Proof of Work VS Proof of Stake: Which One Is Better?

Proof of Work VS Proof of Stake: not sure what's the difference between the two? Learn what's the difference between Proof of Work VS Proof of Stake.

By Laura M. - Senior Editor
✓ Fact Checked
Last Updated: May 19, 2021

Are you interested in the **Proof of Work VS Proof of Stake**

argument? Or maybe you just want to know a little more about the process of how to mine Ethereum, Bitcoin, Dash and other popular blockchains that use Proof of Work? Either way, you've come to the right place.

Both of these models are called '*consensus mechanisms*', and they are a **current requirement** to confirm transactions that take place on a blockchain, without the need for a third party. We'll get more into this soon though.

Anyway, in this Proof of Work VS Proof of Stake guide, I am going to start by explaining the **basics of each model**, followed by which popular blockchains have adopted them.

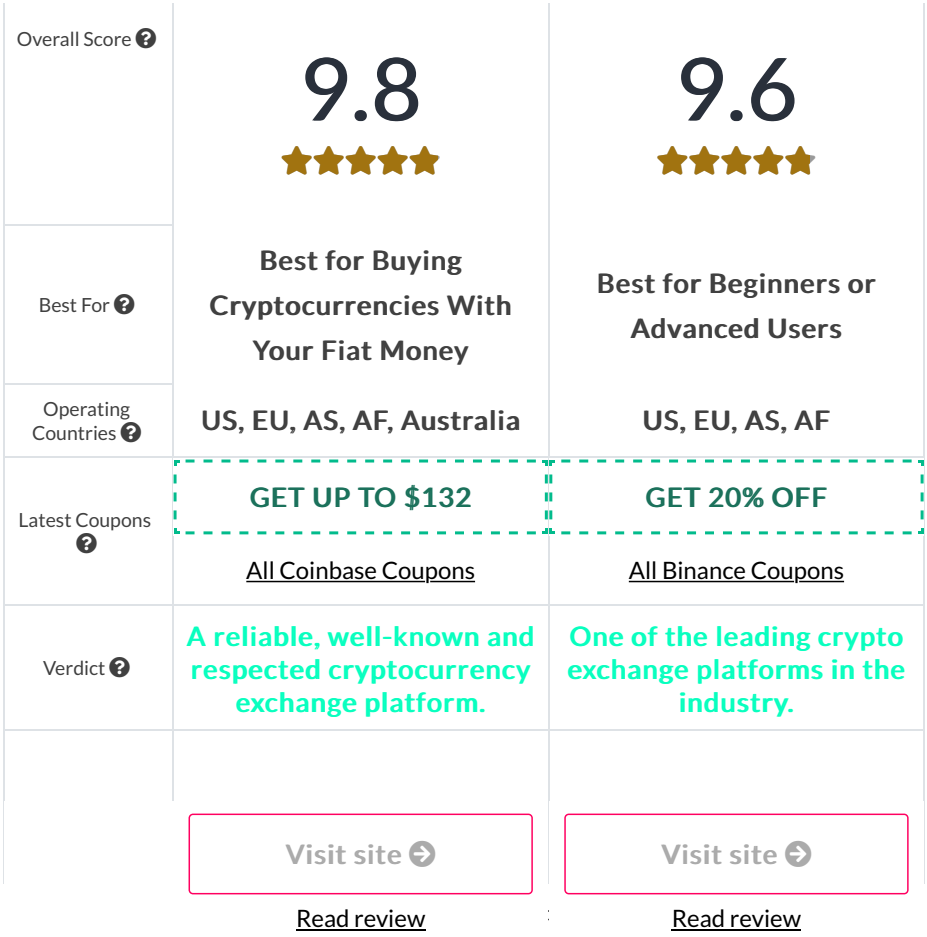
Following that, I am then going to give a really simple explanation about how the technology works and how they allow people to earn extra cryptocurrency by becoming a miner!

Finally, I will then explain why I believe Proof of Stake is a much better model than Proof of Work, as well as giving some **real-world examples** of each model.

By the end of reading my guide from the start to finish, you will be able to comfortably explain to your friends what each consensus mechanism is, how they work and which one is better!

