

# Blockchain para todo el mundo

Dario Castañé @ Guru Talks

# Dario Castañé



Dario@mastodon.social Castañé | 🇪🇸 🎵 ▾  
@im\_dario

#idea Can we use Bitcoin's blockchain to do electronic voting? Would it be secure? Would it be possible to keep the vote secret?

Tradueix el tuit  
11:57 a. m. · 20 d'ag. de 2013 · Twitter Web Client

- Backend Go developer: Loyal Guru
- Divulgador: [speakerdeck.com/dario](https://speakerdeck.com/dario)
- Blockchain Catalunya

# ¿Qué es blockchain?

1. Base de datos (la más lenta del mundo\*)
2. Registro distribuido
3. Cadena de bloques

\*: *tiene una explicación.*

# ¿Por qué es lenta?

Cambiamos velocidad por:

- descentralización
- immutabilidad
- auditoría
- no es necesario confiar en terceros

# Antes de ir al meollo, ¿para qué sirve?

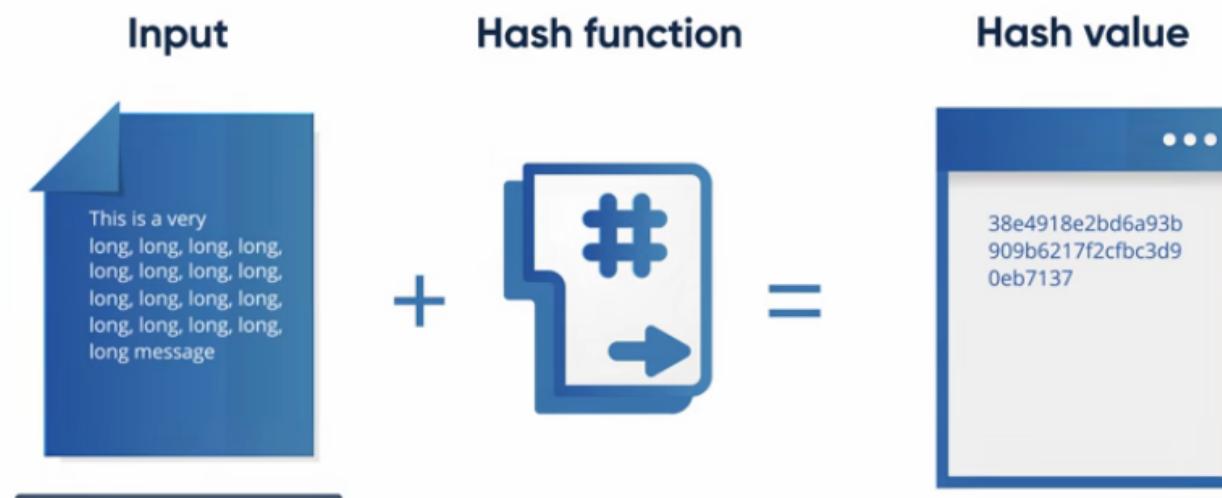
- Pagos y transferencias
- Rastreo de mercancías
- Sistemas de recompensas
- Identidad digital
- Voto digital
- Certificación
- Tokenizar bienes y recursos
- ...

# ¿Cómo funciona?

- Elementos claves:
  - Huella o hash
  - Prueba of X (trabajo, participación, quemado, etc)
  - Criptografía asimétrica: transacciones

# Funciones de huella o hash

What is Hashing? Hash Functions Explained Simply



# Prueba de X

## Explicación simple de PoW vs PoS

### Proof of Work (PoW)



La cantidad de trabajo realizado por un minero en particular determina su posibilidad de extraer un solo bloque y la recompensa de obtener una moneda.

