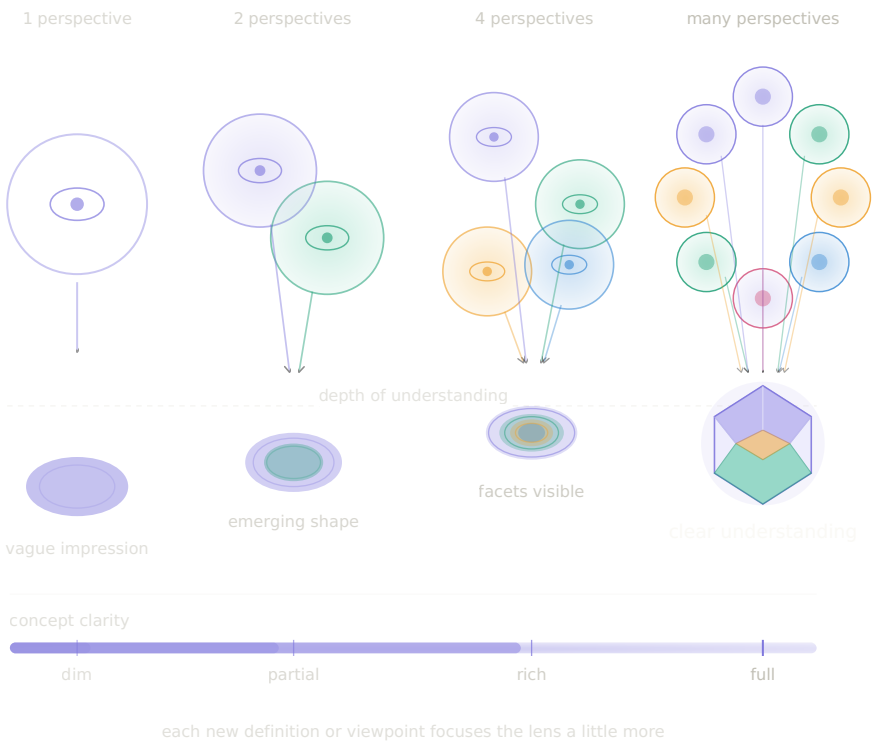
- author = “steffen” draft = false title = “What is bitcoin?” date = “2026-03-22” description = “what is bitcoin” tags = [“bitcoin”, “p2p-electronic-cash-system”, “triple entry accounting”, “small world network”, “resource event agent model”, “write once read many worm”, “blockchain”, “big block bitcoin”,] +++

As an additional option, you can also read this article as a PDF on the blockchain if you want.
https://ordinals.gorillapool.io/content/f75b3e6f589ac62b52d2714263410987b964d60ded6f5ba5da3c39e867e76ae4_0

What is bitcoin?

“What is Bitcoin?” is similar to asking “what is water?”, where several definitions can be equally true.
In my opinion the understanding of a topic improves and gets better, the more definitions you have.
Water i.e. can be described as wet when you have human sensormotorics, as H2O when you are familiar with chemistry, as formless because it takes any shape it is being filled into, as liquid because it can’t be carried (except for ants), as rare if you are living in the desert, or as plentiful, when living at a river or the ocean - and there would be many more definitions.
With bitcoin it is similar.
Therefore I will give you several definitions, analogies and explanations about what bitcoin may be and you can make of it whatever you want.
Hopefully a clearer picture will emerge.
The more explanations and definitions you read, the clearer the picture in your mind (the graph) gets and the better the overall understanding.
Be aware that you should always do your own research and that I may be wrong!



