Proof of Stake and the future of the Blockchain

The proof of stake (PoS) protocol is one of the most significant elements of contemporary blockchain architecture. Not only does it provide efficiency, but it is also cost effective and future-proof. As blockchain technology rapidly expands into fields other than cryptocurrency, the Proof of Work (PoW) protocol is being left behind, mainly because of its inefficiency and archaic nature. While PoW may be useful for cryptocurrencies, PoS is favoured when it comes to unrelated areas such as logistics, big data, artificial intelligence, and other mathematical fields.

As a consensus algorithm, PoS is an elegant solution to creating a trustless system which can be used not just for large-scale currencies like Ethereum but also for smaller institutions. Its use of incentives and penalties also prevents malicious behaviour on both a social level and a computing level.

The Significance of PoS

For those unfamiliar, PoS is a method of validating blocks on a blockchain by having users vote on individual blocks. To be eligible to vote, users must provide a 'stake' which is commonly a currency of some choice. Many Proof of Stake networks such as Lisk demand large quantities of their own currency (LSK) to be staked, therefore raising the bar of entry. The system does not need a huge amount of electricity per user (unlike Proof of Work) allowing it to be used on fairly weak devices such as home computers. With that being said, most PoS systems still drain battery and will degrade computers if used 24/7.

Like every consensus system, Proof of Stake must protect itself from malicious behaviour such as fraudulent blocks and hostile assaults such as 51% attacks. This is where PoS shines as a contemporary mechanism. To prevent 51% attacks, the amount needed to stake for 51% power can be set so high that doing so would no longer be beneficial. This is because staking power can rise exponentially. For instance 10% staking power could be worth $100, whereas 50% could be $100^100 as it can rise exponentially. Validating blocks on invalid or unfavourable chains can also be easily prevented through punishments. Some PoS systems deduct or *burn* a certain amount of staking currency from somebody who tries to validate on minority voted chains.

To fully understand why PoS will forward blockchain technology, we need to compare it to Proof of Work (PoW), the consensus system of Bitcoin, Litecoin and other cryptocurrencies. PoW requires huge electricity for mining, as well as high grade computers which often need upgrading should the system grow larger in size. PoW systems also have a tendency to become a type of 'arm race' between miners. All it would take is for a couple of miners to use high end GPUs (or ASICs) before the majority of miners would *feel* pressured to do so too. This can work for standard cryptocurrencies, but businesses will generally want to avoid it. PoW also struggles with preventing 51% attacks because mining pools can forcefully take a majority position with enough effort. PoS does not suffer from such issues.

PoS for Organisations

An institution or organisation can easily run a PoS blockchain, but they need a few resources. First, they need to have a reasonable amount of people willing to act as validators. For standard cryptocurrencies this can be tough, requiring inventive bootstrapping techniques, but for an organisation this can be as effortless as instructing some employees to take part. The second requirement is that every validator must have something substantial to stake. Currently nobody has discovered a way of running an effective blockchain without having a unique coin/token. These coins/tokens must be created and then given to (or bought by) employees to grant staking rights.

The third requirement is that every staker/validator needs to run their own masternode so that they can vote on certain blocks.

The best way to understand the whole process is to look at a simplified example. Let's say that LogisticsCompany (a fictional organisation) wants to use a blockchain to validate all logistical behaviour. They create a token (LOGC) and decide to set its price to $1.00 per token. 100 LOGC tokens are needed to stake. They offer their employees the option to buy them. The employees then use the LOGC tokens to run a proprietary masternode. Employee can then vote and validate blocks, therefore providing LogisticsCompany with a working blockchain!

Conclusion

It is clear that the Proof of Stake mechanism is forwarding the nature of blockchain technology, making it both desirable and usable to organisations and institutions. Having an immutable and decentralised data entry system is something that many businesses are looking into as it provides a trustless way of keeping information legitimate. With PoS, having a blockchain that does this becomes much simpler.