



WORDS

August 2020

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

Contents

Contents.....	2
Goals and Scope.....	3
Support WORDS	4
Misjudging Bitcoin	6
The AlienCoin Attack Vector	11
Tweet Thread - What Bitcoin Is.....	14
Tweet Thread - Bitcoin and NoSQL	18
Bitcoin's Patronage System Is an Unheralded Strength.....	22
A real talk-blocker	25
Is Bitcoin the world's safest reserve asset?.....	30
Balinese Cockfights & Bitcoins: How one can help us understand the other	40
In Memory of Hal Finney, RIP — Builder of a More Trusted World	48
Lightning is the Better Way to HODL.....	56
Disclaimer:	67

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.

Misjudging Bitcoin

By Beautyon via Decentralize Today

Posted July 27, 2020

In The United States District Court for the District of Columbia, “UNITED STATES OF AMERICA v. LARRY DEAN HARMON”, Chief Judge Beryl A. Howell (a Barack Hussein Obama appointee) made a problematic ruling on the nature of Bitcoin, relying only on hearsay and third party sources, which misguided her to a totally wrong conclusion. Here we dissect the part of the judgement that mischaracterises Bitcoin. It is full of errors, and should not have been used to make the judgement.

Bitcoin is not “a decentralized form of electronic or digital currency that exists only on the internet”. Bitcoin is **a database**, copies of which are held by people who download a piece of software to run it. Bitcoin is also not “an alternative currency” and simply asserting that it is does not make it so. Bitcoin is never transferred anywhere. Entries are made in the publicly visible database. No one “owns” Bitcoin. The fact that Bitcoin has units does not confer the property of money to it. For example, memory storage devices and rulers have units but are not considered money.

Any proof that Bitcoin has a characteristic cannot come from case law or a layman. An accurate description that is not description by analogy is possible in this matter, and in every instance this is the only description that should be submitted to any court in any proceeding. Relying on second hand descriptions of what Bitcoin is is not necessary, and it is not correct to describe discreet technical operations and devices by analogy only.

Bitcoin is not “an alternative currency”. It is **a database**. Bitcoin transactions are **entries in a database**, which is identical in nature to all other databases where information is stored. The numbers in the Bitcoin database can represent literally anything, because it is data. The idea that Bitcoin is money rests solely in the minds of the people who choose to treat Bitcoin as money. **It is not actual money itself**. Bitcoin is never transferred anywhere. Bitcoin users sign messages and write them to the global database. Nothing is transferred from one person to another in Bitcoin, and ownership is never transferred in Bitcoin; all data in the Bitcoin network is a property of the Bitcoin database, and not of any particular user.

The capitalisation conventions in Bitcoin have no bearing on the nature of Bitcoin, and have been adopted by people desperate to try and contextualise

Bitcoin. Anyone can make a copy of the Bitcoin network's database and call it something else, with its own naming conventions. That would not make any aspect of the copy money. It is not true that "tokens" are transferred in Bitcoin. The use of the word "token" emerged from users of Social Media attempting to contextualise Bitcoin through analogy. At no point is Bitcoin ever a "token", like a subway token or ticket.

Units of Bitcoin are not stored by reference to an address. Bitcoin addresses are keys used to sign messages that are sent to the network for storage. The authors making this false claims cited in the memorandum admit themselves that they are analogising the address to a user name and that addresses are *similar* to a bank account number, both of which are absolutely false.

Bitcoin is never transferred from one address to another. Bitcoin is always sent to the network and stored. The controller of a Bitcoin address never receives anything, because nothing is transferred. Bitcoin users scan the database to see if a message signed to their key has been written to the database. This is not "reception" in any sense, because the location of the "recipient" is immaterial. People on the ground seeing skywriting are not, "recipients of messages", they are viewers only. This is how Bitcoin works. The nodes that store copies of the Bitcoin database are not linked together; they are all separate and totally independent of each other.

The "sending" and "receiving" terms in Bitcoin are analogies adopted by the computer illiterate public to help them contextualise Bitcoin's internal processes. Bitcoin confirmations are records on the database, and nothing more. Bitcoin is no different in function to forum software that makes note of what author wrote what text. The only difference being that people have unilaterally chosen to accept messages in lieu of money. This is a choice the public has made that has nothing to do with Bitcoin's nature, and there have been several other attempts to do what Bitcoin does that the public refused to accept. All of these systems relied on databases, and the only difference between them all is the public's acceptance.

Bitcoin addresses are not owned by anyone. They are pieces of text that have a context in the Bitcoin database. Users of Bitcoin have the *power* to sign messages with keys they keep secret, but they are not *owners* of those strings and neither are they owners of the copies of the database they use to verify messages. The only way a claim that users "own" keys is to suffix with "in the ordinary sense of the word", which is not sufficient for a court proceeding where only material facts are to be taken into consideration.

Bitcoin keys can be stored in many media like any other text, or no media at all, in the form of memorised words. To make the claim that a set of memorised words is money stretches the credulity of even the most stupid

person. **Bitcoin is not money, has never been money, and is text only.** It is always text, all the time, and you cannot assert that it is money because a computer illiterate author asserts that it is because he wants to sell a book.

Similarly, no amount of case law can turn Bitcoin into money. The genetically modified seed that grew the tree of “Bitcoin is money” found its genesis with computer illiterates and ambulance chasers desperate to sell books and run crony capitalist front foundations to control this new phenomenon. They don’t have the language or understanding to classify Bitcoin, and those that have the intelligence to do so, quickly realise that they can’t possibly tell the truth, or their new careers as Bitcoin gatekeepers and “Thought Leaders” will be over. They know that Bitcoin is just a database that people accept for accounting. It is as dull and pedestrian as that, and you can’t run a “Legal Centre” or be a “Thought Leader” in something boring and mundane as an Excel spreadsheet.

The various guides written for “Legal Professionals” will all need to be deprecated and replaced with works that accurately describe how Bitcoin works without analogies, comparing its operation to other databases that are in common use. This is the only way the “Legal Professional” and the courts will ever be able to rule on Bitcoin correctly. If they do not, then *all databases on earth will be subject to the same rulings that have been made against users of Bitcoin.*

It will mean that all online video game companies could be sued for being “Money Transmitters” because users can trade in game goods between each other. None of the judgements against Bitcoin users make a distinction that separates game monies with Bitcoin, and the mere difference in operation does not count as a difference in nature. Both Bitcoin and MySQL (a database) are databases working with the same thing; data, or plain text.

In order to say that Bitcoin is different to MySQL in law, a distinction would need to be made so that math operations required for Bitcoin are legally distinct, separate and controlled. This would be a direct violation of the Constitution, and impossible in the USA.

Operating a Bitcoin full node or sending messages to the network is not “Money Transmission”, even if the service is paid for. If you accept money to transmit a message to the Bitcoin network you are no different to a telegraph operator. You can charge by whatever means you see fit to perform this service, per word or per character, and this is the same in Bitcoin, because the database entries are scarce. You therefore, in order to run a business, need to charge sufficient money to make a profit and replace your Bitcoin so you can continue to send messages on the network. This is not “Money Transmission” and Bitcoin has no official price either. If the price of Bitcoin by agreement of the two parties using the network is agreed to be 0, does this mean that the

act is still money transmission, or not? These are the difficult questions that people who assert that Bitcoin is money cannot and will not answer, because they're either ignorant or they know the truth and want to obscure it for their own personal gain.

In no way is writing messages on a database “engaging in the business of receiving money for transmission or transmitting money within the United States, or to locations abroad, by any and all means, including but not limited to payment instrument, wire, facsimile, or electronic transfer.” If this were not the case, every text message that had a number in it could be construed as “Money Transmission” if the two parties agreed to a fee to send or receive text. When your accounts are prepared by H&R Block, and they send you the forms to sign, you have paid them for this service. Their records are kept on a database, and you sign and return the forms for a fee. This is no different to Bitcoin.

1. **A text is prepared**
2. **You sign the text with your unique signature**
3. **You return the text for storage in a database**
4. **You are charged for the service by a service provider**

The database used is irrelevant, and so is the means of identifying you and the method used to identify you by a signature. By this, you can see that H&R Block is, “running a Blockchain”, and their name should be changed to “H&R Blockchain”.

Bitcoins are not funds, any more than your accounts or text messages are “funds”. Calling Bitcoin funds is *an analogy* used to put Bitcoin in a context. Similarly, in the definition of Money Transfer, “electronic transfer” applies only to dollars sent through the traditional banking network. It does not apply to *any other context*, and **cannot**, because if it did, it would capture **all electronic transfers of any kind that contained an explicit representation of money, reference to money or number**.

Bitcoin Tumblers are not “MTAs”. If any court asserts that they are, they will be capturing all dice on earth. A Bitcoin tumbler is nothing more than a computer programme that randomises numbers in a database. It does not accept money as inputs and does not output money either. It takes numbers as inputs, performs calculations on them and then outputs different numbers. This operation has nothing to do with money, and in fact could be done manually with a pencil and paper.

Bitcoin is not a medium of exchange, method of payment, or store of value. For certain, only a fool would assert that Bitcoin is a store of value, since it has historically been very bad at doing that in fiat terms. Bitcoin is not a method of payment either; people have *chosen* to use it to pay for goods and services,

but that doesn't *make* Bitcoin a method of payment. People can use bananas to pay for goods and services, that doesn't *make them* a method of payment. Bitcoin is not a medium of exchange either; **it is a database of numbers**. Numbers can be used to represent anything, and so can Bitcoin. People agree that it is a medium of exchange today. They may not in the future. *That has nothing to do with the nature of Bitcoin*. **Common parlance does not change the nature of things**, and defendants claiming that Bitcoin is money does not make Bitcoin money. Slave owners could testify in court that people he owns are "his property" and only a terribly immoral person would assert that because a defendant said this that people are transformed into property. The same is true of Bitcoin.

Courts do not have the power to claim that human beings are property for the purposes of a judgement, and they do not have the power to create a form of money out of thin air. Only the Congress and Senate have the power to say what money is in the United States. The ordinary meaning of money is also not applicable, as is the Appeal to the People fallacy. The court cannot prove what it is asserting about Bitcoin, and it refers to fallacious arguments to do so without making any direct reference to what Bitcoin is. This should tell you that *the court doesn't know what Bitcoin is and it simply wanted to punish a man* who very foolishly sold drugs online.

Relying on other courts is also faulty. Those courts are similarly ignorant of what Bitcoin is, and are all referring to the same fundamentally flawed material to make their wrong judgements. "The federal district courts have unanimously and unequivocally concluded that Bitcoin constitutes money." This unanimity is the **Faulty Appeal to Authority Fallacy**. The court is not showing us what Bitcoin is, it is merely telling us *what other people have said it is* and it is relying on its "overwhelming authority" to badger, bully and railroad.

All of this is enough for a higher, neutral court to reject this flawed ruling and dismiss it. Further to this, this ruling has no effect outside of the District of Columbia and cannot not affect any business in another jurisdiction, like BitMEX in Hong Kong or the thousands of companies that will inevitably be formed to work on the new global database.

This judgement is vindictive and designed to punish someone who made a very bad mistake and accepted Bitcoin in return for services that are illegal in the USA. By making this entirely erroneous judgement, the court is damaging the reputation of the District of Columbia as a place to do global business with the Bitcoin database. Fortunately, billions are already being made outside of the District world-wide, and this judgement is moot everywhere on earth but there.

The AlienCoin Attack Vector

By Knut Svanholm

Posted July 29, 2020

In response to Reed Wommack and John Vallis discussing Bitcoin and Scarcity <https://www.pscp.tv/w/1PIJQNzqAMBxE>

While writing these words, I've just finished listening to Reed Wommack's conversation with John Vallis. Both Reed and John are great thinkers and I'm proud to have connected and interacted with them both on several occasions. In the conversation, the abstract concept of "AlienCoin" was brought up. Imagine that a species of alien makes contact with earth and that we start trading with them. They're using AlienCoin, a type of money with similar properties to Bitcoin but with a longer history and overall better properties. It is, in other words, a better Bitcoin. Would we humans switch to this coin or not in our search for an absolutely scarce asset that can be used as money?

I've written a lot about the concept of absolute digital scarcity and how it was more of a discovery than an invention and how it could only be discovered once. This is my definition of it, from Bitcoin — Independence Reimagined:

The One Shot Principle:

Absolute mathematical scarcity achieved by consensus in a sufficiently decentralized distributed network was a discovery rather than an invention. It cannot be achieved again by a network made up of participants aware of this discovery, since the very thing discovered was resistance to replicability itself.

Hal Finney said it like this:

"Any successful replacement of the Bitcoin block chain will forever undermine the credibility of any successor. How is an investor to know that it won't happen again? Rebooting now may benefit a few thousand early adopters. What happens when hundreds of millions use Bitcoin 2.0? They'll be just as jealous and envious of you as you are of others. Given the precedent you want to set, how will you argue against yet another reboot?"

In the interview, Reed mentions that there's probably a finite amount of say, Bitcoin Cash as well as Bitcoin. This is not how I see it. As I've mentioned before, scarcity is all about how you choose to frame it. If you see Bitcoin Cash as a "Forks-of-Bitcoin"-token, it is not scarce. There are thousands of those. Around the time when these fork-coins were popular, there was a website

where you could create your own by just a few clicks. My point about the discovery of scarcity on the internet is that we needed to frame this as soon and as rigidly as possible in order for it to actually work. I believe that the early history of Bitcoin was that framing process. It is not over yet. The fact that the Bitcoin Cash fork didn't really work was one of the main things that convinced me that Bitcoin was actually decentralized enough to not give in to proposed monetary policy changes pushed onto the project from the outside. It could only be changed from within and I concluded that this was so unlikely that it would almost certainly never happen.

Now onto AlienCoin, a very fascinating concept indeed. Even though the probability of the scenario ever happening is probably close to zero, it's a thrilling thought experiment nonetheless. A scenario like this wouldn't even have to involve aliens, let's just say that we discovered another decentralized computer network with better properties and more proof of work than Bitcoin somehow. I would still stick to Bitcoin and so should (and most likely would) everyone else. I'll try to explain why.

