Blockchain

There's been a lot of buzz lately surrounding cryptocurrencies, and for good reason. Blockchain technology, the tech which powers Bitcoin, has the potential to disrupt major industries. However, the technology is fairly intricate, which can make it difficult for an investor to understand exactly why Bitcoin and other cryptocurrencies are useful, and where their value comes from. Drawing on expertise in computer science, economics, and markets from across Bespoke's team we have created this *Bespoke Brief* to help you understand how Bitcoin works and what blockchain technologies offer.

Bitcoin's Origin: A Brief History

Here's the quick backstory: in October of 2008, a mysterious writer using the pseudonym "Satoshi Nakamoto" wrote a paper (link) in which he outlined a peer to peer digital cash system. The paper was circulated on a mailing list for cryptographers, and people took notice. In January of 2009 the very first block on the bitcoin blockchain was mined (more on what this means later), and later that year, open source software was released. On December 12, 2010, Nakamoto made his final communication, and has not spoken out since. While his identity and living status remain unknown, he is estimated to have a fortune of roughly 1,000,000 Bitcoin (worth over 4 billion USD at today's prices). Despite Nakamoto's disappearance, the Bitcoin software, now known as Bitcoin Core, was fervently maintained by a small community of developers. The software is the cornerstone of the bitcoin network, and enables transactions to take place between users without the need for a central authority.

Bitcoin: An Overview

Financial systems are able to work because we trust the parties we transact with (or use intermediaries who we trust). We put our faith in these central authorities, and for the most part, it works. However, these trusted parties are not infallible. They can be hacked, they are vulnerable to corruption, and they often do not operate transparently. Bitcoin solves these issues by implementing the principle of "distributed trustless consensus" using *proof-of-work.* To understand why Bitcoin does not share the flaws of a single trusted authority, one must first understand *distributed trustless consensus*. As suggested by the name, there are three components that make up this principle:

1. Consensus

The idea of consensus is not too hard to understand. When you type "define consensus" into Google, you get this very short and sweet definition: "General agreement." But what does consensus mean in the context of money, and what does it mean in the context of Bitcoin? The easiest way to understand this concept is to think about what most of us use to transact with every day, the U.S. Dollar. Similar to Bitcoin, the Dollar has no intrinsic value, but we give it value because there is an agreement that it's an acceptable token of money. All parties who choose to accept this as a form of payment for goods and services have agreed to a similar set of principles around what a valid token of money is. The following is a very simplistic description of the consensus around money from a great article (link) explaining:

"I will accept some token or process in payment for valuable goods or services if:

- it comes from a scarce supply using one of the accepted means of value exchange and creation.
- I expect that everyone else will accept this token as money of comparable value.

I, additionally, believe that

- everyone else adheres to (1), (2) and (3)"

In the context of Bitcoin, consensus means that each "node"—a server running bitcoin software—agrees on what the rules are for a valid transaction, a valid block (a group of transactions that get written to the ledger), and what series of blocks constitutes the current valid blockchain (the entire ledger).

2. Distributed

How can we ensure consistent information across all nodes? In a traditional digital money system, when someone withdraws or deposits money into their account, the transaction information is sent to a central server, which consults a database to ensure that a user is not overdrawing their account. The server then makes the appropriate adjustments to the account, and that server remains the defacto authority of account balance for all participants in the system. When a transaction is sent to a bitcoin node, it must be propagated across the entire network. If we waited for full propagation across nodes before confirming transactions result would be a slow network. Instead, Bitcoin relies on the idea of "eventual consistency" which means that eventually, all nodes will have the latest information. Some academics even argue that if the last N (typically 6) blocks on the blockchain are ignored, Bitcoin has *strong consistency* (which is better than eventual consistency). While waiting for 6 additional blocks to be mined before confirming a transaction takes more time, it ensures that the transaction is not vulnerable to being rewritten by a competing chain (or at the very least, has a vanishingly small probability of being rewritten, increasing its integrity).

Why might there be a competing chain, and what does that even mean? Miners are competing with each other to add new blocks onto the blockchain, and thus claim the reward. Every once in awhile, two miners may arrive at a solution to a block within seconds of each other, which "forks" (not to be confused with a hard fork) the chain and starts a race to see which branch of the fork will be the longest. Eventually, the branches will diverge and the longest branch will emerge as the winner (remember, the nodes consider only the longest chain to be valid, so there is no incentive to mine on a shorter branch). All of the blocks mined on the winning branch are added to the chain, while the blocks on the losing branch are ignored. There is incentive for a miner to mine on their own branch if they believe they can "win" the race because, if their block is included in the chain, they get the block reward. Although these race conditions occur fairly infrequently, they occur often enough that it is common practice to ignore the last 6 blocks in the chain, as it greatly reduces the risk of confirming a transaction which is later is rewritten.