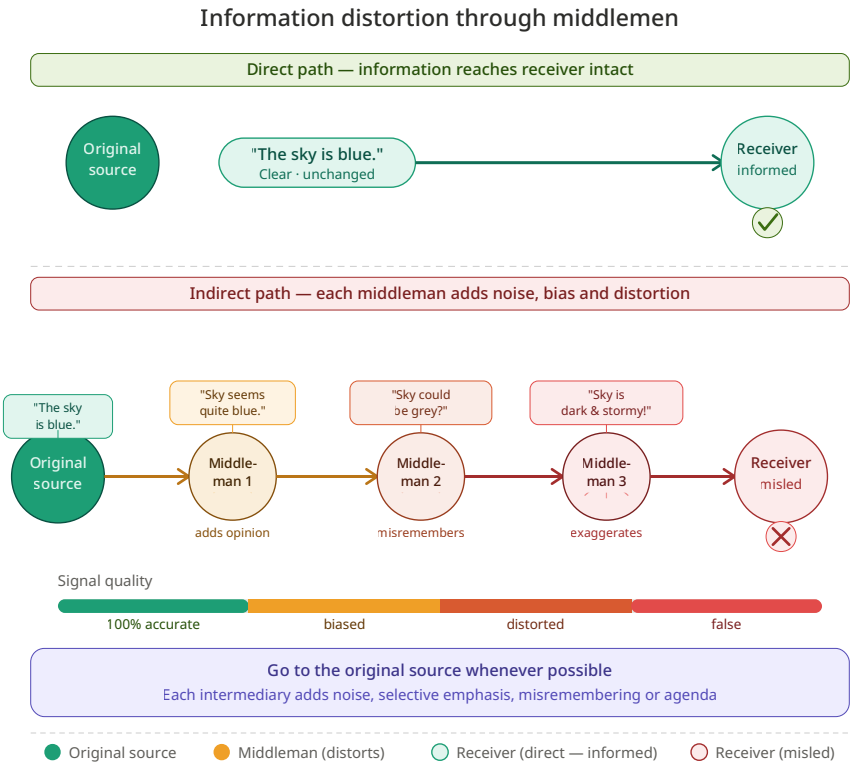
geometrical_shapes_2d_vs_3d_pov

Depending on your point of view and the angle you are looking from, the picture can change and can get more clearly. The more points of view you have, the clearer your overall picture (Most pictures in this article are generated with Claude Sonnet 4.6).

Go to the original source

I highly recommend to always go to the original source, where the definition was initially forged.
In this case you should read The Bitcoin Whitepaper.
You can either interact peer-to-peer with the original source or you introduce a middleman, normally an influencer on social media or an artificial-intelligence, which will always distort the original picture or concept to some degree.
This distortion can happen either intentionally or by accident.
The end result is the same - a distorted picture and understanding of the original content.
Ironically the “peer-to-peer interaction” is one of the main themes in bitcoin, but most people investing and talking about it, haven’t read the bitcoin whitepaper and therefore haven’t interacted peer-to-peer with the original source and information - the irony.
Another problem is, that when you have heard about bitcoin from a

middleman first, you may already have a distorted picture in your mind.
Which may affect the reading of the whitepaper and further research, since you will already be biased even if you are not aware.
Therefore always try to go to the original source as soon as possible and make up your own mind.
You can learn about other peoples opinions and all the different nuances and orientations afterwards.
In our attention driven world you should take great care where you get your information from.
That all being said, I recommend you do pause and read The Bitcoin Whitepaper first.



original_source

What the inventor had to say

Bitcoin was described by a pseudonymous entity named Satoshi Nakamoto in the bitcoin whitepaper in october 2008.
Therefore the name and definition of “bitcoin” is linked to the design and functionality described in this whitepaper.
Definitions are important and you should not arbitrarily change them.
Otherwise you may end up with Newspeak like in George Orwell’s 1984.

According to the whitepaper, one of bitcoins purposes is to enable peer to peer interaction by eliminating the need for middlemen.
Satoshi described bitcoin as a peer-to-peer electronic cash system, not as peer-to-miner-to-peer-digital-gold.
You can read the whitepaper and many of Satoshi's emails and forum posts on the nakamotoinstitute-website.

