
WORDS
October 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.

2-of-3 inputs using Pay-to-Taproot

By Murch

Posted August 18, 2020

The Bitcoin community has been abuzz for a few years about bringing Schnorr signatures to Bitcoin. Since then, the idea has evolved into three formal Bitcoin Improvement Proposals: 'BIP340 — Schnorr Signatures for secp256k1', 'BIP341 — Taproot: SegWit version 1 spending rules', and 'BIP342 — Validation of Taproot Scripts'. Respectively, they define a standard for Schnorr signatures in Bitcoin, introduce the Taproot construction, and formalize the new Script v1 instruction set. Taproot also iterates on the previous proposal of Merklized Alternative Script Trees (MAST).

There are two ways of spending a ***pay-to-taproot*** (P2TR) output. The first way is called ***key path spending.*** P2TR funds are locked to a single public key with the full output script amounting to _' OP_CHECKSIG'._ This script is satisfied by providing a Schnorr signature of the corresponding private key. The key path is the default spending path. It is used in single-sig and collaborative multi-party spending.

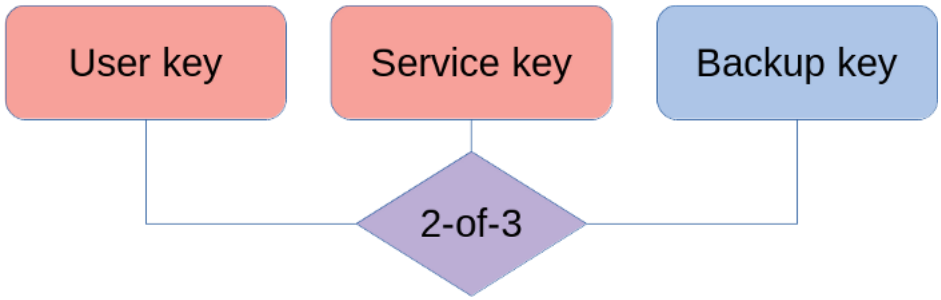
Under the hood, the public key is a composition of an ***inner key*** and the Merkle root of a Taproot tree (the inner key is ***tweaked*** with the Merkle root). The inner key can optionally be a composite itself, for example multiple public keys aggregated via the MuSig scheme. These compositions are possible due to Schnorr signatures being linear.

The second way of spending a P2TR output uses one of the Taproot leaves. We call this ***script path spending.*** First, the existence of the leaf needs to be proven which is done by revealing the inner key, the Merkle path to the Taproot leaf, and the script encoded in the leaf. Then, the spending conditions of the leaf's script are fulfilled.

The remainder of this article explores the input costs of 2-of-3 multisig Taproot constructions. Some familiarity with the details of the proposals is helpful. Check out the Taproot overview and the excellent summary of the three BIPs by the Bitcoin Optech Group if you are looking to refresh the details.

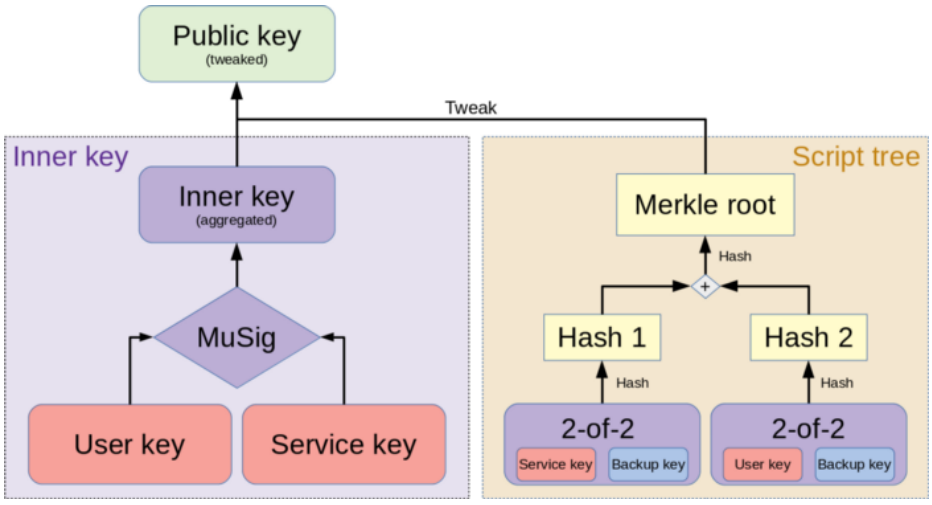
The multisig user story

We are looking at a wallet construction using three keys held by two or three parties. The first key is held by the user, the second key is held by the service provider, and the third key is a backup key either held by the user or a key recovery service. We are assuming that the first two keys are hot and can be used in an interactive signing scheme as employed by MuSig. The backup key may be held cold e.g. on an air-gapped system in which case interactive signing should be avoided.



2-of-3 multisig with two hot keys and one (optionally) cold key

Classically, a 2-of-3 multisig address is constructed in the form of a ***pay-to-scripthash (P2SH)*** output of the form _'2 3 OP_CHECKMULTISIG'._ This construction can logically be expressed as '(A ∧ B) ∨(A ∧ C) ∨(B ∧ C)' which could also be thought of as "one of three 2-of-2 multisig scripts". The latter translates nicely to Taproot: we can encode the preferred condition of spending with the user and the service key (the two hot keys) in an aggregated pubkey for the key path, and put the two spending conditions using the backup key in leaves of the Taproot tree. Two variants are explored: one where the backup key is capable of participating in the interactive MuSig signing scheme, another that falls back to a simpler multisig scheme where signing is non-interactive e.g. because the backup key is air-gapped and the multiple roundtrips required for MuSig are inconvenient.



The most likely spending option with the two hot keys is encoded as an aggregated key in the key path. The two backup spending options are put into leaves of the script tree.

Key path spending costs

In the general case, all parties agree on a course of action and collaborate to use the key path. This is the most cost-effective way to spend a P2TR output and allows multiparty spenders (and other complex spending conditions) to be indistinguishable from single-sig spenders.

Costs of key path input

An input commits to a specific *unspent transaction output (UTXO)* which is defined by the transaction that created it and the position in that transaction's output list. The UTXO entry provides the spending conditions to be satisfied by the spender. An *nSequence* field allows encoding replaceability, and the witness provides the spender's authentication. In the case of the key path this is a single Schnorr signature which in some cases may actually consist of multiple aggregated signatures.

* outpoint (txid:vout): 32 vB+4 vB
* scriptSig size: 1 vB
* nSequence: 4 vB
* count witness items: 1 WU
* witness item size: 1 WU
* signature: 64 WU

32+4+1+4+(1+1+64)/4 = 57.5 vB

Control Blocks

When a fallback to the backup key is necessary, the existence of the Taproot tree must be revealed. If there is only a single leaf, the spender provides only the inner key. Tweaking the inner key with the hashed leaf results in the public key. In sum, the data necessary to prove the existence of a script path is called the *control block*.

Depth 0 control block

* Length of control block: 1 WU
* Header byte (script version, sign of output key): 1 WU
* Inner key: 32 WU

1+1+32 = 34 WU

In case of two leaves, additionally the first hashing partner for the Merkle path must be revealed:

Depth 1 control block

* Length of control block: 1 WU
* Header byte: 1 WU
* Inner key of root key: 32 WU
* Hashing partner in tree: 32 WU

1+ 1+ 32 + 32 = 66 WU

Script path spending cost

The below costs are in addition to the above costs of spending via the key path.

Script path spend assuming 2-of-2 MuSig leaf (hot backup key)

When the backup key is on a networked system, e.g. an HSM, and can participate in a multi-roundtrip signing process, we can make use of MuSig to aggregate the two public keys.

* script size: 1 WU
* script " OP_CHECKSIG": 33 WU+1 WU * Depth 1 Control block: 66 WU

57.5+(1+34+66)/4 = 82.75 vB

Construction with 2-of-2 OP_CHECKSIG (cold backup key, no MuSig)

In the case that the backup key is offline and a human would have to make multiple trips employing USB sticks or QR codes, saving roundtrips may take precedence over saving a few bytes. Instead of an aggregated public key, we use a non-interactive multisig construction.

* second signature: 1 WU+64 WU
* script size: 1 WU
* script " OP_CHECKSIGVERIFY OP_CHECKSIG" 33+1+33+1=68 WU * Depth 1 Control block: 66 WU

57.5+(1+64+1+68+66)/4 = 107.5 vB

Discarded approach: single leaf with 2-of-3 script

It turns out that a single 2-of-3 leaf in lieu of the two 2-of-2 leaves is both more costly and less private.

* +2nd sig: 1+64 WU
* +1 empty witness item: 2 WU
* Length of script: 1 WU
* Script " OP_CHECKSIG OP_CHECKSIGADD OP_CHECKSIGADD 2 OP_EQUAL": 33+1+33+1+33+1+2=104 WU * Depth 0 Control block: 34 WU

57.5+(1+64+2+1+104+34)/4 = 109 vB

Conclusion

Input	Native Segwit	Taproot (P2TR)		
		key path	script path	
Single-sig	68.5 vB P2WPKH	57.5 vB	–	–
2-of-3	104.5 vB P2WSH		82.75 vB MuSig leaf	107.5 vB 2-of-2 leaf

Output	Native Segwit	Taproot (P2TR)
Single-sig	31 B P2WPKH	43 B
2-of-3	43 B P2WSH	

created by @murchandamus

Upper bound of input and output sizes for single-sig and 2-of-3 multisig.

The described 2-of-3 multisig scheme achieves input sizes of 57.5 vbytes for a key path spend, 82.75 vbytes for the leaves using a hot backup key, and 107.5 vbytes for non-interactive backup spends. This results in a fee reduction by 45% for 2-of-3 inputs when switching from P2WSH to P2TR spending. In the uncommon case of a recovery transaction, the cost is negligibly increased for cold keys. Single-sig users are also incentivized to switch to P2TR as they save 11 vbytes on each input — the output cost is externalized on the sender.

Thanks to Gloria Wang.

Thinking Beyond BitMEX: DLCs

By Shinobi

Posted October 1, 2020

Well, firstly I want to say that as of right now the official BitMEX announcement is effectively "We disagree Mr. Government, and intend to fight your charges. For now we will continue normal operations."

Fucking. Chad.

It's going to be an epic showdown, and I don't need to explain to anyone the hypocrisy behind this with the recent FinCEN Files dropping. This very well could wind up being a case of people avoiding US friendly jurisdictions, continuing to run a BTC (which can't be shut down) only business, and going "What are you going to do about it?" Really the only points of attack for the US are 1) DNS, 2) the physical servers, 3) actual people who hold private keys. Honestly who knows how it plays out in the end, but it's going to be an interesting test of how a lean BTC only business can really stand up to the government going "verboten."

Let's entertain for a minute though they lose. The domain is seized, the servers are reachable by US authorities, BitMEX throws in the towel. Then what?

Do we throw in the towel too?

DLCs + Statechains

BitMEX takes your BTC, it custodies it, it acts as a price oracle for the market, and resolves positions customers have entered into (as well as facilitates transferring them).

Bitcoin can be "custodied" in statechains. DLCs can be placed on top of Statechains. Price oracles can be agreed upon indexes that trusted parties sign off on computed from public auditable price data. The only real need for something conventionally centralized is an orderbook to aggregate outstanding offers and contracts in a place where order matching can occur efficiently.

The reality is that something like BitMEX could be effectively coordinated by a trust worthy message board operator with everything else coordinated by federated statechain operators and price oracle entities that wouldn't even know who is using them. Ultimately if BitMEX goes down there are more streamlined alternatives for similar open access no KYC market places.

A lot of thought in this space is centered around decentralized exchanges in the spot market sense, such as Bisq and HodlHodl. But futures exchanges are important too. Not only are they used by so called degenerate traders to amplify positions on spot markets, they are also used by businesses with real operating or capital costs priced in fiat dollars. Degenerate 100x trading is not the only reason for censorship resistant and private futures markets, there are many legitimate reasons for needing such financial hedges. Also, it's morally frankly no one else's business if you ***do*** want to gamble like a degenerate on 100x leverage.

Custodying money and making payments are not the only thing that Bitcoin opens the to door to decentralizing to different degrees.

The Chad Battle Ahead

Worst case possibilities and counter moves aside, BitMEX seems to have every intent to continue operating normally and fight the indictments against them and specific members. Let's just say this will be very interesting.

I'm not going to speculate on strategy here accept delineating the above dynamic of:

Really the only points of attack for the US are 1) DNS, 2) the physical servers, 3) actual people who hold private keys.

We'll see how this works out in the long term, but how it happens blow by blow is going to be a very interesting test of how resilient a conventional company running on just BTC can be against government disapproval.

Also...it would be a real shame if BitMEX survived and started playing with things like statechains and DLC oracles...a real shame...

The Way of the Digital Citadel

By Yuri de Gaia

Posted June 26, 2020

Before building physical citadels, our efforts may prove more fruitful elsewhere—in the digital realm.

The word ***citadel*** is becoming so common among bitcoiners that even newcomers use it. People just get it: why fight the monstrosity that the modern nation-state is when you can start your own?

Satoshi did not blog about the evils of central banking, petition the government to review the monetary system or run for office to "change the system from the inside". He created Bitcoin.

Similarly, opting out of the current social system and creating your own community based on shared principles may prove a lot more effective. It has been done before and it can be done again. If various groups around the world start forming citadels, chances are that at least one of them will get it right. And thus, a blueprint for many more will be available. Like with many things in life, the success of any such project depends on practice, not theory.

Is it possible, however, to start a citadel without having access to a piece of land? What if a group of individuals have already found each other in various corners of the Internet but are currently scattered around the world without an immediate way of getting together physically? I think such a group is already half-way there. Many physical outposts will be preceded by their digital counterparts. This is the way of the ***digital citadel***.

A Digital Country

We are used to thinking of countries as physical locations with defined borders and the State apparatus as its governing body. My definition of the *citadel* suggests that some landmass is required, too. A lot of our citadels, however, will be newly formed communities based on shared principles and values rather than common territory, history, religion or ethnicity. While the search for the perfect lot of land continues (which may take a while), it is entirely possible to organize most aspects of the citadel life elsewhere—in the digital realm.

Online communities are common these days. Cat lovers, car aficionados, carnivores and bitcoiners regularly meet on Internet forums, in chat rooms and video-conferences. These groups are usually formed based on specific common interests. In the physical realm, meetups represent a similar idea. But our interest lies on a higher level. A meetup of steak lovers in Singapore, generally, assumes that all the participants are residents of the Singapore city-state, but not all Singaporeans are steak lovers. What we want to build is not just an interest-specific group, but an online version of Singapore, a *digital country*.

Individual vs Collective

First things first. What are the characteristics of ***classic*** nation-states?

"As a political model, the nation-state fuses two principles: the principle of state sovereignty, first articulated in the Peace of Westphalia (1648), which recognizes the right of states to govern their territories without external interference; and the principle of national sovereignty, which recognizes the right of national communities to govern themselves."—Encyclopaedia Britannica

The current model, as we can see, incorporates two things: ***territory*** and the ***right to self-governance***. We do not have the former. The latter, however, is within reach. When we talk about being able to govern ourselves, we imply ***collective self-determination***.

The idea of collective self-determination seems to stand against ***individual self-determination***. In anarcho-capitalist and Austrian economic circles it is often a sensitive topic. Give up some of your individual freedoms in favour of a group and you find yourself walking on thin ice. Collectivism! In my view, however, the two concepts are not mutually exclusive. The issue deals with two properties: ***tradeoffs*** and ***scale***.

The formula is simple: ***the larger the scale of the group, the more tradeoffs you need to make to exist within it***.

Imagine a world in which individual self-determination is all we have: eight billion self-sufficient individuals going about their business in complete independence. It is quite hard to picture because such a scenario is impossible. The moment you start a family or become friends with someone, this total freedom disappears. Suddenly, you find yourself making concessions in order to keep the relationship. Stop seeing other women if you are to have a solid marriage; sacrifice work and hobbies to spend time with your children; change your spending habits to make sure your family is well off. Such tradeoffs are already quite significant, and we are only talking about a small-scale collective unit: family, the nucleus of society.

What about your neighbourhood? Village? Town? Country? Per the formula given (and common sense), your freedom wanes with scale. There is nothing bad about it, though. Social interactions are all about tradeoffs and concessions. What matters is the ***ability to choose*** the tradeoffs that you are willing to make. And this is precisely what the classic nation-state lacks. Instead of being a service provider and protector, it reaches its ever-growing tentacles into every aspect of your daily interactions, micromanaging your life—all without your consent.

But:

"Collective self-determination ***need not mean*** outright statehood. It could mean instead some form of autonomy or self-government ***within*** another state."—Nationalism, Self-Determination and Secession

If a group of individuals enters into a relationship whereby they agree to follow a pre-determined set of rules, including tradeoffs and concessions characteristic of communities, we get collective self-determination. With its own hierarchy, traditions and culture, such a community engages in self-government. ***In Defense of the Citadel Meme*** provided a few examples, such as the Amish. The issue with existing self-governing collectives is that they do not have their own territory. Normally, they are located within other nation-states, and no matter how much they would like to secede and go about their business separately, the host state is unlikely to give up any of its landmass—not because it does not have any to offer, but because it will set a dangerous precedent.

Our digital citadel, therefore, is an Internet-based collective ***with no physical territory***, organized and entered into ***voluntarily***, the relationships in which are governed by a ***contractually binding*** set of rules.

What would set a digital citadel apart from other online communities?

As mentioned, our collective is more akin to a digital country rather than an interest-based community. Video-gamers, anime lovers and even vegans are welcome as long as they agree to follow the rules.

Personally, I would like to see the following attributes.

The Characteristics of a Digital Citadel

Being a digital country, our citadel must possess certain features that regular countries have enjoyed throughout history. At the same time, we are attempting to improve upon the legacy system, so a few innovative approaches must be expected, too.

Government

As Hierarchy is part of Natural Order, we cannot do away with a government. However, rather than having Government, a modern amorphous entity spelled with capital G, there will be ***a government***—a clearly defined managing body consisting of a limited number of known individuals. As I am a proponent of ***private government***, i.e., leaders who have direct ownership of the citadel's assets, such a country may be referred to, classically, as a kingdom, a principality or an equivalent from other cultures. A more modern name may be used or devised, including ***citadel*** itself, but traditional descriptions are very Lindy.

This government will play a very limited role. The king, like the people, will be ***under*** the law. The law, in this case, is a set of universal ***immutable*** rules that fit on a single piece of paper. As the head and proprietor of the state, the monarch only acts as a judge, not a legislator, the vast majority of relationships in the country being subject to *private law*. As counter-intuitive as it sounds, it is a ***kingdom of sovereign individuals***.

Symbolism

Starting with small clans and ending with supra-national entities, organized people have always preferred to distinguish themselves in many ways. The use of banners and flags dates back to antiquity. In my opinion, a proper country must have a flag, a coat of arms with a motto, a national anthem, a cultural icon, national colors and some abstract symbols. In a monarchy, the head of state himself usually serves as a symbol of the nation and may make use of the dynasty's seal or stamp, which is also associated with the country.

Traditions

I believe that to unite a group of people long-term, there needs to be a common goal shared and revered by all the population. This goal must span decades or, preferably, centuries or even millenia. United around the common vision, the people of the citadel will find purpose and meaning in their lives. Being a part of something larger than yourself and directly

contributing to the grand plan—this is what is missing in many people's lives today.

To further promote unity, national traditions are required. Various events, celebrations, commemorations, competitions will elevate the spirit of the nation and invoke pride in the population.

Traditional values, such as family, community and discipline must be promoted from the young age to ensure that the citadel only grows stronger with new generations. As a root generation, we may not be perfect, but we all know that the future lies with our children.

With time, traditional art, music, theater and even fashion may develop that will reflect in outer forms the inner state of the citizens' minds. This cultural heritage will pass from generation to generation and strengthen the bond between the people of the nation.

Contract

While the above points are not entirely new, the following is what makes a digital country different from the rest.

Unlike in traditional countries where you are bound by an invisible social contract, participation in the citadel is voluntary. Citizenship is represented by *a real contract* between you and the operating entity. Whether the head of state is a monarch or a President aided by a board of directors, you will never be his subject, but a *member of the organization*. Citizenship is membership.

As soon as you feel that you do not share the nation's common goal, do not like its ethos or simply found a better alternative, *vote with your feet*. Leave. At the same time, if you choose to stay, you must abide by the laws of the citadel and expect to be kicked out if you refuse to do so. This way, management is incentivized to provide the best conditions possible to existing and potential members, and members are incentivized to be good citizens. It is as fair as it can get.

A New Renaissance

Finding a place to belong is an issue that many individuals across the world share. These rootless men would give everything to become part of something meaningful and ambitious, a place to which they could dedicate their lives. A digital citadel, a kingdom that is everywhere and nowhere at the same time, populated by real people with a shared vision of the future may be just the place.

Imagine taking a walk along a street of a foreign city and stumbling upon a person wearing a traditional dress with the insignia of your kingdom. A smile

and a warm greeting will surely ensue. Before you know it, he introduces you to other citizens who live in this city. Your stay has just become a lot more pleasant.

It is not a protest or a movement. It is a new culture, a rebirth of traditional values adapted to the modern world. And some day, with enough effort, we may be able to find a piece of land or two upon which our cities will be erected. Thus will start the great consolidation, the unification of the scattered nation.

A New Renaissance is not coming by itself. It must be brought about. Do we have what it takes to make it happen?

SNARKs and the future of blockchains

By Ruben Somsen

Posted October 3, 2020

SNARKs are often seen as a magical panacea to "solve" scaling. While SNARKs can provide incredible benefits, the limitations need to be acknowledged as well — SNARKs can't solve the existing bandwidth constraints that blockchains are facing today.

This article is meant to demystify SNARKs by giving a (relatively) simple overview of what they can and can't do for blockchains. We'll look at how its functionality in relation to blockchains can be concisely summarized as Non-Interactive Witness Aggregation (NIWA). If you understand how Bitcoin works, you'll be able to understand this article.

It should be noted that SNARKs are still very much an area of active research. Many SNARK variants either aren't efficient enough to prove complex statements, have proof sizes that are impractically large, or require a trusted setup. That said, a lot of progress has been made over the years, and it's expected that we'll continue to see improvements in the coming decade. This article is written in anticipation of such improvements, even if it may not be practical today.

What is a SNARK?

A SNARK is a construction that allows you to efficiently validate a result, given a rule set and a starting point. The inputs that led to the result are not revealed ("zero knowledge"). Confused already? This simple chess example will explain.

Chess example

- Rules: The chess rule set
- Start: Starting position A of the board
- Result: New position B of the board

The regular way of proving that the game validly transitioned from position A to B is to simply reveal all the moves and checking whether they were valid. SNARKs can do the same thing, but better:

- The set of moves does not have to be revealed (private, less data)
- Verification is more computationally efficient

There is one caveat — SNARKs tend to be computationally expensive to create. This can however still be worthwhile in systems where many people

wish to validate the same result, such as blockchains. Only one person needs to put in the effort to create the SNARK, increasing verification efficiency for everyone.

Blockchain example

- Rules: The full node software
- Start: The block header & UTXO set hash at time A
- Result: The block header & UTXO set at time B

Similar to our chess example, the regular way of validating the transition would be to start with the UTXO set (all unspent transactions) at time A, receive all the blocks, and update the UTXO set all the way until we reach time B. With a SNARK, none of this data would be needed to prove validity. In fact, if time A is set to the genesis block (empty UTXO set) and time B is set to now, then the entire chain can be validated without receiving any of the historic data.

It's important to note that for time B the entire UTXO set is required, as opposed to just the UTXO set hash. While this data is not strictly required for proving validity, we also care about ***availability***. If all you had was the UTXO set hash, then while you know a valid state exists, you wouldn't actually know what that state is. This would mean you can't spend any coins, because you don't have the data that allows you to prove that a specific UTXO is part of the set. In the chess analogy, you would have a hash of the new board position, but don't actually know what that position is, so you can't continue to play the game.

Note that whoever made the SNARK (presumably miners) ***would*** have this data (as it's needed to create the SNARK in the first place), but they could potentially choose to withhold it from you.

The SNARK blockchain

In order to guarantee that everyone can spend their coins, all the data that's needed to update the UTXO set ***must*** be communicated with each block. You'll need to know which UTXOs were spent (inputs) and which were newly added (outputs). This is so-called non-witness data.

The validity of the transition can be verified by a single SNARK, replacing all witness data (scripts, signatures), and taking up almost no bandwidth. The relationship between inputs and outputs would not be apparent — a block would look like one big coinjoin transaction. The bulk of the data would be non-witness data.

Contrary to popular belief, SNARKs can't solve the fundamental issues behind light clients or non-federated sidechains, because non-witness data must ***always*** be downloaded. Full nodes have the crucial ability to reject a valid

SNARK if non-witness data is missing, whereas if a light client neglected to download non-witness data, it could mistakenly consider a chain with missing data valid. If even a single piece of non-witness data is withheld by miners, nobody would be able to create new blocks with valid SNARKs, except for those specific miners, turning it into a permissioned system.

SNARKs consume witnesses

SNARKs for blockchains can perhaps best be summarized as enabling the following function:

Non-Interactive Witness Aggregation (NIWA)

I use the term "witness" here liberally. In Bitcoin, the witness is the data inside a transaction that proves whether a specific UTXO is allowed to be created. But over time, this UTXO (non-witness data) becomes a witness of its own when it gets spent. When 1 BTC gets sent from Alice to Bob to Carol, Bob's transaction is a witness to the transfer from Alice to Carol. In the same vein, all spent transactions since genesis are witnesses to the current UTXO set.

Also note that a SNARK is in itself a witness. If each individual transaction is validated by a SNARK, we can also NIWA these SNARKs into a single SNARK per block. And because outputs become witnesses the moment they are spent, we can even take unconfirmed but already spent outputs in the mempool and aggregate them as well. Alice to Bob to Carol becomes Alice to Carol, achieving non-interactive transaction cut-through. This can be especially powerful when a single UTXO with many branching off-chain transactions is forced on-chain, such as may be the case for Lightning Channel factories.

