

Transacciones y contratos inteligentes



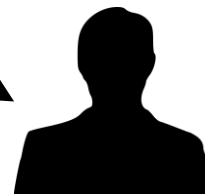
Transacción

transID: 74		type: PayCoins	
coins consumed			
num	consumed coinID		
0	coinID 73(1)		
1	coinID 73(2)		
coins created			
num	value	recipient	
0	3.2	0xf4...	
1	1.7	0xa1...	
2	4.6	0x55...	
Signature by LS_{Alice}			
Signature by LS_{Bob}			

Owned by Alice



Owned by Bob





Una transacción de verdad

<https://www.blockchain.com/es/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2>



Una transacción de verdad

Transacción Ver información de una transacción de Bitcoin

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Salida)



1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (No gastado)

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (No gastado) 0.015 BTC
0.0845 BTC

0.0995 BTC

Resumen

tamaño 258 (bytes)

Peso 1032

Hora de Recepción 2013-12-27 23:03:05

Incluidas en el Bloque [277316](#) (2013-12-27 23:11:54 + 9 minutos)

Confirmaciones 297007

Visualizar [Ver Gráfico de Árbol](#)

Entradas y Salidas

Entrada total 0.1 BTC

Salida Total 0.0995 BTC

Comisiones 0.0005 BTC

Tarifa por byte 193.798 sat/B

Tarifa por unidad de peso 48.45 sat/WU

Estimado de BTCs transaccionados 0.015 BTC

Scripts [Ocultar scripts y Coinbase](#)



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d
05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca
8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

Metadata



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d
05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca
8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

Outputs



Una transacción de verdad

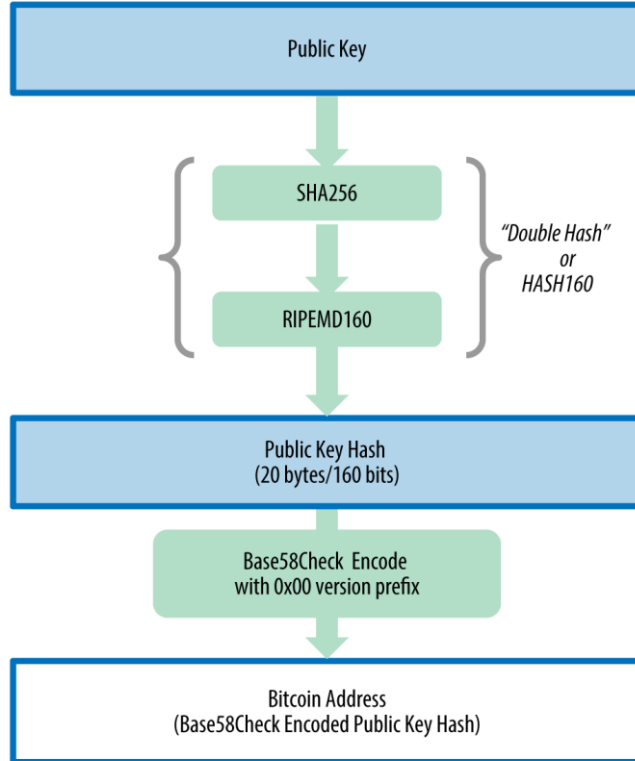
```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d
05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca
8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una dirección de Bitcoin

No es una llave publica

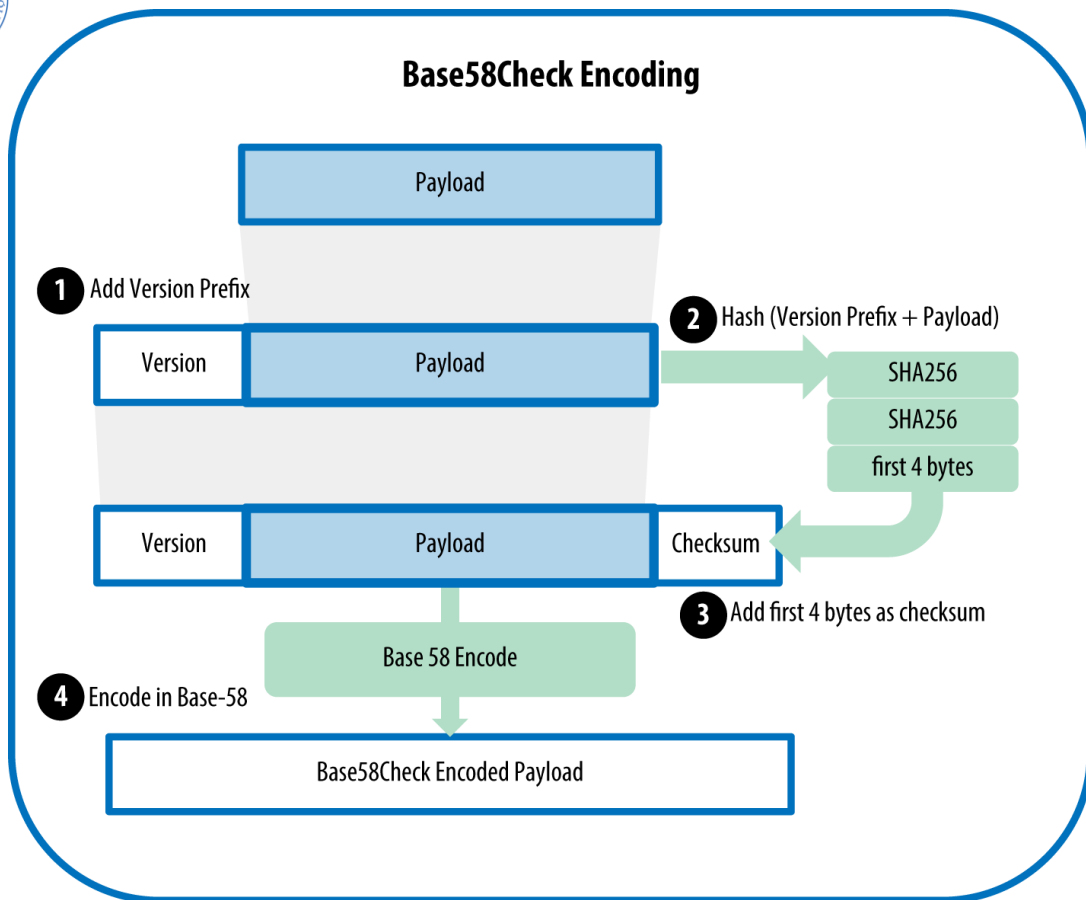
Public Key to Bitcoin Address





Una dirección de Bitcoin

No es una llave publica





Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una transacción de verdad

Transacción Ver información de una transacción de Bitcoin

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Salida)



1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (No gastado)

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (No gastado) 0.015 BTC
0.0845 BTC

0.0995 BTC

Resumen

tamaño 258 (bytes)

Peso 1032

Hora de Recepción 2013-12-27 23:03:05

Incluidas en el Bloque [277316](#) (2013-12-27 23:11:54 + 9 minutos)

Confirmaciones 297007

Visualizar [Ver Gráfico de Árbol](#)

Entradas y Salidas

Entrada total 0.1 BTC

Salida Total 0.0995 BTC

Comisiones 0.0005 BTC

Tarifa por byte 193.798 sat/B

Tarifa por unidad de peso 48.45 sat/WU

Estimado de BTCs transaccionados 0.015 BTC

Scripts

[Ocultar scripts y Coinbase](#)



Una transacción de verdad

Transacción Ver información de una transacción de Bitcoin

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC -
Salida)



1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (No gastado)

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (No
gastado) 0.015 BTC
0.0845 BTC

Scripts de Entrada

ScriptSig: PUSHDATA(72)

[3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301]
PUSHDATA(65)[0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf]

Scripts de Salida

DUP HASH160 PUSHDATA(20)[ab68025513c3dbd2f7b92a94e0581f5d50f654e7] EQUALVERIFY CHECKSIG

DUP HASH160 PUSHDATA(20)[7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8] EQUALVERIFY CHECKSIG

Confirmaciones 297007

Visualizar

[Ver Gráfico de Árbol](#)

Estimado de BTCs
transaccionados

0.015 BTC

Scripts

[Ocultar scripts y
Coinbase](#)



Una transacción de verdad

Lo único que existe en Bitcoin son UTXOs:

- Una transacción gasta UTXOs en inputs y produce outputs



Transacción

coins consumed		
num	consumed coinID	
0	coinID 73(1)	
1	coinID 73(2)	
coins created		
num	value	recipient
0	3.2	0xf4...
1	1.7	0xa1...
2	4.6	0x55...



Una transacción de verdad

Output de una transacción específica:

- Valor de Bitcoins que se pagan
- Llave publica del destinatario



Una transacción de verdad

Output de una transacción específica:

- Valor de Bitcoins que se pagan
- ~~Llave pública del destinatario~~



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d
05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca
8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una transacción de verdad

Output de una transacción específica:

- Valor de Bitcoins que se pagan
- ~~Llave pública del destinatario~~ dirección del destinatario



Una transacción de verdad

Output de una transacción específica:

- Valor de Bitcoins que se pagan
- ~~Llave publica del destinatario dirección del destinatario~~



Una transacción de verdad

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```




Una transacción de verdad

Output de una transacción específica:

- Valor de Bitcoins que se pagan
- ~~Llave pública del destinatario dirección del destinatario~~
- SCRIPT



Una transacción de verdad

Transacción básica:

- Paga al X 1 BTC

En realidad:

- Esto crea un output que dice
- "Este output se puede gastar con una firma de X"

X es una dirección ~ un hash

X no nos dice en realidad la llave publica (para poder verificar la firma)



Una transacción de verdad

Transacción básica:

- Paga al X 1 BTC

En realidad:

- Esto crea un output que dice
- ~~"Este output se puede gastar con una firma de X"~~
- "Este output se puede gastar presentando la llave publica que hashea al X, junto con la firma que corresponde a esta llave publica"



Una transacción de verdad

Transacción básica:

- Paga al X 1 BTC

En realidad realidad una transacción está definida con:

- La cantidad de BTC que gasta
- Un **locking script**

Locking script especifica las condiciones para gastar el output



Una transacción de verdad

Transacción básica:

- Paga al X 1 BTC

Input de esta transacción es:

- Un UTXO (hash de la transacción + numero de output)
- Un **unlocking script**

Qué script hay que correr?

- **Unlocking script (Input) + Locking script (UTXO referenciado en el input)**



Una transacción de verdad

Transacción básica:

- Paga al X 1 BTC

Input de esta transacción es:

- Un UTXO (**hash de la transacción + numero de output**)
- Un **unlocking script**

Qué script hay que correr?

- **Unlocking script (Input) + Locking script (UTXO referenciado en el input)**



Una transacción de verdad

Transacción básica:

- Paga al X 1 BTC

Input de esta transacción es:

- Un UTXO (hash de la transacción + numero de output)
- Un **unlocking script**

Quien corre el script?

- **Todos los nodos de la red!!!**



Un script

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value		Locking script
0	3.1		OP_DUP OP_HASH...
1	2.2		OP_DUP OP_HASH...



Un script

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value		Locking script
0	3.1		OP_DUP OP_HASH...
1	2.2		OP_DUP OP_HASH...



Un script

tx: 0xff...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_DUP OP_HASH...	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	



Un script

tx: 0xff...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_DUP OP_HASH...	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	





Un script

tx: 0xff...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_DUP OP_HASH...	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	





Un script

tx: 0xff...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_DUP OP_HASH...	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	





Un script

tx: 0xff...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_DUP OP_HASH...	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	

012123...



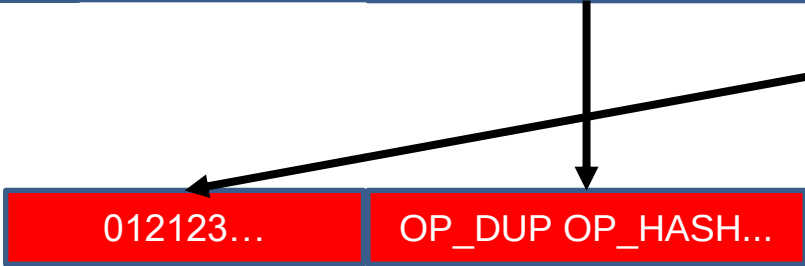
Un script

tx: 0xff...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_DUP OP_HASH...	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	





Un script

tx: 0xff...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_DUP OP_HASH...	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	

012123...	OP_DUP OP_HASH...
-----------	-------------------

Ejecuto este script completo



Un script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d
05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca
8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Un script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d
05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca
8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

Un script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
      "vout": 0,
      "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.10000000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

