Introduction by Kevin Gao (Work in Progress)

Contents:

The Core

Bitcoin becomes the Flag of Technology (https://nakamoto.com/)
January 3, 2020

by Balaji S. Srinivasan

Bitcoin: A Peer-to-Peer Electronic Cash System
October 31, 2008

by Satoshi Nakamoto

Bitcoin for the Open-Minded Skeptic (https://www.paradigm.xyz/)
May 12, 2020

by Matt Huang

User Thoughts

Why Bitcoin (http://www.brianrast.com/)
September 9, 2019

by Brian Rast

How the Bitcoin protocol actually works (http://michaelnielsen.org/)
December 6, 2013

by Michael Nielsen

The case for a small allocation to Bitcoin (https://www.kanaandkatana.com/)
March 1, 2019

by Wences Casares, CEO of Xapo

If you think I'm missing any major essays/papers, shoot me an email at kevin@12mv2.com or a dm on Twitter @kgao1412 with the subject: "Bitcoin Compilation." Thanks!

Investor Theses

Why Bitcoin Matters (https://a16z.com/)
January 22, 2014

by Marc Andreessen

The Great Monetary Inflation
May 7, 2020

by Paul Tudor Jones and Lorenzo Giorgianni

An (Institutional) Investor's Take on Cryptoassets
December 24, 2017

by John Pfeffer

General Talks

BlockCon 2018: Nassim Taleb & Naval Ravikant (h/t http://www.mrsideproject.com/)
October 11, 2018

Nassim Nicholas Taleb and Naval Ravikant

Capitalizing on Tech-Enabled Transformations (Excerpt)
July 20, 2018

Josh Wolfe and Michael Green

If you think I'm missing any major essays/papers, shoot me an email at kevin@12mv2.com or a dm on Twitter @kgao1412 with the subject: "Bitcoin Compilation." Thanks!

The Core

Bitcoin becomes the Flag of Technology (https://nakamoto.com/)
January 3, 2020

by Balaji S. Srinivasan

Bitcoin: A Peer-to-Peer Electronic Cash System
October 31, 2008

by Satoshi Nakamoto

Bitcoin for the Open-Minded Skeptic (https://www.paradigm.xyz/)
May 12, 2020

by Matt Huang

If you think I'm missing any major essays/papers, shoot me an email at kevin@12mv2.com or a dm on Twitter @kgao1412 with the subject: "Bitcoin Compilation." Thanks!

Bitcoin becomes the Flag of Technology (First published at https://nakamoto.com/)
January 3, 2020

by Balaji S. Srinivasan

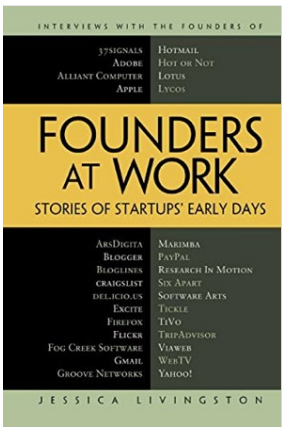
Bitcoin represents the explicit encoding of previously implicit values of the tech community. It's not just software — it is a Schelling point and a symbol. As such, it will become widely recognized as the flag of technology over the course of the 2020s.

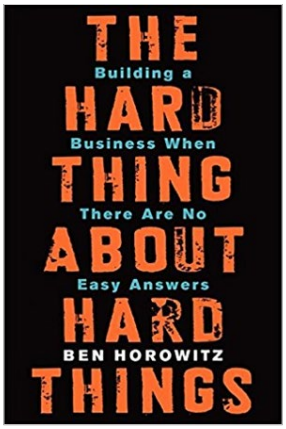
To understand this claim, we need to define what "technology" is, what a "flag" would mean in this context, and why Bitcoin would be chosen as that flag. Let's proceed in turn.

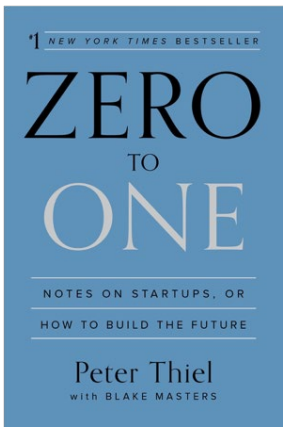
Technology: the values behind the valuations

Technology is the culture that Silicon Valley built and exported. It is the global community of founders, investors, engineers, and designers. And it is the code, apps, products, and billion dollar companies. But most fundamentally, it's the values that underpin the valuations.

These values are implicit in common terms like MVP, product-market fit, or the idea maze. And they are expressed in writing via popular books by the most accomplished people in tech.







But they usually aren't articulated outright. If we were to enumerate them, we'd find that technology is internationalist, capitalist, decentralized, hyperdeflationary, networked, encrypted, digital, volatile, ambitious, and *quietly* revolutionary. These are the values of technology.

Bitcoin (and crypto more generally) moves us beyond the implicit by expressing these values in a piece of code that doubles as an investment vehicle. The code speaks to the developers, the upside appeals to the investors, and the values encoded within speak to both. If you believe in these values, you tend to buy Bitcoin.

Bitcoin: an ideological flag and a Schelling point

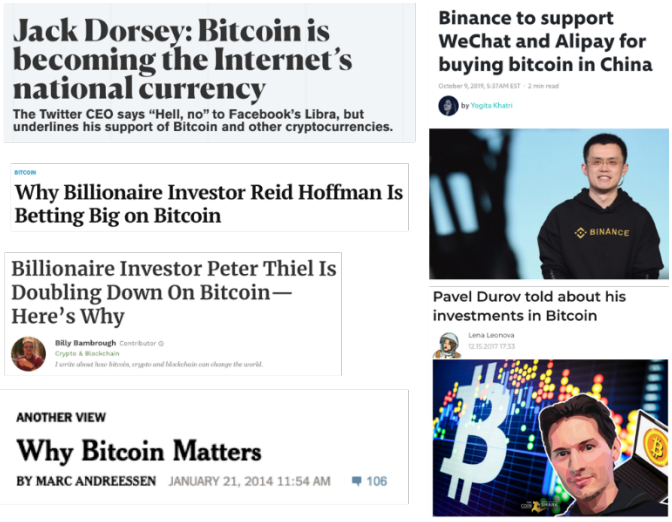
Recall that not every flag represents a geographical entity. Some of them represent movements, like the Gadsen flag or the rainbow flag. Bitcoin becomes a flag in this sense, as the encoding of technology's aforementioned values. An ideological flag, rather than a geographic one.

Bitcoin also becomes a flag in another sense: a rallying point, a Schelling point for an entrepreneurial community.

Recall that a Schelling point occurs when a community coordinates *without* explicit coordination. The classic example is when two strangers know that they must meet in New York City on a given day, but are not told where or when. They need to guess what the other person will do without communicating with them. The equilibrium solution to this is usually "meet at 12 noon in front of the Grand Central Terminal information booth."

Similarly, if we asked the question of what two random people in the *global* tech community would coordinate on, we start to find that American, Chinese, and Russian technologists who otherwise don't agree on much tend to agree that Bitcoin is valuable.

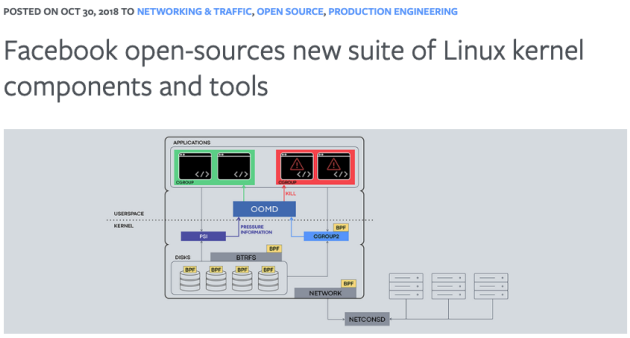
For example, Jack Dorsey runs Twitter, Reid Hoffman founded LinkedIn, and Marc Andreessen and Peter Thiel are on the board of Facebook – but all of them are pro-Bitcoin. Similarly, Binance founder Changpeng Zhao and Telegram founder Pavel Durov are Chinese-Canadian and Russian expatriates respectively, and are also pro-Bitcoin. Different countries, different backgrounds, but a shared belief in digital currency.



It's hard to get folks like this to all agree on something. If you think about it, the global tech community is not going to line up behind Google, or Facebook, or WeChat, or Yandex. Even if a founder respects the products these companies built, as a capitalist they are always aware that there may be economic disalignment at some point in the future. What is good for Google may not always be good for you.

What technologists do tend to align around are (a) open source projects where alignment is less material and (b) investments where alignment is quantifiable. Bitcoin is both of these.

With respect to open source, the closest analogy to Bitcoin may be Linux. Like Linux, all can profit from Bitcoin but none can corrupt it. For example, Google and Facebook are tough competitors – but they cooperate on Linux because it's a demilitarized zone where one party cannot deprive the other of their contributions. Microsoft may have its own OS, but even Microsoft has to respect Linux nowadays.



Similarly, within the crypto community as well – which is overlapping with but not identical to the tech community – whatever project someone is starting, they are aware of Bitcoin, respect it, and likely hold some. Whatever exchange someone is running, they will have Bitcoin support. Whatever crypto tutorial someone is writing, they will assume the user knows something about Bitcoin.

Bitcoin is thus many people's first choice and many people's second choice. This means it will become the community's first choice. That's why Bitcoin is also a flag in the sense of a Schelling Point – something to rally around.

Bitcoin encodes the values of Technology

But when the global tech community rallies around the flag of Bitcoin, what exactly is it getting behind?

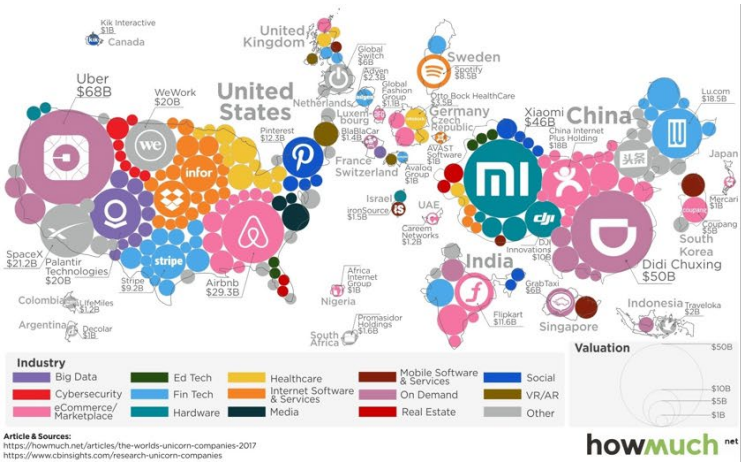
As noted above, we argue that Bitcoin encodes the following implicit values of technology: internationalist, capitalist, decentralized, hyperdeflationary, networked, encrypted, digital, volatile, ambitious, and *quietly* revolutionary. Let's go through each of these in turn.

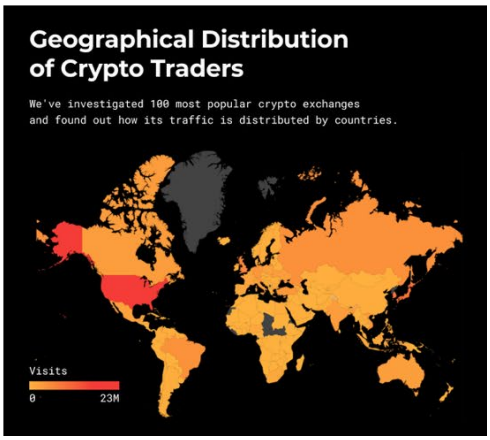
Internationalist

Bitcoin and technology are both intrinsically internationalist.

The tech industry may have begun in Silicon Valley, but it's a global phenomenon at this point. Within the US, more than 60% of the most valuable technology companies were founded by first and second generation immigrants. And with 51% of unicorns now outside the US, tech extends far beyond Silicon Valley to every country with an internet connection.

The same is true for Bitcoin. Millions of crypto traders are distributed across the world, there are thousands of Bitcoin meetups happening in hundreds of cities, and every major nation state is aware of cryptocurrency.





Capitalist

Bitcoin and technology are both fundamentally capitalist.

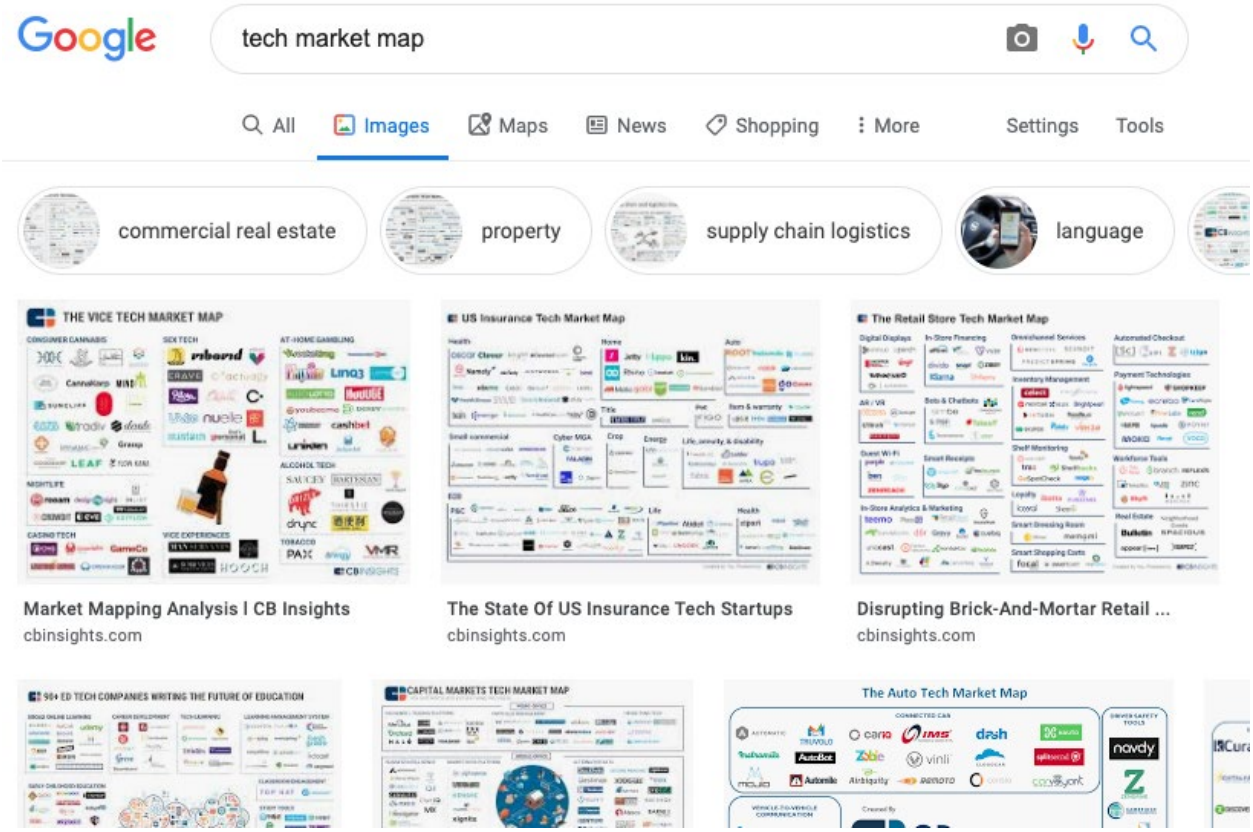
The tech industry proper revolves around entrepreneurs, angel investors, venture capitalists, M&As, and IPOs. The broader tech community also includes academic engineers and the open source community, neither of which are for-profit, but both of which are far more capitalism-friendly than their counterparts in academic humanities departments and traditional nonprofits.

Bitcoin likewise is about capitalism. It is a ledger of transactions. It is a speculative investment. It is the digitization of money. It is a transnational form of property rights. It's delivered venture returns. And it encodes the history of an entire economy in its blockchain. As such it's intrinsically capitalist.

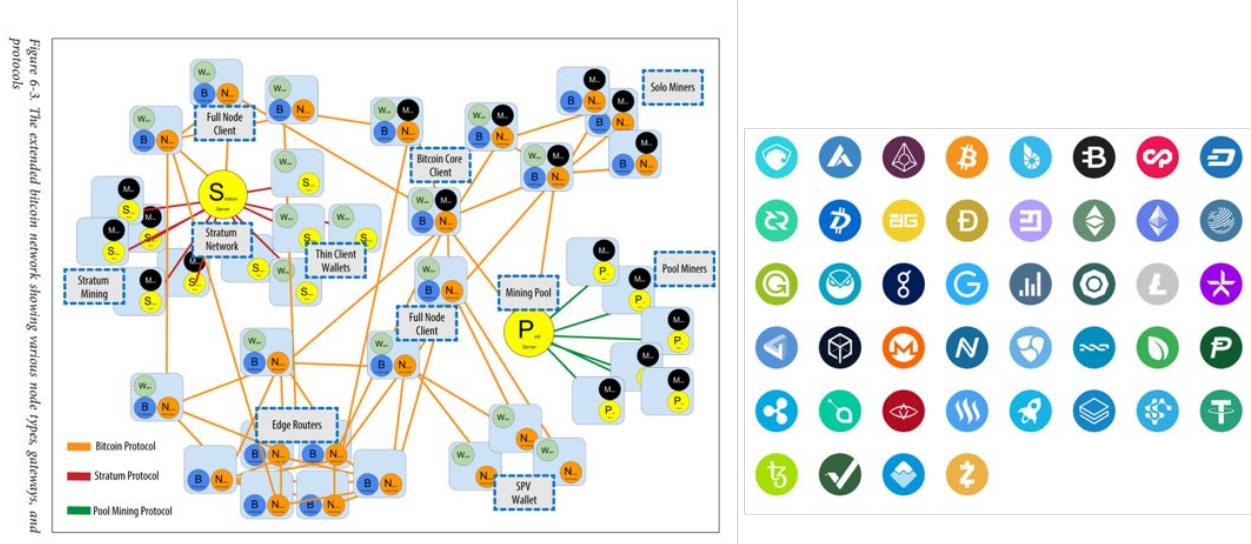
Decentralized

Bitcoin and technology are both highly decentralized.

As Benedict Evans noted recently, the great thing about tech monopolies is how many there are to choose from! Any market map of a tech sector will show the same thing: a profusion of dozens or hundreds of companies in any industry, all vying for different pieces of the market. There are hundreds of millions of websites, almost five million startups on AngelList, thousands of angel investors, and hundreds of large VC firms. There is no single chokepoint in tech, no one financier or platform that you *must* deploy on to succeed.



The same is true for Bitcoin, and crypto more generally. Satoshi famously designed Bitcoin such that no single miner could censor transactions on the network, and called it "completely decentralized with no server or central authority". While there's always more to be done in terms of quantifying and improving decentralization, the ecosystem has miners, nodes, exchanges, developers, and investors, each of whom have competing interests, and (ideally) none of whom has a veto over Bitcoin.



Left: Mastering Bitcoin's diagram of the extended bitcoin network. Right: a random sample of coins.

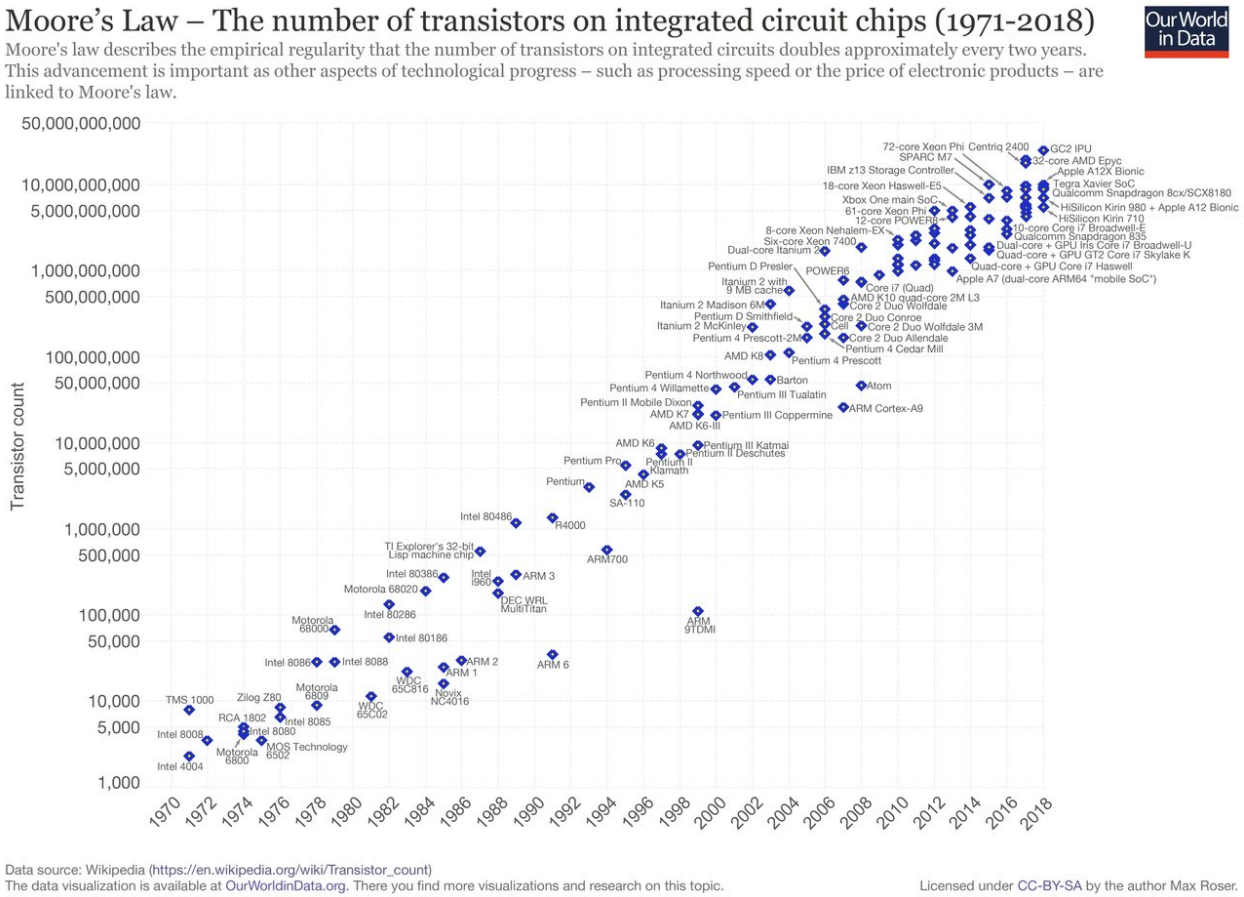
Finally, there's one more level of decentralization: decentralization across coins. There are now enough different approaches to consensus and privacy that it's highly unlikely that cryptocurrency as a phenomenon will ever vanish. The vulnerabilities for proof-of-work are not the same as those for proof-of-stake, delegated proof-of-stake, proof-of-space, and so on. It's unlikely that any single issue can now take out *all* coins and *all* exchanges simultaneously. At least some will survive.

Thus in an absolute worst case scenario of a global crackdown on cryptocurrencies where Bitcoin itself is found to suffer from an unfixable vulnerability, we can expect a partial migration to surviving coins as well as an *import* of the Bitcoin ledger into one of the surviving chains. The reason is that Bitcoin ledger is so highly replicated, and has so many stakeholders behind it, that it is practically impossible to erase from the earth. It will be snapshotted and restored over and over again – even if the original network is shut down.

Hyperdeflationary

Bitcoin and technology are both agents of hyperdeflation.

The single most important graph in technology is arguably Moore's law. That's a story of hyperdeflation: if the number of transistors on an integrated circuit doubles every two years, the cost of computing roughly halves over the same period. In other words, the same dollar will buy more compute power tomorrow than today, even taking inflation into account.



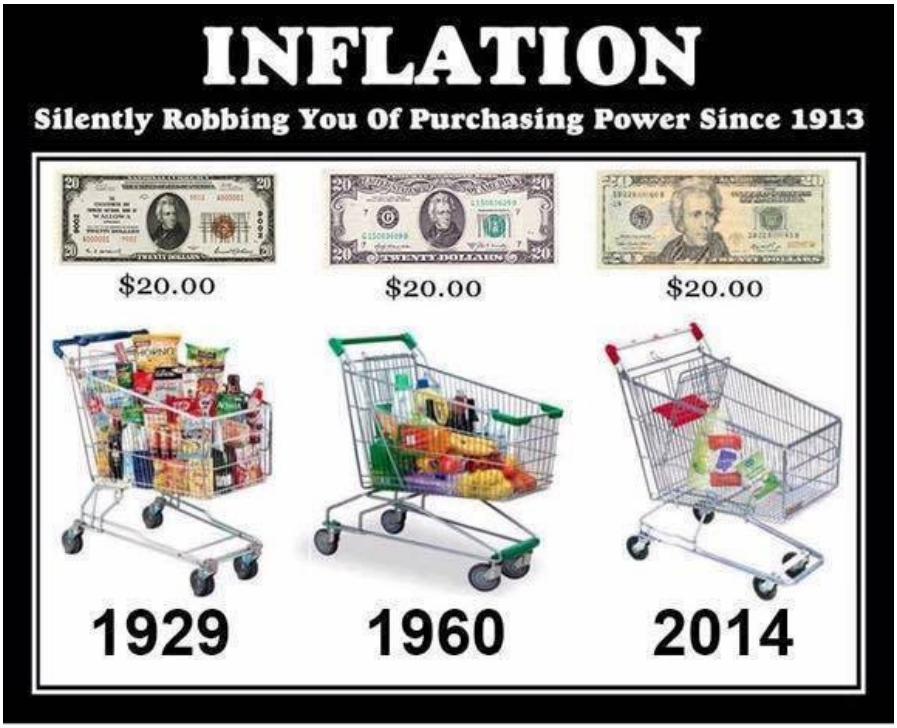
Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

And it's not just compute power. The areas that technology has disrupted have seen plummeting prices. We can see this visually, if we compare the number of different pieces of hardware replaced by a single

iPhone. We can see this quantitatively, if we compare the cost of browsing Wikipedia or Spotify to the equivalent in physical encyclopedias or compact disks. And we can see this visually if we compare the long-term trajectory of costs in the sectors technology has touched (televisions, software, phones) to those it has not yet disrupted (education, healthcare).

Bitcoin is also hyperdeflation incarnate. It's not just that BTC was the best investment of the 2010s, and increased by orders of magnitude in value relative to the USD over the last ten years – though it's always worth keeping this miraculous ten year chart in mind.

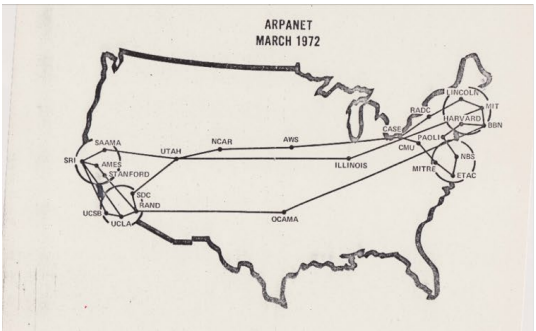
It's also that Bitcoin represents a form of hyperdeflation complementary to and different from Moore's law. If Moore's law was about creating value by reducing the cost of computation, Bitcoin is about capturing value by shielding it from inflationary pressure. Or as the meme goes:



Eventually, if Bitcoin truly achieves its destiny, we'll use BTC as a unit of account. That's called hyperbitcoinization.

Networked

Bitcoin and technology are both network-based.



To say that technology is based on the internet is obvious. To say that it is about social networks, loose collaborations, non-geographical associations, and routing algorithms is also obvious. But the long-term implication of this is that the geodesic distance between two points in a social network is becoming more important than the great circle distance between two points on the surface of the earth.

So too with Bitcoin, and cryptocurrency more generally. Perhaps only one in 100 people on the face of the Earth holds Bitcoin today, at most 50 million people. In the early days of Bitcoin it was far fewer.

But they were effectively all together in the same room thanks to the internet. It didn't matter how far apart they were geographically; they were all part of the same idea, linked through a computer network. They could partially opt out of their country's currency (based on geographical proximity to their neighbors) and partially opt in to this new world (based on ideological proximity to people of shared mind).

The freedom to associate with anyone, anywhere in the world based on ideas shared through a computer network is a core value implicitly shared by both technology and Bitcoin that is radically different from the premises of the Westphalian state.

Encrypted

Bitcoin and technology are both founded on encryption.

Crypto Wars

From Wikipedia, the free encyclopedia

The **Crypto Wars** is an unofficial name for the U.S. and allied governments' attempts to limit the public's and foreign nations' access to cryptography strong enough to resist decryption by national intelligence agencies (especially USA's NSA).[2]

The modern technology industry only exists because of encryption on the internet. Without SSH for encrypted connections there would be no cloud, no remote work, no deployments. Without SSL and HTTPS for encrypting credit card and wire information there would be no ecommerce, no payment companies, no ads, and no subscriptions. The fundamental engineering and payments infrastructure for creating wealth on the internet would not exist.

Similarly, Bitcoin only exists because of decades of work in theoretical and applied cryptography. Without concepts like public key cryptography, digital signatures, hashing, and hashcash or implementations like SHA-256, RIPEMD-160, and secp256k1, Bitcoin would not be feasible. The fundamental cryptographic constructions required to represent, transmit, and safeguard wealth through Nakamoto consensus would not be available.

Digital

Bitcoin and technology are both inherently digital.

This again is almost too obvious to point out, but over the last thirty years the technology industry has digitized books, magazines, movies, newspapers, photos, letters, advertisements, music, documents, radio, television, and every form of media. Tech has also digitized things we didn't even think of as "digital" in the 1980s, from your Fitbit steps to your preference settings within an app. And of course digitization unlocked the ability to copy a file, to share it, to edit it, to aggregate it, to do machine learning on it, and much more.

Bitcoin and cryptocurrency more generally are the next phase in digitization. While the technology industry had digitized everything that was not scarce, until Nakamoto consensus we did not have a native representation of *digital scarcity*. Workarounds like PayPal used a centralized database to simulate digital scarcity, but at base they relied upon a set of permissioned actors with root privileges to guarantee that scarcity. Bitcoin's blockchain changed all that.

Once people realized that Bitcoin's blockchain was a cryptographically secure way to represent a public database of who possessed digital currency, they quickly realized that similar approaches could be used to digitize stocks, bonds, commodities, derivatives, REITs, mortgages, loans, and every single kind of financial asset. Moreover, as with the first wave of tech-driven digitization, we will be able to compose

these building blocks of digital finance to create new applications. And we are also en route to digitizing identity, property rights, and eventually governance itself.

Volatile

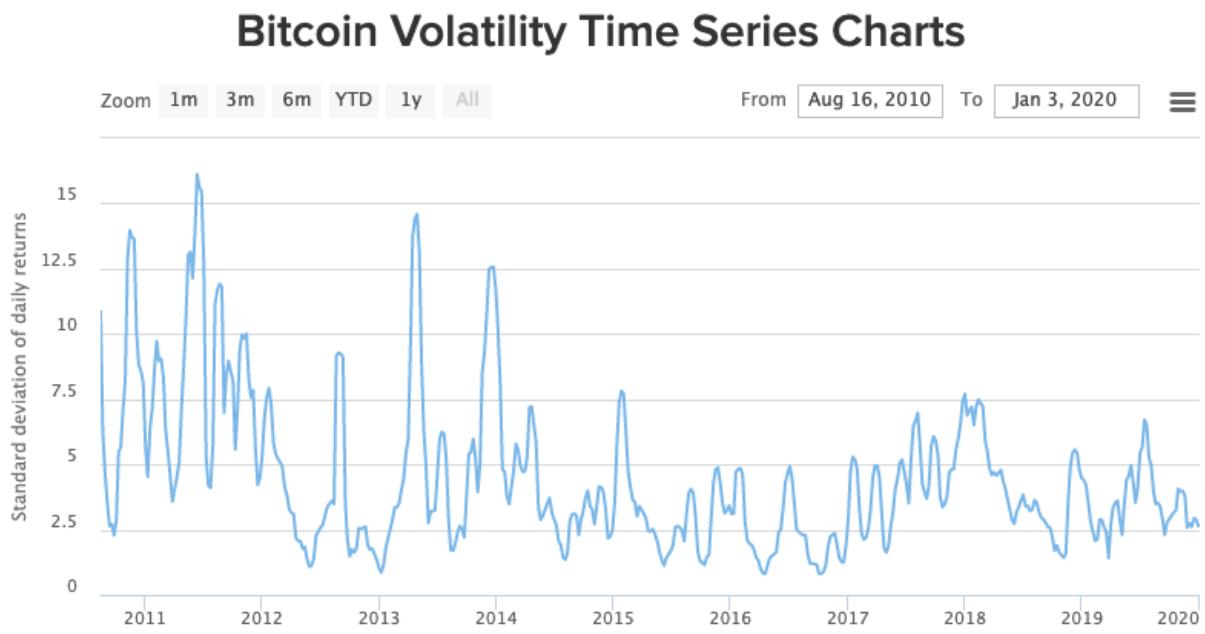
Bitcoin and technology are both highly volatile.

You only ever experience two emotions in a startup: euphoria and terror. And I find that lack of sleep enhances them both.

– Marc Andreessen

Startups are volatile. Many startups fail. Bankruptcies are common. Post-mortems are common. Failure is not welcomed, but it is budgeted for, accepted, and possible. VCs are all about the power law, where a single investment can succeed and pay for all the others. Persistent entrepreneurs can sometimes win big. And patient, long-term capital has a chance of winning 1000X returns.

The underlying reason for this is that variance increases with small sample sizes. When you only have ten employees, a single person quitting can tank the company. Conversely, if you only have ten customers and you bring in a large sale, that one event could boost the revenues of the company by 10%, attract a key investment, and lead to the long-term success of the venture.



Bitcoin is similarly volatile. The price graph alone shows multiple 80-90% drops over the past ten years. The number of failed Bitcoin startups is legion. And the number of new Bitcoin millionaires is as well. Bitcoin is, in many ways, the world's first publicly traded hypergrowth startup. And it is exposing millions of people to the vicissitudes of startup culture, the virtues of persistence and patience, and the downside of quitting too early and proclaiming premature death.

Ambitious

Bitcoin and technology are both breathtakingly but rationally ambitious.

The ambition of the tech entrepreneur is often mocked. But without the belief that one could build a spaceship, create an electric car, organize the world's information, or connect billions of people, we would simply not have the companies we have today. The strength of technology is *realistic* ambition, *rational* ambition, ambition based on calculated risks and quantified upsides.

Bitcoin's ambition was nothing less than the development of a new digital currency to rival the US dollar. Ten years later, it is clear that every central bank and financial institution in the world has heard of Bitcoin. Today, with the existence of multiple at-scale digital dollars, the very real possibility of China potentially rolling out a blockchain-based digital currency, and Bitcoin's #40 ranking on the fiat market cap charts, it's not crazy to say that Bitcoin has changed the world – and may well give the dollar a run for its money.

But it *was* crazy to think that Bitcoin could compete with the dollar in 2009. It was a piece of software posted on a mailing list! Yet in the very first exchange after Satoshi posted the whitepaper, it was clear that Hal Finney and Satoshi were wildly yet rationally ambitious. Hal calculated a scenario in which each BTC was worth $10M per coin:

As an amusing thought experiment, imagine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from $100 trillion to $300 trillion. With 20 million coins, that gives each coin a value of about $10 million.

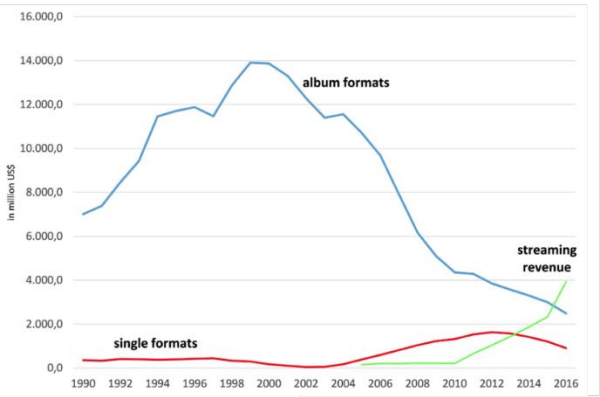
So the possibility of generating coins today with a few cents of compute time may be quite a good bet, with a payoff of something like 100 million to 1! Even if the odds of Bitcoin succeeding to this degree are slim, are they really 100 million to one against? Something to think about...

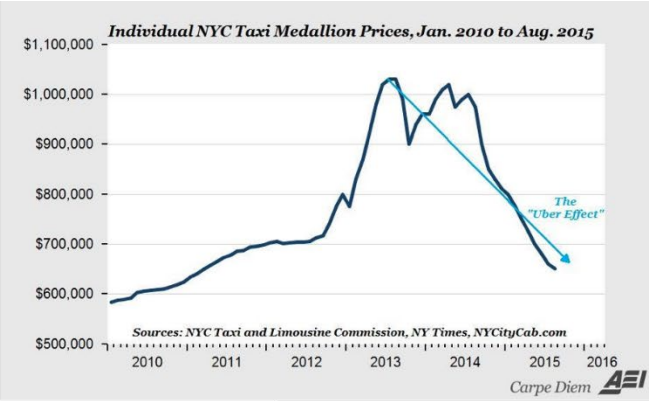
Given the *ad arguendo* supposition that Bitcoin would work at a technical level, he made a Fermi estimate of the valuation based on a set of logical premises. And once Bitcoin's technology did prove to work, and once enough others understood those premises, BTC got to $10,000 per coin in the first ten years. Of course, that's not yet $10M and a replacement for the US dollar – but as they say, the first billion is the hardest.

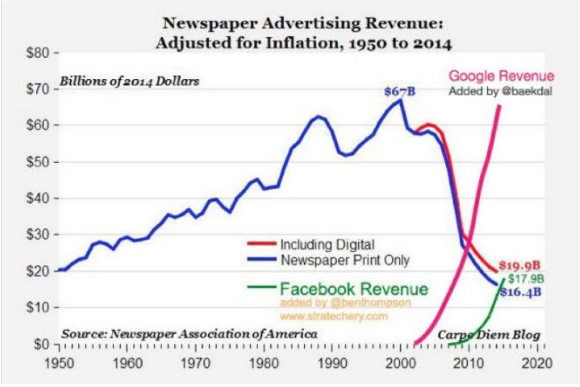
***Quietly* Revolutionary**

Last, but not least, Bitcoin and technology are both *quietly* revolutionary.

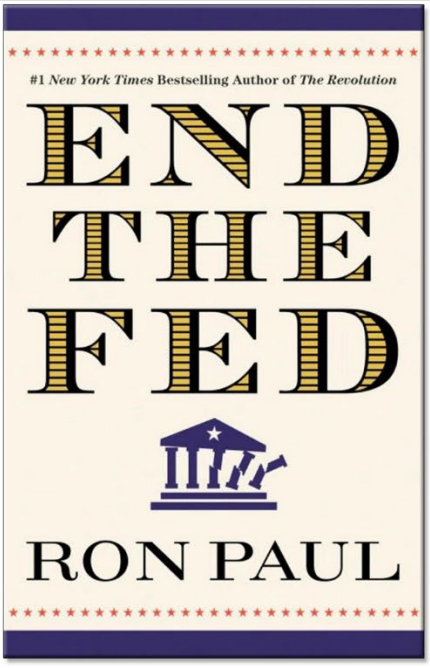
Technology did not disrupt the music industry, the taxi business, or the newspaper business through traditional political activism. It simply built better products that millions of people voluntarily chose to purchase or use of their own accord. And through these many quiet, individual, personal decisions enormous change was wrought, as these graphs demonstrate:







Similarly, Bitcoin is not about accomplishing change through folk activism. It's a network-based phenomenon which has accomplished a revolution in monetary policy through a billion private actions rather standing on the street corner spouting slogans. It is quietly revolutionary.



FINANCE

'We are about to see massive disruptions': IMF's Lagarde says it's time to get serious about digital currency

PUBLISHED FRI, OCT 13 2017·12:49 AM EDT | UPDATED FRI, OCT 13 2017·7:21 AM EDT

China passes cryptography laws, laying framework for a national digital currency

By Bang Xiao and Tasha Wibawa

Updated about 11 hours ago

What comes next?

We've explained how Bitcoin (and crypto more broadly) encodes the implicit values of technology. It is internationalist, capitalist, decentralized, hyperdeflationary, networked, encrypted, digital, volatile, ambitious, and *quietly* revolutionary.

I believe that over the 2020s, the technology industry will end up aligning behind Bitcoin and crypto as part of a broader international realignment. Cryptocurrency simultaneously reflects many fundamental American values (like freedom of speech, freedom of contract, freedom of association, protection against unreasonable search & seizure, the right to privacy, and so on) while *also* demonstrating broad international appeal to millions of people around world.

This realignment would not be traditional right vs left, but rather land vs cloud, state vs network, centralized vs decentralized, new money vs old money, internationalist/capitalist vs nationalist/socialist, MMT vs BTC, and (perhaps most symbolically) Hamilton vs Satoshi. The new American center may be decentralized.

But that is a story for another time. Until then, I leave you with this.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

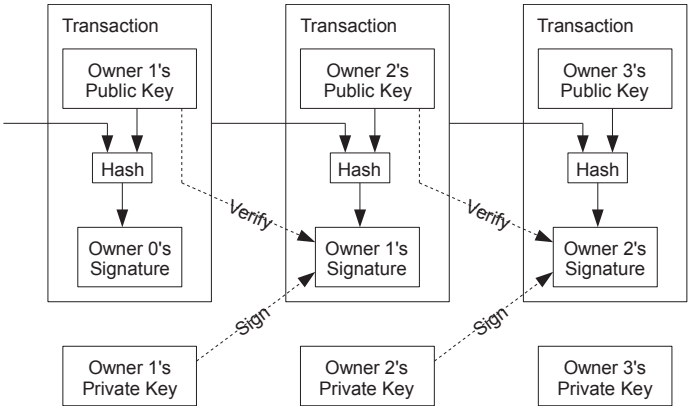
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

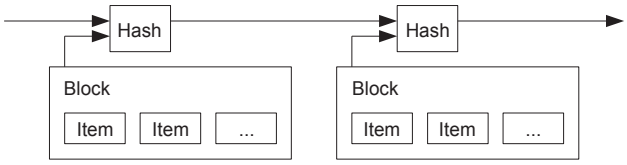


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

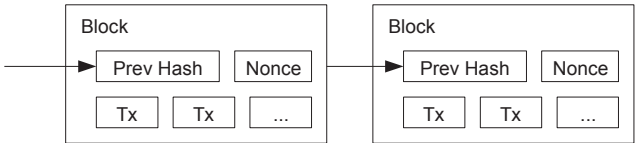
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

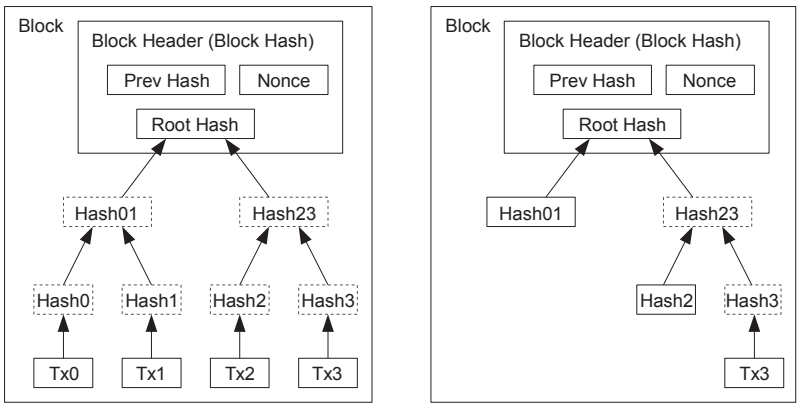
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

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

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



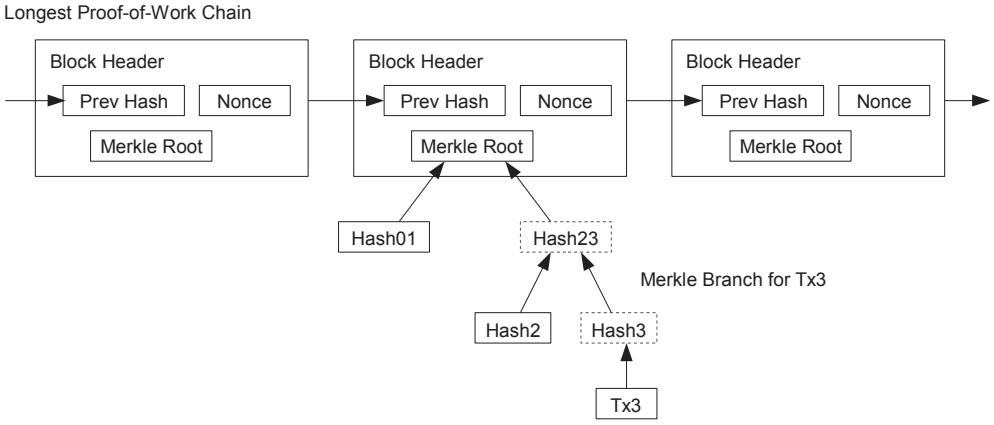
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

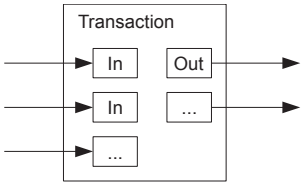
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

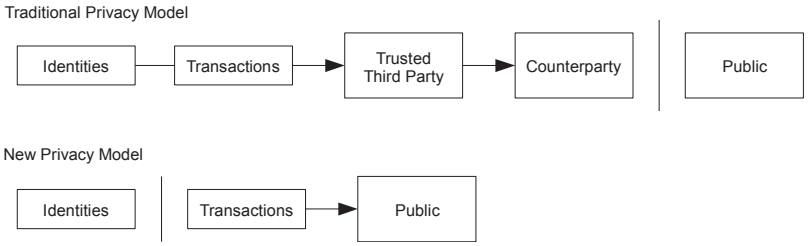
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Paradigm

Bitcoin for the Open-Minded Skeptic

By Matt Huang, on behalf of Paradigm (May 2020)

Bitcoin has grown from idea (2008), to working system (2009), to its first real-world use at <$0.01 per coin (2010), to a global currency valued at $8K+ per coin and $150B+ in aggregate (May 2020).

