Introducción a Bitcoin: Una blockchain abierta, pública, transfronteriza, neutral y resistente a la censura

Mikel Peñagarikano

Departmento de Electricidad y Electrónica
Facultad de Ciencia y tecnología
Universidad del País Vasco/Euskal Herriko Uniberstsitatea, UPV/EHU
mikel.penagarikano@ehu.eus

I Jornadas Bitcoin & Tecnología Blockchain , Leioa 2020

Índice

Presentarme

- Licenciado en Ciencias Físicas, doctor y profesor en el Departamento de Electricidad y Electrónica de la Facultad de Ciencia y Tecnología.
  - Como investigador, me dedico a las *Tecnologías del Habla*.
- No recuerdo mi primer contacto con Bitcoin...
  - Creo que pensé *"Eso debe ser dinero de Second Live"*
- A mediados del 2016 me encontré un software de minería...
  - Me adentré en la madriguera Bitcoin.
- Impulsor del Máster Propio en Tecnología Blockchain y Criptoeconomía

Las fuentes

- **Lunaticoin** (podcast) - https://lunaticoin.com
  - Episodio 66 - **Historia del dinero y Bitcoin** con Juan Ramón Rallo
  - Episodio 101 - **¿Por qué tiene valor Bitcoin?** con Manuel Polavieja
- **Andreas M. Antonopoulos** - https://aantonop.com
  - YouTube - **The Five Pillars of Open Blockchains**
  - YouTube - **Blockchain vs. Bullshit**

Objetivos de esta charla

- Fomentar el debate y el espíritu crítico (*"Don't Trust, Verify."*)
- Analizar los fundamentos monetarios de **Bitcoin**.
- Adentrarnos en la **Madriguera Bitcoin** (*rabbit hole*).

¿Por qué Bitcoin? 🤔

- El 31 de Octubre de 2008 y bajo el pseudónimo de Satoshi Nakamoto, el artículo titulado ***"Bitcoin: A Peer-to-Peer Electronic Cash System"*** fue publicado en una lista de distribución orientada a la criptografía.
  - Revolucionario protocolo para la transferencia de valor P2P (Peer to Peer) a través de Internet
- En Enero de 2009, se crearía la red **Bitcoin**, la primera blockchain **abierta, pública, transfronteriza, neutral y resistente a la censura**.
- ¿Qué es Bitcoin?

  $\rightarrow$ Escasez digital descentralizada

  $\rightarrow$ Dinero electrónico descentralizado

Índice

El dinero: Una tecnología para el intercambio indirecto

Historia de una Tecnología

- En las sociedades primitivas, los individuos se agrupan en pequeños grupos autosuficientes.
- Con la integración en grupos más amplios...
  - → Progresiva división del trabajo.
  - → Los individuos dejan de ser autosuficientes.
  - → Surge la necesidad del **trueque**.

El Trueque

- El individuo puede usar el exceso de su producción para intercambiarlo por otro bien de igual valor o utilidad.
- Para llevar a cabo un trueque se requiere que ambas personas
  - Estén interesadas en las mercancías ajenas.
  - Acuerden las cantidades a intercambiar.

$\rightarrow$ El **Dinero** es una **Tecnología** que aflora de manera espontánea en sociedades de trueque.

Dinero como Medio de Intercambio Indirecto

- Medio de intercambio indirecto de bienes
  - En vez de intercambiar los bienes, se intercambia el bien por dinero, el cual podrá (en un futuro) ser intercambiado por otro bien.
  - Un bien, por consenso emergente, se convertirá en dinero
- El dinero surge como una tecnología facilitadora del intercambio.
  $\rightarrow$ **Reducción de los costes de intercambio**
  - Coste de localización de la contraparte
  - Coste de desplazamiento (personas y mercancías)
  - Coste de establecimiento de *precio* de intercambio
  - Coste de excedente de intercambio
  - Coste de atesoramiento

