What Is Blockchain Technology?

CBINSIGHTS

Few people understand what it is, but Wall Street banks, IT organizations, and consultants are buzzing about blockchain technology. It's hard to remove blockchain from Bitcoin, so we'll start with Bitcoin as we work to understand this technology's potential.

Bitcoin. Blockchain technology. Cryptocurrencies. Initial coin offerings.

Everyone's talking about them, but what do these terms really mean?

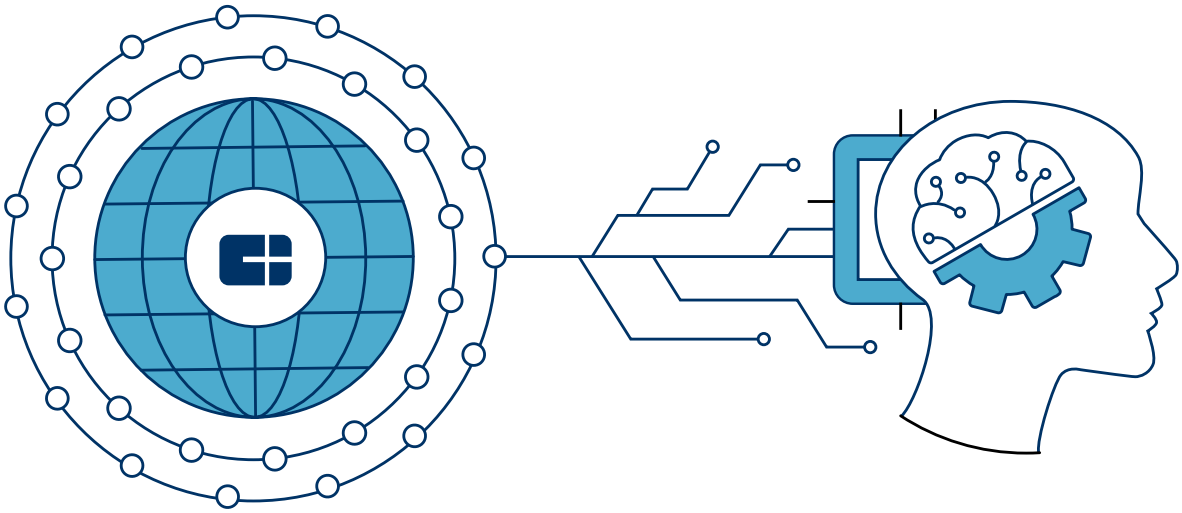
At its peak in January 2018, the total market cap of cryptocurrencies surpassed $800B, according to Coin Market Cap, while the price of bitcoin hit a high of $19,300 in Dec'17, according to Coindesk. Initial coin offerings (ICOs) exploded in popularity, surpassing $18B in the first 8 months of 2018. Huge corporations — like Walmart and Pfizer — have completed successful blockchain pilots, with many more partnering on projects ranging from remittance to title transfer.

This explainer will offer simple definitions and analogies for blockchain technology. It will also define Bitcoin, Bitcoin Cash, Ethereum, Litecoin, blockchain, and initial coin offerings. Along the way, we'll highlight promising use cases for blockchain technology.

(For a deep dive into how Ethereum works specifically, you can read our **What Is Ethereum explainer.**)

Lastly, this report will make clear the distinctions between distributed ledger technology and blockchain, and highlight where these technologies have an application – and where they do not.

Table of Contents



At CB Insights, we believe the most complex strategic business questions are best answered with facts.

We are a machine intelligence company that synthesizes, analyzes and visualizes millions of documents to give our clients fast, fact-based insights.

From Cisco to Citi to Castrol to IBM and hundreds of others, we give companies the power to make better decisions, take control of their own future, and capitalize on change.

WHERE IS ALL THIS DATA FROM?

The CB Insights platform has the underlying data included in this report

CLICK HERE TO SIGN UP FOR FREE

"We use CB Insights to find emerging trends and interesting companies that might signal a shift in technology or require us to reallocate resources."

Beti Cung,
CORPORATE STRATEGY, MICROSOFT

Microsoft

TRUSTED BY THE WORLD'S LEADING COMPANIES

citi IBM GE BARRICK Castrol
SEQUOIA DASSAULT SYSTEMES CISCO salesforce

What Is Bitcoin?

The 2008 financial crisis caused a lot of people to lose trust in banks as trusted third parties. Many questioned whether banks were the best guardians of the global financial system. Bad investment decisions by major banks had proved catastrophic, with rippling consequences.

Bitcoin — also proposed in 2008 — presented something of an alternative.

According to its whitepaper, Bitcoin is a "peer-to-peer electronic cash system" that "allow[s] for online payments to be sent directly from one party to another without going through a financial institution."

In other words, Bitcoin made digital transactions possible without a "trusted intermediary." The technology allowed this to happen at scale, globally, with cryptography doing what institutions like commercial banks, financial regulators, and central banks used to do: verify the legitimacy of transactions and safeguard the integrity of the underlying asset.

Bitcoin is a decentralized, public ledger. There is no trusted third party controlling the ledger. Anyone with bitcoin can participate in the network, send and receive bitcoin, and even hold a copy of this ledger if they want to. In that sense, the ledger is "trustless" and transparent.

The Bitcoin ledger tracks a single asset: bitcoin. (Note: "Bitcoin" capitalized refers to the Bitcoin ledger, or protocol, while "bitcoin" in lowercase refers to the currency or a unit of account on the Bitcoin ledger.)

The ledger has rules encoded into it, one of which states that there will only ever be 21M bitcoin produced. Because of this cap on the number of bitcoins in circulation, which will eventually be reached, bitcoin is inherently resistant to inflation. That means that more bitcoin can't be printed at a whim and reduce the overall value of the currency.

All participants must agree to the ledger's rules in order to use it.

Bitcoin is politically decentralized — no single entity runs bitcoin — but centralized from a data standpoint — all participants (nodes) agree on the state of the ledger and its rules.

A bitcoin or a transaction can't be changed, erased, copied, or forged – everybody would know.

That's it, and it's a big deal.

