author: steffenkd
date: 04.06.2026
wordcount: ~ 3750
reading time: ~ 30 minutes

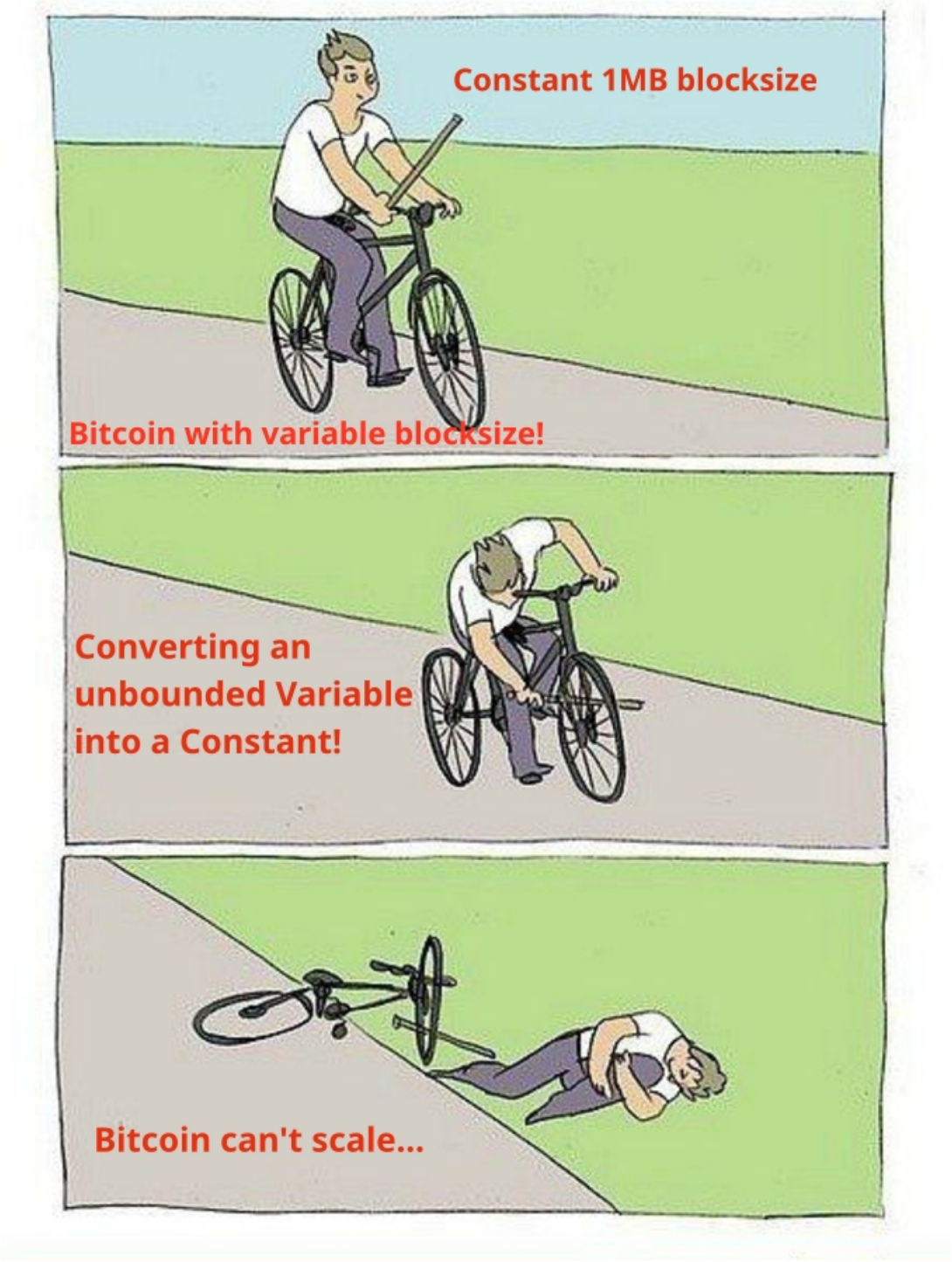
The blockchain trilemma fairytale

TLDR/Summary:

Trilemma somehow has a negative connotation.
It somehow implies, that there is a problem which has to be fixed.
This assumption is based on a false premise.
You simply have three variables, namely decentralization, security and scalability which can be balanced out against each other, like in mathematics.
This is how you solve mathematical equations.
And the same concept of variables being balanced out against each other due to infinite feedback-loops and co-dependencies can be found all over nature.
It is called balance and is not negative at all.
Additionally on small-block-BTC we are not talking about an equation with three variables but with only two variables.
Namely decentralization and security, since the variable blocksize is a frozen constant at 1 MB (one Megabyte).
Which would make it a blockchain dilemma (duos, duo, di, dos, two).
There are only two variables left, because on small-block-BTC the originally variable blocksize, which was set to 1MB as a temporary SPAM and DDOS protection got converted into a frozen constant of 1MB (4MB blockweight).
They sacrificed scalability for decentralization and security, which leaves small-block-BTC with just two variables, namely decentralization and security.
So we are not talking about a problem (dilemma or trilemma), but just about an equation with several variables.
And on small-block-BTC only two variables are left, because the blocksize was converted into a constant of 1MB.
Therefore the term “blockchain trilemma” is just Orwellian Newspeak to artificially create a problem which never existed in the first place.