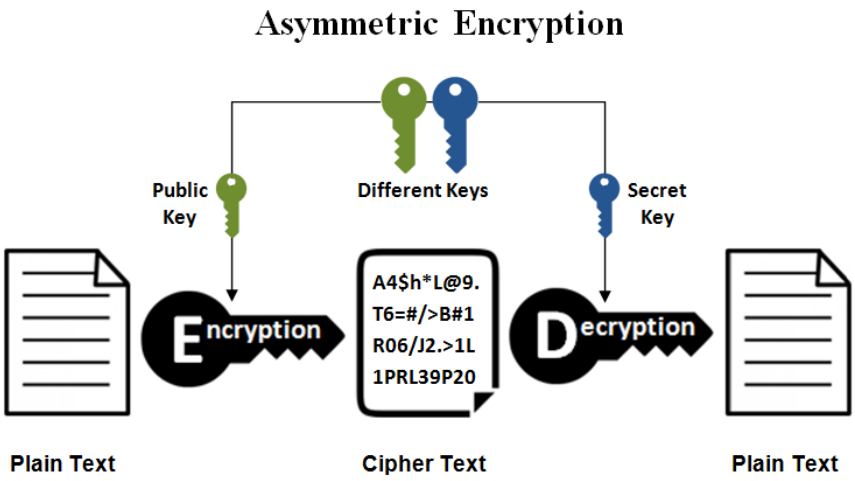
User side - Bitcoin is open accessible and users create accounts themselves

The Bitcoin network can be participated in by creating a pair of asynchronous keys and therefore is openly accessible for everyone.
Similar to math, writing, poetry, languages or the internet where everybody is free to learn the skills and participate.
In previous times you needed pen and paper and the skills of reading and writing.
All you need for participation in bitcoin is an electronic device an internet connection and a program which can generate asynchronous key pairs using the secp256k1 elliptic curve.

!!!This means you can create your user account yourself!!!

The implications are immense.
No facebook or meta, no twitter or x, no microsoft or google, no amazon or apple, no visa, mastercard, paypal, JP Morgan, Deutsche Bank or Lehman Brothers, or other banks, no government or state is needed to issue you a user account or identity.
A user account and identity which, as history has shown, can be arbitrarily censored, banned or deleted whenever those enterprises and institutions decide you have acted against their constantly changing laws, terms and conditions.
Or just because they do not like your narrative or point of view.
On bitcoin you create your account yourself by creating a pair of asynchronous keys.
The public key is like your username or email and the private key is like your password.
Due to a mathematical miracle, those two keys are somehow entangled and connected and you can do all kinds of magical stuff with them, like encrypting all your data and communication.
After creating a key pair you can interact peer to peer with other persons on the internet or in real life and can get a record on the blockchain if needed.
No big tech, big government, big media or big banks needed.

Only big block bitcoin as originally designed.
You then can use those asynchronous keys to delegate read, write and executional access to your personal data, files and content.
Data is money and you now have the tools to own, market and sell your data without intermediaries like big tech, governments or banks taking their cut and interfering with it or restricting you from accessing the network.
More about data being money in another article.
This is the decentralization aspect on the user side, which can only unfold its full potential, when the blocks are large enough, so that every user can transact on chain.
If you restrict the transactions per second like small block BTC is doing with their 1MB blocksize limit, you automatically restrict the decentralization aspect on the user side in favor of the server side - namely people being able to run listening nodes on a raspberry pi.
Small block BTC with its 5 transactions per second which is about half a million transactions per day, is essentially cutting out 99.99% of the world population.
It would be like everyone of the 7 billion people one earth being able to buy, build or create a car but there is only gasoline for around half a million people to drive each day.
You can create your own identity but the probability of using it on the blockchain is close to zero.
Or in small blocker language: you can be your own bank but you won't be able to transact.
But more about that in a later article.

