RECURSIVE CAPITAL

Bitcoin Investment Thesis

Disclaimer

The purpose of this document is to provide an objective investment case for Bitcoin, and also serve as an educational analysis of Bitcoin. This document is not directed at any particular person or group of persons. This material is solely for informational purposes and shall not constitute the solicitation to buy Bitcoin. Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to. This document fairly represents the opinions and sentiments of Recursive Capital inc., which is the issuer of this document, as at the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

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

Recursive Capital inc. and individuals involved in writing this content have direct or indirect exposure to Bitcoin.

If there is any material that hasn't been appropriately cited, sources that might have been improperly credited, or any other inconsistencies, please email **contact@rcrsv.xyz**, with the subject "Bitcoin Investment Thesis (Bug)".

“

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and government interference in economic transactions.

”

- Timothy C May

(Crypto Anarchist Manifesto)

Table of Contents

x. Definitions

Asset - Any item, or resource, of value that can be traded in for cash.

Currency - Any abstraction used in circulation as a means of representing value.

> *The US Dollar (USD) is a real-world manifestation of this concept: an abstracted form of value that is circulated by the US Government and Private Banks*[i]*.*

Digital Currency - Any abstraction used as a means of representing value that is circulated on a digital medium such as a computer network.

> *Private financial institutions abstract currencies in their databases, by keeping digital records of financial transactions they have facilitated, before circulating these records in the broader pool of private financial institutional computer networks.*

Cryptocurrency - A kind of Digital Currency that is *cryptographically* secured, and is circulated and operated on a *decentralized* computer network. Its system of operation must also meet the following criteria provided by Jan Lansky[ii]:

- The system does not require a central authority; its state is maintained through distributed consensus.

- The system keeps an overview of Cryptocurrency units and their ownership.

- The system determines whether new Cryptocurrency units can be created. The system also defines the circumstances of their origin and how to determine the ownership of these new units.

- The ownership of Cryptocurrency units can be proved exclusively cryptographically.

- The system permits transactions in which ownership of the cryptographic units are changed. The transaction statement can only be issued by an entity with provable ownership of these units.

- If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

Cryptoasset - A kind of asset that is *cryptographically* secured, and is stored and operated on a *decentralized* computer network.

Blockchain - Generally, a growing linked list of tamper-proof blocks, embedded with transaction records that form an immutable ledger. They are generally split into two: *permissionless* and *permissioned*, where the former is maintained and operated in an open and decentralized manner, and the latter in a closed and invite-only manner.

Cryptography - The practice and study of techniques for secure communication in the presence of third parties, commonly referred to as *adversaries*.

Background

- Money
- Current State of Money
- Digital Money and Cashless Societies
- Privacy, Anonymity and Autonomy in Cashless Societies
- Cryptocurrency as Cash, Bitcoin, and Society

Money

Money, or at least the concept it tries to represent - value - has been in existence since primordial times. It is a mechanism set up to facilitate trade in a way that is less cumbersome than physically hauling items of value, such as precious metals like Gold, Silver, etc.

Moreover, for something to be considered money, it needs to meet the following criteria:

1. **Store of Value**
2. **Unit of Account**
3. **Medium of Exchange**

Store of Value: This refers to how well it can be used to preserve one's wealth over an extended period. A certain item, for example, could have a predetermined limit placed on its supply in circulation at any given point in time, to preserve its value, and in some cases to stabilize its price volatility. This is based on the basic assumption that value is directly linked to scarcity - *scarce items are valuable*.

Unit of account: This refers to a standard numerical unit of measurement of market value for goods, services, and other transactions. In short, its ability to serve as an anchor for valuing things, to give an insight into their worth or price - whether it is *expensive* or *cheap*.

> *For example, valuing things in Venezuelan Bolivars may not exactly give as much insight into their price as it would if it were valued in US Dollars.*

Medium of Exchange: Its ability to facilitate trade: the transfer of value at the point of sale from the offering party - *the merchant* - to the receiving party - *the buyer*.

Generally, money should also satisfy the following:

Divisible - Can be divided into smaller units of value, e.g. US Dollar to the cent.

Fungible - One unit is viewed as interchangeable with another.

Portable - Individuals can carry money with them and transfer it to others, easily.

Durable - It must be able to withstand repeated use.

Acceptable - Everyone in a society, whether local or global, must be able to use it for transactions.

Uniform - All versions of the same denomination must have the same purchasing power.

Limited Supply - The limited supply of money in circulation ensures value remains relatively constant.

Current State of Money

In 1944, after the Bretton Woods Agreement at the Mount Washington Hotel in Bretton Woods, New Hampshire, United States, the 44 allied nations during World War II decided to redesign the international economic system and agreed on the use of the Dollar as the Global Reserve Currency.

At the time, they assumed it was rather logical, as the US Dollar was directly backed by Gold - an item throughout history assumed to have *intrinsic value* - to serve as the perfect reserve asset. During this time, most of the Gold in existence was held in US bank vaults, and thus the US Dollar could now be exchanged for some amount of Gold - $35 for an ounce (or ~28g) of Gold[1].

On Friday the 15th of August 1971, this all changed and is now known as the Nixon Shock[2]: where the US Dollar ceased being backed by an underlying valuable asset - Gold. This ushered in a new era for money - fiat. A kind of money that has no intrinsic value and is instead backed by the trust individuals place on the issuing Government that it is worth something. This fiat money is what nearly all nations have adopted[3].

Digital Money and Cashless Societies

The increasing digitization of commerce has rendered transacting with physical money infeasible in certain situations, such as online payments on e-commerce websites. This has resulted in the global exchange and proliferation of digital transactions between individuals online by banks and other financial institutions, in an attempt to maintain a global ledger of transaction histories, to track the ownership of money.

This has since resulted in increased convenience for the average individual with an account at these financial institutions, as they can use technologies such as credit cards to purchase items seamlessly on the Internet. However, there are severe consequences for *physical money*, which can already be observed in countries such as Iceland, Finland, Sweden, and South Korea, where physical money is increasingly becoming obsolete as they continue to transition into *cashless societies*. As a result, children born in these societies would not have the privilege of knowing or using physical cash in their lifetime. However, for *millennials* who grew up using cash, but were nonetheless born into the Internet revolution, they are open to this change, including all its attendant effects and benefits, and even see it as a desirable technological progression.

This obsolescence of physical cash would necessitate the use of third party intermediation of transactions. This is because the dependence on financial transaction settlements with cash would be shifted instead to reliance on intermediaries, to confirm all forms of value transfer online. These third-party intermediated financial settlements would bring about the following problems:

- Increased trust in third-party intermediaries
- Potential censorship of transactions
- Financial surveillance
- No anonymity or privacy in transactions
- Permissioned transactions

With all the above stated, intermediaries only advertise one benefit - convenience. Which is certainly not enough a benefit to justify the introduction of the above problems in the long term. For instance, the digital money hosted by intermediaries is not censorship-resistant, as Governments can exert pressure on intermediaries to influence decisions on transactions an individual can make, such as transactions with certain people or entities, purchase of certain items like firearms, etc. However, with cash, such a situation cannot occur, as the bearer is solely in charge of its use, hence making the exclusion of individuals from society's financial system considerably less likely.

In a cashless society, transactions are not confidential, as banks and other financial institutions collect information about the concerned parties in a transaction, which mostly includes metadata - such as

the exact time the transaction took place and the amount transferred - to accurately record transactions on their ledger. This information combined with social media data can give enough insight into their psychology, spending habits, health, future purchases, and friends, which constitutes very sensitive information that can easily be abused by Advertisers, Governments, and Hackers.

This would by extension mean individuals who want to preserve their purchasing ability would have to sacrifice their autonomy, as Governments would have a 360-degree view of their potential thoughts, and could easily censor thought-crimes, by exerting pressure on intermediaries to suspend support for any transaction these individuals wish to make, essentially stripping them of any financial agency.

Fortunately, individuals can defend against the increasingly intrusive level of surveillance from financial institutions and Governments at large, by transacting anonymously with electronic cash to preserve their financial agency.

Privacy, Anonymity and Autonomy in Cashless Societies

> *If you're a Government that is seeking to oppress freedom and remove the ability for people to express their feelings and their true thoughts, then the first thing you attack is privacy. This is why, if we want to preserve democracy and preserve freedom, preserving privacy is a fundamental part of that fight.*
>
> - Andy Yen (*Proton Mail*)[4]

Privacy has traditionally been a difficult concept to define, however, one such definition relevant to this discourse is that of the Mathematician and Computer Scientist Eric Hughs, who states that;

> *"Privacy is not secrecy. A private matter is something one does not want the whole world to know, but a secret matter is something one does not want anybody to know. Privacy is the power to selectively reveal oneself to the world."*[5]

The importance of this definition lies in the explicit declaration of privacy as something that can be exercised by individuals, without the direct involvement of any third parties, such as Governments. More importantly, this implies that privacy is primarily a power that can be exercised by individuals, and confutes the commonly held belief that privacy is only a right to be protected by a Government. A simple example would be as follows:

> *"Think of the $100 bill dropped anonymously into a church's poor box. The donor's privacy depends on no one but himself. The donor's ability to retain his privacy, however, turns on the technology available to him."*[6]

Physical cash is not a practical alternative in our increasingly digital world. Therefore we are forced to seek out an electronic replacement that is equal to or better in utility and benefits - such as preservation of one's autonomy, privacy, and anonymity - to cash.

Bitcoin, an electronic peer-to-peer, open, decentralized, and censorship-resistant Cryptocurrency is designed for such a purpose. Though it is still yet to be fully privacy and anonymity preserving, it is getting there with the help of developments in techniques such as confidential transactions (CTs), CoinJoin, zk-SNARKs, Schnorr signatures, Taproot, SNICKER, DANDELION, and other privacy features being developed and integrated into privacy-focused wallets, such as Samourai wallet.

Privacy and anonymity go hand in hand, and in cashless societies anonymity is a luxury that would fend off any form of intrusive surveillance that would result in financial censorship of individuals. Governments in the presence of anonymity would be unable to trace financial transactions back to these individuals, essentially seeing the waning of their ability to censor transactions, thus making it an increasingly indispensable tool in the fight against government censorship and oppression.

Autonomy is the power individuals possess in making decisions for themselves on their behalf, without interference from any external third parties. The absence of individual autonomy as a result of financial silencing, due to Government pressure on intermediaries, would foster a society of obedient zombies, that would be unable to voice out or express their opinions in an open democratic fashion, culminating in the degradation and desolation of open societies. As such, a solution that quickly comes to mind is the adoption of cash as the primary means of trade, however, this does not scale in our digital world, and is the reason why a digital parallel, such as Bitcoin is a more viable option and long term solution.

In future cashless societies, the most valuable possession that would be seldom expressed is autonomy. As individuals continue to engage in their daily routines, they would face increasingly intrusive policies and laws from financial intermediaries and Governments at large, that would incrementally usurp their individuality. Freedom of thought would be a thing of the past, to be replaced with echoes of mainstream politically correct narratives. For those who do seek to preserve their individuality and freedom of thought, their only refuge would be in transacting with Bitcoin and other Cryptocurrencies that lie beyond the power of state control and censorship, lest they get financially censored, and thus economically disempowered and socially disenfranchised.

Cryptocurrency as Cash, Bitcoin, and Society

For millennia, money has had several physical instantiations, from beads, coins, to paper notes. These physical forms of money have long since provided individuals with a means for performing transactions that retain their privacy and safeguard their autonomy. However, as we have severally stated, this is not a scalable solution in the digital age, therefore, the only way forward is to develop a digital alternative that preserves all the benefits of physical cash, which include privacy and anonymity, without its inefficiencies, to protect our autonomy in the long run.

In line with this objective, a Cryptocurrency like Bitcoin that is both permissionless and private would allow the continued flourishing of open societies globally, as it provides the much-needed amelioration of the above concerns. It would serve as money that can be used to perform both physical and digital transactions, with a reduced level of transaction traceability, allowing individuals to retain their privacy. In doing so, it makes it possible for individuals to make censorship-resistant transactions, which includes contributing to groups or individuals, in form of donations, without fearing that their transactions would be flagged and remain unprocessed by intermediaries who have been pressured by the enemies of such entities. Another benefit worth mentioning is its ability to serve as a suitable means for resisting oppressive authoritarian regimes, as transactions would no longer be subject to state censorship.

Unfortunately, despite all the concomitant benefits of Bitcoin, there is no doubt that it would also foster a platform for criminals, scammers, and like-minded individuals to further perpetuate their illegalities, just as other freedoms continue to be abused. However, in trying to regulate, or curb this issue, suggesting the abandonment of this technology would be tantamount to usurping freedoms, like the freedom of movement in hopes that terrorism would be assuaged, for example.

The same effort that was required of law enforcement agencies to combat the misuse of cash is the same effort it would require to combat the misuse of Bitcoin. There are already measures employed by countries such as the US in combating the misuse of Cryptocurrencies[7]. The Ross Ulbricht case, for example, proved that it is possible to catch individuals that use Bitcoin for illegal activities, through the elaborate tracing of Bitcoin transaction addresses[8]. Other methods that can be used to mitigate crime are mentioned below:

- Mapping public-keys from change addresses - this is based on the assumption that the majority of Bitcoin transactions carry two output addresses, one to the destination and the other back to the sender as change. It could then be possible to figure out which of the two inputs is the change address if the client software implementation is determined and its source code analyzed.

- De-anonymization of clients in the Bitcoin P2P network as described by Alex Biryukov et al[9].

- Using Blockchain forensics tools like Bitfury's Crystal[10].

- Illicit activity identification and intelligence on the Bitcoin Blockchain using Elliptic[11].

- Bitcoin provides the ability to send money in up to eight decimal places (i.e. 1 satoshi), which means, It may be possible to find transactions with specific amounts and thus map public-keys in transactions in certain trades.

- Individuals sometimes re-use their Bitcoin addresses, whether by accident or because it is used to receive donations. It may then be possible to map these addresses to individuals, as described by Fergal Reid and Martin Harrigan in their paper, *"An Analysis of Anonymity in the Bitcoin System"*[12].

Brief History of Bitcoin & Its Internal Structure

- Brief History of Bitcoin
- Formal Definition of Bitcoin
- Internal Structure of Bitcoin
  - The Lightning Network
  - Incentive Scheme
  - Public-Key Cryptography (PKC)
  - Randomness Based Proof-of-Work (PoW)

Bitcoin was invented in 2008 with the publication of "*Bitcoin: A Peer-to-Peer Electronic Cash System*", by an anonymous entity under the pseudonym of Satoshi Nakamoto. The paper described a system for electronic payments that included several known innovations, such as Wei Dai's *b-money*[13] and Dr. Adam Back's *HashCash*[14], to achieve an entirely new decentralized electronic cash system that is not reliant on a central authority for its issuance, transaction settlement, and validation. A key innovation worth citing is the "*Proof-of-Work*" algorithm adapted from HashCash, which enables the periodic global synchronization on the state of all transactions on the network's ledger every ~10 minutes. This system acts as a perfect solution to the double-spend problem - where a single unit of the currency is spent more than once - because this periodic syncing of the state of all transactions ensures that at most one transaction out of two or more spending a given unit of the currency - bitcoin - is logged. Prior solutions usually featured a centralized processor, a flawed approach with numerous vulnerabilities, and was resolved by using a decentralized collective ledger, generally referred to as the *Blockchain*.

The Bitcoin network launched in 2009 with the release of the first reference implementation's source code, by its creator, which featured the *Proof-of-Work* algorithm that facilitated mining: a process that secures the network through compounded computation and issuance of bitcoin, and in the process rewards miners with all transaction fees in a given block and a specific amount of the newly issued bitcoins, known as the *coinbase reward* (currently 12.5 bitcoin), which is halved every ~4 years. All these innovative advances have made Bitcoin a perfect Internet money and digital asset and has prompted the creation of an entirely new market currently valued at ~$130 billion (as of Dec 2019).

Satoshi Nakamoto, the anonymous creator behind Bitcoin withdrew from the public in April 2011, leaving the responsibility of further development of the source code to a growing group of enthusiastic volunteers. This has resulted in the creation of an entire community of developers fully committed to Bitcoin development. To this day, the development of the original reference implementation is handled by this growing global community of Bitcoin developers. Before any protocol changes are integrated into the source code, they must first be proposed through *Bitcoin Improvement Proposals* (or *BIPs* for short) - a practice that was first introduced by Bitcoin developer Amir Taaki[15] and has since become the canonical method of submitting proposals. Since Bitcoin's source code is open-sourced, its internal operation can be easily audited. Though its development is fully maintained by the Bitcoin community, it is pertinent to mention that it is not controlled by any single entity.

Its invention has brought forth a practical solution to the long-standing distributed computing problem, the "*Byzantine Generals Problem*"[16], and has spawned new fields in distributed computing, economics, econometrics, tokenomics and rekindled long-abandoned researches in Cryptography.

We can now formally define Bitcoin thusly:

> *Bitcoin is a peer-to-peer (P2P) decentralized computer network that primarily facilitates transfer of value - bitcoins - from one node to another. The network's security is maintained by a continually dynamically formed group of nodes known as miners, who expend significant computational energy as they compete with one another in the creation of blocks that are appended to a growing list of existing blocks that form an immutable ledger, commonly referred to as the Blockchain, in a process known as mining. All nodes on the network at any given point in time can inspect the validity of the entire blockchain and validate transactions, and subsequently maintain an identical chain as all other nodes, and hence, can maintain consensus on the state of all transactions performed by nodes on the network.*

Below is the internal structure of Bitcoin:-

Layer	Sub-layer	Component(s)
2	0	Lighting Network
1	3	Incentive scheme
1	2	Public-Key Cryptography (PKC)
1	1	Randomness based Proof-of-Work (PoW)

Let's look at these components in more detail:

The Lightning Network

The Lightning Network is a decentralized system for instant high-volume micropayments, which removes the risk posed by delegating custody of funds to trusted third parties to facilitate financial payments. Bitcoin contains an advanced, though limited, scripting system that allows users to program instructions that control how funds are sent and accessed. Due to its decentralized design, transactions confirmed on the Bitcoin Blockchain can take up to one hour (~6 confirmations each of ~10 minutes) before they are considered irreversible. This means, micropayments, or payments less than a few cents, are inconsistently confirmed, and fees render such transactions inviable on the network today.

The Lightning Network currently aims to solve these problems. It is one of the first implementations of a multi-party Smart Contract system using Bitcoin's built-in scripting. The Lightning Network provides the following additional benefits to the Bitcoin network:

Instant Payments - Bitcoin batches transactions into blocks that are spaced ~10 minutes intervals, which is the time taken to mine a block. Payments are widely regarded as secure on the Bitcoin network after a confirmation of 6 blocks (or about 1 hour). On the Lightning Network, however, payments don't need block confirmations and are instant and atomic. Meaning, it can be used at retail point-of-sale terminals, machine-to-machine transactions, or anywhere instant payments are needed.

Micro payments - The Lightning Network enables the transfer of funds as low as 1 Satoshi (0. 00000001 of a bitcoin) without any custodial risk, effectively facilitating micropayments denominated in bitcoin. This helps it circumvent Bitcoin's current fixed per-transaction fee that makes micropayments impractical.

