

How Cardano's transaction fees work ()

The mathematician working on the protocol's incentives explains the research and IOHK's design

OCTOBER 19, 2017  LARS BRÜNJES (/TEAM/LARS-BRUNJES/)  8 MIN READ



Why do we need transaction fees?

There are two main reasons why transaction fees are needed for a cryptocurrency like Cardano:

People who run full Cardano nodes spend time, money and effort to run the protocol, for which they should be compensated and rewarded. In contrast to Bitcoin, where new currency is created with each mined block, in Cardano, transaction fees are the only source of income for participants in the protocol.

The second reason for transaction fees is the prevention of DDoS (Distributed Denial of Service) attacks. In a DDoS attack, an attacker tries to flood the network with dummy transactions, and if he has to pay a sufficiently high fee for each of those dummy transactions, this form of attack will become prohibitively expensive for him.

How do transaction fees work?

Whenever somebody wants to transfer an amount of Ada, some *minimal fees* are computed for that transaction. In order for the transaction to be valid, these minimal fees have to be included (although the sender is free to pay higher fees if he so wishes). All transaction fees are collected in a virtual pool and then later distributed amongst participants in the Cardano protocol.

How are the minimal transaction fees calculated?

The minimal fees for a transaction are calculated according to the formula

$$a + b \times \text{size},$$

where 'a' and 'b' are constants and 'size' is the size of the transaction in Bytes. At the moment, the constants 'a' and 'b' have the values

a = 0.155381 ADA,
b = 0.000043946 ADA/Byte.

This means that each transaction costs at least 0.155381 ADA, with an additional cost of 0.000043946 ADA per Byte of transaction size. For example, a transaction of size 200 Byte (a fairly typical size) costs

$0.155381 \text{ ADA} + 0.000043946 \text{ ADA/Byte} \times 200 \text{ Byte} = 0.1641702 \text{ ADA}.$

Why did we pick this particular formula? The reason for having parameter 'a' is the prevention of DDoS attacks mentioned above: even a very small dummy transaction should cost enough to hurt an attacker who tries to generate many thousands of them. Parameter 'b' has been introduced to reflect actual costs: storing larger transactions needs more computer memory than storing smaller transactions, so larger transactions should be more expensive than smaller ones.

In order to arrive at the particular values for parameters 'a' and 'b', we had to answer questions like:

- How expensive is one byte of computer memory?
- How many transactions will there be on average per second?
- How large will a transaction be on average?
- How much does it cost to run a full node?

We had to *estimate* the answers to those questions, but now that Cardano is up and running, we will be able to gather statistics to find more accurate answers. This means that 'a' and 'b' will probably be adjusted in future to better reflect actual costs.

We even plan to eventually come up with a scheme that will adjust those constants *dynamically* in a *market driven way*, so that no human intervention will be needed to react to changes in traffic and operational costs. How to achieve this is one focus of our active research.

How are fees distributed?

All transaction fees of a given "epoch" are collected in a virtual pool, and the idea is to then redistribute the money from that pool amongst people who were elected "slot leaders" by the [proof of stake algorithm](#) (<https://www.youtube.com/watch?v=JwxVySVF-U4>) during that epoch and who created blocks.

At this stage of Cardano, where all blocks are created by nodes operated by IOHK and our partners, fees are already collected (to prevent [DDoS attacks](#) (https://en.wikipedia.org/wiki/Denial-of-service_attack)), but they will *not* be distributed and instead will be *burnt*.

As soon as Cardano enters its next, fully decentralized stage, fees will be distributed as described above.

What next?

Coming up with a solid scheme for fee distribution is a challenging mathematical problem: How do we incentivize "good" behavior and promote efficiency while punishing "bad" behavior and attacks? How do we make sure that people who participate in the protocol receive their fair reward, while also ensuring that the best way to earn money with Cardano is to make the system as reliable and efficient as possible? The trick is to align incentives for node operators with the "common good", so that rewards are highest when the system is running at optimal performance.

These are questions studied by the mathematical discipline called *Game Theory* (https://en.wikipedia.org/wiki/Game_theory), and we are proud to have prominent game theorist and Gödel Award laureate Prof. Elias Koutsoupias of the University of Oxford working with us on finding solutions to this problem.

