



LA NUEVA REVOLUCIÓN: EL BITCOIN Y EL BLOCKCHAIN

HACE 9 AÑOS

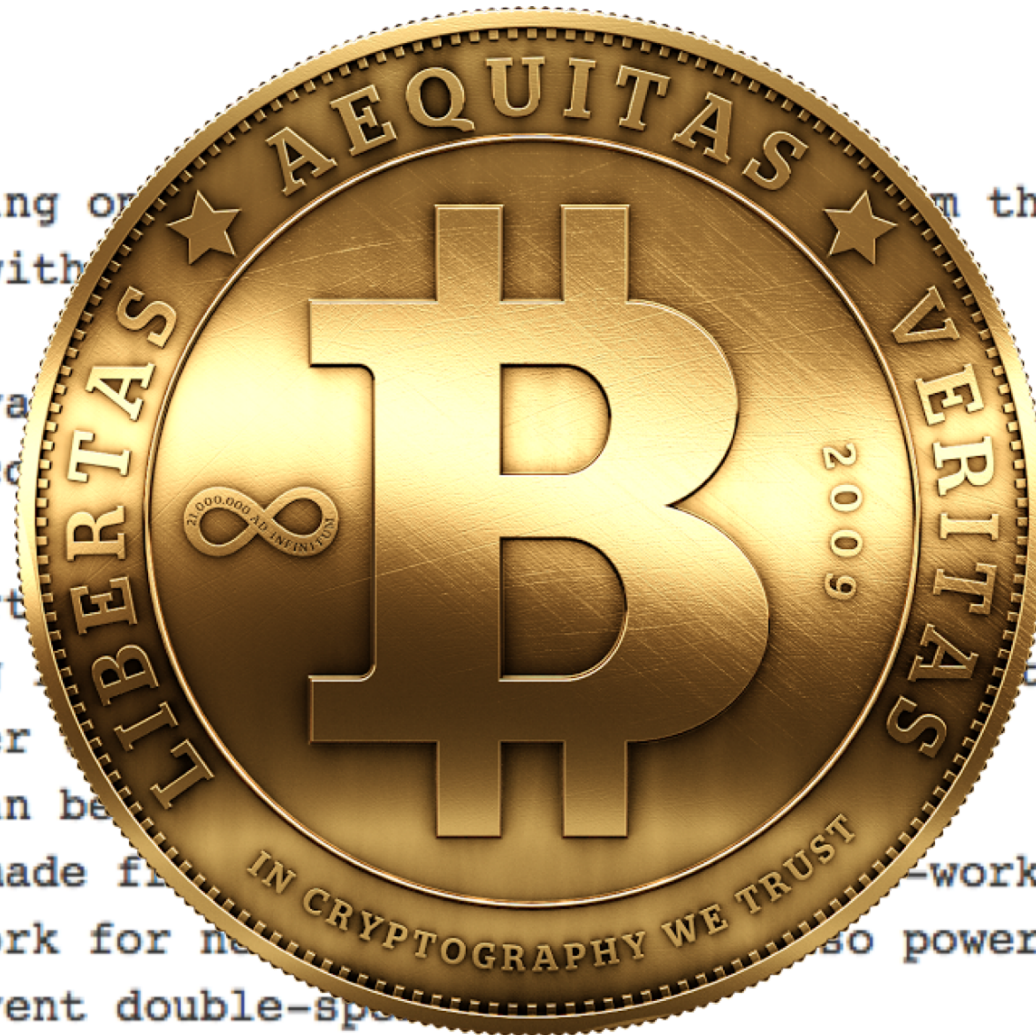
Bitcoin P2P e-cash paper 2008-11-01 19:16:33 UTC

I've been working on a system that's fully peer-to-peer, with

The paper is available at
<http://www.bitcoin.org>

The main properties of the system are:
Double-spending is prevented by a distributed network.
No mint or other central authority.
Participants can be anonymous.
New coins are made from scratch.
The proof-of-work for new blocks is also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System



¿QUÉ ES EL BITCOIN?