Scalability - The Bitcoin network is currently unable to process the large volumes of transactions demanded by *micropayments,* and other *automated payments* performed by automated micropayment services. Since transactions on the Lightning Network are done off the Bitcoin network, and without delegation of trust and ownership, users can perform an unlimited number of transactions between themselves, before the final state of the transactions is broadcasted to the Bitcoin network where it is settled.

The Lightning Network works by placing funds in a two-party multi-signature Bitcoin address (known as a *"channel"*). To spend funds from the channel, both parties must agree on the new balance, which is stored as the most recent transaction signed by both parties spending from the channel. To make a payment, both parties sign a new exit transaction that spends from the channel, which invalidates all older transactions and makes only the most recent exit transaction the only valid one.

The Lightning Network does not require cooperation from a counter-party to exit or close the channel, as both parties have the option to unilaterally close the channel. Since all parties have multiple multi-signature channels with many different users on this network, upon knowing a secure *cryptographic hash*, one can easily send a payment to any other party across this network through these channels. Payments can be made across this network of channels without the need for any party to have unilateral custodial ownership of funds. This allows for dynamic and open network participation, as opposed to the trust-based model that is common with other more vulnerable digital financial systems.

The Lightning Network also brings an additional level of privacy to Bitcoin users, as nearly all the transactions are not logged on the Bitcoin Blockchain, only the funding transaction that opens the channel and the exit transaction are logged. Privacy invading analyses such as c*ommon-input-ownership heuristic*, *address reuse,* and *change address detection* also don't work on Lightning Network transactions.

Incentive Scheme

The Incentive scheme can be broken down in the following way:

Trigger	Incentive beneficiary	Incentive
Newly minted bitcons	Miners	Able to use new bitcoins to HODL - for long term preservation of wealth - or for speculative reasons. Trade them for physical cash to pay for rent, hardware maintenance costs, etc.
Transaction fees	Miners	Additional income besides newly minted bitcoins. Thereafter considered the only incentive, pending the final minting of the last bitcoins (in the maximum 21 million supply).
Transaction (Network Usage)	Everyone	The more transactions performed on the network the more blocks are mined, resulting in the network becoming further secured and the overall blockchain evermore irreversible.

Public-Key Cryptography (PKC)

Public-Key Cryptography (PKC) was invented in the 1970s, but only became widely used after the birth of the Internet, and currently forms part of the core security infrastructure of modern communications systems. There are several methods for constructing such systems, which include the use of prime number exponentiation and elliptic curve multiplication, which happens to be the core component of Bitcoin's Cryptography. These constructions have unique mathematical properties that allow them to be used in constructing one-way functions, that is, functions that provide the same fixed output for any given input, but is practically infeasible to obtain the input from the output. This forms the basis for *unforgeable digital signatures* and encrypted messages - *digital secrets*.

The purpose of PKC in Bitcoin is to provide the creation of a *unique key-pair*, one *private* and one *public* derived from the private, that are in reality just two large numbers (usually represented in base 16). The former is used for digitally signing transactions to transfer ownership of funds, and the latter for creating new bitcoin addresses, to receive these funds.

The mathematical nature of this key-pair provides a unique property: the private key can be used to digitally sign messages, and these digital signatures can be verified against its associated public key pair, as they are uniquely linked, all without requiring knowledge of the private key. Each time a bitcoin transaction is created, it yields a different unique signature that is bundled with the owner's public key and can be used by full nodes on the network to verify the ownership of the bitcoins being spent in a transaction.

Randomness Based Proof-of-Work (PoW)

The mining process that secures the overall network provides miners with two kinds of rewards, or incentives in the economic sense: (i) newly created bicoins with each new block as part of the protocol - until 2140, when bitcoins would no longer be created - and (ii) the combined fees from all transactions in any given block. Miners in anticipation of these rewards compete with one another to solve a mathematical problem, or *puzzle* in the Cryptography sense, using a hashing algorithm, in this case, *SHA256*. This solution, or *Proof-of-Work*, is included in each new block and acts as a 'proof' that the miner expended significant computational power to obtain the solution, and did not cheat or game the system. This PoW is added continuously to each new block, making it incrementally more difficult to tamper with the Blockchain, and is what forms the basis for Bitcoin's security model.

PoW forces the use of brute force, as the possible solution lives in an exceptionally large space, which means it can only be obtained through randomly searching this space, a process known as an "*unbounded probabilistic iterative procedure*" in Computer Science. An oversimplified but fitting analogy would be randomly trying on different hats of varying sizes in an extremely large warehouse until one that fits is found.

PoW provides a link between the digital and physical world, as reasonably large amounts of energy must continuously be expended to continue maintaining the Bitcoin Blockchain. This real-world energy consumption simultaneously bootstraps the value of bitcoin as well as the entire network's security, as the compounded computational effort required to take control of the network is constantly increasing.

Bitcoin Use Cases

- Bitcoin Use Cases
- Volume as an Indicator of Bitcoin Adoption
- Bitcoin as a Hedge Against Economic Crises
- Usage per (Online) Economic Person as a Better Measure of Adoption

Bitcoin by design serves a number of functions, such as:

1. **A means of exchange** - Able to facilitate trade in form of a *digital currency*. This is what is often seen as its *utility* value, as it can be used on the network to transfer value - bitcoin - to facilitate trade, remittance, etc.

2. **A store of value** - Unlike other currencies and commodities, Bitcoin's supply schedule is permanently capped at 21 million. This important property is a major value proposition of bitcoin over time — based on our inherent notion of ascribing value to scarcity — coupled with the amount of computing power invested to secure the network by miners, and its appreciating price makes bitcoin even more valuable than Gold — by having a predefined *absolute* finite supply.

3. **As a security** - For the recent history of Bitcoin, this has constituted a considerable amount of its use *in the wild*. One can simply buy bitcoins through a variety of methods, such as OTCs, Exchanges (such as Coinbase), and simply speculate on its future value. This means individuals have the ability to simply trade bitcoins on the basic assumption that the more people adopt it for example, the higher it would be valued. Though this has formed a core point of criticism for skeptics, who cite that it is simply a *bubble* like the dot-com bubble of the early 2000s[17]. Suggesting that it doesn't possess the above mentioned properties (**1** & **2**) and is simply a medium for gamblers, hustlers, scammers, and those suffering from FOMO is an inflated misreading, because its use as a speculative medium is not a reflection of its design, but rather a normal occurrence initiated by those who trade currencies and other assets.

The increasing financialization of Bitcoin has seen several synthetic securities being built around it. These include LedgerX's physical settlement Bitcoin Futures platform[18], CME's Bitcoin Futures platform[19], ICE's Bitcoin Futures platform, BAKKT[20], and ErisX[21]. All these developments provide the opportunity to recover financial value in the future as Bitcoin price appreciates.

4. A Currency - Bitcoin has properties **1** & **2**, which form the core of all currencies.

5. **It is an open, decentralized, and censorship-resistant currency** - It provides a viable option for the ~1.7 billion unbanked individuals, journalists, others facing exclusion from the financial system due to various reasons, and others haunted by oppressive states to participate in the global economy.

6. **A Commodity** - Gold faces a lot of logistical issues as a commodity, as its physical nature causes serious issues when being transported. For example, due to its weight, only moderate amounts can be transported at a time, to reduce the amount of fees to be paid for transporting it, and chances of it getting looted on the way. Bitcoin on the other hand inherits all the features of Gold (as it is also a *store of value*), and is usually seen as a *Digital Gold,* or *Gold 2.0*, given that it can be traded more efficiently than gold as it is a digital asset, making it serve as a more viable alternative to Gold as a commodity.

Bitcoin can also be considered a commodity in the Crypto ecosystem, in that you can exchange bitcoin for other cryptocurrencies such as Monero (XMR), ZCash (ZEC), Litecoin (LTC), etc.

It is evident that Bitcoin is a versatile asset, and is able to take the form of a commodity, currency, security, etc. depending on what the holder intends to use it for, allowing it to adapt depending on its use.

Volume as an Indicator of Bitcoin Adoption

In recent times we have seen an increasing number of people using bitcoin for its utility value. The popular peer-to-peer Bitcoin exchange localbitcoins.com (LBC) can be used as a case study in analyzing this growing trend, as most of the trades that occur on the exchange are almost all *fiat-to-crypto*. These trades are denominated in up to 150 currencies, which can help provide some insight into countries that are making the most trades.

LBC managed to facilitate 440,000 bitcoins worth of trades, which is equivalent to $3.1 Billion (USD), in 2018 alone. The following tree-map shows a breakdown of the top 15 countries by volumes in that same year:

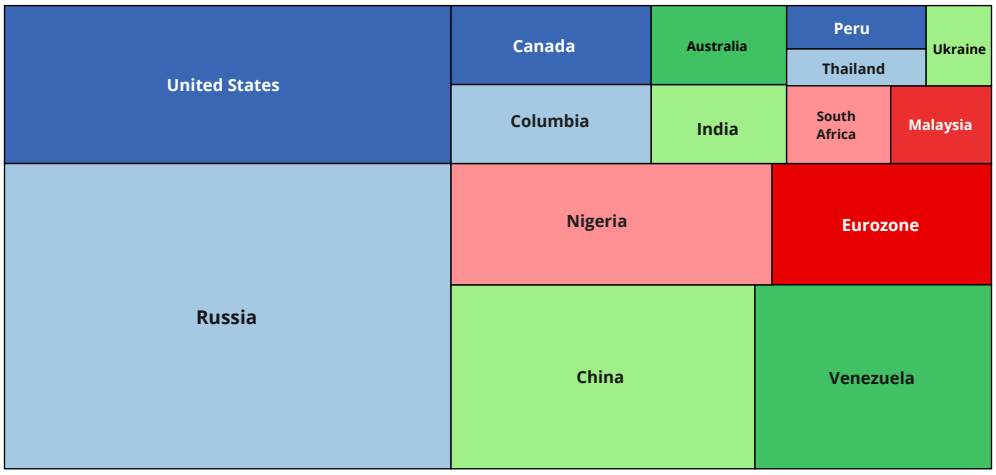

Diagram 1.0: USD Equivalent BTC Volume (2018)
(Credit: Matt Ahlborg, "nuanced analysis of localbitcoins data suggests bitcoin is working as satoshi intended")

Bitcoin as a Hedge Against Economic Crises

The graph below tries to classify the quarterly volumes of countries on LBC according to their various regions, by plotting the volumes in these regions over 6 years, to further elaborate the trends experienced over time:

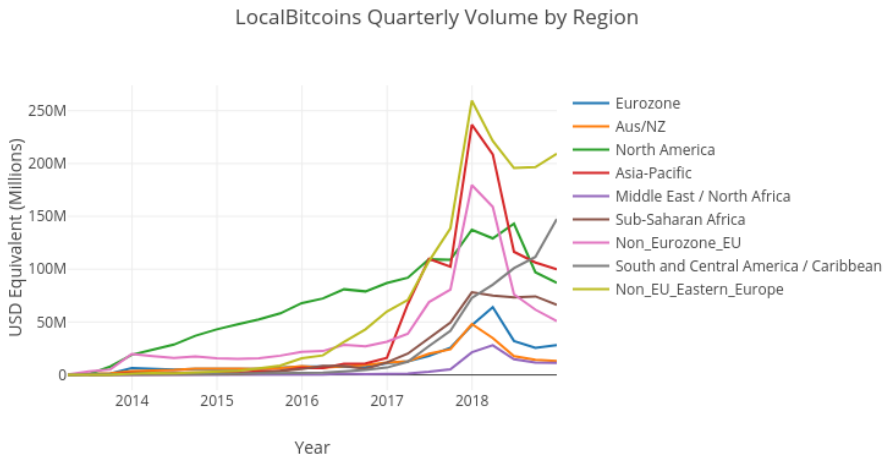

Diagram 1.1: LocalBitcoins Quarterly Volume by Regions
(Credit: Matt Ahlborg, "nuanced analysis of localbitcoins data suggests bitcoin is working as satoshi intended")

The following can be observed from the graph above:

- Speculation is still somewhat high on the platform and can be cited as the reason for the short spikes in volume.

- Bitcoin drew a lot of attention from developed countries during the *bubble* of 2013, but has since slowly been replaced by less developed regions.

- Venezuela's trading in South and North America, for example, has been steadily growing over time, and eventually peaked in 2019. This steady growth clearly shows some independence to *bubble trends*, further indicating a shift from speculation to actual utility use cases.

Usage per (Online) Economic Person as a Better Measure of Adoption

The plots above can only provide us with so much information, as pointed out by Matt Ahlborg in his piece "*nuanced analysis of localbitcoins data suggests bitcoin is working as satoshi intended*", the issue here is that these plots fail to incorporate important factors such as Internet penetration of a given country, GDP, etc. which would have helped in properly categorizing these trends in trading volumes. In developed regions like North America for example, we expect to see more volume than in a less developed region such as Sub-Saharan Africa, primarily due to internet penetration in the region, which would inadvertently cloud any visible trends experienced in these developing regions, and as such Ahlborg has proposed the following insightful metric to address this problem:

$$\frac{\left(\frac{V \times Pr}{Po \times IP}\right)}{E}$$

V = Volume (BTC)
Pr = USD Equivalent price on day of trade
IP = Internet penetration of country
Po = Population of country
E = GDP (Purchasing Power Parity) per Capita of country

Diagram 1.2: Usage per (Online) Economic Person (UP(O)EP)
(Credit: Matt Ahlborg, "nuanced analysis of localbitcoins data suggests bitcoin is working as satoshi intended")

Using the aforementioned metric, he was able to produce a timeline of trading volumes on LBC to provide a better view of the actual volume trends. Below is a snapshot of the volume trends in the last qaurter of 2018:

Local Bitcoins UP(O)EP Values by Quarter

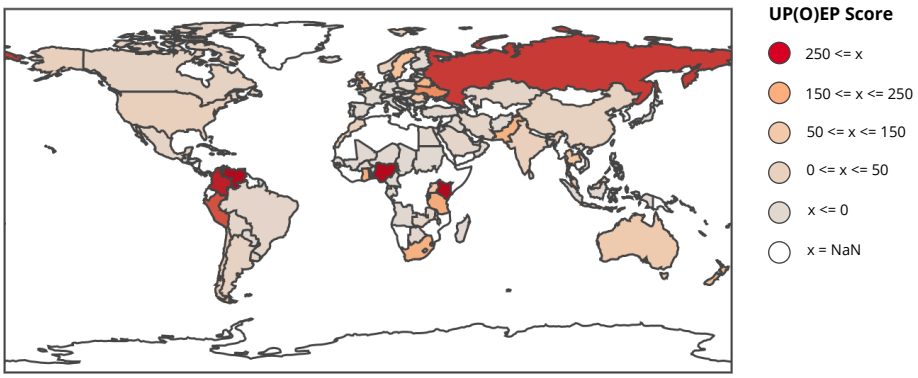

Diagram 1.3: LocalBitcoins UP(O)EP Values by Quarter (2018 Snapshot)

(Credit: Matt Ahlborg, "nuanced analysis of localbitcoins data suggests bitcoin is working as satoshi intended")

This metric provides a more impartial view of the trade volumes across all countries on LBC, and also reflects the events that have surfaced in these regions of high **UP(O)EP**. Examples include the economic crisis in Venezuela, which drove its citizens to seek refuge in Bitcoin for wealth preservation due to runaway inflation and the general loss of faith in their native currency, the Venezuelan Bolívar. Other key events captured by the timeline above include Kenya's M-Pesa revolution, which saw a huge increase in Bitcoin adoption, owing to the rise of mobile phone user adoption, and the lack of payment systems, such as Paypal in West Africa saw an increase in adoption of Bitcoin as an alternative.

As Ahlborg concludes, it is worth noting that there are times where a country may not achieve proper Bitcoin adoption not because its not a useful technology, but because of the country's laws, culture, and other factors such as availability of alternative methods to achieving wealth preservation, capital flight, and remittance.These are merely short term anticipated global headwinds as Bitcoin adoption ultimately seeks to provide an alternative to existing currencies, payment systems and assets.

Despite all these challenges, Bitcoin adoption continues to be on the rise, with more people using it as an alternative currency, remittance vehicle, asset, commodity and security.

Misconceptions of Bitcoin

- Bitcoin Has No Clear Utility
- Bitcoin is a Means for Criminal Trade
- Bitcoin Has No Value
- Bitcoin isn't a Currency its Too Volatile
- Creator's Identity
- Hacking
- Too Complex to be Widely Adopted
- 21 Million Supply Cap and Deflation
- Bitcoin Will Eventually be Dethroned by Some Altcoin
- Transactions are Anonymous
- No Developer Incentives
- Energy Waste
- Small Blocks
- No Turing
- High Fees
- Transaction Finality and Speed

> *The current (fiat-based) monetary system has brought nothing more than an anamorphic implementation of money and has corrupted our understanding of the concept.*

Cryptocurrencies especially Bitcoin have had their fair share of denunciation, from being called a frenzy, Ponzi Scheme, bubble, to an outright scam. We aim to help the astute and willing investor see past these fleeting notions, and headlines like the one below:

> *"To me, it's just dementia. It's like somebody else is trading turds and you decide you can't be left out."*
>
> *— Charlie Munger on Cryptocurrency, May 5, 2018*[22]

Prima facie, one might come to the immediate, although, wrong conclusion that Bitcoin is a global Ponzi scheme, as news headlines often fail to factor in context.

Cryptocurrencies are a culmination of more than 30 years of research and achievements in Cryptographic systems like Public-Key Cryptography (PKC), Signature schemes, Anti-Spam and Time-stamping Systems, Distributed Systems and these achievements in Computer Science have managed to provide one of the most technologically advanced systems that we have ever seen in our modern civilization - Bitcoin.

The primary success of a system like Bitcoin is in its decentralized peer-to-peer network, and Proof-of-Work system that guarantees trust-less network participation and ledger validation. This has for the first time in human history separated money from state control, transferring it instead into the hands of the general public.

Therefore, it is naturally expected for those (businesses, individuals or otherwise) who benefit from state-issued currencies, and Governments in general, to be opposed to the technology, and even repulsed by the very discussion of it.

We have also recently seen enterprise-focused businesses, such as IBM push for enterprise adoption of Blockchain technology - the colloquial term for the triple-entry ledger maintained on the Bitcoin network. Even though this goes against the intended purpose of the Blockchain technology, which is to aid in enabling the ushering of a new monetary system that is free, open, decentralized and censorship-resistant. This sort of propaganda is quite expected of a leading business in a $5 trillion (USD) market[23], to leverage the excitement around the new technology for expanding their profits, albeit at the expense of polluting and mischaracterizing the technology as a whole.

It is, however, a practical certainty, proven ad infinitum, that the joint efforts of passionate volunteers would always out-compete the highly paid corporate methodology, and as such these enterprise efforts would fail to replace or compete with Bitcoin in the long run.

Before we proceed any further, it is of use that we discuss Satoshi Nakamoto - the anonymous entity behind Bitcoin. Satoshi decided to remain unknown for obvious reasons, such as, not wanting to interfere with Bitcoin, which is important for the system to thrive. Having a leader would just make it another open-source attempt at replacing money, which can easily have its leader influenced, manipulated or even sanctioned, and the project subsequently abandoned. It now seems clear that the aim was for Bitcoin to take on a life of its own and become truly open, decentralized and censorship-resistant money, with control being in the hands of all stakeholders: developers, miners, and users, and not any central party.

