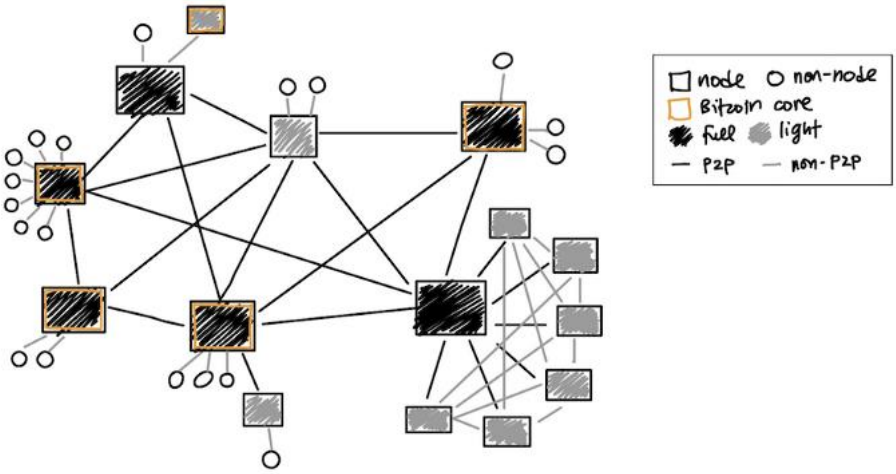
Slightly less simplified view of a node

"Full" Map

Each node has limited information about the network as a whole. Nodes really only see their own peers, and peers could be lying about what type of node they are. All peers could even be the same person in the event of an eclipse attack. This is an advantage for privacy and security because it applies to adversaries as well; having limited information makes targeted attacks more difficult. It's possible to gather approximate information about how many nodes are in the network by creating lots of temporary connections, but this information is far from comprehensive.

For example, whether or not a node participates in a mining pool isn't immediately apparent on the network. With approximate knowledge about which nodes are part of mining pools and observing how many blocks they mine, some websites are able to generate analytics on computing power proportions. However, they can be misleading as it is entirely possible for groups of nodes or even multiple mining pools to be operated by one entity.

Putting it all together, we can imagine this simplified network map:



Simplified Network Map

This map represents various ***possibilities*** instead of network size (which is very large) or topology (which is dynamic and unknown). Notice that the possibilities include:

- A Bitcoin Core full node with various clients connected via non-P2P interfaces, e.g. a user that downloaded the software from bitcoincore.org and is using the command-line or GUI to send and receive coins.
- Light clients that do their best to connect to a variety of full nodes in order to serve its own clients.
- A full node serving one or more light clients, perhaps an individual Bitcoin enthusiast who runs a full node using some cloud service provider and a more lightweight application on their personal device.
- A custom full node (e.g. a pool manager) connected to a group of custom light clients (e.g. individual pool participants) through both the P2P network and some private network.

Conclusion

Hopefully this post helped clarify what people mean when they say “node” and “P2P network,” and connect the dots on how all the participants in the network interact with one another. I hope it also provides some insight and “food for grep” on how Bitcoin Core implements peer-to-peer connections to protect privacy and enable new nodes to participate. Thanks for reading! :)

21 million thanks to John Newbery and Amiti Uttarwar for being very generous with their time helping me understand and document this information.

MPPs & Wumbo Channels: Optimizing Liquidity on the Lightning Network

By Roy Sheinfeld

Posted September 14, 2020

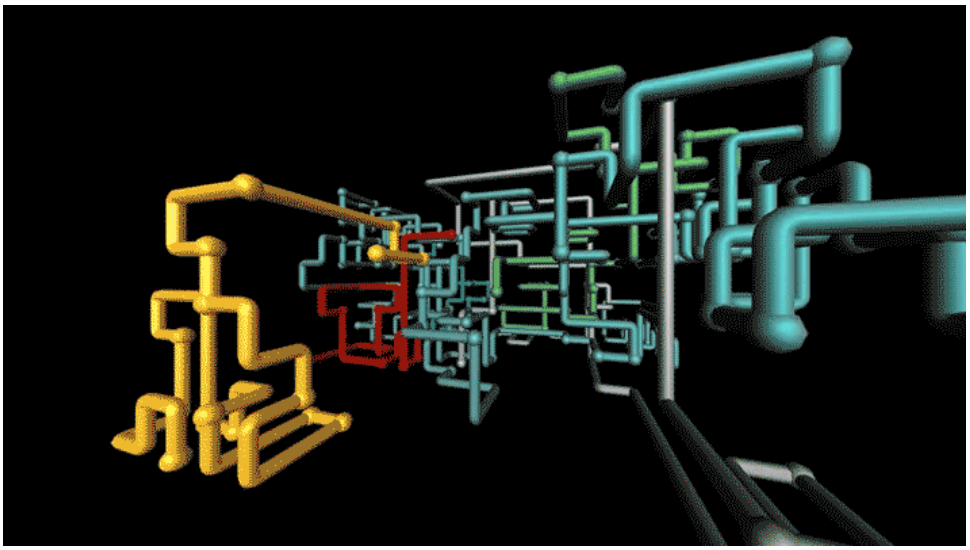
Liquidity is all about flow. On the Lightning Network, bitcoin is the liquid, and the question is how much of it can move and at what speed. Payment channels are the network's pipes, and until just recently, all pipes were fairly small, and a payment could only reside or flow through one pipe at a time. The liquidity was there, but it wasn't ***flowing*** as well as it could have.

In the last few months, a couple of things have changed:

1. Multi-Path Payments (MPPs) went live in May with LND 0.10, which splits payments into smaller parts and allows those parts to be and move in different places simultaneously.
2. Wumbo channels went live in August with LND 0.11. They allow the nodes that share a payment channel to determine its capacity and to diverge from the old one-size-fits-all rule if they please.

We've talked about both MPPs and Wumbo channels before in the context of UX. Our thoughts back then were strictly focused on the user. But as we've been thinking more about the structural requirements of the network, including routing nodes, LSPs and the differences between users who mostly s(p)end and merchants who mostly receive, we realized that these two features have larger implications. MPPs and Wumbo channels have the potential to optimize liquidity throughout the network.

In this post, I'll quickly recap what MPPs and Wumbo channels do, contrast them with standard payment channels, and explain how these two innovations change the face of Lightning.



Mario & Luigi would salivate at what Wumbo and MPPs can do. (Image: Phaidon.com)

Standard payment channels and their limitations

We've already covered standard payment channels in more depth here and here, so now I'll just provide the need-to-know information:

- Two parties on Lightning can open a payment channel with an on-chain transaction.
- They can jointly commit a maximum of 0.1677 BTC to the channel, although they can reallocate that sum back and forth with off-chain transactions.
- Payments between two users without a direct connection are routed through intermediate nodes and channels until they reach their intended destination. 1 payment = 1 HTLC = 1 route.
- A channel stays open with the funds moving back and forth until it's closed with an on-chain transaction by either party or by both together.

Standard channels limit users' exposure to risk, but they fragment the network's liquidity, which also restricts Lightning's utility and convenience. Having access to only one limited local balance at a time and being able to route a transfer over a single route means that all users — but especially routing nodes — have to rebalance their channels often.

Like training wheels on a bike, standard channels were appropriate for a network that was just getting started, but at a certain point they started to impede our speed and progress. Standard channels were becoming an obstacle blocking the flow of liquidity over the network.

Wumbo channels

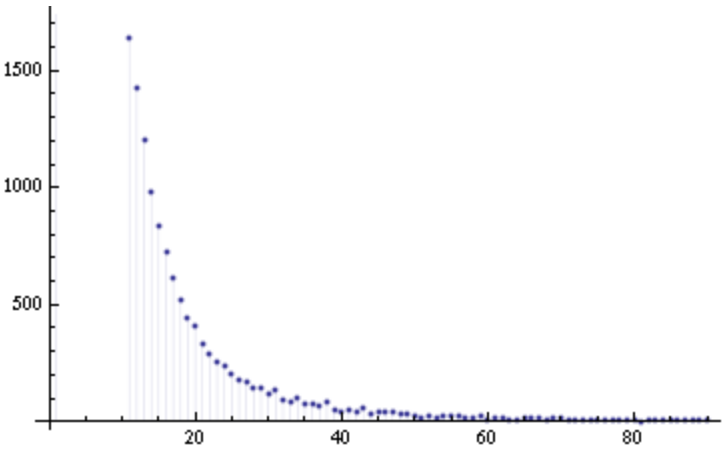
The limit on standard payment channels was designed to shield users from the risks associated with a new, growing network. The lnd software is still in beta, and nobody wanted incoming users to lose everything to unforeseen vulnerabilities.

After a few years of operation and tens of thousands of channels among thousands of nodes, Lightning has proven itself. So far, it's turned out as safe and stable as we had all hoped. Wumbo channels are one of the rewards.

Wumbo channels are effectively standard payment channels without the limit (though there is discussion about implementing a new "soft" limit). They allow the users on either end to open a channel stocked with as much bitcoin as they like.

Wumbos as trunks

Just like the internet itself, Lightning is a network of networks. At the moment, only three nodes have more than 1000 public channels open, and as you scroll down the list of nodes, the number of nodes with a given number of channels increases as the number of channels decreases, more or less. The distribution roughly follows a power law. It looks kind of like this:



I've always thought that "Power Law" would make a great superhero name. (Image: Wikimedia)

Few nodes have many open channels, and many nodes have few open channels. Most users are connected to a small subset of nodes — the routing nodes — that, in turn, have to maintain large amounts of liquidity on the channels among themselves to keep the funds flowing. (Yes, this is the issue of ***liquidity centrality***. We've discussed it before here.)

Whereas most users wouldn't notice a channel limit of 0.1667 BTC on most days, these routing nodes need trunk channels among themselves to handle much higher daily volumes. Wumbos allow a channel between two routing nodes to reflect the volume of transactions they handle. Routing nodes, including Breez, can now manage their liquidity over fewer channels and with fewer on-chain transactions. As Wumbos make operating nodes easier

and cheaper, we'll be able to spend even more time on innovating and improving the Breez client and Lightning as a whole.

Perhaps ironically, helping the network's hubs also helps to decentralize it. Operating a high-capacity Lightning node isn't trivial, and liquidity management is a big part of that challenging task. As it becomes easier to run a routing node, more people will opt to do so, which would help to decentralize the network. Alleviating headaches for existing Lightning operators simultaneously lowers the barriers to entry for incoming operators.

Wumbo hallelujah!

Multi-Path Payments (MPPs)

Even without limits, the maximum transfer size was — until recently — limited by a user's balance on a given channel. Since each payment could only be contained in a single HTLC, and each HTLC could only handle a single route, the client would have to seek a single route with sufficient balances at each step. Forcing a payment along a single route meant that only a minuscule fraction of the network's liquidity was available for a given transaction.

Standard channels and payments fragment the network's liquidity into discrete, mutually inaccessible parts. While preserving ownership, MPPs pool that liquidity and put it at the network's disposal.

How? MPPs teach LND to be patient. LND will first try to execute the payment as usual over a single channel/route. Should that attempt fail, because, say, the payment exceeds the fee limit or the relevant channel capacities, LND will try to send only half the amount. Once that half is en route, LND will search for a suitable path for the remaining half, splitting that half and repeating the process in case of failure. This process repeats until either the transfer succeeds (hooray!) or the minimum, indivisible transfer amount is reached.

And instead of expecting the entire sum to arrive at once, an HTLC sent via MPP tells the receiving node the total payment amount to expect. Thanks to a HODL invoice, the receiving node won't settle the payment until the expected amount has arrived in full. Neither the sender nor the recipient need worry or care about how many parts made the journey over what routes.

Of course, Lightning never stands still. Even though MPPs only went live a few months ago, there are already plans to improve the algorithm. One interesting proposal is to split failed transfers by the Golden Ratio in order to approximate the Fibonacci sequence rather than simply halving them. The

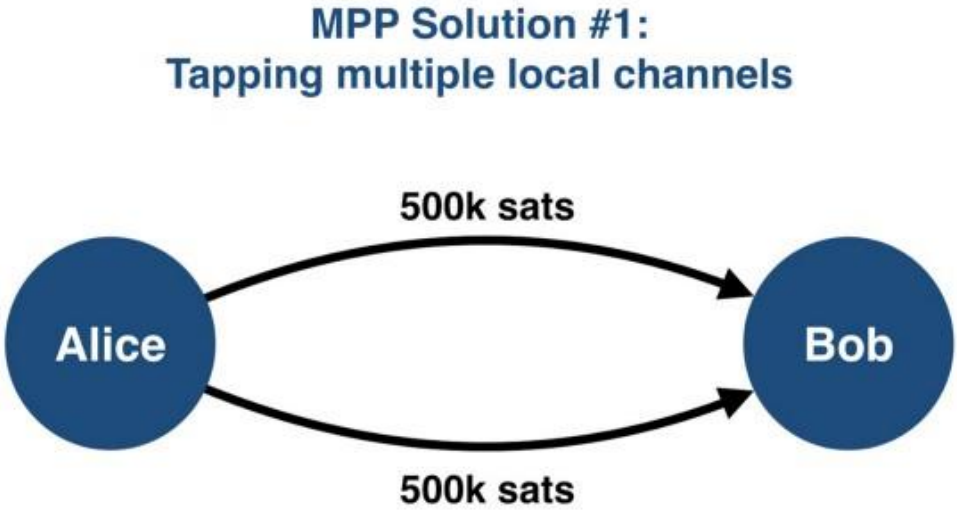
idea is to find the largest viable transfer size in fewer steps with less computation.

Another improvement being prepared by (***ahem*** — Sorry. I need to clear my throat of false modesty.) ***our*** team is to first attempt the transfer with the user's maximum local balance across all their channels rather than half the transfer amount. This would give users a better chance of being able to spend all their funds in a single payment, no matter how they are distributed across their channels.

So let's talk examples. Suppose Alice wants to send 1M sats to Bob. They share two channels, but Alice only has 500k sats in each. Without MPP, she can send him a maximum of 500k in a single payment. To send any more she would have to execute two separate payments.

And the same is true at Bob's end. The rule of 1 payment = 1 HTLC = 1 route applies to the recipient too, so without MPP he can only receive 500k sats at a time from Alice.