The Story Of Alice And Bob

To understand better how this peer-to-peer electronic cash system allows for online payments to move from one party to another without going through a financial institution, let's use a simple example.

Physical Transaction

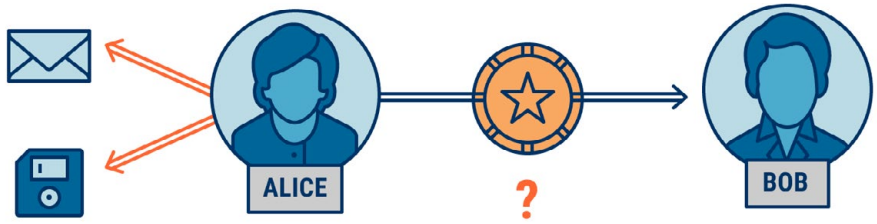
Here's a scenario: Alice hands Bob a physical arcade token. Bob now has one token, and Alice has zero. The transaction is complete. Alice and Bob do not need an intermediary to verify the transaction. Alice can't give Charlie the same token, because she no longer has the token to give — she gave it to Bob.

But what if the same transaction were digital? Alice sends Bob a digital arcade token — via email, for example. Bob should have the digital token, and Alice should not.

Right?

Not so fast. What if Alice made copies or "forgeries" of the digital token? What if Alice put the same digital token online for all to download? After all, a digital token is a string of ones and zeros.

Digital Transaction



If Alice and Bob "own" the same string of ones and zeros, who is the true owner of the digital token? If digital assets can be reproduced so easily, what stops Alice from trying to "spend" the same digital asset twice by also sending it to Charlie?

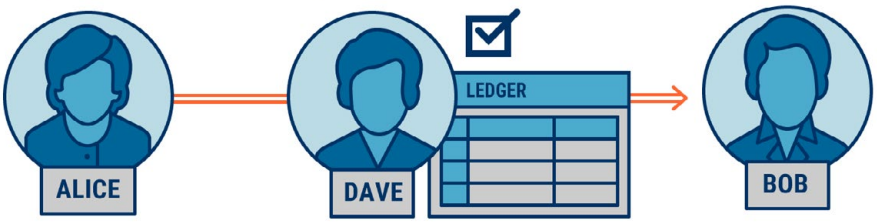
One answer: use a database — a ledger. This ledger will track a single asset: digital arcade tokens. When Alice gives Bob the digital token, the ledger records the transaction. Bob has the token, and Alice does not.

Now, they face a new problem: whose job will it be to hold the ledger? Alice can't hold it because she might erase the transaction and say that she still owns the digital token, even though she gave it to Bob. It also can't be Bob, because he could alter the transaction and lie to say that Alice gave him two tokens, doubling his arcade time.

Bob and Alice can solve this problem by using a trusted third party, an intermediary who is not involved in the transaction at all — let's call him Dave. Dave will hold the ledger and make sure that it's up-to-date.

This situation is fine — until it's not.

Digital Transaction: Ledger



What if Dave decides to charge a fee that neither Alice or Bob want to pay? Or, what if Alice bribes Dave to erase her transaction? Maybe Dave wants the digital token for himself, and adds a false transaction to the ledger in order to embezzle it, saying that Bob gave him the token?

In other words — what happens when Alice and Bob cannot trust the trusted third party?

Think back to the first physical transaction between Alice and Bob. Is there a way to make digital transactions look more like that?

Here's a thought: Alice and Bob could distribute the ledger to all their trusted friends, not just Dave, and decentralize trust. Because the ledger is digital, all copies of the ledger could sync together. If a simple majority of participants agree that the transaction is valid (e.g. confirm that Alice actually owns the token she wants to send), it gets added to the ledger.

Decentralized Ledger

When a lot of people have a copy of the same ledger, it becomes more difficult to cheat. If Alice or Bob wanted to falsify a transaction, they would have to compromise the majority of participants, which is much harder than compromising a single participant.

Alice can't claim that she never sent a digital token to Bob — her ledger would not agree with everyone else's. Bob couldn't claim that Alice gave him two tokens — his ledger would be out of sync. And even if Alice bribes Dave to change his copy of the ledger, Dave only holds a single copy of the ledger; the majority opinion would show the digital token was sent.

In sum, this distributed ledger works because everyone is holding a copy of the same digital ledger. The more trusted people that hold the ledger, the stronger it becomes.

Such a ledger allows Alice to send a digital token to Bob without going through Dave. In a sense she is transforming her digital transaction into something that looks more like a physical one in the real world, where ownership and scarcity of an asset is tangible and obvious.

How secure is Bitcoin?

How can we get all these untrusted "nodes" to agree on the state of the ledger? How can we avoid bad actors corrupting the ledger?

You may have noticed a key difference between the above example and Bitcoin. Specifically, Alice's and Bob's ledger only allows "trusted friends" to participate. In contrast, Bitcoin is entirely public, and anyone can participate.

Let's think about this for a moment. A public ledger would allow for many more participants. The more participants, the stronger the ledger becomes. Right?

As you may have guessed, it's not that simple.

Because Bitcoin expands beyond trusted participants and gives anyone access, it runs a higher risk of bad actors and false transactions.

Sure, we also ran a risk of bad actors when it came to Alice's and Bob's trusted friends: Dave might turn untrustworthy. However, Bitcoin is free and open to anyone, trusted or not, like a Google document that anyone can read and write to.

How can we get all these untrusted "nodes" to agree on the state of the ledger? How can we avoid bad actors corrupting the ledger?

Bitcoin offers a solution: reward good actors and scare off bad ones, a classic carrot and stick act.