Have you ever played Sid Meier's Civilization? In every incarnation of the game there's a technology tree. Some technologies are prerequisites for others. Bitcoin is standing on the shoulders of giants. Not only did it require cryptography, hashing algorithms, merkle trees and ASICs to function properly but before that mathematics, writing, hexadecimals, semiconductors, microprocessors, computer graphics and probably the wheel, agriculture, pottery and even ceremonial burial or archery as well. The point is that time moves in one direction and one direction only. The order in which events play out have a huge impact on the results. If you dry yourself off before you shower, you will have a very different result than if you do it afterwards. This is true for Bitcoin's own history as much as it is true for whatever historical events that played out before it was discovered as well. Each day that passes, Bitcoin becomes more "Lindy". People have a more and more concise view of what it is, and what history it has. Bitcoin was fairly distributed among humans because the earlier you got in, the higher the risk you took. More risk, more reward. I wasn't truly 100% convinced of Bitcoin's functionality until the Bcash fork happened and the users resisted the will of more than 90% of the Bitcoin companies by running their own nodes. An alien coin would have to convince every hodler of last resort on earth that switching to the new coin would be a good idea before they'd part from their bitcoins. Like I said earlier, scarcity is all about how we frame it. The hodlers have agreed already. They hodl Bitcoin, nothing else. The thing about this philosophy is that we've already decided what the finite unit for wealth transfer we have is Bitcoin. An AlienCoin would just be another altcoin, even if it functioned as Bitcoin for the aliens. At least for a very long time. In order for anyone that has lived through the early years of Bitcoin to change their mind, they would have to be convinced of the superiority of this new system and

that would take a long time, if it's possible at all. What guarantees do we have that another, even more superior system wouldn't show up the next day?

Bitcoin is a four dimensional invention. The direction of time itself plays a huge part in what is. Having doubts about it is a fools game because the organism works and grows precisely because we believe it does. It feeds on human incentives and the more you learn about its connection to praxeology and thermodynamics the more convinced you become. This makes the system even more robust and valuable which will onboard, and convince even more users every day and on and on it goes. It is the optimist's version of Roko's basilisk. If we ever interact and trade with aliens in the future, we should exchange all sorts of things with them but we'd better hold on to our most valuable possession. The thing that makes us a type 1+ civilization on the Kardashev scale instead of just a 0,7 one. The best thing we have. The pinnacle of our achievements.

Some of us have been in Bitcoin longer than others and we're all at different stages in our perception of it. I'm not saying that I'm 100% right and that everyone else is wrong, but I have come to realize one thing. This rabbit hole is way deeper than any of us can imagine.

Loved the conversation guys, now I can't get AlienCoin out of my head! A final question: How do you know Satoshi wasn't an alien in the first place?

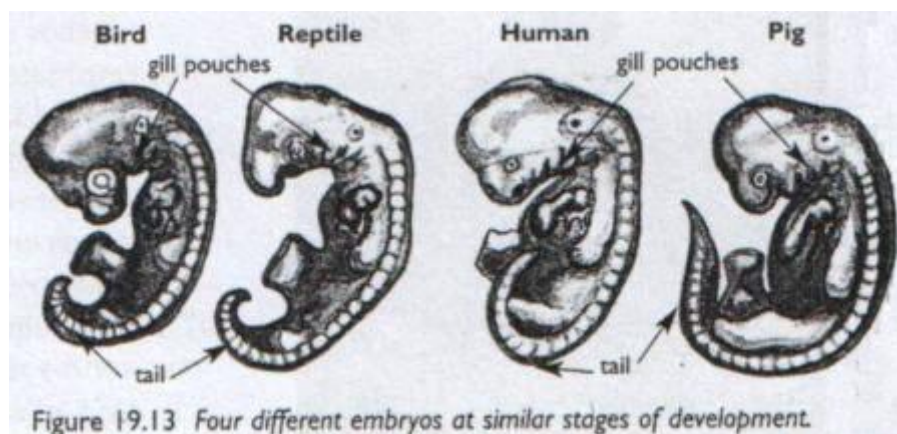
Tweet Thread - What Bitcoin Is

By Vijay Boyapati

Posted June 22, 2020

1/ In their embryonic form many species appear alike. But imprinted in their various DNAs is the code that will evince their great differences in the fullness of time.

A thread on the great debate about what Bitcoin is and why only one of the two major visions makes sense



2/ In its first few years Bitcoin appeared to be both a disruptive payment rail (near zero transaction fees) and a promising store of value (dramatically increasing in value over time).

Yet written in the code that powered its network were rules that guaranteed only one outcome

3/ Bitcoin's "consensus rules" are the set of rules agreed upon by all computers running on the Bitcoin network. Only those computers abiding by these rules are accepted as a part of the network. Perhaps the most famous rule is the number of bitcoins that are created per block.

4/ Bitcoin's consensus rules are, by the game theoretic nature of the network, incredibly difficult to change. To change a rule would require the agreement of overwhelming majority of computers running on the network.

5/ From a purely software perspective, the difficulty of changing Bitcoin's rules and core parameters might seem like a disadvantage that would eventually consign Bitcoin into obsolescence. Rather the difficulty preserves Bitcoin's most valuable property:

It needs to be recognized that immutability is by far Bitcoin's most valuable attribute. There has never in the history of man been any set of rules developed by humankind that you could count on being permanent.

6/ Fundamentally, demand for bitcoins arises from the scarcity of supply (no more than 21 million will ever be created). Yet belief in the scarcity of #Bitcoin's supply rests completely on the credibility of its monetary policy. If easily changed, that policy has no credibility.

7/ Much like a protocol, such as TCP/IP, or the shape and specification of a power socket, changing Bitcoin's consensus rules with a "hard fork" would come at great cost, ultimately destroying Bitcoin's core value proposition.

Consensus protocols, like the design of power sockets, should be absolutely immutable with the exception, perhaps, of fully backward compatible upgrades. The cost of losing consensus and losing backward compatibility is MASSIVE.



8/ Given the necessary difficulty of changing #Bitcoin's rules - in particular the number of transactions that can be processed per block - it becomes clear that as demand for Bitcoin increases, eventually fees per transaction must rise.

9/ Growing fees and a limit to the number of transactions processed per block implies that under widespread adoption, Bitcoin would simply be uneconomical for use in global daily commercial transactions (such as purchasing bread). Yet its purpose is so much larger...

10/ ... Bitcoin is perfectly suited as a global monetary base, much as gold was in the 19th century, providing a means of final settlement between large financial institutions and large-scale value transfer.

Bitcoin is the container ship of value transfer and storage. It's meant for large value transfers among untrusted parties. Trying to shoehorn Bitcoin into a

payment system for buying coffee is like trying to deliver a single Amazon package using a massive sea vessel.



11/ As a global monetary base, a Bitcoin standard would be far superior to a gold standard with all the problems that are attendant of gold's physicality

- Costliness of security and transportation
- Difficulty of assaying
- Centralization of storage (enabling confiscation)

12/ We are still very early in Bitcoin's path to becoming a global monetary base. This presents an odd situation where individuals can still own large fractions of this base. It's almost as peculiar as regular people owning 100 kilogram gold bricks under a gold standard.


13/ As Bitcoin's price continues to rise, large HODLers of its supply will have a powerful incentive to diversify their appreciated bitcoins into other assets (such as homes/stocks/bonds/sports teams etc) and thus the supply will slowly but surely be distributed.

14/ Eventually, most people will have ownership of very small fractions of the monetary base via financial institutions. These institutions will use the Bitcoin network as a means of final settlement between each other. Hal Finney (RIP)

was the first to understand this:

Hal
VIP
Sr. Member

Activity: 314
Merit: 1003



Re: Bitcoin Bank
December 30, 2010, 01:38:40 AM
Merited by mindrust (10), TheNewAnon135246 (5), LoyceV (3), ETFbitcoin (1), wh1rlw1nd (1), DireWolfM14 (1), stortz (1), BitcoinCoreBTCC (1)

Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases.

Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

George Selgin has worked out the theory of competitive free banking in detail, and he argues that such a system would be stable, inflation resistant and self-regulating.

I believe this will be the ultimate fate of Bitcoin, to be the "high-powered money" that serves as a reserve currency for banks that issue their own digital cash. Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as... well, as Bitcoin based purchases are today.

15/ In this final stage of Bitcoin's evolution it will become the backbone of a new much more robust and less corruptible financial system. And so Bitcoin's DNA - its consensus rules - will finally make clear what it is. Not a payment rail but a new, far superior, monetary base.

Beyond the financial case for Bitcoin, its rise as a non-sovereign store of value will have profound geopolitical consequences. A global, non-inflationary reserve currency will force nation-states to alter their primary funding mechanism from inflation to direct taxation, which is far less politically palatable. States will shrink in size commensurate to the political pain of transitioning to taxation as their exclusive means of funding. Furthermore, global trade will be settled in a manner that satisfies Charles de Gaulle's aspiration that no nation should have privilege over any other:

We consider it necessary that international trade be established, as it was the case, before the great misfortunes of the World, on an indisputable monetary base, and one that does not bear the mark of any particular country.

50 years from now, that monetary base will be Bitcoin.

Tweet Thread - Bitcoin and NoSQL

By Dhruv Bansal

Posted August 3, 2020

\1 Try this one on:

Bitcoin is a distributed, append-only, eventually-consistent, content-addressable key-value store written to by public auction.

Multisig UTXOs are stateful synchronization primitives enabling “database transactions” for client applications at higher layers.

\2 Congrats if you made it past tweet #1! (Phew)

This thread explains the tweet above by comparing bitcoin to NoSQL databases.

To be clear, bitcoin is *much* more than “just” a database. But we might learn something from thinking about it like one.

First, a little history...

\3 At one time, “database” generally meant “relational database”: a program with a sophisticated model for storing data and a general-purpose (sometimes Turing-complete) language for querying data (“SQL”).

There were other types of databases, but “SQL databases” were ubiquitous.

\4 SQL databases run on a single *central* server (nerds: ignore sharding & replicas pls). As data volumes increase, the usual strategy is to make the server bigger.

But the huge volumes of data on the Internet led this “scale up” strategy to fail. Servers can only get so big...

\5 This led to a new strategy: “scale out,” distributing your database across many servers.

SQL can’t be scaled out; you need to start from a new design that understands it will be running in a distributed world.

The resulting family of distributed databases was called “NoSQL”.

\6 There are many flavors of NoSQL but they share commonalities:

- Distributed (no “leader” or “single source of truth”)

- Append-only (deletes are new writes, peers gossip & replay the full dataset)
- Eventually-consistent (disparate “forks” can exist)

Remind you of anything??

\7 I sold NoSQL to large companies. Customers worried

- It's too new, I don't understand it
- Seems really hard to use
- There are so many, which should I pick?
- It's too limited, why can't it do more?
- Forks? I need certainty!
- Compliance won't approve this

Seem familiar?

\8 Today NoSQL is widely accepted; it powers many Internet companies (including Twitter).

Bitcoin *is* NoSQL! It inherits all the historical objections NoSQL overcame PLUS a whole new set based on its social & economic innovations.

Let's dig more into bitcoin as NoSQL database.

\9 Most NoSQL databases are also, on some level, key-value stores. Unlike SQL's rich data structures, NoSQL keeps it simple:

GET key1 (None) SET key1 value1 GET key1 value1

Simplicity leads to scalability: KV stores like above are the largest databases in the world today.

\10 Bitcoin is also a key-value store. When you “look up the balance of an address” what are you really doing?

GET address1 [utxo1, utxo2, ...]

Addresses are the keys & UTXOs are the values, the state the database is storing.

But bitcoin is a particular *kind* of KV store.

\11 Bitcoin is content-addressable.

Content-addressing means asking for data by name, not location.
http://google.com not 172.217.164.174.

URLs work because “centralized” DNS maps names to locations.

But how can a *distributed* system choose names? This is a hard problem.

\12 Bitcoin uses a common solution: names (addresses) are created by hashing content (scripts).

There is no “registry” of valid addresses, they are created as needed by hashing scripts & then directly sharing.

This makes bitcoin more distributed (though less human-readable).

\13 But wait, isn't an address a “location”, not a name (e.g. `GET address1` above)?

No! You only think that if you don't know the address' script. If you do (likely because it's *your* address), then your wallet is actually doing

`GET hash(script1) [utxo1, utxo2, ...]`

\14 So bitcoin is a distributed, eventually-consistent, content-addressable, key-value store. This is the “traditional” part of its design.

The novel part is using a public PoW auction to process changes.

Why does bitcoin do this expensive thing no other NoSQL database has to?

\15 NoSQL databases are operated by one party who ensures nodes trust each other.

Bitcoin is the first NoSQL database run by multiple, possibly adversarial parties who *cannot* trust each other.

A PoW public auction was the innovation needed to solve this (double-spend) problem

\16 This catches us up through the first sentence of tweet #1! What about the second?

We've already seen that UTXOs are the state bitcoin stores. The rest of the second sentence might not make a lot of sense right now. We first need to talk about data structures & transactions.

\17 How can “simple” systems such as KV stores support complex systems such as Twitter?

Because programming is all about layers. Simple systems with just the right amount of power are actually the best foundations for more complex systems.

The trick is where one divides layers.

\18 A simple example of a social network app

`GET friends_of_alice [bob]` `GET friends_of_bob [alice]`

Alice & Bob are no longer friends, so we delete:

SET friends_of_alice [] SET friends_of_bob []

An inconsistency will occur if the 1st SET succeeds but the 2nd SET fails.

\19 This is why databases offer “transactions” – a sequence of several changes with a guarantee that either all the changes will occur or none will (never just some).

Transactions avoid inconsistencies like the one above and so are extremely useful for application developers.

\20 This is because the structure of the data in the database may not match that of the data in my application. Changes to one may require multiple steps to be mirrored to the other.

Transactions are thus the locus of division between two layers: the database and the application

\21 Database transactions are also useful b/c they separate rates of change.

A client may make a large number of changes and then “batch” them all to the database. This is more efficient than writing each change individually, esp. if earlier changes are undone by later ones.

\22 Finally, database transactions help multiplex different clients’ access needs. If one client is engaged in a long-running transaction changing lots of data, the system shouldn’t pause for others. It should allow other clients who are changing *different* data to go ahead.

\23 Multisig UTXOs are *how* bitcoin coordinates “database transactions” for complex applications.

Stakeholders in the application hold keys in the multisig. The transaction only “commits to the database” if sufficient keyholders sign.

Meanwhile, all sorts of magic can happen.

