

What is Blockchain Technology? A Step-by-Step Guide For Beginners

An in-depth guide by BlockGeeks

Join over 115,115 Members

Angel Investors, Startups & Blockchain developers...

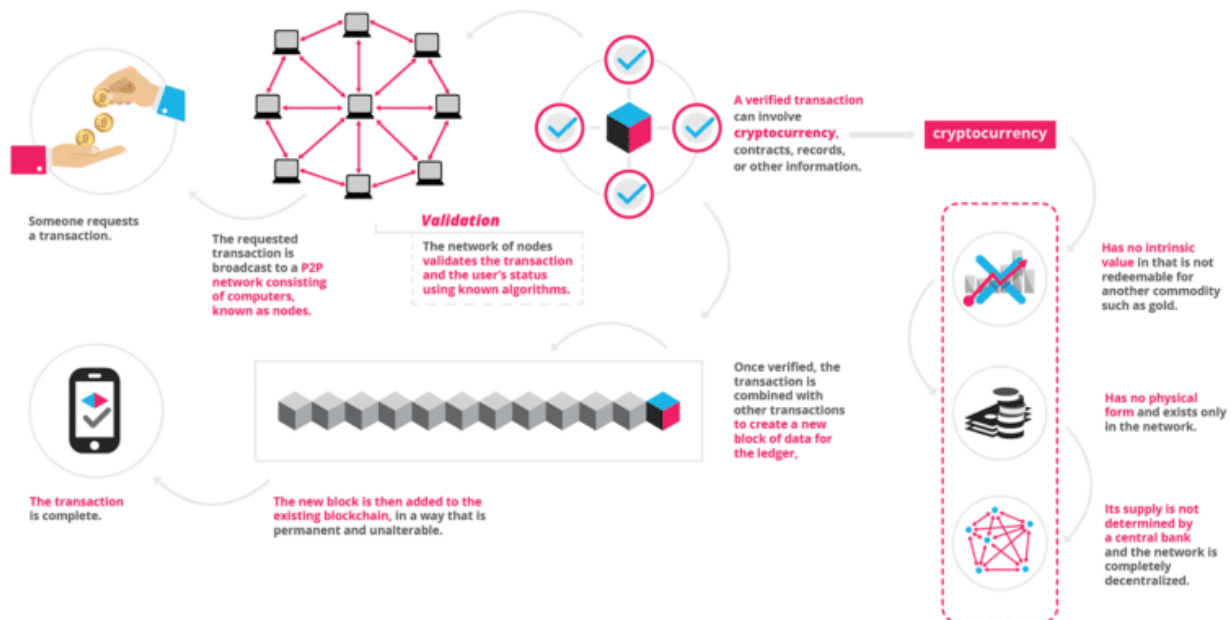
No Thanks!

Is blockchain technology the new internet?

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, [Satoshi Nakamoto](#). But since then, it has evolved into something greater, and the main question every single person is asking is: What is Blockchain?

By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the [digital currency, Bitcoin](#), the tech community is now finding other potential uses for the technology.

Bitcoin has been called “digital gold,” and for a good reason. To date, the total value of the currency is close to \$9 billion US. And blockchains can make other types of digital value. Like the internet (or your car), you don’t need to know how the blockchain works to use it. However, having a basic knowledge of this new technology shows why it’s considered revolutionary. So, we hope you enjoy this, what is Blockchain guide.



What is Blockchain Technology?



A distributed database

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this

information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

To go in deeper with the Google spreadsheet analogy, I would like you to read this piece from a blockchain specialist.

Blockchain as Google Docs



“The traditional way of sharing documents with collaboration is to send a Microsoft Word document to another recipient, and ask them to make revisions to it. The problem with that scenario is that you need to wait until receiving a return copy before you can see or make other changes **because you are locked out of editing it until the other person is done with it. That’s how databases work today. Two owners can’t be messing with the same record at once.** That’s how banks maintain money balances and transfers; they briefly lock access (or decrease the balance) while they make a transfer, then update the other side, then re-open access (or update again). With Google Docs (or Google Sheets), both parties have access to the same document at the same time, and the single version of that document is always visible to both of them. It is like a shared ledger, but it is a shared document. The distributed part comes into play when sharing involves a number of people.