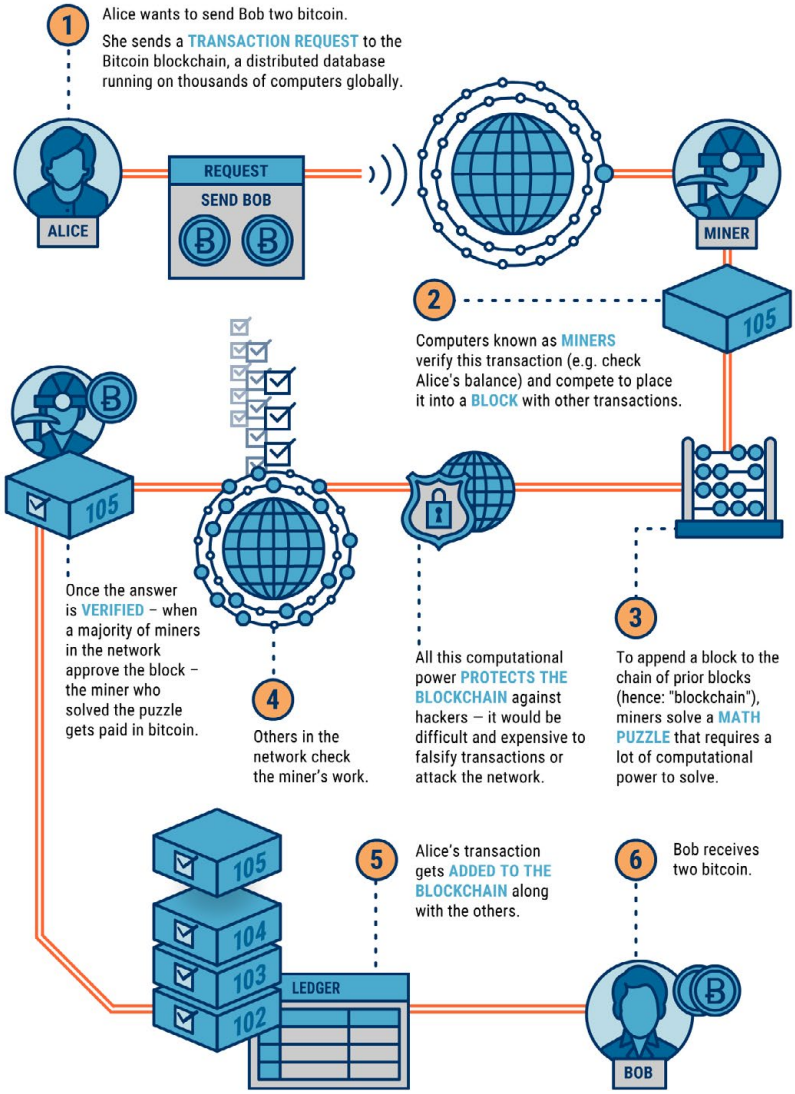
In simple terms, certain Bitcoin participants are incentivized to do the dirty work and maintain the network. These participants — called "miners" — bundle transactions into a "block," add this newest block to the "chain" of prior blocks (hence: blockchain is used to describe Bitcoin's unique database structure), and devote immense computational power to the network in the process. For doing this work, these miners are rewarded with bitcoin. With a single bitcoin worth thousands of dollars, this is a very strong incentive.

When miners devote computational power, they also use a tremendous amount of electricity. So much electricity, in fact, that a recent estimate put the Bitcoin blockchain's total annual energy consumption on par with the entire country of Ireland.

This scares away hackers and bad actors because "hacking" Bitcoin to get everyone's coins would cost a tremendous amount of computing power, electricity, and money. Further, if the Bitcoin community became aware of the hack, it would likely cause the price of bitcoin to drop steeply. *This makes such an attack economically self-defeating.*

Understanding a Bitcoin Transaction

HOW BLOCKCHAIN TECHNOLOGY POWERS BITCOIN



In technical terms, this mining process creates Bitcoin's consensus mechanism, called "Proof of Work."

This clever game-theoretic model creates a ledger that everyone trusts, but nobody controls.

Wait... what is Bitcoin?

OK, let's connect all the dots:

- Bitcoin is a decentralized, public ledger. This ledger is known as a blockchain. There is no trusted third party controlling the Bitcoin blockchain. Instead, anyone can read it, write to it, and hold a copy.
- The Bitcoin blockchain tracks a single asset: bitcoin. The block-chain has rules, one of which states that there will only ever be 21M bitcoin. All participants must agree to Bitcoin's rules in order to use it.
- Because anyone can read it and write to it, Bitcoin needs a method to establish consensus among untrusted nodes — unlike Alice's and Bob's distributed ledger shared among trusted friends. It solves this problem via clever economics:
  - Incentive: The first miner to verify transactions and devote immense computing power to secure the blockchain can append a block of transactions to the chain of previous blocks. This miner is rewarded with bitcoin, and the race starts over every ten minutes.
  - Disincentive: Bad actors are dissuaded from attacking the blockchain, because it's effectively a money-losing proposition.

What are altcoins?

Since Bitcoin launched in 2008, thousands of other cryptocurrencies and altcoins ("alternative coins") have emerged.

Because Bitcoin's code is open-source, anyone can use Bitcoin's code to create an altcoin. Many of them seek to improve on Bitcoin or expand its capabilities. Remember Bitcoin's rules: it caps the number of bitcoin at 21M and uses the Proof of Work system to secure the network. Other cryptocurrencies use different rules and engage with other economic models.

Is Bitcoin a bubble?

Hard to say. It's true that the value of one bitcoin has gone from around $300 in 2015, to almost $20,000 at its peak in December 2017, back down to about $6,400 in early September 2018. Even with all this volatility, bitcoin is still way up over the long run: if you had bought $100 of bitcoin at the end of 2011, it would be worth over $200k today.

As discussed, Bitcoin's blockchain technology allows for the creation of a unique and scarce digital asset where everyone knows the history of each particular bitcoin. A single bitcoin is not just a string of ones and zeros: it's also the first successful (at least so far) censor-proof, portable, easily transactable, durable, and secure digital asset.

Bitcoin's value is subject to the same supply-and-demand mechanics found in any marketplace. If investors find the above characteristics valuable and demand for bitcoin grows, bitcoin's price rises, and vice versa.

Bitcoin's supply is limited to 21M coins, although only about 17M have been mined so far. As of September 6, 2018, investors value bitcoin at about $112B in aggregate.