- ▶ efectivo digital
- ▶ medio de pago
- ▶ registro inmutable
- ▶ software
- ▶ protocolo
- ▶ activo digital
- ▶ reserva de valor

FIAT MONEY

- ▶ Creación ilimitada
- ▶ Controlado
- ▶ Centralizado
- ▶ Inflación variable
- ▶ Censurado

BITCOIN

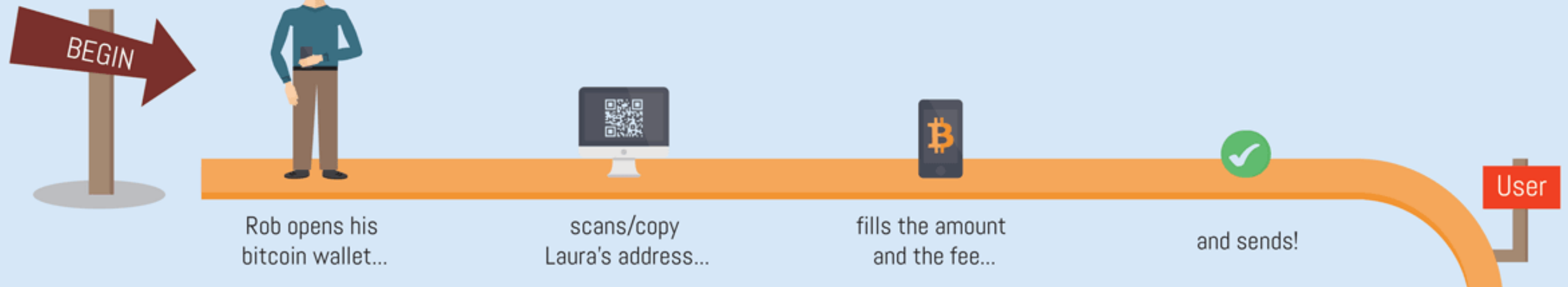
- ▶ 21 millones BTC
- ▶ No es pasivo de control
- ▶ Descentralizado
- ▶ Inflación conocida y controlada
- ▶ Permissionless
- ▶ Censorship resistant
- ▶ Trustless: No confie, verifique

CICLO DE UNA TRANSACCIÓN EN BITCOIN

THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão



CICLO DE UNA TRANSACCIÓN EN BITCOIN

Mining is the computational process of calculating a certain hash.

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Mining time!

New bitcoins
are created!

The miner who solves
the Proof of Work propagates
the new block to the network

Miners include the
transaction in the next
block to be mined

The nodes verify
the result and
propagate the block

The transaction is
propagated and validated
by the network nodes

Laura sees the
first confirmation

The wallet signs
the transaction using
Rob's private key

New confirmations
appear with each new
block that is created

THE END!

Machine

10 seconds
until now!

SÍNTESIS DEL BITCOIN

- ▶ ≈ 17 millones de bitcoins
- ▶ 21 millones en total (2140)
- ▶ 12.5 BTC cada 10 min (cada 4 años cae por la mitad)
- ▶ Poder de procesamiento: + de 500 Googles (2015)
- ▶ Dificultad varia
- ▶ 0,00000001 (8 casas decimales) = 1 satoshi (menor unidad)
- ▶ 1 bitcoin = 100 millones de satoishis
- ▶ 1 bitcoin = U\$ 10.800 (17/feb/18)
- ▶ 6000 nodos
- ▶ Transacciones por segundo $\approx 3-7$

¿POR QUÉ EL BITCOIN ES IMPORTANTE?

- ▶ Internet del dinero
- ▶ Creación del Bitcoin en medio del rescate financiero
- ▶ Reserva de valor
- ▶ Sin fronteras
- ▶ No necesita permiso. (Venezuela)
- ▶ Bearer instrument (título al portador). Chipre 2013 - confisco
- ▶ Intento del gobierno en eliminar efectivo (imponer tasas negativas)



¿POR QUÉ EL BITCOIN ES IMPORTANTE?

- ▶ Seguridad y inmutabilidad:
 - ▶ descentralización
 - ▶ distribuído
 - ▶ sin un líder/empresa
 - ▶ alto poder procesamiento
 - ▶ consenso

¿Y EL BLOCKCHAIN?

