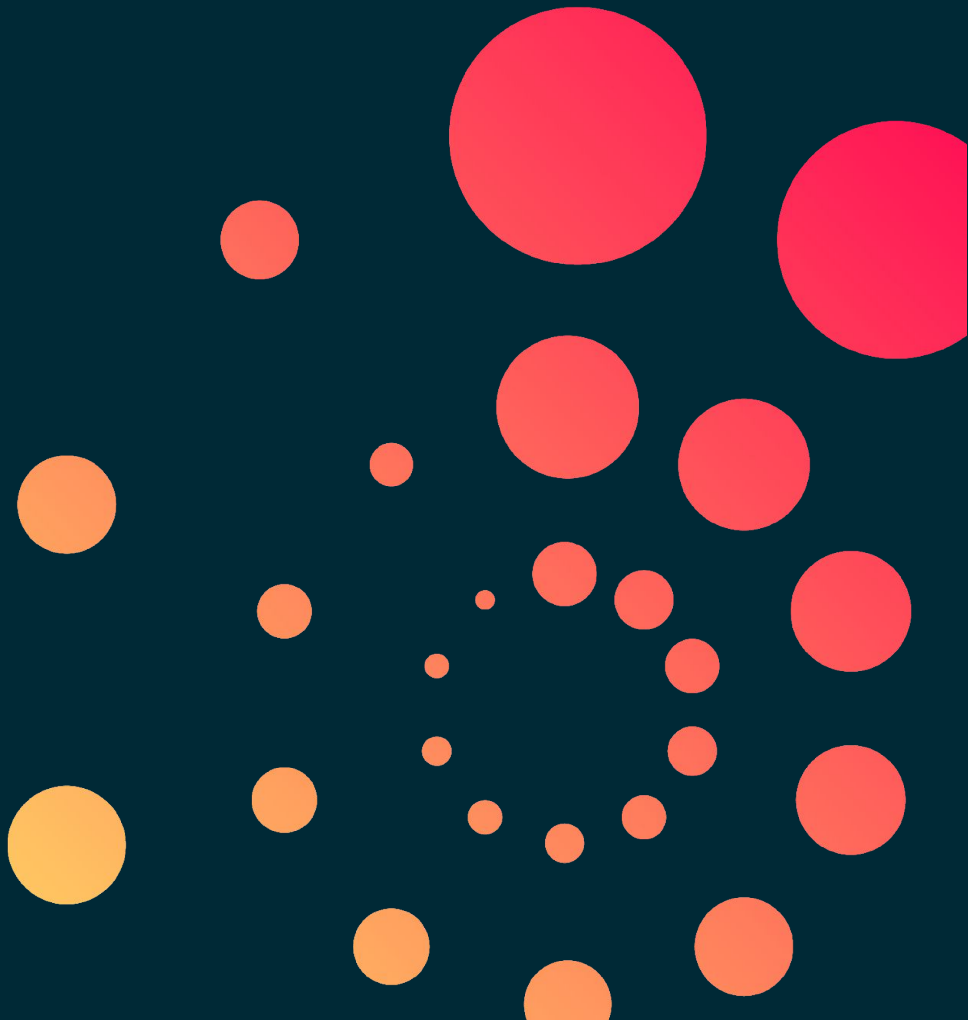


Emurgo

Blockchain España Meetup

Presentador:

Nicolás Arqueros - CTO, Emurgo





¿Qué es Cardano?