Although Bitcoin is empirically one of the best investments of the past decade, it still remains controversial. Is it a new form of money? A speculative bubble? Or a bit of both?

Investors have well-established frameworks for evaluating assets like equities, credit, and real estate. But a new *monetary asset* such as Bitcoin appears so infrequently that no clear framework exists.

This paper outlines a simple and intuitive framework for Bitcoin as a new monetary asset.

Why Now?

In the course of our work, we are often in the position of explaining Bitcoin to investors and institutions approaching it for the first time. Never before have we seen more interest in Bitcoin and its potential as a digital companion to gold.

Financial crises stress the limits of existing systems and can highlight the need for new ones. This was true during the financial crisis of 2008 (out of which Bitcoin was born), and it is perhaps more true today with the unprecedented levels of monetary and fiscal stimulus being pursued by governments worldwide.

There has been no shortage of writing about Bitcoin over the past 11 years. This paper does not claim any novel insight. Instead, it is a summary of the conversation we often have with investors seeking to understand Bitcoin for the first time.

Money

> *"The two greatest inventions of the human mind are Writing and Money — the common language of intelligence and the common language of self-interest."*
> *—Mirabeau*

Money is an old and complex idea. Historically, it has taken many forms: from decorative axes and cowry shells to precious metals and representative paper. The last major shift was arguably in the early 1970s with the end of the US gold standard and the beginning of the modern fiat currency system.

We can think of money as a competitive market like any other. Gold dominated for centuries not by accident but by possessing important features such as being scarce and unforgeable. Today,

fiat currencies dominate largely through local monopoly power, but all monetary assets still compete globally, with gold, US Dollars, and Euros favored as reserve assets.

Like written language, money is a protocol standard with immense network effects. A new monetary asset can only emerge if it better fulfills the core functions of money, and it can overcome the adoption hurdle of a new money. We believe Bitcoin offers a compelling answer to both.

Store of Value

One of the primary functions of money is to be a store of value: a mechanism to transfer purchasing power across time and geography.

All successful money fulfills this function. If a monetary asset loses trust as a store of value, then savings quickly flow elsewhere, as seen in hyperinflationary economies like Venezuela.

Gold

Gold has been trusted as a store of value for millennia. Importantly, the supply of gold on Earth is scarce. Confidence in this scarcity rests in humanity's understanding of nature: that gold cannot yet be cost-effectively synthesized (despite alchemists' best efforts throughout history).

Gold also has many other desirable properties, such as being easy to recognize (no tarnishing), easy to divide, easy to measure (by weight), and easy to verify (through melting), so it is no surprise that gold replaced predecessors to become a global standard.

Paper Currency and the US Dollar

Paper currencies emerged to simplify the daily use of precious metals as a means of exchange (another core function of money). Although paper notes were initially linked to precious metals, today most paper currencies are free-floating and established by government fiat.

The US Dollar is the leading fiat currency and has been the global reserve currency for much of the last century (replacing the British sterling before it). In addition to being a trusted store of value, the US Dollar is the leading means of exchange and unit of account. A significant share of global trade is priced and settled in US Dollars, whether or not the United States is directly involved.

Confidence in the US Dollar rests on trust in the government (e.g., to wisely manage its monetary policy). There is great efficiency in placing such trust in a single institution, but there is also risk. Fiat currencies can lose credibility and be devalued through the actions of the government, who in times of crisis may face short-term pressures that outweigh concerns for long-term credibility. Countries like Venezuela offer an extreme precedent for currency value in the face of eroding trust: the currency becomes worthless.

Many investors, including central banks, own both gold and US Dollars (or US Dollar-denominated assets) because they offer complementary trade-offs. We can think of the US Dollar as a *centralized* monetary asset, which can be devalued by a single actor, and gold as a *decentralized* monetary asset, which cannot.

Bitcoin

Bitcoin is a new *decentralized* monetary asset, akin to gold. It combines the scarce, money-like nature of gold with the digital transferability of modern currency. Although it remains relatively nascent, Bitcoin has great potential as a *future* store of value based on its intrinsic features.

As with any monetary asset, Bitcoin must be scarce, portable, fungible, divisible, durable, and broadly accepted in order to be useful. Bitcoin rates strongly across most of these dimensions, except for broad acceptability:

- Scarcity: Bitcoin supply is scarce, and asymptotically approaches 21 million coins. Achieving scarcity in digital form was Bitcoin's great technical breakthrough (building on decades of computer science research).
- Portability: Bitcoin is extremely portable, especially relative to gold. Arbitrary amounts of value can be held in a USB stick, or digitally transported across the globe in minutes.
- Fungibility: Any two Bitcoins are practically interchangeable, although each Bitcoin has a distinct history on the public ledger.
- Divisibility: Each Bitcoin can be divided into 100 million smaller units (called "satoshis").
- Durability: Bitcoins are durable and do not degrade over time.
- Broad Acceptability: Bitcoin's primary weakness: it is far less broadly accepted than gold or US Dollars, although it has made impressive strides over the past decade. We can think of broad acceptability along two dimensions, both of which are important: the % of people who trust and accept Bitcoin, and the % of wealth that trusts and accepts Bitcoin.

Beyond these classic monetary features, Bitcoin is also:

- Digital: Digital money like Bitcoin is cheaper to store and easier to transfer than gold, which is physically cumbersome. Bitcoin is also instantly verifiable, whereas gold can require a slow and manual verification process.
- Programmable: Bitcoin is programmable, which has subtle but far-reaching implications. Today Bitcoin scripting enables applications like escrow or micropayments. Over time we may be surprised by what can be built with Bitcoin (much as we were surprised by the Internet, another programmable substrate).
- Decentralized and Censorship-Resistant: The rules of the Bitcoin network (such as its monetary policy) are governed by a decentralized peer-to-peer network, involving a disparate and global user base of consumers, investors, companies, developers, and miners. It is impractical (if not impossible) for a single actor to unilaterally influence the rules of the system. This affords Bitcoin holders a special kind of confidence: that Bitcoin cannot be devalued by arbitrary monetary policy decisions, and that they will always be able to hold and transfer their Bitcoin freely. This could be valuable not just to individuals

and companies but also to governments whose foreign currency reserves may be subject to the whims of foreign entities.
- Universal: Similar to physical bearer assets like US Dollar bills or gold, Bitcoin is a digital bearer asset that anyone can hold and transfer. The same is not true of digital US Dollars (which require a bank account that supports US Dollars) or digital exposure to gold (which requires a brokerage account).

A broadly accepted store of value with the above features would represent a significant improvement over gold, but Bitcoin still lacks broad acceptance and remains nascent as a store of value (as compared to gold's millennia of history and credibility). A better product is not enough—Bitcoin must have a go-to-market strategy to reach broad acceptance.

Bitcoin as a Bubble

Since Bitcoin's inception, many intelligent investors have observed that it appears to be a bubble. They are more right than they know.

If we define a bubble asset as one that is *overvalued relative to intrinsic value*, then we can think of all monetary assets as bubble assets. By definition, a store of value is an intermediate asset that people demand, not for its direct utility, but for its ability to be valuable in the future. This value is reflexive: people will believe in a store of value if they expect others to believe in it (who in turn should expect others to believe in it, and so on).

This phenomenon is distinct from other asset classes, which have utility-based demand, with speculation occurring around this underlying utility. For monetary assets, the utility is in the collective speculation itself.

As Nobel-laureate Robert Shiller observes: *"Gold is a bubble, but it's always been a bubble. It has some industrial uses, but basically it's like a fad that's lasted thousands of years."* This is not an argument against gold (or Bitcoin) as a valuable monetary asset, but an astute insight into the bubble-like, reflexive nature of money.

We can think of money as a bubble that never pops (or that hasn't popped yet) and the value of fiat currency, gold, or Bitcoin as relying on collective belief. Other factors like a government's power, the industrial utility of gold, or the robustness of Bitcoin's codebase can help reinforce this belief, but belief is critical.

Such large amounts of value emerging from collective belief may seem circular and non-fundamental. However, there is real value in the social and economic coordination that monetary assets facilitate (much as there is real value in common language). Moreover, such collective belief cannot arise around any arbitrary asset—a successful monetary asset must compete to earn this belief based on intrinsic features. Having superior intrinsic features explains why gold is preferred to silver or fur pelts and Bitcoin is preferred to any number of Bitcoin copycats.

Bubbles as a Go-To-Market Strategy

If Bitcoin succeeds in becoming a trusted store of value, then its end state is to be a bubble. Bubbles are also how Bitcoin gains broader acceptance.

Throughout Bitcoin's 11-year history, there have been at least four Bitcoin bubbles of note.

- 2011: From ~$1 (Apr 2011) to ~$31 (Jun 2011) to ~$2 (Nov 2011)
- 2013: From ~$13 (Jan 2013) to ~$266 (Apr 2013) to ~$65 (Jul 2013)
- 2013-2015: From ~$65 (Jul 2013) to ~$1242 (Nov 2013) to ~$200 (Jan 2015)
- 2017-2018: From ~$1000 (Apr 2017) to ~$19500 (Dec 2017) to ~$3500 (Dec 2018)

Each bubble has a familiar pattern. High conviction investors start buying when Bitcoin is boring and unloved. The resulting rise in Bitcoin price attracts media attention, which then attracts investors (or speculators), many with lower conviction and shorter time horizons. This drives the price of Bitcoin higher, which drives further attention and investor interest. This cycle repeats until demand exhausts and the bubble crashes.

Although painful for those involved, each bubble leads to broader awareness and motivates Bitcoin's underlying adoption, gradually expanding the base of long-term holders who believe in Bitcoin's potential as a future store of value. This dynamic is evident in the successively higher price floors that Bitcoin reaches during times of maximum disillusionment: ~$2 in 2011, ~$200 in 2015, and ~$3500 in 2018. Broader awareness also encourages the building of Bitcoin infrastructure by startups like Coinbase and incumbents like the CME and Fidelity, further improving Bitcoin's liquidity and utility as a monetary asset. Through successive bubbles, Bitcoin reaches greater levels of scale in users, transaction volumes, network security, and other fundamental metrics.

The Future of Bitcoin

As Bitcoin becomes more broadly accepted, what will its future look like? Some wonder whether people will be earning salaries or making everyday payments in Bitcoin. While these behaviors may exist to some degree, Bitcoin seems unlikely to challenge the US Dollar as the leading means of exchange and unit of account (at least anytime soon). Instead, Bitcoin is likely to earn a place alongside gold as a sensible part of many investment portfolios. This has already begun with an early-adopter, tech-forward crowd, and we expect it to grow to include a broader set of investors and institutions over time. Eventually, central banks may come to view Bitcoin as a complement to their existing gold holdings.

Ultimately, monetary assets rise and fall on timescales that stretch beyond human lifespans, making them a challenge to forecast. There was a time before the US Dollar reigned when the reserve currency was British, or French, or Dutch, or further into ancient history, Greek or Roman. Similarly, there was a time before the adoption of gold when more primitive forms of money were dominant. The idea of a fiat currency like the US Dollar being untethered to gold is itself a recent phenomenon that seemed unthinkable half a century ago. In the future, it seems

likely that the global monetary order could change in ways that would be unthinkable to us today, with digital currencies such as Bitcoin playing a significant role.

Market Size

As a decentralized store of value, it is most natural to consider Bitcoin's market size relative to gold, whose aggregate value is estimated to be ~$9T (May 2020) between central bank reserves (17%), private investment holdings (22%), jewelry (47%), and other miscellaneous forms (14%). Some but not all of this value is addressable by Bitcoin.

Over time, the market demand for assets like gold and Bitcoin could expand to exceed ~$9T, especially given the prevailing direction of global monetary policy. According to the IMF, total international reserves reached ~$13T in 2019 between gold (11%), foreign currency reserves (86%), and IMF-related assets (3%). If foreign governments (some of whom already bristle at their dependence on US Dollar FX reserves) begin to adopt Bitcoin as a complement to existing gold holdings, the market size for Bitcoin could expand significantly.

Beyond complementing gold's investment demand, Bitcoin may also address broader store of value markets indirectly. Consider, for example, people who hold fiat currencies with eroding credibility such as the Argentine Peso or the Turkish Lira, but who may have difficulty accessing US Dollars or gold. Or consider various collectibles like art or gemstones, some of which are owned primarily as stores of value. Or consider the empty NYC apartment that is owned by a foreigner interested in storing value outside his or her native country. Bitcoin could plausibly address subsets of these behaviors more effectively.

Deferring a precise estimate of market size, we believe it is clear that Bitcoin has significant headroom if it continues to gain broader acceptance.

Risks

Although it has come a long way in 11 years, many risks remain for Bitcoin:

- Crossing the Chasm: Bitcoin has gained credibility with early adopters, including some large institutional investors, but it remains niche relative to incumbent monetary assets like gold. There is risk that Bitcoin never achieves the broad acceptance that its proponents hope it will. Of course, therein also lies the opportunity. If Bitcoin were already a broadly accepted store of value, then it would likely be worth orders of magnitude more with relatively little remaining upside.
- Volatility: Bitcoin has been (and continues to be) quite volatile relative to US Dollars. There is risk that this volatility limits adoption or prevents investors from considering Bitcoin as a credible store of value. For better or worse, this volatility may be inherent to the process of Bitcoin adoption as natural swings in investor confidence (as faced by any early-stage upstart) are reflected in Bitcoin prices. Bitcoin’s bubble-like adoption process exacerbates this effect. As Bitcoin matures and becomes more broadly accepted as a monetary asset akin to gold, investor confidence and Bitcoin prices should stabilize.

- Regulation: Bitcoin is a new currency and payment rail that sits outside of existing systems, posing a potential challenge to existing regulatory frameworks. Similar to early Internet regulation, there is hope that governments pursue nuanced regulation(s) that allow innovative use-cases to prevail. However, there is risk that regulation is onerous and ultimately hinders broader Bitcoin adoption. One mitigating factor is that Bitcoin is a global, decentralized network like the Internet, which is difficult to control for any single government, although governments can plausibly limit access to Bitcoin in various ways.
- Technical Risk: The Bitcoin codebase and network have been battle-tested for over a decade, but it continues to evolve and there remain some open questions about how the system might behave in the long run (for example, when the Bitcoin supply approaches its asymptote and miners must be compensated primarily with transaction fees rather than block rewards).
- Competitive Risk: Other cryptocurrencies could compete with Bitcoin, as could digital fiat currencies sponsored by governments. Relative to other cryptocurrencies, Bitcoin has a strong first-mover advantage in acceptance, security, and credibility that will be difficult for competitors to overcome. Relative to digital fiat currencies, Bitcoin remains differentiated in its scarce, gold-like nature. Digital US Dollars or digital Renminbi would still be subject to local monetary policy decisions, although they have the benefit that they are currency units people already know and use.
- Unknown Unknowns: We must acknowledge that a digital monetary asset such as Bitcoin has never existed before. We are in uncharted territory with more uncertainty than is typical.

Conclusion

Bitcoin is a new monetary asset that is climbing an adoption curve. Although it is not *yet* a broadly accepted store of value, Bitcoin has great potential as a *future* store of value based on its intrinsic features.

Since monetary assets do not arise frequently, Bitcoin is likely to challenge our ordinary intuitions, and it has stirred (understandable) controversy in the investment world.

Therein lies the opportunity, of course. We believe Bitcoin offers a compelling risk/reward profile for patient, long-term investors willing to spend the time to truly understand Bitcoin. We hope this paper provides a helpful starting point.

About the Author

Matt Huang is co-founder and Managing Partner at Paradigm. Previously, Matt was a partner at Sequoia Capital focusing on early-stage venture investments including leading the firm's cryptocurrency efforts. Matt was the founder and CEO of Hotspots, a YCombinator company acquired by Twitter in 2012, and angel investor in companies such as ByteDance and Instacart. He purchased his first Bitcoin from MtGox in 2012. Matt holds a B.S. in Mathematics from MIT.

Twitter: @matthuang
LinkedIn: Matt Huang

Acknowledgments

This paper benefited from the feedback and contributions of many:

- *Fred Ehrsam, my partner and co-founder at Paradigm, and our colleagues Alana Palmedo, Arjun Balaji, Charlie Noyes, and Dan Robinson.*
- *Michael Abramson, Alfred Lin, and Kevin Kelly of Sequoia Capital. I'm grateful to them and the rest of my former colleagues at Sequoia Capital for their open-minded interest in Bitcoin circa 2014-2018.*
- *Wences Casares of Xapo, and member of the Board of Directors of Paypal and Libra*
- *Pete Briger and Michael Hourigan of Fortress Investment Group*
- *John Pfeffer of Pfeffer Capital, and formerly of KKR*
- *Micky Malka of Ribbit Capital*
- *Nick Shalek of Ribbit Capital, and formerly of the Yale Investments Office*
- *Steve Lee of Square Crypto, and contributor to Bitcoin Core development*
- *Peter Palmedo of Sun Valley Gold*
- *Tyler Cowen of George Mason University and Marginal Revolution*

User Thoughts

Why Bitcoin (http://www.brianrast.com/)
September 9, 2019

by Brian Rast

How the Bitcoin protocol actually works (http://michaelnielsen.org/)
December 6, 2013

by Michael Nielsen

The case for a small allocation to Bitcoin (https://www.kanaandkatana.com/)
March 1, 2019

by Wences Casares, CEO of Xapo

If you think I'm missing any major essays/papers, shoot me an email at kevin@12mv2.com or a dm on Twitter @kgao1412 with the subject: "Bitcoin Compilation." Thanks!

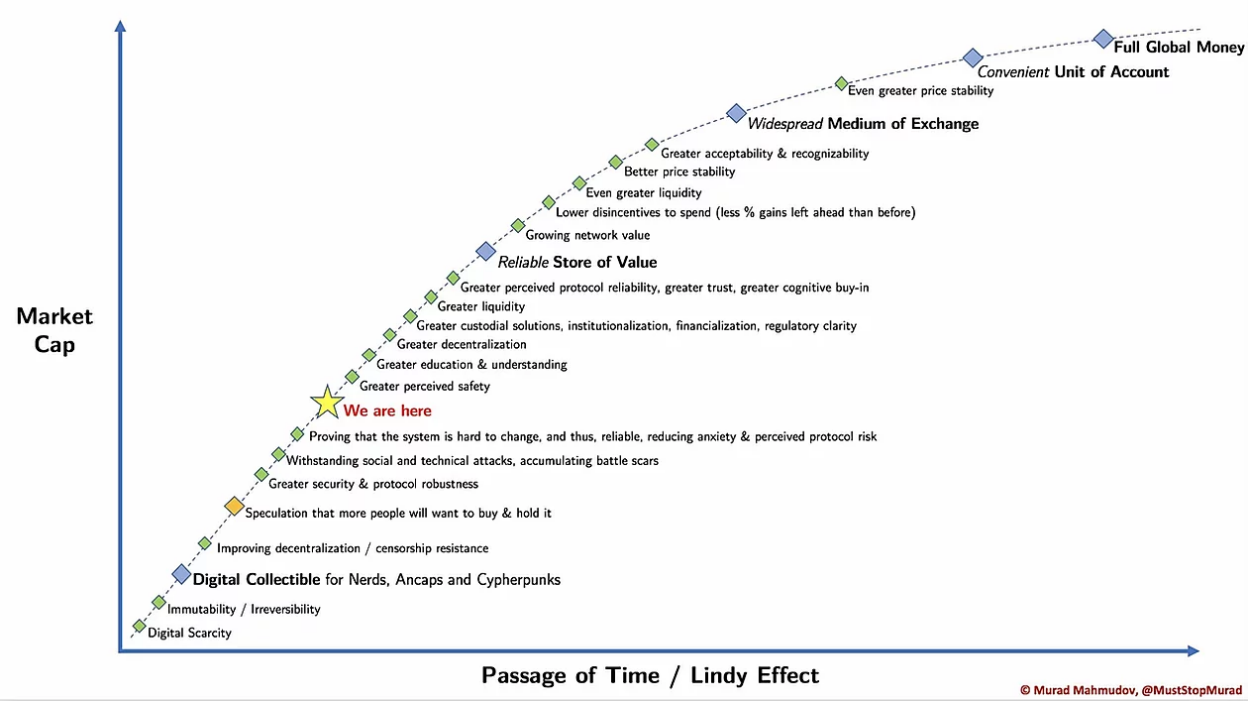
Why Bitcoin (First published at http://www.brianrast.com/)
September 9, 2019

by Brian Rast

While I've linked a number of things related to Bitcoin, I've never actually posted my opinion on the matter. This will be an argument as to why Bitcoin is relevant, why it has value, what that value might be, and why I believe it should be considered for including in a financial portfolio. This argument has been made in many places all over the web (some of the best material I know of is linked here), and I am hoping to speak to people that follow me that might not be exposed and the tone of this is for a layperson who has not already spent much time in the space or already invested. I'm not going to delve much in to the technical aspects of how Bitcoin works - nor do I have a deep understanding of them. I do have a rough idea about how it works, but I believe that investing in Bitcoin for most people is more an economic exercise than a technical one. I also believe that generally you should only invest in things when you have an understanding of what you're investing in, and Bitcoin is no exception here.

Despite the fact that I am bullish on Bitcoin, this article isn't financial advice. Firstly, nobody including myself knows what will happen, especially with something as complex as Bitcoin and the world economic environment. Secondly, everyone's financial situation and risk appetite is different, and what's right for one person or myself might not be right for other people. Do your own research and come to your own conclusions. I'm not sure who is an expert on something as speculative and wide-ranging as Bitcoin, but if there is someone, it's not me. I'm just a guy with an opinion. I just want to share my thoughts and hope that they can help some people on their own journeys.

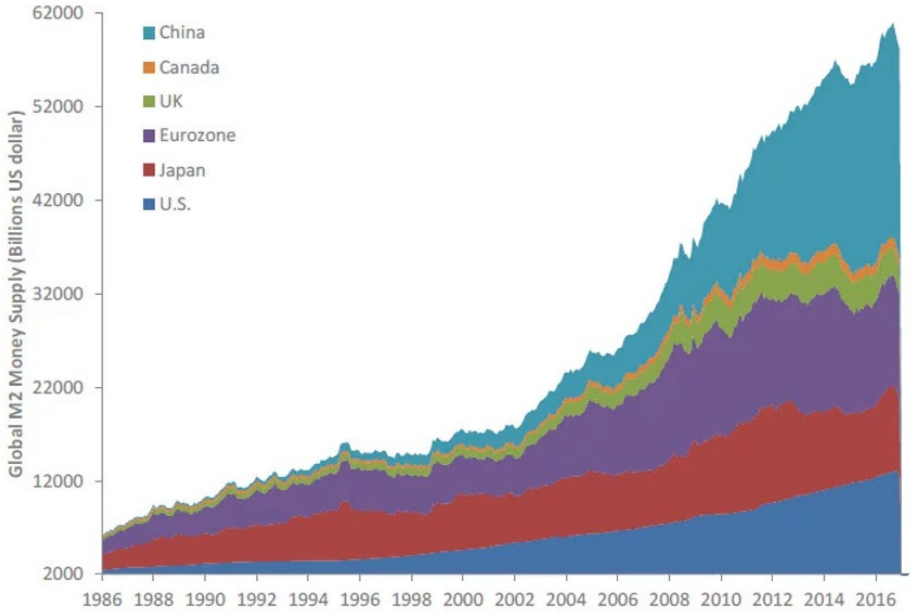
So first I'm going to discuss why Bitcoin is valuable. For those who don't really know what Bitcoin is, there is a lot of great material on the web that can teach you more or less how it works. I'm not going to delve in to that here and don't think it's necessary to understand this blog. That said, having a rudimentary understanding of how Bitcoin works is pretty easy to get and I would recommend doing so if this article makes you interested. Read this link for a nice short piece on Why Bitcoin Matters. Bitcoin is essentially just a ledger. It lets you transact numbers on that ledger (bitcoins and satoshis - the smallest divisible unit of a bitcoin) with other people without having to trust a 3rd party to guarantee the transaction (bank, paypal, credit card, etc...). That is very valuable because now with Bitcoin you don't need to pay for that 3rd party to exist (structural business costs, bank wire fees, credit card fees and interest, etc...) AND you don't have the potential control or censorship from that 3rd party. Bitcoin is not controlled by anyone and is therefore censorship resistant. Bitcoin itself is very secure. All theft is due to carelessness on the part of owners, and incompetency or dishonesty from the companies they used (such as exchanges). Bitcoin transactions are not reversible as well. If you make a mistake, there isn't a way to undo it. That finality can make using Bitcoin intimidating, especially to new users. But that finality is also a feature which ensures increased security for transactions. They will not be reversed, so you know when bitcoin is sent it will not be returned without another transaction, This is a cool chart which shows a potential growth outline of Bitcoin from inception to full blown Global Money from Murad Mahmudov's twitter.

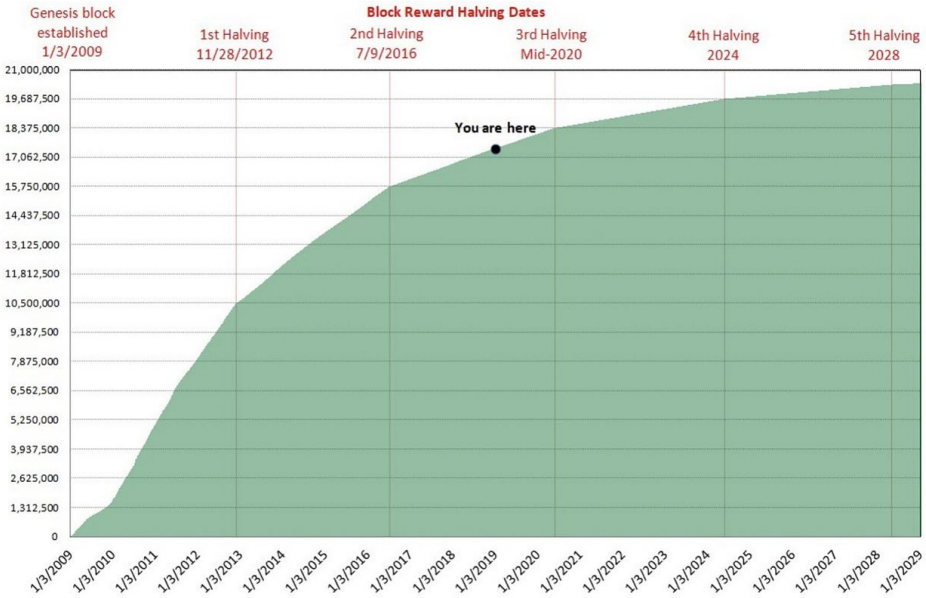


So, Bitcoin is ultimately an attempt at a decentralized, digital/internet money. But Bitcoin isn't really there yet. It's on a path to getting there. The primary thing holding bitcoin back from doing that right now, besides the lack of universal acceptance, is that Bitcoin can't currently process nearly as many transactions as say VISA. But, Bitcoin's most valuable property is not today nor ever going to be its ability to be used as another form of money to buy things every day, even if one day it can be used by people around the world for that. USD, EUROS, and other regular fiat currencies already work very well today when combined with credit cards and other financial instruments in order to facilitate these type of purchases. So I can fully understand why people might ask why they need another internet money to buy things. Most people living in rich countries with successful currencies don't have a need for this (although people living in countries with bad currencies, or poor and unbanked - they are another story. I believe a potential future use case of bitcoin is as a better currency for day-to-day use for the poor unbanked in the world, who can use their cellular phones, computers, or similar devices, and be their own bank with Bitcoin and have their own BTC credit card on say their phone or perhaps later even a card that spends the BTC at your address. That would prove especially valuable in countries with weak and inflationary currencies). But that way of viewing Bitcoin pigeon-holes it in to trying to be something much less than it actually is. Bitcoin doesn't derive most of its value from simply being an alternative currency.

Bitcoin's most valuable property is its programmed scarcity. Bitcoin was created with a scheduled inflationary policy. Every 10 minutes when the transactions are processed on the blockchain, bitcoins are "mined" (created) and given to the miners that process these transactions. The number that is created in these blocks is cut in half every 4 years. This process means that every 4 years the inflationary pressure in Bitcoin is cut in half, and that eventually - mathematically - there will be essentially no new bitcoins mined. Right now there are approximately 18 million bitcoins in existence, and the final total will be 21 million. Therefore, in Bitcoin's entire future lifespan, there will only be an inflation of 3 million more coins, or approximately 1/6 the amount of the current supply. EVER. That seems especially valuable when compared to your local fiat currency controlled by your nation's central bank, whose monetary

policy is at the whims of the political climate, special interests, politicians, bankers, and everyone who isn't you nor has your best interests in mind. Now there is a lot of debate about the exact affects of monetary inflation and money supply, and it's an interesting topic to look in to. I believe that the massive increase in money supply (eg Quantitative Easing) that banks are employing, even if it currently hasn't caused demonstrably massive inflation, will eventually cause the continual devaluation of those currencies and inflation. Here is a chart of the global money supply over the last 30 years followed by a chart of bitcoin supply.





The first chart is showing an exponential growth in Fiat money supply in the world where the rate of supply has been increasing. That might continue or it might not. The Bitcoin supply rate is decreasing, and that WILL continue. It's programmed scarcity. Which of those two moneys would you rather keep value in based on just the supply curves?

Today the monetary solution seems to be to keep lowering interest rates, and keep printing more money. This has caused massive growth in Real Estate and equities (SPX, stock markets) in the last 10 years as all this loose money and credit looks for a place to go. There is basically no interest for saving money in the bank, bond yields everywhere are going negative, and US Dollars purchasing power has gone down. Sure, for goods where the technology is continually improved - the Purchasing Power has gotten a lot better (eg TVs get better and cheaper). But when you factor out technological improvement, I believe you can see quite a lot of inflation (gas prices worldwide, insulin prices, etc...), and it's part of the reason why the average American is struggling.

And in to this environment, I believe assets that store value and have scarcity will have innate value. Bitcoin's greatest use case is simply being a great way to store value because it has a defined and small inflationary policy - programmed scarcity. In this, it is a lot like Gold. It is a scarce asset that people perceive to have value. Gold, however, has been around for thousands of years... and considered by people around the world to have a lot of value and be a Store of Value. Bitcoin does not have that kind of historical track record, obviously. It hasn't quite gotten to 10 years yet. Bitcoin also doesn't have practical use as gold does as a mineral for various industrial uses and for jewelry. On the other hand, Gold is not a practical form of money as it is difficult to send, transport, divide... or basically use. Bitcoin, on the other hand, does all of those things very well. So, in a very real sense, Bitcoin requires people to discover and accept its value as a programmable scarce asset like gold but with a whole lot more utility as a money. That's a key part of this story. BItcoin needs other people to realize it's great properties, its use cases, and buy it. And if that continues to happen, then eventually Bitcoin will become the Store of Value, Unit of Account, and Digital Currency that right now its believers and investors think it might. In that sense, Bitcoin should exhibit some properties as a network.

Just like other forms of money, you have to believe Bitcoin has value, in order for it to ultimately have that value. We accept the dollar in America because our government prints it and backs it, despite the fact that it's merely a piece of paper or a number in a bank account. Bitcoin isn't backed by a government - but has a ledger of transactions and keeps a Unit of Account backed by Proof of Work done by all the miners in order to guarantee that. Ultimately all money is worth something only because someone else will accept it in a transaction. Money by itself is worthless, and just a value holder everyone accepts in order to efficiently transact in a society. This allowed us to move beyond basic bartering and trading, to specialize labor, and so on. There is nothing inherently more valuable about a currency because it's backed by a government. It does provide a greater perceived security in that currency. But I would submit that many many governments throughout history have destroyed the worth of their currencies, and you've seen all kinds of hyper-inflationary events, like the Weimar Republic, Venezuela today, and others, where things got absolutely ridiculous before they broke down.

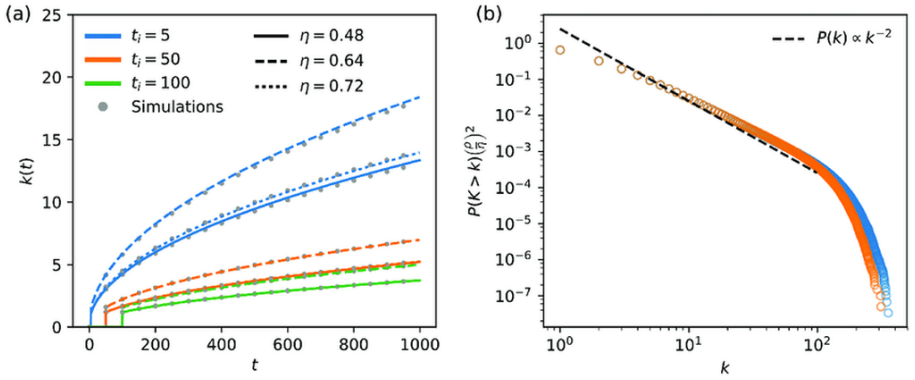
The point is this... Bitcoin has a lot of amazing properties that make it, in my opinion, the best money that man has created to this day. It is the most secure asset. Not only can your bitcoin not be hacked, it can't be seized from you. Someone could put a gun to your head and you still wouldn't have to give them your bitcoin if you didn't want to. Literally everything you own can be taken by force, even if you were willing to do anything - even die - in order to try and stop that. Your property can be seized by the government. Your possessions can be seized, or if you are robbed they can be forcefully taken with or without your consent. Bitcoin isn't something you physically own. Bitcoin cannot be taken without your consent. (This isn't suggesting that if someone puts a gun to your head, or a government threatens jail time, that you wouldn't give up your bitcoin. But you would have the choice not to, and thus your consent is required.) You can access it, but your bitcoin is essentially just an agreed upon number that exists on the Bitcoin blockchain on computers around the world. You only control your access to that, and with

relatively simple security methods, you can easily make it so nobody can access your Bitcoin unless you want them to. There is literally no asset in the world today that is as secure as Bitcoin.

Bitcoin is easy to store. There are currently wallets that are very secure - like a Trezor - which you can carry with you and access your Bitcoin via a USB port (or not carry with you and therefore not be able to access). It's easy to take this with you wherever you want, traveling anywhere in the world with you with the ability to access and send/receive infinite. What other asset is that easy and practical to use? Bitcoin is also divisible to any amount you would conceivably need to send, making it easy to transact. It can be sent relatively quickly (it is not currently as fast as instant transactions such as Credit Cards, but much faster than Bank Wires). It has relatively low fees, that are not based on the amount sent - therefore Bitcoin is perfect for sending and receiving large amounts.

Bitcoin is the perfect asset to store liquid net worth. I believe that one of Bitcoin's primary use cases will be the best way to store net worth that you want to keep liquid. Rather than sit on a fiat currency which will devalue over time because of inflation, someone would instead choose to keep their liquid net worth in Bitcoin, which can be at the very least quickly exchanged to a fiat currency if not used directly.

When you survey it all together and take it in - you are logically forced to admit that Bitcoin is the greatest asset that we have created. The only thing holding it back at this point is simply the progression of it technologically and the acceptance of it by people around the world. Slowly more and more people own and are using Bitcoin, and this growth needs to continue if Bitcoin is going to ultimately succeed. The world doesn't have to be logical and rational - and individuals mostly aren't - but I would bet that the emergent decisions we make economically will tend to be. Interestingly Bitcoin's growth in price as an asset over time is very similar to a network growth model - which makes intuitive sense to me.



Bitcoin has been growing very similar to what a network growth model would predict with a logarithmic growth curve.

So now that hopefully you agree that Bitcoin has value, the next step is trying to wrap your head around how to try to estimate what Bitcoin's value could be. Pfeffer attempts this in his article on Cryptoassets, which I recommend checking out. He postulates the following sources of value: 1) Replacing Gold Bullion 2) Becoming an International Reserve Currency 3) Unit of Account for international trade 4) International payments & Domestic payments in countries w/out stable sovereign currencies. The total speculative range he gives for this if Bitcoin were to become the dominant monetary store of value cryptoasset and realize some or all of those use cases is 4.7 - 14.6 Trillion USD, which gives Bitcoin - fully diluted (all 21M) a range of $260k - $800k per Bitcoin. I would add as a potential use case, Bitcoin supplanting or taking a share out of the offshore private banking market; a market which has been estimated as having over $21 trillion USD worth.

PlanB models scarcity by quantifying it as a stock-to-flow ratio, and gives this mathematical prediction for Bitcoin's value based on this in his work HERE. I would highly recommend reading this, it's very interesting. To take a simple snippet, his estimation for Bitcoin's worth after this halving event next May 2020 is $55,000USD. Every 4 years Bitcoin increases in scarcity with each successive halving, and thus increases in value.

People ask where the money comes from to get Bitcoin from its current price levels to the types of valuations that are being discussed here. This is a great answer to that "People ask me where all the money needed for $1trn bitcoin market value would come from? My answer: silver, gold, countries with negative interest rate (Europe, Japan, US soon), countries with predatory governments (Venezuela, China, Iran, Turkey etc), billionaires and millionaires hedging against quantitative easing (QE), and institutional investors discovering the best performing asset of last 10 yrs." Imagine someone wealthy living in a country with a predatory government wanting the ultimate get-away quick plan to escape with some of their wealth should they need to. Bitcoin is literally perfect for them.

I believe that in the next year or two, a trading firm - like TD - will allow people who have accounts with them to buy and sell Bitcoin. Whether it is through an approved ETF, or because the institution themselves works out a storage solution privately and processes the transaction (with fees), I believe this will happen soon and open up easy access to all the money private investors hold in their brokerage accounts.

I believe that now that this idea is out there, something will become a decentralized, digital Store-of-value, unit of account, and currency. Once the proverbial cat is out of the bag, then you can't put it back. I believe that Bitcoin is by far the best option for that, but why not something else? While I do think it's possible that Bitcoin doesn't realize this and something else does, I think that is unlikely. There are some other cryptocurrencies out there that have been started with other features, like for example Ethereum and many others. A lot of these have good features and will likely be useful and valuable for what they are designed to do. But different functions have different values. First, let me differentiate between the value of a cryptocurrency in so far as it runs some other project - vs the value of a cryptocurrency in so far as it is a digital store of value. Pfeffer discusses this in some depth in his paper and makes the argument that the primary value is in becoming the dominant digital store of value. It's a somewhat intricate argument that I would suggest reading, especially if you own ALT coins or are seriously considering investing in them. I personally do not believe that ALT coins should accrue value like Bitcoin if they are trying to perform some specific function (DAPP platform, decentralized betting market, etc...), because even if their chain is used, there is no direct function or reason why the token

itself will accrue the value the chain is being used for. The token is not like stock in the company, it is not a part of the total value being passed by users of the blockchain. It really just represents the grease inside the machine, necessary to process the transactions, and will likely converge to the value of the processing power needed to run the network. This differs because whatever is being used as a digital store of value will accrue the value of what's used to invest in the network, as it is storing that value.

And why won't one of these coins take over Bitcoin? I would argue that Bitcoin has a large first mover advantage. Its name is much more popular and it's more well known, both important for network growth. Also in terms of a currency, Bitcoin has been proven to be secure for 10 years and with network valuations of 200 Billion USD and higher. No other blockchain has this kind of stability, security, and proven track record. The blockchain is open, on the web, not behind a firewall, open to hostile attacks and hacks - and has remained safe. Many projects aren't nearly as proven, and aren't decentralized enough - and IMO centralization and control would largely defeat the point and one of the main attractions of this type of digital currency. Bitcoin has shown it is reliable and robust, and those things are both extremely important for a currency. I don't believe it will be replaced by a newer cryptocurrency because no added feature will be worth more than that reliability, robustness, or security that has been established already on Bitcoin insofar as it simply being a SoV, Unit of Account, and currency. And most features, if they proved valuable, could eventually be added to Bitcoin if necessary.

So to me the Sharpe Ratio, or return given risk, of every single Alt Coin is significantly lower than Bitcoin when considering as an investment. Therefore at the current time, I believe the best allocation for a prospective investor buying Cryptocurrency is 100% Bitcoin. It is possible and even likely that today there is something out of the 1000s of coins that will outperform Bitcoin in 5 years, but I don't believe it will be easy to pick and investing in many will almost certainly do worse than Bitcoin as a group.

When considering Bitcoin as an investment, I think an investor should think about it like this... You are making a long term investment speculating in Bitcoin realizing the use cases and properties discussed here. If it does this, it's very likely to reach much higher valuations than today (today Bitcoin is just over 10kUSD). Let's say that for this current bull market cycle, we are looking at a 2-3 year price target of. 50-120k. If Bitcoin doesn't work out, or if there is some kind of systemic problem, the value of Bitcoin is likely to crash and it's unclear how much of the value you might be able to recover. So for simplicities sake, let's say that you are looking at Bitcoin going from 10k to either 0 or to 100k in 2-3 years. So, for this bet to be +EV, it only has to be successful 10% or more of the time. With this view, this is a very asymmetrical bet with potential upside much greater than the downside. High risk, high reward, that even if it is +EV should be taken with some caution. That said, I consider the likelihood that Bitcoin fulfills these potentialities to be significantly higher than 10%, and therefore think buying BTC to be a +EV long term move. (Obviously a Bitcoin bear would likely disagree w/ that probability allocation). So something like buying Bitcoin today to hold half for 2-3 years before taking profit at the end of this bull cycle, and the other half in order to hold for a much longer time frame (forever?) seems like the makings of a reasonable plan.

Despite the fact that Bitcoin has a very high long-term risk factor, it seems to be not correlated with other assets like the S&P 500 and equities, therefore a Bitcoin allocation could be part of a balanced portfolio that might achieve higher expected returns without raising raising a portfolio's risk of ruin - something increased by having a lot of correlated assets.