\24 Offline data can be used by a signer to determine whether they’ll sign (See [@unchainedcap’s](#) loans or a friendly wager on Caravan). This is the best current solution to the oracle problem.

A lightning network channel can process many “in-channel” payments before it commits.

\25 To close, just as it’s possible to build any app you want on modern NoSQL databases it will be possible, through multisig UTXOs, to do the same on bitcoin.

No, we won’t be storing all the world’s data in a giant sharded blockchain.

But we will be building a world computer.

Bitcoin's Patronage System Is an Unheralded Strength

By [Nic Carter](#) via [Coindesk](#)

August 6, 2020

CoinDesk columnist Nic Carter is partner at Castle Island Ventures, a public blockchain-focused venture fund based in Cambridge, Mass. He is also the cofounder of Coin Metrics, a blockchain analytics startup.

A quietly important phenomenon has gained steam in the last few months. And I'm not referring to Grayscale gobbling up all the new coins or Cash App's bitcoin volumes exploding.

Bitcoin's patronage system – how future network development is funded – has gained unheralded strength, with many more entities signing on as sponsors. These groups recognize that sponsoring the core developers who keep the system running is profoundly important to keeping this public infrastructure moving ahead.

For a long time, Blockstream, Chaincode and the MIT Digital Currency Initiative were the major patrons sponsoring core developers. Thanks to their support, a handful of the most critical and engaged developers were able to commit their time fully to Bitcoin. However, many more developers active on the Bitcoin codebase or ancillary projects remained unfunded and had to split their time between Bitcoin development and day jobs.

In 2019, Square Crypto burst on the scene and announced its intention to fund a variety of Bitcoin projects, both relating to the main codebase but also targeting less conventional improvements to Bitcoin's design and user experience. Notably, its first grant was to BTCPayServer, a project dedicated to facilitating bitcoin acceptance among merchants. This signaled a broadening of the universe of grant-worthy projects and inspired several other organizations to throw their hat into the ring.

Today, the Bitcoin patronage environment is encouragingly vibrant and diverse. Numerous organizations have recognized the favorable economics of supporting Bitcoin development. In 2020 alone, BitMEX has added to its commitments, venture fund Paradigm has jumped into the ring with a sponsorship of Anthony Towns, exchanges Kraken, BTSE and OKCoin made material grants to BTCPayServer, and Square Crypto made a blizzard of grants to a wide variety of entities.

"No other public blockchains have Bitcoin's combination of industry buy-in, accumulated credibility, and neutrality from inception."

For a fuller accounting of Bitcoin patronage initiatives, see [this piece](#) from BitMEX Research, with supplemental information [here](#). In short, Bitcoin's patronage environment has gone from one in which a half dozen core developers were subsidized by a handful of institutions, to a setting where dozens of individuals and projects – many of which lie entirely outside the domain of “Core” – are able to obtain financing from a much larger variety of donors.

Until recently, it had been virtually impossible for individuals to make tax-deductible donations to Bitcoin development (one shudders in [recollection of the Bitcoin Foundation](#)). This changed when the Human Rights Foundation announced its [Bitcoin Development Fund](#) last month, which comes wrapped in a helpful 501(c)(3) format. For individuals who want to donate directly to core developers, several Bitcoin developers have [signed up](#) to Github's new Sponsors program.

This is incredibly encouraging. Not only is essential but costly security review being funded, but non-Core public goods like BTCPayServer and Lightning are now supported. And critically, the broadening of the donor base means that allegations of capture or co-option ring hollow. Gone are the days where Blockstream faced allegations of hoarding all the most influential developers.

One imagines that the fundamental logic – firms that rely on Bitcoin should support development, not because it's the right thing to do, but because it's the economically rational thing to do – will eventually persuade even the most recalcitrant among them. At this point, large exchanges, custodians and brokers who resist giving back to the protocol which powers their businesses face a PR black eye.

For those versed in the dynamics of open source, Bitcoin's patronage system as a funding model should come as no surprise. Bitcoin works in ways that are not short-term expedient, but pay dividends in the final analysis. Of course, a protocol-derived pool of rewards with which to pay developers would have been much more convenient, but it would have completely undermined the political neutrality of the monetary system.

Every now and again, critics bemoan the lack of a protocol-financed slush fund with which to pay for improvements and public goods. Such pools of capital, derived either through pre-mines or the ongoing diversion of block rewards, exist in Ethereum, XRP, EOS, Zcash, Dash and many other Bitcoin alternatives. But far from enhancing the prospects for these networks, these funds are a source of bickering, self-dealing and graft. They endow the protocol-proximate individuals who control the purse strings with total discretion to direct funds to allies and friends. Governance controls are

generally weak and token holders lack the effective ability to monitor and police these expenditures.

“When it comes to monetary neutrality, projects with protocol financing are no better than the deeply politicized USD.”

These projects choose the unfortunate path of granting fiscal privileges to network administrators, effectively creating poorly-run bureaucracies. Corruption and malinvestment have been the predictable result. For networks aspiring to become critical financial infrastructure on a global scale, this constitutes a significant liability. When it comes to monetary neutrality, projects with protocol financing are no better than the deeply politicized U.S. dollar.

Even projects that do not currently expropriate validator revenue for development funds are not immune. The siren song of cheap money for development constantly rings in their ears. One notable example is Bitcoin Cash, which is currently embroiled in an ugly civil war over protocol financing.

Due to a paucity of developers on BCH, the most influential among them can effectively extort the community into granting them remuneration financed by the protocol itself. As such, major BCH stakeholders proposed an “Infrastructure Financing Plan” that would divert block rewards to a fund dedicated to development. This would constitute an effective redistribution from the already-questionable security budget towards a fund controlled by a small handful of individuals doled out to cronies.

Because BCH never developed a meaningful patronage system, token holders can now be shaken down to divert funds to certain developers. Even if this plan is rejected, the idea will linger. The only remedy is a stable patronage system. But no other public blockchains have Bitcoin's combination of industry buy-in, accumulated credibility, and neutrality from inception, so the emergence of similar patronage models appears unlikely.

This is one of Bitcoin's underappreciated advantages: by committing to a stable set of rules, Bitcoin has insulated itself from the expropriation of its supply for political expediency.

A real talk-blocker

By Bill MacDonald

Posted August 10, 2020

It was a little over a year ago that I first heard the phrase “Toxic Bitcoiner.” I was attending my first BitBlockBoom conference near Dallas. The event itself is Crypto Twitter incarnate, and the sweltering heat did nothing to curb my excitement as I found myself rubbing elbows with the who’s who of the Bitcoin world.



On the first day, I found myself in an Uber with Matt Odell, Marty Bent, and the Bitcoin Sign Guy as we rolled to a BBQ and bar filled with meat, drinks, and Bitcoin fun. Each day of the event was awesome. I found out that Bitcoin Tina looked nothing like I expected her to. I watched Jimmy Song get bullied (in good fun) into auctioning off his iconic hat. I chatted with Saifedean over a drink, learned about ATMs from LibertyX, found out that the cold wallet that I was using wasn’t cold enough, and had amazing “one more drink?”s in the hotel lobby as Gary Leland, the consummate host, greeted and chatted with the guests. The people were interesting, intelligent, and happy to help learners like me. The sense of community was real, though perhaps that was the beers talkin’.

On the second day of the event, Michael Goldstein set Crypto Twitter on fire as he lectured the room on tactics to “bully the people who don’t agree with us” and reclaim the term “toxic,” much in the same way we reframed the term “Bitcoin maximalist” and turned it from a pejorative into a badge of honor. He concluded that “if someone is unwilling to take on your untolerated, toxic opinion... They have simply not deserved yet to have actual

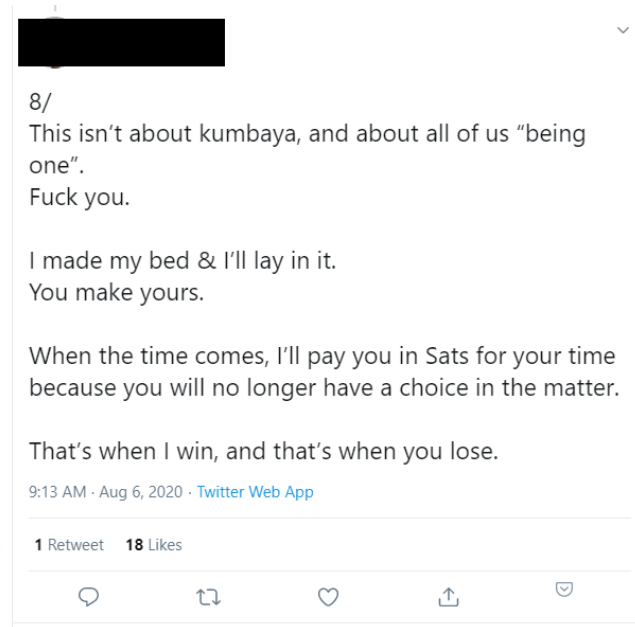
discussion.” Before he even finished his slides, word of the talk made it’s way to Crypto Twitter, sending it into a tizzy.

The truth is the talk was mostly tongue-in-cheek and well crafted for its audience. Funny and intelligent, it was perfect. Watch for yourself [here](#).

That said, it always struck me as a bit on the nose, a “funny ‘cause it’s true” sort of thing. Like many others who are hungry to learn about Bitcoin, I found my way to Twitter. While popular, Twitter is a horrible medium for nuanced discourse, a topic I’ve already [discussed](#). But structure aside, like BitBlockBloom, Twitter is where you find the thought leaders of the community. And unfortunately, it’s all too often where you find the thought leaders acting like assholes.

In the past month alone:





(i've blacked out the authors because im not trying to call out a person but instead point out a pattern.)

The whole thing feels like that dude you need to defend as “actually a really good, smart guy... I promise!” after he offends your wife for the third time. That’s a shame, because in some ways, it’s true. These guys really are good and smart. I follow the same people who tweeted the above, I would recommend others follow them, and I continue to look to them for informative content.

Unfortunately, there is another set of people, like my mom, my coworker, and my neighbor, who aren’t even sure why they are on Twitter... but they want to know more about Bitcoin and what it’s all about. These lay people might read the above and think, “Fuck this shit, I’m out.” The Bitcoin community needs to show this audience greater consideration..

It’s not just about making our moms feel good when they hop on Crypto Twitter for the first time. The community has a huge stake in these moms understanding and getting on board with the movement, and if they do, that has very real implications for Bitcoin’s place in the world... or more selfishly, its price. At some point, someone in Crypto Twitter needs to ask, “Who are we talking to?” If it’s just ourselves, an echo chamber, then what’s the point? And if the audience is broader than that, maybe the tone of our tweets should be crafted for that audience. Maybe memetic warfare isn’t the best way to help Bitcoin expand in all the ways and to all the places we believe are possible.

Roughly a year after that talk, I tweeted this:

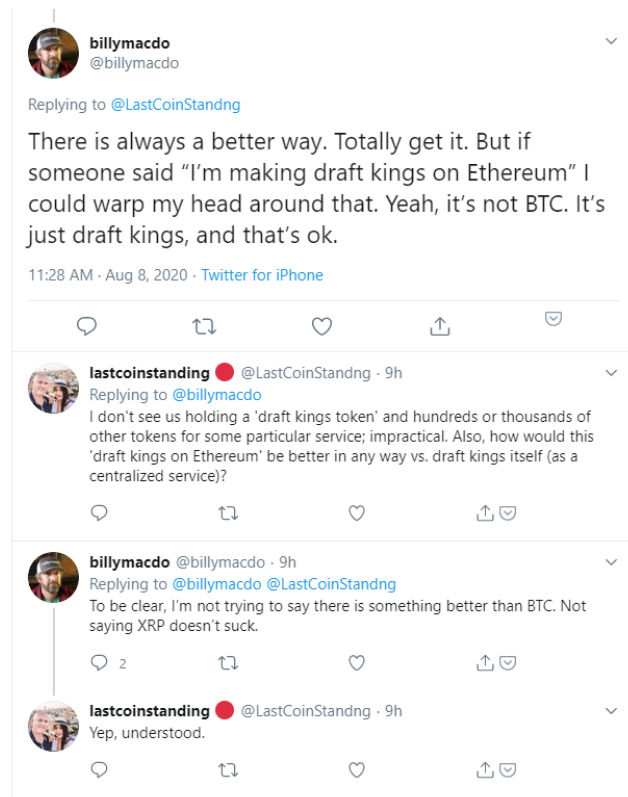


I don't find it controversial, and the logic should make sense even to the everyman who knows nothing about Bitcoin. I have far fewer followers than the heavy hitters of Crypto Twitter, so I didn't expect much in the way of engagement. But I definitely didn't expect to get blocked by anyone.

That conversation resulted in my being blocked by the person who replied, someone I otherwise find to be a thoughtful and measured contributor to the community. And this is where we are at. I didn't think much of it. But a "normie" making that same statement and then being blocked over it would and should leave the interaction with a bad taste in their mouth.

Alternatively, that same statement can lead to more level-headed results. In a different reply thread to the same tweet, I had this exchange with another community member. I'm not sure we agreed, which is great, but we interacted and could do so again in the future.

As BitBlockBoom 2020 rapidly approaches (an event I sadly can't join this year and will suffer from FOMO the entire weekend it takes place), Bitcoin's narrative is stronger than ever. Perhaps it is time to reassess our approach to how we talk about that narrative. Maybe this warfare, which ultimately adds up to insiders fighting with insiders, needs a hard fork.



That isn't to say all projects are created equal or that real problems don't exist in protocols. When problems exist, we should discuss them. However, Twitter isn't a bar full of insiders drinking and ribbing each other at a conference. It's public. We should consider not only who we want to engage but who the real audience is and how they will perceive the infighting. As always, and especially on a platform with as large of an audience as Twitter's, getting more people to understand and use Bitcoin should be the community's goal. Encouraging 5 people to get into Bitcoin is more important than saving one person from buying [*enter shitcoin here*] and our messaging needs to align with that idea.



**Memetic
Warefare**

*Not acting like a dick
on-line*

Is Bitcoin the world's safest reserve asset?

By Thibaud Marechal on [Knox] Custody](<https://blog.knoxcustody.com/>)

Posted August 14, 2020

Bitcoin · Aug 14, 2020

NASDAQ-listed MicroStrategy's opening gambit says so.