Ejemplos históricos de Dinero

- **Dinero Mercancía**. Su valor proviene fundamentalmente del bien del cual se compone.
  - → Conchas, cereal, sal, cabezas de ganado, metales preciosos, monedas acuñadas, etc.
- **Dinero Representativo**. También denominado Dinero Metálico, se basa en otro activo (oro, plata, etc.) y tiene la cualidad de ser convertible al activo al cual representa.
  - → Monedas y billetes en sistemas monetarios basados en patrón oro
- **Dinero Fiat**. *Del latín fiat, 'hágase'*. También denominado Dinero por Decreto. Es una forma de dinero fiduciario caracterizado por el respaldo legal de un Estado.
  - → Monedas y billetes emitidos por estados modernos.

El dinero mercancía es un **activo real**, mientras que el dinero representativo y el fiat son un **activo financiero** (deuda).

La isla de Yap (Micronesia) y las Piedras Rai

Propiedades de un buen dinero

- Propiedades fundamentales del buen dinero:
  - Estabilidad de valor
  - Fácil transferibilidad
  - Fácil atesorabilidad/desatesorabilidad
- Características del buen dinero:
  - Aceptabilidad
  - Alto valor unitario (¿O bajo? Mejor ambos)
  - Verificabilidad
  - Divisibilidad
  - Portabilidad
  - Fungibilidad
  - Coste de atesoramiento y desatesoramiento
  - Durabilidad
  - Suministro/emisión limitada (*escasez*)
  - Solvencia (activos financieros o deuda)

Propiedades de un buen dinero

Un mal dinero es mejor que el trueque

Las tres funciones del dinero

- **Medio de Intercambio (MoE, *Medium of Exchange*)**.

  Al contar con un medio de intercambio indirecto de bienes, vendes lo que tienes y compras lo que quieres.

- **Unidad de Cuenta (UoA, *Unit of Account*)**

  El dinero permite usar un único bien como referencia a la hora de asignar valor a los bienes.

- **Reserva de Valor (SoV, *Store of Value*)**

  El dinero tiende a ser un bien imperecedero idóneo para atesorar la riqueza.

→ ¿Tal vez un trilema?

→ Las mejoras tecnológicas nos permiten posicionarnos

Índice

En busca del dinero electrónico descentralizado

Diffie y Hellman - Criptosistema de Clave Pública

- Previamente: Comunicación mediante algoritmos de cifrado simétrico
  - Remitente y destinatario utilizan la misma clave criptográfica
  - Para nuevas comunicaciones, las claves se transmiten a través de un *canal seguro*
- 1976 - Algoritmos de cifrado asimétrico (basados en clave pública)
  - Remitente y destinatario tienen cada uno un par de claves pública/privada
    - Clave pública: uso público
    - Clave privada: uso privado
  - Intercambio de claves a través de un *canal no seguro*
- Además de la comunicación segura, ofrece la **firma digital**
  - Verificación de la autenticidad de la firma
  - Inviolabilidad del mensaje/contenido (detección de manipulación)

David Chaum - eCash - El antecesor de las criptomonedas

- Años 80 - Publicaciones enfocadas en la privacidad
  - "Correo electrónico inrastreable, direcciones de retorno y pseudónimos digitales"
  - "Firmas ciegas para pagos sin rastreo"
  - "Seguridad sin identificación"
  - "Dinero electrónico no-rastreable"
- 1990 - DigiCash Inc.
- 1994 - eCash : Moneda criptográfica con privacidad
  - El banco emite dinero digital y puede verificar los pagos.
  - No puede rastrear los pagos.
- Buena aceptación (Deutsche Bank, Credit Suisse, Norske Bank . . .)
  - En los años noventa se creía que los servicios de internet se costearían mediante microtransacciones (no mediante publicidad).
  - Bill Gates ofreció $100 millones, Chaum pidió 2$ por cada licencia de Windows 95 vendida... el acuerdo no cuajó.
  - El proyecto no consiguió suficiente tracción y pereció en 1999

