Tema 8 – Tecnología

Profesor: Luis Garvía Vega

Entorno económico

Madrid, 16 de marzo de 2026

¿De qué vamos a hablar esta semana?

- **Introducción**
  - Estructura
  - Metodología
  - Crisis del 2008 y 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
- **Del sector financiero a los tokens**
- **Ethereum**
  - Máquina de Turing - Ethereum Virtual Machine
  - Smart Contracts
  - ERC-20 – El poder de la estandarización

¿Qué lo cambia todo?

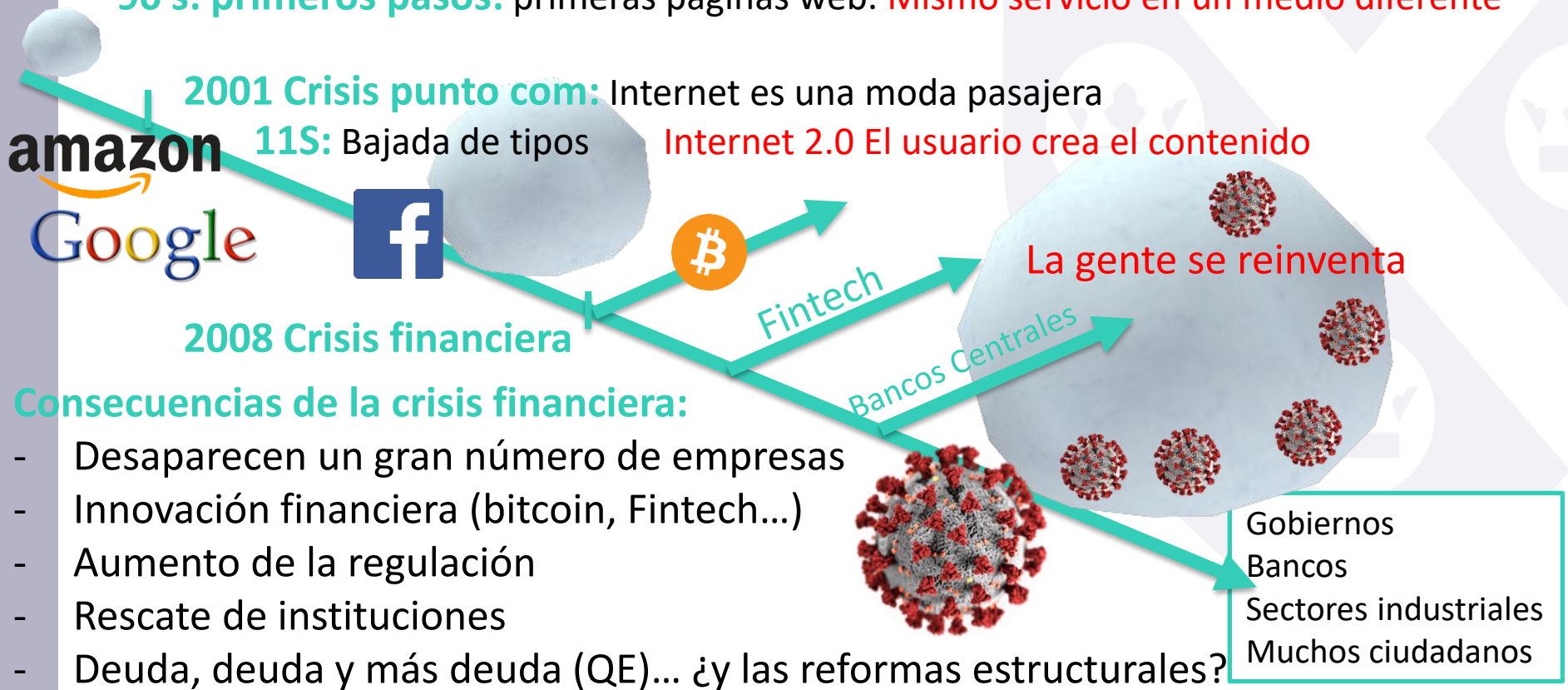
INTERNET

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

