Bitcoin: Criptografía, Consenso y Computación Distribuida

Alejandro Fernández Camello

19 de marzo de 2026

Índice

¿Qué es el dinero?

Un medio de cambio ampliamente aceptado que permite la transferencia de valor entre personas

Características del dinero

- Divisibilidad
- Portabilidad
- Durabilidad
- Liquidez
- Unidad de cuenta

Cómo el oro se convirtió en dinero

El momento en el que cambió todo

- En agosto de 1971, Nixon suspendió la convertibilidad del dólar en oro
- Desde el acuerdo de Bretton Woods se había establecido que todas las monedas pudieran ser convertidas al dólar y este, a su vez, en oro
- Las monedas de los países dejaron de estar respaldadas por oro

Consecuencias

- La estabilidad del dinero depende de la confianza en los gobiernos
- En Europa hemos tenido suerte: tenemos instituciones sólidas y una inflación anual media del 2 %
- Otros países no han tenido tanta suerte como Venezuela o Argentina.

Índice

El nacimiento de Bitcoin

- Satoshi Nakamoto publica el whitepaper en octubre de 2008
- Enero de 2009: bloque génesis y arranque de la red
- Regla clave: el máximo número de bitcoins que habrá es de 21 millones

El problema del doble gasto

- En el mundo digital, copiar tiene coste cero
- Necesitamos un tercero de confianza (el banco) en cada transacción para evitar que se duplique el dinero
- Bitcoin elimina este intermediario con una base de datos pública (Blockchain)

La base de datos: Blockchain

- Blockchain es una “cadena de bloques”
- Cada bloque contiene una serie de transacciones
- El conjunto de bloques te da toda la información de cuánto tiene cada dirección

Direcciones en Bitcoin

- Una dirección es un identificador al que se pueden enviar bitcoins
- Permite de manera sencilla hacer pagos
- Es como el IBAN de tu cuenta bancaria

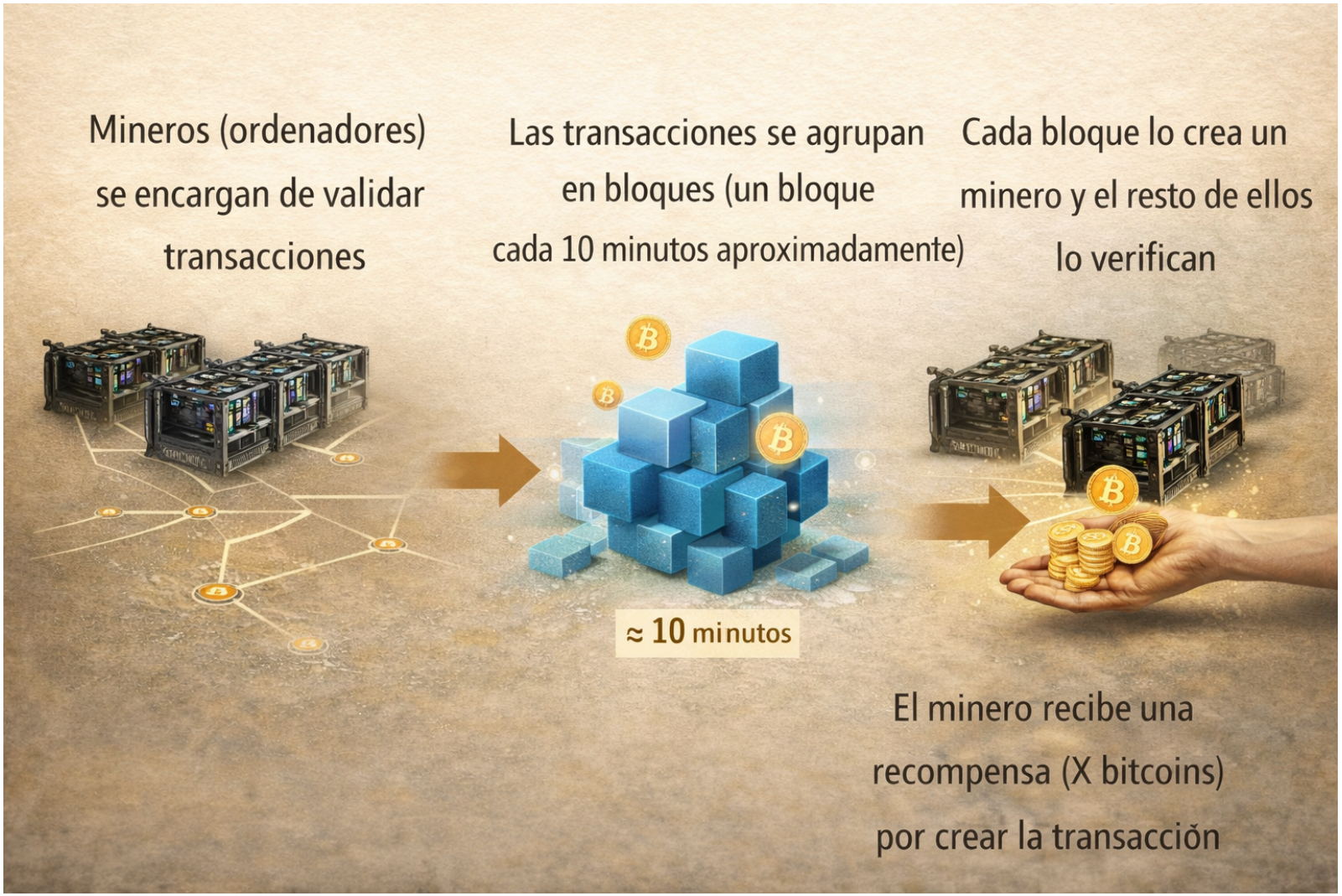
¿Cómo puede la red saber que eres el propietario?

