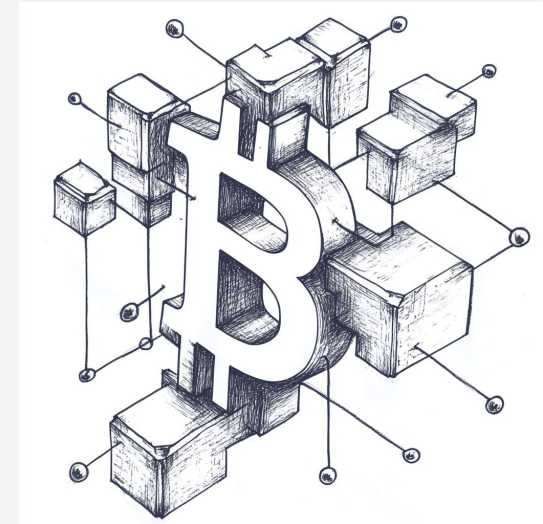


Bitcoin



Características principales



Origen

Características principales



Origen



Primer criptomoneda exitosa

Características principales



Origen



Primer criptomoneda exitosa



Emisión limitada

Características principales



Origen



Primer criptomoneda exitosa



Emisión limitada



Descentralizado

Características principales



Origen



Primer criptomoneda exitosa



Emisión limitada



Descentralizado



Pseudo anónimo

Características principales



Origen



Primer criptomoneda exitosa



Emisión limitada



Descentralizado



Pseudo anónimo



Transparente

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

2009, 3 de Enero

Primer implementación de Bitcoin liberada, se crea el genesis block

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

2009, 3 de Enero

Primer implementación de Bitcoin liberada, se crea el genesis block

2010, 22 de Mayo

Se haga el pago de un bien en Bitcoin 22.000 BTC por 2 pizzas

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

2009, 3 de Enero

Primer implementación de Bitcoin liberada, se crea el genesis block

2010, 22 de Mayo

Se haga el pago de un bien en Bitcoin 22.000 BTC por 2 pizzas

2010, Diciembre

Último mensaje público de Satoshi

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

2011, 9 de Febrero

Bitcoin alcanza la paridad 1:1 con el dólar

2009, 3 de Enero

Primer implementación de Bitcoin liberada, se crea el genesis block

2010, 22 de Mayo

Se haga el pago de un bien en Bitcoin 22.000 BTC por 2 pizzas

2010, Diciembre

Último mensaje público de Satoshi

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

2011, 9 de Febrero

Bitcoin alcanza la paridad 1:1 con el dólar

2009, 3 de Enero

Primer implementación de Bitcoin liberada, se crea el genesis block

2013, Octubre

Cierran Silk Road (se incautan 144.000 Bitcoins)

2010, 22 de Mayo

Se haga el pago de un bien en Bitcoin 22.000 BTC por 2 pizzas

2010, Diciembre

Último mensaje público de Satoshi

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

2011, 9 de Febrero

Bitcoin alcanza la paridad 1:1 con el dólar

2009, 3 de Enero

Primer implementación de Bitcoin liberada, se crea el genesis block

2013, Octubre

Cierran Silk Road (se incautan 144.000 Bitcoins)

2010, 22 de Mayo

Se haga el pago de un bien en Bitcoin 22.000 BTC por 2 pizzas

2014, Febrero

Cierra Mt. Gox (se pierden 850.000 Bitcoins)

2010, Diciembre

Último mensaje público de Satoshi

Algunos hitos

2008, 31 de octubre

Satoshi Nakamoto liberá el paper de Bitcoin

2011, 9 de Febrero

Bitcoin alcanza la paridad 1:1 con el dólar

2009, 3 de Enero

Primer implementación de Bitcoin liberada, se crea el genesis block

2013, Octubre

Cierran Silk Road (se incautan 144.000 Bitcoins)

2010, 22 de Mayo

Se haga el pago de un bien en Bitcoin 22.000 BTC por 2 pizzas

2014, Febrero

Cierra Mt. Gox (se pierden 850.000 Bitcoins)

2010, Diciembre

Último mensaje público de Satoshi

2017, Marzo

Bitcoin supera el precio del oro

Cómo se genera una address en Bitcoin?

https://colab.research.google.com/drive/1sYGMsYyz1CBII-HvbsgXTIvwiEJ_ZJUM?usp=sharing



Cómo se genera una address en Bitcoin?



Cómo se genera una address en Bitcoin?



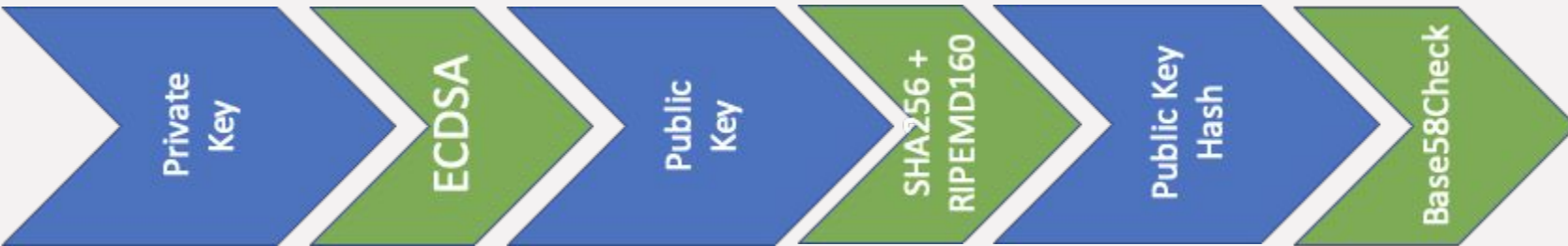
Cómo se genera una address en Bitcoin?



Cómo se genera una address en Bitcoin?



Cómo se genera una address en Bitcoin?



Cómo se genera una address en Bitcoin?



