Cardano Staking and Pledging, Simply Explained

Presented by Allison Fromm

@allison_fromm

October 2020

Table of Contents

A Introduction to Cardano

- This presentation is designed to introduce the general concepts and the **non-technical** process of staking and to those with a basic awareness of the Cardano project
- If you are new to Cardano, the video linked below provides an excellent overview
- Don't be alarmed by the whiteboard — the explanation is easy to follow and does not require technical knowledge
- https://www.youtube.com/watch?v=Ja9D0kpksxw

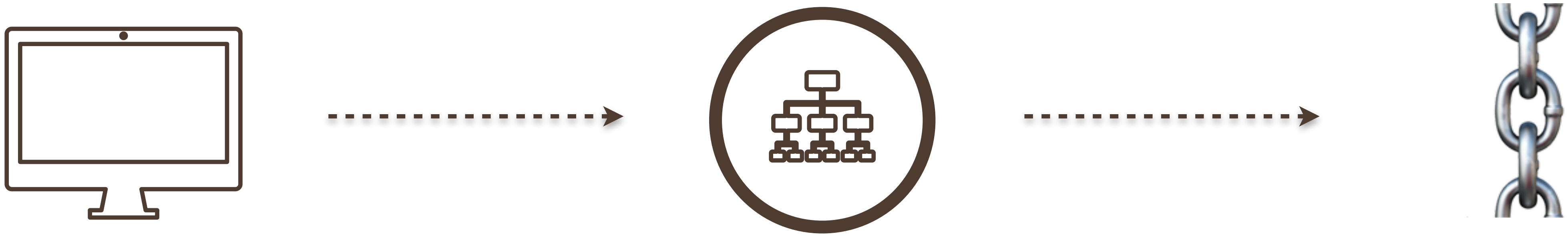
IOHK | Cardano whiteboard; overview with Charles Hoskinson

A A Few Introductory Terms

- **Proof of Stake** systems are one way to create secure, unchangeable, decentralised records of transactions in a **Blockchain** because a large number of independent **Nodes** collectively maintain the **Blockchain**; Cardano is a **Proof of Stake** system

- A **Blockchain** is a permanent method of storing transactional records while ensuring security, transparency, and decentralisation; it is a chain of records stored in the form of **Blocks** which are controlled by no single authority

- A **Block** is a group of transactions that are packaged together by a particular **Node** and added to the **Blockchain**



Node

Block

Blockchain

A A Few Introductory Terms, cont.

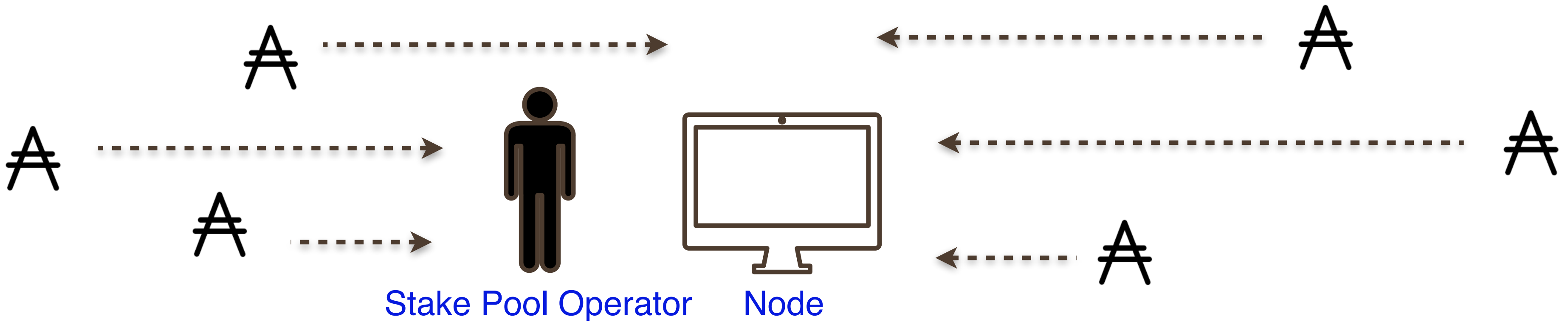
- A **Node** is a computer running certain software that does the work of maintaining the system and may process transactions for a particular **Pool**

- **Pools** are groups of **ADA** holders who have deposited their **ADA** with a **Pool Operator** in exchange for receiving **Rewards*** of more **ADA**

- **Pools** are managed by **Pool Operators**

- A **Stake Pool Operator (SPO)** is someone with technical skills and some amount of **ADA**, who is willing to invest time and resources to operate a **Node** and manage a **Pool**

- **ADA (₳)** is the currency or token used in the Cardano system



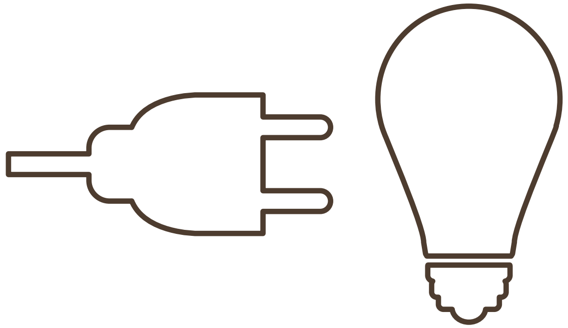
*A bit of patience is needed for the definition of **Rewards**; I promise it is coming, but we need to cover a few other things first

B What is Staking?