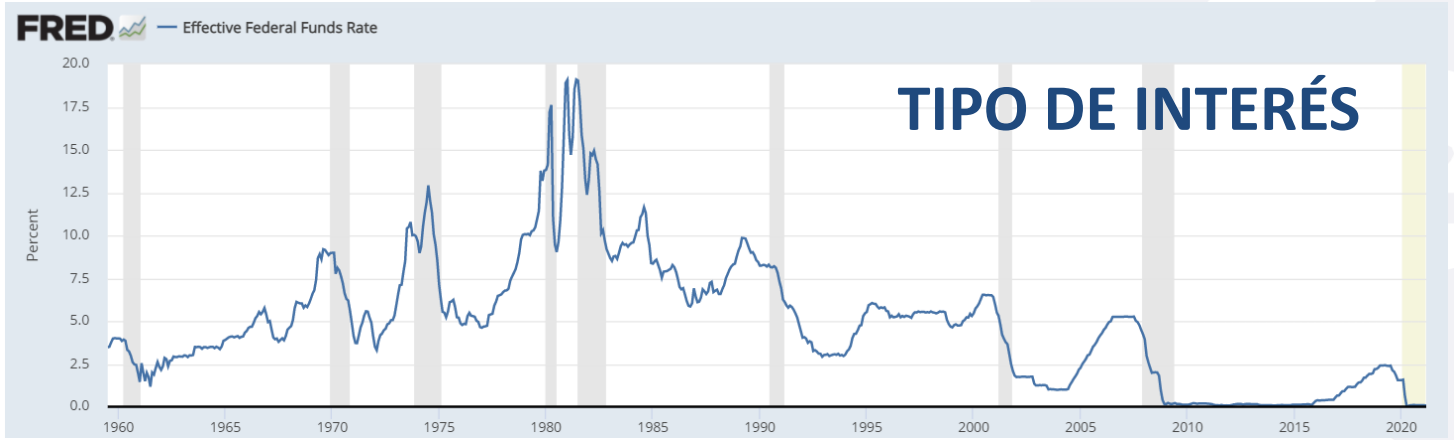


2008 Crisis financiera

Consecuencias de la crisis financiera:

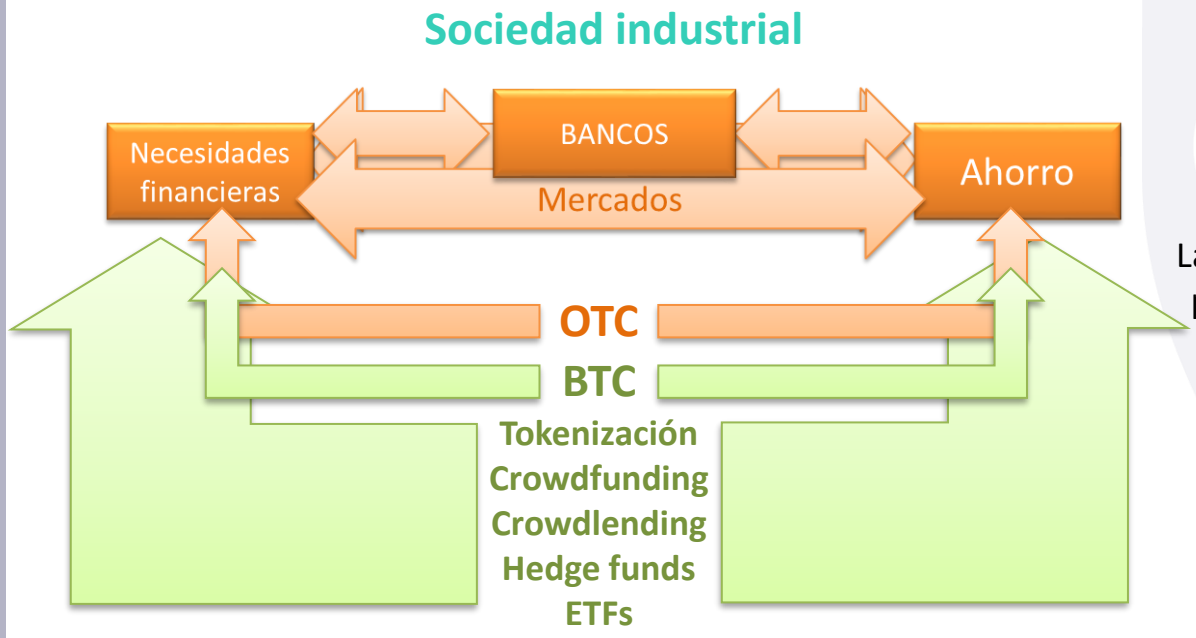
- Desaparecen un gran número de empresas
- Innovación financiera (bitcoin, Fintech…)
- Aumento de la regulación
- Rescate de instituciones
- Deuda, deuda y más deuda (QE)… ¿y las reformas estructurales?

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

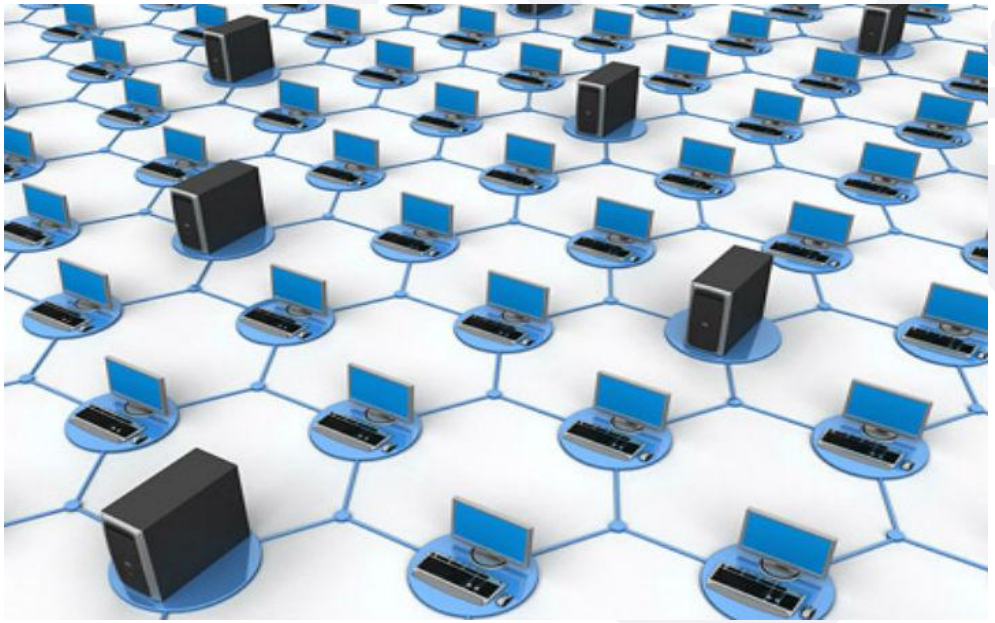
Reacciona: Está preparando inyecciones de dólares digitales

