Dinero Libre

(Introducción a bitcoin)

Martín Dapás

Diciembre 2016

¿Qué es?

Primera moneda digital **descentralizada** (P2P)

Plataforma de confianza distribuida (cuyo **primer servicio** es la moneda)

La Internet de la información

E-mail (*servicio*)

Web (*servicio*)

...

Internet (**plataforma**)

La Internet de la información

Al enviar información (imágenes, texto, etc.), se envía una copia de esa información

Pero para ciertas cosas, no se puede enviar una copia, hay que enviar el original

- Dinero
- Puntos
- Créditos
- Acciones
- Títulos de propiedad
- Etc.

La Internet de la información

Grandes intermediarios en quienes todos “confían”:

- bancos
- gobiernos
- grandes empresas
- tarjetas de crédito
- etc.

La Internet de la información

Problemas

- Único punto de ataque
- Son no inclusivos (>2500 M de personas sin acceso a servicios bancarios o financieros)
- No hay privacidad
- Lentos, burocráticos, monopólicos
- Se quedan con una gran tajada

La Internet de la información

Dinero ***centralizado*** basado en instituciones y leyes

La Internet del dinero

Dinero ***descentralizado*** basado en matemática e internet

Transacciones

Irreversibles (40% de los costos operativos de las CC es prevención de fraude)

Rápidas (pocos segundos de propagación, 5-15 min hasta la 1era confirmación)

Baratas (USD 0.05 – USD 0.25)

Globales

Suministro

Finito (hoy: ~16M; máx: ~21M)

Predecible (12.5 BTC / 10 min)

Se distribuye a quienes ayudan a asegurar la red, en función del poder de cómputo

Principios de funcionamiento

Criptografía de clave pública

Conceptos de redes distribuidas (P2P)

"*Proof-of-work*" para procesar y verificar pagos

(difícil de obtener, fácil de validar)

Seguridad y privacidad

El protocolo y la criptografía de Bitcoin nunca han fallado

El protocolo no requiere que los usuarios asocien su identidad a sus direcciones

Los demás aspectos de seguridad y privacidad están en manos de los usuarios finales (multi-sig, billeteras de papel, por HW, backups encriptados, mixers, etc.)

Aplicaciones

- Pagos por outsourcing o importaciones
- Alternativa con menos comisiones y sin chargebacks para comerciantes
- Giros de dinero (mercado actual de 560.000 M anuales, 10-30% de comisión)
- Inclusión: todo el mundo puede tener el mismo nivel de privacidad, libertad, seguridad y servicios
- Etc.

Blockchain

Registro público, ordenado, distribuido (hoy: >5K nodos), sin ninguna autoridad central, y donde hay consenso global

Elimina la reproducibilidad infinita de un bien digital

El objetivo es obtener la desintermediación

Se puede registrar: eventos, hechos, transacciones, propiedad, etc.

Blockchain

- Dinero programable (*smart contracts*)
- Fondos de inversión automáticos, autotransferencias, facturas automáticas, certificados de acciones automáticos, servicios financieros (préstamos, plazos fijos, etc.)
- Servicios de confianza y notarización
- Trazabilidad
- Social media => Social banking

Preguntas

¿?