To give a sense of how the market values other cryptocurrencies, here's some market information about some of the top ones.

Comparing Top Cryptocurrencies

AS OF 9/6/18

	Bitcoin (BTC)	Ethereum (ETC)	Bitcoin Cash (BCH)	Litecoin (LTC)
Price ($)	$6,400	$225	$510	$55
Market Capitalization ($B)	$111.5	$22.9	$8.8	$3.3
Number of Transactions (24h)	264,000	592,000	20,000	29,000
Avg. Transaction Value ($'000)	$30.9	$1.1	$5.9	$7.7
Avg. Block Time	9m 21s	14s	12m 19s	2m 29s
Circulating Supply (M tokens)	17.3	101.8	17.3	58.2
Blocks Last 24 Hours	155	5,980	100	562
Avg. Blocks per Hour	6	249	4	23
Current Reward Per Block (# tokens)	12.50 BTC	3 ETH	12.5 BCH	25 LTC
Current Reward Per Block ($)	$81,800	$790	$6,400	$1,400
First Block	1/9/2009	7/30/2015	1/9/2009	10/8/2011

A caveat

There's lots more to Bitcoin that we're not going to get into. Hashes, public-private key encryption, segregated witness, and sidechains, among other elements, fall outside of the scope of this piece.

Blockchain

What Is Blockchain?

So far, we've discussed two types of ledgers.

The first, Alice's and Bob's distributed ledger for digital arcade tokens, is private.

The second, Bitcoin's decentralized ledger for bitcoin, is public. Anyone can participate. To ensure its public, decentralized ledger remains secure, Bitcoin uses a blockchain.

If we were to define "blockchain" as a technology separate from Bitcoin, it might look something like this:

Blockchain technology offers a way for untrusted parties to reach agreement (consensus) on a common digital history. A common digital history is important because digital assets and transactions are in theory easily faked and/or duplicated. Blockchain technology solves this problem without using a trusted intermediary.

Where else might blockchain make sense?

The short answer: in unique instances.

To see what those instances might be, let's think about why Bitcoin needs blockchain technology. There are three main reasons.

- Bitcoin is a public ledger of bitcoin transactions
- There are untrusted nodes recording transactions on the Bitcoin ledger
- Bitcoin does not want to trust a third party to administer the ledger

Effectively, Bitcoin uses a blockchain to decentralize payments. Where else could we use this unique database architecture to get rid of the middleman? Are there other things that would be more valuable if they were decentralized?

Let's take this step-by-step. What's another scenario where everyone needs a record of ownership, and where a trusted third party isn't preferred?

A couple of immediate use cases come to mind.

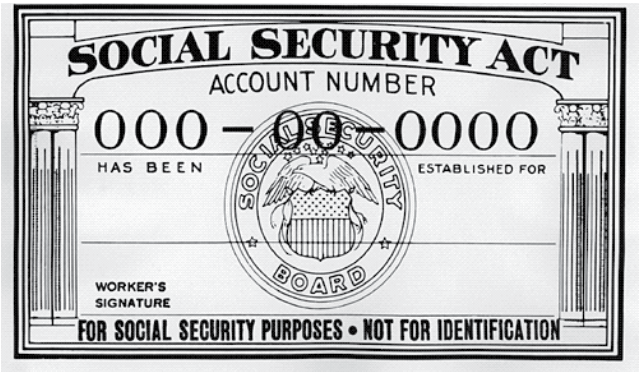
Land title is one. It could be quite useful for everyone to have access to a decentralized source of record saying who owns a given parcel of land. Considering that coups and wars often redistribute land unfairly and/or incorrectly, this could not only prove useful: it could also have humanitarian implications. Once a land distribution is agreed upon, it can be recorded in a distributed ledger and no longer be subject to ongoing debate. A number of companies are working on this, including velox.RE.

In the same vein, a blockchain could be used to establish ownership over any number of physical assets — cars, art, musical instruments, and so on. A paper record of title is prone to forgery and/or physical degradation. Centralized databases are prone to hacking, human error, and/or tampering. A blockchain means there is no single entity controlling the ledger. Therefore, recording physical assets on a blockchain is a prime example of where the technology might come in handy to track ownership with a tamper-proof, neutral, and resilient system.

Taking this one step further, blockchain technology could even prove applicable in virtual reality. If a virtual world is created — for gaming, or for any number of other reasons — blockchain technology could allow users to purchase and own pieces of that virtual world, just like they might purchase a plot of land.

That's certainly a bit far out, but Decentraland is one project already working on it. The team raised $25M in August 2017 for its token, MANA, and has promised to build "the first virtual platform owned by its users."

Identity might also be low-hanging fruit. The 2017 Equifax hack exposed the social security numbers of 143M Americans. Social security numbers were never meant to be used for identification — notice how this old social security card states "not for identification."



Blockchain technology might present a better means of establishing identity. Instead of a state or government issuing it, identity could be verified on an open, global blockchain — controlled by nobody and trusted by everybody. Thus, users could control their own identity. A number of companies are working in this arena, including ID2020 and Civic.

Similarly, Blockstack hopes to build a new decentralized internet, "where users own their data and apps run locally." Technically speaking, Blockstack is one of the first examples of a decentralized DNS (domain name server) system built using blockchain technology. The company raised $52M in December 2017 and hopes that its new internet will help users "own [their] data and maintain [their] privacy, security, and freedom." If it works, Blockstack could disrupt many of the internet giants that act as middlemen today — think Google and Facebook. Of course, that's a big if.

There are also a wide array of potential decentralized internet services, like decentralized advertising. Basic Attention Token has recently been gaining ground as a blockchain-based protocol that promises to make advertising more efficient by distributing value between users, advertisers, and publishers. The project, founded by Brendan Eich, the creator of JavaScript and the co-founder of Firefox and Mozilla, uses a blockchain-based token in a custom-built browser to track and reward focused user attention on advertisements while protecting user privacy.