In short

We've summarized the core functionality of SNARKs for blockchains with NIWA. Any witness data can be non-interactively aggregated by a SNARK. The non-witness data that remains is a direct reflection of the state of the system — the UTXO set. While SNARKs can achieve amazing things

such as allowing you to catch up from genesis by merely downloading the UTXO set and a single SNARK, or non-interactively aggregating sequences of unconfirmed transactions into a single transaction, there still remains a need to publish all non-witness data for each new block in order to allow all nodes to update their UTXO set. The fundamental bandwidth constraints of blockchains are therefore not solved by SNARKs.

— Ruben Somsen

Thanks to Sanket Kanjalkar for the helpful discussion and comments.

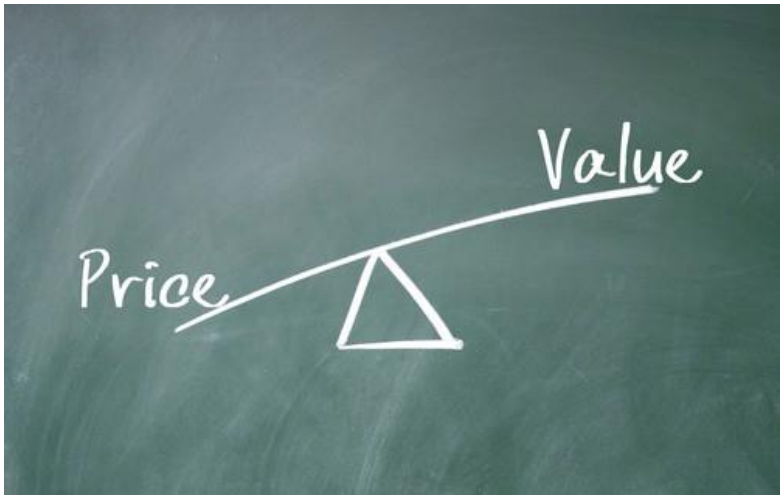
NIWA in action. SNARKs consume witnesses and are also a witness of their own. SNARK eat SNARK.

The "intrinsic" value of Bitcoin (II)

By Manuel Palavieja

Posted October 5, 2020

I am quoting the word "intrinsic" because I don't think it is an appropiate term to refer to value as I explained here. That being said, in this post I'll stick to the definition of intrinsic value normally used in finance.



Bitcoin is a medium of indirect exchange, whether its intended use is short term (payments) or long term (store of value), but in both cases it is a medium of indirect exchange for different holding periods. Therefore, Bitcoin is a **tool** for exchange, and all tools derive its value from the costs they save. Let's find out with an example:

If I am offering 1 kilogram of tulip bulbs in exchange for a hammer, that's because the hammer is more valuable to me than the tulip bulbs. We can express the the raw value I will get from that exchange using the following simplified[1] formula:

Raw Value = Value(hammer) - Value(tulips)

But doing an exchange through barter is very expensive in time and other resources as it will be hard to find someone that offers a hammer in exchange for 1kg of tulip bulbs. The cost of the exchange will probably be greater than the Raw Value[2], so it may never take place. In order to optimize the value I get from the exchange, I can use a medium of indirect exchange (let's call it "X"), and I will choose the one that maximizes the total value for the expected time ("t") needed to complete the exchange:

*Net Value = Value (hammer) - Value (tulips) - Costs (X) * t*

How does Bitcoin fit into the above? Easy: Bitcoin is objectively the asset with the **intrinsic** qualities that render the lowest costs of carry of all available assets, which makes it very convenient for long term exchanges compared to its alternatives (public debt, fiat or gold), those qualities are:

- Lowest dilution costs (gold global stock grows 2% annually)

- No counterparty risk costs (risk of default or inflation)
- Cheap to store and secure (easy to hide, difficult to confiscate)

A more suitable example for Bitcoin would be to exchange my services as a consultant during my young years for a nice home at the beach for my retirement. Nevertheless, there is currently another important cost in Bitcoin which is the cost of its price volatility. However, price is just an exchange ratio, and as such it is **extrinsic** to Bitcoin. Price volatility is a sign of the market assessing the intrinsic qualities of Bitcoin, testing and vetting if those qualities are for real or not, which is a long process as we all know. After all, very few, if any, get Bitcoin at the drop of a hat.

This post is inspired on Fernando Nieto's extremely valuable insights, which can be summarized, in a much rigorous way that I did in this post, with the following formula:

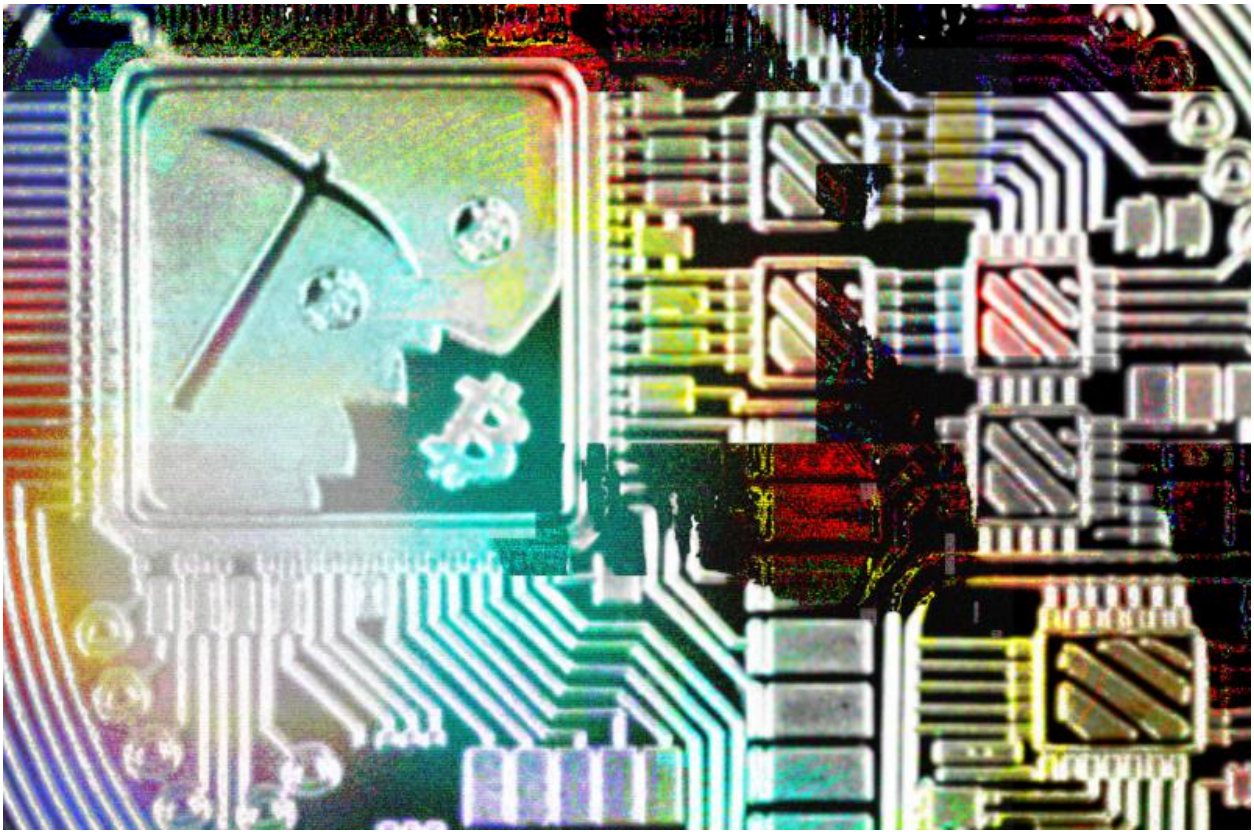
> Voluntary exchanges happen because they create value by improving the situation of both parties. A ***medium of exchange*** will be used, and demanded to be held for a certain period of time, when it allows to reduce the friction in a exchange, helping to maximize the net value it creates.
>
> $$F = 1 - (1 - x_s)\, e^{-st}\, (1 - x_b)$$
>
> where:
>
> F is the friction in trade when using certain intermediate medium of exchange,
>
> x is the cost of interpersonal exchange (validation, divisibility, spread, volatility, transportation, taxes, ...) of the goods you have for a particular medium of exchange (x_s), or of that intermediate asset for the goods you want to purchase (x_b).
>
> e is the exponential function, used for calculating continuous compounding interests,
>
> s is the cost of carry (storage, stocks growth or demand contraction, custody or credit risk, other risks/insurance, ...),
>
> t is the holding period.

[1] For didactical purposes this is a simplification of Fernando Nieto's formula.
[2] "Exchange is an economic good" Chapter 1 - Currency Theory, Bondone 2012

Introducing CBEI: A New Way To Measure Bitcoin Network Electrical Consumption

By Tyler Bain

Posted October 19, 2020



There have been many claims in recent years that bitcoin and the miners securing the network via SHA-256 proof of work use an unconscionable amount of energy. But what data are these claims based on, are the source calculations using flawed or sound approaches and assumptions? How much electrical *power* does the network draw and how much electrical *energy* has the Bitcoin network used historically?

Methodologies And Misconceptions

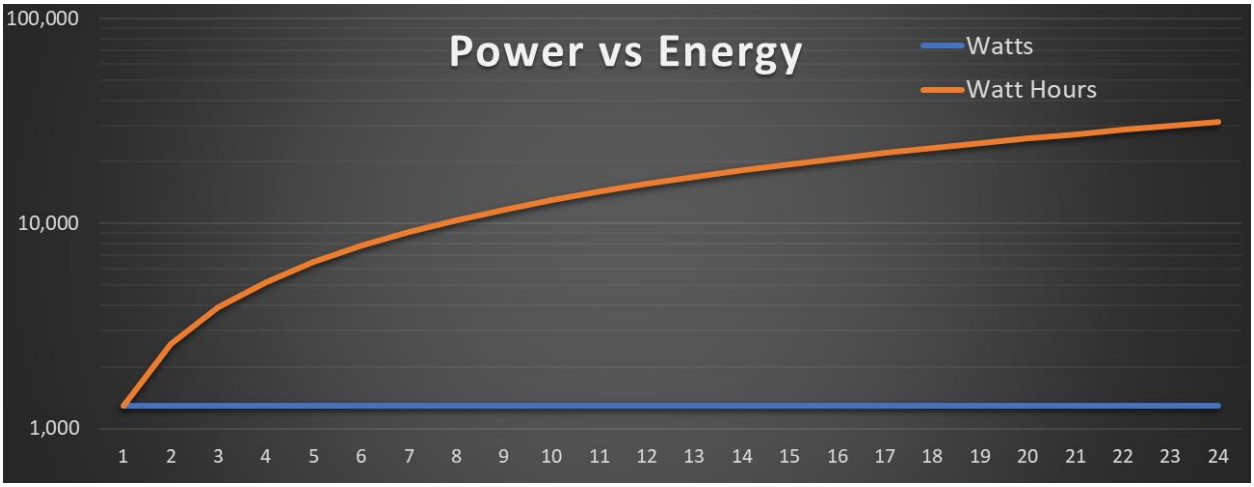
Due to the vast, globally distributed topology of the Bitcoin network, the amount of electrical power and energy that miners consume isn't exactly verifiable, instead it must be estimated. Among the energy consumption hysteria over the previous few years, a surprisingly large number of reputable

sources have weighed in and attempted to estimate Bitcoin's network energy consumption in more level-headed and data-derived ways:

- University of Cambridge, Judge Business School (JBS)
- The International Energy Agency (IEA)
- Electric Power Research Institute (EPRI)
- Coin Center
- CoinShares
- Marc Bevand
- Hass McCook
- Alex de Vries
- Myself

Estimation methodologies seem to fall into two major categories: ***economics-based*** approachesrooted in financial assumptions, as well as ***physics-based*** approaches planted in engineering principles. These two estimation approaches were thoroughly compared and contrasted at BTC2019.

It's important to understand when digesting all of these yearly usage estimations that electrical consumption is typically measured in two ways: instantaneously (power, watts, kilowatts, etc.) and that same instantaneous power measurement integrated over time (energy, joules, kilowatt-hours (kWh), etc.)



Small Bitcoin miners draw about 1,300 watts of power and use about 31,200 watt hours of energy over a 24-hour period.

The Problems With Economics-Based Network Energy Estimations

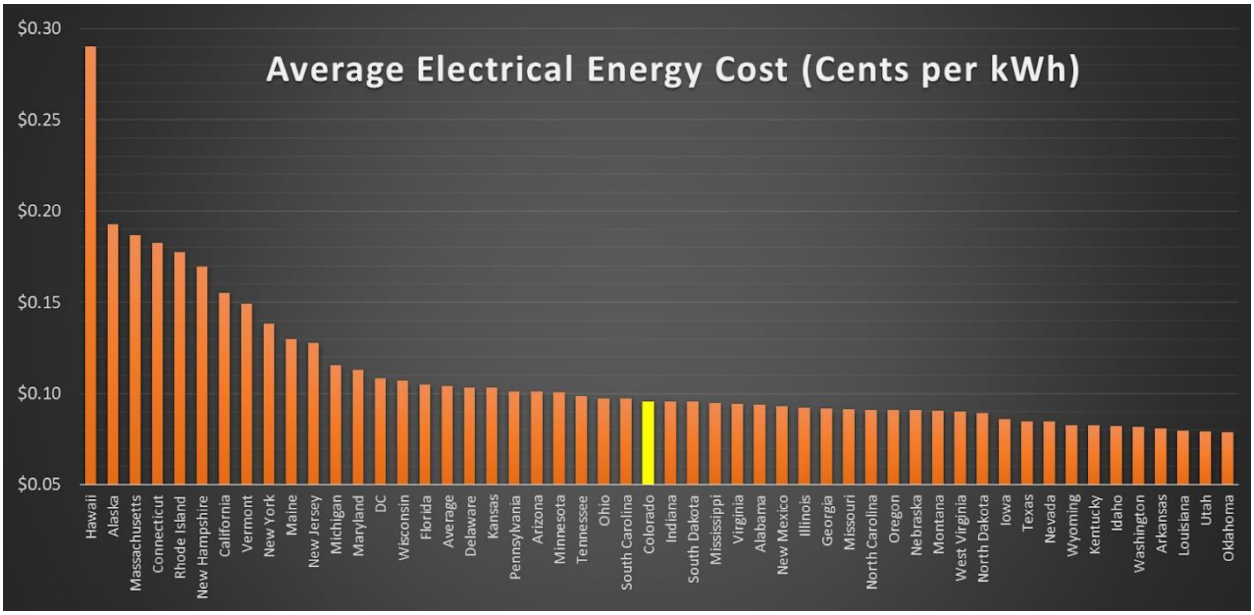
Economics–based approaches that estimate the Bitcoin network energy consumption generally assume perfectly rational market behavior, and can easily be manipulated with a few input variable misassumptions.

In theory, the Bitcoin mining industry is rational, profit maximizing and perfectly competitive: mining marginal revenue should tend to equal marginal cost (MR = MC). Meaning, on long enough time horizons, the market should find an equilibrium, where the cost of energy consumed in a unit of bitcoin's production should be roughly equivalent to the unit's market value at the time of minting. This calculation methodology can be distilled as, "How much can Bitcoin network miners ***afford*** to spend on electricity?"

Typically, these types of estimations are too dependent on a single volatile variable: the market exchange price of bitcoin. Below is a quick, simplified example of this type of estimation:

```
[MR] = [MC]

[(Blocks/Day)*(Reward/Block)*(BTC Price) ]=[(kWh/Day)*($/kWh)]

[(Blocks/Day)*(BTC/Block)*($/BTC)]/($/kWh) = (kWh/Day) = Energy/Day
```

Let's try this estimation. Bitcoin blocks are generated roughly every 10 minutes — a rate of 6 per hour, or 144 every day. Currently, a single bitcoin block contains 6.25 BTC of coinbase block subsidy; that's 37.5 BTC per hour, or 900 newly-minted bitcoin rewarded to miners daily. With bitcoin's current market exchange price of about $10,750 at the time of this writing, that is roughly $9,675,000 earned per day that bitcoin miners have available to spend on electricity.



Average U.S. electrical costs in cents per kWh by state, per EIA data

```
[(144)*(6.25/Block) * $10,750] / ($0.10/kWh) = (96.75 GWh/Day)
```

This amount of daily energy equates to roughly 35.3 TWh of yearly usage that the bitcoin miners could ***afford*** to consume, if we take a snapshot today and assume constant bitcoin price for a year and U.S. average electrical costs.

While this method is overly reliant on bitcoin price, it is also heavily dependent on the assumed electrical energy cost for miners. The calculations and conclusions of this kind of estimate can be drastically different or even manipulated depending on the assumptions used as inputs: energy costs ($/kWh) and the price of bitcoin ($/BTC).

Here we used the average U.S. electrical cost of $0.10/kWh. However, in the U.S., electrical costs actually vary seasonally, from state to state, city to city and, in some cases, neighborhood to neighborhood. Global electrical costs have the same incongruence. This isn't even including wide-ranging industrial, commercial or residential electrical energy rates, adding even more sources of error to these economics-based estimation techniques. And, in fact, this calculation's heavy energy price dependence has yet another flaw: some miners' high in ingenuity have near-zero fuel cost as they harvest excess, otherwise wasted, inaccessible or curtailed energy sources.

This quick exercise highlights, in my opinion, why this type of economics-based estimation approach is a gross oversimplification fraught with the following issues:

- Bitcoin mining, hash rate and, therefore, network energy consumption isn't as responsive to sudden price movements as these economics-based estimation methods are.
- The economics-based model claims energy usage is cut in half along with network miner rewards after each bitcoin block reward halving cycle, which is every 210,000 blocks or about four years, while difficulty and proof-of-work-based data disproves this.
- This type of model assumes a single average global energy cost ($/kWh); electrical energy costs vary widely by region, seasonally and even by energy source.
- This is likely to be an upper-bound estimation.

The Benefits Of Physics-Based Network Energy Estimations

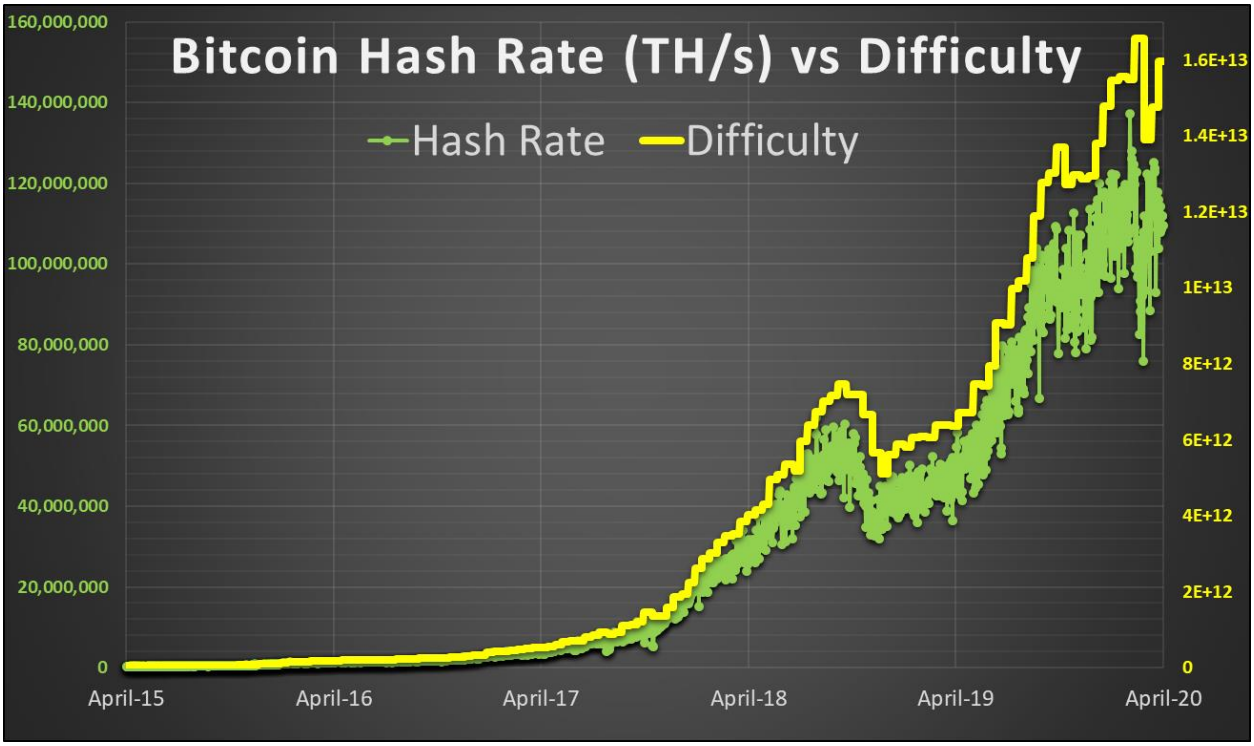
Physics–based network energy estimation approaches, on the other hand, tend to be a very rigorous type of "***running of the numbers"*** that the Bitcoin community is accustomed to.

These methods use independently verifiable on-chain difficulty, proof-of-work data and original equipment manufacturer (OEM) -published heat rate specifications to more accurately estimate historical energy inputs into the

bitcoin mining system. The physics estimation attempt may best be described as a "bitcoin stoichiometric ratio unit analysis calculation:"

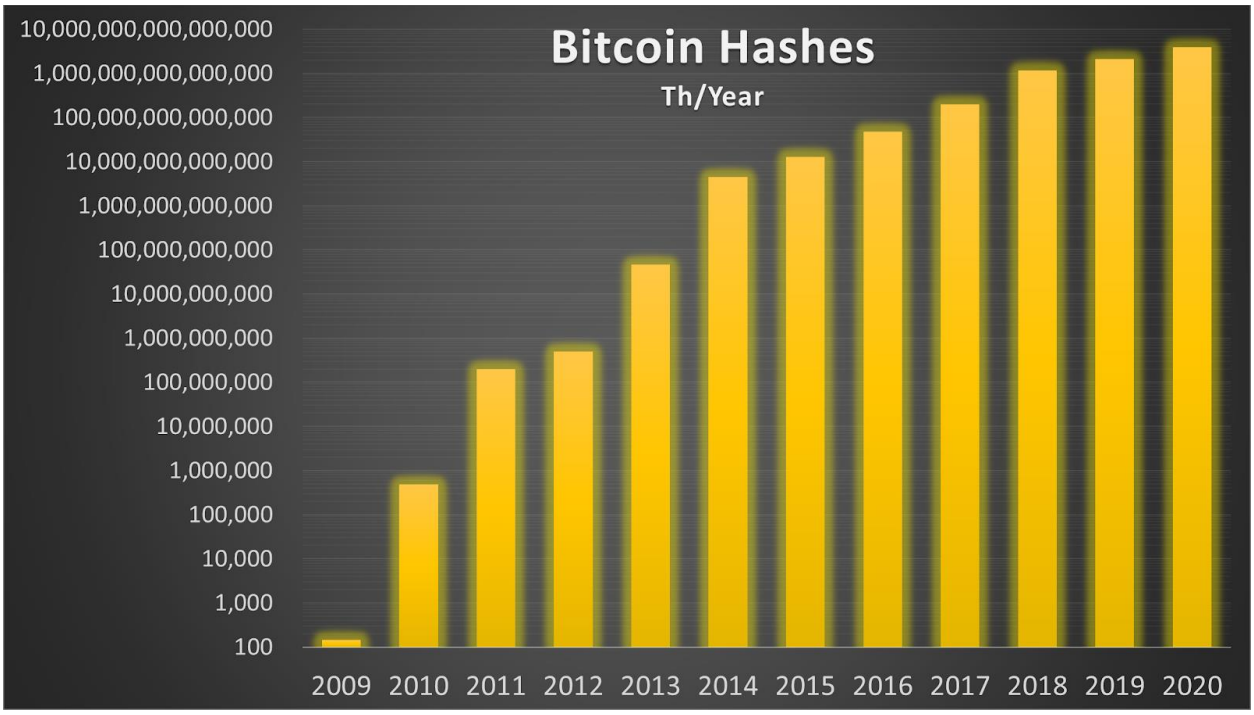
```
Bitcoin Difficulty (Unitless) → Bitcoin Hash Rate (Daily Average TH/s)

Daily Average Hash Rate (TH/s) → Yearly Hashes (TH/Year)

Yearly Hashes (TH/Year) * Yearly Hash Heat Rate (Joules/TH) = (J /Year)

Energy Per Year (Joules/Year) → (kWh/Year) → (TWh/Year) → (ktoe/Year)
```

So, let's try out this style of estimation using bitcoin proof-of-work difficulty data and OEM-published data. Bitcoin network difficulty self-adjusts once every 2,016 blocks, or roughly once every two-week period. This difficulty adjustment is to compensate for block production speed discrepancies and, thus, network hash rate fluctuations.



