**How does the Blockchain Work? (Part 1)**

## **A simple and easy explanation**

## Source: <https://medium.com/blockchain-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093>

Well here is a simple explanation that cuts through the hype.

Blockchain is a hot topic around the world these days, yet for many, the technology remains an elusive concept. Yet it shouldn’t, the concept is simple once you get your head around the architecture and theory of basic crypto economics. When you do have your “a Ha” moment, the world will never seem the same to you again.

This blockchain basics guide is designed to deliver a clear, non-technical introduction to one of the most transformational & misunderstood technologies of our time. If you want to know what blockchain technology is, how it works, and it’s potential impacts, without all the technical lingo, then this post is for you.

### **A short History of Transacting Money**

Historically, when it comes to transacting money or anything of value, people and businesses have relied heavily on intermediaries like banks and governments to ensure trust and certainty.[[1](http://www.weforum.org/agenda/2016/06/blockchain-explained-simply/)] Middlemen perform a range of important tasks that help build trust into the transactional process like authentication & record keeping.

The need for intermediaries is especially acute when making a digital transaction. Because digital assets like money, stocks & intellectual property, are essentially files, they are incredibly easy to reproduce. This creates what’s known as the double spending problem (the act of spending the same unit of value more than once) which until now has prevented the peer to peer transfer of digital assets.

But what if there was a way of conducting digital transactions without a third party intermediary? Well, a new technology exists today that makes this possible. But before we dive into the mechanics of this revolutionary technology, it’s important to provide a little context.

### **Blockchain Vs Bitcoin — What’s the connection?**

Bitcoin first appeared in a 2008 white paper authored by a person, or persons using the pseudonym Satoshi Nakamoto. The [white paper](https://s3-us-east-2.amazonaws.com/br-media/wp-content/uploads/2017/08/31062510/bitcoin.pdf) detailed an innovative peer to peer electronic cash system called Bitcoin that enabled online payments to be transferred directly, without an intermediary.[[4](https://s3-us-east-2.amazonaws.com/br-media/wp-content/uploads/2017/08/31062510/bitcoin.pdf)]



How the blockchain transfers value

Via ([techliberation.com](https://www.google.com/url?q=https://techliberation.com/2013/12/04/why-would-anyone-use-bitcoin-when-paypal-or-visa-work-perfectly-well/&sa=D&ust=1475458755284000&usg=AFQjCNHkJE4m8WZhNx5s5tHVl0GLvbNqkQ))

While the proposed bitcoin payment system was exciting and innovative, it was the mechanics of how it worked that was truly revolutionary. Shortly after the white paper’s release, it became evident that the main technical innovation was not the digital currency itself but the technology that lay behind it, known today as blockchain.

Although commonly associated with Bitcoin, blockchain technology has many other applications. Bitcoin is merely the first and most well-known uses. In fact, Bitcoin is only one of about seven hundred applications that use the blockchain operating system today.[[5](https://www.youtube.com/watch?v=3lMvo0PPxjQ)]

**“[Blockchain] is to Bitcoin, what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one.” [**[**6**](http://video.ft.com/4029769033001/How-bitcoin-and-its-blockchain-work/Companies)**] — Sally Davies, FT Technology Reporter**

One example of the evolution and broad application of blockchain, beyond digital currency, is the development of the Ethereum public blockchain, which is providing a way to execute peer to peer contracts.[[7](https://www.cointelegraph.com/ethereum-for-beginners/what-is-ethereum)]

### **What’s under the blockchain hood?**

Simply put, a blockchain is a type of distributed ledger or decentralized database that keeps continuously updated digital records of who owns what. Rather than having a central administrator like a traditional database, (think banks, governments & accountants), a [distributed ledger](https://www.youtube.com/watch?v=oSP-taqLWPQ&feature=youtu.be) has a network of replicated databases, synchronized via the internet and visible to anyone within the network.[[8]](https://docs.google.com/document/d/1AjE5YERVCExXnyeYfYEZAdtGCocubCDQY9fhLwPyvJ4/pub#ftnt8) Blockchain networks can be [private with restricted membership similar to an intranet, or public](https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/), like the Internet, accessible to any person in the world.[[9](https://www.youtube.com/watch?v=3lMvo0PPxjQ)] [[10](https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/)]

When a digital transaction is carried out, it is grouped together in a cryptographically protected block with other transactions that have occurred in the last 10 minutes and sent out to the entire network. Miners (members in the network with high levels of computing power) then compete to validate the transactions by solving complex coded problems.[[11](https://www.linkedin.com/pulse/what-blockchain-why-so-important-mark-van-rijmenam)] The first miner to solve the problems and validate the block receives a reward. (In the Bitcoin Blockchain network, for example, a miner would receive Bitcoins).