Other good Bitcoin resources:

Ultimate Bitcoin Argument podcast w/ Murad & Pomp - good podcast with discussion about why Bitcoin is important

Woobull charts by Willy Woo - interesting charts modeling different aspects of Bitcoin

Youtube Channel of Aantonop - youtube channel of best Bitcoin speaker/evangelist

Bitcoin Second Layer Medium article - discussion of bitcoin layers and how they will interact. Important to understand how BTC might scale

How the Bitcoin protocol actually works (First published at http://michaelnielsen.org/)
December 6, 2013

by Michael Nielsen

Many thousands of articles have been written purporting to explain Bitcoin, the online, peer-to-peer currency. Most of those articles give a hand-wavy account of the underlying cryptographic protocol, omitting many details. Even those articles which delve deeper often gloss over crucial points. My aim in this post is to explain the major ideas behind the Bitcoin protocol in a clear, easily comprehensible way. We'll start from first principles, build up to a broad theoretical understanding of how the protocol works, and then dig down into the nitty-gritty, examining the raw data in a Bitcoin transaction.

Understanding the protocol in this detailed way is hard work. It is tempting instead to take Bitcoin as given, and to engage in speculation about how to get rich with Bitcoin, whether Bitcoin is a bubble, whether Bitcoin might one day mean the end of taxation, and so on. That's fun, but severely limits your understanding. Understanding the details of the Bitcoin protocol opens up otherwise inaccessible vistas. In particular, it's the basis for understanding Bitcoin's built-in scripting language, which makes it possible to use Bitcoin to create new types of financial instruments, such as smart contracts. New financial instruments can, in turn, be used to create new markets and to enable new forms of collective human behaviour. Talk about fun!

I'll describe Bitcoin scripting and concepts such as smart contracts in future posts. This post concentrates on explaining the nuts-and-bolts of the Bitcoin protocol. To understand the post, you need to be comfortable with public key cryptography, and with the closely related idea of digital signatures. I'll also assume you're familiar with cryptographic hashing. None of this is especially difficult. The basic ideas can be taught in freshman university mathematics or computer science classes. The ideas are beautiful, so if you're not familiar with them, I recommend taking a few hours to get familiar.

It may seem surprising that Bitcoin's basis is cryptography. Isn't Bitcoin a currency, not a way of sending secret messages? In fact, the problems Bitcoin needs to solve are largely about securing transactions — making sure people can't steal from one another, or impersonate one another, and so on. In the world of atoms we achieve security with devices such as locks, safes, signatures, and bank vaults. In the world of bits we achieve this kind of security with cryptography. And that's why Bitcoin is at heart a cryptographic protocol.

My strategy in the post is to build Bitcoin up in stages. I'll begin by explaining a very simple digital currency, based on ideas that are almost obvious. We'll call that currency *Infocoin*, to distinguish it from Bitcoin. Of course, our first version of Infocoin will have many deficiencies, and so we'll go through several iterations of Infocoin, with each iteration introducing just one or two simple new ideas. After several such iterations, we'll arrive at the full Bitcoin protocol. We will have reinvented Bitcoin!

This strategy is slower than if I explained the entire Bitcoin protocol in one shot. But while you can understand the mechanics of Bitcoin through such a one-shot explanation, it would be difficult to understand *why* Bitcoin is designed the way it is. The advantage of the slower iterative explanation is that it gives us a much sharper understanding of each element of Bitcoin.

Finally, I should mention that I'm a relative newcomer to Bitcoin. I've been following it loosely since 2011 (and cryptocurrencies since the late 1990s), but only got seriously into the details of the Bitcoin protocol earlier this year. So I'd certainly appreciate corrections of any misapprehensions on my part. Also in the post I've included a number of "problems for the author" – notes to myself about questions

that came up during the writing. You may find these interesting, but you can also skip them entirely without losing track of the main text.

First steps: a signed letter of intent

So how can we design a digital currency?

On the face of it, a digital currency sounds impossible. Suppose some person – let's call her Alice – has some digital money which she wants to spend. If Alice can use a string of bits as money, how can we prevent her from using the same bit string over and over, thus minting an infinite supply of money? Or, if we can somehow solve that problem, how can we prevent someone else forging such a string of bits, and using that to steal from Alice?

These are just two of the many problems that must be overcome in order to use information as money.

As a first version of Infocoin, let's find a way that Alice can use a string of bits as a (very primitive and incomplete) form of money, in a way that gives her at least some protection against forgery. Suppose Alice wants to give another person, Bob, an infocoin. To do this, Alice writes down the message "I, Alice, am giving Bob one infocoin". She then digitally signs the message using a private cryptographic key, and announces the signed string of bits to the entire world.

(By the way, I'm using capitalized "Infocoin" to refer to the protocol and general concept, and lowercase "infocoin" to refer to specific denominations of the currency. A similar useage is common, though not universal, in the Bitcoin world.)

This isn't terribly impressive as a prototype digital currency! But it does have some virtues. Anyone in the world (including Bob) can use Alice's public key to verify that Alice really was the person who signed the message "I, Alice, am giving Bob one infocoin". No-one else could have created that bit string, and so Alice can't turn around and say "No, I didn't mean to give Bob an infocoin". So the protocol establishes that Alice truly intends to give Bob one infocoin. The same fact – no-one else could compose such a signed message – also gives Alice some limited protection from forgery. Of course, *after* Alice has published her message it's possible for other people to duplicate the message, so in that sense forgery is possible. But it's not possible from scratch. These two properties – establishment of intent on Alice's part, and the limited protection from forgery – are genuinely notable features of this protocol.

I haven't (quite) said exactly what digital money *is* in this protocol. To make this explicit: it's just the message itself, i.e., the string of bits representing the digitally signed message "I, Alice, am giving Bob one infocoin". Later protocols will be similar, in that all our forms of digital money will be just more and more elaborate messages [1].

Using serial numbers to make coins uniquely identifiable

A problem with the first version of Infocoin is that Alice could keep sending Bob the same signed message over and over. Suppose Bob receives ten copies of the signed message "I, Alice, am giving Bob one infocoin". Does that mean Alice sent Bob ten *different* infocoins? Was her message accidentally duplicated? Perhaps she was trying to trick Bob into believing that she had given him ten different infocoins, when the message only proves to the world that she intends to transfer one infocoin.

What we'd like is a way of making infocoins unique. They need a label or serial number. Alice would sign the message "I, Alice, am giving Bob one infocoin, with serial number 8740348". Then, later, Alice could sign the message "I, Alice, am giving Bob one infocoin, with serial number 8770431", and Bob (and everyone else) would know that a different infocoin was being transferred.

To make this scheme work we need a trusted source of serial numbers for the infocoins. One way to create such a source is to introduce a *bank*. This bank would provide serial numbers for infocoins, keep track of who has which infocoins, and verify that transactions really are legitimate,

In more detail, let's suppose Alice goes into the bank, and says "I want to withdraw one infocoin from my account". The bank reduces her account balance by one infocoin, and assigns her a new, never-before used serial number, let's say 1234567. Then, when Alice wants to transfer her infocoin to Bob, she signs the message "I, Alice, am giving Bob one infocoin, with serial number 1234567". But Bob doesn't just accept the infocoin. Instead, he contacts the bank, and verifies that: (a) the infocoin with that serial number belongs to Alice; and (b) Alice hasn't already spent the infocoin. If both those things are true, then Bob tells the bank he wants to accept the infocoin, and the bank updates their records to show that the infocoin with that serial number is now in Bob's possession, and no longer belongs to Alice.

Making everyone collectively the bank

This last solution looks pretty promising. However, it turns out that we can do something much more ambitious. We can eliminate the bank entirely from the protocol. This changes the nature of the currency considerably. It means that there is no longer any single organization in charge of the currency. And when you think about the enormous power a central bank has – control over the money supply – that's a pretty huge change.

The idea is to make it so *everyone* (collectively) is the bank. In particular, we'll assume that everyone using Infocoin keeps a complete record of which infocoins belong to which person. You can think of this as a shared public ledger showing all Infocoin transactions. We'll call this ledger the *block chain*, since that's what the complete record will be called in Bitcoin, once we get to it.

Now, suppose Alice wants to transfer an infocoin to Bob. She signs the message "I, Alice, am giving Bob one infocoin, with serial number 1234567", and gives the signed message to Bob. Bob can use his copy of the block chain to check that, indeed, the infocoin is Alice's to give. If that checks out then he broadcasts both Alice's message and his acceptance of the transaction to the entire network, and everyone updates their copy of the block chain.

We still have the "where do serial number come from" problem, but that turns out to be pretty easy to solve, and so I will defer it to later, in the discussion of Bitcoin. A more challenging problem is that this protocol allows Alice to cheat by double spending her infocoin. She sends the signed message "I, Alice, am giving Bob one infocoin, with serial number 1234567″ to Bob, and the message"I, Alice, am giving Charlie one infocoin, with [the same] serial number 1234567" to Charlie. Both Bob and Charlie use their copy of the block chain to verify that the infocoin is Alice's to spend. Provided they do this verification at nearly the same time (before they've had a chance to hear from one another), both will find that, yes, the block chain shows the coin belongs to Alice. And so they will both accept the transaction, and also broadcast their acceptance of the transaction. Now there's a problem. How should other people update their block chains? There may be no easy way to achieve a consistent shared ledger of transactions. And even if everyone can agree on a consistent way to update their block chains, there is still the problem that either Bob or Charlie will be cheated.

At first glance double spending seems difficult for Alice to pull off. After all, if Alice sends the message first to Bob, then Bob can verify the message, and tell everyone else in the network (including Charlie) to update their block chain. Once that has happened, Charlie would no longer be fooled by Alice. So there is most likely only a brief period of time in which Alice can double spend. However, it's obviously undesirable to have any such a period of time. Worse, there are techniques Alice could use to make that

period longer. She could, for example, use network traffic analysis to find times when Bob and Charlie are likely to have a lot of latency in communication. Or perhaps she could do something to deliberately disrupt their communications. If she can slow communication even a little that makes her task of double spending much easier.

How can we address the problem of double spending? The obvious solution is that when Alice sends Bob an infocoin, Bob shouldn't try to verify the transaction alone. Rather, he should broadcast the possible transaction to the entire network of Infocoin users, and ask them to help determine whether the transaction is legitimate. If they collectively decide that the transaction is okay, then Bob can accept the infocoin, and everyone will update their block chain. This type of protocol can help prevent double spending, since if Alice tries to spend her infocoin with both Bob and Charlie, other people on the network will notice, and network users will tell both Bob and Charlie that there is a problem with the transaction, and the transaction shouldn't go through.

In more detail, let's suppose Alice wants to give Bob an infocoin. As before, she signs the message "I, Alice, am giving Bob one infocoin, with serial number 1234567", and gives the signed message to Bob. Also as before, Bob does a sanity check, using his copy of the block chain to check that, indeed, the coin currently belongs to Alice. But at that point the protocol is modified. Bob doesn't just go ahead and accept the transaction. Instead, he broadcasts Alice's message to the entire network. Other members of the network check to see whether Alice owns that infocoin. If so, they broadcast the message "Yes, Alice owns infocoin 1234567, it can now be transferred to Bob." Once enough people have broadcast that message, everyone updates their block chain to show that infocoin 1234567 now belongs to Bob, and the transaction is complete.

This protocol has many imprecise elements at present. For instance, what does it mean to say "once enough people have broadcast that message"? What exactly does "enough" mean here? It can't mean everyone in the network, since we don't *a priori* know who is on the Infocoin network. For the same reason, it can't mean some fixed fraction of users in the network. We won't try to make these ideas precise right now. Instead, in the next section I'll point out a serious problem with the approach as described. Fixing that problem will at the same time have the pleasant side effect of making the ideas above much more precise.

Proof-of-work

Suppose Alice wants to double spend in the network-based protocol I just described. She could do this by taking over the Infocoin network. Let's suppose she uses an automated system to set up a large number of separate identities, let's say a billion, on the Infocoin network. As before, she tries to double spend the same infocoin with both Bob and Charlie. But when Bob and Charlie ask the network to validate their respective transactions, Alice's sock puppet identities swamp the network, announcing to Bob that they've validated his transaction, and to Charlie that they've validated his transaction, possibly fooling one or both into accepting the transaction.

There's a clever way of avoiding this problem, using an idea known as *proof-of-work*. The idea is counterintuitive and involves a combination of two ideas: (1) to (artificially) make it *computationally costly* for network users to validate transactions; and (2) to *reward* them for trying to help validate transactions. The reward is used so that people on the network will try to help validate transactions, even though that's now been made a computationally costly process. The benefit of making it costly to validate transactions is that validation can no longer be influenced by the number of network identities someone controls, but only by the total computational power they can bring to bear on validation. As we'll see,

with some clever design we can make it so a cheater would need enormous computational resources to cheat, making it impractical.

That's the gist of proof-of-work. But to really understand proof-of-work, we need to go through the details.

Suppose Alice broadcasts to the network the news that "I, Alice, am giving Bob one infocoin, with serial number 1234567".

As other people on the network hear that message, each adds it to a queue of pending transactions that they've been told about, but which haven't yet been approved by the network. For instance, another network user named David might have the following queue of pending transactions:

I, Tom, am giving Sue one infocoin, with serial number 1201174.

I, Sydney, am giving Cynthia one infocoin, with serial number 1295618.

I, Alice, am giving Bob one infocoin, with serial number 1234567.

David checks his copy of the block chain, and can see that each transaction is valid. He would like to help out by broadcasting news of that validity to the entire network.

However, before doing that, as part of the validation protocol David is required to solve a hard computational puzzle – the proof-of-work. Without the solution to that puzzle, the rest of the network won't accept his validation of the transaction.

What puzzle does David need to solve? To explain that, let h be a fixed hash function known by everyone in the network – it's built into the protocol. Bitcoin uses the well-known SHA-256 hash function, but any cryptographically secure hash function will do. Let's give David's queue of pending transactions a label, l, just so it's got a name we can refer to. Suppose David appends a number x (called the *nonce*) to l and hashes the combination. For example, if we use $l =$ "Hello, world!" (obviously this is not a list of transactions, just a string used for illustrative purposes) and the nonce $x = 0$ then (output is in hexadecimal)

h("Hello, world!0") =

1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

The puzzle David has to solve – the proof-of-work – is to find a nonce x such that when we append x to l and hash the combination the output hash begins with a long run of zeroes. The puzzle can be made more or less difficult by varying the number of zeroes required to solve the puzzle. A relatively simple proof-of-work puzzle might require just three or four zeroes at the start of the hash, while a more difficult proof-of-work puzzle might require a much longer run of zeros, say 15 consecutive zeroes. In either case, the above attempt to find a suitable nonce, with $x = 0$, is a failure, since the output doesn't begin with any zeroes at all. Trying $x = 1$ doesn't work either:

h("Hello, world!1") =

e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

We can keep trying different values for the nonce, $x = 2, 3, \ldots$. Finally, at $x = 4250$ we obtain:

h("Hello, world!4250") =

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

This nonce gives us a string of four zeroes at the beginning of the output of the hash. This will be enough to solve a simple proof-of-work puzzle, but not enough to solve a more difficult proof-of-work puzzle.

What makes this puzzle hard to solve is the fact that the output from a cryptographic hash function behaves like a random number: change the input even a tiny bit and the output from the hash function changes completely, in a way that's hard to predict. So if we want the output hash value to begin with 10 zeroes, say, then David will need, on average, to try $16^{10} \approx 10^{12}$ different values for x before he finds a suitable nonce. That's a pretty challenging task, requiring lots of computational power.

Obviously, it's possible to make this puzzle more or less difficult to solve by requiring more or fewer zeroes in the output from the hash function. In fact, the Bitcoin protocol gets quite a fine level of control over the difficulty of the puzzle, by using a slight variation on the proof-of-work puzzle described above. Instead of requiring leading zeroes, the Bitcoin proof-of-work puzzle requires the hash of a block's header to be lower than or equal to a number known as the target. This target is automatically adjusted to ensure that a Bitcoin block takes, on average, about ten minutes to validate.

(In practice there is a sizeable randomness in how long it takes to validate a block – sometimes a new block is validated in just a minute or two, other times it may take 20 minutes or even longer. It's straightforward to modify the Bitcoin protocol so that the time to validation is much more sharply peaked around ten minutes. Instead of solving a single puzzle, we can require that multiple puzzles be solved; with some careful design it is possible to considerably reduce the variance in the time to validate a block of transactions.)

Alright, let's suppose David is lucky and finds a suitable nonce, x. Celebration! (He'll be rewarded for finding the nonce, as described below). He broadcasts the block of transactions he's approving to the network, together with the value for x. Other participants in the Infocoin network can verify that x is a valid solution to the proof-of-work puzzle. And they then update their block chains to include the new block of transactions.

For the proof-of-work idea to have any chance of succeeding, network users need an incentive to help validate transactions. Without such an incentive, they have no reason to expend valuable computational power, merely to help validate other people's transactions. And if network users are not willing to expend that power, then the whole system won't work. The solution to this problem is to reward people who help validate transactions. In particular, suppose we reward whoever successfully validates a block of transactions by crediting them with some infocoins. Provided the infocoin reward is large enough that will give them an incentive to participate in validation.

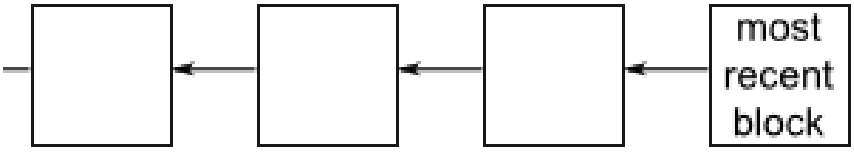
In the Bitcoin protocol, this validation process is called *mining*. For each block of transactions validated, the successful miner receives a bitcoin reward. Initially, this was set to be a 50 bitcoin reward. But for every 210,000 validated blocks (roughly, once every four years) the reward halves. This has happened just once, to date, and so the current reward for mining a block is 25 bitcoins. This halving in the rate will continue every four years until the year 2140 CE. At that point, the reward for mining will drop below 10^{-8} bitcoins per block. 10^{-8} bitcoins is actually the minimal unit of Bitcoin, and is known as

a *satoshi*. So in 2140 CE the total supply of bitcoins will cease to increase. However, that won't eliminate the incentive to help validate transactions. Bitcoin also makes it possible to set aside some currency in a transaction as a *transaction fee*, which goes to the miner who helps validate it. In the early days of Bitcoin transaction fees were mostly set to zero, but as Bitcoin has gained in popularity, transaction fees have gradually risen, and are now a substantial additional incentive on top of the 25 bitcoin reward for mining a block.

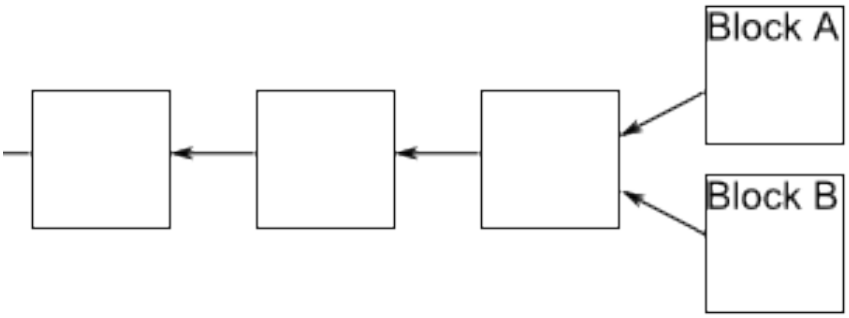
You can think of proof-of-work as a competition to approve transactions. Each entry in the competition costs a little bit of computing power. A miner's chance of winning the competition is (roughly, and with some caveats) equal to the proportion of the total computing power that they control. So, for instance, if a miner controls one percent of the computing power being used to validate Bitcoin transactions, then they have roughly a one percent chance of winning the competition. So provided a lot of computing power is being brought to bear on the competition, a dishonest miner is likely to have only a relatively small chance to corrupt the validation process, unless they expend a huge amount of computing resources.

Of course, while it's encouraging that a dishonest party has only a relatively small chance to corrupt the block chain, that's not enough to give us confidence in the currency. In particular, we haven't yet conclusively addressed the issue of double spending.

I'll analyse double spending shortly. Before doing that, I want to fill in an important detail in the description of Infocoin. We'd ideally like the Infocoin network to agree upon the *order* in which transactions have occurred. If we don't have such an ordering then at any given moment it may not be clear who owns which infocoins. To help do this we'll require that new blocks always include a pointer to the last block validated in the chain, in addition to the list of transactions in the block. (The pointer is actually just a hash of the previous block). So typically the block chain is just a linear chain of blocks of transactions, one after the other, with later blocks each containing a pointer to the immediately prior block:

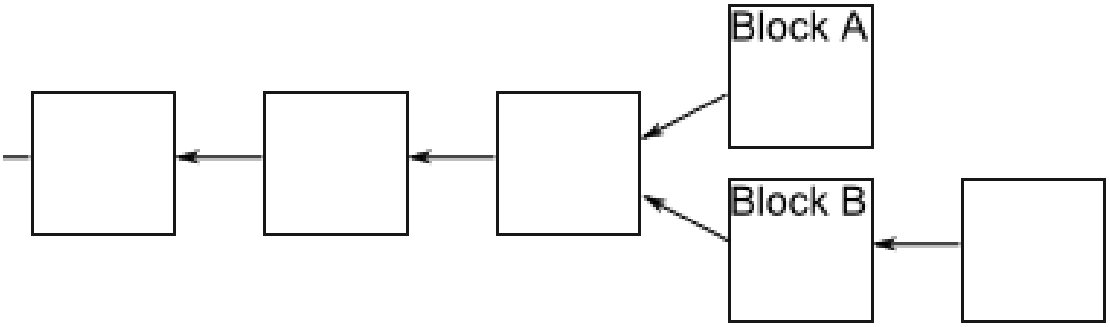


Occasionally, a fork will appear in the block chain. This can happen, for instance, if by chance two miners happen to validate a block of transactions near-simultaneously – both broadcast their newly-validated block out to the network, and some people update their block chain one way, and others update their block chain the other way:



This causes exactly the problem we're trying to avoid – it's no longer clear in what order transactions have occurred, and it may not be clear who owns which infocoins. Fortunately, there's a simple idea that can be used to remove any forks. The rule is this: if a fork occurs, people on the network keep track of both forks. But at any given time, miners only work to extend whichever fork is longest in their copy of the block chain.

Suppose, for example, that we have a fork in which some miners receive block A first, and some miners receive block B first. Those miners who receive block A first will continue mining along that fork, while the others will mine along fork B. Let's suppose that the miners working on fork B are the next to successfully mine a block:



After they receive news that this has happened, the miners working on fork A will notice that fork B is now longer, and will switch to working on that fork. Presto, in short order work on fork A will cease, and everyone will be working on the same linear chain, and block A can be ignored. Of course, any still-pending transactions in A will still be pending in the queues of the miners working on fork B, and so all transactions will eventually be validated.

Likewise, it may be that the miners working on fork A are the first to extend their fork. In that case work on fork B will quickly cease, and again we have a single linear chain.

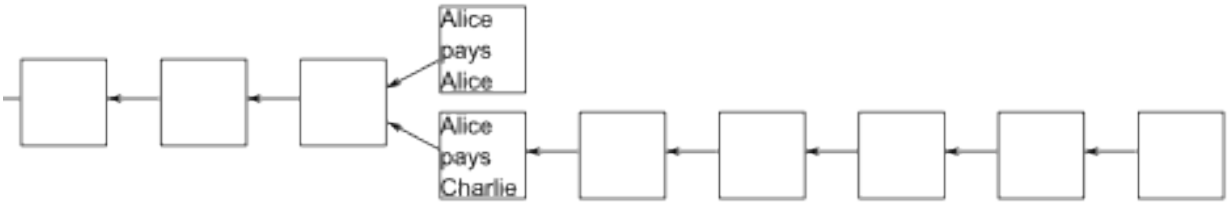
No matter what the outcome, this process ensures that the block chain has an agreed-upon time ordering of the blocks. In Bitcoin proper, a transaction is not considered confirmed until: (1) it is part of a block in the longest fork, and (2) at least 5 blocks follow it in the longest fork. In this case we say that the transaction has "6 confirmations". This gives the network time to come to an agreed-upon the ordering of the blocks. We'll also use this strategy for Infocoin.

With the time-ordering now understood, let's return to think about what happens if a dishonest party tries to double spend. Suppose Alice tries to double spend with Bob and Charlie. One possible approach is for her to try to validate a block that includes both transactions. Assuming she has one percent of the computing power, she will occasionally get lucky and validate the block by solving the proof-of-work. Unfortunately for Alice, the double spending will be immediately spotted by other people in the Infocoin network and rejected, despite solving the proof-of-work problem. So that's not something we need to worry about.

A more serious problem occurs if she broadcasts two separate transactions in which she spends the same infocoin with Bob and Charlie, respectively. She might, for example, broadcast one transaction to a subset of the miners, and the other transaction to another set of miners, hoping to get both transactions validated in this way. Fortunately, in this case, as we've seen, the network will eventually confirm one of these transactions, but not both. So, for instance, Bob's transaction might ultimately be confirmed, in which

case Bob can go ahead confidently. Meanwhile, Charlie will see that his transaction has not been confirmed, and so will decline Alice's offer. So this isn't a problem either. In fact, knowing that this will be the case, there is little reason for Alice to try this in the first place.

An important variant on double spending is if Alice = Bob, i.e., Alice tries to spend a coin with Charlie which she is also "spending" with herself (i.e., giving back to herself). This sounds like it ought to be easy to detect and deal with, but, of course, it's easy on a network to set up multiple identities associated with the same person or organization, so this possibility needs to be considered. In this case, Alice's strategy is to wait until Charlie accepts the infocoin, which happens after the transaction has been confirmed 6 times in the longest chain. She will then attempt to fork the chain before the transaction with Charlie, adding a block which includes a transaction in which she pays herself:



Unfortunately for Alice, it's now very difficult for her to catch up with the longer fork. Other miners won't want to help her out, since they'll be working on the longer fork. And unless Alice is able to solve the proof-of-work at least as fast as everyone else in the network combined – roughly, that means controlling more than fifty percent of the computing power – then she will just keep falling further and further behind. Of course, she might get lucky. We can, for example, imagine a scenario in which Alice controls one percent of the computing power, but happens to get lucky and finds six extra blocks in a row, before the rest of the network has found any extra blocks. In this case, she might be able to get ahead, and get control of the block chain. But this particular event will occur with probability $1/100^6 = 10^{-12}$. A more general analysis along these lines shows that Alice's probability of ever catching up is infinitesimal, unless she is able to solve proof-of-work puzzles at a rate approaching all other miners combined.

Of course, this is not a rigorous security analysis showing that Alice cannot double spend. It's merely an informal plausibility argument. The original paper introducing Bitcoin did not, in fact, contain a rigorous security analysis, only informal arguments along the lines I've presented here. The security community is still analysing Bitcoin, and trying to understand possible vulnerabilities. You can see some of this research listed here, and I mention a few related problems in the "Problems for the author" below. At this point I think it's fair to say that the jury is still out on how secure Bitcoin is.

The proof-of-work and mining ideas give rise to many questions. How much reward is enough to persuade people to mine? How does the change in supply of infocoins affect the Infocoin economy? Will Infocoin mining end up concentrated in the hands of a few, or many? If it's just a few, doesn't that endanger the security of the system? Presumably transaction fees will eventually equilibriate – won't this introduce an unwanted source of friction, and make small transactions less desirable? These are all great questions, but beyond the scope of this post. I may come back to the questions (in the context of Bitcoin) in a future post. For now, we'll stick to our focus on understanding how the Bitcoin protocol works.

Problems for the author

- × I don't understand why double spending can't be prevented in a simpler manner using two-phase commit. Suppose Alice tries to double spend an infocoin with both Bob and Charlie. The idea is that Bob and Charlie would each broadcast their respective messages to the Infocoin network, along with a request: "Should I accept this?" They'd then wait some period – perhaps ten minutes – to hear any naysayers who could prove that Alice was trying to double spend. If no such nays are heard (and provided there are no signs of attempts to disrupt the network), they'd then accept the transaction. This protocol needs to be hardened against network attacks, but it seems to me to be the core of a good alternate idea. How well does this work? What drawbacks and advantages does it have compared to the full Bitcoin protocol?

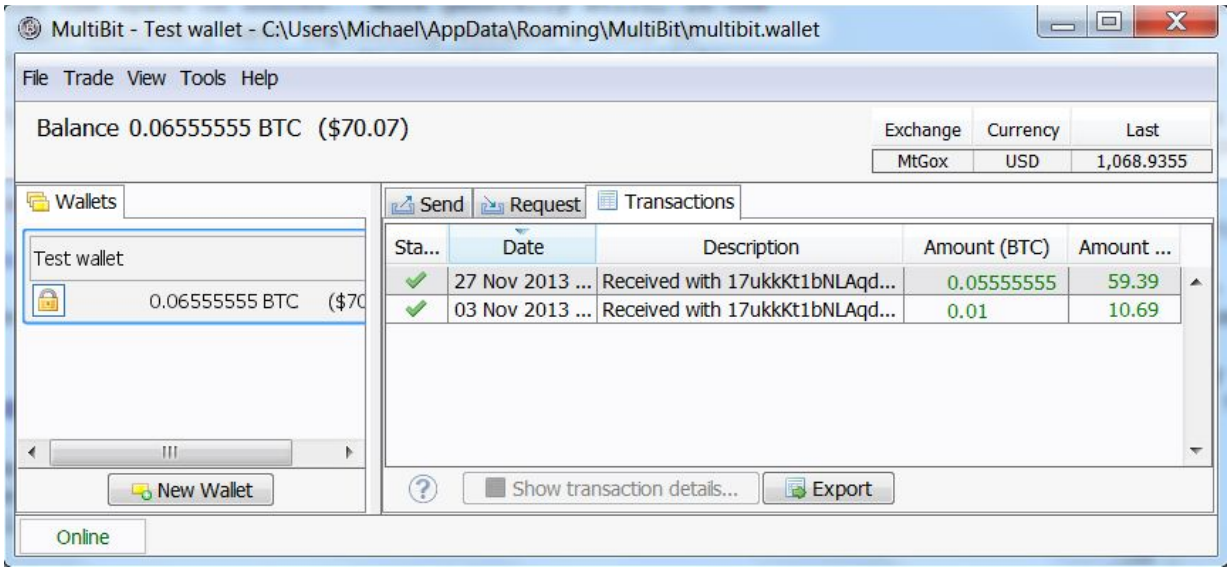
- × Early in the section I mentioned that there is a natural way of reducing the variance in time required to validate a block of transactions. If that variance is reduced too much, then it creates an interesting attack possibility. Suppose Alice tries to fork the chain in such a way that: (a) one fork starts with a block in which Alice pays herself, while the other fork starts with a block in which Alice pays Bob; (b) both blocks are announced nearly simultaneously, so roughly half the miners will attempt to mine each fork; (c) Alice uses her mining power to try to keep the forks of roughly equal length, mining whichever fork is shorter – this is ordinarily hard to pull off, but becomes significantly easier if the standard deviation of the time-to-validation is much shorter than the network latency; (d) after 5 blocks have been mined on both forks, Alice throws her mining power into making it more likely that Charles's transaction is confirmed; and (e) after confirmation of Charles's transaction, she then throws her computational power into the other fork, and attempts to regain the lead. This balancing strategy will have only a small chance of success. But while the probability is small, it will certainly be much larger than in the standard protocol, with high variance in the time to validate a block. Is there a way of avoiding this problem?

- × Suppose Bitcoin mining software always explored nonces starting with $x = 0$, then $x = 1, x = 2, \ldots$. If this is done by all (or even just a substantial fraction) of Bitcoin miners then it creates a vulnerability. Namely, it's possible for someone to improve their odds of solving the proof-of-work merely by starting with some other (much larger) nonce. More generally, it may be possible for attackers to exploit any systematic patterns in the way miners explore the space of nonces. More generally still, in the analysis of this section I have implicitly assumed a kind of symmetry between different miners. In practice, there will be asymmetries and a thorough security analysis will need to account for those asymmetries.

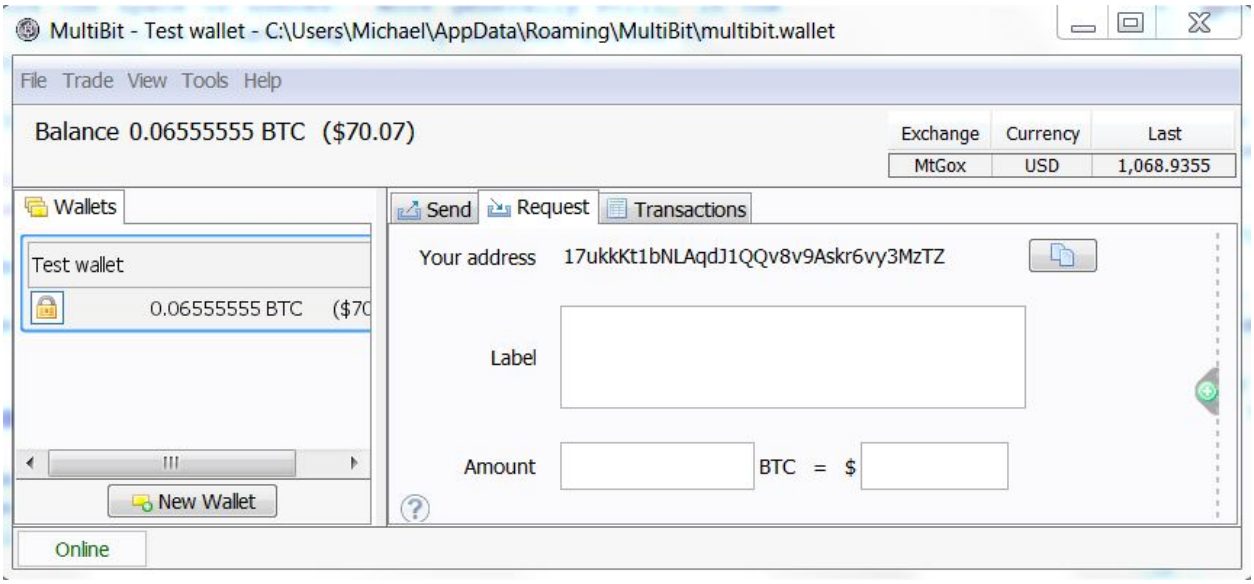
Bitcoin

Let's move away from Infocoin, and describe the actual Bitcoin protocol. There are a few new ideas here, but with one exception (discussed below) they're mostly obvious modifications to Infocoin.

To use Bitcoin in practice, you first install a wallet program on your computer. To give you a sense of what that means, here's a screenshot of a wallet called Multbit. You can see the Bitcoin balance on the left — 0.06555555 Bitcoins, or about 70 dollars at the exchange rate on the day I took this screenshot — and on the right two recent transactions, which deposited those 0.06555555 Bitcoins:



Suppose you're a merchant who has set up an online store, and you've decided to allow people to pay using Bitcoin. What you do is tell your wallet program to generate a *Bitcoin address*. In response, it will generate a public / private key pair, and then hash the public key to form your Bitcoin address:



You then send your Bitcoin address to the person who wants to buy from you. You could do this in email, or even put the address up publicly on a webpage. This is safe, since the address is merely a hash of your public key, which can safely be known by the world anyway. (I'll return later to the question of why the Bitcoin address is a hash, and not just the public key.)

The person who is going to pay you then generates a *transaction*. Let's take a look at the data from an actual transaction transferring 0.31900000 bitcoins. What's shown below is very nearly the raw data. It's changed in three ways: (1) the data has been deserialized; (2) line numbers have been added, for ease of reference; and (3) I've abbreviated various hashes and public keys, just putting in the first six hexadecimal digits of each, when in reality they are much longer. Here's the data:

```
1. {"hash":"7c4025...",
2. "ver":1,
3. "vin_sz":1,
4. "vout_sz":1,
5. "lock_time":0,
6. "size":224,
7. "in":[
8.  {"prev_out":
9.   {"hash":"2007ae...",
10.   "n":0},
11.  "scriptSig":"304502... 042b2d..."}],
12. "out":[
13.  {"value":"0.31900000",
14.  "scriptPubKey":"OP_DUP OP_HASH160 a7db6f OP_EQUALVERIFY OP_CHECKSIG"}]}
```

Let's go through this, line by line.

Line 1 contains the hash of the remainder of the transaction, 7c4025..., expressed in hexadecimal. This is used as an identifier for the transaction.

Line 2 tells us that this is a transaction in version 1 of the Bitcoin protocol.

Lines 3 and 4 tell us that the transaction has one input and one output, respectively. I'll talk below about transactions with more inputs and outputs, and why that's useful.

Line 5 contains the value for lock_time, which can be used to control when a transaction is finalized. For most Bitcoin transactions being carried out today the lock_time is set to 0, which means the transaction is finalized immediately.

Line 6 tells us the size (in bytes) of the transaction. Note that it's not the monetary amount being transferred! That comes later.

Lines 7 through 11 define the input to the transaction. In particular, lines 8 through 10 tell us that the input is to be taken from the output from an earlier transaction, with the given hash, which is expressed in hexadecimal as 2007ae.... The n=0 tells us it's to be the first output from that transaction; we'll see soon how multiple outputs (and inputs) from a transaction work, so don't worry too much about this for now. Line 11 contains the signature of the person sending the money, 304502..., followed by a space, and then the corresponding public key, 04b2d.... Again, these are both in hexadecimal.

One thing to note about the input is that there's nothing explicitly specifying how many bitcoins from the previous transaction should be spent in this transaction. In fact, *all* the bitcoins from the n=0th output of

the previous transaction are spent. So, for example, if the n=0th output of the earlier transaction was 2 bitcoins, then 2 bitcoins will be spent in this transaction. This seems like an inconvenient restriction – like trying to buy bread with a 20 dollar note, and not being able to break the note down. The solution, of course, is to have a mechanism for providing change. This can be done using transactions with multiple inputs and outputs, which we'll discuss in the next section.

Lines 12 through 14 define the output from the transaction. In particular, line 13 tells us the value of the output, 0.319 bitcoins. Line 14 is somewhat complicated. The main thing to note is that the string a7db6f... is the Bitcoin address of the intended recipient of the funds (written in hexadecimal). In fact, Line 14 is actually an expression in Bitcoin's scripting language. I'm not going to describe that language in detail in this post, the important thing to take away now is just that a7db6f... is the Bitcoin address.

You can now see, by the way, how Bitcoin addresses the question I swept under the rug in the last section: where do Bitcoin serial numbers come from? In fact, the role of the serial number is played by transaction hashes. In the transaction above, for example, the recipient is receiving 0.319 Bitcoins, which come out of the first output of an earlier transaction with hash 2007ae... (line 9). If you go and look in the block chain for that transaction, you'd see that its output comes from a still earlier transaction. And so on.

There are two clever things about using transaction hashes instead of serial numbers. First, in Bitcoin there's not really any separate, persistent "coins" at all, just a long series of transactions in the block chain. It's a clever idea to realize that you don't need persistent coins, and can just get by with a ledger of transactions. Second, by operating in this way we remove the need for any central authority issuing serial numbers. Instead, the serial numbers can be self-generated, merely by hashing the transaction.

In fact, it's possible to keep following the chain of transactions further back in history. Ultimately, this process must terminate. This can happen in one of two ways. The first possibilitty is that you'll arrive at the very first Bitcoin transaction, contained in the so-called Genesis block. This is a special transaction, having no inputs, but a 50 Bitcoin output. In other words, this transaction establishes an initial money supply. The Genesis block is treated separately by Bitcoin clients, and I won't get into the details here, although it's along similar lines to the transaction above. You can see the deserialized raw data here, and read about the Genesis block here.

The second possibility when you follow a chain of transactions back in time is that eventually you'll arrive at a so-called *coinbase transaction*. With the exception of the Genesis block, every block of transactions in the block chain starts with a special coinbase transaction. This is the transaction rewarding the miner who validated that block of transactions. It uses a similar but not identical format to the transaction above. I won't go through the format in detail, but if you want to see an example, see here. You can read a little more about coinbase transactions here.

Something I haven't been precise about above is what exactly is being signed by the digital signature in line 11. The obvious thing to do is for the payer to sign the whole transaction (apart from the transaction hash, which, of course, must be generated later). Currently, this is *not* what is done – some pieces of the transaction are omitted. This makes some pieces of the transaction malleable, i.e., they can be changed later. However, this malleability does not include the amounts being paid out, senders and recipients, which can't be changed later. I must admit I haven't dug down into the details here. I gather that this malleability is under discussion in the Bitcoin developer community, and there are efforts afoot to reduce or eliminate this malleability.

Transactions with multiple inputs and outputs

In the last section I described how a transaction with a single input and a single output works. In practice, it's often extremely convenient to create Bitcoin transactions with multiple inputs or multiple outputs. I'll talk below about why this can be useful. But first let's take a look at the data from an actual transaction:


```
{"hash":"993830...",
"ver":1,
"vin_sz":3,
 "vout_sz":2,
 "lock_time":0,
 "size":552,
 "in":[
  {"prev_out":{
    "hash":"3beabc...",
      "n":0},
   "scriptSig":"304402... 04c7d2..."},
  {"prev_out":{
      "hash":"fdae9b...",
      "n":0},
    "scriptSig":"304502... 026e15..."},
  {"prev_out":{
      "hash":"20c86b...",
      "n":1},
    "scriptSig":"304402... 038a52..."}],
 "out":[
  {"value":"0.01068000",
    "scriptPubKey":"OP_DUP OP_HASH160 e8c306... OP_EQUALVERIFY OP_CHECKSIG"},
  {"value":"4.00000000",
    "scriptPubKey":"OP_DUP OP_HASH160 d644e3... OP_EQUALVERIFY
OP_CHECKSIG"}]}
```

Let’s go through the data, line by line. It’s very similar to the single-input-single-output transaction, so I’ll do this pretty quickly.

Line 1 contains the hash of the remainder of the transaction. This is used as an identifier for the transaction.

Line 2 tells us that this is a transaction in version 1 of the Bitcoin protocol.

Lines 3 and 4 tell us that the transaction has three inputs and two outputs, respectively.

Line 5 contains the lock_time. As in the single-input-single-output case this is set to 0, which means the transaction is finalized immediately.

Line 6 tells us the size of the transaction in bytes.

Lines 7 through 19 define a list of the inputs to the transaction. Each corresponds to an output from a previous Bitcoin transaction.

The first input is defined in lines 8 through 11.

In particular, lines 8 through 10 tell us that the input is to be taken from the n=0th output from the transaction with hash 3beabc.... Line 11 contains the signature, followed by a space, and then the public key of the person sending the bitcoins.

Lines 12 through 15 define the second input, with a similar format to lines 8 through 11. And lines 16 through 19 define the third input.

Lines 20 through 24 define a list containing the two outputs from the transaction.

The first output is defined in lines 21 and 22. Line 21 tells us the value of the output, 0.01068000 bitcoins. As before, line 22 is an expression in Bitcoin’s scripting language. The main thing to take away here is that the string e8c30622... is the Bitcoin address of the intended recipient of the funds.

The second output is defined lines 23 and 24, with a similar format to the first output.

One apparent oddity in this description is that although each output has a Bitcoin value associated to it, the inputs do not. Of course, the values of the respective inputs can be found by consulting the corresponding outputs in earlier transactions. In a standard Bitcoin transaction, the sum of all the inputs in the transaction must be at least as much as the sum of all the outputs. (The only exception to this principle is the Genesis block, and in coinbase transactions, both of which add to the overall Bitcoin supply.) If the inputs sum up to more than the outputs, then the excess is used as a *transaction fee*. This is paid to whichever miner successfully validates the block which the current transaction is a part of.

That’s all there is to multiple-input-multiple-output transactions! They’re a pretty simple variation on single-input-single-output-transactions.

One nice application of multiple-input-multiple-output transactions is the idea of *change*. Suppose, for example, that I want to send you 0.15 bitcoins. I can do so by spending money from a previous transaction in which I received 0.2 bitcoins. Of course, I don’t want to send you the entire 0.2 bitcoins. The solution is to send you 0.15 bitcoins, and to send 0.05 bitcoins to a Bitcoin address which I own. Those 0.05 bitcoins are the change. Of course, it differs a little from the change you might receive in a store, since change in this case is what you pay yourself. But the broad idea is similar.