On the original Big Block Bitcoin, those three variables are still variable and can be balanced out against each other.
Therefore it scales and can match the demand for transactions with a corresponding supply like free markets always do.
The same way a marathon runner can run a marathon because his heart rate is variable, adapts to the stimuli and supplies the demanded heart rate increase.
If you want a more detailed version with some pictures, analogies and explanations, keep on reading.

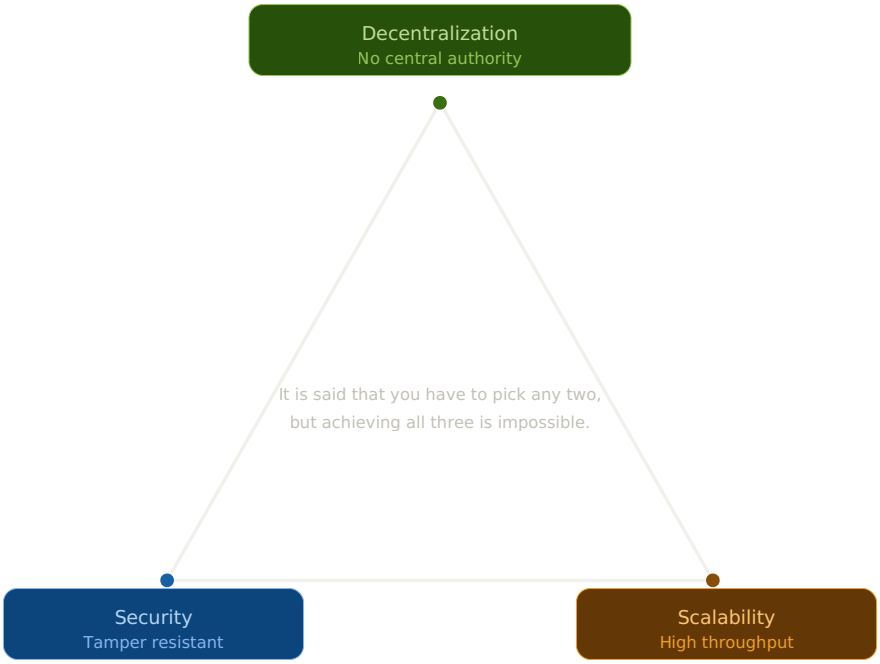
A classical meme to visualize what happened:



Picture: the bike represents the original bitcoin protocol, while the stick represents the artificially and arbitrarily introduced blocksize limit.
The temporary blocksize limit wasn't removed as the demand for transactions rose.
No law of demand and supply possible.

Bitcoin - there never was a blockchain trilemma

The so called blockchain-trilemma is often visually represented by an equilateral triangle with the three points and sides “decentralization”, “security” and “scalability”.
This triangle analogy was introduced by Zoko Wilcox O’Hearn and Vitalik Buterin and the three points of the triangle had different names.



blockchain_trilemma

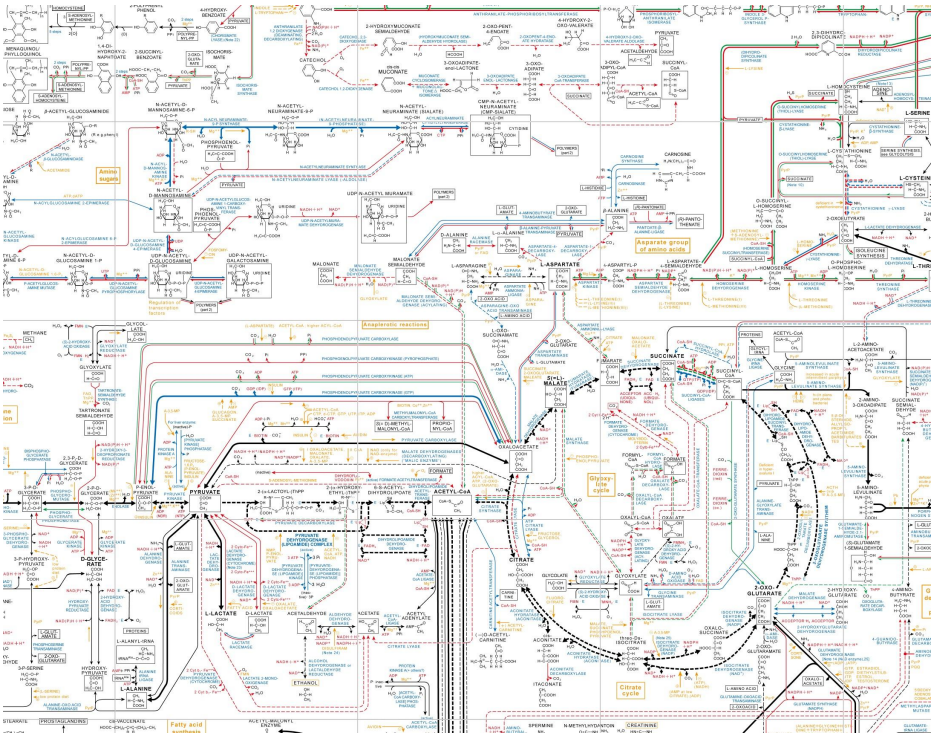
Picture: The so called blockchain trilemma, visualized as an equilateral triangle with three variables.
Normally it is said, that you can only pick two variables.
But this is a fallacy.
You can pick all three.