This decision along with certain key design choices have resulted in the $1.3 trillion per annum worth of transactions, that Bitcoin has seen only a decade after its initial release[24], surpassing even PayPal's[25]. This is a significant feat that has never been achieved by any open-source effort, owing greatly to the technical design decisions made by its anonymous creator, the entire community effort in maintaining the code that powers the network, the miners that bring immense computing power to secure the network, full nodes that broadcast and validate transactions and its growing popularity as a useful technology.

Given this somewhat brief context, we now have a minimal knowledge framework to proceed with breaking down some common misconceptions of Bitcoin.

Bitcoin Has No Clear Utility

Utility in the economic sense is generally understood as the use of some resources to serve some financial function, whether it be as a means of exchange, store of value, or as a security. In that sense, Bitcoin does have a clear utility, which is an open, decentralized and censorship-resistant money, and is gradually adding a store of value as well.

Since its inception, we have seen Bitcoin transform from a collectible amongst cypherpunks to being used as a means of exchange, a unit of account, security and more recently a store of value, and a possible reserve currency in the future. There are countless examples that can be cited were Bitcoin has been used to serve a function, such as a means of exchanging value even from within hostile regimes, and to protect one's assets from state seizure by buying bitcoin and HODLing - holding on to the asset as is done with other assets like gold - to preserve one's wealth or possibly to sell at a later time for more value.

In a country like Nigeria for example, the Government could unjustly sanction individuals they claim are a threat to national security. In such cases, Bitcoin offers these individuals the ability to still freely continue to use their finances without suffering Government induced financial oppression. This is of huge benefit to those who ordinarily would have had their finances & assets frozen by banks due to unjust Government decrees, and would now enjoy financial freedom, to do as they deem fit with their wealth.

Bitcoin is a Means for Criminal Trade

It should be quite obvious that any technology that can be used as money, be it Gold, physical Cash or *Electronic Cash* would still serve as a means for criminal trade. Physical cash, at least at the moment, guarantees better anonymity and privacy for criminals since its original creation point can't be traced or its holder easily.

Additionally, it should be noted that, the current estimate for the Darknet market is ~$1.5 trillion[26] (as of 2018), which is about 11.5x larger than Bitcoin's total market cap (~$130 billion, as of Dec 2019), meaning, even if all the Bitcoin in circulation were to be channeled to the Darknet, it still wouldn't be enough to sustain it, as it would only make ~10% of the entire Darknet market.

If a criminal doesn't want to get caught, it is much safer for them to use physical cash to perform transactions, because they are extremely less likely to be caught than if they used Bitcoin, which has all its transactions permanently logged on the Blockchain for all to see forever, or at least for as long as the Bitcoin Blockchain exists.

In most cases, criminals have a hard time clearing up their tracks and leave digital prints that can be used to link the illegality they have perpetrated back to them. This means, even after Bitcoin transactions become more anonymous and private, individuals engaging in criminal acts can still get caught.

Bitcoin Has No Value

> *We should consider utility value as, the value derived from the use of the item being discussed, and speculative value as the value derived from predictions of the item's future market value. The latter at least theoretically does track the former, and to some extent holds in reality.*

Bitcoin's price valuation tracks its utility value; where the longer the Bitcoin network lasts to support the use of bitcoins, the more valuable the native asset - bitcoin - becomes, spurring a further increase in its real-world value.

A similar case can be made for fiat-based currencies like the US Dollar, where its value is fully based on the US Government's acceptance of it as a legal tender, which essentially means, its value is wholly dependent on its increasing use in society as a valuable resource. This suggests that, as long as Bitcoin is increasingly being adopted and used, it would also continue to have value.

Nonetheless, even if we were to overlook all of this, Bitcoin's value as an asset is primarily a direct result of its provable scarcity. Its supply is permanently capped at 21 million, and this scarcity is what makes bitcoin a valuable asset, at least if we maintain the view that scarce items have value.

Bitcoin isn't a Currency its Too Volatile

This mostly stems from an evident misunderstanding about attributes of things and their defining properties.

Minimal volatility is not a requirement for something to be a currency, volatility is just an expression of market size - the smaller the market the more volatile, and the larger the more stable - with time, as markets grow and mature prices tend to stabilize.

Bitcoin only seems very volatile when compared to mature currencies like the US Dollar, British Pound, and the Euro, and is not immediately evident, however, when compared to currencies of countries like Ukraine, Turkey,and so on. The US Dollar is a mature currency and as a consequence has minimal volatility. This quality, or *attribute,* is then falsely adopted as part of the definition of a currency.

Below is the price history of Bitcoin (**BTC**), Turkish Lira (**TRY**) and Ukranian Hryvnia (**UAH**) to the US Dollar (**USD**) over the span of the last 6 years (2013-02-15 to 2019-02-15) on a logarithmic scale, to further buttress the above point:

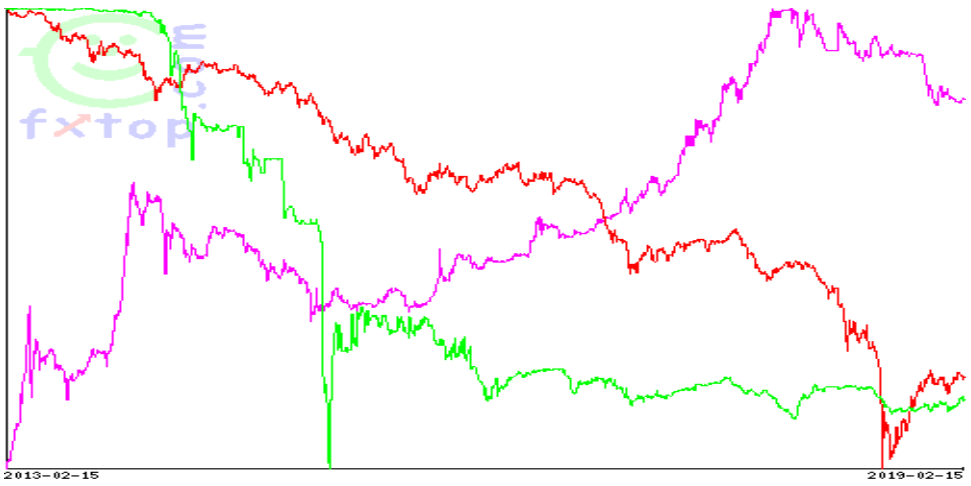

Diagram 2.0: Price comparison of BTC (purple), TRY (red) & UAH (green) to USD (2013 - 19)
(Credit: fxtop.com)

Creator's Identity

Bitcoin as an open-source project has greatly benefited from not having a "*leader*", as oftentimes, having a leader introduces the potential of centralizing decision making and tying the project's importance and livelihood to its creator. This sort of centralization is usually around governance when certain potentially costly decisions need to be made, having a leader would mean, their opinion would inevitably weigh more than that of other project stakeholders, such as developers, miners, and users.

A simple example of such cases would be, the 4chan hoax about the Ethereum founder's death[27], which saw the crash of Ether from $300 to $260 (an almost 13% decrease), following the announcement. This level of project value centralization is not something very beneficial to the health of the project. Another would be the Ethereum DAO hack, which saw the heavy involvement of its founder and other founding members, eventually leading to the decision to hard fork the chain; splitting it into Ethereum and Ethereum Classic[28].

Satoshi was aware of the potential risks mentioned above, and ensured they did not become an impediment for the development and governance of the project, by simply stepping away indefinitely. Projects like Litecoin have also followed in the same direction, where their founder withdrew from his leadership role to minimize the effect his presence had on the project.

Hacking

Bitcoin is heralded as a digital scam that is easily hackable, because it essentially lives on the Internet on the thousands of computers of random individuals around the world. Nevertheless, all computer systems whether the ones used by banks and other financial institutions or average users are hackable and doesn't mean we should all stop using computers. Banks and other financial institutions' portals are known to be more prone to hacking due to their centralized structure and usual poor design[29] than the Bitcoin protocol.

Generally, there are steps that can be taken to mitigate the risks of having a computer system hacked. In the case of Bitcoin, there are methods used to protect against common hacks like having your funds

stolen, which can be avoided by keeping private keys locally stored offline or using hardware wallets. The use of a hardware wallet, for example, would require the attacker to gain physical access to the device or use some other difficult method, which would still require them to crack the device user-set-passcode before they can access it. This provides the much needed added security to fend off most attackers.

Too Complex to be Widely Adopted

The complexity of the Internet and its underlying protocols like TCP/IP didn't have any effect on its adoption, it just took time before users could easily access and use it conveniently.

Users nowadays are unaware of the details of complex protocols like SMTP (*Send Mail Transfer Protocol*), but still manage to use Email clients like Gmail, Outlook, and such, daily, to send their Emails. The wide adoption of complex technologies isn't solved by just simplifying the protocols underneath, but in simplifying client-side applications and UI/UX of access points.

21 Million Supply Cap and Deflation

Bitcoin at the moment is experiencing inflation due to the mining of blocks, by design this is supposed to:

- Act as an additional incentive for miners along with transaction fees.
- Introduce more of the currency, at an ever-decreasing rate, due to the scheduled halvings.

According to classical economics, increasing the amount of currency in circulation reduces its value (at least theoretically). However, because the demand for bitcoin outweighs the supply, it has the inverse effect of increasing its value, as the increase of the bitcoin supply is deflationary in nature - each ~4 years the supply rate is cut in half. After the minting of the last of the 21 million bitcoins, it would begin to benefit from the effects of scarce assets like Gold.

This would further cement its use case as a store of value. Although, this would just make it only that - a store of value, but due to its digital nature, it can still be used for micropayments, where the divisibility of its units are not entirely capped - units as small as 1 Satoshi (0.00000001 of a bitcoin) can be used - allowing microtransactions to still be performed using bitcoin, effectively still enabling it to be a means of exchange. Gold, on the other hand, would have required the extra work of turning it into coins, to use as a currency, but Bitcoin allows for this functionality *out of the box*.

Bitcoin Will Eventually be Dethroned by Some Altcoin

> "*Altcoins simply cannot compete with Bitcoin because fundamentally they are companies, not protocols.*"
>
> - *Willem Van Den Bergh*[30]

A common critique of Bitcoin is that the changes to the Bitcoin protocol take too long to implement. However, this is not the case, as several protocol changes have been implemented such as Segwit, and a few privacy-enhancing features, and the Lightning Network all within a span of three years, while projects like Ethereum are still yet to implement their Proof-of-Stake (PoS) protocol upgrade as of writing (Jan 2020).

In trying to replace Bitcoin, the altcoin would have to be more secure, decentralized, have a larger developer base for continued code maintenance/enhancement and community tools and services. However, this is not an easy task, mainly because as new altcoins prop up that aim to replace Bitcoin, their individual network effects further fragment, meaning achieving Bitcoin's level of network effect becomes increasingly unrealistic.

It is also widely assumed that hard forks - which are the supposed main source of competition for Bitcoin - result in a dampening of its price. In response, Morgan Stanley has suggested that Bitcoin hard forks could be seen as a stock split, and further stated that "*unlike a stock split, the fork is not lowering the price per Bitcoin*"[31]. Meaning, contrary to popular belief, a hard fork sees the increase in Bitcoin's price and not a decrease, with certain cases where its price seems unaffected. The graph below highlights this price effect on Bitcoin.

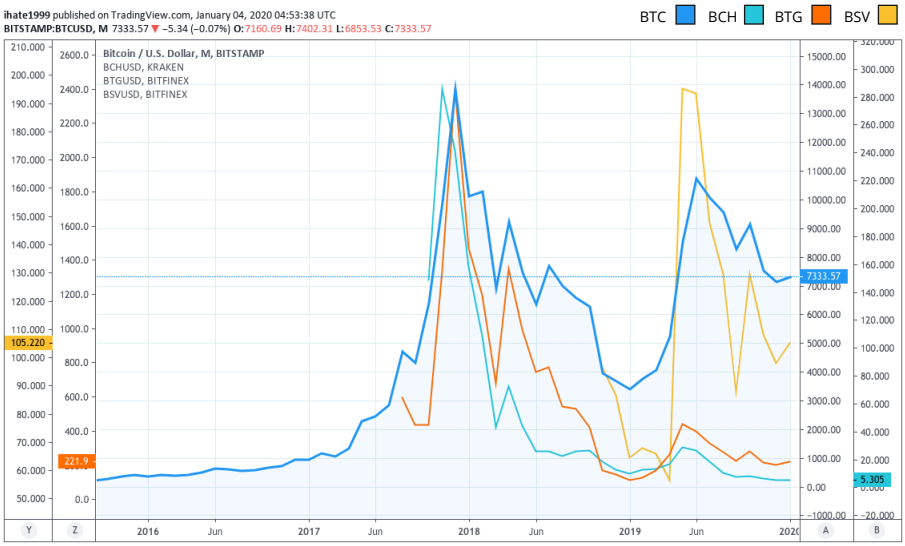

Diagram 2.1: Price comparison of BTC and hard forks; BCH, BTG, BSV to USD
(Credit: tradingview)

As observed in the graph above, these hard forks have little to no effect on the general price of Bitcoin over time. The graph seems to suggest the opposite, where the prices of other hard forks are directly affected by the price of Bitcoin - a fall in the price of Bitcoin sees a resulting decrease in the price of the hard forks, and a rise in Bitcoin price results in a increase in the price of hard forks - instead of the other way round.

Transactions are Anonymous

Bitcoin addresses are visible for as long as the Bitcoin Blockchain exists, essentially, it means that if a Bitcoin address or set of addresses is somehow able to be linked to a person, all their transaction histories become visible to the public.

Projects like Bitfury's Crystal - a set of software tools that help track illicit activity on Bitcoin's public ledger - can be used to detect whether a certain Bitcoin address or set of addresses have engaged in any form of illegal/criminal activities online, such as the purchase of illegal drugs. This allows these addresses to be flagged by Cryptocurrency exchanges, and also provide law enforcement with the necessary evidence to indite the guilty party or parties, assuming their addresses can be linked back to their identity. Other methods of identity discovery also exist, and have already been outlined in the *'Background'* section, and are therefore not repeated here.

No Developer Incentives

Developers contribute their time, skills and resources to projects like Bitcoin, even in the absence of any evident incentives, for the following reasons:

- Developers who own bitcoins have tremendous incentive to keep the protocol secure and functioning, through constant maintenance and upgrades to the source code.
- Open Source developers spend their time on projects they care about, even without financial incentives.

Nonetheless, there are still projects, organizations, and individuals who finance developers to continue contributing code to Bitcoin[32], these entities include the Bitcoin Foundation, MIT Media Lab's Digital Currency Initiative, Blockstream, Chaincode Labs Inc, etc.

Energy Waste

Bitcoin uses relatively large amounts of energy during the mining process, to secure the ledger, and thus, the entire network at large.

However, fiat-based currencies like the US Dollar instead rely on their army, who are charged with enforcing it upon nations to use, hence, the energy expended in keeping the US military-industrial complex going is what continues to ensure the US Dollar's value, meaning, while Bitcoin is secured with only electricity, the US Dollar is secured with nuclear plants, weapons, and wars, which evidently towers Bitcoin's energy use.

We would go into more detail much later, in the "*Understanding Bitcoin's Energy Consumption*" section.

Small Blocks

> *Larger blocks mean a larger Blockchain, which means fewer nodes able to download it, eventually leading to centralization.*

It is widely known that data scales to fill up space, therefore, increasing the block size could result in more transactions being added in a block, thereby filling the block(s), further requiring yet another increase.

The reasons for this are purely technical, the smaller the block size the thinner the ledger, and the faster the transactions are processed over the network. Increasing the block size sacrifices the network throughput, causing blocks to take longer to transmit over the network.

However, Bitcoin experienced an increase in its block size, which resulted in an increase from ~1MB to a ~4MB (theoretic limit) due to the SegWit upgrade[33]. The upgrade also had additional benefits like decoupling signatures from a transaction, to allow swapping of signature schemes if necessary in the future, and certainly much-needed base layer upgrades for later integration of second-layer solutions like the Lightning Network.

Small blocks help ensure the maintenance of the entire system, as larger blocks would mean running anonymous full nodes over TOR would be infeasible due to network latency, eventually

causing a decrease in the number of censorship-resistant full nodes, thereby increasing the chances of malicious full nodes colluding to censor the network, allowing them the ability to potentially edit consensus rules, such as, changing the 21 million supply, and ultimately causing potential security problems.

Identity traceability would become relatively easy, as the few consolidated nodes would act as guarded gates, working with exchanges and other on/off-ramp services that require personal information during sign up, would enable them to easily trace transaction graphs and link them back to real-world identities.

Consequently, blacklisted individuals would have their transactions easily blocked, because these exchanges could collaborate with the miners to ensure these transactions are not included in subsequent blocks, indefinitely.

Small blocks are also necessary to build fee pressure, enabling the continued financing of the PoW security model following the termination of block rewards.

No Turing

Bitcoin does have support for scripting, the method of spending bitcoins or UTXOs (unspent transaction output), this UTXO model is geared toward privacy, but other methods would soon be introduced like Taproot, MAST, etc. that would further extend the behavior of how bitcoins can be spent. Lightning smart contracts for opening and closing payment channels are also currently possible, using this existing scripting model of the UTXO.

It should be understood that a Blockchain can only be theoretically Turing complete. This is because code that evokes a loop that could run forever cannot be executed, as it would cause the whole system to grind to a halt[34]: where the execution of the looping code would never terminate, meaning, syncing the chain would be paused until the code has been executed, which cannot happen. Allowing practical Turing completeness would result in a larger attack surface, as was the case with the Ethereum DAO hack[35].

High Fees

Without the fee structure to ensure the longevity of the network, miners are left with no incentive besides philosophical stances to participate in the network, pending the last minting of the 21 million bitcoins.

It is still however possible to set transaction fees as low as 1000 Satoshis (0.000010000 of a bitcoin), and still get the transaction picked up by a miner. Some miners do pickup low fee transactions and include it in the blocks, albeit not as rapidly as transactions with higher fees. This means that most of the time it would require waiting several blocks before your transaction is picked up from the transaction pool.

You only add higher fees when you need your transaction to be processed as soon as possible. As such, one can even increase the fees on transactions that they have sent, by using techniques such as *Replace By Fees* (RBF) and *Child Pays for Parent* (CPFP), where the former simply replaces the transaction with another of higher fees, and the latter attaches a new child transaction that spends

the outputs of the parent transaction with higher fees.

Sometimes, the Bitcoin transaction fees can be affected by spamming the mempool (where unconfirmed transactions are stored) as a result of creating a lot of low fees transactions, thereby causing a spike in fees, as was the case in 2017[36]. This form of attack forces the creation of transactions with larger fees, to get their transactions included in future blocks, thus, moving the average transaction fees higher.

It seems as Bitcoin further transitions into Digital Gold, sending large amounts of money using Bitcoin would continue to be more efficient than through Banks. This is because, as it stands, the transaction fees for international payments, using Bank of America international wire transfers, for example, would result in a minimum fee of $30[37], while the minimum fee using Bitcoin is roughly at $0.50 (as of Jan 2020).

Transaction Finality and Speed

When we make a purchase online with say, a credit card, we get prompted that the funds have left our account to the merchant's - the transaction is completed. Sadly, there is more to it in reality, these transactions aren't completed for another day, week, or month(s) later, after your funds have gone through several checks before reaching the merchant. This period between when you make a purchase, and when the funds in your account have left to the merchant's account is known as *transaction finality*.