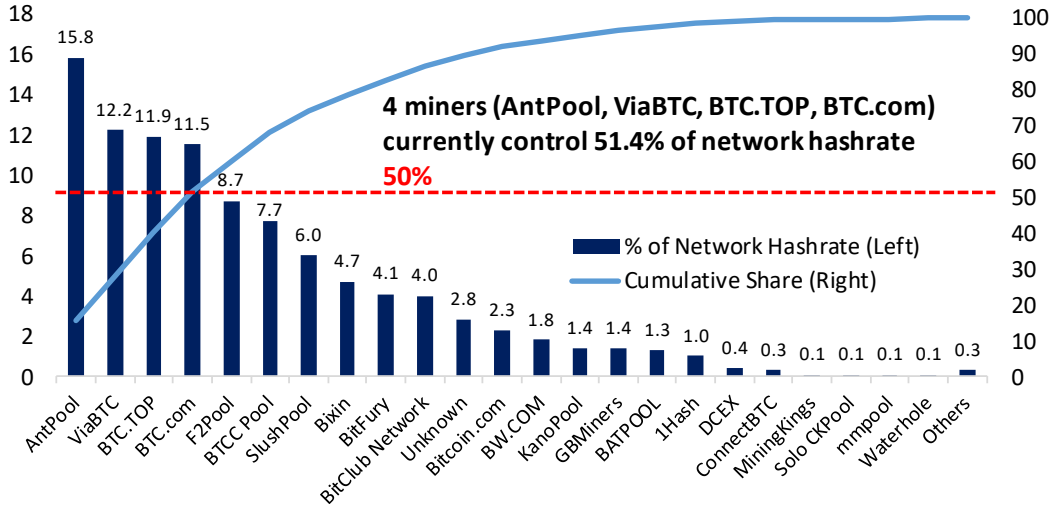
This possibility of "rewriting" the blockchain also means that malicious miners who have greater than 51% of the combined network hash rate could execute a "double spend" attack, where they spend bitcoin on one "branch" while secretly mining another branch in which the coins are not spent. They then broadcast this secret branch, only after the transactions on the public branch are confirmed. If the secret branch is longer than the public one at the time of broadcast, it will become the new valid blockchain, and all transactions occurring prior to the block at which the secret branch forked away from the original will be invalidated. However, there are several reasons why this attack is not really considered a threat to the blockchain ecosystem. (*con't on page 3*)

1. No single entity has enough hashing power to execute this attack. (Although the PRC might be a good candidate. Almost all of the top mining pools are based in China.) Below are pictures of the hashrate distribution among the top Bitcoin mining pools, as well as a table of the success probability of a double spend attack based on confirmations and hashrate share of the hacker:

Probability of Double Spend As Function of Confirmations/Hashrate

Hacker's Hashrate Share of Total Network (q)	Number of Confirmations 1	2	3	4	5	6	7	8	9	10
2%	4.000%	0.237%	0.016%	0.001%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
4%	8.000%	0.934%	0.120%	0.016%	0.002%	0.000%	0.000%	0.000%	0.000%	0.000%
6%	12.000%	2.074%	0.394%	0.078%	0.016%	0.003%	0.001%	0.000%	0.000%	0.000%
8%	16.000%	3.635%	0.905%	0.235%	0.063%	0.017%	0.005%	0.001%	0.000%	0.000%
10%	20.000%	5.600%	1.712%	0.546%	0.178%	0.059%	0.020%	0.007%	0.002%	0.001%
12%	24.000%	7.949%	2.864%	1.074%	0.412%	0.161%	0.063%	0.025%	0.010%	0.004%
14%	28.000%	10.662%	4.400%	1.887%	0.828%	0.369%	0.166%	0.075%	0.034%	0.016%
16%	32.000%	13.722%	6.352%	3.050%	1.497%	0.745%	0.375%	0.190%	0.097%	0.050%
18%	36.000%	17.107%	8.741%	4.626%	2.499%	1.369%	0.758%	0.423%	0.237%	0.134%
20%	40.000%	20.800%	11.584%	6.669%	3.916%	2.331%	1.401%	0.848%	0.516%	0.316%
22%	44.000%	24.781%	14.887%	9.227%	5.828%	3.729%	2.407%	1.565%	1.023%	0.672%
24%	48.000%	29.030%	18.650%	12.339%	8.310%	5.664%	3.895%	2.696%	1.876%	1.311%
26%	52.000%	33.530%	22.868%	16.031%	11.427%	8.238%	5.988%	4.380%	3.220%	2.377%
28%	56.000%	38.259%	27.530%	20.319%	15.232%	11.539%	8.810%	6.766%	5.221%	4.044%
30%	60.000%	43.200%	32.616%	25.207%	19.762%	15.645%	12.475%	10.003%	8.055%	6.511%
32%	64.000%	48.333%	38.105%	30.687%	25.037%	20.611%	17.080%	14.226%	11.897%	9.983%
34%	68.000%	53.638%	43.970%	36.738%	31.058%	26.470%	22.695%	19.548%	16.900%	14.655%
36%	72.000%	59.098%	50.179%	43.330%	37.807%	33.226%	29.356%	26.044%	23.182%	20.692%
38%	76.000%	64.691%	56.698%	50.421%	45.245%	40.854%	37.062%	33.743%	30.811%	28.201%
40%	80.000%	70.400%	63.488%	57.958%	53.314%	49.300%	45.769%	42.621%	39.787%	37.218%
42%	84.000%	76.205%	70.508%	65.882%	61.938%	58.480%	55.390%	52.595%	50.042%	47.692%
44%	88.000%	82.086%	77.715%	74.125%	71.028%	68.282%	65.801%	63.530%	61.431%	59.478%
46%	92.000%	88.026%	85.064%	82.612%	80.480%	78.573%	76.836%	75.234%	73.742%	72.342%
48%	96.000%	94.003%	92.508%	91.264%	90.177%	89.201%	88.307%	87.478%	86.703%	85.972%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Bitcoin Miner Pool Share of Network Hashrate



2. Miners and mining pools are long Bitcoin by default, and have an incentive to keep the Bitcoin ecosystem stable.

If the top mining pools colluded to pull off this attack, it would be extremely obvious to Bitcoin users, and the ecosystem would collapse. This would severely impact the value of Bitcoin, possibly rendering it worthless depending on the severity of the attack. As a result, miners and mining pools would lose out on tons of potential revenue had they operated honestly instead. Even though double spending is still possible without having over 50% of the network hashrate, the low success rate makes it economically unfeasible, as it would be more profitable to operate honestly and collect the block reward immediately than to "hoard" blocks (create a secret branch) for a very low chance of executing a double spend.

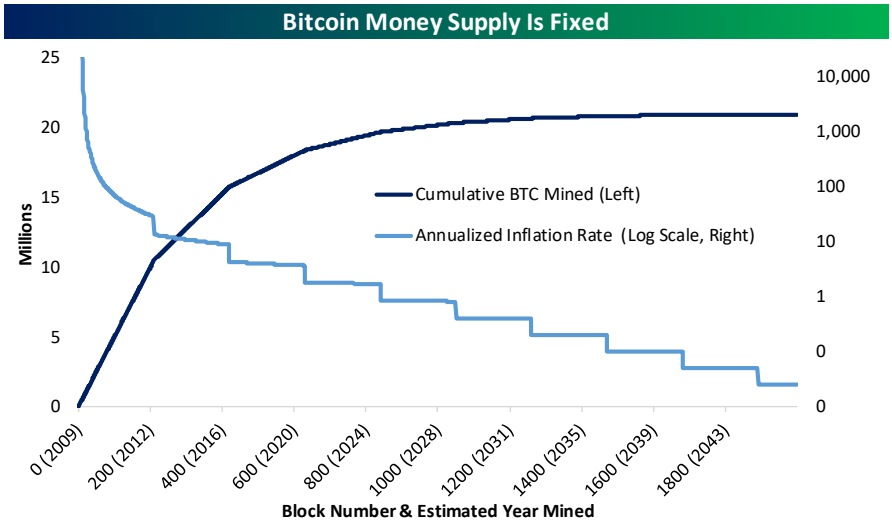
3. Trustless

The last question is, how do we ensure trust in the system? To help answer that, I will again quote the fantastic article written by Aleksander Bulkin:

> "Trust is implicitly present in digital finance in many different ways. There is trust that the entity that holds your account information doesn't go about randomly subtracting value from it, the *trust of safety*. There is trust that the entity who ensures circulation doesn't go about randomly assigning money to itself out of nowhere — *trust of issuance*. Finally, there is trust that the system in fact ensures consistency of information, that is it performs its main function — *trust of correctness*."