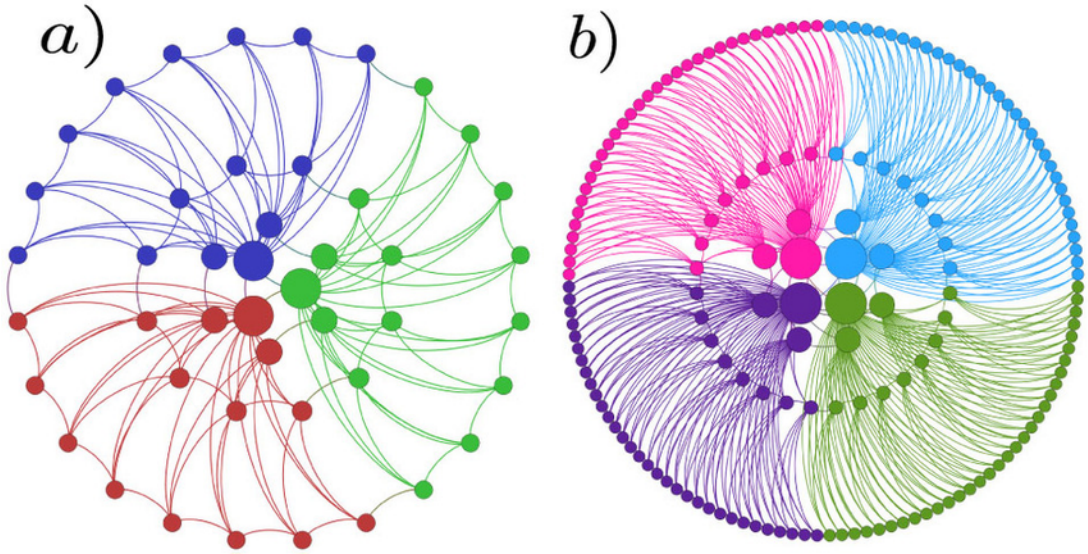


asynchronous_keys

Source of picture

Server side - Bitcoin is a small world network and open accessible for server operators (miners)

Bitcoin can be described as a Small World Network or Mandala Network which can be visualized and described through graph theory.



Source of picture

Those networks do consist of more than just one centralized server which introduces redundancy and backup capabilities.
Additionally it kinda decentralizes and splits up the power position from one entity like governments, big tech enterprises or central banks into several entities.
You then can run whatever you want on top of the network, be it identity, money, social media content or any other form of data.
In essence you have several servers, run by different entities which are all acting as auditors which are constantly auditing each other.
This way they hold each other accountable and the chance of one party cheating and enriching itself without the other parties recognizing, is highly unlikely.
This is how societies kept themselves in check in previous times as well - we audited each other constantly.

A short quote from Leopold Kohr's - Breakdown of Nations:
> "Even a confirmed thief will not steal if he has no chance of getting away with it.
On the other hand, even an honest man will misbehave if he has the opportunity, the power to do so."

Criminal actors are rational actors - they won't steal when the chances of getting caught are at 99.99%.
Therefore they won't.

The business model of those servers is the timestamping of user transactions for a small transaction fee to cut their costs and make a profit - but more about that in another article.
Nodes which do not find a block can't break even on their initial investment and won't make a profit.
This is not necessarily bad, but it is not a working business model and more like a cash bleeder.
Additional information with regards to home run user nodes like on a raspberry pi.

Bitcoin is a database with an address space of potentially 2.099.999.997.690.000 data entries or addresses

Written out: Two quadrillion, 99 trillion, 999 billion, 997 million, 690 thousand addresses.
An address is essentially the smallest unit of account in bitcoin.
Other words for addresses which are being used as synonyms in the blockchain space are: satoshis, utxos (unspent transaction output), tokens, electronic coins, data entries, chains of digital signatures.
On bitcoin there won't be more than those 2.099.999.997.690.000 addresses.
Addresses, satoshis, tokens, utxos, chains of digital signatures, or electronic-coins are mainly made for usage not for hodling.
The same way, shoes are made for walking, beer for drinking, e-books for reading and ip-addresses for hosting not for hodling.