```

{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig": "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccde7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

Un script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
      "vout": 0,
      "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbf6e6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.10000000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

scriptSig + scriptPubKey

```

"version": 1,
"locktime": 0,
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccde7fb5c1b1a91137999818d17c73d0f80aef9",
    "sequence": 4294967295
  }
],
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
  }
]
}
```



Scripting language

Qué scripts podemos usar?

Script (Bitcoin scripting language):

- Un **lenguaje de stack**
 - Instrucciones se ejecutan una después de otra una sola vez
 - No se permiten loops (tiempo de ejecución limitado por el tamaño del script)
 - Lenguaje no es Turing completo (mineros validan todas las transacciones)
 - Solo 256 instrucciones
-
- Stateless verification (mismo en todos los compu, no parten en un estado)



Scripting language

Script (Bitcoin scripting language):

- Dos posibles resultados de ejecutar un script:
 1. Todo bien (un ejecución válida) significa que el input se puede gastar
 2. Error – la transacción se rechaza



Instrucciones en Script:

- Data instruction (pushed onto stack) – dirección/firma
- Operaciones de stack (OP_PUSH, OP_POP, OP_DUP)
- Crypto (OP_HASH, OP_CHECKSIG)
- +, -, *, OP_EQUALVERIFY
- OP_IF, OP_ELSE, OP_OR



Script

OP_DUP	Duplicates the top item on the stack
OP_HASH160	Hashes twice: first using SHA-256 and then RIPEMD-160
OP_EQUALVERIFY	Returns true if the inputs are equal. Returns false and marks the transaction as invalid if they are unequal
OP_CHECKSIG	Checks that the input signature is a valid signature using the input public key for the hash of the current transaction



Ejecución de un script:

- Via stack (push/pop)
- No se permite uso de memoria/variables

Comentario: desde 2010 unlocking script se ejecuta primero, y después su stack se pasa al locking script por motivos de seguridad.

P2PKH script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
      "vout": 0,
      "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbf6e6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.10000000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

scriptSig + scriptPubKey

```
"version": 1,
"locktime": 0,
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccde7fb5c1b1a91137999818d17c73d0f80aef9",
    "sequence": 4294967295
  }
],
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
  }
]
}
```

P2PKH script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "713eef22615fffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
      "vout": 0,
      "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.10000000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

<sig>

<pubKey>

OP_DUP

OP_HASH160

<pubKeyHash?>

OP_EQUALVERIFY

OP_CHECKSIG

```
"version": 1,
"locktime": 0,
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig": "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccdd6e7fb5c1b1a91137999818d17c73d0f80aef9",
    "sequence": 4294967295
  }
],
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
  }
]
}
```

P2PKH script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "713eef22615fffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
      "vout": 0,
      "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.10000000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

<sig>
<pubKey>

OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG

```
"version": 1,
"locktime": 0,
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig": "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815cdd6e7fb5c1b1a91137999818d17c73d0f80aef9",
    "sequence": 4294967295
  }
],
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aaaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
  }
]
}
```

P2PKH script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "713eef22615fffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
      "vout": 0,
      "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.10000000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

<sig>
<pubKey>

OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG

```
"version": 1,
"locktime": 0,
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig": "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815cdd6e7fb5c1b1a91137999818d17c73d0f80aef9",
    "sequence": 4294967295
  }
],
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
  }
]
}
```