NOTE! It's always crucial to keep your cryptocurrencies in secure wallets, such as Ledger Nano X, Ledger Nano S, or Trezor Model T. Also, if you decide to exchange your cryptocurrencies, you should choose **reliable crypto exchanges**. Coinbase and Binance are among the most popular and reliable options.

	COINBASE	BINANCE
	coinbase	BINANCE

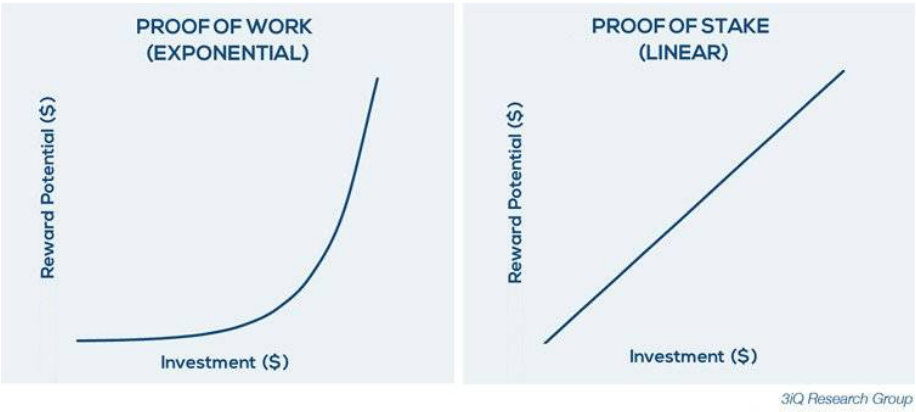


So, what are you waiting for? Let's start with the basics.

Table of Contents

Proof of Stake VS Proof of Work: The Basics

When Satoshi Nakamoto was building the first-ever cryptocurrency, Bitcoin, he had to find a way for transactions to be verified without the need to use a third party. This he achieved when he created the **Proof of Work system**.



Essentially, Proof of Work is used to **determine how the blockchain reaches consensus**. In other words, how can the network be sure that the transaction is valid and that someone isn't

trying to do bad things, such as spend the same funds twice?

Although I will explain it in more detail later on, Proof of Work is based on an **advanced form of mathematics** called '*cryptography*'. This is why digital coins like Bitcoin and Ethereum and called '*cryptocurrencies*'!

Cryptography uses **mathematical equations** that are so difficult that **only powerful computers can solve them**. No equation is ever the same, meaning that once it is solved, the network knows that the transaction is authentic.

Lots of other blockchains copied the original Bitcoin code and as such, also use the Proof of Work model. Although Proof of Work is an amazing invention, it is anything but perfect. Not only does it need **significant amounts of electricity**, but it is also **very limited** in the number of transactions it can process at the same time.

As a result, other consensus mechanisms have been created, with one of the most popular being the **Proof of Stake model**. Proof of Stake was first **created in 2012** by two developers called **Scott Nadal** and **Sunny King**. At the time of its launch, the founders argued that Bitcoin and its Proof of Work model required the *equivalent of $150,000 in daily electricity costs*.

Since then, this figure has increased to millions of dollars, which I will discuss in more detail further down this article.

Anyway, the **first-ever blockchain project** to use the Proof of Stake model was Peercoin. The initial benefits include a **fairer** and **more equal** *mining system, more scalable transactions and less reliance on electricity.*

As a result, the world's second most popular cryptocurrency – Ethereum, is in the process of attempting to move from Proof of Work to Proof of Stake. The Ethereum Proof of Stake date is **yet to**

be confirmed, however, the team is working hard to get there as quickly as possible.

So, now that you know the basics, the next part of my '*Proof of Work VS Proof of Stake*' guide is going to look at which blockchains have adopted each of the two models!

PoW Adoption VS PoS Adoption

The most obvious starting point is to discuss the **original adopter** of Proof of Work, which is the **Bitcoin blockchain**. Every time a transaction is sent, it *takes about 10 minutes for the network to confirm it*. Furthermore, the Bitcoin blockchain can only handle **about 7 transactions per second**.

This has led to **transaction fees** increasing significantly from when the project first **started in 2009**. For example, Bitcoin fees initially cost a very small fraction of a cent, which made the network useful for transferring small amounts. However, as you will see from the **chart below**, this increased to **as much as $40 per transaction** during its busiest period in December 2017!