To say that the bitcoin network is *trustless* is to say that we do not need to rely on the intentions, malicious or otherwise, of any particular party. Trustless systems are not new. If you are reading this, then you are using the internet, and any junction where your data is sent can eavesdrop on your connection. This problem is easily solved with cryptography, and if it wasn't obvious by the name "cryptocurrency", Bitcoin also uses cryptography—in this case to prove one's ownership of assets. This addresses trust of safety, and ensures that only you can spend the Bitcoins you own.

The next trust issue, trust of issuance, is solved by the agreement of the nodes to issue bitcoin to miners (network participants who ensure the integrity of the public ledger) at a scheduled rate. This rate decreases as the blockchain grows (halves every 210,000 blocks). The graph below illustrates this concept: (A clarifying note: These charts show the monetary (supply) inflation of Bitcoin. They bear no relation to price inflation, which is an entirely distinct phenomenon.)

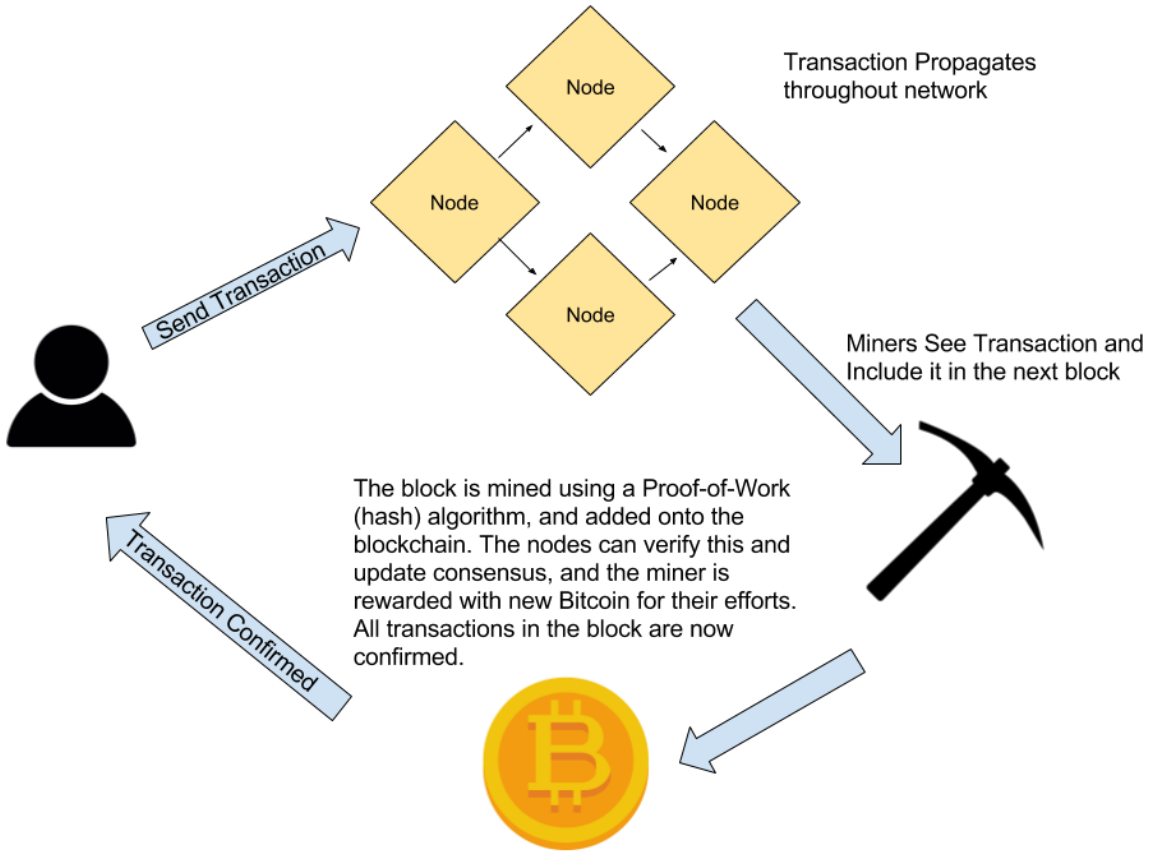


The maximum amount of Bitcoin which will ever circulate is capped at 21 million, making Bitcoin more like a scarce resource—a "digital gold"—than a currency.