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

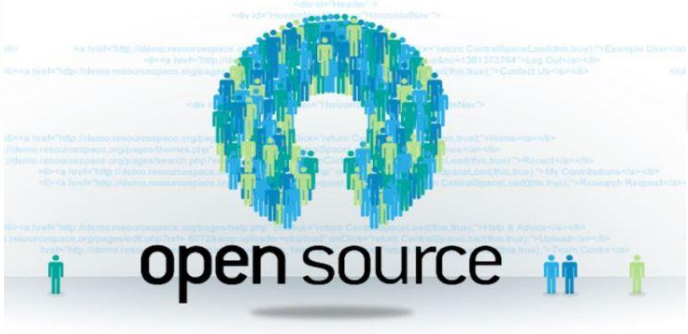
Resumen. Una forma de dinero en efectivo electrónico puramente *peer-to-peer* debería permitir enviar pagos *online* directamente entre las partes y sin pasar a través de una institución financiera. Las firmas digitales son parte de la solución, pero los beneficios principales desaparecen si un tercero 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



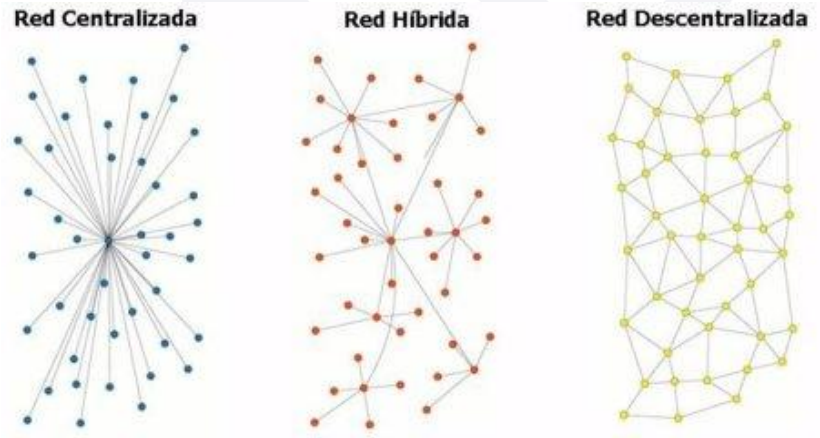
El **código abierto** se utiliza en las comunidades de software libre desde 1990

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

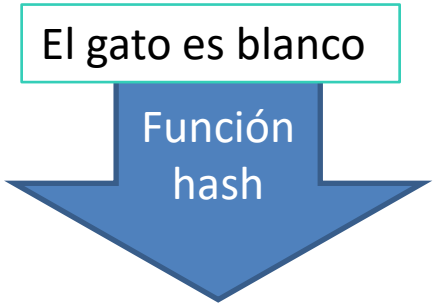
9.817 * 2.371 = 25.043.167

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}

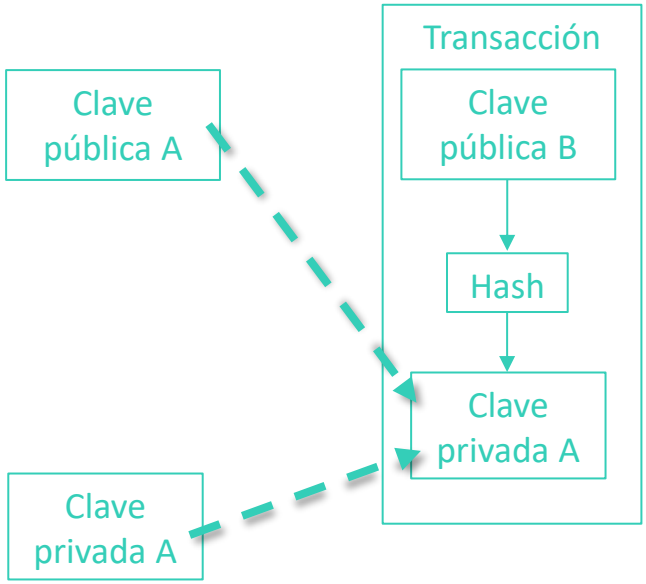
0 = 0000	4 = 0100	8 = 1000	C = 1100
1 = 0001	5 = 0101	9 = 1001	D = 1101
2 = 0010	6 = 0110	A = 1010	E = 1110
3 = 0011	7 = 0111	B = 1011	F = 1111

