IOHK | Summit 2019

CV LABS ZUG

CARDANO FOUNDATION

CV VC

Cardano Incentives

Enabling a Fair Decentralized System

About myself

- PhD in Pure Mathematics from Regensburg University (Germany).
- Postdoc at Cambridge University (UK).
- Ten years working in Software Development prior to joining IOHK.
- Haskell enthusiast for more than 15 years.
- Joined IOHK November 2016.
- Director of Education at IOHK.
- Leading the ”Incentives” workstream.

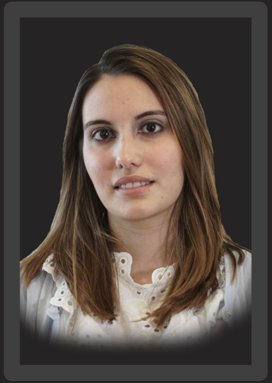
Doing the Hard Work

Prof. Dr. Aggelos Kiayias

Chief Scientist

Prof. Dr. Elias Koutsoupias

Senior Research Fellow



Aikaterini-Panagiota Stouka

Researcher

What are Incentives?

- Incentives in the context of a cryptocurrency are ways of encouraging people to participate in the protocol and to follow it faithfully.
- In the case of Cardano:
  - Being online and creating a block when having been elected slot leader.
  - Providing necessary network infrastructure.

Incentive Types

- In this talk, when we talk about incentives, we mean monetary incentives in the form of ADA.
- There are other types of incentives as well: things like idealism and morality and the general desire to ”do the right thing”.
- Design goal for Cardano incentives: Monetary and moral incentives should align perfectly.

Desired Configuration

- A solid majority of stake (ca. 80%) should be delegated to a number of k stake pools (k ~ 100 seems to be reasonable).
- The stake pools should be online when needed, and they should provide additional network infrastructure (”relay nodes”).

Incentive Sources

- Transaction fees.
- Non-refundable deposits.
- Monetary expansion.

Incentives Distribution

- In Cardano, time is divided into epochs and slots.
- A slot lasts 20 seconds, an epoch contains 21,600 slots and lasts five days.
- Incentives are distributed on an epoch by epoch base: Transaction fees, deposits and monetary expansion are collected into a virtual rewards pool; then this pool is distributed amongst the stakeholders.

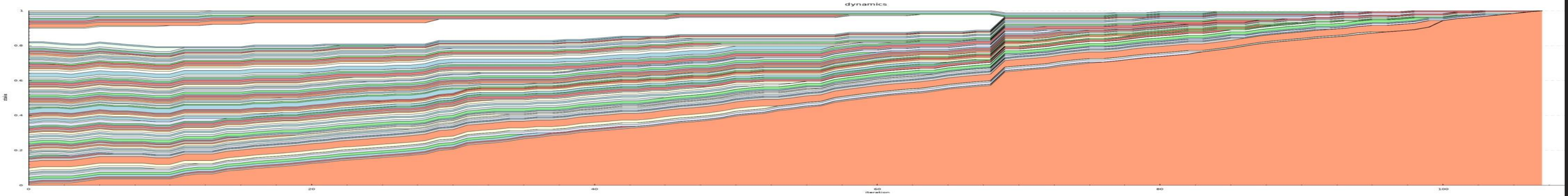
Basic Idea of Distribution

The rewards pool from one epoch is distributed amongst stake pools (and individual protocol participants) according to their stake.

Problem with the Basic Idea

The basic idea is a good guideline, but too naive: The fewer pools there are, the lower total costs will be, the higher everybody’s rewards will be.

So the system will tend towards a single dictatorial pool that everybody else delegates to.



First refinement: Large Pools

The maximal proportion of the rewards pool that a stake pool can receive will be limited by 1/k, where k is the number of desired pools (k ~ 100).

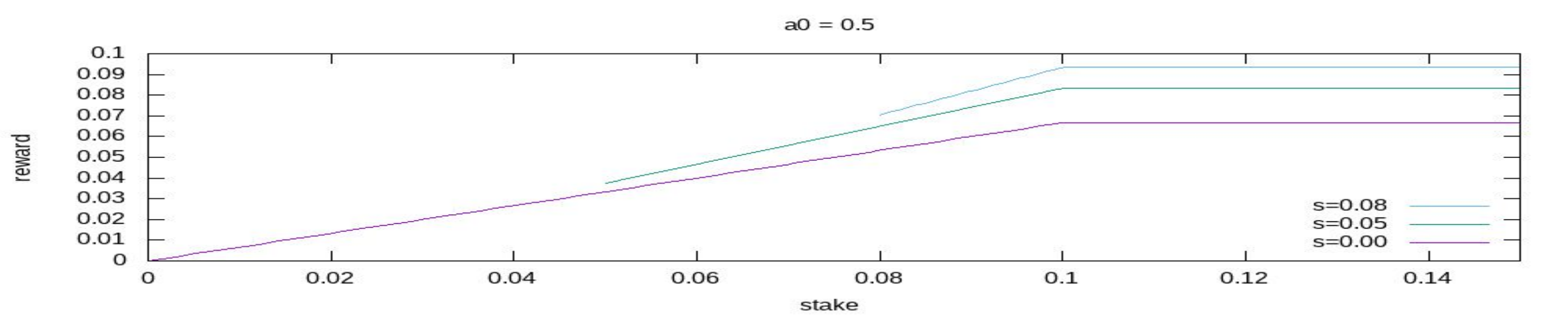
Second refinement: Being Online

- Stake pools should be penalized for not following the protocol and not being online when it is their turn.
- Rewards will be proportional to performance.
- In a protocol without public leader schedule like Ouroboros Praos, performance has to be estimated.

Third refinement: Sybil Prevention

- An attacker could create hundreds of ”attractive” pools and have more than 50% of people delegating to one of them.

- Handled by making pool operators ”pledge” some stake to their pools and make pool rewards depend on the pledged amount.



Undistributed Rewards

- These refinements can lead to a situation where not all funds contained in the rewards pool will be distributed.
- This, however, is a feature, not a bug, because the remaining funds can instead be put to use in the treasury.

Distribution to Pool Members

- The pool leader herself should be compensated for her costs (computing power, online time) and rewarded for her efforts.

- Pool members should be rewarded proportional to the stake they delegated to the pool.

Not Being Short Sighted

- It might seems profitable for a pool operator to change his strategy and increase his margin.
- In reality, of course, pool operators will know that people will leave their pools if they do that.
- So expected rewards displayed in the wallet will ”look ahead” and take into account that only the k most attractive pools will actually have members.

Thank you!