

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
- 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?

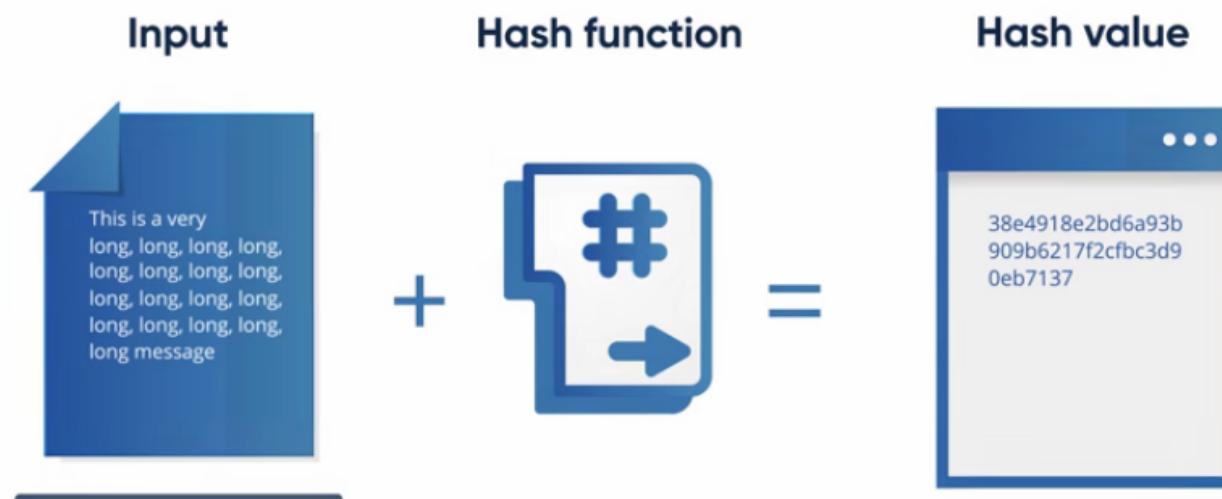
- Pagos y transferencias
- Rastreo de mercancías
- Sistemas de recompensas
- Identidad digital
- Voto digital
- Certificación
- Tokenizar bienes y recursos
- ...

¿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)



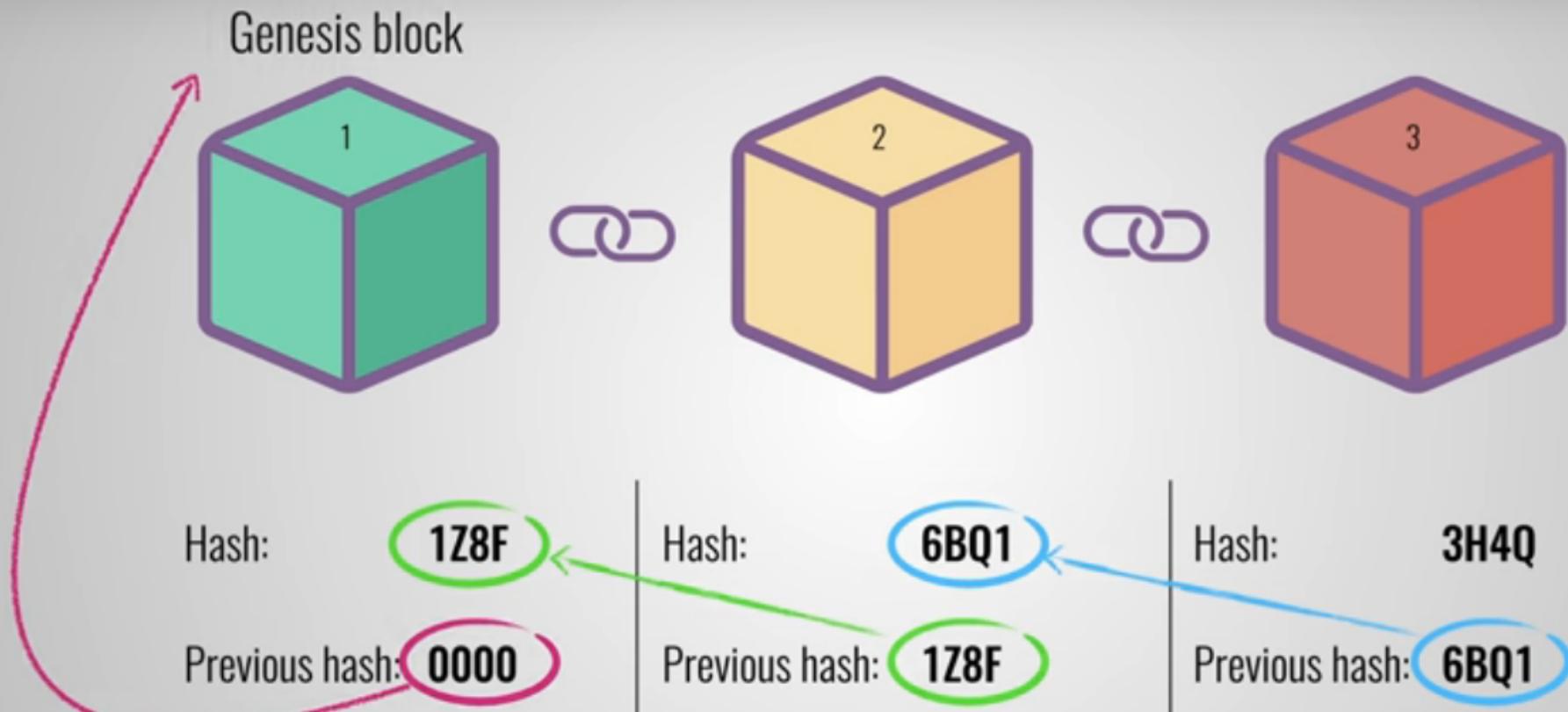
La capacidad de extracción de un minero en particular depende de cuántas monedas ya tenga.



