



# 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. Cryptocurrencies. Initial coin offerings.

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

As of this writing in mid-November 2017, the total market capitalization of cryptocurrencies hovers around \$220B (with a single bitcoin trading for upwards of \$8,000). Initial coin offerings (ICOs) have exploded in popularity, closing on \$3B+ in funding in 2017 alone. Huge corporations — like Walmart and Pfizer — have completed successful blockchain pilots.

This explainer will offer simple definitions and analogies for blockchain technology. It will also define Bitcoin, Ethereum, blockchain broadly, and initial coin offerings, and highlight promising use cases for the technology.

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**

---

1. **What Is Bitcoin?**
2. **What Is Blockchain?**
3. **What Is Ethereum?**
4. **Closing Remarks**

# 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 was a “peer-to-peer electronic cash system.” It would allow for online payments [to move] 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



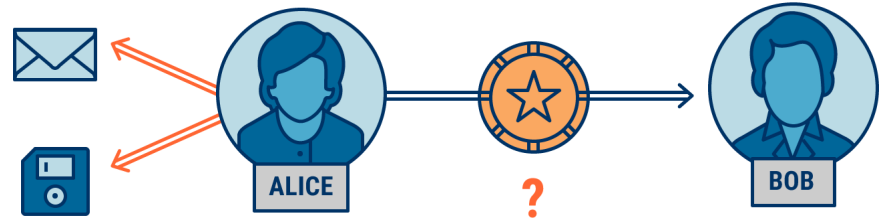
Here's a scenario: Alice hands Bob a physical arcade token. Bob now has one token, and Alice has zero. The transaction is complete. Alice and Bob do not need an intermediary to verify the transaction. Alice can't give Charlie the same token, because she no longer has the token to give – she gave it to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



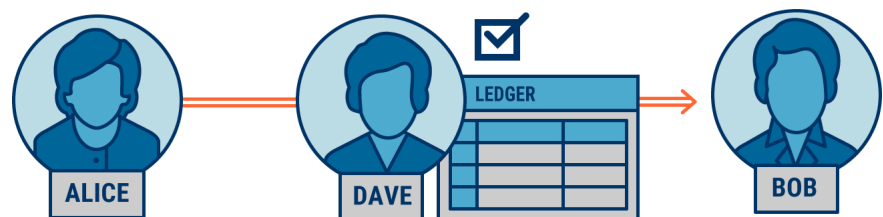
If Alice and Bob “own” the same string of ones and zeros, who is the true owner of the digital token? If digital assets can be reproduced so easily, what stops Alice from trying to “spend” the same digital asset twice by also sending it to Charlie?

How can Alice and Bob establish unique ownership over the digital token?

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.

A trusted third party, an intermediary — let’s call him Dave — will hold the ledger and make sure that it’s up-to-date. Alice can’t hold the ledger because she might erase the transaction and say that she still owns the digital token, although 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.

## Digital Transaction: Ledger



By default, Dave — who is not involved in the transaction at all, will have to control the ledger. Dave is trusted.

This situation is fine, until it’s not.

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

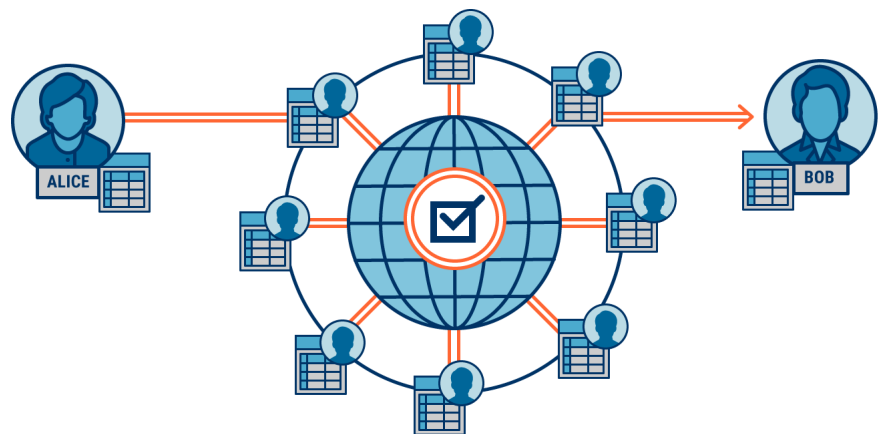
gave him the token?

