

FINE 434: FinTech

Lecture 22

Professor Fahad Saleh

McGill University - Desautels

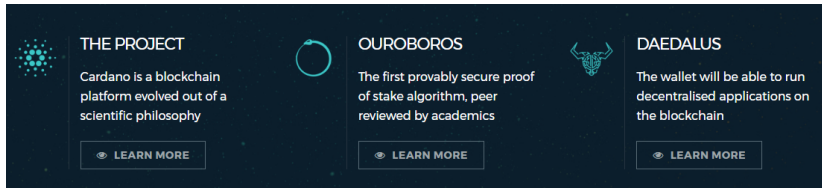





CARDANO

Cardano is a decentralised public blockchain and cryptocurrency project and is fully open source. Cardano is developing a smart contract platform which seeks to deliver more advanced features than any protocol previously developed. It is the first blockchain platform to evolve out of a scientific philosophy and a research-first driven approach. The development team consists of a large global collective of expert engineers and researchers

Cardano is more than just a cryptocurrency, however, it is a technological platform that will be capable of running financial applications currently used every day by individuals, organisations and governments all around the world. The platform is being constructed in layers, which gives the system the flexibility to be more easily maintained and allow for upgrades by way of soft forks. After the settlement layer that will run Ada is complete, a separate computing layer will be built to handle smart contracts, the digital legal agreements that will underpin future commerce and business. Cardano will also run decentralised applications, or dapps, services not controlled by any single party but instead operate on a blockchain.




The banner features a dark blue background with a subtle pattern of small white dots. It is divided into three main sections, each with a distinct icon and a 'LEARN MORE' button. The first section, 'THE PROJECT', uses a cluster of blue dots as an icon. The second, 'Ouroboros', features a blue circular arrow icon. The third, 'DAEDALUS', has a blue bull head icon. Each section contains a brief description of the respective component.



THE PROJECT

Cardano is a blockchain platform evolved out of a scientific philosophy


[LEARN MORE](#)



Ouroboros

The first provably secure proof of stake algorithm, peer reviewed by academics

[LEARN MORE](#)



DAEDALUS

The wallet will be able to run decentralised applications on the blockchain

[LEARN MORE](#)

... so what's the value proposition?

Value Proposition

WHAT MAKES CARDANO SL SPECIAL?

While there are similarities between Bitcoin and Cardano SL, there are also many differences between these two cryptocurrencies. The most significant difference is that Bitcoin is a proof of work type cryptocurrency, while Cardano SL makes use of a proof of stake approach to reach consensus. This encourages honesty and long term participation.

Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol

Aggelos Kiayias*

Alexander Russell†

Bernardo David‡

Roman Oliynykov§

Motivation

WHY PROOF OF STAKE?

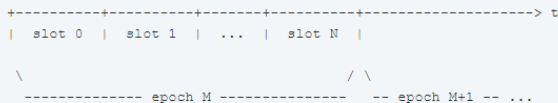
The most important thing about picking a Proof of Stake (PoS) algorithm over a Proof of Work (PoW) algorithm (as adopted by Bitcoin), is the energy consumption considerations. Running the bitcoin protocol is a very expensive endeavor which uses large amounts of energy. It is estimated that 3.8 American households can be powered for a day by the energy that is spent to generate one bitcoin transaction. These energy requirements for running the bitcoin protocol continue to grow as more and more bitcoin miners sink money into mining. In addition, more energy is needed as the difficulty of the problems that their computers or mining rigs, encounter increases. This is why researchers have investigated alternative ways to reach consensus — such as using the so-called BFT (Byzantine Fault Tolerant), consensus algorithms and PoS algorithms.

Let's look at the specific implementation...