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

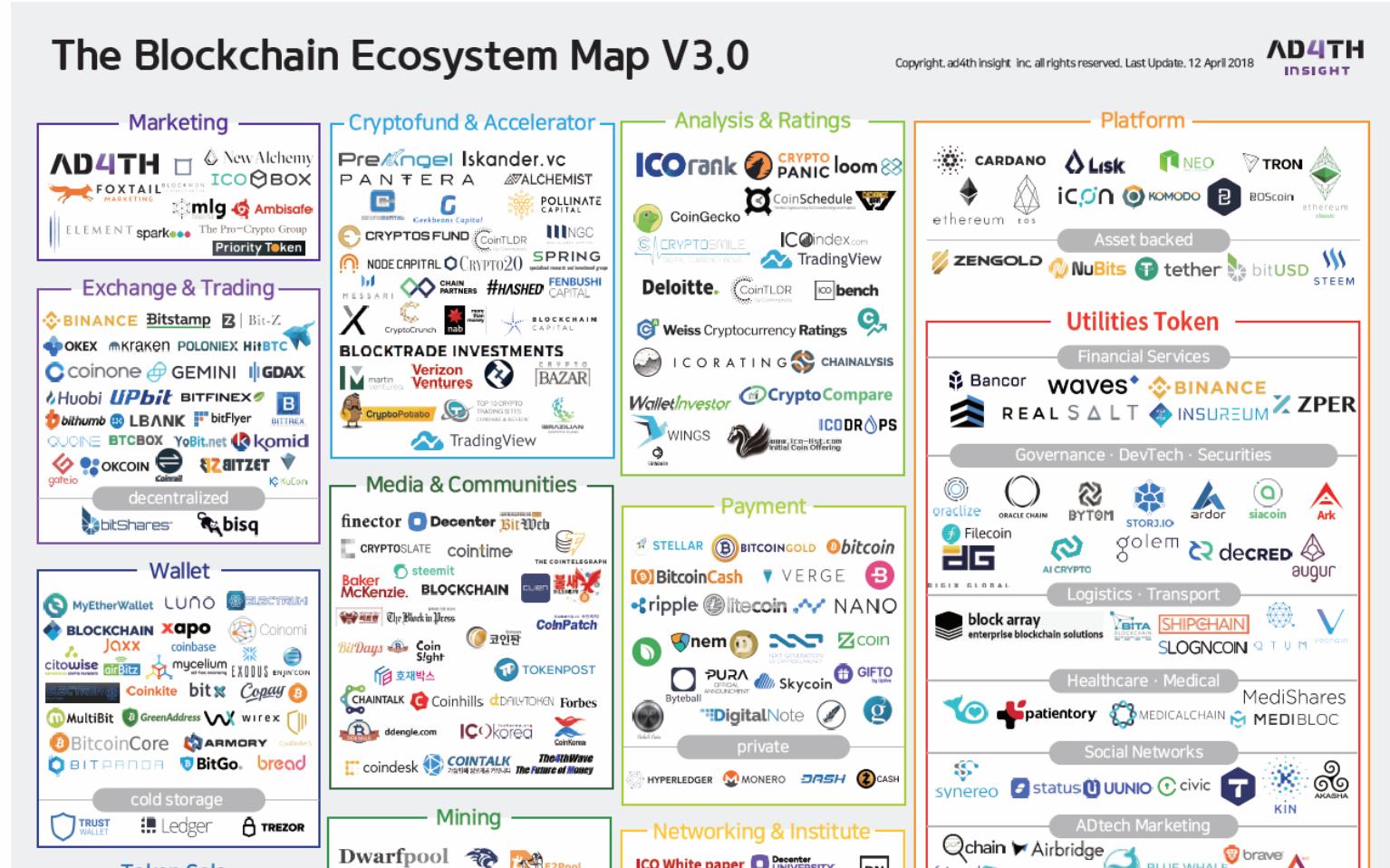


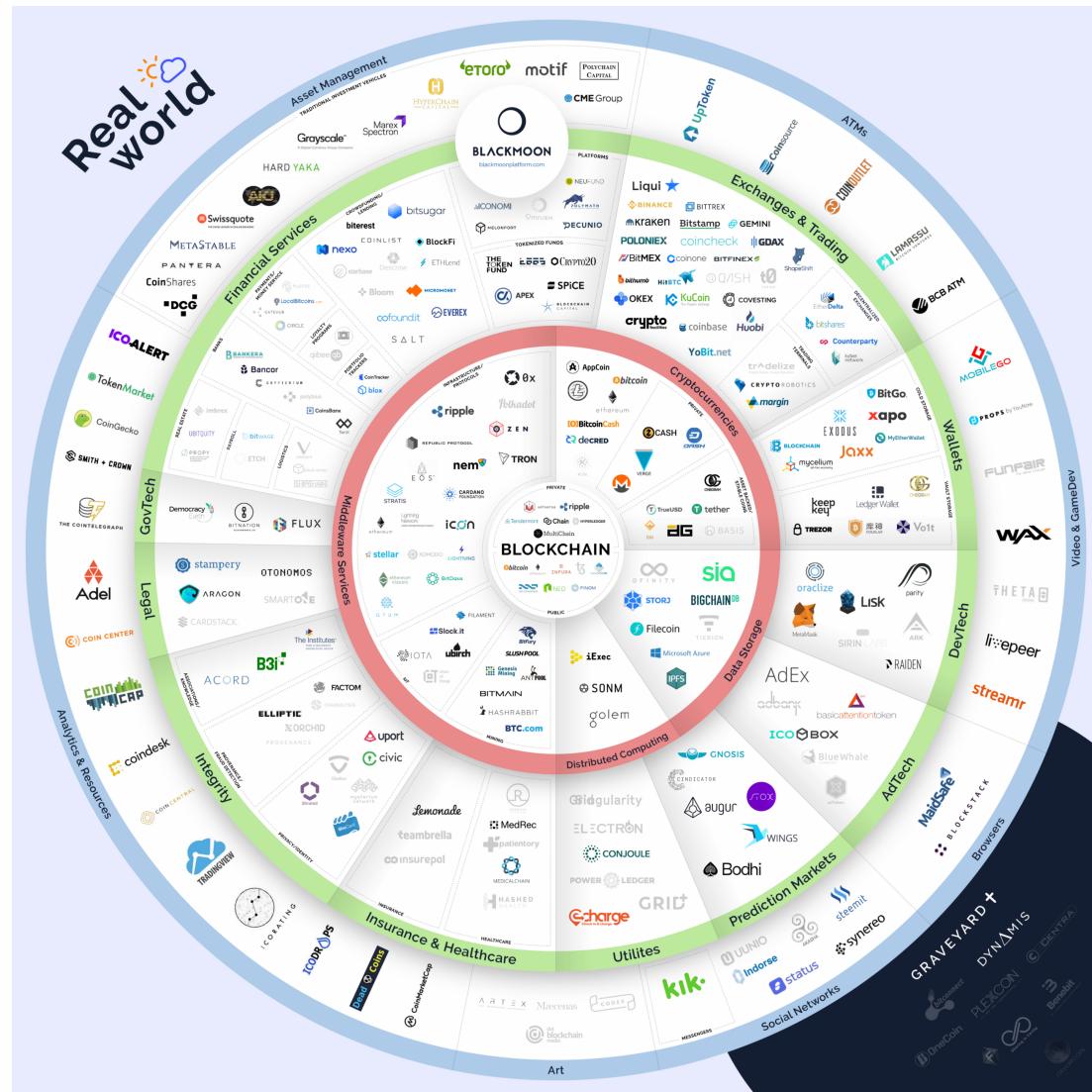
=



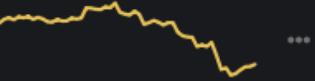
Authenticated

It's full of st... projects!





Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾		Exchanges ▾	Watchlist			Filters	EUR ▾	Next 100 →	View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)		
1	฿ Bitcoin	€146.863.173.360	€8051,54	€46.433.980.847	18.240.387 BTC	-1,33%		...	
2	ethereum	€23.049.563.505	€209,78	€25.514.998.230	109.875.237 ETH	1,24%		...	
3	XRP	€9.612.154.857	€0,219709	€2.776.822.681	43.749.413.421 XRP *	2,92%		...	