Bitcoin Block Header

FIELD	DESCRIPTION
VERSION	Block version number
HASH PREV BLOCK	256-bit hash of the previous block header
HASH MERKLE ROOT	256-bit hash based on <u>all of</u> the transactions in the block
TIME	Current block timestamp as seconds since 1970-01-01T00:00:00 UTC
BITS	Current target
NONCE	32-bit number

Participantes



Full Node

Participantes



Full Node



Miner

Proceso de minado



Creates new blocks

Proceso de minado



Creates new blocks



Search of incentives

Proceso de minado



Creates new blocks

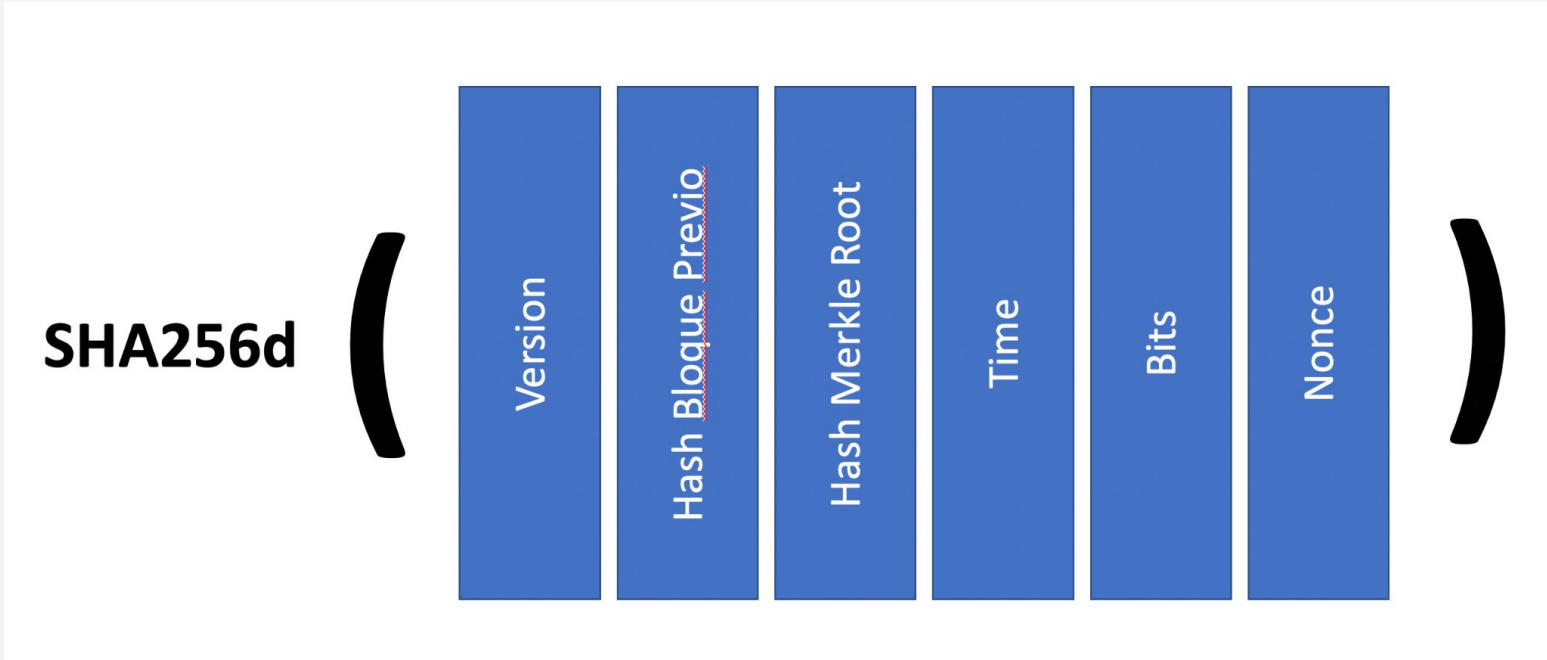


Search of incentives



Mathematical puzzle

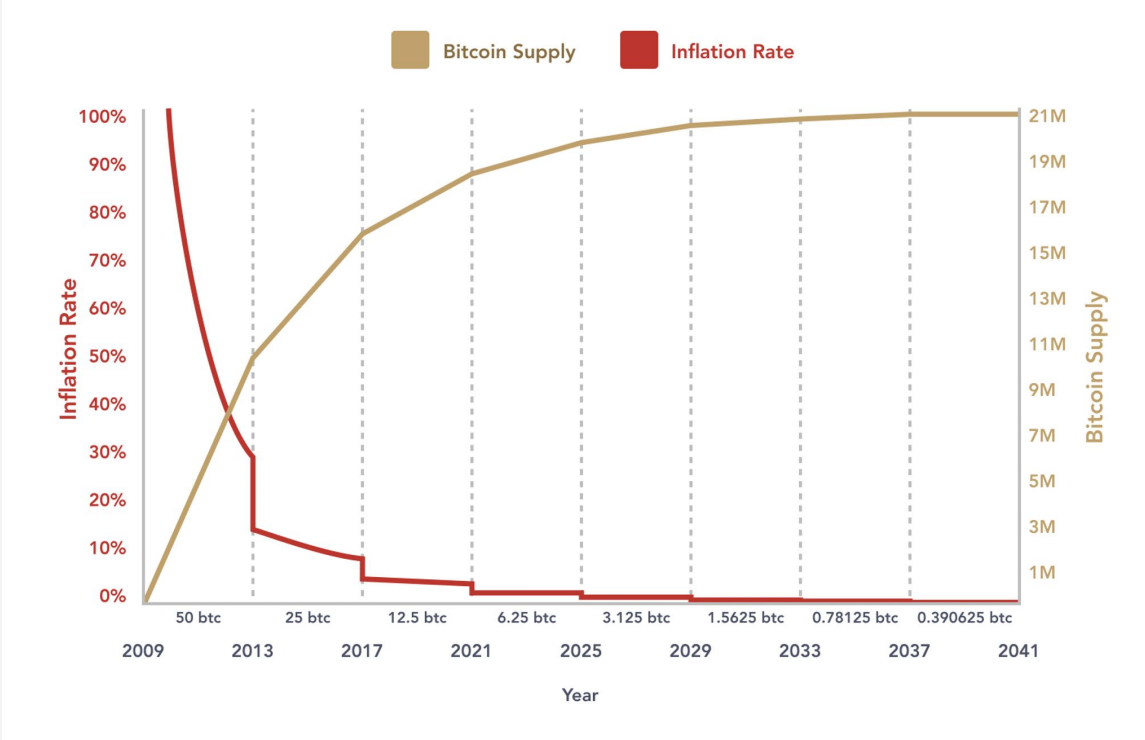
Proceso de minado



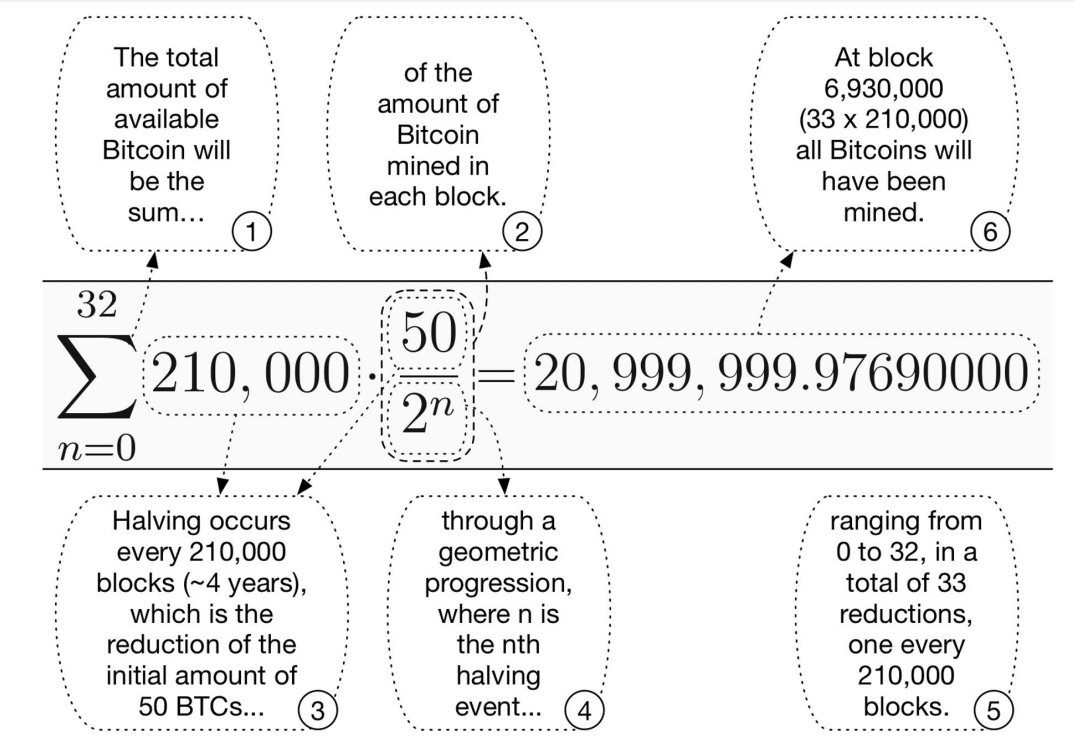
Proceso de minado



Proceso de minado - Halving



Proceso de minado - Halving



Proceso de minado - Dificultad

Se evalúa cada 2016 bloques

Se desea que esos bloques se hayan minado en 2 semanas (1 bloque cada 10 minutos)

Proceso de minado - Dificultad

Se evalúa cada 2016 bloques

Se desea que esos bloques se hayan minado en 2 semanas (1 bloque cada 10 minutos)

La dificultad mínima es 1

Es la dificultad del genesis block

Proceso de minado - Dificultad

Se evalua cada 2016 bloques

Se desea que esos bloques se hayan minado en 2 semanas (1 bloque cada 10 minutos)

La dificultad mínima es 1

Es la dificultad del genesis block

Que significa?

Que tan dificil es minar el bloque con respecto a lo que llevo minar el genesis block

Proceso de minado - Dificultad

Se evalua cada 2016 bloques

Se desea que esos bloques se hayan minado en 2 semanas (1 bloque cada 10 minutos)

La dificultad mínima es 1

Es la dificultad del genesis block

Que significa?