- **Staking** means depositing **ADA** into a specific **Pool**
- **Staked ADA** always remains under the control of the individual holder (not the **Stake Pool Operator**) and the individual can spend/transfer the **Staked ADA** at any time
- Individuals are willing to **Stake** their **ADA** to a particular **Pool** due to the expectation of receiving **Rewards** in the form of more **ADA**
- The **Staked ADA** is referred to as **Stake**

What is Proof of Work? How is it Different from Proof of Stake?

- Bitcoin, a **Proof of Work (PoW)** system, revolutionised the transfer of value because the technology behind Bitcoin allows many unrelated actors (**Nodes**) to work together to process transfer of value transactions
- These unrelated **Nodes** do not need to trust each other because in a **PoW** system, each demonstrates their commitment to honestly maintaining the system by expending significant amounts of energy to produce **Blocks**
- Given the amount of energy required to maintain the system, each unrelated **PoW Node** has an incentive to act honestly because they have “skin in the game” and are committed to the honest and reliable functioning of the system
- If they cheat, or produce a bad **Block**, other **PoW Nodes** ignore it and all of that energy the **Node** spent is wasted
- In **Proof of Stake (PoS)** systems, **PoS Nodes** prove their commitment to the system by **Staking**
- A large amount **Stake** demonstrates the **PoS Node's** legitimacy to maintain the record of transactions
- If a **Node** cheats, or produces a bad **Block**, other **PoS Nodes** ignore it and the **Pool** does not earn any **Rewards**
- **PoS** systems use much, much less electricity than **PoW** systems

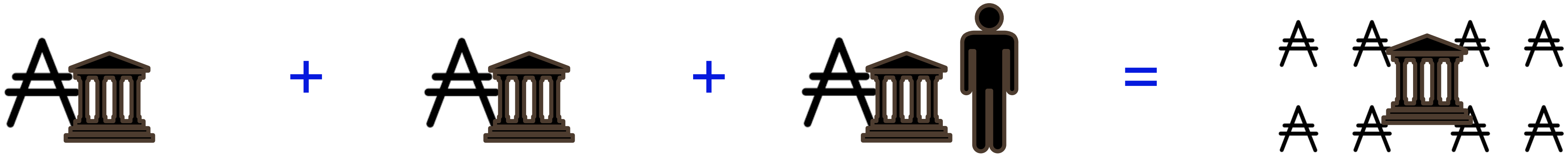


D What is the Difference between Pledging and Staking?

- **Staking** is the the process of depositing **ADA** into a **Pool**, in order to maintain the **Blockchain**, and with the expectation of receiving more **ADA** as a **Reward**

- **Stake** has different meanings, depending on who is depositing the **ADA**

- To avoid confusion, this presentation uses the following definitions:
  - **Individual Stake** - amount of **ADA** deposited by an individual who is not a **Pool Operator**
  - **Pool Operator Stake** - amount of **ADA** deposited by a **Pool Operator,** also referred to as **Pledge**
  - **Pool Stake** - total amount of **ADA** in a particular **Pool,** comprised of **Pool Operator Stake/Pledge** plus **Individual Stakes**
  - **Total Stake** - total amount of **ADA** in existence



Individual Stake

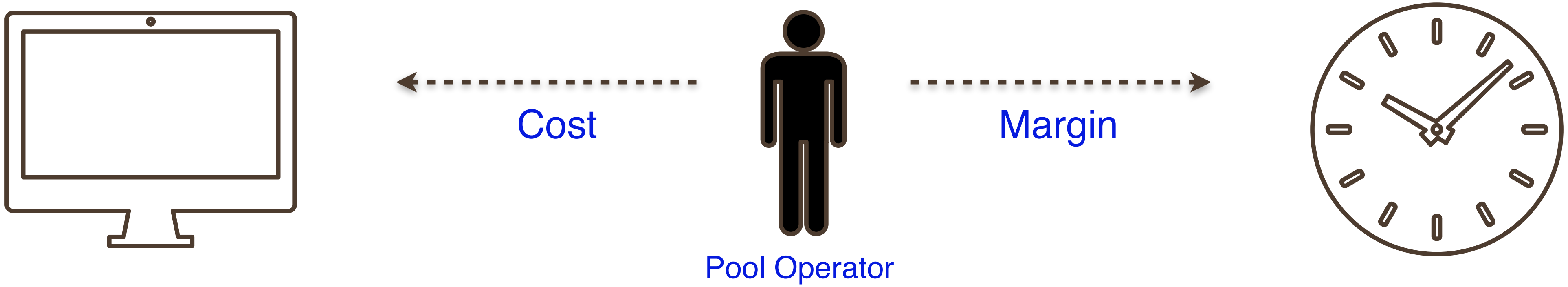
Individual Stake

Pool Operator Stake / Pledge

Pool Stake

E I want to be a Pool Operator. What should I think about?

