COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

5º E2 + Analytics

ITINERARIO DE ECONOMICS & FINANCE

Análisis de Servicios Financieros

Sesión 7. Bitcoin

6 de noviembre de 2025

comillas.edu

¿Dónde estamos?

#	Fecha	Tema
1	4 S	Situación actual y primeros pasos
		Bloque 1 - Situación de partida
2	11 S	El mapa: competencias y supervisores
3	18 S	Regulación e innovación
4	25 S	Instrumentos financieros
5	2 O	Rentabilidad, riesgo y liquidez
		Bloque 2 - Análisis de entidades
6	9 O	CAMELS y Capital
7	16 O	Rentabilidad y eficiencia
8	23 O	Liquidez bancaria
9	30 O	Riesgos y riesgo de mercado
		Bloque 3 - Fintech y disrupción
10	6 N	Bitcoin, medios de pago y blockchain
11	13 N	Ethereum, smart contracts y automatización de procesos
12	20 N	DeFi - El modelo User to Contract y Money Legos
13	27 N	DeFi - Innovación incremental
14	4D	DeFi - Innovación disruptiva

¿Qué vamos a hacer hoy?

- **Introducción**
  - ¿Qué lo cambia todo?
  - Crisis del 2008
  - Origen del bitcoin

- **Antecedentes de la tecnología BlockChain**
  - El poder del código abierto (Open Source)
  - P2P, relación entre iguales
  - Criptografía, clave pública y clave privada

¿Qué lo cambia todo?

INTERNET

90's: primeros pasos: primeras páginas web. Mismo servicio en un medio diferente

2001 Crisis punto com: Internet es una moda pasajera

11S: Bajada de tipos

Internet 2.0 El usuario crea el contenido

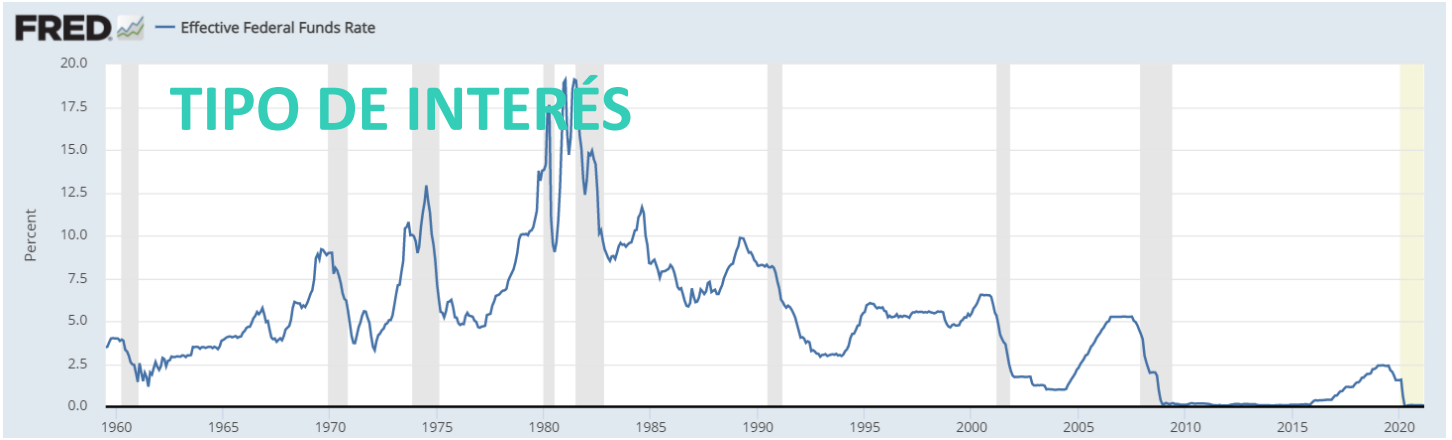
2008 Crisis financiera

Consecuencias de la crisis financiera:

- Desaparecen un gran número de empresas
- Innovación financiera (bitcoin, Fintech…)
- Aumento de la regulación
- Rescate de instituciones
- Deuda, deuda y más deuda (QE)… ¿y las reformas estructurales?