*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.

## Is Bitcoin Really Secure?

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 priced at upwards of \$8,000, 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 daily energy consumption at greater than Ecuador's, a country of 17M people.

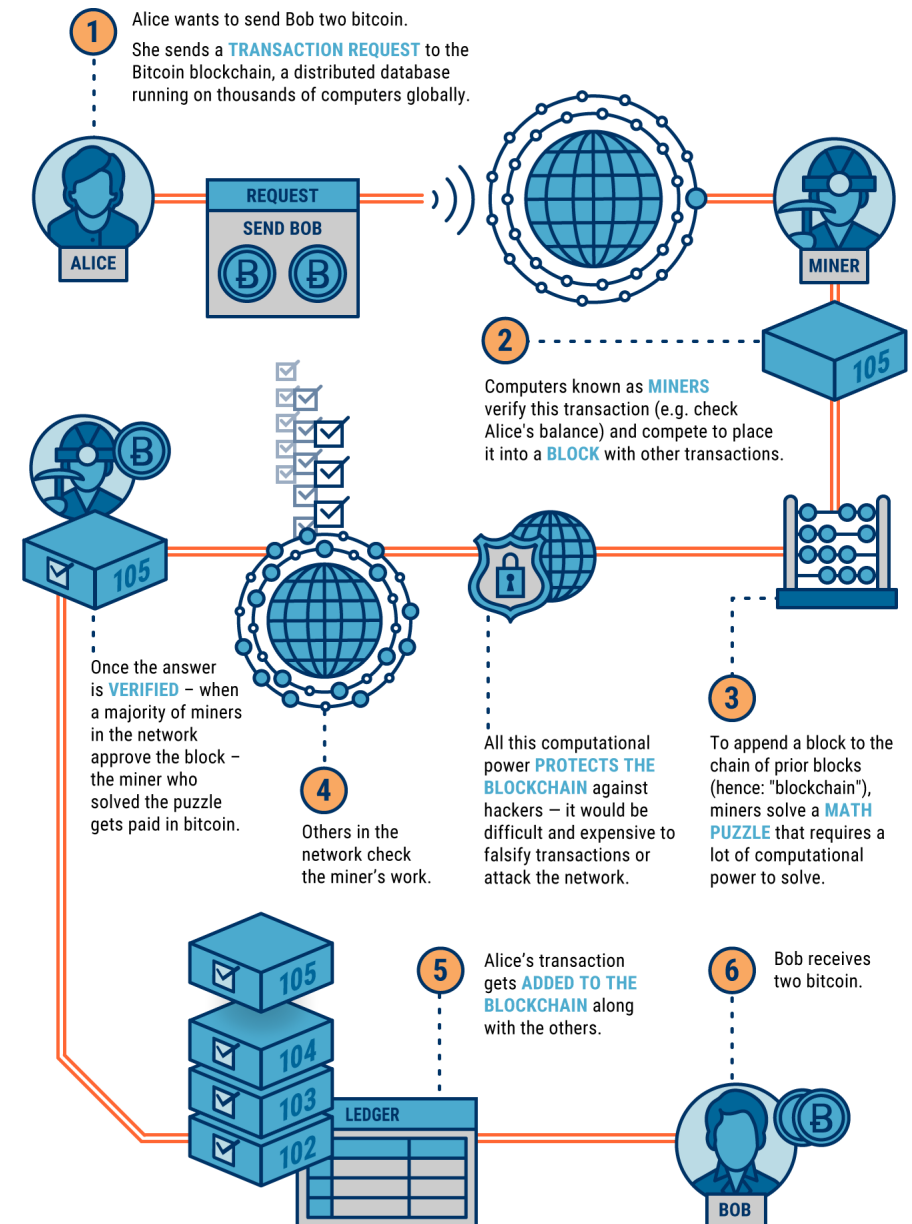
---

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?