Imagine the number of legal documents that should be used that

way. Instead of passing them to each other, losing track of versions, and not being in sync with the other version, why can't *all* business documents become shared instead of transferred back and forth? So many types of legal contracts would be ideal for that kind of workflow. You don't need a blockchain to share documents, but the shared documents analogy is a powerful one."

[William Mougayar, Venture advisor, 4x entrepreneur, marketer, strategist and blockchain specialist](#)

Blockchain Durability and robustness

Blockchain technology is like the internet in that it has a built-in robustness. By storing blocks of information that are identical across its network, the blockchain cannot:

1. Be controlled by any single entity.
2. Has no single point of failure.

Bitcoin was invented in 2008. Since that time, the Bitcoin blockchain has operated without significant disruption. (To date, any of problems associated with Bitcoin have been due to hacking or mismanagement. In other words, these problems come from bad intention and human error, not flaws in the underlying concepts.)

The internet itself has proven to be durable for almost 30 years. It's a track record that bodes well for blockchain technology as it continues to be developed.



“As revolutionary as it sounds, Blockchain truly is a mechanism to bring everyone to the highest degree of accountability. No more missed transactions, human or machine errors, or even an exchange that was not done with the consent of the parties involved. Above anything else, the most critical area where Blockchain helps is to guarantee the validity of a transaction by recording it not only on a main register but a connected distributed system of registers, all of which are connected through a secure validation mechanism.”

– [Ian Khan, TEDx Speaker](#) | Author | Technology Futurist

Transparent and incorruptible

The blockchain network lives in a state of consensus, one that automatically checks in with itself every ten minutes. A kind of self-auditing ecosystem of a digital value, the network reconciles every transaction that happens in ten-minute intervals. Each group of these transactions is referred to as a “block”. Two important properties result from this:

1. **Transparency** data is embedded within the network as a whole, by definition it is public.
2. **It cannot be corrupted** altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.

In theory, this could be possible. In practice, it's unlikely to happen. Taking control of the system to capture Bitcoins, for instance, would also have the effect of destroying their value.

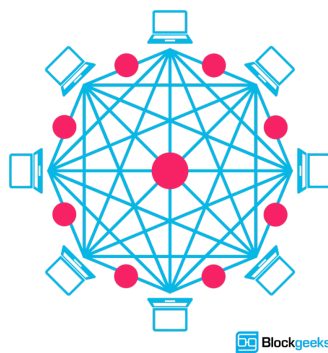


"Blockchain solves the problem of manipulation. When I speak about it in the West, people say they trust Google, Facebook, or their banks. But the rest of the world doesn't trust organizations and corporations that much — I mean Africa, India, the Eastern Europe, or Russia. It's not about the places where people are really rich. Blockchain's opportunities are the highest in the countries that haven't reached that level yet."

[Vitalik Buterin, inventor of Ethereum](#)

A network of nodes

A network of so-called computing "nodes" make up the blockchain.



Node

(computer connected to the blockchain network using a client that performs the task of validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the blockchain network.

Together they create a powerful second-level network, a wholly different vision for how the internet can function.

Every node is an “administrator” of the blockchain, and joins the network voluntarily (in this sense, the network is decentralized). However, each one has an incentive for participating in the network: the chance of winning Bitcoins.

Nodes are said to be “mining” Bitcoin, but the term is something of a misnomer. In fact, each one is competing to win Bitcoins by solving computational puzzles. Bitcoin was the *raison d’être* of the blockchain as it was originally conceived. It’s now recognized to be only the first of many potential applications of the technology.

There are an estimated 700 Bitcoin-like [cryptocurrencies](#) (exchangeable value tokens) already available. As well, a range of other potential adaptations of the original blockchain concept are currently active, or in development.



The idea of decentralization

By design, the blockchain is a decentralized technology.

Anything that happens on it is a function of the network as a whole. Some important implications stem from this. By creating a new way to verify transactions aspects of traditional commerce could become unnecessary. Stock market trades become almost simultaneous on the blockchain, for instance — or it could make types of record keeping, like a land registry, fully public. And decentralization is already a reality.