Breve descripción

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





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?**



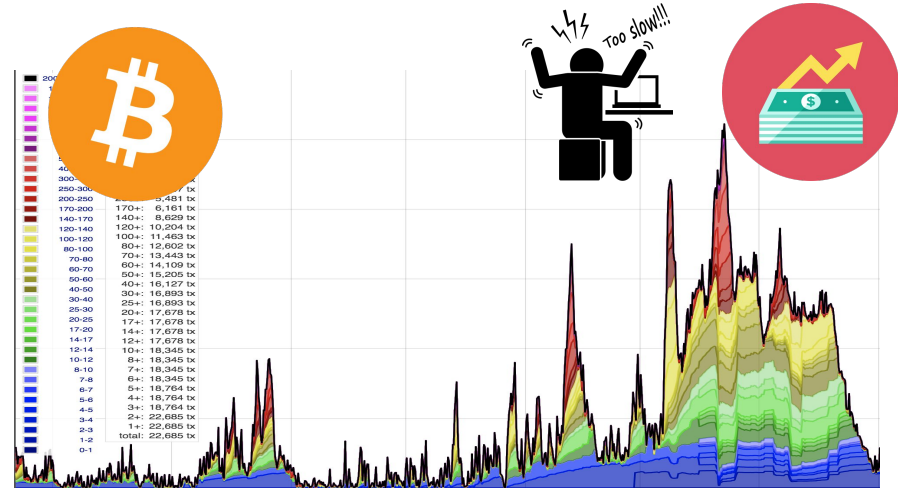
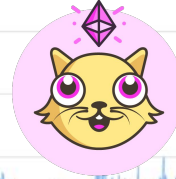
Escalabilidad

de transacciones, tamaño del blockchain y red



Ethereum Pending Transactions Queue – Time Series

Source: Etherscan.io
(From 7/30/2015 to 12/5/2017)
Click and drag in the plot area to zoom in



200+	200+	22,685 tx
150-200	150+	22,685 tx
100-150	100+	22,685 tx
50-100	50+	22,685 tx
0-50	0+	22,685 tx
250-300	250+	9,481 tx
200-250	200+	8,161 tx
170-200	170+	8,629 tx
140-170	140+	10,204 tx
120-140	120+	11,463 tx
100-120	100+	12,652 tx
80-100	80+	13,443 tx
70-80	70+	14,109 tx
60-70	60+	15,205 tx
50-60	50+	16,127 tx
40-50	40+	16,893 tx
30-40	30+	17,678 tx
20-30	20+	17,678 tx
17-20	17+	17,678 tx
14-17	14+	17,678 tx
12-14	12+	18,345 tx
10-12	10+	18,345 tx
8-10	8+	18,345 tx
7-8	7+	18,345 tx
6-7	6+	18,345 tx
5-6	5+	18,764 tx
4-5	4+	18,764 tx
3-4	3+	18,764 tx
2-3	2+	22,685 tx
1-2	1+	22,685 tx
0-1	0+	22,685 tx
Total:	Total:	22,685 tx

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=500000000, value=10, data=0x60806040526000805534801561001457600080fd5b5061
0101806100246000396000f3006080604052600436106053576000357c010000000000000000000000000000000000000000000000000000000000
0463ffffffff1680635b34b966146058578063a87d942c14606c578063f5c5ad83146094575b600080fd5b348015606357600080fd5b50606a60a8
565b005b348015607757600080fd5b50607e60ba565b6040518082015260200191505060405180910390f35b348015609f57600080fd5b5060a660
c3565b005b60016000808282540192505081905550565b60008054905090565b600160008082825403925050819055505600a165627a7a72305820
3273467350624f703e91bf9bf391c341ba359cf94ac3461f945b02eb4d5f1da10029)
```