Trilemma or self balancing equation?

There never was a trilemma in the first place.
The triangle is just a visual analogy for an equation with three variables and the solution to the equation is quite simple.
It is a basic principle which can be found all over nature and which is

being applied in mathematics as well.
It is called “balance”.
So it is not a trilemma but just an equation with three variables, which can be balanced out against each other.
It would be similar to call the human body with the linkage between blood pressure, stroke-volume, heart rate and the resulting overall performance a trilemma.
Which isn’t a trilemma at all.
It is just natures universal concept of balance at work.
But of course you can also intervene planned economy style and convert one of the variables into a constant of 1MB if you think you can outsmart nature or the free market.
Welcome to our old system, where problems are artificially created so power hungry middlemen and intermediaries can step in and come up with a prepared solution.
A solution which in many cases provides them with control, power and money.
This is by the way one of the main reasons, why the original bitcoin design with big blocks is hated and ridiculed so much.
Because it enables peer to peer interaction and eliminates middlemen and intermediaries.

To be clear: in the human body scenario there are much more variables at work.
For example breath frequency and volume, glucose storage capabilities of muscles and liver, fat storage, body weight, muscle mass; the list would be very long and the variables are all interconnected with feedback loops and co-dependencies.
There is a visualization from Roche, called “biochemical pathways” which is about the chemical processes and interconnections in the human body and may serve as another analogy how complex and interconnected certain systems can be.
And you can either let these equations balance themselves out or you arbitrarily intervene because you know whats best for all - choose wisely!
Free market versus centrally planned economy.
History doesn’t repeat itself but it rhymes.



roches_chemical_pathways

Picture: “Roches chemical pathways” provides a graphical representation of the most important biochemical pathways in living organisms, like glycolysis, the citric acid cycle, fatty acid metabolism, amino acid biosynthesis, nucleotide metabolism, and much more.

Variables versus constants

A variable is, by definition, flexible.
Which means it can adapt to external stimuli - the so called “free market” with the law of demand and supply at work.
If the demand for transactions rises, the size of the blocks can be increased accordingly and vice versa.
Simple as that.
If you convert a variable into a constant this has certain consequences though.
Convert your variable heart rate into a constant of 20 beats per minute and watch whats going to happen.
Or fix the variable longitude of your GPS positioning system at 30° west and try to navigate to your destination point - but don’t forget to bring a rubber boat or life vest.
Whenever you convert a variable into a constant you have consequences.