A global network of computers uses blockchain technology to jointly manage the database that records Bitcoin transactions. That is, Bitcoin is managed by its network, and not any one central authority. Decentralization means the network operates on a user-to-user (or peer-to-peer) basis. The forms of mass collaboration this makes possible are just beginning to be investigated.



Who will use the blockchain?

As web infrastructure, you don't need to know about the blockchain for it to be useful in your life.

Currently, finance offers the strongest use cases for the technology. International remittances, for instance. The World Bank estimates that over \$430 billion US in money transfers were sent in 2015. And at the moment there is a [high demand for blockchain developers](#).

The blockchain potentially cuts out the middleman for these types of transactions. Personal computing became accessible to the general public with the invention of the Graphical User Interface (GUI), which took the form of a “desktop”. Similarly, the most common GUI devised for the blockchain are the so-called “wallet” applications, which people use to buy things with Bitcoin, and store it along with other cryptocurrencies.

Transactions online are closely connected to the processes of identity verification. It is easy to imagine that wallet apps will transform in the coming years to include other types of identity management.



The Blockchain & Enhanced security

By storing data across its network, the blockchain eliminates the risks that come with data being held centrally.

Its network lacks centralized points of vulnerability that computer hackers can exploit. Today’s internet has security problems that are familiar to everyone. We all rely on the “username/password” system to protect our identity and assets online. Blockchain security methods use encryption technology.

The basis for this are the so-called public and private “keys”. A “public key” (a long, randomly-generated string of numbers) is a

users' address on the blockchain. Bitcoins sent across the network gets recorded as belonging to that address. The "private key" is like a password that gives its owner access to their Bitcoin or other digital assets. Store your data on the blockchain and it is incorruptible. This is true, although protecting your digital assets will also require safeguarding of your private key by printing it out, creating what's referred to as a paper wallet.

Centralized



Decentralized



Distributed Ledgers



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the ledger and participates in confirming transactions independently

- Users (●) are not anonymous

- Permission is required for users to have a copy of the ledger and participate in confirming transactions



A second-level network

With blockchain technology, the web gains a new layer of functionality.

Already, users can transact directly with one another — Bitcoin transactions in 2016 averaged over \$200,000 US per day. With the added security brought by the blockchain new internet business are on track to unbundle the traditional institutions of finance.

Goldman Sachs believes that blockchain technology holds great

potential especially to optimize clearing and settlements, and could represent global savings of up to \$6bn per year.



“2017 will be a pivotal year for blockchain tech. Many of the startups in the space will either begin generating revenue – via providing products the market demands/values – or vaporize due to running out of cash. In other words, 2017 should be the year where there is more implementation of products utilizing blockchain tech, and less talk about blockchain tech being the magical pixie dust that can just be sprinkled atop everything. Of course, from a customers viewpoint, this will not be obvious as blockchain tech should dominantly be invisible – even as its features and functionality improve peoples’/business’ lives. I personally am familiar with a number of large-scale blockchain tech use cases that are launching soon/2017. This implementation stage, which 2017 should represent, is a crucial step in the larger adoption of blockchain tech, as it will allow skeptics to see the functionality, rather than just hear of its promise.”

– [George Howard](#), Associate Professor Brown University, Berklee College of Music and Founder of George Howard Strategic

The Blockchain a New Web 3.0?

The blockchain gives internet users the ability to create value and

authenticates digital information. What will new business applications result?

- **[Smart contracts](#)**

Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met. [Ethereum](#) is an open source blockchain project that was built specifically to realize this possibility. Still, in its early stages, Ethereum has the potential to leverage the usefulness of blockchains on a truly world-changing scale.

At the technology's current level of development, smart contracts can be programmed to perform simple functions. For instance, a derivative could be paid out when a financial instrument meets certain benchmark, with the use of blockchain technology and Bitcoin enabling the payout to be automated.

