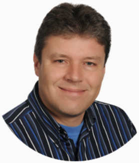
Incentives in Cardano

A Symphony Of Blockchains - London Kick off

Dr. Lars Brünjes, Director of Education at IOHK

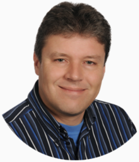
2018-05-15

About myself



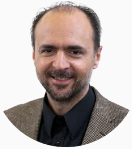
- PhD in Pure Mathematics from Regensburg University (Germany).
- Postdoc at Cambridge University (UK).
- Ten years working in Sofware Development prior to joining IOHK.
- Haskell enthusiast for more than 15 years.
- Joint IOHK November 2016.
- Director of Education at IOHK: Haskell courses (Athens, Barbados, Addis Abeba, ...), responsible for internal and external trainings.

About myself

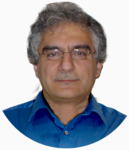


- PhD in Pure Mathematics from Regensburg University (Germany).
- Postdoc at Cambridge University (UK).
- Ten years working in Sofware Development prior to joining IOHK.
- Haskell enthusiast for more than 15 years.
- Joint IOHK November 2016.
- Director of Education at IOHK: Haskell courses (Athens, Barbados, Addis Abeba, ...), responsible for internal and external trainings.
- Leading the "Incentives" workstream.

The people doing all the hard work...



Prof. Aggelos Kiayias, University of Edinburgh (UK), Chief Scientist at IOHK



Prof. Elias Koutsoupias, University of Oxford (UK), Senior Research Fellow at IOHK

Aikaterini-Panagiota Stouka, University of Edinburgh (UK), Researcher at IOHK

Introduction

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 Bitcoin, this means mining blocks and including as many valid transactions in those blocks as possible.

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, it means being online and creating a block when they have been elected slot leader and to participate in the election process.

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.

Participating in the Cardano protocol encurs far less computational costs than participating in Bitcoin.
Nevertheless, having slot leaders online when it is their turn is important for both security and efficiency.

Monetary incentives

In this talk, when we talk about incentives, we mean monetary incentives in the form of ADA.

In exchange for participating in the protocol and supporting the efficient operation of the system, stakeholders get rewarded by a certain amount of ADA.

Other types of incentives

However, it should be noted that there are other types of incentives as well: things like idealism and morality and the general desire to ”do the right thing”.

Other types of incentives

However, it should be noted that there are other types of incentives as well: things like idealism and morality and the general desire to ”do the right thing”.

For example, when the Bitcoin mining pool Ghash.io accumulated 42% of total mining power, people voluntarily started leaving the pool and brought it down to 38% in only two days.

(CoinDesk, 2014-01-09)

Other types of incentives

However, it should be noted that there are other types of incentives as well: things like idealism and morality and the general desire to ”do the right thing”.

The people who left Ghash.io did not receive any Bitcoin for leaving.
Rather, they believed that concentrating too much mining power was *bad* and that leaving was *the right thing to do*.

Other types of incentives

However, it should be noted that there are other types of incentives as well: things like idealism and morality and the general desire to ”do the right thing”.

Ideal

Monetary and moral incentives should align perfectly.

Other types of incentives

However, it should be noted that there are other types of incentives as well: things like idealism and morality and the general desire to ”do the right thing”.

The above example shows that in Bitcoin, this ideal is not always achieved.
Sometimes people have to choose between doing the morally right thing and pursuing their financial gain.

Other types of incentives

However, it should be noted that there are other types of incentives as well: things like idealism and morality and the general desire to ”do the right thing”.

Our goal

In Cardano, we strive for perfect alignment of incentives.

Incentivized behavior in Cardano

As mentioned above, we want to incentivize stakeholders to be online when they have to participate in the protocol (for example to create a block).

People who lack the interest, technical know-how or time to be online when needed can still participate by delegating their stake to a stake pool.

Desired configuration

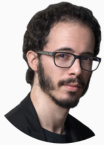
For maximal efficiency and security, a solid majority of stake (ca. 80%) should be delegated to a number of k stake pools ($k \sim 100$ seems to be reasonable).