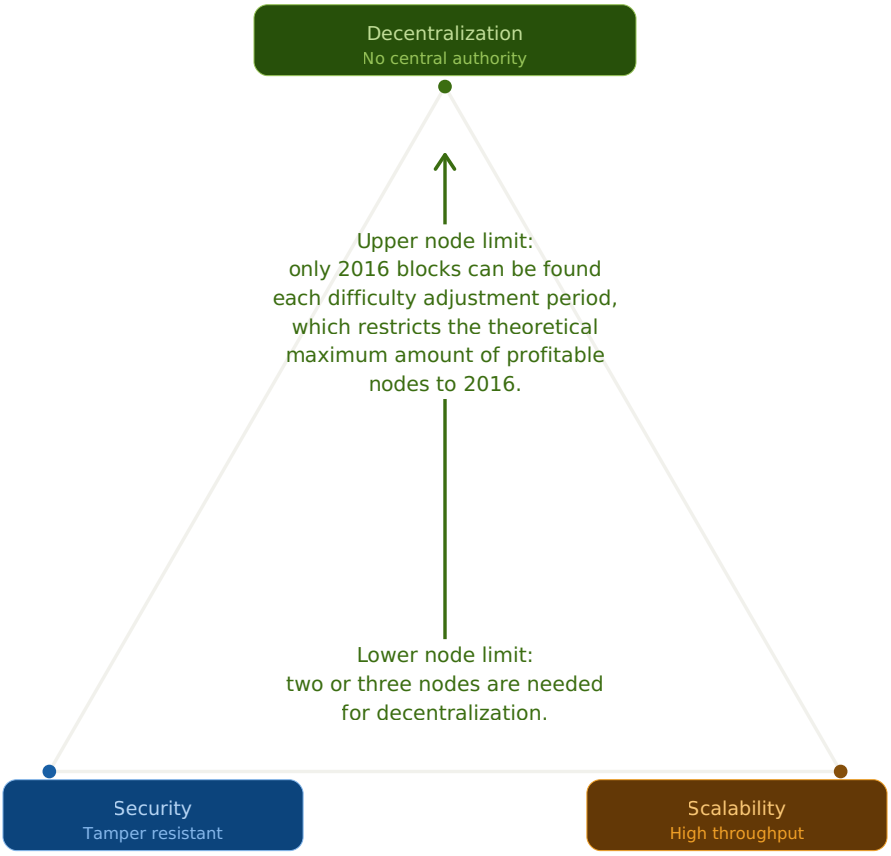
The three variables

Decentralization

Centralization means that something is centered in one point.
Therefore decentralization means that something is not centered in one point but exists in at least two points.
For bitcoins game theoretical advantages to come into play a minimal amount of three points or nodes is needed longterm.

In my opinion “decentralization” is one of, if not the most, misunderstood concept in the so called crypto and bitcoin space.
Which is why it deserves its own article.

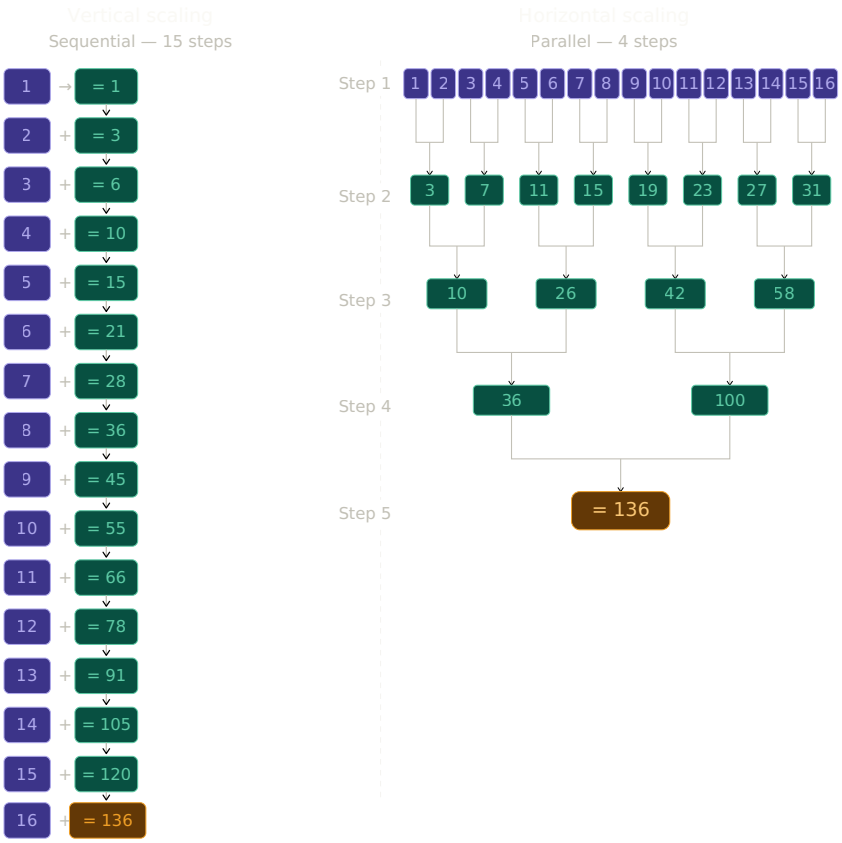
For those who want to read more about the decentralization in bitcoin.
Spoiler alert: the decentralization in bitcoin is also an equation, which can be balanced.
In this case we have two variables: “the user-decentralization” due to identity creation by the users themselves through asynchronous keys, versus “the miner-decentralization (or server-decentralization)” due to economic incentives like finding a block and getting paid for timestamping the users transactions.
If you limit the amount of transactions you automatically limit the amount of user-decentralization.
Users can create their digital identity themselves by generating an asynchronous key pair, but 99.99% of them won’t be able to use it on the small-block-BTC blockchain.
Or in small block BTC language: You can be your own bank, but you won’t be able to transact.
You would essentially end up with something like another PGP implementation.
I recommend reading the article to get a better understanding of the concept.



blockchain_trilemma_decentralization

Scalability

Scalability is the ability of a system, application, or process to handle increased load or demand by expanding its capacity — without sacrificing performance, reliability, or efficiency.
There are two main types:
- Vertical scaling (scaling up): Adding more power to an existing machine (more CPU, RAM, storage).
- Horizontal scaling (scaling out): Adding more machines or instances to distribute the load.
A scalable system can grow smoothly as users, data, or transactions increase — ideally with proportional or sublinear cost increases rather than exponential ones.



horizontal-scaling_vs_vertical-scaling

The diagram shows how the same sum (1+2+...+16 = 136) is computed in two very different ways:
- Left (vertical/sequential): Each number is added one at a time which needs a total of 15 steps - no parallelization possible.
- Right (horizontal/parallel): Numbers are paired up simultaneously at each level — 8 pairs in step 1, then 4 pairs, then 2, then 1 — having also 15 steps in total, but reaching the answer in just 4 steps due to parallelization.
This is the essence of parallel processing: more workers doing work at the same time, fewer steps overall.