- **The sharing economy**

With companies like Uber and AirBnB flourishing, the sharing economy is already a proven success. Currently, however, users who want to hail a ride-sharing service have to rely on an intermediary like Uber. By enabling peer-to-peer payments, the blockchain opens the door to direct interaction between parties — a truly decentralized sharing economy results.

An early example, [OpenBazaar](#) uses the blockchain to create a peer-to-peer eBay. Download the app onto your computing device, and you can transact with OpenBazaar vendors without paying transaction fees. The "no rules" ethos of the protocol means that personal reputation will be even more important to

business interactions than it currently is on eBay.

- **Crowdfunding**

Crowdfunding initiatives like Kickstarter and Gofundme are doing the advance work for the emerging peer-to-peer economy. The popularity of these sites suggests people want to have a direct say in product development. Blockchains take this interest to the next level, potentially creating crowd-sourced venture capital funds.

In 2016, one such experiment, the [Ethereum](#)-based DAO (Decentralized Autonomous Organization), raised an astonishing \$200 million USD in just over two months. Participants purchased "DAO tokens" allowing them to vote on smart contract venture capital investments (voting power was proportionate to the number of DAO they were holding). A subsequent hack of project funds proved that the project was launched without proper due diligence, with disastrous consequences. Regardless, the DAO experiment suggests the blockchain has the potential to usher in "a new paradigm of economic cooperation."

- **Governance**

By making the results fully transparent and publicly accessible, distributed database technology could bring full transparency to elections or any other kind of poll taking. Ethereum-based smart contracts help to automate the process.

The app, Boardroom, enables organizational decision-making to happen on the blockchain. In practice, this means company governance becomes fully transparent and verifiable when

managing digital assets, equity or information.

- **Supply chain auditing**

Consumers increasingly want to know that the ethical claims companies make about their products are real. Distributed ledgers provide an easy way to certify that the backstories of the things we buy are genuine. Transparency comes with blockchain-based timestamping of a date and location — on ethical diamonds, for instance — that corresponds to a product number.

The UK-based Provenance offers supply chain auditing for a range of consumer goods. Making use of the Ethereum blockchain, a Provenance pilot project ensures that fish sold in Sushi restaurants in Japan has been sustainably harvested by its suppliers in Indonesia.

- **File storage**

Decentralizing file storage on the internet brings clear benefits. Distributing data throughout the network protects files from getting hacked or lost.

Inter Planetary File System (IPFS) makes it easy to conceptualize how a distributed web might operate. Similar to the way a bittorrent moves data around the internet, IPFS gets rid of the need for centralized client-server relationships (i.e., the current web). An internet made up of completely decentralized websites has the potential to speed up file transfer and streaming times. Such an improvement is not only convenient. It's a necessary upgrade to the web's currently overloaded content-delivery systems.

- **Prediction markets**

The crowdsourcing of predictions on event probability is proven to have a high degree of accuracy. Averaging opinions cancels out the unexamined biases that distort judgment. Prediction markets that payout according to event outcomes are already active. Blockchains are a “wisdom of the crowd” technology that will no doubt find other applications in the years to come.

Still, in Beta, the prediction market application [Augur](#) makes share offerings on the outcome of real-world events.

Participants can earn money by buying into the correct prediction. The more shares purchased in the correct outcome, the higher the payout will be. With a small commitment of funds (less than a dollar), anyone can ask a question, create a market based on a predicted outcome, and collect half of all transaction fees the market generates.

- **Protection of intellectual property**

As is well known, digital information can be infinitely reproduced — and distributed widely thanks to the internet. This has given web users globally a goldmine of free content. However, copyright holders have not been so lucky, losing control over their intellectual property and suffering financially as a consequence. Smart contracts can protect copyright and automate the sale of creative works online, eliminating the risk of file copying and redistribution.

Mycelia uses the blockchain to create a peer-to-peer music distribution system. Founded by the UK singer-songwriter Imogen Heap, Mycelia enables musicians to sell songs directly to audiences, as well as license samples to producers and divvy

up royalties to songwriters and musicians — all of these functions being automated by smart contracts. The capacity of blockchains to issue payments in fractional cryptocurrency amounts (micropayments) suggests this use case for the blockchain has a strong chance of success.