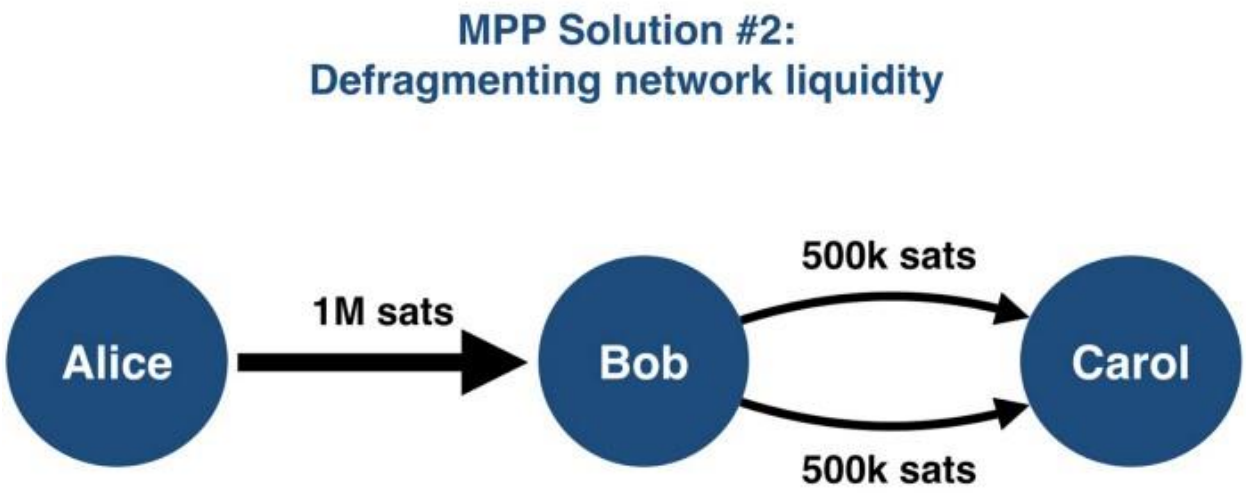
MPP provides flexibility at both ends. It can automatically split the payment between the two channels, send the two parts separately, and Bob's client can recombine them.



Second, let's suppose Alice wants to send 1M sats to Carol. She doesn't share a channel with Carol, but who cares? It's a ***network***. She has 1M sats on her channel with Bob all ready to send. Bob shares two channels with Carol, but tragically, he only has 500k sats on each. Without MPPs, the maximum

transfer size is limited by the lowest local balance along the route. So if Bob only has 500k sats in any given channel with Carol, that limit applies to Alice too. Like with any liquid, the flow rate is limited by the narrowest pipe along the route.

MPPs effectively "defragment" the liquidity between Bob and Carol. Instead of being limited by the narrowest pipe, the flow is limited by the ***sum*** of pipes along the route. It combines those fragments into a greater, more useful whole. Since the sum of local balances between Bob and Carol is 1M sats, the constraint on Alice has vanished.



Instead of being limited by the lowest local balance of any ***channel*** along the route, payment size is now limited by the least total liquidity of any ***node*** along the route. The key restriction is now how much bitcoin is in the sender's Lightning wallet, which makes perfect sense.

The effects at the network level are at least as momentous. Instead of each possible route being a stream of liquidity with a maximum capacity, like a water pipe, each node becomes its own little pool of liquidity. Channel capacities are no longer discrete; ***they're additive***.

Now imagine MPPs and Wumbos combined. Pools connected by channels of unlimited capacity aren't pools any more. They're not even lakes. It's a single, vast ocean. No fragmentation, no obstacles, pure liquidity, optimal flow.

Breez & MPPs

Since we strive to eliminate all of Lightning's seams and MPPs bring us one step closer to a seamless network, we immediately saw their utility and began implementing them. The client already receives MPPs automatically.

Advanced users can already open multiple channels to increase their capacity. However, Breez doesn't yet support sending MPPs. Doing so is in the works for the next major update. We're also working to simplify the process of creating multiple channels, and further improvements are coming soon. MPP is too good not to use, so we're integrating it deeply into the Breez DNA.

Lightning over a sea of liquidity. And what causes those waves? The Breez, of course. (Image: pxfuel)

The coevolution of Lightning technologies

As any rabbit in the forest, pandemic survivor, or evolutionary biologist can tell you, the most important selective pressure on any species is the other species with which it comes into contact. The utility of any biological function or physiological feature — running, swimming, digesting pine needles, gills, wings, and big brains — depends on what other creatures are around, and what functions and features ***they*** have developed. Nothing evolves in a vacuum.

The same applies to the evolution of Lightning technologies. The utility of Wumbo channels fosters the proliferation of routing nodes and increasing payment sizes. But developments on trunk channels don't serve much purpose unless the UX improves, attracting users and their liquidity. MPPs defragment the network's liquidity and increase transaction volumes, necessitating Wumbos, which allow for still greater volumes over more channels, which makes life still easier for users …

The technologies we use evolve together, symbiotically, reinforcing each other, creating new niches, new opportunities, and new challenges. And like any evolutionary process, the best innovations of each generation will constitute the foundations for their successors. Lightning can't help but improve. We just have to keep at it.

The Alchemy of Hashpower, Part II.

By Leo Zhang & Karthik Venkatesh

Posted September 15, 2020

"When events have thinking participants, the subject matter is no longer confined to facts but also includes the participants' perceptions. The chain of causation does not lead directly from fact to fact but from fact to perception and from perception to fact."

-George Soros, The Alchemy of Finance

In Part I of this series, we presented a simple heuristic for understanding hashpower as an asset class. In mining, everything is connected. To establish a comprehensive understanding of the market dynamic, we need to scrutinize the interactions between the underlying forces in greater depth.

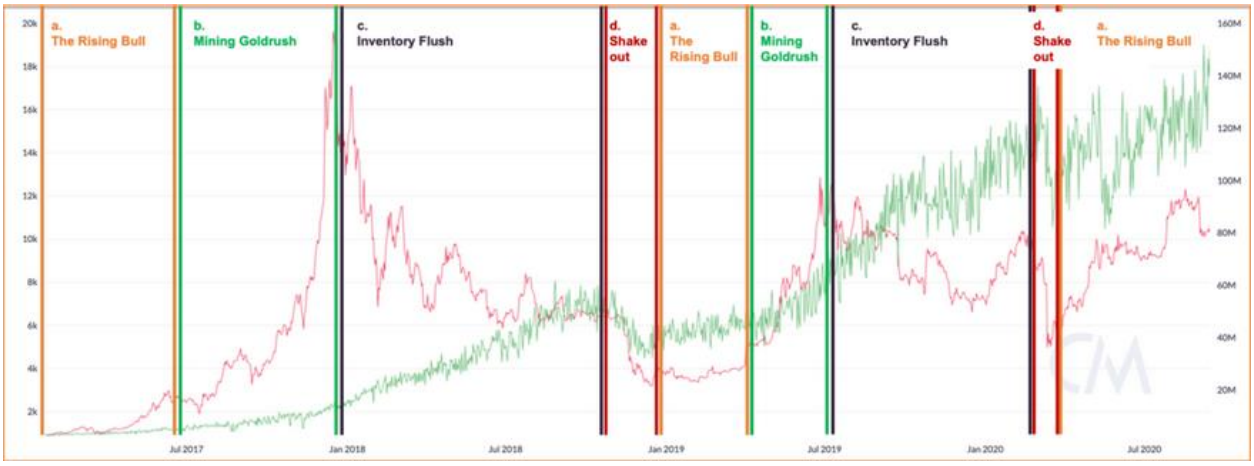
In this article, we start by breaking the mining market cycle into four archetypal stages, each with distinct price trends, hardware capacity, and sentiments. We examine the driving forces in each scenario, and illustrate the roles that the hardware reaction time, and reflexivity in hashpower play in shaping these macro cycles.

Through a series of case studies and theoretical arguments, we intend to **introduce a guiding framework for understanding different investment environments in mining**. As a coda, we discuss the rising significance of fees in mining calculation. The new opportunities around the fees market, and how fees as a principal variable profoundly changes the hashpower market dynamic.

The Cycles of Mining

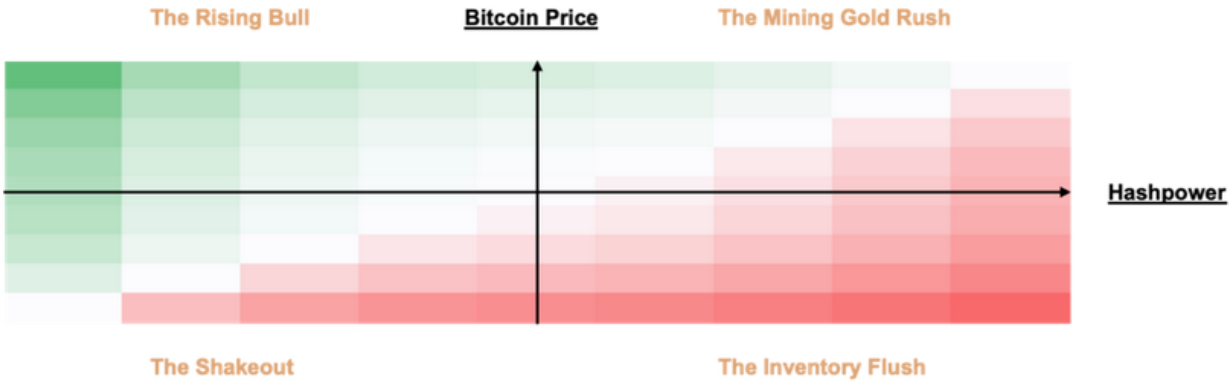
The hashpower market dynamics is driven by a convoluted interplay of exogenous and endogenous factors such as price trends, hashpower reflexivity, hardware reaction time, and fees. While the logic that connects them may seem rather straightforward, the unpredictability of each of the variables makes it challenging to produce timeless generalizations.

As a result, sometimes the macro patterns emerged may not make any sense, as if price and hashpower live in completely different frames of references. Nevertheless, miners' actual profitability can be traced. Based on how the market's impact on historical Bitcoin mining revenue evolves, we can identify four archetypal stages in the mining boom-bust cycle:



(Source: Bitcoin, [CoinMetrics](#))

The cycle is characterized by the vectors of price and network hashpower moving in different directions at different rates. Based on the specs of a Antminer S19 Pro, we can illustrate how its mining revenue change in each scenario:



The Rising Bull

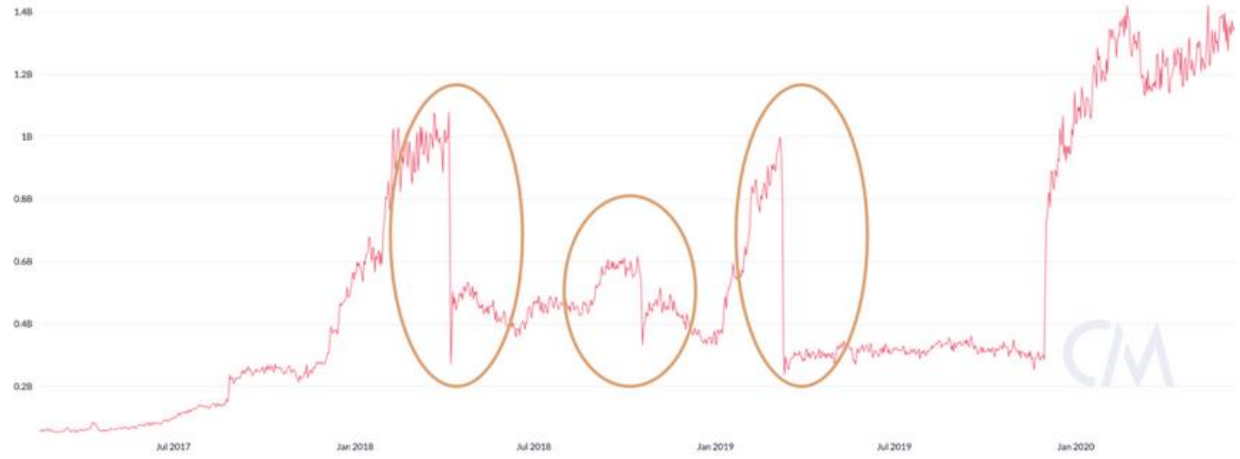
Price outpaces global hashrate growth rate

Mining is the most profitable when difficulty significantly lags the price rally. The “Rising Bull” phase usually happens after long periods where volatility is relatively muted, and the price just begins building momentum while the rest of the market is still uncertain which direction it is going next. Hashpower grows much slower than the price. The increase in hashpower primarily attributed to miners that strongly expect price will rally, or those with access to extremely cheap power sources. For example, between January to April 2019, Bitcoin price was suppressed after the BCH-BSV “Hashpower War” that took place around the same time as the China dry season. Resourceful miners acquired cheap used machines that were trading

cheap on the secondary market. Some were also able to capture the opportunity through synthetic mining contracts or cloud mining.

Sometimes exogenous factors can even cause hashpower to drop despite an upward trend in price. Often has to do with physical conditions such as extreme weather flooding that force large data centers to go offline. The flood during the rainy season in Sichuan in 2020 is particularly disastrous. However, these are temporarily setbacks that usually recover overtime.

Another special situation that can force hashpower to decline is hard-fork. After the first Bitmain ASICs were announced, Monero devs decided to switch hashing algorithms once every six months. Every time the network changes the algorithm, a portion of the network hashpower would drop. The developer-initiated hard forks is not just a phenomenon in anti-ASIC projects. The Sia devs embrace ASICs, but they proceeded to hard fork in order to brick specifically Bitmain and Canaan ASICs.



(Source: Monero, CoinMetrics)

The special situations may temporarily halt the hashpower increase, but as the overall upward trend continues, the participants' positive bias gets reinforced, demand for hashpower increases.

Mining Gold Rush

Price growth rate high, hashpower growth picking up

Once the bull formation has been validated, people are much more eager to purchase machines. New machines are sold out almost right away. Large miners place handsome orders at manufacturers to have their shipment prioritized. In Part I., we described how machines are loosely priced based on ***static-days-to-breakeven***. The shorter the time it takes to breakeven, the more expensive the sellers get to price the machines. Coin price rapidly rallies, demand for new machines follows, but hashrate growth hasn't picked

up the speed yet. These are the windows that manufacturers rake in astronomic profits. Both machine secondary market and cloud mining markets trade at a premium.

This is the same for both ASIC and GPU mining. From 2016 to late 2017, AMD and Nvidia benefited greatly from the meteoric rise of Ethereum. Miners were willing to pay top dollar to get their hands on every GPU available. At one point, the supply shortage was so severe that Nvidia even considered asking retailers to limit sales to 2 per customer. In today's market, as DeFi brings attention to Ethereum again, manufacturers are racing to produce ETH ASICs.

The hype easily creates FOMO among miners. The positive bias continues to self-reinforce and the expectation rises even faster. Younger altcoin networks going through this phase for the first time may start to attract the attention of ASIC manufacturers.

