# [Proof of stake vs. Proof of work](https://forum.cardano.org/t/proof-of-stake-vs-proof-of-work/45273)

A participation testing algorithm, also known by the acronym PoS, is a distributed consensus protocol for distributed networks that secures a network of a cryptocurrency by testing possession of those coins to validate information in the network.

A Test Work System, or PoW System, is a system that, in order to avoid undesired behavior, requires the client of the service to perform some type of work that has a certain cost and is easily verified on the server side. Usually the work consists of performing a computation on the client computer.

**Why is consensus used?**

First, let’s explain why consensus is necessary. In distributed networks there should be no central authority. Consensus means that most participants agree on a certain version of the truth, at a given time. There are many independent authorities, and thus decision-making power is distributed.

**Persistence and security**

Let’s talk first about persistence and security. I have described these properties in more detail, here.

Persistence is the ability to add new blocks continuously. Security means that only valid blocks will be added. Both qualities complement each other.

Bitcoin’s persistence is high because in step 1 there’s a competition among all the mining pools to quickly propose a block. So, if one fails, another one will be ready. This ensures that a new block is eventually ready at a given time. However, it is a very slow process that takes about 10 minutes (sometimes 2 minutes, sometimes 1 hour).

The Cardano protocol actively participates in the choice of the node with the right to create a block. Each node can ask if it has the right to produce the block at a given interval, and all other nodes can verify this. The node must insert a cryptographic test into the block, and sign it. If the node is not available for any reason, the interval remains empty (no blocks). However, this situation is compensated for by the fact that an interval only lasts 20 seconds. So there is a high probability that after the next 20 seconds another available node will produce a block. We could see large delays in block production only if there were no more nodes available at any given time. Eventually, some running node gets the right and produces a block. We can conclude that the persistence is also high compared to Bitcoin, because mainly the period for block production in step 1 is shorter. Still, Bitcoin could be considered a bit better if we don’t worry about other variables such as block irrevocability, transaction speed and commissions.

**Decentralization**

Public competition with PoW leads to having only a few entities that collect decision power. In PoW, the more powerful the participant, the higher the hash rate, wins more often. It makes sense for users to delegate their hash rate to larger pools, as they have a greater chance of being rewarded.

In Cardano PoS, all users with ADA can participate in a consensus algorithm. It is similar to mining, with the difference that there is less risk. Users can buy ADA coins and delegate them to a stake pool. When the user’s ADA achieves the correct creation of a block, the pool will create the block on behalf of the user. Operators and users of the stake pool will be rewarded. In this way, all users are encouraged to participate in the decentralization.

**Security**

To consider a protocol as safe, it must be true that no one can change the history of the ledger. The ledger is distributed in many computers around the world. The attacker has no chance to find all the computers and try to change the ledger of all the hard disks.

Power consumption in PoW was replaced by science and mathematics in PoS. It is more complex and there may be a greater chance that something will go wrong. Still, there is no reason to be afraid and PoS can work well.

**Scalability**

Scalability is the ability to process all transactions as new users join the network. It is easy to scale when the network is used by only a few people. However, it becomes increasingly difficult as the number of users grows gradually.

If we consider that both projects will have a similar block size, then Cardano is more scalable only for the reason that it has a shorter block time. It is 20 seconds against 10 minutes. This is a very approximate comparison, since we should have to compare also the transaction size and other parameters of the project. Within the Shelley Cardano era, it is expected to handle 250 transactions per second (TpS).

In addition, PoS allows the introduction of sharding, so in the future we can expect thousands of transactions per second. For now, let’s conclude that Cardano is more scalable than Bitcoin.

**Fees per transaction**

Transaction fees are influenced by two aspects. Firstly, by the number of transactions that the network is capable of processing at any given time and secondly, by the cost required to keep the network up and running.

In the previous part, I concluded that PoS is more scalable. It is common sense that if the system is more scalable and processes a greater number of transactions, then the fees could be lower to charge the same amount of value.

**Sustainability**

This topic is not discussed much, but I think it is very important. People would like to have digital gold. It’s usually thought to be a Bitcoin. However, I can see some obstacles. Gold is very stable for thousands of years, but Bitcoin is a very young project and has changed radically in the last decade. Gold doesn’t care that we invented electricity, the Internet and distributed networks that are supported by electricity consumption. Bitcoin and other projects depend on it. So protocols can never be as stable as gold. Gold doesn’t need anyone to survive. The protocols do. But we can do everything we can to ensure a high level of sustainability.

**Rewards**

Cardano rewards participants proportionately and fairly according to the ADA tenure of the users. Not so in Bitcoin, where a few major participants get most of the rewards, and small owners of a connected ASIC miner have no chance to create a block. Cardano is fairer than Bitcoin in the reward mechanism.