4	฿ Bitcoin Cash	€5.430.699.615	€296,73	€5.647.208.225	18.301.588 BCH	3,16%		...	
5	Tether	€4.221.798.230	€0,909406	€62.921.602.415	4.642.367.414 USDT *	-0,26%		...	
6	฿ Bitcoin SV	€3.804.209.040	€207,89	€2.737.697.243	18.298.777 BSV	0,04%		...	
7	฿ Litecoin	€3.658.708.878	€57,01	€5.799.919.452	64.175.350 LTC	-0,41%		...	

Blockchain para todo el mundo

Guru Talks · 35 Members

jue 27 de feb a las 18:30

Carrer de Pallars, 85

Carrer de Pallars, 85

blockchain

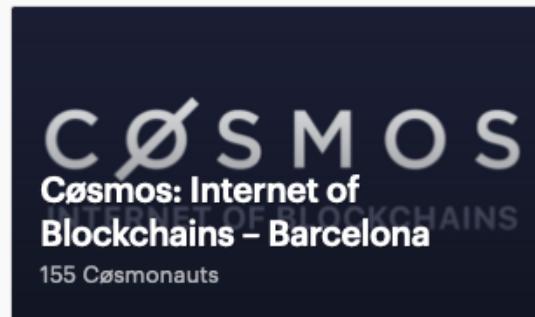


a menos de 5 km de Barcelona, ES

Grupos

Calendario

Ordenar por Recomendados



Grupo de Meetup de
Blockchain en Barcelona

Más de 50 interesados >



Apropem la revolució Blockchain a la ciutadania

Activitats de Blockchain Catalunya

Dissabte
30/11/2019

09 30

Col·laborem amb el Blockchain Challenge

PARTICIPA AL BLOCKCHAIN CHALLENGE!

Col·labora, involucra't i contribueix en la hackató per trobar



Blockchain Catalunya

[Follow](#)



Alex Puig 19 Feb

Do you think it is possible to organize an event for 450pax in one week? Yes! If the community work together <https://t.co/Ubb7E3ZFZx>



Recursos adicionales

- Binance Academy: binance.vision/es
- Coinbase Learn: coinbase.com/learn

¿APM? ¡Gracias!

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