# BITCOIN

Una nueva visión  tecnológica de la transmisión de valor entre pares

# José Antonio Bravo Mateu

- Economista asesor fiscal (Negotians)
- Miembro de avalBit

- Twitter: @jabravo
- Facebook: Jose Antonio Bravo Mateu
- LinkedIn: Jose Antonio Bravo Mateu
- Telegram: @jabravo

# Creación de Bitcoin

- Primeros trabajos de Satoshi Nakamoto: 2007
- Publicación del whitepaper de Bitcoin: octubre de 2008
- Publicación primer cliente de Bitcoin: enero de 2009

En esta última fecha se crea el bloque Génesis.

# Propósito principal de Bitcoin

Realizar transacciones entre dos o más partes sin que exista confianza entre ellos, y sin que se necesite un tercero que verifique que la transacción ha sido exitosa.

# Conceptos más importantes de Bitcoin

- Un libro público (cadena de bloques o blockchain) donde se registran todas las transacciones realizadas.
- Un algoritmo criptográfico (cifrado asimétrico) utilizado para autorizar transacciones
- Una red distribuida de nodos (mineros) que verifican y validan las transacciones, y actualizan la cadena de bloques.

# Blockchain

Libro contable distribuido

Cada página del libro es un *bloque*

Se crea un nuevo bloque aproximadamente cada 10 minutos

La creación de un bloque se recompensa (coinbase) creando nueva masa monetaria

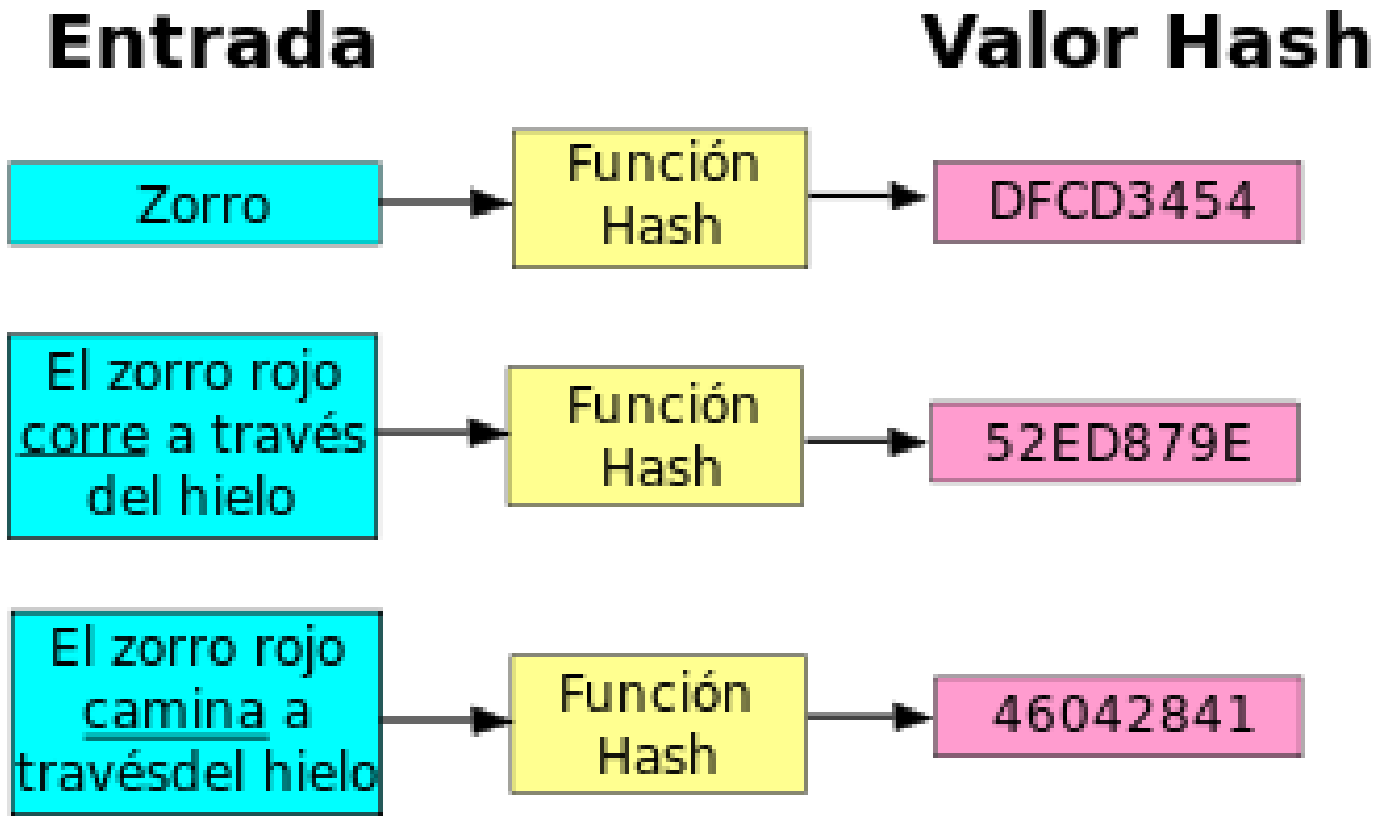
Cualquiera puede descargar la blockchain (pública) y tener un archivo de todas las transacciones desde el bloque