Adam Back -Hashcash - La prueba de trabajo como dinero

- En los años 90, el spam (correo basura) comenzó a ser un problema.
  - Solución Policial/judicial $\leftrightarrow$ Solución Tecnológica
- Si cada vez que se envía un correo hubiera que pagar una pequeña cantidad de dinero . . .
  - $\rightarrow$ Enviar un correo podria resultar asumible (p.e. 0,0001 €)
  - $\rightarrow$ Enviar 100.000.000 correos no (10.000 €)
- La prueba de trabajo como dinero.
  - $\rightarrow$ El servidor le reclama al remitente una prueba de trabajo
  - $\rightarrow$ El remitente debe consumir electricidad (€) para obtenerla

¿Pero qué es una **prueba de trabajo**?

Proof-of-Work (PoW) - Prueba de trabajo

- Dato difícil de producir pero fácil de validar
- Típicamente obtenido mediante una **Función de Hash**
  - → Convierte una secuencia de datos de entrada (de tamaño variable) en una dato de salida (de tamaño fijo).
  - → Resumen Digital (*digest*)
  - → *Pseudoinversa no-computable*
- Función de Hash: picadora de datos

Napster y el comienzo de las redes P2P

- 1999 - Napster: servicio de distribución de archivos de audio
  - Red P2P para intercambio de música
  - Los participantes intercambian directamente los archivos
- No era del todo descentralizada
  - Un servidor central gestionaba el listado de usuarios y archivos
- 2000 - Las discográficas se querellan contra Napster
  - 2001 - Se clausuran los servidores por orden judicial

$\rightarrow$ incentivo para desarrollar plataformas más dencentralizadas

- Gnutella, Emule, eDonkey, BitTorrent ...

Cypherpunks y dinero descentralizado

- California, 1992. Cypherpunks: cyphers $\leftrightarrow$ cyberpunks
- Interesados en: Privacidad, Tecnología, Encriptación, Polítca, Criptoanarquía y Dinero digital
- Las monedas digitales precisaban de un actor central validador que gestiona el libro de cuentas.
  - $\rightarrow$ Punto de Fallo Singular (*single point of failure*).
  - $\rightarrow$ Conlleva una confianza sobre un tercero.
- Tratarán de desarrollar monedas digitales descentralizadas

Wei Dai - b-money - La primera *stablecoin* descentralizada

- Una criptomoneda estable con un *Registro Contable Descentralizado*
  - Cada participante tiene una copia local
- Creación/distribución del dinero:
  - La red permitiría acuñar monedas a partir de un PoW equivalente a una cesta de bienes.
- Algunos problemas quedaron sin resolver
- No llegó a implementarse

Nick Szabo - Bit Gold - El oro digital

- Una criptomoneda escasa y con Registro Contable Descentralizado.
  - **Oro Digital**
- Emisión basada en PoW
  - Cada unidad de PoW es una *Pepita de Oro* $\rightarrow$ Bit Gold
  - Emisión infinita, pero limitada y descentralizada.
- Los *bits* de oro se encadenan