- **[Internet of Things \(IoT\)](#)**

What is the IoT? The network-controlled management of certain types of electronic devices — for instance, the monitoring of air temperature in a storage facility. Smart contracts make the automation of remote systems management possible. A combination of software, sensors, and the network facilitates an exchange of data between objects and mechanisms. The result increases system efficiency and improves cost monitoring.

The biggest players in manufacturing, tech and telecommunications are all vying for IoT dominance. Think Samsung, IBM and AT&T. A natural extension of existing infrastructure controlled by incumbents, IoT applications will run the gamut from predictive maintenance of mechanical parts to data analytics, and mass-scale automated systems management.

- **Neighbourhood Microgrids**

Blockchain technology enables the buying and selling of the renewable energy generated by neighborhood microgrids. When solar panels make excess energy, Ethereum-based smart contracts automatically redistribute it. Similar types of smart contract automation will have many other applications as the IoT becomes a reality.

Located in Brooklyn, [Consensys](#) is one of the foremost companies globally that is developing a range of applications for Ethereum. One project they are partnering on is Transactive Grid, working with the distributed energy outfit, LO3. A prototype project currently up and running uses Ethereum smart contracts to automate the monitoring and redistribution of microgrid energy. This so-called “intelligent grid” is an early example of IoT functionality.

- **Identity management**

There is a definite need for better identity management on the web. The ability to verify your identity is the lynchpin of financial transactions that happen online. However, remedies for the security risks that come with web commerce are imperfect at best. Distributed ledgers offer enhanced methods for proving who you are, along with the possibility to digitize personal documents. Having a secure identity will also be important for online interactions — for instance, in the sharing economy. A good reputation, after all, is the most important condition for conducting transactions online.

Developing digital identity standards is proving to be a highly complex process. Technical challenges aside, a universal online identity solution requires cooperation between private entities and government. Add to that the need to navigate legal systems in different countries and the problem becomes exponentially difficult. E-Commerce on the internet currently relies on the SSL certificate (the little green lock) for secure transactions on the web. Netki is a startup that aspires to create an SSL standard for the blockchain. Having recently announced a \$3.5 million seed round, Netki expects a product

launch in early 2017.

- **AML and KYC**

Anti-money laundering (AML) and know your customer (KYC) practices have a strong potential for being adapted to the blockchain. Currently, financial institutions must perform a labour intensive multi-step process for each new customer. KYC costs could be reduced through cross-institution client verification, and at the same time increase monitoring and analysis effectiveness.

Startup Polycoin has an AML/KYC solution that involves analysing transactions. Those transactions identified as being suspicious are forwarded on to compliance officers. Another startup Tradle is developing an application called Trust in Motion (TiM). Characterized as an “Instagram for KYC”, TiM allows customers to take a snapshot of key documents (passport, utility bill, etc.). Once verified by the bank, this data is cryptographically stored on the blockchain.

- **Data management**

Today, in exchange for their personal data people can use social media platforms like Facebook for free. In future, users will have the ability to manage and sell the data their online activity generates. Because it can be easily distributed in small fractional amounts, Bitcoin — or something like it — will most likely be the currency that gets used for this type of transaction.

The MIT project Enigma understands that user privacy is the key precondition for creating of a personal data marketplace.

Enigma uses cryptographic techniques to allow individual data sets to be split between nodes, and at the same time run bulk computations over the data group as a whole. Fragmenting the data also makes Enigma scalable (unlike those blockchain solutions where data gets replicated on every node). A Beta launch is promised within the next six months.

- **Land title registration**

As Publicly-accessible ledgers, blockchains can make all kinds of record-keeping more efficient. Property titles are a case in point. They tend to be susceptible to fraud, as well as costly and labour intensive to administer.

A number of countries are undertaking blockchain-based land registry projects. Honduras was the first government to announce such an initiative in 2015, although the current status of that project is unclear. This year, the Republic of Georgia cemented a deal with the Bitfury Group to develop a blockchain system for property titles. Reportedly, Hernando de Soto, the high-profile economist and property rights advocate, will be advising on the project. Most recently, Sweden announced it was experimenting with a blockchain application for property titles.