Bitcoin has a transaction finality of ~10 minutes on average, which is the approximate time it takes for a block to be added to the Blockchain. Not only is the transaction finality faster than traditional financial services, but the likelihood of the merchant having their funds taken away after a transaction is just as likely as the entire Bitcoin network being taken over, reversing all transactions ever made. At the moment, that would require spending a ludicrous amount of money, to buy hardware that has the equivalent computational power of 51% of the network, and paying for the electricity bills to sustain it, in an attack effort famously known as the "*51% attack*".

Visa and other centralized payment systems have higher transaction speeds than Bitcoin, this is because Bitcoin is no longer used to transact small amounts of money, and is now regarded as a settlement layer - where large amounts of funds are transferred and transactions confirmed. Visa and others are used to make what are known as micropayments (transactions of small amounts), therefore, to compare transaction speeds, one should compare the transaction speed between Bitcoin's Lightning Network and Visa. At the moment Lightning transactions can process magnitudes of transactions higher than Visa, due to its design.

The Lightning Network acts as a micropayments layer that sits on top of Bitcoin, able to facilitate transactions off-chain - that is, on an ad hoc network instead of the Bitcoin network itself. Individuals simply set up what is known as a "*payment channel*", and transact instantly as many times as they please, and subsequently broadcast the final state of those transactions to the Bitcoin network, hence, the analogy of the Bitcoin network being a settlement layer.

Bitcoin isn't as Fast as Project 'X'

We do often hear some project 'X' being called out as the new challenger to Bitcoin, because it can perform 1000x more transactions per second than Bitcoin, begging the question:

Why isn't Bitcoin being upgraded to handle 1000x or more transactions per second like project X?

These projects handle these levels of transaction throughput mainly because of the following three reasons:

- Whitepaper Propaganda
- Network Size
- Sacrificed Decentralization

Whitepaper Propaganda

These projects simply quote theoretical estimations that don't take into account real-world factors like network participant size, information loss in network communications, and a host of other known technicalities.

They more often than not just raise money to build a Cryptocurrency or Blockchain-based project, and abscond with the funds, leaving those with a vested interest in the project with nothing more than an overly complex written document - i.e. the project whitepaper.

Network Size

It is well known in the field of networking that, the fewer the nodes on the network, the faster the overall network throughput, and gradually plateaus as new nodes join the network.

These projects' network size is extremely small compared to Bitcoin's network, meaning, they could with time, as new nodes join, experience transaction speeds even lower than what Bitcoin can handle.

Sacrificed Decentralization

It is very easy for a centralized network to handle extremely higher transaction speeds than Bitcoin, as there are fewer paths to traverse, and no global consensus required. However, this defeats the whole purpose of a Cryptocurrency, and these projects often leave out this important information to raise funds. Bitcoin developers and contributors are aware of the potential speeds achievable, if centralized components are introduced into the design of the system, and are careful not to do so.

A typical feature of such a project is to have what they call *"master nodes"* and/or *"validator nodes"*. These are a small number of entities that engage in the mining and validation process, usually mostly controlled by the project themselves or representatives, making it a regular centralized payment network under the guise of a Cryptocurrency.

Understanding Bitcoin's Energy Consumption

- Governing factors of resource consumption for currencies
  - Production
  - Distribution
  - Maintenance of its Value
- Bitcoin Mining as a Catalyst for Green Energy
- Bitcoin Mining as a Potential Solution to "*Curtailment*"

> *"To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system ... 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."*
>
> *- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System*

We can immediately see that energy consumption is a necessary part of Bitcoin's functionality and security. The more blocks are mined, the more the energy it would require to edit a block on the chain, and the more energy that is added, the more the transactions become immutable. This effectively reduces the entropy level within the system and further secures the ledger.

There have been growing concerns about the amount of electricity consumption that goes into maintaining this system. Before one makes the exaggerated claim that *''Bitcoin is contributing to climate change*'', let us explore 3 factors that govern resource consumption for currencies, which are:

- Production
- Distribution
- Maintenance of its value

Production

Firstly, let's look at how a currency like the US Dollar fairs to Bitcoin in its production. The US Dollar requires relatively low energy consumption for the production of its physical form, all that is needed is the typical energy required to print large amounts of documents.

In the US, the electricity used during printing is ~97, 850 MWh of electricity or 350,000 GJ according to the *''sustainability assessment, on the quantification of the environmental impact of the dollar, in contrast with Australia's polymer-based notes''* by Ahlers, et al in 2010[38].

Distribution

In considering the energy consumption that these newly printed physical dollars require during distribution in the economy, we are mainly talking about the fuel required to power the vehicles that physically transport these dollars around the globe annually, from armored cars, cargo planes, to the other modes of transport that are used in its global distribution. This is not a light resource-consuming process at all.

Additionally, we have also not factored in the network infrastructure sustaining its digital distribution, as attaining estimates beyond guess work is highly unlikely.

Maintenance of its Value

> *All value comes at a cost, financial or otherwise.*

Remember that currencies of the world are fiat - without *intrinsic value*. Their value is ensured by the continued acceptance by Governments as a legal tender, meaning, the currency's value is contingent on the continued existence of the Government issuing the currency.

By extension, the maintenance of the value of these currencies is wholly dependent on the survival of

the Government that issued it, which means considering all the resources required to safeguard its existence. Simply put, we are talking about the resources expended by the military in protecting the Government from being toppled.

Therefore, the total energy consumption for maintaining the value of of a currency like the US Dollar is in the energy consumed by the US military, which is known to be one of the most resource-intensive endeavors on the face of the planet. This includes resources expended to produce nuclear weapons, aircrafts, military bases, and the energy expended in maintaining them.

In 2006, the US Department of Defense (DoD) used almost 30,000 GWh of electricity. This electricity could have been used to power more than 2.6 million average American homes[39], thus ranking the DoD 58th if it were a country, in terms of electricity consumption[40]. According to the 2005 CIA World Factbook, it would rank 34th if it were a country, in terms of oil consumption, where it used 4.6 billion US gallons of fuel annually[41]. In the fiscal year of 2009, the DoD consumed 932 trillion Btu of electricity[42].

Another major industry in the fiat currency space is banking. It is a known fact that the banking industry is a high energy-consuming sector. However, what remains largely unknown is exactly how many banks there are worldwide. These figures usually range between 14,600[43] and 25,000[44] or more. The very fact that there are more than 60,000 quasi-banks, that are almost as rigorously regulated as banks further clouds any possibility of obtaining a definite number, and as such, quantification of energy consumption would be almost always based on guess work.

However, based on the conservative estimates of Carlos Domingo in his piece *"The bitcoin vs visa electricity consumption fallacy"*, the energy consumption assuming there are 30,000 banks would be ~100 TWh[45]. That is, only accounting for the servers, bank branches and ATM energy consumption. The actual figure would definitely be much higher than the 100 TWh stated, and should be duly noted that these figures would keep increasing year in year out, as these banks continue to expand. As such, Bitcoin doesn't require the unnecessary electricity consumed by intermediaries in the current monetary system, and hence, is a more efficient use of electricity for powering the monetary system that it facilitates.

As Bitcoin is a peer-to-peer network, its liveliness is dependent on the participation of full nodes in constantly validating and propagating blocks. These full nodes ensure consensus rules are followed, as they reject invalid blocks that violate these rules, such as exceeding the 21 million supply cap. Some of these full nodes double as miners. The hardware requirements for setting up a non-mining Bitcoin full node are relatively low, as individuals can use inexpensive single board computers such as a Raspberry Pi. The costs are mainly in the Internet (due to the high bandwidth requirements) and electricity costs to keep the node connected to other nodes over the Internet. However, it is possible to cut down on the cost by limiting the total uptime of the node to 12 or 6 hours a day.

Further, Bitcoin full nodes are required to keep the network running, and hence are responsible for maintaining its value, as without active participation, consensus rules could potentially be broken and the network overtaken by bad actors, effectively making Bitcoin worthless.

The total number of full nodes on the network is very difficult to determine, as some full nodes do not allow open queries on their network ports, but what is known is that of the full nodes that do allow this, they number in the thousands. To estimate the annual energy consumption of these full nodes it would require a lot of assumptions about the total electricity each node consumes.

Given that some full nodes are miners, this value becomes even more difficult to determine. We can however attempt to estimate a lower bound on the electricity consumed by non-mining full nodes. Assuming there are about ~10, 000 full nodes worldwide, and 40% of them are Rasberry Pis that do not mine, each requiring 14,016 kWh of electricity annually, the total annual energy consumed by these full nodes would be around 0.056 TWh.

The energy consumed in the distribution of bitcoins is implicitly included in the energy consumed in its maintenance of value, as it is a digital asset that lives on the ledger hosted and shared by the thousands of full nodes on the network.

As of Dec 2019, Bitcoin mining is said to consume over 73.12 TWh annually[46], which is about 0. 000000004% of the DoD's electricity consumption in 2009 alone. Nonetheless, future mining equipment would ensure more efficient use of this energy, which would bring this number down.

Effectively, when comparing the energy Bitcoin as a whole consumes to fiat currencies like the US Dollar, we are essentially comparing the energy consumed by miners in each block creation, and the energy consumed by printers, servers, ATMs, in (central) banks, vehicles that transport and distribute the physical form of the currency, and the nuclear weapons et al in the military. Without going any further it should be obvious that the energy consumption of the former is extremely negligible compared to that of the latter.

Bitcoin Mining as a Catalyst for Green Energy

The mining of bitcoins as we already know requires electricity, and since the primary generation method of electricity around the world is fossil fuel-based, the advent of Bitcoin mining has resulted in more efforts towards greener and more efficient/sustainable sources of electricity. This is because the cost of electricity would be greatly reduced by using greener sources of energy, which means, miners have a high incentive to back up the change.

Maintenance costs of mining rigs would drastically reduce, meaning miners can enjoy the additional income from the mining process that would have ordinarily been channeled to electricity costs. As more miners seek to adopt greener electricity, the price of these technologies would continue to reduce, eventually leading to levels that would facilitate the global transition from *dirty* to *clean* electricity, further contributing to the collective efforts of providing an open, decentralized and censorship-resistant system of money, whilst leading the clean energy revolution.

According to Coinshares Research report *"THE BITCOIN MINING NETWORK Trends, Average Creation Costs, Electricity Consumption & Sources"* (Dec 2019), the current approximate percentage of renewable power generation in the Bitcoin mining energy mix stands at 73%, therefore, making Bitcoin mining more renewables-driven than almost every other large-scale industry in the world. Meaning, Bitcoin mining is already leading the Green revolution.

Bitcoin Mining as a Potential Solution to "Curtailment"

Renewable energy production has to deal with what to do with excess energy produced by solar panels, windmills, and other green energy production sources. Storing this excess energy for later use is often suggested, however, storing this energy in batteries can be costly, inefficient and sometimes impossible.

This has since led to some power grids just cutting off energy productional together as a solution to overproduction - a phenomenon often referred to as "*curtailment*". We would proceed to analyze China's solar, wind and hydroelectric curtailment, as they are the Global leaders in all three fronts, for some idea on the energy that is lost due to curtailment.

China experienced solar curtailment of about 6% - 7% in 2017[47], effectively curtailing about 11 TWh out of the 188 TWh they produced. China's curtailment of wind energy was 12% or 41.9 TWh in 2017, this combined with the energy curtailment of solar could have powered the entire country of Ireland for 2 years[48], and added with the curtailment of hydroelectric energy (about 2% - 3% or 31 TWh in 2016) could have powered it for a total of 4 years[49].

A common approach to combat curtailment is to store this excess energy in batteries, to improve energy grid management, however, it too faces a number of challenges. For example, batteries are expensive, and experience energy loss of about 10 - 20% to heat during charging[50]. If this excess energy were to instead be sold to other countries, the energy losses from transporting electricity is estimated to be at 8 - 15% [51]. All these problems pose a huge challenge for these solutions, and thus indicates the need for better and more efficient use of this excess energy.

The renewable energy industry could begin to use ASICs - specialized hardware used for mining bitcoin - to help remedy the problems brought by curtailment. By simply channeling this excess energy to Bitcoin mining they can introduce a new alternative revenue stream, resulting in both the securing of the Bitcoin network and the provision of an alternative income stream.

Giving the renewable energy industry an alternative revenue stream could see the potential reduction in the cost of renewable energy equipment, potentially resulting in more adoption due to their new affordable prices. Ultimately fast-tracking the global transition from fossil fuel-based energy production, to more eco-friendly energy production methods, such as solar, wind and hydroelectric.

One might be tempted at this point to raise the question, "*what would happen after the last of the 21 million coins have been minted?*" The current estimates suggest that this would take place sometime in the next century (~2140), and in that time frame, there are huge profits to be made from mining Bitcoin.

By investing in mining equipment to aid with the problem of curtailment, they can gain huge amounts of additional income from mining Bitcoin. The tremendous amount of time between now and 2140 provides ample time for the potential discovery of better solutions to curtailment in the future. Mining bitcoin could, therefore, act as a very profitable solution, albeit in the short term, which could provide the necessary capital for funding R & D programs to search for potential long term solutions.

Why Invest in Bitcoin?

- Bitcoin as Money
- Antifragility of Bitcoin
- The Lindy Effect and Bitcoin
- Proof-of-Work (PoW) as a Core Component
- Privacy Features
- Bitcoin as a Store of Value
- Bitcoin Returns
- Bitcoin Portfolio Allocation

Bitcoin as Money

Money has 3 fundamental use cases:

- Store of value
- Means of exchange
- Unit of account

Store of Value

Though over the years price volatility has seen dents in the value of bitcoin, one's wealth would have still been preserved and increased if they held bitcoin since late 2012 to date. Store of value can only be properly measured over a long period of time, as such, Bitcoin has evidently performed quite well, going from $1 in 2011 to ~$7,200 as of Jan 1st 2020. The graph below highlights this growth:

Diagram 3.0: Plot of Bitcoin returns over the years
(Credit: tradingview)

Means of Exchange

It is very easy to cheaply send large volumes of bitcoin openly from one party to another globally, and also possible to engage in micropayments using the Lightning Network with negligible fees.

Unit of Account

Bitcoin can be used as a benchmark for pricing items, in an attempt to determine the increase or reduction in their price. Bitcoin is already used in the Cryptocurrency community amongst altcoins as the benchmark for their prices, to highlight their value changes, and also has the following use cases as a unit of account:

- Miners have to consider whether a mining rig would mine more bitcoin than it would cost.
- Merchants price their items online in terms of bitcoin (or satoshis - 100 millionth of a bitcoin).
- Electricity consumption can be tracked using bitcoin, by calculating watts consumed per bitcoin.

During times were bitcoin prices rise, items priced in bitcoin fall, generally signaling the ability to purchase more items with bitcoin.

Due to the continual increase in the price of bitcoin to the US Dollar, valuing items in bitcoin does not provide as much insight into its price. As such, bits or micro-bitcoin (0.000001 of a bitcoin) were used by wallets, for example, to adjust for the price of bitcoin to the US Dollar for better price valuation. However, even that doesn't exactly capture prices as accurately anymore, as a result of the further increase in the price of bitcoin to the US Dollar. This has prompted the switch to use satoshis, which are the smallest useable unit of bitcoin, to become the standardized unit of valuation.

Below is a diagram to elaborate more on using bitcoin as a unit of account in terms of satoshis:

Unit	Abbreviation	Decimal (BTC)	Decimal (Satoshi)
bitcoin	BTC	1	100,000,000
deca-bitcoin	dBTC	0.1	10,000,000
centi-bitcoin	cBTC	0.01	1,000,000
milli-bitcoin	mBTC	0.001	100,000
micro-bitcoin	µBTC	0.000001	1,000
Satoshi	sat	0.000000001	1

Diagram 3.1: Satoshi Unit of Account
(Credit: Recursive Capital)

Money Properties of Bitcoin

Bitcoin possesses all the properties of money as elaborated in the following diagram:

Property	Description
Fungible	1 BTC is always equivalent to 1 BTC
Durable	Its digital and thus can't wear down from use
Divisble	Its divisibility depends on the divisbility of an integer on computer systems.
Portable	It is digital and therefore nowhere, while being available everywhere
Acceptible	It is accepted by an increasingly large amount of merchants, individuals, etc.
Limited supply	It is permanently capped at 21 million coins.
Uniform	It is digital; the same throughout its copies.

Diagram 3.2: Money properties of bitcoin
(Credit: Recursive Capital)

Bitcoin having surpassed Gold and the US Dollar in possessing the above qualities is definitely on course to be a global reserve currency for the exchange of global goods and services, and a store of wealth for nations, Sovereign Wealth Funds (SWF), Hedge Funds, Central Banks and households in general.

Antifragility of Bitcoin

It was well known to Bitcoin's creator that, for Bitcoin to succeed it would require a global effort, which eventually led to the natural decision to open-source its code. Essentially placing the building blocks of an entirely new financial system solely in the hands of the public. Where on the one hand, there are individuals willing to invest their skills, time and resources into improving and securing the protocol's source code and overall network, and on the other hand, are individuals whose primary aim is to take advantage of security holes, and other design flaws to their often financial advantage. Thereon, Bitcoin would ultimately be subject to constant attacks by those aiming to enrich themselves with this new Internet Money.

What is Antifragility?

For Bitcoin to succeed, it would not only have to be robust - able to withstand these attacks - but would have to benefit from these attacks, meaning, the underlying protocol should become even more secure with new attacks. This property of benefiting from chaos - hacks and other negative forces - has since been aptly termed *antifragility*[52].

Additionally, all things that are antifragile have their sources of chaos, and in the case of Bitcoin, these have majorly come from the following four sources:

- Hacks
- Forks
- Media Coverage
- Government Pressure

Hacks

Throughout the course of Bitcoin's history, it has suffered numerous hacks to its underlying protocol, and businesses/services around it. These hacks range from taking advantage of protocol-level bugs, to purely attacking Bitcoin exchanges, as they act as a perfect wealth collection point for attackers.

Forks

Bitcoin is a global effort, which means, its governance model would have to be democratic. Naturally, there would inevitably be contrasting opinions and clashing interests, as it is an inherent feature of democracy. As such, there is always the potential for minorities in the community who no longer share the majority's values/interests, to decide to create an entirely new separate community. They tend to do so by copying the Bitcoin source code and extending it based on their new ideas, in a process widely known as a *hard fork*. Which causes an initial confusion for newcomers, as they are now faced with the decision to choose which community to join.

This has the potential short term effect of fragmenting the pool of talented developers in the community, as they are now faced with a decision to join the new community. However, with time, it eventually becomes obvious which community is the derived fork.

Media Coverage

The Internet has fully democratized information access, which has resulted in greater access to an ever increasing audience of people. The shear number of news/information outlets is overwhelming,

and individuals are constantly being bombarded with eye catching news headlines and narratives, as these outlets continue to battle for their attention.

Bitcoin has so many intriguing angles to it, and all but a few have since been covered. What started out as weird a digital currency initialized by an anonymous creator that facilitates illegal trade online, has since become the "*Global Ponzi Scheme*"/"*Tulip Bubble 2.0*", with more narratives constantly being developed.