Conclusion

That completes a basic description of the main ideas behind Bitcoin. Of course, I've omitted many details – this isn't a formal specification. But I have described the main ideas behind the most common use cases for Bitcoin.

While the rules of Bitcoin are simple and easy to understand, that doesn't mean that it's easy to understand all the consequences of the rules. There is vastly more that could be said about Bitcoin, and I'll investigate some of these issues in future posts.

For now, though, I'll wrap up by addressing a few loose ends.

How anonymous is Bitcoin? Many people claim that Bitcoin can be used anonymously. This claim has led to the formation of marketplaces such as Silk Road (and various successors), which specialize in illegal goods. However, the claim that Bitcoin is anonymous is a myth. The block chain is public, meaning that it's possible for anyone to see every Bitcoin transaction ever. Although Bitcoin addresses aren't immediately associated to real-world identities, computer scientists have done a great deal of work figuring out how to de-anonymize "anonymous" social networks. The block chain is a marvellous target for these techniques. I will be extremely surprised if the great majority of Bitcoin users are not identified with relatively high confidence and ease in the near future. The confidence won't be high enough to achieve convictions, but will be high enough to identify likely targets. Furthermore, identification will be retrospective, meaning that someone who bought drugs on Silk Road in 2011 will still be identifiable on the basis of the block chain in, say, 2020. These de-anonymization techniques are well known to computer scientists, and, one presumes, therefore to the NSA. I would not be at all surprised if the NSA and other agencies have already de-anonymized many users. It is, in fact, ironic that Bitcoin is often touted as anonymous. It's not. Bitcoin is, instead, perhaps the most open and transparent financial instrument the world has ever seen.

Can you get rich with Bitcoin? Well, maybe. Tim O'Reilly once said: "Money is like gas in the car – you need to pay attention or you'll end up on the side of the road – but a well-lived life is not a tour of gas stations!" Much of the interest in Bitcoin comes from people whose life mission seems to be to find a *really big* gas station. I must admit I find this perplexing. What is, I believe, much more interesting and enjoyable is to think of Bitcoin and other cryptocurrencies as a way of enabling new forms of collective behaviour. That's intellectually fascinating, offers marvellous creative possibilities, is socially valuable, and may just also put some money in the bank. But if money in the bank is your primary concern, then I believe that other strategies are much more likely to succeed.

Details I've omitted: Although this post has described the main ideas behind Bitcoin, there are many details I haven't mentioned. One is a nice space-saving trick used by the protocol, based on a data structure known as a Merkle tree. It's a detail, but a splendid detail, and worth checking out if fun data structures are your thing. You can get an overview in the original Bitcoin paper. Second, I've said little about the Bitcoin network – questions like how the network deals with denial of service attacks, how nodes join and leave the network, and so on. This is a fascinating topic, but it's also something of a mess of details, and so I've omitted it. You can read more about it at some of the links above.

Bitcoin scripting: In this post I've explained Bitcoin as a form of digital, online money. But this is only a small part of a much bigger and more interesting story. As we've seen, every Bitcoin transaction is associated to a script in the Bitcoin programming language. The scripts we've seen in this post describe simple transactions like "Alice gave Bob 10 bitcoins". But the scripting language can also be used to express far more complicated transactions. To put it another way, Bitcoin is *programmable money*. In

later posts I will explain the scripting system, and how it is possible to use Bitcoin scripting as a platform to experiment with all sorts of amazing financial instruments.

Thanks for reading. Enjoy the essay? You can tip me with Bitcoin (!) at address: 17ukkKt1bNLAqdJ1QQv8v9Askr6vy3MzTZ. You may also enjoy the first chapter of my forthcoming book on neural networks and deep learning, and may wish to follow me on Twitter.

Footnote

[1] In the United States the question "Is money a form of speech?" is an important legal question, because of the protection afforded speech under the US Constitution. In my (legally uninformed) opinion digital money may make this issue more complicated. As we'll see, the Bitcoin protocol is really a way of standing up before the rest of the world (or at least the rest of the Bitcoin network) and avowing "I'm going to give such-and-such a number of bitcoins to so-and-so a person" in a way that's extremely difficult to repudiate. At least naively, it looks more like speech than exchanging copper coins, say.

The case for a small allocation to Bitcoin (First published at https://www.kanaandkatana.com/)
March 1, 2019

by Wences Casares, CEO of Xapo

Why most portfolios should allocate up to 1% to Bitcoin

Summary

Bitcoin is a fascinating experiment but it is still just that: an experiment. As such it still has a chance of failing and becoming worthless. In my (subjective) opinion the chances of Bitcoin failing are at least 20%. But after 10 years of working well without interruption, with more than 60 million holders, adding more than 1 million new holders per month and moving more than $1 billion per day worldwide, it has a good chance of succeeding. In my (subjective) opinion those chances of succeeding are at least 50%. If Bitcoin does succeed, 1 Bitcoin may be worth more than $1 million in 7 to 10 years. That is 250 times what it is worth today (at the time of writing the price of Bitcoin is ~ $4,000).

I suggest that a $10 million portfolio should invest at most $100,000 in Bitcoin (up to 1% but not more as the risk of losing this investment is high). If Bitcoin fails, this portfolio will lose at most $100,000 or 1% of its value over 3 to 5 years, which most portfolios can bear. But if Bitcoin succeeds, in 7 to 10 years those $100,000 may be worth more than $25 million, more than twice the value of the entire initial portfolio.

In today's world where every asset seems priced for perfection, it is hard, if not impossible, to find an asset that is so mispriced and where the possible outcomes are so asymmetrical. Bitcoin offers a unique opportunity for a non-material exposure to produce a material outcome.

It would be irresponsible to have an exposure to Bitcoin that one cannot afford to lose because the risk of losing the principal is very real. But it would be almost as irresponsible to not have any exposure at all.

What is interesting about the Bitcoin Blockchain?

Throughout this essay I refer to the "Bitcoin Blockchain" when I am referring to the Bitcoin platform as a whole, including the Bitcoin Blockchain and the Bitcoin currency. Many different systems for different use cases may one day run on top of the Bitcoin Blockchain. When I refer to "Bitcoin" I am referring to Bitcoin the currency, that can be bought, sold, sent, received, held, etc. You can think of the Bitcoin currency as the first system to run on top of the Bitcoin Blockchain.

The current state of the Bitcoin Blockchain is similar to the state of the Internet in 1992. Back then the Internet was very nascent and experimental. Just like with the early days of the Internet there are many bold claims about how the Bitcoin Blockchain will revolutionize the world and solve so many problems. Many of these claims are exaggerated or wrong. Even though right now most of us feel like we do not fully understand the Bitcoin Blockchain, over time we will all understand it as well and as intuitively as we understand the Internet today. You do not need to know the technical underbelly of the Internet to understand The Internet and, similarly, you do not need to know the technical intricacies of the Bitcoin Blockchain to understand it. If the Bitcoin Blockchain succeeds, the investors who develop this understanding and this intuition earlier will have an advantage over the investors that take longer to do so.

Understanding the Bitcoin Blockchain first principles will allow you to form your own judgment about its potential applications without you having to trust any expert. To understand the Bitcoin Blockchain first principles let's understand what changed when the Bitcoin Blockchain first started running in January 2009. All of the Bitcoin Blockchain separate components (Public key cryptography, distributed databases,

open databases, tokens and proof of work) existed many years before Bitcoin went live. What changed when Bitcoin went live? What was new and potentially revolutionary? The only thing that changed, that may potentially be revolutionary, is that all of those components were combined in a new, creative and intelligent way to create the first potentially sovereign computer platform. Up until that moment, all computer platforms belonged to a person, to a company or to a government and those platforms had to obey the will of their owners and the rules of the jurisdiction where they resided. A sovereign only obeys its own rules, no one can impose rules on a sovereign. Kings and Queens used to be sovereign, then nation states became sovereign and now, for the first time, a humble computer platform has the aspiration to be sovereign. That is potentially revolutionary.

The Bitcoin Blockchain is sovereign in that no one can change the transactions that already exist in its database and nobody can keep the system from accepting new transactions.

The main resources securing the Bitcoin Blockchain sovereignty are the Bitcoin miners and the Bitcoin nodes. If my laptop was the only computer mining Bitcoin in the world and it was also the only Bitcoin node in the world, the Bitcoin Blockchain would not be a sovereign platform, anyone who used it would simply be using my platform and trusting me. The Bitcoin miners and the Bitcoin nodes make sure that each transaction is valid, that new bitcoins are not being created out of thin air, etc. The more miners and the more nodes that join the Bitcoin network, the more sovereign the Bitcoin Blockchain is.

In the world of crypto you see the word “decentralized” a lot, often hailed as an end in itself when in reality decentralization is the means by which the Bitcoin Blockchain achieves the end goal of sovereignty.

Today the Bitcoin mining network consumes more than 5 GW of electricity a day which is equal to the total electricity production of the largest hydroelectric dam in the United States. Often this exorbitant electricity consumption is cited as a criticism of Bitcoin because of its environmental impact. I believe those criticisms are misplaced: the Bitcoin Blockchain’s value to society is proportional to its electricity consumption. If the Bitcoin Blockchain did not consume any electricity it would not be sovereign and it would be worthless. Only if you believe that society does not get any value from having a sovereign platform can you be correct to assume that the Bitcoin Blockchain electricity consumption is an enormous waste.

Bitcoin miners secure the Bitcoin Blockchain because they get paid in bitcoins to do so. The Bitcoin Blockchain is secured, to an important degree, by the bitcoins that the miners earn. If you were to remove the bitcoins, most miners would stop mining and, therefore, the Bitcoin Blockchain would not be very robust and not very sovereign. In corporate circles, especially in financial institutions, it has become fashionable to say “I am interested in the Blockchain but not in Bitcoin”, which is the same as saying “I am interested in the web but not interested in the Internet” (remember Intranets?), not understanding that the web could not exist without the Internet. The only innovation of the Blockchain is it’s sovereignty, the only sovereign Blockchain so far is the Bitcoin Blockchain and the fuel that keeps it sovereign is the Bitcoin currency. It is like a boa eating its own tail.

If a group of people wanted to take away the Bitcoin Blockchain sovereignty today they would not only need an extraordinary amount of capital and the capacity to develop specialized mining hardware in very large quantities, but they would also need access to the equivalent of the United States largest hydroelectric dam for an extended period of time. That would be hard to do but not impossible. Every day that goes by it gets even harder to “break” the Bitcoin Blockchain sovereignty. The Bitcoin Blockchain sovereignty has been attacked in the past (in fact, one of those attacks found me on the wrong side of history and that is how I painfully learned many of these lessons, but that’s another story...) and so far it

has always survived intact. We can expect the Bitcoin Blockchain sovereignty to come under attack from more and more resourceful bad actors, coalitions of bad actors or even from nation states eventually. Only time will tell if Bitcoin is truly sovereign or not.

Where can a sovereign platform add value?

It is a lot easier to see where the Bitcoin Blockchain will NOT add any value. For any Blockchain to add value it has to be the ultimate arbiter of truth: nothing has to be able to contest it or change it. For any use case in which the Blockchain information can be contested or changed by a government, by a registrar of deeds, by a court, by the police, by the SEC or by any other authority it does not make sense to use a Blockchain. Claims that the Blockchain can solve property titles, securities settlement, supply chain management, the authenticity of works of art and many other similar cases are misplaced. It is true that the systems that we are using today in all of those cases are old, antiquated and inefficient. And it is true that all of those cases involve many stakeholders that use different data formats and transaction protocols that are often proprietary, but all of those problems would be better solved if those stakeholders agreed to use open standards and if they used better technology. Most often the word “Blockchain” is being waved frantically by consultants who want to scare their corporate customers into buying new technology projects, or by executives at those corporations who do not yet understand the Blockchain but understand that they may get the budget they want if they say their project is using “Blockchain”, or by entrepreneurs who think they are more likely to get the funding or press coverage they want if they add the word “Blockchain” to whatever they are doing.

So, where does a sovereign platform add value? As an example, an identity system may benefit from a sovereign platform. We would rather not keep all of our identity information (full name, social security #, date of birth, name of our parents, name of our spouses and kids, our address, passport information, payment information, etc.) on our phone which can be easily hacked, but we also do not want to give all that information to Google or Facebook or to our government. A sovereign system that no one can corrupt or control that will keep our information safe and will ask us every time someone wants a piece of our information may make sense. With this example we are simply trying to be creative and guess one possible use case, I am sure we will be surprised by creative and revolutionary entrepreneurs coming up with uses cases that take full advantage of a sovereign platform and that we cannot imagine right now.

But there is a use case that makes a lot of sense and, in fact, it is already working quite well. That is to use this sovereign platform to run a global system of value and settlement which is what Bitcoin, the currency, may become. Similar to what gold was for 2,000 years and similar to what the US dollar has been for the last 70 years. Bitcoin is potentially superior to gold and to the US dollar as a global non-political standard of value and settlement because there will never be more than 21 million bitcoins and because Bitcoin is open and uncensorable. There will never be more than 21 million bitcoins because it runs on a sovereign platform so no one can change or inflate that number. Additionally, Bitcoin is uncensorable because it runs on a sovereign platform so no one can change the transactions that already exist in the system and no one can keep the system from accepting new transactions. This allows for unprecedented economic freedom in the same way the internet allowed for unprecedented freedom of information. Gold has the advantage that it is tangible and many people (especially older ones, who tend to have more capital) strongly prefer something that they can touch. Gold also has in its favor that it has been around for over 2,000 years, and it may be impossible for Bitcoin to match that history and reputation. The dollar has the advantage that it is already easily understood and accepted globally and it is a platform with remarkable network effects. These qualities may be too much for Bitcoin to overcome. Or it may be that we collectively come to appreciate the advantages of a digital unit that cannot be inflated or censored. Only time will tell.

Bitcoin is not an asset. It does not produce earnings or dividends and it does not generate interest. And Bitcoin has no intrinsic value. Bitcoin is simply money and most forms of good money have no intrinsic value. Gold, the US dollar and national currencies do not have any intrinsic value either but because they have had a monetary value for a long time most people perceive them as being intrinsically valuable, which is a big advantage. The main hurdle Bitcoin has to clear to become successful is to develop a similar widespread social perception of value and achieving that is quite an ambitious goal.

What does a world in which Bitcoin succeeded look like?

If Bitcoin succeeds it will most likely not replace any national currency. It may be a supranational currency that exists on top of all national currencies. If Bitcoin succeeds it may be a global non-political standard of value and settlement.

The world already has a global non-political standard of measure in the meter, and a global non-political standard of weight in the kilo. Could you imagine a world in which we changed the length of the meter or the weight of the kilo regularly according to political considerations? Yet that is what we are doing with our standard of value. Today we use the US dollar as a global standard of value which is much better than nothing but quite imperfect: it has lost significant value since inception, it is hard to know how many dollars will be outstanding in the future and, increasingly, the ability or inability to use it as a platform depends on political considerations. The world would be much better off with a global non-political standard of value.

The same is true for a global non-political standard of settlement. Only banks can participate in most settlement networks (like SWIFT, Fedwire, ACH in the US, CHAPS in the UK, SEPA in Europe, Visa and Mastercard, etc). Individuals, corporations and governments can only access these settlement networks through banks. Using these settlement networks takes time (sometimes days), the process is opaque and costly and, increasingly, the ability to use them is determined by political considerations. Imagine an open platform where any individual, corporation or government could settle with any other individual, corporation or government anywhere in the world, in real time and for free, 24/7 and 365 days of the year. This would do for money what the Internet did for information.

In a world in which Bitcoin succeeds all currencies may be quoted in satoshis (the smallest fraction of a Bitcoin). When your granddaughter asks what is the price of the New Zealand dollar she may receive an answer in satoshis: the New Zealand dollar is 72 satoshis today. And the price of the Turkish Lira? 21 satoshis today. The US dollar? 107 satoshis today. A barrel of oil? 5,600 satoshis today. Global GDP? 97,356,765 bitcoins. The GDP of Indonesia? 1,417,007 bitcoins. The reserves of the South African Reserve Bank? 53,230 bitcoins. You get the idea. Then all of these values would be easily comparable across time and across geographies.

When your granddaughter asks “Grandpa, how did you guys keep track of all these things when you did not have Bitcoin?” your answer will be “We used the US dollar”. Then she may ask, “Really? But isn’t that the currency of the United States?” after you say yes she may ask “And how did you keep track of the US dollar?” to which you will say “Well… mostly in Euros, sometimes in Yen, Swiss Francs or other currencies depending on what we were talking about”. She may think we were weird.

Why not another cryptocurrency instead of Bitcoin?

There are about 1,000 cryptocurrencies that have at least one transaction a day. So why Bitcoin and not any one of those other ones? Over 60 million people own Bitcoin and over 1 million people become new owners every month. The other 1,000 cryptocurrencies have less than 5 million owners combined, so

Bitcoin will add more users in the next 5 months than those 1,000 cryptocurrencies added in their combined history. Bitcoin is moving over $1 billion a day which is also more than all the other cryptocurrencies combined.

The most important metric of all, though, is how much can we trust these platforms or how sovereign they are. The measure of how sovereign these platforms are is the square of the computing power they have. If we use electricity consumption as a proxy of the computing power each of these platforms have, all of those 1,000 cryptocurrencies combined have less than 1% of the Bitcoin Blockchain processing (mining) power so none of them is (yet) really sovereign and in many cases their code is controlled by a person or a small group of people. New technologies may achieve sovereignty without relying on processing power and that may seriously challenge the Bitcoin Blockchain. But if those technologies do not get developed or it takes too long it may be difficult to unseat the Bitcoin Blockchain.

The Bitcoin Blockchain is a open protocol, not a company. The history of protocols is very different than the history of companies. In the history of companies there is a lot of change, disruption and churn (Microsoft-Apple, eBay-Amazon, Altavista-Google, MySpace-Facebook, etc.). However, the history of protocols is very different. Once a protocol gets established it almost never changes. For example, we are using IP (Internet Protocol, or just "the Internet" colloquially) for almost all transport of data (until the late 90s cisco routers used to route dozens of protocols, today they only route IP). We are using only one web protocol and only one email protocol. The email protocol, for example, is quite lousy. At the protocol level there is no way for me to know if you received my email, much less if you read it, there is no way for you to verify my identity when you receive my email, there is no way to handle spam and many, many other things that could be fixed at the protocol level. I am sure some people have already developed much better email protocols, but we never heard about them and most likely we never will: once a protocol gets established it becomes the only protocol for that use case and it is not possible to displace it with a better protocol. Right now it looks like the standard protocol for a sovereign platform will be the Bitcoin Blockchain.

Many interesting technologies and applications that are being tested with other cryptocurrencies and other Blockchains and, if they are successful, they may be implemented on top of the Bitcoin Blockchain. It is not efficient to invest massive amounts of new hardware and electricity to replicate sovereignty when we already have a most solid and robust sovereign Bitcoin Blockchain. It is more efficient to simply build on top of it. For example, the Bitcoin Blockchain is limited in that it can only process approximately 3,000 transactions every 10 minutes, you have to wait 10 minutes for the transaction to be recorded in the Blockchain and up to 1 hour if you want to make sure it is irreversible. And you have to pay anywhere from 5 cents to 50 cents in transaction fees for the miners to process your transaction. The Lightning Network takes advantage of the robustness of the Bitcoin Blockchain and it works as a "Layer 2" solution on top of the Bitcoin Blockchain, enabling thousands of transactions per second of as little as 1 satoshi ($0.00004), for free and in real time. Similarly, other early examples of Layer 2 solutions that work on top of the Bitcoin Blockchain are RSK which enables the full functionality of Ethereum but on top of the much more robust Bitcoin Blockchain. Liquid is an open source wholesale settlement network developed by Blockstream that operates on top of the Bitcoin Blockchain. There are many more examples of technologies being developed to take advantage of the sovereignty and robustness of the Bitcoin Blockchain and enhance its capabilities by building on top of it.

How can Bitcoin fail?

Bitcoin can fail in many different ways. It could be taken over by a bad actor. It could be displaced by a better platform. It could be hacked. And Bitcoin can probably fail in many ways that we cannot imagine

yet. Because Bitcoin does not have any intrinsic value, and because it's value depends on a social consensus which is a sort of collective delusion, in my opinion, the most likely way in which Bitcoin could fail is a price panic. If we all decide at the same time that we think Bitcoin is worthless, then it will be worthless. It is a self-fulfilled prophecy. If the price of Bitcoin were to plummet to zero or near zero, even if the platform remained intact, its reputation would suffer immensely and it could take a generation to rebuild that credibility. This could happen if people buy amounts of Bitcoin they cannot afford to lose, for example if people invest their retirement funds or their kids' college funds into Bitcoin, and as the price goes does down they are forced to sell, pushing the price further down and forcing others to sell. So, in my opinion, the biggest risk to Bitcoin is people investing amounts they cannot afford to lose.

Most of the capital invested in Bitcoin today seems to be capital that people can afford to lose. That is not because people are wise, or because the regulators have been very effective or that the industry has been prudent. The only reason why most people today do not have an amount of Bitcoin they cannot afford to lose is because of Bitcoin's price volatility. Ironically Bitcoin's price volatility is the best insurance against Bitcoin's biggest risk. If Bitcoin ever begins to be perceived as a safe asset before it has matured and people begin to allocate capital they cannot afford to lose we should be concerned. This happens to some degree during every Bitcoin price rally but, fortunately, so far each rally has corrected without destroying Bitcoin, but one day that could not be the case.

After 10 years of Bitcoin working well without interruption more concerning than a complete failure is a scenario where Bitcoin does not fail but it becomes irrelevant. Something similar to what happened to the BitTorrent protocol, which still exists but is less and less relevant as the real revolution in digital file sharing and entertainment happened through Dropbox, Spotify, Netflix, and many others. Similarly, there is a chance that Bitcoin does not fail but that it never becomes mainstream, that is only used by a group of believers and fanatics but not much more beyond that. That could happen because financial institutions, governments, and regulators manage to keep Bitcoin separate and ostracized from the rest of the financial world, like a non-convertible currency, but it could also happen even if financial institutions, governments, and regulators keep going on their current path of enabling Bitcoin to be fully connected to the financial world. If Bitcoin never becomes mainstream bitcoins will still have a price but most likely lower than what it is today. In my (subjective) opinion the chance of this happening is 30%.

Bitcoin's price action

Bitcoin launched in January 2009 but it did not have a price until July 2010 when it began to to change hands informally at $0.05 cents per bitcoin. In November 2010 Bitcoin had its first price rally that took the price to a peak of $0.39 cents to then "crash" to $0.19 cents. The price was at its peak of $0.39 cents only very briefly and the volume on prices near $0.39 cents was negligible, for most casual observers the rally simply took the price of Bitcoin from $0.05 cents to $0.19 cents, an increase of 280%, but most of the commentary at the time focused on the Bitcoin "crash" of over 50% from $0.39 to $0.19 cents. This exact same story has repeated itself 6 times in Bitcoin's history so far. There have been 6 of these rallies in Bitcoin's 10-year history and in between the rallies the price of Bitcoin has traded sideways or downward for months or years at a time. During most of Bitcoin's 10-year history, the press has been commenting and worrying about Bitcoin's latest "crash". How can something that constantly crashes go from $0.05 cents to $4,000 you ask? If you want something to go from $0.05 cents to $4,000 and fool everybody into believing that it is failing, do it with as much volatility as possible.

The second Bitcoin price rally happened in February 2011 and it took the price of Bitcoin over $1.00 for the first time to then "crash" to $0.68 cents. The third rally happened in August 2011 and it took the price of Bitcoin to $29 to then "crash" to $2. The fourth rally happened in April 2013 and it took the price to

$230 to then “crash” to $66. The fifth rally happened in December 2013 and it took the price to $1,147 to then “crash” to $177. The 6th (and currently last) rally happened in December 2017 and it took the price of Bitcoin to $19,783 to then “crash” below $3,200 (and until this bear market is over we don’t know how low it may go).

The Bitcoin price rallies are the most important feature of how Bitcoin propagates, how people spread the word and how more people want to own it. It is a risky mechanism, so far it has worked well but it could lead to a disaster one day. The Bitcoin price rallies are Bitcoin’s best moments but they are also it most dangerous and vulnerable moments.

Every Bitcoin bear market is about working out the excesses of the rally. During the rally too many people buy too many bitcoins thinking that they will be able to sell them for a big gain very soon and that usually does not happen. Imagine a fruit tree that has some good fruit and some rotten fruit. The Bitcoin bear markets resembles a period in which the tree is shaken until all the rotten fruit has fallen to the ground. Every time the tree is shaken some rotten fruit falls to the ground. The Bitcoin tree is shaken by the price going down and by letting time pass by. The more the price goes down and the more time passes without another rally the more people give up their original expectations, they sell, they adjust their exposure and their expectations. Eventually, no matter how much you shake the tree there is no more fruit to fall to the ground and the market may be getting ready for another rally.

If Bitcoin succeeds it is likely that the price will do another 6 of these rallies over the next 7 to 10 years. Anyone who tells you that they know what the price of Bitcoin will be next week, much less next year is either ignorant or outright lying to you. It is not possible to know when the price will hit bottom or when the next rally will come and the penalty for trying to time the bottom or the top and getting it wrong can be much higher than the money you were trying to save. If you decide to buy Bitcoin simply decide what is the amount of money you can afford to lose (ideally less than 1% of your net worth), deploy it at market and at once and forget about it for 7 to 10 years. I have been giving this advice for 6 years and, by watching what people do with this advice, I can tell you that “Forget about it for 7 to 10 years” is the most difficult part of the simple recipe I am proposing. This lack of discipline destroys a lot more value than you would anticipate. The price volatility rattles people and makes them trade. If the price goes down a lot they want to buy more to reduce their average their cost, they buy more and now they have more than they can afford to lose so they care even more about the price volatility. Even worse: when the price goes up 10 times they decide to sell to rebalance because now Bitcoin represents too much of their net worth and it is too risky (it is hard to double your portfolio with a 1% exposure if you rebalance it every time it multiplies by 10). If you think this may happen to you, I suggest you invest in two buckets: keep one bucket that you will not trade for 7 to 10 years, and another bucket that you will trade as much as you want (but be responsible and be sure that both buckets combined add to an amount then you can afford to lose).

Why do I believe 1 Bitcoin may be worth $1 million in 7 to 10 years?

How much a Bitcoin may be worth if Bitcoin succeeds is pure speculation. Today Bitcoin is worth a total of ~ $70 billion (~ 17.5 million bitcoins in circulation x ~ $4,000 per Bitcoin). If Bitcoin ever becomes the world’s standard of value and settlement it may have to be worth more than gold and less than the world’s narrow supply of money. All the gold that was ever been mined is worth ~ $7 trillion the world’s narrow supply of money is ~ $40 trillion. If Bitcoin is ever worth as much as gold each Bitcoin would be worth ~ $300,000, and if Bitcoin is ever worth as much as the world’s narrow supply of money it would be worth ~ $2 million.

My preferred way of guessing how the price of Bitcoin may evolve is much more prosaic. I have noticed over time that the price of Bitcoin fluctuates around ~ $7,000 x how many people own bitcoins. So if that constant maintains and if 3 billion people ever own Bitcoin it would be worth ~ $21 trillion (~ $7,000 x 3 billion) or $1 million per Bitcoin.

In closing

This essay is focused on making the case for a small allocation to Bitcoin and, therefore, it focuses on the possible financial gain to be had if Bitcoin succeeds. But if Bitcoin does for Money what the Internet did for information the prospect of unprecedented economic freedom is much more exciting than any possible financial gain.

I grew up in Patagonia, Argentina, where my parents are sheep ranchers. Growing up I saw my family lose their entire savings three times: the first time because of an enormous devaluation, the second time because of hyperinflation and the last time because the government confiscated all bank deposits. It seemed like every time we were recovering, a new and different economic storm would wipe us out again. My memory of these events is not economic or financial but very emotional. I remember my parents fighting about money, I remember being scared, I remember everybody around us being scared and returning to desperate, almost animal like behavior. I also remember thinking how unfair it was that these crises hit the poor the hardest. People who had enough money to get some US dollars protected themselves that way, people who had even more money and could afford to buy a house or apartment protected themselves that way, and people who had even more money and could have a bank account abroad protected themselves that way. But the poor could not do any of those things and got hit the hardest. When I saw the emergence of the Internet I was young and idealistic and I sincerely thought the Internet was going to democratize money and fix money forever. But it has been 30 years since the Internet was created and it has fixed many problems but increasing economic freedom is not one of them. I was about to give up hope for the Internet to fix this problem when I ran into Bitcoin by accident. At first I was very cynical but the more I learned about it the more curious I became, after six months of studying and using Bitcoin I decided to dedicate the rest of my career, my capital and my reputation to help Bitcoin succeed. Nothing would make me prouder than to be able to tell my grandkids that I was part one of a very large community who helped Bitcoin succeed. And that because Bitcoin succeeded now billions of people can safely send, receive and store any form of money they want as easily as they can send or store a picture. So that what I saw happen to my parents and countless others can never happen again.

Further reading:

➔ "Shelling Out: The Origins of Money" by Nick Szabo. Essential background on the nature of money.

➔ "An (Institutional) Investor's Take on Cryptoassets" by John Pfeffer. Bitcoin analysis from an investor's perspective

➔ "The Bitcoin Standard" by Saifedean Ammous. Non technical explanation of Bitcoin and what it may become.

➔ "Mastering Bitcoin" by Andreas Antonopoulos. Technical explanation of Bitcoin for non-technical people.

➔ "Programming Bitcoin" book by Jimmy Song. Technical explanation of Bitcoin for technical people and programming guide.

Investor Theses

Why Bitcoin Matters (https://a16z.com/)
January 22, 2014

by Marc Andreessen

The Great Monetary Inflation
May 7, 2020

by Paul Tudor Jones and Lorenzo Giorgianni

An (Institutional) Investor's Take on Cryptoassets
December 24, 2017

by John Pfeffer

If you think I'm missing any major essays/papers, shoot me an email at kevin@12mv2.com or a dm on Twitter @kgao1412 with the subject: "Bitcoin Compilation." Thanks!

Why Bitcoin Matters (First published at https://a16z.com/)
January 22, 2014

by Marc Andreessen

This article was originally published in The New York Times on January 21, 2014.

NYT editor's note: Marc Andreessen's venture capital firm, Andreessen Horowitz, has invested just under $50 million in Bitcoin-related start-ups. The firm is actively searching for more Bitcoin-based investment opportunities. He does not personally own more than a de minimis amount of Bitcoin.

A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers.

Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it.

On the other hand, technologists –- nerds — are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it.

Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start.

What technology am I talking about? Personal computers in 1975, the Internet in 1993, and — I believe — Bitcoin in 2014.

One can hardly accuse Bitcoin of being an uncovered topic, yet the gulf between what the press and many regular people believe Bitcoin is, and what a growing critical mass of technologists believe Bitcoin is, remains enormous. In this post, I will explain why Bitcoin has so many Silicon Valley programmers and entrepreneurs all lathered up, and what I think Bitcoin's future potential is.

First, Bitcoin at its most fundamental level is a breakthrough in computer science – one that builds on 20 years of research into cryptographic currency, and 40 years of research in cryptography, by thousands of researchers around the world.

Bitcoin is the first practical solution to a longstanding problem in computer science called the Byzantine Generals Problem. To quote from the original paper defining the B.G.P.: "[Imagine] a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement."

More generally, the B.G.P. poses the question of how to establish trust between otherwise unrelated parties over an untrusted network like the Internet.

The practical consequence of solving this problem is that Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.

What kinds of digital property might be transferred in this way? Think about digital signatures, digital contracts, digital keys (to physical locks, or to online lockers), digital ownership of physical assets such as cars and houses, digital stocks and bonds … and digital money.

All these are exchanged through a distributed network of trust that does not require or rely upon a central intermediary like a bank or broker. And all in a way where only the owner of an asset can send it, only the intended recipient can receive it, the asset can only exist in one place at a time, and everyone can validate transactions and ownership of all assets anytime they want.

How does this work?

Bitcoin is an Internet-wide distributed ledger. You buy into the ledger by purchasing one of a fixed number of slots, either with cash or by selling a product and service for Bitcoin. You sell out of the ledger by trading your Bitcoin to someone else who wants to buy into the ledger. Anyone in the world can buy into or sell out of the ledger any time they want – with no approval needed, and with no or very low fees. The Bitcoin "coins" themselves are simply slots in the ledger, analogous in some ways to seats on a stock exchange, except much more broadly applicable to real world transactions.

The Bitcoin ledger is a new kind of payment system. Anyone in the world can pay anyone else in the world any amount of value of Bitcoin by simply transferring ownership of the corresponding slot in the ledger. Put value in, transfer it, the recipient gets value out, no authorization required, and in many cases, no fees.

That last part is enormously important. Bitcoin is the first Internetwide payment system where transactions either happen with no fees or very low fees (down to fractions of pennies). Existing payment systems charge fees of about 2 to 3 percent – and that's in the developed world. In lots of other places, there either are no modern payment systems or the rates are significantly higher. We'll come back to that.

Bitcoin is a digital bearer instrument. It is a way to exchange money or assets between parties with no pre-existing trust: A string of numbers is sent over email or text message in the simplest case. The sender doesn't need to know or trust the receiver or vice versa. Related, there are no chargebacks — this is the part that is literally like cash – if you have the money or the asset, you can pay with it; if you don't, you can't. This is brand new. This has never existed in digital form before.

Bitcoin is a digital currency, whose value is based directly on two things: use of the payment system today – volume and velocity of payments running through the ledger – and speculation on future use of the payment system. This is one part that is confusing people. It's not as much that the Bitcoin currency has some arbitrary value and then people are trading with it; it's more that people can trade with Bitcoin (anywhere, everywhere, with no fraud and no or very low fees) and as a result it has value.

It is perhaps true right at this moment that the value of Bitcoin currency is based more on speculation than actual payment volume, but it is equally true that that speculation is establishing a sufficiently high price for the currency that payments have become practically possible. The Bitcoin currency had to be worth something before it could bear any amount of real-world payment volume. This is the classic "chicken and egg" problem with new technology: new technology is not worth much until it's worth a lot. And so the fact that Bitcoin has risen in value in part because of speculation is making the reality of its usefulness arrive much faster than it would have otherwise.

Critics of Bitcoin point to limited usage by ordinary consumers and merchants, but that same criticism was leveled against PCs and the Internet at the same stage. Every day, more and more consumers and merchants are buying, using and selling Bitcoin, all around the world. The overall numbers are still small, but they are growing quickly. And ease of use for all participants is rapidly increasing as Bitcoin tools and technologies are improved. Remember, it used to be technically challenging to even get on the Internet. Now it's not.

The criticism that merchants will not accept Bitcoin because of its volatility is also incorrect. Bitcoin can be used entirely as a payment system; merchants do not need to hold any Bitcoin currency or be exposed to Bitcoin volatility at any time. Any consumer or merchant can trade in and out of Bitcoin and other currencies any time they want.

Why would any merchant — online or in the real world — want to accept Bitcoin as payment, given the currently small number of consumers who want to pay with it? My partner Chris Dixon recently gave this example:

"Let's say you sell electronics online. Profit margins in those businesses are usually under 5 percent, which means conventional 2.5 percent payment fees consume half the margin. That's money that could be reinvested in the business, passed back to consumers or taxed by the government. Of all of those choices, handing 2.5 percent to banks to move bits around the Internet is the worst possible choice. Another challenge merchants have with payments is accepting international payments. If you are wondering why your favorite product or service isn't available in your country, the answer is often payments."

In addition, merchants are highly attracted to Bitcoin because it eliminates the risk of credit card fraud. This is the form of fraud that motivates so many criminals to put so much work into stealing personal customer information and credit card numbers.

Since Bitcoin is a digital bearer instrument, the receiver of a payment does not get any information from the sender that can be used to steal money from the sender in the future, either by that merchant or by a criminal who steals that information from the merchant.

Credit card fraud is such a big deal for merchants, credit card processors and banks that online fraud detection systems are hair-trigger wired to stop transactions that look even slightly suspicious, whether or not they are actually fraudulent. As a result, many online merchants are forced to turn away 5 to 10 percent of incoming orders that they could take without fear if the customers were paying with Bitcoin, where such fraud would not be possible. Since these are orders that were coming in already, they are inherently the highest margin orders a merchant can get, and so being able to take them will drastically increase many merchants' profit margins.

Bitcoin's antifraud properties even extend into the physical world of retail stores and shoppers.

For example, with Bitcoin, the huge hack that recently stole 70 million consumers' credit card information from the Target department store chain would not have been possible. Here's how that would work:

You fill your cart and go to the checkout station like you do now. But instead of handing over your credit card to pay, you pull out your smartphone and take a snapshot of a QR code displayed by the cash register. The QR code contains all the information required for you to send Bitcoin to Target, including the amount. You click "Confirm" on your phone and the transaction is done (including converting dollars from your account into Bitcoin, if you did not own any Bitcoin).

Target is happy because it has the money in the form of Bitcoin, which it can immediately turn into dollars if it wants, and it paid no or very low payment processing fees; you are happy because there is no way for hackers to steal any of your personal information; and organized crime is unhappy. (Well, maybe criminals are still happy: They can try to steal money directly from poorly-secured merchant computer systems. But even if they succeed, consumers bear no risk of loss, fraud or identity theft.)

Finally, I'd like to address the claim made by some critics that Bitcoin is a haven for bad behavior, for criminals and terrorists to transfer money anonymously with impunity. This is a myth, fostered mostly by sensationalistic press coverage and an incomplete understanding of the technology. Much like email, which is quite traceable, Bitcoin is pseudonymous, not anonymous. Further, every transaction in the Bitcoin network is tracked and logged forever in the Bitcoin blockchain, or permanent record, available for all to see. As a result, Bitcoin is considerably easier for law enforcement to trace than cash, gold or diamonds.

What's the future of Bitcoin?

Bitcoin is a classic network effect, a positive feedback loop. The more people who use Bitcoin, the more valuable Bitcoin is for everyone who uses it, and the higher the incentive for the next user to start using the technology. Bitcoin shares this network effect property with the telephone system, the web, and popular Internet services like eBay and Facebook.

In fact, Bitcoin is a four-sided network effect. There are four constituencies that participate in expanding the value of Bitcoin as a consequence of their own self-interested participation. Those constituencies are (1) consumers who pay with Bitcoin, (2) merchants who accept Bitcoin, (3) "miners" who run the computers that process and validate all the transactions and enable the distributed trust network to exist, and (4) developers and entrepreneurs who are building new products and services with and on top of Bitcoin.

All four sides of the network effect are playing a valuable part in expanding the value of the overall system, but the fourth is particularly important.

All over Silicon Valley and around the world, many thousands of programmers are using Bitcoin as a building block for a kaleidoscope of new product and service ideas that were not possible before. And at our venture capital firm, Andreessen Horowitz, we are seeing a rapidly increasing number of outstanding entrepreneurs – not a few with highly respected track records in the financial industry – building companies on top of Bitcoin.

For this reason alone, new challengers to Bitcoin face a hard uphill battle. If something is to displace Bitcoin now, it will have to have sizable improvements and it will have to happen quickly. Otherwise, this network effect will carry Bitcoin to dominance.

One immediately obvious and enormous area for Bitcoin-based innovation is international remittance. Every day, hundreds of millions of low-income people go to work in hard jobs in foreign countries to make money to send back to their families in their home countries – over $400 billion in total annually, according to the World Bank. Every day, banks and payment companies extract mind-boggling fees, up to 10 percent and sometimes even higher, to send this money.

Switching to Bitcoin, which charges no or very low fees, for these remittance payments will therefore raise the quality of life of migrant workers and their families significantly. In fact, it is hard to think of any one thing that would have a faster and more positive effect on so many people in the world's poorest countries.

Moreover, Bitcoin generally can be a powerful force to bring a much larger number of people around the world into the modern economic system. Only about 20 countries around the world have what we would consider to be fully modern banking and payment systems; the other roughly 175 have a long way to go. As a result, many people in many countries are excluded from products and services that we in the West take for granted. Even Netflix, a completely virtual service, is only available in about 40 countries.

Bitcoin, as a global payment system anyone can use from anywhere at any time, can be a powerful catalyst to extend the benefits of the modern economic system to virtually everyone on the planet.

And even here in the United States, a long-recognized problem is the extremely high fees that the "unbanked" — people without conventional bank accounts — pay for even basic financial services. Bitcoin can be used to go straight at that problem, by making it easy to offer extremely low-fee services to people outside of the traditional financial system.

A third fascinating use case for Bitcoin is micropayments, or ultrasmall payments. Micropayments have never been feasible, despite 20 years of attempts, because it is not cost effective to run small payments (think $1 and below, down to pennies or fractions of a penny) through the existing credit/debit and banking systems. The fee structure of those systems makes that nonviable.

All of a sudden, with Bitcoin, that's trivially easy. Bitcoins have the nifty property of infinite divisibility: currently down to eight decimal places after the dot, but more in the future. So you can specify an arbitrarily small amount of money, like a thousandth of a penny, and send it to anyone in the world for free or near-free.

Think about content monetization, for example. One reason media businesses such as newspapers struggle to charge for content is because they need to charge either all (pay the entire subscription fee for all the content) or nothing (which then results in all those terrible banner ads everywhere on the web). All of a sudden, with Bitcoin, there is an economically viable way to charge arbitrarily small amounts of money per article, or per section, or per hour, or per video play, or per archive access, or per news alert.

Another potential use of Bitcoin micropayments is to fight spam. Future email systems and social networks could refuse to accept incoming messages unless they were accompanied with tiny amounts of Bitcoin — tiny enough to not matter to the sender, but large enough to deter spammers, who today can send uncounted billions of spam messages for free with impunity.

Finally, a fourth interesting use case is public payments. This idea first came to my attention in a news article a few months ago. A random spectator at a televised sports event held up a placard with a QR code and the text "Send me Bitcoin!" He received $25,000 in Bitcoin in the first 24 hours, all from people he had never met. This was the first time in history that you could see someone holding up a sign, in person or on TV or in a photo, and then send them money with two clicks on your smartphone: take the photo of the QR code on the sign, and click to send the money.

Think about the implications for protest movements. Today protesters want to get on TV so people learn about their cause. Tomorrow they'll want to get on TV because that's how they'll raise money, by literally holding up signs that let people anywhere in the world who sympathize with them send them money on the spot. Bitcoin is a financial technology dream come true for even the most hardened anticapitalist political organizer.

The coming years will be a period of great drama and excitement revolving around this new technology.

For example, some prominent economists are deeply skeptical of Bitcoin, even though Ben S. Bernanke, formerly Federal Reserve chairman, recently wrote that digital currencies like Bitcoin "may hold long-term promise, particularly if they promote a faster, more secure and more efficient payment system." And in 1999, the legendary economist Milton Friedman said: "One thing that's missing but will soon be developed is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A – the way I can take a $20 bill and hand it over to you, and you may get that without knowing who I am."

Economists who attack Bitcoin today might be correct, but I'm with Ben and Milton.

Further, there is no shortage of regulatory topics and issues that will have to be addressed, since almost no country's regulatory framework for banking and payments anticipated a technology like Bitcoin.

But I hope that I have given you a sense of the enormous promise of Bitcoin. Far from a mere libertarian fairy tale or a simple Silicon Valley exercise in hype, Bitcoin offers a sweeping vista of opportunity to reimagine how the financial system can and should work in the Internet era, and a catalyst to reshape that system in ways that are more powerful for individuals and businesses alike.

MARKET OUTLOOK – MACRO PERSPECTIVE

Paul Jones & Lorenzo Giorgianni

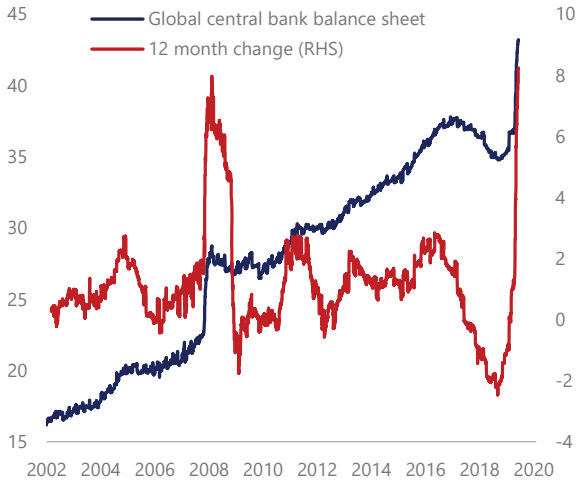
THE GREAT MONETARY INFLATION

COVID-19 is a one-of-a-kind virus that has triggered a one-of-a-kind policy response globally.