Source: privacypros.io

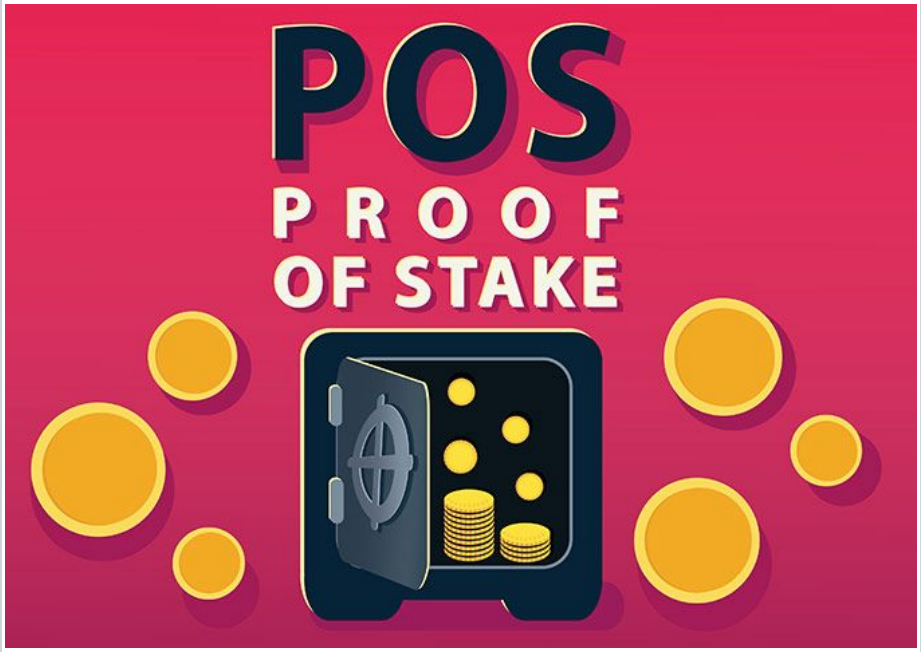
Although these fees have since been reduced, they are still too high to make it **suitable as a global payment system**. Most of these issues are mainly due to the **limits of Proof of Work**.

The second most popular cryptocurrency in the world, **Ethereum** also uses **Proof of Work**. Interestingly, the developers made a few changes to the **original code**, which allowed the network to process **transactions in just 16 seconds**. Although this isn't the fastest in the industry, it is significantly quicker than the 10 minutes it takes Bitcoin.

Nevertheless, the **scalability issues** that Proof of Work has caused Bitcoin is also a problem for Ethereum. The **maximum amount of transactions** that the Ethereum blockchain can process is **15**, which again, is substantially lower than the network needs. However, although the Ethereum Proof of Stake date isn't yet official, it is hoped that it will increase this number to thousands per second.

Just like Ethereum, other blockchains sometimes use a variation of Proof of Work by changing the type of algorithm which **supports the transaction validation process**. Other popular blockchains that have installed Proof of Work include Bitcoin Cash and Litecoin.

On the other hand, some really popular cryptocurrencies now use **Proof of Stake**. One of these is Dash, which allows users to *send and receive funds in just a couple of seconds*.



Another well-known blockchain that uses the Proof of Stake model is NEO. The Chinese smart contract protocol has had an amazing journey since it was first launched in 2016, *increasing the value of its coin by more than 100,000%*!

So, now that you know which popular blockchains use Proof of Work and which use Proof of Stake, the next part of my '*Proof of Work VS Proof of Stake*' guide is going to look at **how transactions are verified**. Let's start with Proof of Work!

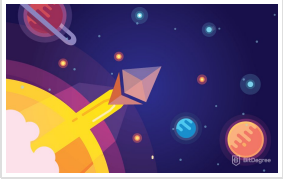
The Most Liked Findings

Looking for more in-depth information on related topics? We have gathered similar articles for you to spare your time. Take a look!

CRYPTO

What is an ICO? Understanding Initial Coin Offerings

The complete guide to understanding what is an ICO and how do Initial Coin Offerings work.