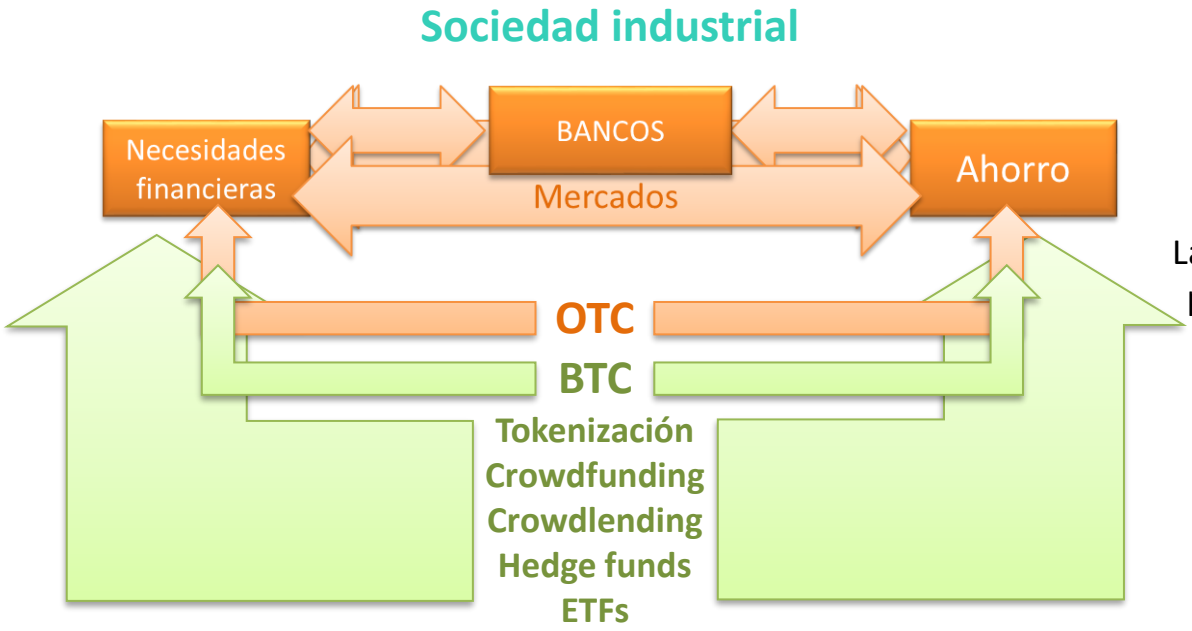
Gobiernos
Bancos
Sectores industriales
Muchos ciudadanos

Crisis del 2008



Origen del bitcoin

El poder del mercado OTC (Over The Counter)



Sistema financiero oficial, regulado y centralizado

Las operaciones OTC estaban reservadas para agentes altamente especializados

En 2008 el sistema financiero se rompe

Grandes gigantes supranacionales (Black Rock – 10 billones (trillions) USD en AUM –Assets Under Managment –, GAFAM (Capitalización conjunta: 7 billones USD (trill))

Origen del bitcoin

El dinero tradicional es lento, grande e ineficiente

2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

bitcoin

ethereum

Prepara una regulación para el dinero digital revolucionaria

Directiva 2015/2366 PSD2 – Medios de pago

Directiva 2014/65/EU (MiFID II) - Mercados de instrumentos financieros

Directiva 2009/110/CE – Dinero electrónico

Europa

libra

WeChat

Alibaba.com

Prepara su criptomoneda digital oficial, (DC/EP) y la prueba en sus cuatro principales bancos

China

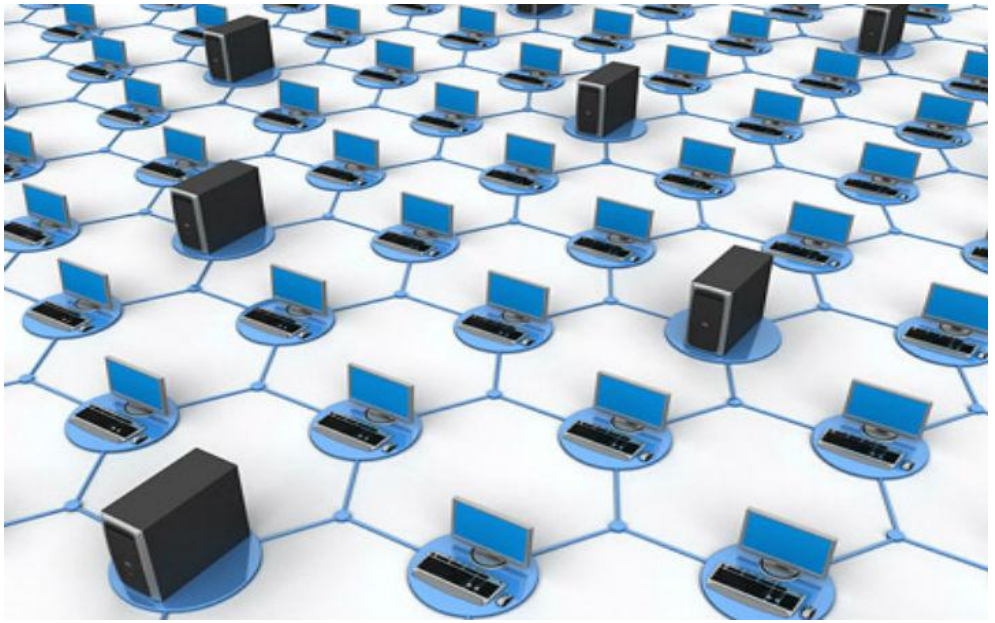
Reacciona: Está preparando inyecciones de dólares digitales