P2PKH script

<Sig> <PubKey>

DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG



P2PKH script

<Sig> <PubKey>

DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack





P2PKH script



<Sig> <PubKey>

DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack





P2PKH script



Stack





P2PKH script



Stack





P2PKH script



Stack





P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



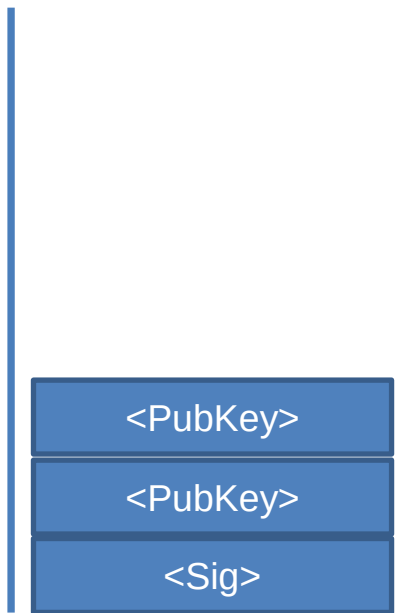


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



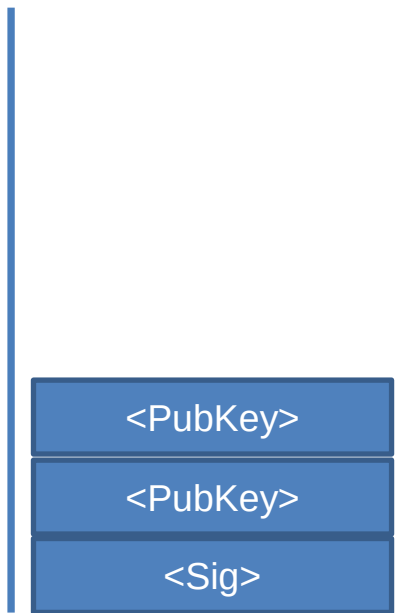


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



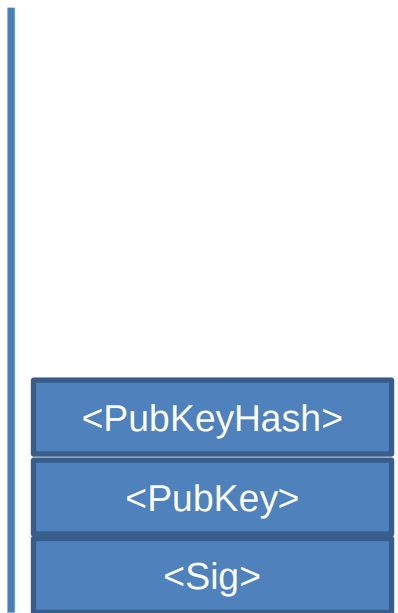


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



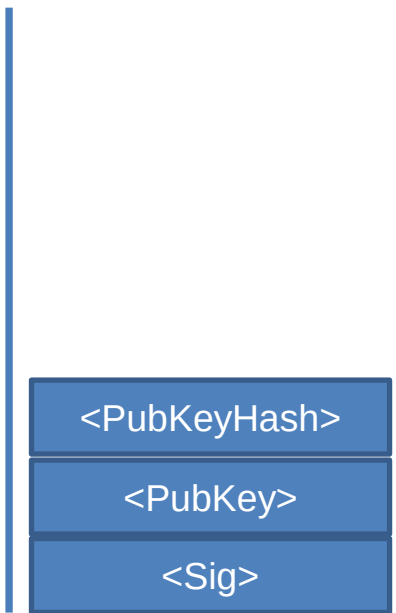


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



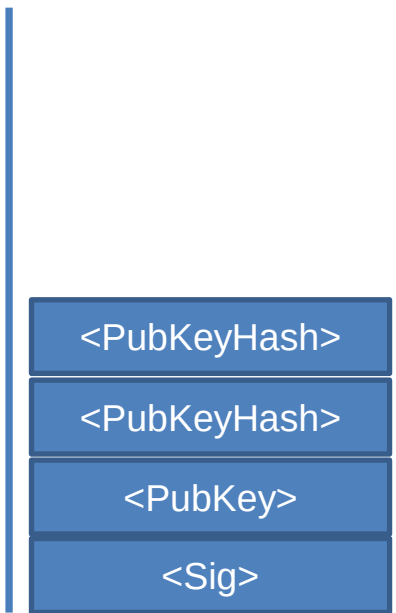


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



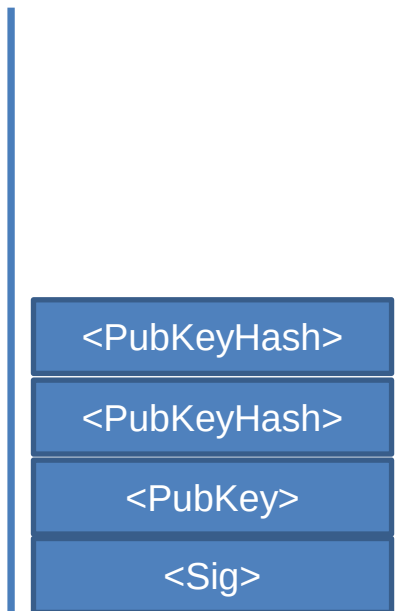


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



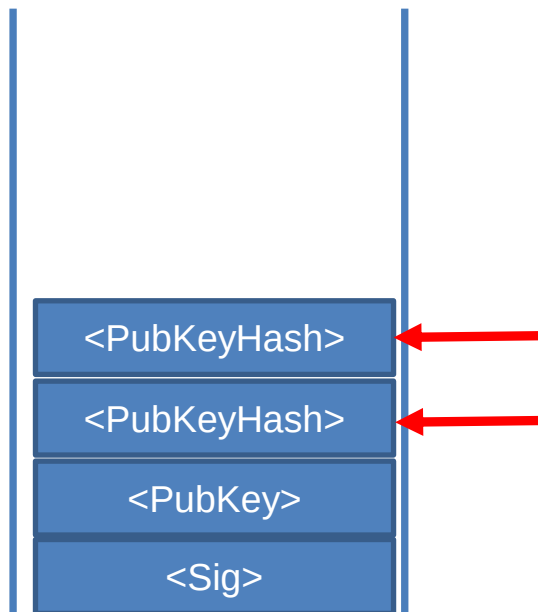


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack



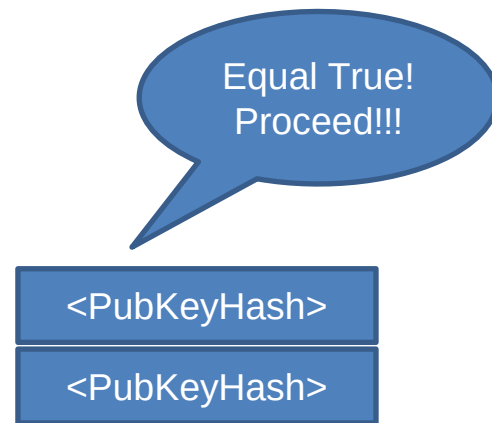


P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack





P2PKH script



<Sig> <PubKey> DUP HASH160 <PubKeyHash> EQUALVERIFY CHECKSIG

Stack

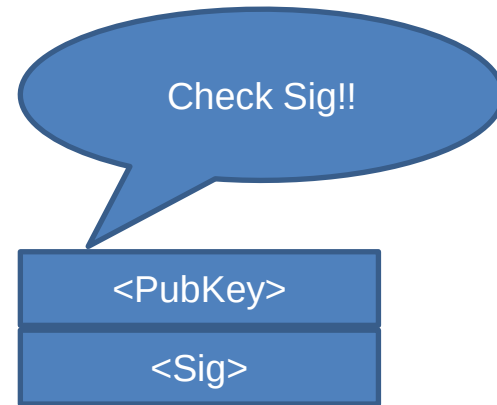


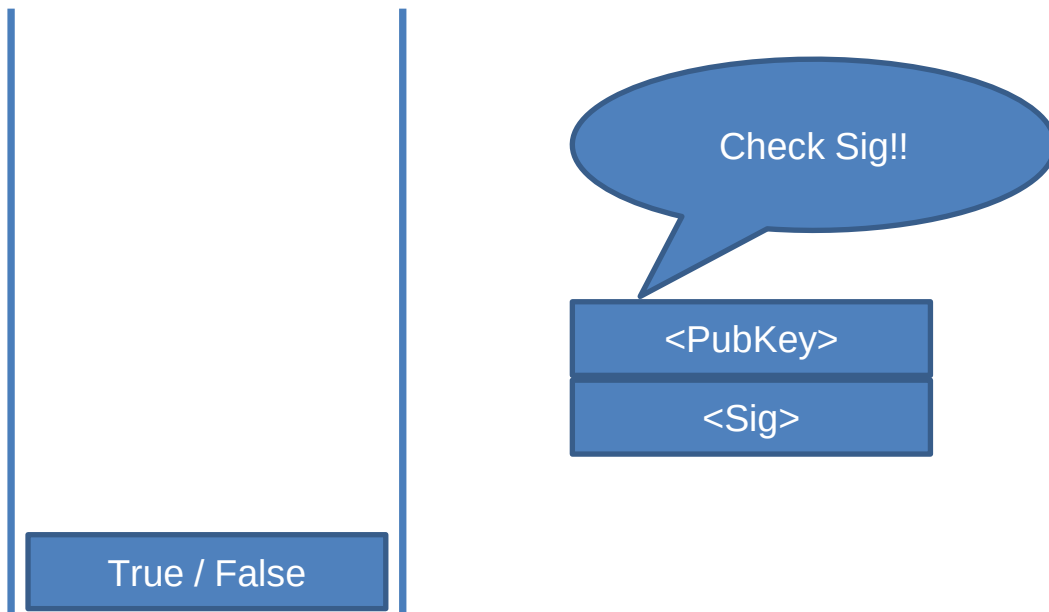


P2PKH script



Stack







Qué se firma en sig?

- En Bitcoin se puede firmar solo una cosa: **la transacción entera**

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```




Qué se firma en sig?

