



Seguridad en la era de Bitcoin

Luis Daniel Beltrán

# moneda criptográfica





# p2p



# ¿quien lo invento?

2008 - 2009





# ¿Como funciona?



dan@microbit.com

13ypnJ6niL3YfnUNsFskQz7BwwmLvPEK9



password



5HpHagT65TZzG1PH3CSu63k8Dbpv  
D8s5ip4nEB3kEsreBR6zCMU



# Como funciona

## Public Bitcoin Address



1F724qnBYt3RzNwtTqTN85gF8KyHTG9tUB

## Private Key WIF

51 characters base58, starts with a '5'

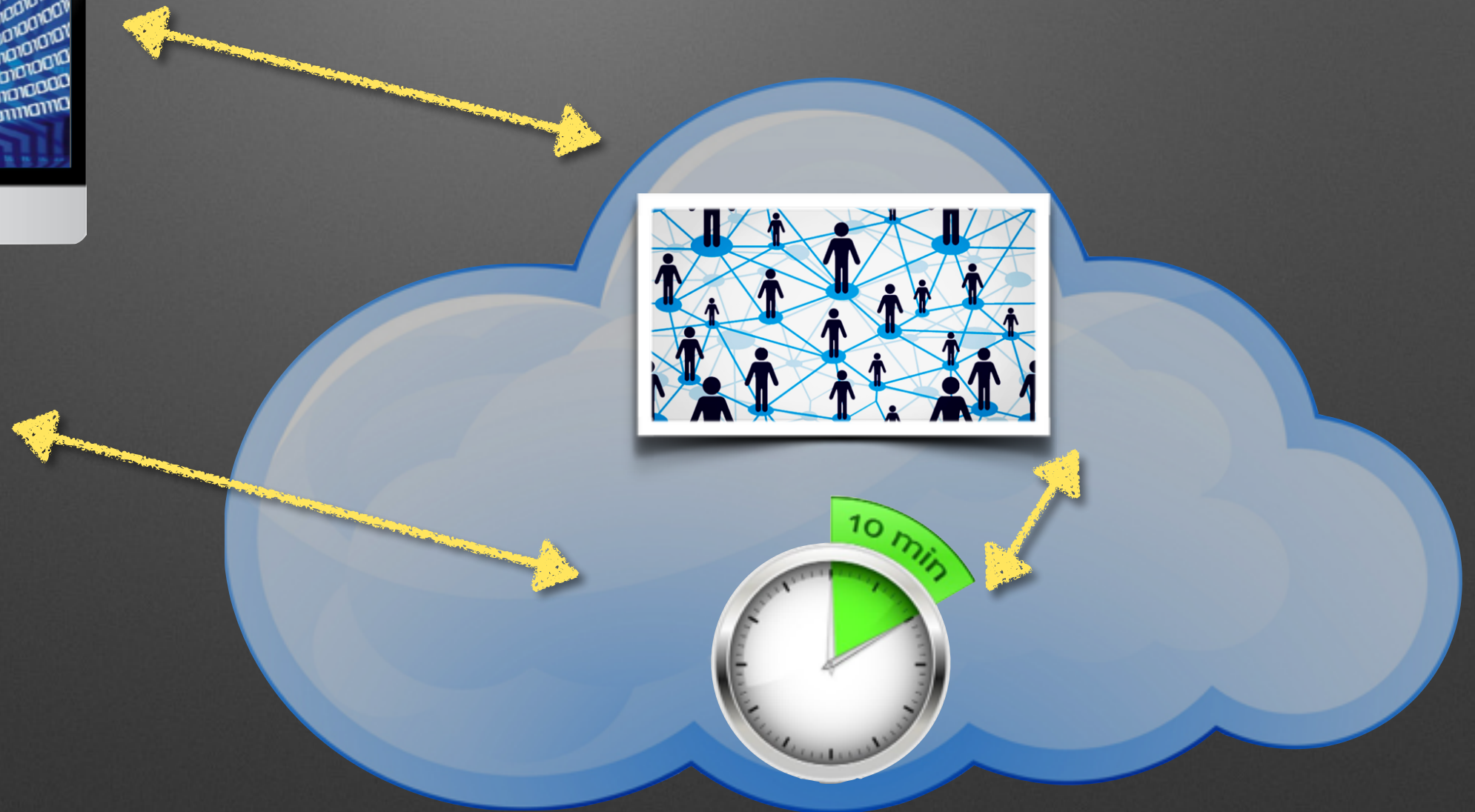


5JGoHMxp4G5NBm5ExijEVqrgbvxrX8RT5x4q56GbJa2yxMjKQgv





# ¿Que sucede atras?



# carteras digitales

MultiBit - butterfly120 - /Users/dan/Library/Application Support/MultiBit/btcguild.wallet

Balance 0.02470273 BTC  
Spendable 0.02470271 BTC

Exchange	Currency	Last
Bitstamp	USD	
OpenExchangeRates	MXN	

**Wallets**

- mis bitcoins 2.32071945
- byteminr 0.02207465
- butterfly120 0.02470273**

**Send** **Request** **Transactions**

Address: 1EZj98XK1dL5j7eZ3Q29BGqg5bwRYopyT1

Label: Multibit

Amount: 0.74595469 BTC

**Send**

**QR Code**

**Addresses to send bitcoin to**

Label	Address
Cold Wallet 09	17ZKPvnuwoFWQPLz8k98YnWQx8xHtw7MhU
<b>Multibit</b>	<b>1EZj98XK1dL5j7eZ3Q29BGqg5bwRYopyT1</b>

**New Wallet**

Connecting...





# carteras digitales



The screenshot shows a mobile application interface for sending Bitcoin. At the top, there is a status bar with various icons and the time 01:54. Below this is a header bar with a back arrow, a Rubik's cube icon, the text "Send Bitcoins", a question mark icon, and a "QR" label. The main content area has four sections: "Pay to" with a text input field containing the address "1A8JiWcwvpY7tAopUkSnGuEYHmzGYfZPiq"; "Available for spending" with a text input field showing "BTC 33.55603735"; "Amount to pay" with a text input field showing "BTC 0.00" and a pencil icon; and "Fee (optional)" with a text input field showing "BTC 0.0005" and a delete icon. At the bottom, there are two buttons: "Send" (highlighted with an orange border) and "Cancel".

01:54

<  Send Bitcoins ? QR

Pay to

1A8JiWcwvpY7tAopUkSnGuEYHmzGYfZPiq

Available for spending

BTC **33.55**603735

Amount to pay

BTC **0.00** 

Fee (optional)

BTC **0.0005** 

Send Cancel



# 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](https://consensodigital.org)

# **Cadena de Bloques para México**



# Gracias