EEUU

Origen del bitcoin

Algunas ideas básicas:

- Bitcoin con mayúscula y bitcoin con minúscula
- El BlockChain
- Token (1 Satoshi)
- 10^8 Satoshis = 1 BTC
- Funciones de los mineros:
  - Buscar nuevos bloques
  - Guardar la cadena
  - Validar las transacciones



Origen del bitcoin

Bitcoin: un sistema de dinero en efectivo electrónico *peer-to-peer*[1]

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Satoshi Nakamoto:

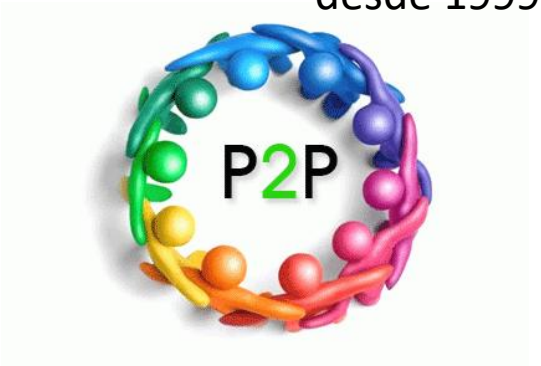
- 2007 – Empieza a escribir el código
- 18 de agosto de 2008 – Se registra el dominio bitcoin.org
- 31 de octubre de 2008 – Se publica el artículo fundacional
- 9 de enero de 2009 – Bloque génesis

Resumen. Una forma de dinero en efectivo electrónico puramente *peer-to-peer* debería permitir enviar pagos *online* directamente entre las partes y sin pasar a través de una institución financiera. Las firmas digitales son parte de la solución, pero los beneficios principales desaparecen si un tercero de confianza sigue siendo imprescindible para prevenir el doble gasto. Proponemos una solución para el problema del doble gasto usando una red *peer-to-peer*. La red sella las transacciones en el tiempo en una cadena continua de *proof-of-work*[2] basada en *hash*[3], estableciendo un registro que no se puede modificar sin rehacer la *proof-of-work*. La cadena más larga no solo sirve de prueba efectiva de la secuencia de eventos, sino que también demuestra que procede del conjunto de CPU más potente. Mientras la mayoría de la potencia CPU esté controlada por nodos que no cooperen para atacar la propia red, se generará la cadena más larga y se aventajará a los atacantes. La red en sí misma precisa de una estructura mínima. Los mensajes se transmiten en base a "mejor esfuerzo"[4], y los nodos pueden abandonar la red y regresar a ella a voluntad, aceptando la cadena *proof-of-work* más larga como prueba de lo que ha sucedido durante su ausencia.

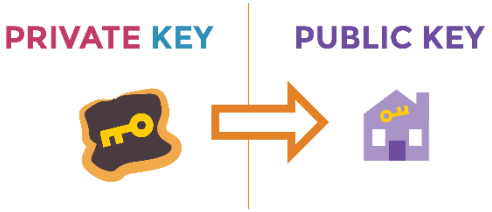
Origen del bitcoin

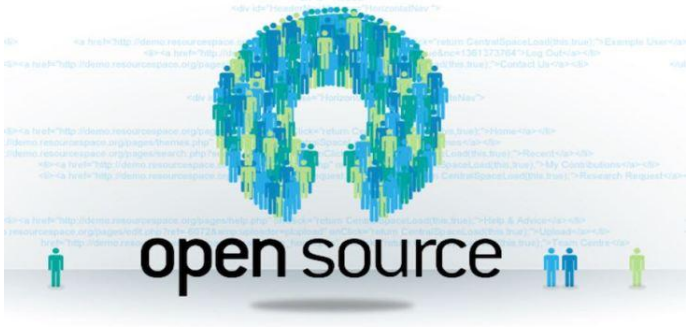
Los ingredientes ya estaban allí. Solo había que mezclarlos:

La **tecnología P2P** es popular desde 1999



La **criptografía de clave pública** o **asimétrica** se conoce desde el año 1976





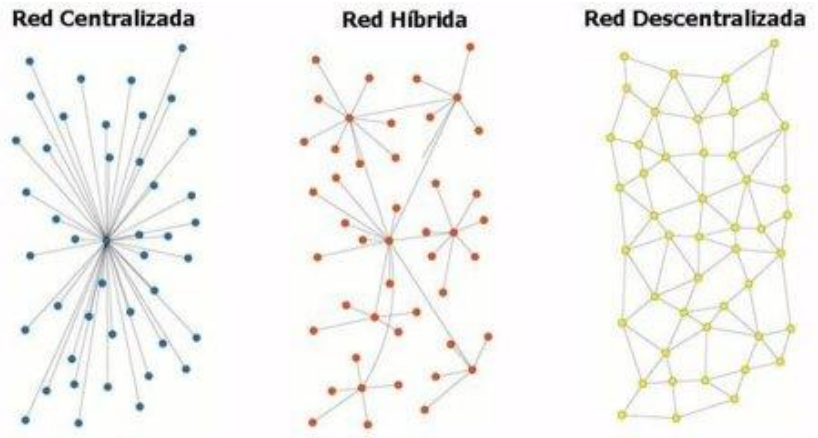
El **código abierto** se utiliza en las comunidades de software libre desde 1990

Tecnología P2P

Antes: Productores y consumidores

Ahora: Prosumers

¿Quién es el dueño del sistema?



Características deseables:

- Escalabilidad
- Robustez
- Descentralización
- Distribución de costes entre los usuarios
- Anonimato
- Seguridad

Tecnología P2P

Decentralized Autonomous Organization (DAO)

- Los usuarios compran tokens de la DAO en un **Exchange** (a cambio de Ether)
- Los dueños de los tokens pueden votar, decidir (**gobernanza**) u obtener servicios
- Si existiesen beneficios, los dueños de los tokens los podrían compartir en función de su inversión inicial

Proceso tradicional OPV (Oferta Pública de Venta, en inglés IPO Initial Public Offering)

Según PWC:

- Se tarda en planificar: 12-18 meses. En ejecutar: 6-9 meses
- En el 83% de las ocasiones se gasta más de 1M$ en la OPV
- 2/3 de los casos tienen entre 1M y 1,9M$ de gastos anuales por cotizar

ICO – Initial Coin Offering
TAO - Tokenized Asset Offering

Código abierto

Software libre – Richard Stallman (1983) El software es "libre" cuando garantiza las siguientes libertades:

0. la libertad de usar el programa, con cualquier propósito (**uso**)
1. la libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a las propias necesidades (**estudio**)
2. la libertad de distribuir copias del programa, con lo cual se puede ayudar a otros usuarios (**distribución**)
3. la libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie (**mejora**).

Las libertades 1 y 3 requieren acceso al código fuente.

Código abierto

El código abierto se comenzó a usar en las comunidades de software libre en 1990.

Ventajas del Código abierto vs. Software propietario:

- No dependes de que un fabricante permita el cambio o no.
- Más flexibilidad, menos coste
- Un mundo de soporte
- Vida más larga del software…

"Solo con software propietario hubiese sido imposible": así es como el Open Source ha ayudado en la gesta del Ingenuity en Marte (https://bit.ly/3xMOCwy)

Código abierto

https://github.com/bitcoin/bitcoin

- Litecoin (2011) – LTC – más ligera
- Bytecoin (2012) – Mejora el algoritmo, hoy vale prácticamente cero, como muchas otras miles de criptos…
- Dogecoin (2013) – En su día fue una broma ☺
- Verge (2014) – Usa redes TOR e I2P… en teoría es anónima, pero no tanto
- Monero (2014) – La clave pública cambia

…Ethereum (2014)

Clave pública y clave privada

Una primera aproximación:

Una operación asimétrica es algo que es fácil de hacer pero difícil de deshacer… salvo que conozcas la **clave privada**.

19 * 23 = es fácil de hacer

¿Cuáles son los divisores de 437?