The depth and magnitude of the economic drop-off took modern monetary theory—or the direct monetization of massive fiscal spending—from the theoretical to practice without any debate. It has happened globally with such speed that even a market veteran like myself was left speechless. Just since February, a global total of $3.9 trillion (6.6% of global GDP) has been magically created through quantitative easing. We are witnessing the Great Monetary Inflation (GMI)—an unprecedented expansion of every form of money unlike anything the developed world has ever seen.

Global Central Bank Balance Sheet 1/

% GDP; Source: Haver and Bloomberg

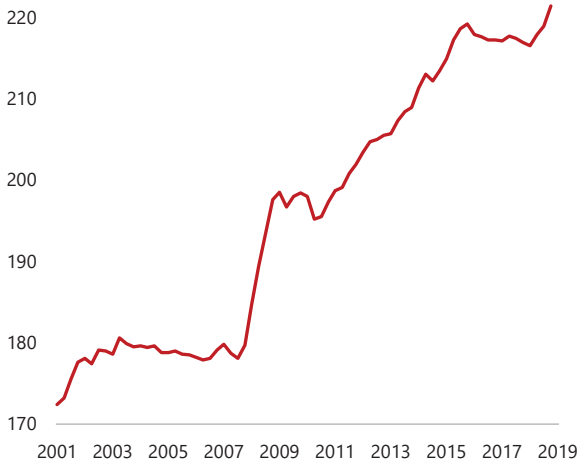


1/ Total assets of the Federal Reserve Bank, European Central Bank, Bank of Japan, Bank of England, Swiss National Bank, Reserve Bank of Australia, Bank of Canada and the People's Bank of China scaled by the aggregate GDP of these countries in current dollars.

Global debt of nonfinancial sector

Credit to corporates, households and governments from all sectors

% GDP at PPP exchange rates; Source: BIS

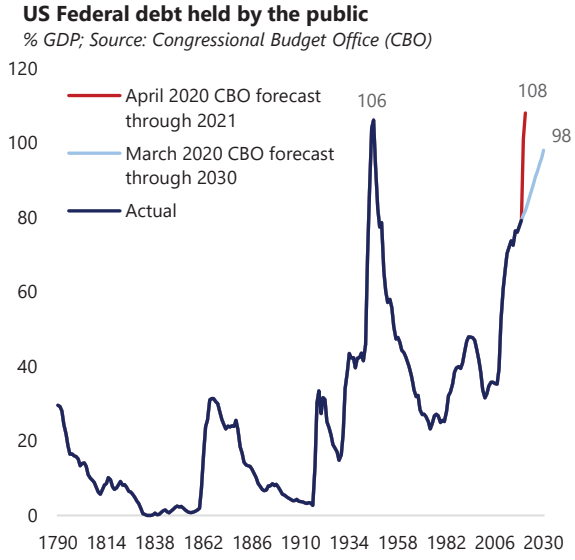


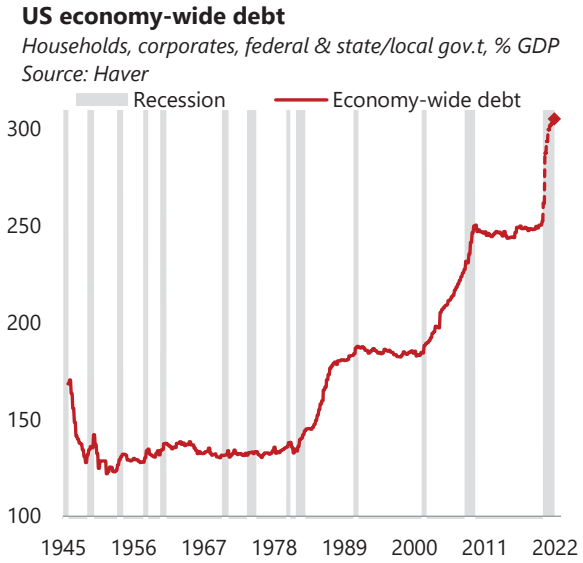
Global debt was very elevated entering the pandemic, and this monetary expansion is funding additional large debt creation, for now, without provoking the disciplining response of rising market yields. So far, the result has been asset price reflation. A large demand shortfall will prevent goods and services inflation from rising in the short term. The question is whether that will be the case in the long term with a central bank whose central focus will be repairing the worst employment crisis since the Great Depression.

One thing is for sure, there will be many assets that will move as a result of this money creation. So what is an investor to do? Traditional hedges like gold have done well, and we expect investors to continue to seek refuge in this safe asset. One thing I have learned over time is the best thing to do is let market price action guide your decision-making and then try to understand the fundamentals as they become more evident and comprehensible. Quite often, how the markets respond will be at odds with your priors. But remember, the P&L always wins in the long run. With that in mind, in a world that craves new safe assets, there may be a growing role for Bitcoin.

Debt Addiction

What is apparent to all is the global ramp-up in debt from every sector to deal with the economic downturn. In addition to debt ratios increasing by virtue of a larger numerator, such ratios will also be buoyed by a falling denominator: it may take more than two years to bring nominal GDP back to its pre-shock level. The Congressional Budget Office, for example, projects the US government debt ratio to reach a new historic high next year, above the World War II peak. Corporate debt is also rising briskly to record levels as firms draw down revolving credit lines to self-fund cash flow shortfalls. At this pace, it is not inconceivable that the economy-wide debt ratio may increase by 50% of GDP over the next year and a half.

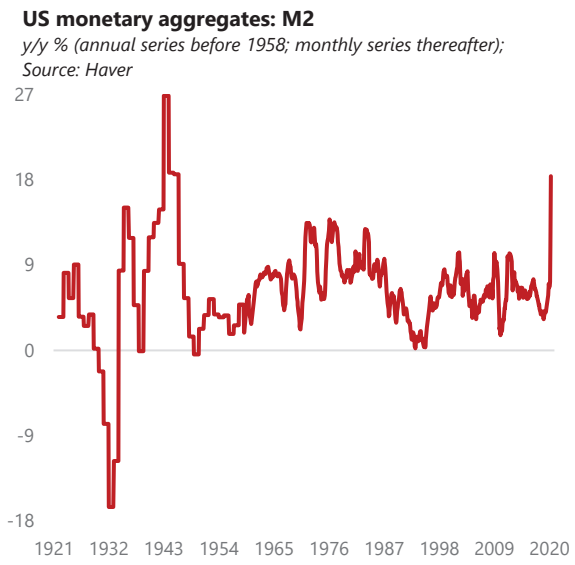




Money Printing is a Hard Habit to Kick

Central banks are on the hook to help fund this debt increase. Since the end of February, the Fed's balance sheet has already grown by 60% and is on track to more than double by the end of the year. Even two QE novice central banks have unleashed their printing presses. The Bank of Canada has already tripled its balance sheet, and the Reserve Bank of Australia has allowed its balance sheet to increase by 43%.

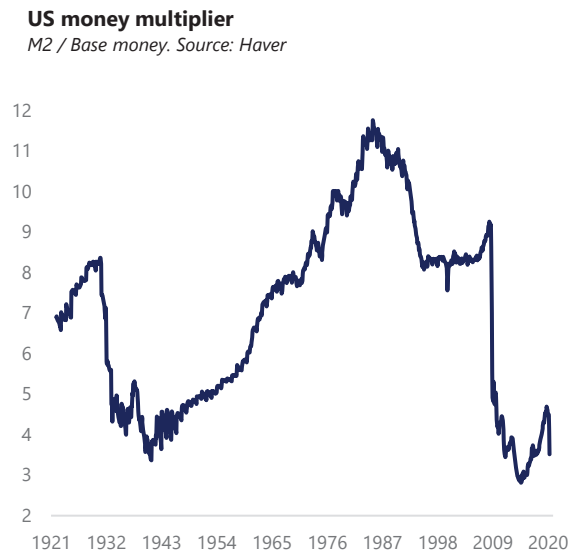
The counterpart of this rapid central bank balance sheet expansion has been a sharp increase in monetary aggregates. In the last weekly release of the Fed's Money Stock data, M2 rose 18.5% over a year ago, an unprecedented pace of growth in the history of the weekly time series starting from 1981. It is likely that the annual growth in M2 will continue to increase to somewhere between 20% and 40% by year-end. We got these estimates on M2 from a few of the dinosaurs who still work on Wall Street. Rarely have we ever seen so many economists dismissive of an economic metric than when we asked about their notion on this record M2 growth and its meaning. The last time M2 grew at such a high pace was during World War II, when annual M2 growth peaked at almost 27%.

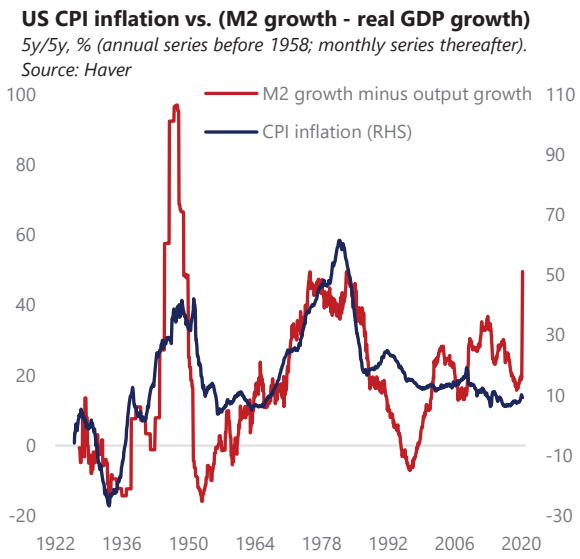


But, monetary expansion alone is not sufficient to generate inflation. The context is very important too. Take Japan, the poster child of debt-deflation. Arguably, this is a case where monetary financing of the deficit has been ineffective. But, Japan was already in a prolonged deflationary spiral that had unanchored inflation expectations when this policy was unleashed in full. In any event, since 1999, their M2 never grew by more than 5% a year. A hobbled banking system focused on healing from a prolonged banking crisis had probably a lot to do with this. In the US, it can also be argued that a large deficit combined with massive money printing were ineffectual at stoking inflation in the aftermath of the Global Financial Crisis (GFC).

Again, context matters, and the post-pandemic recovery may be different from the GFC aftermath. First, an austerity movement similar to the one that swept the Tea Party to prominence in the 2010 US mid-term elections is very unlikely to emerge. The opposite forces are at play today as growing income inequality breeds populism. Second, the bank-centric GFC induced a one-time paradigm shift in banks' preference for liquidity, later enforced through regulatory changes. As a result, only a small share of the Fed's massive injection of high-powered money was re-lent in the banking system: M2 never grew by more than 10% a year even after subsequent rounds of large-scale asset purchases by the Fed. Effectively, banks' preference for liquidity and the need to rebuild their capital cushions quashed the money multiplier. While the multiplier has recently started to fall—in a crisis, banks are wary to lend to potentially insolvent borrowers and, in fact, start building provisions for loan losses—this time banks entered the crisis in a stronger footing and policy is more squarely aimed at putting liquidity directly in the hands of businesses and households shielding, to some extent, banks from losses. As such, the chance of a large fall in the multiplier as seen in the aftermath of the GFC is now smaller. Plus, the Fed's elimination of the reserve requirement means that the theoretical money multiplier is now infinite (the multiplier is the inverse of the reserve requirement).

Milton Friedman famously stated that "inflation is always and everywhere a monetary phenomenon that arises from a more rapid expansion in the quantity of money than in total output." And while the relationship between inflation and M2 growth in excess of real output growth has not been stable over short horizons, it seems to hold over longer horizons. There are only a few times in history when M2 growth exceeded real output growth over a 5-year span by the same or a faster pace than is currently the case: the inflationary periods of the 1970s–80s and the late 1940s. But remember, it is reasonable to expect inflation to first fall in the coming months, given the large contraction in demand relative to supply.





The issue is whether a large monetary overhang in the recovery phase will eventually stoke consumer price inflation.

To answer this question, we need to ask, how reasonable is it to expect that in the recovery phase the Fed will be able to deliver an increase in interest rates of a magnitude sufficient to suck back the money it so easily printed during the downswing? The current Fed leadership has made it a centerpiece of its new monetary policy framework to do whatever it takes to overshoot the inflation target in the recovery phase. This is a risky strategy. If the Phillips curve is truly flat, it requires a large increase in interest rates to bring inflation under control. But, a more levered economy is also one that does not digest interest rate increases well. So, when the time for lift-off finally occurs, any hiking cycle is likely to be delayed and unambitious. Furthermore, the risk of a complicit (politically-appointed) central bank chairman cannot be easily dismissed given that central bank independence is no longer a sacred cow.

High debt accommodated by money printing is difficult to banish. Inflation expectations could one day respond to this reality. It is the risk of fiscal dominance that makes the current GMI potentially inflationary during the next cyclical upswing. After all, fiscal dominance was a key reason for inflation to flare up in the late 1930s and the 1940s when the Fed was strong-armed to keep rates low and to monetize Treasury debt issuance well beyond the economic recovery phase.

There are other reinforcing considerations to fear a resurgence of inflation down the line. The pandemic has exposed the vulnerability inherent in global interdependence and stoked tensions between the US and China. There may come a tipping point when a breakdown in global supply chains spills overs to goods prices, undoing two decades of disinflation attributable to globalization.

Seeking Refuge from the Great Monetary Inflation

So with this type of monetary growth as a backdrop, here is one way to navigate these extraordinary times and policy actions. Below is a list of inflation hedges, rank-ordered in what we call the Inflation Race. While some of this list will track inflation in the classic sense, other instruments have been added to pick up the assets that will respond best to an acceleration in monetary growth,

not just consumer goods and service price inflation. So, it includes a host of assets that at one time or another have worked well in reflationary periods:

1. **Gold** – A 2,500 year store of value
2. **The Yield Curve** – Historically a great defense against stagflation or a central bank intent on inflating. For our purposes we use long 2-year notes and short 30-year bonds
3. **NASDAQ 100** – The events of the last decade have shown that quantitative easing can rapidly leak into equity markets
4. **Bitcoin** – There is a lengthy discussion of this below
5. **US cyclicals (long)/US defensive (short)** – A pure goods' inflation play historically
6. **AUDJPY** – Long commodity exporter and short commodity importer
7. **TIPS** (Treasury Inflation-Protected Securities) – Indexed to CPI to protect against inflation
8. **GSCI** (Goldman Sachs Commodity Index) – A basket of 24 commodities that reflects underlying global economic growth
9. **JPM Emerging Market Currency Index** – Historically when global growth is high and inflationary pressures are building, emerging market currencies have done quite well

Now it would be wonderful if we knew ex-ante which horse to bet on. The goal, of course, is to be invested in the fastest horses over the duration of the ride. And to help monitor this, we review the horse race over the short, intermediate, and long term by averaging price performance over such periods. This provides a snapshot such as shown below, which was taken on May 6th (Table 1). We have rank-ordered the instruments below by averaging the 1-week, 1-month, 3-month, and 12-month returns. We show the performance in volatility-adjusted returns, not in nominal returns, so think of each unit as approximately a day's average trading range. So, gold under the "Last year" column has gone up about 26 daily ranges, which also equates to about $406, from $1,280 to $1,686.

Table 1. US inflation race 1/

	Average 2/	Last week	Last month	Last 3 months	Last year
Gold	7.8	-0.6	1.2	4.7	25.9
Yield curve (2s30s)	5.1	1.7	1.8	6.8	10.3
NASDAQ 100	2.3	0.1	2.9	-5.4	11.4
Bitcoin	0.8	0.4	3.5	-3.7	2.9
US equity cyclicals/defensive	0.2	0.9	3.9	1.0	-4.8
AUDJPY	-5.1	-1.3	0.7	-7.1	-12.8
JPM Emerging Market Currency Index	-6.0	-0.2	1.2	-11.2	-13.6
TIPS breakevens	-8.1	0.0	-0.6	-11.9	-19.9
GSCI	-10.4	2.0	-3.0	-16.4	-24.1

Source: Bloomberg and own calculations.

1/ Entries show returns over specified period, in units of average 60-day true ranges.

2/ Average is the mean of the weekly, monthly, three-month, and one-year returns.

From the table, gold is the clear winner of the Inflation Race at this time. In second place is long the US 2s30s yield curve. In third place is the NASDAQ 100: remember this GMI is going to show up somewhere so why not stocks? And in fourth place it is Bitcoin—yes, Bitcoin. It did trade $18 billion of volume on the last day of April and is an "emerging" asset class by any metric. Of course, bringing up the bottom with a hugely damaging return of *negative* 10 daily ranges (also equivalent to -46% in the trailing 12 months) is the Goldman Sachs Commodity Index. This index has been pummeled due to the crash in oil prices as producers are at war to preserve their market share and stay afloat.

One thing that piqued my interest from this list of assets, and that one day might be brought to prominence by the GMI, is Bitcoin. Truth in advertising, I am not a hard-money nor a crypto nut. I am not a millennial investing in cryptocurrency, which is very popular in that generation, but a baby boomer who wants to capture the opportunity set while protecting my capital in ever-changing environments. One way to do that is to make sure I am invested in the instruments that respond first to the massive increases in global money. And given that Bitcoin has positive returns over the most recent time frames, a deeper dive into it was warranted. I did have some experience with it back in 2017, having a tiny amount in my personal account for fun. Amazingly, I doubled my money and got out near the top when it was apparent to any market technician we were blowing off. It is amazing how well one can trade when there is no leverage, no performance pressure and no greed to intrude upon rational reflection! When it doesn't count, we are all geniuses.

But the GMI caused me to revisit Bitcoin as an investable asset for the first time in two and a half years. It falls into the category of a store of value and it has the added bonus of being semi-transactional in nature. The average Bitcoin transaction takes around 60 minutes to complete which makes it "near money." It must compete with other stores of value such as financial assets, gold and fiat currency, and less liquid ones such as art, precious stones and land. The question facing every investor is, "What will be the winner in ten years' time?"

At the end of the day, the best profit-maximizing strategy is to own the fastest horse. Just own the best performer and not get wed to an intellectual side that might leave you weeping in the performance dust because you thought you were smarter than the market. If I am forced to forecast, my bet is it will be Bitcoin.

A store of value is anything that holds its purchasing power in the future. It is completely a function of people's perception of its worth. Even tulips at one time were considered a store of value. Financial assets comprise the largest store of wealth in the world as they generally have the added advantage of providing yield, which helps offset the impact of inflation. Gold has survived the test of time although a rational person could ask "Why gold over any of the other 118 elements?" Fiat currency (cash) is backed by the full faith and credit of the people of that country, although that promise has high variability, as history has shown. And the newest entrant is Bitcoin, which seems to have emerged from the crypto war of 2017 as the clear winner with a market cap 10x that of its closest competitor.

So how do these stores of value stack up against each other? We graded stores of value on four characteristics:

1. **Purchasing Power** – How does this asset retain its value over time?
2. **Trustworthiness** – How is it perceived through time and universally as a store of value?
3. **Liquidity** – How quickly can the asset be monetized into a transactional currency?
4. **Portability** – Can you geographically move this asset if you had to for an unforeseen reason?

For the purpose of this exercise, real estate, art and precious stones have been excluded as they will fall to the bottom of the ranking automatically because of generally poor liquidity and portability characteristics. So let's focus on financial assets, fiat currency, gold, and now Bitcoin. To offer perspective, Table 2 shows the value of these assets at the present time. It is an important table, which I will come back to.

Table 2. Global assets outstanding

	USD bn
1. Global fincancial assets (stocks and credit)	266,917
2. Cash (proxy for global M1)	39,806
3. Total value of above ground gold	9,918
4. Total market capitalization of Bitcoin	186

Sources: Haver, Bloomberg, GoldMoney Foundation, and World Gold Council

Remember, the challenge here is to understand which store of value will be the winner in the next ten years. The first thing is to score the four assets against the four criteria laid out above. So I polled my research group to see what this team of informed persons thought. After discussion, we created a scoring system for a store of value with the maximum score being 100. We considered some categories more important than others, so we allocated 30% each to the categories of purchasing power and trustworthiness and 20% to each of liquidity and portability. Then, we scored the four sets of assets above and came up with a composite and highly-subjective value for each in Table 3 below.

Table 3. Grading assets by their ability to store value

	Subjective score
1. Financial Assets	71
2. Fiat cash	54
3. Gold	62
4. Bitcoin	43

Before drawing broad conclusions, here were some of the more salient points in each category. When it came to **purchasing power**, everyone was a carry merchant arguing the only way to defeat inflation was with some type of yield—i.e., financial assets. This was particularly popular with the 30-something crowd who gave financial assets the highest score across the board. I reminded them that in the 1970s, inflation was near double-digits at times and the road to hell was paved with carry. In fact, virtually all financial assets were shunned because the yield could not keep up with inflation—in many cases like now.

I also made the case for owning Bitcoin, the quintessence of scarcity premium. It is literally the only large tradeable asset in the world that has a known fixed maximum supply. By its design, the total quantity of Bitcoins (including those not yet mined) cannot exceed 21 million. Approximately 18.5 million Bitcoins have already been mined, leaving about 10% remaining. On May 12th Bitcoin's mining reward – the pace at which the supply of Bitcoin is increased – will for the third time be "halved" (falling from 12.5 to 6.25 Bitcoins per block of transactions added to the blockchain). Future halvings will likewise occur approximately every four years consistent with Bitcoin's design, thus continuing to slow the rate of supply increase and causing some to estimate that the last available Bitcoin will not be mined for another 100+ years. This brilliant feature of Bitcoin was designed by the anonymous creator of Bitcoin to protect its integrity by making it increasingly near and dear, a concept alien to the current thinking of central banks and governments.

The most surprising result of our research group poll was the score ascribed to fiat cash. It got a 0 almost across the board! The cry from the troops was "If something is by design going to depreciate 2% per year through inflation, why own it?"

The next category we discussed in determining whether or not something was a good store of value was **trustworthiness**. No surprise here Bitcoin got the lowest score because it is also the youngest entrant at 11 years of age. Someone mentioned that it has 60 million users in almost 200 countries, but that did nothing to sway people. Gold, as one would have guessed, scored first in this category, as it has stood the test of time for thousands of years.

Liquidity is one of those things that never matters until it does (every 10 years it seems), which is why we weighted it only 2/3 of the value of purchasing power and trustworthiness. But as we have all probably experienced in the last two months, liquidity is hugely important when things go pear shaped. It is reasonable to assume, given the number of bankruptcies we are about to witness and the number of people who will be jobless and near poverty, that both companies and individuals will have a much higher preference for liquidity in coming years. Cash scored the highest here and rightly so. Financial assets are a mixed bag because some, like private equity and bespoke credit instruments, take forever to liquidate and often at severe discounts. Interestingly, Bitcoin is the only store of value that actually trades 24/7 in the entire world.

Finally, there is **portability**. Like liquidity, it is not an issue until it is. Imagine a geographic upheaval whether it be caused by war, an epidemic, or change in government that becomes hostile to holders of wealth. A great store of value can be seamlessly moved from one jurisdiction to another with little or no transaction costs. Cash is obviously good for that; gold is ok but clunky; but, of course, nothing beats Bitcoin, which can be stored on a smartphone among other options.

So that was the flavor behind some of the discussions that were had when scoring the suitability of each asset as a store of value. What was surprising to me was not that Bitcoin came in last, but that it scored as high as it did. Bitcoin had an overall score nearly 60% of that of financial assets but has a market cap that is $1/1200^{th}$ of that. It scores 66% of gold as a store of value, but has a market cap that is $1/60^{th}$ of gold's outstanding value. Something appears wrong here and my guess is it is the price of Bitcoin.

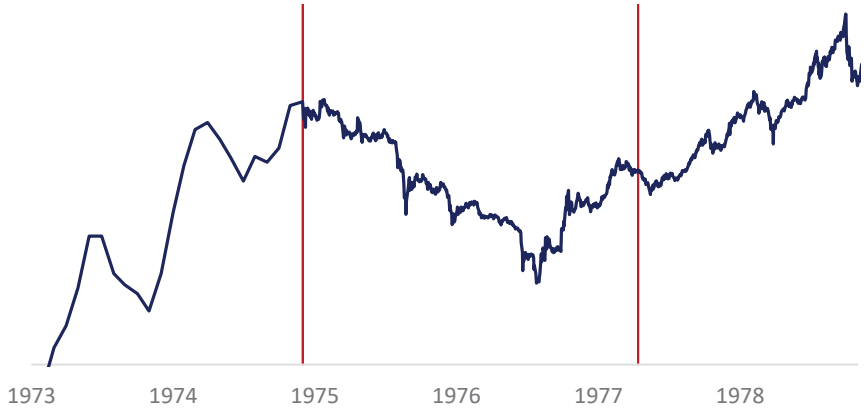
The most compelling argument for owning Bitcoin is the coming digitization of currency everywhere, accelerated by COVID-19. Bull markets are built on an ever-expanding universe of buyers. Central to the price of Bitcoin is how many more (or less) owners of Bitcoin will there be beyond the 60 million who currently own it? The probable introduction of Facebook's Libra (whose value will be pegged to the US dollar and will not be a store of value in that sense) as well as China's DCEP, also tied to the yuan, will make virtual digital wallets a commonplace tool for the world. It will make the understanding, utility, and ease of ownership of Bitcoin a much more commonplace option than it is today.

Owning Bitcoin is a great way to defend oneself against the GMI, given the current fact set. As Satoshi Nakamoto, the anonymous creator of Bitcoin, stated in an online forum around the time he launched Bitcoin, "the root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust." I am not an advocate of Bitcoin ownership in isolation, but do recognize its potential in a period when we have the most unorthodox economic policies in modern history. So, we need to adapt our investment strategy. We have updated the Tudor BVI offering memoranda to disclose that we may trade Bitcoin futures for Tudor BVI. We have set the initial maximum exposure guideline for purchasing Bitcoin futures to a low single digit exposure percentage of Tudor BVI's net assets, which seems prudent. We will review this exposure guideline regularly.

Many of you know my fondness for analogues. Bitcoin reminds me of gold when I first got in the business in 1976. Gold had just been productized as a futures instrument (like Bitcoin recently) and had enjoyed a heck of a bull market, almost tripling in price. It then corrected almost 50% in nearly two years similar to Bitcoin's 28-month 80% correction! You can see the similarities in the two charts below.

Gold price

USD per Troy Ounces in log scale. Source: Bloomberg



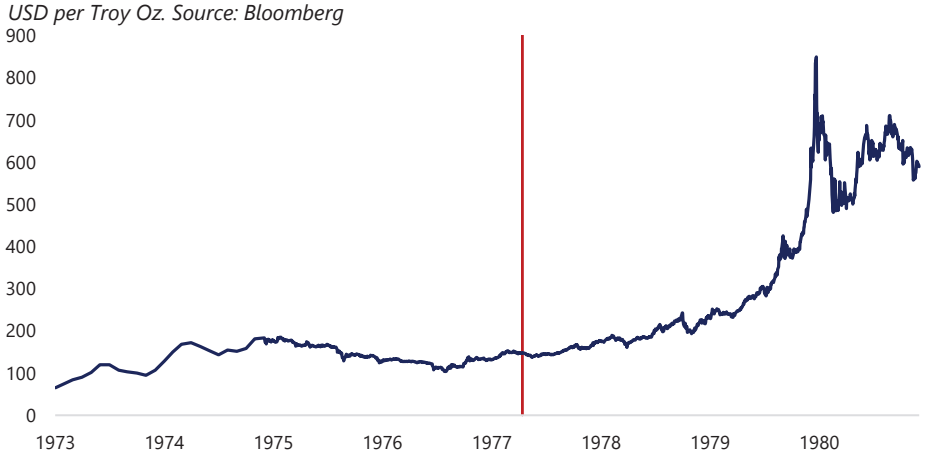
Bitcoin price

USD per 1 Bitcoin in log scale. Source: Bloomberg

But in the case of gold, it was a tremendous buying opportunity as gold went on to more than quadruple past the prior highs. The red line in the chart below is where we might be in Bitcoin today.

Gold price

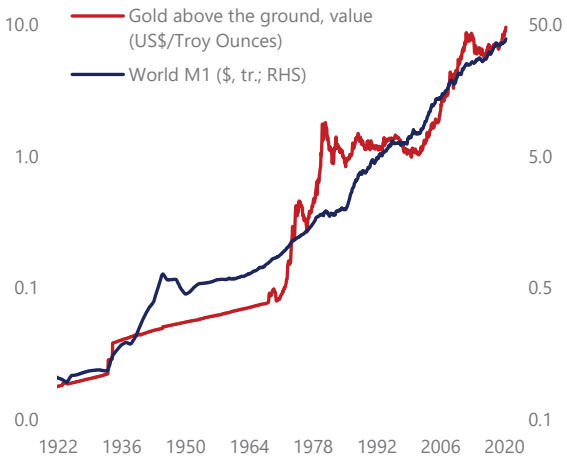
USD per Troy Oz. Source: Bloomberg



Speaking of gold, in a low-carry world, gold remains a very attractive hedge against the Great Monetary Inflation and hedges against other risks clouding the outlook, including a renewed flare up in the China-US relationship where financial sanctions could eventually be used in a brute-force decoupling. How far can gold rally from its current price? A simple metric based on the ratio of the value of gold above ground to global M1 suggests gold could rally to 2,400 before it reaches valuations consistent with the lowest of the last three peaks in this valuation metric and 6,700 if we went back to the 1980 extremes. One thing is for sure, these are going to be incredibly interesting times.

Gold above the ground and global M1

Log scales; last obs. = April 2020. Sources: Haver, Bloomberg, GoldMoney Foundation and World Gold Council



Gold above the ground / Global M1

Last obs. = April 2020. Sources: Haver, Bloomberg, GoldMoney Foundation and World Gold Council

An (Institutional) Investor's Take on Cryptoassets

December 24, 2017 • version 6[1]

John Pfeffer
Medium • @jlppfeffer • LinkedIn

John Pfeffer is an entrepreneur and investor. In the 2000s, he was a London-based partner at private equity firm Kohlberg Kravis Roberts, and in the 1990s, he was Chairman of the Executive Board of leading French IT company Groupe Allium S.A. Before that, he advised on turnarounds while with McKinsey in Europe and Latin America.

Amidst the indiscriminate speculation, sensationalist and mostly misguided media coverage and roller-coaster price volatility, this paper sets out to consider cryptoassets from the perspective of a rational, long-term investor. As investors, we look for things that generate sustainable, ideally growing economic rent—an economic surplus that will accrete to us. This paper evaluates the extent to which cryptoassets offer the foregoing. It aims to assess the potential future value of cryptoassets at mature equilibrium,[2] on the assumption that they *develop successfully and achieve widescale adoption.* By design, it does not dwell on the significant risks that a given cryptoasset could fail, for technical, regulatory, political, or other reasons. These risks are very real, and are well documented elsewhere. Temporarily setting them aside allows for an objective analysis of the *potential* value of different kinds of cryptoassets and their use cases.

I write not from the perspective of a trader, but from that of an investor who believes the long term is easier to predict than the short term. The paper thus focuses entirely on long-term equilibrium outcomes and investment strategy rather than short-term price movements. It also assumes the reader has some familiarity with the topic.

Blockchain technology has the potential to disrupt a number of industries and to create significant economic surplus. The open-source nature of public blockchain protocols,

[1] Earlier versions of this paper were drafted beginning in June 2017.

[2] The notion of mature equilibrium as I use it here is admittedly imprecise. Conceptually I mean once the speculative phase has passed and (i) in the case of monetary store of value, once there is a mainstream, institutional view that crypto is a core monetary store of value like gold is today and (ii) in the context of infrastructure and applications, once markets are valuing cryptoassets based on significant realised user penetration. The obvious analogy is the internet. Internet penetration and internet-enabled businesses are still growing today but growth is slowing. Today, large internet-enabled businesses are valued based on financial ratios such as PEG and EBITDA multiples rather than clicks or eyeballs as was the case in the late 1990s. That's the end point I'm thinking about. For shorthand, let's assume 10 years from now.

combined with intrinsic mechanisms to break down monopoly effects, mean that the vast majority of this economic surplus will accrue to users. While tens or perhaps hundreds of billions of dollars of value will also likely accrue to the cryptoassets underlying these protocols and therefore to investors in them, this potential value will be fragmented across many different protocols and is generally insufficient in relation to current valuations to offer a long-term investor attractive returns relative to the inherent risks. The one key exception is the potential for a cryptoasset to emerge as a dominant, non-sovereign monetary store of value, which could be worth many trillions of dollars. While also risky, this potential value and the probability that it might develop for the current leading candidate for this use case (Bitcoin) would appear to be sufficiently high to make it rational for many investors to allocate a small portion of their assets to Bitcoin with a long-term investment horizon.

We can break cryptographic token use cases into three broad categories:

1. Network backbone / Virtual Machine (e.g., Ethereum)
2. Distributed applications (Dapps)
3. Money, and in particular:
    a. Payments
    b. Monetary store of value.

I will start by looking at the first two use cases from a general perspective and then dive deeper in analysing the largest current example of the first one, Ethereum. I'll then turn to a discussion of the different functions of money, the potential for cryptoassets to perform them and the implications for the value of such cryptoassets, including Bitcoin.

The economics and valuation of utility protocols

Use cases 1 and 2 can be grouped into what I call utility protocols. I will start with some general observations on utility protocols and the implications for their network valuation at equilibrium and then specifically consider the network value of Ethereum at mature equilibrium.

General observations

A blockchain protocol is a database maintained by a decentralised consensus mechanism operated by its nodes. Utility protocol tokens serve to provision scarce network resources: the processing power, memory, and bandwidth necessary for maintaining the blockchain in question. These resources have a real-world cost in terms of energy and the equipment employed, and these costs are borne by the miners who maintain the blockchain by providing computational services. The miners may be remunerated for their service with block rewards, paid in protocol tokens, and/or transaction fees, paid in protocol tokens or some other means of exchange. While protocol developers may claim that tokens are the basis for other kinds of exchange among users and not just a means of allocating and paying for computing resources, it is my argument that, at mature equilibrium, tokens will do no more than allocate computing resource, with the exception of the special case of a cryptoasset that serves as a monetary store of value.

A given protocol is analogous to a simplified economy. The GDP of such an economy would be the aggregate cost of the computing resources necessary to maintain the blockchain, based on the quantity of processing power, memory and bandwidth consumed, multiplied by the unit cost of each. The token is typically the currency used to pay for those resources. The total network value is analogous to the money supply M (i.e., all tokens in issuance), where $M = PQ/V$; PQ (Price x Quantity) is the total cost of the computing resources consumed, V is

a measure of how frequently a token is used and reused in the system (its velocity, V). The value of a single token is therefore M/T, where T is the total number of tokens.

If a given utility protocol does not have a built-in mechanism, such as Ethereum's GASPRICE, to ensure that the cost of using the network does not arbitrarily and sustainably diverge from the underlying cost of the computational resources it consumes, one of three things happens: (a) the token's price trades to a level such that there is no premium cost to using the network (i.e., there is no economic rent); (b) the chain forks into a functionally identical but less rent-seeking chains until any premium usage cost and economic rent on the network declines to a level at which it is no longer worthwhile to arbitrage; (c) the protocol's adoption is temporarily limited to the highest-value use cases until (a) or (b) occurs. In all cases, the equilibrium result must be at or near marginal revenue = marginal cost for the mining industry maintaining the blockchain in question, so that the token's value cannot materially decouple from the underlying computing resource cost.

PQ, the cost of computing resources required to maintain a blockchain, is not only low relative to the current network values being attributed to cryptoassets; it is also inflated by the prevalence of proof-of-work consensus mechanisms, which mean that the vast majority of computing resource consumed is make-work. To the extent that new scaling technologies such as proof-of-stake, sharding, Segregated Witness, Lightning, Raiden and Plasma become prevalent, the amount of computing resource consumed may become quite small. Note also that in the context of cryptoassets, V could go very high at equilibrium. Even if a significant portion of a given cryptoasset has a low velocity because it is being hodl'd by speculators or because it is staked by miners under a proof-of-stake consensus mechanism, the circulating portion of the tokens can circulate at the speed of computer processing and bandwidth—i.e., fast and accelerating. The implication is that average velocities can and are likely to be high, regardless of how many tokens are actually actively circulating for utility purposes to allocate network resources.[3] The combined effect of low and falling PQ and potentially very high V is that the utility value of utility cryptoassets at equilibrium should in fact be relatively low.

Clearly, scaling solutions such as proof-of-stake, etc. are bullish for adoption/users but bearish for token value/investors. Even without those technology shifts, the cost of using decentralised protocols is deflationary, since the cost of processing power, storage and bandwidth are deflationary. This is also bullish for adoption and users and bearish for token value and investors.[4]

Whatever scaling solutions are developed, the inherent redundancy of the consensus mechanism means that there may be fewer use cases than many decentralised revolutionaries think in which a decentralised solution displaces a centralised solution. Use cases will be limited to dematerialised networks where the value of decentralisation, censorship-resistance and trustlessness is high enough to justify the inherent inefficiency and redundancy of the consensus mechanism. Is it worth the cost for payments? Yes for some, but not for all. Consider Twitter -- what is the added value to the user of a massively redundant, trustless,

[3] Chris Burniske's recent blog post "Cryptoasset Valuations" (https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7) estimates an average V of 7, after adjusting for hodlers, stakers, etc. This assumption may be optimistic (meaning, it is probably a low value of V to assume at equilibrium and therefore an optimistic number to be using to estimate the potential equilibrium value of a given cryptoasset), but his framework is useful for thinking about the different drivers of V for a given cryptoasset.

[4] I have yet to come across any examples of a protocol where I have been persuaded that when all is said and done the underlying scarce resource being provisioned is something other than computing resources, or at least where that is what it will boil down to at competitive equilibrium after competition in mining, forks, etc. Please alert me to any counter examples you have seen or can think of.

decentralised Twitter? Is that added value enough to offset its inefficiency compared to the incumbent centralised Twitter? Would Token Twitter offer compellingly higher utility compared to centralised Twitter, including enough surplus utility to offset the cost of operating the consensus mechanism? I'm not so sure.

People often make the mistake of conflating the monopoly network effects of, say, Facebook to blockchain protocols. This notion is fallacious on several levels:

- Blockchain protocols can be forked to a functionally identical blockchain with the same history and users up to that moment if a parent chain persists in being arbitrarily expensive to use (i.e., rent-seeking). Like TCP/IP but unlike Facebook, blockchain protocols are open-source software that anyone can copy or fork freely. A protocol fork is analogous to a team of Facebook developers who decide one Tuesday morning that Zuck is not paying them enough; they could simply flip a switch and use the servers and software that run Facebook to run a new Facebook that is functionally identical, with all the same users and data up to that point. That can, does, and will happen all the time in protocol-land, but would be theft in the context of private companies that own their code, data, intellectual property, etc. Those property rights are why Zuck is rich, and their absence in the protocol economy has profound implications. The ability to fork protocols maximises utility for users but suppresses economic rent for token holders.

- When people talk about the potential value of cryptoassets, they often refer to Metcalfe's Law. Metcalfe's Law asserts that network value = $\Theta \cdot n(n-1)$, where Θ is a constant that captures the differences in the economics built into the business model of each network and where n is the number of nodes in the network. It's not enough to focus on n(n-1). You must also consider what Θ is. Wikipedia has a lot of contributors and users but not a lot of monetary value because it doesn't charge users or have advertisers or attract any other sources of revenue apart from donations. Facebook's Θ is higher than Twitter's because its advertising business model is stronger. TCP/IP lacks financial value not only because no one owns it but also because it doesn't have a revenue model. The problem for utility protocols is that the Θ in question is driven by the cost of the computing resources to maintain the network, which is relatively low and deflationary and which must remain low for their adoption to be successful vs. non-distributed technologies.

- When thinking about whether a protocol's token can capture and sustain economic rent, what is relevant is whether the mining industry maintaining the protocol's blockchain is competitive, not the stickiness of users. The mining industry supporting any decentralised protocol must be a competitive market; otherwise the protocol isn't decentralised. It is the economic competition amongst miners that will ultimately drive the cost of using the protocol and therefore the value of the token. No mechanisms for monopoly rents there.

- Not only must protocols compete against their own potential forks; competition amongst protocols is also fierce. Witness, for example, recent press reports that Kik is considering migrating its token network from the Ethereum backbone to another blockchain because the Ethereum network is becoming too expensive to use.[5]

[5] https://www.coindesk.com/kik-might-move-its-ico-tokens-to-a-new-blockchain/

- The network value of a tokenised version of a dematerialised network business (a social network, Uber, AirBnB, a betting exchange, etc.) will by construction be a small fraction of the enterprise value of its centralised, joint-stock-company equivalent. Holding the number of users constant, you basically take the fully-loaded IT budget (including energy and a capital charge) of those companies (representing PQ) and divide by some (likely high) velocity V. The disruption of traditional networked businesses by decentralised protocol challengers will represent an enormous transfer of utility to users and an enormous destruction of market value. Great for users, the economy and society; bad for investors.

The next topic to address is the impact of a move to proof-of-stake mining and of staking models in general on the network values of Ethereum and other protocols. The idea is that miners are compensated for maintaining the network either in a native cryptoasset or another cryptoasset (such as ETH or BTC), in proportion to the amount of the native network cryptoasset that they stake (i.e., effectively put into escrow and at risk of loss if they attempt to validate false transactions and the like). The promoters of this idea hope that it will reduce the actual computing costs of maintaining the network, by eliminating the costly proof-of-work mechanism, while at the same time creating an alchemic virtuous cycle wherein miners buy and lock up significant amounts of the native cryptoasset as an investment conveying them a right to a mining revenue stream, thereby reducing the velocity of the native cryptoasset and causing its value to rise to a level representing some multiple of their mining profits, much as taxi medallions or shares in a company are valued based on the net present value of future cash flows.

Let's think through how this plays out.

First, before staking is introduced into the equation, we've established that forks and competition in mining and among protocols lead us to an equilibrium outcome where PQ equals the aggregate cost of the computational resources (capital charge on or usage cost of processing and storage hardware, cost of bandwidth and energy) of maintaining the network.

Second, recall that the impetus for moving from proof-of-work to proof-of-stake is to reduce the amount of computational resource and energy required to maintain the network by a couple orders of magnitude. That's good for scalability and potential adoption, but also means a commensurate reduction in the PQ of the network.

Third, let's layer on the idea that in order to participate in mining and the associated revenues, on top of paying for processing power, storage, bandwidth and energy, you must now bear an additional cost in the form of a capital charge from acquiring and immobilising an amount of the native cryptoasset. This capital charge on immobilised cryptoasset is added to PQ, making the protocol in question more expensive to use than an equivalent utility protocol that doesn't require staking (or where staking is less expensive because the native cryptoasset is cheaper).

This system operates a bit like a taxi medallion system: an authority issues a finite number of licenses, and you must buy one from another medallion holder if you want to operate a taxi. The value of the license captures the discounted value of any economic profits that are expected to accrue from operation. Whoever owned the license first is the primary beneficiary of this monopoly, and he receives that value when he sells the license to someone. The buyer of the license does not enjoy any economic rent because he paid the discounted present value of it to the previous license holder, and so on as the license changes hands. Passengers pay higher fares because the taxi driver's capital cost of buying the license must be compensated for, all for the benefit of the first owner of the license.

Imagine there are several different taxi companies operating that have acquired a number of licenses. Now imagine that a new entrant decides it would like to take market share. In the world of a taxi medallion monopoly created by an issuing public authority, they would have no option other than to buy medallions from other medallion owners. But here is where protocol-land is different from real-world taxi medallion schemes. Protocols are open source software and can be freely forked.