Government Pressure

Bitcoin by design is a competitor to Governments, as it aims to be a global currency system, meaning it would effectively compete with their native currencies. This has since resulted in several Governments banning Bitcoin-related activities and businesses, such as the purchase of items using bitcoins and Bitcoin exchanges. This has resulted in preemptive bans that dampen its price in the short term. Bans that affect exchanges make it difficult for investors that use these exchanges, by burdening them with the task of seeking out alternative solutions.

All this chaos and disorder has benefited the following three main facets of Bitcoin:

- Technology
- Community
- Economics

Technology

The fall of Bitcoin companies such as Mt. Gox provided the necessary pretext for the creation of better, more secure exchanges, and other businesses. This helps fragment the global Bitcoin transaction volumes across different regions, as different exchanges around the globe continue to prop up in response, providing it with the opportunity to withstand potential bans in certain jurisdictions.

As an open-sourced project, Bitcoin is constantly being subjected to attacks to its underlying protocol, exchanges and the other services built around it. In the case of protocol hacks, this was originally the most sought after avenue for stealing bitcoins but has since been abandoned, due to the work put in by developers in sealing off all known security flaws in the protocol. The most used techniques now tend toward hacking exchanges and wallets. This has prompted the adoption of industry-standard security measures and techniques to safeguard against hacks.

Another less popular technique is mempool spamming; where thousands of diminutive low fee transactions are sent over the network to handicap its functionality or boost up miner fees. This has since become easier to detect, and the layers of redundancy in the Bitcoin protocol, coupled with the level of decentralization of the network enable it to circumvent such attacks, rendering this attack vector not as effective as it otherwise would have been.

A major benefit worth mentioning is that the experimentation of technologies performed on Bitcoin forks provides the opportunity for integration into Bitcoin at a later stage, after having been tested to the point of stability and acceptance amongst the community. This allows Bitcoin to leverage new ideas that would greatly increase its utility value, whilst remaining largely unaffected as they are being tested on other forks. The experimentation of second layer solutions also provides a similar opportunity, in that, the stability of the underlying protocol is unaffected by the development of

second-layer networks and other ad hoc networks.

For the past 10 years, Bitcoin has survived numerous hacks, battle testing from security audits, and other security and technology vetting techniques. This has oftentimes placed it in a situation of absolute failure or success, in which case it has proven and continues to prove its superiority as a technology over its assumed competitors.

Community

As the quote goes, "*First they ignore you, then they laugh at you, then they fight you, then you win*". For 10 years now, Bitcoin has been the subject of bad press, which continues to greatly contribute to its "underdog" narrative, as individuals would be more interested in seeing it succeed. This eventually leads to the indoctrination of new members to its community. The bad press also ensures that it continues to stay relevant as an important technology, as it after all must be important for it to be critiqued by policy makers, and banned by Governments.

The "*forking*" optionality provided by Bitcoin enables the unique opportunity of providing others with the ability to experiment on its source code, without affecting it. This allows experimental features to be tested simultaneously, providing stakeholders the ability to see through the narratives, propaganda and hidden interests. Furthermore, each time there is a Bitcoin fork, the Bitcoin community becomes stronger, because malicious or contemptuous forks become more evident, resulting in the consolidation of the core community ideals amongst its members, in an attempt to distinguish themselves from these new forks.

Each of these new forks acts as a new separate entity, requiring it to build up its trust, rebuilding its image and coming up with new fundamentals in the process, while Bitcoin increases its trust amongst existing stakeholders, as it continues to survive contentious and malicious forks. Meaning, the Bitcoin community becomes stronger and more united with each new fork.

The continued hacks to Bitcoin-related businesses and services (e.g. exchanges and wallets) results in more security conscious design of Apps and services by developers, increased education by the community on proper security measures to guard against theft/loss of funds, and an increased number of more secure exchanges, wallets and other services.

Economics

Continued hacks on Bitcoin and its related services see evident decreases in the following:

- Amount of bitcoins stolen
- Market effect

Governments that decide to ban Bitcoin would have the adverse effect of promoting it in the long run, as more individuals would be interested in Bitcoin, resulting in more adoption, and existing Bitcoin users/exchanges would flock to more Bitcoin-friendly jurisdictions, eventually seeing the potential increase in Bitcoin's price. For example, in 2017, as part of several measures taken by the Chinese Government to ban Bitcoin-related activities, the first of the many attempts saw the almost immediate drop in Bitcoin's price by 20%, however, Bitcoin's price reached record-breaking levels (~$20,000) that same year, even spilling over to the next.

Due to several factors, one of which is media coverage, Bitcoin goes through boom/bust cycles, where

each boom is catalyzed by intense media optimism, which is then eventually followed by an eventual market price adjustment - burst. According to Bitcoin *"bubblists"* - those who believe Bitcoin is a bubble - we have had 3 major bubbles so far, and have provided the summary of these bubbles below:

Bitcoin Bubble Bursts

Period	Name	Price Decrease	Percentage Decrease	Google Trends Decrease	Market Cap	TX Volume High	TX Volume Low
2011 - 12	The Great Bubble	$39 - $2	93%	N/A	$190.4 Million	12, 000	4, 700
2013 - 15	MT.GOX Hack	$1,151 - $177	85%	85%	$13.94 B	102, 000	41, 476
2017 - 18	FUD Wave	$20k - $3.2k	84%	93%	$327 B	450, 000	130, 000

Diagram 3.3: Bitcoin Bubble Bursts
(Credit: Recursive Capital)

It is evident in the diagram above that each Bitcoin bubble burst results in a significant record increase in its overall price, market cap, and transaction volume. This could be attributed to the initial media buzz that brought an increased number of nodes to the network, both validators and miners, who introduce immense computational power that increases the security of the entire network, coupled with an increased level of developer interest, which then sees an increase in the number of bug fixes, security/functionality upgrades and maintenance of the source code, ultimately leading the way for greater adoption.

Bitcoin forks also bootstrap Bitcoin's price, as was seen in **diagram 2.1** of the "*Misconceptions of Bitcoin*" section.

The Lindy Effect and Bitcoin

So far, in the 10 years of Bitcoin's existence, it has managed to successfully weather all forms of external attacks, whether it is notoriety in mainstream media, Government pressure, hacking, or hard forks. This continues to greatly contribute to the increasing level of trust individuals continue to place in it, as a truly open *Internet Money* and *Gold 2.0*. It seems that the longer Bitcoin exists, the more certain its likelihood of long-term success becomes, a property since termed the *Lindy Effect*.

The Lindy Effect is a heuristic that ensures investors and other stakeholders seeking to get in on Cryptocurrencies that Bitcoin is a superior choice, having been the oldest standing Cryptocurrency further guarantees its continued existence, vis-a-vis any other Cryptocurrency. It is also the reason why protocol level encryption schemes such as RSA are used instead of much newer ones like zk-SNARKS.

The longer Bitcoin exists, the more it would continue to be subjected to intense attacks, of which, as we have analyzed above, it always gains from. Its antifragility to such attacks would continue to be pronounced over the coming years. Bitcoin would likely continue to remain unseated by any other Cryptocurrency, as they lack the necessary antifragility to match it in being an actual *Internet Money* and *Gold 2.0*.

Proof-of-Work (PoW) as a Core Component

There has been growing condemnation around the consensus mechanism Bitcoin implements - Proof-of-Work (PoW) - for mainly being a huge strain on the environment, due to its electricity requirements.

PoW is a computation system that requires the expenditure of compute-power, to find a hash output (a large number usually represented in base 16) that meets a certain criteria, e.g. a minimum number of prepended zeros. This process of finding a *'valid'* hash involves searching for a large random number, a process that is known to have no efficient shortcut, except through brute force. Meaning, to find a solution, there must have been significant computation done, which provides the *'proof '* that *'work'* had been done to find the valid hash.

This provides a very straight forward way of determining the validity of the hash itself because it involves using a one-way hashing function, which can be verified fairly easily but is computationally infeasible to reverse engineer.

Due to the intentional randomness involved in the mining process, open participation amongst existing and future miners is maintained, with no effect whatsoever to the network's overall security and operations. By extension, miners alike at any given point can participate in the mining process.

However, other consensus mechanisms such as Proof-of-stake (PoS) suffer from a variety of problems and could tend toward an overly complicated design and method of operation. Mostly, *potentially* featuring an eventual aristocratic design: where validators of high wealth (i.e. *coins*) make decisions about the state of the network.

Bitcoin's PoW has so far been the only consensus mechanism to achieve the following:

- Minimize the opportunity and motivation for miners to cheat or hassle the participants.
- Attract skilled developers to build the system without direct compensation.
- Eliminate gatekeeping, and allow anyone to use the system without permission; to achieve the maximum growth and success of the software.

PoW by design selects a winner pseudo-randomly from the pool of miners, by requiring their candidate block to meet certain difficult characteristics, such as requiring a certain number of prepended zeros in the block hash. Once these validation criteria are met, this winning block is propagated through the network, accepted by each full node, and is subsequently appended to the Blockchain - at which time the winning miner is also rewarded with a *coinbase reward*. This reward as of Dec 2019 is 12.5 BTC.

This is why Bitcoin is seen as having a more strict supply schedule than Gold and fiat currencies and having absolute scarcity, which aims to guarantee a proper solution to the current inflation of the currency, through the mining process.

Effects of a PoW Based Network

The Bitcoin network grows in value from two factors:

- Developers
- Hardware

Developers happily volunteer time, energy, ideas, bug fixes, and computing resources to a project, which ensures that malicious code does not sneak into the source code or potential security holes, in the form of bugs.

Bitcoin leverages Linus Torvald's Law: *given enough eyeballs, all bugs are shallow*. Where needed upgrades that enhance/maintain its functionality and security are added relatively quickly, resulting in better network architecture and code, due to the heavy involvement of more talented developers.

More developers would also result in a visible influx of hardware, since developers that upgrade and maintain the software would want to test out these changes, contributing more computational power that further secures the overall network.

There are huge benefits on the part of developers for the continued development of Bitcoin, as they enjoy the externalities that come with its maintenance, that is, open, decentralized, censorship-resistant money. Also, for the developers that also double as miners, the reward is substantial: from the coinbase reward, fees, to the availability of open money.

New miners also introduce immense computing power, through the additional mining hardware they bring into the network, which would help further raise the long term level of security in the network. If these miners join a mining pool that has relatively low hash rates, they would be able to contribute and increase the overall hash rate of the pool, thus, further fragmenting potential mining pool monopolies, fostering more decentralization across the network.

Proof-of-Stake (PoS) as an Alternative to Proof-of-Work (PoW)

Since Bitcoin's initial release into the world, there have been those critics who were quick to point out the potential shortcomings of its consensus mechanism - PoW. Viewed by them as an unnecessary resource-consuming system, which could be replaced by a more efficient and low resource-intensive process known as Proof-of-Stake (PoS), albeit at the implicit expense of decentralization.

In this new proposed system, the mining of blocks would no longer require miners to expend computing power to produce blocks, instead, they would have to prove their ownership of coins and " stake" these coins on a possible candidate - that would be randomly selected - to produce the next block.

In theory, the staking of coins should be viewed as a disincentive for miners to not cheat the system, since their coin holding's value would be at risk.

However, in practice, when coins that are to be staked are created ex nihilo, that is, at no production cost, it would undermine the value of these coins, and would no longer serve as a good deterrent for possible future profitable attacks on the system. This scenario has since been dubbed, the *Nothing-at-stake* problem.

In spite of the above-mentioned problem, there are still attempts by projects like Ethereum, that aim to provide viable solutions using techniques such as "*Slasher*" for example, to curtail these problems.

Nevertheless, even with such mechanisms in place, there is still a potentially fatal flaw that resides in this system. This potential attack vector is in how the *pseudo-random* generator that picks the winning miner is implemented. If an attacker can study the pattern of the generator, and successfully predict the subsequent miners that would be chosen, there would be no incentive whatsoever that would stop them from exploiting this low-cost vulnerability. It is in the miner's interest to find such a pattern to make a *"killing*".

Needless to say, the history that is built atop PoS is not immutable, since the system can be (easily) manipulated. This is one of the primary problems that contribute to its inability to potentially replace PoW, for the simple reason that, it cannot form a useful basis for a global digital economy if transactions' finality and logging are not fully immutable.

As such, in recent times, the potential application often cited for such a system is in its deployment as a consensus mechanism for *Permissioned Blockchains* in enterprise solutions. This is because enterprise networks are closed off, and don't need the level of security that is required for open global networks like Bitcoin. These enterprise solutions cannot be comparable to PoW systems, in that, they require tremendous costly upgrades both security and function-wise to compete with them, rendering their utility limited and unable to scale to compete with cheaper, more reliable, secure, and accessible PoW based systems. These enterprise networks also do not require any form of network decentralization, meaning, PoS is a perfect fit, as the decentralization-efficiency trade-off is no longer present.

Proof-of-Stake (PoS) and Proof-of-Work (PoW) Hybrid Systems

Attempts to use PoS as an abstraction layer atop PoW have been severely proposed, where the creation of blocks is still done using PoW and PoS as a governance layer. The aim here is to use PoS to distribute coins to full nodes and miners, not just miners, in hopes to ensure power doesn't get concentrated into the hands of miners or developers - which could lead the formation of miner cartels. Though this hybrid system is still yet to be as successful and as decentralized as purely PoW systems. It seems it is easier for decentralization to emerge as a consequence of design and not forced by design, as is the case with this hybrid system.

Bitcoin is only where it is today because of the design simplicity of PoW and its beneficial consequences, hence, for there to be a proper contender to Bitcoin, it would need to surpass PoW in function - to foster better Internet money, store of value and be more decentralized.

Privacy Features

Bitcoin's fungibility is at risk, due to privacy-invading tools that blacklist certain addresses, essentially reducing the worth of those bitcoins associated with them. Meaning certain bitcoins could be worth more than others - greatly affecting fungibility - and as a result, bitcoins would be classified into two: *'clean'* and *'dirty'* bitcoins. Where the former describes coins that haven't been used to engage in shady commerce online, and the latter, ones that have. Exchanges blacklist these *'dirty bitcoins'*, resulting in holders of these funds being unable to engage in trade on these exchanges, reducing the value of their funds.

There are, however, measures used by some privacy-focused wallets such as, Samourai wallet and Wasabi wallet that implement techniques such as *Ricochet* and *CoinJoin* that obfuscate the origin of bitcoins, to avoid *dirty bitcoins* from becoming worthless, ultimately preserving fungibility - a fundamental feature of money, and hence, Bitcoin.

We briefly explore some of these privacy features that have been included in the Bitcoin protocol and wallet software - mostly visible in privacy-focused wallets, such as Samourai and Wasabi Wallet.

Stealth Mode

A wallet feature that allows an individual to hide the wallet software on their phone, to safeguard against unauthorized individuals from gaining access to their funds, or Government officials in Bitcoin unfriendly countries that check for and confiscate Crypto-related devices, from being able to do so.

PayNym & PayNym Bot

A wallet feature that allows individuals to send and receive bitcoins privately using a public reusable code. A PayNym Bot is a unique visual representation of a (valid BIP47) Reusable Payment Code, that can only be controlled by the private key holder. BIP47-enabled-wallets produce a special static publicly shareable code, which can be scanned by other compatible wallets, that generate unique unused bitcoin addresses that are void of prior transaction or balance histories. Ensuring that previous transaction/balance histories stay private.

Ricochet & nLockTime Based Ricochet

The basic concept behind **Ricochet** is as follows: transactions go through several hops before reaching their intended address.

This helps obfuscate the transaction origin, by including additional transaction hops between numerous addresses created by a single private key. This along with other privacy features are aiming to solve the fungibility problems faced by Bitcoin.

Automated flagging techniques employed by third parties such as Coinbase determine if a transaction is suspicious, by tracing the origin of the funds, backtracking five hops back for example, in a transaction graph. Ricochet adds additional hops to each transaction, forcing Blockchain spies to put in a lot more work in their analysis, increasing costs and overheads, ultimately aiming to make it far less appealing to get involved in these transaction investigations.

As for *nLockTime*-based Ricochet, it provides the opportunity to delay the inclusion of transactions in blocks, causing transactions to be delayed, to be mined only after a certain time - in some future block. This along with increased hops in a transaction graph would aid in combating against being flagged by Blockchain investigation software.

Watch Only Address(es)

One can set up a watch-only address in the bitcoin core software. This allows the user to monitor all transactions that affect a given address or set of addresses, to monitor any, and all activity. This feature allows users to have their very own block explorer, to watch for any incoming or outgoing transactions associated with a certain address or set of addresses that they control.

Bitcoins that are in this watch only address cannot be spent unless the private keys are available to the user, and imported into the wallet.

VPN + Tor

This is the canonical method used to setup a full node, to reduce the likelihood of the original transaction sender's IP address being discovered. Meaning, even if an adversary was to get the IP address of the sender of a transaction, they would be unable to trace it back to the actual sender, because the IP address would belong to some random computer somewhere in the world, leaving your identity anonymous and essentially untraceable.

CoinJoin

CoinJoin was first detailed in 2013 by Gregory Maxwell on bitcointalk.org, and is described as a situation where multiple participants add inputs and outputs to a common transaction to obfuscate the transaction graph.

The basic concept behind CoinJoin being;

> *"When you want to make a payment, find someone else who also wants to make a payment and make a joint payment together."* [53]

CoinJoin is a Blockchain space-efficient privacy technique, as transactions are batched together, making it amongst the cheaper on-chain solutions, as fees are paid at once for the batched transactions, and not individually.

STONEWALL and Stowaway

STONEWALL, a unique method of transaction construction, aims to obfuscate the linkability between the sender and receiver in a transaction. These transactions are designed to mimic joint transactions, through the addition of arbitrary inputs and outputs to a regular Bitcoin transaction, enabling it to pass off as a CoinJoin transaction to an outside observer. Which makes it more difficult for Blockchain forensic tools to analyze, as its design lies outside their standard assumptions of Blockchain transactions.

Stonewall transactions can force Blockchain forensic tools to rely on probabilistic analysis of transactions, as it assists in polluting the Blockchain analysis process, helping in solving the fungibility problem.

Another currently usable privacy feature is pay-to-endpoint (P2EP), Its aim, however, is to obfuscate the identity of the sender and receiver in a transaction, by requiring both the sender and receiver to contribute inputs to the transaction. Stowaway, a form of this technique, is available in the privacy-focused Samourai wallet as part of their Cahoots framework.

Transaction Privacy and Anonymity

It is quite common to conflate privacy and anonymity as being the same thing. In a general sense, they are almost interchangeable, as they are usually discussed in the context of identity. Their differences only seem obvious when the context changes. That is, without a predefined context for discussing the terms, anonymity could be seen as being a subset of privacy in a certain sense.

However, when talking about transactions, privacy and anonymity are not quite the same. Private transactions are ones that have the amount obfuscated or hidden, and an anonymous transaction is one where the parties involved in the transaction have their identities obfuscated or hidden. Below is a diagram to buttress this point:

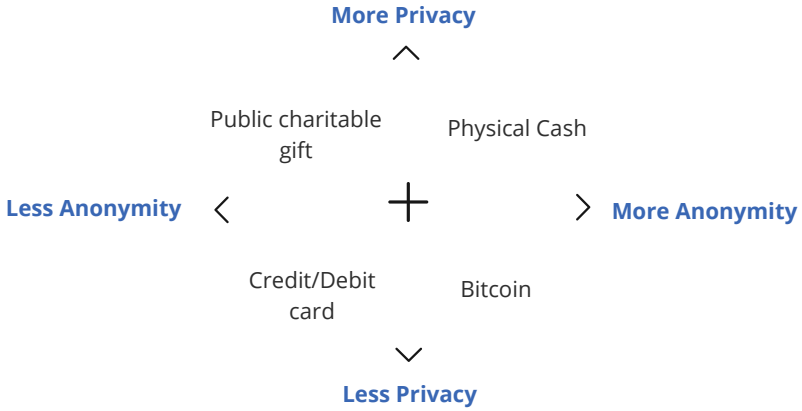

Diagram 3.4: Transaction privacy & anonymity classification matrix
(Credit: Recursive Capital)

It is evident that tools like cash are the perfect mix of both privacy and anonymity, and is a better solution for problems posed by cashless societies and increasingly surveilled states toward individual privacy, autonomy, and anonymity, at least for now.