- **Pool Operators** will need to spend money on the hardware and software required to set-up, register, and run a **Pool**
- **Cost** is the amount of money **Pool Operators** spend on that hardware and software
- **Pool Operators** will also need to spend time setting up, running, and maintaining the **Node**
- The portion of the **Reward** that compensates **Pool Operators** for their time is called the **Margin**



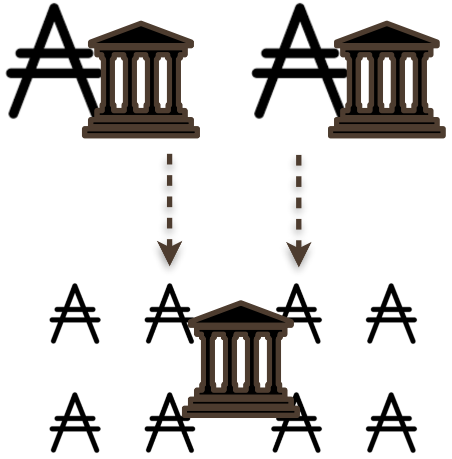
Cost

Margin

Pool Operator

E I want to be a Pool Operator. What else should I think about?

- In order to register the **Pool** on the blockchain, the **Pool Operator** must pay a small registration fee and indicate their **Cost, Margin,** and **Pool Operator Stake (Pledge)**
- The optimal amount of **Pool Operator Stake** will be determined by the different **Pools** competing against each other*
- While a **Pool Operator** is always free to remove or spend the **Pool Operator Stake,** if the **Pool Operator Stake** amount drops below the amount indicated during registration, the **Pool** will not earn any rewards
- Importantly, nothing in the system requires a particular level of **Pool Operator Stake; Pool** competition simply determines the *optimal* amount of **Pool Operator Stake** needed to maximise rewards
- In order to increase **Rewards**, the **Pool Operator** will typically need a way to convince other **ADA** holders to join the **Pool**



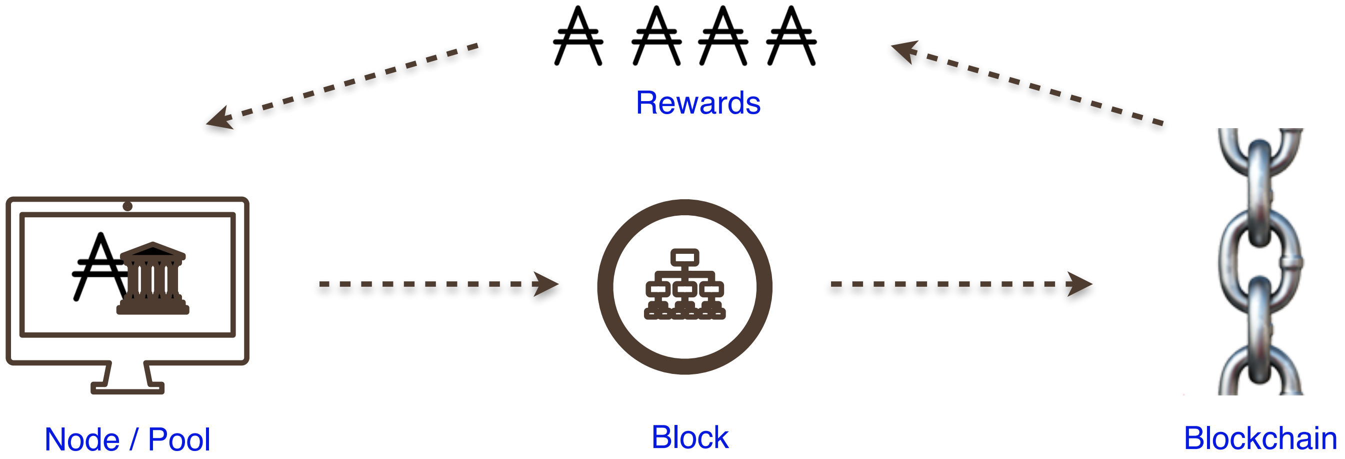
*There is a lot of complex math behind these concepts, which will be mentioned at the end

F Can We Please Talk about Rewards Now?