The utxo-model in bitcoin is another design, which enables parallel processing and therefore horizontal scaling.
Different users can compute their utxos on the blockchain in parallel if they have the corresponding private keys.
This makes bitcoin with its utxo based system very flexible and fast compared to an account based system.

So if something scales it means that there is more of it and that the supply can be raised.
This is another free market principle.
If the demand for a good or service rises, it normally gets matched by a corresponding supply if physical possible.

In the technical area i.e., we experience an increase in computational power due to Moores Law, which is driven by an increased demand for computation.
Similar to running a profitable node or miner instead of a non profit one, processing and timestamping a transaction is just a service which can be calculated and priced in economical.
You just need a few metrics, like energy costs, technical equipment, storage costs, bandwidth costs, rental fees and a few others.
Afterwards you add a certain percentage on top, depending on how many transactions you are able to process or mine, what your competitors charge and how much profit you want to make.
And voila, you get a realistic price for processing a transaction based on simple market principles and metrics.
You can restrict yourself to running a marathon at once centimeter/minute so everybody on earth, even turtles and slugs can run with you.
Or you can compete against the best 10, 100 or 2016 other runners and find out whats possible.
Ask the best runners in the world how they trained: by competing against the best or by competing against slugs?
1MB blocks versus unbounded blocks.
One system is arbitrarily restricted to 1MB (4MB blockweight), the other one is unbounded.
Only limited by the markets demand for transactions and by technical limitations like processing power, bandwidth and storage capacity.

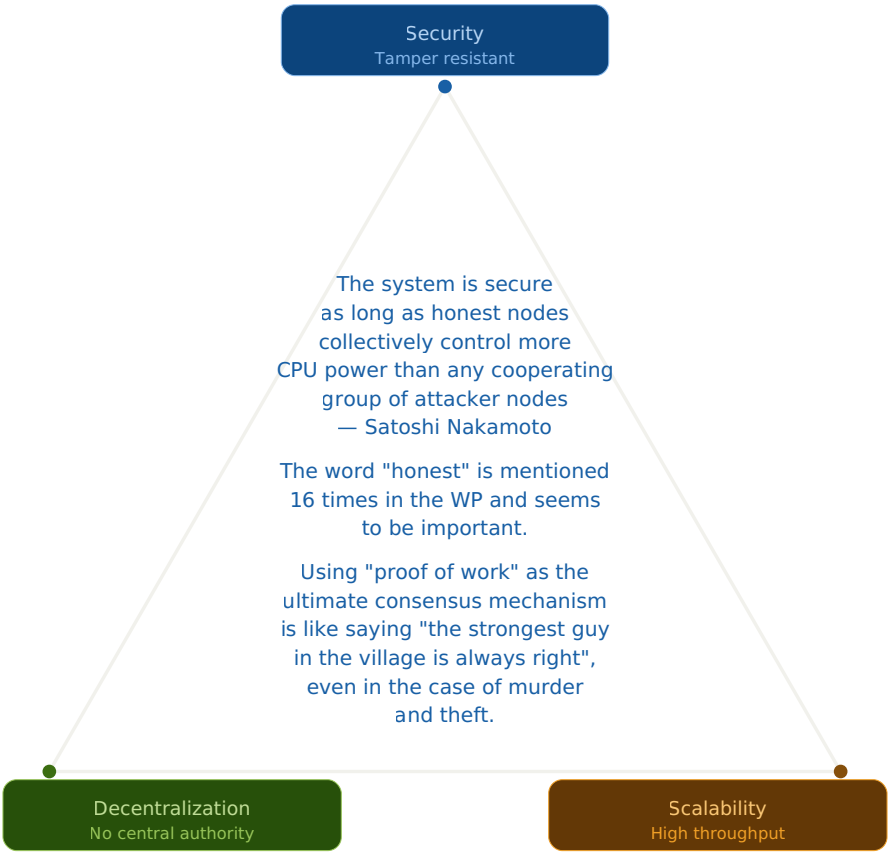
I thought about writing a separate article about “Scalability in bitcoin”, but in my opinion the concept is not that hard to grasp.