The integration of technologies such as Taproot, Confidential Transactions (CTs), MuSig, Schnorr signatures, DANDELION, and SNICKER, to Bitcoin, would finally enable it to become a full parallel to cash in the digital realm, making the above diagram look more like this:

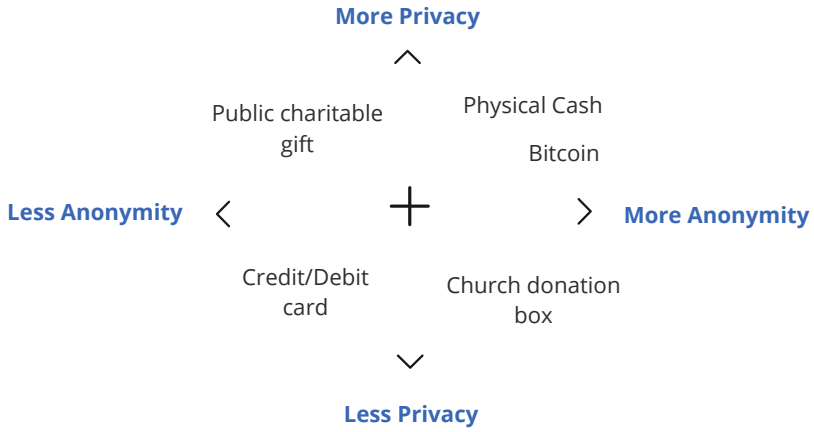

Diagram 3.5: Transaction privacy & anonymity classification matrix
(Credit: Recursive Capital)

Bitcoin as a Store of Value

For anything to be considered a good store of value, it requires proper value retention over time, and in order for this value retention to exist, it must to some extent be independent in its valuation and supply of any central authority - Governments, Banks or otherwise - to avoid value disruption over time through supply interference, and other avenues of value control.

In the case of Bitcoin, its decentralized, open, censorship-resistant qualities, and fixed supply are what effectively ensure the value retention. Devaluation and supply manipulations/alterations of any kind, with or without the involvement/co-operation of any central force cannot take place outside the strict set of rules defined by the protocol itself. Other assets like Gold also share a similar property, in that, no central authority can significantly influence its valuation, which enables it to further retain its value over time.

Historically, Gold tends to consolidate under the control of a few, whether it be aristocrats, monarchs or central banks, a flaw in which has historically been exploited ad infinitum. It is not far fetched to claim that this is because of the cycles of wealth exchange from existing to new Gold holders, whicmainly occurred when large amounts were taken from the existing holders, usually through theft, instead of through commercial activities. Bitcoin, however, can avoid the inherent centralization mechanisms of Gold and has for the first time essentially separated monetary policy from any interference by central or state actors.

Additionally, a Cryptocurrency that has little to no utility value, but possesses all the open, decentralized, censorship-resistant properties that enhance, and to some extent guarantees, value retention would most likely lose value over time, as there is no base (utility) value to hold or persist said value over time.

The skeptic may still have questions about the underlying utility value of an asset like Bitcoin, suffice to say that, the underlying utility value of Bitcoin is in the degree to which it accomplishes its promised use case - Internet Money. Which we can to some large extent say it has achieved; as anyone from anywhere in the world can exchange value openly and freely with one another, and also preserve their wealth using this Internet Money.

We have so far seen, and continue to see considerably large increases in its utility value; driven primarily by increases in mass adoption, which further sees increases in its speculative value, and overall value in general, further increasing and maintaining the value being retained over time. We can attribute this increase in adoption to the following benefits that Bitcoin offers to individuals who invest in it long term (i.e. HODLers):

- Exposure to gains from speculative trading, as is shown in **diagram 3.0**.
- Asset benefits of Gold: Preservation and compounding of wealth.
- Asset seizure resistance: Governments are unable to seize one's assets.
- Hedging vehicle against possible future bank crises and currency inflation.
- Portfolio diversification asset: further discussed on **page 55 - 57**.

As Bitcoin continues to evolve, from an experimental disestablishment side project for cypherpunks to an openly accessible censorship-resistant Internet Money, it would continue to further pronounce its uniqueness over other cryptocurrencies (or *Altcoins* for short*)*. This would increase its utility value, as there is an evident use for it - that is, to be an actual *Internet Money* and *Gold 2.0* - effectively outgrowing the oft-touted depiction of being easy/scam money.

Bitcoin Returns

A cursory review of Bitcoin's superior returns Year-to-Date (YTD) over the past decade vis-a-vis other asset classes sheds some light on the asymmetric returns its been able to deliver to early adopters and those with the right risk appetite who bought in early despite its volatile swings.

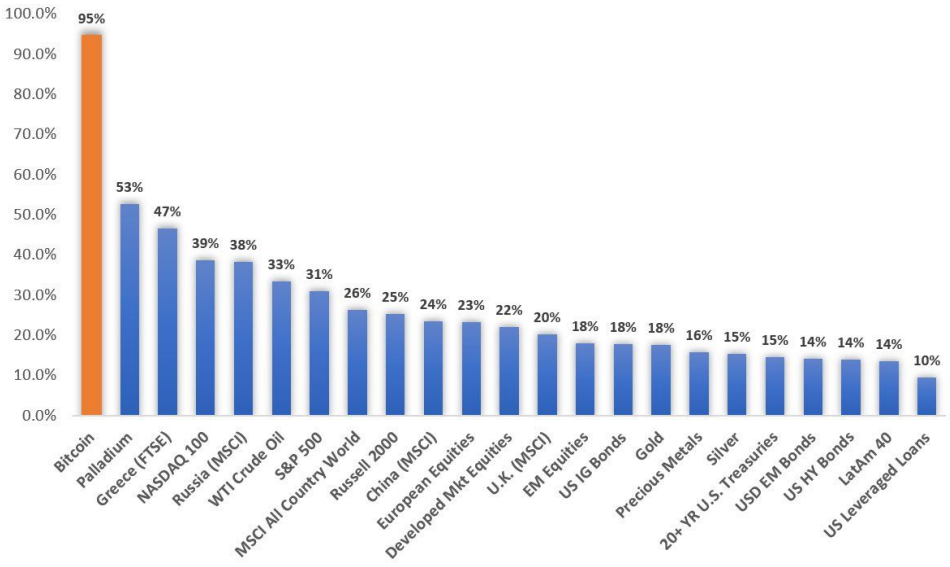

Diagram 3.4: YTD % change in notable asset classes in 2019
(Credit: Delphi Digital)

Despite falling from its all time record highs of ~$20,000 in December of 2017, Bitcoin was down roughly 83% YTD at the end of 2018 ($3,230 on Bitstamp in Dec 2019). The price however rallied to a year's high of ~$12,000 in July 2019 and closed the year with a 95% return YTD at a price of ~$7,200 in December of 2019. Gold paled in comparison to Bitcoin's 95% return, averaging an 18% return YTD for Gold holders.

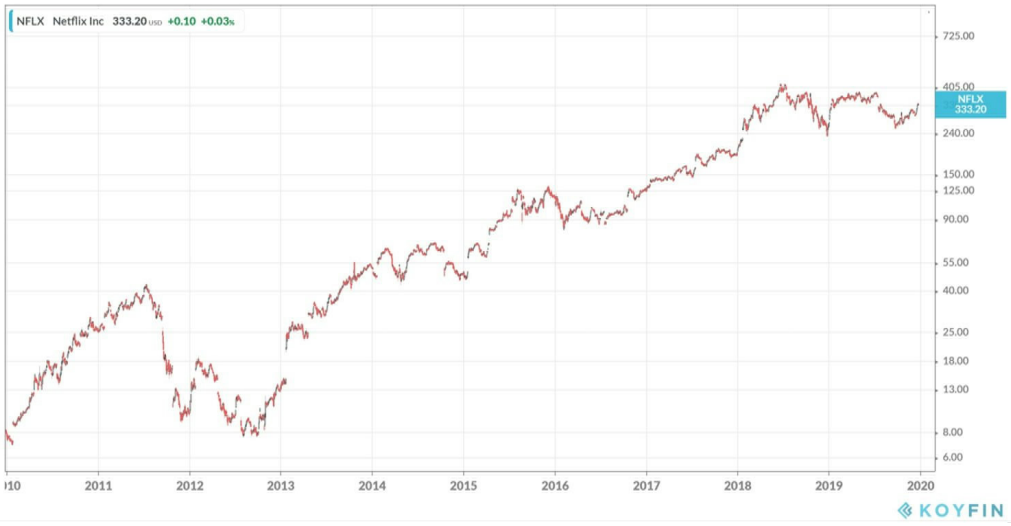

Diagram 3.5: Netflix 10 year return
(Credit: Koyfin)

Outside of the *cryptospehere*, the best performing asset of the last decade was one of the largest worldwide streaming platforms, Netflix stock ($NFLX), which returned more than 4,181%[54]. Netflix's stock price was less than $8 when 2010 began, and subsequently reached an all-time high in June of 2018 of over $420, and currently trades around $330 (as of Dec 2019). $1 invested in Netflix in 2010 would have been worth more than $41 in 2019.

Diagram 3.6: BTC/USD historic price chart
(Credit: tradingview)

Bitcoin has however confounded those investors who have consistently propagated the "Bitcoin is dead" narrative over the past decade, and much to their chagrin, Bitcoin has been the best performing asset of the last decade.

The first bitcoin to fiat exchange occurred on 12th October 2009 when 5,050 bitcoins were exchanged for $5.04 giving us an exchange rate of 1 bitcoin to $0.00099. The bitcoin price eventually hit $1.00 on February 9, 2011.

Bitcoin price in July 2010 was around $0.07 and is currently trading at ~$7,200 at the time of Jan 2020. $1 invested in Bitcoin back in July 2010 would be worth more than $90,000 today, representing gains of more than 9,000,000% return on investment in 10 years[55].

Bitcoin Portfolio Allocation

From an investor's perspective, we argue that Bitcoin could serve as a perfect safe haven during times of economic downturn or recession, and could be used to exit riskier assets like conventional stocks. However, Bitcoin is yet to reach the level of trust amongst investors to be considered a viable asset for hedging against economic downturn. After having been established as the best performing asset of the decade, Bitcoin is likely to garner the required level of investor sentiment to assert itself as a viable long term store of value.

For the meantime, a modest Bitcoin allocation of 3% or more in traditional investment portfolios can significantly decrease drawdown risk and increase overall returns. This is because Bitcoin maintains a

low correlation with most traditional asset classes, including Gold. The plot below demonstrates this by highlighting Bitcoin's correlation with the S&P 500 and Gold (SPDR):

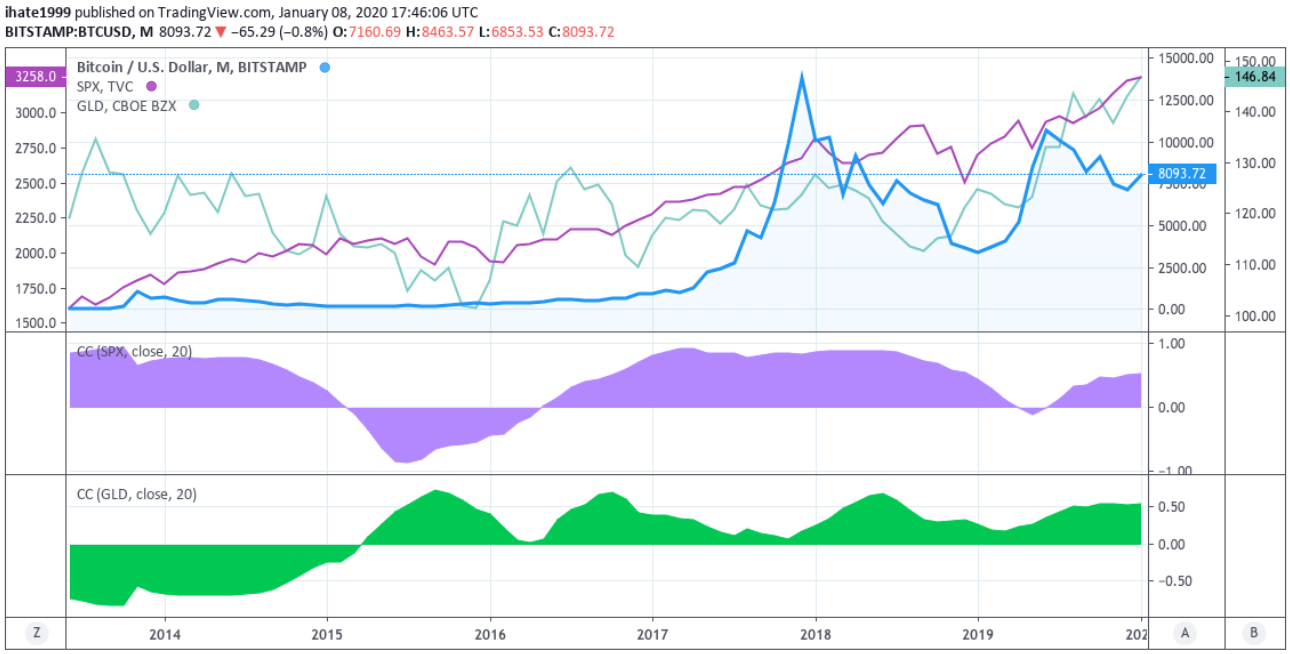

Diagram 3.7: BTC vs SPDR Gold Shares ETF and S&P 500 price correlation
(Credit: Tradingview)

The persistent lack of correlation between Gold and Bitcoin might seem counterintuitive, given that they are both quite similar in terms of their value proposition as a store of value and hedge against economic uncertainty. However, it may be a direct result of Bitcoin's perceived risk profile, as many investors still view Gold as the less riskier investment. Though Bitcoin was the best performing asset of the decade, increased education amongst investors, and its continued unrivaled performance, would certainly prompt the re-evaluation of its risk profile.

In analyzing the potential increase in overall returns that bitcoin introduces, we take the model 60-40 portfolio (60% stocks and 40% bonds) as a template, to compare with similar portfolios of varying Bitcoin allocations. Below is the breakdown of three portfolios with varying Bitcoin allocations, all with an initial investment of $1000:

Port	Vanguard Total World Stock ETF	Fidelity Total Bond Fund	GBTC
●	60%	40%	0%
●	59%	38%	3%
●	58%	37%	5%

Diagram 3.7: Simulated Portfolios Breakdown
(Credit: https://portfoliovisualizer.com)

To simulate the stock market allocation we have used the Vanguard Total World Stock ETF (VT), Fidelity Total Bond Fund (FTBFX) for bonds, and Greyscale's Bitcoin Trust (GBTC). We performed a backtest portfolio analyses using the 3 portfolios above, over a 4 year period as opposed to 5 years, because the GBTC data only goes as far back as Jun 2015.

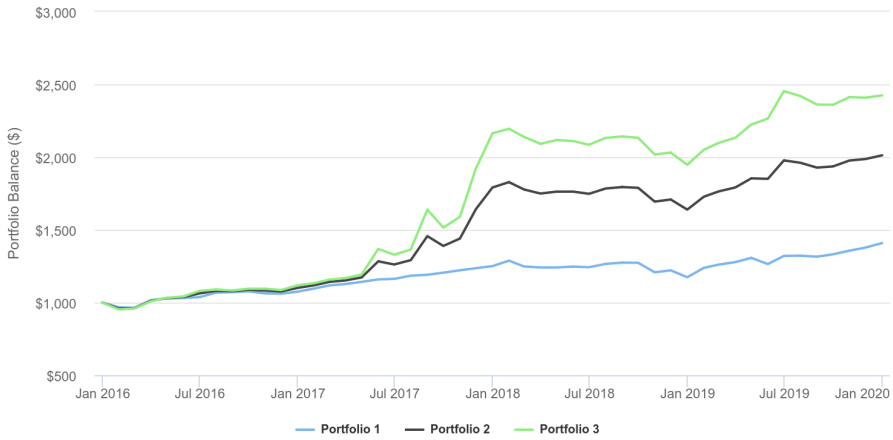

Diagram 3.8: 4 yr portfolio perfomance growth
(Credit: https://portfoliovisualizer.com)

As can be seen in plot above, each increase in Bitcoin allocation results an appropriate increase in the portfolio's overall performance. Despite the 2017 Bitcoin bull run, the market correction in the later parts of 2018 still maintained significant growth. With as little as 3% allocation, the portfolio growth experienced is unrivaled by the traditional portfolio, and further illustrates the potential gains introduced by Bitcoin exposure. Below is a breakdown of the 4 year performance of the 3 portfolios:

Port	CAGR	Std. Dev.	Best Year	Worst Year	Mx Drawdown	Sharp Ratio
●	6.69%	7.17%	20.04%	-6.13%	-8.86%	1.05
●	19.10%	13.46%	62.75%	-8.48%	-10.33%	1.27
●	24.79%	19.10%	93.61%	-10.02%	-11.28%	1.19

Diagram 3.9: 4 yr portfolio perfomance breakdown
(Credit: https://portfoliovisualizer.com)

It is evident that the portfolio with 3% Bitcoin allocation yields the best Sharpe Ratio (1.27) of the group. Portfolios with this level of Bitcoin exposure could also benefit from reduced volatility when other assets like stocks become riskier, as in the case of economic crises. Bitcoin, though a relatively volatile asset, significantly increases the overall performance of a portfolio, and therefore remains a valuable addition to any portfolio looking to increase overall returns and reduce volatility, especially in times of economic meltdown.

Bitcoin Investment Cycles

- The Hype Cycle Theory
- The Halving Theory
- Hashrate Theory
- The Rising Bottom Hypothesis
- Stock-to-Flow (S2F)

Generally, it is estimated that the potential market for Bitcoin is worth trillions of US Dollars, and the current total market cap for Bitcoin as of Dec 2019 is still below $500 billion (~$130 Billion).

There is still a lot of room for growth that would foster even larger value realization. Ergo, the time to invest is now, because the potential value of Bitcoin is still yet to be fully explored.

As a result, there is a growing abundance of competing theories for optimal periods to invest in Bitcoin, but the best thus far is aptly summed up below:

> "*Buy the dip*"

Meaning one should invest when the price of Bitcoin tanks. Though a tried and trusted strategy, the catch, however, is being able to tell when the bottom price will be reached before there is a price rebound. Unfortunately, the ability one needs to possess to make such calls are usually based on luck.

Traders generally share a few foundational ideologies about the future price trends of Bitcoin, for example:

- Its shapes are repeating *fractals*.
- It exhibits *Wyckoff Market Cycles*.
- Its value will generally increase over time.
- Its deflationary emission rate causes regular price increases, particularly acutely in response to halving events.