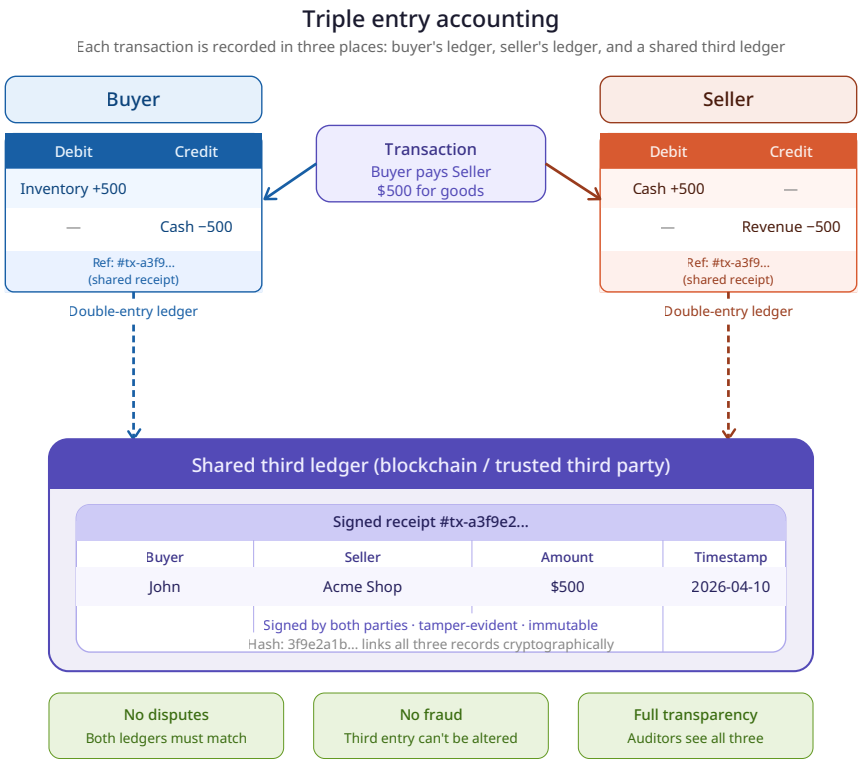
Bitcoin is a triple entry accounting system.

Most exchanges over the counter are a so called "implied-in-fact" contracts due to acceptance through conduct.
This evolved over hundreds, maybe even thousands of years and is so called "common law".
If you want proof that you bought something in case of filing warranty or getting compensation for a faulty or defective product, you need a receipt.
On bitcoin this would be a satoshi, utxo, electronic token or chain of

digital signatures.
For an over the counter exchange you do not even need money, you could also just sign a contract.
Money or cash is just a hack for instant settlement to skip the signing of a contract and the additional work and time it implies.
The signature part is quite interesting, especially with regards to established contract law and the real signature of a person under a contract.
This can be done in an electronic way as well with the already mentioned asynchronous keys.

Since 2008 there are three different kinds of book keeping:

single entry accounting	**double entry accounting**	**triple entry accounting**
Simplest form of accounting.	Every transaction affects two accounts, ensuring the accounting equation (assets = liabilities + equity) remains balanced.	Builds upon double entry accounting.
Only one account per transaction.	Introduced in the 15th century by Luca Pacioli.	Incorporates a third entry, usually recorded on a blockchain.
Mostly used by small businesses.	Significantly improved the accuracy and reliability of financial data.	This additional entry acts as a verification mechanism, enhancing transparency and security.



triple-entry-accounting

Here is some more information with regards to blockchain.
And just another link if you can't get enough.

