Emurgo

Blockchain España Meetup

Presentador:
Nicolás Arqueros - CTO, Emurgo

EMURGO

CARDANO

¿Qué es Cardano?

Breve descripción

Cardano es un **blockchain**
que busca entregar
más funcionalidades avanzadas
que cualquier otro protocolo
desarrollado previamente.

CARDANO FOUNDATION

INPUT | OUTPUT

EMURGO

Temas

1. Filosofía de trabajo
2. Problemas en la industria
3. Superioridad Técnica
4. Stake Pools
5. Preguntas

1. Filosofía de Trabajo

Research

Peer Review

High Assurance And Formal Verification

2. Superioridad Técnica

La industria tiene algunos problemas

Conoce a Cardano

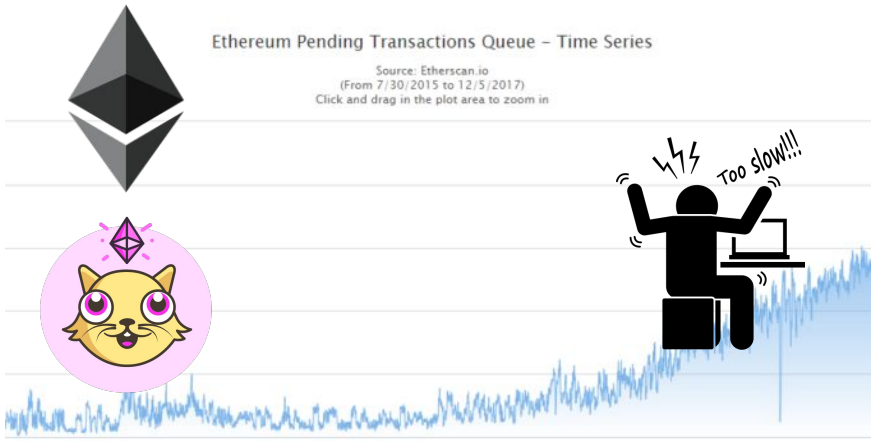
- **Escalabilidad**
- **Interoperabilidad**
- **Sustentabilidad**

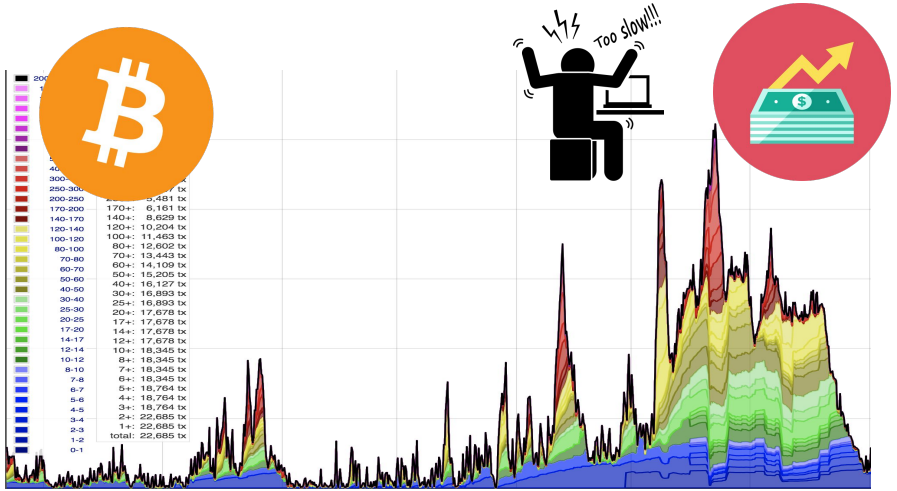
Siguiente nivel de Smart Contracts

¿Cuáles problemas?

Escalabilidad

de transacciones, tamaño del blockchain y red





Escalabilidad

de transacciones, tamaño del blockchain y red

Tamaño de Ethereum-blockchain ha superado los 1TB

Hacks

El peligro de Smart Contracts!

Parity Freeze
Parity's multisig wallet
The DAO
Input Overflow (Abril 2018)
Y muchos otros...

Sobre $350 millones de dólares PERDIDOS

Financiamiento?

Desarrollo de software necesita dinero

Proyectos se han movido desde Bitcoin a Ethereum por motivos de financiamiento.

Pero el financiamiento es para proyectos que utilizan tokens y no para protocolo.