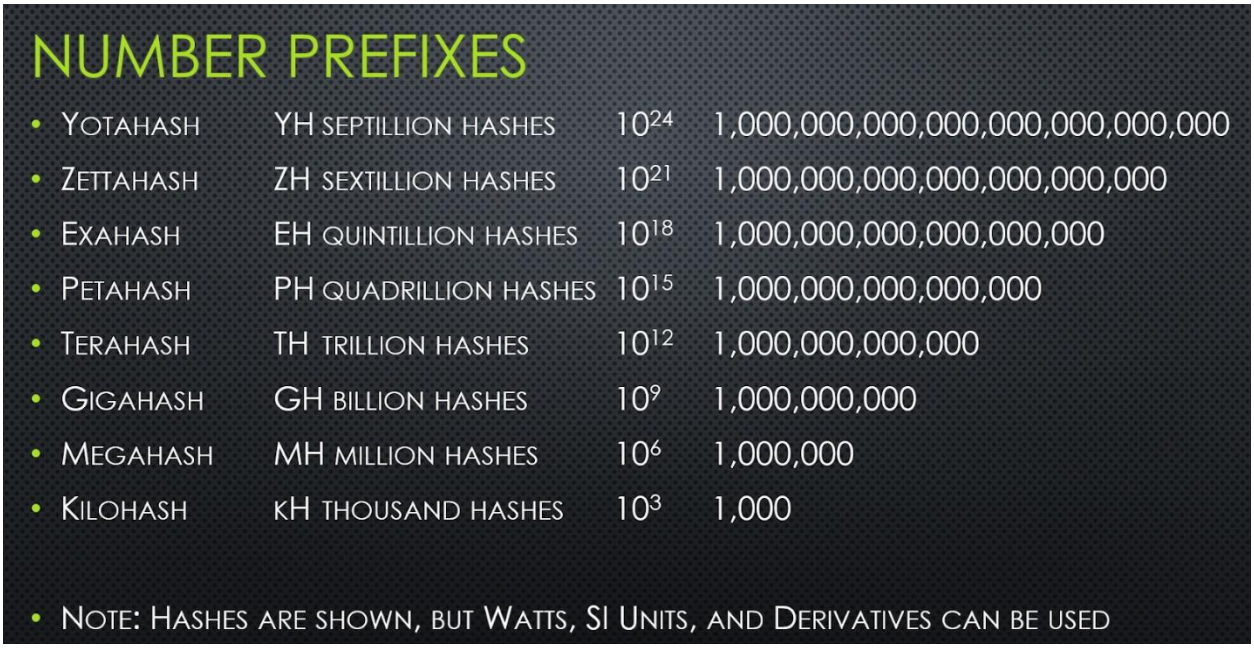
Bitcoin network hash rate (Th/s) compared to difficulty, April 2015 to April 2020.

This difficulty and proof-of-work relationship allows us to derive an estimate for network hash rate based on the block production rate and the associated difficulty level. From the amount of work done at the various difficulty levels over the previous decade, we can roughly estimate the amount of SHA-256 hashes computed per year on the Bitcoin network, shown below in terahashes per year (Th/year) or a trillion hashes per year. We can also do this same type of exercise with daily data to produce more granular calculations (spoiler: keep reading).



Estimated total Bitcoin network terahashes by year.

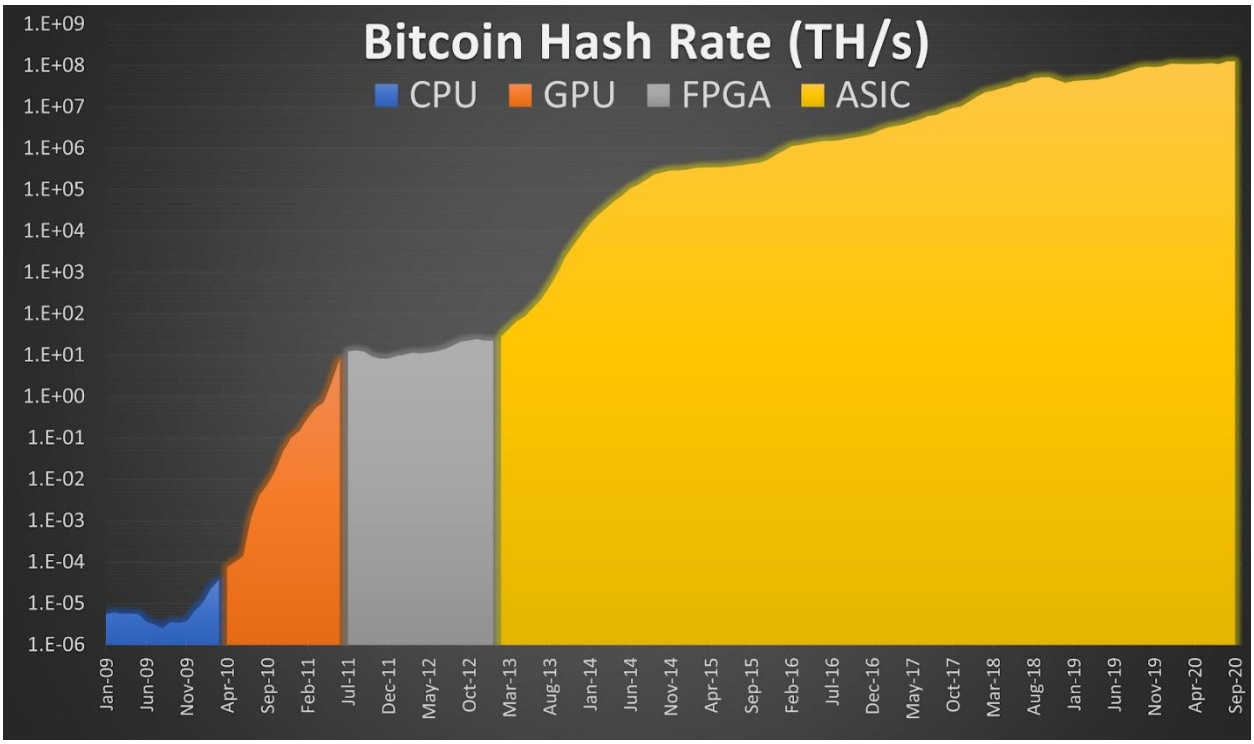
Bitcoin is on pace to have roughly 3,934 yotahashes computed on the network in 2020 or about 3,934 septillion hashes ("yota" and "septillion" are the largest of the Scientific International (SI) prefixes to date, (10^{24})),



Scientific International (SI) unit prefixes, based on NIST data here.

Now that we have an estimation for the amount of hashes per year, next we must compile mining rig efficiency data over the past 11 years to understand how much energy would have been required to produce that amount of work.

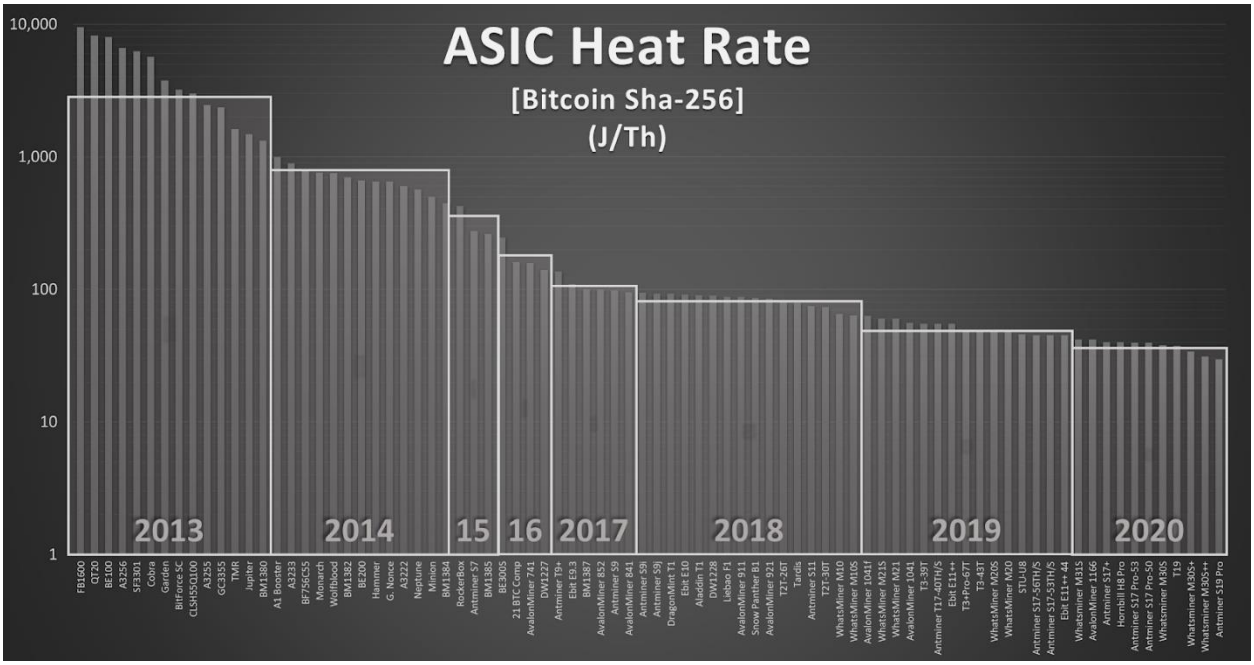
Here it is important to understand the different types of mining equipment that have provided work toward the Bitcoin blockchain over the years. Each era and year has distinctly different proof-of-work efficiency characteristics, which change the network's energy consumption values over time. From the humble beginnings of the Bitcoin genesis block being built by work derived from CPUs (central processing units), to blocks eventually being constructed with GPUs (graphics processing units), then on to FPGAs (field programmable gate arrays), and finally ASICs (application-specific integrated circuits) the Bitcoin network has evolved at a stunning pace.



Bitcoin network hash rate colored by general device type eras, in terahashes per second.

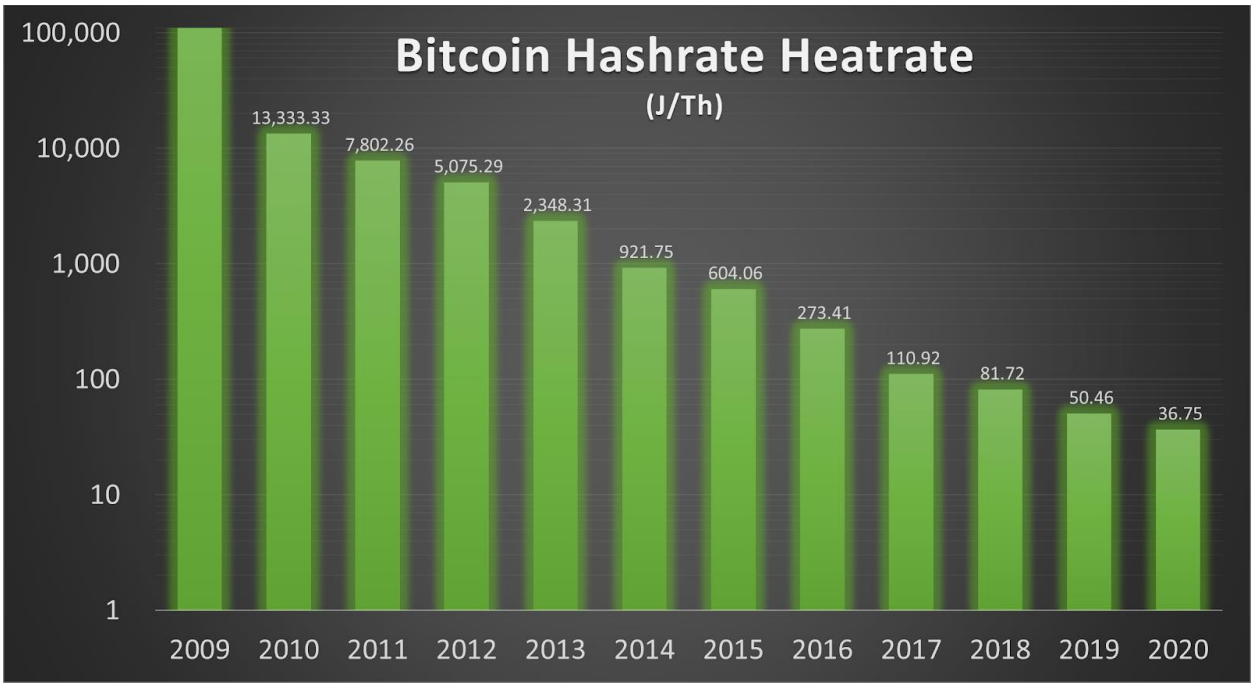
Important note: efficiency is defined as useful work performed over energy expended to complete that work (terahash/joules — Th/J). However, ASIC original equipment manufacturers typically cite a type of heat rate specification, or the inverse of efficiency, showing energy expended over useful work (joules per terahash — J/Th).

As you can see in the log scale chart below, over the past eight years, bitcoin mining ASICs' heat rates have been steadily marching lower every year, meaning network mining efficiency has been increasing.



Manufacturer published SHA-256 ASIC energy per hash heat rate in joules/terahash by bitcoin mining rig.

Translating this data into an average yearly heat rate (chart below) shows a similar steep decline during the entire history of bitcoin mining. CPU, GPU and FPGA benchmarks along with published OEM power usage data was used to estimate 2009 to 2012 network average heat rate. ASIC miners announced in 2020 were visualized above and below to show the continued decrease in hash heat rate, but they were discarded from the energy estimations as they are not yet publicly available.



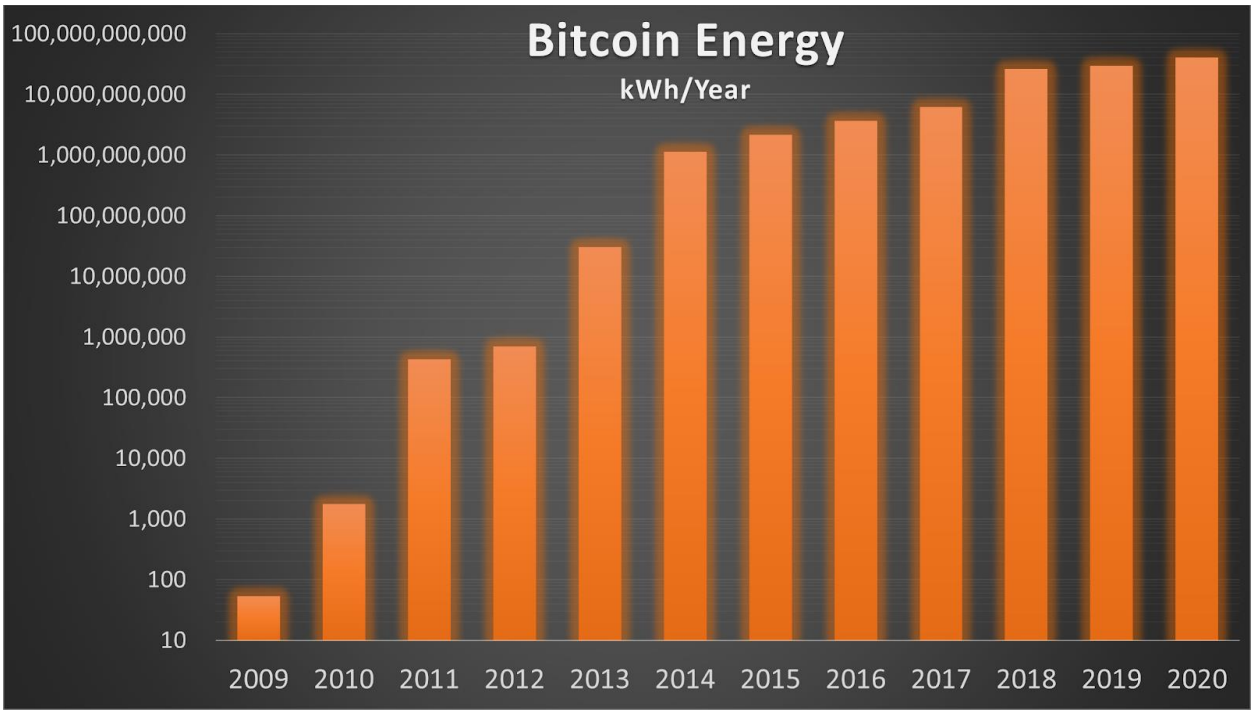
Bitcoin mining equipment average yearly heat rate, the inverse of efficiency (j/Th)

So, now that we have compiled all of the necessary data (yearly hashes and yearly hash heat rate), let's combine them via an engineer's attempt at bitcoin mining energy stoichiometry:

`Yearly Hashes (TH/Year) * Yearly Hash Heat Rate (Joules/TH) = (J /Year)` See Also

`Energy Per Year (Joules/Year) → (kWh/Year) → (TWh/Year)`

Simply multiply the yearly work completed (terahash/year) by the yearly estimated heat rate (in joules/terahash) for miners on the system and you arrive at a joules/year estimation. We will convert from joules/year to kWh/year (a kWh is equal to 3.6 megajoules) and below those yearly energy estimates are charted.



Yearly estimates For Bitcoin network energy consumption, in kWh

However, this physics-based estimation method also has some issues:

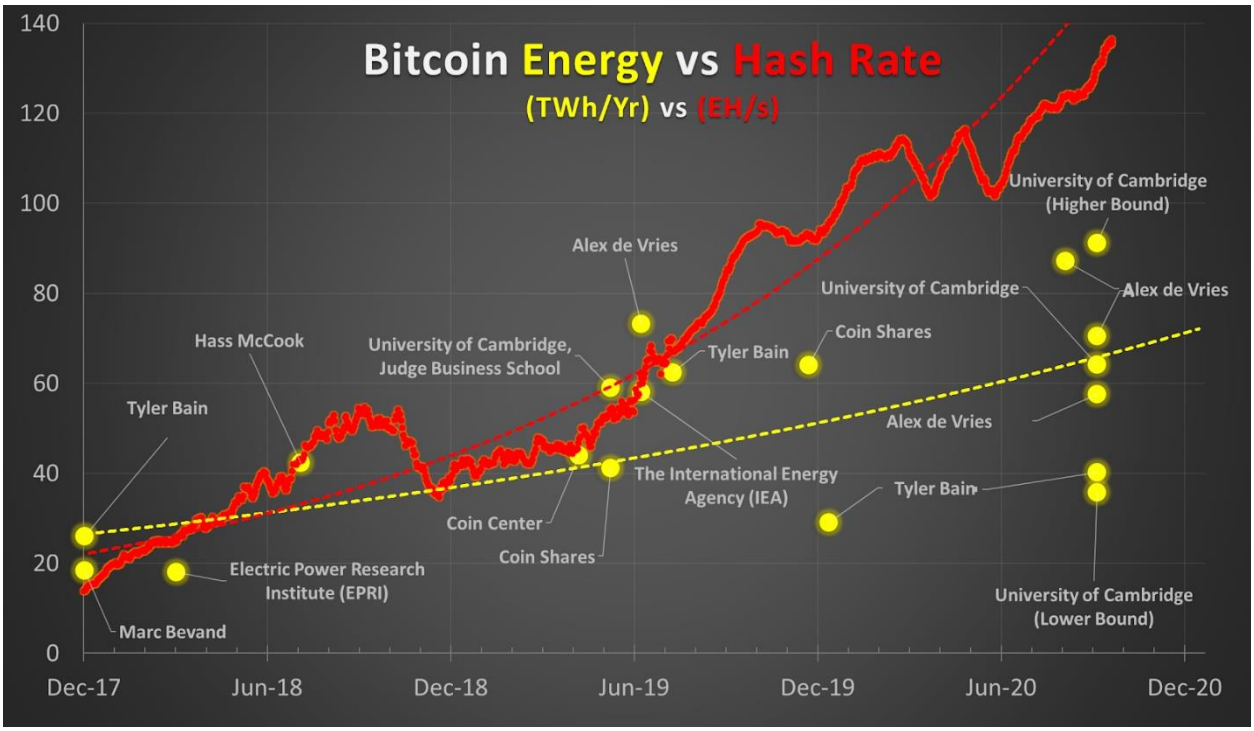
- The quantity of active miners by level of efficiency isn't known, and this physics-based model assumes equal participation from all miner models available on the market by year released.
- This model also uses a step function for yearly heat rate data as in input. That yearly data abruptly changes at the first of each year, a gradual heat rate decline would be more realistic as older miners steadily retire and new ones fire up.
- It assumes old miners retire after a year, which is also unlikely as equipment life cycles are now ranging for two or more years.
- This is likely to be a lower-bound type of estimation.

Comparing Different Network Energy Estimations

Where do these yearly energy consumption estimates fall among the previously-cited calculation attempts? Interestingly enough, both of our calculations, even using drastically different methodologies and with all of the shortcomings discussed above — the ***economic-based*** estimation (35.3 TWh) and the ***physics-based*** estimation (40.17 TWh) — are very similar in value. They also fall within the range of a variety of other popular estimations from noteworthy individuals, entities and institutions shown in the chart below. That all of these estimations are fairly similar in magnitude lends

credibility to the various different estimators as well as the wide variety of methodologies and different assumptions used.

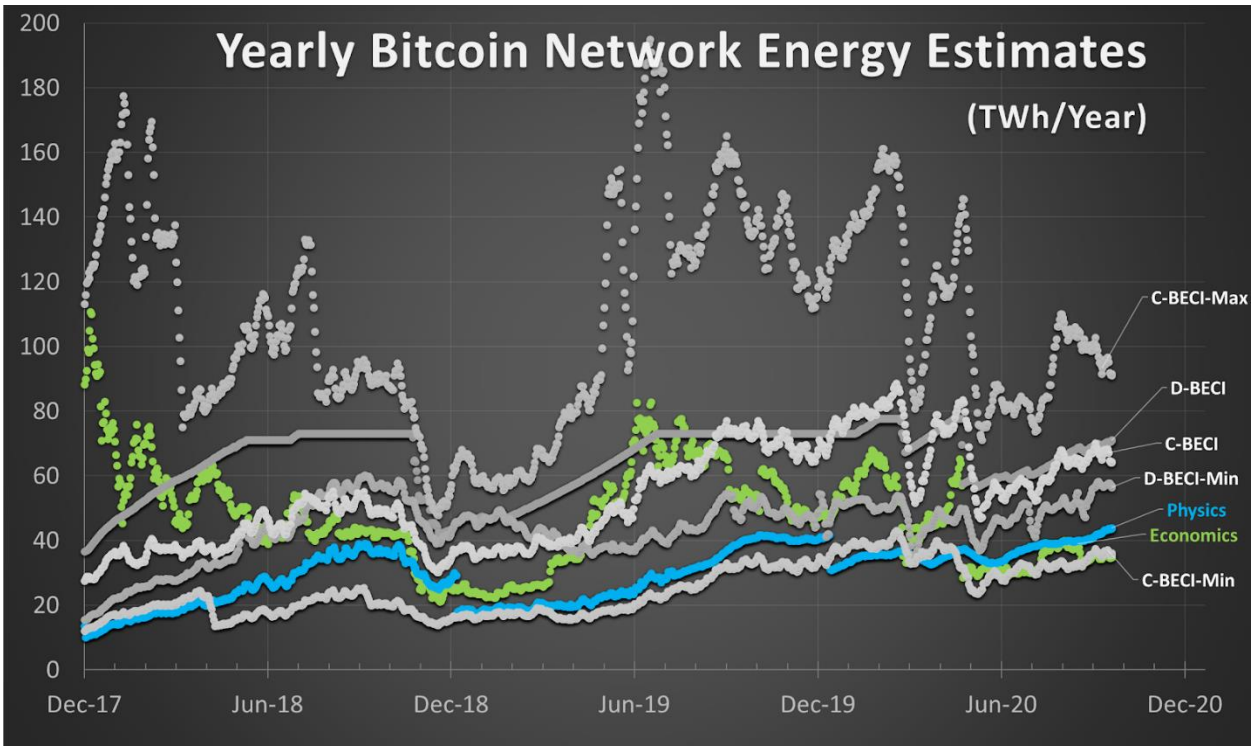
Noteworthy below: it appears that the Bitcoin network hash rate (EH/s) is beginning to decouple from the general yearly energy (TWh/year) estimation trend. This may be due to the decreasing heat rate of SHA-256 ASIC mining equipment if the estimate is physics based, or due to the halving and price stagnation if the estimate is economics based.



Bitcoin network hash rate (EH/s) and yearly electrical energy (TWh/year) estimates from various sources

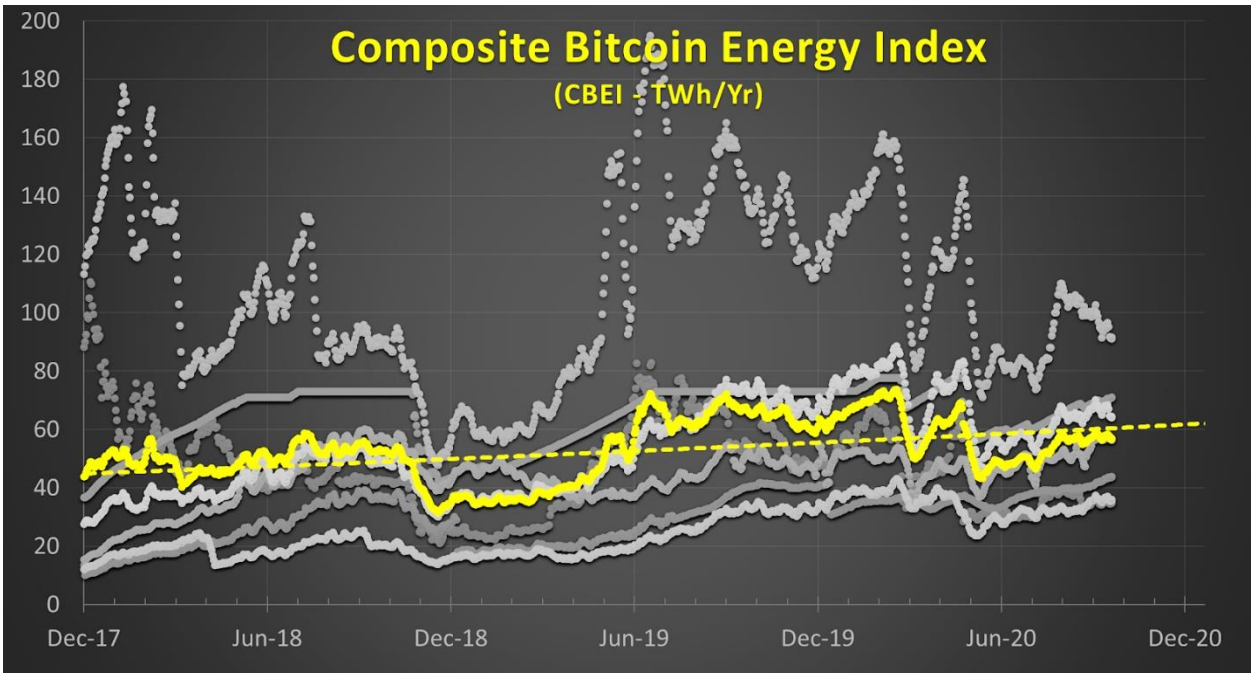
This chart above shows yearly energy estimation snapshots at time of publishing in TWh/year, but a few of these sources (University of Cambridge [C-BECI] and Alex de Vries [D-BECI]) actually publish these yearly estimates on a daily graph going back a few years. This gets back to the previous ***energy vs. power*** discussion: logic should prevent plotting yearly energy estimations on a daily axis.