- Unlike a bank, which processes transactions based on customers trust that the bank will operate honestly, there is no centralised, trusted authority monitoring, storing, and processing **ADA** transactions

- Remember that **Proof of Stake** systems work because a large number of independent and diverse **Pools** collectively maintain the **Blockchain**

- Each **ADA** holder deposits their **ADA** in a **Pool** because they expect to receive **Rewards**



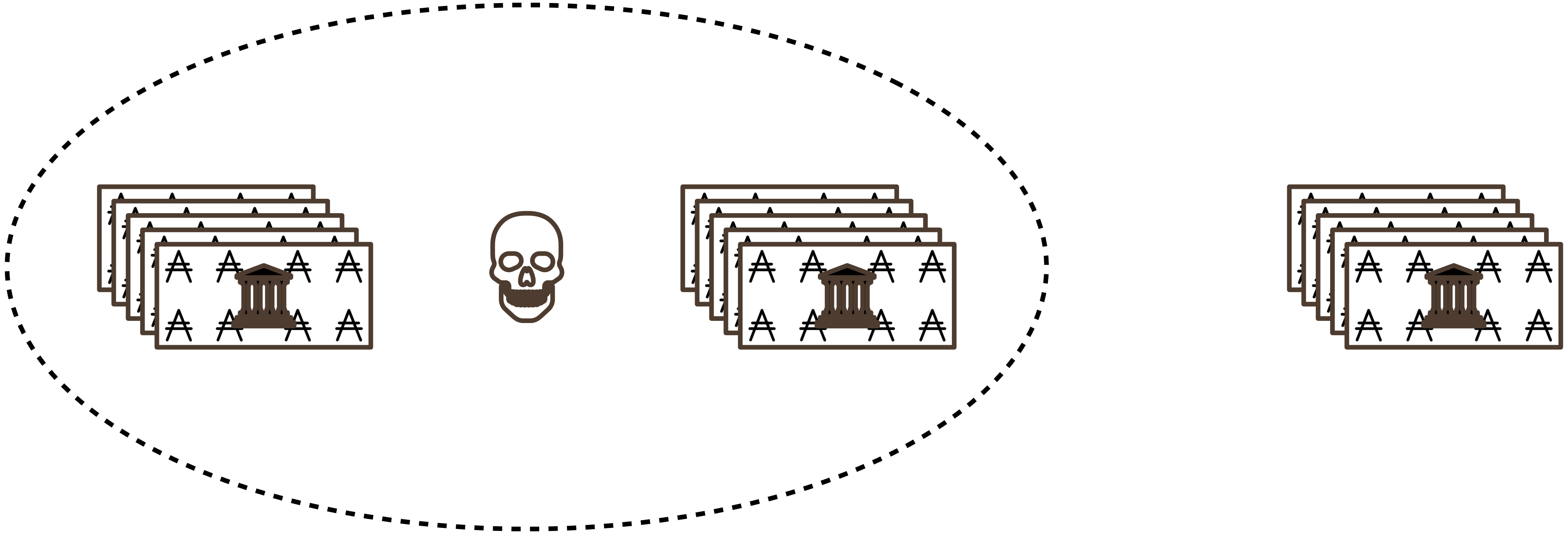
Can We Please Talk about Rewards Now?

- The **Blockchain** is programmed to give out **Rewards** based on a few guiding principles:
  - **Rewards** earned by a **Pool** are generally proportional to the amount of **Pool Stake**, up to a certain point (more on this on slide 19)
  - **Pool** numbers should remain high, avoiding ever greater centralisation (as happens with **Proof of Work** systems)
  - There should be a diverse number of individuals within each **Pool**
  - Individuals should want to deposit their **Individual Stake** with high performing **Pools**
  - There should be a way to protect against **Sybil Attacks***

*Don't panic about this term, just go to the next page!

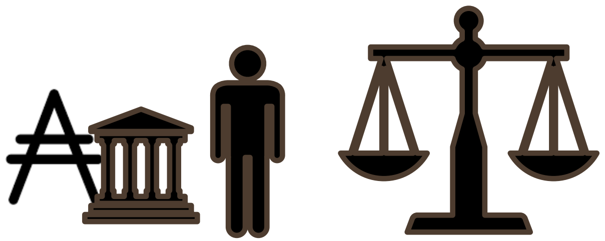
G What the Heck is a Sybil Attack?

- **Proof of Stake** systems face a difficult challenge - with no central authority defending the system, who guards against the bad actors?
- **Proof of Stake** systems build protections into the **Blockchain** in order to guard against different attacks
- A **Sybil Attack** is when a single bad actor creates a large number of **Pools** in order to take control of the system



What the Heck is a Sybil Attack?

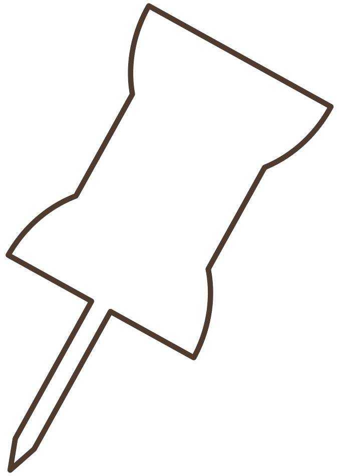
- The Cardano system guards against **Sybil Attacks** in two related ways*:
  - **Pledging -**
    - In order to build a **Pool,** a **Pool Operator** must **Pledge** some of their own **ADA** (the **Pool Operator Stake**)
    - The **Pool Operator Stake** amount is high enough to make it very expensive for a single person to create a large number of **Pools**
  - **Rewards -**
    - Complicated math is used to calculate the amount of **ADA** distributed to each **Pool** and **Pool Operator** as a **Reward**
    - **Pools** with higher amounts of **Pool Operator Stake** will earn slightly higher **Rewards** because of the larger **Pool Operator Stake**
  - The Cardano system will ensure that **Pool Operator Stake** is high enough so that it is expensive to create a large number of **Pools,** but not so high that the only **Pool Operators** are only those with a very large amount of **Pool Operator Stake** (Whales)