The last component of trust, trust of correctness, is achieved by utilizing a publicly verifiable ledger (the blockchain), and a *proof-of-work*. For there to be a consensus on the blockchain, new blocks should be easy to verify, but difficult to add. In this way, would-be attackers cannot easily add or remove blocks and deem their new chain valid. This is where *proof-of-work* and miners come in. It is a miner's job to ensure the integrity of the chain by performing millions of computationally difficult calculations. The difficulty of these calculations is controlled by the network so that only one solution should be found by the *entire network* every 10 minutes (one block/solution per 10 minutes is part of the rules that the nodes agree upon). The entire purpose of this is to ensure that an attacker cannot arbitrarily rewrite the chain to spend his coins multiple times. As long as an attacker does not control over 50% of the total computational power of the network, it should be infeasible for a single entity to rewrite the blockchain. These rules also set a precedent for which chain is the "correct" chain. As long as the nodes agree that the longest / most "difficult" chain is the valid chain, it will be extremely difficult to perform a "double spend" attack. As an incentive to perform this energy-intensive public service, miners are rewarded with new Bitcoin.

So what does this all look like in practice? Here is a watered down diagram which illustrates the flow of a transaction within the Bitcoin network:

Stylized Flow of A Transaction Through The Bitcoin Network



The Rise of the Blockchain: A Look into the Growth of Blockchain Technology

Lately, there's been a bit of a blockchain gold rush, and it seems that investors are ready to throw their money at just about anything that has the word "crypto", "coin", or "blockchain" in it. While this new technology will certainly be industry-disrupting, it's important to consider why blockchain is useful and what problems it can solve.

Blockchain, at its core, is essentially a decentralized database, with a set of agreed upon rules (these rules will vary and are dependant on implementation). While Bitcoin may have been the first and most well known use of the blockchain, people are finding use for it outside the realm of digital finance. One such example is the use of blockchain for a decentralized file storage system. The decentralization of file storage removes the barrier to entry from an industry dominated by tech giants, and allows anyone to rent out space on their hard drive in exchange for digital tokens. Another use for blockchain is tracking real-estate and property records. Its unlikely that all of the uses for blockchain have been discovered, and it will be interesting to see where this technology will be applied in coming years. There will be many blockchain winners, and even more losers, but with a little knowledge about the advantages and disadvantages of blockchain technology, any investor can make a well-informed decision.

Unfortunately, the current blockchain investment culture is somewhat reminiscent of the dotcom bubble, maybe even worse. However, this also provides those in the know with a unique opportunity to scout out legitimate startups and profit from their success. With the right business and technical knowledge, it is not too hard to determine which of these startups could provide real utility, and which ones are totally bogus. In that spirit, I've come up with a few common sense guidelines to follow if you want to invest in blockchain technology.

Read the documentation. Any coder or person with a computer science background will be familiar with this golden rule. Any blockchain startup worth their salt should have detailed, clear, and easy to understand documentation on how their technology works. If you can't understand it, or it seems like a bad application of blockchain tech, then forget about it.

Trust your gut. If you have a nagging feeling that the whole thing is a scam to make the creators money, then it probably is. As of now, ICO's (Initial Coin Offerings) are not regulated in any meaningful way, and investors should be careful because they may not be legally protected from a scam artist.

Look for red flags. Ask yourself the following questions:

1. Does the product actually exist yet? Good businesses are built on good products, not promises.
2. Is there a development team? Is there an open source code repository with a lot of contributors? An open source project allows anyone to verify and contribute to the code. Of course not all code is open source, but part of the blockchain dogma is transparency which usually extends into the codebase.
3. Would you actually use this product? If you can't get behind a blockchain product yourself, why would you expect anyone else to?

Don't put in more money than you can afford to lose. Even the top investors don't always pick winners, and the cryptocurrency ecosystem is far more volatile than traditional investing routes. While this can make for big profits, it can also mean big losses, and the "Wild West" atmosphere of ICOs and other blockchain-related investments means losing every penny you invest should be a very real risk you consider.

Drawbacks

Despite the hype, blockchain tech has plenty of drawbacks and risks. These include, but are not limited to the following.