- En Bitcoin se puede firmar solo una cosa: **la transacción entera**

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca8b756786098567550d4820c09db988fe9997d049d687292f815ccd6e7fb5c1b1a91137999818d17c73d0f80aef9",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Qué se firma en sig?

- En realidad, firmo los siguiente:

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      [REDACTED]
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Qué firmo?

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	012123...
Outputs			
num	value		Locking script
0	3.1		OP_DUP OP_HASH...
1	2.2		OP_DUP OP_HASH...

Ya contiene la
firma!!!



Qué firmo?

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	2.2	OP_DUP OP_HASH...	

Lo dejo vacio. Y
firmo esto.



ScriptSig, ScriptPubKey

¿De dónde viene el nombre?

Transacción básica:

- Paga al X 1 BTC

En realidad:

- Esto crea un output que dice
- "Este output se puede gastar con una firma de X"

X es una llave publica



ScriptSig, ScriptPubKey

¿De dónde viene el nombre?

Transacción básica:

- Paga al X 1 BTC

En realidad:

- "Este output se puede gastar con una firma de X"

X es una llave publica

La mayoría de transacciones coinbase de Satoshi son así

Pay to Public Key (P2PK)

P2PK script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "04e6ed5b1b015c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "n": 0,
      "scriptPubKey": "04283338ffd784c198147f99aed2cc16709c90b1522e3b3637b312a6f9130
e0eda7081e373a96d36be319710cd5c134aaffba81ff08650d7de8af332fe4d8cde20 OP_CHECKSIG"
    }
  ]
}
```

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
      "vout": 0,
      "scriptSig": "304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c
4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b2415",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "scriptPubKey": "OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

P2PK script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "04e6ed5b1b015c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "n": 0,
      "scriptPubKey": "04283338ffd784c198147f99aed2cc16709c90b1522e3b3637b312a6f9130
e0eda7081e373a96d36be319710cd5c134aaffba81ff08650d7de8af332fe4d8cde20 OP_CHECKSIG"
    }
  ]
}
```

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
      "vout": 0,
      "scriptSig": "304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c
4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b2415",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "scriptPubKey": "OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```


P2PK script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "04e6ed5b1b015c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "n": 0,
      "scriptPubKey": "04283338ffd784c198147f99aed2cc16709c90b1522e3b3637b312a6f9130
e0eda7081e373a96d36be319710cd5c134aaffba81ff08650d7de8af332fe4d8cde20 OP_CHECKSIG"
    }
  ]
}
```

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
      "vout": 0,
      "scriptSig": "304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c
4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b2415",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "scriptPubKey": "OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG",
      "n": 0
    }
  ]
}
```

P2PK script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "04e6ed5b1b015c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "n": 0,
      "scriptPubKey": "04283338ffd784c198147f99aed2cc16709c90b1522e3b3637b312a6f9130
e0eda7081e373a96d36be319710cd5c134aaffba81ff08650d7de8af332fe4d8cde20 OP_CHECKSIG"
    }
  ]
}
```

scriptSig + scriptPubKey

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
      "vout": 0,
      "scriptSig": "304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c
4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b2415",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "scriptPubKey": "OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

P2PK script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "04e6ed5b1b015c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "n": 0,
      "scriptPubKey": "04283338ffd784c198147f99aed2cc16709c90b1522e3b3637b312a6f9130
e0eda7081e373a96d36be319710cd5c134aaffba81ff08650d7de8af332fe4d8cde20 OP_CHECKSIG"
    }
  ]
}
```

<Sig>

<PubKey>
OP_CHECKSIG

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
      "vout": 0,
      "scriptSig": "304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c
4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b2415",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "scriptPubKey": "OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

P2PK script

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "04e6ed5b1b015c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "n": 0,
      "scriptPubKey": "04283338ffd784c198147f99aed2cc16709c90b1522e3b3637b312a6f9130
e0eda7081e373a96d36be319710cd5c134aaffba81ff08650d7de8af332fe4d8cde20 OP_CHECKSIG"
    }
  ]
}
```

<Sig>

<PubKey>
OP_CHECKSIG

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
      "vout": 0,
      "scriptSig": "304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c
4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b2415",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 50,
      "scriptPubKey": "OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```



Una transacción de verdad

P2PK ya no se usa:

- Por motivos de privacidad
- Por motivos de pesar mucho

(originalmente SEC no comprimido == 65 bytes contra 20 bytes de P2PKH)



P2PKH script:

- Más de 90% de todas las transacciones

Pero scripts pueden ser mucho más distintos:

2 3 OP_ADD 5 OP_EQUAL

¿Qué pasa si esto es mi locking script?



Script

2 3 OP_ADD 5 OP_EQUAL

Stack





Script



Stack





Script

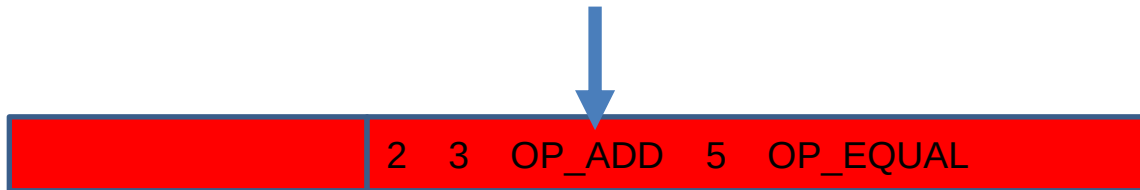


Stack

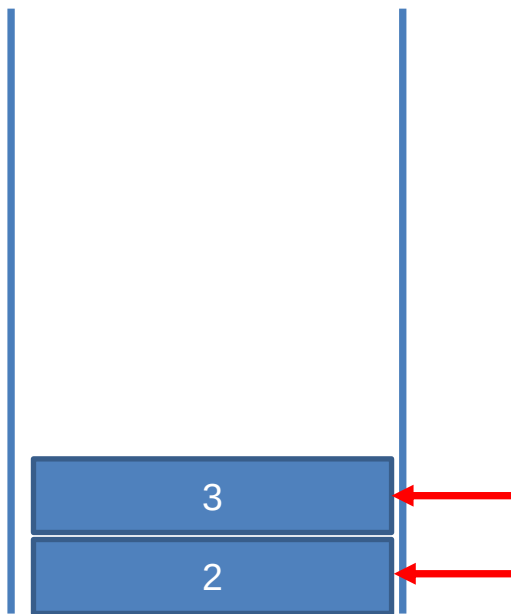




Script

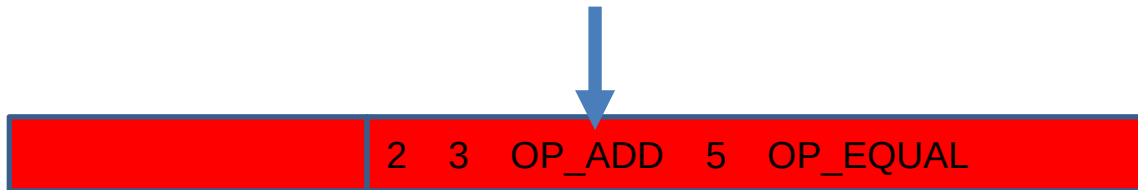


Stack





Script



Stack





Script



Stack





Script



Stack





Script



Stack





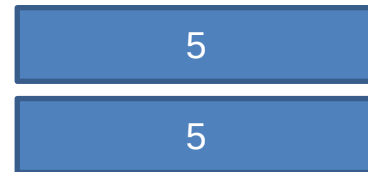
Script



Stack



Equal?

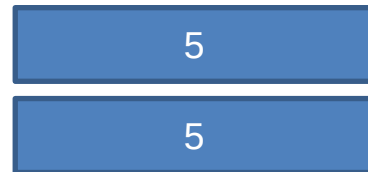
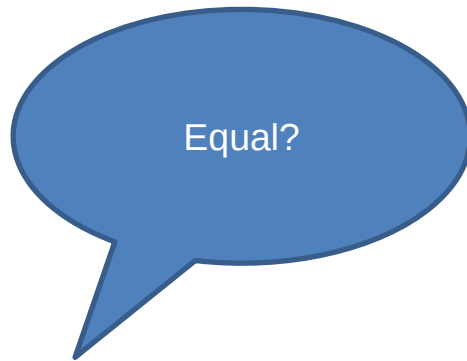




Script



Stack





Coinbase

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "03323b04040001bb1844124d696e656420627920425443204775696c642cfabe6d6d1e910cc21520338a2e
a55b3ad96e37206a19ab19bc28664cca85697f26ed1b0100000000000000800134cd50000066c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 25.00526000,
      "n": 0,
      "scriptPubKey": "OP_DUP OP_HASH160 27a1f12771de5cc3b73941664b2537c15316be43 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```



Coinbase

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "coinbase": "03323b04040001bb1844124d696e656420627920425443204775696c642cfabe6d6d1e910cc21520338a2e
a55b3ad96e37206a19ab19bc28664cca85697f26ed1b0100000000000000800134cd50000066c",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 25.00526000,
      "n": 0,
      "scriptPubKey": "OP_DUP OP_HASH160 27a1f12771de5cc3b73941664b2537c15316be43 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```



Tracking transactions

<https://www.blockchain.com/es/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2>

<http://chainquery.com/bitcoin-api/getrawtransaction>



Scripts más avanzados

OP_DUP	Duplicates the top item on the stack
OP_HASH160	Hashes twice: first using SHA-256 and then RIPEMD-160
OP_EQUALVERIFY	Returns true if the inputs are equal. Returns false and marks the transaction as invalid if they are unequal
OP_CHECKSIG	Checks that the input signature is a valid signature using the input public key for the hash of the current transaction
OP_CHECKMULTISIG	Checks that the k signatures on the transaction are valid signatures from k of the specified public keys.



Locking script de tipo multisig:

```
M <Public Key 1> <Public Key 2> ... <Public Key N> N OP_CHECKMULTISIG
```



Locking script de tipo multisig:

```
M <Public Key 1> <Public Key 2> ... <Public Key N> N OP_CHECKMULTISIG
```

Por ejemplo

```
2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG
```



Multisig

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "5bea28af51ba9b22ab2a0aff7a9f5d66582f9f63e031bc524dabd0b47784ed27",
      "vout": 0,
      "scriptSig": "30440220279b45f812ebd1004ee041eb75a3f42657dce19bdba06b30b2d1b7
0f45e2590602201b06ecbbbf6fae0a3455d98ac2924cd6dc3022425a2f08c60ffb46e96dbdc8
e9[ALL] 04a84d304aa8963fbd36287e674f109827b6d6ea60d57a7d9357df03be1fcedb2c47
475ca128b1a50408b7f584041ffd52d6b19aba5256e99dcdbbe2ed7373775d"
    },
    "sequence": 4294967295
  ],
  "vout": [
    {
      "value": 0.10000000,
      "n": 0,
      "scriptPubKey": "2
04478f498fe3f6872a9559ae0fd5975bc44f500eed955a835027962099c333536f60b4e60383e6e1
081efa0a76df1ef0aefb4da87ff0c8f12dab5da2969fc7b24e
044f09a164267c635c6991f7a96bc7901d035c07161a0074d719be723f6a9c50bc72b900092cfffec
5f3c3484dae35d04a5a2fa2e75f3a99e17577537c1227b44ba
04971e5b8b222fe47f742fa07d3327d36a6cd37088656ce29842ed82e1dc8bffa81848b3219359f
df9d8b590d3af85cfff2d06d4b19fde5ed560b2c9caa5dd656
3 OP_CHECKMULTISIG"
    }
  ]
}
```



Multisig

2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG

Unlocking script:

<Signature A> <Signature B>



Multisig

2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG

Unlocking script:

<Signature A> <Signature B>

<Signature A> <Signature C>



2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG

Unlocking script:

<Signature A> <Signature B>

<Signature A> <Signature C>

<Signature B> <Signature C>



tx: 0xff...

MSIG

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<Sig A> <Sig C>
Outputs			
num	value	Locking script	



tx: 0xff...

MSIG

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG	

tx: 0x20ff1...

<Sig A> <Sig C>

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<Sig A> <Sig C>
Outputs			
num	value	Locking script	



tx: 0xff...

MSIG

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<Sig A> <Sig C>
Outputs			
num	value	Locking script	

<Sig A> <Sig C>

2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG



tx: 0xff...

MSIG

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<Sig A> <Sig C>
Outputs			
num	value	Locking script	

