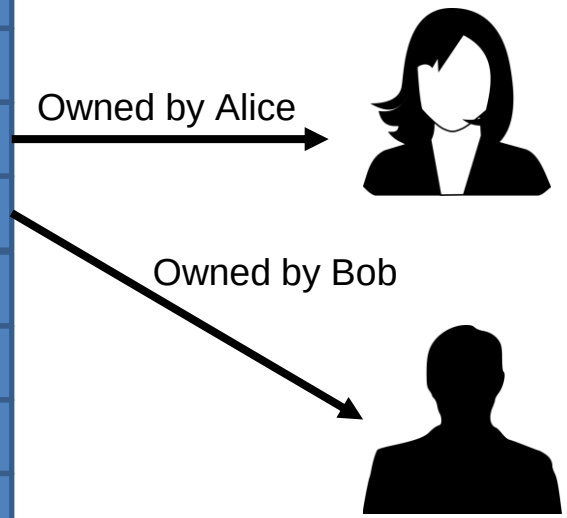
Transactions and smart contracts

Transaction

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 $\mathbf{LS_{Alice}}$		
Signature by $\mathbf{LS_{Bob}}$		



A real transaction

https://www.blockchain.com/en/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

A real transaction

Summary

USD BTC

Fee	0.00050000 BTC (193.798 sat/B - 48.450 sat/WU - 258 bytes)	0.09950000 BTC
Hash	0627052b6f28912f2703066a912ea577f2ce4da4caa5a...	2013-12-27 20:11

1Cdid9KFAaatwczBwBttQcwXYCpvK8...	0.10000000 BTC	1GdK9UzpHBzqzX2A9JFP3Di4weBwq...	0.01500000 BTC
		1Cdid9KFAaatwczBwBttQcwXYCpvK8...	0.08450000 BTC

A real transaction

Details

Hash	0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
Status	Confirmed
Received Time	2013-12-27 20:11
Size	258 bytes
Weight	1,032
Included in Block	277316
Confirmations	487,231
Total Input	0.10000000 BTC
Total Output	0.09950000 BTC
Fees	0.00050000 BTC

A real transaction

Inputs

HEX ASM

Index	0	Details	Output
Address	1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	Value	0.10000000 BTC
Pkscript	OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301 0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf		

A real transaction

Outputs

Index	0	Details	Unspent
Address	1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA	Value	0.01500000 BTC
Pkscript	OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG		

Index	1	Details	Unspent
Address	1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	Value	0.08450000 BTC
Pkscript	OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG		

A real transaction


```
{
  "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",
    }
  ]
}
```

A real transaction

Metadata


```
{
  "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",
    }
  ]
}
```

A real transaction

Inputs


```
{
  "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",
    }
  ]
}
```

A real transaction


```
{
  "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",
    }
  ]
}
```