```
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

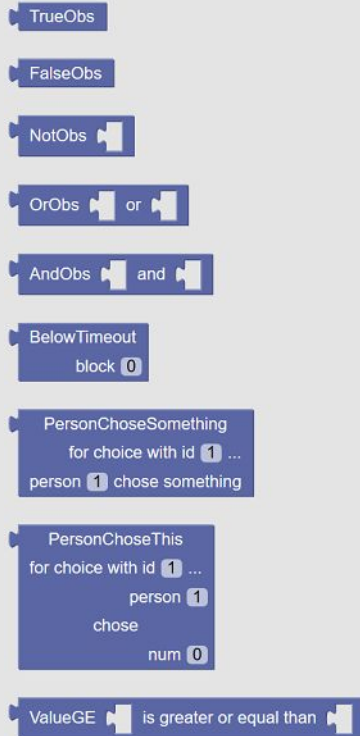
Demos: [Crowdfunding](#) [Game](#) [Messages](#) [Vesting](#)

```
44 -- | Lock some funds with the vesting validator script and return a
45 -- [[VestingData]] representing the current state of the process
46 vestFunds :: Vesting -> Value -> MockWallet ()
47 vestFunds vst value = do
48   _ <- if value < totalAmount vst then throwError "Value must not be smaller than vested amount" else pure ()
49   (payment, change) <- createPaymentWithChange value
50   let contractAddress = Ledger.scriptAddress (validatorScript vst)
51       dataScript      = DataScript (Ledger.lifted vd)
52       vd = VestingData (validatorScriptHash vst) 0
53   payToScript_ contractAddress value dataScript
54
55 -- | Register this wallet as the owner of the vesting scheme. At each of the
56 -- two dates (tranche 1, tranche 2) we take out the funds that have been
57 -- released so far.
58 -- This function has to be called before the funds are vested, so that the
59 -- wallet can start watching the contract address for changes.
60 registerVestingOwner :: Vesting -> MockWallet ()
61 registerVestingOwner v = do
62   ourPubKey <- ownPubKey
63   let
```

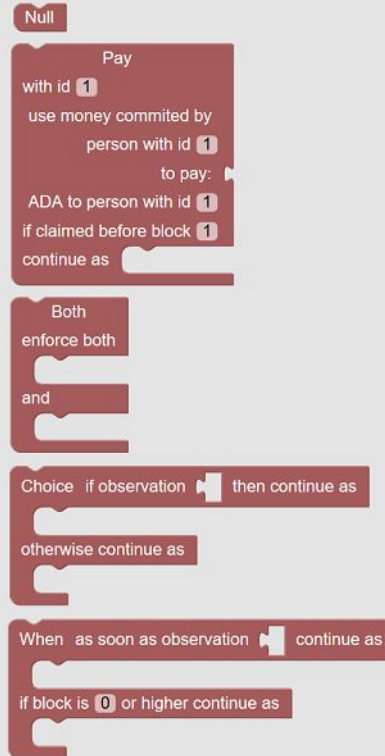
Compile

Marlowe - DSL

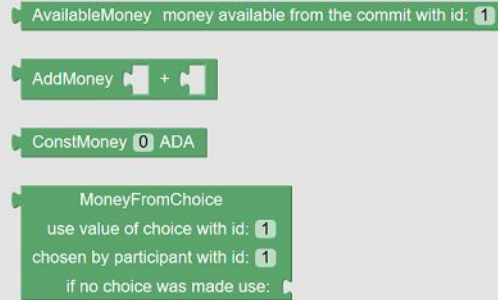
Observations



Contract

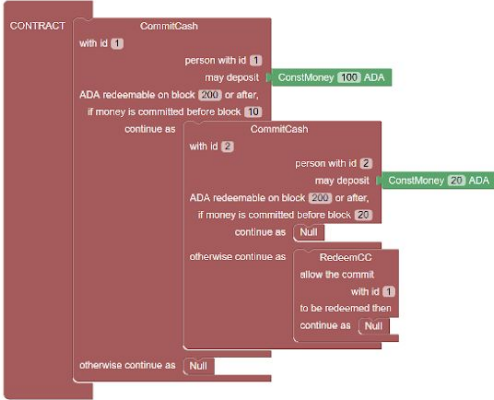
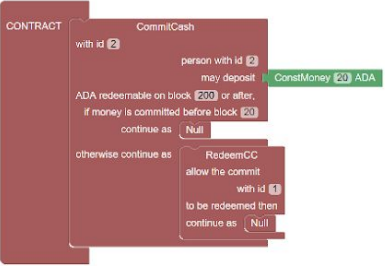


Money



*No todos los bloques son mostrados.