Que tan dificil es minar el bloque con respecto a lo que llevo minar el genesis block

Hashrate actual

~846 EH/s (846.000.000.000.000.000.000)

Proceso de minado - Hardware



CPU

Proceso de minado - Hardware



CPU



GPU

Proceso de minado - Hardware



CPU



GPU



ASIC

(Application-Specific Integrated Circuit)

UTXO (Unspent Transaction Output)

Bitcoin es UTXO base

Bitcoin se basa en un conjunto de UTXO

UTXO (Unspent Transaction Output)

Bitcoin es UTXO base

Bitcoin se basa en un conjunto de UTXO

Parte fundamental de las transacciones

Cada transacción se compone de un header, un conjunto de UTXOs de entrada y un conjunto de UTXOs de salida.

<https://www.blockchain.com/explorer/transactions/btc/6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4>

UTXO (Unspent Transaction Output)

Bitcoin es UTXO base

Bitcoin se basa en un conjunto de UTXO

Parte fundamental de las transacciones

Cada transacción se compone de un header, un conjunto de UTXOs de entrada y un conjunto de UTXOs de salida.

<https://www.blockchain.com/explorer/transactions/btc/6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4>

No se pueden reutilizar

Cuando una UTXO es utilizada como entrada en una transacción deja de estar disponible para su uso en otra tx.

UTXO (Unspent Transaction Output)

Bitcoin es UTXO base

Bitcoin se basa en un conjunto de UTXO

Parte fundamental de las transacciones

Cada transacción se compone de un header, un conjunto de UTXOs de entrada y un conjunto de UTXOs de salida.

<https://www.blockchain.com/explorer/transactions/btc/6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4>

No se pueden reutilizar

Cuando una UTXO es utilizada como entrada en una transacción deja de estar disponible para su uso en otra tx.