Other potential applications include a platform where traditionally illiquid assets are represented and traded through blockchain-powered tokens. Imagine a decentralized asset market, where you can buy, sell, and trade fractional ownership of high-value paintings, real estate, and companies via interoperable databases, without any kind of intermediary. That's the kind

of liquidity that 0x Project is working to make possible with its protocol for decentralized asset exchanges.

Of course, the **applications for blockchain technology** extend well beyond these six examples.

Where does distributed ledger technology make sense?

Let's back up for a moment.

We mentioned that Alice's and Bob's private implementation — where everyone knows and trusts everyone involved — doesn't need a blockchain (nor does it need miners to verify and append transactions to the cryptographically-protected blockchain).

Without the blockchain's verification step, we're left with a "distributed ledger," or a decentralized spreadsheet that is only accessible to a select group of trusted parties. Because this ledger is private, it doesn't need the same security measures as the blockchain.

The hype around Bitcoin, blockchain, and cryptocurrencies has contributed to renewed interest in distributed ledger technology. This is the idea of distributing a database among participants to ensure a common record of truth. Bitcoin uses distributed ledger technology and adds a consensus layer on top — the blockchain.

Because Alice and Bob's participants are trusted and their ledger is private, Bitcoin's blockchain isn't needed. In fact, a blockchain might prove unwieldy, slow, and overly complex for Alice and Bob's ledger, for reasons which we'll address below. Instead, a trusted third party could be used to lightly administer a distributed ledger.

Bitcoin and Ethereum (which we'll dive into below) are considered public, "permissionless" blockchains: anyone can access them. On the other hand, if all parties are known and trusted, distributed ledger technology could provide sufficient security. One example of distributed ledger technology is R3's Corda, which is working with major financial services organizations to improve banking processes.

While distributed ledger technology and blockchain technology each have their own pros and cons, the important thing to remember here is that blockchain technology is not a cure-all. For Bitcoin, a public, permissionless blockchain is the only possible solution. In many other instances, a blockchain would be a terrible idea.

What are the major issues with blockchain technology?

Blockchain technology is really good at some things and absolutely awful at others.

The three major questions about blockchain technology concern its scalability, its anonymity, and its economical viability.

IS BLOCKCHAIN SCALABLE?

For a blockchain to work, lots of participants need to hold up-to-date copies. This means that the same database is held by thousands of nodes. This is fairly inefficient.

If we were to look at how technology has developed over the past fifteen years, blockchain runs counter to the logic behind cloud computing. Cloud computing trends toward a single database that multiple nodes can access. These nodes don't have to hold their own private copy of this database.

Further, nodes holding copies of the blockchain receive constant updates. These nodes are distributed around the world. Because of this, blockchains have high latency (latency is the amount of time it takes for data to move through the network).

As a result, blockchain technology faces scaling issues. Bitcoin can process about 4-5 transactions per second. Ethereum maxes out at about 25 transactions per second. Visa can process over 24,000 transactions per second.

IS BLOCKCHAIN ANONYMOUS?

In the early days of Bitcoin, blockchain technology — like many nascent technologies — was popularly associated with illicit activities.

Why was blockchain technology like Bitcoin effective for this kind of enterprise? Even though Bitcoin's record of transactions is publicly available, the network's global, decentralized nature means that no single entity — like the US government or Visa — can shut it down, freeze funds, or reverse transactions. And in those early days, it was very hard to link a Bitcoin wallet to a given individual, even if there was evidence that the wallet was used in illicit activities.

One of the reasons why Bitcoin has gained more mainstream popularity as a store of value and financial instrument is that it's no longer as anonymous as it was in those early days. Most major services that allow you to buy and sell Bitcoin use "know your customer" (KYC) standards, and law enforcement agencies have gotten more adept at linking Bitcoin transactions to specific people. There are other projects that have emerged in an effort to use blockchain technology to protect user anonymity (e.g. Monero and ZCash), but these are significantly less mainstream.

IS BLOCKCHAIN ECONOMICAL?

One of the keys to blockchain technology being viable in the long-run is making sure that transactions like Alice and Bob's can be executed with minimal fees. Fees are important because they incentivize miners to add your transactions to the blockchain in a timely manner — but high fees make it harder to convince potential users to get on board.

In December 2017, the median transaction fee on the Bitcoin network peaked at $34 per transaction. Companies like Stripe and Valve announced they would no longer accept Bitcoin payments due to high fees.

Today, the median transaction size on the Bitcoin network is about $300, while the median transaction fee wavers around $0.10 — that's a 0.03% median transaction fee, much better than the 0.7% fees of its peak.

Though the fees have come down, Bitcoin is still not capable of everyday commerce — the platform would have to solve issues with scaling, transaction block time, and more before it's ready for the big leagues.

Ethereum

What is Ethereum?

We asked earlier what other applications could be built with blockchain technology.

Recall that Bitcoin is, effectively, a decentralized application for payments. Ethereum adds another layer by allowing users to put code on its blockchain that executes automatically. This code is called a "smart contract." In this way, Ethereum hopes to create a decentralized computing platform — a global supercomputer.

What is a smart contract?

To illustrate a smart contract, let's say Alice and Bob enter into a bet.

Alice thinks that the temperature tomorrow morning will reach 70 degrees. Bob thinks that it will stay lower. They wager 10 bitcoin on the outcome. If Alice and Bob don't trust each other, they will have to use a trusted third party as an escrow agent. In other words, they will each have to give the agent that amount of bitcoin, and the agent will distribute the winnings and the amount staked to the winner.

There's no way around the middleman in this scenario, even using bitcoin.

Ethereum, though, offers a decentralized solution. Alice and Bob could agree to use some basic code — a contract of sorts — to alert the system to what the temperature ended up being and pay out based on who was correct. If the temperature goes higher than 70 degrees, the code pays Alice, otherwise, it pays Bob. Alice and Bob could then place this code (their bet) on Ethereum's blockchain.

This looks like a "contract," because all participants in the Ethereum blockchain hold a copy of this agreement. Just like the Bitcoin blockchain knows that Alice sent Bob a bitcoin (in our example above), the Ethereum blockchain knows that Alice and Bob have entered into an agreement. Therefore, this contract is self-enforcing.