In early 2019, rumors about hundreds of millions of investments in Grin spread like wildfire. Venture capitals rushed to fund special-purpose vehicles to procure and operate GPU miners. Difficulty skyrocketed not long after the project launched on mainnet, and manufacturers such as Innosilicon and Obelisk were racing to build the first ASIC. The rest is history, the project never lived up to the hype and the ASICs never filled enough order to get produced.

Inventory-flush

Price drops, hashpower growth rate still high

As Howard Marks says, ***"Everything that produces unusual profitability will attract incremental capital until it becomes overcrowded."*** The most destructive effect of a reverting bull market is the Inventory flush.

It is a common occurrence after bull runs and manufacturers overproduce machines. In 2017, manufacturers such as Bitmain misjudged the length of the bull market, and produced an excessive amount of machines throughout 2018. They had to flush out their inventory by gradually lowering the machine prices. In order to get rid of excess chips, Bitmain even rolled out undesirable products such as mining home Wifi routers. As a result, despite the price drop, hashrate continued to climb for several months until profit margin became sufficiently squeezed.

During the same period, many GPU farms became unprofitable due to exponentially-growing hashpower competition, altcoin ASICs (Dash, Zcash etc.) were released into the market while the altcoin prices fell off a cliff. The bear market hit the hardware supply chain so fast that they barely had any time to react. Nvidia posted *"disappointing"* financial results, and the founder

Jen-Hsun Huang went from: *"crypto will be an important driver to our business"* during the peak of 2017 to: *"Can we all please — I don't want anybody buying cryptocurrencies, okay? Stop it. Enough already. Or buy Bitcoin, don't buy Ethereum."*

Inventory flush due to overproduction happens in many markets that suffer from high reaction delay. For example, around ten years ago New York City luxury apartments had an epic bull market thanks to generous international buyers. Developers rushed to start new projects. In recent years, the buying power dried up due to various reasons such as currency control, but those new luxury apartments are just becoming available for the market. As a result, developers are stuck with empty buildings.

The Shakeout

Price drops, hashpower drops

Occasionally, mining revenue drops below a threshold where it becomes unprofitable for miners to keep them on. Chinese miners call it the "shut-off price". In a traditional market, when a correction sets in, negative bias may snowball into a downturn trend. But since hashpower is self-referential, the more hashpower leaves the market, the more "concentrated" remaining hashpower gets.

That's why in Bitcoin, these over-corrections tend to be ephemeral. In Bitcoin, the threshold is buffered by miners' expectation of the future mining revenue. They believe the chance to recover is high, hence they are willing to mine at-loss or even deploy more machines while the market goes through the Shakeout. On the other hand in networks infested with speculative miners, such capitulations happen frequently

Things that perform poorly for too long eventually become cheap and attractive. The same cycle will repeat again and again due to, what John Kenneth Galbraith calls, *"the extreme brevity of financial memory."*

Plato's Allegory of Market Fundamentals

Why does the hashpower market manifest these cycles? Intuitively hashrate growth and price trends are connected. How come changes in price don't lead to commensurate adjustments in hashpower? **In other words, why isn't the hashpower market efficient?**

Conceptually, the market is an information-aggregation device that alchemises participants' perceptions into price information. The faster the price absorbs new information, the more efficient the market is. In a theoretical equilibrium state, the network difficulty should converge to a level where the majority of the miners are operating close to breakeven.

In an early BitcoinTalk post, Satoshi wrote, *"The price of any commodity tends to gravitate toward the production cost. If the price is below cost, then production slows down. If the price is above cost, profit can be made by generating and selling more. At the same time, the increased production would increase the difficulty, pushing the cost of generating towards the price."*

However, the Bitcoin market today is far from a passive reflection of its production cost. It's rare to observe the type of equilibrium that Satoshi envisioned.

While for most physical commodities, the supply is largely determined by production and demand by consumption, speculation pushes the crypto investors to make decisions based on expectation of future price rather than the current supply and demand curves. Thus, the snapshot calculation of mining cost-basis provides very little insight about the market.

Market participants always bring their own biases when processing new information. It's similar to guessing the shape of a high-dimensional object by examining its projection on a surface in lower-dimension. This is Plato's Allegory of Cave for the market fundamentals.

With cognitive fallibility comes reflexivity. Reflexivity is an iterative process: The market, a melting pot of biased perceptions, is always flawed in representing reality. As investors make bets on the market, the changes in prices begin to influence the market fundamentals (e.g. companies become more or less capitalized), which in turn affect the price, thus forming a reflexive feedback loop.

Rather than focusing on the hypothetical outcome, it's more practical to study the process of the change. Reflexivity theory has gained mainstream popularity over the years. Its patterns have been widely observed in equities, currencies, crypto, and even the mining markets.

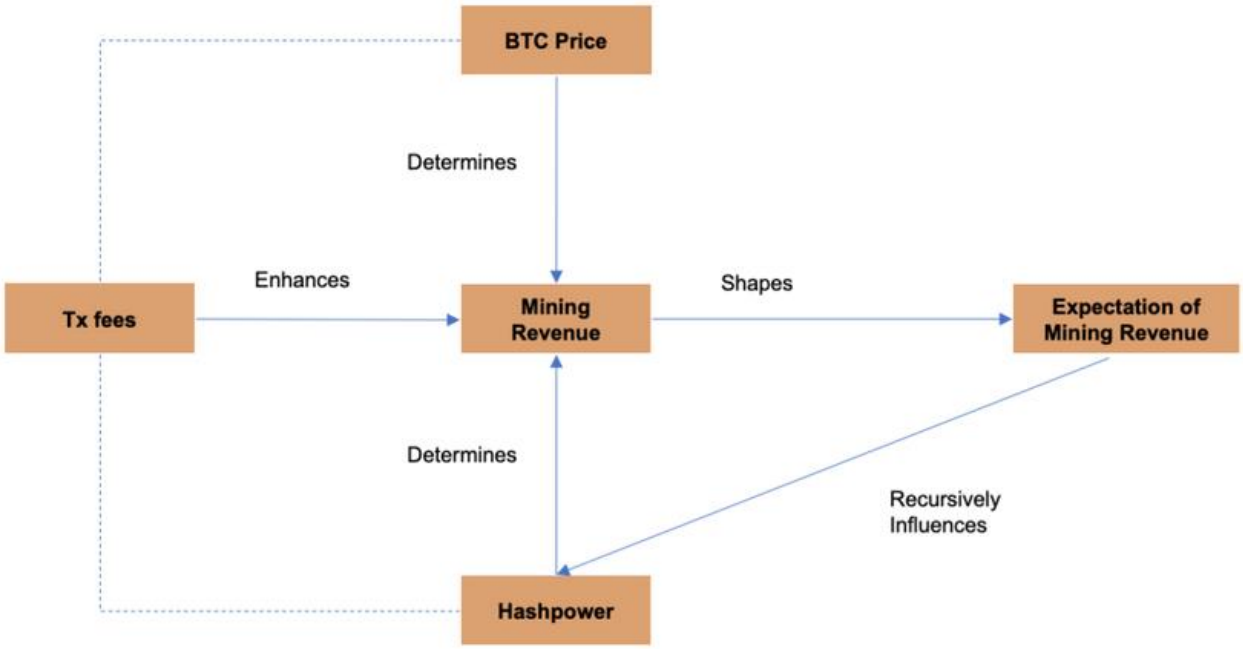
Reflexivity in Hashpower

How does reflexivity work in the hashpower market?

It's no secret that the demand for hashpower is driven by the value of the coins it produces. **Buy and sell decisions are based on the participant's own expectation of the future mining revenue.** Equity investors set their expectation of future price by performing macro, industry, and company analysis. Hashpower investors set their expectation of the future mining revenue by assessing trends in price, fees, and network hashrate growth.

	Reflexivity in Equities	Reflexivity in Hashpower Assets
Fundamentals	Macroeconomy, industry, business performances	Mining revenue (price, fees, hashrate)
Measures	Cash flow metrics, trading multiples etc.	USD/Th/S, Days-to-breakeven etc.
Bias	1.Market thinks valuation is too high 2.Market thinks valuation is too low	1.Long-term bear market 2.Short-term bear market 3.Mining overheating 4.Long-term bull market

Everyone has their own (often flawed) heuristic for setting expectations for price trends. Hashrate growth, on the other hand, is much more challenging to build models for. One reason is that it's dynamically recursive: the more hashpower floods the market the more diluted each unit becomes. Changes lead to adjustments in expectations, and thus it recursively influences the current mining revenue. **Every participant in the hashpower market constantly changes the rest of the market.**



This means the most scientific way to predict hashrate growth is by collecting sales numbers from manufacturers, large miners, service providers, and distributors. But the mining machine business is plagued with recondite information. It takes Herculean effort to acquire accurate and updated data. Since it is difficult to reliably set expectations for hashrate growth, and income from fees is still eclipsed by block rewards, naturally expectation for

future price becomes the de facto driver. After all, why would anyone spend so much capital and energy getting involved in mining if the person is not optimistic about the future price?

Gathering mining data is an onerous task, but is it possible to untangle the dependence structure between price trend and hashrate growth?

We often see divergences in hashpower and price as illustrated in the four stages of the market. Information in capital markets travels fast. Hardware manufacturing & transportation is slow. **The hashpower market is the opposite of what's idealized in Efficient Market Hypothesis.** This renders vanilla correlation analysis useless. We need to interrogate the data at different time scales.

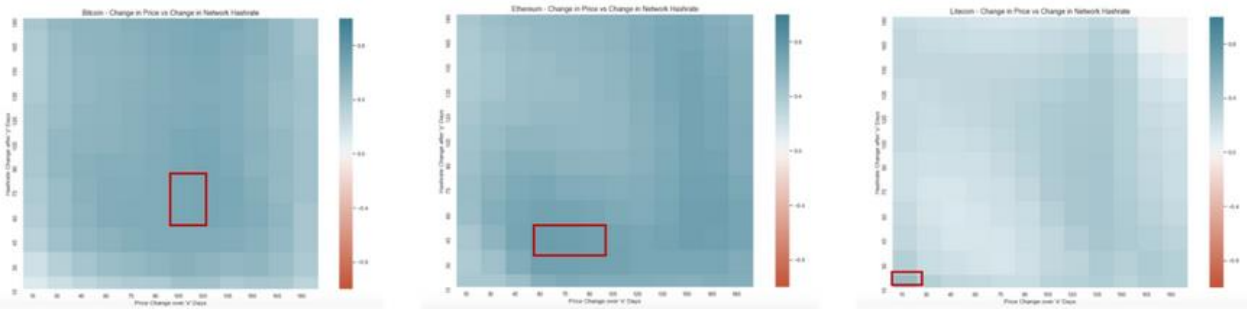
In a comprehensive research report published by BitOoda, they analyzed the price & hashrate changes in 2019, and discovered that it took around an average of 4-6 months before hashrate started following the price rally.

Note that this lag time is not fixed. Depending on the production capacity and availability on secondary markets, the lag time varies for each market move. Different networks also have different response times.

Take Litcoin for example, between Jan-May 2018 its hashrate took a long time to respond to the price change. After July, hashpower and price became very synchronized.

(Source: Litecoin, CoinMetrics)

Extending the analysis to Bitcoin, Ethereum, and Litecoin over a longer period to 2017-2020, we discovered that the average response times are 60-120 days, 30-60 days, and 15 days respectively.



*Process:**Aggregate data into periods of 15 days:__Columns in the dataset are Date (15 days ending), mean Price over 15 days, mean hash rate over 15 days__For each 15 day period, calculate:**% change in price after 15 days, 30 days, 45 days, ..., 180 days__% change in hashrate after 15 days, 30 days, 45 days, ..., 180 days__Compute correlation between price change and hashrate change over different time periods__Read the matrix as: correlation between price change over 'y' days and change in hashrate after a period of 'y' days (following the x-days period that saw a change in price)*

In the future, we intend to examine how the response time evolves over time, and anatomize the underlying driving forces. Our next project is to quantify the endogeneity of the hashpower market, and build an index to measure reflexivity in various networks.

The responsiveness is neither inherently good or bad. It is a function of the availability of the hashpower on the market at the given time. Some smaller networks dominated by general-purpose hardwares on average have much shorter response time. Their hashpower responds to price ups and downs faster because the miners on these networks are less loyal. Compared to ASIC miners, they can easily switch to a different network when profitable. Some mining pools offer automatic switching services that constantly hops over several different networks to maximize profit (known as *"Profit Switchers"*, or *"Machine-gun Pools"*).

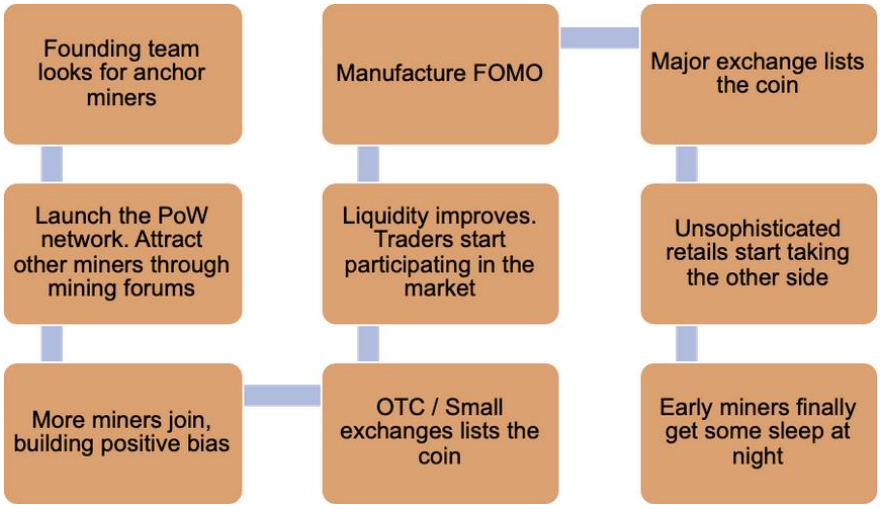
	Speculative Mining	Hybrid	Value-Driven Mining
Hardware Type	Mostly GPUs	Mix of GPU, FPGA, and some ASICs	Mostly ASICs
Price-Hashpower Disparity	Short	Short	Long
Mining Horizon	High Time Preference	Mixed	Low Time Preference

Note that a network dominated by ASICs doesn't necessarily make it Value-Driven (e.g. Litecoin post 2019); and a network dominated by GPUs are not entirely Speculative (e.g. Ethereum). That is determined by the project itself and its community.