CRYPTO

Ethereum Price Prediction: Will Ethereum Crash?

Read through the Ethereum price predictions, and learn about the cryptocurrency and its price fluctuations!

CRYPTO

How to Create a Cryptocurrency: Tips and Tricks

Wish to know how to create a cryptocurrency? Learn top tips on how to make a cryptocurrency. Start now & find out how to create a cryptocurrency with ease!

Proof of Work: How are Transactions Verified?

As you can imagine, thousands of people use Bitcoin, Ethereum and **other blockchains** that use the **Proof of Work model**. In my example below, I am going to use Bitcoin, however, the process is the same across alternative Proof of Work blockchains.

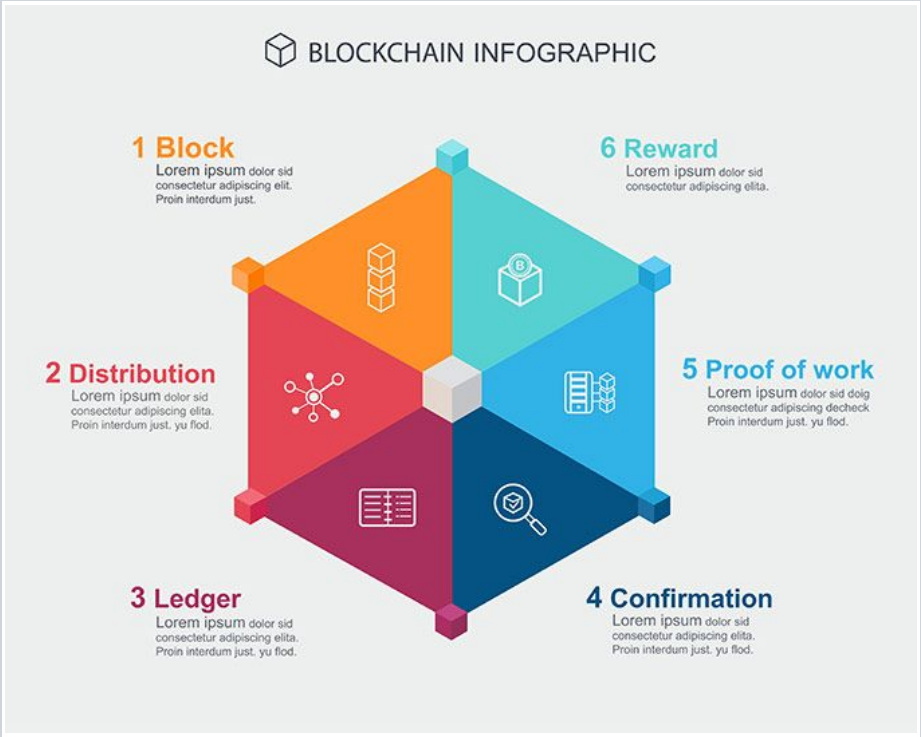
I mentioned earlier that Bitcoin transactions **take 10 minutes** before they are confirmed as valid. Well, in each 10-minute interval, something called a new "*block*" is created.

Every block contains different transactions within it, which must each be **independently verified**. For the Bitcoin network to achieve this without a third party, somebody must use their computational power to **solve a cryptographic algorithm**, otherwise known as Proof of Work.

Once this is achieved, not only is the transaction marked as valid, but it is also posted to the public blockchain for everybody to view. You might be wondering *why somebody would buy hardware and consume lots of electricity just to help confirm Bitcoin transactions*.

Well, the simple answer is that people are **rewarded with additional Bitcoin** (*or whichever cryptocurrency Proof of Work is confirming*) for their efforts. The important thing to understand is that not everybody gets a reward. Thousands of **individual devices** all compete to become the first to solve the cryptographic algorithm. Whoever gets there first, wins the reward.

I'll talk about this in more detail later on, but one of the major issues with Proof of Work is that it is **not a fair system**, because those with the most **powerful** and **expensive** hardware devices will always have the greatest chance of winning the reward.