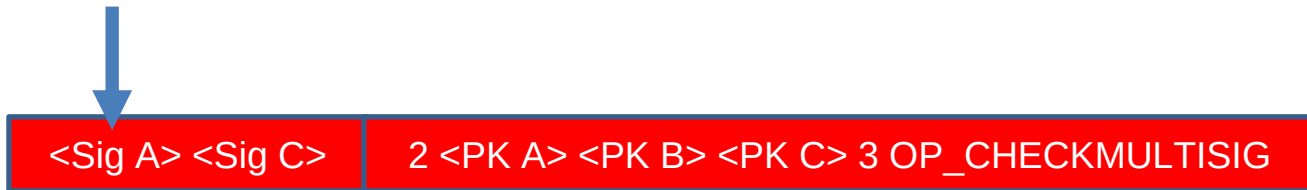
<Sig A> <Sig C>

2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

run this



Multisig

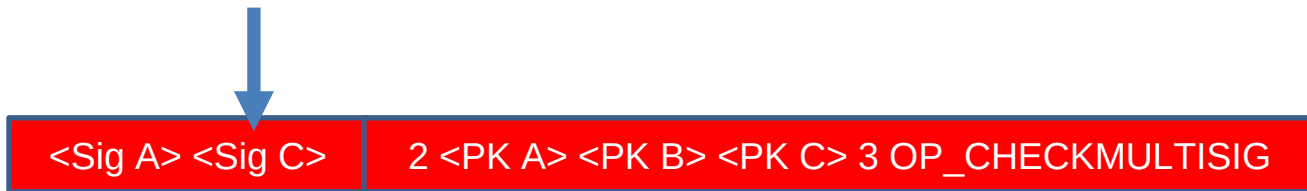


Stack





Multisig

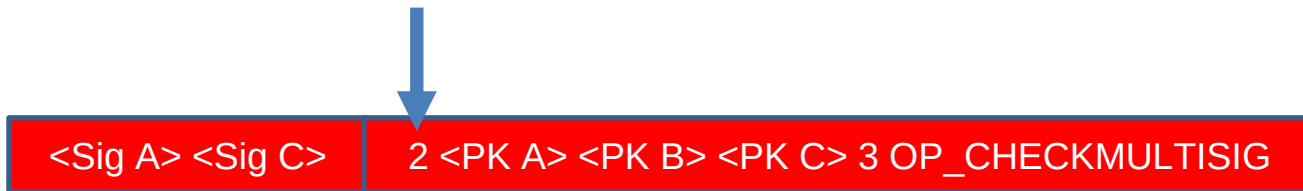


Stack

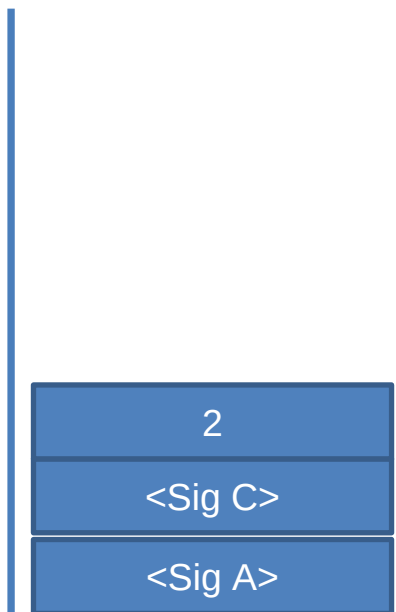




Multisig

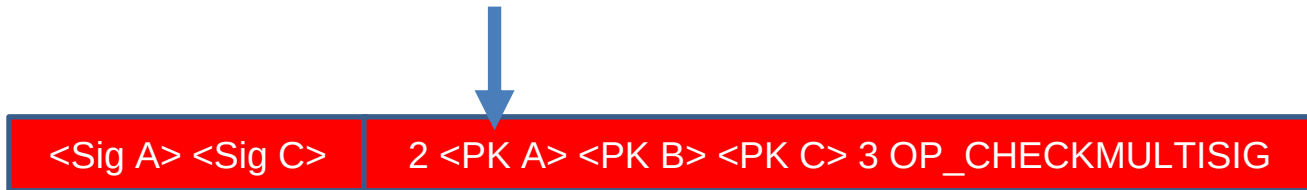


Stack

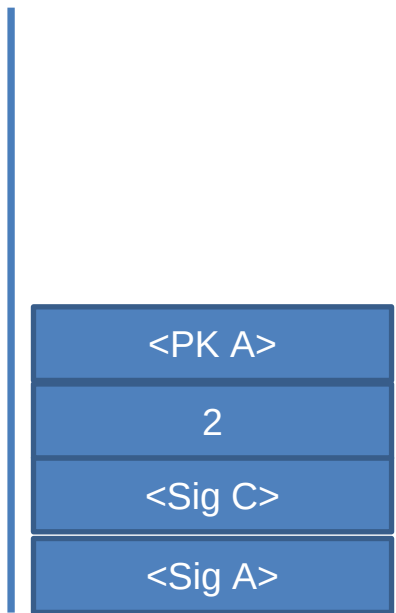




Multisig

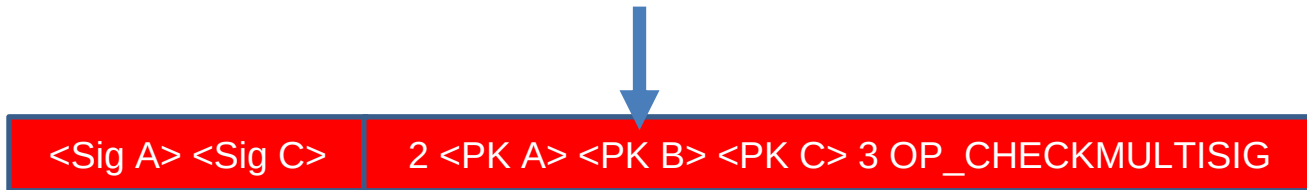


Stack

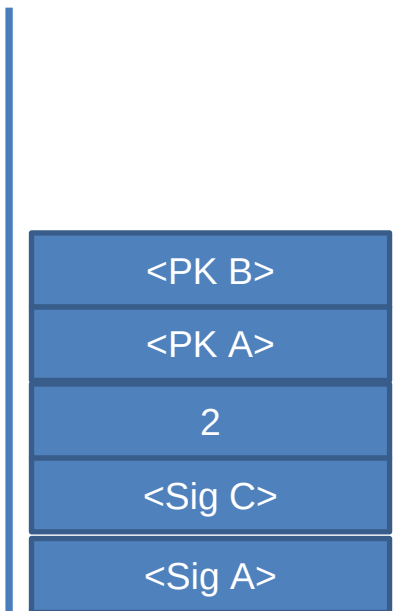




Multisig

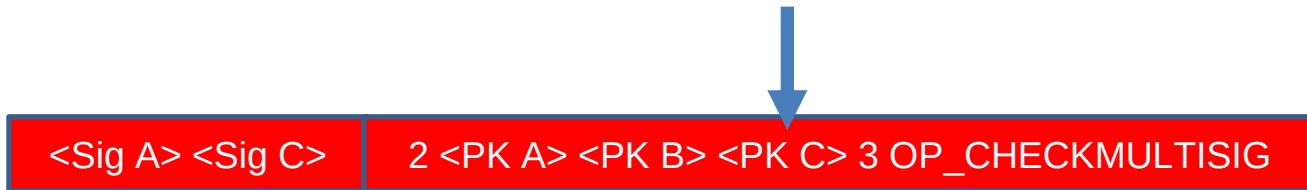


Stack

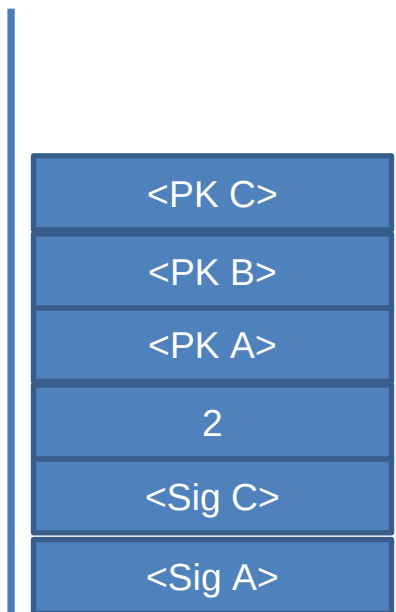




Multisig

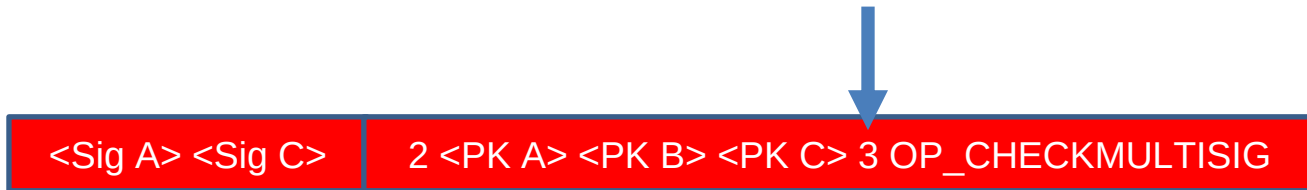


Stack

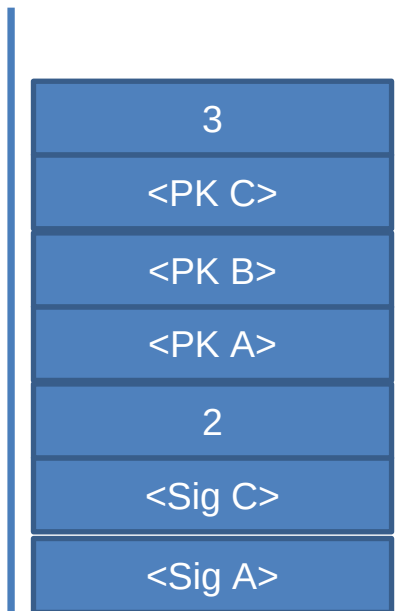




Multisig



Stack

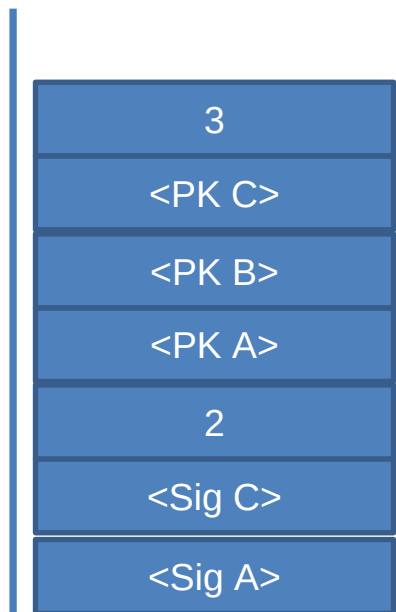




Multisig



Stack

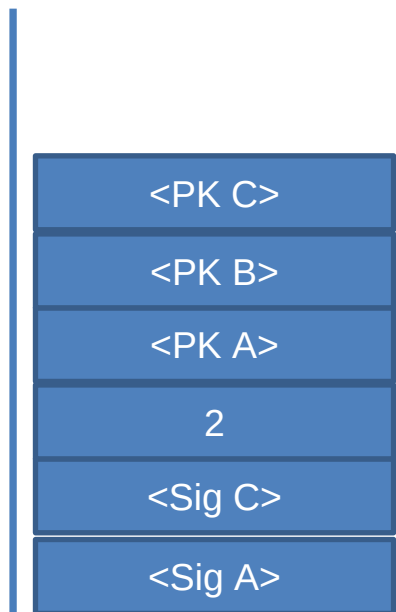




Multisig



Stack

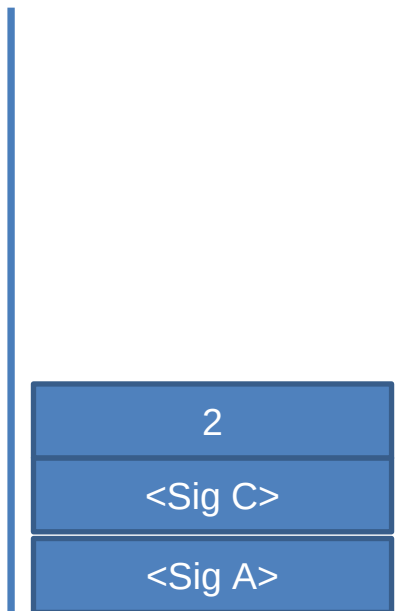




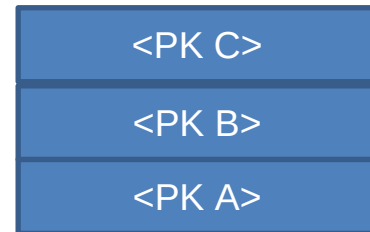
Multisig



Stack



Keys





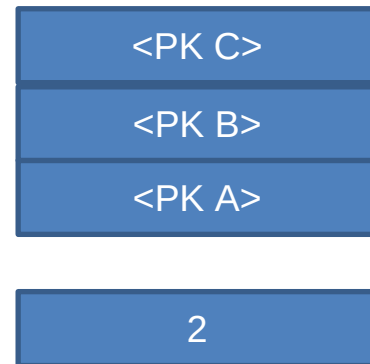
Multisig



Stack



Keys





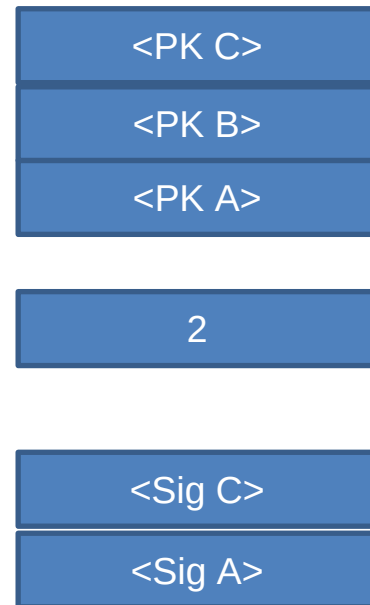
Multisig



Stack

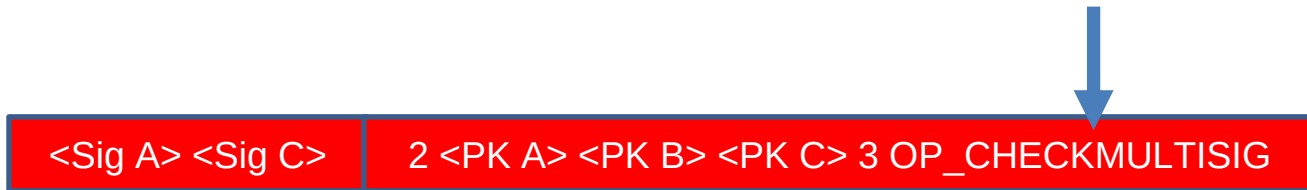


Keys



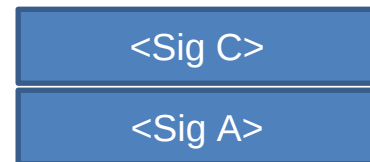
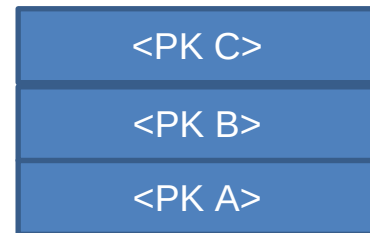


Multisig



Stack

Keys



Verify



En la practica:

- **CHECKMULTISIG hace un pop extra**

0 <Sig A> <Sig C>

2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG



Escrow transactions

Un uso de MULTISIG

Alice



Bob





Escrow transactions

Un uso de MULTISIG

Alice



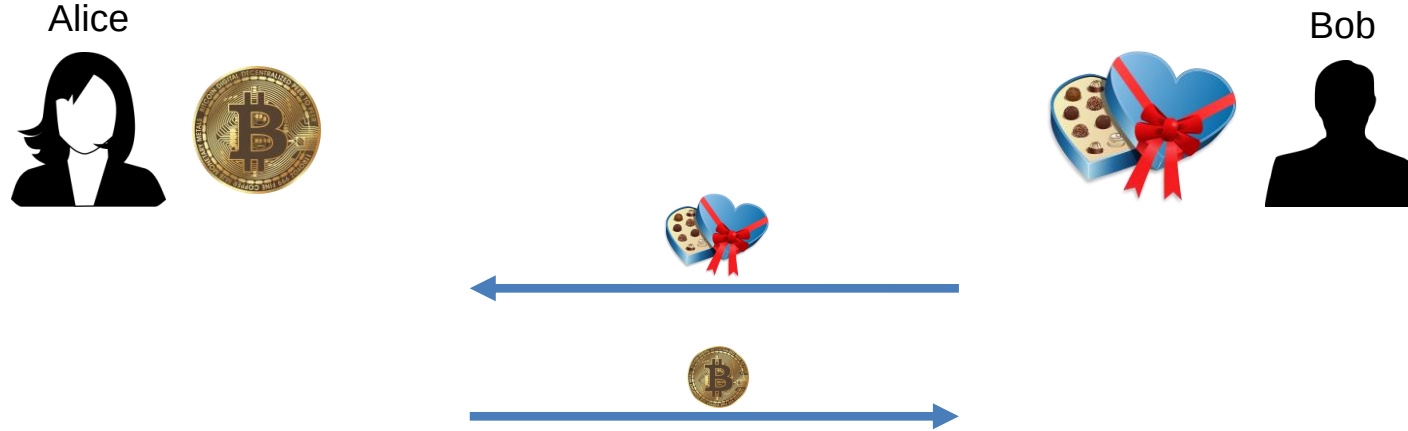
Bob





Escrow transactions

Un uso de MULTISIG





Escrow transactions

Un uso de MULTISIG

Alice



Bob



Charlie





Escrow transactions

Un uso de MULTISIG

Alice



Bob



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

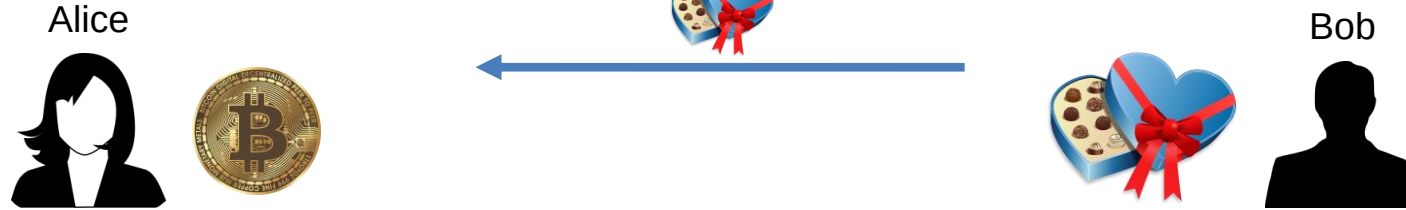
Charlie





Escrow transactions

Un uso de MULTISIG



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

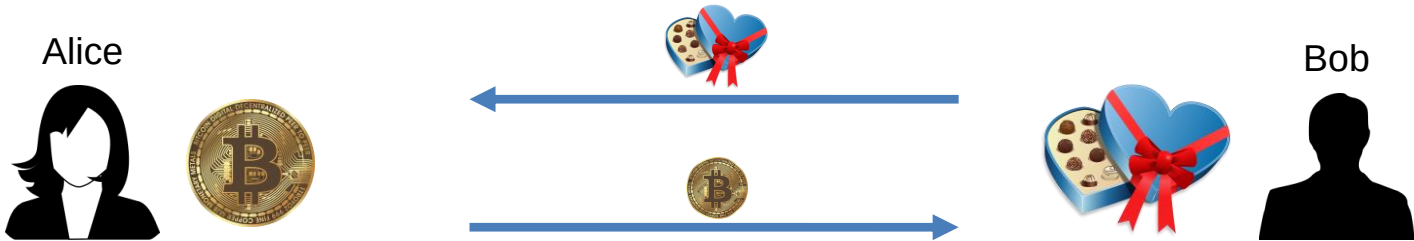
Charlie





Escrow transactions

Un uso de MULTISIG



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

Charlie



Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<Sig A> <Sig B>
Outputs			
Nr out	value	Locking script	