Efficiency. The act of mining Bitcoin sucks up an enormous amount of electricity. This is the unfortunate byproduct of a *proof-of-work* based cryptocurrency. Some have argued that this has incentivized the creation of more energy efficient technology, but the reality is that it has only incentivized the creation of more energy efficient *bitcoin mining* technology, which unfortunately is not useful for general computing. Assuming all miners are using the Antminer S9 (state of the art mining hardware) the total energy consumption of mining activity on the Bitcoin network can be calculated quite easily.

Bitcoin Network Electricity Use Statistics	
Bitcoin Network Peak Hash Rate (TH/s)	8,697,799
Antminer S9 Efficiency (W/(TH/s))	98
U.S. Electricity cost ($ / kWh)	$0.12
Bitcoin network electricity usage (Watts)	852,384,302
Bitcoin network electricity annual usage (kWh)	7,466,886,486
Bitcoin network electricity cost ($/hour)	$102,286
Bitcoin network electricity cost ($/year)	$896,026,378

It's likely that this figure is even higher, as not all miners are using the most energy efficient hardware. According to the EIA, the average American home consumes 10,812 kWh annually. So, a low end estimate is that the entire Bitcoin network consumes the same amount of energy as (7,466,886,485.52 / 10,812) ≈ 690,611 American homes. While other more energy efficient algorithms have been suggested, such as *proof-of-stake*, or *proof-of-importance*, these other algorithms also come with their own advantages and disadvantages. In the case of proof-of-stake, large holdings of the currency are rewarded with network fees. This creates its own issues, as it incentivizes holders of any token utilizing this proof to continue holding their token. There is an economic benefit to holding rather than transacting, which creates an ever increasing wealth gap between those who hold the most tokens and those who hold the least. *Proof-of-importance* attempts to solve these issues by rewarding not only wealth, but transaction volume and other metrics deemed important to the health of the network (this proof is currently being used by NEM, link). However, both of these systems are more vulnerable to gaming and exploitation than *proof-of-work*. There is no simple solution.

Regulatory. You may have heard that China recently banned ICOs, which caused a downward gap in the price of many cryptocurrencies (cryptocurrencies are used to participate in ICOs). While the Securities and Exchange Commission (SEC) has remained fairly quiet on the topic, they have said that certain cryptocurrencies may qualify as securities, and will be regulated as such. The regulation of the crypto-ecosystem may have beneficial long-term impacts, like protecting investors as well as giving legitimacy to crypto assets, but the short term effects might cause volatility in the market.

In addition to the honest business activity that goes on in the blockchain world, there is also a dark side. Cryptos are the money of choice for tax evaders, money launderers, and black market operators. With the recent FBI seizure of Alphabay (a darknet black market), Bitcoin has come under scrutiny for its role in facilitating illegal activity. It's still a possibility that the U.S. could declare Bitcoin or other crypto assets illegal and bring the party to screeching halt.

Competition. There are plenty of Bitcoin enthusiasts who believe cryptocurrencies could replace modern payment systems, but there are many scaling issues that come with a blockchain-only solution. Below is a table comparing and contrasting blockchain-based transaction systems to traditional systems.

Bitcoin Versus Tradtional Payments

Category	*Blockchain (Bitcoin)*	*Traditional (Visa)*
Energy Cost	Large	Small
Trust	Decentralized	Central Authority
Fraud Protection?	No	Yes
Transaction Fees	Typical Bitcoin fees as of today are roughly $3 per transaction (fees are per transaction instead of a percentage of the transaction)	In the range of 1-3%
Transaction Throughput	≈ 300,000 transactions / day	416mm per day in 12m ended March 21 2017 (max capacity of 65k/second).
Transaction Speed	Minutes to hours for confirmed transactions	milliseconds
Fully Transparent?	Yes	No