The validated block of transactions is then timestamped and added to a chain in a linear, chronological order. New blocks of validated transactions are linked to older blocks, making a chain of blocks that show every transaction made in the history of that blockchain.[[12](http://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business/transcript?language=en)] The entire chain is continually updated so that every ledger in the network is the same, giving each member the ability to prove who owns what at any given time.

**“A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.” — Vitalik Buterin**

Blockchain’s decentralized, open & cryptographic nature allow people to trust each other and transact peer to peer, making the need for intermediaries obsolete. This also brings unprecedented security benefits. Hacking attacks that commonly impact large centralized intermediaries like banks would be virtually impossible to pull off on the blockchain. For example — if someone wanted to hack into a particular block in a blockchain, a hacker would not only need to hack into that specific block, but all of the proceeding blocks going back the entire history of that blockchain. And they would need to do it on every ledger in the network, which could be millions, simultaneously.[[13](http://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business/transcript?language=en)]

### **Will the blockchain transform the Internet & the global economy?**

Make no mistake about it. Blockchain is a highly disruptive technology that promises to change the world as we know it. The technology is not only shifting the way we use the Internet, but it is also revolutionizing the global economy.[[14](http://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world)]

By enabling the digitization of assets, blockchain is driving a fundamental shift from the Internet of information, where we can instantly view, exchange and communicate information to the Internet of value, where we can instantly exchange assets.[[15](http://www.economist.com/news/special-report/21650295-or-it-next-big-thing)] A new global economy of immediate value transfer is on its way, where big intermediaries no longer play a major role. An economy where trust is established not by central intermediaries but through consensus and complex computer code.[[16](http://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business/transcript?language=en)]

**“The technology likely to have the greatest impact on the next few decades has arrived. And it’s not social media. It’s not big data. It’s not robotics. It’s not even AI. You’ll be surprised to learn that it’s the underlying technology of digital currencies like Bitcoin. It’s called the blockchain.” — Don Tapscott**

Blockchain has [applications](https://www.google.com/url?q=http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable&sa=D&ust=1475458755304000&usg=AFQjCNFlr73mvGrBmCfHYgNTB8OSROlkbA) that go way beyond obvious things like digital currencies and money transfers. From electronic voting, [smart contracts](https://www.google.com/url?q=https://www.youtube.com/watch?v%3DFkeLDPZ-v8g&sa=D&ust=1475458755304000&usg=AFQjCNHS3g86jhkKqQelrYYseie52LBwCw) & digitally recorded property assets to patient health records management and proof of ownership for digital content.

Blockchain will profoundly disrupt hundreds of industries that rely on intermediaries, including banking, finance, academia, real estate, insurance, legal, health care and the public sector — amongst many others.[[17](http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine)] This will result in job losses and the complete transformation of entire industries. But overall, the elimination of intermediaries brings mostly positive benefits. Banks & governments for example, often impede the free flow of business because of the time it takes to process transactions and regulatory requirements. The blockchain will enable an increased amount of people and businesses to trade much more frequently and efficiently, significantly boosting local and international trade. Blockchain technology would also eliminate expensive intermediary fees that have become a burden on individuals and businesses, especially in the remittances space.

Perhaps most profoundly, [blockchain promises to democratize & expand the global financial system](https://www.google.com/url?q=https://www.youtube.com/watch?v%3Djbu6I-8mNUo&sa=D&ust=1475458755308000&usg=AFQjCNHSr4AuVSNZhmUPQahK5-9GZ63qww). Giving people who have limited exposure to the global economy, better access to financial and payment systems and stronger protection against corruption and exploitation.

**“Every human being on the planet with a phone, will have equal access. Expanding the total addressable market by 4X” — Brock Pierce**

The potential impacts of blockchain technology on society and the global economy are hugely significant. With an ever growing list of real-world uses, blockchain technology promises to have a massive impact. This is just the beginning.

Many of the most exciting applications and platforms haven’t even been invented yet!