Moving on, because of the way that the cryptographic puzzle is created, the only way that it can be solved is by using **trial** or **error**. Although I have simplified it significantly, take a look at **the following example**:

1. The Proof of Work mathematical sum = 5+7

2. The answer is 12.

3. Whoever gets the answer first, wins the mining reward.

4. Miner 1 and Miner 2 compete with each other, with the results displayed below.

Miner 1

Attempt 1: *5+7 = 10 *Incorrect**

Attempt 2: *5+7 = 13 *Incorrect**

Attempt 3: *5+7 = 9 *Incorrect**

Miner 2

Attempt 1: *5+7 = 17 *Incorrect**

Attempt 2: *5+7 = 8 *Incorrect**

Attempt 3: 5+7 = 12 *Correct*

As you can see from the above example, it was Miner 2 that guessed the correct answer on the third attempt. That means that they would have been the miner to get the mining reward! In the real world, **computers can guess millions of different combinations per second,** which requires such a large amount of electricity.

Generally speaking, the more powerful the hardware is, or the more hardware devices you have, the more chance you have of solving the puzzle first. I'll talk about this in **more detail** shortly, but for these reasons, *it is not a fair system*.

Before I move on to Proof of Stake, I just wanted to make it clear that although the above example is similar across most Proof of Work models, **some blockchains use a slightly different process**. However, *let's just keep things simple, shall we*?

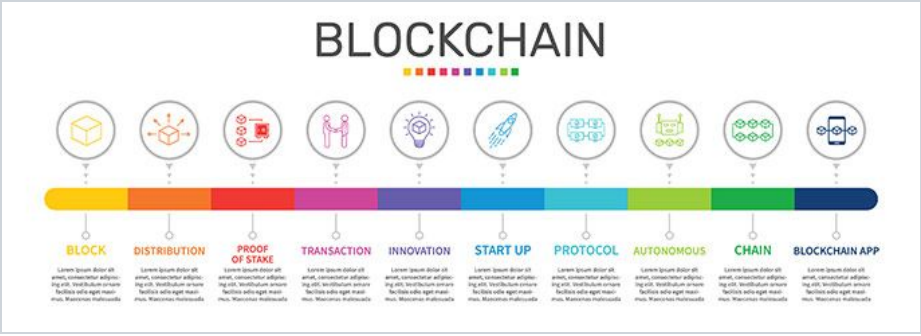
Anyway, now you know briefly how mining Ethereum, Bitcoin and other Proof of Work blockchains operate, the next part of my 'Proof of Work VS Proof of Stake' guide is going to find out how Proof of Work works.

Proof of Stake: How are Transactions Verified?

The **Proof of Stake model** uses a **different process to confirm transactions** and **reach consensus**. The system still uses a cryptographic algorithm, but the objective of the mechanism is different.

While Proof of Work rewards its miner for solving complex equations, in Proof of Stake, the **individual that creates the next block** is based on how much they have '*staked*'. To make things simple for you, the stake is based on the number of coins the person has for the particular blockchain they are attempting to mine.

However, technically speaking, individuals aren't mining. Instead, they are called '*forgers*', because there is no block reward. While Bitcoin, which uses the Proof of Work model, awards a block reward every time a new block is verified, those who contribute to the Proof of Stake system simply **earn the transaction fee**.



Anyway, let's find out how the 'forger' would attempt to successfully verify the transaction...

Firstly, to have the opportunity to validate transactions, the user **must put their coins into a specific wallet**. This wallet freezes the coins, meaning that they are being used to stake the network. Most Proofs of Stake blockchains have a **minimum requirement of coins** required to start staking, which of course requires a large upfront investment.

For example, to validate transactions for the Dash network, you would be required to stake and **freeze a minimum of 1,000 Dash coins**. During the cryptocurrency's all-time high in December 2017, where Dash reached more than $1,500 a coin, it would have cost the real-world equivalent of $1.5 million.

Nevertheless, assuming you have staked the required minimum, your **chances of winning** the reward (*transaction fees*) is linked to the total **percentage of coins you hold**. Take a look at the following example.