Security

Like the decentralization in bitcoin, this is another misunderstood concept in bitcoin.
Since it is highly correlated with proof of work and honesty I recommend you read both of my articles on the topic.
Here is a short excerpt from the introduction of the bitcoin whitepaper:
> “The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a

majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers."

As can be seen, there is a sequence about "a majority of CPU power being controlled by nodes that are not cooperating" which means, that it is not just about hashpower, but about honesty.
Which is the main reason why the word "honest" is mentioned over 16 times in the bitcoin whitepaper.
Nine times in relation with "honest node".
So if you think that the security of the bitcoin network is solely about hashrate, which is equivalent to "brute force" and would be analogous to "the strongest guy is always right", you may eventually find out that you are wrong.
Ask yourself a simple question: do you want to live in a society, where the strongest guy is always right?
Like Ragnar Redbeard states in his book "Might is Right"?
No?
Then you may see "proof of work" not as the ultimate consensus mechanism, but more like a signal and investment up front, which will vanish and be lost in case of getting caught cheating by another bitcoin miner (server operator).
Again, read my article about proof of work.
If you think that the strongest guy in the village can just take your bike, car or house or murder someone else, because he is the strongest guy, then well…good luck with that narrative longterm.
And good luck with the concepts of ownership, possession, law, accountability, fairness, honesty and peace.

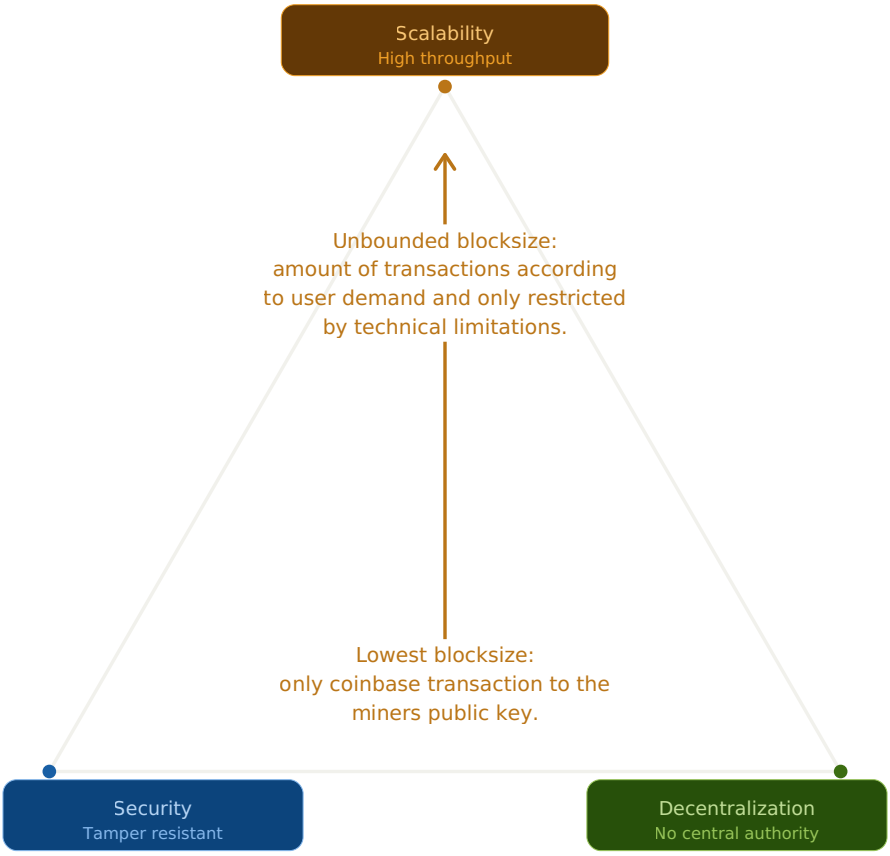


blockchain_trilemma_security

Thievery is thievery, murder is murder and scamming is scamming no matter how strong you may be.
As long as a majority of users has a demand for honesty, accountability, law and truth, bitcoin will come up with the corresponding supply.
Natures concept of demand and supply at work.

The original bitcoin protocol - balance at work

On the original bitcoin protocol, the three variables “security”, “scalability” and “decentralization” can be balanced against each other.
Simple as that.
Some may call it the free market principle of supply and demand.



big_blocks

Picture: All three variables can be balanced out against each other, which would result in a slightly different shaped triangle.
It will never be perfect and will constantly change, similar to your heartbeat, stroke-volume, blood pressure or heart-beat-variability.
But that's the beauty of it.
This is quite easy, since variables can either be increased or decreased while only being restricted by technical or economical thresholds or limits.
If you are familiar with Moore's Law you may know, that processing power, storage capacity and data transmission speeds are all growing exponentially.
Which is the main reason why most people have a super computer in their pockets or on their desk right now on which they are reading this article.