Una vez descargada toda la blockchain puede crearse un nodo que valide transacciones

# Encriptación asimétrica

- Bitcoin utiliza criptografía de clave pública.
  - Hash: Introduciendo una cadena con un número aleatorio de caracteres, la función ofrece un número fijo de caracteres en hexadecimal
  - Dos claves: pública y privada. Conociendo la privada se puede derivar la pública, pero no a la inversa.
- El propósito de la criptografía es verificar que el emisor es el dueño de los bitcoins y puede transmitirlos (permite “gastar” bitcoins)

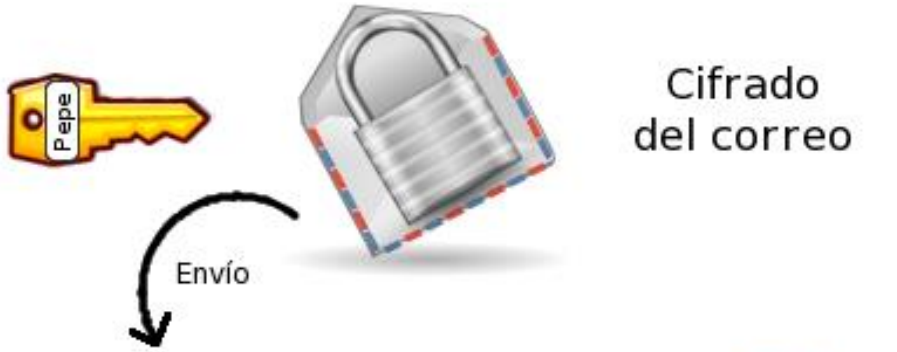
# Funciones Hash (digest/resumen)






Usando nuestra clave pública comprueba la firma

Disponemos de la
clave pública del destinatario

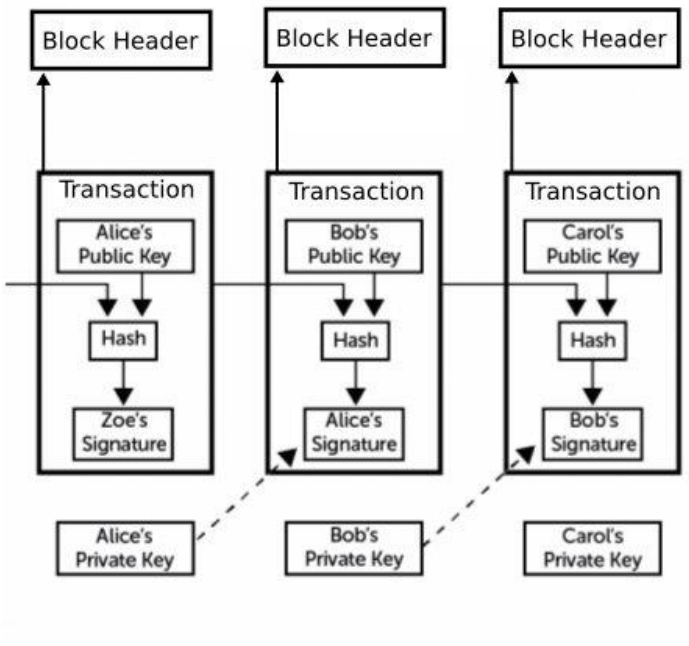


Usando su clave privada
el destinatario descifra el correo

# Red distribuida

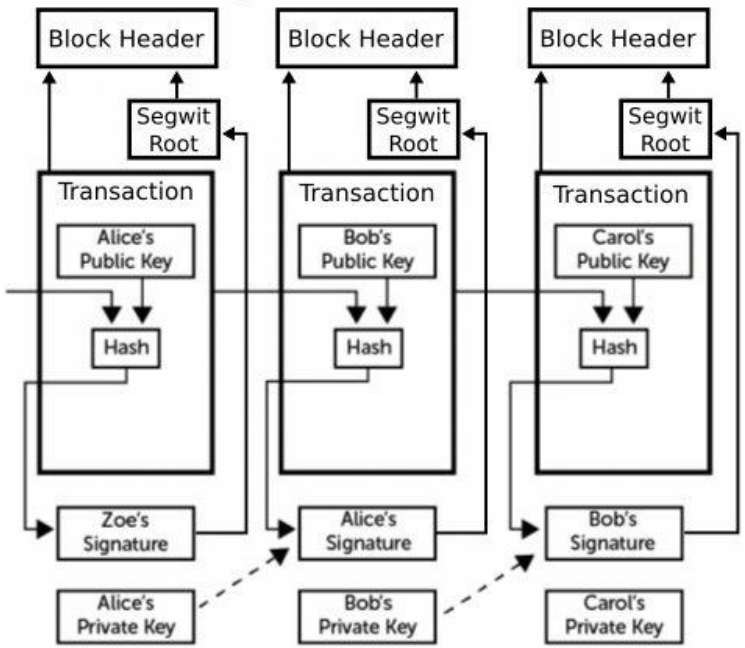
- Los nodos mineros verifican que las transacciones que se han comunicado son válidas y las añaden en nuevos bloques
- Todos los mineros compiten en el hallazgo de una solución a un problema complejo. (Proof of Work)
- El minero que halla en primer lugar la solución introduce un nuevo bloque con transacciones.
- A cambio de introducir este bloque, recibe una recompensa (coinbase) y las comisiones (fees) de las transacciones.
- El sistema está programado para que haya un bloque cada 10 minutos aproximadamente.