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**

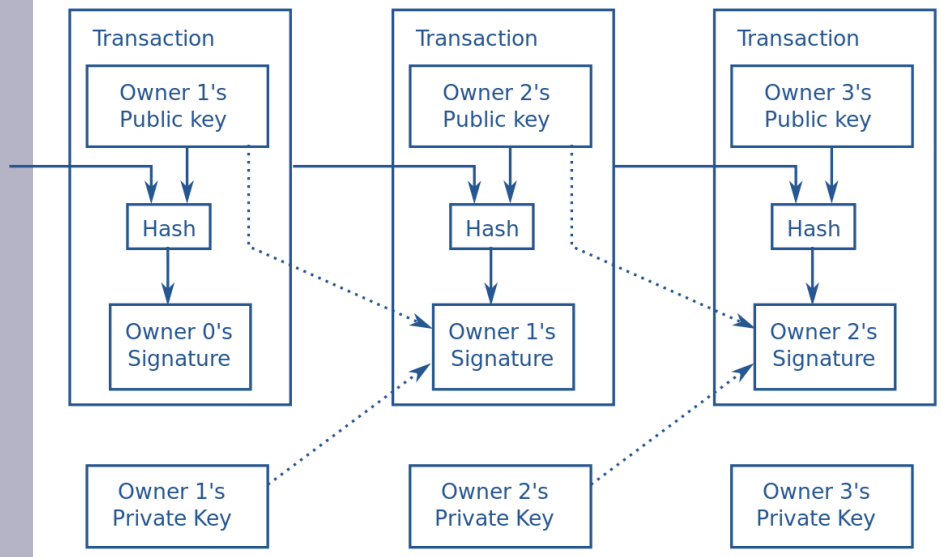
B manda "**Clave pública B"** a A
A desde su monedero entra en su monedero ("**Clave pública A"**) usando su "**Clave privada A"**

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

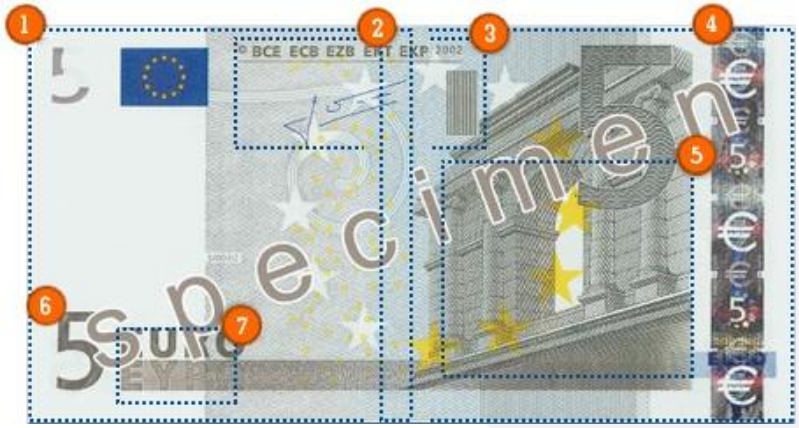
Clave pública 1421pqgSvmee8t196A69n7TSxS2vaPQ6L1

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

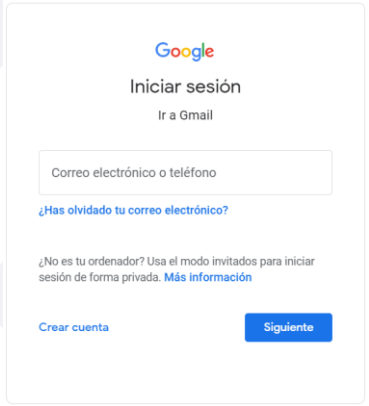
Clave privada: AF18 A03B BFD2 5E8C D036 4141

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

Del sector financiero a los tokens

¿Quién trabaja en los mercados financieros?

EAFIs (Asesores)

Empresas de Servicios de Inversión (ESIs)

- Sociedades de valores
- Agencias de valores
- Gestoras de carteras

Inversión Colectiva

Bancos trabajando como ESIs

Compañías de seguros

Plataformas Online
Brokers Online

¿Qué se negocia?