### Proof of Stake (PoS)



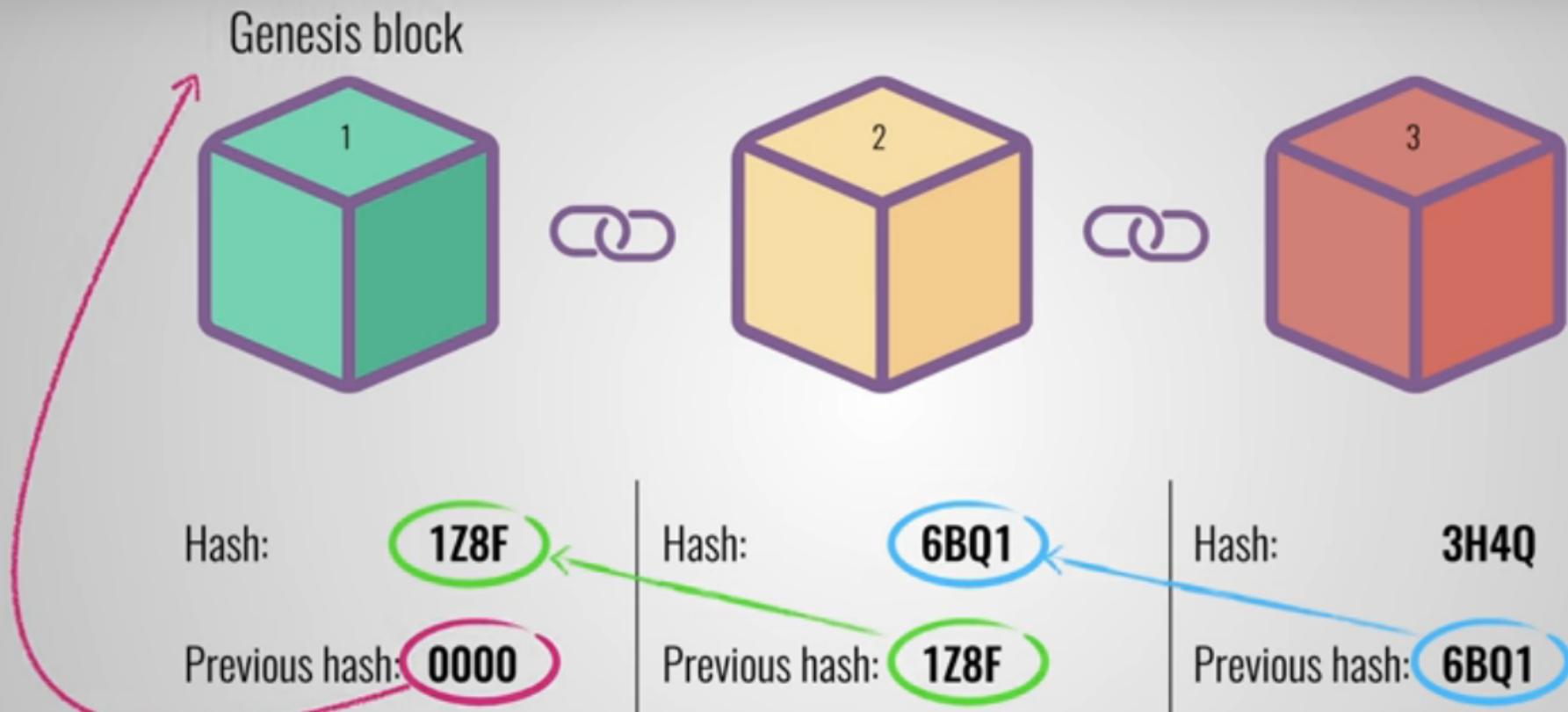
La capacidad de extracción de un minero en particular depende de cuántas monedas ya tenga.



Los mineros obtienen menos Bitcoins con el tiempo. Estos pequeños incentivos aseguran una menor probabilidad de un ataque de 51%.