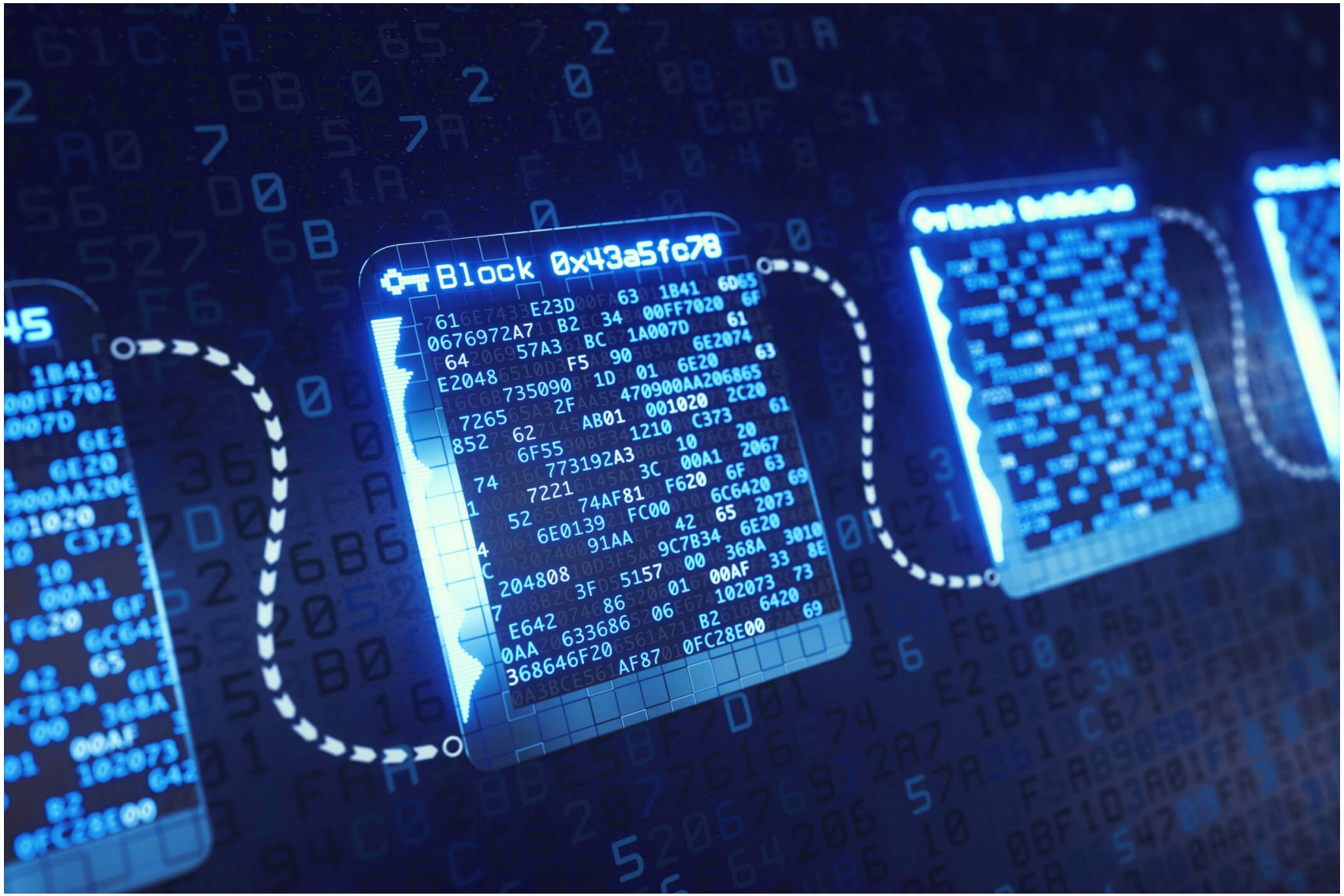
  $\rightarrow$ *Bitchain* $\approx$ *Blockchain*
- Algunos problemas quedaron sin resolver
- No llegó a implementarse

El problema del Doble Gasto

- El problema del doble gasto se da en las monedas digitales descentralizadas.
  - ¿Cómo saber si una moneda no ha sido ya gastada?
- Las monedas físicas no tienen este problema
  - No pueden ser fácilmente duplicadas
- Las monedas digitales centralizadas no tienen este problema
  - El validador central procesa las transacciones por orden de llegada
- **Problema de los Generales Bizantinos**
  - Un problema clásico de los sistemas distribuidos
  - Asegurar que todos los nodos del sistema comparten un mismo estado
  - **¿Cómo consensuar el orden de las transacciones?**