In most cases changes in price precedes changes in hashpower. Occasionally we can observe the inverse in altcoin markets, usually altcoins that are about to go through Halving or special market events.The Halving is one of the biggest recurring self-fulling prophecies in cryptocurrency, and expectations of a post-Halving rally drives miners to deploy new machines to mine on the network ahead of time. Sometimes coordinated pump & dump groups would deploy hashrate to accumulate enough coins before pushing up the price for the ultimate reap.

This game is also common among the GPU miners speculating on new projects. Upon launch, most coins are traded exclusively on OTC markets with terrible liquidity. Miners don't have good channels to exit their positions as they continue to operate at a loss until community development gains momentum. As the community grows, bigger exchanges will list the coin, giving early miners a chance to take some profits.

This does not imply the hashpower increase will cause the price to increase. It's a high risk bet and there are a myriad of examples of failures. Many stars need to align in order for such a heist to work out favorably. It can go sideway in every step of the process below:



GPU-launch was popular between 2017 and early 2019. Some analysts suggested that proof-of-work may be a fairer launch model than ICOs that issue SAFTs to venture capitals. What constitutes a fair launch is a much broader topic. It's a controversial subject even among DeFi projects that have nothing to do with proof-of-work. The launch method and the hashpower acquired do not guarantee price rally in the future. In essence it is a varied

form of ICO with a higher barrier of entry, the same casino game of throwing darts in the dark.

The hardware reaction time, regardless of the length, is a source of endogeneity. This means that when modeling the impact of price on hashrate growth (or vice versa), the impact is likely underestimated or overestimated. Hence decisions based on inferences from the model could be disastrous as an input to investment decisions.

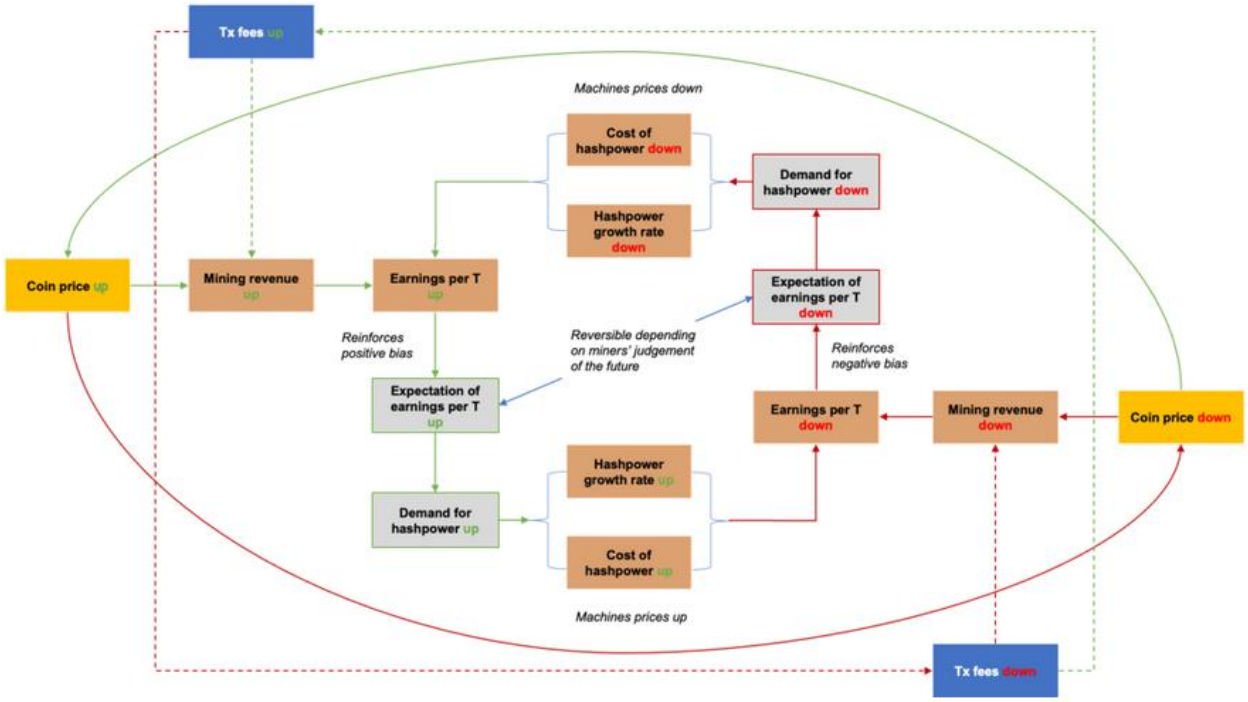
The moral of the story is that the connection does not imply a causal relation between hashpower and price.One does not mechanically induce the other. **It is the expectation of future mining revenue and the expectation of hashpower growth that are continuously reinforcing each other.**

The Rising Significance of Fees

To take the macro model at the beginning of the article one step further, fee trend should be a principal variable as well. As discussed, at the moment the expectation of mining revenue is primarily driven by price trends. In the past August, Ethereum miners made a total of $113 million in profit. The previous all-time high ($64 million) was reported in January 2018. The exorbitant fees is explainable in light of the rising on-chain traffics from the DeFi projects.

Having transaction fees as a key variable opens possibilities for new games. For instance, arbitrage opportunities on Ethereum-based decentralized exchanges incentivize competing bots to bid up transaction fees in priority gas auctions. Miners who have control over the ordering of transactions can take advantage of these auctions via ordering optimization fees. This is part of a broader topic called miner-extractable value (MEV), that is the value that miners can earn directly from smart contracts. There will be more services and infrastructures (such as Sparkpool's Taichi network, which improves transaction broadcast) that tackle various aspects of the emerging fees market.

As fee income constitutes a growing portion of the mining revenue, it adds another dimension to mining revenue calculations. **Both the expectation of price and the expectation of fees will influence the expectation of future mining revenue:**



The reflexivity theory is a useful heuristic for understanding the ebb and flow. However, the model cannot replace understanding the fundamental vulnerabilities in the hashpower market. As the mining industry becomes more industrialized, the capital expenditure inevitably grows. Meanwhile, fees as % mining revenue increases, and the four archetypal stages will expand to even more complex scenarios. The combined effect will introduce more challenges and uncertainties to cash flow management.

After a decade of development, the hashpower capital markets still suffer from the lack of standard terms and pricing heuristics. The industry demands proper risk management practices and mature market mechanisms to secure continuous long-term investments into hashpower.

In the next article, we will discuss in-depth on risk management framework, creative financing & hedging strategies, as well as the long-term impact of financialization to the mining industry.

Tweet Thread on the Lightning Network User Experience

By Giacomo Zucco

Posted September 15, 2020

1/ Many people complain that “managing Lightning Network liquidity is still very hard” when they talk of Bitcoin & LN as a possible online payment solution. After using it to send & receive most <$50 payments for almost 1 year, I strongly disagree, especially within the context.

2/ When we compare LNP with other, existing online payment systems, we compare it with Credit Cards, Debit Cards & newer Fintech Systems like PayPal. Debit Cards are especially used (especially for frequent, small payments, where the “refill” mechanism provides more security).

3/ How does a Debit Card work? There’s a consequential distinction to be made here: the way Debit Cards work for people using them to ***pay*** over the internet (most of us, most of the time) is different from the way they work for people using them to ***receive*** (online merchants).

4/ In order to spend, you have to periodically fill up a bigger amount using a slower & possibly more expensive (especially wrt fixed costs) transaction (bank wire, typically). When the refill is complete, you can finally send small & frequent transactions, almost seamlessly.

5/ You can keep paying until the bigger amount, the one you filled up before, is over. Then you will have to fill up again (slower process, typically with fixed costs inconvenient for very small amounts), & so on. It may not be perfect, but it’s the typical UX for this use-case.

6/ Now, receiving online payments via Debit Card is an entirely different story. There’s a lot of regulatory friction: legal paperwork, KYC/AML compliance (which literally excludes the majority of people on this planet), fixed & dynamic fees, chargebacks. Truly terrible UX.

7/ How does LNP compare, UX-wise? I would argue it provides a strictly better UX in both cases (that is, assuming a merchant does accept it in the 1st place, which is still very uncommon, thus degrading the ***overall*** utility of this payment method for now). Let’s see both cases.

8/ In order to spend, you have to periodically fill up a bigger amount using a slower & possibly more expensive (especially wrt fixed costs: the blockspace

fees on-chain) transaction. When the refill is complete, you can finally send small & frequent transactions, quite easily.

9/ Unlike Debit Card spending, which is often actually free, LNP is not free: you have to pay for liquidity & "distance" from your payee in the graph. But fixed costs are still negligible &, of course, you have some advantages compensating: possible anonymity being the main 1.

10/ There's another important advantage: unlike w/ Debit Cards, where you ***always*** have to refill after your spending balance is empty, w/ LNP you may actually manage to rebalance it w/o getting back onchain: either receiving (see below) or routing other people's transactions!

11/ Granted: managing inbound liquidity in order to receive is not trivial (more on this below), & routing other people's transaction effectively, either for profit or to get some spending balance back is quite complex. But this is not even an option at all w/ our benchmark!!!

12/ Now, receiving. First you have to get some inbound liquidity: while not easy, it's orders of magnitude easier than getting a KYC/AML identity. Then you have to maintain it, which I'd argue it's not that more complex than the paperwork required for the Debit Card benchmark.

12/ Now, receiving. First you have to get some inbound liquidity: while not easy, it's orders of magnitude easier than getting a KYC/AML identity. Then you have to maintain it, which I'd argue it's not that more complex than the paperwork required for the Debit Card benchmark.

13/ So, in conclusion: basically identical to the "standard" online-payment UX for payers (thus also familiar, easy to learn/explain); very different but not necessarily harder to the "standard" online-payment UX for payees (the difference is technical complexity vs legal 1).

14/ If people find LNP UX confusing/complex, it's probably because they are comparing it w/ some inexistent "magical free lunch" that some Bitcoin advocates made up, where you somehow have all the advantages of on-chain BP, but not the drawbacks (cost, time, chain-privacy, etc.).

15/ If instead of this fake red herring you compare LNP with ***actual*** widespread alternatives in online payments, ie Debit Cards, I don't see any "liquidity management" complexity for payers, & I see why such complexity may compensate for lack of legal friction for payees.

16/ Of course, you may argue that the assumption that opening a well-connected channel with outbound liquidity is trivial, depends on the fact that there are huge "famous" LN nodes, which in itself carries some centralization risk. Fair. Still nothing compared to the benchmark.

17/ You may also argue that routing becomes very difficult when you have to pay very large amounts, even if you "filled up" your spending balance enough. But bigger amounts are exactly the use case where fixed blockspace fees become negligible, making on-chain BP more convenient.

18/ If anything we can agree that switching between on-chain BP & off-chain LNP could be made even smoother, hiding stuff from the user (ie: if LN routing fails the wallet tries to open a direct channel with the receiving node, if that fails it falls back on a normal BP address).

19/ Having said this, during an ongoing monetization process it's more rational to spend shitty fiat if you still have it & you can (NgU!). So people will probably not spend much with LNP. They will stack sats & limit spending to black/grey markets or privacy-sensitive purchases.

20/20 Eh, I forgot to add: The end.

Bitcoin In The Institutional Investment Portfolio

By Marcel Burger

Posted September 18, 2020

In May 2020, Paul Tudor Jones sent a remarkable letter to the participants of his "Tudor BVI Global Macro" Fund ^1. He revealed that the fund would take a position in bitcoin. Should institutional investors follow this example?

The increased market capitalisation of bitcoin in 2017 meant that a single Dutch institutional asset manager felt compelled to get a better idea of bitcoin and other crypto assets. There was a new asset class on the rise that quickly surpassed the market capitalisation of other asset classes in which investments were already made. A lack of solid fundamental valuation methods and sky high volatility led to continuing domination of skepticism. Nevertheless, renowned institutional parties give bitcoin a place in the portfolio 3 years later. Why would an institutional party consider investing in bitcoin? In this article I share two thoughts to help you formulate an answer to that question yourself and I conclude with a vision for the future.

What drove bitcoin's creation?

Satoshi Nakamoto (the pseudonym of bitcoin's still unknown creator) saw the 'trust problem' as the main reason behind bitcoin's design. According to Satoshi, the biggest problem with conventional money was the huge role that trust plays in making the system work. For example, to transfer money you have to trust a number of central parties in order for that transaction to be successful and you must be convinced that your funds are safe in custody. But a level higher, holders of the funds have to rely on central banks not to allow for (too much) devaluation of this money. Unfortunately, over the years and even today, there are plenty of examples where this trust is broken. Think for example of Argentina, Zimbabwe or Lebanon. The most terrifying example is Hungary in 1946, where prices doubled every 15 hours. In the first block of the bitcoin blockchain, Satoshi refers to this trust issue in a hidden message: "The Times 03 / Jan / 2009 Chancellor on brink of second bailout for banks".

Current state of fiscal and monetary policy

Prior to the Covid19 outbreak, global debt levels were already at unprecedented levels. Despite the fact that we all believe that the amount of debt must be curbed and that we also make clear agreements about this

(think of a debt ceiling in the United States and the use of a debt / GDP limit of 60% in the EU), we do not always succeed to meet those agreements.

Every time the financial markets fall (or threaten to) fall into decline, the central banks' buy back programs are revived to keep the markets afloat. According to the ECB, debt-to-gdp ratios will mainly deteriorate further in 2020.

Paul Tudor Jones reported to his clients in May that global money creation of USD 3.9 trillion has already been seen since February 2020, and is expected to grow even further to USD 16 trillion. Contrasted with the global money supply (M2), which was 95.7 trillion USD at the end of 2017, according to the CIA ^2, printing 16 trillion is a significant change in supply.

Ok, but what does bitcoin have to do with that?

Travis Kling, the CEO of Ikigai Asset Management, recently framed this well in two sentences in Peter McCormack's "What Bitcoin Did" podcast ^3:

"Bitcoin is a non-sovereign, hard-capped supply, global, immutable, decentralized, digital store of value. And it's an insurance policy against monetary and fiscal policy irresponsibility from central banks and governments globally."

These two sentences perfectly sum up the essence of bitcoin, and that last sentence in particular is the driving force behind institutional interest. Bitcoin is a digital decentralised medium whose maximum number of units in circulation is limited to 21 million. That 21 million is estimated to be reached asymptotically in 2140 because inflation automatically halves every 210,000 blocks (approximately 4 years). This makes it the first and only implementation of absolute scarcity. It enables us worldwide to store and irreversibly exchange value with each other without the involvement of a central all-powerful entity. In countries such as the Netherlands where the payment system works fine, everyone has a bank account and the value of the money is relatively stable, bitcoin seems to have little added value at first sight. However, where people are struggling with capital controls, war, political unrest or economic instability, bitcoin is adored. As we witness monetary easing globally, further devaluation of our conventional money is looming. Especially from this angle, bitcoin is found interesting by institutional parties and corporates, as most recently shown by MicroStrategy.