The stake pools should be online when needed, and they should provide additional network infrastructure (”relay nodes”).

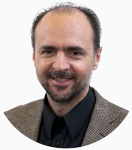
The remaining ca. 20% should belong to ”small” stake holders, who can decide to either participate in the protocol on their own or to simply do nothing.

Delegation

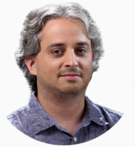
The people behind the delegation mechanism



Dimitris Karakostas, University of Edinburgh (UK), Researcher at IOHK



Prof. Aggelos Kiayias, University of Edinburgh (UK), Chief Scientist at IOHK



Dr. Mario Larangeira, Tokyo Institute of Technology (Japan), Research Fellow at IOHK

Delegating stake in Cardano

Cardano is a Proof of Stake system, so holding stake, i.e. owning ADA, means more than holding Bitcoin means for the Bitcoin protocol.

Cardano is a fully-fledged cryptocurrency, so of course ADA can be used to buy goods or services.

In addition to that, holding ADA also comes with the right (and obligation!) to participate in the protocol and to create blocks.

These two uses of holding ADA can be separated via delegation: A stakeholder can delegate her right to protocol participation while retaining the monetary value.

Control over funds

Note

The act of delegation does not relinquish spending power.
Only the right to participate in the protocol is delegated.
Funds can be spend normally at any time.

Stake pool registration

Somebody wanting to create a stake pool creates a registration certificate and embeds it in a transaction that pays the pool registration fees to a special address.

The certificate contains the staking key of the pool leader (in addition to some meta information like pool costs).

People wishing to delegate to the pool must create delegation certificates delegating their stake to that key.

Scenarios

Using combinations of base- and pointer addresses and ”chains” of delegation certificates, a large number of scenarios can be covered, including

- regular user wallets
- offline user wallets with cold staking
- wallets with enhanced privacy
- staking pool wallets
- enterprise (exchange) wallets

Scenarios

Using combinations of base- and pointer addresses and ”chains” of delegation certificates, a large number of scenarios can be covered, including

- regular user wallets
- offline user wallets with cold staking
- wallets with enhanced privacy
- staking pool wallets
- enterprise (exchange) wallets

Note

For exchange wallets, staking will not be possible. Exchanges are not supposed to use funds entrusted to them for protocol participation.

Mechanism

Transaction fees

There are two main reasons for having transaction fees in Cardano (or any other cryptocurrency):

- 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.
- Important for this talk: To provide funds for incentives.

How 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.

Minimal fees

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

$$a + b \times size$$

where:

- a is a special constant, at the moment it is 0.155381 ADA;
- b is a special constant, at the moment it is 0.000043946 ADA/byte;
- $size$ is the size of the transaction in bytes.

For example, a transaction of size 200 bytes (a fairly typical size) costs:

$$0.155381\ \mathrm{ADA} + 0.000043946\ \mathrm{ADA/byte} \times 200\ \mathrm{byte} \\ = 0.1641702\ \mathrm{ADA}.$$

Minimal fees

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

$$a + b \times size$$

where:

- a is a special constant, at the moment it is 0.155381 ADA;
- b is a special constant, at the moment it is 0.000043946 ADA/byte;
- $size$ is the size of the transaction in bytes.

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.

Minimal fees

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

$$a + b \times size$$

where:

- a is a special constant, at the moment it is 0.155381 ADA;
- b is a special constant, at the moment it is 0.000043946 ADA/byte;
- $size$ is the size of the transaction in bytes.

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.

Minimal fees

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

$$a + b \times size$$

where:

- a is a special constant, at the moment it is 0.155381 ADA;
- b is a special constant, at the moment it is 0.000043946 ADA/byte;
- $size$ is the size of the transaction in bytes.

Although particular values for parameters a and b were calculated, these values will probably be adjusted in future to better reflect actual costs.

Monetary expansion

- Total supply of ADA today: ca. 31,000,000,000 ADA.
- Maximal supply: 45,000,000,000 ADA.