Índice

Fundamentos Tecnológicos de Bitcoin



Transacciones, Bloques y Minería

- Las transacciones son agrupadas en bloques
  - Los bloques se encadenan, creando una **Cadena de Bloques**
  - La mínima modificación en un bloque provoca una modificación en cadena en **todos** los bloques posteriores.
- La PoW se ha realizado sobre cada uno de los bloques de la cadena
  - La mínima modificación en un bloque provoca una invalidación en cadena de las PoW de **todos** los bloques posteriores.
- Los nodos mineros compiten por resolver la PoW sobre el bloque candidato
  - Cada minero puede tener un bloque candidato distinto
  - Ha recibido un conjunto de transacciones distinto y en distinto orden
- Un minero consigue resolver la PoW $\rightarrow$ se lo comunica al resto
  - Verifican la PoW y las transacciones
  - Rehacen el bloque candidato y comienzan a resolver una nueva PoW

Transacciones, Bloques y Minería

- El consenso de la red emerge como consecuencia de la competición de lo mineros
- Incentivos para la minería
  - Con cada bloque, se acuñan nuevos bitcoin
  - Las tasas de transacción que deben aportar los usuarios van a parar a los mineros
- Recompensa probabilística de la minería
  - Los mineros sólo reciben la recompensa si son los primeros en resolver la PoW
- En caso de existir versiones alternativas, los nodos siempre se decantarán por la cadena con mayor prueba de trabajo
  - $\approx$ Cadena más larga (no es lo mismo)