# How does the Blockchain Work? (Part 2)

## **The top 5 things that you need to know.**

The talk about Blockchain technology seems ubiquitous. But what exactly is a Blockchain? More specifically, what are the Blockchain essentials that you should really know?

Let’s dive in to find out more about and separate the hype from the realit

### 1. What is a Blockchain?

A Blockchain is a tamper-proof distributed public ledger that manages transactions.

Think of it like a magical Google spreadsheet in the cloud, or more specifically on a network.

Put simply, a Blockchain is basically an incorruptible distributed ledger of data, which can be used to store informational assets ranging from managing cryptographic contracts to transferring value.

The most recognized application on a blockchain is bitcoin transactions.

The transferring of value from one person to another with no central intermediary, and without allowing a person or party to spend their bitcoin twice “the double spend rule”.

**What does this mean?**

It means that “value” can have a change of title and ownership from one person/party to another, without the need of a trusted third party to validate/govern the trade.

**How is that you might ask?**

Well, the governance is in the protocol   
(you will find more information on this below so keep reading)

Beside being a ledger for “data of value”, or cryptocurrencies, Blockchain technology is finding broader usage in peer to peer lending, (smart) contracts managements, healthcare data, stock transfers, and even elections.

Like any emerging and disruptive technology, no one can predict the future of Blockchain technology. But one thing’s for sure — it isn’t (just) for purchasing black-market goods and services!

As a matter of fact, Blockchain technology is finding its way into big firms such as IBM, Microsoft, and major banks.

Interest in the technology is driven by (fear of disruption) the fact that it excludes trusted third parties (banks and clearinghouses) during transfer of values, which in turn results in fast, private and less expensive financial transactions.

**Blockchain can facilitate the peer-to-peer transfer of anything that’s of value.**

This may range from assets, properties, and contracts. The most crucial and far-reaching Blockchain applications is applied in Bitcoin, with transfer of value, and Ethereum, with its enhancement of smart contracts.

Let’s jump in and learn the historical background of these Blockchain essentials.

### 2. Bitcoin

The Bitcoin currency, as many have come to know it, has been with us since 2008 when Satoshi Nakamoto — A person, or group of people, published a [whitepaper](https://bitcoin.org/en/bitcoin-paper)about peer-to-peer electronic currency.

The major innovation that bitcoin unveiled was direct and secure transfer of money or “value” directly to any party on the network.

The Bitcoin currency network is decentralized — there’s no central authority — the underlying Blockchain technology is used to store information which is verified by a network of “miners” who validate all transactions on the network.

**How should I think of this?**

Bitcoin is simply a virtual currency system which resembles the real world cash system.

Since it’s un-eponymous launch in 2008, through the boom and bust of the hype cycle, Bitcoin has continued to grow at an exponential rate, and the fringe curiosity that consumed a group of highly capable (Tech Nerds) has ushered in some new upgrades that has brought blockchain closer to the mainstream.

### 3. Ethereum — Blockchain 2.0

**Ethereum is a blockchain system based on the concepts of bitcoin.**

It is considered a second generation blockchain technology that was designed to let any person, with a basic level of computer skills, to develop and deploy their own decentralized applications on the Blockchain.

Just like the Bitcoin, [Ethereum](https://github.com/ethereum/wiki/wiki/White-Paper) is decentralized — no one regulates or owns it — it has it’s own cryptocurrency or “fuel” called “Ether” which acts in the same way bitcoin does. However, Ethereum has a few innovations worth noting. The first being a second application on its blockchain infrastructure called a “smart contract”, it’s own virtual machine which powers the memory and applications on the network called the “ethereum virtual Machine”, and it own programmable language called “Solidity”.

Ethereum is kinda like Bitcoin on steroids, but made to be more accessible.

It was developed by Vitalik Buterin, a 19 year old Russian Canadian in 2013 as a Blockchain 2.0 — next generation Blockchain technology — with capabilities to be able to program and perform, arbitrary and complex computations.

Rather than just providing users with a set of predefined operations — like Bitcoin transactions — Ethereum lets users develop their own operations with the complexity they wish.

### 4. Smart Contracts

**What is a “smart” contract?  
 — Well they actually aren’t that “smart”**

Think of them like self executing dumb software robots that live and do business on a decentralized network.

Smart contracts are autonomous computer systems, written in code, that manage executions between individuals on the Blockchain.