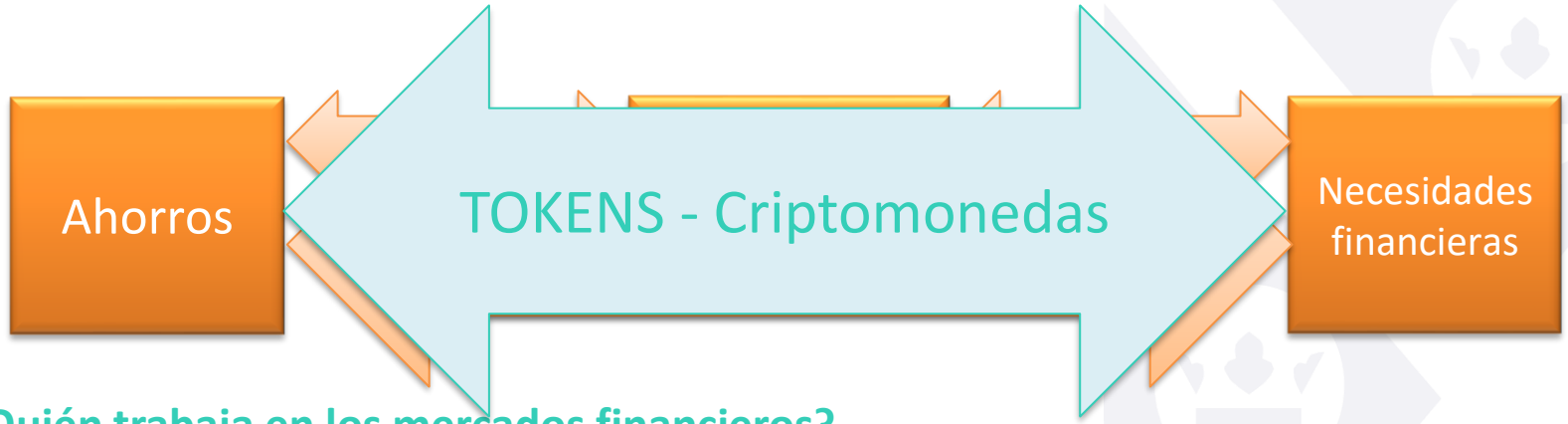
Instrumentos financieros:

- Dinero
- Acciones
- Bonos
- Préstamos
- Derivados

Requerimientos de Compliance

- Requerimientos generales de los mercados financieros (LMV)
- Requerimientos específicos de cada activo
- Requisitos específicos por cada agente
- En el caso de los bancos: Basilea y requerimientos de los BC
- MiFiD II (requisitos sobre riesgos, clientes y productos)
- Blanqueo de capitales, protección de datos, transparencia, interoperabilidad…

Del sector financiero a los tokens



¿Quién trabaja en los mercados financieros?

SMART-CONTRACTS

Plataformas Online
Brokers Online

¿Qué se negocia?

Instrumentos financieros:

- Dinero
- Acciones
- Bonos
- Préstamos
- Derivados

Requerimientos de Compliance

????

¿Quién cumple mejor con la ley? ¿Un Robot o un human? ¿Es suficiente con cumplir con la ley?

Del sector financiero a los tokens

¿De qué estamos hablando?

- Es un pájaro… Es un avión... No, es Superman
- Es inteligente... Es un contrato... No, es un **Smart Contract**

Un algoritmo que proporciona servicios de inversión a un inversor

Solo es Software

- Es dinero... Es un instrumento financiero...No, son **criptomonedas**

Son un Token

¿Qué es un token?

Un token es un derecho digital que solo existe en Internet (una unidad)

Una unidad, dos unidades, tres unidades…

Ethereum

Recordemos de la última clase:

- Vitalik Buterin
- 2013: WhitePaper
- 2014: Crowfunding
- La red nació el 20/07/2015

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)

DISRUPTIVE TRAINING

¿Por qué no incorporar una máquina de Turing completa a los nodos del sistema que trabajan con la cadena de bloques?

Ethereum

Conceptos básicos:

- Ethereum y Ether (ETH)
- **Bitcoin** + Máquina de Turing
- Token (Wei): 10^{18} = 1ETH
- 10^{9} Gweig = 1ETH
- **Smart contracts** – Gas
  - Unidad fija que cotiza en Gweig (para evitar volatilidad)
  - Gas Limit:
    - Transacción: 21.000 unidades de Gas
    - Smart contract: variable entre los 130 y 145 mil Unidades de Gas.
    - Bloque: 8 millones de Unidades de Gas.

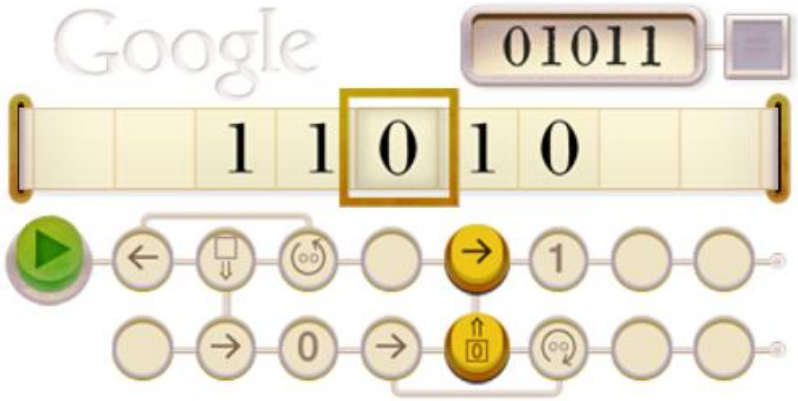
Ethereum

Máquina de Turing conocida desde 1936 Ethereum Virtual Machine

Smart Contracts desde 1995

La estandarización (**ERC-20**)

Ethereum – Máquina de Turing



Alan Turing (1936) (link)

Datos + Programas

Elementos:

- Cinta (memoria)
- Cabezal (autómata) que lee o escribe en la cinta
- Programa (le dice al cabezal como moverse)

Ethereum Virtual Machine. Los nodos del sistema, además del BlockChain incluyen una máquina de Turing completa. Es un verdadero ordenador en red.