Bitcoin is a Resource Event Agent Model

If I would buy a bread at the bakery, the bread would be the resource, the trade of bread for money would be the event and me and the baker would be the agents.
So you have a resource, commodity, service or good, which can be mapped to a utxo, token, satoshi or digital chain of signatures.
You have an event, like an exchange or trade over the counter, which is represented by the transaction or utxo itself.
And you have one or more agents, which is/are the identities behind the asynchronous key pairs which are trading with each other.
Voila - resource event agent model.
It is interesting with regards to economics, trade and Artificial Intelligence, where a database for memory and a record about what happened would be quite convenient.
Additional explanation of resource-event-agent-model.

resource_event_agent_model
resource_event_agent_model

Bitcoin and blockchain are WORM databases

WORM stands for write-once-read-many.
It is very simple and is already used for quite some time in enterprise databases.
There is a difference between hardware implementations (punch-cards, tape, CD's) and software implementations (blockchain).
A WORM database can't be changed retroactively without leaving trails.
This can be of use in many areas, where you want clear traces of evidence.
For example when a programmer working at a bank steals a few million dollars and edits the database afterwards to cover his tracks.

Error code "402 - Payment Required"

There is an http status code, namely "402 - Payment Required", which was reserved for future usage.
It essentially means, that a website can only be accessed after a payment was received.
So the server serves the content only, when a transaction was made.
Since every youtube-video, blogpost or twitter post has its own web-address and therefore its own website, a content creator can directly delegate access to his content.
Think about the implications and what that means for big tech and the advertisement business.
You could pay a cent or even less directly to the content creator for accessing a post, article, meme, video or podcast.
No middlemen or intermediaries like google required.

> 402_payment_required
> 402_payment_required

KISS - keep it simple stupid - minimalistic design

Asynchronous keys combined with 256bit hashes provide uniqueness due to a really large address space, security due to close to no collisions and a minimalistic amount of data.
This is a really good equilibrium.
In other words: Similar to ipv6 we will have enough addresses with those 2.1 quadrillion satoshis.

Additionally there won't be any identical asynchronous key pairs, because the address space of the secp256k1 eliptic curve is so large, that the probability is close to zero. This means the chance of someone stealing someone elses keypair by accident is neglectable.
And on top of all that this beautiful design only needs a minimalistic amount of data, since it is based on 256 bit data.
A standard bitcoin transaction is normally not larger than 400 bytes. Instead of a 3MB (3000000 bytes) picture you could send 7500 bitcoin transactions.

Bitcoin is a database and therefore memory

If a person wants to record an action and pays a fee the bitcoin network can record which private key(s) interacted with which public key(s) at which point in time and if the signatures were valid.
Identities can be linked and the stories behind every transaction can also be linked but are firewalled by default and therefore are private.
Purchase of coffee in real life or buying a song over the internet versus buying a car or a house.
You do not want everyone to know that you have bought a song or a coffee, but you want people to know that you are the owner of you house and your car.
If you have created a pair of asynchronous keys you can use this keypair on all three bitcoin versions, namely BTC, BCH and BSV.
Beware of the chains capabilities and their potential network effects and utility in the future though.
Two chains are arbitrarily restricted, one is unbounded.

Memory and identities

Identity is a very abstract concept.
If you are interested you may find Ian Griggs book Identity Cycle interesting.
The history of "identity" is quite fascinating, whereas the church started birth registers around 1500, but it took till the mid 1800s for broader adoption of birth certificates.
Today our identities are normally issued by centralized governments/ states or big tech companies.
Remember, that on bitcoin you are creating your account yourself, without any centralized entity.
Parents can create digital identities for themselves and for their newborn child.

You then can link your identity to your asynchronous key pair and other identities can verify yours while at the same time you are verifying theirs through interactions or transactions.
Those interactions have to be recorded and therefore memorized, which is why bitcoin and the blockchain is memory.
Reputation and trust probably will play a huge role in this future.