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 blockchain 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 above \$8,000 in recent weeks. If you had invested \$100 in bitcoin in 2011 that bitcoin would be worth over \$2.5M today.

As discussed, Bitcoin's "blockchain" allows for the creation of a unique and scarce digital asset where everyone knows the history of each bitcoin. A single bitcoin is not just a string of ones and zeros, but 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). You can do the math, but as of this writing investors value bitcoin at upwards of \$120B 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 11/08/2017



Bitcoin



Ethereum



Litecoin



Dash



Monero

	Bitcoin	Ethereum	Litecoin	Dash	Monero
Price (\$)	\$ 7,200.00	\$ 315.00	\$ 62.00	\$ 308.00	\$ 107.00
Market Capitalization (\$B)	\$ 119.95	\$ 30.15	\$ 3.36	\$ 2.37	\$ 1.65
Transactions last 24h	308,097.00	471,778.00	28,546.00	6,585.00	5,133.00
Avg. Transaction Value	16.36 BTC	24.57 ETH	1,259 LTC	26.96 DASH	
Avg. Block Time	9m 28s	13.7s	2m 34s	2m 37s	1m 56s
Total Blocks	493,667	4,515,690	1,309,524	767,460	1,438,645
Blocks Last 24 Hours	151	6290	562	550	743
Avg. Blocks per Hour	6	262	23	23	31
Current Reward Per Block	12.50 BTC	3 ETH	25 LTC	3.60 DASH	5.95 XMR
First Block	1/9/2009	7/30/2015	10/8/2011	1/19/2014	4/18/2014

## A Caveat

There's lots more to Bitcoin that we're not going to get into. Hashes, public-private key encryption, segregated witness, sidechains, forks, and block size, 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.

Specifically, a blockchain is needed for Bitcoin because:

- » 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 could be 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?*

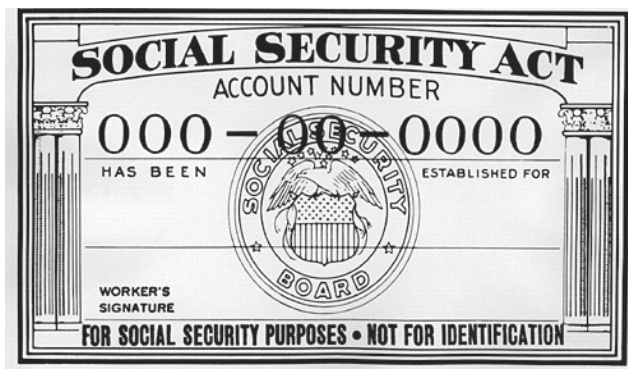
A couple of immediate use cases come to mind.

**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, but 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. Let's think about why this makes sense.*

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.

**Identity** might also be low-hanging fruit. The recent 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 proudly 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.

The applications for blockchain technology extend well beyond these two 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 (or miners to verify and append transactions to the cryptographically-protected blockchain).

Without blockchain's verification step, we're left with a "distributed ledger," basically 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 Bitcoin.

It's important to make this distinction.

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's 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's 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. This means 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 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?

Blockchains are really good at a couple of things and absolutely awful at others.

We've addressed the distributed ledger versus blockchain debate above. Another major issue is scaling blockchains.

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, blockchains face scaling issues. Bitcoin can process about 3-4 transactions per second. Ethereum maxes out at about 20 transactions per second. Visa can process over 1,500 transactions per second.

Scaling is just one of the issues facing blockchain technology, but it's an important one.