August 11th, 2020 marked Bitcoin as a corporate treasury asset on Wall Street. The public \$1.2 billion business intelligence software company, MicroStrategy, announced that it bought 21,454 BTC, converting \$250 million of their cash treasury. It is the first mainstream public corporation to announce Bitcoin holdings at this scale. In this article, we will attempt to analyze what this means for corporate treasury, public company valuations and indirect institutional participation in Bitcoin.

MicroStrategy's move snapped up 0.1% of Bitcoin's fixed supply of 21 million units, accounting for 50% of their excess cash reserves in a novel capital allocation strategy. Given the finite pool, such a material grab of bitcoin could only be accomplished by 978 companies before the supply technically "runs out", though in practice a large chunk of extant supply is not even for sale.

During their second quarter earnings call in late July 2020, Michael Saylor, CEO of MicroStrategy, announced his intention to explore purchasing Bitcoin, gold or other alternative assets. During the Covid-19 recession, MicroStrategy saw its cash, cash equivalents and short-term investments grow to over \$500 million, with only \$50 million needed to cover operational expenditures for the year, leaving the company with extra cash on hand.

MicroStrategy 2Q 2020 Earnings Call

Capital Allocation

- \$500+ million cash and short-term investments is a strategic asset
- We are confident we can be more active using our balance sheet to generate long-term shareholder value
- Planning to return up to \$250M of excess cash to shareholders over the next 12 months
- Seeking to invest up to \$250 million of excess cash in alternative investments over the next 12 months

MicroStrategy's 2Q 2020 Earnings Call

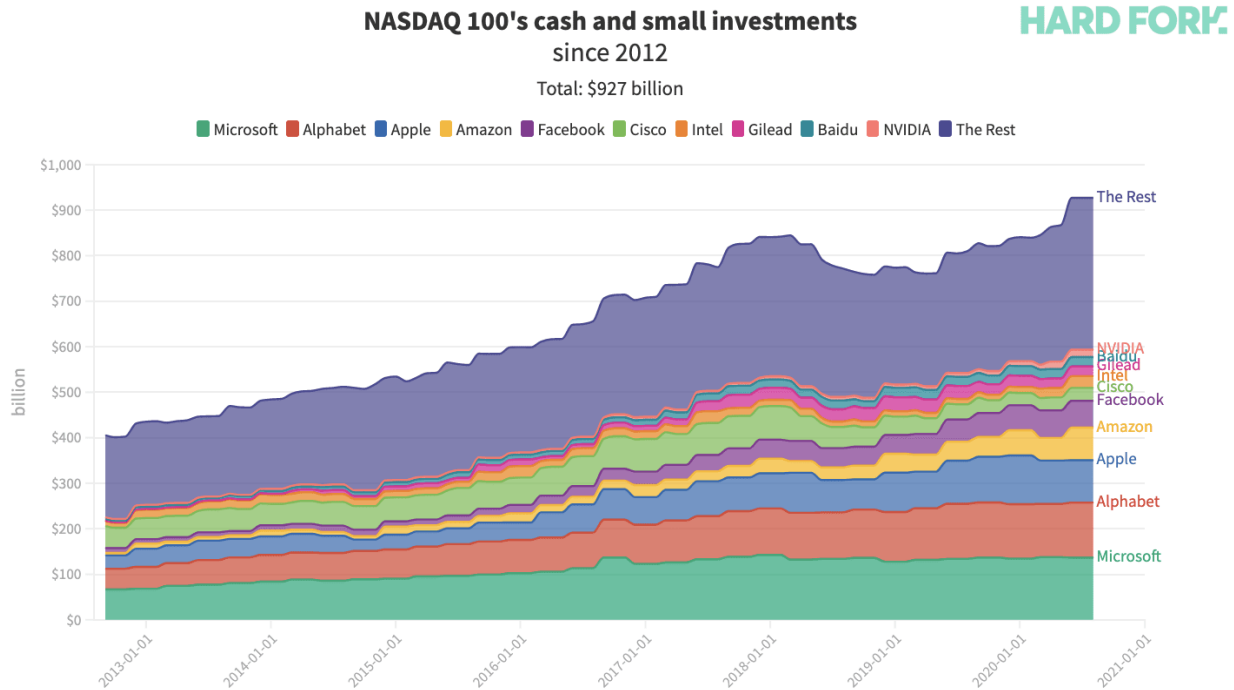
While initially hinting at a broader portfolio of alternative assets, the full allocation targeted only one of the assets previously mentioned: Bitcoin. All-in. The argument was built around the potential for the deterioration of real value in fiat currencies, and a belief that Bitcoin represents a safer store of value than other alternatives. These concerns were explained in the [announcement](#) MicroStrategy released earlier this week, expanding on the rationale behind exclusively purchasing bitcoin as part of their new capital allocation strategy, which seeks to support their fiduciary obligations to maximize long-term value creation for their shareholders.

“MicroStrategy spent months deliberating to determine our capital allocation strategy. Our decision to invest in Bitcoin at this time was driven in part by a confluence of macro factors affecting the economic and business landscape that we believe is creating long-term risks for our corporate treasury program — risks that should be addressed proactively,”

Is this capital allocation into Bitcoin signaling the emergence of a novel trend in corporate treasury programs? Should CFOs and executive teams of other publicly-listed firms reconsider their allocation plans for their excess cash reserves? How exposed are the aggregate cash holdings of businesses to currency debasement and other global macro risks? What does Bitcoin as a corporate reserve asset mean for Wall Street's balance sheets and cash flow modelling?

A glut of cash is being hoarded

Now that Bitcoin has been adopted as a primary reserve asset by MicroStrategy, a well-capitalized NASDAQ-listed firm, other companies will be forced to sit up and take notice. Amid the recent economic downturn driven by globalized lockdowns and supply chain disruptions in the first half of 2020, companies slowed down their investment programs, reduced costs, and raised cash reserves to adjust to the economic uncertainty. The companies comprising the Nasdaq 100, the index of the 100 largest non-financial companies traded on the Nasdaq stock market, are now sitting on [nearly \\$1 trillion in cash](#). US tech moguls like Microsoft, Google and Apple are accumulating more cash than ever. Despite sitting on \$121 billion of cash and cash equivalents, Alphabet, Google's parent company, [raised \\$10 billion issuing its most affordable bonds ever recorded](#). Collectively, since 2012, the Nasdaq 100 went from holding \$405 billion to just shy of \$1 trillion in cash reserves.



NASDAQ 100 sits on nearly \$1T in cash

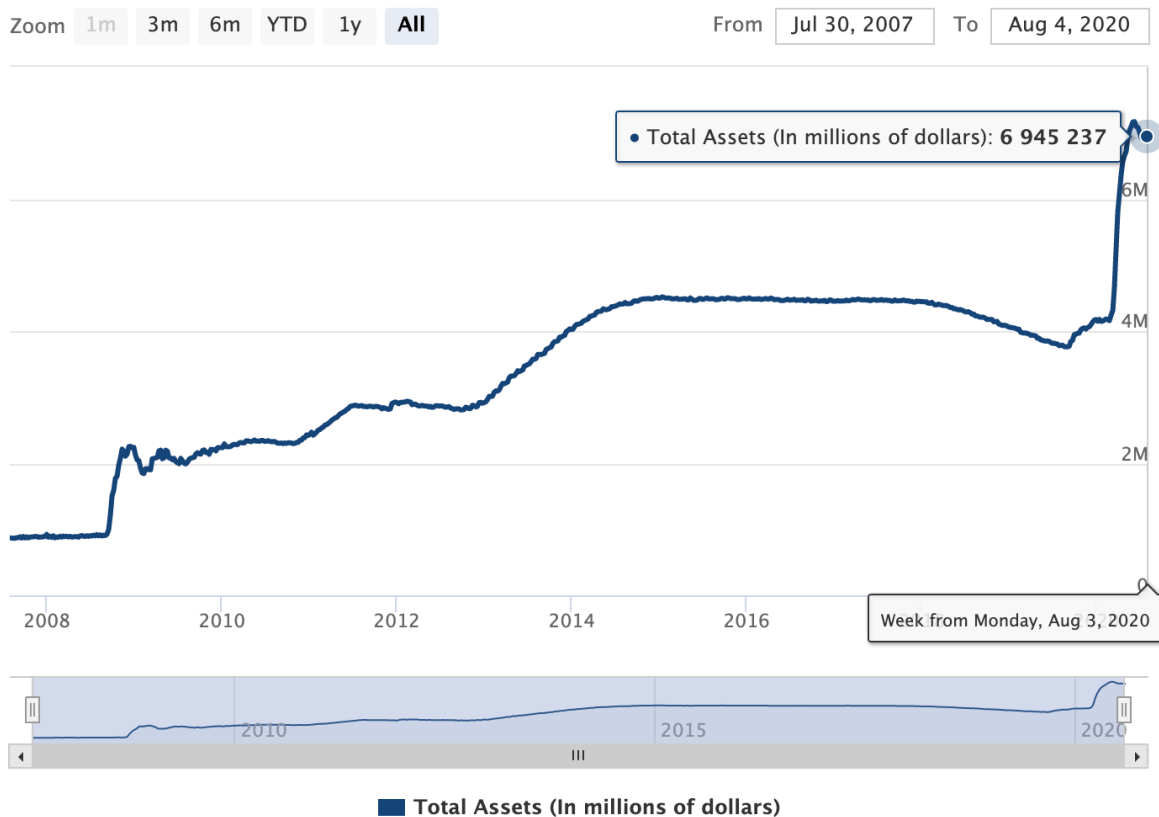
Global stimulus is hurting cash

Near-zero interest rates pulled down the cost of capital, acting as a favorable ingredient for an \$840 million surge in corporate debt financing in the first half of 2020 alone, while monetary expansion is adding to the global stimulus programs that were triggered earlier in March, as a result of the response to the Covid outbreak. Business operators liquidating assets and cutting costs to manage operational risk end up raising their excess cash reserves, but now must also ensure these reserves are not excessively devalued in the face of aggressive quantitative easing programs.

“Macro factors include, among other things, the economic and public health crisis precipitated by COVID-19, unprecedented government financial stimulus measures including quantitative easing adopted around the world, and global political and economic uncertainty. We believe that, together, these and other factors may well have a significant depreciating effect on the long-term real value of fiat currencies and many other conventional asset types, including many of the assets traditionally held as part of corporate treasury operations.”

Led by the US Federal Reserve and supported by other central banks, global QE asset purchases in 2020 alone are set to hit a staggering \$6 trillion, more than half the cumulative global QE seen between 2009 and 2018. While equities have been soaring with new liquidity injections via corporate debt purchasing programs, the US Federal Reserve now holds almost \$7 trillion of

assets on its balance sheet, an astounding rise of around 72% in less than 3 months, according to The St. Louis Fed.



Credit and Liquidity Programs and the Balance Sheet

As demonstrated by MicroStrategy's move, monetary expansion at this scale is triggering even large publicly listed companies to reconsider the long-term real value of existing cash reserves, as the supply of fiat currencies are inflated away to prevent generalized deleveraging events, and drastic market sell-offs. While the dollar may not see inflation right away given its dominant global reserve currency status, some firms such as MicroStrategy are noticing and taking preventive measures to protect their balance sheets and to manage long-term risk for their shareholders. The evolution of capital allocation strategies is now favoring assets that are not trivially debasable to guard against currency devaluation risks.

Bitcoinization of corporate treasury

Treasury operations generally include the management of a firm's cash holdings, with the ultimate goal of managing the enterprise's liquidity and mitigating operational and financial risks. Based on the size of the firm and its activities, such operations may include holding positions in a variety of fiat currencies, trading bonds or using financial derivatives. It is an essential

activity of any company, especially for listed entities who have a duty to publicly disclose their financial health to the markets.

A good and reliable holding in a corporate treasury should be dependable over the long term whether it be for price stability, liquidity or long term value creation for shareholders. MicroStrategy's decision to hold bitcoin as a primary reserve asset is a market signal that Nakamoto's digital cash is gradually being adopted for its sound properties by responsible institutions.

"This investment reflects our belief that Bitcoin, as the world's most widely-adopted cryptocurrency, is a dependable store of value and an attractive investment asset with more long-term appreciation potential than holding cash. Since its inception over a decade ago, Bitcoin has emerged as a significant addition to the global financial system, with characteristics that are useful to both individuals and institutions. MicroStrategy has recognized Bitcoin as a legitimate investment asset that can be superior to cash and accordingly has made Bitcoin the principal holding in its treasury reserve strategy."

Fiduciaries need Bitcoin

Senior management executives or CFOs managing corporate treasury programs may be in breach of their fiduciary duty if due diligence and adequate capital allocation strategies are not developed for bitcoin. As a public company, MicroStrategy's move effectively "removed career risk for CFOs from putting company treasury into Bitcoin". Andy Yee, Senior Director of Public Policy at Visa pointed out that this allocation is similar to hedge fund billionaire Paul Tudor Jones's letter about his recent 1–2% allocation into bitcoin as part of his portfolio.

Paul Tudor Jones removed career risk for hedge fund managers from investing in Bitcoin.

MicroStrategy removed career risk for CFOs from putting company treasury into Bitcoin. #Bitcoin #crypto— Andy Yee (@ahkyee) August 11, 2020

MicroStrategy's ownership structure is mostly institutional, which accounts for 466 firms representing 97% of total shares. BlackRock and Vanguard, two leading institutional fund and wealth managers, holding \$7.43 trillion and \$6.2 trillion of assets under management respectively, comprise more than 25% of MicroStrategy's capitalization table, as surfaced by Swan Bitcoin, a US Bitcoin brokerage service. Both institutional participants now have an indirect exposure to bitcoin, which will incentivize them to perform extensive due diligence and research on Bitcoin. Being shareholders of a multitude of other public companies, these institutional investors regularly assess the health of their portfolio, comparing industry benchmarks, cash flow modeling

and competitors' use of capital in production among other things. Bitcoin is now part of the equation.

Top 10 Owners of MicroStrategy Inc

Stockholder	Stake	Shares owned	Total value (\$)	Shares bought / sold	Total change
BlackRock Fund Advisors	15.24%	1,166,307	144,528,763	-44,916	-3.71%
The Vanguard Group, Inc.	11.72%	896,921	111,146,450	+17,190	+1.95%

MicroStrategy Inc - Ownership Structure

Bitcoin is no one else's liability

One obvious question comes to mind: what happens if MicroStrategy's bitcoin holdings appreciate substantially in the coming years? How does management handle this exposure and decide to rebalance their risk? As bitcoin's purchasing power rises, it could act as major leverage for MicroStrategy's future capital deployments when it comes to entering others markets, launching new products or even acquiring competitors. As Preston Pysh, host of the Investors Podcast suggested, the practice of companies holding bitcoin on their balance sheet is just getting started. MicroStrategy investing \$250 million from close to \$420 million of cash reserves into bitcoin is the beginning of a new era in corporate treasury.