Lock script

Cada UTXO tiene asociado un código script que debe ser resuelto para poder gastar esa UTXO

UTXO (Unspent Transaction Output)

Bitcoin es UTXO base

Bitcoin se basa en un conjunto de UTXO

Parte fundamental de las transacciones

Cada transacción se compone de un header, un conjunto de UTXOs de entrada y un conjunto de UTXOs de salida.

<https://www.blockchain.com/explorer/transactions/btc/6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4>

No se pueden reutilizar

Cuando una UTXO es utilizada como entrada en una transacción deja de estar disponible para su uso en otra tx.

Lock script

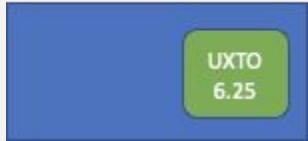
Cada UTXO tiene asociado un código script que debe ser resuelto para poder gastar esa UTXO

Coinbase transactions

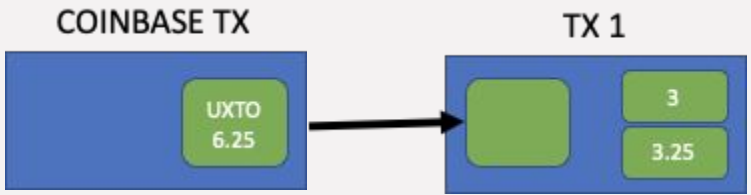
Son las únicas que tienen permitido no tener UTXOs de entrada