Regardless, I thought it would be worth comparing these published estimates with our above calculations using more continuous time series data going back to late 2017 (the previous market all-time high). The economic and physics calculations, the Cambridge estimates, as well as Digiconomist's results are all fairly similar in magnitude over time, again adding some peer review and validity to these different estimation techniques.



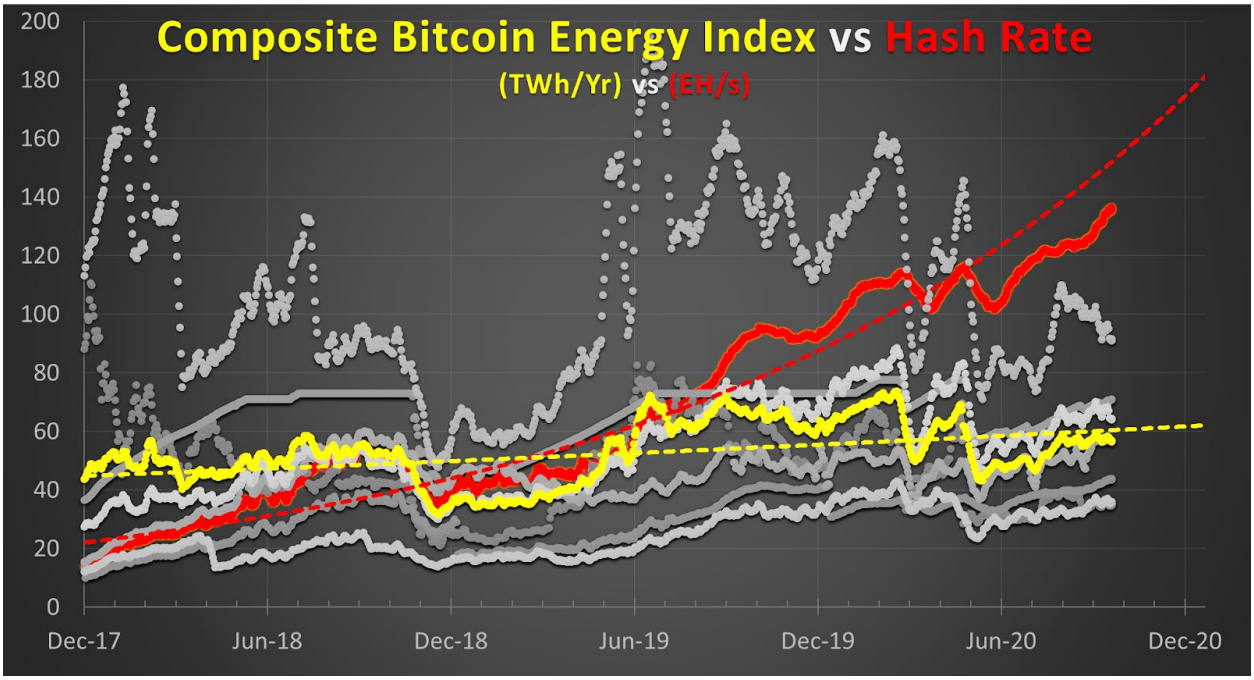
A yearly energy estimation comparison (TWh/year)

Our above estimation methodologies appear to align nicely with the other various daily interval yearly energy estimates, so they were averaged together to create a sort of ***Composite Bitcoin Energy Index (CBEI)*** as shown below in TWh/year. Each of these estimations have different assumptions, varying levels and sources of inaccuracy, and thus their composite may be more accurate. This composite of estimations (CBEI) has just recently retested the 60 TWh threshold for total yearly Bitcoin network energy consumption.



A yearly energy estimation average, Composite Bitcoin Energy Index (CBEI)

How does this composite energy index compare to Bitcoin network hash rate over time? The CBEI shows a similar decoupling as hash rate and energy around early 2019 with hash rate continuing to rise and energy consumption staying relatively steady as ASIC heat rates and bitcoin mining incentives have shrunk.

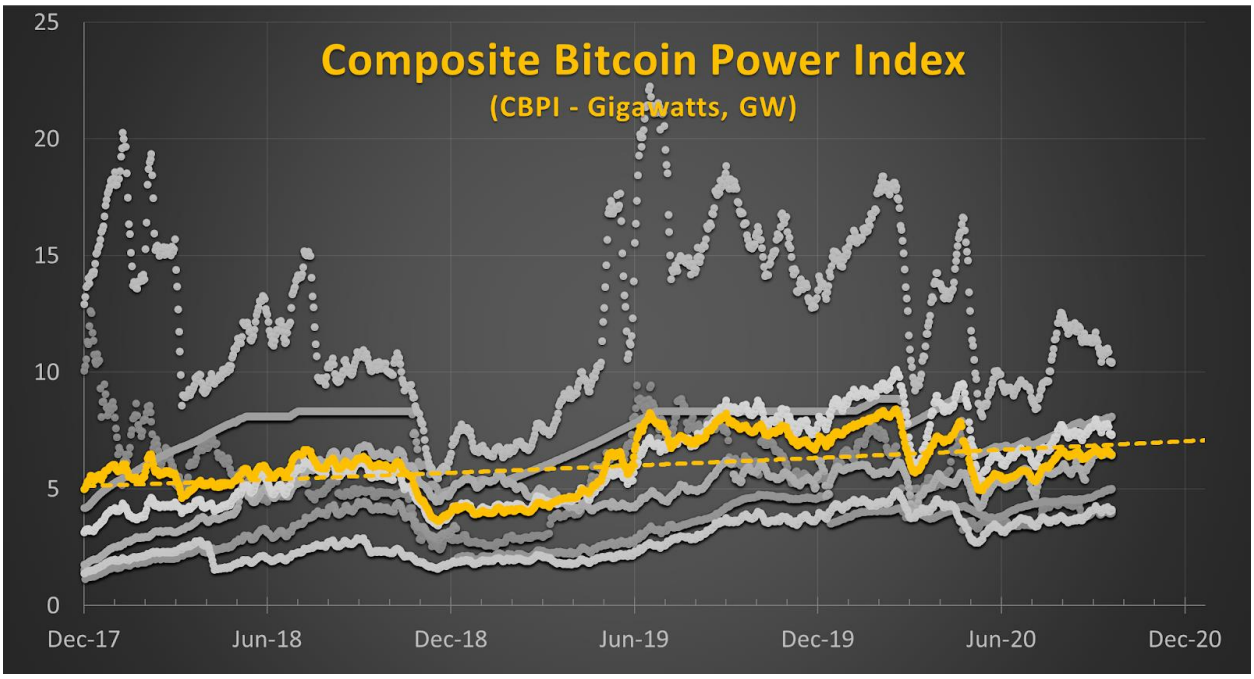


Interestingly, snapshot bitcoin consumption estimations are commonly extrapolated for an entire year, expressed as an ***energy*** value in TWh/Year without supporting time data or evidence. Daily network ***power*** estimations would be much preferred to all of these ***yearly*** energy consumption estimates plotted on a ***daily*** chart. The chart crime in this case is the egregious graphical error that makes folks massively misinterpret the data: yearly energy estimates graphed on a daily axis. So, I took the liberty of converting these daily interval estimates into a daily power estimation chart to correct for these above chart errors that force data misinterpretations.

I present the ***Composite Bitcoin Power Index (CBPI)*** compiled from the D-BECI and Minimum, the C-BECI Maximum, Minimum and Estimated, as well as our above ***economics- and physics-based estimates***.

This CBPI composite estimates for Bitcoin's instantaneous electrical usage as expressed in ***watts,*** the unit of ***electrical power.*** The CBPI peaked recently at nearly 7.58 GW, or about 6 DeLorean time machines at 1.21 Gigawatts (or should I say jigawatts?).

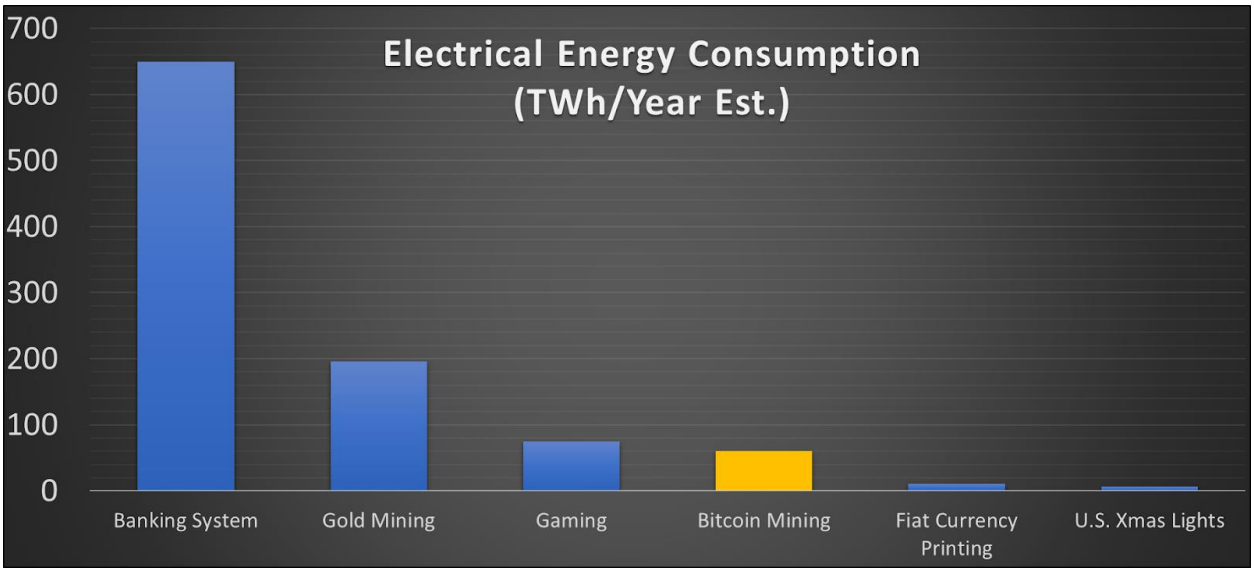
CBPI In Context



Energy values that large are difficult to digest, especially in a yearly context, so let's put these estimations in perspective with some quick comparisons:

- 650 TWh/year consumed by the banking system
- 200 TWh/year used in gold mining
- 75 TWh/year used on PC and console gaming

- 60 TWh/year on bitcoin mining (CBEI)
- 11 TWh/year used on paper currency and coin minting
- 7 TWh/year used on Christmas lights in the U.S.



A comparison of our index to other popular energy usage estimates.

Based on our estimations above, the Bitcoin network consumes roughly 40 to 60 TWh/Year or around 0.15 percent of global yearly ***electricity*** generation (26,700 TWh) and only about 0.024 percent of global ***total energy*** production (14,421,151 ktoe). (A ktoe is also a unit of energy: a kiloton of oil equivalent, 11.36 MWh.)

So, Bitcoin energy consumption today is only a very tiny portion of what many consider to be a significant civilization-level problem: ever-increasing human energy consumption. Check out interesting solutions to this problem outlined a century ago by Nikola Tesla. As recently as September 2020, a study claimed that nearly 76 percent of the Bitcoin network is powered by clean energy sources. Also, remember that once Einstein discovered mass-energy equivalence and humanity harnessed the energy embedded in the atom, energy for the advancement of mankind has become materially abundant.

Home On The Range

By .615

POsted October 21, 2020

Dystopian Dreams

If you are reading this, then you likely know the origin story of the Bitcoin Citadel concept.

In 2015, a time traveling anon from the year 2025 posted on Reddit (edited in 2019) a vision of the future in which hyperbitcoinization has resulted in a grossly dystopian world. In this future, anyone who obtained bitcoin prior to 2020 through luck, virtuous stacking, or online shitposting became exceedingly rich while the rest of the world was left begging for scraps. Instead of working to solve problems for the world, the few bitcoin rich have cloistered themselves from the many bitcoin poor in walled cities.

This vision of the future was latched onto by many bitcoin hodlers primarily because of its aggressive price predictions which seemed to be playing out – until 2019 came and went. Others were taken in by the idea of protected Bitcoin only communities that would serve as islands of prosperity in the event of societal collapse.

Much like the term Bitcoin Maximalist, the citadel concept was adopted in spite of its negative connotations.

What was once an admonishment of future actions has become a battle cry for hodlers large and small. Many Bitcoiners now believe that it may be essential to either build their own fortified dwellings or join forces with like-minded individuals in larger citadels to protect their physical and digital assets.

At best, the original Reddit post was weak disaster porn, and the idea of a walled city isolated from the world seems like a one dimensional vision for the future. A gradual then sudden collapse of the current global world order is certainly a possibility, but even in this scenario, it is likely that the future will be more nuanced than any dystopian fantasy has imagined.

While preparing for worst case outcomes is important, more can be gained from focusing time, energy, and efforts on building a world that you would want to live in.

If one merely survives a Mad Max style future, or worse yet, thrives at the expense of others, what's the point?

Voluntary Means

With these thoughts in mind, a slightly different conception of a Bitcoin citadel can be imagined.

Instead of beginning with a worst case scenario as the foundation, this vision aims to build a *circular Bitcoin economy and community from the ground up* within the existing system. The concept brings together elements of fraternal organizations, for-profit corporations, intentional communities, and idealistic visions for the maintenance and preservation of the Bitcoin protocol.

What is left out are preconceived notions about how such an organization should be governed or how any of its members will want to live.

The most successful citadels will be those which grow organically and operate with as little centralization as possible.

Respecting the individuality and autonomy of all is how this revolution in personal responsibility, money, culture, and industry will begin. If a Bitcoin Renaissance is on the horizon, it must have some space to take hold and flourish.

The example which follows is a rough proposal for a voluntary association of **Hodlers of Last Resort** which will ultimately coalesce into a functioning citadel. After beginning as a virtual association it is envisioned that it will eventually morph into a physically based citadel.

This concept, and its formation model, could be applied to virtual citadels, physical citadels, and hybrid models which operate in both the physical and virtual worlds. Likewise, the methods of forming and funding the citadel could be scaled up or down depending on the size and scope each citadel is aiming to achieve.

By sharing this, it is intended for everything that follows to be open source in nature. While I would love to engage with anyone interested in further refining the concept, I would be equally happy to see others run with the idea and make it work for their own locality – let a thousand citadels bloom.

HODLERS OF LAST RESORT

Mission

To unite hodlers of last resort and plan for a future where Bitcoin is the standard.

Goal 1:

Form a Voluntary Association of Hodlers of Last Resort

In the beginning this will be a voluntary and decentralized membership association comprised of those willing to eventually commit a portion of their bitcoin hodlings to fulfill a common set of goals. The return for each member will be creating something of lasting value and possibly increased personal wealth from the ownership stake. Initiation will be managed via a Lightning Torch which is to be passed to bitcoiners who are viewed by their peers as being “Hodlers of Last Resort”.

The following are some answers to the common questions of Who, What, Why, When, and How. The question of Where will be addressed in *Goal 3*.

Who is a Hodler of Last Resort (HOLR)

Technically, this determination will be at the discretion of each invitor/invitee in the chain. But the general idea is someone who is committed to advancing the technology and adoption of bitcoin, hodling their bitcoin for the long-haul, and preserving bitcoin for the ages. It is also important that each invitee be respected by other bitcoiners.

What is Required for Membership/Ownership

The first requirement of membership is to be bestowed an invite by a peer. Once the invite has been accepted, the member should work towards refining the concept and furthering the goals of the association. Ultimately, members will be required to commit an agreed upon amount of bitcoin to an association managed Multisig Wallet. These funds will provide the seed capital for future operations. Issues relating to continued membership, governance, and the return of deposited funds should be discussed and agreed upon in advance of the initial funding.

Why Should Anyone Do This

Because we can, because at some point we may need to, and because a physical manifestation of the spirit and ethos of bitcoin which lives online must happen at some point. To my knowledge, there has not been an association of this type previously suggested, and such an organization would ideally be populated with its most ardent and thoughtful users.

When Will the Torch Begin Its Journey

Member 0 will begin the process by sending the first formal invite via a Lighting Torch. From then on, the timing will depend on the continued acceptance and passing of the torch. (**NOTE:** *It is expected that each prospective member will have unique criticisms and ideas for improvement of the proposal. As such, the passing of the torch is likely to be a time consuming process.*)

How are HOLRs Invited

Member 0 will invite the first prospective HOLR by initiating a Lightning Torch carrying a balance of 6,102,000 sats. This torch is intended to survive 20 passes and result in an initial membership of 21. Outside of the symbolic purpose (see note below) this amount was chosen for three primary reasons.

The balance of 0.06102 BTC represents enough value that it will signal some measure of validity of intent for both the inviter and invitee.

Allowing for the possible theft of the balance will provide a way to root out dishonest invitees. In the long-run, it's a small price to pay for that type of information.

Due to the relative value, the amount will serve as a way to ensure that membership is carefully considered and only passed along those most likely to accept and successfully pass the Torch.

Initial membership will be limited to 21. I.e. Member 0 will invite Member 1 via a DM and Lightning Torch carrying 0.06102 BTC. The process will repeat until the first 20 invitees have accepted and the 20th invitee has returned the torch to Member 0.

Once there are 21 members, and the association has sufficiently coalesced, each member will initiate their own Lightning Torch and begin the selection of 9 additional members. This will result in a total membership of 210.

Upon acceptance of the 9th pass in each new chain, the 10th person in each chain will return the funds to the first member in their respective chain. At this point, no member will be out any funds, and the group can decide upon the initial funding requirements of the citadel. Funding by members could be managed in infinite ways, but for the sake of example, let's assume that the

initial funding results in each member contributing 10,000,000 Sats for a total of 21 BTC. This amount will be managed in a Multisig Wallet under predetermined and agreed upon procedures.

The dual purposes of collecting these funds are to create skin in the game for each member/owner of the citadel and to establish the seed funding for the citadel. This is meant to be a low time preference endeavor, and its ultimate success will be tied to that of Bitcoin's success. By the time the citadel has moved from virtual space to meatspace these funds could provide more than adequate initial funding.
(**NOTE:** *The Torch amount of 0.06102 has been chosen to symbolically represent bitcoin's effective revocation of Executive Order 6102 which gave the US Government the ability to confiscate citizens gold and ultimately remove the gold backing of US currency. These actions paved the way for a fiat based central banking system, and bitcoin has given the power of money creation back to the people. A distributed network of Citadels may provide protections against future seizure attempts in ways that are not possible without organizations of this type.*)

Goal 2:

Create Online Repository for Association & Organize Virtual and IRL Meetups

These are short-term goals which can begin simultaneously to the invite process. The purpose is to clarify and harden the goals of the association, develop protocols for furthering association work, and begin the process of engaging with other members.

Online Repository

Those members with the deepest experience in setting up decentralized projects can hopefully arrange the establishment and maintenance of an online repository. This space can be used to refine the goals, governance protocols, and project development for the citadel.

Meetups

Establishing a rapport with other members will be essential. It is envisioned that members will likely meet in virtual and real world spaces throughout all phases of the citadel project. Virtual meetings could begin at any time, and in-person meetups could take place in conjunction with larger bitcoin events at first. This would allow members to gather without attracting too much additional attention (if that is desirable). As time goes on, dedicated meetups could be held regionally on a regular basis. Larger and more global meetups could be organized less frequently.

Goal 3:

Establish Real World Presence

Once the virtual citadel has reached maturity, the goal will be to establish a formal legal structure, formulate and vet business plans, obtain property, and build physical structures that embody the spirit and ethos of bitcoin.

Legal Structure

Creating a legal entity presents numerous potential problems for a bitcoin focused organization. This is especially true for organizations that want to maintain as much member privacy as possible. As such, it will be imperative to carefully consider the jurisdictions and entity types that will be chosen. Despite these challenges, the efforts will be necessary as venturing into meatspace will require a legal structure and its accompanying protections.

Corporate Structure

It is likely that a corporate structure of some form will be most desirable. The state of Wyoming has some of the most privacy focused laws in regards to LLC and C Corporations, and it happens to be the most Bitcoin friendly US state at this time. LLCs may work in some cases, but the requirements to issue K-1s and pass-through income to the owners is likely a nonstarter for an organization like this. As such, a C Corporation is the most likely entity choice. This will allow for more anonymity of members, a diverse stream of income, and will allow for the accumulation of assets without directly resulting in tax reporting requirements and liabilities for its owners. If members desire to maintain a relatively high level of anonymity, a Wyoming based business attorney can be retained to manage the issuance of shares among other matters which may require identity disclosure.

Formulate and Vet Business Plans

This step may be taking place from the beginning of the organization; however, any realization of these plans will not come to fruition until there is a consensus on their feasibility and ways to ensure their ability to operate and obtain funding.

Purchase Land

The first plot of land that is purchased must be located somewhere. While there are many enchanting locations to choose from in the world, **Wyoming** feels appropriate for three reasons in particular:

Bitcoin Friendly - The state is the first in the US to aggressively incorporate laws which are friendly to bitcoin based businesses.

Bitcoin Spirit & Ethos - Wyoming is known as the “Equality State” and the “Cowboy State”. The state is sparsely populated while being rich in agriculture, energy, rugged individuals, and natural beauty. The list could go on, but these anecdotes seem to be the most relevant and in line with the ideals of individualism and self-sovereignty espoused by many Bitcoiners.

Natural Resources & Community - A citadel formed in Wyoming could be home to innumerable businesses due to its rich natural resources and business friendly environment. It’s wide open spaces are also an inviting opportunity to create communities from scratch. Some of the more obvious businesses would include energy production, Bitcoin mining operations, ranching and farming. It may also make sense to invest in an ASIC foundry and other hardware production facilities. Education and art are likely other key enterprises to founding a successful citadel as these are the best ways to communicate values and reinforce a culture. Establishing studios, workshops, and meeting venues for Bitcoin educators and artists would help spread ideas to a wider audience. Creating a thriving community requires nourishing its inhabitants and providing outlets to interact with the outside world. Having a robust culture built around sustainable businesses, arts, and education will be the foundation of the citadel.

Build a Ranch of Last Resort

This step seems self-explanatory. Why purchase land if you do not plan to build on it (conservation aside)? The purpose here is to build something of lasting utilitarian and aesthetic value. Ideally this would be a set of structures which bridge the ancient and modern and will be rugged enough to hold up for centuries and provide for the protection of its inhabitants if the need arises. Imagine giving someone like @wrathofgnon the opportunity to consult on designs for an entire community from scratch. Just as the medieval Renaissance produced beautiful and enduring architecture built to enhance its environment, the Bitcoin Renaissance will no doubt provide similar opportunities.

Protection

While it’s possible that the citadel could be a place for physically protecting life, liberty, and property, a citadel’s primary purpose need not be as a place to cloister oneself and family from the world. Some may choose to live within or near the citadel, but physical autonomy of citadel members should be a primary goal. For those who seek to live in or near a citadel, security would obviously be a primary consideration as it is for all Bitcoin projects.

Let Them Come

If all of this is done thoughtfully, others will come. The space will be a “home” for citadel members, but it is also envisioned to serve as a public meeting space to further bitcoin adoption and citadel goals.

Replicate

Assuming the goals to this point have been achieved, the citadel should begin the process of establishing additional operational bases throughout the world. It’s possible that sister associations will begin this process as well which would be a welcomed development. In a world of competing and cooperating citadel projects, it’s likely that many people would become members/owners in multiple citadels. Like owning bitcoin, it might make sense to join citadels in case they catch on.

Goal 4:

Moonshot

It would not be a Bitcoin project if a shot at the moon, and ultimately the stars, were not imagined. In this case, Bitcoin will literally be brought to the stars.

Bitcoin Seed Vault

Before reaching for the stars, the citadel will seek to preserve the bitcoin protocol on Earth in as robust a way as is possible. Imagine creating multiple physical locations to mine and preserve bitcoin in facilities that are analogous to, but more resilient than, the Svalbard Global Seed Vault. The mining operations could be a source of additional income, but they would primarily finance the ongoing maintenance of the facilities to ensure that the citadel can safeguard literal rock solid copies of bitcoin’s protocol and history. The protocol code and transaction ledger could be backed up to various physical media including gold discs.

Bitcoin Node Space Probes

Once appropriate resources and technologies have been acquired, the citadel could develop Voyager style space probes to carry and record bitcoin’s protocol and ledger to the stars. This node will batch sync and record the ledger to gold discs. The options for bringing bitcoin to space are likely endless, but the analogy to Voyager seems fitting.

Being the Change

A common theme running through cypherpunk ideology, and the emerging ideologies connected to Bitcoin itself, is creating the things you want to see in the world. Passivity is a cancer and expunging its influence is likely going to be most complete by removing the host from its current environment.

There is nothing novel about claiming new lands or creating communities from scratch - this urge has been a primary driver of human history. Instead, the novelty comes from providing spaces which allow for new forms of cooperation to emerge.

Any future worth living in will require real work and coordination. Despite advances in telecommunications technology, it is not likely that humans will so easily give up their need for personal and physical interaction.

So, while the idea of intentionally forming a “Bitcoin community” may seem abhorrent to some, it seems like a necessary and logical outcome. Such a community does not have to be organized in the traditional sense, and certainly not in the modern political sense, but I do believe that being grounded in a physical community is both desirable and necessary in order to further worthy causes.