If you want to visualize it, you can imagine a flat triangle being balanced on top of a pencil.
The balance point is most certainly not on one of the corners or edges but somewhere in the center instead.
It is not at the extremes but somewhere in the middle which can be proven mathematically, geometrically and physically.
A lot of nature is just numbers, calculus and geometry.
Like it is said to be stated on Plato's academy in Athens: "Let no man ignorant of geometry enter here!"

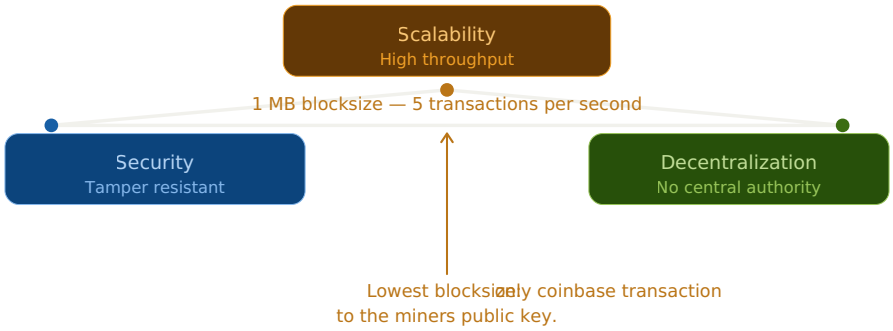
You can focus on just one or two sides, like security and decentralization and completely ignore the third, namely scalability.
You can sacrifice scalability for the goddess of decentralization.
But this is an extreme.
And nature has a tendency for Galton's "regression to the mean", which means, that it will go for a point somewhere in between the two extremes over time.
Extremes are good to test thresholds and to have reference points to actually find the mean or comfort zone.
But they are normally not longterm sustainable without high costs or sacrifices - in this case the sacrifice of "scalability".
Nature flows like a wave, and every wave fluctuates between two extremes.
But the extremes themselves are just reference points for the Gaussian playground in the middle.
The Yin and the Yang with the S-curve in between.
The twilight, wave or snake - which keeps the two sides hidden from each other for an endless godly play.
And sometimes the mean or median can travel up or down.
Due to Moore's Law for example, certain computational metrics have increased over time.
This is also how wealth is created or how it increases.
Wealth is not created by hodling magic numbers though.
You have to use those magic numbers.
Those magically entangled key pairs.
And you should use those magic numbers at scale.
To enable peer-to-peer trade to nourish the magical creation of wealth.

On small block BTC you can use those magical numbers five times per second.
On Big Block Bitcoin the usage is mainly restricted by technical limitations.
At the moment the capabilities are at around one million transactions per second.
And one million isn't the limit or in Satoshis words according to Mike

Hearn:
> “The existing Visa credit card network processes about 15 million Internet purchases per day worldwide.
Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost.
It never really hits a scale ceiling.
If you’re interested, I can go over the ways it would cope with extreme size.”

The blockchain dilemma with 1MB-BTC-Core:

By converting the blocksize variable into a constant of 1MB (4MB blockweight), 1MB-BTC-Core essentially converted the so called blockchain-trilemma into a dilemma.



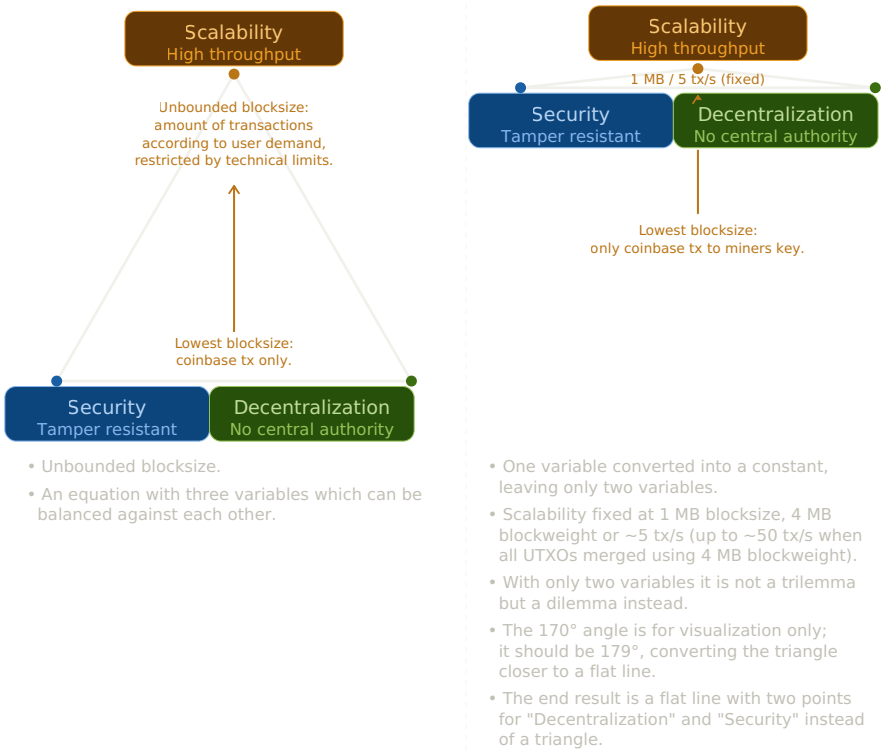
small_blocks

Due to the frozen blocksize of 1MB, the blockchain trilemma on small-block-BTC is like a triangle which is so flat, that it looks more like a straight line than a triangle.
Since you can easily have 1GB blocks, you would have to shrink the size of the triangle on one side by x1000 to adjust for the scale difference.
Which would make it look more like a flat line.
And that is not up for debate, it is a simple and obvious fact and can be verified mathematical and geometrical.
One of the most basic market principles is the law of demand and