# 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



### EXCHANGES & WALLETS



### BROWSERS & SOCIAL



### MEDIA & ADVERTISING



### TRADING



### CROWDFUNDING & LENDING



### GAMBLING & GAMING



### DAO & TOKEN LAUNCH



### PREDICTION MARKETS



### HEALTHCARE & INSURANCE



### INFRASTRUCTURE & DEVELOPMENT



### COMPUTING & STORAGE



### IDENTITY & INTERNET OF THINGS



### PAYMENTS & BANKING



### OTHER



### FINANCIAL SERVICES



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

## 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, yet, 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 Ethereum Worth More Than \$300?

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.

Ether’s dollar value is subject to the supply-and-demand mechanics found in any marketplace. If investors find the Ethereum blockchain valuable – and developers are building decentralized applications – then demand for ether might rise and its price could rise. The opposite could also happen.

## 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, e.g. if you want to use it to send a payment to someone across the planet.

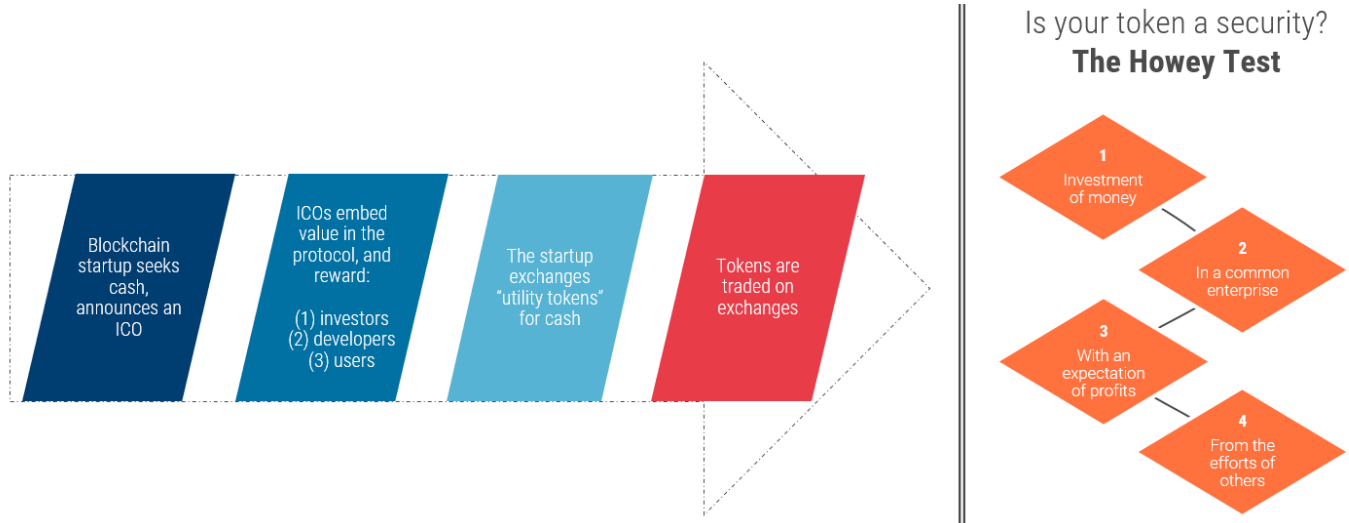
If a team issued a token for a decentralized social media platform, the team could mandate that a user needs to hold a token to access the platform. If demand for the platform goes up, then the token might rise in value.

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 ethereum 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 (developers, investors, users).

At the same time, ICOs are on shaky regulatory footing — if the SEC or other regulators ultimately deem these tokens securities, then many of the teams behind these ICOs could be guilty of illegal securities offerings.

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 bitcoin; bitcoin is the network's exclusive means of exchange. In this sense, bitcoin isn't a security, but utility within a network.

However, many of these teams have yet to build functional networks. Teams often present a white paper 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.

## Closing Remarks

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

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.