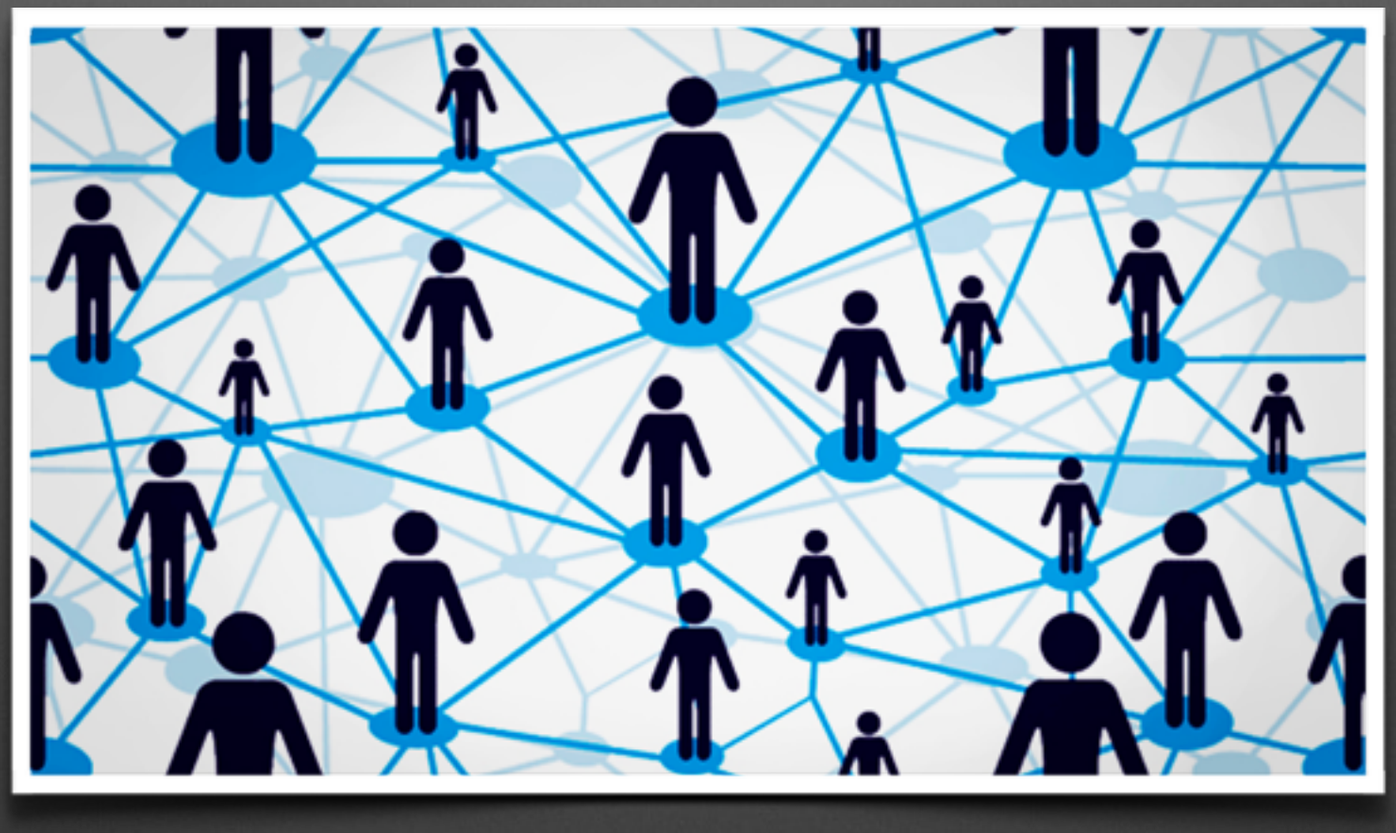
bitcoin

Seguidad en la era de Bitcoin

Luis Daniel Beltrán

moneda criptográfica

p2p



¿quien lo invento?