*There is a lot of complex math behind these concepts, which will be mentioned at the end

H All this Theory is Great, but What’s in it for Me?

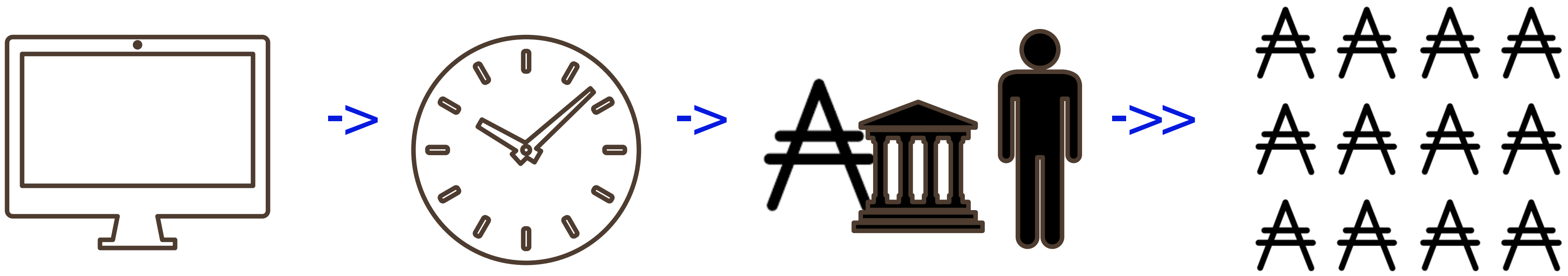
- First, a quick recap:
  - Back on Slide 11, we said that when **Pool Operators** register their **Pool** on the **Blockchain,** each **Pool Operator** announces their **Cost,** their **Margin,** and the amount of **Pool Operator Stake**
  - Slide 10 said that the **Pool Operator’s Cost** is the amount of money the **Pool Operator** spends to set-up, register, and run the **Node**
  - Slide 10 also said that **Pool Operators** earn a **Margin** (which is a percentage) that pays them for the time they spend operating the **Node** and running the **Pool**
  - Slide 15 explained why the **Pool Operator Stake** must be a reasonably high number



All this Theory is Great, but What’s in it for Me?

- And now for the **Pool Operator’s Reward!**

- The **Pool Operator’s Reward** depends on their **Cost,** their **Margin,** and the amount of **Pool Operator Stake**:
    - When the **Reward** is distributed to a **Pool,** the **Pool Operator** first gets to keep an amount equal to their **Cost**
    - Next, the **Pool Operator** gets to keep the **Margin,** which is a percentage of the remaining **Reward**
    - Whatever is left after those two deductions is given to each person in the **Pool,** according to the amount of **Individual Stake**
    - As a result, for the **Pool Operator,** the third portion of their **Reward** will depend on the amount of their **Pool Operator Stake / Pledge**



Cost -> Margin -> Pool Operator Stake ->> Reward

I I Don’t Want to Run a Pool. Can I Still Get Rewards?

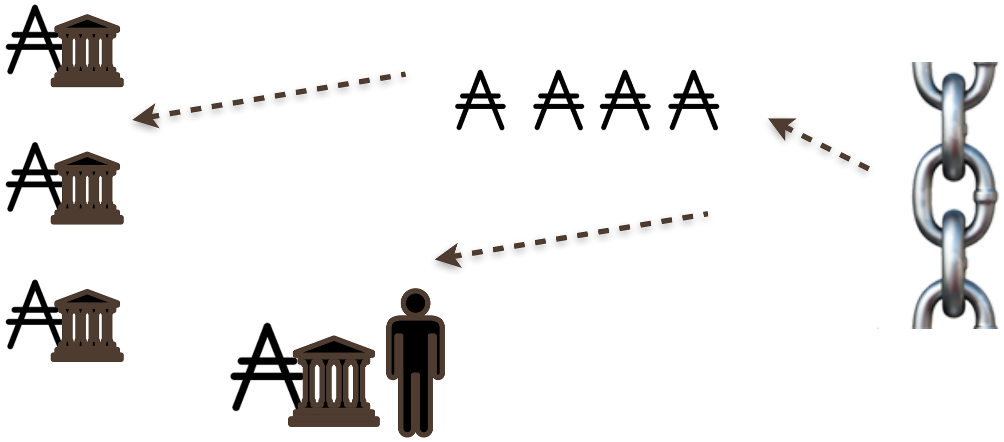
- Anyone can **Delegate** (or deposit) their **ADA** to a **Pool** and share in the **Rewards** of that **Pool;** the individual is a **Delegator**