Below we present a few of the numerous theories and analyses around future Bitcoin prices and explanations of previous price action trends.

> ***Note**: We do not endorse these predictions, and merely aim to present the numerous views that are held within the different communities of traders.*

The Hype Cycle Theory

As Bitcoin's protocol continues to be upgraded and improved, adoption would rise, resulting in the growth of general optimism around bitcoin. This optimism is further catalyzed by media coverage, which most often than not propagates ill-informed implications of these new changes. This further increases the level of interest in Bitcoin, causing the price to inflate, which provides more educated individuals the opportunity to dump their bitcoins on victims of FOMO. The chart below illustrates the relationship between price and these hype periods, highlighted in blue.

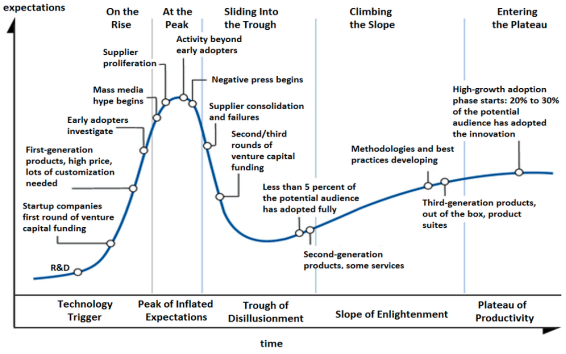

Diagram 4.0: "Hype Cycle" price chart, based upon Gartner's Hype Cycle (Credit: Wikimedia)

The Halving Theory

There is generally a firm belief amongst traders and other Bitcoin spectators that future price action is driven by the Bitcoin halving periods. These periods, which occur every ~4 years, exist to ensure Bitcoin doesn't go beyond the 21 million supply cap. This deflationary supply rate is intended to ensure the value is not dampened over time. This theory suggests that each halving period results in a corresponding increase in Bitcoin price. However, the theory seems to be a bit self-reinforcing: a belief that each halving results in a surge in Bitcoin prices, further driving up the speculation around its price at the start of each of these periods, thus, reinforcing the belief in subsequent periods. Additionally, miners also seem to hold on to bitcoins for longer periods after each halving, which may also contribute to the price action trend highlighted in the chart below:

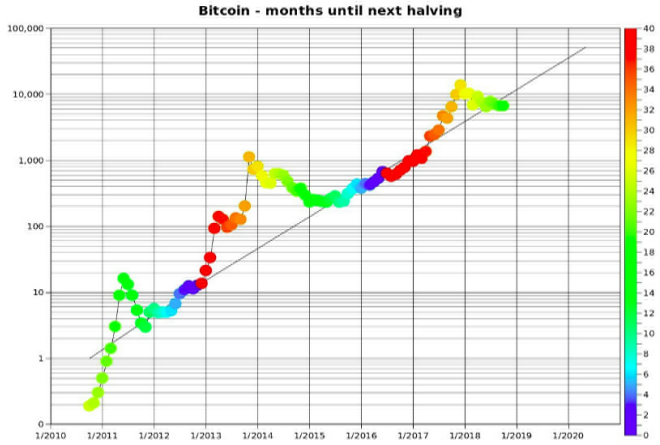

Diagram 4.1: Color-coded chart showing the distance between halvings relative to Bitcoin price.
(Credit: @100Trillion on Twitter)

The Hashrate Theory

It is commonly assumed that miners join a network when it is profitable to mine, however, there is reasonable evidence to suggest an inverse relationship between network hash rate and price. It seems as though miners mine in anticipation of future price, and not in pursuit of immediate bitcoin reward liquidation. Miners, especially in the case of Bitcoin, tend to be one of the major individuals that hold bitcoins for extended periods, in anticipation of cashing out in the future or when necessary, to pay rent and other expenses. The chart below further highlights this hash rate-to-price relationship:

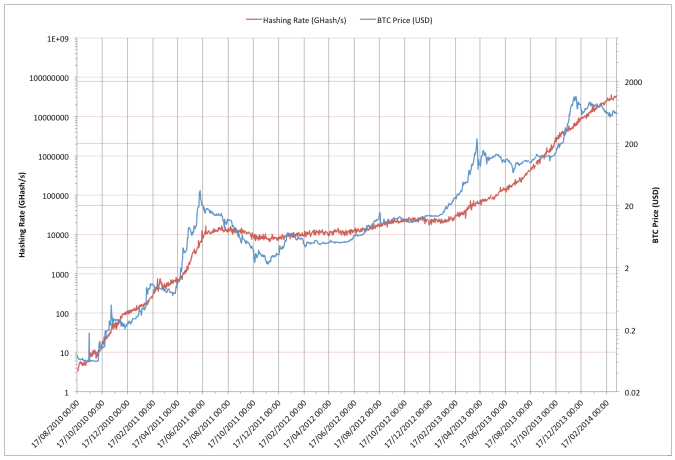

Diagram 4.2: Bitcoin price charted against hashrate, 2010 - 2014
(Credit: HashingIt.com)

The Rising Bottom Hypothesis

Entirely derived from analysis of the BTC/USD price chart, it asserts that with each new halving period, there exists a bull run that triggers a reset of the bottom price for that period that is at least an order of magnitude higher than the previous period's bottom. Effectively seeing the permanent vanishing of the previous period's bottom.

Diagram 4.4: BTC/USD price chart with bottoms and resetting bull runs highlighted.
(Credit: @ihate1999 on Twitter)

Stock-to-Flow (S2F)

Stock-to-Flow (S2F) is a ratio between the amount of an asset held in reserve (or mined i.e. supply) and the amount produced over a certain period such as a year, essentially its supply-rate. There is an inverse relationship between an asset's S2F ratio and its inflation rate, such that, higher levels indicate its scarcity. Assuming asset scarcity is directly correlated with its value, this ratio can be used to predict the future market value of the asset. According to the analysis provided by PlanB (@100trillionUSD on twitter), an early Dutch Bitcoin adopter, Bitcoin's stock S2F ratio can be used to predict its future value as is shown in the diagram below:

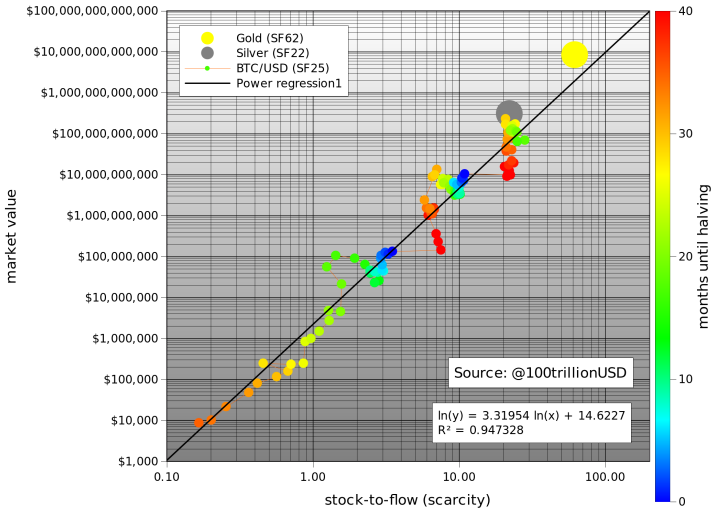

Diagram 4.4: Future Bitcoin price as a function of Stock-to-Flow
(Credit: @100Trillion on Twitter)

All these theories and analyses simply indicate the thirst traders have in exploiting the ever-increasing price of Bitcoin. Nevertheless, this trading helps distribute liquidity across the market.

Risks of Investing in Bitcoin

- Irreversible Transactions
- Hacking
- Scams
- Hard Forks
- Price Volatility
- Absent Client-side Infrastructure
- Scaling Solutions
- Regulation
- Competition
- PoW Energy Consumption
- Long Term Network Incentive Scheme
- Protocol-level Bugs and Security Holes
- Miner Centralization

It is no secret that investing in Bitcoin yields substantial returns, however, this portfolio spearheading asset does indeed come with its fair share of risks, that is why it is expected that investments be of negligible amounts, to reduce any financial loss. However, for those who seek to make even more substantial returns, knowledge of the risks that come with investing is of paramount importance.

We therefore explore these risks below:

Hacking

It is no surprise that hackers and individuals who possess the skills necessary to circumvent digital security measures would inevitably target Cryptocurrency exchanges and client-side wallet apps. Mainly because the amount of money processed by Cryptocurrency exchanges are of considerable amounts, with leading exchanges such as Binance reporting daily transaction volumes of ~ $1.53 Billion (as of Dec 2019), and other exchanges including BitMax reporting similar.

Hacking in this respect is performed on two fronts:

- Cryptocurrency Exchanges
- Client-side Wallets

Moreover, ever so often we do witness reports of exchanges being hacked, from the first widely publicized Mt. Gox hack, to the recent Bithumb hack in July 2017. It will likely not subside any time soon, as exchanges would continue to be targeted as Bitcoin adoption grows globally. These exchanges process large volumes of bitcoins, with some including web wallets for storing coins as part of their services, and are thus viewed by hackers as treasure chests. These hacks are usually the result of mediocre coin storage management systems, the use of vulnerable homegrown technology solutions for securing private keys, poorly designed web wallets, and other commonly exploitable security flaws.

As a result of the continued hacks to exchanges, users have been warned to seek offline or standalone wallets, instead of the web wallets hosted by these exchanges, to mitigate against being victims of hacks. Previously, these web wallets stored and generated a private key to be used for spending bitcoins, which were easily swiped by hackers, but have since understood the dangers of directly storing user private keys in-app.

Irreversible Transactions

By design, Bitcoin ensures transactions are irreversible, a foundational concept that acts as a safeguard against the double-spending of funds. Nevertheless, human error is inevitable, and in the unfortunate event that an individual makes a mistake during a transaction - sending more funds than necessary or sending funds to the wrong or inexistent address - there is no method of reversing the transaction, or performing a reverse entry as is common with banking services. The absence of an intermediary guarantor means fund recovery is impossible. Investors are expected to properly check all transactions before they are made, to avoid making any costly mistakes.

In response, wallet key management is now done through the generation of a random set of 12-24 words, known as the mnemonic (as part of the BIP39 spec), and the use of a user set passphrase. These two pieces of information are used to generate and control all current and future addresses in the wallet. The security advantage of this approach lies in its redundancy: both pieces of information

are required to compromise the wallet, as opposed to just the private key.

Unfortunately, hackers have realized that some common vulnerabilities still slip past Cryptocurrency wallet designers, and proceed to exploit these vulnerabilities to gain access to private keys (in the case of older wallets), mnemonics, and in some rare cases passphrases. To combat these sorts of hacks, some wallets require the user to set a passcode for the wallet app itself to avoid unauthorized access to the wallet.

If an investor is looking to secure their bitcoins, the most advised technique is to use a hardware wallet - a physical device that does not communicate with the Internet, to securely store your coins offline - or opt for industry-leading secure third-party custodian services, such as Xapo.

Scams

The most popular method of purchasing Bitcoin is through Cryptocurrency exchanges and Over-the-counter (OTC) services. Due to the growing interests in Cryptocurrencies and Bitcoin especially, numerous fraudulent exchanges continue to surface. These exchanges set up fake websites with misleading information, defrauding unsuspecting investors. Fraudulent OTC services also exist, where individuals are conned into sending their bitcoins to an address without the other party completing their end of the trade, and hence stealing their funds. Certain services and individuals on the Internet that claim huge guaranteed returns in exchange for some Bitcoin should also be avoided, as they are common attempts at defrauding and scamming unsuspecting investors.

At the moment, the only measure against this is research. These fraudulent services post misleading information that is easily spotted by the Cryptocurrency community, who then warn potential investors accordingly. Nevertheless, these exchanges are constantly being created and might sometimes temporarily go undetected, and in this situation, it is expected that potential investors do their research. Furthermore, in the absence of certainty, they should opt for reputable and widely used exchanges and OTC services, such as Coinbase, Gemini, Binance, etc.

Hard Forks

In the open-source world, disagreements regarding the current trajectory of the project are sometimes settled by hard forking the codebase. For a project like Bitcoin, the case is no different. Although, these hard forks are usually more contentious, as they end up creating more confusion and enmity amongst members of the communities, and could even risk the stability of the forked project - Bitcoin.

As a precautionary measure, the Bitcoin community upgrades the protocol through soft forks, a process with built-in backward compatibility that requires voluntary upgrade by users, to provide a less disruptive way of introducing, and adopting, protocol changes.

Price Volatility

In terms of global currency markets, Bitcoin is still a relatively small market, and hence susceptible to frequent wild price swings. This is universally understood as a feature of such markets, and with time, as the Bitcoin market matures, price volatility would stabilize. At the moment, the variance in its price has a lot to do with large volumes of exchange trading, integration into various experimental tech stacks, regulatory scrutiny, and other exogenous factors.

Admittedly, these price swings have precarious effects on short term returns on investments, in December of 2017 for example, the price of Bitcoin dropped from $18,936 on the 19th to $14,048 on the 23rd, a ~22% price decrease in just 4 days, clearly indicating the level of volatility in the market.

In light of the above, investors seeking substantial returns on their investments usually invest across a time horizon for upwards of 2 years, because volatility is not as vigorous in that time frame as is experienced within a year or less.

Absent Client-side Services

Despite all the progress being made with the underlying Bitcoin protocol, the absence of client-side tools, services, and apps would impede Bitcoin adoption. Without these, users would be unable to buy, sell, and spend their bitcoins, which could make nearly the entire protocol useless, as it would affect most of its use cases.

Fortunately, there are already numerous services, tools, and apps that are currently available to users and merchants. For merchants, services such as BitPay make the integration of Bitcoin as a payment option hassle-free, and on the user end, there are numerous wallets to choose from, all with their own different but related goal - spending, and receiving bitcoins. Users have the option to use privacy-focused wallets such as samourai and wasabi wallet, wallets such as Electrum that focus on flexibility for more technical users, and wallets that prioritize user experience such as DropBit.

The future looks bright for these tools and services, as more investments continue to flow into funding and developing even better tools and services for both users and merchants.

Scaling Solutions

Bitcoin currently has a limited rate of transactions that the network can process. Though intended as an additional security feature, the storage of the entire chain history by all nodes along with the block size limit and average block creation time reduces network throughput.

Various solutions have been proposed to address the scalability issue, of which the Lightning Network is among the few currently live. Others like Bulletproofs and confidential transactions are geared toward increasing Bitcoin's privacy by hiding transaction amounts - and making it available only to the participants of a transaction - are still yet to be integrated into the Bitcoin codebase. While other proposed solutions such as Merklized Abstract Syntax Trees (MAST) are yet to have a definite release date, Schnorr signatures and Taproot would likely be integrated sometime this year.

However, there is a whole class of other off-chain solutions being actively discussed called Sidechains, which include Drivechains, Mimblewimble, and RSK. Liquid, a sidechain developed by Blockstream, is already live and facilitates faster BTC transactions between businesses and individuals.

Additionally, there is a whole class of other off-chain solutions being actively discussed called Sidechains, which include Drivechains, Mimblewimble, and RSK. Liquid, a sidechain developed by Blockstream, is already live and facilitates faster BTC transactions between businesses and individuals.

Regulation

Since its inception, Bitcoin has presented problems for regulators who are unable to properly classify it under a specific asset class, due to its flexibility as an asset. Certain Governments have decided to implement strict regulations, while others are more open to it, such as in the case of the Japanese Government, where it is recognized as a legal tender. Bitcoin regulation is still by and large dependent on the region, and ranges from very strict regulation and outright bans - from fear of insufficient KYC/AML - to open acceptance.

The absence of Bitcoin regulation, or requiring payment of tax on the investment, has severe consequences for Governments. Bitcoin if left untaxed could potentially compete with the Government's currency. In countries where a majority of Bitcoin trading occurs, such as China, banning Bitcoin trading would result in a noticeable short term price crash, as was seen in mid-2017, which can erase a reasonable amount of gains on capital invested in the short term. Notwithstanding, the price did eventually rebound, and reached its all-time high of ~$20,000 in December of 2017.

Fortunately, as Bitcoin adoption grows, the market becomes more fragmented, causing situations where a single country holds more than 50% of the traded volume to be increasingly less likely. At that point, Bitcoin's price would not be as dented in the event of being subjected to bans in certain countries.

Competition

So far, Bitcoin in its current form continues to deliver on its thesis of being a superior store of value, however, investors could shift to other Cryptocurrencies, or revert to fiat, in the future, if they feel it no longer meets this thesis or is no longer a compelling investment.

This situation seems increasingly less likely, as Bitcoin continues to outperform all its competitors, in network security, native asset price performance, and possesses several other unique attributes. Numerous changes yet to be integrated would also further distinguish it from all the competing Cryptocurrencies.

PoW Energy Consumption

PoW is a necessary component of Bitcoin’s security model and has so far managed to secure the Bitcoin network against several hacks since its inception. Initially, single miners contributed their CPU power to secure the network, however, as time progressed, CPU mining became unprofitable as the computational requirement of PoW grew almost exponentially. At the moment, individuals seeking to make a profit through mining Bitcoin contribute their computational resources to a mining pool, a collection of miners, to secure the network.

This aggregation of computational expenditure is not without a cost, as the amount of electricity required to sustain it is enough to power an entire country. As such, there are growing concerns about its long term environmental effects. Miners looking to increase their profit margins must now seek out cheaper renewable sources of electricity, as the costs of non-renewable powered electricity grows. Which has the positive effect of shifting Bitcoin toward even more greener sources of energy, and thus alleviating the environmental concerns.

Long Term Network Incentive Structure

Currently, the Bitcoin network provides miners with two incentives: the coinbase reward and transaction fees. This coinbase reward is currently at 12.5 BTC and would soon become 6.25 BTC after the halving, sometime in May. The transaction fees, on the other hand, are currently less than $0.50 (as of Jan 2020).

The block reward would eventually diminish to 0, sometime in 2140, and at that point, the only incentive for miners would be the transaction fees. This means, in the future, the transaction fee market needs to be able to sustain the network by providing the necessary economic incentive for miners. On that point, another more suitable solution might be introduced in the future, to plug-in this incentive deficit, before the 2140 deadline.

Protocol-level Bugs and Security Holes

All software, no matter the purpose, is invariably vulnerable to software bugs, and in the case of Bitcoin, this could be a minor bug that has little to no effect on the overall network or one that could open up extremely detrimental attack vectors.

Several protocol-level bugs have been discovered over the years, among them were the infelicitous CVE 2018-17144 bug in 2018, which introduced the possibility of inflating Bitcoin's supply through the elaborate use of a kind of double input, and the value overflow incident in 2010, where an edge case in the code responsible for checking transaction outputs was exploited and resulted in the creation of over 180 million bitcoins in a single transaction.

In each instance, the vulnerability is quickly patched by the dedicated team of Bitcoin developers and contributors. This is only possible because of the level of transparency that open-source development offers, as the code base is constantly being peer-reviewed by numerous contributors around the world, making vulnerability detection and reporting prompt.

Miner Centralization

One of Bitcoin's primary value propositions is its censorship resistance. To achieve this, the bitcoin network requires nodes to be decentralized to avoid the risk of having centralized points of censorship or failure. A special group of nodes, known as miners, are tasked with securing the network by expending their computational energy in creating new blocks. In the process, these miners are rewarded for their hard work by receiving newly created bitcoins. For a miner, reducing the cost of electricity translates to increased profit from mining.