More about memory, trust and the search for a path

There is a paper from Narayana Kocherlakota about “money being memory”.
> “There is a simple reasoning behind the main proposition. John and Mary meet. John has apples and wants bananas. Mary wants apples but doesn’t have bananas. In monetary economies, this problem is solved by Mary’s giving John money in exchange for apples. John then uses the money to buy bananas from Paul; if John doesn’t give the apples to Mary, John doesn’t get the money and can’t buy the the bananas from Paul. But of course the money itself is intrinsically useless. In terms of reallocation of intrinsically valuable resources, we can think about the situation as being one in which John is considering making Mary a gift of apples. If he makes the gift, Paul will give him bananas in the future; if he doesn’t make the gift, Paul won’t give him the bananas. The money that John receives from Mary is merely a way of letting Paul know that John has fulfilled his societal obligations and given Mary her apples.”

money_as_hack
money_as_hack

And I would also recommend reading Mike Hearn’s annotations about the early ripple protocol which has some parallels with regards to “memory” where he also states, that Satoshi found that: “Ripple is interesting in that it’s the only other system that does something with trust besides concentrate it into a central server”.
> “John buys his groceries at the local food cooperative, and uses a smart card to make a Ripple payment in the store. The Ripple routing system finds that the food coop has a balance owing at the local hardware store where they buy maintenance supplies. The hardware store in turn has an outstanding bill with the lawyer up the street. John often does landscaping for the lawyer on credit. To complete John’s

payment to the food coop, the Ripple system reduces the food coop's bill at the hardware store, the hardware store's debt to the lawyer, and finally lawyer's debt to John. John walks out with his groceries."

search_for_a_path
search_for_a_path

Money is a technology and bitcoin may be John Nash's ideal money

I would recommend reading John Nash Jr's statements about "ideal money".
According to his point of view: > "The special commodity or medium that we call money has a long and interesting history.
And since we are so dependent on our use of it and so much controlled and motivated by the wish to have more of it or not to lose what we have we may become irrational in thinking about it and fail to be able to reason about it like about a technology, such as radio, to be used more or less efficiently."

Money is a technology and…

Data is money - the Bit and the Coin

Bitcoin is a new technology for monetizing data. And since data is money it kinda is monetizing itself as long as users see a value in this economical approach of monetization of data by using the protocol and thereby putting their signature behind it.
"Bit" is the data aspect, whereas "Coin" is the monetary part.
More about what "data is money" means in another article.
One short example though: if you have accurate data about how many homes are burning each year in a certain area and you see, that the current insurance company is making a surplus of 200% each year you can compete against them by making an offer with a 60% reduction in price.
You are essentially undercutting your competitors by 140% and still making a 60% profit.
This can only be done when the data is accurate and it is one of the main reasons, why large enterprises and other institutions are keeping certain data secret.
And it is one of the reasons the governments of this world allow no competition in certain areas, like money, education, identity,

bureaucracy and other areas.
Because the data may show how inefficient it has become.
They have essentially eliminated the control groups and their competition, because the easiest competition is always the one, where you are the only participant.

Peer to peer

Bitcoin works peer to peer which means two persons can interact directly with each other, without any middlemen who can use a man in the middle attack to obfuscate or distort the original intention.
Think about it with regards to politics and other centralized positions of power where your vote doesn't matter because the person who got your vote has no obligation or duty to do what they have promised.
Citizens on both sides may vote for peace but get war at the end.
Vote with your money.
Pay for what you like and don't pay for what you dislike - simple as that.
A representative democracy is essentially a system, where you can;t pay for what you like, because someone else decides for you.
Bitcoin is a timestamp server with a decentralized structure, where users can vote or delegate read, write and execute access rules to unique tokens and linked data through asynchronous keys and signatures.
They own their data and can sell it to whoever they want, whenever they want, at what price they want.
Without google, governments, insurance companies, banks or other intermediaries or middlemen in between.
More about peer-to-peer and "simplified payment verification" in another article.
I want to add, that small block BTC does not work peer-to-peer but peer-to-miner-to-peer, which is not how bitcoin was designed to work - and that is not my opinion, but a verifiable fact.
It is stated in the whitepaper, under "section 8 - simplified payment verification".
Again, read the whitepaper.