Conoce a Cardano

Escalabilidad

Peer Review Research

Ouroboros
(Primer provably secure PoS)

Ouroboros Praos
(Practicalidad)

Ouroboros Genesis
(Proof of stake resuelto!)

***Ouroboros Hydra**
(Rendimiento a través de Sharding)

* Under research

Interoperabilidad

Sidechains

(Otras blockchain)

Autenticación y Cumplimiento usando metadatos

(Industria tradicional como la banquera)

Sustentabilidad

Gobierno Comunitario usando Democracia Líquida

Integración con el protocolo para tesorería y votación.

Siguiente nivel en Smart Contracts

Smart Contracts

- **Verificación Formal**
- **K-Framework (KEVM, IELE)**
- **Plutus**
- **Marlowe**

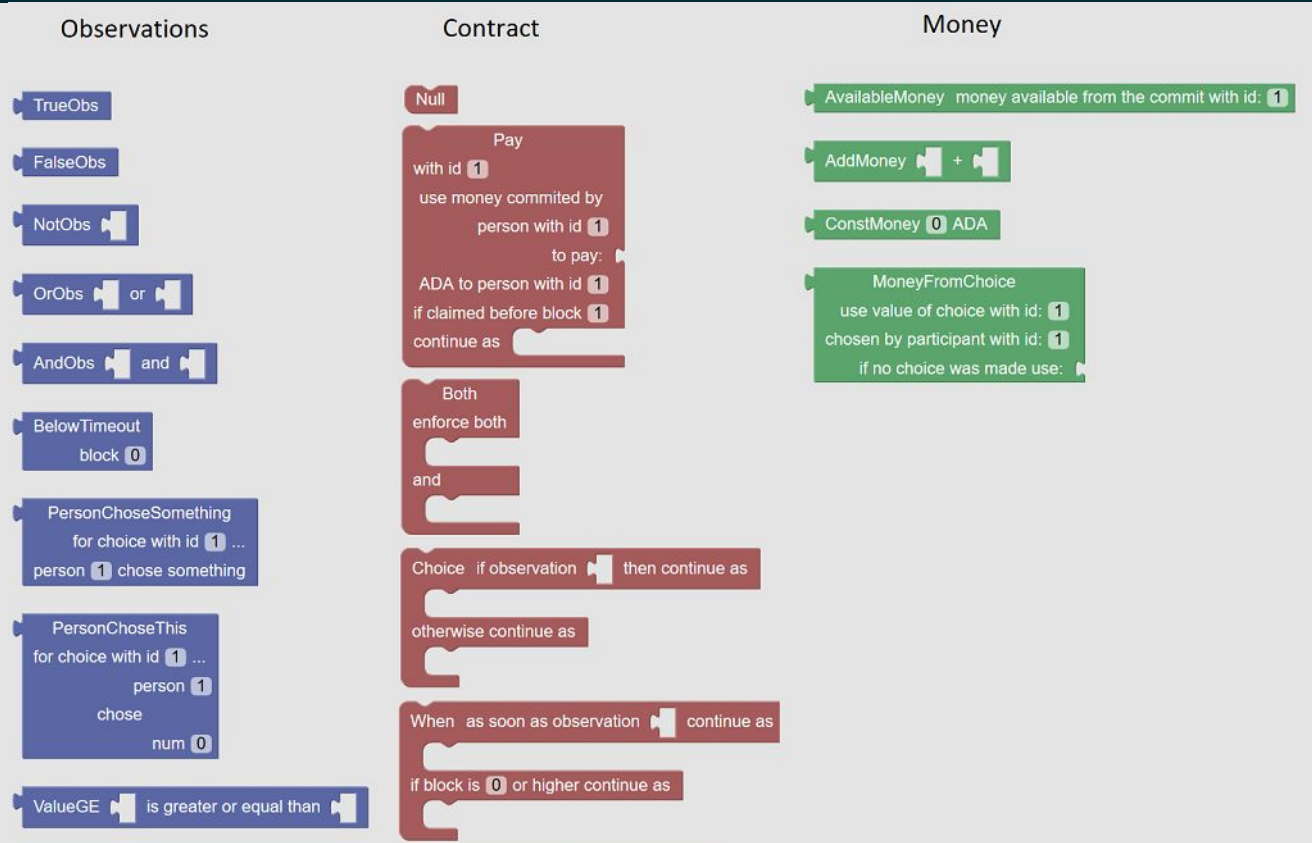
Smart Contracts
KEVM / IELE

```
mallet> sendTransaction(gas=5000000,gasPrice=5000000000,value=10,data=0x6080604052600080553480156100145760008
0fd5b5061010180610024600039600f3006080604052600436106053576000357c0100000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0463ffffffff1680635b34b966146058578063a87d942c14606c578063f5c5ad83146094575b600080fd5b348015606357600080fd5
b50606a60a8565b005b348015607757600080fd5b50607e60ba565b604051808281526020019150506040518091039
0f35b348015609f57600080fd5b5060a660c3565b005b60016000808282540192505081905550565b600080549050905
65b60016000808282540392505081905550565b600160008082825403925050819055505600a165627a7a72305820
3273467350624f703e91bf9fb391c341ba359cf94ac3461f945b02eb4d5f1da10029)
Enter password:
0x408b24bd1128d7a74fadead229120103b018a90ad8a964e07958c47b6ddae1db

mallet> getReceipt(0x408b24bd1128d7a74fadead229120103b018a90ad8a964e07958c47b6ddae1db)
{
    "transactionHash" : "0x408b24bd1128d7a74fadead229120103b018a90ad8a964e07958c47b6ddae1db",
    "transactionIndex" : 0,
    "blockNumber" : 145212,
    "blockHash" : "0x44c0d5d6374a0061ab6da671333231c1d4a768398958dbf8f403f4c905a42723",
    "cumulativeGasUsed" : 5e6,
    "gasUsed" : 5e6,
    "contractAddress" : "0x75da06113d45c3e2b552c09910a60284e23a4d45",
    "logs" : [
    ]
}

mallet> help
Available commands:
  getBalance
  getReceipt
  help
  iele_createContract
  iele_messageCall
  importPrivateKey
  listAccounts
  newAccount
  selectAccount
  sendTransaction

Use 'help([command])' for more information

mallet>
```