But aren't there enough other instruments that are able to protect us against inflation?

There are several instruments and investment strategies available that protect against inflation. Jones's letter lists all the alternatives and gives them

a score on the properties of purchasing power retention, reliability, liquidity and portability. In that comparison, bitcoin ends last place. But if we look at the differences in order of magnitude for both the score and the market cap, we see that while the scores are close in order of magnitude, the market cap for bitcoin is several orders of magnitude smaller. Jones concludes that although bitcoin is a suitable instrument to protect against inflation, there are alternatives that are more suitable. But the magnitude difference of the differences between eligibility scores and market cap leads Jones to believe bitcoin offers a great investment opportunity.

Change

When you compare the investment preferences of different generations, you see that each generation clearly has its own preferences. For example, according to research by Tom Lee of Fundstrat ^4, the silent generation was interested in gold, baby boomers particularly liked to buy equities and generation X was crazy about hedge funds. But now the millennials are presenting themselves as investors and this generation is even larger than the baby boom generation and has grown in a world that is becoming increasingly digital. The change in lifestyle and attitudes directly affects investment preferences. If the majority of invested capital comes from those younger generations, then you can expect the preferences of these generations to be reflected in the asset allocations. Bitcoin will increasingly be found there.

What does the future hold?

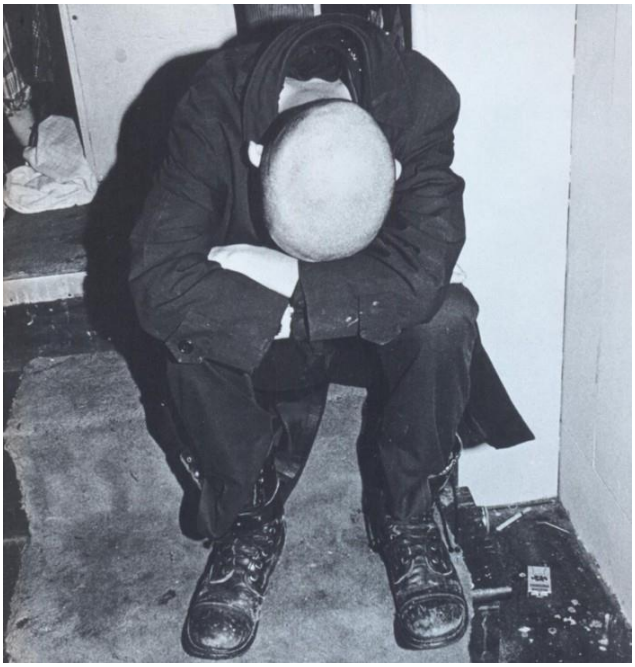
I foresee that there will be an increasing demand for bitcoin and other crypto assets in the coming years. The introduction of Central Bank Digital Currencies will certainly contribute to this. After all, one will have to work with digital currencies in wallets specifically set up for this purpose. As a result, everyone gets a crash course in digital assets and then the step to crypto assets is suddenly not very big anymore. Although in the Netherlands it is still mainly a party of retail, high net worth and family offices, I expect that more institutional parties will follow due to further strengthening of the infrastructure and a better understanding of the opportunity. Outside our borders, the first large parties are already anticipating. Now that this course has been set, I expect that within 5 years the use of crypto assets will be just as normal as the use of mobile phones. I think that bitcoin has further strengthened its position and that every pension fund board, following corporate treasury departments ^5, has at least seriously considered bitcoin as an investment.

References

Things Bitcoiners Don't Want To Hear

By Shinobi

Posted September 16, 2020



Bitcoin is suffering from an autoimmune disease right now. People have historically referred to active members in this ecosystem as "Bitcoin's white blood cells." They are now attacking Bitcoin itself, and no I am not referring to "plebs" calling out "influencers" for doing dumb shit. I am talking about the inability to confront shortcomings with layers of the system. The inability to confront substantial threats or attack surfaces that are not being worked on in terms of creating solutions and defenses.

People act like Bitcoin is invincible, preordained. It is not. And this is not to say Bitcoin will "fail" in the sense that it will die, even I think that is very unlikely. But it can lose its scalability. It can lose its characteristic of open access. It can lose its censorship resistance. Bitcoin as a system can survive while losing and gaining new characteristics. The progression of the blockchain, with the thermodynamic and probabilistic guarantee of current state, does not in and of itself guarantee these qualities that we value continue.

As long as that central quality of scarcity continues, it can absolutely lose/gain other characteristics and still maintain value through market demand. I'm going to run through two distinct areas in which this is happening at wide scale, one holding the potential for massive internal disruption and disagreement in the same way that things like Bcash played out, and the other massive potential for government corrosion of censorship resistance.

Ouch

Short Circuit With Lightning

Lightning is almost certainly not going to scale for micropayments in the long term. Lightning fees are not disconnected from the fee market for blockspace, they are derivative of them. The reason micropayments work natively on Lightning right now is because fees for blockspace are so low right now; when fees for blockspace go up that will drag fees up for Lightning payments as well. It is not economically rational to be routing payments for profit on Lightning if the eventually necessary on chain operations immediately eat up everything you have earned off chain. Fees on Lightning will increase to compensate for this. And that is just the first issue with micropayments on Lightning.

Another issue is the value of payments. Every Lightning payment, regardless of the value being routed (and remember, part of the fees on Lightning are % based, so higher value = higher revenue for routing), costs the same amount of data. It costs the same amount of CPU operations, of electricity expended, however you want to conceptualize it. Pushed extremely to the margins with the ability to profitably perform 'x' computational operations in a time period, won't you always prefer higher value transactions to maximize revenue?

And yet another issue, are the problems with too many unresolved HTLCs live in one channel at a time opening nodes up to attacks unless they limit the amount of unresolved HTLCs they will engage in at one time. This is a further introduction of scarcity in terms of opportunity cost with income. Why would I route your 1/10th of a penny microtransaction which might get me a 1/10th of a penny when I can route this other guy's 10$ payment and earn 15 cents?

These kinds of false expectations are ultimately at the root of what lead to the big block divide and the split off by Bcash. A long period played out of completely unreasonable expectations being set, and when the time finally came that they were shattered a large swath of people would or could not accept that. Now I don't think similar expectations being shattered now is going to lead to some doomsday fork or fracture (though it could), but micropayments are very important. They are in general a mechanism to shift the internet away from KYCed tagged and tracked access to services and infrastructure online. But imagine if as micropayments start to embed themselves into applications, they do so in a naive and short sighted way. They assume that Lightning will be a suitable micropayments layer natively. That is potentially a large amount of broken infrastructure when reality kicks in. How does that play out in the war of network effects? Adapt to reality vs. force reality to adapt.

We have things like LNURL Auth. That can create anonymous "micropayment credits" that can be topped up in cost effective chunks. We have alternatives like chaumian ecash tokens (which can be similarly bought in chunks to "top

up") to improve the privacy of micropayments to individual services. These would be actually independent from the on chain fee market, unlike native Lightning, and could in the long term scale to facilitate micropayments. There are even ways you can make chaumian tokens (assuming you trust the issuer to enforce this of course) atomic with native Lightning payments.

Bitcoin is in a race. There are all kinds of entities in the world that would like to stomp out censorship resistant microtransactions that create a foundation to keep an open internet alive. Ignoring long term realities because they make things more complex is wasting time and handing them a win.

It's Thermodynamics Stupid

Mining is industrial consumption of energy or people playing hobbyist in their own home. When was the last time (at least in most of the West) you heard of a major industrial consumer of electricity that wasn't a registered company? Didn't have legal identities on contracts with electricity producers? With grid operators? We are in an era of Bitcoin where exchanges and market places are being bent over backwards to comply with all the fun legacy regulation and legislation that Bitcoin itself is "natively immune" to. Why wouldn't that type of application of regulations eventually domino out to miners as well? Doesn't that threaten Bitcoin's "native immunity" to regulation?

Miners process transactions, they are what actually facilitates transfer of control of UTXOs. They are the ones who decide which UTXO operations to process or not. Miners' freedom to do whatever people will pay the highest for is your freedom to transact with censorship resistance. They are two sides of the same coin. Regulation is coming for the entire stack.

Centralized pools are how coordination dominantly occurs between individual hashrate operators. They don't just help coordinate though, they actually take custody of individual operators money and pay them out for their contributions to the pool. They custody money. They. Custody. Money. A regulatable act. There's the in to go after them; the prize is the dominant coordination mechanism for hashrate. The part of the process that decides which UTXOs operations to process or not process. The hashers facilitate that process, and pools custody their money. Therefore...pools must KYC their hashers in jurisdictions where regulations apply™.

(Aside: Solo mining just means the only way you're mining is with a massive single operation which is going to stand out like a sore thumb)

This necessitates decentralizing the operations of the pool. Both of them. It requires a decentralized solution to individual miners coordinating and each doing their own transaction selection, and it also requires a trustless way for individual miners to be paid out on chain when someone in the decentralized "pool" actually finds a block. P2Pool did this with their sharechain, but it has

massive scalability issues. Every individual miner has their own output for each "share block" directly in the Coinbase transaction. The only real way to alleviate this issue is off chain protocols to accomplish the same trust guarantees without explicitly including an on chain UTXO for each hasher. Otherwise the effect of massive Coinbase TXes both has externalities to the non-mining fee market by taking up scarce blockspace, and a cost is incurred by individual miners having to manage small individual outputs that may approach dust levels.

Even solving these issues does not deal with the root of the problem in this layer of the stack: energy consumption. I call back to the first paragraph relating to this issue. Where do you see industrial level power consumption without KYC? Without knowing whose door to knock on? Who is legally accountable? This comes down to energy at the root. The life force. The meme magic that is rooted in thermodynamics and not you intellectually masturbating in your head. Anyone who knows what they are talking about knows the vast majority of competitive mining equipment is 240 volt. Welcome to the realm of, on a personal level, making the choice between mining and your clothes dryer. Welcome to getting around making that choice between mining and laundry requiring explicit conversations with the utility company. Paperwork. Red tape. Signals. Red flags. The only way to really get around this type of default "registry" governments can look for is at home off the grid energy production. Residentially. With all kinds of restrictions (legal and practical) that a warehouse with industrial lines doesn't run into. And the minute you consume the available non-suspicious quota of power by giving up your washer and dryer, you can't scale your mining operation beyond that without undetected off grid power generation.

You can't escape the fingerprints of thermodynamics. This space is shifting "legit" and corporate. It's meming about bucking the regulators, the governments, but really on a micro level starting to kiss their asses and cater to it. Anyone reading this know the logistics of an illegal cannabis grow op? The power concerns? The infrared foot print? Disguising that? Recognizing when authorities are looking for such fingerprints? To the few who do, can you imagine the extra complications on top of that baseline that Bitcoin mining entails? The noise? The exponentially larger energy draw at scale? The extra heat? This is really in a worst case scenario an outright illegal market like growing drugs that requires in depth and serious scientific research to scale and operate that infrastructure undetected...how do you attract mindshare here exactly? How is this not career and reputational suicide in the mainstream?

Solve the coordination problem, solve the trustless payout for hashes problem, solve all of that: you still have the thermodynamic problem. That last problem at the foundation is a doozy. How do you source electricity at scale

without standing out in paperwork, on licenses, in redtape that flows through government? How do you obscure the noise foot print of a large mining operation? The thermal foot print to helicopters buzzing around overhead with infrared cameras? In a worst case scenario, a large enough percentage of miners need to be able to operate like this in order to make it unprofitable for "legitimate" miners to outright orphan blocks with "verboten transactions" in them. Otherwise kiss censorship resistance goodbye folks. It's thermodynamics.