- **Stock trading**

The potential for added efficiency in share settlement makes a strong use case for blockchains in stock trading. When executed peer-to-peer, trade confirmations become almost instantaneous (as opposed to taking three days for clearance). Potentially, this means intermediaries — such as the clearing house, auditors and custodians — get removed from the

process.

Numerous stock and commodities exchanges are prototyping blockchain applications for the services they offer, including the ASX (Australian Securities Exchange), the Deutsche Börse (Frankfurt's stock exchange) and the JPX (Japan Exchange Group). Most high profile because the acknowledged first mover in the area, is the Nasdaq's Linq, a platform for private market trading (typically between pre-IPO startups and investors). A partnership with the blockchain tech company Chain, Linq announced the completion of its first share trade in 2015. More recently, Nasdaq announced the development of a trial blockchain project for proxy voting on the Estonian Stock Market.

Web 3.0

The blockchain gives internet users the ability to create value and authenticate digital information. What new business applications will result?



Smart contracts

Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met.



The sharing economy

By enabling peer-to-peer payments, the blockchain opens the door to direct interaction between parties – a truly decentralized sharing economy results.



Crowd funding

Blockchains take this interest to the next level, potentially creating crowd-sourced venture capital funds.



Governance

By making the results fully transparent and publically accessible, distributed database technology could bring full transparency to elections or any other kind of poll taking.



Supply chain auditing

Distributed ledgers provide an easy way to certify that the backstories of the things we buy are genuine. Transparency comes with blockchain-based timestamping of a date and location – on ethical diamonds, for instance – that corresponds to a product number.



File storage

Decentralizing file storage on the internet brings clear benefits. Distributing data throughout the network protects files from getting hacked or lost.



Prediction markets



Prediction markets that pay out according to event outcomes are already active. Blockchains are a “wisdom of the crowd” technology that will no doubt find other applications in the years to come.



Protection of intellectual property

Smart contracts can protect copyright and automate the sale of creative works online, eliminating the risk of file copying and redistribution.



Internet of Things (IoT)

Smart contracts make the automation of remote systems management possible. A combination of software, sensors, and the network facilitates an exchange of data between objects and mechanisms.



Neighbourhood Microgrids

Blockchain technology enables the buying and selling of the renewable energy generated by neighbourhood microgrids.



Identity management

Distributed ledgers offer enhanced methods for proving who you are, along with the possibility to digitize personal documents. Having a secure identity will also be important for online interactions – for instance, in the sharing economy.



AML and KYC

Anti-money laundering (AML) and know your customer (KYC) practices have a strong potential for being adapted to the blockchain. Currently, financial institutions must perform a labour intensive multi-step process for each new customer. KYC costs could be reduced through cross-institution client verification, and at the same time increase monitoring and analysis effectiveness.



Data management

In the future, users will have the ability to manage and sell the data their online activity generates. Because it can be easily distributed in small fractional amounts, Bitcoin – or something like it.



Land title registration

As Publicly-accessible ledgers, blockchains can make all kinds of record-keeping more efficient. Property titles are a case in point. They tend to be susceptible to fraud, as well as costly and labour intensive to administer.



Stock trading

When executed peer-to-peer, trade confirmations become almost instantaneous. This means intermediaries – such as the clearing house, auditors and custodians – get removed from the process.



[Save](#)



“2016 was the year in which blockchain theory achieved general acceptance, but remained in theory, with the big players lingering around the hoop waiting to see who would take the first shot. As the year comes to an end, blockchain technology is tantalizingly close to turning the corner and entering the realm of small-scale commercial ability. Overall, 2017 is going to be the year of the very well-considered and well-funded proof of concept, with a few projects achieving revenue positive status. Venture investment is going to continue to be substantial but less than we saw in 2016 and 2015. I’d predict one or two exits by acquisition.”

– [Judd Bagley](#) Director of Communications at [Overstock.com](#) and Chief Evangelist at [t0.com](#)

Join over 115,115 Members

Angel Investors, Startups & Blockchain developers...

No Thanks!

Join the conversation