Plutus!

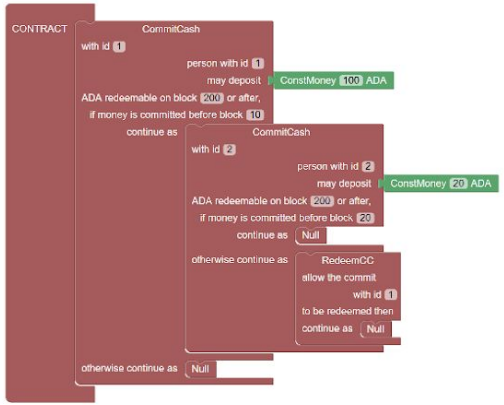
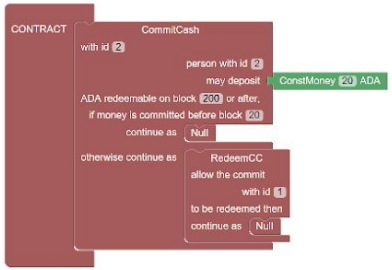

Plutus Playground
Getting Started
Tutorial
API
Privacy
Editor
Demos:
Crowdfunding
Game
Messages
Vesting
-- | Lock some funds with the vesting validator script and return a
-- [[VestingData]] representing the current state of the process
vestFunds :: Vesting -> Value -> MockWallet ()
vestFunds vst value = do
_ <- if value < totalAmount vst then throwOtherError "Value must not be smaller than vested amount" else pure ()
(payment, change) <- createPaymentWithChange value
let contractAddress = Ledger.scriptAddress (validatorScript vst)
dataScript = DataScript (Ledger.lifted vd)
vd = VestingData (validatorScriptHash vst) 0
payToScript_ contractAddress value dataScript
-- | Register this wallet as the owner of the vesting scheme. At each of the
-- two dates (tranche 1, tranche 2) we take out the funds that have been
-- released so far.
-- This function has to be called before the funds are vested, so that the
-- wallet can start watching the contract address for changes.
registerVestingOwner :: Vesting -> MockWallet ()
registerVestingOwner v = do
ourPubKey <- ownPubKey
let
Compile

Marlowe - DSL



*No todos los bloques son mostrados.