- ▶ ¿Qué es un Blockchain?
 - ▶ Libro mayor digital público (ledger)
 - ▶ Distribuido
 - ▶ Proof of work (PoW)
 - ▶ Descentralizado
 - ▶ Inalterable
 - ▶ No confie, verifique
 - ▶ No todo blockchain es un Blockchain
 - ▶ Blockchain privados. E.g: IBM, KSI Estonia
 - ▶ Ripple, IOTA (tangle)

¿Y EL BLOCKCHAIN?

▶ ALTCOINS

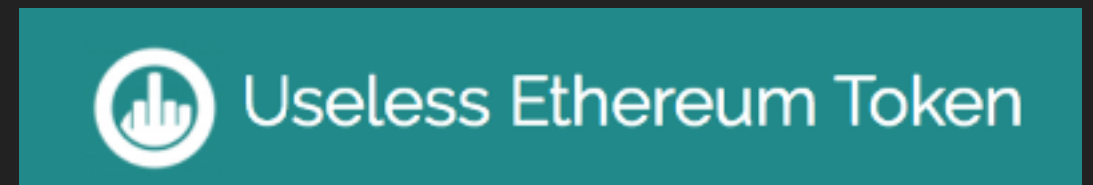


▶ TOKENS



¿Y EL BLOCKCHAIN?

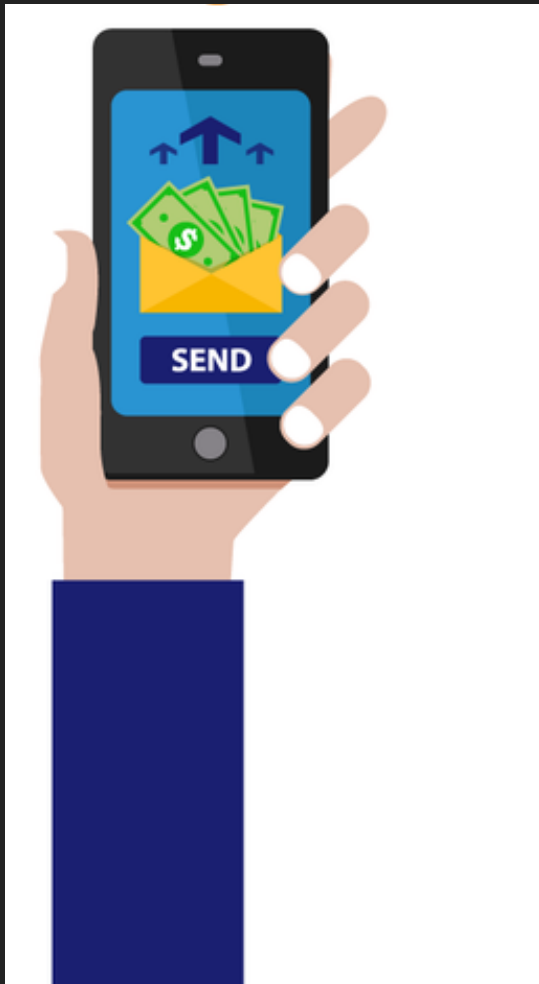
ICOs



- ▶ 211 en 2017
- ▶ \$ 3.800 millones
- ▶ Security tokens (valor mobiliario)
- ▶ Utility tokens (promesa de venta de un producto)

APLICACIONES DEL BITCOIN / BLOCKCHAIN

REMESAS INTERNACIONALES



DONACIONES



CRUZ ROJA COSTARRICENSE No. 0107855
RECIBO DE TESORERIA

DIA	MES	AÑO
10	10	17

RECIBIMOS DE: Comunidad Bitcoin Costa Rica
LA SUMA DE: mil doscientos setenta y cuatro (1264) siete dólares.
PER CONCEPTO DE: Donación damnificados tormenta tropical NATE.
C/C: 204-7
DEPOSITO: ☒ C. CONTAR: ☐

CRUZ ROJA COSTARRICENSE
CAJA
102727
Daniel Alvarado
CANCELADO
ALAS DEL SELLO Y FIRMA DEL CULPADO

COBRO CUENTA
EFFECTIVO ☐ CHEQUE No. ☐ BANCO ☐

FIRMA RESPONSABLE

LA VALIDEZ DE ESTE RECIBO DEPENDE DE QUE LOS CHEQUES RECIBIDOS SEAN PAGADOS POR EL BANCO A NUESTRA INSTITUCIÓN.