Monetary expansion

- Total supply of ADA today: ca. 31,000,000,000 ADA.
- Maximal supply: 45,000,000,000 ADA.
- So there are almost 14,000,000,000 ADA available for incentives.
- This is a very large amount, but not an infinite one — its use should exponentially decrease over time.

Monetary expansion

- Total supply of ADA today: ca. 31,000,000,000 ADA.
- Maximal supply: 45,000,000,000 ADA.
- So there are almost 14,000,000,000 ADA available for incentives.
- This is a very large amount, but not an infinite one — its use should exponentially decrease over time.

Justification

Over time, when more and more people use Cardano, more and more transaction fees will be available to compensate for the decrease in monetary expansion.

Example of exponential decrease

For an arbitrary example of exponential decrease, we could set the policy of using 5% of the remaining ADA per year for incentives:

year	used for incentives	remaining
1	700,000,000	13,300,000,000
2	665,000,000	12,635,000,000
3	631,750,000	12,003,250,000
4	600,162,500	11,403,087,500
5	570,154,375	10,832,933,125
6	541,646,656	10,291,286,469
7	514,564,323	9,776,722,145
8	488,836,107	9,287,886,038
9	464,394,302	8,823,491,736
10	441,174,587	8,382,317,149

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: All transaction fees of the blocks created during the epoch (together with ADA from 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.

There are two conceivable ways of doing this:

- Proportional to stake controlled at the beginning of that epoch.
- Proportional to the number of slots the stake pool was *elected* slot leader (*not* to the number of blocks created).

Basic idea of distribution

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

There are two conceivable ways of doing this:

- Proportional to stake controlled at the beginning of that epoch.
- Proportional to the number of slots the stake pool was *elected* slot leader (*not* to the number of blocks created).

Note

Due to how the Cardano protocol works, these methods have the same expected reward, because the probability of being elected slot leader is proportional to the controlled stake.

First refinement: large pools

As a first refinement to the basic idea, 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 ($k \sim 100$).

First refinement: large pools

As a first refinement to the basic idea, 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 ($k \sim 100$).

Example

Let us assume $k = 100$, and consider stake pools A and B with 0.3% and 1.2% of stake respectively. Then A will receive 0.3% of the rewards pool, but B will only receive 1%.

First refinement: large pools

As a first refinement to the basic idea, 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 ($k \sim 100$).

Example

Let us assume $k = 100$, and consider stake pools A and B with 0.3% and 1.2% of stake respectively. Then A will receive 0.3% of the rewards pool, but B will only receive 1%.

Motivtion

This policy should prevent stake pools from growing too large.

Second refinement: being online

As explained in the introduction, the whole point of incentives is to incentivize people to follow the protocol.

Thus stake pools should be penalized for not following the protocol and not being online when it is their turn.

Second refinement: being online

As explained in the introduction, the whole point of incentives is to incentivize people to follow the protocol.

Thus stake pools should be penalized for not following the protocol and not being online when it is their turn.

Eligibility

As a consequence, there will be a predicate that, looking at the slots a given stake pool was elected for as leader and the number of blocks it actually created, will decide whether the stake pool is eligible for its share of the rewards pool.

Second refinement: being online

As explained in the introduction, the whole point of incentives is to incentivize people to follow the protocol.

Thus stake pools should be penalized for not following the protocol and not being online when it is their turn.

Remark

This predicate might also not be all-or-nothing, but instead award a certain percentage of available rewards based on adherence to the protocol.

Second refinement: being online

As explained in the introduction, the whole point of incentives is to incentivize people to follow the protocol.

Thus stake pools should be penalized for not following the protocol and not being online when it is their turn.

Note

The predicate can not be as simple as ”created at least $x\%$ of the blocks it was supposed to”, because this could lead to nobody being online towards the end of an epoch.

Undistributed funds

Note that the two refinements explained before 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.

No competition

Note also that the way distribution of funds works implies that there is no competition between pools: There is nothing one pool can do to increase its rewards by decreasing another pool's rewards.

No competition

Note also that the way distribution of funds works implies that there is no competition between pools: There is nothing one pool can do to increase its rewards by decreasing another pool's rewards.