In the last few years, there has been a large growth in Bitcoin mining in China, which is because of the cheap electricity cost offered by coal and other non-renewable sources, VIP access to latest mining technology, and closeness to dominant manufacturers like Bitmain. This trend has brought significant concern, as the increased concentration of miners in a single geographic location - china - could result in increased centralization, or worse, lead to a 51% attack. In this scenario, miners in the region could exclude certain transactions from inclusion in newer blocks.

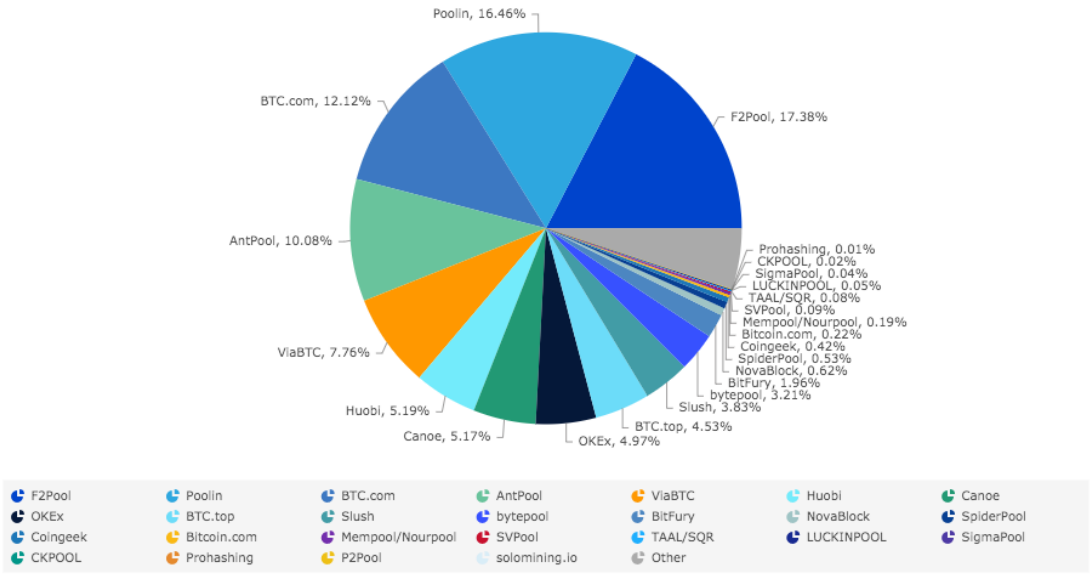

Diagram 5.0: Total Bitcoin Hashrate by Mining Pool (last 7 days, Jan 10 2020)
(Credit: coin.dance)

Compounding to this issue is the fact that Bitmain, the largest manufacture of ASICs (specialized mining equipment), is also a Chinese company, which directly controls AntPool and has an influence over other pools like BTC.com, ViaBTC, and potentially more, giving them a combined dominance of ~40% of the mining hash rate in 2018. This level of influence could also result in collusive attempts to censor transactions.

However, as of Dec 2019, CoinShares Research reports that Bitmain's market share dropped from ~70% to 66%, allowing for its competitors to establish themselves, thereby diluting Bitmain's monopoly, and thus furthering decentralization efforts. As for the concentration of miners in China, the concentration did experience a drastic decline in 2019, but soon rebounded following the announcement by Chinese president Xi on China's intentions to "seize the opportunity" afforded by blockchain technology, as it was assumed to be a sort of lift on the ban on Bitcoin mining. Fortunately, numerous factors would continue to limit this concentration in miners, such as cheaper electricity costs that would drive them out to other locations, or bans on mining by the Chinese government.

Though the Bitcoin network remains at constant risk of a 51% attack, it has only occurred on other smaller - in terms of hashrate - PoW based networks and not Bitcoin. The economic incentive provided by the coinbase reward and fees are there by design to dissuade miners from colluding and tacking down, or gaming the network, and from a game theoretical perspective, it is rather irrational and counterproductive for miners to collude and negatively affect or take down the network. The Bitcoin protocol was designed with safeguards against 51% attacks, and was even explicitly mentioned in the white paper that honest nodes would reject the invalid blocks created by the attackers, meaning, the valid chain can always be maintained. It is also worth noting that PoW incrementally increases the difficulty level of carrying out this attack, as the computational requirement is increased with every new block created. This makes the attack less profitable and thus meaningless, as the effort required is not worth it.

Future of Bitcoin

Unfortunately, Bitcoin is yet to be fully adopted by those who would benefit from its value proposition as a global open, decentralized, and censorship-resistant money. These are individuals who are suffering from plummeting currency prices of their home country's native currency (as in the case of Venezuela), and are unable to preserve their wealth, or make ends meet; unbanked individuals in developing countries; and journalists/individuals who are under immense Government pressure and oppression.

Regardless, efforts are underway to help with the onboarding of these individuals. In recent times we have seen a global increase in mobile adoption in Africa, which is providing those without formal financial accounts the ability to engage in day-to-day commercial activities, with the help of bitcoin, through the use of technologies such as BitPesa [56]. The existing shift from traditional bank accounts to mobile money accounts lays the foundation for future Bitcoin adoption as an electronic supplement to their mobile money.

We have also seen an evident increase in the use of bitcoin as a means for global remittance. Though it still makes up a small amount of the currencies used today, trends in adoption still show its increasing use in the global remittance market.

At the moment, Bitcoin cannot handle the kind of transaction capacity required for micropayments amongst individuals and merchants. In an attempt to seek out a viable solution, the Bitcoin community suggested implementing an ad hoc parallel network for processing micropayments off-chain. This proposal, first formally proposed in a paper by Poon and Dryja (2016), was dubbed the *Lightning Network*.[57]

Within just three years this network has already been implemented by Lightning Labs[58],Blockstream and others, and is currently functional for bitcoin micropayments. The network allows individuals to send transactions through bi-directional or uni-directional payment channels.

Additionally, it has the potential capacity to handle an arbitrary amount of transactions per second with negligible fees. After having completed transacting, individuals can proceed to close the channel and broadcast their transaction history to the Bitcoin network, where all their transactions would be settled. The network provides the necessary infrastructure for global retail payments, micropayments, and Machine-to-Machine payments.

Currently, there are still technical difficulties facing the current implementation, which include concerns around the routing algorithms used in the network and the absence of *SIGHASH_NOINPUT*. However, this is just a feature of early implementations and is something that would be fixed with time. At the moment, the Lightning Network allows for different routing algorithms to be used in unison, depending on the needs of the implementor. The inclusion of an additional operation code for signing scripts instead of transaction IDs is also being heavily discussed, as this addition would allow lightning payment channels to shift away from punitive to correct based ones. As such, these channels would work based on their correctness, and not when adversarial punishment conditions are met. The continued functionality of the channel is ensured by the correctness of its construction, rather than the punishment of misuse by adversaries.

Also, the global adoption of Bitcoin seems to be increasing at a rapid pace. Technological advancements in the network that weren't present a few years back, such as the Lightning Network, are already useable today, and therefore serves as an indication of the growing importance of making it more feasible for mass adoption. Subsequent additions such as Schnorr signatures, CTs, MuSigs,

DANDELION, and SNICKER would see a large increase in Bitcoin's privacy and transaction anonymity, and would effectively certify Bitcoin as the ideal "*Internet Money*".

The evolution of these advancements and their respect domains is aptly depicted in the diagram below:

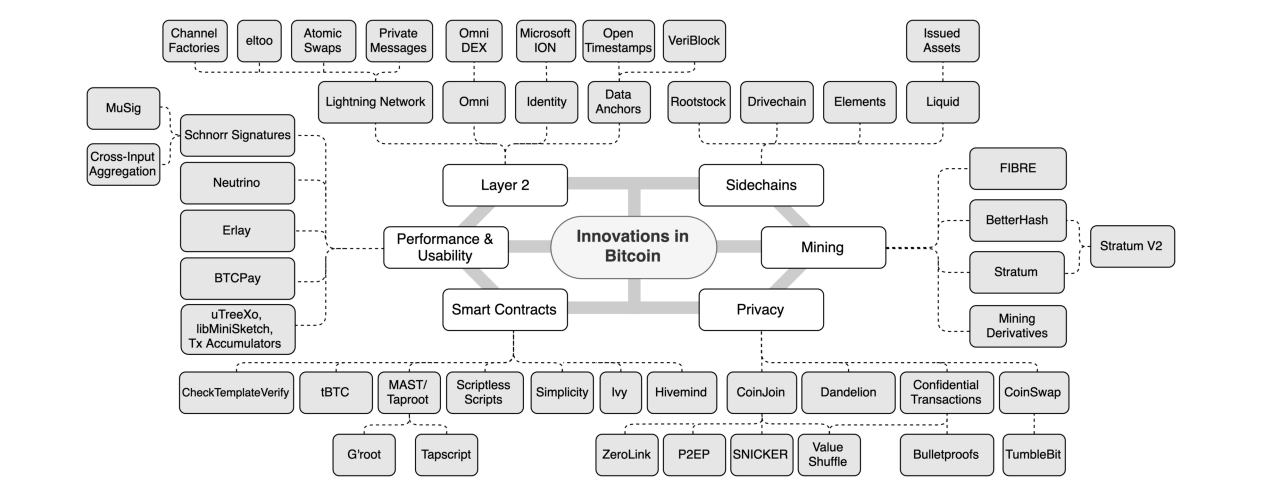

Diagram 5.0: Map of Bitcoin advancements
(Credit: "A Look at Innovation in Bitcoin's Technology Stack", by digitalassetresearch on medium.com)

The constant crackdown on Darknet markets such as the Silk Road in 2013 (which accounted for 99% of all Darknet market activity at the time[59]), provides a unique opportunity for the introduction of a set of new Bitcoin users, as individuals and Darknet market vendors who owned Bitcoins would likely offload their holdings on these new users, swapping Bitcoin's association with illegal activity for less neferious use. This phenomenon has resulted in the decline of Bitcoin transactions sent to Darknet markets from 30% in 2012, to less than 1% in 2017[60]. Other factors driving the change include the increasing use of alternative Cryptocurrencies, such as ZCash and Monero in these Darknet markets, and the discovery of alternative uses for Bitcoin, such as a financial asset or store of value.

We are therefore highly optimistic about the future of Bitcoin as an asset, whether it ends up being Gold 2.0/Digital Gold or a means of exchange, and can ultimately foresee its eventual adoption as the global reserve currency. We also believe it to be very likely that Bitcoin establishes itself as the financial (or money) layer that would sit atop the application layer of the Internet protocol suite, thereby allowing it to facilitate the transfer of micropayments and even substantially large amounts of money over the Internet, such as the $1 billion transaction that was processed in 2019. The transaction is largest ever performed on the Bitcoin network and is a positive indication of the level of trust people continue to place in it.

To quote Ray Dillinger:

> *"I believe that blockchain technology, once the current state of confusion is over, will contribute vastly more to the world than all the scams put together have taken or destroyed."*[61]

We, therefore, feel very humbled to be alive and able to contribute to the growth of what is likely to be: *The next natural and logical progression in our monetary evolution.*

xx. References

[i] Richard A. Werner, "How do banks create money, and why can other firms not do the same? An explanation for the coexistence of lending and deposit-taking". Available at: https://www.sciencedirect.com/science/article/pii/S1057521914001434

[ii] Lansky, Jan (January 2018), "Possible State Approaches to Cryptocurrencies". Available at: http://si-journal.org/index.php/JSI/article/viewFile/335/325 Journal of Systems Integration. 9/1: 19–31. doi:10.20470/jsi.v9i1.335.

[1] https://mises.org/library/losing-battle-fix-gold-35

[2] https://wikipedia.org/wiki/Nixon_shock/

[3] https://wikipedia.org/wiki/Fiat_Money see also for all fiat currencies https://whatcurrency.net/world-fiat-money-list

[4] https://medium.com/zulurepublic/defending-privacy-an-interview-with-andy-yen-of-protonmail-38e7f12b1c71

[5] Eric Hughes, "A Cypherpunk's Manifesto" (1993). Available at: https://www.activism.net/cypherpunk/manifesto.html

[6] Pg 22. Jerry Brito, February 2019. Coin Center report. "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society". Available at: https://coincenter.org/entry/the_case_for_electronic_cash

[7] https://investinblockchain.com/us-congress-combat-crypto-price-manipulation see also: https://cnn.com/us-regulators-working-together-combat-crypto-fraud-says-cftcs-giancarlo and: https://thebitcoinnews.com/us-house-passes-bill-for-task-force-to-combat-crypto-use-by-terrorists

[8] https://arstechnica.com/tech-policy/2016/08/stealing-bitcoins-with-badges-how-silk-roads-dirty-cops-got-caught

[9] Alex Biryukov et al, "Deanonymisation of clients in Bitcoin P2P network". Available at: https://arxiv.org/abs/1405.7418

[10] https://crystalblockchain.com

[11] https://elliptic.co

[12] Pg. 25, Fergal Reid and Martin Harrigan. "An Analysis of Anonymity in the Bitcoin System". Available at: https://arxiv.org/abs/1107.4524

[13] https://nakamotoinstitute.org/literature/b-money

[14] https://hashcash.org

[15] https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki

[16] https://wikipedia.org/wiki/Byzantine_fault

[17] https://wikipedia.org/wiki/Dot-com_bubble

[18] https://twitter.com/tuurdemeester/status/938243958781763584

[19] https://cnbc.com/2017/12/17/worlds-largest-futures-exchange-set-to-launch-bitcoin-futures/-sunday-nighthtml

[20] https://bakkt.com

[21] https://erisx.com

[22] https://buffet.cnbc.com/video/2018/05/05/warren-buffet-on-cryptocurrencies-to-me-its-just-diementiahtml

[23] https://comptia.org/resources/it-industry-trends-analysis

[24] https://dailyhodl.com/2018/08/26/bitcoin-btc-transaction-value-passes-paypal-at-1-3-trillion

[25] Ibid

[26] https://darkreading.com/vulnerabilities—threats/cybercrime-economy-generates-$15-trillion-a-year/d/d-id/1331613

[27] https://bitsonline.com/ethereum-vitalik-death-hoax

[28] https://tokenmeister.com/blog/blockchain/the-dao-hack-the-story-of-the-strangest-digital-attack/

[29] https://helpnetsecurity.com/2008/07/25/security-flaws-in-online-banking-sites

[30] https://youtube.com/watch?v=9pyVvq-vrrM

[31] https://theblockcrypto.com/2018/11/01/morgan-stanley-releases-a-report-looking-at-the-current-state-of-cryptocurrencies

[32] https://bitcoinmagazine.com/articles/who-funds-bitcoin-core-development-how-the-industry-supports-bitcoin-s-reference-client-1459967859

[33] https://coindesk.com/50-blocks-segwit-bitcoins-coming-upgrade-blockchain-game-changer

[34] http://en.wikipedia.org/wiki/Halting_problem

[35] https://coindesk.com/understanding-dao-hack-journalists

[36] https://cointelegraph.com/news/analyst-suspicious-bitcoin-mempool-activity-transaction-fees-spike-to-16
see also: https://www.reddit.com/r/Bitcoin/comments/6rgz6l/someone_is_spamming_the_mempool_with_extremely

[37] https://bankofamerica.com/foreign-exchange/wire-transfergo

[38] https://coindesk.com/microscope-real-costs-dollar

[39] https://wikipedia.com/wiki/Energy_usage_of_the_United_States_military

[40] Ibid

[41] Ibid

[42] https://oilprice.com/Energy/Energy-General/A-Look-At-US-Military-Energy-Consumption

[43] https://www.quora.com/How-many-banks-are-there-in-the-world-1

[44] https://www.linkedin.com/pulse/how-many-banks-globally-david-gyori/

[45] https://hackernoon.com/the-bitcoin-vs-visa-electricity-consumption-fallacy-8cf194987a50

[46] https://archive.org/download/bitcoinenergyconsumptionindexdigiconomist/Screen%20Shot.png
Full Archive: https://archive.org/details/bitcoinenergyconsumptionindexdigiconomist

[47] https://ren21.net/wp-content/uploads/2018/06/17-8652_GSR2018_FullReport_web_final_.pdf

[48] Ibid

[49] https://researchgate.net/publication/327992077_Reform_and_renewables_in_China_The_architecture_of_Yunnan's_hydropower_dominated_electricity_market

[50] https://physicsforums.com/threads/power-consumed-during-battery-charging.570315/

[51] https://blog.schneider-electric.com/energy-management-energy-efficiency/2013/03/25/how-big-are-power-line-losses/

[52] https://wikipedia.org/wiki/Antifragile

[53] https://bitcointalk.org/index.php?topic=279249.0

[54] https://cnbc.com/2019/12/23/netflix-was-the-top-stock-of-the-decade-delivering-over-4000percent-return.html

[55] https://bloomberg.com/news/articles/2019-12-31/bitcoin-s-9-000-000-rise-this-decade-leaves-the-skeptics-aghast

[56] https://cointelegraph.com/news/kenya-adopts-bitcoin-with-bitpesa-tagpesa-and-m-pesa

[57] https://lightning.network/lightning-network-paper.pdf

[58] https://lightning.labs

[59] https://blog.chainalysis.com/reports/report-the-changing-nature-of-cryptocrime

[60] Ibid

[61] https://linkedin.com/pulse/id-known-what-we-were-starting-ray-dillinger

Appendix

i. Timeline of The Bitcoin Network

Time	Description
1990	**Linked timestamping proposed** by Haber and Stornetta.
1992	Intel Chief Scientist Tim May publishes the **Crypto-Anarchist Manifesto**.
1992	**Cypherpunks Mailing List starts**, attracting people like Julian Assange and Satoshi Nakamoto.
1993	**Cypherpunks Manifesto** published.
1996	"***Declaration of Independence of Cyberspace***" published by John Perry Barlow.
1996	**The open source movement** emerges as a marketing campaign for free software use in business.
1997	Eric Raymond presents "***Cathedral versus Bazaar***", an ode to open source development.
1997	Adam Back invents **Hashcash**, a denial of service protection mechanism for P2P networks
1998	Wei Dai publishes **B-money** proposal.
1999	**Freenet launches**, a censor-resistant document store and networking suite.
2005	Nick Szabo suggests a "***distributed title registry***" or ledger as a common resource.
2008	Satoshi Nakamoto publishes the **Bitcoin Whitepaper**.
2009	**Bicoin Genesis Block** is mined.
2009	**Bitcoin first transaction** between Satoshi and Hal Finney (in **block 170**).
2010	First real world Bitcoin transaction: **10, 000 BTC** spent on **two (2) pizzas**.
2010	Bitcoin exchange **MtGox** launched.

Adapted from **99bitcoins.com**

ii. Additional Reading Sources

[1] https://bitcoin.org

[2] https://nakamotoinstitute.org

[3] https://bitcoin.page

[4] https://medium.com see also: https://hackernoon.com

[5] https://coindesk.com

[6] https://theblockcrypto.com

[7] https://blockonomi.com

[8] https://bitcoinmagazine.com

[9] https://cointelegraph.com

[10] https://truthcoin.info

[11] https://www.reddit.com/r/Bitcoin

[12] https://bitcointalk.org

[13] https://bitcoin.stackexchange.com

[14] https://bitcoin.it/wiki