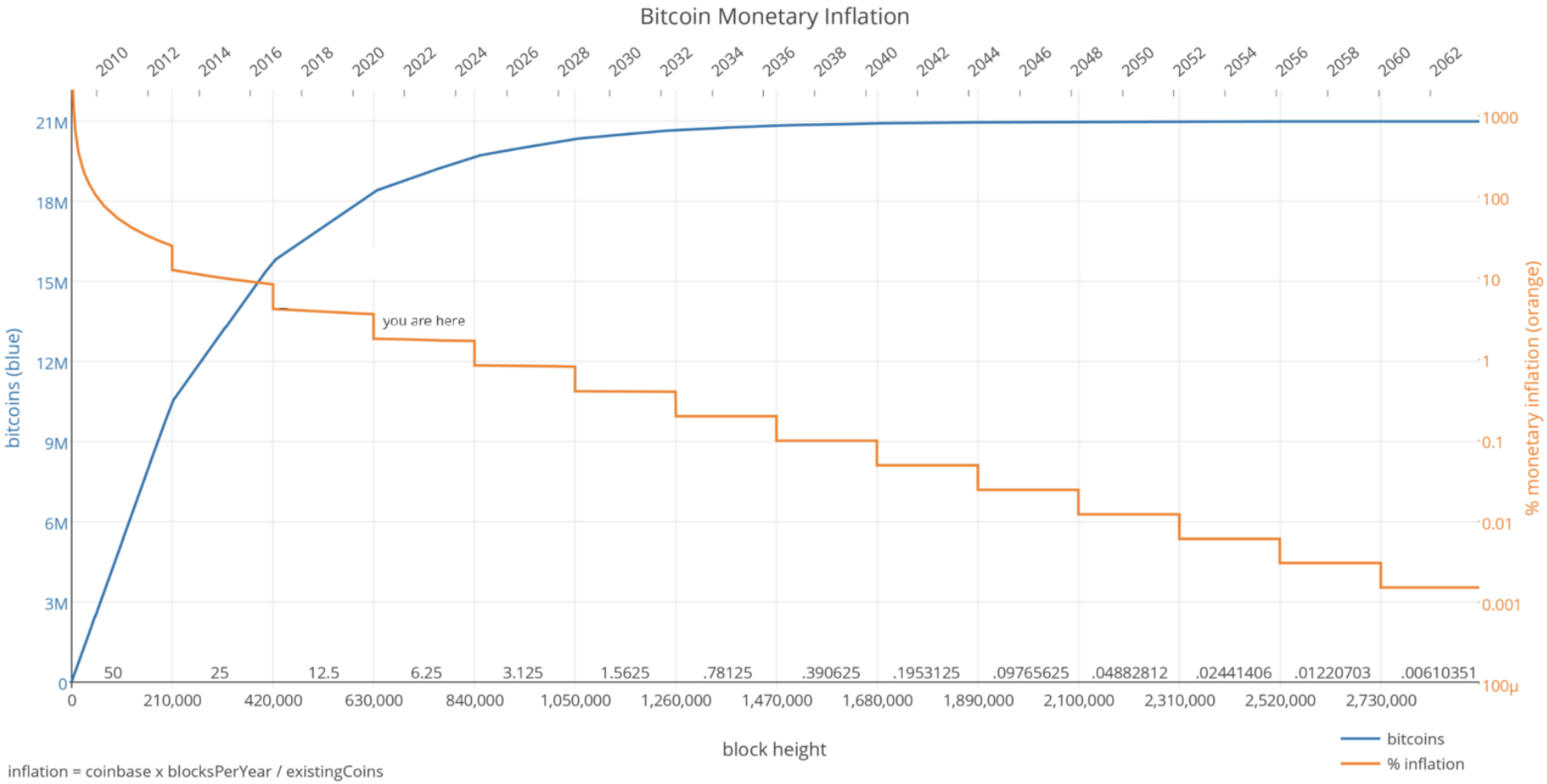
Ajuste de Dificultad

- Objetivo: $\mathbf{t} \approx 10min$ (tiempo promedio de generación de bloques)
  - **R** : hashrate (capacidad de trabajo de la red)
  - Si **R** aumenta, los bloque se minarán más rápido
  - Si **R** disminuye, los bloque se minarán más lento
- El ajuste de dificultad trata de compensar los cambios en el hashrate
  - Cada 2016 bloques ($\approx$ 2 semanas) se recalcula la dificultad de la PoW en función del valor estimado del hasrate **R** (para los 2016 bloques)
  - Si **R** aumenta, se aumenta la dificultad para que $\mathbf{t} \approx 10min$
  - Si **R** disminuye, se disminuye la dificultad para que $\mathbf{t} \approx 10min$