Sabes que 19 es divisor de 437, ¿Cuál es el otro?

89 * 97 = 8633

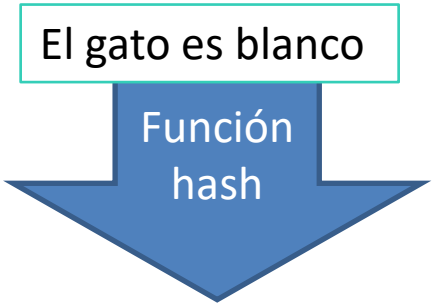
9.817 * 2.371 = 25.043.167

Clave pública y clave privada

SHA-256 – Algoritmo de hash

Buscad en Google: SHA 256 online

https://emn178.github.io/online-tools/sha256.html



d8e74ded1f738f949bb4d9a28fd848d608a5e0e4d8536c73aedf22a8bfa21e4a

64 caracteres hexadecimales

1 hexadecimal = 2^4 = 4 bits

(Un Byte = 8 bits = 2 hexadecimales).

64 x 4 =256

2^{256} alternativas = 1.16×10^{77}

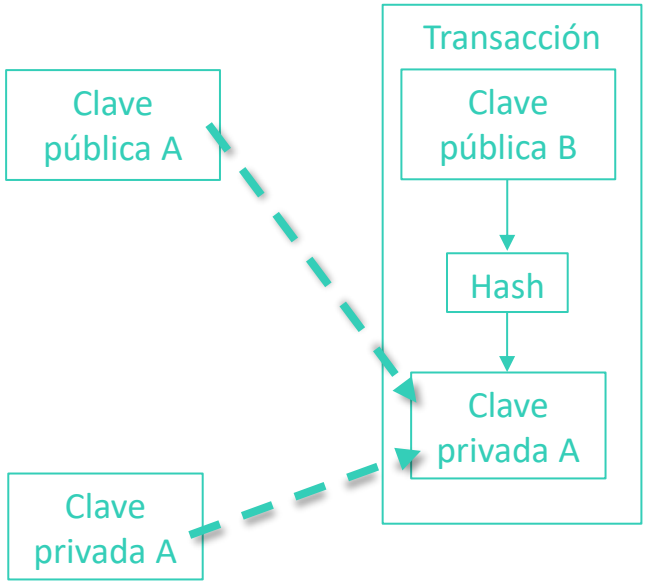
0 = 0000	4 = 0100	8 = 1000	C = 1100
1 = 0001	5 = 0101	9 = 1001	D = 1101
2 = 0010	6 = 0110	A = 1010	E = 1110
3 = 0011	7 = 0111	B = 1011	F = 1111

Clave pública y clave privada

Clave privada: AF18 A03B BFD2 5E8C D036 4141

Clave pública 1421pqgSvmee8t196A69n7TSxS2vaPQ6L1

Monedero (Wallet)



TRANSACCIÓN

A quiere mandar **tokens** a **B**

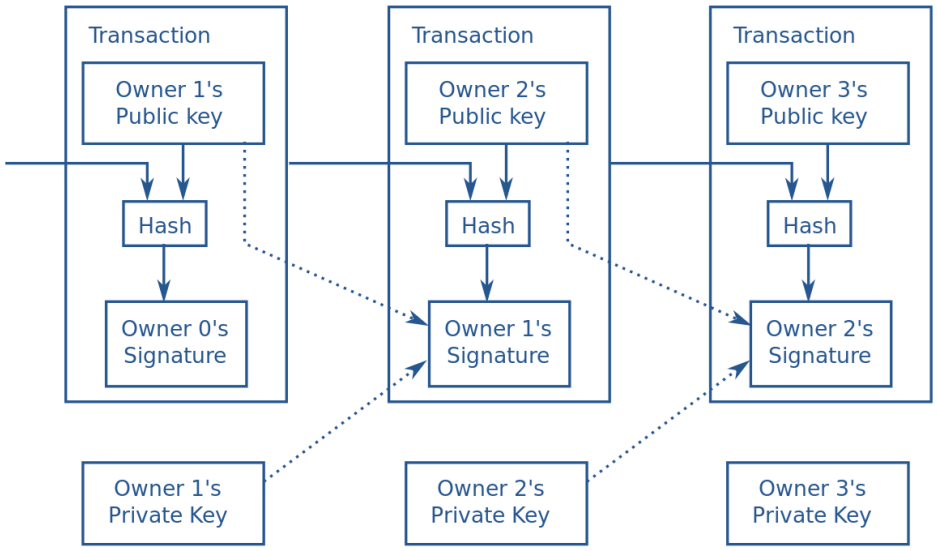
B manda "**Clave pública B"** a A
A desde su monedero entra en su monedero ("**Clave pública A"**) usando su "**Clave privada A"**

Clave pública y clave privada

Clave privada: AF18 A03B BFD2 5E8C D036 4141

Clave pública 1421pqgSvmee8t196A69n7TSxS2vaPQ6L1

Monedero (Wallet)



Hash asociado con cada transacción

¿Qué es el BlockChain?