UTXO

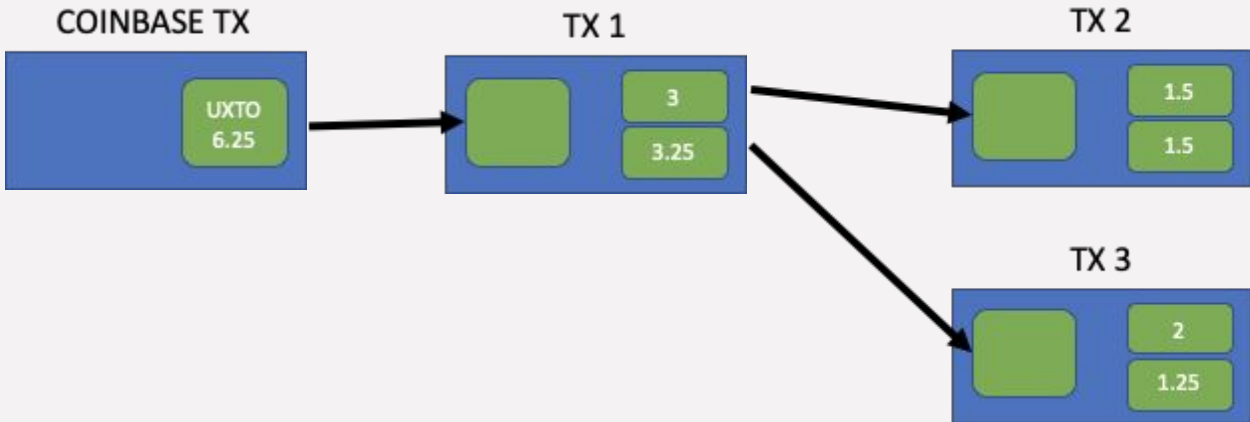
COINBASE TX



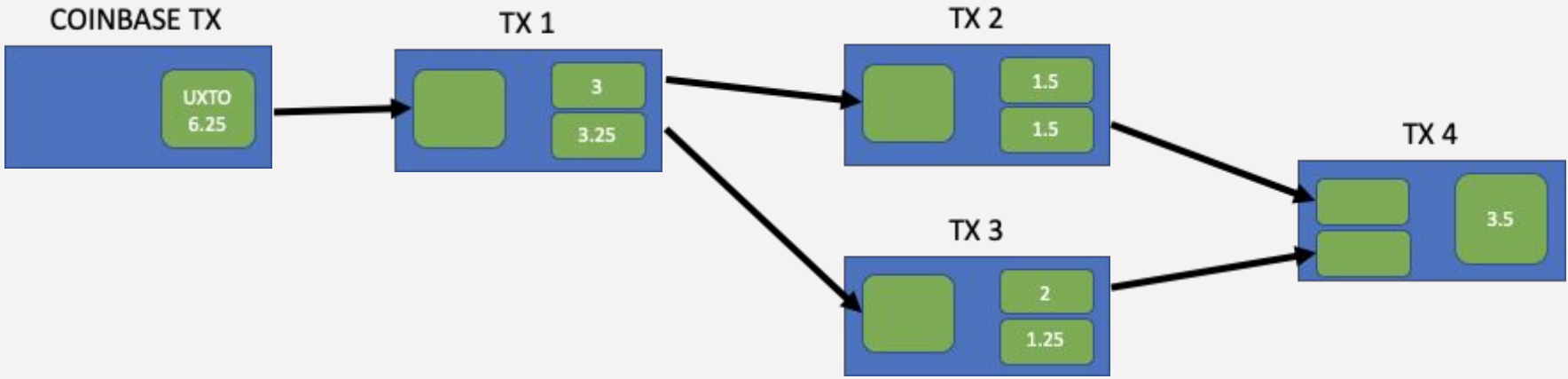
UTXO



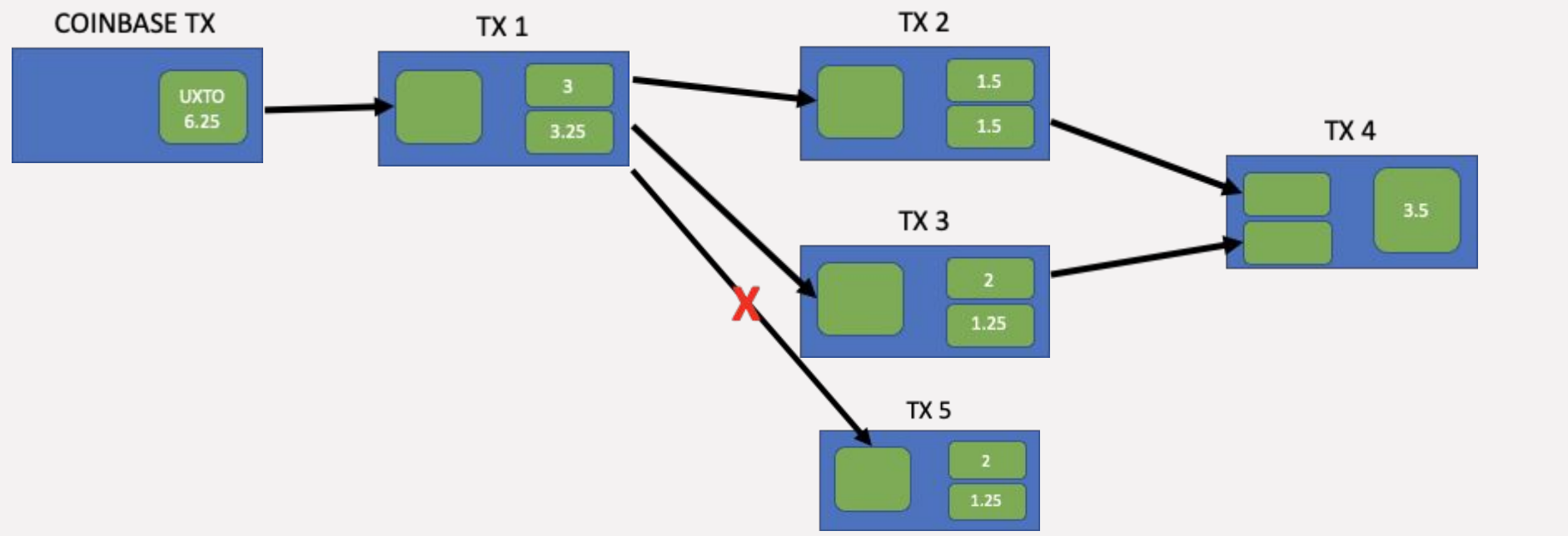
UTXO



UTXO



UTXO



Lenguaje Script

Forth-like

Lenguaje Script

Forth-like

Stack based

Se basa en utilizar una pila de comandos

Lenguaje Script

Forth-like

Stack based

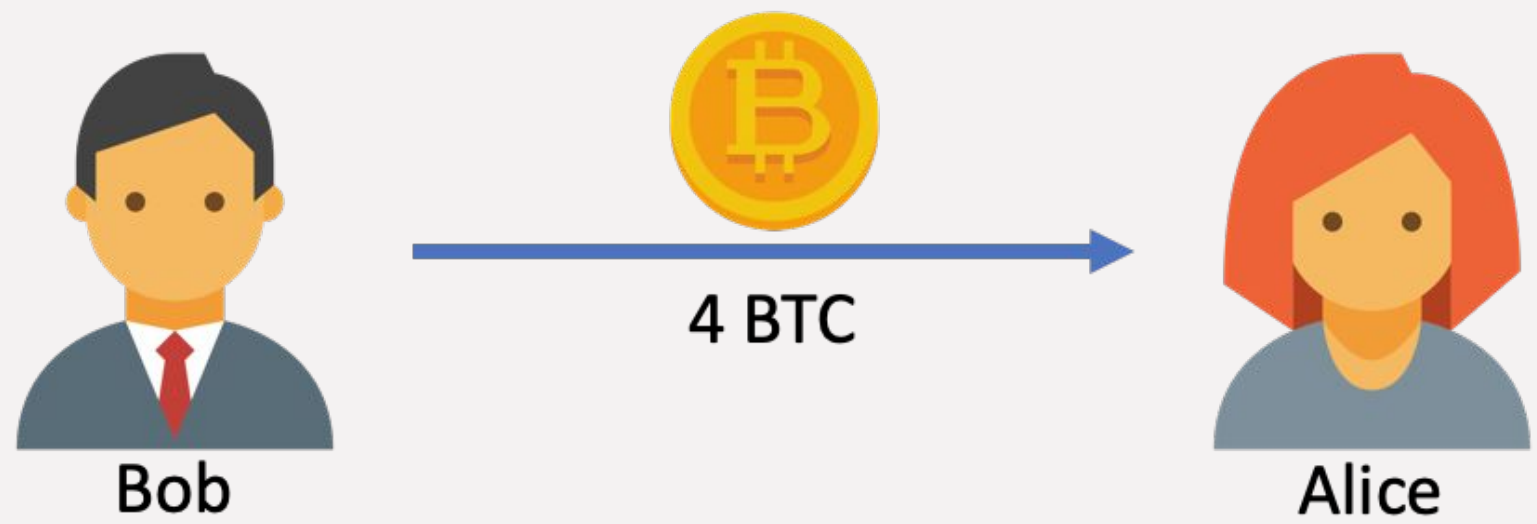
Se basa en utilizar una pila de comandos