- Any **ADA Delegated** by an individual is the **Individual Stake**

- The **Delegator** retains control of the **Delegated ADA** and can spend it any time

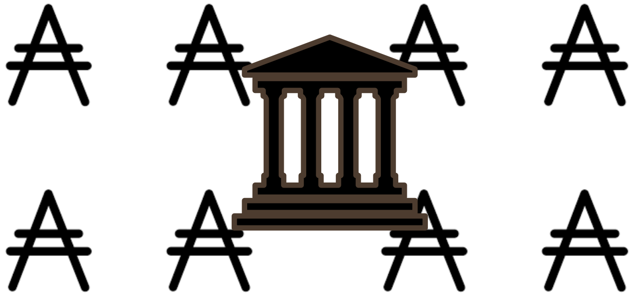
- **Delegated ADA / Individual Stake** must be **Staked / Delegated** to a **Pool** in order to receive **Rewards**

- **Rewards** are distributed automatically, by the **Blockchain**, to each **Pool** and to each **Delegator**



I Don’t Want to Run a Pool. Can I Still Get Rewards?

- Here are a few things for **Delegators** to think about in choosing a **Pool:**
  - **Rewards** are bigger for **Pools** that aren’t yet **Saturated**
  - A **Pool** is **Saturated** when it has a lot of **Pool Stake** and a lot of individuals contributing their **Individual Stake**
  - **Reliability** - the strength of the **Node’s** technology and ability to create **Blocks** as scheduled
  - **Cost** - the fixed amount deducted from the **Pool’s Reward** before the **Delegators’** share
  - **Margin** - the percentage deducted from the **Pool’s Reward** before the **Delegators’** share
  - **Pool Operator Stake** - the amount of **ADA Pledged** by the **Pool Operator**
- **ADA** wallets (Deadalus and Yoroi) will rank **Pools** based on these factors



J Where do Rewards Come From?

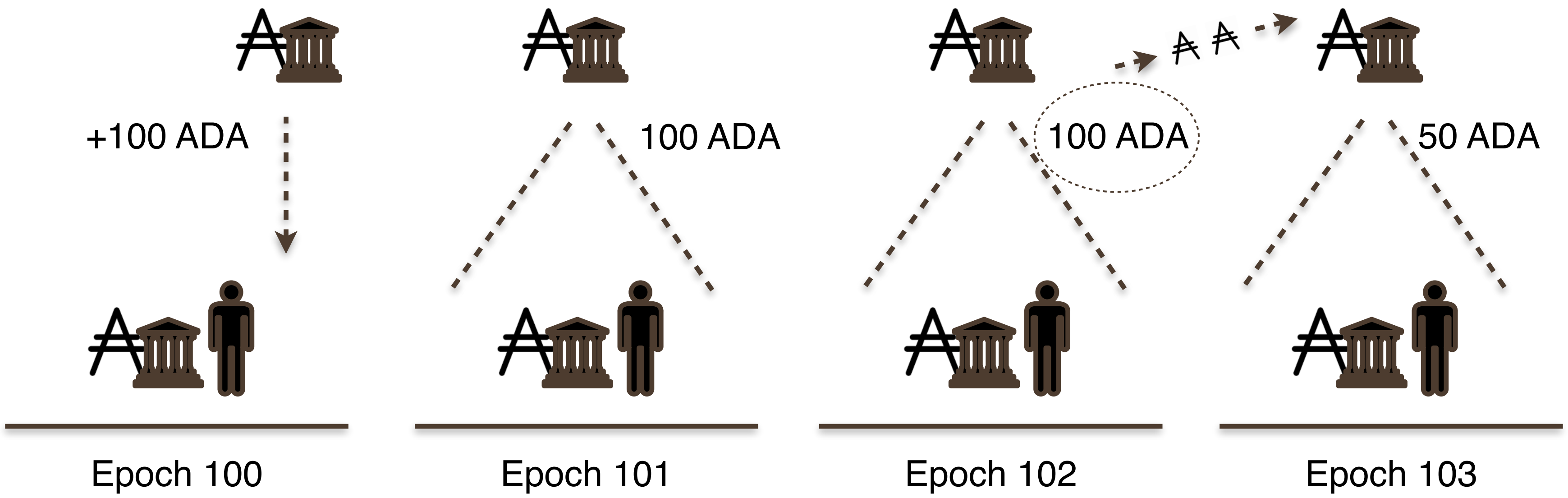
- The two primary sources of the **ADA** that is used for **Rewards** are:
  - New **ADA** that the Cardano Blockchain creates according to a set schedule, until there is total amount of 45 billion **ADA** in existence*
  - Transaction fees paid by every individual who uses the Cardano system for a transaction
- Once the total **ADA** in existence reaches 45 billion, the main source of rewards will be the fees users pay for sending transactions on the Cardano system

*There is a lot of complex math behind this concept, which will be mentioned at the end

K Do I Really Have to Understand These Other Technical Terms?