0	1	OP_DUP OP_HASH PK B ...	



Escrow transactions

Un uso de MULTISIG

Alice



Bob



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

Charlie





Escrow transactions

Un uso de MULTISIG



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

Charlie



Es culpa de
Bob



Escrow transactions

Un uso de MULTISIG



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

Charlie



Es culpa de Bob

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<Sig A> <Sig C>
Outputs			
Nr out	value	Locking script	
0	1	OP_DUP OP_HASH PK A ...	



Escrow transactions

Un uso de MULTISIG



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

Charlie





Escrow transactions

Un uso de MULTISIG

Alice



No te voy a pagar!



Bob



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

Charlie



Si, le vas a pagar 😊



Escrow transactions

Un uso de MULTISIG

Alice



No te voy a pagar!



Bob



0xff...

Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

Charlie



Si, le vas a pagar 😊

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<Sig B> <Sig C>
Outputs			
Nr out	value	Locking script	
0	1	OP_DUP OP_HASH PK B ...	



Pay to script hash (P2SH)

```
2 <Public Key 1> <Public Key 2> <Public Key 3> <Public Key 4> <Public Key 5> 5 OP_CHECKMULTISIG
```

Desventajas de MULTISIG:

- Pesado para un usuario quien paga (tiene que construir un custom script)
- Un script grande (el quien paga tiene extra costo de tx fee)
- Un script grande (se queda en el UTXO pool y ocupa mucho espacio en RAM)



Pay to script hash (P2SH)

```
{
  "txid": "40eee3ae1760e3a8532263678cdf64569e6ad06abc133af64f735e52562bccc8",
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "42a3fdd7d7baea12221f259f38549930b47cec288b55e4a8facc3c899f4775da",
      "vout": 0,
      "scriptSig": "473044022048d1468895910edafe53d4ec4209192cc3a8f0f21e7b9811f83b5e419bfb57e002203fef249b56682dbbb1528d4338969abb14583858488a3a766f609185efe68bca0121031a455dab5e1f614e574a2f4f12f22990717e93899695fb0d81e4ac2dcfd25d00",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.00990000,
      "n": 0,
      "scriptPubKey": "OP_HASH160 e9c3dd0c07aac76179ebc76a6c78d4d67c6c160a OP_EQUAL",
    }
  ]
}
```



tx: 0xff...