NO es Turing complete

Esta limitación es buscada y no accidental

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

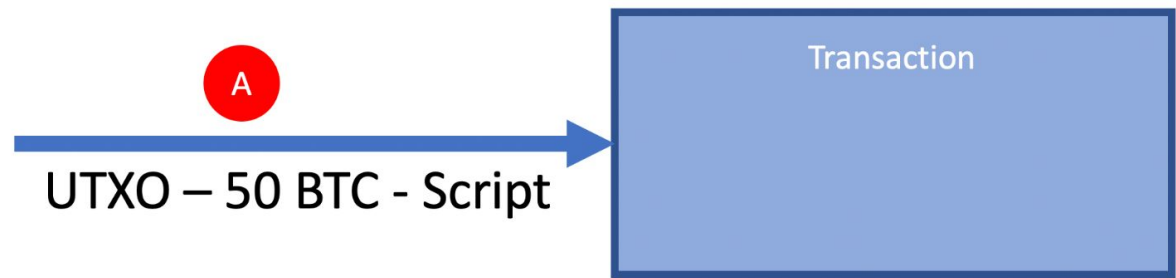
CREATE A NEW TRANSACTION



Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

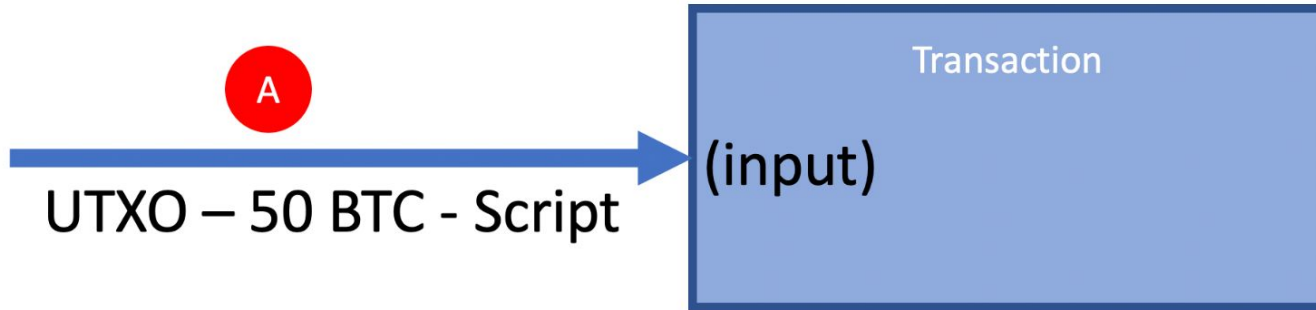
SELECT 1 OR MORE UTXO WITH EQUALS OR MORE BTC



Lenguaje Script - Enviar Bitcoin

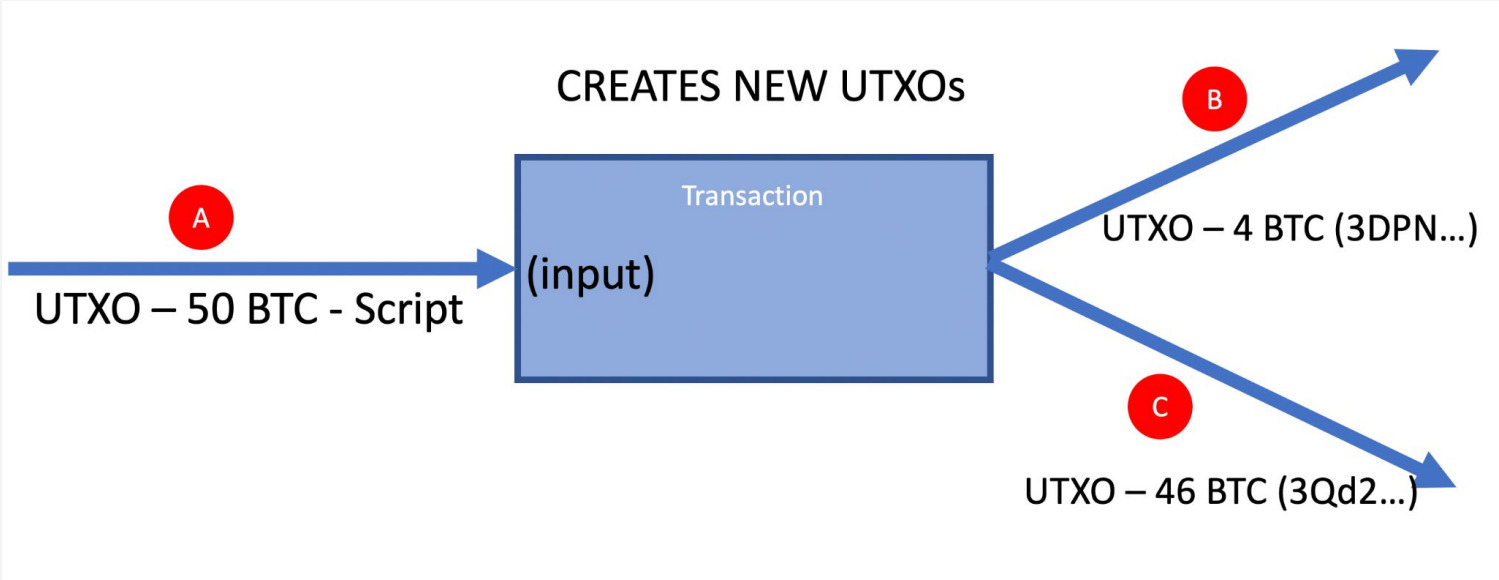
Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