Whether you choose to join forces with other Bitcoiners in physical community, build your own fortress of solitude, or take on the life of a techno-nomad, it may be wise to

---

Visualization of the halving's supply shock

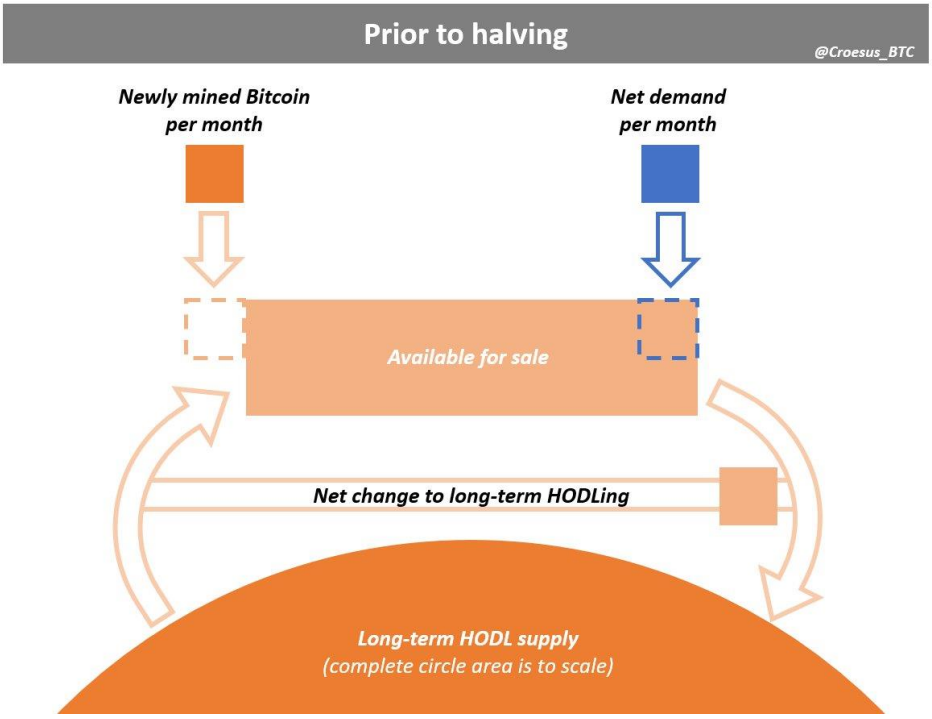
By Croesus

Posted October 23, 2020

Bitcoin halvings cause a supply shock. The slow accumulation of this supply shortage drives a bull market in the ensuing ~18 months.

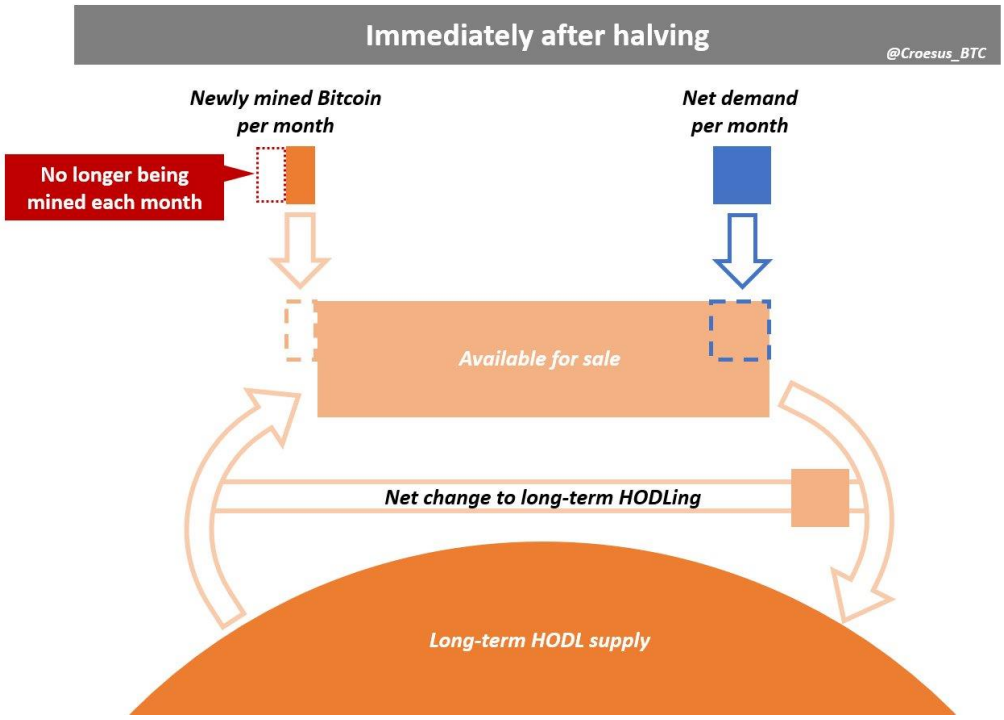
2012 and 2016 halving -> 2013 and 2017 mania. 2020 halving on track for same.

This thread attempts to visualize those mechanics.



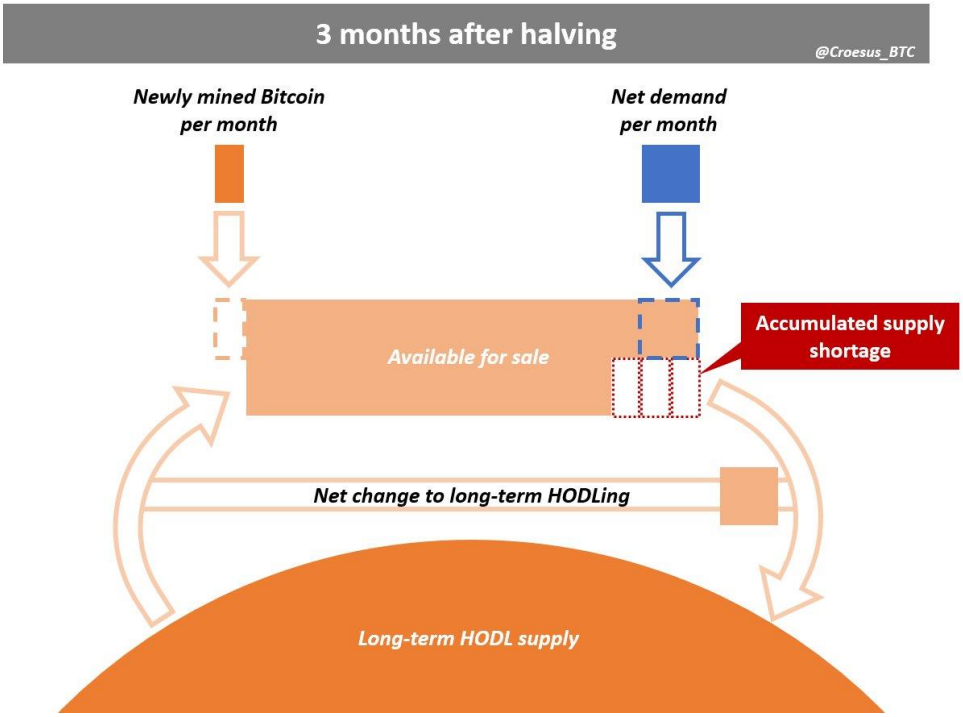
The halving causes new supply to be cut in half, but net demand remains the same. From this point on, a supply shortage accumulates.

Note: areas shown to scale for May 2020 halving. Assumed "available for sale" supply = UTXOs moved in prior month, aka 5% of circulating supply.



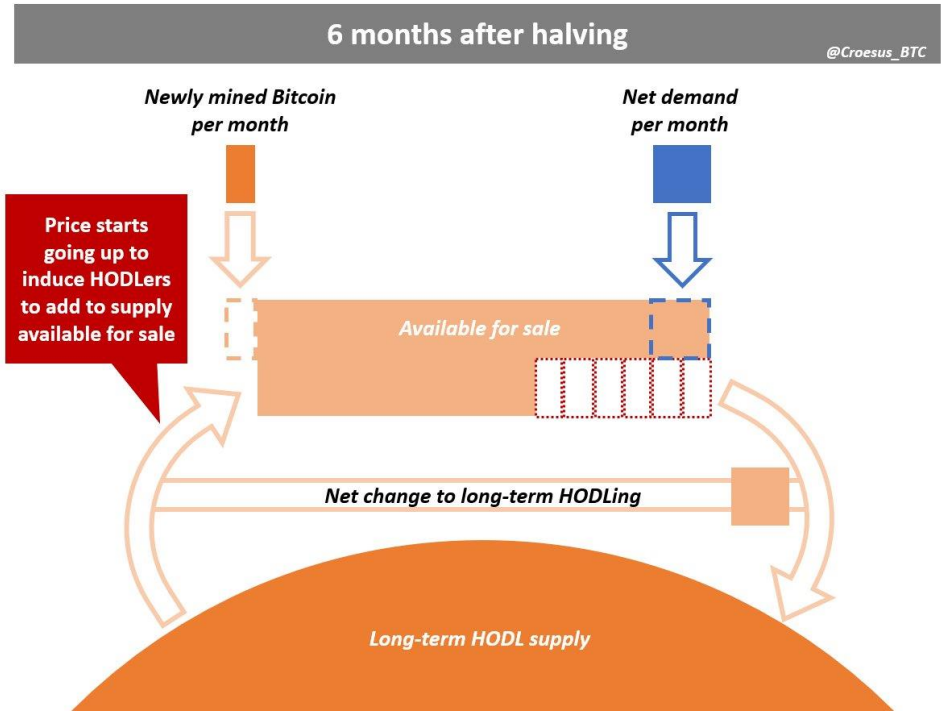
Supply shortage slowly accumulates. Net demand is moving twice as much supply into long-term HODLing as mining is creating each month.

Supply "available for sale" on exchanges shrinking, but accumulated impact still small.



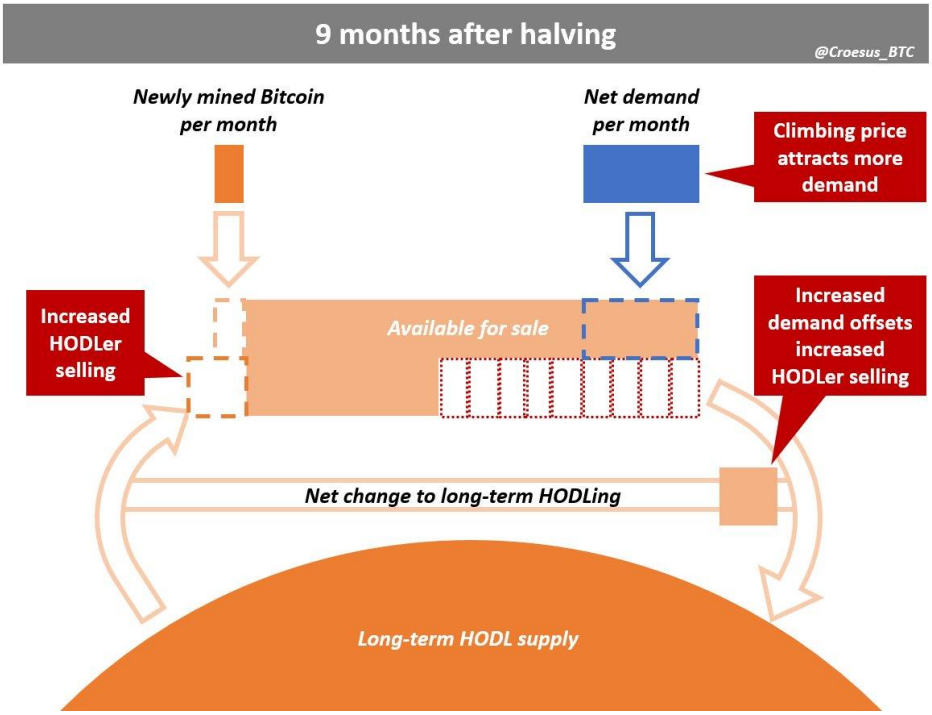
Accumulated supply shortage now significant. As market participants bid for significantly reduced "available for sale" supply, price drifts upwards.

In a typical market, this induces new supply production to increase and selling from existing holders to increase.



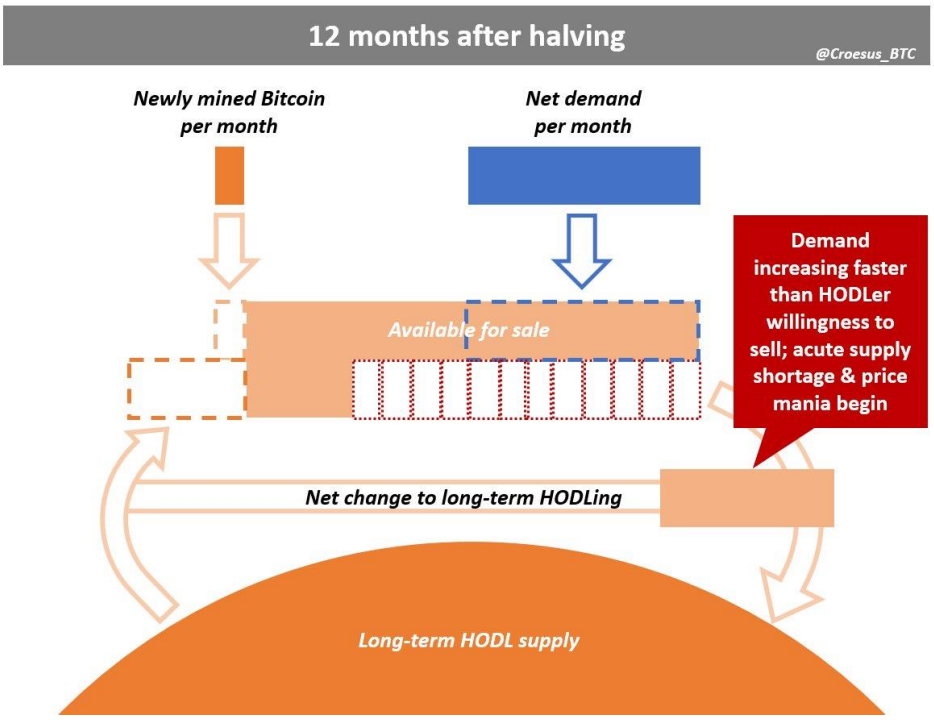
Miners cannot increase production, but HODLers do start to add supply to "available for sale".

However, because of Bitcoin's characteristics as a startup SoV asset that 99%+ of people don't have significant positions in yet… price going up also attracts interest & more demand.



As enthusiasm builds, new demand increases faster than HODLer willingness to sell. This causes a sharp increase in the rate of supply shortage accumulation, accelerating price growth.

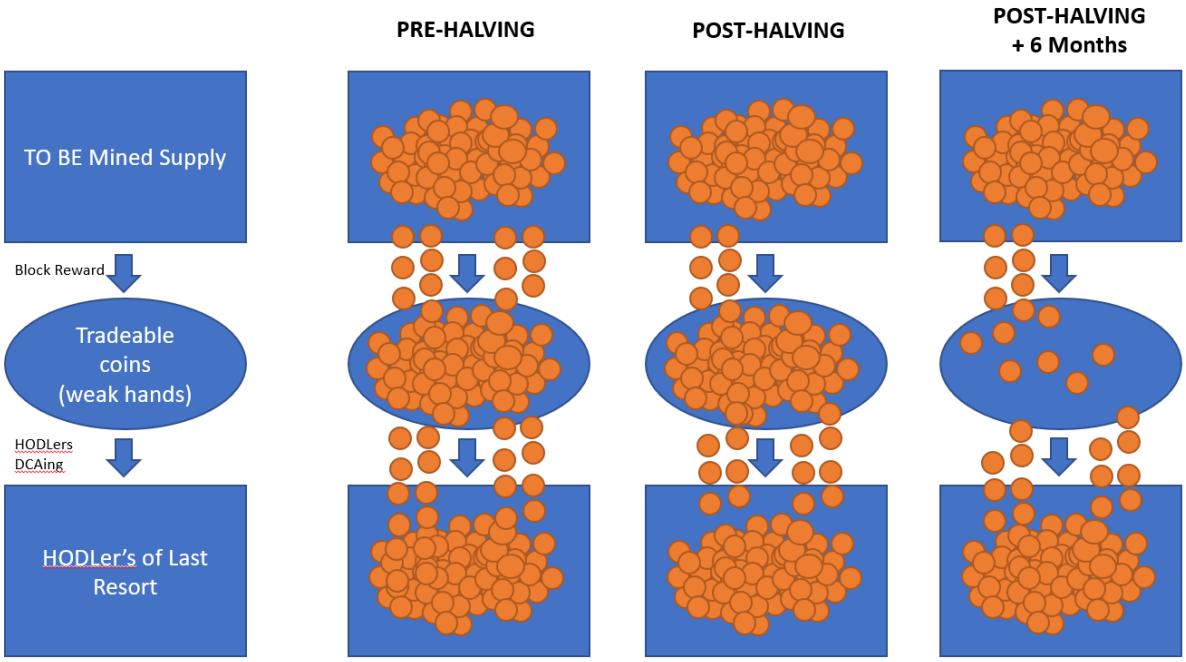
This begins the mania phase, which ends when HODLer willingness to sell flips net demand.



Granted, there is a great deal of noise obscuring these mechanics, so it's certainly not as clean as I've portrayed here. However, I believe this is the signal underneath the noise - the mechanics at the heart of how halvings drive 18-month parabolic bull markets.

Shoutout to @Moon__Capital for inspiring these diagrams with this excellent tweet:

How does a Bitcoin Halving drive UP price? It's simple. Coins get allocated to strong hands that understand bitcoin FASTER than new coins are mined. Eventually there are no more bitcoin for sale at $10k, only $500k.



Bitcoin and the Rhythms of History

By Brandon Quittem

Posted October 29, 2020

You're living through a particularly potent period in history.

But *you* already knew that.

Since the 2008 Global Financial Crisis, we've been in what Neil Howe and William Strauss describe as a "Fourth Turning." The final act in a drama that began on the heels of WWII.

Fourth Turnings are defined by the collective realization that "things are bad enough that we're willing to actually do something about it." The cement is wet and everything in the ***exterior world*** gets redesigned. Political, social, and economic structures reimagined.

"Sometime before the year 2025, America will pass through a great gate in history, commensurate with the American Revolution, Civil War, and the twin emergencies of the Great Depression and World War II." - The Fourth Turning by Neil Howe and William Strauss.

This essay explores the Strauss–Howe generational theory through the lens of Bitcoin.

Common ailments of the day, namely economic inequality, failing institutions, cultural decay, and the rise of populism were all predicted (and are easily explained) by this theory.

Practically speaking, you'll learn a new framework for understanding the world around you. It's neither perfect nor precise. However, if you squint hard enough you might catch a glimpse of the future.

Sections

Author's Note__: The first few sections are focused on summarizing the key concepts of The Fourth Turning. If you've already read the book, feel free to skip ahead for my analysis.

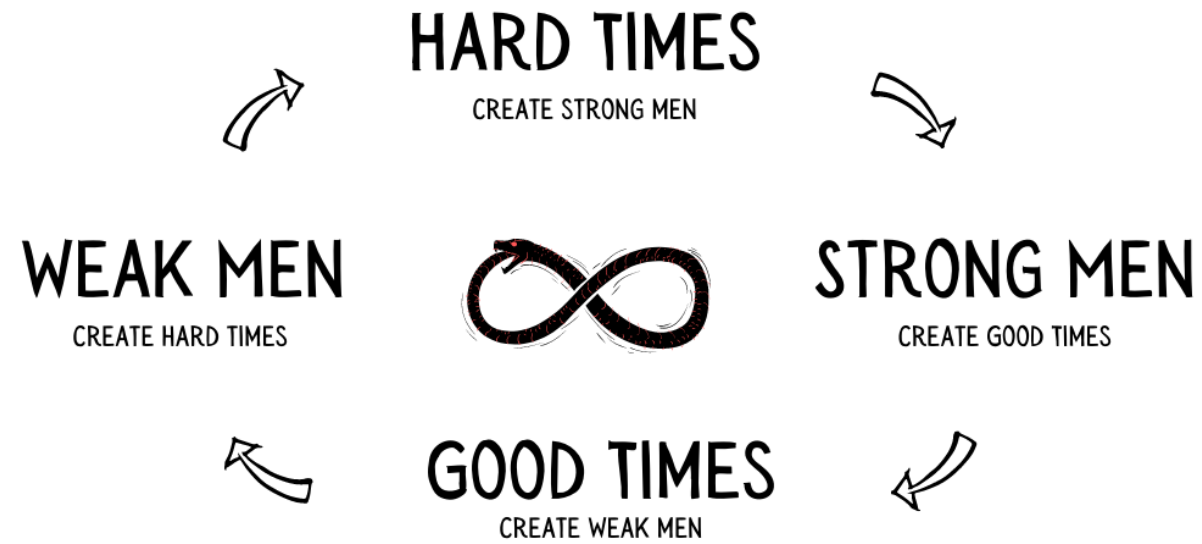
Seasons of Time (Introducing Fourth Turning Concepts)

Modern humans view time as a linear phenomenon. A steady march of progress from a "worst past" to an "improved future." However, life doesn't progress linearly, instead, it follows a natural rhythm, a circle of life if you will.

Practically speaking, days, months, and years are simply convenient names given to the observable cycles in astronomy. The earth rotating on an axis, the moon around our earth, and the earth circumnavigating the sun.

Spring, Summer, Fall, and Winter. Life and death. The carbon cycle, the water cycle. We're surrounded by natural cycles.

The wisdom of cycles is embedded in modern culture. Represented by common phrases like "history doesn't repeat, but it rhymes," and "there are decades when nothing happens, and weeks when decades happen."



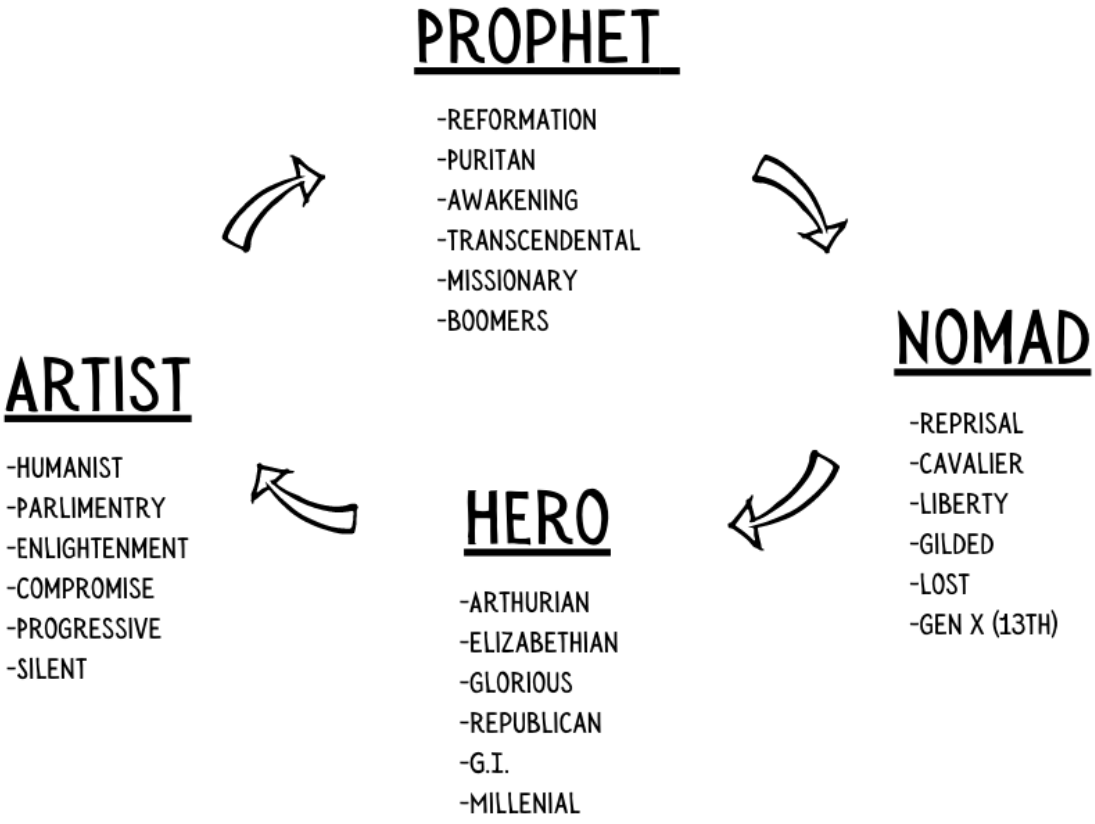
Ancient man observed a human cycle called the "Saeculum." Which essentially means "a long human life" or roughly 90 years.

The original meaning was "the amount of time between an event happening (ex: founding a city) and when everyone who experienced that event had died." At that point, a new Saeculum would start. According to legend, the gods allot a certain number of Saecula for every leader or civilization. For example, the gods allotted the Etruscans ten Saecula.

Each 90-year period (Saecula) can be divided into four stages (Turnings) each lasting approximately 22 years. These Turnings are often represented by the seasons (spring, summer, etc) or represented by the stages of life, namely youth, young adulthood, midlife, and old age.

The Four Generational Archetypes

Each Turning has a well-defined mood that produces a well-defined generation of people. Each generation embodies one of four archetypes that appear in a specific, repeating order.



The full cycle (four human generations) takes roughly 90 years or one full *Saeculum*. Each archetype follows a similar script throughout history:

- **Prophet (Baby Boomers) – principled, yet narcissistic
  **"Prophets grow up as the indulged, post-crisis children, come of age as the narcissistic crusaders of an Awakening, cultivate principle as moralistic midlifers, and emerge as wise elders during the next Crisis."
- **Nomad (Gen X) – Practical, yet unfeeling
  **"Nomads grow up as under-protected children during an Awakening, come of age as alienated young adults, mellow into pragmatic midlife leaders during a Crisis, and age into tough post-Crisis elders."

- **Hero (Millennials) – Competent, yet unreflective
  **"Heroes grow up as increasingly protected post-Awakening children, come of ages as the heroic young teamworkers of a Crisis, demonstrate hubris as energic midlifers, and emerge as powerful elders attacked by the next Awakening"
- **Artist (Gen Z) – Caring, yet indecisive
  **"Artists grow up as overprotected children during a crisis, come of age as the sensitive young adults of a post-crisis world, break free of indecisive midlife leaders during an Awakening, and age into empathic post-Awakening elders.

These generational trends are a natural, emergent, human phenomenon. We have well-defined stages of life and predictable human characteristics. Interestingly, we can observe this cyclical pattern going back 500+ years.

There is a symbiotic relationship between history and generations. The historic moment imprints itself onto the new generation. Then when that generation grows up it changes history. Repeat ad infinitum.

Each Saeculum is made up of Four Turnings

Just as generations follow cyclical patterns, each ~90-year Saeculum is composed of four well-defined stages called "Turnings" or "moods" that dictate how society responds to events.