Ethereum – Máquina de Turing

Bitcoin – Cuenta

Ethereum – Un ordenador

dApps (Aplicaciones descentralizadas) – Son Apps (aplicaciones) que se ejecutan en una red descentralizada (P2P). **¿Confiaríais en ellas?**

Cuando convergen con el BlockChain son 100% fiables

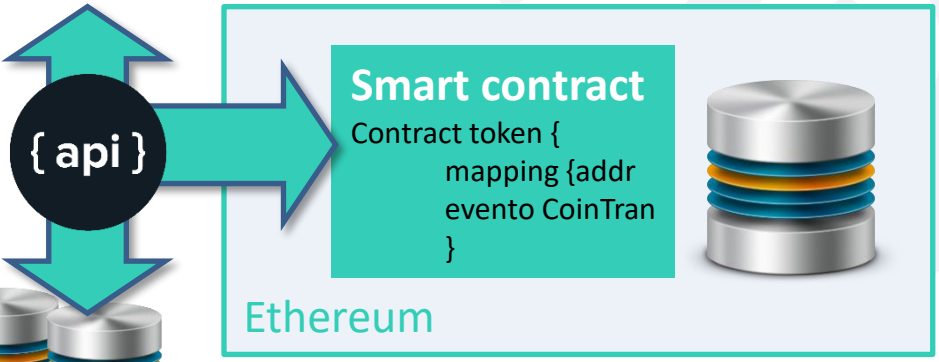
¿Recordáis lo de que el sistema financiero se rompió en el 2008?

Ethereum – Máquina de Turing

Full Stack

Front end – Lo que ve el usuario final
UI (interfaz de usuario) y **UX** (experiencia de usuario)
HTML, **CSS** y **Javascript**

Back End – Del lado del servidor: bases de datos, interacción con cuentas de usuarios, realización de pagos…
Python, **Java**, **MySQL**… trabajo con **APIs**



Bases de datos

Ethereum – Smart contracts

Son inteligentes… son contratos… no, son **Smart Contracts**

¿Qué es un Smart Contract?

Es sólo **software**: un programa informático

Es código asociado a una **clave pública**:

- Por lo tanto hay EOAs (Externally Owned Account) y smart contracts
- Realmente el smart contract está asociado a dos claves públicas: la de su creador y la del propio smart contract

Una vez programado se **despliega** (instala) en la BlockChain esperando a que se active por una transacción desde una EOA u otro Smart contract.

Sobre los visionarios: Alan Turing y Nick Szabo (1995): https://web.archive.org/web/20160417212209/https://szabo.best.vwh.net/smart_contracts_glossary.html

Ethereum – Smart contracts

El **BlockChain** es una **base de datos** abierta al mundo…

… y los Smart Contracts también están **abiertos** y **no se pueden modificar**

¿**Smart**? ¿Qué pasa si hay un **error** en la programación?

- El ataque DAO – 50 millones de dólares (Link) 2016
- ¿El código es ley? ¿Cómo se regula?
- Error al meter las cantidades (Link), error en la programación (Link), con la protección de datos…

Ethereum – ERC20

Los primeros días de Ethereum debieron de ser complejos. La gente programaba tokens sin orden ni concierto.

Y así aparece el ERC (Ethereum Request for Comment) 20, y los **tokens ERC20**. Se estandarizan los Smart Contracts.

Características del contrato:

- Emite nuevos tokens (denominación –ticket–, decimales y volumen)
- Gestiona las transacciones
- Controla el saldo de cada usuario

Hay muchos: https://eips.ethereum.org/erc

Ethereum – ERC20

Tokens fungibles y **tokens no fungibles** (**NFT**s)

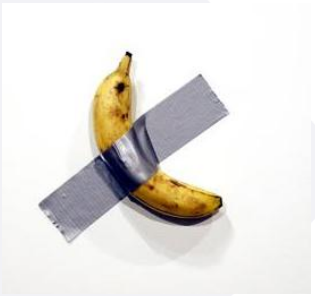
Non Fungible Tokens (NFTs) – **ERC -721**

¿Y 100 euros por una firma de Picasso?