Consequence

There is no incentive for any pool to sabotage another pool's work.

No competition

Note also that the way distribution of funds works implies that there is no competition between pools: There is nothing one pool can do to increase its rewards by decreasing another pool's rewards.

Selfish mining

Attacks like selfish mining or block withholding can not work, because the pools are ”fenced off” from eachother. The actions of one pool only affect its own rewards.

Distribution to stake pool members

After the rewards pool has been split between stake pools, each stake pool leader has to distribute her share of the rewards amongst her pool members, i.e. the people who delegated their stake to her pool.

Distribution to stake pool members

After the rewards pool has been split between stake pools, each stake pool leader has to distribute her share of the rewards amongst her pool members, i.e. the people who delegated their stake to her pool.

The way this happens should follow two guidelines:

Distribution to stake pool members

After the rewards pool has been split between stake pools, each stake pool leader has to distribute her share of the rewards amongst her pool members, i.e. the people who delegated their stake to her pool.

The way this happens should follow two guidelines:

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

Distribution to stake pool members

After the rewards pool has been split between stake pools, each stake pool leader has to distribute her share of the rewards amongst her pool members, i.e. the people who delegated their stake to her pool.

The way this happens should follow two guidelines:

- 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.

Example

As an arbitrary example, consider pool leader Alice with 0.2% of stake, who forms her pool with Bob (0.1% of stake) and Charlie (0.2% of stake).

Example

As an arbitrary example, consider pool leader Alice with 0.2% of stake, who forms her pool with Bob (0.1% of stake) and Charlie (0.2% of stake).

Let us further assume that the reward pool for a fictional epoch contains 5,000,000 ADA and that Alice's pool dutifully created blocks during all slots it was elected slot leader.

Example

As an arbitrary example, consider pool leader Alice with 0.2% of stake, who forms her pool with Bob (0.1% of stake) and Charlie (0.2% of stake).

Let us further assume that the reward pool for a fictional epoch contains 5,000,000 ADA and that Alice's pool dutifully created blocks during all slots it was elected slot leader.

Then Alice's pool, which holds 0.5% of stake, will receive 25,000 ADA from the reward pool for this epoch.

Example

As an arbitrary example, consider pool leader Alice with 0.2% of stake, who forms her pool with Bob (0.1% of stake) and Charlie (0.2% of stake).

Let us further assume that the reward pool for a fictional epoch contains 5,000,000 ADA and that Alice's pool dutifully created blocks during all slots it was elected slot leader.

Then Alice's pool, which holds 0.5% of stake, will receive 25,000 ADA from the reward pool for this epoch.

Of the 25,000 ADA, Bob will get half of what Charlie gets, but Charlie will get less than Alice herself, to reward Alice for the cost and trouble of running her pool.

Example

As an arbitrary example, consider pool leader Alice with 0.2% of stake, who forms her pool with Bob (0.1% of stake) and Charlie (0.2% of stake).

Let us further assume that the reward pool for a fictional epoch contains 5,000,000 ADA and that Alice's pool dutifully created blocks during all slots it was elected slot leader.

Then Alice's pool, which holds 0.5% of stake, will receive 25,000 ADA from the reward pool for this epoch.

If Alice gets an additional 5,000 ADA for her trouble, she would end up with 13,000 ADA, Bob with 4,000 ADA and Charlie with 8,000 ADA.

Example

As an arbitrary example, consider pool leader Alice with 0.2% of stake, who forms her pool with Bob (0.1% of stake) and Charlie (0.2% of stake).

Let us further assume that the reward pool for a fictional epoch contains 5,000,000 ADA and that Alice's pool dutifully created blocks during all slots it was elected slot leader.

Then Alice's pool, which holds 0.5% of stake, will receive 25,000 ADA from the reward pool for this epoch.

Note

This example is purely fictional and meant to explain the idea of reward distribution. It by no means reflects future actual reward amounts!

Thank you!

- Please subscribe to the IOHK YouTube channel!
- Follow us on Twitter: InputOutputHK