MICROSTRATEGY INCORPORATED CONSOLIDATED BALANCE SHEETS (in thousands, except per share data)			
	June 30, 2020 (unaudited)	December 31, 2019*	
Assets			
Current assets			
Cash and cash equivalents	\$ 420,899	\$ 456,727	
Restricted cash	1,221	1,089	
Short-term investments	109,972	108,919	
Accounts receivable, net	123,794	163,516	
Prepaid expenses and other current assets	16,887	23,195	
Total current assets	672,773	753,446	

MicroStrategy Incorporated - Consolidated Balance Sheets

More than an inflation hedge, holding bitcoin may become a capital-efficient way to strengthen corporate balance sheets in times of financial turmoil when income flows lessen. As bitcoin holdings inflate unrealized gains for corporate owners, it may be used as a source of liquidity to service operational expenditures and stay afloat while other competitors suffer from bad economic conditions and over-leveraged balance sheets. The massive rise in US corporate debt from \$3.3 trillion to \$6.5 trillion, combined with the most brutal decline in consumer spending ever experienced in the US will

prove very profitable for companies holding bitcoin and seeking acquisitions of distressed competitors. The competitive landscape may be completely reshaped by Bitcoin in the next decade, proving that balance sheet resilience is worth more than efficiency and cheap leverage.

Strikingly, MicroStrategy's board of directors has five members acting as fiduciaries for an institutional-centric shareholder base. Responsible for capital allocation strategies and long term value creation, the board elected bitcoin as the desired primary reserve asset for the company's treasury, allowing MicroStrategy to become an indirect vehicle for public bitcoin price exposure. If bitcoin appreciates in the coming years, MicroStrategy's stocks may rise substantially, as Wall Street's equities investing is already established and seeking diversified yield. At what point does MicroStrategy become a Bitcoin ETF, rather than a software firm? If Bitcoin rises, is management under pressure to execute regular treasury rebalancing? Is it their duty to seek the dollar profits or hold onto unrealized gains for future leverage? These remain open questions that MicroStrategy's management team will have to sort out for their shareholders.

The rise of a new numeraire

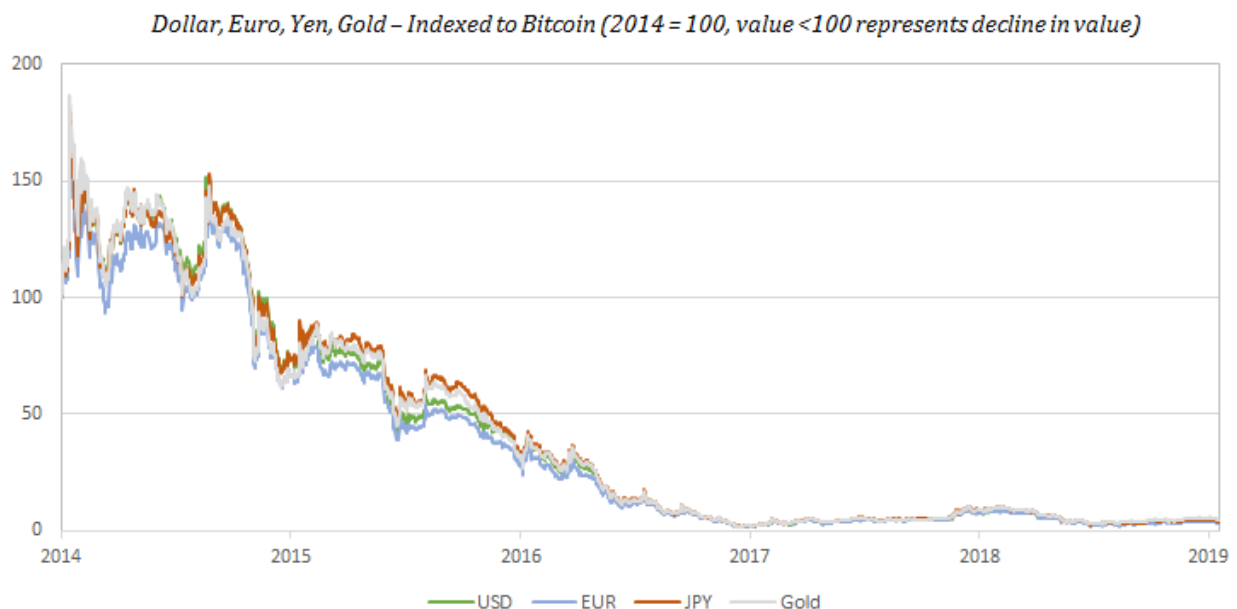
As part of an inescapable Monetary Darwinism, CFOs and executive teams will gradually, then suddenly add bitcoin to their books in an effort to protect their cash reserves for productive use later on. MicroStrategy's CEO tweeted back in 2013 that "Bitcoin days are numbered". Some seven years later, MicroStrategy has now moved \$250 million or around 50% of its cash treasuries into it. Eventually, everyone will understand the monetary evolution that Bitcoin brings. For most it will take time, and the revisiting of pre-established yet obsolete mental models. Michael Saylor should be commended for updating his views, and it is likely his peers will soon follow suit.

MICROSTRATEGY INCORPORATED			
CONSOLIDATED BALANCE SHEETS			
(in thousands, except per share data)			
	June 30,	December 31,	
	2020	2019*	
	(unaudited)		
Assets			
Current assets			
Cash and cash equivalents	\$ 420,899	\$ 456,727	
Restricted cash	1,221	1,089	
Short-term investments	109,972	108,919	
Accounts receivable, net	123,794	163,516	
Prepaid expenses and other current assets	16,887	23,195	
Total current assets	672,773	753,446	

Appearing as a de facto hedge against inflation with its inalterable scarcity, bitcoin can also be understood as a high-return investable asset. Companies in the future could even decide to denominate their operating margins and

returns on investment using bitcoin, not dollars or other inflation-based fiat currency. Holding bitcoin in corporate treasury accounts may become a standard for all Wall Street tickers. As bitcoin obsolesces all other money and its value appreciates over time, bitcoin capital deployment to resources for production will become more conservative. Simply holding bitcoin for long term price appreciation is resetting the importance of opportunity cost in the economic calculus to plan for resource allocation in the production cycle for most companies.

Once it reaches a certain monetary base and purchasing power stability, corporate returns may have to be denominated in bitcoin, not dollars or any other fiat currency. As Preston Pysh highlighted on Stephan Livera's podcast, Bitcoin could become the default global numeraire—a benchmark item in comparing the value of similar products or financial instruments. Cash flow and treasury denomination in bitcoin will change how companies such as MicroStrategy shape their capital allocation strategies in the long term, turning bitcoin into a unit of account, its ultimate monetization tipping point leading to sustained global deflation—the root of an abundant future.



Unchained Capital Blog - Gradually, Then Suddenly

Zooming out, it remains to be seen what will happen if and when other companies decide to update their capital allocation strategies to include bitcoin as part of their corporate treasury programs. Should they invest 1%, 5% or 50% of their excess cash reserves walking in MicroStrategy's footsteps? One thing is certain: this target number should no longer be zero. Management teams of public companies have a fiduciary duty to their shareholders, and must get off zero, a meme popularized by Partner of institutional fund Morgan Creek Digital, Anthony Pompliano.

Pragmatic risk management

Short term, a slew of additional questions emerge around the custody of bitcoin holdings for listed companies that are not specialized in managing private keys, including the internal controls and governance model that must be adopted by management teams. Should they be using trusted custodians such as Knox or Fidelity, or should the fund administrators be holding keys in sovereign collaborative multisig quorums such as Unchained Capital? What about a hybrid custody model? From their SEC filings on August 11, 2020, it appears that MicroStrategy's bitcoin holdings are currently held at various custodians, with the absence of insurance clearly presented as an unmitigated risk:

"While we hold the bulk of our BTC assets with established cryptocurrency custodians, a successful security breach or cyberattack could result in a partial or total loss of our BTC assets in a manner that may not be covered by insurance or indemnity provisions of our custody agreements with those custodians. Such a loss could have a material adverse effect on our financial condition and results of operations."

Considering how much time we at Knox spend managing Bitcoin custodial systems with comprehensive insurance coverage, this has become another interesting area to watch. Our own questions include wondering if auditors and securities regulators may demand that NASDAQ-listed companies such as MicroStrategy's holdings be protected by full insurance coverage, which has been historically difficult to obtain for the first wave of mainstream Bitcoin custodians. We believe that fiduciaries, executives and the management teams of listed companies will continue having to think through all risks present in allocating to bitcoin, whether it be limiting onerous costs such as execution slippage when building large bitcoin treasury positions, or attaining adequate insurance coverage for their long-term holdings.

Towards deflation-based markets

After over a decade of successful block production, 99.98% uptime, appreciating value, community growth, infrastructure build-out, and deepening liquidity, Bitcoin can no longer be ignored. Michael Saylor's Bitcoin dismissal in 2013 juxtaposed against MicroStrategy's attitude today speaks volumes. "MicroStrategy's investment thesis on Bitcoin as a store of value is spot on. Across all other assets, Bitcoin matches all the properties of being a treasury asset that a company can allocate cash into to preserve its future buying power in an environment of easy money. Now, since it has made the first move, the game of musical chairs for corporations buying bitcoin is

officially on,” mentioned Louis Liu, CIO at Mimesis Capital, a single-family office that focuses on wealth preservation through Bitcoin.

Overall this news is undeniably bullish for Bitcoin's scarce information space, considering bitcoin's stock-to-flow ratio strengthened to over 50 during last May's halving event, and is catching up to gold's S2F of 60. With all the documentation made available openly on the Internet, will CFOs and finance executive teams still be able to meet their fiduciary obligations if they don't hold bitcoin in their corporate treasury within the next 10 years? Bitcoin price appreciation will also be a direct result of this new adoption if companies start allocating their treasuries into bitcoin, though one may wonder if other traditional asset classes can depreciate from corporate treasury divestments. Once bitcoin gets adopted by most companies, a global and sustained deflationary future may await us, allowing responsible capital allocators to invest soundly accumulated capital for truly productive uses, as popularized by Jeff Booth, author of The Price of Tomorrow.

We may look back on this move in years and see it as a historical moment for Bitcoin.

Balinese Cockfights & Bitcoins: How one can help us understand the other

By Mick Morucci

Posted August 17, 2020



Balinese cockfights and cryptocurrencies, can you think of two more unrelated topics? You'd be surprised then to discover that at closer inspection, looking beyond blockchains and metal spurs, the social dynamics taking place around cockfight rings can help us understand those around cryptocurrencies.

As an anthropologist, I take the view that for outsiders to understand different world views, such as those of indigenous populations, or entirely new phenomena, such as crypto communities, taking a one-glance-view is simply never enough. To better understand these worlds, we must instead suspend our biases and (dis)beliefs to truly observe what's happening within. With this in mind, this analogy doesn't aim to trivialise crypto communities as narrow tribalistic phenomena. Rather, aims to expose the values and beliefs at the hearts of its communities.

It's from there, from this outsider's perspective, that Balinese cockfights are reduced to a senseless form of gambling based purely on violence. Similarly, Bitcoin might at first be associated with gambling, black markets, and

malicious hackers. But dive into these two worlds, and things start looking quite differently.

A one-glance view

The basics of Balinese cockfights are easy to grasp: two male cocks fight against each other, sometimes with a metal spur tied around one leg to increase physical intensity, while people cheer around them in an arena, betting money on which cock they think will win. This has been a popular sport for millennia, mostly in South and Southeast Asia. Today, this activity is regulated or banned in many countries as a response to foreigners and onlookers having judged it as a 'primitive' and a 'ruthless' form of gambling.

A similar view prevails amongst outsiders looking into the world of Bitcoin: that it is primarily a form of gambling. And understandably so: since the 2017 bubble, major players in the news industry share this view, painting Bitcoin as a kind of Pinocchio's Land of Toys where greedy speculators make money through a ponzi scheme. Famous investors and influential public figures replay this simplistic notion. And then there are the malicious hackers actually employing cryptocurrencies to do harm, which never fail to capture the spotlight of online news. Most recently, an attack that took over several high-profile Twitter accounts was associated with Bitcoin. It is therefore only natural that an onlooker might associate Bitcoin with bubbles, gambling, and hackers, at first glance.

While these elements are undoubtedly part of the Bitcoin phenomenon, they are certainly not all there is to it. A much more informed and holistic understanding of it can be gained only by taking a peek inside. Let's practice that approach by looking at Balinese Cockfights first, and at the inner worlds of a Bitcoin community later.

Meaning and speculation in the Balinese Cockfight

Anthropologists have been recording cockfights since the 1930s. And what they've seen is that for many Balinese, cockfights are an activity with deep significance. Through it, people establish in-group affiliations, play the everyday politics of prestige, and learn and reiterate cultural values and beliefs.

One thing that makes cockfights sociologically relevant is that they are often carried out between members of different kin-groups or villages, and gamblers must never place bets against those in their own kin-group, indicating that profit is not the only goal here. Additionally, fights of greater importance are always carried out by the leading members of kin-groups, to reaffirm their authority (Geerts). This means that cockfights are a means to many ends, among which money is only one.

These fights also help entire villages to reaffirm their cultural values, and the Balinese are deeply aware of this. In this [video](#), Balinese cockfighters make clear that this activity is a means of expression. They use this space to display their anger as well as to find the emotional balance that's essential for them to be considered a true cockfighter and a truer man, more broadly. Being a true cockfighter is part of an archetype of 'man' they aspire to, which is "being arrogant, resolute and honor-mad player with real fire" ([Geerts](#)).

But not all participants in these cockfights see this. While those in the inside ring of the arena understand the cultural value and social meanings of the cockfight, the ones in the outer ring "are in it mainly for the money" ([Geertz](#)).