Marlowe - DSL

		**Contract** 
No deposits made **State**	[User 1 deposited 100 ADA]	[User 1 deposited 100 ADA, User 2 deposited 20 ADA]
Block #1	Block #2	Block #3

Stake Pools

Proof of Stake

¿Por qué?

Mejor uso de recursos

Es realmente investigación de hardware ASIC.

Mejor uso de energía

El minado de Proof of Work.

Protección contra ataques

Protección en contra de mineros de otros blockchains.

HODLers son premiados

Mejores incentivos para la comunidad

Otros...

(trade off)

Stake Pools

¿Suficiente descentralización?

Me conviene como usuario?

Pros and cons versus staking directo

Parámetro K (Protocolo)

No es conveniente delegar a pools por sobre el punto de saturación.

Pledge amount

Monto inicial. Puede ser multi-persona.

¿Cuál Stake Pool es mejor?

Ranking automatico para maximizar ganancias. Considera Pool Size %, Cost y Margin.

Nash Equilibrium

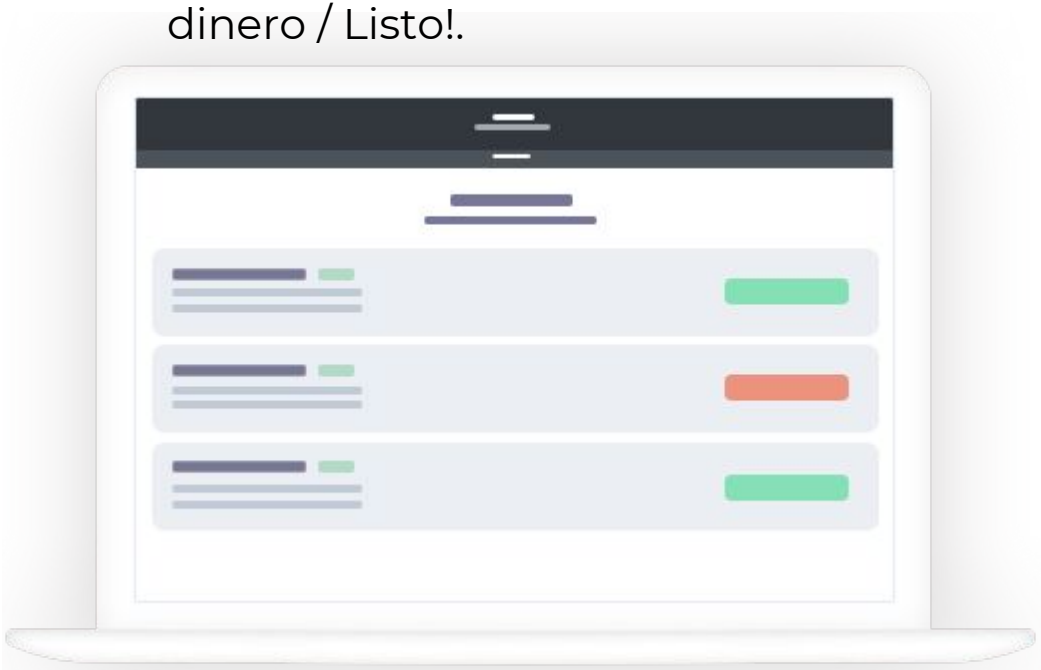
A través de los supuestos del Reward Paper se comprobó que se alcanza Nash Equilibrium.


¿Que tan dificil
será participar?

Staking como usuario

¿Qué tan difícil va a ser?

- Entrar a Yoroi o Daedalus
- Ir a sección de Stake Pools
- Listado de Stake Pools por ranking automatico.
- Click / Tap para delegar.
- Show me the money / Muestrame el dinero / Listo!.



Staking

Diferentes temas

Seguridad

Delegación no incluye control de ADA.

Confianza

Recompensas son repartidas automaticamente.

Hardware Wallets

Podrás delegar usando Trezor / Ledger.

¿Cuál Stake Pool es mejor?

Ranking automatico para maximizar ganancias.

Desde exchange?

Nuevo tipo de address para exchanges que no posibilita staking (opcional).

Stake Pools POC

Thank You!

info@emurgo.io
emurgo.io

AD-O Shibuya-dogenzaka Building
8F, Dogenzaka,
Shibuya-ku, Tokyo, 150-0043