Each Turning is defined by the constellation of generational archetypes in respective stages of life. Are the Hero archetypes still children or middle-aged managers? Are Prophets coming of age or are they elders controlling politics?

- First Turning (Rebirth/High/Spring) — 1946-1964
- Second Turning (Revolution/Summer) — 1964-1984
- Third Turning (Unraveling/Fall) — 1984-2008
- Fourth Turning (Crisis/Winter) —2008-2030?

The two most potent times in history are when Prophets and Heroes enter adulthood. Prophets come of age in Second Turnings and "cause a revolution" (eg: 60s Consciousness Revolution, Protestant Reformation) then two generations later the Hero generation "goes to war" during a Fourth Turning "crisis" (eg: WWII, Civil War, American Revolution, etc).

Throughout these generational cycles, history oscillates between classical opposing forces. Capital vs labor, liberty vs equality, isolationism vs expansionism. Again, driven by the constellation of generational archetypes at that point in time.

Humans have a tendency to rebel against the previous generation. This causes wild shifts in public sentiment. For example, the white-picket-fence 1950s sparked a backlash from the young Boomers who felt the culture was spiritually bankrupt. This led to the Consciousness Revolution.

Are some generations better than others?

The short answer is no. Each generation has strengths and weaknesses that must be balanced out by the others. This cycle serves as a guardrail ensuring humanity doesn't spiral out of control.

If the Prophet archetype is in power too long (Baby Boomer/Missionary), society would decay and nothing would be built because everyone is selfishly focused on their own interior world. Sound familiar?

On the other hand, the Hero archetype (Millennial/GI) rebuilds our socio-political institutions. However, if society was led by the Hero archetype alone, everything would become too orderly, bland, lacking liberty, art, or a rich internal experience. Example: Nazi Germany rise to power.

Doesn't technology drive changes more than demographics?

Most people assume technology is the primary force behind change. However, the Fourth Turning thesis claims the opposite. The cultural mood determines what technology gets built and ultimately adopted. Simply, the

mood signals the unmet demands which will ultimately be satisfied by entrepreneurs.

New technology, or any specific catalyst for that matter, doesn't guarantee a consistent outcome. Instead, our "response to a catalyst" is what drives change. Is society seeking change? Or hoping for stability after a period of chaos?

Our response to any catalyst is determined by which "Turning" we're in.

Let's explore two catalysts, the sinking of Lusitania and Pearl Harbor.

Both are similar events which resulted in dramatically different outcomes.

World War 1 started in 1914, right in the middle of a Third Turning. The Germans sunk the US Ship Lusitania in 1915. However, President Woodrow Wilson proclaimed the US would remain neutral. Americans widely supported this policy of nonintervention. It wasn't until 1917, when the US commercial interests were being disrupted, that the US officially entered the conflict.

Fast forward to December 7, 1941, when the Japanese bombed Pearl Harbor. The U.S. declared war on Japan the very next day and the whole country rallied around the decision. This was a similar catalyst as Lusitania, however this time it was during a Fourth Turning which is when the people are primed for war.

Where Are We In The Current Cycle?

The Millennial Saeculum at a glance:

- First Turning (The American High) — 1946-1964
- Second Turning (Consciousness Revolution) — 1964-1984
- Third Turning (Culture Wars) — 1984-2008
- Fourth Turning (Millennial Crisis) –2008-2030?

Since 2008, America has been in the Fourth Turning (crisis) which is the final stage in a roughly 90-year cycle. In order to set the context, let's rewind to the beginning of our current cycle, known as the "Millennial Saeculum."

First Turning: The Great American High (1946-1964)

Lost generation enters elderhood / G.I. generation enters midlife / Silent generation enters young adulthood / Boomers enter childhood

Our current cycle began as we wrapped up WWII and America ascended to a global superpower. Everyone's grown tired of fighting, civic duty reaches a

peak as we rebuild back home. Soldiers returned from battle and wanted a "decent life." Social movements stalled. Middle class grew and prospered. Increased peacetime government budgets were uncontroversial. Collectivist infrastructure flourished as we built suburbs, interstates, and (regulated) mass communications. Declaring an "end to ideology," authorities presided over a bland, modernist, spiritually dead culture.

Second Turning: Consciousness Revolution (1964-1984)

G.I. generation enters elderhood / Silent enters midlife / Boomers enter young adulthood / Gen X enter childhood

Kicked off with urban riots and campus protests. Supercharged by anti-Vietnam War sentiment led by a rebellious youth. Even though they were given everything, Boomers led the revolution. They clashed with the bland "Leave it to Beaver" culture lacking anything resembling spirituality. This gave rise to feminist, environmentalist, and black power movements. We also saw the destruction of the nuclear family and a rise in violent crime. Peak chaos hit with Watergate in 1974 and passions turned inward towards "New Age" lifestyles and spiritual rebirth. The revolutionary mood expired when Reagan was elected for a second term, converting former hippies into selfish yuppies.

Third Turning: Culture Wars (1984-2007)

Silent enter elderhood / Boomers enter midlife / GenX enter young adulthood / Millennials enter childhood

An unraveling begins as society embraces the liberating cultural forces let loose by the boomer-led consciousness revolution of the psychedelic 60s. Personal satisfaction is high, and few national problems demand immediate action. Public is concerned about widening inequality, civic duty declines, and culture begins to diverge into competing value camps. Pervasive distrust of leaders and institutions, popular culture bends towards futuristic dystopia memorialized by ***Total Recall*** dysfunction, ***Robocop*** crimes, ***Terminator*** punishment, and ***Independence Day*** deliverance from evil. People can now ***feel*** the pain, but collectively we cannot yet ***do*** anything.

Fourth Turning: Millennial Crisis (2008-2030?)

Boomers enter elderhood / GenX enter midlife / Millennials enter young adulthood / Zoomers enter childhood

37 years after leaving the gold standard, Americans have experienced rising inequality, increased debt, and rampant inflation. Eventually, we have to pay the piper, and the time is nigh.

The 2008-2009 Global Financial Crises kicked off the Millennial Crisis, and the population finally demanded change. Occupy Wallstreet movement surged, Obama took office campaigning on "Hope and Change." Society shifts away from individualism and towards collectivism marked by the rise of Social Justice Warriors, cancel culture, and policing speech. The crisis heats up in 2020 with the Covid pandemic, widespread economic depression, and riots erupting on the streets.

Anatomy of a Fourth Turning (Crisis)

During Fourth Turnings, the old social order combusts and gives birth to something entirely new. The ancients called this ***ekpyrosis***, nature's fiery moment of death and discontinuity.

Welcome to winter. A time of fire and ice. The supply of social order is still falling, but the demand for order is steadily rising. Although not required, Fourth Turnings historically end with total war.

"Pleasures recede, tempests hurt, pretense is exposed, and toughness rewarded" -Victor Hugo

While Fourth Turnings are not fun, this is not a doom and gloom prophecy. As a society, we need these moments of crisis. They serve as brush fires to clean out the decrepit institutions to make way for new growth. This generates buy-in from young people. Out with the old and in with the new. Optimistically, it's a regenerative process allowing the cycle to continue.

Morphology of a Crisis (Fourth Turning)

- **Catalyst (2008)** – each crisis begins with an event (or series of events) that produces a sudden shift in the mood. *2008 global financial crisis, Occupy Wall Street, and Obama's "Hope and Change."*
- **Regeneracy (2012)** – once catalyzed, society finds a new counter entropy that reunifies and re-energizes civic life. *Rise of "Democratic Socialism," Bernie Sanders's popularity, "equal pay for equal jobs," and Social Justice Warriors enforcing civic duty to ensure everyone is "equal" during hard times.*
- **Climax (2020?)** – A crucial moment that confirms the death of the old order and birth of the new. Typically the climax is a war (WWII, Civil War, etc), but so far all we've experienced is the Covid Pandemic. Are we destined for war? *War on the Virus, loss of liberties, riots, economic inequality becomes the hot topic, and Universal Basic Income begins*.
- **Resolution (2026?)** – A triumphant or tragic conclusion that separates the winners from the losers, resolves the big public questions, and establishes the new order. *This has yet to play out in our current cycle.*

> *Speculation: Overcoming Covid (or another, larger conflict), UBI lightens the mood, bootstrap a new global financial system.*

Each Crisis ends with a "resolution period" which historically speaking is 3-5 years before a crisis concludes. We haven't hit the resolution yet, but we'll know when the mood transforms into one of exhaustion, relief, and optimism. We'll see a resurgence of faith in humanity and authority, and society will yearn for a good and simple life.

"When you're going through hell, keep on going" -Winston Churchill

Today's oldest Americans recognize this mood from the previous Fourth Turning during the Great Depression and WWII. Cultural artifacts from the last Resolution period include "Somewhere over the rainbow" and the 1939 New York World's Fair. *A better future on the horizon, if we could only work together and make personal sacrifices*.

Fourth Turnings of the Last 500 Years

During a Crisis, the outer world of power and politics is completely rearranged. The old paradigm dies making way for anew. Historically, Fourth Turnings have been settled with bloody conflicts. Are we destined for war sometime in the 2020s? Maybe not, but more on that later...

"History never repeats itself. Man always does." — Voltaire

What can we learn from previous Fourth Turnings?

Wars of Roses Crisis (1459-1487) — Kicked off with a fracturing of England's most powerful families, the Lancasters (Lannisters) and the Yorks (Starks). Defined by a period of political turmoil, decades of conflict, and the crown changed heads six different times. Fun fact: This was the period George R.R. Martin based Game of Thrones on.

Transition: England entered the crisis as a traditional medieval kingdom; later emerged a modern monarchical nation-state.

Armada Crisis (1569-1594) — Newly Protestant England was threatened by the mighty Catholic Habsburgs. Lead to Assassination attempts on Queen Elizabeth, Francis Drake circumnavigating the globe with Spanish treasure, and eventually, the great Spanish Armada fell.

Transition: England entered the Crisis as a struggling heretical nation; later emerged as the global superpower with an expanding global empire.

Glorious Revolution Crisis (1675-1704) — Began with Bacon's Rebellion, King Philip's war, and escalating conflicts with the Algonquin Indians. Hit a crescendo with the Americans winning a decade long war against Canadian

New France. Churchill described this period as having "changed the political axis of the world forever."

Transition: English-speaking America entered the Crisis as a fanatical colonial backwater, and later emerged as a stable society whose education and affluence rivaled its former European home.

American Revolution Crisis (1773-1794) — Began with the Boston Tea Party, Samuel Adams "committees of correspondence," arming local militias, and the signing of the Declaration of Independence. The "mood of emergency" calmed after the ratification of the Constitution.

Transition: British America entered the Crisis as a collection of violent, yet loyal, Colonies. Later emerged as the most ambitious experiment in Republican Democracy the world had ever seen.

Civil War Crisis (1860-1865) — Began with John Brown's raid and Abraham Lincoln's election which quickly led to Southern states seceding and the Civil War. Hit its climax during the Emancipation Proclamation and Battle of Gettysburg. Eventually concluding after Robert E Lee surrendered, and soon after the assassination of Lincoln. Uniquely, America didn't feel optimistic after this crisis; instead, there was a feeling that a tragedy had simply run its course.

Transition: The United States entered the crisis as a racially divided agrarian republic, and emerged as an industrializing dynamo, battle scared yet newly dedicated to equal citizenship.

Great Depression and WWII Crisis (1929-1946) — Kicked off with the stock market crash, leading into the dust bowls and great depression. Attack on Pearl harbor ignited a unified public response leading to World War II. Crisis mood calmed down when the Axis capitulated, demobilized, and brought a surprising period of peacetime prosperity.

Transition: The US entered the Crisis as an Isolationist, fledgling nation; and later emerged a global superpower with industrial prowess, democratic institutions, and control over much of the world's gold. New institutions include the UN, NATO, World Bank, IMF, Bretton Woods, etc.

Supply and Demand for Order

The "supply and demand for order" in society fluctuates over time. Depending on the position of these two variables, you can determine the direction society is heading.

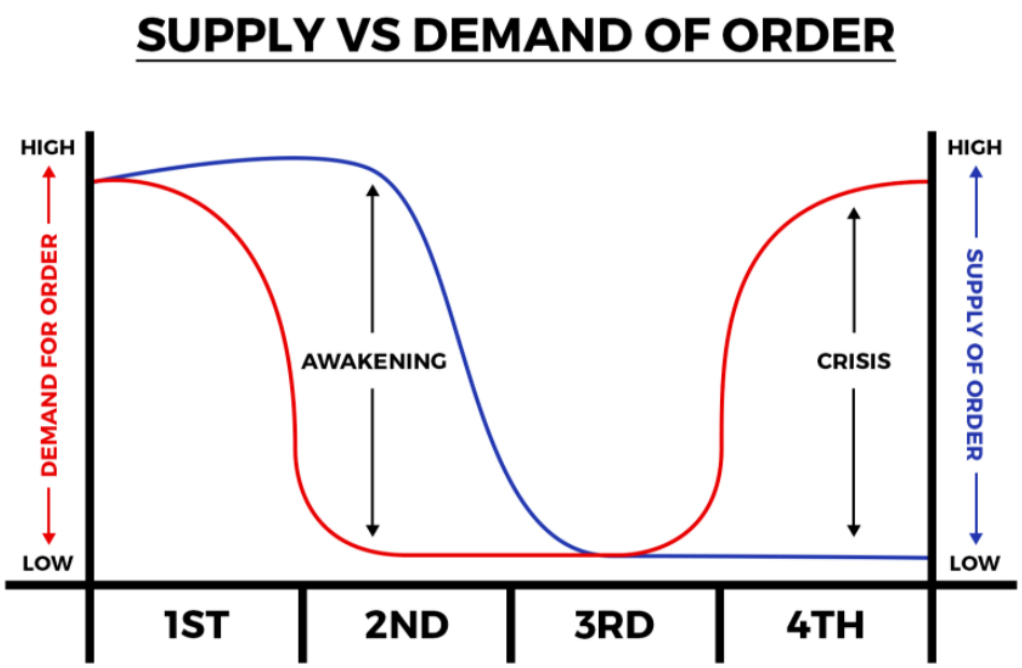


Chart designed by Nick Ward @nckbtc

The two most explosive points come when the gap between supply and demand for order is widest. Second Turnings produce an Awakening (internal change) and the Fourth Turnings produce a Crisis (external change).

During Third Turnings, called "unravelings," we see both low supply and low demand for order. Everything is slowly falling apart but no one seems to care. Then after enough potential energy is stored during the Third Turning, the mood shifts. Fourth Turnings are a period when the supply of order is at rock bottom, but the demand for order starts rising.

After roughly 40 years of declining order, we've let our institutions crumble. It's no secret that our governmental bodies, legal system, banking, healthcare, and education are derelict. Beginning around the 2008 global financial crisis, people increasingly realized how important our institutions actually are. The mood shifts and the demand for order rises.

What if our government was helpful? What if healthcare was great? What if our education system was incredible? This increasing demand for order juxtaposed next to failing institutions (low supply of order) catalyzes widespread structural change.

Lessons From The Previous Fourth Turning (1929-1946)

The previous Fourth Turning (1929-1946) has the most in common with our current situation. Join me for a stroll down memory lane.

"Those who don't read history are doomed to repeat the mistakes of the past"

In response to the stock market crash of 1929 and the widespread economic hardship, the mood became one of desperation. Previously unthinkable policies (born out of the New Deal) gained popular support as Roosevelt led the greatest expansion of the Federal Government ever known. This was a natural consequence of implementing the Federal Reserve in 1913.

Social dynamics in the 1930s mirror today

Both the 1930s and the 2010s produced declining fertility rates, low migration to America, declining violent crimes, declining use of alcohol and tobacco, and many young people living with their parents.

This social dynamic is consistent anytime you have the "hero" archetype in young adulthood. For example, Millennials today and GI Generation in the 1930s.

The start of widespread deficit spending (The New Deal)

In 1933, Roosevelt issued Executive Order 6102 which "forbid the hoarding of gold coins, gold bullion, and gold certificates within the continental United States." The stated reason for this desperate move was "hard times caused hoarding of gold, stalling economic growth and worsened the depression."

Also in 1933, FDR kicked off his flagship program The New Deal which focused on three things: relief for the poor (and unemployed), recovery of the economy, and reforming the financial system to prevent another depression.

Since the crisis was so severe, progressive leaders and average Americans demanded the Fed take greater responsibility to "help the poor" and "prevent poverty." The Social Security Act of 1935 birthed unemployment insurance, Social Security, and Welfare.

National Recovery Administration (NRA) was formed which sought to stabilize the economy by artificially fixing wages and prices, establishing production quotas to deter "dumping" of surplus inventories of products on the consumer market. Similarly, the Agricultural Adjustment Agency was created to curtail farm production in order to maintain higher farm prices.

The Federal Deposit Insurance Corporation (FDIC) was created to rebuild confidence in the banking sector. Now depositors could trust banks as their deposits were "insured."

The Securities and Exchange Commission (SEC) was formed in response to public sentiment that "excessive speculation" led to the 1929 stock market crash and the subsequent great depression.

The tax rate for the highest earners soared from 25% to almost 63% by 1937 in an attempt to "soak-the-rich." Blaming the rich is common during Fourth Turnings as the social consensus is led by the Hero Archetype (G.I. and Millenials) who reject individualism and fan the flames of populism.

Roosevelt goes full Keynesian

Roosevelt took office in 1932 claiming he would balance the federal budget. After the "Roosevelt Recession" of 1937-1938 was blamed on "a reduction in federal spending," Roosevelt accepted the advice of British economist John Maynard Keynes.

Keynes argued that technically advanced economies would need either:

(i) Permanent budget deficits or (ii) Redistribution of income away from the wealthy to stimulate the consumption of goods and to maintain full employment.

The acceptance by the Roosevelt Administration of what became known as Keynesianism established the precedent of using deficit spending as a vehicle for promoting economic recovery in times of national crisis.

Big business leaders joined the Keynesian train (incentives win the day)

The obvious connection between deficit spending and economic expansion was not lost on many Americans, including business leaders who much preferred large deficits to Keynes's alternative of massive redistribution of wealth through taxation as a way to sustain America's prosperity in peacetime. As Charlie Munger says, "show me the incentives and I'll show you the outcome."

The 1940s and WWII

The period of tremendous fiscal spending continued into the 1940s to support the war efforts. Debt levels reached their peak but were quickly resolved after WWII due to America's relative position of strength and the new monetary system (Bretton Woods)

WWII left the world in shambles, a typical process during Fourth Turnings. Now what? Time to rebuild while the *cement is still wet*.

Enter Bretton Woods: Bancor vs Gold-pegged USD

In an effort to put the financial pieces back together, world leaders gathered in Bretton Woods, New Hampshire to create a new global monetary system.

The two main proposals were:

- **Bancor —** Keynes championed the bancor system, a supranational settlement medium based on a basket of currencies. Under this system, no one could independently print more bancors, ironically similar to Facebook's Libra.
- **Gold-backed USD** —Since the US was in a relative position of global power, they could create a gold proxy by pegging all U.S. Dollars to gold. This system was to be managed by the IMF and World Bank. The entire world can rest easy knowing U.S. dollars are "as good as gold."

Obviously, they decided on a USD proxy for gold which only lasted about 25 years before Nixon closed the gold window pushing us into a strictly fiat system in 1971.

Besides a new monetary standard, both the IMF and World Bank were also created at Bretton Woods.

The seen and unseen

During Fourth Turnings, the global structures are torn down and rebuilt. These drastic measures seem warranted in the moment. However, each decision comes with a bouquet of seen and unseen consequences. This is often called the cobra effect which occurs when an attempted solution to a problem makes the problem worse. In other words, centrally planned institutions usually fail in managing complex systems.

Unintended outcomes aka "unseen consequences" of the previous Fourth Turning:

- **National Recovery Administration** – Intended to "manage the recovery." Ultimately fixed prices, stifled competition and sometimes made American exports uncompetitive. Another reminder that central planning slows economic recovery.
- **Agricultural Adjustment Act** – Intended to improve food production. Ultimately paid farmers not to produce, raised food prices and kicked thousands of farmers off the land and into the unemployment lines.
- **FDIC insurance** – Intended to reduce the risk of bank runs. Ultimately taught bank customers they no longer need to shop around for a well-run bank. If the market doesn't force banks to behave, they will take advantage of their position. This led to a moral hazard we're still paying for 60+ years later.
- **Keynesianism** – Intended to avoid economic damages today, at the expense of tomorrow. Resulted in never-ending deficit spending and a pattern of ongoing currency devaluation which we may see come to a head in the 2020s.

- **SEC (and other regulators)** – Intended to "prevent" excessive market speculation. Ultimately got captured and now serves as an extension of the most powerful corporations (creating harmful monopolies that stifle innovation).
- **Pensions and Social Security** – Intended to quell social unrest, which can work when young people are producing enough to pay for the entitlements of the elderly. Ultimately as soon as demographics flipped, the mounting entitlements from a retiring boomer generation created a catastrophe.

It's clear we've outgrown the infrastructure created between 1929-1946. As the cycle goes, it's time to tear down the old world and build anew.

Does that mean we should just succumb to nihilism? No. Your actions matter as the results of this decade will define the next 100 years. However, you can be sure they'll have unseen consequences for future generations to remedy.

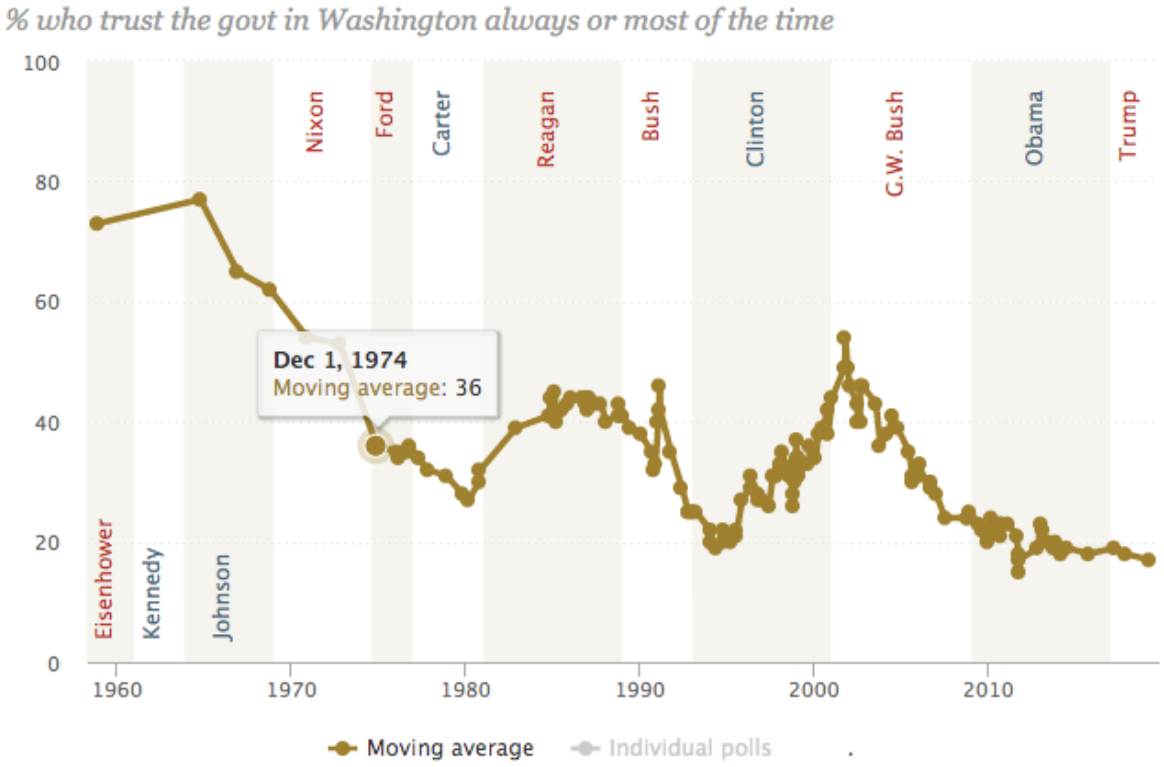
Analyzing our Current Fourth Turning (2008-2030?)

Considering what we know about previous Fourth Turnings, here are the key trends to follow as society seeks to deconstruct existing institutions.

Domestic Politics, The rise of Populism, and Everyone's a Socialist

2020 marks the widest partisan gap since the 1930s. People under 30 are predominantly left-leaning and those over 60 heavily lean right. To make matters worse, the most ideological generation in history (Boomers) controls politics.

Trust in the central government is the lowest it's been in the last century. In 1961, 80% of people said they "trust the Federal government to do the right thing." In 2020, that number dropped to only 20% trust the Federal government.



Source: *Pew Research*

The people realize the socio-political infrastructure is not working and they're grasping for a solution. This creates demand for a "strong man" leader to get us out of this mess.

People increasingly believe that collective action is the only way to make a civic change. This leads to popular culture demanding consensus instead of accepting individualism. Popular sentiment gets harnessed (Populism) as propaganda for the purpose of overtly reinforcing "good" conduct (cancel culture, etc). With the ability to make a change, leaders start exaggerating the bad stuff (instead of downplaying it like they do in Third Turnings).

Trump's 2016 presidential victory is a symptom of the "crisis mood." The people wanted change and Trump successfully captured the mood with a successful "drain the swamp" campaign. The rise of Bernie can be explained in the same way. The consolidation of power is guaranteed, but if we're not careful we'll fall into totalitarianism as we're seeing around the world.

Just like FDR in the 1930s, America is doomed to repeat a decade of expanding the Federal government. In 2020 alone, we saw Universal Basic Income ("Trump Bucks"), business bailouts, yield curve control via QE, and more. Will this be enough? Not a chance. We're just getting warmed up.

"By the end of this decade, the Fed's balance sheet will be between $40T and $50T" - Felix Zulauf on The Grant Williams Podcast

Before the decade is over, Modern Monetary Theory (MMT) will run its course. We'll see some combination of Universal Basic Income (via Central Bank Digital Currencies), college loan forgiveness, free healthcare, A New New Deal, Increased minimum wage, and more. The appetite for handouts will be insatiable.