Marlowe - DSL

		<h2>Contract</h2>
 <p>The diagram for Block #1 shows a 'CONTRACT' block with a 'CommitCash' sub-block. This sub-block contains a 'person with id 1' who 'may deposit' 'ConstMoney 100 ADA'. The contract is 'ADA redeemable on block 200 or after, if money is committed before block 10'. It 'continue as' another 'CommitCash' block for 'person with id 2' who 'may deposit' 'ConstMoney 20 ADA', which is 'ADA redeemable on block 200 or after, if money is committed before block 20'. This second block 'continue as' a 'RedeemCC' block 'with id 1' that 'allow the commit to be redeemed then continue as Null'. The main contract 'otherwise continue as Null'.</p>	 <p>The diagram for Block #2 shows the 'CONTRACT' block continuing from Block #1. The 'CommitCash' sub-block for 'person with id 2' is active, showing 'ConstMoney 20 ADA' being deposited. The 'RedeemCC' block for 'person with id 1' is also shown, indicating that the 100 ADA from Block #1 is now being redeemed. The contract 'continue as Null'.</p>	<p>[User 1 deposited 100 ADA, User 2 deposited 20 ADA]</p>
<p>*No deposits made*</p> <h2>State</h2>	<p>[User 1 deposited 100 ADA]</p>	<p>[User 1 deposited 100 ADA, User 2 deposited 20 ADA]</p>
<p>Block #1</p>	<p>Block #2</p>	<p>Block #3</p>

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.



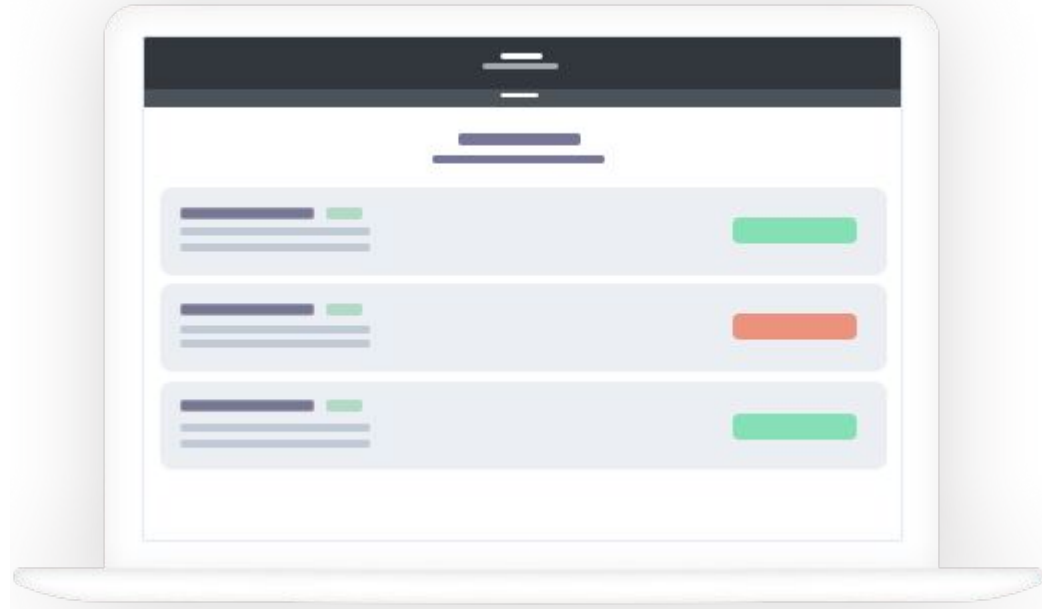


¿Que tan difícil
será participar?

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 automáticamente.

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