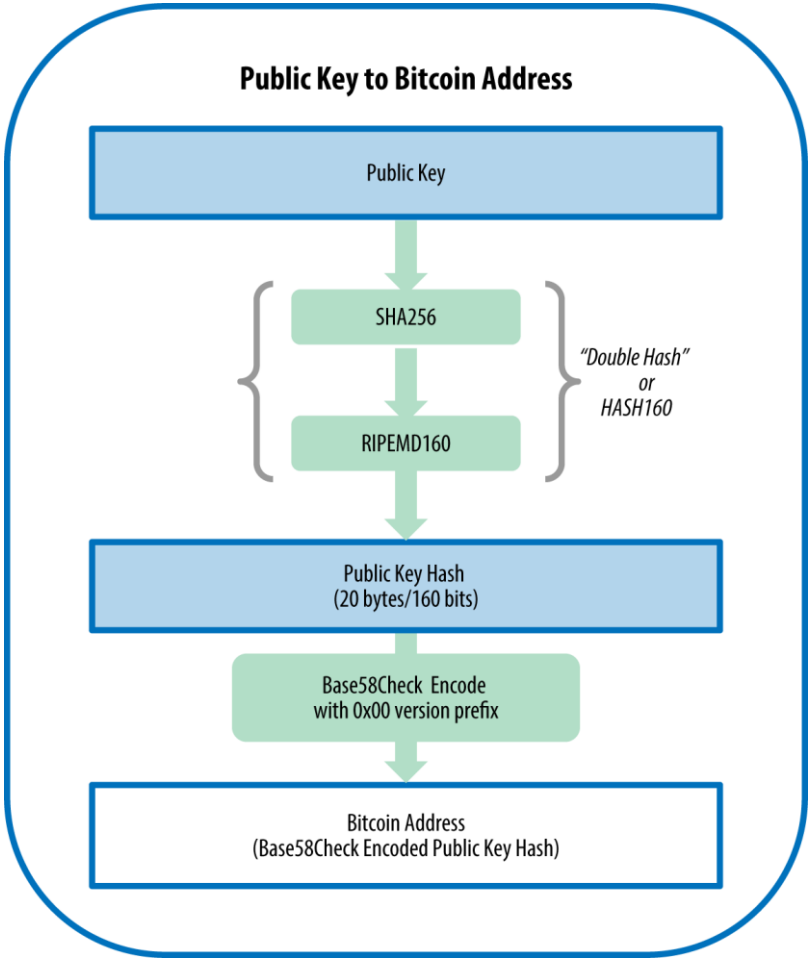

Outputs

A real transaction


```
{
  "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",
    }
  ]
}
```

A Bitcoin address

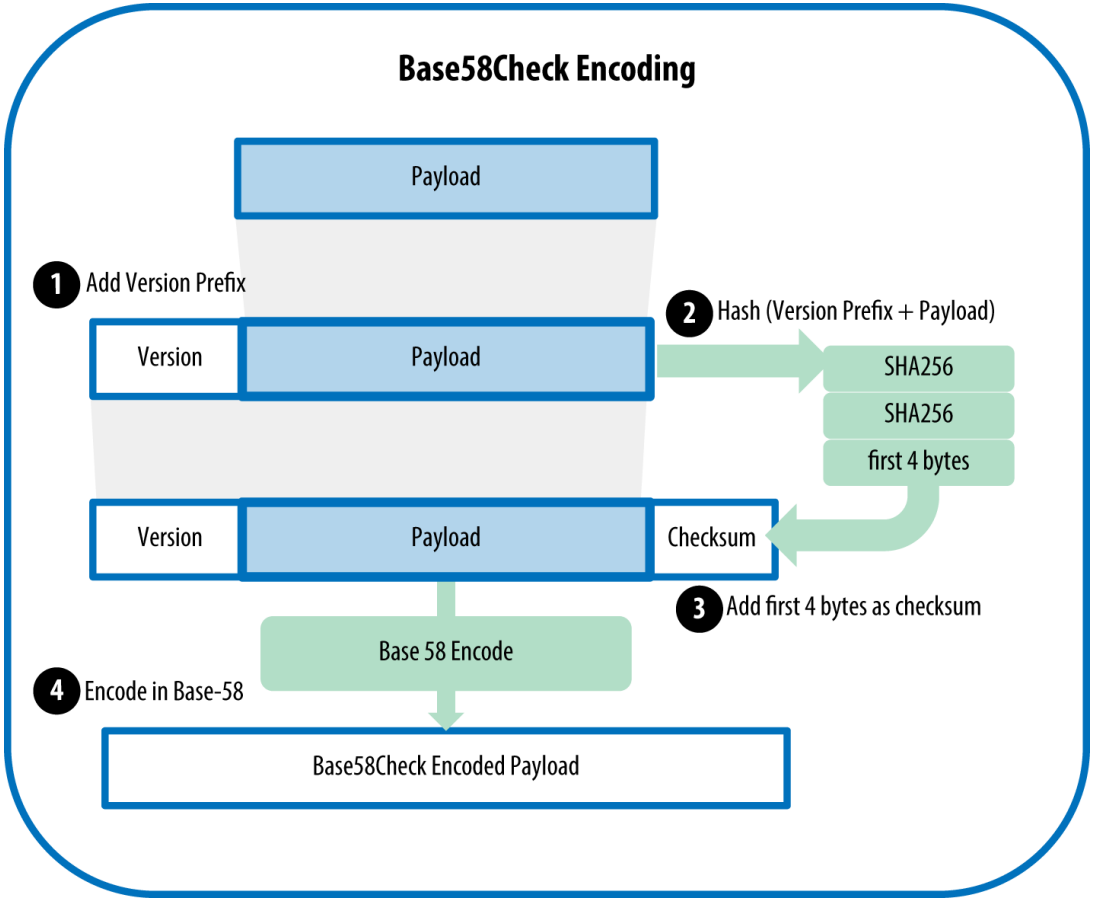
Is not a public key



https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04.asciidoc

A Bitcoin address

Is not a public key



https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04.asciidoc

A real transaction


```
{
  "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",
    }
  ]
}
```

A real transaction


```
{
  "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",
    }
  ]
}
```

A real transaction


```
{
  "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",
    }
  ]
}
```

A real transaction

Inputs

HEX ASM

Index	0	Details	Output
Address	1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	Value	0.10000000 BTC
Pkscript	OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301 0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf		