1. You decide you want to stake coins to earn some Proof of stake rewards.

2. The blockchain has a total of 1000 coins in circulation.

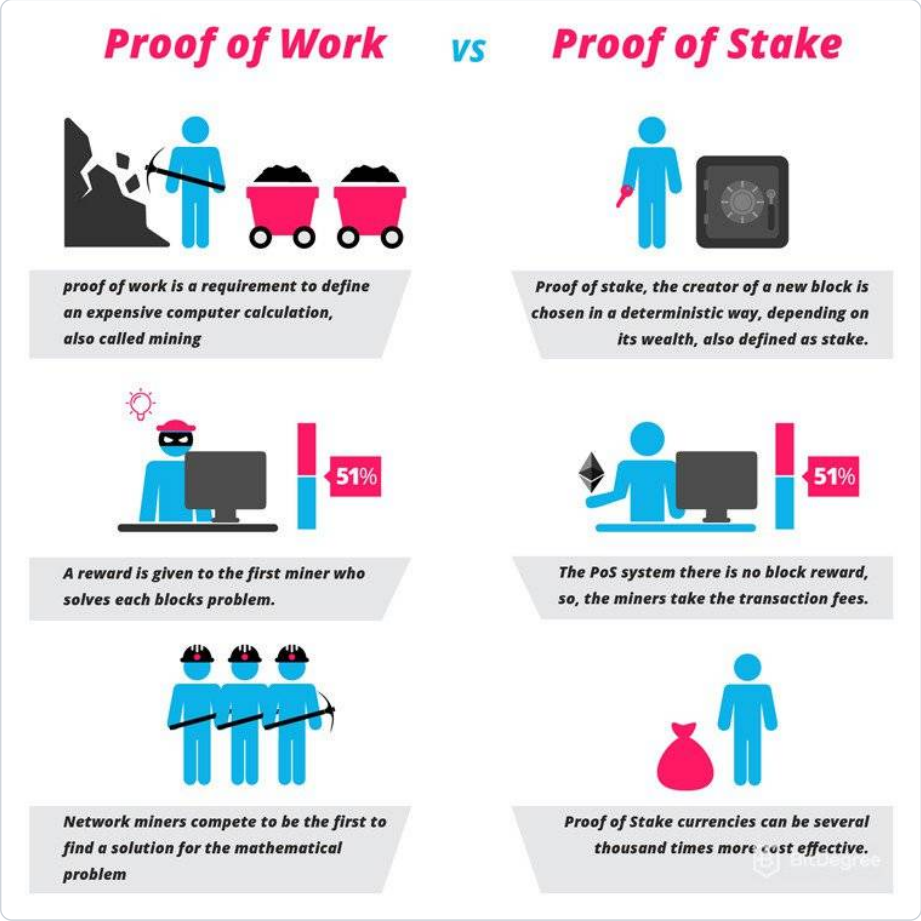
3. Your purchase and stake 100 coins.

4. This means you have staked 10% of the total coins in circulation.

5. You now have a 10% chance of winning every reward.

So, to **clarify**:

- Proof of Work requires ALL of its miners to attempt to solve a complex sum, with the winner determined by the person who has the most powerful/quantity of hardware devices.
- Proof of Stake model randomly chooses the winner based on the amount they have staked.



Source: blockgeeks

The most important **theory supporting the Proof of Stake consensus** mechanism is that those who stake are going to want to *help keep the network secure by doing things correctly*. If a forger attempted to hack the network or *process malicious transactions*, then they **would lose their entire stake**.

This is why the model works so well. The more you stake, the more you earn. But at the same time, the more you lose if you go against the system.

So, now that you know how each consensus mechanism **confirms** and **validates transactions**, the next part of my Proof of Work VS Proof of Stake guide will explain why I believe the Proof of Stake model is much better than Proof of Work!

DON'T FORGET! If you own cryptocurrencies, make sure to get a **secure and trusted hardware wallet** for storing them. *Don't know where to start?*Check out Ledger Nano X and Trezor Model T, they're known as the **top-rated cold wallets**.

Why is Proof of Stake better than Proof of Work?

I believe that the **Proof of Stake model is a much better model than Proof of Work** because it **solves lots of issues**, which I will now break down for you.

Centralization

If you have read my Proof of Work VS Proof of Stake guide up to this point, you might remember that I said Proof of Work blockchains give people who purchase **powerful hardware devices** a greater chance of winning the mining reward.

What this has resulted in is centralized **organizations** buying thousands of devices (known as ASIC's) which generate the highest mining power. This type of operation is known as a 'mining pool' and it allows people to 'pool' their resources together to give them the greatest chance of solving the cryptographic sum first.