PROVIDE THE NECESSARY INPUT TO SPEND EACH UTXO



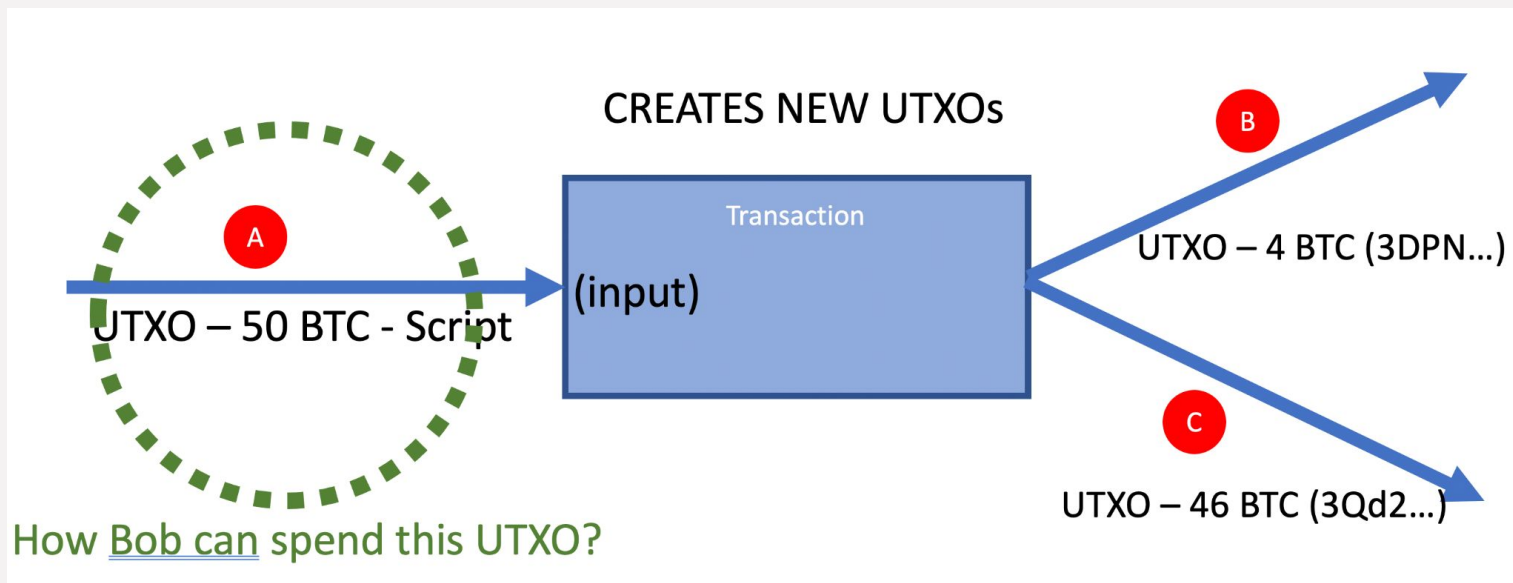
Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEAQ3QtHb8wM15VCQU3



Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

Imaginemos UTXO A tiene el siguiente código script::

```
OP_DUP OP_HASH160 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE  
OP_EQUALVERIFY OP_CHECKSIG
```

Bob debe proveer un input que haga que dicho código evalúe a
TRUE:

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

Imaginemos UTXO A tiene el siguiente código script::

```
OP_DUP OP_HASH160 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE  
OP_EQUALVERIFY OP_CHECKSIG
```

Bob debe proveer un input que haga que dicho código evalúe a TRUE:

```
<BOB SIGNATURE> <BOB PUBLIC KEY>
```

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

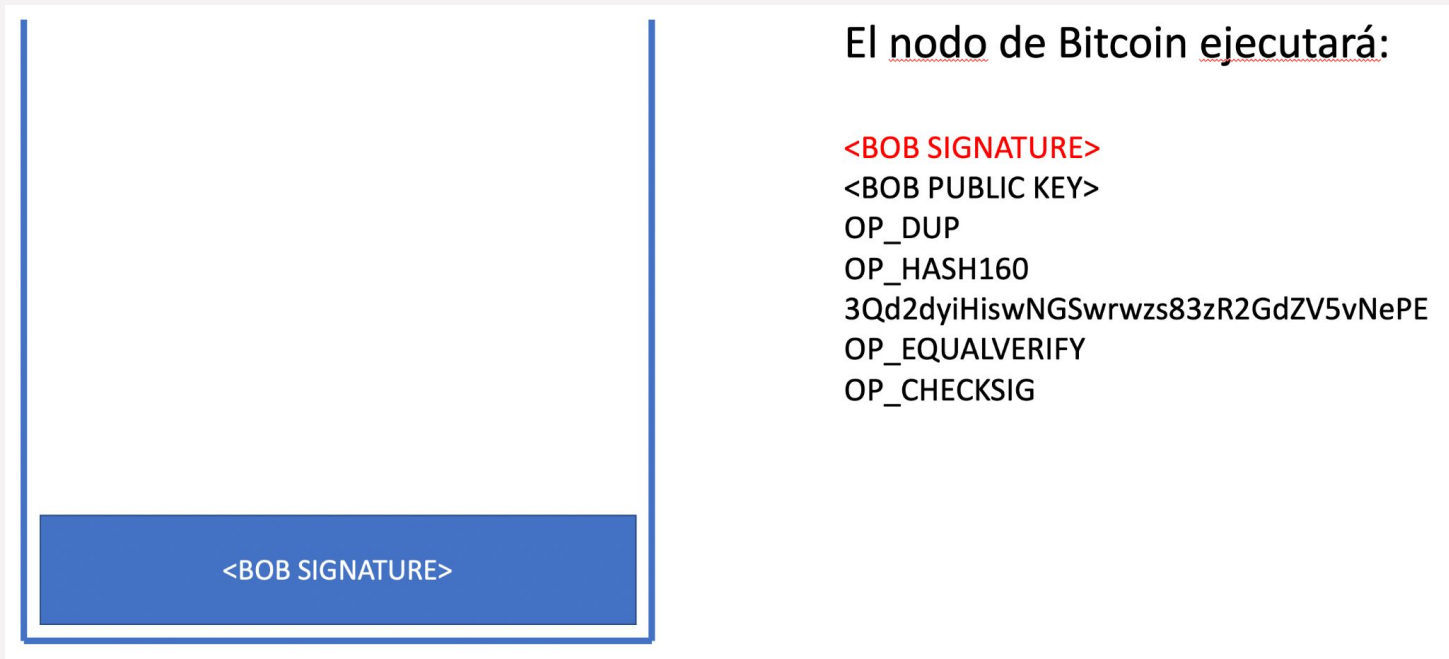


El nodo de Bitcoin ejecutará:

```
<BOB SIGNATURE>  
<BOB PUBLIC KEY>  
OP_DUP  
OP_HASH160  
3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE  
OP_EQUALVERIFY  
OP_CHECKSIG
```

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



El nodo de Bitcoin ejecutará:

<BOB SIGNATURE>

<BOB PUBLIC KEY>

OP_DUP

OP_HASH160

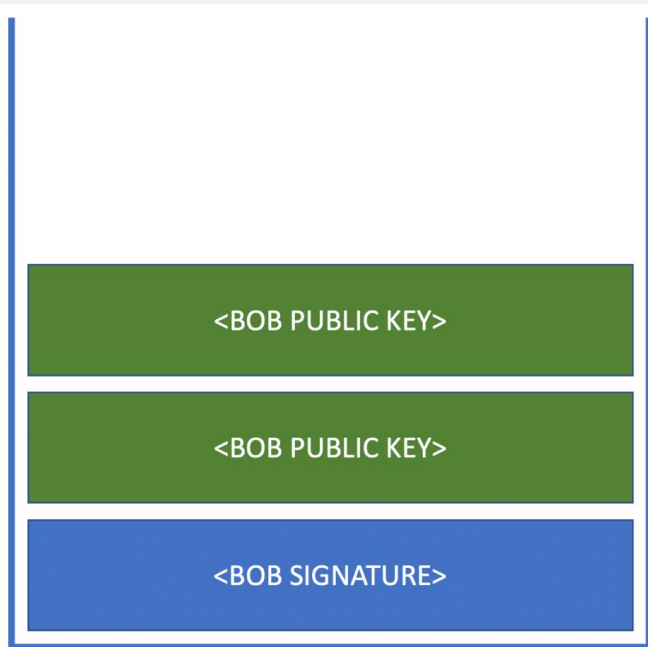
3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE

OP_EQUALVERIFY

OP_CHECKSIG

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



El nodo de Bitcoin ejecutará:

~~<BOB SIGNATURE>~~

~~<BOB PUBLIC KEY>~~

OP_DUP

OP_HASH160

3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE

OP_EQUALVERIFY

OP_CHECKSIG

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE

<BOB PUBLIC KEY>

<BOB SIGNATURE>

El nodo de Bitcoin ejecutará:

<BOB SIGNATURE>
<BOB PUBLIC KEY>
OP_DUP
OP_HASH160
3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE
OP_EQUALVERIFY
OP_CHECKSIG

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3

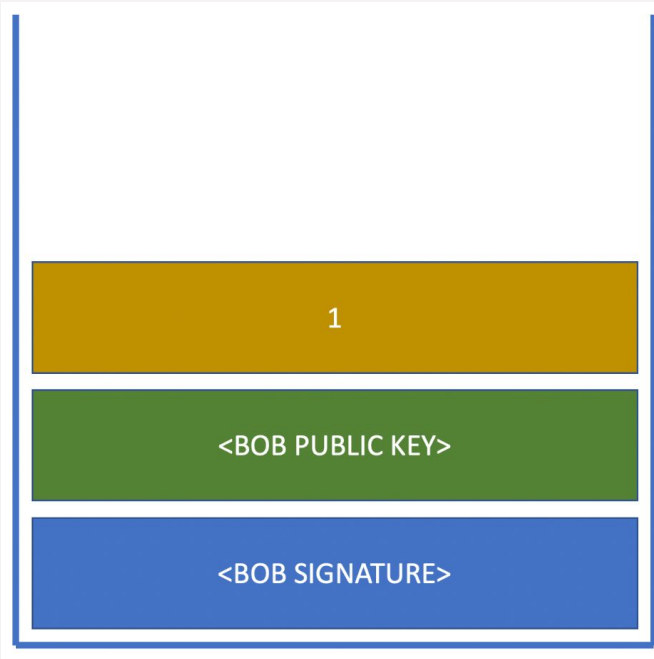


El nodo de Bitcoin ejecutará:

```
<BOB SIGNATURE>  
<BOB PUBLIC KEY>  
OP_DUP  
OP_HASH160  
3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE  
OP_EQUALVERIFY  
OP_CHECKSIG
```

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



El nodo de Bitcoin ejecutará:

~~<BOB SIGNATURE>~~
~~<BOB PUBLIC KEY>~~
~~OP_DUP~~
~~OP_HASH160~~
~~3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE~~
OP_EQUALVERIFY (EQUAL)
~~OP_CHECKSIG~~

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



El nodo de Bitcoin ejecutará:

~~<BOB SIGNATURE>~~

~~<BOB PUBLIC KEY>~~

~~OP_DUP~~

~~OP_HASH160~~

~~3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE~~

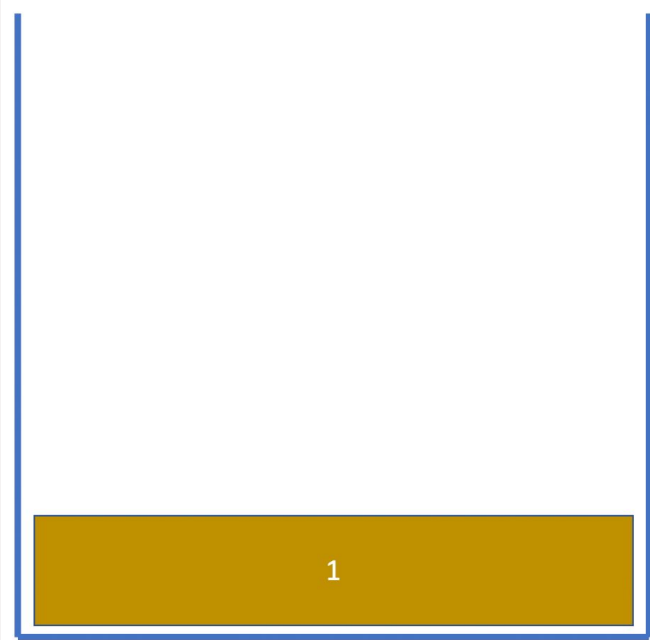
OP_EQUALVERIFY (VERIFY)

OP_CHECKSIG

En este punto sabemos que la clave pública es la que puede generar el address.
Todavía debemos verificar si quien genero la firma conoce la privada.

Lenguaje Script - Enviar Bitcoin

Enviar 4 BTC de 3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE a 3DPNFXGoe8QGiEXEApQ3QtHb8wM15VCQU3



El nodo de Bitcoin ejecutará:

```
<BOB-SIGNATURE>  
<BOB-PUBLIC KEY>  
OP_DUP  
OP_HASH160  
3Qd2dyiHiswNGSwrwzs83zR2GdZV5vNePE  
OP_EQUALVERIFY  
OP_CHECKSIG
```