p2p_vs_middleman
p2p_vs_middleman

Data integrity

The bitcoin network is like a notary, where you can timestamp the hash of a video, audio file, text document or any other file to proof that it existed at least at this point in time and that you have been the person who timestamped it first.
Satoshi did the same, when he created the genesis block and included the message “Chancellor on the brink of second bailout for banks” from “The Times” which shows that bitcoin couldn’t have started earlier, because the headline hasn’t been written yet.
When you want to patent an invention or timestamp a piece of content, you can hash the file which describes your invention and can put that hash into a transaction, send the transaction to yourself and let the miners timestamp it.
You then have solid proof that you had this idea or piece of content at this point in time and can proof it later if necessary.
The timestamping costs the fraction of a cent.
A notary or patent office costs hundreds if not thousands of dollars for doing something quite similar.
There is an endless amount of usecases for this kind of service.
I want to add, that the patent office also checks for already existing patents and a few other things.
If patents are a good idea would be a separate discussion.
However, the service still is very valuable, especially with regards to private contracts and their attestation.

Sunlight law, transparency and honesty

Bitcoins transparent design incentivizes honesty, because as a node/miner, you are rewarded when playing by the rules and punished when cheating.
This is true as long as more than 50% of network participants (not nodes/miners) demand honesty.
Criminal actors are rational actors and they normally only defraud others if they get more out of it - this makes no sense in bitcoin.
Quoting Leopold Kohr - Breakdown of Nations once more:
> “Even a confirmed thief will not steal if he has no chance of getting away with it.
On the other hand, even an honest man will misbehave if he has the opportunity, the power to do so.”

The word “honesty” is mentioned 16 times in the bitcoin whitepaper and therefore seems to play an important role in bitcoin and deserves its own article.

Private law societies

Bitcoin is a peer to peer electronic contract and signature network where the validators (miners) are getting paid with empty contracts for validating and timestamping other peoples signatures and contracts - a simple computational service for a small fee (money).
Private law society fans like anarchists or libertarians may find bitcoin interesting since you can use electronic contracts similar to private contracts.
Because every exchange, be it at the bakery, barbershop or sawmill is essentially a contract through conduct and communication or in other words, acceptance through conduct, a so called “implied-in-fact” contract.
I already mentioned this with regards to “triple entry accounting” and for me it was very enlightening.
You could use pen and paper at the bakery and write a contract for getting the bread against a credit and certain conditions in the future.
Money is just a hack for instant settlement, where the monopoly commodity (monopoly + commodity = money) is being used, because due to its monopoly it is being accepted by the majority of people.
And normally it reached its monopoly because of utility.
Currency is a state issued security and is not money.
More about “what is money?” in another article.

What Bitcoin is not

Bitcoin is not digital gold and it is not for hodling, which essentially means not using it.
Hodling and not using something is the opposite of peer-to-peer-electronic-cash.
Sure, you can do it, but you can also hodl a basketball instead of playing with it, or hodl a house instead of living in it.
No wealth is created through hodling something.
Lightning and Sidechains like Liquid are not bitcoin, those are separate networks and protocols which are reintroducing intermediaries and middlemen - welcome to the old system.
But more about lightning in a separate article.
Bitcoin is designed as an electronic peer-to-peer-cash-system and was

made for onchain usage.
Everybody can make up his own mind, if all the mentioned definitions and concepts in this article are making sense for eight billion people operating on a network capable of five transactions or timestamps per second - do the math.

-	BTC	BCH	BSV
Transactions per second	7	116	> 1000000

Thanks for reading.