Consequently, just four mining pools (of which the majority are located in China where electricity is cheap) **control more than 50% of the total Bitcoin mining power**.

This is an **unfair system** as it means that the average person has no chance of ever winning the mining reward. This is where **Proof of Stake is different**. This model **prevents groups of people joining forces to dominate the network** just to make a profit. Instead, those who *contribute to the network by freezing their coins are rewarded proportionately* to the amount they have invested.

The next example in this '*Proof of Work VS Proof of Stake*' guide is going to discuss electricity consumption.

Did you know?

Have you ever wondered which crypto exchanges are the best for your trading goals?

See & compare TOP3 crypto exchanges side by side

Electricity Consumption

I mentioned earlier in my Proof of Work VS Proof of Stake guide that some Proof of Work blockchains like Bitcoin use **large amounts of electricity**. This is because the **cryptographic sum** that miners must solve is incredibly difficult.

A recent study found that the **total amount of electricity** required to keep the Bitcoin network functional is more than the amount used by **more than 159 individual countries**!

Not only is this bad for the environment, but it also **slows down the rate** at which cryptocurrencies can increase their **real-world adoption**. This is because electricity bills must be paid using fiat currency!

On the other hand, Proof of Stake **does not need highly complex sums** to be solved, meaning that the electricity costs to verify transactions are **substantially lower**.

51% Attack

A **51% attack** is used to **describe the unfortunate event** that a group or single person gains more than 50% of the total mining power. If that happened in a Proof of Work blockchain like Bitcoin, it would **allow the person to make changes** to a particular block. If this person was a criminal, they could alter the block for their gain.

A recent example of a 51% attack happened against the Verge blockchain, which allowed the hacker to walk away with 35 million XVG coins. At the time of the attack, this amounted to a **real-world value of $1.75 million**!

When using a **Proof of Stake** consensus mechanism, it **would not make financial sense** to attempt to perform a 51% attack. For this to be achieved, the bad actor would need to stake at least 51% of the total amount of cryptocurrency in circulation. The only way they could do this is to purchase the coins on the open market.

If they decided to buy an amount this substantial, then the *real-world value of the coin would increase along the way*. As a result, they would **end up spending significantly more** than they could gain from the attack. Not only this but once the rest of the network had realized what had happened, *the bad actor would lose all of their stakes!*

So, now that you know the issues of Proof of Work and how Proof of Stake solves them, the final part of my Proof of Work vs Proof of Stake guide is going to discuss whether there are any **disadvantages to using Proof of Stake**!

Disadvantages of the Proof of Stake Model?

The first concern when discussing Proof of Stake VS Proof of Work is the issue that some people have about Proof of Stake **helping the rich get richer**. This is because the more coins you can afford to buy, the more coins you can stake and earn.

Think of it like this. If you had enough money to meet the minimum staking requirement (which most people don't) then you can guarantee yourself a **very good return on your investment**. Those who have the most money will always have the best chance of winning the reward, making the rich richer.

However, this is almost **no different from the Proof of Work** consensus mechanism, whereby *wealthy miners can simply purchase thousands of ASIC devices.*

The second concern that some people have about Proof of Stake is that it allows people to **verify transactions on multiple chains**, which Proof of Work doesn't. The reason this could be an issue is that it *might allow a hacker to perform a double-spend attack*.

This is when somebody transfers funds to somebody else, but before the transaction is confirmed, they manage to **spend the funds again**. Under normal circumstances, such an attempt would be prevented when all of the other miners on the network see it. Furthermore, because Proof of Work only allows devices to mine on one chain, the dishonest chain would **simply be rejected**.

On the other hand, in a Proof of Stake model, it **doesn't cost forgers any money to mine** on multiple chains, possibly allowing somebody to successfully perform a double-spend. Which is otherwise known as the "'*nothing at stake*' problem?

In reality, the Proof of Stake VS Proof of Work argument is something that will always **divide people's opinions**. However, seeing as though the original way of how to mine Ethereum is going to be changed, it's clear to see which mechanism is the most favored.