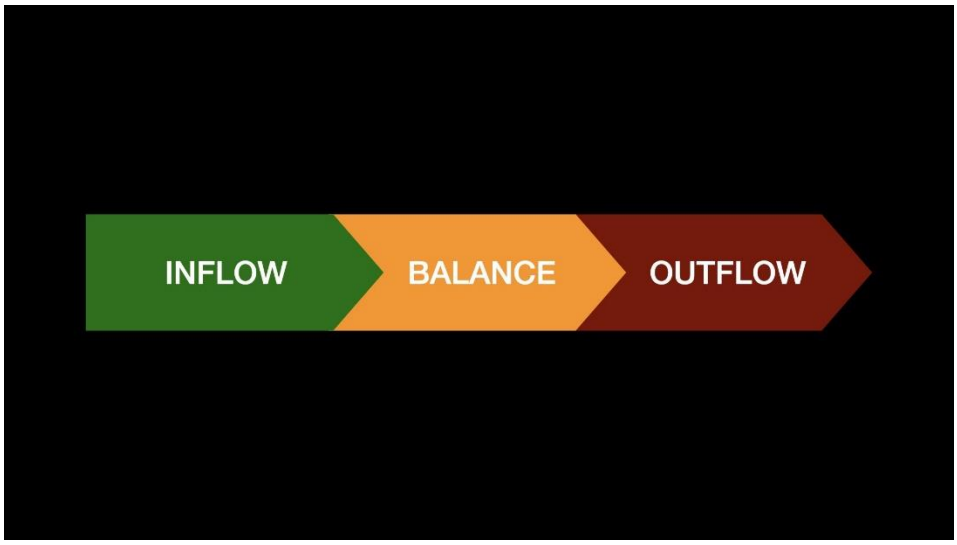
Tweet Thread: Chad Money

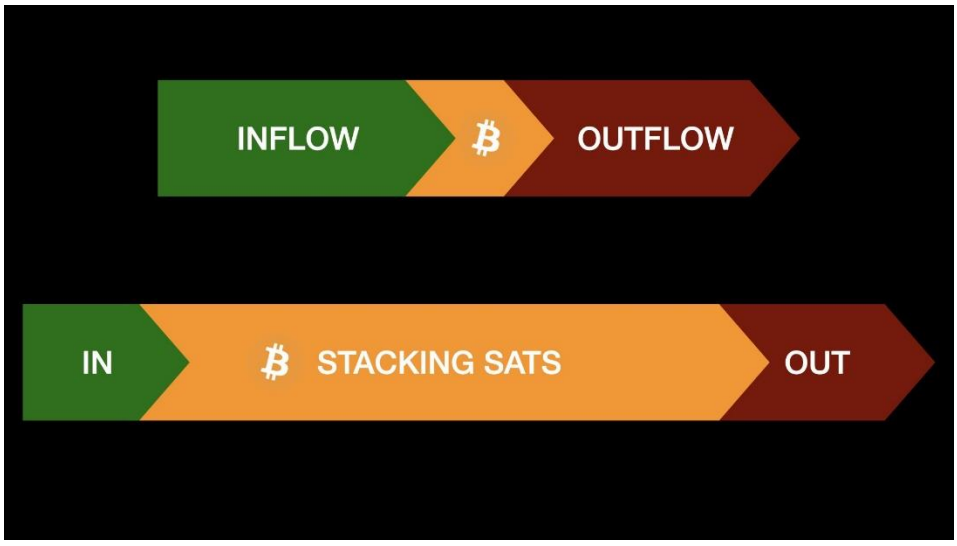
By Gigi

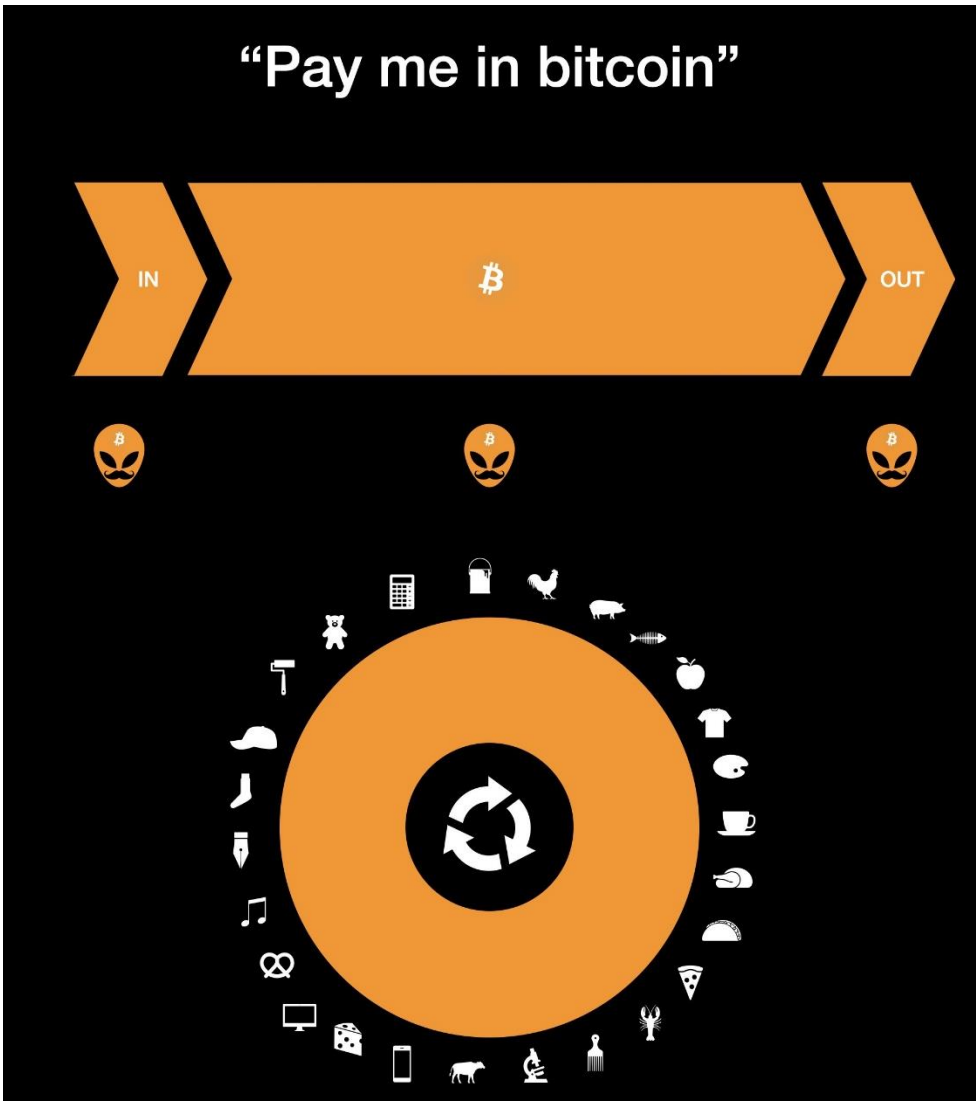
Posted September 19, 2020

1/ Now that the Chad money is coming in, let's look at what moving to a bitcoin-denominated balance sheet might mean.

On inflows, outflows, balance sheets, and how a circular orange future might resolve the points of contention in Bitcoin.

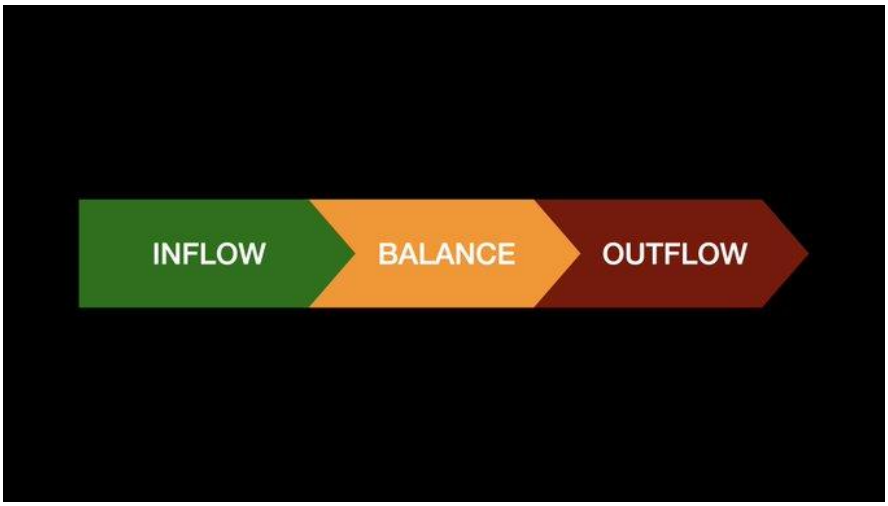




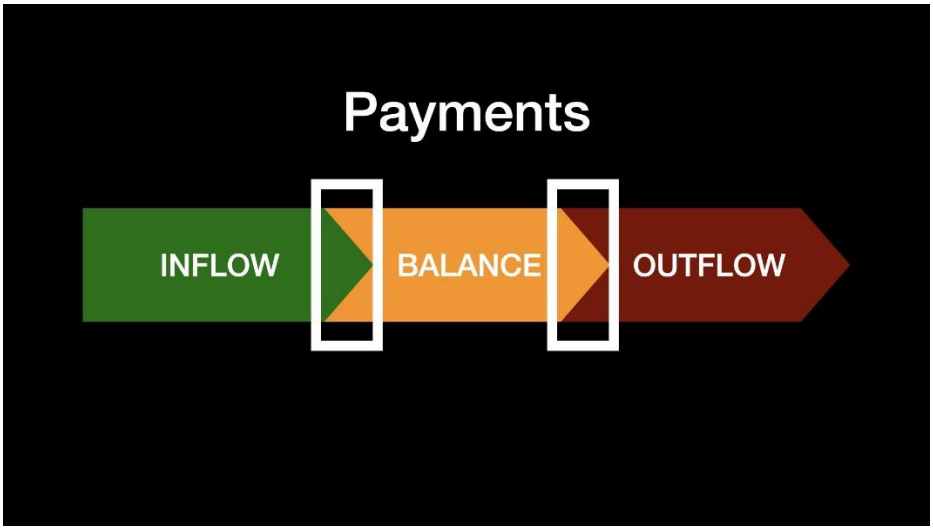


2/ In essence, every economic actor needs to have an economic inflow to survive. This is true for individuals, companies, and even states.

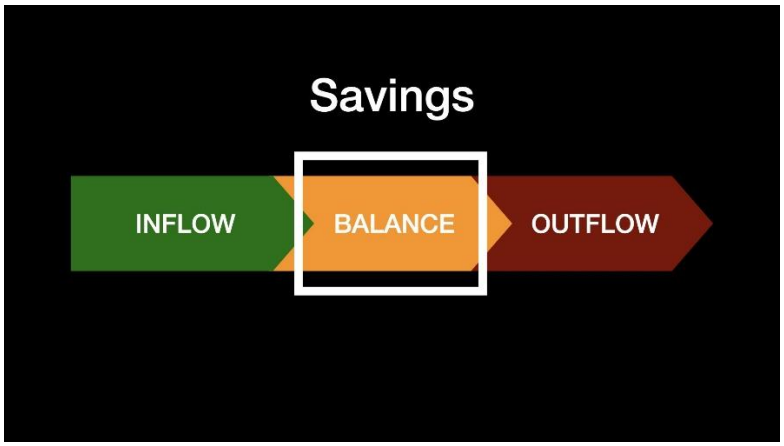
A healthy actor has more inflow than outflow, resulting in a positive balance. Spending is necessary for survival or growth.



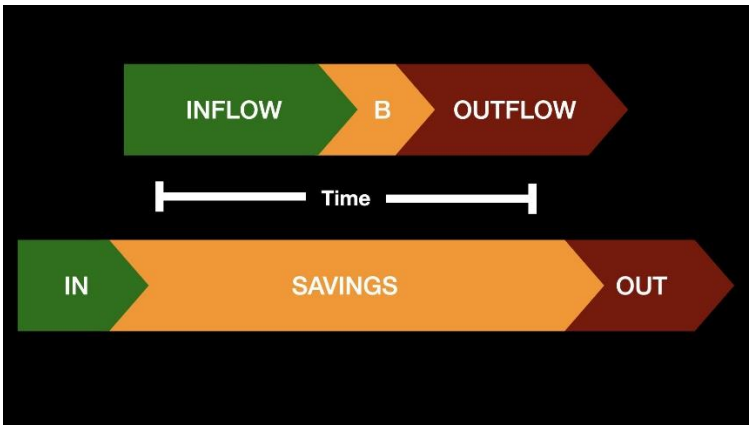
3/ Most economic actors sell goods and services to generate inflow. Sooner or later, what they earn is spent again on other goods and services. A payment is simply a moment in time where one is given what is due for goods or services.



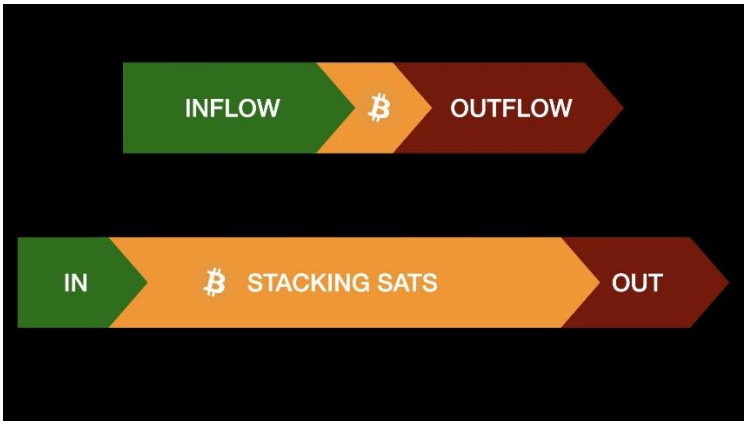
4/ Because the future is uncertain, you might want to hold some cash on your balance sheet. A better time to spend the money might arise, or you might need the money more than you need it now. You put something aside for a rainy day. These are your savings.



5/ Saving is simply the act of delaying spending. In the same way that you might want to save your dessert in order to savor it even more at a later point, you might want to save your money so you can put it to better use in the future.

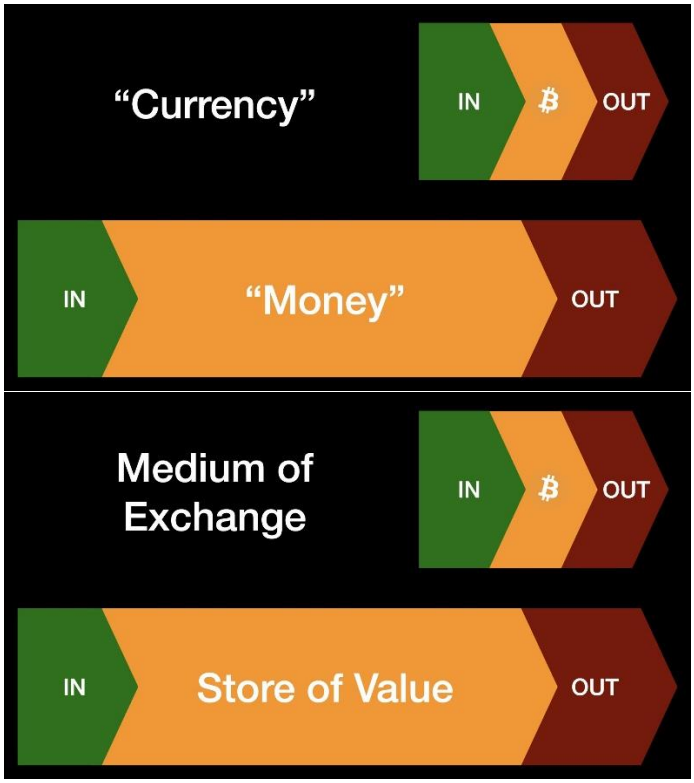


6/ In Bitcoin, this distinction is especially relevant because there continues to be tension around what Bitcoin is and what it is good for. Due to its resistance to censorship, confiscation, and inflation, bitcoin is useful for both payments and savings.



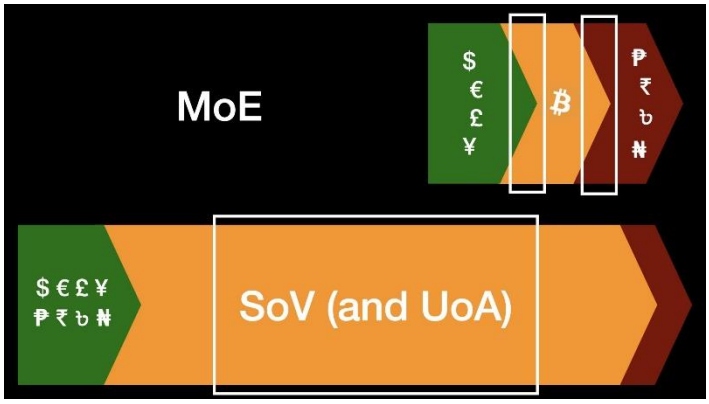
7/ Those who focus on the payments side of things often speak of "(crypto)currency" and emphasize the "medium of exchange" aspect.

Those who focus on the savings side of things speak of "money" and emphasize the "store of value" aspect.



