Bitcoin

ReD

Cofundador de Hacklabs

Apasionado de la tecnología

Defensor de la privacidad

Base del sistema económico

- Pago directo
- Pago a distancia
- Pago con intermediarios (bancos)
- ...

Criptomoneda
B-money

- Concepto descrito por Wei Daide
- Lista de correo cypherpunks (1998)

Bitcoin

- `BTCs = bitcoins`
- 3 de enero de 2009 se crea el BLOQUE GENESIS
- Creador Satoshi Nakamoto
  - Paper Bitcoin: A Peer-to-Peer Electronic Cash System
  - Cliente Bitcoind

Bitcoin
Características de la moneda

- Basado en criptografía de clave pública
- Moneda descentralizada (Bancos, gobiernos...)
- Las transacciones son irreversibles
  - No duplicados
  - Fe en las devoluciones
- Sin comisiones por defecto (en MTGox son ínfimas)
- No pueden bloquearla
- Transacciones públicas y por seudónimos

Bitcoin
Características de la moneda

- Deflación lenta y constante de la moneda.
  Crecimiento de bitcoins disminuye y aumenta su valor
- Nunca pasará de los 21 millones de Bitcoins
- Se permite un máximo de 8 decimales.
- BBDD distribuida de transacciones (P2P)

Bitcoin
Características de la moneda

- Se puede especular (traders)

- El protocolo es capaz de admitir en el futuro,
  la creación de direcciones basadas en nuevas primitivas criptográficas

Bitcoin
Conceptos básicos

- **Dirección**
  - Tan Fácil como llave pública y privada
  - 32 caracteres
  - Base 58, base 64 menos
    - 0 cero, O mayúscula
    - I (i mayúscula), l (L minúscula)
    - +(más)
    - / (slash)
  - Anónimas
  - Ilimitadas

185MZPVxc3asL88PYwJjybkuqUwQy4EMrc

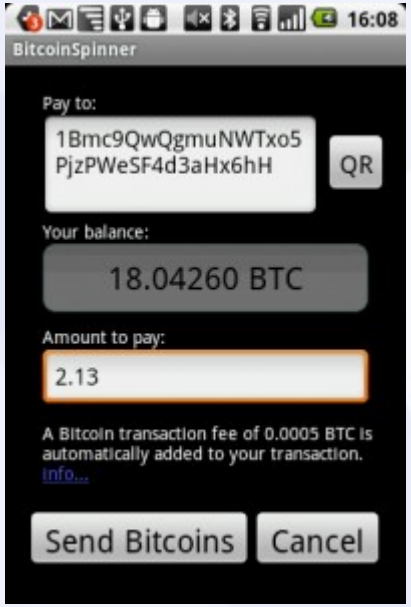
Bitcoin
Conceptos básicos

- **Billetera**
  - Contenedor de varias direcciones.
  - Locales o remotas (servicio)