supply like already mentioned several times.
It implies, that whenever a market signals a higher demand, it normally is met by other market participants with an equivalent raise of supply, if possible.
On small-block-BTC, this market principle no longer works, since it was artificially and arbitrarily restricted to 1MB - planned economy style.
And since small blockers have completely sacrificed scalability for decentralization, they won't even consider scaling in parallel to Moore's Law.
Coming back to the human body analogy: if you start running a marathon, and the demand for energy rises, your body automatically increases breath frequency, heart rate, stroke volume and blood pressure to supply your muscles with the demanded surplus of energy and oxygen - supply and demand at work.
The variables go up or down to keep a balance and react to external stimuli.
Now convert your variable heart rate into a constant and restrict it to 30 beats per minute and watch what's going to happen.
Spoiler alert: no marathons, no sports and no walks in nature possible.
Lying in bed will be your sole activity.
You have artificially and arbitrarily crippled yourself.
The same happened with small-block-BTC with its 1MB blocksize.
That doesn't necessarily mean, that there are no usecases for small-block-BTC.
But it is not bitcoin as described in the whitepaper by Satoshi Nakamoto.
Additionally the trilemma is actually a dilemma and on top of all that, it was artificially created.
Small-block-BTC is by design unusable as "peer to peer electronic cash", which is the heading of the whitepaper.

Long story short:

I would argue, that there never was a blockchain trilemma in the first place and that it is just an endless self balancing equation with three variables.
And on small-block-BTC it is an artificially and arbitrarily created problem.
Additionally on small-block-BTC it isn't a trilemma, since there are only two variables involved, which makes it more of a dilemma (duos, dos, two).



small_vs_big

If you have any understanding about nature and supply and demand at work, you may come to the conclusion, that there never was a problem with the original bitcoin design.
The small blocker narrative was socially engineered to delay the mass adoption of a global peer-to-peer protocol, with less centralized points of power and potential corruption.
And if you think about what this actually means, you may come to another conclusion: that most people, who have any position of power in our current system, have an interest in bitcoin not being able to scale.
Because if it scales, its game over for most of the power hungry

middlemen and intermediaries world wide.
The end for the control freaks, wannabe dictators, regulators, puppet masters and parasites.
The end for big media, big banks, big tech and big government in its current state.

This probably is one of the main reasons why Jack Dorsey is pushing small-block-BTC-Core.
He has a conflict of interest with his 2009 founded payment provider business Square/Block-Inc.
A scalable bitcoin is directly competing with his business.
And his business is mainly about power and control.
Therefore he and the powers behind him prefer bitcoin to be crippled so they can establish themselves as payment providers to stay in control.
All the so called “second layer solutions” are not bitcoin and they are introducing intermediaries, middlemen and gatekeepers again - welcome back to the old system which bitcoin initially was meant to replace.
They are rich already, but they want to control the payment-, data- and information-streams and those who have access to it.
This can be done through intermediaries, middlemen and gatekeepers like Dorsey or Bill Gates and other people in positions of power like them.

Arbitrary censorship and moderation:

The small blocker narrative took over due to arbitrary censorship and moderation on bitcointalk and reddit.
You can also read Roger Ver’s “Hijacking Bitcoin”.
It is similar to looking back to 2020 and arguing that the media and governments around the world have acted completely ethical and moral during COVID and that people took the vaccination completely unbiased and free from any form of propaganda, censorship or moderation.
And the same people will tell you that the free markets invisible hand has decided and that it was all about the UASF (user activated soft fork).
More about the user activated soft fork in another article, but be aware that instead of using the “proof of work signal”, which can’t be faked, it reintroduced the old account voting system, where one person could fake a potential infinite amount of votes - the irony.

A bitcoin miner has to put his money where his mouth is, whereas a raspberry node essentially can be just an IP-address which is not much of an investment at all and can be faked.

There is nothing wrong with having a different opinion.
I don’t even have a problem with censorship and moderation, if the rules are clear up front.
But using your power to arbitrarily censor and moderate your opposition on established discussion boards and forums essentially means, that your arguments are too weak to stand on their own.
You have lost and time will show.
Time will always show.
Compute will always show.

Thanks for reading!