RESERVA DE VALOR



AUTENTICACIÓN DE DOCUMENTOS



DIGITAL SIGNATURE, REGISTRY AND CERTIFICATION

BitRegistro: Blockchain providing a Proof-of-Authenticity protecting your creations,
ideas, contracts and much more

APUESTAS

Event : 2016 US Presidential Election

Start Time : 11/08/2016 04:59

Competition : 2016 US Presidential Election

Bet Type : Next President

Your Selection : *Donald Trump @ Best Available Odds On Receipt.*

No more bets can be accepted at this time.



Bet Received :

Amount Received : 0.024 BTC.

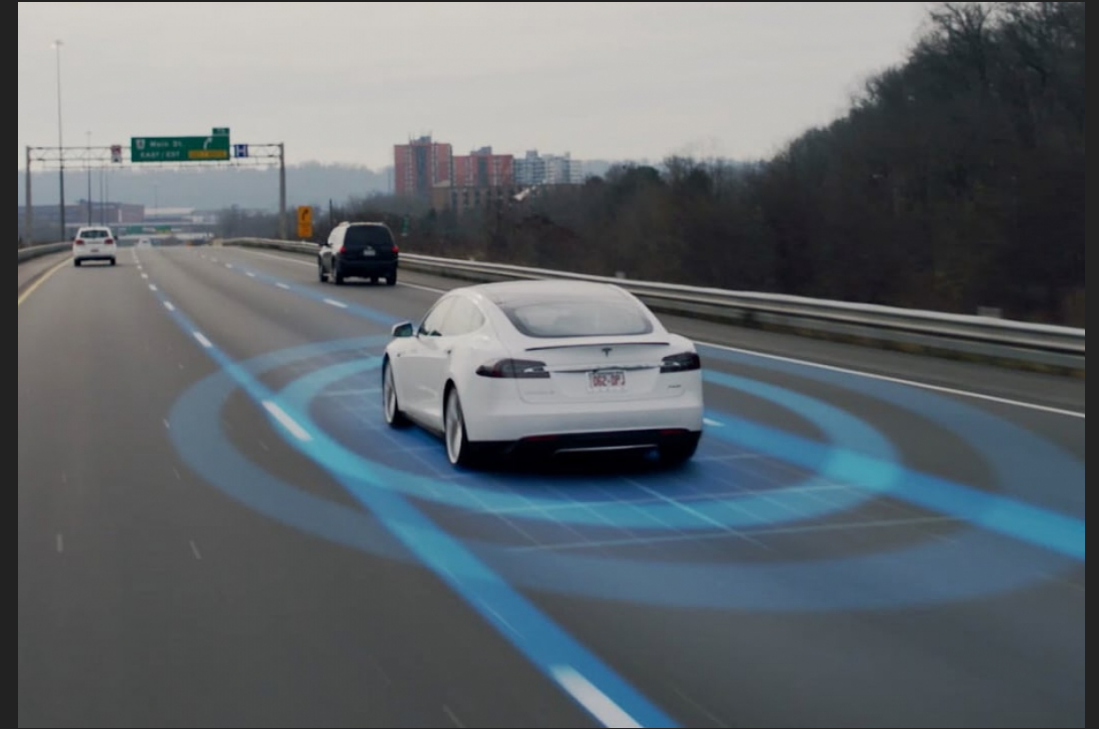
Bitcoin Transaction ID :

Confirmed Odds : 5.3

Bet Status : *Settled*

Message : A Payout was issued. Payout Transaction ID #

SMART CONTRACTS



DESAFIOS Y HORIZONTES

- ▶ Marco regulatorio
- ▶ Escalabilidad
- ▶ Usos para la tecnología
- ▶ Satélites
- ▶ Lightning network
- ▶ Sidechains

CONTACTO

- ▶ **Felipe Kirsch**
- ▶ **felipebtc@icloud.com**

- ▶ **Telegram:** <https://t.me/btccr>

- ▶ **WhatsApp:**



- ▶ **Encuentros:** [meetup.com/Comunidad-Bitcoin](https://www.meetup.com/Comunidad-Bitcoin)