While comparing Bitcoin to Visa isn't exactly apples to apples, it's clear that on-chain transactions of Bitcoin are unable to compete with the speed, fraud protection, and energy efficiency that a centralized third party can offer. For a moment, let's imagine that the Bitcoin network could handle the same max transaction throughput as Visa (recent data states this is about 65,000 transactions per second). Based on the earlier chart of Bitcoin's energy efficiency, it takes roughly ((7,466,886,485.52 kWh per year / 365) / 300,000 transactions per day) ≈ 70 kWh of electricity per transaction. If this energy cost remained constant, Bitcoin's network would consume 393,120,000 MWh / day processing as many transactions as Visa can. For some perspective, that amount of electricity is roughly equivalent to 4,160 times the peak output of the Palo Verde nuclear power plant, the largest nuclear power plant in the United States. The Bitcoin blockchain is obviously not scalable as a payment processing system due to the energy limits imposed by proof-of-work. Another scaling issue that would come with an increased transaction throughput is the rate of blockchain growth. The current rate of blockchain growth is roughly 150 MB per day. To achieve a similar throughput to Visa, the blockchain growth would look something like 2.3 Petabytes per day, assuming the same information density as today's blockchain. Not only is 2.3 Petabytes per day completely unfeasible in any circumstance, but even a modest increase in throughput could have a "centralizing" effect on what is meant to be a decentralized network. Only those with access to superior tech would have the capabilities to run a full Bitcoin node, increasing the barrier to entry and moving even further away from the original vision of Bitcoin. That said, off-chain bitcoin transaction solutions are emerging which seek to combat these scaling issues, but they defeat the transactional integrity and transparency that blockchain offer to begin with.

Economic Utility. The examination of Bitcoin versus Visa in the previous section shows that Bitcoin alone will clearly never compete as a payment processor, but If Bitcoin falls short as a payment processing system, then what kind of economic utility might it have? As a currency, Bitcoin would be an utter failure. It's slow and difficult to transact, and lacks a flexible monetary policy. Prices of goods and services are constantly falling because the money supply can't rise. That creates very high real rates of interest that would destroy profitability of economic agents trying to conduct activity in bitcoin. There's a reason modern central banks are terrified of deflation!

Viewing bitcoins as a store of value might make more sense. There's a limited quantity of bitcoins that will ever be in circulation, which bears some similarities to gold, but there's still too much uncertainty around what sustained demand might look like to determine an appropriate valuation. In other words, for a store of value to actually store value, it must have some intrinsic worth. For the US dollar, the intrinsic worth is the ability to purchase goods and services within the US economy and in other dollar-denominated markets around the world, trade financial instruments, and pay taxes. Currently bitcoin offers nothing like this; everyone's reference for economic activity is ultimately still to other currencies because that's where the vast majority of output for any country is.

Gold and Bitcoin also diverge when it comes to volatility. People see gold as a safe investment during times of uncertainty, but at the moment, bitcoins are anything but safe. Wild price fluctuations make bitcoins unattractive to anyone trying to curb their risk or minimize exposure in traditional markets. Eventually these price fluctuations may settle as the crypto market matures, but we are still in the very early stages. However, Bitcoin does have some utility to offer in its present state. It makes tax evasion easy, and facilitates the exchange of black market goods. These uses have obvious negative social impacts, and have lead to the creation of services such as Chainalysis, which is used by law enforcement and banks alike to track "dirty" bitcoins and tax evaders. Ultimately only time will tell what kind of utility bitcoins are apt to provide, but we caution against any bull case built on the idea they will be either a dominant payments system or a meaningful currency that supports real economic activity.

Implementation Complexity. In the frantic rush to get blockchain startups off the ground, code integrity is sacrificed for development speed. This may be true for any software-driven business looking to get on its feet quickly, but the consequences for a blockchain based company can be dire. For example, users of the "Parity" wallet (A wallet is where users store their cryptocurrencies) for ethereum (a "smart-contract" blockchain platform) had over $30 million worth of ethereum stolen from them due to poor implementation in the wallet software. Countless blockchain startups have had their ICO funding hacked due to insecure websites. Fatal vulnerabilities have even been found in Trezor's hardware wallets, widely considered to be the most secure wallet on the market.

One of the promises of blockchain tech is security, and yet so many implementations have fallen short of that. Blockchain promotes the idea of "decentralization", but the typical user must interact with many centralized parties in order to facilitate exchange of bitcoins. For example, if you are looking to trade US dollars for bitcoins, the typical route is through a third party exchange. At some point during this transaction, your bitcoins will transferred to the exchange. During the time in which your bitcoins remain on this exchange, you are trusting the security of the servers and integrity of some third party to protect your assets. (*Con't on page 10*)