Política Monetaria

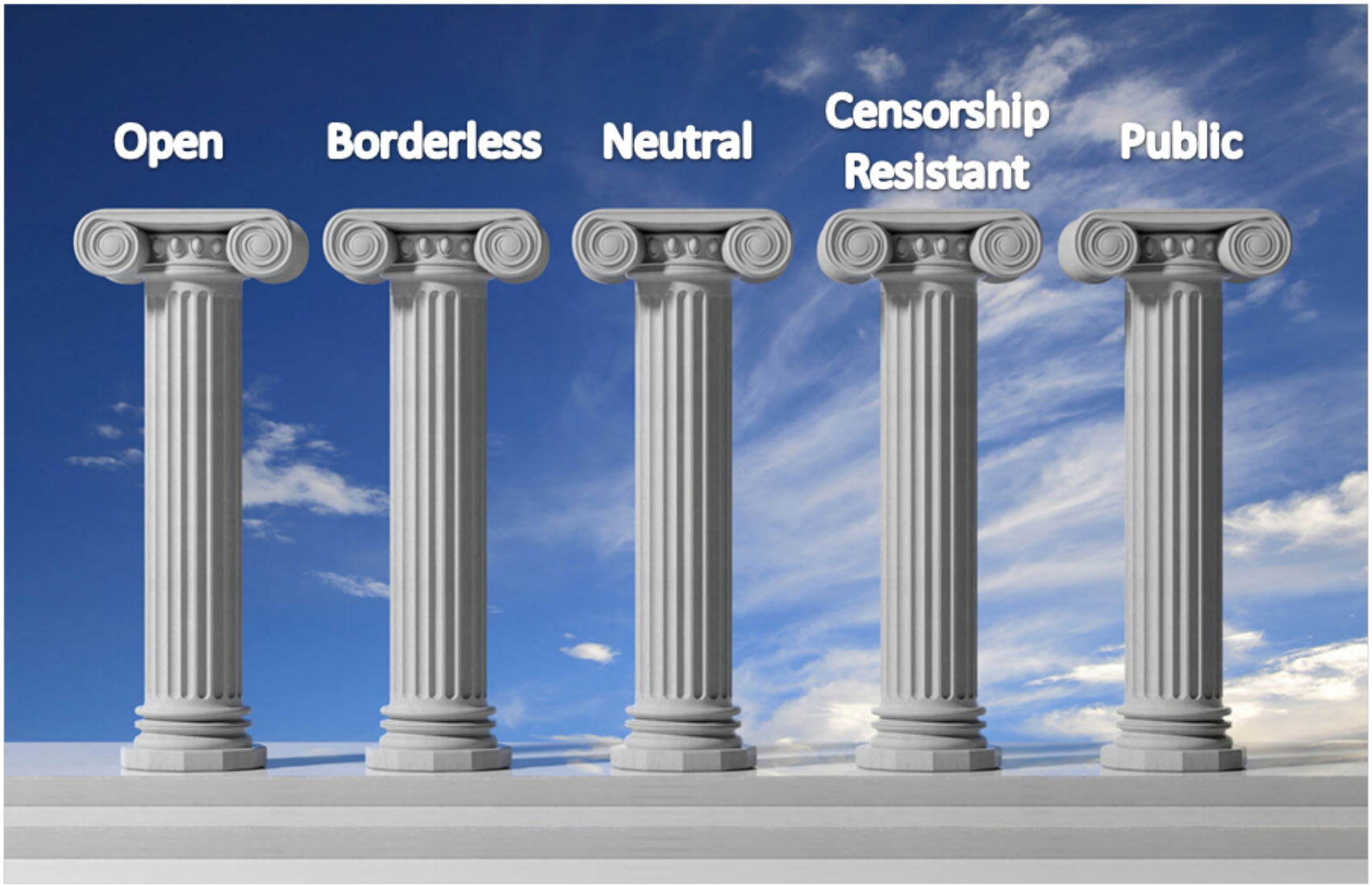
- Nuevos bitcoins son creados como recompensa a la PoW.
- Todo bitcoin en circulación procede de la Recompensa de Bloque
- Cada 210.000 bloques ($\approx$ 4 años) la recompensa se reduce a la mitad
  - **Halving**
  - 2009/01/03 (bloque 0): 50฿
  - 2012/11/28 (bloque 210000): 50฿ $\rightarrow$ 25฿
  - 2016/07/09 (bloque 420000): 25฿ $\rightarrow$ 12,5฿
  - 2020/05/11 (bloque 630000): 12,5฿ $\rightarrow$ 6,25฿
- Emisión finita
  - Nunca llegará a haber 21M฿ .
  - Ya se han minado más de 18M฿ ($\approx$ 89%)
  - Si tengo 1฿ atesoro una 1/21.000.000 parte del total.

Curva de Emisión Monetaria



Índice

Los cinco pilares de Bitcoin



Los cinco pilares de Bitcoin

- **Abierta**. Cualquiera puede acceder/participar sin autorización/identificación.
  - → No precisas ser hombre, blanco, mayor de edad, ni siquiera humano.
- **Transfronteriza**. Como internet.
  - → El valor no reside en un ordenador/país.
  - → Cuando el dinero se convierte en información, no tiene ni forma ni presencia física ni existe en ningún sitio.
- **Neutral**. No existe un por qué / para qué, sólo el qué.
  - → La red procesa cualquier transacción, independientemente del remitente, destinatario o cantidad.
- **Resistente a la Censura**. Nadie puede evitar una transacción.
- **Publica**. Todo es verificable por todos.

Índice

Conclusiones

- El dinero es una tecnología para el intercambio indirecto de bienes
  - → Reduce los costes de intercambio
- Bitcoin es el primer Dinero Digital Descentralizado
  - → Escasez Digital Descentralizada
- Bitcoin propone la separación del dinero y el estado
  - → El estado pierde el control del dinero
- Bitcoin nos ofrece la Soberanía Monetaria
  - → La libertad conlleva responsabilidad

"Not your keys; Not your bitcoin."


Thank You!