In protocol-land, all the upstart taxi company needs to do is to fork the protocol, effectively issuing an identical number of new taxi medallions and reallocating medallions owned by existing large taxi companies to itself and perhaps a few other friends. Because the upstart taxi company didn't have to pay for its taxi medallions, it and the other recipients of the new medallions can charge its passengers lower fares. Passengers thus flock to the upstart company, and the monopoly value embedded in the original taxi medallions vanishes. Everyone in the system except for the large taxi company wins. If necessary, this process can be repeated indefinitely. The result is that the medallions have low values (as would the analogous native cryptoasset).[6]

Another mechanism for utility protocols is mine and burn. In this system, new coins are minted and allocated to miners based on the network services they provide, and users must buy these coins and burn them to pay for transaction processing. This is a perfectly fine mechanism, but it simply ensures that the network value equals PQ/V, where PQ is the actual fiat cost of maintaining the network and V is the average time from minting to burning. That gets you to the same low equilibrium network value more simply and quickly.

Other general observations:

- Analysts often use a working capital analogy in order to assess how much of a given cryptoasset a user will stock to facilitate actual use of a given blockchain's utility function. Fair enough, but digging further into that line of thinking, the way optimal inventories of a good are set is based on the relationship of the volume and volatility of demand, optimal order sizes, communication and delivery latency and production times. Since cryptoassets are generally highly divisible and may circulate very fast (as fast as processor speed and bandwidth allow), it would seem to me that a user would, by the same maths as those used to determine optimal inventory quantities, conclude that he needs to hold very little inventory of a given cryptoasset. Friction moving among cryptoassets is already low and will quickly disappear entirely with technologies like atomic swaps. Consequently, one would expect velocity to be very high at equilibrium. It would make no more sense for users to hoard utility cryptoassets beyond the minimum they need to carry out their desired operations than it would be for individuals to hoard petrol or for companies to hoard giant warehouses full of whatever goods they sell. Companies need inventories of goods to run a business and those inventories have a value on their balance sheet, but they try to minimise such holdings, as they are unproductive assets that are costly to finance and carry. They certainly don't try to accumulate more inventory than necessary as a way to store their retained earnings. Similarly, individuals have petrol in the tanks of their cars, but they don't stockpile petrol in their basements as a form of savings.[7]

[6] The competitive forces to eliminate economic rent would function in largely the same way whether the staking system involves payment for services in cryptoassets that are native or external to the protocol at hand.

[7] See also Vitalik Buterin's recent blog post: "On Medium of Exchange Token Valuations" (http://vitalik.ca/general/2017/10/17/moe.html)

- For every successful utility protocol (certainly for every successful Dapp), there will be *n* failed versions. In fact, one of the advantages of the protocol economy is that it facilitates open and inexpensive experimentation, which will mean that there will be many more attempts and many more failures, and that each success will be individually smaller in its value and reach. The open-source, forkable nature of this kind of software will likely drive toward a fragmentation of use cases and protocol functionality; businesses built on top of the protocols will be protocol agnostic and capable of using and combining modularly a changing array of protocols to deliver whatever service or value chain they are trying to deliver. These dynamics are great for users and generate lots of positive economic and social externalities, but they are bad dynamics for investors.[8] The problem of making money by investing in utility protocols is aggravated by: (a) the fact that this is a fragmented space with very high failure rates, so selecting winners *a priori* will be very difficult; and (b) the fact that most of the long-term winning protocols probably haven't even been launched yet (witness the fact that the most valuable internet businesses were founded after 2001).

- Developer incentives over time are a fundamental issue in crypto. For most protocols, such incentives are heavily front-ended around launch and insufficiently provided for over time. The more ambitious and long-term a protocol's development roadmap is, the more problematic this failure of incentives becomes. The incentives to improve an existing protocol by forking it may be strong if some tokens are reallocated at the fork to the developers making the improvements. For example, where tokens have been retained by a foundation linked to the original protocol developers, an aggressive group of forking developers could reallocate the foundation's tokens to their own new entity in their fork, leaving all other users in the same position and letting the market decide which fork to support. The incentives for a developer to create a new, competing protocol are also strong, but network effects do make it harder to displace an existing protocol than to improve or fork it. Miners and perhaps large users have a strong economic incentive to invest in development of the protocol they are mining either through changes to the protocol or by forking it. The foregoing suggests that we're likely to see (a) more success with protocols focused on simple use-cases that require less ambitious future development; (b) future protocols launched with better long-term developer incentive schemes (easier said than done)[9]; (c) aggressive forks that transfer value from incumbent to challenger developers[10]; and (d) large miners/users or groups of miners/users acting together employing or paying developers to improve legacy protocols either directly or via forks.

The implication of this section is not that utility protocols won't have any network value. PQ/V does represent positive value. The implication is that network value of a utility

[8] See also Teemu Paivenen's blog post "Thin Protocols" (https://blog.zeppelin.solutions/thin-protocols-cc872258379f).

[9] Tezos proposes an interesting potential solution to the developer incentive problem. Tezos combines a PoS consensus mechanism with a system whereby token-holders can vote on improvements to the protocol proposed by developers and reward the developers for their contribution. We'll see if it works, but the problem for Tezos remains that the mature equilibrium value of the Tezos token will be $T_{Tezos} = PQ/VM$ where PQ is the cost of the computing resource maintaining the Tezos blockchain, i.e., T_{Tezos} probably won't have a high value when the dust settles.

[10] See also Fred Ersham's blogpost "Accelerating Evolution through Forking" (https://medium.com/@FEhrsam/accelerating-evolution-through-forking-6b0bba85a2ba)

protocol will converge on or near an equilibrium, where it is a fraction (denominator V) of the actual cost of the computing resources consumed to maintain the networks.

For a fork to succeed, there needs to be enough value available to arbitrage to incentivise users, some miners and a sufficiently credible developer group to support the fork. It should therefore be acknowledged that, to the extent the equilibrium outcome is arrived by way of one or more forks, there could be a sustainable level of network value economic rent premium above computing cost that is too small to provide adequate incentives for a fork to succeed. I would not, however, consider it to be a very compelling investment thesis when the best I can hope for is to keep an amount of value corresponding to an economic rent that's too small for anyone to bother arbitraging it away from me despite relatively low barriers to doing so. While a protocol's core development team may be bound by various soft ties, in protocol-land (unlike in a traditional software business), the work product is all open-source; intellectual property isn't generally owned or protected; and developers have little or nothing in the way of contractual ties or limitations (e.g., no non-compete, no non-disclosure, no non-solicit). That means developers can defect or take the work of others. At a minimum, these factors place a low ceiling on how much economic rent can be created and sustained.[11]

As illustrated in the ETH valuation example to follow, it is likely that the combined network values of all utility protocol cryptoassets together will total between tens of billions and hundreds of billions of dollars. That is significant value, but not when compared to the current ~$250 billion combined network value of protocols other than Bitcoin. Investing in utility protocol cryptoassets could make sense if their current network values were one or two orders of magnitude lower than they currently are, but at current valuations, the risk/return to investors is not attractive.

The Network Value of ETH

ETH, the Ethereum token, is an interesting case to explore because of its significant current network value and Ethereum's potential as the ultimate utility protocol. Ethereum could serve as the backbone for processing smart contract operations for (hopefully) untold numbers of decentralised applications, DAOs, etc., and perhaps one day maybe even something like the fabled Ethereum Virtual Machine (EVM).

Ethereum's developers understood that for Ethereum to fulfil its potential, the cost of using it as a smart-contract-executing utility must be as low as possible and must not depart at equilibrium from the actual cost of the computational resources consumed. To ensure this will be the case, they built the GAS mechanism into Ethereum to decouple the use of the network (and the cost thereof) from the value of the ETH token.

Each possible type of computing operation has a pre-defined GASCOST, measured in units of GAS. GAS may then be paid for using ETH (or another token or currency) based on the GASPRICE 'exchange rate', which is freely set among users and miners.[12]

[11] An interesting business idea that someone could logically pursue at some point would be to raise capital to fund a crack team of mercenary blockchain developers and systematically target technically-mature or maturing protocols where there is still a significant economic rent premium and arbitrage that value via hostile forks of those protocols in a way that reduces cost and/or improves functionality to users and reassigns network tokens held by the incumbent developer team and backers to the insurgent team and backers.

[12] Note that because GASPRICE is fully-flexible, GASCOST might only need to be updated in the system from time to time if and to the extent the relative cost of certain sub-components of computing costs changes, for example the cost of processing power vs storage.

The Ethereum Homestead Documentation makes this all clear:

> "Gas Price is how much Gas costs in terms of another currency or token like Ether. To stabilise the value of gas, the Gas Price is a floating value such that if the cost of tokens or currency fluctuates, the Gas Price changes to keep the same real value. The Gas Price is set by the equilibrium price of how much users are willing to spend, and how much processing nodes are willing to accept[13]." (Ethereum Homestead Documentation Release 0.1, p49)

> "Gas and ether are decoupled deliberately since units of gas align with computation units having a natural cost, while the price of ether generally fluctuates as a result of market forces. The two are mediated by a free market: the price of gas is actually decided by the miners, who can refuse to process a transaction with a lower gas price than their minimum limit." (Ethereum Homestead Documentation Release 0.1, p68)

This is all logical in the sense that GAS, and by extension the ETH token itself, is a metering device meant to ensure correct economic allocation and remuneration of the network's resources. In the long term, the GASPRICE (and through it the value of ETH) should therefore tend toward the actual marginal cost of computing resource on the network. It could not possibly be otherwise, since if the cost of running operations on the Ethereum blockchain became materially more expensive than the actual underlying cost of computing resources consumed by it, people would simply use another blockchain where that premium doesn't exist (or fork to create a cheaper Ethereum network that has identical functionality and users at that moment)? Also, if the GASPRICE were to decouple sustainably from the actual computing cost of operations, then mining would be the only perfectly competitive industry in history to earn sustainably positive economic rent. There is no reason for this to be the case in an industry where capacity can be freely added and withdrawn and the market price freely set.

Since the value of ETH is decoupled from GAS and therefore from the volume of transactions on the Ethereum protocol, an ETH bull could argue that ETH tokens could have an arbitrarily high value without compromising the cost-efficiency of operations on the chain. But let's first agree that because of the GASPRICE mechanism[14] the volume of transactions on the ETH blockchain and the scale of its adoption are not transitive to a high ETH token value. This point is important as observers often erroneously assume that a high volume of network transaction volume driven by all of the different potential uses of the Ethereum protocol will necessarily give the ETH token high value.

Let's work through some numbers to see what in fact the utility value of ETH might be. Ethereum GDP (i.e., PQ) is the total 'revenue' of the computing network performing the

[13] Today in practice it seems that the vast majority of transactions use the default 0.02 microETH price, but that most likely reflects the incipient nature of activity on the network. GASPRICE can be expected to become more market-driven as use of the Ethereum network grows. From a basic microeconomic perspective, if the GASPRICE (in fiat terms converted via the GASPRICE to ETH exchange rate and the fiat value of ETH) exceeds from time to time the actual fiat cost of providing the requisite computing resources, you would expect users to reduce GASPRICE offered or miners to add competing computing resources to the network until the marginal cost again equals the marginal revenue, driving a decline in the GASPRICE. This relationship should hold no matter what the scale of the operations being performed on the blockchain. The market will just keep allocating more computing and storage resources to the network as long as it is profitable to do so.

[14] Note that the GASPRICE mechanism helps to reduce the incentives to fork the chain because economic rent can be eliminated quickly through it without necessitating a fork. Protocols without a GAS mechanism can be expected to end up at a similar economic equilibrium through forks as Ethereum will reach through the GAS mechanism. Ethereum may still fork for other reasons.

underlying operations, which can be directly measured as GAS used multiplied by the average GASPRICE. On 23 December 2017, the total amount of ETH used to fuel (pay miners for) transactions on the Ethereum network was ETH 1,388 (derived from the total GAS used[15] multiplied by the average GASPRICE that day[16])[17]. ETH 1,388 is worth about $1 million at $700 per ETH. Annualised (simplistically multiplying by 365), this is about $355m per year.

We can then play with different assumptions for how fast the Ethereum network will grow vs the declining computing and energy costs. For example, let's assume Ethereum network traffic grows from here at the same rate internet traffic grew from 1995 to 2005 (roughly 150% growth per year)[18] and that the combined offsetting impact of declining computing costs is -20% per year (optimistic as this approximates only the effects of the average rate of decline in computing costs without a change in the consensus mechanism; implementation of proof-of-stake or other scaling solutions could represent a step change down in the computing costs of the network by orders of magnitude). The combined net effect would imply 'Ethereum GDP' (PQ) doubles each year. At this rate, Ethereum GDP would grow from $355 million to $363 billion in ten years, an over thousand-fold increase. If we assume an ETH velocity of 7, the network value of ETH would be $52 billion *in 10 years*, about 24% *less* than its current network value of approximately $68 billion. Of course, in order to provide an attractive return to investors buying ETH today, its current network value would have to be significantly lower than $52 billion (assuming investors would expect to make a 30 – 40% annual rate of return over that period, the current network value would need to be in the range of $1.8 – 3.8 billion).

The foregoing calculation implicitly assumes that GASPRICE is already set at the level where miners are making zero economic rent and that Ethereum does not change its proof-of-work system, for example to proof-of-stake. As it's early days for Ethereum and mining computing resources are still catching up with demand, miners are probably still temporarily making positive economic rent, which means this back-of-the-envelope calculation in fact overstates PQ even if proof-of-work is maintained. More significantly, if Ethereum successfully moves to a proof-of-stake mining system and thereby substantially reduces the computational inefficiency inherent in proof-of-work where 99% of the computing power goes to proof-of-work and only a very small portion to actually maintaining the ledger, the PQ of the blockchain would fall massively and along with it the Ethereum network value. Recall also the analysis in the previous section explaining why staking of tokens for mining under proof-of-stake won't allow Ethereum to sustain a network monopoly premium.

Another way to look at this is to relate the Ethereum GDP to the total revenue of Amazon Web Services. AWS total revenue in 2017 is estimated to be $16.8b, growing to $40b in 2021 (according to JP Morgan), an order of magnitude smaller than our 10-year estimation for ETH GDP in the previous paragraph. If the velocity of ETH is 7, the Ethereum GDP (PQ of computational resources running the network) would need to reach approximately $476 billion or 28 times AWS' current revenue to justify its current network value and excluding any return on investment during the years while Ethereum grows to reach that scale. Now, of course, AWS is just one provider of cloud services, but Ethereum is just one blockchain. Even if we assume that Ethereum will have some greater market share of blockchain than

[15] https://etherscan.io/chart/gasused
[16] https://etherscan.io/chart/gasprice
[17] On 23 December 2017: GAS Used 41,686.74 million x Average GASPRICE 0.000000033285710975 ETH = 1,388 ETH.
[18] https://blogs.cisco.com/sp/the-history-and-future-of-internet-traffic

AWS has of cloud, it is still hard to see how the current Ethereum network value can be remotely justified on this basis.

Note that in my reasoning about the future value of ETH at equilibrium, I have so far not taken into account the mined tokens that miners receive for performing computational services for the network as that value does not accrue to token holders. Rather the opposite. There are in fact two negative impacts of mining rewards on the value per token:

- Issuance of new tokens doesn't increase the total network value, just as printing fiat money doesn't make people collectively richer in real terms. The new issuance goes to the miners at a one-for-one cost of dilution spread across the value of all pre-existing tokens. This must also be true for the interest rate (BIR) paid on ETH tokens deposited in a proof-of-stake system. The new tokens generated to pay the interest dilute all existing tokens such that the effect on the overall total value of ETH tokens is neutral. Those engaged in mining will benefit from the interest earned while those not engaged in mining will suffer from the corresponding dilution. But the existence of this system does not drive growth in the network value of ETH and in fact drives devaluation of each ETH token at the rate of total interest paid in ETH divided by the total issuance of ETH.[19]
- There is a second, subtler negative effect of this new token issuance. It subsidises the cost of operating the network, which at competitive equilibrium puts downward pressure on GASPRICE, which in turn puts downward pressure on the value of ETH at a constant GAS <> ETH exchange rate.

The paradoxical combined effect is that the cost of new token issuance through mining rewards is effectively borne twice by non-miner token holders.

The implication of all of the foregoing is that, even if Ethereum is hugely successful, the value implied by its use as a backbone utility protocol is likely a small fraction of its current value. All of this raises a question for ETH bulls: why would ETH be arbitrarily valuable if it's not some scarcity in relation to the volume of transactions and operations on the chain?

One proposed reason has been that people will hoard ETH as a currency with which to make financial investments, for example in ERC20 token ICOs or DAOs built on the Ethereum protocol. In his blog post "Platform Currencies May Soon Be Obsolete" [20], Aleksandr Bulkin articulates why it is unlikely that a single blockchain will host a large number of Dapps and at the same time function as a major monetary store of value. Also, if utility protocols turn out to be poor financial investments as the foregoing analysis suggests, how much investment demand will there be? Finally, in a frictionless, multi-protocol future, why stockpile a particular token specifically to make a particular type of investment rather than store your value in the best pure store of value protocol (or in productive investment assets) and acquire the amount of ETH or any other currency for a particular purpose (including a subset of investment purposes) at the time of need?

So that leaves the possibility that ETH replaces Bitcoin and becomes the dominant non-sovereign monetary store of value simply on pure store-of-value merits. We'll go deeper into the topic of monetary store of value below, but from where we are today, an objective observer would give Bitcoin significantly higher odds than ETH of becoming such a store of value. And as for those who argue that you can recreate Bitcoin on top of Ethereum, the

[19] Vitalik Buterin, Incentives in Casper the Friendly Finality Gadget (v 27 August 2017), p6.
[20] Aleksandr Bulkin, https://blog.coinfund.io/platform-currencies-may-soon-be-obsolete-78d9b263d902.

question is, why would you? Why substitute a new sub-token on top of a more complex protocol with a larger attack surface, shorter track record, less decentralised governance and propensity to make backwards incompatible protocol changes, for a hugely robust, stable, proven, and widely accepted protocol that already performs that narrow function very well?

Cryptoassets as Money

Money is a debt ledger with three sub-functions:

1. Store of value
2. Means of payment
3. Unit of account.

Cryptocurrency's performance advantage over incumbent forms of money is (a) strongest and most obvious as a monetary store of value; (b) stronger for some, but far from all, payments; and (c) differentiated as a unit of account for a few select purposes.

Cryptocurrency is overwhelmingly better as a monetary store of value than, say, gold. (I won't enumerate the reasons why, as it's pretty intuitive and has been written about widely.) As a means of payment, it can perform better than incumbent technologies in specific instances (think international payments), but Visa, Apple Pay, Google Pay, PayPal and fiat currency work well and better than cryptocurrency for most day-to-day payments. As a unit of account, a non-sovereign cryptocurrency could be most useful in international trade, global commodity markets, foreign reserves, and jurisdictions with unstable domestic currencies.

Before addressing the question of how to think about valuing the payment and the monetary store of value functions of a cryptocurrency, I'll first examine the link between payments and monetary store of value. Many observers presume this link to be very strong, but the reality is more nuanced.

First, let me draw a distinction between a monetary store of value and a run-of-the-mill asset. A monetary store of value is characterised by having a value that is decoupled from its utility for other purposes and from the cost of making/extracting and storing it. A warehouse full of goods, a stockpile of copper and a tankful of petrol are all assets and have value (determined by the market at the equilibrium point where their marginal utility meets their marginal cost of manufacture/extraction, i.e., MR = MC). Inventories of assets such as these appear on a company's balance sheet, but companies seek to minimise how much they have to hold to carry out their business, given the capital carrying cost. They don't try to accumulate these inventories to store their retained earnings. Gold, by contrast, is a monetary store of value. Its value is decoupled at equilibrium from the cost of extracting and storing it. While we may also use it for jewellery (an ancient way of signalling our wealth to other members of society), and we use a bit of it for manufacturing electronic goods and other industrial uses, we also store tonnes of it at great expense in giant inert lumps as a form of savings—a store of value—with no intent of ever using those lumps for any other purpose. Gold is therefore arbitrarily expensive relative to its extraction and storage cost. Its value is subjective.

Consider some examples of the things we use as means of payment versus those we use as monetary stores of value today[21]:

[21] Note that I exclude here things like pre-paid debit cards, gift cards, pre-paid telephone plans and air miles as they are relatively immaterial to the financial system. As it happens, these can all be used for payments and are assets but people treat them as working capital (immobilised balance sheet assets with a carrying cost) rather than a form of savings, so if anything, they are more payment rails than monetary stores of value.

- Means of payment: Visa (credit and debit), SWIFT, PayPal, Apple Pay, Google Pay, Western Union, physical cash
- Monetary stores of value: Gold, fixed and demand bank deposits, physical cash.

What's interesting is that the only thing that appears as both a means of payment and a monetary store of value is physical cash. Yet even though physical cash is clearly both a means of payment and a monetary store of value, individuals typically hold only what's in their pockets and extract more from a deposit account as they need it. Companies that aren't retailers typically hold zero or close to zero actual physical cash (instead keeping their treasury in bank deposits, commercial paper, treasuries, etc.). For a retailer, cash in tills is not even treated as money but rather as working capital. Bank deposits are a monetary store of value but are neither a payment rail nor cash; rather they are contractual obligations of a financial institution operating on a fractional reserve model. When you make a payment, you can convert the deposit (store of value) into physical cash (payment rail) and pay with the cash or you use your Visa (payment rail), which is then paid by way of your local interbank payment network (payment rail) through a change in ledger entries of bank deposits held by you, Visa and the merchant. Credit cards clearly aren't a store of value. SWIFT is a payment rail but stores no value. On the other hand, gold is just a monetary store of value but not a payment rail. No companies keep their accounts and no retailers price their goods in ounces of gold. No one pays for coffee with gold. But that doesn't dissuade people from using gold as a store of value.

The reality is that means of payment and monetary stores of value are more generally separated than combined. The point of all of this is to illustrate that there are lots of means of payment which don't represent stores of value. It is thus overly simplistic to assume that people will hoard that which they use to make payments as opposed to converting their store of value via the payment rail at the time of payment in the exact amount needed and for as little time as possible.

There is substantial evidence that economic actors choose what to use as a means of payment and what to use as a monetary store of value somewhat independently of one another, based on the inherent functional merits and demerits of the 'thing' in question as a payment rail or monetary store of value. Cryptoassets are an interesting special case where, since the technology is potentially advantageous compared to incumbent forms of money as a monetary store of value and also for some payments, it is possible that a single cryptoasset might successfully compete as both. (The counterargument is that, because it is likely to be effectively frictionless to convert between two cryptocurrencies, it will be even easier to disaggregate the payment and store of value functions than it is with incumbent forms of money.)

A useful thought experiment in this regard is to imagine there are competing cryptocurrencies that have the following hypothetical relative utility scores across the five key characteristics of money:

Utility (10 high - 1 low)	Coin A	Coin B	Coin C
Scarcity	10	2	7
Durability	10	3	7
Portability	6	10	7
Divisibility	6	10	7
Acceptability	3	10	7
Total	*35*	*35*	*35*

When the dust settles, what will be the outcome? Which hypothetical coin will be the dominant payment rail and which one the dominant monetary store of value? Will Coin C be the one coin to rule them all?[22] Or will Coin A emerge as the dominant monetary store of value and Coin B the dominant payment rail with users converting as required between the two? Much will depend on the technical and political trade-offs in creating cryptoassets that score relatively higher or lower on each of the five dimensions, but I lean towards the view that specialisation combined with protocol interoperability is a more likely equilibrium than one coin to rule them all.

It would be rash to go so far as to dismiss payments functionality as a necessary feature of a dominant monetary store of value (despite gold having none). A cryptoasset aspiring to be the dominant monetary store of value should prudently strive to have reasonably good payment functionality (divisibility, fungibility, acceptability); the more the better, provided that its monetary store of value functionality (scarcity and durability) isn't compromised. Poor or no payment functionality could impair a cryptoasset's ability to be adopted as a monetary store of value, so it's an important feature. But the point of all of this is to observe that a cryptoasset with the strongest monetary store of value functionality and with good but perhaps not the strongest payment functionality has a strong chance of winning out as the dominant store of value. Payments functionality in a monetary store of value cryptoasset is a satisficing, rather than a maximising, condition.

By corollary, just because a cryptoasset has an edge in payments doesn't mean it will automatically become a store of value. To wit, the only means of payment listed above that is also a store of value is physical cash. If a cryptoasset like Ripple is better for payments (cheaper transactions and more bank support) but weaker as a store of value than Bitcoin (due to centralisation of governance and supply uncertainty), it's unlikely that Ripple will win out as a store of value. And just because users employ some utility cryptoasset (such as ETH) for practical purposes, it doesn't mean that they will see it as a monetary store of value and hoard it as a form of savings rather than treat it as working capital to be minimised on their balance sheets by buying just as much ETH as needed when needed.

[22] A crypto-spork? The crypto equivalent of that hybrid spoon and fork that no one uses because it's not as good as a fork in piercing solids nor as good as a spoon in transporting liquids. Insightful humour credit: https://medium.com/@hamptonfischer/bitcoin-cash-a-spork-7f9f6230a57. Or rather, a crypto-fpoon? But I digress.

What does all of this mean for assessing the potential value of cryptoassets as money? First, you should look at payment functionality valuation and monetary store-of-value valuation as two separate and additive things. You should then consider the relative functional strength of the cryptoasset you are valuing on payment and store-of-value dimensions compared to competing cryptoassets, to check that extreme weakness on one dimension doesn't result in weakness on the other dimension; you shouldn't just assume that payments and monetary store of value are inseparable. The network value of a hypothetical cryptoasset that ends up serving as both a monetary store of value and a payment rail can be thought of on a sum-of-the-parts basis, where (total network value) = (monetary store-of-value valuation) + (means of payment valuation).

What do I think could be the equilibrium outcome? A very credible scenario is that you end up with a mix of non-sovereign cryptocurrencies, sovereign digital currencies, off-chain/layer-two payment solutions and evolved versions of centralised payment systems such as Visa, PayPal and Apple/Google Pay, competing in payments (with each having different strengths and weaknesses for specific types of payments), along with a single dominant non-sovereign monetary store of value, playing a role much like that of gold today. That monetary store of value could also replace a significant portion of foreign reserves and perhaps become a unit of account for international trade and commodities.

It seems likely that payments will remain a fragmented market and that sovereign digital currencies, off-chain (censorship-resistant or not) payment solutions and centralised payment systems will successfully compete for the vast majority of global payment volumes, most of which are small, domestic and mundane, and where speed and cost matter more than strong censorship-resistance. In this scenario, non-sovereign, censorship-resistant, decentralised payment protocols could end up being a niche product for international payments, markets with a failed domestic sovereign currency or payments where censorship-resistance is important (capital controls, sanctions, political repression, illicit activity). I can imagine sovereign states creating regulations that favour use of sovereign digital currencies rather than non-sovereign cryptocurrencies for domestic payments to help them retain control over domestic monetary policy and taxation. It's worth highlighting that, while sovereign digital currencies will probably successfully compete with non-sovereign payment-focused cryptocurrencies for payment volumes, they will likely facilitate the emergence of a non-sovereign monetary store of value, since their existence will help to eliminate the on- and off-ramp banking issues and friction currently involved in exchanging fiat for crypto.

To preview what follows, monetary store-of-value functionality is potentially far more valuable than payments functionality. Thus, if a monetary store-of-value cryptocurrency also works well as a means of payment, that's just a little additional value upside. What matters far more to us as investors is store of value.

Payments

Proceeding from the general observations at the beginning of this paper, a means of payment, examined in isolation from the monetary store-of-value function, is just another utility protocol where the value of the token cannot decouple from $M = PQ/V$ of the computing resource maintaining the payment blockchain. Payments on a large scale must be cost efficient. To the extent a cryptoasset is both a store of value and major payment rail, in order to be cost-efficient and competitive as a means of payment, the payment part will have to be economically disassociated from the store-of-value function, such that the incremental M for payments still equals PQ/V for the computing resources facilitating the payment function and where V can go very high. This dissociation can be achieved by way of an explicit

mechanism like Ethereum's GAS; by way of various scaling solutions like off-chain transaction processing; and/or by emphasising transaction fees rather than block rewards in rewarding the mining network. The effect of something like Layer 2 transaction processing is to massively increase V (and reduce M) for the payment component of the sum-of-parts valuation of a cryptoasset.

Blockchain payments will in fact be worth (to token-holders) much less than their centralised counterparts like Visa, Apple/Google Pay and PayPal are worth today. It is incorrect to think that because a cryptoasset serves as a payment rail, owners of the token in the system would own something comparable to the enterprise value of, say, Visa divided by the number of tokens issued. Rather, at mature equilibrium, the network value of such a token would be M = PQ/V where PQ is just the aggregate cost of the computing resources to run the chain (which may be thought of as the annual IT budget of an equivalent-volume incumbent payment system multiplied by some coefficient to adjust for the relative computing inefficiency of decentralised vs. centralised architectures) and V is of course some (probably high) velocity. The value implied by the correct valuation framework of M = PQ/V is much, much lower than the enterprise value of the incumbents. Blockchain payments may disrupt and displace the incumbents to the enormous benefit of users, but the value of these protocols as expressed through their tokens will be much less than the value of the disrupted enterprises.

An additional factor to consider is the extent to which companies and individuals choose to keep an inventory of payment tokens as working capital on their balance sheets. The question is how strong this working capital driver will actually be. Companies and individuals hold very little physical cash. To the extent they hold cash-equivalents as a buffer against uncertainty, they hold it in the same currency in which they incur expenses, which will play to the advantage of sovereign digital currencies and incumbent payment systems unless retailers and suppliers begin to reprice directly in cryptocurrency units on a large scale. Except for users who make lots of international payments, who are primarily engaged in international or commodity-based trade or who operate in economies with weak domestic currencies, it may not make a lot of sense to maintain a significant stock of a non-sovereign-denominated payment rail cryptocurrency. In a crypto-native world, moving from one cryptoasset to another (for example from a store-of-value cryptoasset to a means-of-payment cryptoasset or converting between alternative payment cryptoassets) will be trivial, immediate and frictionless. What would the rationale be for holding an inventory of a given means-of-payment cryptoasset?

It's also worth reflecting on the difference between cash equivalents, such as deposits at a fractional reserve bank, and physical cash, and how that distinction reads over to a cryptoasset. If there is no fractional reserve banking system available for the cryptoasset, users may opt to store their value in yielding fiat-denominated deposits while keeping a low inventory of the payment rail cryptoasset rather than have a large holding of a cryptoasset that doesn't yield anything, or they may lend their cryptoassets out by buying yielding cryptoasset-denominated bonds and commercial paper.[23]

Finally, in thinking about the potential value of the payments function of a single non-sovereign cryptocurrency, it's noteworthy that, while there clearly are network effects in payments (Visa is more useful and worth more as a business than Diners Club because it's accepted by more merchants and used by more consumers), payments today do appear to be a

[23] Note that both of these things increase the money multiplier and effectively decrease the scarcity of the cryptoasset in question.

structurally somewhat fragmented space. How many non-sovereign monetary stores of value are held in portfolios? Gold is pretty much it. Now think about how many different payment rails you've used over the past month: physical cash (perhaps in multiple currencies), Visa, Amex, PayPal, direct debit, SWIFT, etc. They were all good and reasonably fit for purpose in slightly different ways and with slightly different features for a specific payment: cash to tip the porter, Visa to pay on Amazon, Amex to buy a plane ticket and get the points, PayPal to pay on that dodgy website you don't trust with your card number, direct debit to pay your utilities bill, SWIFT for an international transfer. We should always be careful not to assume the new paradigm will function like the old paradigm (in the 90s, for example, we imagined old media online rather than social media). But we can arrive at the expectation that payments will be a fragmented space by applying first principles rather than extrapolating from the present. Moving among cryptoassets will be frictionless, and there are lots of nuanced differences across payment instances. It's thus more likely that we'll use lots of different payment rails based on how their respective features mesh with the circumstances. Time will tell what those will be, but it's not hard to come up with an initial list of possibilities: fully-autonomous smart contract payments that require a Turing-complete language overlay, payments where speed is of the essence or where cost is of the essence, payments where security or anonymity dominate, cases where one merchant simply accepts Litecoin while another takes Dash and many, many others.

In sum, I can imagine constant innovation and an ever-changing, fragmented, increasingly competitive payments landscape. This stands in contrast to monetary store of value, where leadership tends to strengthen over time. Path dependency is likely to be much stronger in store of value than means of payment. While there is some value in a payment rail exclusive of monetary store-of-value value, it is relatively low. Absence of payment functionality may hinder a cryptoasset's monetary store of value utility, but there are many examples where that isn't the case and where payment functionality doesn't translate into store of value, so any causality is weak.

Monetary Store of Value

I would argue that one cryptocurrency will likely become the dominant non-sovereign monetary store of value, because it's not clear what utility having two or more of them would add. Gold is the one dominant monetary store of value that isn't a fiat currency or tied to one. Yes, there's silver, but the value of all silver is a tiny fraction of the value of all gold, only about 20% of annual silver demand (worth about USD 3.3 billion in 2016) is for monetary uses[24], and it's trivial from a financial markets perspective. Why would we need multiple cryptocurrencies serving as non-fiat monetary stores of value? What utility would that add?

That brings us to the matter of quantifying the potential future value of the dominant store-of-value cryptoasset—and therefore the upside relative to today's value. If a cryptoasset becomes a dominant non-fiat monetary store of value, a logical place to start in estimating its potential network value is as a fraction or a multiple of the value of the total stock of the current technology filling that role, i.e., gold, which has a total value of USD 7.8 trillion.[25] The question of what fraction or multiple to apply is more subjective. You may feel it will be hard or take a very long time for a cryptoasset to fully replace gold, which has been around for millennia, in which case you think it will be a fraction. Or you may argue that the

[24] https://www.silverinstitute.org/silver-supply-demand/

[25] USD 7.8 trillion = total estimated gold above ground of 187,200 metric tonnes x 32,150.7 troy ounces per metric tonne x USD 1,292 per troy ounce on 21 August 2017, the date this section was written.

technical advantages in terms of divisibility and portability in particular will mean that more of the world's population will hold this cryptoasset than they do gold (anyone with a smartphone, a memory stick or a paper wallet can hold any quantity of a cryptoasset, but carrying and storing investment gold is more difficult). That cryptoasset, moreover, will likely play some role in payments while gold does not.

To try to bring some objectivity to this last question, let's look at the breakdown of where gold is today. Of total above ground stocks of gold of 187,200 metric tonnes, 38% is in the form of bullion holdings, of which a little less than half was held by the official sector (i.e., national treasuries) and the remainder by the private sector. The remainder of above-ground gold is almost all in the form of fabricated products, which breaks down roughly into 80% jewellery and 20% industrial products.[26]

With those building blocks you can play with your own different scenarios of what success looks like. I'll develop a strawman scenario for consideration below.

While some jewellery may be notionally held for investment purposes, and there may be some collectible coins in the fabricated products number that holders think of as 'investments', I broadly exclude fabricated products, as a cryptoasset isn't a substitute for the vast majority if not all of those uses. Instead I focus on the bullion holdings. Because of cryptoassets' superior features over gold and its additional utility advantage for some payments, we might assume that a successfully dominant cryptoasset store of value being worth at maturity 1 – 3x private bullion holdings. Because national treasuries may be slower and reluctant to adapt, I'll suggest an assumption at a ten-year horizon of 0.25 – 1x official bullion holdings. Breaking the 38% of gold represented by bullion into 20% private and 18% official holdings and using the foregoing assumptions, we would estimate that the dominant store-of-value crypto could be worth 25 – 78%[27] of total gold stocks at maturity, i.e., USD 1.9 – 6.1 trillion.

Displacing gold bullion could, however, just be the tip of the iceberg. Gold represents a little less than 11% of the USD 12.7 trillion of total international reserves, with fiat currencies making up 86% and IMF Special Drawing Rights (SDRs) and IMF-related assets the remaining 3%.[28] The fiat currency portion is made up of 63% USD, 20% EUR and the remainder other currencies (most significantly GBP, JPY and CHF).

We need to separate fiat currencies' use for domestic payments from their use as international reserves. As stated above, there are good reasons to be sceptical about how significant a portion of domestic payments a non-sovereign cryptoasset will replace outside of countries with unstable sovereign currencies, namely: the existence of incumbent low cost and efficient centralised payment rails, the unwillingness of states to give up control over domestic monetary policy and the inevitability of sovereign digital currencies. But think how uncomfortable a situation it is for countries to hold the bulk of their international reserves in other countries' fiat currencies. We know that China and Russia in particular chafe at this situation. They would love to have an alternative to the USD and EUR and have even talked about creating an alternative (which didn't go very far, since creating such an alternative would require their trusting each other). Think about how difficult it must be for the Chinese to have exports often priced in USD and for commodity-producing nations that commodities are priced globally in USD. Furthermore, any USD-based transactions must pass through

[26] GFMS Gold Survey 2017 p.36

[27] Low end: ((20% * 1) + (18% * 0.25)) = 25%; High end: ((20% * 3) + (18% * 1.0)) = 78%.

[28] As of 28 April 2017. International Monetary Fund 2017 Annual Report. Note that on 28 April 2017 an IMF Special Drawing Right = 1.371020 USD.

SWIFT, which is controlled by the US, and exclusion from SWIFT would be tantamount to near-complete isolation from the international financial system (witness Iran). This is an increasingly untenable situation for many sovereigns, particularly as the global power and influence of the US wanes. A non-sovereign, non-fiat, trustless, censorship-resistant cryptoasset would be a far better alternative for most foreign currency international reserves. IMF SDRs are already a synthetic store of value, so could also be easily and sensibly replaced by such a cryptoasset.

Building on our gold bullion analysis above to put some numbers around the potential implications for the network value of our monetary store-of-value cryptoasset, we might assume that it replaces somewhere between 0.25x and 0.75x of non-gold international reserves. My low-end assumption is fairly arbitrary but my high-end assumption reflects the likelihood that states will want to diversify their foreign reserves to some extent as they already do in holding fiat currencies other than the USD. These assumptions would add a further USD 2.8 – 8.5 trillion in value to our dominant monetary store-of-value cryptoasset. Adding these amounts to our gold bullion-based numbers above gives a total potential value range for our dominant monetary store-of-value cryptoasset of USD 4.7 – 14.6 trillion.[29]

I'll stop there for now, but there are two further upsides that I haven't explicitly taken into account. First, it could make sense for such a cryptoasset to replace the USD as the standard unit of account for global trade and commodity prices. Trade- and commodity-centric firms may therefore choose to capitalise themselves in such a cryptoasset, creating further demand for its limited supply, mitigated by the inevitable emergence of fractional reserve banking and bond markets denominated in the cryptoasset which would increase its money multiplier. Second, such a cryptoasset will likely be used for some payments, such as international payments or domestic payments in countries without stable sovereign currencies (where this is already happening). This latter potential is at least somewhat, if not fully, captured in the high end of the range above in the sense that, when we start thinking about this cryptoasset store of value representing a multiple of private gold bullion holdings, we are implicitly already accounting for some displacement of physical cash holdings.[30] As explained in the previous section, the incremental sum-of-parts value contribution from the payments functionality arguably won't be that significant compared to the store-of-value component, so ignoring it here probably doesn't very materially impact the potential value target.

The next question is, which cryptocurrency has the highest probability today of becoming the dominant store of value? It seems to me that the probable answer based on the information in our possession today is Bitcoin (BTC). It has more users; has decentralised (to the point of dysfunctional) governance; has more hashing power than any other crypto; is highly stable and robust; has been around longest; and has never been hacked. Other cryptoassets may have features that Bitcoin doesn't have that are useful in sundry use cases other than store of value, but store of value is a simple functionality (perhaps the simplest of all the cryptoasset use cases), and Bitcoin has been and continues to acquit that functionality flawlessly. Critics point to the conflictual politics that complicate changes to Bitcoin's code, but seen purely through a monetary-store-of-value lens, that can be seen as more of a feature than a bug. It seems to me that it is far more likely that Bitcoin becomes the dominant store-of-value crypto than some other existing or future contender that isn't Bitcoin. If Bitcoin were to become the dominant monetary store of value cryptoasset, based on my total mature network value

[29] Total international reserves of USD 12.6 trillion, of which 89% non-gold reserves = USD 11.3 trillion. Low end: USD 11.3 trillion x 25% = USD 2.8 trillion; high end: USD 11.3 trillion x 75% = USD 8.5 trillion.

[30] To give some bounded idea of the potential value of displacement of some domestic fiat currency holdings, global M0 is about USD 5 trillion, so we'd be talking about a relatively small fraction of that.

estimate of USD 4.7 – 14.6 trillion, it would be worth approximately USD 260,000 – 800,000 per BTC fully-diluted[31] at maturity.

We should pause here to think about how long the emergence of a cryptoasset as a dominant monetary store of value might take. On the one hand, gold has been around for millennia, so the mental paradigm shift required might take longer than 10 years and never occur fully. On the other hand, we rode horses for transportation for millennia and moved on from that pretty quickly and categorically with the advent of the superior technology of the motorcar. That transition required a major build-out of physical infrastructure while the one that interests us here requires little more than a shift in mindset. Also, financial markets tend to discount the future as soon as there is consensus about it, so the value per Bitcoin could anticipate the levels of adoption I'm holding up for consideration. (For a more extensive discussion of this topic, see below for **Addendum on Pace of BTC Price Rise**)

Regarding risk, an investment with a 20x – 60x upside[32] only requires a probability of success of between 2% to 5% to be a positive net expected value investment. Each of us can reflect on his own view of what that the probability is of the foregoing scenario materialising. I'm personally pretty comfortable that, given where we are today in Bitcoin's development and adoption, that the probability is higher than 2 – 5%, likely much higher. While there are many technical, political, regulatory and psychological hurdles ahead, the store-of-value use case is by far the simplest one, and already closest to reality. I would argue therefore that here you have an investment with a downside:upside skew of -1x : 60x and a positive net expected value. Investments with both those characteristics are extremely rare.

While this paper isn't focused on analysing the risks ahead, it's interesting to observe that, of all the potential use cases for cryptoassets, monetary store of value is the one with the least technological risk. While Bitcoin will continue to evolve and improve over time (hopefully becoming more scalable, more fungible, etc.) and those improvements represent upsides, it doesn't in fact need to improve (or at least not materially) in order to replace gold and most foreign reserves. The existing state of the software and the existing network infrastructure is basically in place for this basic gold 2.0 / foreign reserves 2.0 function. Pretty much all that is required for that to happen is adoption and a change in popular and institutional perception and attitudes. In contrast, the more significant EVM-type ambitions of decentralised utility protocols require a number of technical advances and significant investments in infrastructure beyond what we have today. It is reasonable to believe those advances will occur in time, and we should all hope that they do, as they have the potential to make the world a better place, but it is obviously a longer, riskier path.

It is often proposed that Bitcoin's lead as the emergent dominant crypto monetary store of value could be usurped by another existing or future cryptoasset. This is true, but as Bayesians, we arrive at our views using probabilities based on the information at our disposal and update them as new information emerges. Based on the current information available to us, Bitcoin has the highest probability of becoming the dominant crypto monetary store of value, and that probability would appear to be high enough (greater than 5%) to make it a rational investment. As new information emerges regarding existing and new contenders for

[31] To arrive at this target price, I have used a fully-diluted number of BTC of 21 million – 2.8 million = 18.2 million. While the total number of BTC that will ever be issued is fixed at 21 million, blockchain analytics firm Chainalysis estimates that 2.8 – 3.8 million BTC have probably already been permanently lost and are unrecoverable. Even if some of these BTC are later recovered, it is reasonable to expect that more BTC will be lost over time, so using the low-end estimate of 2.8 million for our purposes here seems reasonable.

[32] At the time of this update in late December 2017, BTC was trading at around USD 13,000.

the monetary store of value crown, we can and should update our assessment. So far, as Bitcoin's price has risen, so have its odds of success. For now, Bitcoin appears to remain a rational bet.