Smart contracts like these are what make Ethereum so compelling. Because Ethereum is a blockchain, it's very hard to attack, change, or forge these smart contracts, just like it's economically self-defeating to attack Bitcoin.

So, what is Ethereum?

A smart contract allowed Alice and Bob to build a very small decentralized application. What if we could build larger and more complex decentralized applications?

Ethereum wants to be the platform on which these decentralized applications are built.

Recall that Bitcoin is a very simple decentralized application, for payments. Ethereum builds on Bitcoin by incorporating robust computing capabilities and smart contracts. In simple terms, this means that developers can use more complex code to build decentralized applications on top of Ethereum. These apps would be less error prone, more neutral, and more transparent. They would have lower administrative costs and greater built-in security.

Let's unpack this:

- Ethereum allows participants to execute code on its ledger, including "smart contracts." Coupled with its ability to incorporate complex code, Ethereum hopes to be a massive decentralized computer.
- In the same way that Bitcoin uses a blockchain to track bitcoin, Ethereum uses a blockchain to track a cryptocurrency called "ether." Users spend ether to run programs on the Ethereum supercomputer.
- Because Ethereum is decentralized, once a program is uploaded it can't be shut down by any sort of centralized actor. Just like Bitcoin, there is no central point of attack.
- Therefore, Ethereum is also a construction set for building decentralized applications. Instead of building their own blockchains from scratch, developers can use Ethereum's blockchain.

Here are some decentralized applications attacking different verticals. Many of these are building on top of Ethereum:

134 blockchain startups with ICOs

CLOSED INITIAL COIN OFFERINGS GREATER THAN OR EQUAL TO $500K. 2014 – 2017 (09/08/2017)

ASSET MANAGEMENT

ICONOMI · Blockchain Capital · Zr coin · DIGIX GLOBAL · 2025 · MELONPORT · DIMCOIN · Starta Accelerator · MYBIT.io · DDF

MEDIA & ADVERTISING

synereo · basicattentiontoken · SingularDTV · LUNYR · DECENT · AdEx · adToken · VOISE · OPUS · VIBERATE · po.et · ROC · XPLAY

GAMBLING & GAMING

FunFair · wagerr · ETHER FOR THE FIRST OF THE WORLD · CRYPTOKITTY · PEERPLAYS · MOBILEGO · Kibo · edgeless.io · FootballCoin · SkinCoin · BETKING · Monster BYTE

INFRASTRUCTURE & DEVELOPMENT

Lisk · STRATIS · BLOCKPOOL · aeternity · Bancor · ethereum · BOScoin · COSMOS · NEO · neblio

EXCHANGES & WALLETS

omisego · DAX · EXSCUDO · NVO · MOTHERSHIP · Bitquence · 0x · CORION PLATFORM · DCORP

TRADING

Lykke · santiment · CryptoPing · ETHBITS · RIALTO AI · investFeed

DAO & TOKEN LAUNCH

ARAGON · Adel · ICOO

COMPUTING & STORAGE

SONM · iEx.ec · golem · DFINITY · STORJ.IO · Filecoin

OTHER

particl · QRL · mysterium network · EcoBit · primalbase · KOMODO · EncryptoTel · Decentraland · aventus · AQUARIUS · REX · incent

BROWSERS & SOCIAL

Status · matchpool · NIMIQ · BitBOunce · OBSIDIAN · crypviser

CROWDFUNDING & LENDING

cofound.it · WeTrust · SURETLY · SALT · EVEREX

PREDICTION MARKETS

GNOSIS · augur · WINGS · ROX

HEALTHCARE & INSURANCE

patientory · ENCRYPGEN · INSUREX

IDENTITY & INTERNET OF THINGS

civic · PILLAR · AIR · IOTA

PAYMENTS & BANKING

polybius · MONACO · PLUTUS · BlockPay · humaniq · TenX · monetha · Minexcoin · token · atbcoin

FINANCIAL SERVICES

Veritaseum · the internet of coins · hive · EQUIBIT GROUP · POPULOUS

Sources: CB Insights, TokenData, CoinSchedule. Map is illustrative; not exhaustive.
We make no claims to the value of any of these projects.

CB INSIGHTS

Why does Ethereum matter?

In August 2016, then-Union Square Ventures investor Joel Monegro published a blog post entitled "Fat Protocols." In it, he examines the protocols or systems on which our modern internet has been built:

"The previous generation of shared protocols (TCP/IP, HTTP, SMTP, etc.) produced immeasurable amounts of value, but most of it got captured and re-aggregated on top at the applications layer, largely in the form of data (think Google, Facebook, and so on)."

In other words, the internet as we know it works because of TCP/IP, HTTP, and SMTP, among others. These protocols are often open-source and maintained by devoted developers.

If the entire internet relies on these protocols, one would expect these protocols to extract value (read: make money). However, that hasn't happened. Instead, the applications built on top of these protocols have made all the money. Google, Facebook, and Amazon can't exist without TCP/IP, but they have captured all the value, while TCP/IP has not.

By effectively creating a decentralized supercomputer, Ethereum acts as a base layer for decentralized applications. Ethereum's built-in cryptocurrency, ether, can be traded on exchanges for dollars or other government-backed currency — just like bitcoin. Therefore, the value of this supercomputer can be captured at the protocol layer.

Why is the price of Ethereum so high?

Ethereum's blockchain allows for the creation of a decentralized supercomputer. This supercomputer is the first one of its kind.

Computational power is limited, and developers pay with ether to use the Ethereum blockchain. Users also buy and spend ether to interact with its various decentralized applications. For example, CryptoKitties is a popular app built on top of the Ethereum blockchain that allows individuals to buy collectible cartoon cats. In order to purchase a CryptoKitty, you have to use ether.

Ether's dollar value is subject to supply-and-demand — if investors find the Ethereum blockchain valuable, and developers are building valuable decentralized applications on top of the platform that require the use of ether, then demand might rise and the price of ether could rise. The opposite can also happen.

As more and more applications are built on Ethereum, the demand for ether has gone up, driving up the price of the token. However, the price of the coin has fallen nearly 85% since its peak.