In so being, these outer ring speculators take little notice of the layers of meaning and significance that come with the game. And interestingly, these people are usually unwelcome in this environment. 'True cockfighters' see them as "fools who do not understand what the sport is about, vulgarians who simply miss the point of it all" ([Geertz](#)). And to top it off these avid gamblers are usually the people who get burned financially and don't last long.

For "true cockfighters", money is not entirely unimportant, but it is a secondary matter in the play of the game. How much money one wins or loses evens out with time, and, in any case, money moves around the group of serious and respected players. And that's the point: "What makes Balinese cockfighting deep is not money in itself, but what money causes to happen: the migration of the Balinese status hierarchy into the body of the cockfight" ([Geertz](#)). Money causes members to have skin in the game in the community, and in so doing making the meanings and values real.

While cockfight speculators solely interested in making money do exist, they represent the outer fringes of Balinese cockfights, and not the heart of it__. For those at the centre of the game, cockfighting is a tale of values, status, and belonging. What does this mean for the Bitcoin community?

Meaning in the Bitcoin community

What is meant by "Bitcoin community" is itself hard to grasp, let alone visualise in place. This is not only because it is a highly heterogeneous group, but because, although it occasionally meets up in physical locations worldwide, this community is digitally native: members mostly inhabit Twitter, Reddit, Telegram groups, and [Bitcointalk.org](https://bitcointalk.org) chatrooms.

So to help us imagine the Bitcoin community, a visual metaphor of the cockfight arena comes in handy: at its centre are the competing

cryptocurrencies being discussed, in the first outside ring are the holders of the cryptocurrencies, and further out are the speculators.

Let's start from the centre of the online cyber arena, where different cryptocurrencies communities fight among each other over the relative merits of their own cryptocurrencies over the other. To illustrate this take the recent confrontation between the Bitcoin and the Ethereum communities over the current supply of Eth coins, which isn't so easy to discern, thus termed [#supplygate](#). Bitcoiners, deeply valuing scarcity and its audit, attacked Ethereum for what they believe to be an unsound monetary structure.

Discussions can get very technical, but they stem from fundamentally different cultural values and beliefs. There is much more to say on this topic, but for now, suffice it to say that the Bitcoin and Ethereum communities are very, very different cultures: see Tweet below for a personification of what these cultures might look like.



But the fight is not just against other crypto communities. In fact, the Bitcoin community's biggest competitor is the current monetary paradigm governed by the Central Banks, who have monopoly power over what money is, how it is issued and who issues it, and to whom it is issued to. More on this soon, but this is what Bitcoiners are fighting against.

At the heart of these cryptocurrency "fights" are the memes which, like the metal spurs attached to fighting cocks, intensify the game and render it more significant. Memes can be shallow or deep, sentimental or antagonistic, funny or sad. But they almost always capture the beliefs and values of the communities. Many themes emerge from the Bitcoin community's memes,

but the most recurring ones include references to Bitcoin's price (it being a rollercoaster of volatility or it "going to the moon" when the price goes up rapidly), references to the FED printing money (money printer go 'brrr'), and references to members' expectations and hopes that Bitcoin will become the hard money of the future.



The Bitcoin community's underlying belief is that the world needs Bitcoin. That Bitcoin was built by the people for the people to enable a world that values self-sovereignty, privacy, and a better form of money. This ideal world is seen in stark contrast to the current financial and monetary system, which is seen as broken and economically disempowering due to inflation, increasing inequality and monetary irresponsibility of central banks.

This view becomes even clearer when we look at Bitcoin's origin story. The white paper was published soon after the American government bailed out major banks following the 2008 financial crisis under the banner "too big to fail". On the 3rd of January 2009, the first block of Bitcoin was released with an encoded message: "***The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.***" Who created Bitcoin, we still don't know. What we do know is that the person or group behind it, going by the pseudonym Satoshi Nakamoto, saw systemic fragility and economic unfairness in our financial monetary paradigm and decided to address that by creating an alternative: an open-source, decentralised, permissionless value-sharing protocol.

```

00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;fiyz{.2z>...
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.E.A~SQ2:Y...
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)=iyy...~|
00000050 01 01 00 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....yyyyy..y...
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ...Ethe Times 03...
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksyyyyy..
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 58 48 27 ...CA.g5Y"bun"
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gn"qo..C"(a9;..
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybae.ab?I64?Ll8A
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 08 8D 57 ou.A.A.D)8M...w
00000110 8A 4C 70 2B 6B F1 1D 5F AC AC 00 00 00 00 00 00 Slp+kn..?....

```

It's clear, then, why for the Bitcoin community Bitcoin stands for much more than gambling, black markets, and hackers: it represents the pursuit of a new type of freedom.

This is not to say that the speculation of the price of

Bitcoin and other crypto does not exist within the community or is not important. The price of Bitcoin is actually a function of the in-built scarcity of Bitcoin, which halves the issuance of new coins every 4 years, thereby leading to a consistent and abrupt rise in value that occurs in cycles. This creates an incentive for people to hold the currency and gives different waves of adopters a chance to join and build critical mass through time.

If you look closely, the in-coded design of Bitcoin incentivises long-term investment decisions rather than narrow short-term speculation.

Hodling and Lambos in the Bitcoin community

Similarly to the Balinese cockfights, these values and beliefs I just touched upon are not evenly spread across the Bitcoin community. In the first concentric circle around the arena, at the core of the cryptocurrency community, we have the hodlers, the long-term ‘holders’ of Bitcoins. Further out, we have what we here call the lambo guys, the speculators.

Hodlers are a highly heterogeneous group with differing beliefs and values. The practice of hodling is common among all insiders in such a way that we might call it a cultural motif or philosophy. But if we were to explain Bitcoiners more simply to an outsider looking in, and put all the sub-groups and tribes aside for a minute, we might come to see hodlers as the heart of the Bitcoin community.

Hodlers continuously buy Bitcoins, or “stack sats” (sats being the cent-like units of Bitcoin) while they ‘Hold On for Dear Life’ as the Bitcoin price soars and crashes due to its high volatility. They hold on because they believe the world needs a new monetary system and because they expect Bitcoin’s price to inevitably rise in the long term. This leads many Hodlers taking “irresponsibly long” Bitcoin positions — meaning putting 30%, 50%, or even all of their portfolio into Bitcoin. This, more than anything else, should demonstrate that at the heart of the Bitcoin community lie deep convictions and beliefs, it’s not quite a ponzi scheme.

Outside these hodler circles are the lambo guys, for whom Bitcoin is only a means to getting rich. They often resort to the “When Lambo?” meme, asking when Bitcoin price will soar in order to buy themselves a Lamborghini. Hodlers, on the other hand, will never or rarely sell their Bitcoins as they are committed to Bitcoin for the long-run.

Similarly to the ‘true cockfighters’ of Bali, who understand the underlying significance of a cockfight and look down upon gamblers, ‘true hodlers’ despise speculators who see Bitcoin simply as a way of getting rich without understanding what Bitcoin is and means. They don’t get it, they don’t see the significance of Bitcoin as a revolutionary tool (read Dan Held’s article for

more). And as a result of their short-termism, many speculators end up being burned financially because they lack this foundational understanding.

The fact that 'money' is involved in the world of Bitcoin, and big money indeed, does not render it shallow. Rather, the opposite is true. Just like in the Balinese Cockfight, money makes the fight more real, makes people's involvement more concrete because their skin is in the game. Group affiliations grow and aspirations of a fairer (less unequal), de-centralised (less monopolised), democratic (less authoritarian) and more equal world order.

If you gamble for money, you don't get cockfighting. If you speculate with Bitcoin, you don't get Bitcoin.

Perhaps by now you'll agree with me: Between cockfights and bitcoins there might be a technological abyss. But the social dynamics revolving around the topic of speculation may not be all that different. You still have shallow speculation on the margins, and deep play closer to the arena.

Bitcoin and other cryptocurrencies surely have the capacity to wake up the speculative nature in any of us. But what keeps the Bitcoin community going is not shallow short-term speculation. It's the strong values of the hodlers, the state of play articulated by the frustration and hope in the humorous memes, the political philosophy focused on human freedoms. The irresponsibly long positions taken by the Bitcoin hodlers make all of it more real.

When it comes to Bitcoin and Balinese cockfights alike, conversations that focus exclusively on speculation, gambling, and greed risk totally missing their points. Discussions surrounding Bitcoin in particular need to consider the political and philosophical questions this community raises about money, privacy, self-sovereignty, and of course, memes.

To this end, journalists, the media, academics, politicians, and individuals need to start paying closer attention to this world before jumping to conclusions. The next time people invoke straw-man arguments of Bitcoin being all about speculation, teach them about Balinese Cockfights and perhaps this article might be a good place to start. Even better, introduce them to some hodlers. After all, at some point or another, we might all have to join the Bitcoin arena.

Notes & Acknowledgements:

Thanks to Maggie for her the invaluable conversations that gave way to insights that inspired this article, Paula for her generous editing and Giulio and Lawson for their valuable suggestions. Cockfights are illegal in many countries due to animal violence.

As the author I do not condone animal violence, but simply wish to provide a glimpse into the perspectives of traditional Balinese insiders who practice the sport in order to build a more complex picture of the phenomenon.



If you liked this article you can follow me on:

- **Twitter:** <https://twitter.com/metamick14>
 - **Website:** <https://www.mickmorucci.com/>
-

In Memory of Hal Finney, RIP — Builder of a More Trusted World

By Bill Buchanan

Posted August 22, 2020



Did you know that the first proof-of-concept of Bitcoin was created on a Window's XP?

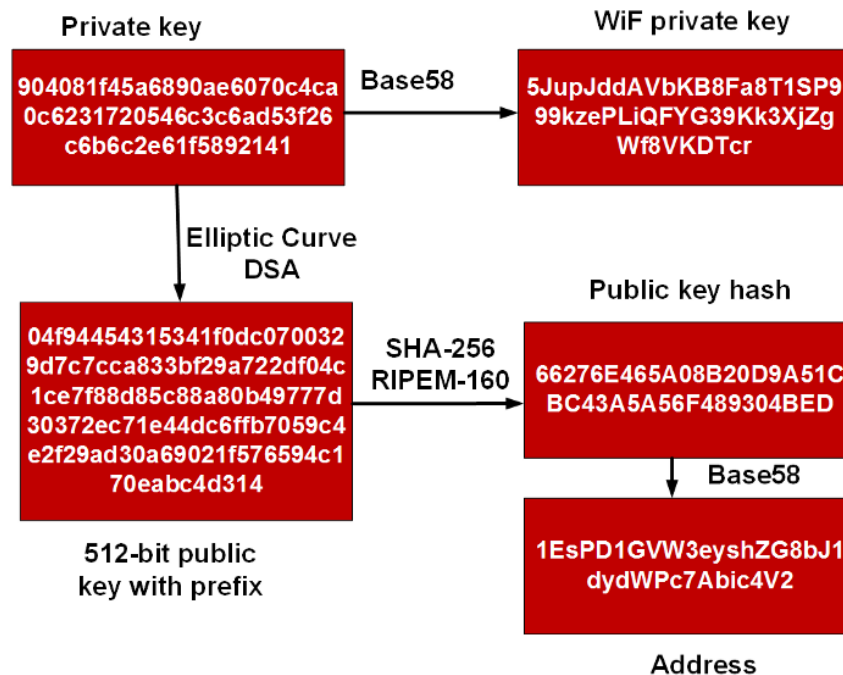
In January 2009, Hal Finney — never a person to write long tweets — sent a message of “Running bitcoin”, and which was the start of a new world:



I've spoken to quite a few of the great people who developed the foundations of cryptography, but the one person I would have loved to have spoken to is Hal Finney. He was the person who received the first transaction of 10 BTC from *Satoshi Nakamoto* and was the person who created the first proof-of-concept of the cryptocurrency. In fact, Hal lived a few blocks away from a

person named Dorian Satoshi Nakamoto, and, as if someone, somewhere, took a random name from the local telephone directory.

So, Hal, in helping to create Bitcoins, created a fascinating jumble of crypto that works surprisingly well:



His name appears in so many places within the rise of cryptography, such as an acknowledgement from Daniel Bleichenbacher (Bell Labs) on the publication of his classic attack on SSL [[here](#)]:

Acknowledgments

I thank Markus Jakobsson, David M. Kristol, and Jean-François Misarsky, as well as the members of the program committee, for all their comments and suggestions. I am grateful for the cooperation of the people at RSA Laboratories. I thank **Hal Finney** for telling me about his experiments on different SSL servers. I am also grateful to Lyn Dupré for editing this paper.

Hal was also the second developer hired for the PGP Corporation, after Phil Zimmerman, and he is quoted that he loved the technology as it **protected the rights of individuals to privacy**. He remained there until his retirement in 2011.



Bio

Born May 4, 1956. BS Engineering 1979, California Institute of Technology. Married, two children.

Cryptography

Much of my free time and effort these days are devoted to my activities in cryptography. In the past, I have participated actively on the Cypherpunks mailing list. [Cypherpunks Archives](#) seem to go down suspiciously often; too much "burn before reading" stuff there, I guess.

PGP

I was one of the original programmers on PGP version 2.0, working directly with Philip Zimmermann, author of the program.

Today, I work for [Network Associates](#), developing the crypto library for the commercial version of PGP.

Crypto Related Links

Zero Knowledge Systems is a startup which is attempting to commercialize many cypherpunk related technologies. I wish them good luck!



ZKS can be accessed through the button above.

An excellent crypto link farm is operated by [Peter Gutmann](#) of New Zealand.

Hal was completely enchanted by the magic of cryptography and his Web page announced:

Much of my free time and effort these days are **devoted to my activities in cryptography**. In the past, I have participated actively on the Cypherpunks mailing list. [Cypherpunks Archives](#) seem to go down suspiciously often; too much "burn before reading" stuff there, I guess.

and for PGP:

I was one of the original programmers on PGP version 2.0, working directly with Philip Zimmermann, author of the program. Today, I work for [Network Associates](#), developing the crypto library for the commercial version of PGP.

Hal ended up, too, on the RFC which outlined the OpenPGP message format:

Network Working Group
Request for Comments: 2440
Category: Standards Track

J. Callas
Network Associates
L. Donnerhacke
IN-Root-CA Individual Network e.V.
H. Finney
Network Associates
R. Thayer
EIS Corporation
November 1998

OpenPGP Message Format


Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

His key contributions were often his posting to the cypherpunks listserv, and was involved in a range of cryptographic activism, such as running a contest to break the export-grade encryption that Netscape used for SSL. He successfully broke SSL, and showcased the major weaknesses of the technology.