The question of forks often comes up and whether forks of Bitcoin undermine its scarcity. Because they share same hash power, Bitcoin forks will either need to demonstrate some differentiated and valuable niche functionality compared to BTC, or they will wither and die in time. As long as BTC continues to perform well as a non-sovereign, monetary store of value, any such differentiated functionality will likely need to focus on less valuable use cases. It's possible that a Bitcoin fork finds such a non-store-of-value use case and survives with some relatively low, sustainable value reflecting the niche functionality it has addressed. It's also possible that the market assigns some fractional value for some period of time to an alternative store-of-value fork either irrationally (an ideological schism occurs and self-sustains for a little while) or as a kind of ace-in-the-hole back-up against some corruption of the main blockchain. In the end, the equilibrium outcome is more likely to be a single, dominant, monetary store of value, and it currently appears more likely that that will be BTC. For an investor who already owns BTC, the prudent investment strategy is simply to hold onto any forked versions that credibly appear to have a sustainable use case and value as they are received. For a new investor, it probably doesn't make sense allocating capital to prior forks due to their lower probability of success and their relatively niche potential value.

BTC v BCH

This is a good juncture to touch on the recent Bitcoin Cash (BCH) fork from Bitcoin (BTC) in August and the subsequent community ideological split behind them following the abandonment of the 2x fork in November. BTC appears to be focusing first on being a censorship-resistant store of value and improving its scalability over the long term, foremost through second-layer solutions; BCH is focused on immediate payments competitiveness through on-chain scaling. At the time of writing, BCH is cheaper for payments than BTC, acceptance of BCH for payments appears to be growing, and there are doubts in some quarters about both the timing and degree of success of BTC's second-layer scaling efforts. On the other hand, BCH is seen as weaker as a store of value and to have a weaker development team. BCH would just be another alt-coin as far as BTC is concerned but for (a) potential user confusion due to the similarity of the names and the ownership of the domain bitcoin.com by one of BCH's promoters, who actively claims that BCH is the 'true Bitcoin'; (b) the fact that BCH and BTC share and compete for the same hash power; and (c) the fact that BCH is being promoted by individuals with significant BTC holdings, who run large exchanges and wallet companies and hold sway over a significant amount (maybe more than 50% collectively) of hash power. Factor (b) raises the concern that, because BTC's difficulty adjustment is fortnightly while BCH's is daily, a significant increase in the price of BCH relative to BTC would cause hash power to swing away from BTC to BCH, slowing or halting BTC block times until the next BTC difficulty adjustment.[33] Factor (c) means that BCH's main backers may try to attack BTC by various means with a non-zero probability of success.

This blog post and this blog post go into scenarios in which the price of BCH could increase in the short run relative to the price of BTC. In a nutshell, if such price swings are temporary, so should be the disruption caused by them, and as a store of value BTC is less sensitive (store-of-value use implies generally larger, less time-sensitive transactions) to this kind of short term disruption than BCH is as a means of payment (generally smaller, time-sensitive

[33] You can follow the swings in hashrate between BTC and BCH here.

transactions). Furthermore, this disruption in block times assumes transaction fees are held constant, but in reality transaction fees can adjust upwards to defend against short term attacks to keep hash power allocated to BTC and keep blocks moving, especially again because BTC functions more as a store of value than as a means of payment and as such is less sensitive to fluctuations in transaction fees.

The easiest and most prudent way to hedge against this risk is simply to own the same number of both tokens.[34] But if forced to get off the fence, the implications of the investment thesis laid out in this paper are that we should bet on store-of-value strength over means-of-payment strength, as we expect the former to be worth more than the latter over time. By focusing on the competitive and commoditised payments space, BCH is fighting for a place in a structurally fragmented use case where it doesn't really seem to do anything new or better compared to existing payment rail cryptocurrencies such as Dash and Litecoin,[35] not to mention the sovereign digital currencies that will soon appear; BTC is currently out ahead on its own as the leading crypto monetary store of value, a use case that is less prone to fragmentation and more likely to be dominated by a single cryptoasset. If BTC is the stronger store of value, it should remain more valuable than BCH and profit-driven miners should continue to allocate more hash power to it over the long run. Tortoise and hare-style, there's also a good chance that BTC's various second-layer development efforts will make it more relevant for payments, smart contracts and the like over time, providing potential upsides beyond the core store-of-value case.

Conclusion

Due to protocols being open-source, the ability to fork, the competitiveness of mining and the importance of relative cost to adoption levels, the value of utility protocol tokens will at equilibrium not decouple from an M = PQ/V valuation, where PQ is the total cost of the computing resources required to maintain the blockchains. This value will likely be relatively low due to the very high potential values of V (velocity) and will be deflationary in line with deflation in the cost of processing power, storage and bandwidth and due to scalability-enhancing innovation.

Public blockchain technology is an incredibly powerful engine for creating significant user surplus, but that surplus will go to users, not to token holders or miners. Investing in utility tokens is in the end tantamount to investing to own a bit of the currency used to operate a big, commoditised, perfectly competitive SaaS business that itself earns no sustainable economic rent. There will be some value there, but perhaps not much. It is possible, and in fact quite reasonable, to construct very bullish protocol adoption scenarios where the equilibrium network values are very low and lower than the current network values of utility protocols such as Ethereum.

While the scale of use of utility protocols may be very large (caveated by the fact that the inherent redundancy of trustless, censorship-resistant consensus mechanisms compared to centralised ones makes them more expensive to operate and therefore only economically relevant for a subset of potential use cases), the potentially very high velocity suggests that this future mature equilibrium value may be thought of as something in the tens or hundreds of billions of USD in aggregate. A sizeable amount, no doubt, but perhaps not sufficiently

[34] The BCH:BTC price is currently hovering around 20% and even if BCH fails to win dominance it is likely to persist and retain value for some time, so the cost of the hedge isn't huge.

[35] Bitcoin Cash's main selling points relative to other payment rail cryptocurrencies seems to be that its name includes the word 'Bitcoin' and that holders of BTC on 1 August 2017 received BCH for free in the fork.

attractive compared to the current ~$250 billion of network value of all alt coins combined to provide an attractive risk/return for investors from where we are today.

In the context of evaluating cryptoassets as money and in a world where value can be moved among protocols with little or no friction, a cryptoasset can be a monetary store of value without being most efficient for payments or a great means of payment without being a store of value. We can therefore look at the potential value of a cryptoasset's monetary store of value function separately from its payments functionality. Monetary store of value functionality will likely be one or two orders of magnitude more valuable than means of payment functionality.

Payments are likely to be fragmented and transaction volumes shared across a range of sovereign digital currencies, off-chain payment systems, centralised payment systems and multiple non-sovereign cryptocurrencies, each with their respective strengths and weaknesses for specific payment instances. This, combined with the fact that payment functionality is analogous to utility protocols and will therefore be valued on a M = PQ/V basis, means that the means of payment value of any given cryptocurrency will be relatively low.

In contrast, the potential value of a winning monetary store of value protocol can be measured in relation to the total value of gold bullion and foreign reserves, suggesting a potential value in the USD 4.7 – 14.6 trillion range. If Bitcoin were to become that monetary store of value (and it currently appears to be the strongest contender by some margin), it could be worth USD 260,000 – 800,000 per BTC, i.e., 20 – 60x its current value. If one places a higher than ~5% chance of Bitcoin succeeding in this way, it is a rational and attractive investment for a long-term investor before considering other potential upsides stemming from payments and unit of account utility. Investing in other cryptoassets based on use cases other than monetary store of value appears less compelling.

Let's be clear. This could all go substantially to zero for various reasons. Being 'right' in an investment with a high risk of failure but a highly positively-skewed distribution of potential outcomes is about getting the *a priori* probabilities right (as adjusted for new information as it arises) and getting position sizing right. Provided you accept that Bitcoin's net expected value is positive, even marginally so, the right answer on position sizing isn't zero. Nor of course is it 100% of assets. For those stuck at the step of whether or not to invest, the logical thing to do is to move past that point and focus on position sizing. If you're more sceptical, invest less. If more confident, invest more. But even for the most sceptical, you might constructively ask yourself, why wouldn't you invest USD 1? Well, rationally, you probably would. Now how about USD 2? Repeat until you get to your Bayesian optimal position size. Given the significant risk of loss, in most circumstances the correct answer is probably a long-term, buy-and-hold, unlevered investment of a low single-digit percentage of assets (at cost).

Addendum: Thoughts on pace of BTC price rise

9 December 2017

How alarmed should we be about the recent rapid run-up in the price of Bitcoin? We read every day now that the speed of the increase itself is a tell-tale sign of a bubble.

Let's think further about how long it could or should take Bitcoin to reach its long-term equilibrium value and the shape of the path it might follow. When considering the potential or appropriate pace of price discovery for different kinds of cryptoassets, we again need to distinguish between utility protocols (including means-of-payment protocols) and a monetary store of value protocol.

When we value the shares of a growing company, we discount our expectations of future cash flows based on the expected growth path of the business in acquiring customers, building its team, building out its infrastructure for delivering value to customers, developing its technology or products, etc. at some discount rate that reflects our assessment of how much risk there is around the realisation of those expectations. This means that a company's shares can be overvalued at price x at time t_0 but undervalued at the same price x at time t_n. To frame this with an example, it is not necessarily inconsistent to say that Amazon was overvalued at $107 per share in 1999 even though it trades at $1,162 per share in 2017. Amazon has grown exponentially and navigated tremendous risks while competitors have progressively ceded market share and while the economy and the markets Amazon serves grew over those 18 years. If you had bought shares when they first peaked around $107 in December 1999 and held them until December 2017 at $1,162 per share, you would have made a 14% annual rate of return. In hindsight that would have been a very good investment, but there are a lot of other companies you could have invested in at 1999 prices that would have been bad investments and it was very difficult to know *a priori* that Amazon would be an exception. A 14% return arguably wasn't all that great, or certainly not excessive, based on a reasonable assessment of the risks in 1999. If you had sat down at the time to do a DCF valuation of Amazon in 2000 and were discounting a set of financial projections reflecting what actually happened, you would have reasonably applied a higher discount rate than 14%. You could have earned a similar return investing for example in a fairly pedestrian diversified leveraged buyout fund with arguably much less risk of loss of capital.

What does all this have to do with how long it could or should take a cryptoasset to appreciate in price? Similar to the shares in a company[36], the growth of the value of a utility protocol (including a payments protocol) should accompany the growth in the number of users, volume of use/transactions, buildout of the network (for example, merchants accepting a particular payment protocol or the installed base of IoT devices running a kind of smart contract), progress in following any development roadmap, etc. So, when we say ETH should be worth $52 billion 10 years, we aren't saying it should be worth $52 billion today. Lots has to happen to make it worth $52 billion in 10 years. Accordingly, you should discount the $52 billion back to the present using some discount rate reflecting the perceived risk of that actually happening, versus something better or worse.

A monetary store of value protocol works completely differently in terms of the potential (or even appropriate) timing and pace of price appreciation. Provided a monetary store of value protocol and the network running it is technically capable of acquitting its function as a monetary store of value (as arguably is already the case of BTC), the pace of it reaching its mature equilibrium value is as fast or slow as the pace of collective mindsets seeing it as such. This could take centuries or only as long as it takes synapses to fire. The value of a bar of gold or of a Picasso at a point in time is simply the value we collectively assign to it. Of course, that value might still evolve over time along with the accumulated wealth of our society and the size of our economy, but it is decoupled from some path of growing cash flows or expected cash flows.

If we relate this back to the potential equilibrium value of a dominant non-sovereign monetary store of value, there are two distinct steps, each of which could take a very long time or only days/weeks/months and with a long or short hiatus between the two. Of the overall potential value estimate of USD 4.7 – 14.6 trillion, USD 1.5 – 4.7 trillion is based on private sector holdings and USD 3.2 – 9.9 trillion on public sector holdings. The first step is

[36] The analogy to equity is used narrowly here in the context of price appreciation. As discussed above, utility protocols are akin to money supply, not equity, in other respects.

for private investors to reach a consensus that it is a strong monetary store of value. It could take a very long time for private investors to reach this consensus, *or* the network value could simply gap up to that level in a matter of weeks or months as adoption moves from just retail investors to institutional and retail investors. This is the stage we're in the middle of today with BTC. Until 2017, BTC ownership was predominantly a retail investor phenomenon, dominated by techie early adopters and some UHNWIs and family offices with connections to tech.[37] Then, over the course of 2017, we saw a proliferation of crypto-focused funds (still collectively only representing an estimated USD 2 – 3 billion across 119 funds[38]). While both those groups continue to grow, we are now seeing the much larger collective firepower of mainstream hedge funds, family offices and (U)HNWIs starting to come in. This could very easily turn into a stampede for the entrance and value could very credibly gap up to at least the low-end private-sector target of USD 1.5 trillion in a matter of months, with subsequent growth to the high-end private-sector target of USD 4.7 trillion happening more slowly over the course of two or three years. The potentially rapid move to USD 1.5 trillion would imply a BTC price of USD 112,000 based on the current number of BTC[39] (potentially relevant given the short time frame being considered) or USD 86,000 fully-diluted[40].

The speed with which this move, especially the first leg of it, could happen is accentuated by the fact that Bitcoin ownership is concentrated; that most Bitcoin haven't changed hands since the price was in the double digits;[41] and that these owners have high conviction and high long-term BTC price expectations and have already weathered tremendous volatility for years without blinking. Fewer than perhaps 1 million BTC effectively circulate at all, and any new money will be forced to compete mostly for those, so the propensity for price to gap up as new institutional money flows in is high.

The second step is adoption by public institutions as a store of value and as a replacement of gold and foreign fiat in countries' international reserves. Of course, this could take a very long time, even after the private sector has embraced and accepted it. Governments move slowly. Decision processes are political. On the other hand, as soon as one government is known to have bought its first Bitcoin into its reserves, we could see a second stampede for the entrance as national treasuries around the world realise they need to diversify at least some of their reserves into Bitcoin before all their rivals do or be left at a strategic disadvantage. So here again, we could see a rapid addition to total network value of the low-end public-sector network value estimate of another USD 3.2 trillion, with that subsequently growing to the high-end target of USD 9.9 trillion (in addition to the private sector value above) over a few years.

The above scenario suggests that the price of BTC could increase by a very steep slope in the very near term as network value moves quickly to USD 1.5 trillion, then a flatter slope as private sector adoption matures towards USD 4.7 trillion and before the first adoption by countries as a component of international reserves. Then we could see another steep slope addition of USD 3.2 trillion to BTC's network value as countries stampede to the entrance, followed by a slower slope appreciation to USD 9.9 trillion of public sector adoption.

An interesting aside is that, with the shares of a company or the price of a utility cryptoasset, the higher the price from time to time, the higher the risk. For Bitcoin, paradoxically, the

[37] And people lucky enough to count Wences Casares as a friend.
[38] https://www.hfalert.com/search.pl?ARTICLE=175427
[39] 16.7 million BTC in existence less estimated 2.8 million lost BTC = 13.9 million BTC.
[40] 21 million BTC maximum less estimated 2.8 million lost BTC = 18.2 million BTC.
[41] https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

opposite may be true up to a point and for certain periods. Right now, Bitcoin is still an insignificant curiosity to the financial markets, with a network value of just USD 218 billion. If and when it breaks through the USD 1 trillion level, it will likely be seen and accepted as a fully-fledged asset class and the financial world will go about building out complete financial markets infrastructure (full suite of derivatives, more robust and liquid exchanges and trading platforms, more custody options). That, combined with broadening private and public institutional ownership over time, will serve to consolidate Bitcoin's position as a monetary store of value and reduce risk. Of course, if at some point price starts to overshoot the potential value estimates for the relevant stage of adoption we're in, we could reasonably begin to worry. But let's cross that bridge if and when we come to it.

Consistent with the overall approach of this paper, the point of the foregoing isn't to say that the above necessarily will happen but rather to look at what reasonably could happen. Depending on what stage of the adoption path we are on and where we are relative to long-term potential network value and the interim milestone value points along the way, it may be entirely reasonable for the price to move up by a lot in a very short period. Such moves don't necessarily reflect irrational, bubble behaviour.

General Talks

BlockCon 2018: Nassim Taleb & Naval Ravikant (h/t http://www.mrsideproject.com/)
October 11, 2018

Nassim Nicholas Taleb and Naval Ravikant

Capitalizing on Tech-Enabled Transformations (Excerpt)
July 20, 2018

Josh Wolfe and Michael Green

If you think I'm missing any major essays/papers, shoot me an email at kevin@12mv2.com or a dm on Twitter @kgao1412 with the subject: "Bitcoin Compilation." Thanks!

BlockCon 2018: Nassim Taleb & Naval Ravikant (h/t http://www.mrsideproject.com/)
October 11, 2018

Nassim Nicholas Taleb and Naval Ravikant

Nassim: So, I'm honored to be here. Hopefully, this will fail because the best way to illustrate the problem with technical devices is by having a failure. Oh, it failed, it's not working. What do you think? Ah, unfortunately, it didn't fully fail.

So, Naval. We're going to do a mono for a little bit and then we'll have a conversation. And tell me during my mono, stop me if I'm covering points that you want to cover yourself.

Naval: Sure.

Nassim: It's much easier. That's the whole idea of having someone to rely upon when you forget your own ideas.

Naval: We're going to keep it interactive and informal.

Nassim: So, this is the German version of Skin In The Game. Given that I don't read German I don't know what it means. But they use the English words "skin in the game". So let me talk about the concept, but it's not as straightforward as you think. So I'm going to start with a counterintuitive aspect of skin in the game before I even define it. It's about how you acquire knowledge, how you do things.

So, my origin, my natural origin is Trader. A lot of people have a natural origin as mathematician or scientist or something like that and then they become traders, I started as a trader. This means I stood with these people at some point and, you know, they spit on you and you acquire all the germs. Particularly if they have children, go to schools, so on, and in a couple of years, it can practically cover every possible airborne disease that the planet can have in staying with these people in the pit. And it's not always crazy but when it's crazy it's even crazier than it seems here.

So, you spend your time as a trader, I was working with mathematical products, I was also trading from a desk as well which is less romantic as this kind of wild jungle atmosphere, so when you do mathematical trading you quickly realize that theoreticians are full of baloney, to be polite. There's something wrong about theory and their view of the world clashes with, you know, with that of every trader. We do things – like people who ride bicycles or say a prostitute being lectured by nuns about, you know, about how to do their business. It's the kind of thing that, academics for us were people really outside the practical world who've never done anything and their models – it's not that they're imprecise, it's a different world.

Okay, so that's how the idea of skin the game came to me. Because, eventually, you retire from trading. You lose hair, I had hair when I started, I lost my hair. You want to do something else with your life. Twenty-one years of trading, you know, you sort of miss it but you want to grow up and become a real person. So what do you do? I kept looking for professions, but I wasn't good at anything else. Then I tried the retirement activities; tennis, do you play tennis?

Naval: No. That's why I don't, though. Terrible.

Nassim: Okay. I can't concentrate, you know, playing tennis. So you lose concentration and particularly when you play – when you have partners they get angry at you. Okay, couldn't play tennis, couldn't play chess for the same reason. You have an idea to start meditating or playing chess and you forget you're playing chess. So I realized I wasn't good at anything. So I said okay, I'm going to give a little academia a try, so I tried – I started an academic career, working on modeling. And telling academics they're full of

baloney, alright. And I'm being polite; the Bologna replaced with the usual things that are clipped on the radio, okay.

So this is the idea, this is my bio: so in other words instead of going from theory to practice, I went from practice to theory. I saw something completely different. So, and let me explain something, I developed something called the Ludic Fallacy. The Ludic Fallacy is that the randomness – and I deal with probability – the randomness that you encounter in real life has absolutely nothing to do with the randomness you find in textbooks or in games. And I used the word "ludic" because ludic means "games" in Latin.

Now, sure enough, someone has a painting for sale at Saatchi you know, or I think exhibited at a Saatchi museum, called the Ludic Fallacy. And I, you know, can't make heads or tails of what it means, alright, but it's nice to have your concept – someone painting something after your concept. He's probably on drugs and painted something and then read the Ludic Fallacy and decide to name what he painted the Ludic Fallacy. Whatever it is I'm just showing it to you in case you can figure it out because I couldn't figure it out.

Now comes the Expert Problem. Still, I haven't defined Skin In The Game, have you noticed, okay, I may leave it to you. But see my bio, started practice to theory, realized that things in practice are much more complicated than theory and that of course in theory there's no difference between theory and practice, in practice there is. And then that concept of Ludic Fallacy because my specialty was randomness and probability, and give it a name as we can see in the painting. So, with this I'm going to explain the Expert Problem because there's two kinds of professions. In The Black Swan I define there's a profession in which the professionals aren't really professionals, and they don't know what the hell is going on yet nobody knows that they don't know or at least, you know, those who pay them don't know that they don't know what's going on – and the professions where people know what's going on.

But how can we make the difference between these two? So in The Black Swan I said okay, in domains like what I call Black Swan fraught – like climate studies, they have no clue. But weather forecaster over next week has a lot of clue, otherwise they can't survive.

So I came up with this idea of Expert Problem, but I can illustrate it best with a story of a friend of mine who's also a trader and had the brilliant idea to go lose his money in the restaurant business. And when you retire, he, you know, he, and it was very nice because he lost his money and prevented me from losing mine in that business. Now, what did he learn in the restaurant business? Something quite central that can illustrate what's going on with our society. All the ills of society summarized in one, as well as the Ludic Fallacy.

In the restaurant business they have awards, granted by newspapers, and of course by other restaurateurs; "the best wood-paneled restaurant in the eastern United States", "the best tuna sushi in Western Canada", okay and then you have all these awards.

So my friend noticed that there was a gala dinner at every year, you know, say every year and during that dinner, the awards are given. So guess what? Most restaurants that got awards were out of business by the time they had the gala dinner. So what's the lesson there? Very simple lesson: whenever you're judged by peers you don't want to impress your peers and that's one thing I learned as a trader.

As a trader there's a rule, and I remember when I was very very young as a trader I had a lot of hair and the badge said "new trader", "new member" it's called. There's an old fellow, you know bald typically, old trader, grouchy and bored, alright, so he said "hey come in here kiddo", he said "stand up here" okay,

he said “if people like you over here, you got to be doing something wrong. Okay kiddo, now you can go now”. Right, so the lesson I learned from when you’re judged by reality; it’s a complete different dynamics than when you’re judged by your peers. So businesses were you’re charged by peers, are businesses – like the restaurant business – will rot, okay, and businesses where you’re d by reality, by your P&L, by your accountant; the only person you want to impress at the end of the day is your accountant. Now, true, you don’t want to be hated by your peers but they’re not the ones whose approval you need to seek.

Now, academia, it’s a business where people are entirely judged by peers. Entirely. This is what causes all the problems we have; bureaucrats – who judges bureaucrats? Other bureaucrats. The boss, this, it doesn’t work. There starts to have meetings, you see, and when a firm becomes very large you start – you cannot associate the P&L attributed directly to a certain person. That you start having meetings, busy, fly to Omaha, come back, you know, do things, you know, talk to you on the phone for two hours, write long emails, stuff like that, that’s the problem.

Naval: Yeah we see this in the tech industry too. There’s a lot of tracking of inputs instead of tracking outputs.

Nassim: Exactly.

Naval: A great engineer can create a billion dollars worth of value, look at Satoshi Nakamoto, and a bad engineer can cost you value. It has nothing to do with the amount of time they put in, yet they’re still managers who want the engineers in at 8:00 a.m., they want them working 40-50 hour weeks and it’s just complete nonsense.

Nassim: Exactly, and trading basically you’re just judged by your P&L; if you lose money, no matter how nice you are, it’s not gonna work and if you make money, no matter how nasty you are, it doesn’t make a difference. So, here, plumbers; a plumber has got to be judged not by other plumbers. You don’t, like, you know, their compensation isn’t determined by like our government calls up other plumbers “how much should we give them in bonus”, alright it doesn’t work that way, okay, it’s judged by you. Same with a dentist; if you show up to the dentist office with your teeth intact and leave the dentist’s office with half of them missing, visibly, there’s a problem, okay. You can catch incompetence very quickly. So there’s a judgment either by metrics, as in mathematics or physics, or in hard science, or engineering, or by some – or because they have laws – or by some the clients, by reality, just like restaurants.

So, but, you have businesses where people are judged entirely by other people. So the minute – this is why you can figure out if journalism is going to die, because journalists try to impress other journalists, that’s their business. They’re not, you know, they’re not trying working on the reader. So you can have monoculture and become very vulnerable. So this to me explains what I call the expert problem; is that they don’t get it, the New Yorker doesn’t get it because they are part of the expert problem. There’s that 1% of people that you’re gonna call the IYI (intellectual yet idiots) and that class of people, they have no accountability to reality they just account to one another and of course they’re gonna have, it’s gonna degrade as a business. And this is where, what do experts do when they want, when you catch them with their pants down? Basically macroeconomists have never forecast anything; a guy like Paul Krugman – I hope I’m recorded, please make sure I’m recorded – Paul Krugman, he knows, it’s like worse than random, okay. Why do we keep – why don’t we replace him with Miss Bri, she’s an astrologist in the Lower East Side, and has a much better track record. Why don’t we … Miss Bri?

Naval: I think the equivalent with this crowd is someone like a Nouriel Roubini or all the people who are recently criticizing crypto.

Nassim: I don't want to comment on my friends. Okay, let me comment on-

Naval: Well, this is a crypto conference, and with a crypto crowd, right, it's become popular to say like "Bitcoin is rat poison" or "it's a ponzi" and so on. And every time one of these experts has called it out as being a failure it goes up, you know, 10x in the next year.

Nassim: I see, okay, yeah. I know, but if these guys had a P&L, there we go, if Paul Krugman had a P&L; he'd be bust long before Bitcoin.

Naval: Exactly.

Nassim: He'd have been bust with the election. Because when you have a P&L you can't really bullshit your way through life.

Naval: And the funny thing is, there's no point in bullshitting financial assets because you can just go short it, just put your money where your mouth is.

Nassim: Exactly.

Naval: But people get into arguments about, online, whether bitcoin is going to hit a certain price by a certain date. You don't have to argue online, you can go to LedgerX, or you can go to your favorite exchange and short it or just take a position.

Nassim: Exactly, so yeah, I have an aphorism that "you don't want to win an argument, you just want to win". It's very different.

Naval: Yeah.

Nassim: So, and here, of course, what do the pseudo-experts do? They compare themselves to pilots, and we know that a pilot is an expert because a pilot has skin in the game. Bad pilots; where are the bad pilots?

Naval: Underwater.

Nassim: Underwater, right, because they have skin in the game, okay. It's even worse – it's not just like a restaurant that can fold, they're gone. So there is a selection mechanism that doesn't depend on judgment of other pilots. At least you know, in the later phases of life.

So that's the problem, so you end up having fields like economics. This is a mind, pick any economist, this is how they think. You know, they have that clarity of mind, that's on a good day, after a cup of coffee, two espresso. That's how they think, and it's just to tell you how their mind works, okay, and they don't realize what's going on. So phase one –

Naval: I made the mistake of getting an economics degree alongside my computer science degree and I can tell you that in 20 years of venture investing in startups, macro has been completely worthless. If anything it's been distraction, entertainment, arguing about things that don't matter. It's just another branch of politics. Micro has been very –

Nassim: Yeah, they're not judged – even micro – they're not judged by any contact with reality, basically. They don't have a P&L; if you don't have a P&L; you pretty much, can, because they can get what I call a "circular citation ring", they can get into any kind of game, grant one another Nobels and nobody would know the difference.

So now I'm going to define Skin In The Game with a notion of symmetry. Okay, so before I was introducing Skin In The Game from the back door, you know, my own experience with it. This is in the Louvre in Paris, and this is Hammurabi's code. It's the earliest code we have found so far 3,800 years ago. This was in a public place in Babylon, most people couldn't read, so there were people who would read it for you, tell them "hey reader, come over tell me what it says", and it says the following: if the architect builds a house, and the house collapses, the architect shall be put to death.

Okay, now, of course, it's quite harsh, it was Hammurabi remember. it's not like, we're not talking about Jimmy Carter or someone, this was much earlier, okay. So how was Hammurabi's law – what does Hammurabi's law aim at? It prevents you from hiding risk. You cannot hide risk and then walk away from it. The architect will always know more about where the risk is located then you, so they can hide it in the basement, in somewhere, they can hide it in a foundation, where they can cut corners and then walk away and go to another city and let the building collapse and say "oh it's no longer my problem, you bought it", ok, you can't, you cannot walk away from the risk you've hidden. That's the core of Hammurabi's law.

And let me show how I encountered it in my life as a trader with something I call the Bob Rubin trade that people still don't understand. It's as follows; Robert Rubin collected 120 million dollars in compensation at CitiBank for over a decade and, of course, stuffing Citibank – he was a vice chairman – and Citibank was in a, you know, taking some classes of hidden risks in like industrial proportion. And sure enough, there was absolutely no edge to these trades, they just blow up infrequently. And in 2008 Citibank was insolvent. And who paid for Citibank? Who stopped it out?

Naval: We did.

Nassim: Taxpayers; we did. Taxpayers, Maybe not you because…

Naval: I'm a taxpayer.

Nassim: You're a taxpayer, but I'm sure you know how to, uh, "defer taxes".

Naval: Trust me, there are no loopholes if there were they would let me know.

Nassim: Okay, but so included in that class of people is your dentist, your bus driver, the uber drivers – they pay taxes, you know. That's because anything online, anything electronic, you know…

Naval: Well the worst part is after these kinds of collapses, they say "never again" so then they put in place tax and policies that actually suppress entrepreneurship who are actually the people who would create the upside black swans.

Nassim: They put more regulation, and then they call it "some very unfortunate highly unexpected event, often called 'Black Swan' for which we apologize profusely but we are excused as nobody can predict these things".

Naval: We're actually all gathered here as a direct consequence of the Bob Rubin trade, because the Bob Rubins of the world lost enormous amounts of money. It was a generational theft of trillions of dollars, both through printing money and through taxes and hidden risk, we all paid for it, but in 2009 an unknown character named Satoshi Nakamoto released Bitcoin and in the genesis block of Bitcoin he cited bank bailouts as the reason why –

Nassim: Why you can't trust the Fed.

Naval: – why he created Bitcoin.

Nassim: Ah really, really, alright.

Naval: I think he was inspired, at least a dedication to Bitcoin in the Genesis block is revenge for the Bob Rubin trade.

Nassim: That's even more impressive, about that story. So, and of course, needless to say, that this has happened many times in history; in '93 there's something called the Resolution Trust Corporation mint 600 billion dollars at a time to bail out a category called savings and loans, they all got rich, one of them went to jail, one single person went to jail, the rest they all got rich and retired, and of course nobody showed up with a checkbook. Like Bob Rubin didn't show up on that day with his checkbook, he just resigned and say it's a black swan. 1982, banks lost more money than they ever made in history, (inaudible), so banks virtually have never made any money they've just been living off of the taxpayer but yet bankers are very rich.

Naval: They just know how to socialize losses-

Nassim: Exactly, they know how to hide their losses. So that's the Skin In The Game: "thou shalt not have the upside without bearing the downside yourself", you need to own your own risk. So that's the whole idea. After Hammurabi of course, we have had a little more, let's say more, what should we call them, more human, you know, softer rules, okay, like don't do to others – no more of this killing architects or something. It became the notion of symmetry, society became based on notion of symmetry, okay. You don't want to punish someone too much you want to punish too little, you don't want to have you know someone victimize others with impunity.

So there's a bunch of rules, of which the better-known one is the Golden Rule: "do to others as you want them to do to you", and I of course in Skin In The Game don't like the Golden Rule because the Golden Rule is a positive rule. If I, you know, I can force you to eat Lebanese Kibbeh, alright, because that's what I'd like to do. So, and it also can invite busybodies, governmental people –

Naval: Yeah.

Nassim: – who make you do things because they like it. So, much more robust is the Silver Rule: "don't do to others what you don't want them to do to you", or the "negative Golden Rule" – vastly more robust.

Naval: It's like all the people who are talking about censorship mechanisms of social media, I think the intellectually honest way is you build the censorship mechanism then you hand it over to your enemy to run it and if you're not willing to do that then what you're basically just saying is "I want to be in charge" but you're trying to do it in an intellectually dishonest way, you're trying to do it a face-saving way where people will give it to you but it's just a naked exercise of power again.

Nassim: I see. So, and, but the Greeks and the ancients were aware of it. Basically that the captain of the ship needs to be, you get off last, not like the, you don't sneak out first like the captain of the Titanic. And then you had rules one of which was that you eat your own cooking. Mercury was walking by one day and a bunch of fishermen had a lot of, I think it was tortoises right?

Naval: Tortoises, yeah.

Nassim: So yeah a bunch of tortoises, in Libya it was or somewhere, and they didn't like him so they invited him to eat the tortoises. So Mercury looked at them and said "do you think I'm an idiot?" okay,

like with a New Jersey accent. Mercury, he said okay you guys are gonna eat all these tortoises, right, first, and then I'll eat the rest. So he forced them to eat their own cooking.

So that has been present in, pretty much, in commercial law forever, as a guiding principle, ethical principle, and you even see entire sections of the Talmud are based on the symmetry. In other words in transactions where there's consideration in the contract, in Anglo-Saxon contract based on consideration; that's where that comes from. Whether someone is taking too much risk for others, like for example in Rodian law, that comes from Phoenician law, for example, if a boat sinks, if you know pirates say take the merchandise or something, who loses the money? How do you share it? Okay, all parties who can benefit from the transaction are obligated to pay the cost, so you have to have complete, you know, equity there.

And there are other concepts like how much information should you disclose to the buyer, say how much should you disclose to the buyer when you have a transaction? There's an ethical – there are series of ethical rules, yes if the buyer is someone from your community you're obligated to divulge everything, but if he's a stranger? How much do you divulge? A lot of ethical rules that have, I mean from that you can see in the Talmud, you can see in Islamic law, and you can see it of course in Roman ethics.

Naval: There's also the phenomenon when you have like long caravans of people crossing the desert or going through a difficult situation like the exodus from Pakistan to India, during that separation. If you were in the last few carts you were most likely to get picked off by brigands and robbers and if you'd lost something there then the rest of the caravan was supposed to make it up to you, they're supposed to repay you because you were taking the most dangerous position in the back.

Nassim: Yeah so this risk sharing, is actually, this was a part of Islamic caravans as well because in a desert it's the same story as robbers will attack those who are isolated in the back, they won't kill you but will take your merchandise and the other people are forced to compensate them or take turns on who's gonna be in the back.

Naval: Right.

Nassim: So this is not new but there are a lot of nuances and as we will see in a conversation, basically, modern life has lost some of these considerations and we'll see how.

At no point in time in history, I'm saying at no point in time with few exceptions; one exception was India another was I think like Egypt at some point, ancient Egypt, and one of them was modern-day France, I mean modern day like hundred years ago France. Except for these situations, at no time in history did you have leaders who took less physical risk than the common person, at no time. The whole idea being a Lord is you've got to protect; you're trading status for obligation to protect, so now you've got to take more risk. And in the Falkland Wars, or sorry it's called the Malvinas in some countries, you know the Falkland Wars they had to find someone from the royal family to fly, you know, take the most dangerous mission in helicopter simply to, you know, confirm that role.

So and of course, we lost that. So you can have some schmuck in Washington, warmonger, okay, you can have warmongers who never take risks.

Naval: Yeah, generals now lead from the rear, not from the front.

Nassim: Exactly, and no, but warmongers, civilian warmongers, whereas in the past warmongers had to be in battle. And what does this symmetry do, is that if you want to cause people to die you got to be exposed to it. It brings some kind of natural balance to society and let me explain how. If you get on the

freeway, okay, you can easily kill 30 or 40 people, okay. All you have to do is go in reverse, okay. If you have a Tesla, a car that accelerates very well even better. Alright, how come you don't see these freak accidents anymore?

Naval: Obvious, skin in the game.

Nassim: Skin in the game. Because the driver, bad drivers, are dead. Just like bad pilots. Okay, there is – so that is a regulator. It's the same thing with wars. Hannibal was first in battle, Napoleon first in battle; Napoleon was actually, they complained, he was way too overexposed in battle, okay, on his horse going around the battlefield, okay, Napoleon. Roman emperors, this is Valerian, a Roman emperor, who was captured by the Persians. Why? because he had to be on the frontline, he wanted to be on the frontline, he's an emperor, you gotta be, you know, you gotta have a little bit of dignity – come on. Julian, my hero, Julian the apostate and the Roman Emperor, died with a spear lodged in his chest. Why? He didn't have a shield. So, you know, you had to take more risk because that's your business.

Naval: Yeah, this guy, actually he ended up being used as a footstool by the Persians.

Nassim: Yeah, footstool. Valerian was used as a footstool by the Persian Emperor.

Naval: That's risk. Holding crypto isn't risk, this is risk.

Nassim: Only one-third of emperors died in their bed, and we're not even sure they died of natural causes, okay.

So we never had that situation, but people aren't fools. You can tell that a person, a warmonger in Washington, working for a think-tank wants to destroy Syria like the way we destroyed Iraq and Libya in the name of democracy, so we destroy because for them democracy is very important. So, they cannot learn from experiences. You can -, never learn from experiences. So these people, but we know they're full of crap, we know Thomas Friedman is just a hack full of crap, okay. It's just unfortunate that people listen to him in Washington, but the general population detects that because the general population can detect if a person has scars or not, takes more risks or not.

This is what's called Zahavian Signaling, in the sense that when you're a risk-taker you have scars, no? And you produce these scars as an ornament. Zahavian Signaling is a concept that we discovered, why do peacocks have these fancy tails? These tails, in fact, are a handicap, it's just to show their genetic superiority that they can function in spite of having these large burdening tails that bring predators because they're good and strong. And they use this – I took this in Jaipur India, this picture of the, in front of me, of the peacock – so there's a concept of Zahavian Signaling, in other words, it's called costly signaling. It's not cheap signaling, it's costly signaling. You see, there're a lot of virtues, we're going to talk about virtues, that are fake because anybody can signal these virtues. But risk-taking is real, you cannot fake risk-taking, you cannot fake risk; you can fake virtue. Or what we call, regularly, virtue.

So this explained to me, fundamentally, why we spend so much time haggling, I mean in theology, over the nature of the Christ – I come from that part of the world where if these discussions taking place, the Greek Orthodox Church, if you had I mean if you had to, if you had a library, you would have probably – you'd fill in a stadium with documents about the discussions of you know, and the arguments of whether the Christ was God or was not God but something like a God.

What's the big difference? And why did they always revert to the notion that the Christ could not be full God, why? Because think about it, if you're God, you don't have skin in the game, it's like in a Superman thing, alright, you have to have some vulnerability somewhere, alright, you have to suffer. So you suffer

because you have skin in the game; that's the whole concept. And in Christology people didn't think of that, effectively, let's think about it; if you go to a circus and see an acrobat with a parachute, or instead of an acrobat with a parachute they show you a movie, alright, of an acrobat. You want the person in front of you to take risks, that's what you want, that's what you paid for, okay, you want real risk because, otherwise, you're not signaling any virtue unless you take these risks. And this is, that was the story of the Christ.

And this is something that people don't get, is that any virtue that doesn't entail some kind of sacrifice or cost is not virtue. The gods in the old days did not let you, you know, just, you know, claim to be their subject or something without paying a price, without having something to lose for it.

And now, in our society, we have fake virtue. What's fake virtue? This is in a hotel room, they tell you "save the planet, dear guest, save the planet". What am I doing here, saving the planet or saving their bottom line? Okay, so they're using the planet as an excuse, alright, that's what I call virtue signaling. A virtue that doesn't cost you anything, doesn't entail any risk-taking, there's no risk in what they're doing and you cannot have virtue that way.

So, here when young kids ask me "what should I be doing?", okay, in life. Start a business. Don't try to get a salary, don't join an NGO because all they do is virtue signaling. Maybe initially the founders really mean well, but then you end up with people trying to game the system. People I call rent seekers. Like the UN office in Lebanon, for example, they talk about deforestation so they can have the staff and they can have the funds so they can fly first-class and get a nice apartment, but when you look at the numbers there's no deforestation, you see. So you have all these, all this industry, of NGOs, so the first thing you tell a young person: do not join an NGO if you want to do well. Start a business and fail, alright. Because, basically, we need people – we can't live off of, if everybody is a seller, you need to fail. To take risks. Just like a fallen soldier, okay, remains more honorable than someone who has never been a soldier. You see, is there such a thing as a dishonorable fallen soldier? No, that soldier is very honorable. Why a dead entrepreneur, or a failed entrepreneur – why should a failed entrepreneur be not something very honorable? More honorable than some who've never been an entrepreneur.

Naval: Come back with your shield or on it.

Nassim: Exactly, come back with your shield or on it. So this is the recommendation, you know, I make: is to start a business. And then one thing I noticed – some people won't like this – but I didn't think that Trump had any chance until I saw him standing with the 11 in the primary, with 11 or 12 Republican opponents. And at a time there was a campaign to explain to us that Trump was an incompetent businessman because he lost a billion dollars, of his own money. The American public is no fool. There's something real about losing a billion dollars, if it's only, if it's your own money. So, although, it makes a professor at a university would think "oh it's horrible to lose a billion dollars", like failing an exam. Life is not an exam. Losing a billion dollars makes you real, and that helped him get elected, at least helped him in that stage of the election in the primary.

So, inequality. A lot of people talk about inequality. First of all there's an error in the way we measure inequality; we measure static inequality. Static inequality in the U.S. we don't do very well compared to say Italy or France. But dynamic inequality, you realize, that if you take 1982, the 1982 Forbes 500 richest people compare them to the 2012, you realize that only 10% of the families cross the list, okay. Whereas in Italy if you do Florence 1620, and Florence 2015, you will notice that the same names will be on the list, alright. You won't find an outsider, on the list. So, you got to look at it dynamically, basically, in America, I think 60% of Americans spend 10 years, sorry, 1 year in the 10 percent. And something like more than 12 percent of Americans spend at least one year in the 1%. So we have the dynamic vs static.

That's the thing, there's something fundamental about inequality. People are willing to accept inequality if the person who is richer is taking risks, you see. You don't accept inequality if it's a rent-seeking CEO making fifty times a worker makes, and people got upset about it. But people are never upset about Steve Jobs being richer than others. And actually the Swiss were trying to pass a law, the Swiss could see the difference, the public who was trying to pass a law, I mean it didn't pass but, you know, it was not close but it was like 30 or 40 percent of people wanted to limit the salary of CEOs, but not entrepreneurs. There's a difference between entrepreneur, because entrepreneurs have skin in the game, to limit, because society doesn't like rich people who made their wealth without skin in the game. You can detect it, that's what's unpopular.

Naval: Yeah, people with a political agenda will conflate equality of opportunity with equality of outcome. Equality of outcome is communism, it's a terrible thing, it requires coercion.

Nassim: Exactly, yes.

Naval: But equality of opportunity is what you strive for, not that you can ever really have it – we all get dealt a different DNA hand, and where we were born, and how we grow up, and what we learn, and what our temperaments are, but you can kind of at least narrow it down through education.

Nassim: But you can measure, you can also measure this inequality, the equality of opportunity with a negative metric. Most people look at the opportunity of people to rise, well if you rise someone else has got to come down, no?

Naval: Right.

Nassim: So you got to take someone else's spot. So, it's not quite a zero-sum game but still, you don't want dinosaurs to stick around, so the best metric is how many large corporations fail.

Naval: Yeah.

Nassim: Today, in the United States, the company's average life in the S&P 500 is 11 years, today, and dropping. It used to be 60.

Naval: But the average price to earnings ratio is much higher than that. But that's because of extremistan, there are a few huge outliers.

Nassim: Yeah, extremistan, exactly. So there's nothing wrong, provided Google has – is exposed to going bust one day, you see. The same with the other firms, some of the firm's in which you've invested.

Naval: Oh, the failure rate for small startups or for small cryptocurrencies, as we all know, is very very high.

Nassim: So I'm gonna finish with a – and then we start the conversation – with one more point, that again is a trader's story, there's something I call the Green Lumber Fallacy, is after the following metaphor. There's a trader who is a fellow who wrote a book on "how I lost a million dollars", which at the time when he wrote it is very respectable, a million dollars was a lot of money, okay. Now, you know, they didn't have the Obama years and Greenspan, printing.