What are initial coin offerings?

We've now discussed Bitcoin and Ethereum. Both blockchains use a "token" that provides utility. Bitcoin uses bitcoin, while Ethereum uses ether.

Remember how we mentioned other decentralized applications? An initial coin offering is a way for these applications to raise money. Instead of going the traditional venture capital route, a team could announce that — just like bitcoin or ether — it's issuing a token.

That token might do any number of things. Most of the time, it provides some sort of access to the decentralized application, in the same way that bitcoin provides access to the Bitcoin blockchain (like if you want to send a payment across the globe).

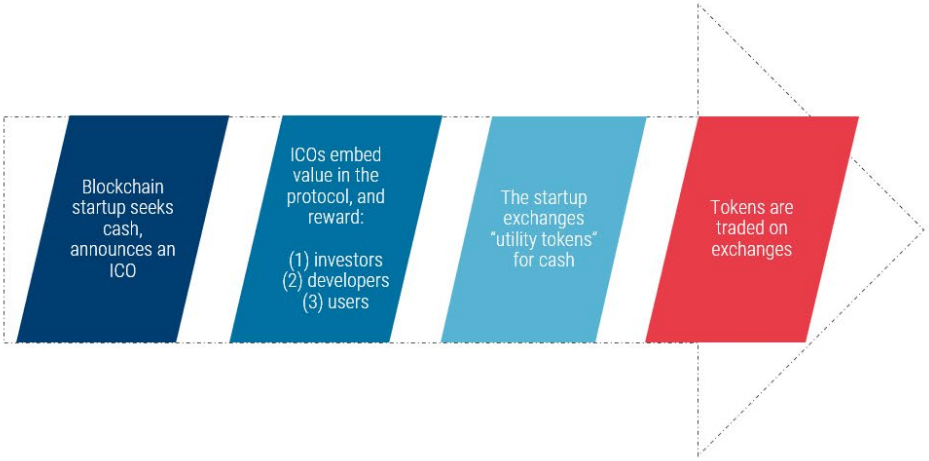
If a team issued a token for a decentralized social media platform, the team could mandate that a user needs to hold a token to access the platform. If demand for the platform goes up, then the token might rise in value.

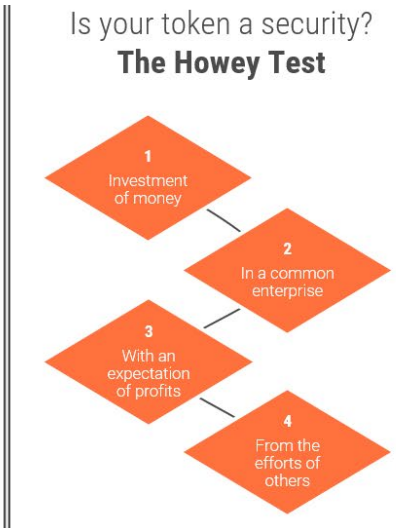
So, an ICO is simply:

- The sale of tokens by a blockchain company looking to raise funds.
- These tokens are often subsequently traded on cryptocurrency exchanges.

Investors in ICOs hope to turn a profit by buying early access to potentially foundational decentralized applications, just as early investors into bitcoin and ether did.

What's An ICO?





Why are ICOs so controversial?

Initial coin offerings could represent a big shift in how companies raise money and/or incentivize various stakeholders (e.g., developers, investors, users).

At the same time, ICOs are on shaky regulatory footing — in recent months, the SEC has become increasingly interested in highlighting misinformation about ICOs, and many have come under fire for a lack of transparency, no viable product, or even fraud.

If the SEC or other regulators ultimately rule that a given token is a security, then many of the teams behind these ICOs could be guilty of illegal securities offerings. The Howey Test, created by the Supreme Court in the 1940s to determine if certain transactions were classified as securities, is also commonly applied to ICOs.

According to this test, a transaction constitutes the purchase of a security if it satisfies the following four conditions:

- The transaction is an investment of money (or comparable financial instruments)
- The investment is entered into with an expectation of profit
- The investment of money (or comparable financial instruments)

is in a common enterprise

- Profit comes from the work of a third party or promoter

In February, 2018, SEC Chairman Jay Clayton said, "I want to go back to separating ICOs and cryptocurrencies. ICOs that are securities offerings, we should regulate them like we regulate securities offerings. End of story." At around the same time, the SEC subpoenaed a number of cryptocurrency hedge funds and organizations that held ICOs. You can read more about regulatory concerns **here.**

What are utility tokens?

Teams holding ICOs are adamant that they do not represent securities offerings and instead market their coins or tokens as part of an entirely new asset class altogether.

Again, let's use Bitcoin to illustrate.

Bitcoin is a token that provides ownership of a unit of account on the Bitcoin ledger. It is impossible to participate in the Bitcoin ledger without owning bitcoins; bitcoins are the network's exclusive means of exchange. In this sense, bitcoin isn't a security, but rather utility within a network. When teams call their tokens a "utility token" or "utility coin" to verbally distance themselves from securities law, this is what they're referencing.

However, many of these teams have yet to build functional networks for which their tokens would provide utility. Teams often present a whitepaper in lieu of an investment memorandum, product, or roadmap, and ICOs regularly raise upwards of $10M, stoking concerns of overcapitalization. Many of these companies could run the risk of mismanagement after receiving such large sums.

Bitcoin Cash

What is Bitcoin Cash?

Bitcoin Cash is not the same thing as Bitcoin, although it shares much of its history with that protocol.

Bitcoin Cash is a new network that "forked" from the Bitcoin network at the beginning of August 2017. In the blockchain space, a "fork" is what happens when developers in the network decide to materially change the code of the platform. Nodes, run by miners, can update to the new code — if enough nodes make the switch, it can become a completely new platform with its own token.

When a significant number of nodes running a protocol like Bitcoin agree to update to a new and significantly different software, it creates a new blockchain that (1) has the same history as the previous protocol leading up to the fork but (2) has a different history than the previous protocol following the fork.