A real transaction

Outputs

Index	0	Details	Unspent
Address	1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA	Value	0.01500000 BTC
Pkscript	OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG		

Index	1	Details	Unspent
Address	1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	Value	0.08450000 BTC
Pkscript	OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG		

A real transaction

The only thing that exists in Bitcoin are UTXOs:

- A transaction spends UTXOs in its inputs, and produces outputs

Transaction

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…

A real transaction

Output of a transaction specifies:

- Value of Bitcoins being paid
- Public key of the recipient

A real transaction

Output of a transaction specifies:

- Value of Bitcoins being paid
- ~~Public key of the recipient~~

A real transaction


```
{
  "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",
    }
  ]
}
```

A real transaction

Output of a transaction specifies:

- Value of Bitcoins being paid
- ~~Public key of the recipient~~ address of the recipient

A real transaction

Output of a transaction specifies:

- Value of Bitcoins being paid
- ~~Public key of the recipient~~ address of the recipient

A real transaction


```
{
  "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",
    }
  ]
}
```

A real transaction

Output of a transaction specifies:

- Value of Bitcoins being paid
- ~~Public key of the recipient~~ address of the recipient
- SCRIPT

A real transaction

A basic transaction

- Pay 1 BTC to X

In reality:

- This creates an output that says
- ‘’This output can be spent by provinding a signature of X"

X is a Bitcoin address ~ i.e. a hash

X does not really tell us the public key (to be able to verify the signature)

A real transaction

A basic transaction

- Pay 1 BTC to X

In reality:

- This creates an output that says
- ~~‘’This output can be spent by provinding a signature of X"~~
- „This output can be spent by providing a public key that hashes to X, together with a signature corresponding to this public key"

A real transaction

A basic transaction

- Pay 1 BTC to X

In reality a transaction is defined by:

- The quantity of BTC it spends
- A **locking script**

Locking script specifies conditions required to spend the output

A real transaction

A basic transaction

- Pay 1 BTC to X

Input for this transaction is:

- A UTXO (hash of the transaction + number of the output in this transaction)
- An **unlocking script**

Which script do we run?

- **Unlocking script (Input) + Locking script (UTXO referenced in the input)**

A real transaction

A basic transaction

- Pay 1 BTC to X

Input for this transaction is:

- A UTXO (hash of the transaction + number of the output in this transaction)
- An **unlocking script**

Which script do we run?

- **Unlocking script (Input) + Locking script (UTXO referenced in the input)**

A real transaction

A basic transaction

- Pay 1 BTC to X

Input for this transaction is:

- A UTXO (hash of the transaction + number of the output in this transaction)
- An **unlocking script**

Who runs the script?

- **All nodes in the network!!!**

Example of a 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...

Example of a 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...

Example of a 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...

Example of a 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...

Example of a 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...

Example of a 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...

Example of a 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…

Example of a 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...

Example of a 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...

Execute this entire script

Example of a 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",
    }
  ]
}
```

Example of a 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",
    }
  ]
}
```

nple of a script


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
            "vout": 0,
            "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100
            f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42
            657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462"
            ,
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 0.10000000,
            "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
        }
    ]
}
```

```
"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",
  }
]
}
```

nple of a script


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
            "vout": 0,
            "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100
            f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42
            657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462"
            ,
            "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" : "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",
  }
]
}
```

Scripting language

Which scripts can we use?

Script (Bitocoin scripting language):

- A **stack-based language**
- Instructions executed one after the other without repetitions (one execution)
- Loops are not allowed (runtime bounded by script size)
- Language is not Turing complete (miners validate all the transactions)
- Only 256 instructions

- Stateless verification (same in each machine, does not start in some state)

Scripting language

Script (Bitcoin scripting language):

- Two possible results when executing a script:

1. All good (a successful execution) means that the input can be spent
2. Error – the transaction is rejected

Script

Instructions in Script:

- Data instruction (pushed onto stack) – address/signature
- Operating the 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

Script

Executing a script:

- Via stack (push/pop)
- We can ***not*** use memory/variables

Observation: from 2010 unlocking script is executed first, and then its stack is passed onto the locking script to execute (for security reasons).