Okay, so how did he lose that million dollars. He traded green lumber, and he knew everything about green lumber. He knew the statistics, physics, chemistry, everything, the supply, the demand, the geography, the consumption – he knew everything about green lumber, read every magazine, every book he could find on lumber. And yet, he lost all his money. Turned out there was in the pit a fellow, an old

trader, who was very very wealthy, and always made money trading green lumber, he traded nothing else. And one day the narrator discovered that that fellow thought that green lumber was not freshly cut lumber, that it was lumber that they took lumber and painted it green, right, and yet he made a fortune using green lumber.

So what does it tell us, it tells us that from the outside, like an academic approaching a problem, what you need to know it's not that, what the fellow who made a lot of money his name is I think Siegel, like Jerry Siegel or something like that, was that what he knew was not like it's not like he didn't know anything, he knew a lot of stuff, but that stuff you can only detect from the inside, you can never know from the outside what it is, you see.

Naval: You have to play the game to understand it.

Nassim: You have to play the game to know what you need to know. Okay, from the inside not from the outside.

Naval: People are always asking me to recommend a game theory textbook, and the reality is I never read a game theory textbook, when I was young I just played a lot of games.

Naval: Okay, there you go. So you, from being in that game you see things differently. Which is why education, I think, in Antifragile – and hopefully we'll discuss that – in Antifragile, I rail against education.

And then finally, my final slide, and we're going to start a conversation, is about the following quiz. Which applies to any business where there is skin in the game. Say you go to a hospital and, for your brain surgery, you need to have a brain surgery, which probably will enhance your mathematical skills, there's a special surgery, alright, you go and you can do integrals after that surgery. So you show up to the hospital and you have the choice between two doctors; the first one looks like what Hollywood here would put in a movie, you know; measured, clear English, Harvard degree on the wall, someone who really looked like a Hollywood doctor, Hollywood version of a doctor, a brain surgeon. And the other person, same rank in the hospital, looks like a butcher; thick fingers, no diploma on the wall, and speak with a thick New York accent, okay, like you can put him in a mafia movie if you're going to put him somewhere, alright. So, and no diploma on the wall means he's embarrassed by his background.

Which doctor should you rationally pick? Who would pick the butcher? Who would pick the slick Hollywood doctor? Okay, there you go. So the point is; unconditionally you should pick the Hollywood doctor, right, but here they're the same rank in the University so think about it; the person who looks the least like a doctor has got to have the most skills because he had to overcome the perception bias against him.

Naval: There's a similar learning in early-stage investing, where you tend to avoid teams that look incredibly polished.

Nassim: Exactly.

Naval: They have good powerpoints, they're well dressed, they present well. What you want is the person who's been busy in front of the computer, flustered, gets up in front of a whiteboard, explains things a little too complicated but has the genuine substance.

Nassim: Exactly.

Naval: But the form alone lets you avoid it, so you get business plans that are too well written and they use too many buzzwords and you reject them just on that basis, you know.

Nassim: I would take it one step further and argue against a business plan; anybody who's capable of writing a business plan, you don't want to invest with them.

Naval: Yeah.

Nassim: So okay, so now let's start the conversation, based on these things-

Discussion

Naval: Yeah before we get into it, I want to give Nassim a proper introduction because I should have done that at the beginning but I didn't know I was going to be part of the presentation. I normally have a rule that I don't travel for conferences, and neither probably should you because they fall very much on this whole side of signaling, right, where you're kind of like looking busy for your boss rather than actually doing work. Now there can be huge benefits, you can network with the right people, when they're small you can meet the right people, but you know sitting in an audience doesn't have that much value for you, you could sit at home and watch it on YouTube.

So I normally don't travel for conferences, but when I got the opportunity to speak with Nassim, I had to come down from San Francisco. To me, he is one of the very very few living natural philosophers; which is someone who practices science, does real work in science, but outside of a scientific institution, outside of the credentialed system and I think his work is the kind of work that will last for a thousand years. I don't say that lightly. But I think people will be reading, you know, there are books that Nassim has written and I won't insult him by calling him Dr. Taleb, is that ok – I'll just call you Nassim?

Nassim: Yeah, it is an insult typically.

Naval: Yeah, so I won't insult you by calling you Dr. Taleb, but Nassim has written books that I think people will be reading a thousand years from now. His new book Skin In The Game is fantastic, it's part five in his Incerto series which includes Fooled by Randomness, Black Swan, Antifragile, The Bed of Procrustes. It's written in a very timeless way, the concepts are very simple, there's not a lot of math to it although there is a huge math backing to the Incerto if you want to get into it, and I would rather reread his work than anything on the bestseller lists, and I have. Many of his books I've reread. Now the interesting thing is that I I do get push-back when I say I'm talking to Nassim because people say "well, he's so angry", "he's so mean", "he's so rude", because they can't they can't fight him on the math and they can't fight him on the principles so they go after just the-

Nassim: Also I think it's that I derive a huge amount of pleasure from Twitter fights.

Naval: Yes, and he does.

Nassim: Yeah, so and why do I derive pleasure from Twitter fights? So think about it, if you're bored it wakes you up. And at the gym, you see, I'm into weightlifting and you have to take 15-minute breaks between sets – perfect time.

Naval: Yeah and I think, you say that you do it for fun, but I think it's also it's having skin in the game in your principles, right, because as you say courage is the only virtue that cannot be faked. I can fake any virtue on Twitter, but the one that I can't fake is courage, and that means going up under your name, not under some troll account name, and taking on somebody that you think has unfairly benefited from

exploiting the system like the Bob Rubin trade for example, or the IYI's, the intellectual idiots, that you call out and name, or when you call out Monsanto.

Nassim: Yeah, but he's giving me too much credit, alright. I just, I don't do it because of these principles.

Naval: He just likes to fight.

Nassim: I do it because I get bored, alright, and sometimes waiting in line or in traffic, when you're stuck in traffic, that's the best time for a Twitter fight. So, really it's not as lofty a goal, but it so happened that, okay, it, you know, can impress people.

Naval: I mean there's not a lot of people that'll take on Saudi Arabia on Twitter and call them Saudi Barbaria on a regular basis. But anyways, so I'm very happy to be here with Nassim. I think the books are absolutely worth reading, if you haven't read all 5 of his books I wouldn't read anything else this year I would literally just absorb them. And I don't say that lightly. That's true for me; like I'm going through Skin in the Game again a second time.

Nassim: He's gonna convince me to try to read my books now.

Naval: Yeah, they're amazing.

Nassim: The first one was finished 20 years ago, so you gotta understand that I'm –

Naval: Well there is some redundancy in there, as you would expect, and I think a common theme that Nassim pointed out to me when we talked earlier running through the whole thing is this concept of symmetry and asymmetry. Skin in the Game is about symmetry between your consequences of your actions and learning and feedback loops, and asymmetry is about extreme outcomes, so you know Black Swan and those kinds of principles. So I think we can just dive into it.

Nassim: You want me to explain to them of the symmetry thing?

Naval: I'm sorry?

Nassim: I didn't put slides on symmetry, hoping – you want me to explain it to them?

Naval: Yeah, I think – yeah, let's go ahead, why don't you explain symmetry and asymmetry in your words.

Nassim: Okay so, in other words, you don't understand random events, you can't predict what's going to happen. But you can pretty much tell how the random event would hit you, no? You know whether you're gonna make from it, lose from it, make a lot, lose a lot, okay. So you try to position yourself in a way to benefit more than you would lose from a random event, okay, or to lose less than your neighbor from a random event. That's the idea of asymmetry. It's pretty much like an option, when I call an option. An option you make more on the upside than you would on the downside. And if you, in general make more from a random event than you lose from it, then you're gonna do very well in the long run provided you make sure you're going to survive. That's the asymmetry that's present in contracts, and options, stuff like that. Asymmetry becomes bad when you make the upside, like Bob Rubin, and transfer the downside to someone else, and the easiest thing to transfer to, a person to transfer to is the taxpayer, anonymous taxpayer, you see. That is an asymmetry, okay, a bad asymmetry. But tinkering, trial and error, it is – has a really positive asymmetry. So, a simple, you know, example I give is if we wanted – what's your favorite dish?

Naval: It's pizza, but I shouldn't be eating it.

Nassim: Pizza, okay, so pizza. Okay, so let's say we decide to make the best pizza, we would call it the Santa Monica flying pizza, alright, here. So you rent a bus, you go to the local university and bring every chemist, run up every chemist you can find, okay. And then you take another bus and round up every overweight person you can find in LA who's well dressed, this is my metric when you go to a restaurant is look at for overweight people who are well-dressed. That's sort of like, you know, my thing. So, and then, so we have two crowds now, okay. So if we ask the chemist, that's the top-down, okay, to invent that pizza, you ask the chemists, you have about 150 chemists all looking boring and poorly fed and visibly not well dressed, and then you ask the well-dressed people, whatever, and overweight, you tell them listen, let's make the best pizza. So the way you do it is you take an existing recipe, and you start adding ingredients to it, no? And you taste, if it's good you ratchet it up, okay, so you have the upside. If it's good, you discovered something that really has good taste, you go up, or ratchet it up, in other words you lock up your gain, okay. Now, if it's bad you give it to the chemists; very little to lose, alright. So that is trial and error, a lot of trial and error, and I showed in Antifragile – and that's the main argument – that trial and error will always outperform design, simply because of that property. That we're vastly more intelligent, we have an IQ of a thousand when we do trial and error.

Naval: Yeah these basic concepts, by the way, are cropping up all over in cryptocurrencies like Bitcoin, that it is literally a lot of your principles realized. Like Bitcoin, for example, is an asymmetric bet; if you lose, you just lose your money, if you win – if it becomes digital gold – you can make 50 times or 100 times your money, so it has that option –

Nassim: Obviously depends on what price you buy it at, if you buy it at $100,000 maybe not, if you buy it for here, maybe.

Naval: For sure, yeah. But it's also antifragile in the sense that every time it survives a hack or an attack or a failure of some part of the ecosystem, the developers improve the code, they improve the system, and then it gets better at surviving future shocks.

Nassim: I see, so that's Antifragile, yeah. So this idea of symmetry, you say convexity because a convex function is very simply makes – you make more when you go up than you lose when you go down, okay. And it links to fragility, it's antifragile, because fragility has the exact opposite attribute, you see, if I jump from 10 meters I'm harmed more than twice that if I jump from 5 meters, and more than 10 times if I jumped 1 meter, and more than a hundred times… so that's concave, it means you don't like volatility, and if you're convex during that range you like volatility. You'd rather have volatility, you'd rather have shocks, you'd rather have turmoil. So this is the idea of antifragile, which applies to both the physical system and anthropology.

Naval: It's like people who are shorting cryptocurrencies, they're on the wrong side of that. They're doing concave trades.

Nassim: Concave trade, yeah. Because you have a lot more downside, I mean, think of Paul Krugman bearish at what, 40?

Naval: Sorry?

Nassim: He was bearish at 40? He was short –

Naval: Bearish 40, yeah.

Nassim: Imagine his P&L, if you went short at 40, okay, think about it. First of all, you would never hear of him.

Naval: He would have lost 100x, yeah.

Nassim: He would have disappeared if he had a P&L, so this is why, you know, I'm glad he didn't because we want to just have someone to make fun of, alright. So, surprisingly he doesn't engage me in Twitter fights. Because, simply he doesn't, for some reason. He attacks other people, but not, for some reason, he doesn't.

Naval: It's easier to attack people from behind the shield of the New York Times than it is to go out and battle by yourself.

Nassim: Yeah, that's true. But even the New York Times, they don't. By the way, I saw a copy of it, Skin in the Game was open as a best-seller, two on a best-seller list, without a single book review. Not a single book review in America, in the United States, zero, okay. Just to tell you that we don't really need the New York Times. Ok, it's becoming…

Naval: Yeah, even in my industry what's funny is that people give out awards like VC of the year or Angel of the year and so on, and they're all nonsense because the reward is in investing and making the money, you know. Like, who wants to win the award for a Bitcoiner of the year? You just want to own the bitcoin, right?

Nassim: Okay, so there are a couple of things we're going to talk about, the Lindy effect, linked to fragility, like the test of time.

Naval: Yeah.

Nassim: You present the Lindy, but let me first say one property of the news that was – that's not, you know, never existed before in history. Before 1940, or 1946 I think when families had a television set, so you have a small family now watching television, getting one-way information, reading the New York Times, you don't go to the square, you don't get – okay, before that period in time, people did not get the news from one source, they, it was like Facebook or Twitter. People traditionally were both conveyors and recipients of the news, so we're all involved in the news making, you see. So you go to the barber, you get the news, you go you transmit it, you tell the fisherman, they counter, then tell your barber you bring back information to the barber that was – so, news were something that was organically spread in society and it was nobody could control it as a source before the 1940s propaganda, New York Times, all that era of television, and we broke out of it with Twitter and social media. So and there's a concept called Lindy and the news, the way, you know, it was organized during that period from 1946 to the election of 2016 was not Lindy, can you explain to them what Lindy is?

Naval: Yeah, Lindy just means sort of stands the test of time, which is like any book that's been around for thousands of years is likely to be around for thousands of more years. The best predictor of the survivability of something is how long it has survived.

Nassim: For some-thing or all things?

Naval: For certain things, for things in the intellectual domain for things in the social domain.

Nassim: Exactly, so it was discovered Lindy is a restaurant in New York that has cheesecake, it was a horrible cheesecake, and I spoke about it and discussed it in Skin in the Game and it had the great idea to go bust on the Tuesday the very the same day Skin in the Game was published, alright, after 60-70 years. So Lindy was a restaurant were actors used to meet, and they discovered that plays that survived 200 days had 200 more days, a thousand days? A thousand more days. They discovered that rule. So you can classify things on whether they're Lindy or not. Now Lindy tells you that technology, okay, it's gonna be,

old technology will outlive new technologies. Not because new technologies are bad, but they will be more vulnerable, new technologies, to other newer technologies whereas old ones are not.

Naval: Take the fork, for example, it is a piece of technology that's become invisible to us but it is technology, something that helps you eat things, and the fork is going to be around forever – it's a tried-and-true model. And the fact it's been around thousands of years means it'll be around for thousands of years.

Nassim: There's something in blockchain, the concept of transaction coupled with, a commercial transaction, coupled with a financial transaction that's entirely Lindy.

Naval: Yeah.

Nassim: And that's the letter credit, which itself was replicating something used in maritime commerce. In other words, banking they devised this system by which you can – you trigger a currency the minute you deliver the merchandise. Now you own – you go there with merchandise, you come back with a currency. So mixing the physical transaction with the financial one, all in one, it's the same transaction, coupling them, is an old very old thing.

Naval: Yeah and in crypto, like, Bitcoin is the Lindy currency. It survived a long time, survived the longest, and it won't be digital gold until it's survived long enough, but the longer it survives the longer it will survive, the more faith people can put in it and the more money they can put into it,

Nassim: Exactly and government-issued currencies has never been Lindy. People don't realize, and you can you get a clear idea if you read history, okay. You know the story of the, remember the story of the Christ in the temple? Why did he fight the money changers? Why were there money changers in the temple? Because God of the temple did not like all these currencies, he didn't trust these currencies, he wanted the shekel of Tyre and now current day in Phoenicia, okay, because they're the only reputable ones. So he forced cities to, you know, to compete on who's gonna have the most solid currency for the god to take it, and then money changers would change into that shekel of Tyre.

Naval: God's practical.

Nassim: So, currencies have always – I mean the governments have always debased their currency.

Naval: Yeah.

Nassim: And but yet citizens had the choice between currencies, what currencies to use and what would God want? He would select the one that was the least debased.

Naval: You pointed out that one of the big things in history was separating the state from church, and some religions have done that and some haven't, where they still combine them. But that was a major revolution; you render unto Caesar what is Caesar's. And the interesting thing with crypto is we're trying to separate money from the state and that transition, if it successfully happens, will probably be just as impactful and take quite a while to play out.

Nassim: I see, and it is interesting because if you start having competition between cryptocurrencies, it would be the same competition as the one that prevailed in ancient times between issuers. Because, you know, the was a Sater of Asia Minor, each King produced his or her, Queen her own currency, and then you'd go by the one that was the least prone to debasement, the one you can have faith in.

Naval: Right, in my opinion it's good to have the competition though because it makes them antifragile, it exposes them to randomness and variation and makes them evolve.

Nassim: Exactly, exactly. It's not until recently, where you're forced, you know, you can only conduct transactions in peso, dollar, and this and that. In the past, people picked the currency that was the most reliable for transactions.

Naval: Yeah, another point in asymmetry that you brought up which I thought was very counterintuitive, at least for me, and completely changed the way I think about many important things in the world, is the Minority Rule. I don't think that one's obvious at all. It's one of the things that maybe it's obvious in hindsight, once you fully understand it, but I think the repercussions aren't obvious and the fact that even it is a very stable outcome isn't very obvious, so I'd love for you to just go to the Minority Rule.

Nassim: Okay, I discovered the Minority Rule one day, ironically, I was trying to explain what a complex system was at a barbecue of a complex system Institute, okay. And that complex systems have one attribute, that at different scales things behave differently, okay. So in other words, a collection of individuals don't behave like separate individuals, they behave as separate animals, a very separate animal. Which is something that a lot of people don't understand in government today, is that if I understood the psychology of each person in this room I can't predict the collective, how they will behave collectively, okay. But nurses know that, people know that from children, alright, you know you could predict each child independently put them together it's unpredictable, okay, it's a different animal. So that's the concept of complex systems.

Trying to explain it, okay, I was hit with the best example of a complex system because at that barbecue there was, there's, you know, it had food, alright, and drinks and a delegation came from Jerusalem and they're all Orthodox. Bunch of people. So a fellow showed up, you know, to say hello and I felt embarrassed, I said "oh I'm so sorry we don't have kosher drinks". He looked at me, he said "all drinks are kosher here" I said "what?" he said "yeah, where'd you buy the drinks?" "here in Boston" "okay, they're going to be kosher". What? I googled the proportion of kosher eaters and drinkers in America, less than 0.3%, that's on a good day, alright, a religious holiday; 0.3%. Yet close to a hundred percent of drinks in America are kosher, why is that so?

Naval: Because the Jews run the world. [laughter] Don't quote me on that!

Nassim: No, no. You're being filmed, you're being filmed. It's because of this very simple concept, if let's say I'm coca-cola what are you going to have: kosher coca-cola, nonkosher coca-cola? Alright, you're gonna have different departments, different things, different trucks so they don't get mixed? And then supermarkets will have a different, you know, ailes? This is kosher ailes? What you're going to do is just make them all kosher, okay. Those who, like me, don't know the difference, okay, will drink coca-cola – I don't drink coca-cola – but so it so happened that when we looked at the bottom of the lemonade bottle there was a sign saying it was kosher, that only the kosher people know how to identify, okay. So that's the Minority Rule. So if a martian came from space and sampled food preferences, okay, he would say that America's 100% kosher in drinks, okay, not 0.3%, so why? There's an asymmetry, the kosher person will never drink not kosher, but the nonkosher you see can drink kosher.

Naval: Yeah, that's the key, that for the minority to control the majority, the minority has to be intransigent. They have to be absolutely unwilling to go along.

Nassim: So, for example, people didn't notice one thing about the preferences, marketing preferences, they don't understand, they look at marketing preference of individuals and they make cars accordingly.

Most Americans at a time when where cars were, you know, still had stick shift preferred stick shift – the majority, seventy-five percent. But most of them had a family member who didn't like stick shift, so you're a family of five and one family member, at the time that people didn't have a lot of cars per household, one household member can't drive, so what do you do, this is gonna go automatic.

Naval: Yeah. Also, I think if someone in the house has a peanut allergy or gluten allergy their whole house ends up with no gluten or no peanuts.

Nassim: Exactly, same thing. So there's nothing wrong with accommodating the minority, so long as you know it. Now the interesting thing about the Minority Rule is that seems to me that it's a norm rather than the exception in society, and about anything. The reason we have non-smoking spaces – I joked with a friend of mine, one day I had a French visitor. When I was a student and he came, you know, he met me, I said meet me in front of this restaurant and book a table, He couldn't find a non-smoking table. I told him did you try the smoking one, he said yeah, I said okay go buy pack of cigarettes and we'll go to smoking section. He believed he thought that, you know, you're forced to smoke in a smoking section. So, and we smoked in the smoking section, to be there, play the game. So, but, really we have these asymmetries actually running our lives. The formation of ethics.

Naval: Yeah and actually, so, this is very interesting for me because like on Twitter, for example, if you go on there you will always find somebody who's outraged about something, right. There's someone in the extreme left or the extreme right in politics, or in cryptoland, and they're just really angry about something. And for a while I thought they were just being super ineffective, and that's what I was hoping, I was hoping that the most outraged, most angry people are actually very ineffective and they're just misguided and they're kind of on the corner. But the sad thing is the minority rule kind of shows that if these people are intransigent enough they actually run and control society, they establish the laws for the rest of us. And we kind of intuitively know this, like from revolutions, like revolutionaries tend to be small bands, small groups that won't put up with the status quo that overthrow the entire system. Because most people in the center just kind of don't care, they just kind of want to get along, and they want to go along.

So this comes back to, like, if you're willing to tolerate intolerance then you're gonna live with the consequences. If you look at for example elections, there is a belief in politics and political science that it's the voter in the center, the median voter, who everybody competes for and decides how the election runs. But that's not true when you have third parties with intransigent minorities. So, for example, if the Bernie voters absolutely will not vote for the mainstream Democrat, the Clinton, or if the extreme, you know, right voters won't vote for the Jeb Bush, then they'll actually stay home or they'll vote for a third party. Then you actually have to appeal to them, you have to go with their preferences. As long as there's enough of them, it doesn't have to be a large number, it's just a few percentage points and they're enough to control the entire outcome. So we live in a world that is actually structured around the preferences of radicals who won't compromise, it's not built around the will of the majority, the will of the majority does apply in some cases but in many more cases it's the minority rule and there are all kinds of other implications –

Nassim: Ethics – I mean ethics, for example, people have the illusion that society is getting more ethical because the majority is becoming more ethical. No, no, it's minority rule. Another mistake made by Monsanto is that when introducing GMOs they thought that all it took was convincing 51% of consumers to have GMOs, okay, they did not think it through properly because think about it; all you need is 3 percent of people who are absolutely against eating GMOs, alright, and then you're gonna have a party here to celebrate the collapse of, say, Saudi Barbaria, say, okay, we have a party, alright, what do you do?

You send a list saying GMO / non-GMO? We make everything non-GMO. You make everything organic. And the difference in price, when the difference in price is small everybody switches to the one that the minority wants, to the choice of the minority. When difference in price is large, then you may have two varieties. Like, for example, for meat; kosher meat and kosher stuff is much more cumbersome to have everything kosher, because it's more costly and it's complicated.

Naval: Right, so there's the evidence the Jews don't run the world.

Nassim: But believe it or not, 100 percent of the meat you get, imported meat, imported lamb, in the United States about a hundred percent is halal. Because New Zealand exports, ok, they're the main exporter, what're they gonna do, what if put in a ship to Malaysia what if Malaysia doesn't want – there's less demand – we're gonna de-halal it to send it to the United States? So they made everything halal, so all their meat is, all their exports are halal. So, at Christmas, I saw this at Christmas, halal was – because I can detect, I read Arabic – it was all halal, yeah so it was probably, you know, they produce it and then we don't have to worry about merchandising, about perishability, and stuff like that, to make it make everything halal it's much simpler.

Naval: So the minority rule applies when the minority is not willing to compromise, when it's relatively distributed amongst the whole population. Like if they're off by themselves in a corner, then maybe you can service them just as a minority and leave the majority.

Nassim: Exactly, if you have a geographic diversity, ok, then you don't have minority rules, alright, if you say the people who eat halal live in the neighborhood, people who eat kosher live in the neighborhood – have their own ecosystem – then you'd have, you won't have minority rules. As you open up the country, then the minority rule would prevail about anything.

Naval: Yeah.

Nassim: And conditional on the majority not being ticked off by it.

Naval: That's right.

Nassim: In Europe, for example, now pretty much schools have to have halal meat, and you have reaction. People didn't know, I mean, you should have done it in a more –

Naval: Quiet way.

Nassim: – surreptitious way. Yeah. But because parents say no I refuse, you know, that my child eats halal, okay. Now we have a counter-reaction. Just like the Christians, in a Roman world, halal meat resembles all sacrificed meat in the near East, actually. You have to, you know, sacrifice the cow or the lamb, the sheep in a certain way. And Christians would never eat sacrificial meat, you know, in the old times pagans would have sacrificial meat and then a lot of people would die of hunger in front of a table full of meat just to show that they were Christian and they would not eat sacrificial meat. Because for them it's polluted. So you may have a counter minority rule coming from somewhere, you see.

Naval: Yeah, I think for, there are cases where the minorities themselves are – and a minority here obviously you know what it means, it means a small group of people who are intransigent – themselves are very intolerant of maybe even the existence of the majority or the way the majority likes to function, so it does create a counter-reaction, so it's not that all revolutionaries, you know, necessarily control the world, very often they just get lynched or stamped out.

Nassim: Exactly, so we have a thin balance here between majority rule and minority rule. And Tocqueville wanted to protect the minority from the majority, alright, and now we may have to do an inverse Tocqueville as well to bring symmetry, protect the majority from the minority.

Naval: Yeah, it applies in crypto, for example, if imagine that you know something like, I don't know, if I had to make up a number like call it like ten or twenty percent of the good developers in Silicon Valley are now working on crypto related projects, or at least dabbling on it. And if they all announce tomorrow that they are only gonna work for companies that pay them in crypto then pretty soon you would see every payroll system switch to also offering crypto payments.

Nassim: That's true, if you're unconditional about getting or paying or receiving in crypto, you install the minority rule.

Naval: Minority rule is a very powerful concept, it's one of the ones in Skin in the Game, I highly encourage you to go through it. Let's talk a little bit about black swans, which is an old concept, you're very famous for it, did you coin the term?

Nassim: No, Black Swan term was, the earliest use of it was by a Roman poet who said that a good person is as rare as a Black Swan. And it was used for something, you know, rare but not completely impossible.

Naval: Yeah and now we see them everywhere, now that you kind of popularized it I think it's very –

Nassim: Because now we use as a logical problem, that no matter how many white swans you've seen you cannot rule out a Black Swan.

Naval: Right.

Nassim: But there's an asymmetry, if you've seen one Black Swan then you can say that there are black swans.

Naval: It's kind of like how science works too, where you can never completely prove anything you can only make it falsifiable, you can only disprove, disprove, disprove. Right, so anytime somebody says this is proven by science, they usually don't understand science.

Nassim: They don't understand science, or they work for Monsanto.

Naval: Yeah.

Nassim: Or the ex-Monsanto. When they say it's proven by science. Science is not about proving, science is about disproving and having something that has not been producing a result that has not yet been disproved or superseded by something else. So it's a process, not a result.

Naval: There are whole branches –

Nassim: But science is a minority rule by the way.

Naval: Yeah?

Nassim: Yeah. Science, when someone tells you 300 Nobel Prize winner said this, okay. That doesn't count, because one counterexample can destroy the whole argument.

Naval: Right. Consensus doesn't matter.

Nassim: Consensus doesn't matter, it works by minority, but the system is there to protect that minority that is right against the majority, except in economics, of course.

Naval: Right. Like was it Galileo who said "but yet it moves" when he was –

Nassim: Yeah, yeah "E pur si muove".

Naval: Right. Very interesting related concept that you've tried to bring into the mainstream, which I don't think has quite gotten mainstream yet, is Ergodicity. I don't think most people understand it, I think it's one of your more complicated concepts, I think I finally do understand it, but I'd love to have you explain it and see if we can spread the meme a little bit.

Nassim: I'm gonna explain one thing, one thing that if, called path dependence, if you wash your clothes first and then iron them, say you wash your pants and then iron, you get different results from if you ironed your pants first then wash them, okay. So the sequence matters, no? Okay, so it's trivial, but you need to analyze things dynamically to get that point. So, Skin in the Game really is organized around two concepts, things seen statically that when you view them dynamically have completely different properties. And you can only get that if you're either super smart mathematically, which nobody is, or have skin in the game because you realize that. So, if you go to a casino and you have a small probability blowing up, no matter what your edge is, you will blow up. That's it. So no matter what your – because you cannot say okay I'm gonna blow up and then get rich, you can't, you've got to get rich then blow up. So the sequence matters. So that is the path dependence, we detect it. This is the reason why we're paranoid.

And I noticed that there's a guy who got a Nobel, Thaler? A pseudo-Nobel, in economics, it shouldn't count, should count as a negative, alright. So and then all his work is based on showing how we are irrational statically, okay. He, for example, in one of his – the example where he shows we're irrational – if you go to a casino and play with house money in the sense that you bet small and that you win big, if you win big then you risk big, but if you lose you don't take risk. So in other words, your initial endowment you try to preserve it, but you risk everything you make from the casino, okay. He found it irrational, but if you look at it dynamically, that's what every trader does. You play with the house money. If you don't follow such a strategy you're eventually going to go bust one day.

Naval: Right.

Nassim: Because you can't say I can look at the average return, because if you're bust on day 28 there is no day 29, you see. Whereas if you take an average of people's returns, if number 28 goes bust, number 29, you know, can operate freely. You see, so that concept of path dependence was not incorporated into the psychology of decision-making and therefore they found that we're irrational in many places where in reality we're not. Because if you look at things in sequence, you see, so you gotta always look at things in sequence not look at things statically.

Naval: Right, so like a lot of behavioral psych studies and economic studies will say that if I offered you a billion dollars to play a Russian Roulette, right, and six people play Russian roulette well five out of the six make a billion dollars each. So assuming that your value of your life is lower than a billion dollars, you'll play Russian roulette once. But would you, one person, play Russian roulette six times? Alright, no. So confusing those two, the probability of a group going once each versus an individual taking all of the risks in sequence gives you completely different answers. And there's this concept, which I'm sure you've all heard, of loss aversion where, you know, people are irrationally loss averse. No, they're not irrationally loss averse, they're rationing loss averse because if you go bust you can never recover. So

like, for example, in your crypto asset accumulation and trading if you go super short and you sell everything and you lose everything you'll never get to get back in the game. You have to stay in the game. And it's kind of an obvious concept once it's explained and described, but there are entire books written on it. Like the Kelly Criterion, and Fortune's Formula, that book and so on. But uh –

Nassim: Yeah, only traders and mathematicians will do information theory or computer science get the point like Kelly, Shannon and Shannon entropy, they get the point that you got to look at things dynamically. But psychologists are so naive and they keep getting Nobels, you know, they're naive by saying we're irrational to be paranoid, they don't understand that, you know, dynamically if we were not paranoid we wouldn't be here.

Okay, so you cannot analyze one event, you got to see how that event is going to shorten your life expectancy, so there are some classes of risk you should never be taking. And effectively when you take Goldman Sachs, been around 159 years, you may hate them – I hate them – but you gotta admire how they stayed alive. Why? They never take risk of ruin, and that's the same thing as a lesson I had as a trader by an old trader who came and told me "listen take all the risk you can but make sure you're in tomorrow". So make sure you survive. So it tells you that you gotta gear your risk taking first toward survival, and that entails you take more risk as you're making more money, with the casino money and that, called mental accounting, is deemed irrational and being paranoid is deemed irrational because they only look at the single event, not series of events.

And something has been happening now with psychologists, we're in the middle of a replication crisis and their papers don't replicate, and those that replicate don't really have the same effect, so, which tells us that whatever they call science is vastly outperformed by your grandmother. So, if you go ask your grandmother, particularly if she has Mediterranean wisdom – I'm biased, right, so Mediterranean or some kind of Russian, particularly, but the babushkas are, they're very – ask grandmothers, alright, so, or grandparents or grandfathers as well, they will whatever they will tell you will be Lindy, will have survived the test of time. And if psychologists agree with your grandparents, okay, means they're right, if they bring something new that your grandparents didn't know, odds are it's going to be suspicious.

Naval: Yeah any field where you need to add the word science to the end to make it seem legit probably is not.

Nassim: Exactly. So this, just if we were to summarize, because time's up –

Naval: Yeah they're flashing "time's up" at us.

Nassim: They're flashing time's up, but possession is nine-tenths of the law, so –

Naval: Yeah, exactly; until the audience leaves, we're here.

Nassim: So, to wrap things up here, what I was saying in Antifragile and in Skin in the Game is there are two things that are wrong when you analyze naively, is scale; a large country is not like small cities that you blow up, Singapore is not like a small China, and likewise a group of people acts differently, that's complexity. And the second one is with time, if you, under repeated behavior you have to have complete different strategies from the static ones. And that was detected by practically every grandparent and people who have skin in the game. So that's sort of the local message from Skin in the Game, and the overall message is, my message before you conclude, is the idea of the Incerto is that there's a lot of uncertainty out there, there's a lot of stuff we don't know. But the good news is that there's only one, and one way to go about it, okay, and this is quite interesting to see that the more uncertainty there is – take global warming, there's a lot of uncertainty because there's a high probability that the IPCC they're full

of a full of crap, okay, and there's a probability that their, you know, that their opponents are full of crap, alright – but the more uncertainty there is a system the less you want to pollute because you don't know what's going on.

Naval: You don't know what's happening.

Nassim: Right, so interestingly the more uncertainty there exists in the system, okay, the more you gotta follow a certain paranoid route; try to position yourself to have more upside than downside and effectively your decisions become much easier, so let's not waste time trying to argue about the niceties of the future because the more uncertainty there is the more we know how to act. So that's sort of the idea of the Incerto in general.

Naval: Well I recommend everybody just devour all of Nassim's books; it'll improve your decision-making in life, in crypto, in –

Nassim: Yeah, put pressure on me.

Naval: Yeah, figuring out even like which doctor you should go to, which restaurant you should eat at, how you should conduct yourself honorably and morally, I think it's an amazing work and I hope he keeps putting them out. It's not the last one I hope?

Nassim: I don't know, if you if you keep talking like this I'll stop.

Naval: Alright, thank you everyone.

Capitalizing on Tech-Enabled Transformations (Excerpt)
July 20, 2018

Josh Wolfe and Michael Green

MG = Michael Green (Thiel Capital)
JW = Josh Wolfe (Lux Capital)

MG: W-O-L-F-E. You're going to get, hopefully a whole bunch of new Twitter followers, if anybody is silly enough not to be following you already. But you've been talking about Bitcoin, which to me feels like the exact opposite, right? It's the virtual world.

JW: Well, the dollar itself is a virtual world. And so, it's interesting because I was a hardcore skeptic and cynic about this. And I felt like if anything, you have to understand both sides of the argument. On one side, this is nothing but tulip bubble. And this is inter-subjective belief. It only has value but for the fact that I believe that you believe that he believes that she believes that infant item.

And then I started looking at it and there was actually a curmudgeonly value investor. A guy, Murray Stahl, from Horizon Kinetics, I spent time with Murray. And I was sort of swayed by a few simple arguments. One, if there's 60 million millionaires in the world and each one owned the Bitcoin of which the supply is roughly 60 million. That basically takes the entire supply and any incremental demand for it would sort of tip it favorably higher.

Well, then the counter to that is well about infinite forking, right? I mean, you can sort of keep forking these things and the mere fact that this didn't exist 10 years ago. And the mere fact that people say, well it's totally immune from sovereign decree. But yet when Korea says that they're going to crack down on it, the price drops.

And so, I've sort of accepted that this is, at the moment, less about utility and more about a store of value-- an alternative store value. Just like we subjectively decide that gold, in it's perceived scarcity or real scarcity, is a store of value. That this too, for some period of time, will be a store of value. The idea of its utility, I'm more skeptical about.

And then, what everybody says, which I think is totally cliched as well, I'm skeptical about Bitcoin but Blockchain, you know, I'm bullish on. Well, you know, there's been a lot of evidence that says right now, there's not really anything that's functionally working on Blockchain. We have a bunch of investments in companies that are working on Blockchain.

The thing that attracted us to one or more of those was the idea of a decentralized internet. That the-- and you see this in the backlash over the past few months with some of the tech giants, that you ought to own your own information. That that information should be licensed to some of the big guys, but that your photos and your content and your social graph and all of that should not be siloed inside of Facebook or Google. The sort of classic, either you buy the product or you are the product.

And so I see a shift where some of that decentralization will be enabled because of that. All the people though, that come and pitch us, we're going to use Blockchain for health care records. We're going to use Blockchain for mortgages. We're going-- it's just an endless supply of people that are proposing that this is the answer to market x.

And usually our first question is well, why couldn't you just use an Excel spreadsheet? Or what the-- you know, is this just an old business that just needs some modern-- the main virtue is the idea of triangulating and having proof that if I had some digital currency, or some digital contract, and I send it to you and I

also sent it to her, that I haven't simultaneously sent the same contract. And that there's some way to reconcile, through a third party, but that third party being the network, that I have in fact only sent it once to you.

And so that, itself, has value. But in the same way that a double ledger accounting had value as a protocol. Or that internet protocol, IP, had value as a protocol. I think it's very unlikely that people are going to profit from that in itself. With the exception of one thing, which I think is actually at first blush, totally crazy. And then I thought about it, it may be really valuable. We're not investors in it, but CryptoKittie's. This was ridiculous. This was like Tamagotchi's collectibles, you know--

MG: One of the things is CryptoKitties?

JW: Yeah, so-- I mean, I-- when I first heard about this, I said this is the most ridiculous thing. But then as I thought about, I said, this might actually be genius. In part because everybody is underestimating it. But in part because what CryptoKittie's is, is this verifiable-- almost like the holograms of sports memorabilia back in the day that you wanted to ensure that this thing had veracity, infidelity.

I actually think that if you have a digital asset-- now that digital asset could be a photograph, it could be a music file, it could be a piece of art. But something that you want to prove its provenance and be able to track it. I think that you're going to have some aspect of crypto involved in that verifying. A long hash of where this thing came from, where it has been sent, how it has been used, and that it's not just copied and pasted. And and I actually I think that that will end up becoming itself a protocol that becomes somewhat valuable.

MG: So, I think it's interesting you bring that up because that's also where I see the opportunities. And somebody used the phrase for me that it gives you the opportunity to create scarcity in digital assets. Because digital assets by themselves are obviously quite duplicatable. So it's very easy to make a copy of something.

JW: Which, itself, by the way, has another facet that I think is quite valuable. And I'm not sure if a single company is going to profit from this or it's going to be a feature from the big ones. And we'll come down to CryptoKittie's. But any time that something is abundant, you want to ask what's scarce. And anytime that something's scarce, you want to say, OK, what's abundant?

Throughout the 90s, the thing that became abundant because of the democratization of the tools of producing content, was text. Text everywhere. And so articles were published and blogs were published and Twitter and Facebook posts and all this kind of stuff. And the scarce thing became search. Whether it was within Twitter, or within Facebook, or, of course, Google, that became one of the most valuable things. Being able to search through the abundance of content and text. And of course, that turned also to photos and images and sound files and all that.

Today, with the ability to produce, of questionable veracity, an enormous amount of content. Again, I think, the valuable thing is search. But the search is for truth. Is that picture undoctored? Is that video undoctored? And you see some of these techniques. I mean, we talked before about bits and atoms and some of the techniques of virtual reality and being able to use an off the shelf camera that used to cost tens of millions of dollars for a Hollywood special effects rig.

Where I can take your face, map it to Putin or to Trumps', and make you act like a puppet of Trump or Putin. Where you are controlling the mouth and you can create the audio sound files. And you can create a war with that. I mean, you can send markets into turmoil. And so, there's a lot of danger that can happen

from that because it's so hard to tell if it is real or not. And it's only going to get better. So that becomes abundant.

The scarce thing is how do you tell the veracity? And that might be in this sort of CryptoKitty like digital veracity to be able to tell, that file, those frames, those pixels have been doctored.

MG: I mean, you bring up the dynamic of start of the war with fakes data. The Wag the Dog, Dustin Hoffman movie. Under-appreciated, I would say. I had an interesting exchange with Ryan, my oldest son, the other day where I was talking about the importance of being truthful. The importance of veracity. and his response to me was, well, Dad. Look at our world leaders. Clearly, it's not particularly important today.

It is an interesting question, right? Can you actually create value from veracity in an environment in which a casual relationship with the truth seems to have a relatively high payoff structure?

JW: Today, it does, right? And one hopes, for moral reasons, that it swings back. But I do think that that line, right? I mean, there's two lines that we're talking about. One is, earlier in the conversation, between atoms and bits. Between the physical world and the digital. And then you have this other world which is between truth and fiction. And I really feel like it is blurring. People, increasingly-- not today. I mean, today you can sort of tell like, OK, that's fake news. There's a fake image that was doctored. OK, haha, we just got you to tweet out the thing that wasn't really fa-- it wasn't really real.

But I think in the near future, it is going to be really hard to tell whether something is true or not. And people are going to be confounded by it. Now, there's going to be some virtue in that, right? Because people look at virtual reality and you say, OK, this is just gaming.

But there's going to be experiences where you can say, OK, I am there. I feel like I'm there. The real virtue of news, right? When a journalist is writing something, what they're really saying is, I'm here. You are not. This is true, this is what's happening.

New York Times experimented with this. They sent out Google Cardboard, you put it on, and you're sitting there in a Syrian village watching as refugees are fleeing on your left and your right. I mean, that's an experience that's a hint of what is to come in the coming years that I think will give those kinds of experiences.

But then there's going to be versions of that that are doctored. And I think our ability to tell whether-- and I do not believe we're living in a simulation-- but between the real and the similacrum, it's going to be much more like Westworld. And I love the quote from one of the protagonists early on, one of the hosts. He looks at her and he says, are you real? And she says, what does it matter if you can't tell the difference?

MG: Yeah it's a very powerful world that we're currently inhabiting and also moving to. And I agree with you, the part of the challenge, for my oldest son and others, is this dynamic of, how do you actually make truth matter, right? And in a world where digital assets are valued so highly and they can be copied and manipulated and changed, it becomes very easy to tell the dynamic of, it's fake news. And hopefully you're correct.

And I agree with you that this issue of creating scarcity, creating truth, creating a document that says, no this is the actual fact record. I think that has to have value. If it doesn't, I think that we're in a very dangerous place.

JW: Which itself, right, was the basis for science, right? And ushered in an Enlightenment and the Renaissance, and I feel strongly that there is a group of people that sees the virtue in empirical information that is true. I mean, I know of companies right now that are trying to almost create a scientific graph of entities and objects to get to ground truth of the food-- the food network of where it's coming from and what the actual content is so that these are kinds of things that almost get locked into the graph and they can't be tampered with. And going back to the idea of Blockchain, that has that same virtue. Where there's some truth that transcends any one individual, and it's very hard to change.

Wikipedia is another example that. Somebody can come in and they can lie and they could say, no, no. Mike Green didn't grow up in San Francisco, he grew up in Oklahoma. But then somebody changes it back, right? And so, the network itself is almost this corrective, this immune system for false information.

MG: Well, remarkably close. My mother grew up in Oklahoma. But, that is actually I think an incredibly important link that you just made, which is the Dark Ages, the Middle Ages, the myth based world of what you're told is true, what you believe is true, has no basis in the physical world. Now, I have no objection to anyone harboring any beliefs that they have in terms of spirituality or God or anything else. But there is an importance in the Francis Bacon letter of illusion that says, look, this is a testable hypothesis. We actually have the tools that allow us to declare what is true.

And we forfeited some of that in the world where we've moved away from the physical and into the world of Second Life where anything can happen. And anything can be true. And you can reboot the machine and retell it. And I think that's actually really interesting-- it's a really interesting link to the importance of crypto.

JW: You touched on something which is interesting. Which is, you know, you would think one would have hypothesized 20 years ago we're going to have an abundant internet that's going to provide always on information at the touch of your fingertips. And you'll be able to contact experts and get truth and all that kind of stuff. And what we've seen, of course, is the opposite, right? We've seen-- not that that doesn't exist. But a spiraling of crazy, fake information and false information. And the rise of people who are famous just for being famous. And all the good stuff has been amplified. But the bad stuff seems to be amplified more.

(End Excerpt)