What about the fiscally conservative party? There isn't one. You wouldn't expect helicopter money from the "fiscally conservative" party, but things are different in 2020. Everyone's a Socialist now.

Foreign Affairs, Geopolitics, and Isolationism

Populism, and in many cases totalitarianism, is rising all around the world. Look no further than Maduro's Venezuela, Duterte's Philippines, Modi's India, Xi's China, the Yellow Vest Movement in France, and many more. This points to a global synchronization of these demographic cycles since WWII. In addition, this is the first time in history we've seen the world connected under a globally dominant reserve currency (USD). If every country is in a Fourth Turning simultaneously, the results could be explosive.

3rd Turnings produce relaxed borders, increased international travel, and waves of immigration. Fourth Turnings reverse all of that. Global trade as a percentage of global GDP peaked in 2008 and has been declining since. The pendulum is swinging towards isolationism.

Covid exposed our reliance on foreign imports, especially from an increasingly hostile China. Politicians will respond by incentivizing manufacturing in America and the market will support it.

America's foreign policy will support global trade as long as it comes with no political baggage. A nice parallel to America's foreign policy at the end of the 18th century:

"The great rule of conduct for us, in regard to foreign nations, is, to extend our commercial relations with as little political connection as possible." -George Washington's farewell address (1796)

Minimizing political baggage abroad is good for many things, including the fact that trade is more profitable than war.

The shift to isolationism will expose nations who are reliant on crucial foreign imports such as energy, food, and medicine. Combined with a slowing GDP and increasing sovereign debt, nation-states will flail in desperation. Expect more civil wars, hyperinflation events, deadly totalitarianism, and regional

conflicts. Smart nations will start monetizing energy assets by mining Bitcoin and eventually buying it outright.

Optimistically, isolationism will increase the competition between nation-states. When countries compete for citizens, individuals win. Nations will increasingly compete for capital by selling passports and offering favorable tax treatment. Those with capital can shop around, those without are tied to the fate of their passport.

Protectionism, Demographics, and Entitlements

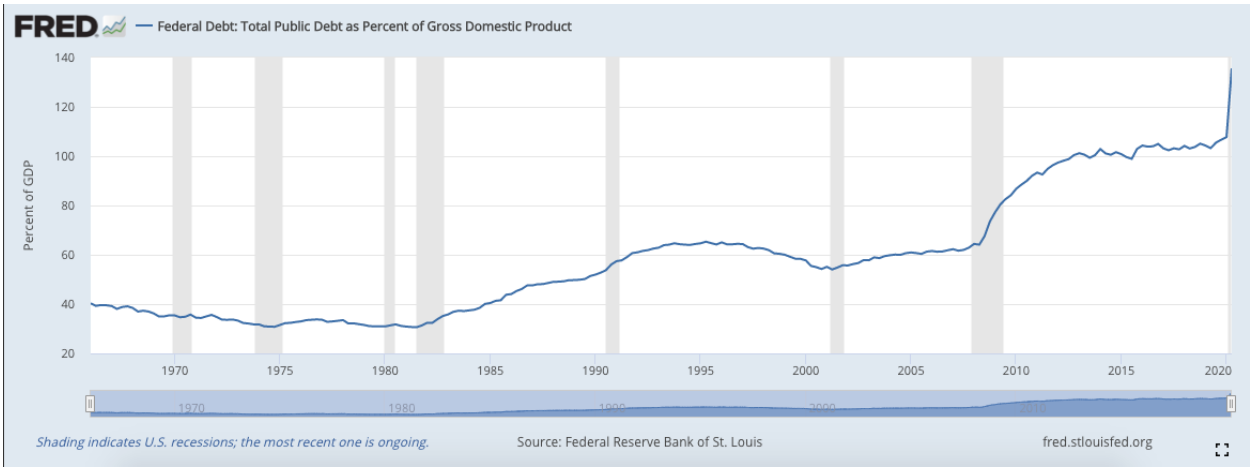
In the 1990s, America made a conscious effort to increase child-rearing efforts. The young gen Xers at the time were universally disliked by adults. They were the neglected bad boys, the Latchkey kids, as portrayed by Mikauley Caulkin in ***Home Alone***. This produced a popular backlash in America resulting in the Millennial generation. Millennials were defined by a period of over-parenting, baby-on-board stickers, bike helmets, D.A.R.E. programs, and 13th place ribbons.

This mood of "protectionism" was not isolated to child-rearing. In fact, our central bankers and governments had a protectionist bias. The "can't let anything fail" attitude created an economic environment where companies cannot fail, interest rates are suppressed, and the fed will backstop the economy with QE infinity. This pushed up boomer assets and left millennials with nothing to buy.

In 2020 we have top-heavy demographics. The Boomers are retiring which means entitlement liabilities are increasing steadily. Unfortunately, there isn't enough value being produced by young people to pay for Boomer retirements.

"Long term productivity has slowed, this has driven entitlements from 4.7% of U.S. GDP in 1965 to 14.7% of GDP now....We need to shrink entitlements back as % of the pie and need to resolve it before we have a crisis. Unfortunately, though, I don't see how we're going to get out of this." - Alan Greenspan, 2015 [source]

Due to these entitlements, America is forced to "print more or allow a revolution." We've already seen a 22% increase in base money in 2020 alone. This brought the U.S. Debt-to-GDP Ratio to 135%. Not to mention the economy is slowing down. This means sovereign debt must continually increase, likely to unsustainable levels.



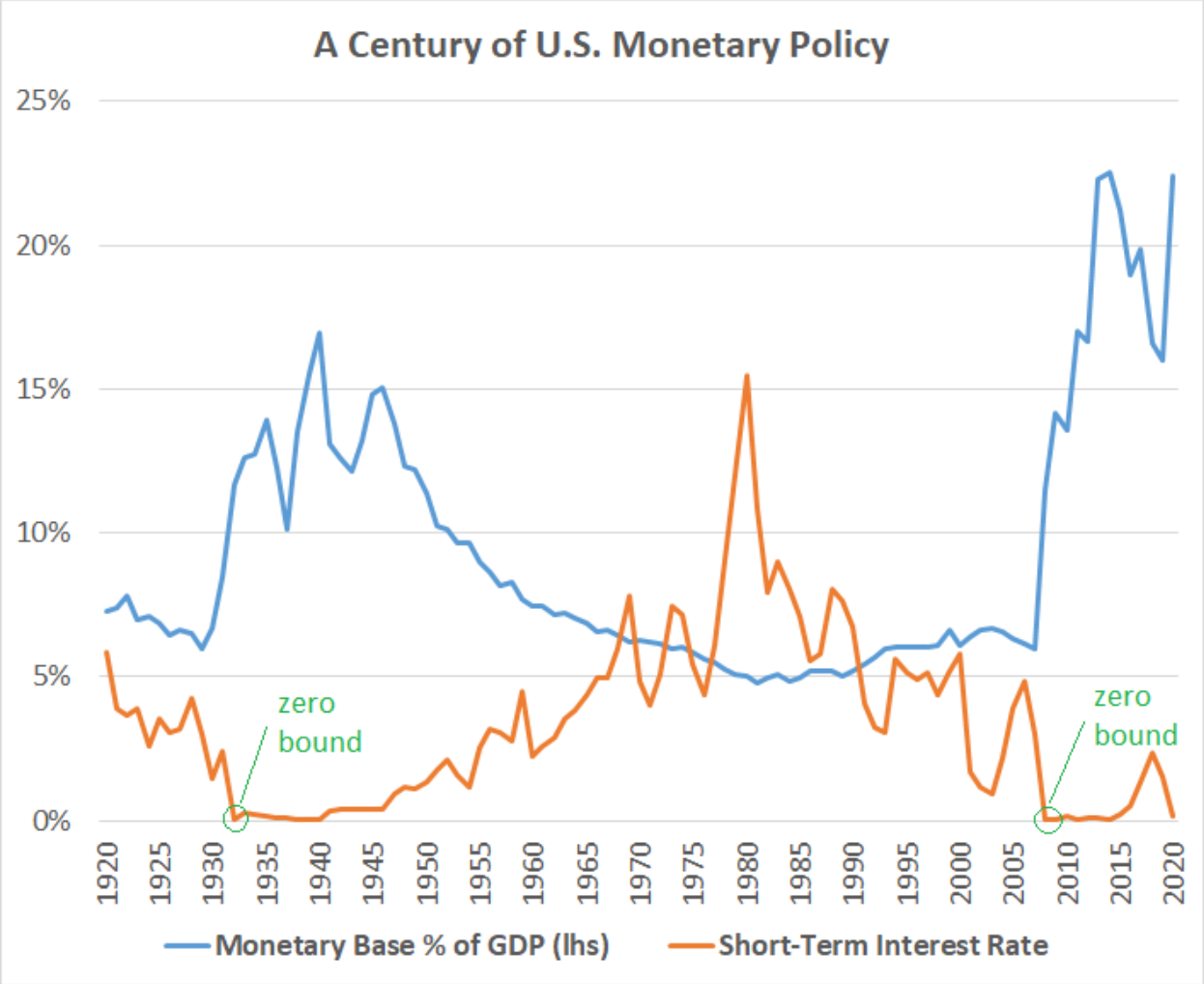
Source: *Federal Reserve Bank of St Louis*

In previous Fourth Turnings, wealth gets taken from the old and wealthy and given to the young and poor. However, wealth redistribution only eases social tensions temporarily, it doesn't fix the underlying debt problem.

What do we do with all the debt?

In Lyn Alden's recent essay, she examines the fiscal and monetary policy of the last century. She explains Ray Dalio's long term credit cycles and the inevitable monetary reset that follows. Interestingly this long-term credit cycle overlaps nicely with the 90-year cycles laid out in the Fourth Turning. Do demographics drive the long-term credit cycle or is it the other way around?

Notably, there is a major overlap with the 1930s-1940s and today. Both are Fourth Turnings that began with a monetary/banking crisis (1929 vs 2008) which led to interest rates being pushed to 0%. This makes central banks less powerful as their main tool (interest rate manipulation) is impotent.



Source: Lyn Alden

Soon after, America gets plunged into a spending/fiscal crisis marked by WWII and Covid-19 (potentially another conflict in the 2020s). With powerless central banks, the only option is massive government spending in the form of QE and UBI. Just like in the 1940s, this setup indicates an inflationary period and a high risk of currency failures coming in the 2020s. Although, we'll likely see a couple of years of deflation first.

This brings us to the key question: what do we do with all the debt?

One option is a decade or two of austerity (think high taxes and low government spending). Highly unlikely since there is no political will for austerity.

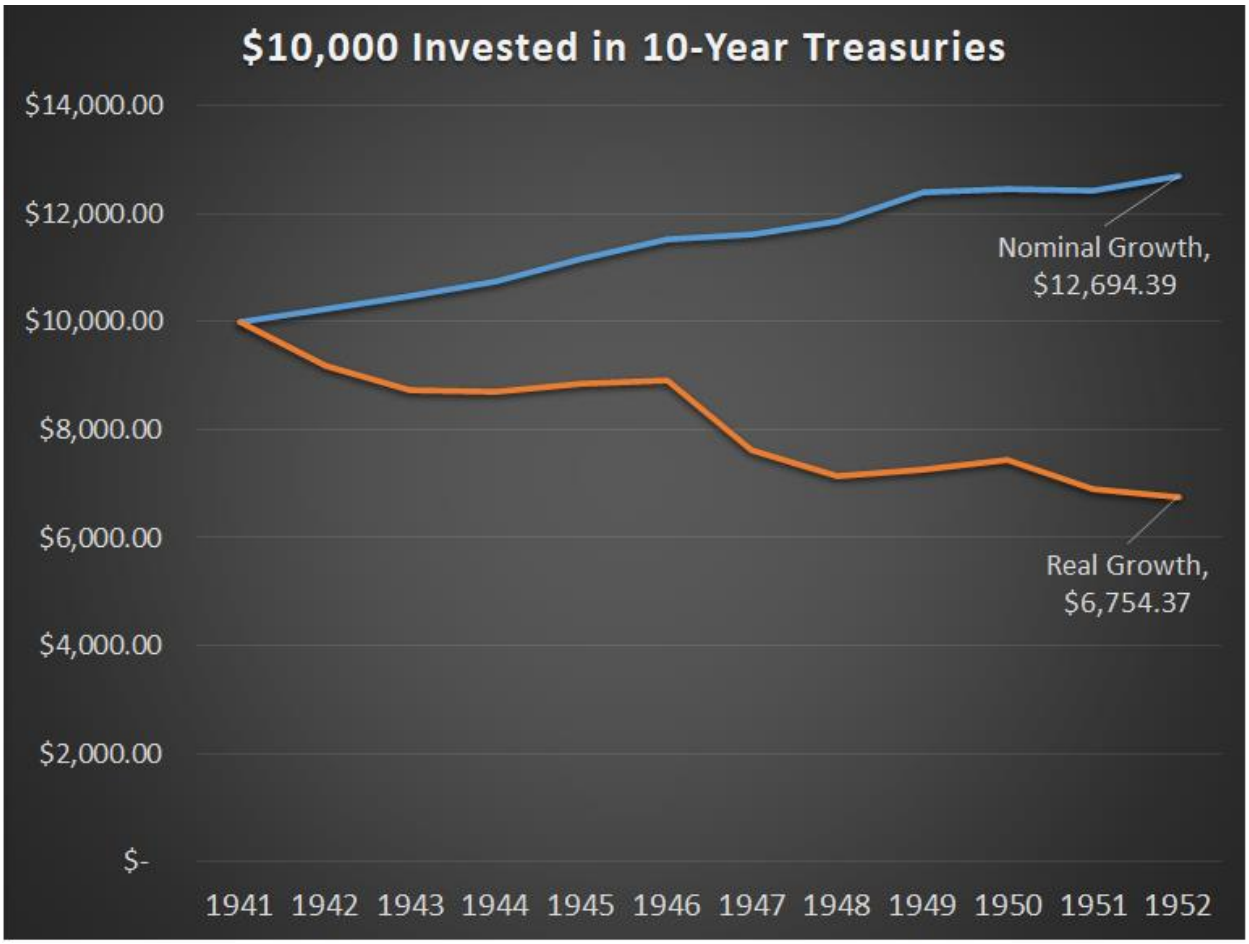
Increase global GDP? Highly unlikely as the world is heading into a recession and the demographics are against us.

What about debt forgiveness? Since the Fed owns most of the student loan debt, they can simply press "delete" on their spreadsheet. Seems pretty likely under the circumstances and it would empower young people to start families and buy homes from boomers.

How about increasing taxes on the wealthy? During the previous Fourth Turning, the tax rate for the highest earners soared from 25% to almost 63% by 1937. This was known as "soak the rich" in the 1930s and a similar sentiment is gaining steam in America today. Seems inevitable as millennials take power away from aging boomers.

Our final option is to devalue the debt in real terms (inflation). This would likely be accomplished by Quantitative Easing (QE) and increasing the broad money base.

The federal reserve will now have an unlimited budget to buy as many assets (treasuries, corporate debt, and soon to be equities) as necessary to keep interest rates down. Practically speaking, that means anyone holding dollars or bonds will see negative real returns for the next decade. Again, just like the 1940s.



Source: Lyn Alden by way of Robert Shiller, Aswath Damodaran

At the same time, the government will increase the broad money base with various forms of government spending and UBI. Programs like a "New New Deal" and direct to individual UBI facilitated by a Central Bank Digital Currencies (CBDC) are likely.

What about hyperinflation?

As weak currencies break down, some will hyperinflate which draws more attention to Bitcoin's value proposition. Volume taken from LocalBitcoins exchange shows that nations with weakening currencies lead to increased Bitcoin adoption.

How long before a nation-state moves heavily into Bitcoin? Venezuela already runs BTC Pay Server, Iran gives tax incentives to miners, Marshall Island tried launching their own ICO. The writing's on the wall. Judging by incentives alone, smaller nations will adopt Bitcoin by 2030, likely sooner.

What about the United States? Although some Bitcoiners believe we'll see hyperinflation with the USD, I'm skeptical. The USD is still in high demand globally and the U.S. has a ***relatively*** strong economy with ***relatively*** sound demographics. The USD won't hyperinflate this decade, but it will be majorly devalued (along with all other currencies).

We haven't seen enough Conflict yet

Every Fourth Turning in the last 500 years climaxed with a bloody conflict. Climaxes of previous Fourth Turnings include WWII, Civil War, and the American Revolution.

Does that mean we're destined for total war in the 2020s?

Not necessarily. War represents a period of maximum urgency which mobilizes society for a specific purpose. We don't necessarily need bloodshed, simply a catalyst on par with war. Wartime creates conditions needed to reboot society: increased centralized planning, populous willing to make sacrifices, easier to confiscate money from the wealthy, etc.

Four potential conflicts which may serve as the Climax of our current Crisis:

1. Covid — is this big enough to mobilize the nation?
2. Civil War — feels more likely by the day
3. Total War — tensions rising with China, a battle over the future financial system could spark conflict

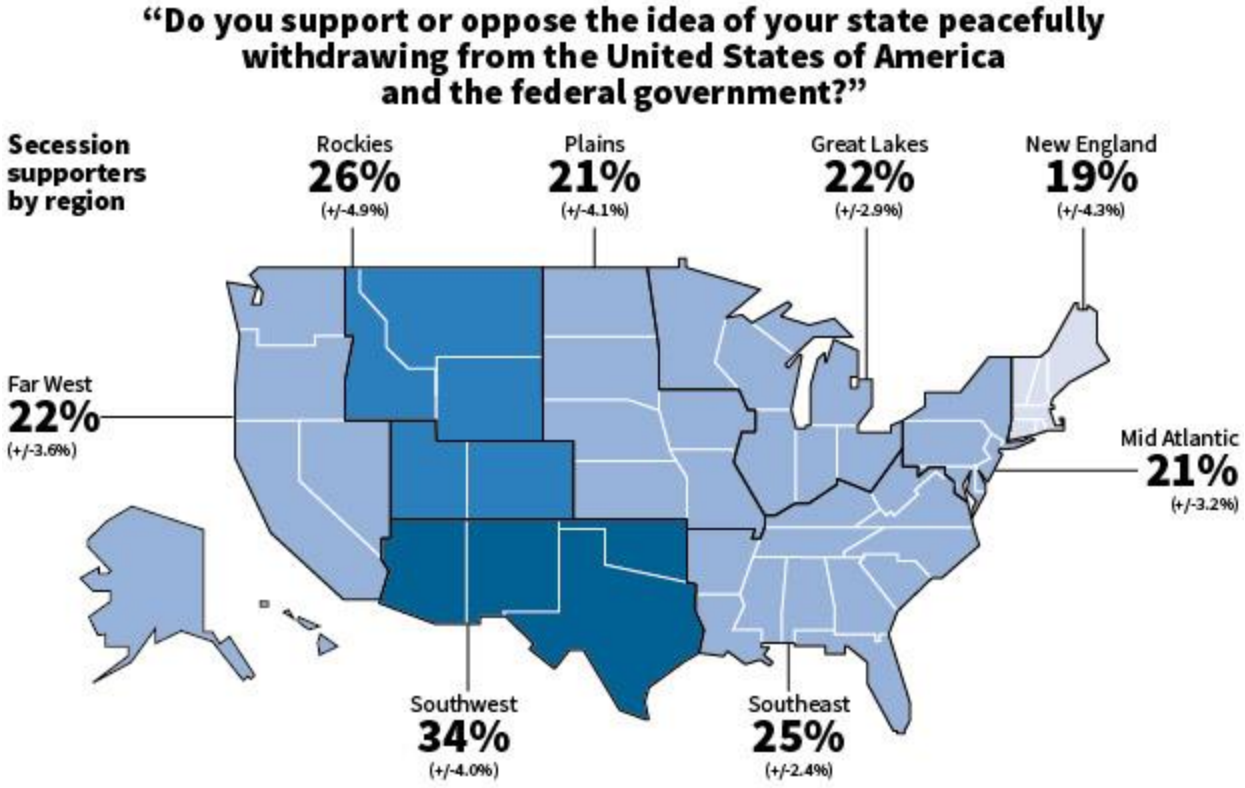
4. Black Swan — unpredictable spark that would catapult the world into conflict (financial collapse, terrorism, cyber-attacks, etc)

In March 2020 I thought Covid would serve as our Climax to rally the troops through the dark night. We saw increased government spending, begging for the central government to manage the crisis, Universal Basic Income, business bailouts, and many people willing to give up liberties for the "greater good."

However, the issue became politicized and created a wider gap between political party lines. Could Covid be the climax? Yes, it's possible, but I fear we have a much bigger event on the horizon.

The Case for a Second American Civil War

A 2014 poll showed that 23.9% of Americans support secession from the Federal Government. If they ran the same poll today, it would no doubt be higher. This is alarming because it only requires a strong minority to kickstart a conflict. For example, most people in the colonies didn't support the American Revolution.



Source: *Reuters poll data*

We're not doomed to see a repeat of the first American Civil War. Instead, they can materialize in all shapes and sizes. There doesn't need to be a clear beginning, clearly defined sides, each with their own clearly defined goal. Instead, Civil wars are often a quagmire of different factions fighting over an ever-changing landscape.

Civil wars become more likely when the community that commands the greatest loyalty doesn't necessarily align to the political or geographic boundaries. The biggest points of contention in America right now are Rural vs Urban, States vs Federal Government, and Red vs Blue.

Unsurprisingly, wartime is when humans create all the deadly weapons (ex: Project Manhattan). If America unravels into civil war, we'll see new weapons developed and deployed on our own citizens. We're already seeing a militarization of police, unmarked paramilitary troops occupying hot zones, increasing surveillance technology, spyware, Fed Coin being discussed, and attacks against encryption. Sadly, the state can cook up much worse things if the "need arises."

If you want to understand the risks of a Second American Civil War, I recommend the podcast series It Could Happen here (2019).

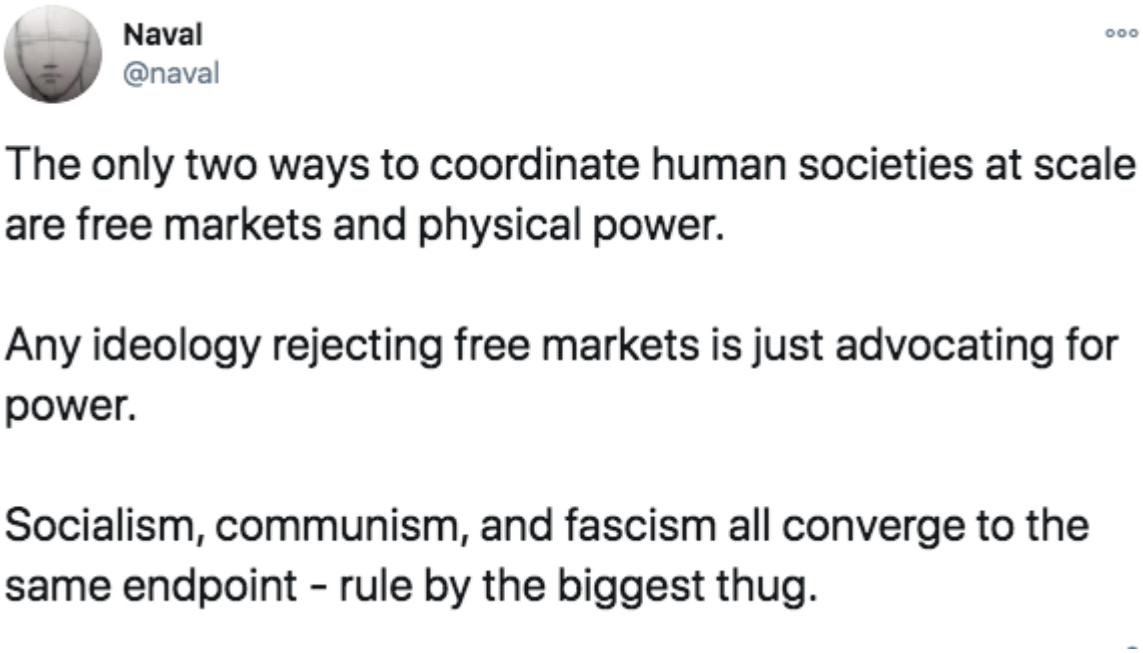
Plan for the worst; hope for the best.

The Fulcrum of this Crisis: Individualism vs Collectivism

Each Fourth Turning resolves some deep point of friction in society. The previous one (1930s and 1940s) was rooted in a battle between capitalism and socialism. The next decade's battleground will be Individualism vs Collectivism. At a glance, these concepts sound similar. The difference is the previous cycle was a fight over the means of production. State or Market? Our current cycle is a fight over "the culture." Is individualism celebrated or condemned?

Collectivism is growing today (see: rising populism). If this continues, society will become a totalitarian nightmare. The trick is to get support for individualism (liberty) from collectivist minded people. This will shift the pendulum back towards freedom. As Matt Ridley says "Innovation is the child of freedom and the parent of prosperity." In other words, freedom leads to innovation which leads to prosperity.

Free individuals can take on more risk, with less red tape, in an attempt to create value. Most fail (necessary sacrifice) but the few who succeed produce fruits enjoyed by society at large.



This point cannot be overstated during a Fourth Turning – when the temptation is to succumb to collectivism. As Naval has rightly pointed out, there are only two ways to coordinate societies at scale… by free markets or by force.Bitcoin acts as a novel institution that improves society's ability to coordinate through free markets, rather than state-enforced violence.

Bitcoin is also a monetary asset outside anyone's control. This contests the state's monopoly on money and banking. Less state control empowers individuals to unleash latent creativity that would otherwise be stifled by government or cultural censorship. In other words, Bitcoin increases marginal productivity in society.

Bitcoin is the life raft during the great fiat flood

Bitcoin is our best hope for a peaceful transition to a new financial system.

Individuals can opt-out of their local currency by joining the Bitcoin life raft. Protect purchasing power, rather than go down with the sinking ship that is their state. This reduces conflict risk as fewer citizens become desperate.

As currencies collapse and resources become scarce, nations will become desperate which often leads to bloody conflict. Adopting Bitcoin early means states and individuals will benefit from Bitcoin's price appreciation, increased economic opportunity, and a headstart in a new paradigm. In some cases, this may de-escalate conflicts by minimizing fallout from failed states.