Last year, a group of developers came to an agreement that the Bitcoin protocol was straying from what they saw as its primary function: serving as a ubiquitous, low-fee, fast-execution, peer-to-peer means of transferring value. They decided to fork Bitcoin in order to create a new cryptocurrency, Bitcoin Cash, that would be solely focused on serving as that kind of value transfer.

Why is Bitcoin Cash controversial?

Supporters of Bitcoin Cash and Bitcoin commonly spar over the functionality of the two coins.

While Bitcoin supporters identify the original blockchain as the "true" Bitcoin protocol and dismiss Bitcoin Cash, supporters of Bitcoin Cash claim that their protocol does a better job of fulfilling Bitcoin's initial goal of being peer-to-peer cash.

Why all the bad blood? There's a number of possible explanations, but a particularly promising one is about ensuring the long-term viability of the crypto sector.

When the Bitcoin community fragments and pulls users away from the main protocol with other blockchains (like Bitcoin Cash), some feel that it threatens the united front — in other words, a fractured space will make it more difficult for widespread adoption.

Why is Bitcoin Cash valuable?

Controversy aside, is the value proposition of Bitcoin Cash a sound one? Like the crypto sector at large, the price is highly volatile — the price of BCH has gone from ~$500 to a peak of just over $4,000 in late December 2017, before returning to the same ~$500 levels in September 2018.

Because Bitcoin Cash is focused on a single function — ubiquitous, low-fee, fast-execution, peer-to-peer value transfer — it could be valuable if merchants accept it as a form of value transfer, and consumers use it as such.

Bitcoin Cash has progressively been accepted by more merchants since its fork from Bitcoin. Recently, the thousands of merchants that use BitPay were given the option to accept Bitcoin Cash. More broadly, the Accept Bitcoin Cash Initiative tracks merchants, by industry, who accept Bitcoin Cash (as of 9/6/18, only 750 merchants accept the token as payment).

On the other hand, the number of transactions of the Bitcoin Cash network have been almost uniformly an order of magnitude less than the number of transactions on the Bitcoin network — in the past few months, Bitcoin has averaged around 200k transactions per day, whereas Bitcoin Cash has averaged around 20k.

Litecoin

What is Litecoin?

Another altcoin that's gradually entered the popular vernacular is Litecoin. It was invented in 2011 by former Google engineer Charlie Lee to act as cheaper and faster version of Bitcoin. It's a lower-priced cryptocurrency that's almost identical to Bitcoin — there are just a few minor tweaks that are intended to make it a more fitting tool for daily commerce.

In May 2017, Litecoin was listed on Coinbase, where Lee was a head engineer. It instantly became the fourth most valuable cryptocurrency in the world, and prices jumped 25% overnight.

Litecoin vs. Bitcoin: what's the difference?

Litecoin has an intended function that's identical to Bitcoin Cash, but with a different origin story. Both of these cryptocurrencies are designed for small, daily transactions, but Bitcoin Cash forked from Bitcoin while Litecoin was early spinoff that never relied on the Bitcoin blockchain — which probably explains why it isn't as controversial.

There are a couple of key differences between Litecoin and Bitcoin:

Litecoin has a different "hashing algorithm" than Bitcoin. This basically means that the kind of computational process that miners use to add new blocks in the blockchain is different.

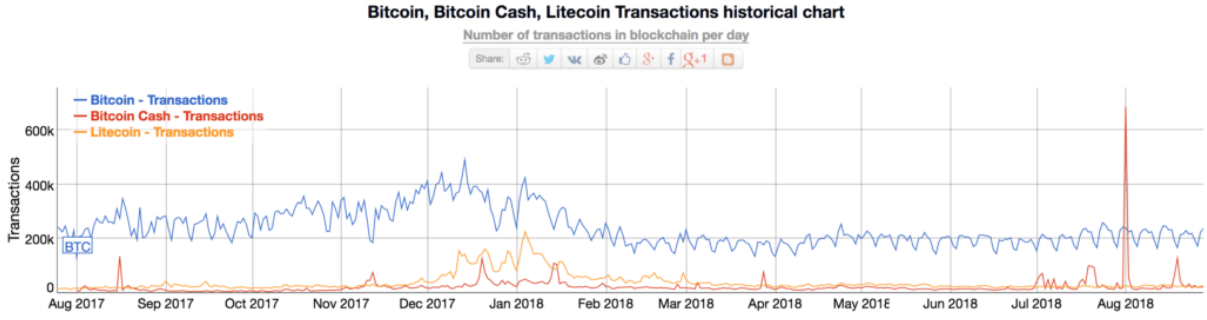
The upshot of this is that there are fewer highly specialized Litecoin mining pools than there are Bitcoin mining pools, making it more accessible for the population at large to mine (although specialized Litecoin-mining computers are now on the rise).

Litecoin is faster than Bitcoin. The altcoin adds new blocks added to its blockchain roughly every 2.5 minutes, in contrast to Bitcoin's 10 minute block frequency. In practice, this means that transactions can be confirmed more quickly on Litecoin than on Bitcoin.

Why is Litecoin valuable?

Compared to Bitcoin Cash, Litecoin has historically had slightly more transaction volume, but, like Bitcoin Cash, Litecoin is still an order of magnitude off from Bitcoin transaction volume.

Take a look at this chart to get a sense of how the three have stacked up in the last 13 months:



Daily transaction volume of Bitcoin (blue), Litecoin (orange), and Bitcoin Cash (red).

Worth noting, however, is the fact that Charlie Lee, the founder of Litecoin himself, sold all of his holdings in December 2017 due to a "conflict of interest."

As we've highlighted, blockchain is still in its nascent stages. However, blockchain technology promises various applications in money, middlemen, and trust.

The future

The future of blockchain technology

Ultimately, blockchain is as much a political and economic hypothesis as a technological one. Blockchain technology provides a new way to think about how we agree on things. For the first time, multiple untrusted parties can create and agree on a single source of truth, without the use of a middleman. The technology's implications for traditional middlemen and corporate players are therefore potentially enormous.

As the landscape evolves, the future of blockchain will likely take on forms yet to be imagined.