Picasso

La Fuente de Duchamp en 1917

El **plátano** de Cattelan (2018)

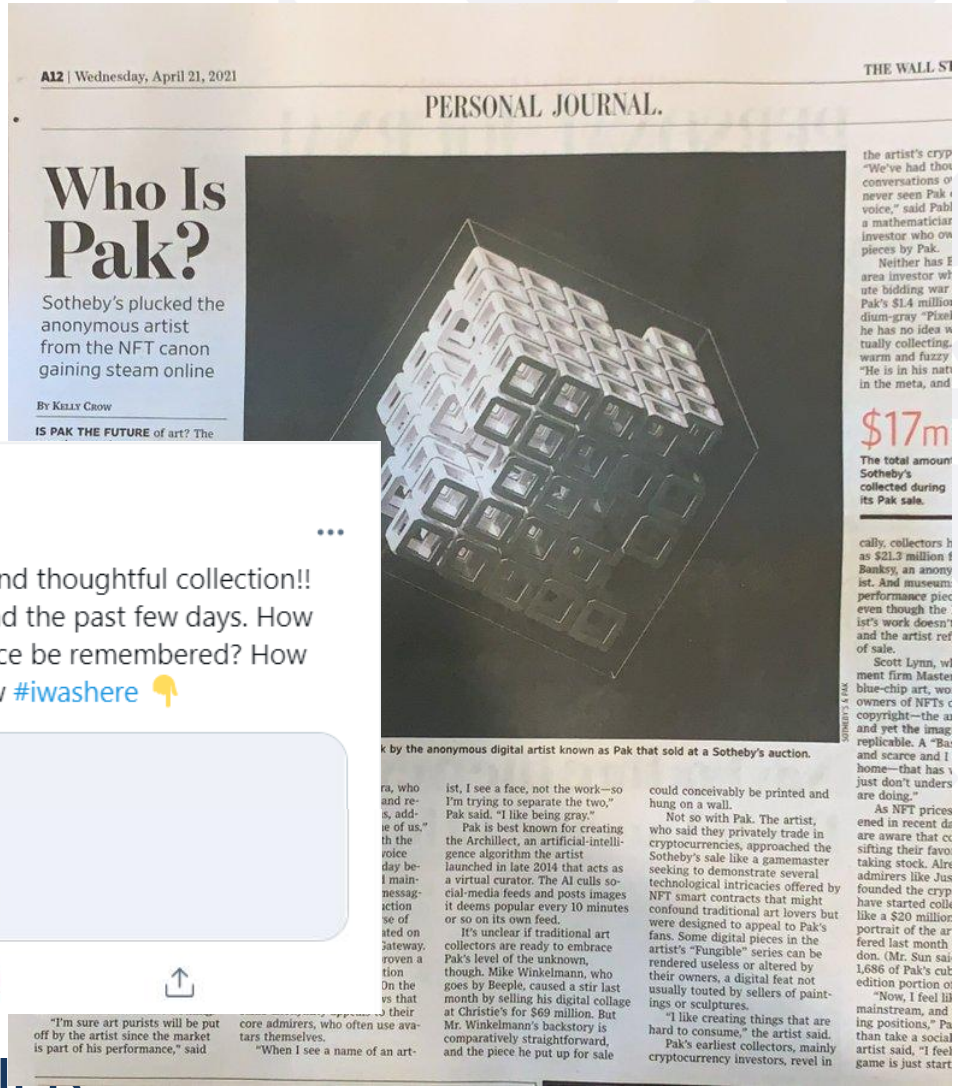


Salvator Mundi – 450M$ **¿Pagaríais 450 millones por un cuadro?**

Ethereum – NFTs

El arte digital

- https://twitter.com/muratpak
- Sothebys – The fungible collection



A12 | Wednesday, April 21, 2021

PERSONAL JOURNAL.

THE WALL ST

Who Is Pak?

Sotheby's plucked the anonymous artist from the NFT canon gaining steam online

By Kelly Crow

IS PAK THE FUTURE of art? The

by the anonymous digital artist known as Pak that sold at a Sotheby's auction.

$17m

The total amount Sotheby's collected during its Pak sale.

Retwitteaste

Eric Young @etyoung · 15 abr.

Congratulations to @muratpak on an amazing and thoughtful collection!! 🎉🎉 The Pixel occupied a great deal of my mind the past few days. How will history reflect on this time? How will this piece be remembered? How will I be remembered? #pakwashere 🧠 and now #iwashere 👇

The Pixel #1/1

This Edition Last Sold For:

$1,355,555.00

104 88 622

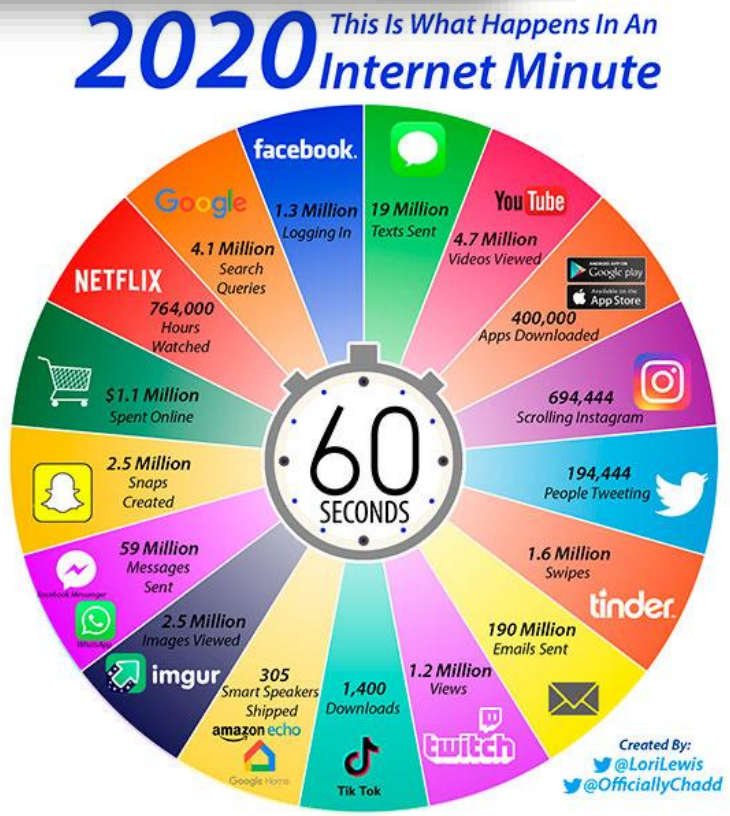
Ethereum – NFTs

Un mercado con un enorme potencial

Jack Dorsey, CEO de Twitter, vende en una subasta el primer tuit de la historia por 2,4 millones de euros

POR 20BITS Marta Gascón NOTICIA 22.03.2021 - 22:05H

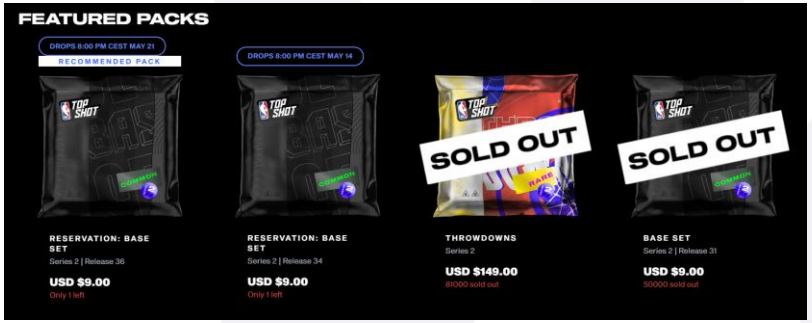
¿Cuál es el objetivo de Jack Dorsey?

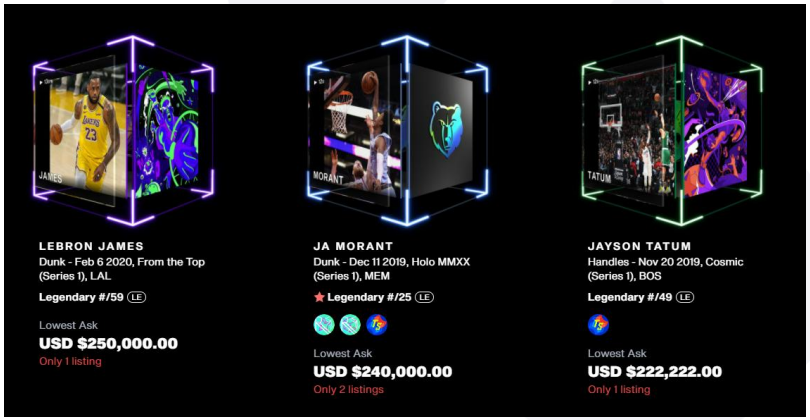


Ethereum – NFTs

NBA Top Shots – https://nbatopshot.com/

- Mercado primario
- Mercado secundario





Ethereum – Liquidez

El Sistema financiero

¿Qué es un mercado?

- Es un sitio
- dónde se venden productos (o servicios),
- entre **compradores** y **vendedores**,
- que tiene **reglas**,
- y **agentes** que ayudan a que todo esto suceda

Liquidez

- ¿Cuál es el instrumento más líquido?
- Cuanto más estándar más líquido
- La estandarización tiene un coste
- ¿Y si necesito una solución a medida?

Mercados regulados vs. OTC

Cuidado: Una cosa es la liquidez y otra el exceso de liquidez

Resumen

- Cuidado con las palabras y las emociones – confusión
- **Bitcoin** – El origen (2008) – Con el bitcoin contamos
- **Ethereum** – Un ordenador al servicio del BlockChain
- **Aspectos filosóficos muy poderosos:** P2P, código abierto, la automatización de procesos, el error, la estandarización…
- **Clave pública**, **tokens**, **smart contracts**… un mundo curioso.
  - No es necesario conocer como funciona la tecnología para usarla.
  - Aún así hay que tener claro de qué estamos hablando.
  - Hay que empezar a cambiar la manera de pensar ciertas cosas.
- El futuro: **Finanzas Descentralizadas**, la **Identidad Digital** y el **Euro digital**

¡Gracias!