Which country will announce they've been accumulating Bitcoin first? Hard to say.

All I know is you don't want to be the last country to do so.

Is Bitcoin the Fifth Turning that finally breaks the cycle?

My original thesis for this essay was: Bitcoin will break the Fourth Turning cycle. However, after spending [a lot] more time with the material, I no longer believe that.

These generational cycles appear to be an emergent phenomenon foundational to human civilization. It "shouldn't happen" but it does. Any technology, including Bitcoin, is processed on "higher layers" in the human stack.

Through this lens, the question becomes: "how will the current mood affect Bitcoin?"

Bitcoin is the Perfect Fourth Turning Money.

Bitcoin was born at the dawn of the Fourth Turning in 2009, at the peak of the global financial crisis. It was engineered for maximum survivability and grew up during a period of high volatility. Bitcoin is the perfect Fourth Turning money.

Our existing Fiat Financial system was born during peacetime, was sheltered by central bankers, and has never faced real adversity. Fiat is not well suited for the volatility of Fourth Turnings.

"Oh, you think the Fourth Turning is your ally. But you merely adopted the Fourth Turning; I was born in it, molded by it. I didn't see the First Turning until I was already a man, by then it was nothing to me but BLINDING! The volatility betrays you, because it belongs to me!" -Bitcoin

Or as Andreas Antonopolous would say: Fiat is Bubble Boy trying to compete against the battle-hardened sewer rat that is Bitcoin.

How does BTC perform in this Fourth Turning?

In a world where central bankers are racing to devalue their currency, scarce assets win. Bitcoin is the most scarce asset in history and it's still 50x smaller than gold. As Paul Tudor Jones said, "Bitcoin is the fastest horse."

The stakes are high during Fourth Turnings and governments will intervene in markets in unpredictable ways. In other words, even if you make the right trade, the gamemaster might change the rules on you. Bitcoin is the least manipulable asset, it's prudent to hold some.

It takes considerable effort to grasp Bitcoin and most people haven't bothered. Current Bitcoin investors benefit from this information asymmetry. As the world wakes up to Bitcoin, it will become "the asset heard round the world."

Will governments ban Bitcoin?

Some governments are hostile to Bitcoin today and others will be hostile tomorrow. Luckily, nations are in competition with each other. Banning Bitcoin in one jurisdiction creates an opportunity for another nation to attract that capital.

Bitcoin is really hard to attack head-on and failing to stop it could easily backfire. Optimistically, just like gold became accepted by the powers that be, Bitcoin might get a similar pass.

However, this doesn't mean they won't try to suppress Bitcoin. Be prepared for a repeat of the 1933 Executive Order 6102 (making self custody of gold illegal). Self custody your Bitcoin and encourage others to do the same.

Lastly, increasing isolationism will reduce the United States' role as the world police and decrease intergovernmental cooperation. Increased competition is good for customers (citizens). Enterprising governments will offer favorable tax treatment for Bitcoiners, sell passports, and offer digital citizenship.

Millennials love Bitcoin, they just don't know it yet

In 2017, Neil Howe, the author of The Fourth Turning, made a video explaining why he's bearish on Bitcoin long term. Neil makes rookie mistakes like: "Bitcoin is anonymous and only good for illicit activity," and "Bitcoin can't be money because it's not a commodity or government debt." Not worth the effort debunking these claims for the Nth time.

Neil also argued that most Millennials won't adopt Bitcoin because they're community-oriented, want to trust strong central institutions, and they're famously risk-averse. Neil thinks Millennials will avoid Bitcoin and adopt Central Bank Digital Currencies (CBDCs) because they'll be regulated, transparent, accountable, and safe. Interesting critiques, but only partially true.

Neil's right that millennials are collectivists and deeply desire to trust institutions. Millennials don't want to "defund the state" or "separate money from state" or have unfettered free markets. An important point for Bitcoin evangelists to consider. However, Neil missed a few key points about Bitcoin. In short, Millennials love Bitcoin, they just don't know it yet.

Bitcoin is based on principles of community, transparency (open ledger), equal opportunity for everyone in the economy. It's the perfect institution upon which Millenials will reorient society.

Bitcoin is the most community-oriented monetary network in existence. Replace the old white guys at the Fed with software. Everyone can run a node. Consensus is king. Protocols over bureaucrats.

Millennials are definitely risk-averse. They won't volunteer to be the first person buying Bitcoin, but they'll avoid being last at all costs. Luckily for them, Bitcoin is becoming de-risked as public companies, famous people, and their friends adopt Bitcoin. Not to mention, Bitcoin is one of the only options for a positive real yield in the 2020s. Millennials can either adopt Bitcoin or ***have fun staying poor*** (as the meme goes).

To Neil's credit, UBI delivered via CBDCs will be popular with millennials. However, millennials will also get more comfortable with a new monetary system and they'll observe Bitcoin increasing in price relative to their Fed Coin. Ultimately, CBDCs will accelerate Bitcoin adoption.

MILLENIALS		GEN X		BABY BOOMERS	
AMAZON.COM INC	7.87%	APPLE INC	10.52%	APPLE INC	9.19%
APPLE INC	6.18%	AMAZON.COM INC	7.16%	AMAZON.COM INC	5.32%
TESLA INC	3.22%	BERKSHIRE HATHAWAY	2.37%	BERKSHIRE HATHAWAY	2.75%
FACEBOOK INC	3.03%	FACEBOOK INC	2.26%	MICROSOFT CORP	2.69%
GRAYSCALE BITCOIN TRUST	1.84%	MICROSOFT CORP	2.16%	FACEBOOK INC	1.43%
BERKSHIRE HATHAWAY	1.73%	TESLA	1.45%	VISA INC	1.25%
WALT DISNEY CO	1.68%	ALPHABET INC.	1.30%	ALPHABET INC.	1.23%
NETFLIX INC	1.58%	NETFLIX	1.29%	AT&T INC	1.17%
MICROSOFT CORP	1.53%	ALIBABA GROUP HOLDING	1.23%	BOEING	1.08%
ALIBABA GROUP HOLDING	1.39%	VISA INC	1.23%	ALIBABA GROUP HOLDING	0.98%

Finally, a quick look at some data. Unsurprisingly, 90% of Millennials prefer Bitcoin over Gold. Millennials also picked cryptocurrencies as their top long-term investment 9% of the time, triple the rate of Gen X. Charles Schwab

published their top 10 holdings by generation in the chart below, again Millennials are leading the charge with the Grayscale Bitcoin Trust.

Source: Charles Schwab (emphasis mine)

Based on the current data we have and the reasons listed above, Bitcoin will be adopted by Millenials at an increasing rate over the coming decade.

Bitcoin as a treasury reserve asset

The chaos kicked off by Covid in 2020 served as a wake-up call. Everyone around the world is forced to reevaluate assumptions, hard conversations are being had, big changes being made. This shakeup led to individuals, companies, and governments reevaluating Bitcoin.

Notably, major corporations started adding Bitcoin to their balance sheet. Two narratives drive this decision: economics and ideology.

Michael Saylor, CEO of MicroStrategy, bought $425m worth of Bitcoin "not as a speculation, but rather a deliberate corporate strategy to adopt a Bitcoin Standard." He sees fiat money like an ice cube melting between his fingers. Bitcoin is a way to protect the purchasing power of their treasury. A rational economic decision.

Jack Dorsey, CEO of Square, bought $50m worth of Bitcoin because it's an "instrument of economic empowerment....which aligns with the company's purpose." This is a sound ideological decision.

Buying Bitcoin to support "economic empowerment" sends a very powerful message today as equality is being widely discussed. Not to mention, corporations feel the weight of economic uncertainty. Two separate threads, both leading to more Bitcoin ending up on corporate balance sheets. Corporate FOMO here we come.

At the time of writing, 3.74% of all Bitcoins are held on publicly-traded company balance sheets.

Can Bitcoin become too big to fail?

As of October 2020, Bitcoin's market cap is around $250b. Impressive, but still a rounding error in the global financial system. With that in mind, Bitcoin has a lot of growing up to do. Many challenges yet to overcome. However, I remain optimistic.

The community coalescing around Bitcoin is unparalleled. But don't take my word for it...

"Bitcoin has this enormous contingence of really, really smart and sophisticated people who believe in it....It's like investing with Steve Jobs and Apple or investing in Google early." - Paul Tudor Jones

"Bitcoin is a swarm of cyber hornets serving the goddess of wisdom, feeding on the fire of truth, exponentially growing ever smarter, faster, and stronger behind a wall of encrypted energy." - Michael Saylor

"The Bitcoin guys have a perspective on what the true liberation of America and humanity will be." - Kanye West

In other words, if you bet against Bitcoiners, you're going to have a bad time.

An increasing number of American politicians have publicly voiced support for Bitcoin. An optimistic sign for the future of Bitcoin.

Publically traded corporations owning Bitcoin reduces the chance of a state-level attack because doing so would crash the almighty stock market.

At a certain point, Bitcoin will have reached enough market penetration that dislocating it would be impossible.

Not to mention, Bitcoin held in self custody is really hard to confiscate. Orders of magnitude harder to seize than gold or marijuana, both of which survived state-level attacks.

Global reserve asset: What comes next?

The monetary system sits at the base of humanity. All other institutions reference the monetary layer making it the primordial institution.

In the previous Fourth Turning, we birthed the Bretton Woods system, the World Bank, IMF, United Nations, and much more. As the current fiat financial system starts to crumble, maybe it's time for an upgrade.

In 2009, the head of the PBOC, Zhou Xiaochuan, called for reforming the international monetary system (citing Keynes bancor system). Since then, China has been publicly developing a central bank-backed digital currency.

In 2019, the Governor of the BOE argued for Central Bank Digital Currencies to replace the dollar. Then weeks before the 2020 presidential election, the IMF calls for a new Bretton Woods moment.

In other words, the global financial system is going to be rebooted. What will come out the other side? Central Bank Digital Currencies? Bancor 2.0? Libra? Return to a Gold Standard? Bitcoin Standard?

A return to the Gold Standard is nearly impossible today because the economy demands stimulus and gold forces austerity. There is no political will for austerity. Sorry, gold bugs. It's not happening.

Libra or a similar "corporate money" seems to have taken a back seat for now. Not because it wouldn't work, instead because governments are fighting back. As it stands today, big tech is the bad guy.

This leaves CBDCs, Bancor 2.0, and a Bitcoin standard left to discuss.

Central Bank Digital Currencies are inevitable.

Currently, central banks can only indirectly manage the economy by adjusting interest rates and QE. A clumsy approach that's becoming less effective every year. Interest rates cannot be lowered further and QE isn't very effective. This leaves fiscal policy as the solution available today (aka spend our way out of this mess).

Enter Central Bank Digital Currencies (CBDC). They'll serve two purposes: enable central banks to manipulate the economy in more sophisticated ways and serve as a surveillance tool that would make Hitler, Stalin, Mao jealous.

CBDCs will enable the central banks to surgically manage the economy. They can simultaneously inject cash in one sector while taxing another (negative interest rates). They'll deduct taxes automatically and send UBI payments directly from the Fed to the plebs.

This will give incredible power to central banks at the expense of liberty for individuals. This new digital dollar will spy on you and will only work at government-approved vendors. If the government doesn't like your political views, they'll turn your money off. This is the weaponization of behavioral economics through an all-powerful, closed-loop, financial system. Apparently, the banking class has no upper limit on hubris.

Whether we like it or not, all major countries are racing to create their own CBDC. By 2030, an entirely new financial system will be in place.

New Global Reserve Asset?

In a few years, all major nations will have successfully forced their citizens onto their CBDC system. Smaller nations will adopt regional CBDC standards.

How will nations settle between each other? Currently, this is done with gold, dollars, or U.S. treasuries.

One option is to create a new global reserve asset pegged to a basket of CBDCs, we can call this Bancor 2.0. Governments are incentivized to support this as it enables everyone to print money simultaneously without destroying their foreign exchange rates. This will lead to a major devaluation of the entire fiat system. This is the most likely outcome by 2030. Raoul Pal explores this in a recent video.

However, Bancor 2.0 comes with major execution risk and requires cooperation from major nation-states. Do governments have the technical chops to pull it off? Will they partner with Facebook to build the tech? Will competitive nations agree to terms for a Bancor 2.0? This plan is attractive to technocrats, but it's not bulletproof. Even if Bancor 2.0 is implemented,

Bitcoin's uncompromising monetary policy will serve as the true barometer of success. In other words, all ***shitcoins*** trend to zero in Bitcoin terms.

Bitcoin is the most pristine collateral.

Bitcoin is the perfect settlement medium between nations. It's scarce, verifiable, secure, publicly auditable, and resistant to capture. Most importantly, it doesn't require trusting your counterparty.

The question becomes: is Bitcoin ready to serve as the foundation of a new global financial system? The short answer is not yet. However, competitors such as Bancor 2.0, aren't ready either.

The Fourth Turning will end sometime around 2030. This leaves room for Bitcoin to continue its exponential path of adoption. While I fear Bancor 2.0 will be attempted, Bitcoin will be the future reserve asset of the planet. The only question is will Bitcoin be ready by 2030?

Author's note: It would be poetic if Bitcoin became the global reserve asset in 2030, just in time for Bitcoin's 21st birthday.

How to Protect Yourself During The Fourth Turning

The next decade will be chaotic and unpredictable. There will be many losers and a few big winners. So how do you protect yourself during a Fourth Turning? The short answer is to make yourself antifragile.

How to protect yourself during this Fourth Turning:

1. **Protect your wealth with Bitcoin (self custody)** – Bitcoin cannot be seized, will likely increase in value, and you can travel anywhere with money stored in your head. Self custody is required to defend against a 6102-₿ type attack.
2. **Minimize debt** – Don't get wiped out by volatility. Fixed-rate mortgages are OK.
3. **Live below your means** – Survive on one spouse's income, invest the rest.
4. **Multiple sources of income** – what happens if you lose your primary income? Invest in yourself, build skills for the future, find a side hustle.
5. **Acquire a second passport** – Do not be locked into the fate of your jurisdiction. Useful for immigration, reducing tax burden, and peace of mind. Katie Ananina helps Bitcoiners acquire a second passport at Plan B Passports.
6. **Don't be cancelable** – If your income is independent of mob sentiment, being "canceled" will not sting so bad. Start a business, side hustle, or work for someone you trust.

7. **Don't invest in politics du jour** – Culture is not your friend. Opt-out.
8. **Be self-reliant** – Grow food, defend yourself, have access to energy.
9. **Become more technical** – Learn digital privacy, how to code, and Bitcoin.
10. **Become super literate** – Avoid junk-food content. Read books and write essays. The more you read and write, the better you think, and the more effective your decision-making will be.
11. **Find community (citadel)** – Individuals are vulnerable on their own, join a citadel. Build a community of like-minded people. Digital and Analog communities.
12. **Stay vigilant** – Pay attention, be proactive, make a plan, stick to it.

First and foremost take care of you and yours during this tumultuous time. If you have extra bandwidth, build a better future. If you don't step up, who will?

Will this Fourth Turning End in Tragedy or Triumph?

Art by CRYPTOXEER-IV

The chess pieces are set, but the game is not over.

Fourth Turnings, despite their unpredictable nature, present a rare opportunity to redesign society. We're alive to witness the global power

struggle to shape the future of humanity. Will this crisis end in tragedy or triumph?

Let's face it, we're tragically trending towards totalitarianism. And I'm not interested in being farmed by our fiat overlords.

Thankfully we have Bitcoin to serve as a protection against tyranny. A beacon of hope during the cold dark night.

By 2030, America will have completed this Fourth Turning and the global order will have been reshaped. Hopefully, we'll begin the next Saeculum on a sturdy foundation enabling a new era of prosperity.

Better fasten your seatbelt because this decade defines the next 100 years.

. . .

Thank you for reading ***Bitcoin and the Rhythms of History.***

- Follow me on Twitter @bquittem
- Please share this article with a friend
- Stack Sats at SwanBitcoin.com/Quittem ($10 free BTC after signing up)
- Signup to receive future essays by email
- Bitcoin accepted here: 3QpL5n3Cj3nW6QpRJMHV6hD1F2d9ST65jk

Acknowledgments

- Huge thanks to Neil Howe for writing The Fourth Turning. I've learned so much from your ideas and look forward to your upcoming book.
- **Editors**: Robert Breedlove, Mark Stephany, Justin Evidon, Lee, Steven Oustecky, Derek Waltchack

- **Inspiration and mentions**: William Strauss (deceased), Lyn Alden, Raoul Pal, Luke Gromen, Naval Ravikant, Robert Evans, Tuur Demeester, Pierre Rochard, Michael Saylor, Sahil Bloom, Cory Klippsten, NVK, Katie Ananina, Brady Swenson, Andreas Antonopolous, Matt Ridley, Grant Williams, Felix Zulauf, Kanye, Paul Tudor Jones, WTF happened in 1971, and anyone else I forgot ☺

Creative Direction: Nick Ward helped with creative direction and the Supply vs Demand of Order chart

- **Audio Version**: Read by Guy Swann @ Bitcoin Audible
- Finally, thanks to everyone who sharpened my thinking through conversations on this topic over the last few months.

Bitcoin at 12

By Nic Carter

Posted October 31, 2020

St Andrews Cathedral, St Andrews Scotland (image courtesy of photoeverywhere)

Twelve years ago today, on Halloween 2008, exactly 491 years after Martin Luther nailed his theses to the door of Wittenberg Castle Church, the idea of Bitcoin was born. More accurately, you could say it was baptized. The network itself wouldn't exist in a truly live and peer-to-peer fashion until the following January. Block 1, the first 'true' block, was mined on the ninth, and digital cash pioneer Hal Finney received the first transaction on the tenth of the month.

The idea of digital cash had existed previously, of course, as had cash-like schemes based on computational work. But this specific scheme — capped supply, not dollar-pegged (many of the early digital cash ideas relied on maintaining a dollar peg), running on a peer-to-peer network, based on a shared ledger, with minting through proof-of-work — was new, and so Satoshi had the privilege of naming it. When you create new things, whether they're fictional characters or nation-states, you get to name them. In some cases, merely discovering things endows you with a nominative right. But it's unambiguous that inventors get to christen their inventions.

This matters, because October 31, 2008 was the first time Bitcoin's core qualities were sketched out, and paired with the name. This makes the

system known as 'Bitcoin' rather specific. It's not simply a generic name assigned to the first successful digital cash implementation. It's the name that Satoshi bestowed upon a system with a predefined monetary schedule, 21 million units, based on proof of work, and so on. Other digital cash systems have existed and will exist. But this one is special, and it's opinionated. It's not just a way to move value through a communications medium. It's an entire monetary manifesto. An affront to the fiat system.

Bitcoin has often confused people. It's perhaps one of the most misunderstood phenomena of the last decade. If you lack sufficient ideological and historical context, you most likely consider it a complete boondoggle or a bizarre, unnecessary waste of computing power and effort. This is the default position. Most people in the West rarely give any thought to monetary policy or banking — why should they? Their currencies depreciate at a slow, barely perceptible rate. Their bank arrangements work fairly well, and they don't find themselves frozen out of the financial system too often.

Of course, this isn't the reality for the majority of the world's population, who suffer under inflationary regimes, or politicized and untrustworthy banking systems. But the views of American coastal elites are far overrepresented in the discourse, so the press is replete with confused assessments of this purportedly useless monetary scheme. But understanding the purpose of Bitcoin is itself a shibboleth. If you don't get it, it's probably not meant for you.

Even among acolytes, Bitcoin's true nature is hard to pin down. It's a fast-settling payments and settlements network, which led people to believe it would be suitable for petty-cash style payments on the internet, or even at brick and mortar points of sale. It's a highly-available, replicated, and consistent database, which led many to envision it as a tool for the storage of arbitrary data. It's highly innovative, and relies on new discoveries and improvements in computer science, cryptography, and peer to peer networking, yet it is perceived as antediluvian, a relic almost. These contradictions are core to the nature of Bitcoin. Something unowned, with no one to speak for it, will appear multitudinous in the minds of its users. It's a glittering prism, refracting the opinions of observers, spitting out radically different visions of itself based on their perspectives.

An endless time horizon

Recently, the great monetary historian George Selgin pointed out that Bitcoin was unlikely to displace the dollar anytime soon, because monetary network effects are incredibly powerful and enduring. And I fully agree. The difference between us is simply one of time horizons. I am willing to be patient. I believe Bitcoiners have this in common. They recognize that they have undertaken a near-hopeless task. Creating a global, neutral, apolitical

settlement medium and standard of value will not happen overnight. We have barely begun the project. We are only twelve years in. But we have made some great progress so far. So we push forward.

What's the measure of a healthy society? Arguably, it's a willingness to undertake long term projects, whose completion their originators will never live to see. Virtually anything worth building takes time to build. Enduring institutions don't come easy.

The cathedral is not the stones that compose it. Nor is Bitcoin the blocks. The cathedral is the physical embodiment of a singular idea: ***something greater exists.*** Its greatness makes you feel small, and reminds you of your place in the universe. We modern folks, who trivially fly through the heavens for the price of one-tenth of a day's labor, still find cathedrals imposing and sublime. Imagine how a medieval peasant would have felt in the somber coolness of the great hall. The spires towering above him, the tallest building he would see in his lifetime. The sun's light filtering through colored glass, revealing an array he would never witness anywhere else. All of it, painstakingly built not for vanity, or commerce, but for the glory of God, over generations and generations. Fathers and sons and grandsons toiling over the same edifice.

My university years were spent studying philosophy in St. Andrews, a small town on the east coast of Scotland. St Andrews was the site of a cathedral constructed to house the relics of Andrew the Apostle, the patron saint of Scotland. The diagonal white cross on the blue background, the one seen on the Scottish flag, the Saltire, represents the cross upon which he was crucified. For one hundred and fifty-eight years, starting in 1160, thousands of stone masons, laborers, and townsfolk labored with hand tools to build a suitable container for these holy relics. Only a tiny fraction of the people who poured the whole energy of their lives into this magnificent building would ever see it completed. For the rest of them, knowing that they were working on a sublime, civilizational project was enough. They were happy to submit to a vision far greater than themselves, rising above their transient concerns. This was the height of culture, beauty, and technology at the time. What more could one hope to live for?

It's virtually impossible to set foot in an ancient cathedral today, a thousand years old, without contemplating the sheer human effort expended to place every last stone and every last pane of colored glass. It's a monument to and a digest of the embodied work sunk into those ancient stones.

The Satoshean critique

Martin Luther had ninety-five critiques. Satoshi had, effectively, one. Satoshi's animus lay with the centralized nature of banking, credit, and base money itself.

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.

Martin Luther sought to reform the Church, to return it to a truer, earlier state. Aside from presenting us with a rubric and then a first implementation of a system, Satoshi was not as forthcoming. The Bitcoin whitepaper is probably one of the most semantically dense documents in history. Not a word is wasted. Satoshi was famously terse on forum posts, only sparingly opining on the political and economic objectives of the system. The blanks have been left to us to fill in.

And we have been doing so with gusto. Bitcoiners, through the mechanism of novel technology, seek to restore a monetary arrangement of the past. Bitcoin is new technology designed to pursue baroque ideas. It hearkens back to the era of sound money, in particular the harmonious period from 1880 to 1914 when the international order was largely united on a gold standard and free trade flourished. In the minds of bitcoiners, we sit at an epochal turning point. With any luck, future historians will speak of the bitcoinist restoration, which reversed the losses suffered in the fiat interregnum of 1971–2020. I call it an interregnum because a fully fiat standard is a historical anomaly rather than the default. In this manner, Bitcoin can be understood as revanchist or restorative. We are reclaiming lost territory, discarded ideas, and lost time.

Some critics allege that a Bitcoin standard mirroring the one supported by gold is unoriginal and trite; that a Bitcoin standard would suffer the same failures. Why bother revisiting failed monetary arrangements of the past? But Bitcoin, being a dematerialized monetary commodity, is new, and distinct from gold.

These critics fail to grasp its superiority over classic monetary technologies, which should give a Bitcoin-centric system more robustness. It's more auditable, meaning that banks and deposit-taking institutions can be held accountable by their users. It's cheaper to verify, requiring only basic computer hardware. This globalizes and democratizes the monetary system. Anyone can participate, not just a large institution with the resources to safeguard large quantities of gold.

Unlike gold, it's trivial to take physical delivery of the asset. This means that users have a free choice between self-custody and an intermediated approach. This permanent optionality — in the worst case, I can take physical,

final ownership of my own assets — is an incredibly powerful feature, that tilts the balance of power towards the individual, away from the State or corporate oligarchs. It's about time the pendulum swung back.

Even where service providers are involved, competition for depositors is fierce. Closing your account at a bitcoin bank is as simple as withdrawing your coins and depositing them at another. And it's programmable. Sophisticated conditions can be encoded directly into transactions. This is a design space we have barely begun to explore. The immediate concern is the integrity of the network, which is why system-wide upgrades require such careful vetting. There is likely no open source project on earth that has witnessed as much scrutiny as Bitcoin. It's a $250 billion bug bounty, after all. So we move slowly, but deliberately.

People sometimes ask me what Bitcoin means to me, and this is my best attempt at an answer. Bitcoiners who earnestly believe in a better monetary world, and aren't afraid to bring that reality to bear, are the equivalent of masons and laborers, working on a monetary cathedral which they may never see come to fruition. But this is ok. As long as we believe in a big, audacious vision, believe that there is still beauty in the world, and that there remain great things worth striving for, we will succeed and inspire.

Today, I can't imagine anything else I'd rather be working on. I couldn't be happier to devote my career and energy to the vision laid out by Satoshi twelve years ago. The satoshean critique is true, and it is continually reinforced, as established monetary authorities grow more erratic and capricious. The instantiation of a stable, Bitcoin-based monetary system is by no means guaranteed, but it becomes more plausible by the day. I don't know if I will see the completion of this project, or even if it will work in the long term. But that doesn't bother me. I'm focused on placing the next brick.

Nic Carter

October 31, 2020

Thanks to Sam Abbassi.

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