El ataque del 51% es ridículamente caro en el método de Proof of Stake (PoS)



# Criptografia de clave asimétrica

PKI / PGP Primer:



Public Key



Private Key



Message



+



=



Encrypted



+



=



Decrypted



=



Signed

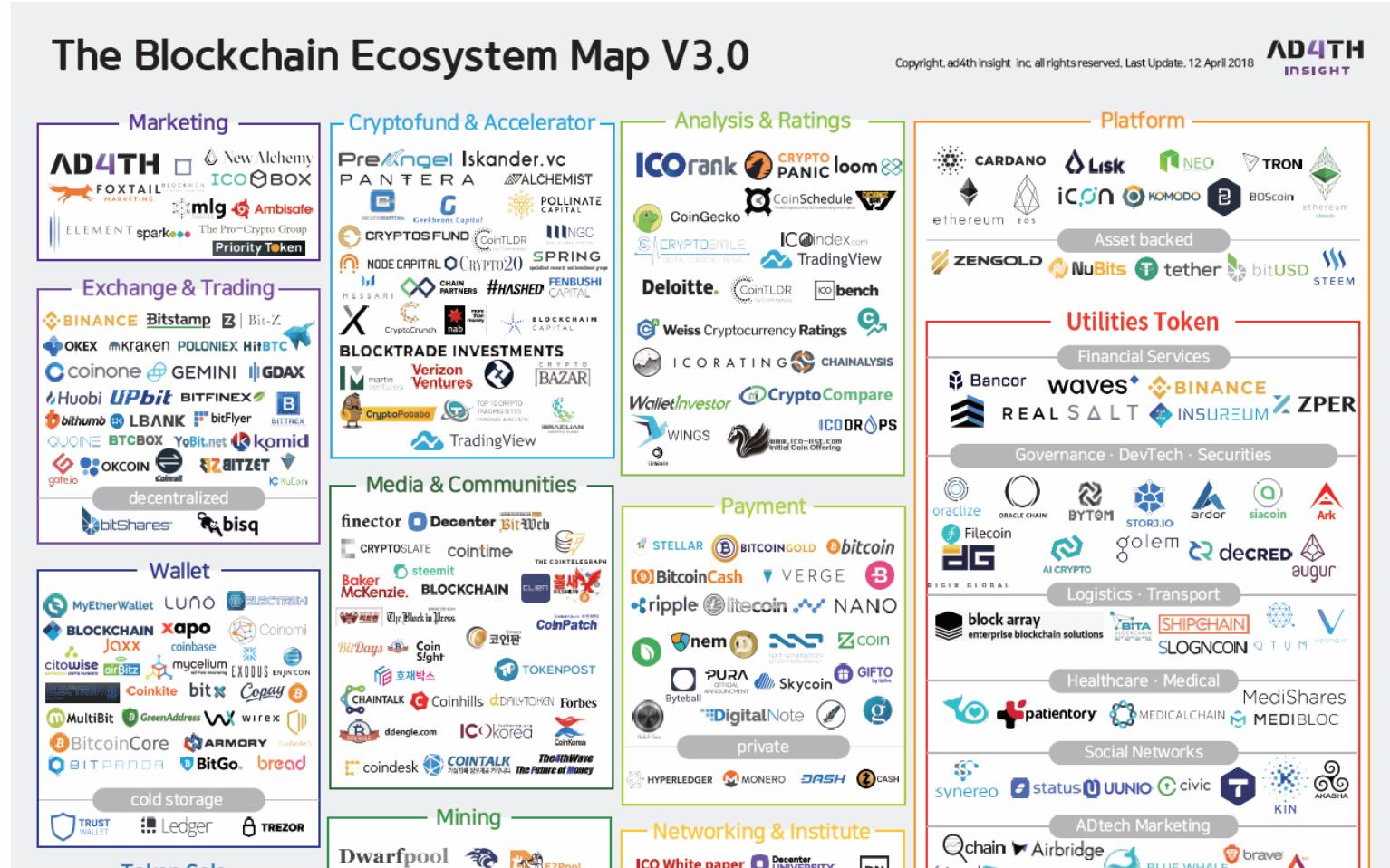


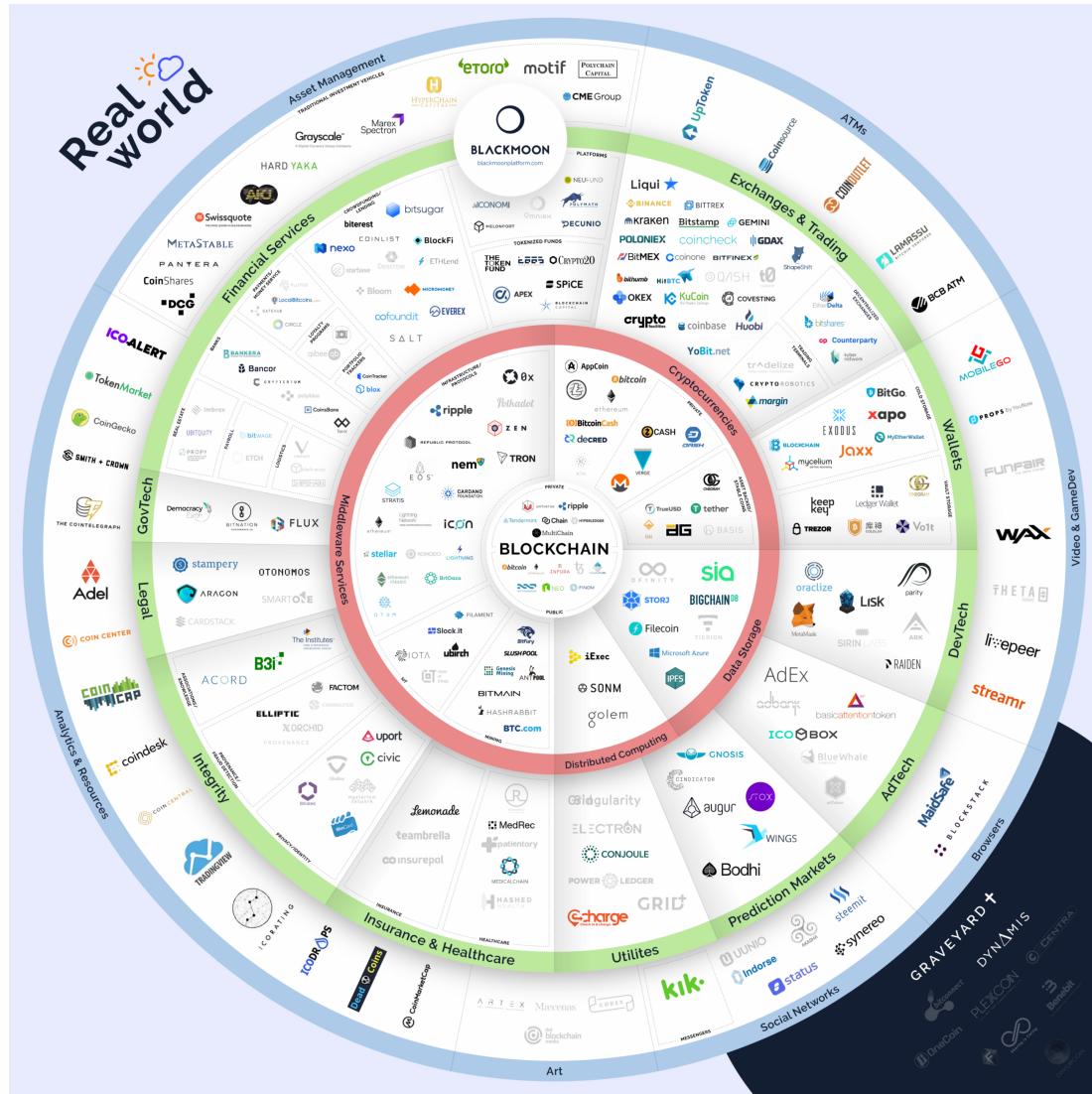
=



Authenticated

# It's full of st... projects!













# Recursos adicionales

- Binance Academy: [binance.vision/es](https://binance.vision/es)
- Coinbase Learn: [coinbase.com/learn](https://coinbase.com/learn)

# ¿APM? ¡Gracias!

- dcastane@loyal.guru
- speakerdeck.com/dario
- twitter.com/@im\_dario
- @dario@mastodon.social
- github.com/imdario
- keybase.io/dario