Epochs and Slots

EPOCHS AND SLOTS

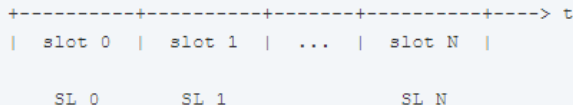
The Ouroboros protocol divides the physical time into **epochs**, and each epoch is divided into **slots**. For example:



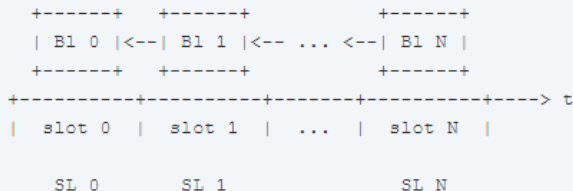
Note: a slot is a relatively short period of time (for example, 20 seconds).

Slot Leaders

Each slot has one and only one leader (slot leader, SL):



The slot leader has a (sole) right to produce one and only one block during his slot:



Honest Majority Assumption

If slot leader missed their slot (for example, when offline), the right to produce a block is lost until they are elected again.

Note: One or more slots can remain empty (without generated blocks), but the majority of blocks (at least $50\% + 1$) **must** be generated during an epoch.

honest majority with advantage ϵ is assumed among those initial stakeholders. Specifically, the environment initially will allow the corruption of a number of stakeholders whose relative stake represents $\frac{1-\epsilon}{2}$ for some $\epsilon > 0$. The environ-

Slot Leader Election

HOW SLOT LEADERS ELECTIONS WORK

Slot leaders are elected from the group of all stakeholders. Please note that not all stakeholders participate in this election, but only ones who have enough stake (for example, 2% of the total stake). This group of stakeholders are known as "electors".

Electors elect slot leaders for the next epoch during the current epoch. Thus, at the end of epoch N it is already known who are slot leaders for the epoch $N+1$, and it cannot be changed.

There are some technical details involved that we overlook here. These details aim to ensure security. Intuitively, we need slot leader selection to be sufficiently random to overcome attacks.

Follow The Satoshi

At this moment, electors have the seed (randomness we need). Now they have to select a particular slot leaders for the next epoch. This is where the Follow the Satoshi (FTS) algorithm comes into effect:

```
      +-----+  
SEED --->| FTS |---> ELECTED_SLOT_LEADERS  
      +-----+
```

To explain how a slot leader gets selected, think of the smallest, atomic piece of value as a coin called "Lovelace". Fundamentally, the ledger produces the distribution of coins, and since slot leaders can only be selected from stakeholders distribution of stake. FTS is an algorithm that verifiably picks a coin, and when coin owned by stakeholder **S** selected, **S** become a slot leader. It is clear that the more coins **S** has, the higher the probability that one of his coins will be picked.

FTS: Implementation

The node sorts all unspent outputs (`utxo`) in a deterministic way (lexicographically), so result is an ordered `sequence` of pairs (`StakeholderId`, `Coin`), where `StakeholderId` is an id of stakeholder (its public key hash) and `Coin` is an amount of coins this stakeholder has. It's assumed that `utxo` isn't empty.

Then the node chooses several random `i` s between `1` and `amount of Lovelaces in the system`. To find owner of `i` -th coin node finds the lowest `x` such that sum of all coins in this list up to `i`-th is not less than `i` (and then `x`-th address is the owner of `i` -th coin).

The result is a non-empty sequence of `StakeholderId`. Ids of selected stakeholders. This sequence of `SlotLeaders` is storing in the `node's runtime context`.

Cardano Roadmap

- ▶ Testnet Era
- ▶ **Bootstrap Era**
- ▶ Reward Era
- ▶ ...

Current Era

The Bootstrap era is the period of Cardano SL existence that allows only fixed predefined users to have control over the system. The set of such users (the bootstrap stakeholders) and proportion of total stake each of them controls is defined in genesis block.

Purpose of Bootstrap era is to address concern that at the beginning of mainnet majority of stake will probably be offline (which breaks the protocol at the start). Bootstrap era is to be ended when network stabilizes and majority of stake is present online.

The next era after Bootstrap is called [the Reward era](#). Reward era is actually a "normal" operation mode of Cardano SL as a PoS-cryptocurrency.