El registro de todas las transacciones

https://www.blockchain.com/explorer

https://privacypros.io/tools/bitbonkers/
https://symphony.iohk.io/en/

Clave pública y clave privada

Clave privada: AF18 A03B BFD2 5E8C D036 4141

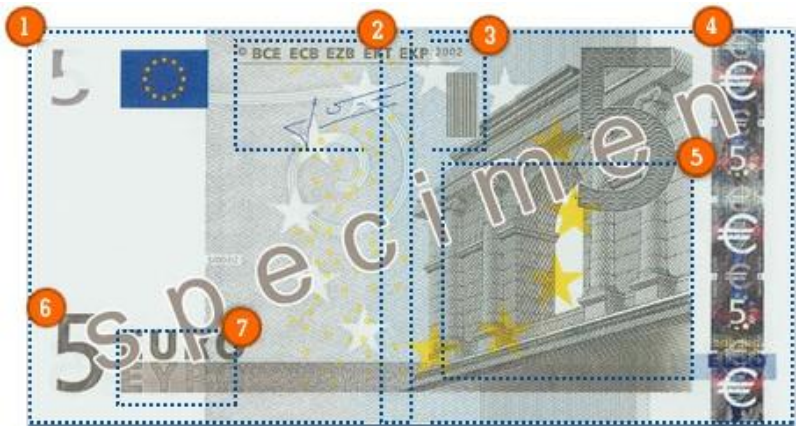
Clave pública 1421pqgSvmee8t196A69n7TSxS2vaPQ6L1

Monedero (Wallet)

¿Cómo funciona un holograma?

Importante: Para usar la tecnología no es necesario entenderla

BlockChain permite contar, hacer registros asociados con personas



Clave pública y clave privada

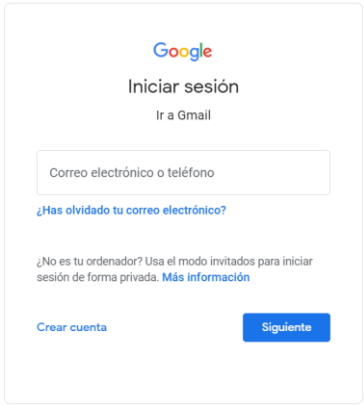
Clave privada: AF18 A03B BFD2 5E8C D036 4141

Clave pública 1421pqgSvmee8t196A69n7TSxS2vaPQ6L1

Monedero (Wallet)

Identidad digital (digital ID)

- Primer nivel biométrico
- Información personal:
  - Edad
  - Empadronamiento
  - Sanidad
  - Información bancaria
  - DGT, Federaciones…
  - Seguros contratados
  - …



Clave pública y clave privada

Los mineros del Bitcoin

Funciones:

- Conservar la cadena (343,25 GB)
  https://ycharts.com/indicators/bitcoin_blockchain_size
- Validar las transacciones. Cobran comisión por ello

- Encontrar los nuevos bloques:
  - 1 nuevo bloque cada 10 minutos
  - https://www.blockchain.com/es/stats
  - Dificultad del minado

Clave pública y clave privada

Resumen

- **Bitcoin** – El origen (2008) – La rueda de madera
- El **token**… hoy ha dado poco juego
- **Aspectos filosóficos muy poderosos:** P2P, código abierto…
- Wallets, hashes, mineros… un mundo curioso.
  - No es necesario conocer como funciona la tecnología para usarla.
  - Aún así hay que tener claro de qué estamos hablando.
- Identidad digital, gobernanza…

¿Cómo encaja todo esto en un mundo que está en total transformación?

¿Qué vamos a hacer la próxima sesión?

- **Repasar** todo lo que hemos hecho hoy… y resolver todas las dudas que tengáis

- Trabajar con **Ethereum** (Smart contracts, tokenización…)

GRACIAS