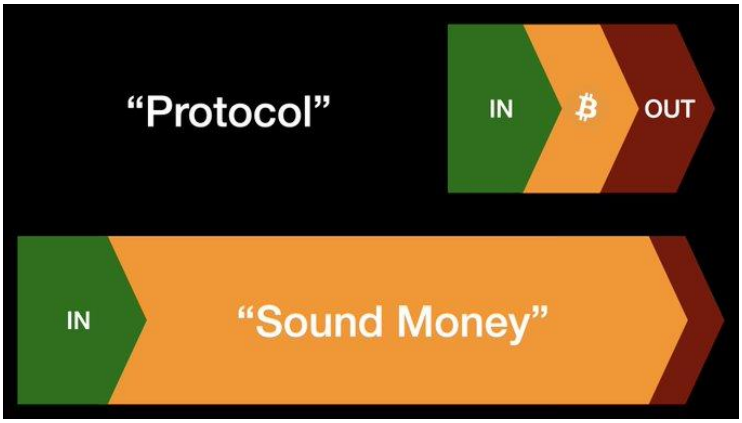
8/ The MoE crowd is mostly concerned about making exchange and payments easier. Bitcoin is seen as a tool to improve commerce. Focus: inflows and outflows.

The SoV crowd is mostly concerned about security and certainty, e.g. monetary policy and auditability. Focus: balance.

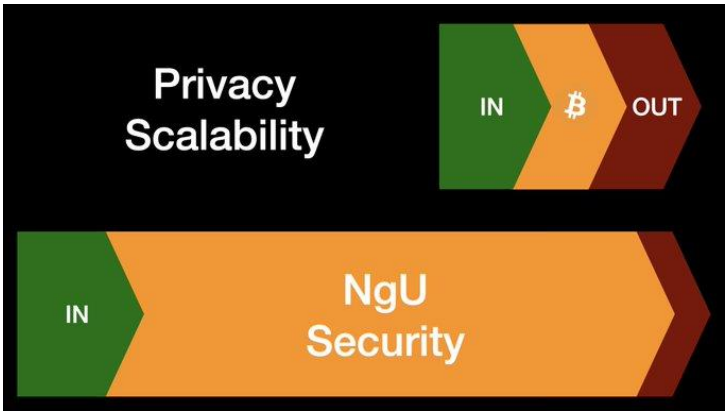


9/ Yes, Bitcoin is a protocol for value transfer. From this point of view, the value of BTC does not matter. Value in -> BTC -> value out.

But Bitcoin is also the soundest money we ever had. The realization and appreciation of this fact will be reflected in its buying power.

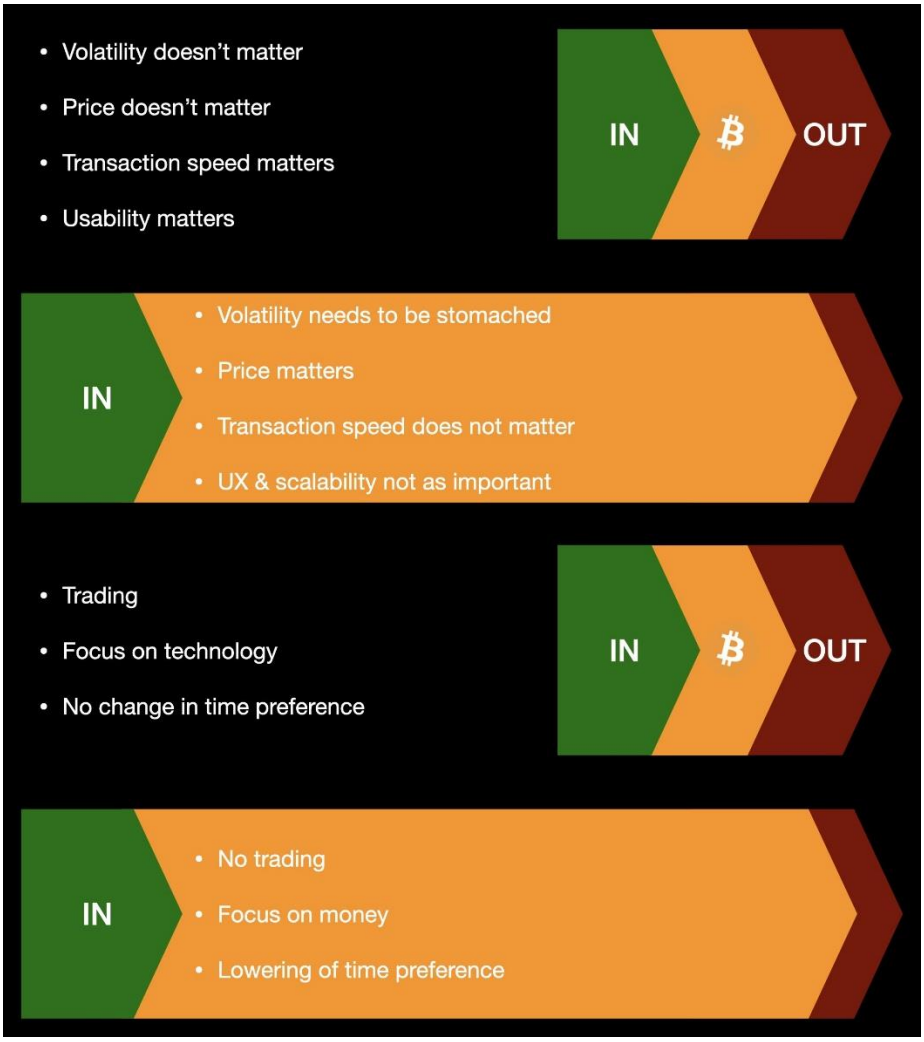


10/ Different focal points highlight different concerns. For the first, these concerns are around privacy and scalability. For the second, they are security and valuation (reflected in NgU).



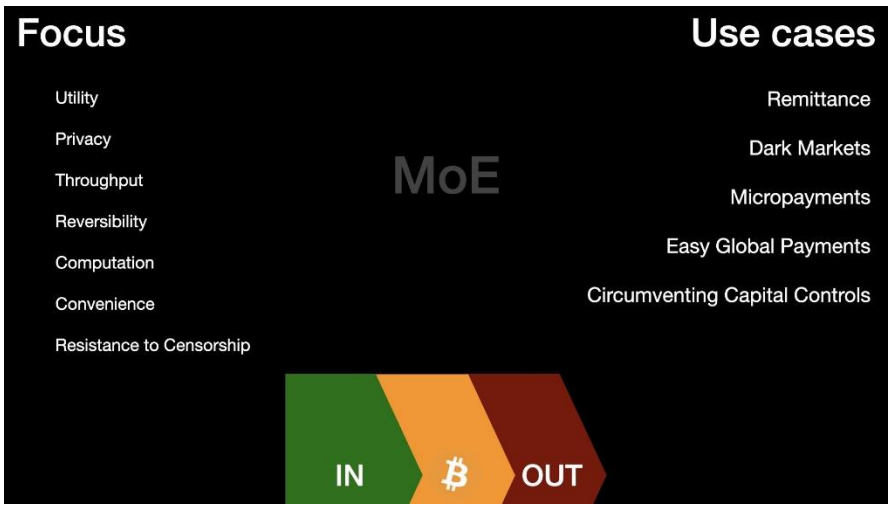
11/ No bitcoin balance? Volatility and price don't matter! Bitcoin is technology that needs to be improved.

Large bitcoin balance? Transaction speeds, UX, and scalability don't matter that much! Bitcoin is sound money and could soon ossify.



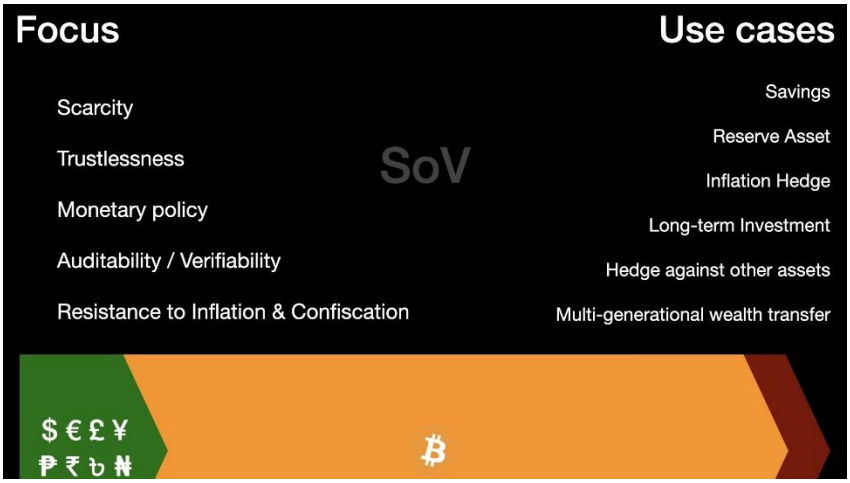
12/ Medium of Exchange: remittance payments, dark markets, micropayments, cross-border payments, evading capital controls.

Focus on utility, privacy, throughput, and censorship-resistance.

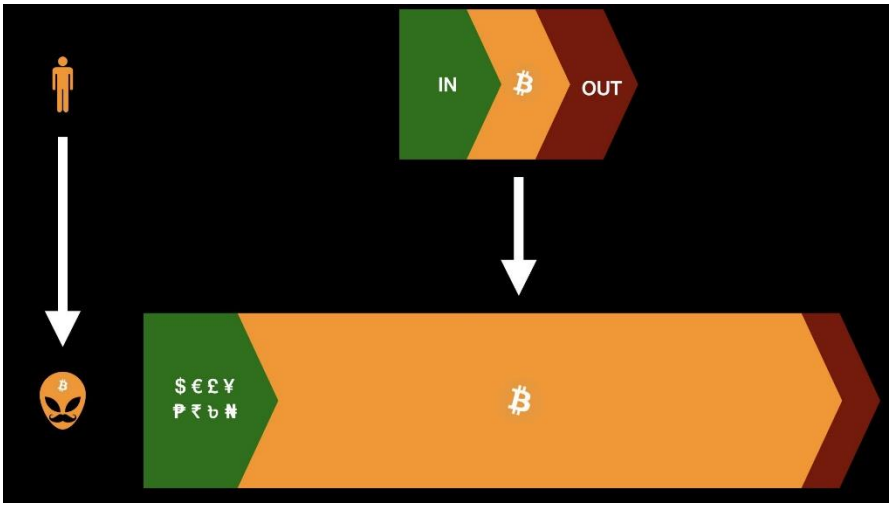


13/ Store of Value: savings, (personal or company) reserve asset, inflation hedge, long-term investment, hedge.

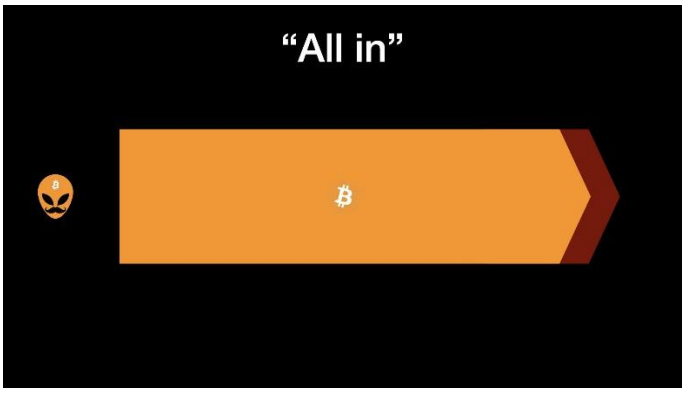
Focus on scarcity, trustlessness, monetary policy, auditability, verifiability, resistance to inflation & confiscation.



14/ Currently, it seems to me that Bitcoin is a one-way street. Many people had to use bitcoin as a medium of exchange for one reason or another, fell down the rabbit hole, and are now bitcoiners that use it to save for the long term.



15/ A rising number of bitcoiners are all in, forcing them to spend some of their bitcoin. If 100% of your inflow is in bitcoin (or: no inflow, 100% BTC balance), you will have to spend sats on food, shelter, and other necessities. No matter how much you don't want to.



16/ As more and more bitcoiners prefer to receive payments in bitcoin, more and more economic flows will be bitcoin-based. In other words: bitcoiners will be willing to part with their sats to pay other bitcoiners for goods and services. This is already happening (h/t @ctdl21).

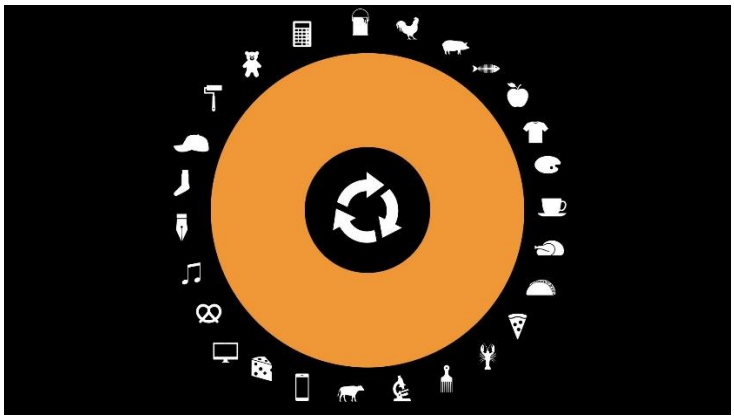
17/ While still small, this circular economy is bound to grow. Everyone who ever did cross-border fiat payments knows how much of a hassle it can be. Bitcoin is frictionless, especially when going from bitcoiner to bitcoiner. Discounts of 21% will help too.

18/ Zooming out, the economy is still operating on a fiat standard. However, the number of individuals and companies that move towards a bitcoin standard is growing.

More HODL = more and larger bitcoin balance sheets. More AutoDCA = more fiat inflow / less fiat outflow.

19/ Earning and spending bitcoin is a natural thing once you drop fiat and bitcoin becomes the money of your choice. This is where SoV meets MoE and - once the orange circle is big enough - will eventually become UoA.

20/ As more people gravitate towards Bitcoin, more goods and services will gravitate towards a bitcoin economy. The Bitcoin Standard is coming, it just won't happen overnight. It will happen one by one, individual by individual, company by company. Balance sheet by balance sheet.



21/ When all is said and done, bitcoin will be taken for granted just like electricity and the internet is today. What remains in the background is a beautiful orange circle of interlocking incentives. Settling transactions, block by block.

FIN/ Thanks to @michael_saylor for being such a Chad, and thanks to @pierre_rochard for letting me expand on this idea (and making me sell all my chairs). You can find Pierre's presentation on Google Slides.

Why we may fail Lightning

By Antoine Riard

Posted September 28, 2020

A number of years have passed since I started contributing to Bitcoin protocol development. First on Rust-Lightning, then also on Bitcoin Core. I've been lucky to work on these projects full-time for the previous year, and it is a good opportunity to reflect on how Bitcoin is doing thus far.