P2PKH script


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
            "vout": 0,
            "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100
            f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42
            657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462"
            ,
            "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" : "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",
  }
]
}
```

P2PKH script


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
            "vout": 0,
            "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100
            f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42
            657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462"
            ,
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 0.10000000,
            "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
        }
    ]
}
```



```
"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",
  }
]
}
```


```
<sig>
<pubKey>
--------------
OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG
```

P2PKH script


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
            "vout": 0,
            "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100
            f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42
            657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462"
            ,
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 0.10000000,
            "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
        }
    ]
}
```



```
"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",
  }
]
}
```


<sig>
<pubKey>

OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG

P2PKH script


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "txid": "713eef22615ffb7c2f8f813e79a0d1e170d05a99218e291c33daca258f284d52",
            "vout": 0,
            "scriptSig": "493046022100a59e516883459706ac2e6ed6a97ef9788942d3c96a0108f2699fa48d9a5725d1022100
            f9bb4434943e87901c0c96b5f3af4e7b83e12c69b1edbfe6965f933fcd17d014104e5a0b4de6c09bd9d3f730ce56ff42
            657da3a7ec4798c0ace2459fb007236bc3249f70170509ed663da0300023a5de700998bfec49d4da4c66288a5837462"
            ,
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 0.10000000,
            "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
        }
    ]
}
```



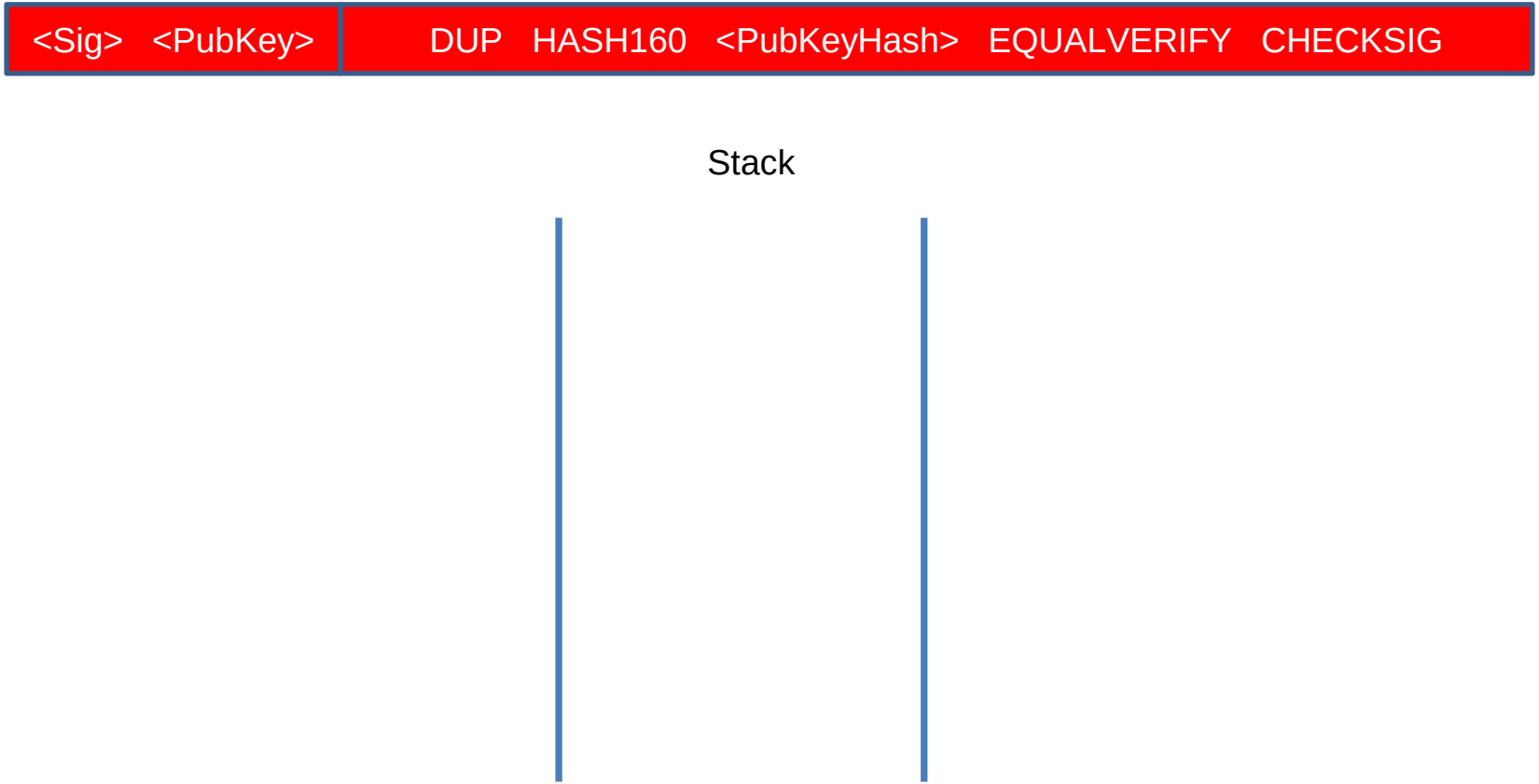
```
"version": 1,
"locktime": 0,
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" : "3045022100da43201760bda697222002f56266bf65023fef2094519e13077f777baed553b102205ce35d
    05eabda58cd50a67977a65706347cc25ef43153e309ff210a134722e9e01042daa93315eebbe2cb9b5c3505df4c6fb6caca
    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",
  }
]
}
```


```
<sig>
<pubKey>
--------------
OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG
```