[About CH](#)[Search CH](#)[Feedback](#)

Established 1995 - most extensive archive of discussions on crypto, tech & civil liberty



Thread Index for the current week

[\[Date Index\]](#) [\[Author Index\]](#) [\[Subject Index\]](#)

Current week

Year 2000

- 2000.08.07 - 2000.08.13
- 2000.07.31 - 2000.08.06
- 2000.07.24 - 2000.07.30
- 2000.07.17 - 2000.07.23
- 2000.07.10 - 2000.07.16
- 2000.07.03 - 2000.07.09
- 2000.06.26 - 2000.07.02
- 2000.06.19 - 2000.06.25
- 2000.06.12 - 2000.06.18
- 2000.06.05 - 2000.06.11
- 2000.05.29 - 2000.06.04
- 2000.05.22 - 2000.05.28
- 2000.05.15 - 2000.05.21
- 2000.05.08 - 2000.05.14
- 2000.05.01 - 2000.05.07
- 2000.04.24 - 2000.04.30
- 2000.04.17 - 2000.04.23
- 2000.04.10 - 2000.04.16
- 2000.04.03 - 2000.04.09
- 2000.03.27 - 2000.04.02
- 2000.03.20 - 2000.03.26
- 2000.03.13 - 2000.03.19
- 2000.03.06 - 2000.03.12
- 2000.02.28 - 2000.03.05
- 2000.02.21 - 2000.02.27
- 2000.02.14 - 2000.02.20
- 2000.02.07 - 2000.02.13
- 2000.01.31 - 2000.02.06
- 2000.01.24 - 2000.01.30

- [Re: FBI gets new hacking tools - any ideas?](#), *Kerry L. Bonin*
 - <Possible follow-up(s)>
 - [Re: FBI gets new hacking tools - any ideas?](#), *Tim May*
 - [Re: FBI gets new hacking tools - any ideas?](#), *lcs Mixmaster Remailer*
 - [Re: FBI gets new hacking tools - any ideas?](#), *Kerry L. Bonin*
 - [CDR: Child Porn == Thoughtcrime](#), *Tim May*
 - [CDR: Re: Child Porn == Thoughtcrime](#), *Tom Vogt*
 - [CDR: Re: Child Porn == Thoughtcrime](#), *Joe Baptista*
- [CDR: new thoughts on mp3 \(fwd\)](#), *Jim Choate*
- [CDR: Re: FBI gets new hacking tools - any ideas?](#), *Anonymous*
 - <Possible follow-up(s)>
 - [CDR: Re: FBI gets new hacking tools - any ideas?](#), *Kerry L. Bonin*
 - [CDR: Re: FBI gets new hacking tools - any ideas?](#), *Kerry L. Bonin*
 - [CDR: Re: FBI gets new hacking tools - any ideas?](#), *Tim May*
 - [CDR: Re: FBI gets new hacking tools - any ideas?](#), *Tom Vogt*
 - [CDR: Re: FBI gets new hacking tools - any ideas?](#), *Tom Vogt*
 - [CDR: Re: FBI gets new hacking tools - any ideas?](#), *David Honig*

His work on bitcoins came in 2004, and he produced the first proof-of-concept for bitcoins, and we continued to work on it until his death in 2014. His illness — Amyotrophic Lateral Sclerosis (ALS)- was announced in 2009, and, by 2013, he was essentially paralyzed, but he continued to program and push forward cryptography. His death arrived on 28 August 2014, and he was cryo-preserved by the Alcor Life Extension Foundation.

His crypto challenge to break SSL was published in August 1995, where he posted a sample of capture, and within a short time, the 40-bit secret part of the key was found within 8 days (half the keyspace) using 120 workstations at INRIA, Ecole Polytechnique. The solution was posted [here](#).

The godfather of Bitcoin?

On 3 January 2009 at 6:15pm, something amazing was born, and Hal played a key part in the testing of the newly created infrastructure:

Summary	Hashes
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC
Hash	0000000013d689c025ae165831e354f763ae462a8c17231b0a3d9cc28f
Previous Block	00
Next Block(s)	00000000839a8e686ab5551d76411475428af09047ac320161b2f18c6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f6181776673c2cc77ab2127b7afdeda33b

Transactions

4a5e1e4baab89f3a32518a88c31bc87f6181776673c2cc77ab2127b7afdeda33b		(Size: 204 bytes) 2009-01-03 18:15:05
No Inputs (Newly Generated Coins)	➡ 1A1zP1eP5QGefi... (Genesis of Bitcoin) - (Unspent)	50 BTC
		50 BTC

The emails from Satoshi to Hal are now a key part of the history of Bitcoins:

----- Forwarded message -----

From: **Satoshi Nakamoto** <satoshi@vistomail.com>

Date: Sat, Jan 10, 2009 at 11:52 AM

Subject: RE:Crash in bitcoin 0.1.0

To: hal.finney@gmail.com

Normally I would keep the symbols in, but they increased the size of the EXE from 6.5MB to 50MB so I just couldn't justify not stripping them. I guess I made the wrong decision, at least for this early version. I'm kind of surprised there was a crash, I've tested heavily and haven't had an outright exception for a while. Come to think of it, there isn't even an exception print at the end of debug.log. I've been testing on XP SP2, maybe SP3 is something.

I've attached bitcoin.exe with symbols. (gcc symbols for gdb, if you're using MSVC I can send you an MSVC build with symbols)

Thanks for your help!

>Hi Satoshi - I tried running bitcoin.exe from the 0.1.0 package, and
>it crashed. I am running on an up to date version of XP, SP3. The
>debug.log output is attached. There was also a file db.log but it was
>empty.

>

>The crash allowed me to start up a debugger, but there were no
>symbols. The exception was at address 00930AF7. The displayed call
>stack was 942316 called by 508936.

>

>When I have a chance, I'll try building it, although it looks like it

and who would believe it, but the initial code was developed on a Microsoft Windows platform with references to MSVC60.DLL:

----- Forwarded message -----

From: **Satoshi Nakamoto** <satoshi@vistomail.com>

Date: Sat, Jan 10, 2009 at 7:11 PM

Subject: Re: Crash in bitcoin 0.1.0

To: hal.finney@gmail.com

OK, thanks. The one in bitcoin-0.1.1-exe-dbg.rar is the same build as in bitcoin-0.1.1.rar.

I forgot, when you build debug on MSVC, it uses the debug versions of the runtime DLLs, which aren't included with Windows distributions. Actually, MSVC 6.0's runtime (MSVC60.DLL) is the last version that shipped preinstalled on Windows, which is why the continued interest in that ancient version of the compiler. Later Visual C versions can't create a standalone EXE that doesn't require additional runtime packages installed.

I can't use MSVC 6.0 for the release because its optimization of the SHA-256 routines is too slow.

I've attached a copy of the debug runtime DLLs. (They're redistributable)

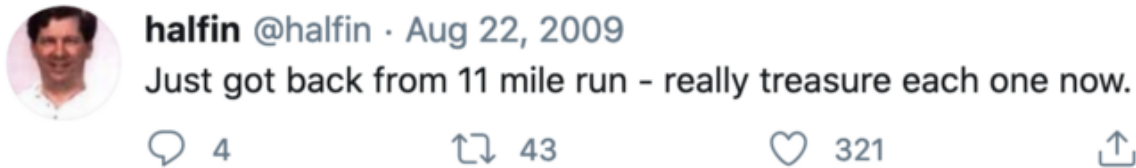
>Hi Satoshi - The version with the .pdb file did not run for me, I got
>an error about MSVCP60D.DLL not being found. I imagine this is due to
>the version incompatibility you were worried about.
>
>The next version, that deleted the questionable line of code and
>turned off optimization, seems to run fine for me. So the problem may
>be related to that bit.
>
>Hal

The emails show that Satoshi Nakamoto was the main developer, and Hal was basically the tester of the first version. Some think that Hal was Satoshi, but the email show otherwise.

Even so, others say that he faked the emails in order to cover his tracks. The mystery gets even stranger when you find out that a someone named Satoshi Nakamoto lived just two miles away from Hal (and who isn't the actual creator of Bitcoins). Did Hal just look up the phone book and pick Satoshi as the fake creator, where he was the real creator. At the time, those involved in creating Bitcoins were worried that they would be arrested for creating an infrastructure which was a threat to the US Dollar and hide their tracks.

His last few years

In August 2009, Hal was diagnosed with Amyotrophic Lateral Sclerosis (ALS), and a tweet perhaps highlighted this:



Unfortunately, he spent his last weeks before his death (August 2014) faced with an extortion attempt of 37.63289114 bitcoins (exactly \$20,000) from a hacker who used the names of “Nitrous,” “Savaged,” and “Clerk1337”, and who threatened to publish personal details on-line. The hacker outlined,

... there is nothing you can do to have me caught. I need to raise funds for my mother.

There were other attempts of extortion against Hal, including one for 1,000 bitcoins (\$400,000), on the posting of his family’s health data on-line.

Conclusion

Hal was a giant of the industry and was motivated by his love of his work, and on whose shoulders we all stand on. Over the past few weeks, I’ve enjoyed delving into his mind in the creation of the crypto methods, and his success is for all to see. So forget the cynics, the technology behind bitcoins is amazing, and it has flourished against the resistance of many.

Cryptography and machine learning are the future of cybersecurity, so go learn them now.

Please consider donating some of your cryptocurrency to help support the families of those affected by Amyotrophic Lateral Sclerosis (ALS):

<https://www.coindesk.com/community-honors-hal-finney-bitcoin-fund-als-research/>

Lightning is the Better Way to HODL

By Roy Sheinfeld

Posted August 31, 2020

Bitcoin is revolutionizing the monetary system by decentralizing and democratizing it. Lightning is revolutionizing bitcoin transactions by making them faster and cheaper (I'll never get tired of saying that) while preserving bitcoin's openness, resistance to censorship, immutability, and decentralization. We must be moving in the right direction.

But there seems to be a contradiction. On the one hand, Lightning is mobilizing, liquifying, actualizing bitcoin. With Lightning, you can actually live on bitcoin and use it for day-to-day purchases. In the USA. In Europe. Probably everywhere.

On the other hand, HODLing is at a three-year high. Eight million bitcoin are static, immobile, in storage. That's about 43% of the roughly 18.5 million bitcoin that have been mined so far. Nearly half of the world's supply of the greatest cryptocurrency in existence is not liquid. A currency needs a current. It needs to flow.



I haven't made it all the way through the Encyclopedia of Philosophical Sciences, but I'm pretty sure he was talking about HODLing on Lightning. Like 85% sure. ([Wikimedia](#))

Contradictions are crises of logic, and in every crisis lies opportunity. Hegel was the master in this particular discipline. He based his whole philosophy on the generative capacity that results when opposites meet. When Being encounters Nothing, the result is Becoming. "**Truth is found neither in the thesis nor the antithesis, but in an emergent synthesis which reconciles the two.**"

What if HODLing and Lightning can be reconciled? What if HODLers could store their bitcoin *on Lightning*? What if HODLing on Lightning is actually *better* for HODLers, better for bitcoin, and better

for Lightning? If we combine these two awesome things, what can they become?

HODLing and HODLers


HODLing refers to the strategy of “holding on for dear life” and not selling your bitcoin, no matter what the market does. In fact, it’s more than a strategy; it’s an expression of love. HODLers stick to their bitcoin whatever fate brings.

And the relationship is mutual. Bitcoin needs HODLers too. When the bitcoin price falls, HODLers are its parachutes and its trampoline. Bitcoin could have died in the crib if the first generation of HODLers hadn’t seen its potential and made a commitment to the currency we all love. With every subsequent price dip, bitcoin has faced the risk of evaporation. If everybody sold their bitcoin, it would simply become worthless and join the list of dead coins. HODLers are those few, those happy few, who have the fortitude to stand by their bitcoin, come what may.

Topic: I AM HODLING (Read 792127 times)

I AM HODLING

December 18, 2013, 10:03:03 AM

 Merited by goxed (50), Seccour (50), coblee (50), notsofast (50), naypalm (50), HabBear (50), allyouracid (20), jojo69 (20), botany (20), teeGUMES (12), Vod (10), 600watt (10), adroitful_one (10), Melnik (10), saugwurm (10), medsi2 (10), rusbitcoinuser (10), suchmoon (9), OgNasty (5), nutildah (5), ebliever (5), bitfish (5), SHBlizzard (4), vapourminer (3), mindrust (3), bones261 (2), Nemo1024 (2), marlboroza (2), krogthmanhattan (2), zoldberg (2), taserz (2), BobLawblaw (2), Elwar (1), Cyrus (1), Gyrsur (1), EFS (1), Timelord2067 (1), alani123 (1), layer1gfx (1), iluvbitcoins (1), LoyceV (1), Lesbian Cow (1), pugman (1), Limx Dev (1), TookDk (1), johhnyUA (1), Raja_MBZ (1), sunsilk (1), coolcoinz (1), ruletheworld (1), nullColner (1), escrow.ms (1), poptop (1), psycodad (1), apoorvathey (1), l8orre (1), styca (1), Goran_ (1), Halab (1), o_e_l_e_o (1), ivomm (1), Bardman (1), otrkid70 (1), dragonvslinux (1), soulyG (1), chimk (1), peonminer (1), crypto_curious (1), ambrosus (1), Xavier59 (1), escalicha (1), 7jaka7 (1), Financisto (1), wavug (1), seekoin (1), tim-bc (1), Whtwabbit (1), keyzersoze (1), hacidasi (1), kropot (1), GazetaBitcoin (1), Fitzy (1), IntroVert (1), Ivor Biggun (1), kha0S (1), gumshed (1), ThatRandomDude (1), jochemin (1), nelruk (1), alia (1), inkling (1) #1

I type d that tyitle twice because I knew it was wrong the first time. Still wrong. w/e. GF's out at a lesbian bar, BTC crashing WHY AM I HOLDING? I'LL TELL YOU WHY. It's because I'm a bad trader and I KNOW I'M A BAD TRADER. Yeah you good traders can spot the highs and the lows pit pat piffy wing wong wang just like that and make a millino bucks sure no problem bro. Likewise the weak hands are like OH NO IT'S GOING DOWN I'M GONNA SELL he he he and then they're like OH GOD MY ASSHOLE when the SMART traders who KNOW WHAT THE FUCK THEY'RE DOING buy back in but you know what? I'm not part of that group. When the traders buy back in I'm already part of the market capital so GUESS WHO YOU'RE CHEATING day traders NOT ME~! Those taunt threads saying "OHH YOU SHOULD HAVE SOLD" YEAH NO SHIT. NO SHIT I SHOULD HAVE SOLD. I SHOULD HAVE SOLD MOMENTS BEFORE EVERY SELL AND BOUGHT MOMENTS BEFORE EVERY BUY BUT YOU KNOW WHAT NOT EVERYBODY IS AS COOL AS YOU. You only sell in a bear market if you are a good day trader or an illusioned noob. The people inbetween hold. In a zero-sum game such as this, traders can only take your money if you sell.

so i've had some whiskey
actually on the bottle it's spelled whisky
w/e
sue me
(but only if it's payable in BTC)

Who's bold enough to draw the line between prophecy and madness? Not I. A thousand blessings be upon you, GameKyuubi.