Paytunia

Blockchain

Bitcoin Spinner



Bitcoin
Conceptos básicos

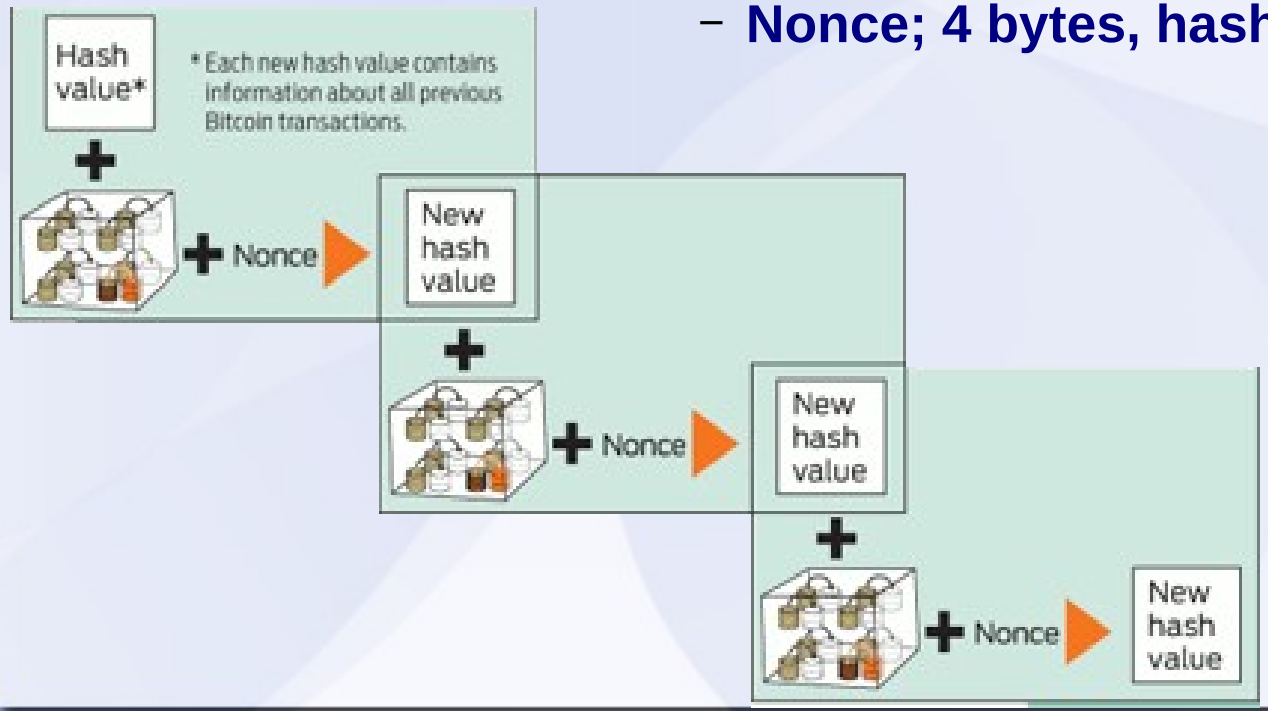
Bitcoin
Conceptos básicos

- **Transacción**
  - R → pub-key(R) → E
  - E; pub-key(R) + n Bitcoins
  - E; firma pri-key(E)
  - E → red bitcoin (P2P)
  - Los nodos validan la transacción (6)

https://blockexplorer.com/

Bitcoin
Conceptos básicos

- **Bloques**
  - **Se generan casa 10 minutos**
  - **7 confirmaciones == 7 bloques atrás**
  - **Dificultad; qué complejo es crear bloque**
  - **Nonce; 4 bytes, hash del bloque x ceros**



Bitcoin - Funcionamiento

How a ฿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

CREATING A NEW ADDRESS

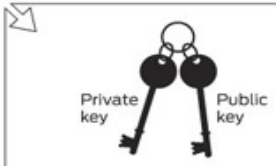
Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

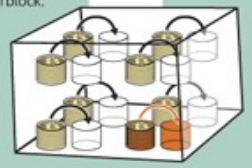
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

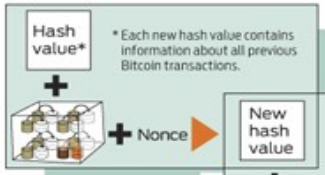
Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.



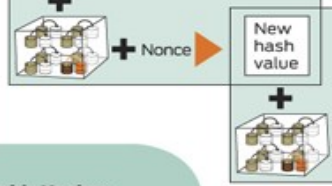
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.



* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.



Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

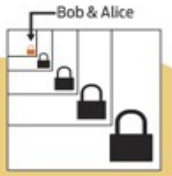
The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED



As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA HOWARD, BRANDON ROACH & KARL SOMMALLIER

Bitcoin
Valor actual

- ÚLTIMO: 10.53578
- MÁS ALTO: 10.83883
- MÁS BAJO: 9.8

Evolución de la minería

- 1º PC Estándar
- 2º Uso de varias GPUs

Evolución de la minería

- Minería en grupo (mining pools)

Evolución de la minería

- minería en grupo (mining pools)

  http://mining.bitcoin.cz/

  http://deepbit.net/

  btcmine.com

  Bitcoins.lc

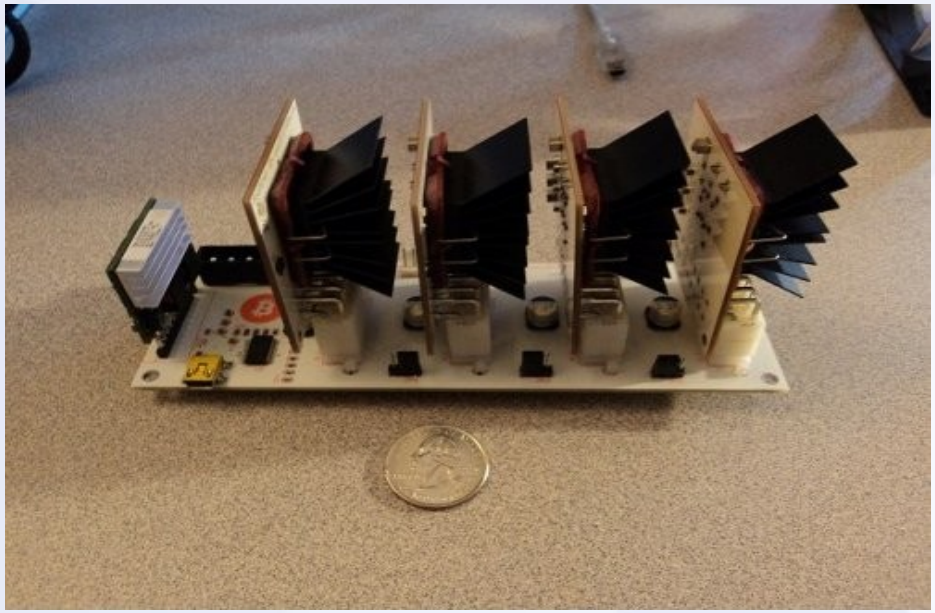
  btcguild.com

Evolución de la minería

- Supercomputadoras
  - Países con luz barata.

Evolución de la minería

- Supercomputadoras
  - Hardware especializado
  - FPGAs y ASICs



Bitcoin

- PELIGROS
  - Doble gasto (aceptar operaciones sin validar)
  - > 51% bajo único control, (falsificación)
- ATAQUES
  - Agosto de 2011 ataques de Trojan.Antiminer.A para crear una bootnet de Mimeria.
    Arranca de forma silenciosa un mimer Botcoin que utiliza la GPU de jugón para el proceso.

Conseguir Bitcoin

1ºwww.ukash.com
2ºhttps://www.cashu.com/
3ºwww.bitcoinnordic.com

- **Con comisión**
  - http://www.mtgox.com
  - https://localbitcoins.com/

Bitcoin
Monedas físicas

Bitcoin y el porno

- Streaptes
  - http://www.reddit.com/r/girlsgonebitcoin

¿Preguntas?

ReD

red@nosoloaulas.com

Sitios de interés

- Bitcoin Talk Forum (pruebas y niveles).

  https://bitcointalk.org/

- Consulta de saldo (key publica necesaria)
  - Blockexplorer.com
  - Blockchain.info
- FPGA para bitcoin
  - https://www.btcfpga.com/

Sitios de interés

- Tiendas estilo ebay
  - https://www.bitmit.net
  - http://conbitcoin.com/
  - http://www.biddingpond.com/

Sitios de interés

- Minería en grupo (mining pools)
  - páginas para ir sacando unos pocos céntimos
  - http://mining.bitcoin.cz/
  - http://deepbit.net/
  - btcmine.com
  - Bitcoins.lc
  - btcguild.com