It is a frenzied and noisy environment, and at times you need to reflect and evaluate your roadmap for future Bitcoin contributions. Otherwise, you will quickly get lost and finish each day without making the desired progress.

Let's get started by honestly looking into the Lightning infrastructure. Then diving into the exciting fringes of Bitcoin and what the different Bitcoin tribes stand for today. It might help us cast a light on the perpetual challenge of bringing Bitcoin to the masses.

The State of the Lightning Network

Lightning is considered as the flagship of Bitcoin innovation and for good reason. A few years ago it was just a wild dream on a whiteboard, and now you can interact with thousands of LN users all around the world without caring about bank clearing hours or segregated payment networks.

That said, let's dig into the true state of its infrastructure.

Lightning is binding to a blockchain-as-a-judge model. Namely, a set of transactions binding a contract between participants. In the case of misbehavior the blockchain serves as a judge. The case will be adjudged using the plaintiff's cryptographic proofs. This is a completely different model than the first layer one.

On the base layer, coalitions of full-nodes will protect your coins against miners misbehaving, assuming you're sharing the same consensus rules. On off-chain layers, other peers don't care about your counterparty misbehaving. The double spend problem within your channel is a private matter.

This model presents a new class of attacks on your Lightning node. Your counterparty may try to burn in fees your channel balance. Or exploit the public nature of the base layer to block your channel close attempts. Or leverage malleability to break the contract semantics. Or directly attack your full-node associated with your Lightning one.

Further, your fee-estimator also becomes a critical component for the safety of your funds. Holistic network behaviors like mass channel closing could break your security. It should be also remembered that Lightning keys are hot, with all the challenges that presents.

Sadly most of the attack vectors laid out above are practical today. A subset of them are inter-dependencies with the base layer and need work at this level to be mitigated.

We should remind that Bitcoin protocols won't be immune to DAO-like failures by the holy spirit of Satoshi. At this point, onboarding millions of users on the network is most likely to produce one of two outcomes.

Either, the whole network burns in flight due to a number of exploited securities issues, greatly impacting the long term public confidence in the platform's trustworthiness. Or after the first wave of serious attacks, network operators double down on requiring strong identification before any channel opening, using the existing public key infrastructure. This grandly leads to centralization.

None of these scenarios is appealing. Honestly, we would all be heartbroken if we were to end there after all our hard efforts.

On the privacy side, things looks better on paper. The fact is we have to take a cross-layer approach, and it might not be as good as expected. For now, Lightning transaction format makes onchain channel openings obvious. Balances are leaked for routing peers which opens the door to traffic observance. A dearth of LSPs to initially peer with will compromise privacy. Receiver-confidentiality is still a work in progress.

Lightning privacy is definitively an area that requires more research before making any strong assertions on the level of privacy provided.

Scalability presents its own concerns. The size of the UTXO set is going to be a bottleneck at some point. Cheap access to onchain resources isn't guaranteed in the long-term. The prospect of malicious congestion and spamming hasn't been addressed yet. Routing tables will likely be too large for mobile clients, hence they will need to delegate, decreasing their privacy. Removing the onliness requirement for payments is still being worked on.

I am very confident that these challenges will be addressed in the long term but in the short term they require considerable technological efforts. Step by step, we will make Lightning a robust, efficient, trustworthy financial platform.

If you want to help us in these tasks and get involved with one of the brightest engineering communities, this is the right time to join!

The nascent Stack of Bitcoin Contract Protocols

That said, narrowing exclusively Bitcoin innovations to Lightning, you will miss the forest for the trees. Other protocols that are being developed at the margins of Bitcoin are fascinating. As a side-note, let's define a contract protocol as a wider scope rather than the off-chain one as some of the steps can be played on-chain and thus even in optimistic scenarios.

Vaults are the next-step in key management. By combining multisignature with timelocks they make coin custodial solutions far safer while enabling more fine-grained withdrawal operations. Future refinements will serve as building blocks for inheritance schemes or multi-stakeholder management.

Discreet Log Contract are leading the way in bringing oracles in Bitcoin. By leveraging elliptic curve linearity they make the betting contract unobservable by the oracle provider, only known by the participants posting collateral. They radically reduce the incentive to maliciously misreport the outcome. A future iteration will be to distribute them directly on Lightning as a new class of packets. One use-case example is to let anyone hedge against their local currency devaluing.

CoinSwap is the next iteration in privacy-technology. By building on atomic swaps, they hide the exchange of coins from any blockchain observer. Their usage could become massive if they're used to context-switch coins between different privacy domains (e.g Lightning channels to cold storage).

Payment Pools are still at the whiteboard phase but are promising in their attempt to combine confidentiality, scalability and cost-effectiveness for future massive usage of off-chain protocols.

What should not be underestimated is how these protocols are generating a measurable feedback loop that is improving the base layer.

Off-chain or contracts protocols, require stronger blockchain assurances including protection from certain network failures, whether they be accidental or malicious. As routing nodes earn fees by keeping their coins locked in channels they lose money when transactions get stuck in mempools, and thus they are incentivized to pay more compelling fees. By breaking a number of deanonymization heuristics these new protocols enhance coin fungibility.

In addition, by providing access to financial services to parts of the world devoid of alternatives, they grow the Bitcoin user base, in an ever more geographically distributed way.

It's likely that each unit of usage of higher layer protocols will bring non-linear growth of value for the base layer. Layering private contracts on the top of the public constitution will make the latter stronger.

The Bitcoin contract protocols stack is still in its infancy. We still have a number of frontiers to approach by combining applied cryptography, distributed systems, financial engineering, law practice and game-theory.

In the future, this stack of contract protocols will gradually form the backbone of more Bitcoin-powered economies. They need to be matured sensibly with lessons learned from previous iterations.

The Tribes of the Bitcoin Stack

What might end up hindering our attempts to build a stronger Lightning and Bitcoin isn't any particular technical difficulty. That is something we will address with creativity, craftiness and sweat as per usual. When we look back at Bitcoin's short yet intense history perhaps we should be more concerned with the risks presented from community disagreements.

Said differently, the discrepancy between the public excitement for Lightning, and the state of infrastructure, sounds like a cultural misalignment.

If you have been to both a Bitcoin and a Lightning conference it is easy to observe divergent communities. Bitcoin conferences often focus on deep technical talks, prioritizing security and protocol engineering, and are attended by seasoned Internet citizens, hackers of all sorts and civil libertarians. After endless waves of scams, they are naturally skeptical but intellectual debates remain open and honest.

On the other side the Lightning crowds feel different. Younger for sure, more startup minded and with talks focused on user experience and product design. Energy is flowing through the air and you have a thousand dazzling Lapps to play with. You can taste the Silicon-Valley influence, and easily recall that some participants were happily promoting their ICOs a few years ago. It is flashier too, the Lightning crowd does like garish yellow and bright purple!

That's a rough sketch, I guess a lot of us are belonging to these two tribes, at least I would confess so myself.

Let's sketch these two tribes further.

The LWN Tribe

We have the OG tribe, they built the Bitcoin of today. Their determination, craftsmanship, intellectual rigor and uncompromising ethics have built and saved the system from both technical and social attacks over the years.

A good chunk of them are sharing a strong Unix background and that's the best school of sound software engineering. You can appreciate the kinship

between the major Internet protocols (TCP/IP) and the Bitcoin ones. They both strive for simplicity.

It is displaying the strengths of the wider open source movement but we should also explore its weaknesses. Our kernels and compilers consist of millions of code lines, hindering their clear prehension. Our chips are closed and a seemingly permanent security disaster. And we are too few considering the Internet as a house for the curious mind.

That is not to say the hard work of the previous years has been wasted nor that we should give up our harshly conquered spaces of freedom. But we should have a clear understanding of the environment that is changing around us.

Bitcoin fungibility is under attack and it's going to worsen. Network-level disruptions should be anticipated. Block rewards are going to dwindle and fees will have to pay for a consistent network hash rate. Clumsily written codebases will hinder attempts to pass down hard earned knowledge to younger Bitcoiners. And that is just a few of the challenges ahead.

After you, someone needs to come in turn running the full-node. Lightning and contract protocols are likely our best shots to continue the Bitcoin history in the brightest way.

The Product Hunt Tribe

Then we have the more startup-like tribe. They are talented at listening to users' needs, executing and serving those users. They make complexity intelligible by wrapping it inside attractive products. It is they who build the gateway to connect to the outside world which allows liquidity to flow in. All oiled with burn rate, ARR and churn.

But it is even easier to look at the failures of the startup movement. Funding cycles, startup bubbles, chasing extreme growth and living in a constant state of urgency are good ingredients for delivering new digital products. But it is not a healthy environment when your main KPI should be optimizing the financial autonomy of your users.

Admittedly, Bitcoin businesses are unique: the typical startup playbook doesn't apply here. Automatic updates and trust-minimized financial software don't merge well. Selling a security product and storing user data is quite an oxymoron. Offering nodes in the cloud whilst promising total financial control to your users is just a lie.

If you require your users to trust you in any way, just say it plainly and bear the responsibility. Otherwise you are deceiving when you use terms like

privacy and trust-minimization. Be ready to be scrutinized with the same rigor as when we are verifying our protocols.

It's a worthy goal to reduce information asymmetries, and we should aim for Bitcoin users to allocate their funds and time with the best knowledge available.

Further, the current digital world has been built with the image of the passive user in mind. In Bitcoin that translates into a user who can't rely on himself to manage his keys, won't be able to afford the fees for usage and who is too narrow-minded to care about the behavior of the system.

I dare you to do better. One should not forget that Bitcoin is first and foremost a tool for self-determination. If people fail to understand that, you're the teacher to blame.

The truth is you have real humans on the other side who strongly desire autonomy. One of the most magical experiences of Bitcoin is hanging out at meetups and observing people from all ages and backgrounds eager to learn.

There is no fatality. If keys are too complex to handle, then we should roll out better designed key management solutions. If onchain or off-chain fees are too high, we should craft better optimized protocols. And if the learning curve is too steep, we should produce better educational content.

Failing to keep Lightning & consorts decentralized might be all-right for base layer stability. But there is a non-zero risk of it backfiring. A decade from now, if a good chunk of the coin supply is allocated in channels operated by centralized services, even distributed base layer operators won't have much economical weight in the bargain to conserve consensus rules.

We may wake up one morning and see them being broken in our plain-sight just as Bitcoin history warned us.

Beyond the Tribes, our Living Community

Bitcoin is a unique experience, and if we want to pursue it forward we have to draw bridges between the divergent tribes. We need to learn all we can from each of them. But sincerely we shouldn't bind to their past failures or accept outdated models.

Due to personal ignorance I'm only highlighting two of the Bitcoin tribes and their universes. A global picture would include a thousand of others like the Chinese mining community or the Venezuelan meshnet community. There is a Babel-like diversity in Bitcoin and that's a force.

We may spend more time fighting each other on social media on insignificant topics instead of solving common problems around a beer at a

conference. And we might live in a more fragmented world, trapped within borders, and without access to those high bandwidth events. It's a first-class necessity to maintain good communication interfaces between all stakeholders.

We are all citizens of this Bitcoin Commonwealth. At least the secp256k1 curve is the same between BitDevs NYC, Berlin's Room 77, the Dakar Bitcoin Developers meetup and the Bitcoin emBassy TLV.

What Bitcoin do you want to see ?

Bitcoin presents a fantastic game theory equation to align the long term interests of all of its players. Understanding and respecting its internal rules are the surest path to maximize wealth creation for everyone.

But if we state the problem clearly, if we onboard millions of users in the same way as the Internet, we are more likely to break Bitcoin than anything else.

There is a fear about Bitcoin's future that it will not achieve as much as the Internet but honestly what we should fear is not doing better than the Internet.

We aren't playing a zero-sum game. But we may be worried about some minority of its players, driven by the fear of missing opportunities, tapping into the wider majority's fear of never scaling to drive them against its own interests. Focusing on a adamant definition of onboarding as the only way forward, breaking the rules, giving up on past principles and thus destroying the long term value of Bitcoin.

Looking forward, we can actively choose to onboard new Bitcoin citizens in our own sustainable terms. In a way which preserves the properties which have made the system successful so far. At our own pace, as we have done so far, servicing the human layer.

A Bitcoin onboarding where you rely on an exhaustive set of resources in your native language to get started. Where you have a great network of local meetups to learn from. Where you have a wide set of easy-to-use tools to protect your digital estate. Where you can positively interact with businesses on your own conditions. Where you're always advancing forward on your personal quest for greater self-determination.

Choosing this way, we're all going to be winners. Remind that empowered users will have a stronger economic activity. At term this means more flourishing Bitcoin business and thriving economies.

Zooming out, we should always remind ourselves that Bitcoin has its own temporality. Despite floods and riots, the halving did happen. Obviously we

are on the edge of a revolution. But coming from a continent which has experienced a bunch of them, the true story with revolutions is that most of the time they fail.

As social and cultural changes are slow to unravel, it is tempting to lose patience and burn to the ground the foundations that have been laid out in a desperate attempt to fasten the process. For Bitcoin to turn into its full-strength, it will take at least a generation, and we have to be steady with this outgrowth.

Always remember that in days of doubts, we have the choice between comfort and complacency, or freedom and adventure. We can achieve a walled garden or a free jungle.

Which one are you going to build?

Hacking Forward

Welcome those words with prudence. Don't take them for granted. Make your own opinion. Then act on your own definition of Bitcoin. As a friendly whisper, you've always been free to contribute.

Meanwhile, as talk is cheaper than code, here is my promised personal roadmap. It is mostly continuing what I have been working on thus far:

- On the Bitcoin Core side, there are a thousand interesting things happening. Personally I will be working on improving transaction relay and fee models for off-chain protocols, AltNet, to make it easier to deploy alternative transport communications and hopefully addressing some of the off-chain security issues I previously referred to. Contributing to the Bitcoin Core review process with a focus on refactoring and code modularity changes, as the health of the Core codebase is critical in the long term.
- On the Rust-Lightning side, refining our cutting-edge features. Adding more test coverage and auditing the critical parts. Onboarding our new contributors. Moving towards deployment. On top of it scratching the wider Lightning Development Kit ecosystem with the awesome Square Crypto team.
- On a more research-oriented side, contributing to the Discreet Log Contract specification as the setting up of reliable oracles will be such an exciting breakthrough.

Thanks to the reviewers, thanks to Chaincode Labs for the last 12 months, thanks to John Pfeffer for his confidence and thanks to my fellow Bitcoin hackers, from whom I'm learning so much every day.

Have fun on this crazy Bitcoin ride! -Antoine

Disclaimer:

WORDS

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

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

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

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

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

DYOR | BTFD | HODL

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

Read **WORDS**

- @_joerodgers