**Ouroboros How does the protocol work?**

Blockchains require an agreement mechanism known as consensus protocol which is to ensure that only one chain is adopted and followed, otherwise the system would collapse immediately.

**Ouroboros, a participation test consensus algorithm**

In Ouroboros, there is no race between interested parties to produce a block (as in bitcoin PoW). Instead, a slot leader is selected at random, in proportion to the number of tokens it holds (stake), to have a chance to create a new block.

So it’s not the power that gives you the opportunity to produce a new block (and be rewarded for it), it’s the stake that increases your chances of being chosen.

Since there is no race to mine a block, there is no waste of energy or computer resources. In that sense, Ouroboros is a more efficient and economical protocol than the Bitcoin protocol, maintaining all the security guarantees.

The rewards come from two sources: transaction fees and funds drawn from the ADA reserve.

In Ouroboros, the incentives are not dependent on the blocks, but the rewards of a cycle (epoch) are collected from a reserve fund and distributed among the stake pools and the delegating parties that participated during the intervals (slots) in proportion to their participation.

In the case of the pools, each leading pool obtains a fraction of the rewards to cover its operating costs and a profit margin. The rest is distributed among the members of the leading pool, in proportion to the participation they have delegated to it.

**What if for some reason a bifurcation occurs?**

The key feature of Ouroboros Genesis is that, thanks to a single chain selection rule, it allows new or rejoining parties to synchronize with the “good chain” with only one reliable copy of the Genesis block. This makes the protocol safe against the so-called “long-range attack”.

**Self-generated randomness**

The Ouroboros protocol (specifically Ouroboros Praos and Ouroboros Genesis) incorporates a feature called Global Random Oracle that produces a different randomness in each cycle.

This is achieved by implementing a Verifiable Random Function. When evaluated with the key of a stake pool, it returns a random value that is stored in each block produced. The hashing of all values from the previous cycle becomes the random seed for the staking procedure. The block chain itself becomes its source of new randomness.

This is why the protocol is called Ouroboros, the snake that eats its own tail.

**Promoting decentralization**

Finally, the Ouroboros incentive mechanism promotes the decentralization of the system because Ouroboros considers two key scenarios:

1. On the one hand, a stake pool can only act as a delegate if it represents a certain number of stakeholders whose joint participation exceeds a certain threshold, for example, 0.1% of the entire participation in the block chain. This avoids a fragmentation attack, where someone tries to affect the functioning of the protocol by increasing the delegate population.
2. At the same time, when the aggregate participation of a stake pool grows beyond a certain threshold, the rewards become constant. This makes that particular pool less attractive, as stakeholders would not be maximizing their rewards. For example, if the threshold is set at 1%, a stake pool with a 2% share would get the same rewards as one with only a 1% share.

All these features make Ouroboros the best PoS technology to date. And its implementation is exclusively in the Cardano block chain.