- La red conoce tu clave pública, pero solo tú sabes tu clave privada
- Firmas tu transacción con tu clave privada y cualquiera con tu clave pública puede verificar que la transacción es válida
- Así los mineros pueden ver la validez de tu transacción

Índice

El problema bizantino

Los mineros del siglo XXI



Lotería algorítmica

- Hay que elegir en cada bloque un minero afortunado que reciba la recompensa
- La recompensa la obtiene quien resuelva antes un problema matemático

El problema matemático

- Hay que encontrar un hash menor que una cierta cantidad X
- Es un problema de pura fuerza bruta
- Es un problema muy difícil de resolver, pero fácil de verificar

He resuelto el problema, ¿y ahora qué?

El proceso de una transacción

Índice

Los ordenadores cuánticos al ataque

- El algoritmo Shor es capaz de obtener la clave privada desde la clave pública
- Los ordenadores cuánticos no tienen la potencia (y les falta mucho) para poder usar Shor contra Bitcoin
- En las últimas actualizaciones del protocolo de Bitcoin, la clave pública deja de ser pública

Privacidad y custodia

- Bitcoin es seudónimo, no es anónimo
- Para almacenar bitcoins puedes hacerlo tú mismo o delegarlo a un *exchange*
- Si lo guardas tú mismo, eres el único responsable de custodiar de forma segura la clave privada

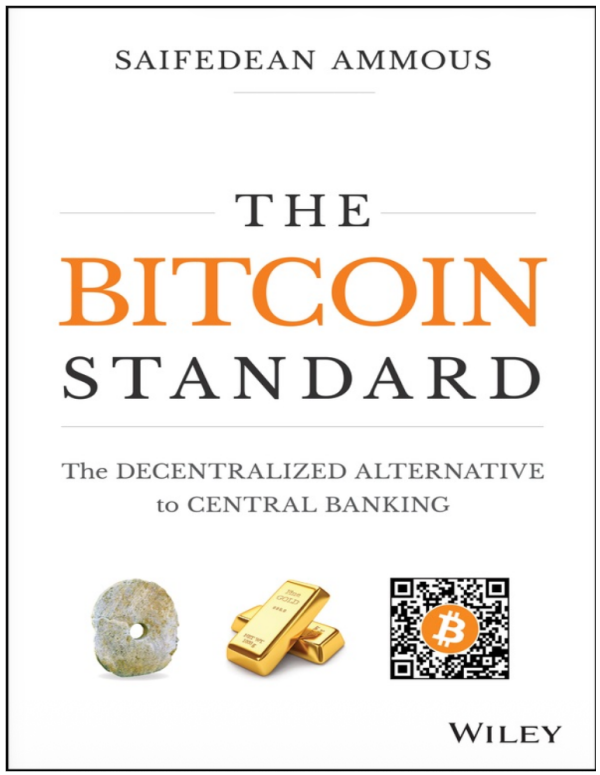
No todo va a ser tan bonito

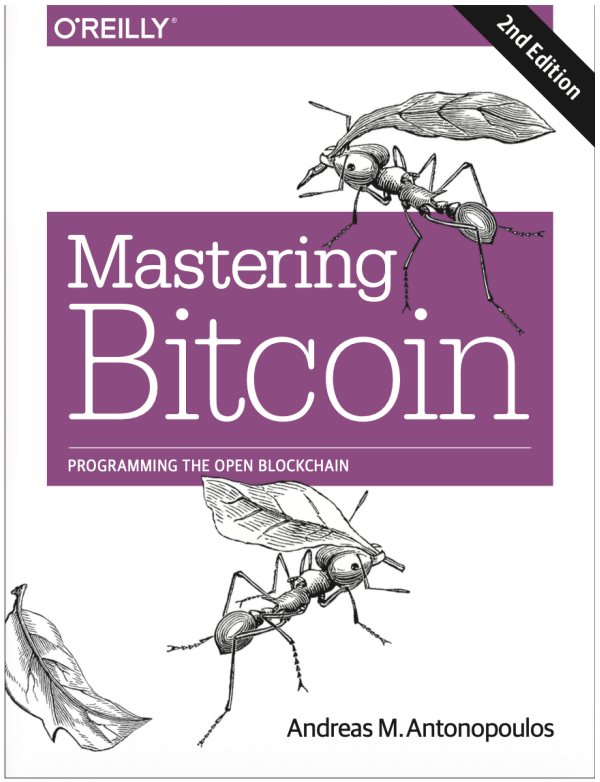
- El precio de Bitcoin puede ser muy volátil a corto plazo
- En momentos de alta demanda, suben las comisiones y los tiempos de espera
- Si pierdes tu clave privada, puedes perder tus fondos para siempre
- Gran gasto energético, ¿merece la pena?

Conclusiones

- Bitcoin resuelve el doble gasto sin necesidad de una autoridad central
- Su seguridad combina criptografía, incentivos económicos y consenso distribuido
- La autocustodia ofrece soberanía financiera, pero exige responsabilidad
- Su evolución dependerá de la adopción, la regulación y la educación técnica

Recomendaciones





Despedida

Espero que os haya gustado, si tenéis alguna pregunta es el momento de hacerla