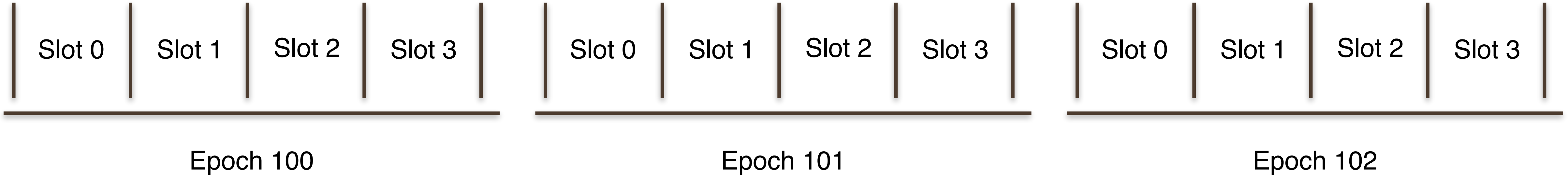
- Nope! But if you do want to understand more, here are a few things to think about:

- **Epoch** - an amount of time; 5 days on Shelley Mainnet
- Before collecting **Rewards,** individuals must leave their **Individual Stake** in a particular **Pool** for at least one full **Epoch**
- In the timeline below, the individual **Delegates 100 ADA** with a **Pool** at the end of **Epoch 100**; no **Rewards** are calculated for **Epoch 101**
- In **Epoch 102, Rewards** are calculated based on the **100 ADA** on deposit; those rewards are paid in **Epoch 103**
- Recall that an individual always retains control of the **Individual Stake;** if the individual spends some **ADA** in **Epoch 103,** the new balance will only impact future **Reward** calculations



Do I Really Have to Understand These Other Terms, cont.

- **Slot** - an arbitrary division of each **Epoch**
  - During each **Slot** one **Block** may be created
  - The **Node** creating a **Block** for a particular **Slot** is the **Slot Leader**
  - **Minting** (or creating) a **Block** is another way of saying that a **Node** is packaging together transactions into a **Block**
  - According to a mathematical lottery, the **Blockchain** assigns **Nodes** a certain number of **Slots** in each **Epoch**
  - **Pool Rewards** depend on a **Node's** ability to **Create Blocks** during the assigned **Slot**



Slot 0 Slot 1 Slot 2 Slot 3

Epoch 100

Slot 0 Slot 1 Slot 2 Slot 3

Epoch 101

Slot 0 Slot 1 Slot 2 Slot 3

Epoch 102

K Do I Really Have to Understand These Other Terms, cont.

- **ROA (Return on ADA)** or **ROS (Return on Stake)** or **ROI (Return on Investment)**- refer to the amount of **ADA** earned in **Rewards** compared to the amount of **Pledged ADA;** can be calculated for individuals or for **Pool Operators**

- **A0,** also referred to as **Alpha,** is part of the mathematical formula that determines **Rewards** and has an impact on **Pool** rankings in **ADA** wallets
  - Lower values of **A0** favour **Pools** with low **Costs**
  - Higher values of **A0** favour **Pools** with higher **Pool Operator Stake**
  - The higher **A0,** the more resistant the system is to **Sybil Attacks**
  - The lower **A0,** the easier it will be for small **Pool Operators** to compete
  - The value for **A0** will balance between allowing small **Pools** to compete and protecting the system against **Sybil Attacks**
  - The initial value for **A0** is 0.3, which can be adjusted later, if necessary

- **K** is the optimal number of **Pools** in the system; **K** will initially be set at 150 and will increase over time

- **Z0** is the mathematical representation of the **Saturation** point, and is defined as **1/K**

- At the **Saturation** point, the amount of **Rewards** stops increasing

- If new individuals **Delegate Individual Stake** to a **Saturated Pool,** the **Reward** for everyone in that **Pool** will decrease

L *Why Should I “Trust” that all of this is Really “True”?

- All the Cardano code is Open Source, which means that anyone can review it to see that the ideas captured in this presentation are actually built into the software
- The guiding ideas, principles, and theories behind the code (and briefly summarised here) were developed by academics in the fields of computer science, software engineering, cryptography, economics, and game theory
- Those academics published their research in papers that were “peer reviewed,” which means other, unrelated, equally qualified academics rigorously tested the concepts and mathematics in those papers, and agreed that the work was legitimate and reasonable
- All of those papers are readily available to anyone who wants to read them
- Since no human being can ever be an expert on everything, as participants in collective society, we must decide how to make decisions in areas where we are not experts; in other words, whom do we trust?
- In the past, banks served as the experts who could be trusted to manage financial transactions, but recent history provides many examples of abuse of this trust
- In contrast, Cardano’s Open Source code and academic, peer-reviewed underpinnings provide a different and incredibly strong source of validation and reason for trust
- **The Cardano team’s work demonstrates that the ideas presented in this presentation are being reliably implemented into the code base, and represent a healthy, safe, sustainable, and fair method of establishing and running a decentralised financial system**