The code resides at specified addresses on the Ethereum Blockchain. These contracts are powered by our friend the Ethereum Virtual Machine (EVM) and by Ether. It’s the little engine that could, that keeps all the smart contracts running on time and coordinates them with the rest of the network.

In order to create an added layer of customization and security Ethereum created some high-level languages that are used to create smart contracts for the EVM. Solidity, Serpent, and LLL.

These are the major innovation that Ethereum has brought to blockchains and it allows for many amazing types of autonomous programs.

Next, let’s explore the consensus mechanisms in Blockchain.

### 5. Consensus Mechanisms

*“When you interact with multiple parties, you need some sort of consensus mechanism to ensure everyone has got the right records”–Dan O’Prey, Co-founder of Hyperledger.*

Both Bitcoin and Ethereum use a decentralized system to confirm the transactions without relying on a trusted third party.

Therefore, consensus, or coming to a uniform agreement, helps a network of autonomous programs and computers come to an agreed state of the blockchain without conflict.

As a matter of fact, the consensus is the backbone of the Blockchain and any other decentralized and distributed technology

The proof of work, proof of stake and closed consensus are the most common mechanisms used in Blockchain technologies.

### A: Proof of work

The most common consensus mechanism that’s used for Blockchain technology is what’s called “proof of work”. It is the system used in Bitcoin.

When a transaction is initiated, the information is stored in a candidate block which is filled with the transaction’s information. A cryptographic beacon is sent out to the mining network that the candidate block has been created, and the miners get to work on solving a cryptographic puzzle that has a prize for whomever solves it, in the form of newly minted coins/currency.

Miners have what some would think of as supercomputers that are much more powerful than the average Person’s Macbook pro. These machines have a “hashrate” or computing power that gives them an advantage when competing to solve consensus problems for reward.

**I know what all you climate control advocates are saying: Doesn’t that demand a lot of electricity and processing power?**

The short answer is yes, the cost of mining is based primarily, on hardware, electricity costs, and to some degree temperature.

The problem with the Proof of work consensus is that it requires the miner to use their supercomputer to try out millions computations per second, in competition with other supercomputers around the world, to determine if the Blockchain can be updated or not.

### B: Proof of Stake

The main objective of this mechanism is to allow stakeholders, the people with the most invested, or owned, in the Blockchain ecosystem to have the strongest incentives to lead in the provision of consensus solutions for a Blockchain transaction.

**In simple terms:**

Proof of stake consensus allows miners that have more “money”, cryptocurrency, or “skin in the game” to have a greater opportunity to mine blocks and make decisions for the network.

The process starts by the miner consuming his/her cryptocurrency — commonly referred to as the kernel — which provides privileges for updating the Blockchain which is similar to Proof of work.

However, the hashing computation in Proof of stakes is done using a limited search space where stakeholders with the greatest stakes have the ability to mine a commensurate allocation of the network, and are effectively stewards of the Blockchain system.

**Think of it like**: the more a miner has, the more they can get, and the more they can decide.

The one benefit of this controversial crypto-economic system is that by allowing stakeholders with incentives take charge of consensus the mechanism reduces the computing power required for consensus.

**This should make the climate control kids happy, but**

The main problem of this mechanism is that disadvantages other miners in the network since only the “richest” stakeholders are permitted to have control of consensus in the Blockchain.

### C: Closed Consensus

In a Closed consensus mechanism certain nodes are required to put up a security deposit in order to participate in updating the Blockchain.

This consensus mechanism doesn’t require mining, and is growing in popularity in some banking and insurance segments.

The management of the consensus is done using security deposits which incentivize the validators. The “arbitrators” — conflict management nodes are the enforcers on the blockchain and the adjudicate when something is not write or if a miner is not acting fairly.

The main objective of using an arbitrator’s protocol is to enforce consensus among the autonomous nodes in the Blockchain.

If a validator authenticates a transaction which the arbitrators have considered illegitimate, then the validator losses their security deposit and they also forfeit their privileges of providing consensus in the Blockchain network in the future.

### Conclusion

Now that you understand the basic essentials of Blockchain technology you should be able to distinguish very easily:

***1. What is a blockchain?***

***2. How does bitcoin work?***

***3. What are the major innovations that The Ethereum blockchain brought to the technology?***

***4. What is a smart contract?***

***5. What are the different types of consensus mechanisms that power a blockchain?***

Hopefully this inspires further exploration and your own personal discovery, in what everyone is talking about, and how perhaps you might be able to join in the conversation and or project/experiment.