P2SH

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	4	012123...
Outputs			
num	value	Locking script	
0	3.1	OP_DUP OP_HASH...	
1	5.5	OP_HASH160 <script hash> OP_EQUAL	

tx: 0x20ff1...

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff...	1	<data> <redeem script>
Outputs			
num	value	Locking script	
0	2.1	OP_DUP OP_HASH...	
1	0.5	OP_HASH160 <script hash> EQUAL	





Pay to script hash (P2SH)

Solución: Pay to script hash (P2SH):

- Permite especificar un script complicado como si fuese pago a una dirección
- Idea: **Locking script** no contiene el script, pero el hash de un script
- Para gastar los fondos: **Unlocking script** especifica el script mismo y sus datos

P2SH tiene una ejecución especial:

- Reconoce un P2SH locking script
- Y hace validación en dos fases



Unlocking script

<data> <redeem script>

Locking script

OP_HASH160 <script hash> OP_EQUAL



P2SH

It's a P2SH!!!

Unlocking script

Locking script

<data> <redeem script>

OP_HASH160 <script hash> OP_EQUAL



P2SH

It's a P2SH!!!

Unlocking script

Locking script

<data> <redeem script>

OP_HASH160 <script hash> OP_EQUAL

Phase 1: run

<redeem script>

OP_HASH160 <script hash> OP_EQUAL



It's a P2SH!!!

Unlocking script

<data> <redeem script>

Locking script

OP_HASH160 <script hash> OP_EQUAL

Phase 1: run

<redeem script>

OP_HASH160 <script hash> OP_EQUAL

Stack

<redeem script>



P2SH

It's a P2SH!!!

Unlocking script

<data> <redeem script>

Locking script

OP_HASH160 <script hash> OP_EQUAL

Phase 1: run

<redeem script>

OP_HASH160 <script hash> OP_EQUAL

Stack

<redeem script>



It's a P2SH!!!

Unlocking script

<data> <redeem script>

Locking script

OP_HASH160 <script hash> OP_EQUAL

Phase 1: run

<redeem script>

OP_HASH160 <script hash> OP_EQUAL

Stack

h(<redeem script>)



It's a P2SH!!!

Unlocking script

<data> <redeem script>

Locking script

OP_HASH160 <script hash> OP_EQUAL

Phase 1: run

<redeem script>

OP_HASH160 **<script hash>** OP_EQUAL

Stack

<script hash>

h(<redeem script>)



P2SH

It's a P2SH!!!

Unlocking script

<data> <redeem script>

Locking script

OP_HASH160 <script hash> OP_EQUAL

Phase 1: run

<redeem script>

OP_HASH160 <script hash> OP_EQUAL

Stack

<script hash>

h(<redeem script>)

Proceed if the same!!!



P2SH

It's a P2SH!!!

Unlocking script

Locking script

<data> <redeem script>

OP_HASH160 <script hash> OP_EQUAL

Phase 2: run

<data>

redeem script



| Inputs (UTXO referenced) | | | |
|--------------------------|---------|---|------------------|
| num | hash | Nr_output | Unlocking script |
| 0 | 0xff... | 4 | 012123... |
| Outputs | | | |
| num | value | Locking script | |
| 0 | 3.1 | OP_DUP OP_HASH... | |
| 1 | 5.5 | 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG | |



| Inputs (UTXO referenced) | | | |
|--------------------------|---------|--|------------------|
| num | hash | Nr_output | Unlocking script |
| 0 | 0xff... | 4 | 012123... |
| Outputs | | | |
| num | value | Locking script | |
| 0 | 3.1 | OP_DUP OP_HASH... | |
| 1 | 5.5 | OP_HASH160 <h(redeem script)> OP_EQUAL | |

redeem script

2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG



| Inputs (UTXO referenced) | | | |
|--------------------------|---------|--|------------------|
| num | hash | Nr_output | Unlocking script |
| 0 | 0xff... | 4 | 012123... |
| Outputs | | | |
| num | value | Locking script | |
| 0 | 3.1 | OP_DUP OP_HASH... | |
| 1 | 5.5 | OP_HASH160 <h(redeem script)> OP_EQUAL | |

Unlocking:

<sig A> <sig B> < 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG >



Unlock

<sig A> <sig B> < 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG >

Lock

OP_HASH160 <h(redeem script)> OP_EQUAL



P2SH

Unlock

<sig A> <sig B> < 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG >

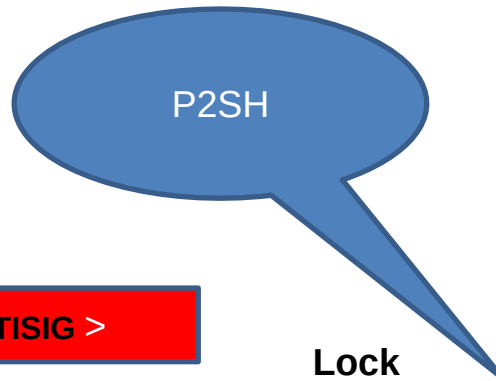
Lock

OP_HASH160 <h(redeem script)> OP_EQUAL

P2SH



P2SH



Unlock

<sig A> <sig B> < 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG >

Lock

OP_HASH160 <h(redeem script)> OP_EQUAL

$h(2 \text{ <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG}) == \text{<h(redeem script)>}$



P2SH

Unlock

<sig A> <sig B> < 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG >

Lock

OP_HASH160 <h(redeem script)> OP_EQUAL

P2SH

YES!!!

$h(2 \text{ <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG}) == \text{<h(redeem script)>}$



P2SH

Unlock

<sig A> <sig B> < 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG >

P2SH

Lock

OP_HASH160 <h(redeem script)> OP_EQUAL

YES!!!

$h(2 \text{ <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG}) == \text{<h(redeem script)>}$

OK, run
this

<sig A> <sig B> 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG



Pay to script hash (P2SH)

Redeem script: 2 <PK1> <PK2> <PK3> <PK4> <PK5> 5 CHECKMULTISIG

Lock: HASH160 <h(Redeem script)> EQUAL

Unlock: <sig 1> <sig 2> <Redeem script>

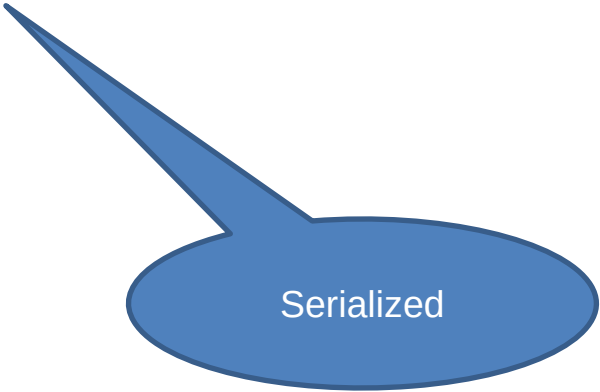


Pay to script hash (P2SH)

Redeem script: 2 <PK1> <PK2> <PK3> <PK4> <PK5> 5 CHECKMULTISIG

Lock: HASH160 <h(Redeem script)> EQUAL

Unlock: <sig 1> <sig 2> <Redeem script>



Serialized



Pay to script hash (P2SH)

Beneficios de P2SH:

- Input pequeño, incluso para un script complicado (su hash)
- El quien manda el dinero no paga mucho (pega es para gastar)
- El script grande no se guarda en UTXO (RAM), sino blockchain (disco duro)
- El script grande no se guarda hasta gastar el dinero
- El vendedor es responsable de construir su script complicado



Bitcoin como tamper proof log

Quiero mostrar que tenía cierta información en tal fecha:

- Publico su hash en el blockchain de Bitcoin
 - I.e. hago una transacción a hash de mi documento en base58 encoding
 - Problema: "Blockchain/UTXO bloat"
-
- E.g. <https://proofofexistence.com>



Bitcoin como tamper proof log

Solución: OP_RETURN

- Un comando que hace un output unspendable
- Introducido en BitcoinCore 0.9 para achicar el UTXO set

| Inputs (UTXO referenced) | | | |
|--------------------------|----------|-----------------------------------|------------------|
| num | hash | Nr_output | Unlocking script |
| 0 | 0xff... | 4 | 012123... |
| Outputs | | | |
| num | value | Locking script | |
| 0 | 0.000001 | OP_RETURN H("Hola. Soy Satoshi!") | |



Bitcoin como tamper proof log

Usos de esto:

- Digital timestamping
- Proof of burn

<https://www.blockchain.com/btc/tx/52dd20f60d6e14e5a783e7668cf410efdea40cd9a92479b0f2423d0bc63575fa>