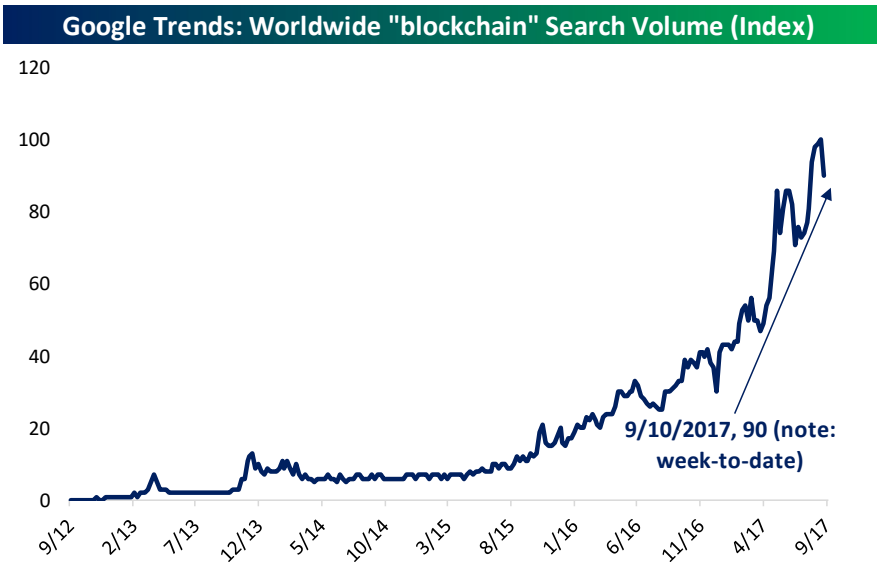
Whether or not the promises made by blockchain tech are kept remain in the hands of the exchange, which is just as vulnerable to being hacked as any other centralized payment system (lets not forget the MtGox hack or BTC-E's money laundering scheme).

Hacking and security issues aside, another problem with blockchain tech is that when these hacks occur, there is no easy way to reverse them on a distributed network. There is no restoring from a back-up database. There is no insurance, and no fraud protection. In cases of extreme hacks, the only answer is a hard fork, such as the one that split Ethereum into "Ethereum" and "Ethereum Classic" as the result of a $50 million dollar hack. Hard forks are generally undesirable due to their disruptive nature.

In order to gain mass penetration beyond highly specialized implementations, bitcoin needs to be easy to use *and* secure. The problem is, current deployments have to make significant trade offs between these two priorities. Bitcoin can be extremely secure, but keeping it that way requires technical know-how. It can also be extremely easy to use, but keeping it that way requires exposure to the very risks that the cryptocurrency was designed to avoid.

Closing Remarks

Here's a graph of Google's Worldwide interest over time for the search term "blockchain".



The interest has been growing steadily, and may continue to grow for the next several years as more blockchain-backed applications come out. While this technology may not be as revolutionary as the internet, it is still changing the way we think about applications, and challenging current data-storage paradigms. From our perspective, the technology is exciting and will yield new applications that drive investment returns. But we caution investors against large exposure to volatile cryptocurrencies; the current market is being driven by speculation (both fear and greed). Instead, we encourage you to learn about the space and innovations taking place within it, investing rather than simply trying to get a piece of the explosive price action of cryptocurrencies like bitcoin, and always keeping in mind that investment of any kind entails significant risk. For blockchain-related investments, those risks are *much* higher than most investors are used to.

Glossary

BIP: Bitcoin Improvement Protocol. Updates and changes to the core bitcoin software are done democratically, and must be presented to the developer community as a "Bitcoin Improvement Protocol" which is then reviewed and implemented if it has enough support.

Blockchain: The technology behind Bitcoin and many other cryptocurrencies. The blockchain serves as a decentralized ledger which tracks all transaction activity. Each full node must have a copy of the blockchain.

Hash: The output of a "hash function". A hash function will take some kind of input, scramble it up, and create a fixed-size output, which is completely different from the input. Even a small change in the input can create a wildly different change in output. In the case of a cryptographic hash function, the input should never be reproducible from the output (the hash function should not be invertible).

ICO: Initial Coin Offering. An unregulated means by which funds are raised for a new cryptocurrency venture. An Initial Coin Offering (ICO) is used by startups to bypass the rigorous and regulated capital-raising process required by venture capitalists or banks.

Mining: The act of performing millions of computationally intensive calculations to preserve the integrity of the blockchain. Miners are rewarded with new Bitcoins and transaction fees for their efforts.

Node: A server running bitcoin software, and possessing a full copy of the blockchain. While there are multiple versions of the bitcoin software available, they typically all agree on the same basic set of rules.

Proof-of-Work: "A proof-of-work (PoW) system (or protocol, or function) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer" (Wikipedia).

Wallet: The Bitcoin equivalent of a bank account. Wallets may contain multiple "addresses" which funds can be sent to or from.