2008 - 2009

¿Como funciona?

dan@microbit.com

13ypnJ6niL3YfnUNsFskQz7BwwmLvuPEK9

password

5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBR6zCMU

Como funciona

Public Bitcoin Address

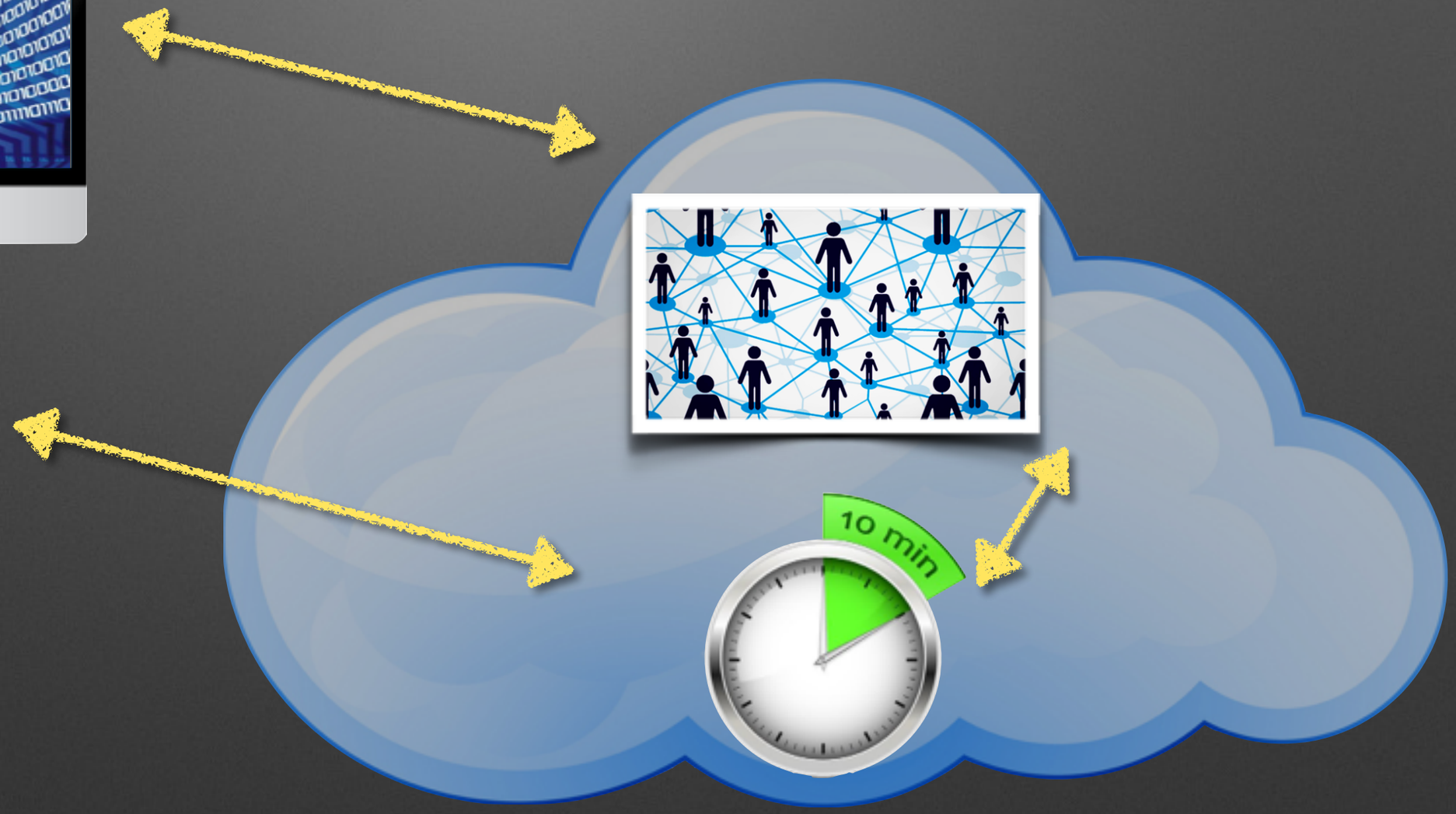
1F724qnBYt3RzNwtTqTN85gF8KyHTG9tUB

Private Key WIF

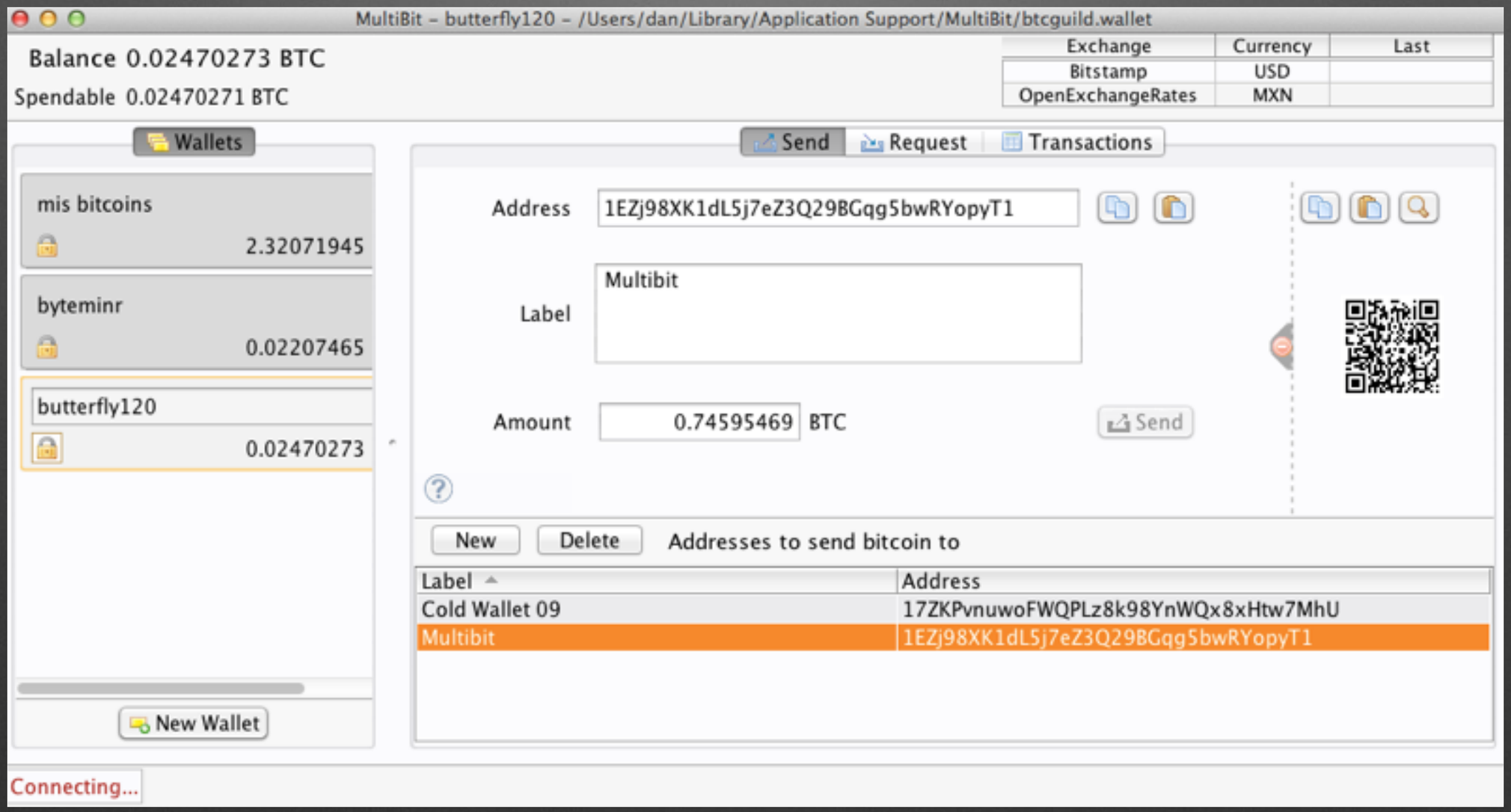
51 characters base58, starts with a '5'

5JGoHMxp4G5NBm5ExijEVqrgbvxrX8RT5x4q56GbJa2yxMjKQgv

¿Que sucede atras?



carteras digitales



carteras digitales

Cadena de Bloques

Es un invento tecnológico que substituye a una entidad central que da fe por un algoritmo lógico y matemático.

Esto en consecuencia crea una red descentralizada de consensos lo cual tiene una trascendencia inédita en la historia de la humanidad.

Tarjeta vs BTC

- 1950 vs 2009
- TCP/IP principios de los 80´s
- Se requiere un medio seguro en BTC no
- Pull en vez de Push

¿Por que es seguro?

- SHA 256
- El protocolo Bitcoin utiliza el algoritmo ECDSA firmas digitales asimétricas basadas en curva elíptica.
- 2^{256}
=115792089237316195423570985008687907853269984665640564039457584007913129639936

Puntos Fuertes del Protocolo

- No es susceptible a MiM
- Pagos Push en vez de Pull.
- No se crean monedas según criterio de Banco Central
- Libro contable abierto.

Puntos Débiles

- Red de minería centralizada.
- Su valor es sumamente volátil
- Precio manipulable.
- Altamente susceptible a Malware.
- Poca experiencia en manejo y falta de buenas prácticas.

PESO
DIGITAL

Prueba de Concepto
Una moneda criptográfica avalada por el banco central.

consensodigital.org

Cadena de Bloques para México

Gracias