## Non-segwit blocks



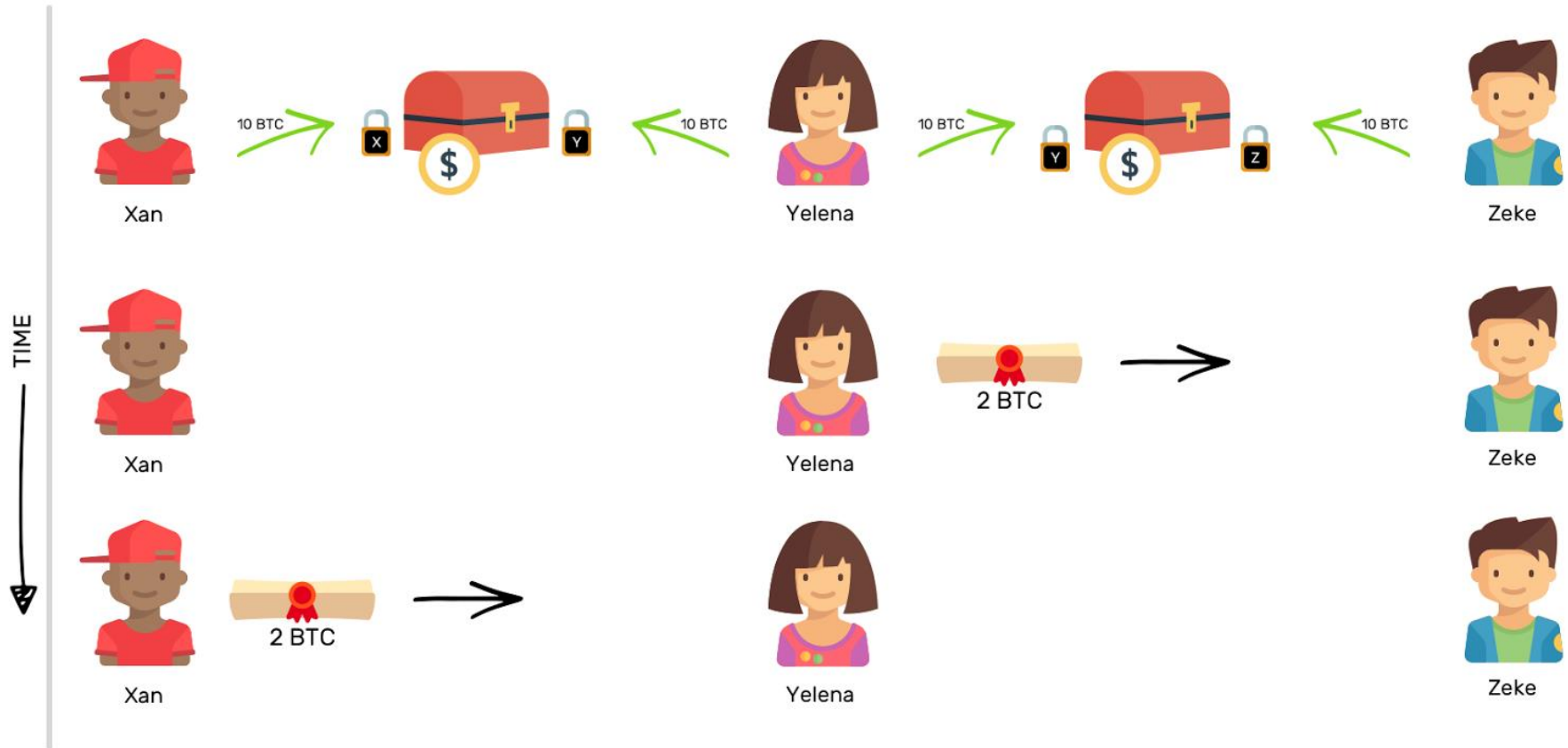

Each block header includes a cryptographically-secured reference to all of the transaction data in that block.

## Segwit blocks




Each block header still includes a cryptographically-secured reference to all of the transaction data in that block, but encumbrances (public keys) are referenced separately from witnesses (signatures) so that software can use each part independently.

# Bitcoin Lightning network



# Otros desarrollos a futuro en Bitcoin

- Confidential Transactions
- Bulletproof
- Dandelion
- Schnorr signatures
- Merklized Abstract Syntax Trees