M Useful Links that Informed this Presentation

- Adatainment Website - https://www.adatainment.com/index.php?page=home&lang=en
- Cardano effect podcast about pledge, rewards, and network security —https://www.youtube.com/watch?v=X-ziLksiPOE&feature=youtu.be
- Cardano Forum — https://forum.cardano.org/
- Cardano Overview - https://www.youtube.com/watch?v=Ja9D0kpksxw
- Delegation and Incentive Paper — https://www.adatainment.com/_downloads/docs/delegation_design_spec.pdf
- Emurgo video explaining incentives paper — https://www.youtube.com/watch?v=2pdkIXDU1no&list=PLFLTrdAG7xRbAqhF3Tg8BeAea7Ard-ttn
- IOHK Blog - https://iohk.io/en/blog/posts/page-1/
- Reward Sharing Schemes for Stake Pools — https://arxiv.org/ftp/arxiv/papers/1807/1807.11218.pdf
- Why Cardano paper — https://cardano.org/why/

Alphabetical Glossary

- **A0,** also referred to as **Alpha,** is part of the mathematical formula that determines **Rewards** and has an impact on **Pool** rankings in **ADA** wallets
- **ADA (₳)** is the currency or token used in the Cardano system
- **Block** is a group of transactions that are packaged together by a particular **Node** and added to the **Blockchain**
- **Blockchain** is a permanent method of storing transactional records while ensuring security, transparency, and decentralisation; it is a chain of records stored in the form of **Blocks** which are controlled by no single authority
- **Cost** is the amount of money **Pool Operators** spend on the hardware and software required to set-up, register, and run a **Node**
- **Delegation** is when an individual deposits **ADA** in a **Pool** and shares in the **Rewards** of that **Pool;** the individual is a **Delegator**
- **Individual Stake** - amount of **ADA** deposited in a **Pool** by an individual who is not a **Pool Operator**
- **K** is the optimal number of **Pools** in the system
- **Margin** is the portion of the **Reward** that compensates **Pool Operators** for their time
- **Minting** is when a **Slot Leade**r creates a **Block** for a particular **Slot**
- **Node** is a computer running certain software that does the work of maintaining the system and processing transactions
- **Pledge** typically refers to the **Pool Operator Stake**
- **Pools** are groups of **ADA** holders who agree to **Stake** (or deposit) their **ADA** exchange for receiving **Rewards** of more **ADA; Pools** are managed by **Pool Operators**
- **Pool Operator** is someone with technical skills and some amount of **ADA**, who is willing to invest time and resources to operate a **Node** and manage a **Pool**
- **Pool Operator Stake** - amount of **ADA** deposited by a **Pool Operator;** while the **Pool Operator** can move the **Pool Operator Stake** at any time, if the **Pool Operator Stake** drops below the amount indicated during **Pool** registration, the **Pool** will not earn **Rewards**
- **Pool Stake** - total amount of **ADA** in a particular **Pool,** comprised of **Pool Operator Stake** plus **Individual Stakes**

Alphabetical Glossary, cont.

- **Proof of Stake (PoS)** systems are one way to create secure, unchangeable, decentralised records of transactions in a **Blockchain** because a large number of independent **Nodes** collectively maintain the **Blockchain**; Cardano is a **Proof of Stake** system
- **Proof of Work (PoW)** systems have **Nodes** demonstrating their commitment to honestly maintaining the system by expending significant amounts of energy to produce **Blocks**
- **ROA (Return on ADA)** the amount of **ADA** earned in **Rewards** compared to the amount of **Pledged ADA;** can be calculated for individuals or for **Pool Operators**
- **ROI (Return on Investment)** - same as **ROA**
- **ROS (Return on Stake)** - same as **ROA**
- **Reliability** - the strength of the **Node's** technology and ability to create **Blocks** as scheduled
- **Rewards** are the **ADA** the **Blockchain** pays to **Pools** in return for their **Staked ADA**
- **Saturation** is when a **Pool** has a lot of **Pool Stake** and a lot of individuals contributing their **Individual Stake** (see **Z0**)
- **Slot -** an arbitrary division of each **Epoch;** During each **Slot** one **Block** should be Created
- **Slot Leader** is the **Node** creating a **Block** for a particular **Slot**
- **Stake Pool Operator (SPO) -** same as a **Pool Operator**
- **Staking** is the action of depositing **ADA** in a **Pool,** and the deposited **ADA** is referred to as **Stake**
- **Sybil Attack** is when a single bad actor creates a large number of **Pools** in order to take control of the system
- **System Stake** - total amount of **ADA** in existence
- **Z0** is the mathematical notation for the **Saturation** point, and is defined as **1/K** of the **System Stake**