Proof of Work VS Proof of Stake: The Conclusion

That's the end of my Proof of Work VS Proof of Stake guide! If you have read it from start to finish, you should now have a good understanding of how each consensus mechanism works, and how they differ from one another.

Proof of Work is the current way how to *mine Ethereum, Bitcoin, Dash, and some other cryptocurrencies*. However, you should now be fully aware of the many issues associated with Proof of Work. This includes the **amount of electricity it requires**, the **centralization of power** that mining pools now have, and the **threats of a 51% attack**.

I have also listed some of the solutions that the **Proof of Stake model** brings to the cryptocurrency industry. However, as blockchain technology becomes more advanced, lots of other consensus algorithms are hitting the market, all with their pros and cons.

Now, if you managed to mine yourself a good amount of cryptocurrencies, you should make sure to keep them in secure wallets. Ledger Nano X and Trezor Model T are among the **most recommended options**. Also, if you decide to exchange them to other coins, choose reliable crypto exchanges, such as Coinbase and Binance.

	LEDGER NANO X	TREZOR MODEL T
	Ledger Nano X	TREZOR Model T
Security Level	Very Poor | Average | Excellent	Very Poor | Average | Excellent
2FA Two-factor Authentification	✓	✓

Multi-signature	✗	✓
Pin Code	✓	✓
Anonimity Level	Very Poor | Average | Excellent	Very Poor | Average | Excellent
Backup Type	24-word Recovery Phrase	12-word Recovery Phrase
Private Key Owner	You	You
Full Wallet Control	No | Partial | Yes	No | Partial | Yes
	Visit site	Visit site
	Read review	Read review

Table: Ledger Nano X and Trezor Model T security comparison.

Leave your honest feedback

Leave your genuine opinion & help thousands of people to choose the best crypto exchange. All feedback, either positive or negative, are accepted as long as they're honest. We do not publish biased feedback or spam. So if you want to share your experience, opinion or give advice - the scene is yours!

Your name

Email

Your feedback

Leave your feedback

FAQ

Is Ethereum Proof of Work or Stake?

Which cryptocurrency exchange is best for

Is Ethereum Proof of Work or Stake?

Ethereum, just like Bitcoin and many other popular cryptocurrencies, uses a **Proof of Work system**. It's mainly used to determine how the blockchain reaches consensus.

What are the main issues associated with Proof of Work?

The **main issues** associated with **Proof of Work** are *the amount of electricity it requires, the centralization of power that mining pools now have, and the threats of a 51% attack.*

How to pick the best crypto exchange for yourself?

Picking out the best crypto exchange for yourself, you should always focus on maintaining a balance between the essential features that all top crypto exchanges should have, and those that are important to you, personally. For example, all of the best exchanges should possess **top-tier security features,** but if you're looking to trade only the main cryptocurrencies, you probably don't really care too much about the variety of coins available on the exchange. It's all a case-by-case scenario!

beginners?

Reading through various best crypto exchange reviews online, you're bound to notice that one of the things that most of these exchanges have in common is that they are **very simple to use.** While some are more straightforward and beginner-friendly than others, you shouldn't encounter any difficulties with either of the top-rated exchanges. That said, many users believe that **Coinbase is one of the simpler exchanges on the current market.**

What is the difference between a crypto exchange and a brokerage?

In layman's terms, a cryptocurrency exchange is a place where you **meet and exchange cryptocurrencies with another person.** The exchange platform (i.e. Binance) acts as a middleman - it connects you (your offer or request) with that other person (the seller or the buyer). With a brokerage, however, there is no "other person" - you come and **exchange your crypto coins or fiat money with the platform in question,** without the interference of any third party. When considering cryptocurrency exchange rankings, though, both of these types of businesses (exchanges and brokerages) are usually just thrown under the umbrella term - exchange. This is done for the sake of simplicity.

Are all the top cryptocurrency exchanges based in the United States?

No, definitely not! While some of the **top cryptocurrency exchanges** are, indeed, based in the United States (i.e. Coinbase or Kraken), there are other very well-known **industry leaders that are located all over the world.** For example, Binance is based in Tokyo, Japan, while Bittrex is located in Liechtenstein. While there are many reasons for why an exchange would prefer to be based in one location over another, most of them boil down to business intricacies, and usually have no effect on the user of the platform.