Why HODLing needs an upgrade

Conventional wisdom says that the best way to HODL is cold storage in one of the many digital or graphite/cellulose (i.e. pencil & paper) solutions available. The rationale is that each connection to the network is an attack vector, but HODLers don't need the connectivity and exposure of a hot wallet, so they cut the cord. If you love something, lock it away from the world where nothing can touch or harm it. It's a thoroughly understandable impulse.

But as a wise fellow once said, "*A ship in harbor is safe, but that is not what ships are built for.*" An idle crew doesn't earn anything, and in time an idle ship's hull will rot. Similarly, HODLing by shielding bitcoin from the world is suboptimal for HODLers and detrimental for bitcoin.

Caught between gains and custody

In the fiat world, earning returns from your money virtually always entails lending it to someone else. Borrowers either remit a portion of their profits to investors in the form of a dividend, or they pay lenders rent in the form of interest for borrowing their money.

The advantage of lending capital is that it can do useful, productive, profitable things in the world as long as the owner doesn't actively need it. The major problem is that investors must sacrifice custody over their funds, which implies risk and trust.

The trustless and risk-free fiat financial plan is to store money in a sock under the mattress. Sadly, money in a sock does nobody any good. This strategy makes custody easy to determine, but that's it. Understandably wanting to retain custody over their funds, HODLers tend to put their bitcoin into a digital sock under the mattress. In doing so, however, they forego the funds' full potential to grow and they deny the world the productive potential of their capital.



Please don't tell me that you're going to take the fruit of the most powerful, dedicated computer network in history, and you're going to put it in a sock. (Image: Marco Verch)

A better way to HODL should provide HODLers with returns on their capital while preserving their custody over it.

Caught between the present and the future

Another way to think about this is that HODLers live in the future. Not only are they spending their fiat, which is currently fungible, on bitcoin, whose fungibility is still a work in progress, but they are also living in a future time when something like \$350 trillion in fiat will have been replaced by ~~about~~ exactly 21 million BTC. In a HODLer's vision, their modest bitcoin reserves will have appreciated about 16.7 million times over. I get it.

However, HODLing locks up capital. It takes wealth that people have already worked hard to generate and does ... nothing much with it. Meanwhile, the world could use that capital to research vaccines, build universities, and pump up its hash rate. HODLers are keeping the supply of bitcoin-based capital in the future, but the demand for the capital is in the present.

The word to describe something — a wine, an idea, a person, an asset — that displays future potential but whose current performance still disappoints is *immature*.

Maturity, of course, comes with experience. Just like new software or a new skill, assets need to be tested in the real world in order to determine what they're worth. Bitcoin needs to engage with the present world in order to realize its future potential. An apple seed may one day grow into a tree that will feed a family, but not unless it is planted. For bitcoin to have *real value*, it needs to engage with the *real world*.

HODLers' funds are no exception. They need a way to HODL that is secure, that preserves their custody, but that allows their capital realize its future value by engaging with the present world.



The future is often closer than you think, so stop dreaming and actualize it.
(Image: [Pikist](#))

The benefits of HODLing on Lightning

Before I get into the technical details of HODLing on Lightning, let's talk about the benefits. There's no point in learning about *how* to do it before you're convinced that it's worthwhile in the first place.

What's in it for bitcoin and the HODLers?

Anything that raises bitcoin's value is good for HODLers. Their interests are the same.

So what is bitcoin and what does it need? First, the uncontroversial: bitcoin converts energy into immutable and scarce cryptographic units (i.e. blocks) on a dynamic ledger. That has no inherent value. And given the difficulty in exchanging bitcoin for anything useful, its momentary value is strictly conventional. The price has swung between effectively nothing and nearly \$20 000 because that was the rough consensus of all market participants at the time. Nothing relevant changed about bitcoin between those values. Its value just swings like Michael Keaton's career.



Okay, bitcoin never starred in Mr. Mom. Fair point. (Image: [Alan Noah & James Brief](#))

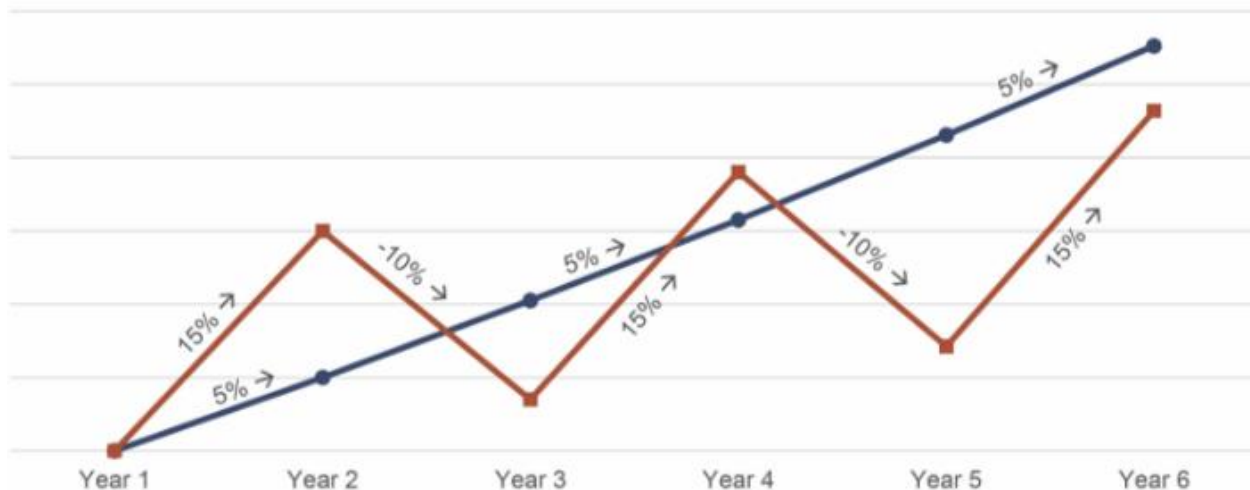
Now for the controversial: bitcoin is a currency. Many of us would argue that bitcoin is divisible, portable, durable, and limited in supply, which are the prerequisites for a currency. Others would argue more genetically than analytically, noting that Nakamoto originally called bitcoin "a peer-to-peer electronic *cash* system" right in the title.

Those who deny it is a currency also come in two camps. Some are sceptical of the bitcoin project entirely, but my time is too precious to argue with the chronically ignorant. Others resist thinking of bitcoin as a currency for instrumental reasons — it just doesn't fit their strategy. In other words, currencies are liquid and they flow, but these resistors have committed to HODLing, the whole point of which is *not* to move bitcoin.

Again, I understand HODLers' motives, and I sympathize. However, I suspect that their resistance to considering bitcoin a currency comes from a desire to defend HODLing and avoid the cognitive dissonance induced by never spending their currency.

But sheltering bitcoin from the real world is a self-defeating strategy. The more bitcoin is exchanged for sofas, legal services, and strawberry daiquiris, the wider the community of those agreeing on its value grows and the more their opinions about its value in diverse contexts will converge. Bitcoin's value will become more practical and less speculative; more actual and less potential.

Importantly, as I explain below, HODLers can achieve this *without* spending their bitcoin or losing custody over it. Lightning lets people use their bitcoin in different ways, so bitcoin can function as a currency, gain value, and lose volatility, and HODLers will *not have to spend* their bitcoin or relinquish custody. Functioning as a currency is good for bitcoin, and what's good for bitcoin is good for HODLers.



More growth with less volatility? Flatten all the curves!

What's in it for Lightning?

I've told you why HODLing on Lightning is good for HODLers. Do I also believe that onboarding HODLers would be good for Lightning? Of course I do. Here's why.

Crucially, funds on Lightning don't move unless users move them. Yes, users open payment channels to connect themselves with others, but the bitcoins in those payment channels ***do not enter joint custody***. They reside at one end or the other of the channel, completely under the control of one user at a time. Payment channels are a secure storage medium.

To reiterate: every bitcoin on Lightning is only owned by one user at a time, and they cannot move unless their owner actively transfers them. In that sense, *every Lightning user is already HODLing their balances until they spend a portion.*

You don't have to send or receive payments to be a part of the Lightning Network. It *is* possible to just HODL on Lightning. Not only is HODLing on Lightning possible, it's *already happening*.

Routing nodes are the best way to HODL on Lightning, and they are crucial to how Lightning functions. As Lightning transactions move through the network, they hop privately from node to node until they've found their destination. A routing node simply accepts a payment from a previous waypoint and forwards the payment — minus a modest routing fee — to the next waypoint on the route.

Every step is backed by various layers of encryption pertaining to the route itself, the sender and the receiver, the private keys, etc. Lightning is 100% real bitcoin.

If Lightning were a network of roads, routing nodes would be its roundabouts. Without wanting to push the analogy too far, the incoming and outgoing connections — the nodes' payment channels — are the roads feeding into and out of the roundabouts. Routing nodes/roundabouts increase the efficiency of the network by increasing the number and probably decreasing the length of possible routes between any two points.

The funds stored in a routing node's payment channels are analogous to the lanes going around the roundabout. As above, more is better. And as more funds are stored on a node, it will be able to handle more and larger transactions.

However, a network that relies on just a few massive nodes will be vulnerable to all kinds of problems. Anyone who's driven around the Place de Charles de Gaulle in Paris or the magic roundabout in Swindon knows that centralizing traffic around a massive, central point makes life difficult for those in transit. Many smaller roundabouts, on the other hand, make travel faster and more efficient — just like a decentralized network with many routing nodes.



Centralization — what fun! (Image: [GoMetro](#))

In short, routing nodes increase the network's connectivity and liquidity while decreasing its centralization.

Forwarding funds through routing nodes is also a service, which generates fees — just like tolls in a road network. At the moment, those fees are modest, and the volumes are still growing. Their growth, however, depends on the penetration and utility of the Lightning Network. As HODLers help to build Lightning with routing nodes, Lightning will help to build their bitcoin reserves with routing fees.

By running routing nodes, HODLers can increase Lightning's capacity, increase bitcoin's fungibility, grow their investments, and give the world the benefits of access to their capital without ever losing custody over it. Lightning gives HODLers returns *and* custody, utility in the present *and* value in the future.

This is the awesome synthesis I was talking about.



How to set up a routing node and become the best HODLer you can be

Okay, so HODLing on Lightning means setting up a routing node. It's more technically demanding than installing Breez, but even enthusiastic n00bs could probably tackle it. There are also three different paths to get started, depending on the time and budget available:

1. The first method is to set up a Lightning node on a device at home. The benefits are low cost and full control. The hardware requirements are relatively modest, and the required software is free and open-source. The disadvantages are the technical difficulty, inevitable maintenance, and the drain on resources. This method requires you to configure the software yourself and poke around in the code a bit. It will also take around 250 GB and processing power. And a few more steps than what are listed in those instructions will be required to move your bitcoin onto your node and open payment channels.
2. Buy pre-configured hardware. There are several hardware products that deliver a functioning Bitcoin node with either LND or c-lightning pre-installed. The advantage of these products is that someone else has already configured the software and intends to update it, and they won't sap the resources of your other machine(s). The disadvantage is the cost. You're looking at a few hundred dollars across the board, though many can be constructed on a DIY basis at less cost and more difficulty.

3. There is also a cloud-based node solution, which was introduced just a couple of months ago. They claim to provide non-custodial, fully functional, low-configuration Lightning nodes hosted on their servers, but with full user control. The advantage: that all *sounds* pretty good. The disadvantage: the service is not yet live, so it's too early to comment on their reliability, security, cost, etc. But it's definitely worth watching.

Ready to go full LSP?

At Breez, we've introduced the concept of LSPs, which are basically just routing nodes that actively and intentionally connect end users to the network. Whereas a routing node is a more passive operation, an LSP requires more active management. Attracting users generates more returns, but it also requires publicity, responding to user queries, and so on.

LSPs also require more capital. One bitcoin on a routing node is probably enough to make a meaningful contribution to the network and become a HODLer ~~of the future~~ of the present. A viable LSP requires ... well ... more. How much depends on the services provided, the user base, and other factors.

However, the network needs LSPs, and the Lightning economy certainly does, so it's a worthwhile pursuit. We're proving that it can be done, and we'd be happy to help others get started. Just ask.

HODL for you, HODL for bitcoin, HODL for (and on!) Lightning

Lightning lets HODLers grow their capital without losing custody. They get to help the world adopt bitcoin while getting richer in the process. Bitcoin becomes real money in the present, and its future growth becomes more stable and more certain.

There is no contradiction between Lightning and HODLing. Combining them improves each. Thanks Hegel!

Before closing, we have to mention a couple of potential snags. First, getting set up costs some money. Every potential return requires an initial investment. Second, bitcoin stored in Lightning channels is as safe as the system running the client or node, but it cannot be as secure as an air-gapped, cold-storage device. Lightning channels are effectively "hot wallets," and a routing node must be online with multiple connections to the network in order to function. These are attack vectors. HODLing bitcoin as capital on Lightning allows it to grow and strengthen the currency while preserving custody, but it *will* have contact with the wider world.

And attentive readers might have noticed that we never refer to bitcoin as "locked" in a payment channel. Instead, we say "stored," which implies less

constraint and more liquidity. We'd like to thank Andreas Antonopoulos and Francesco Calderón for the mind-expanding reformulation:



I'll drink to that. Cheers. 🍷

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](#)