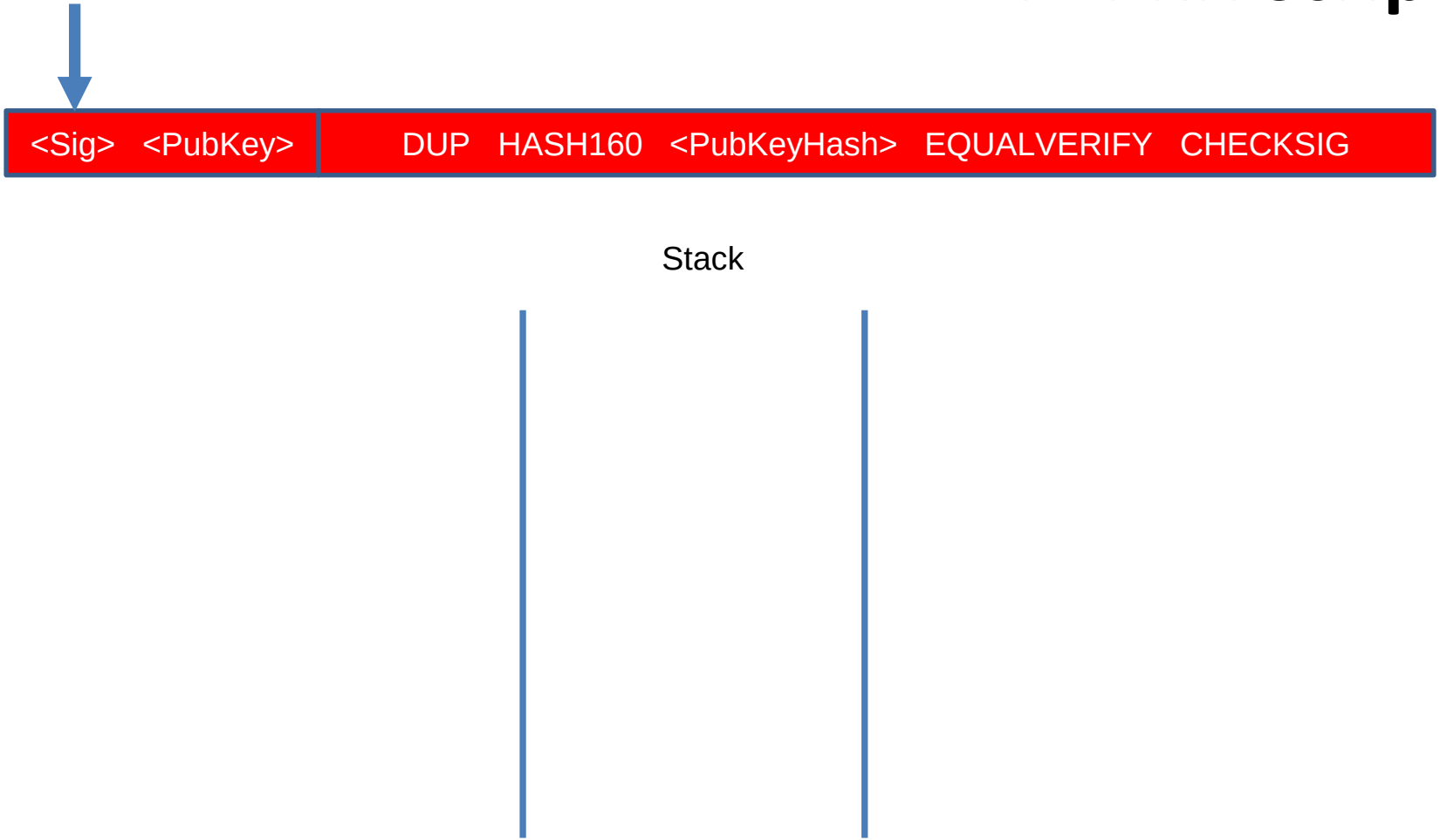
P2PKH script

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

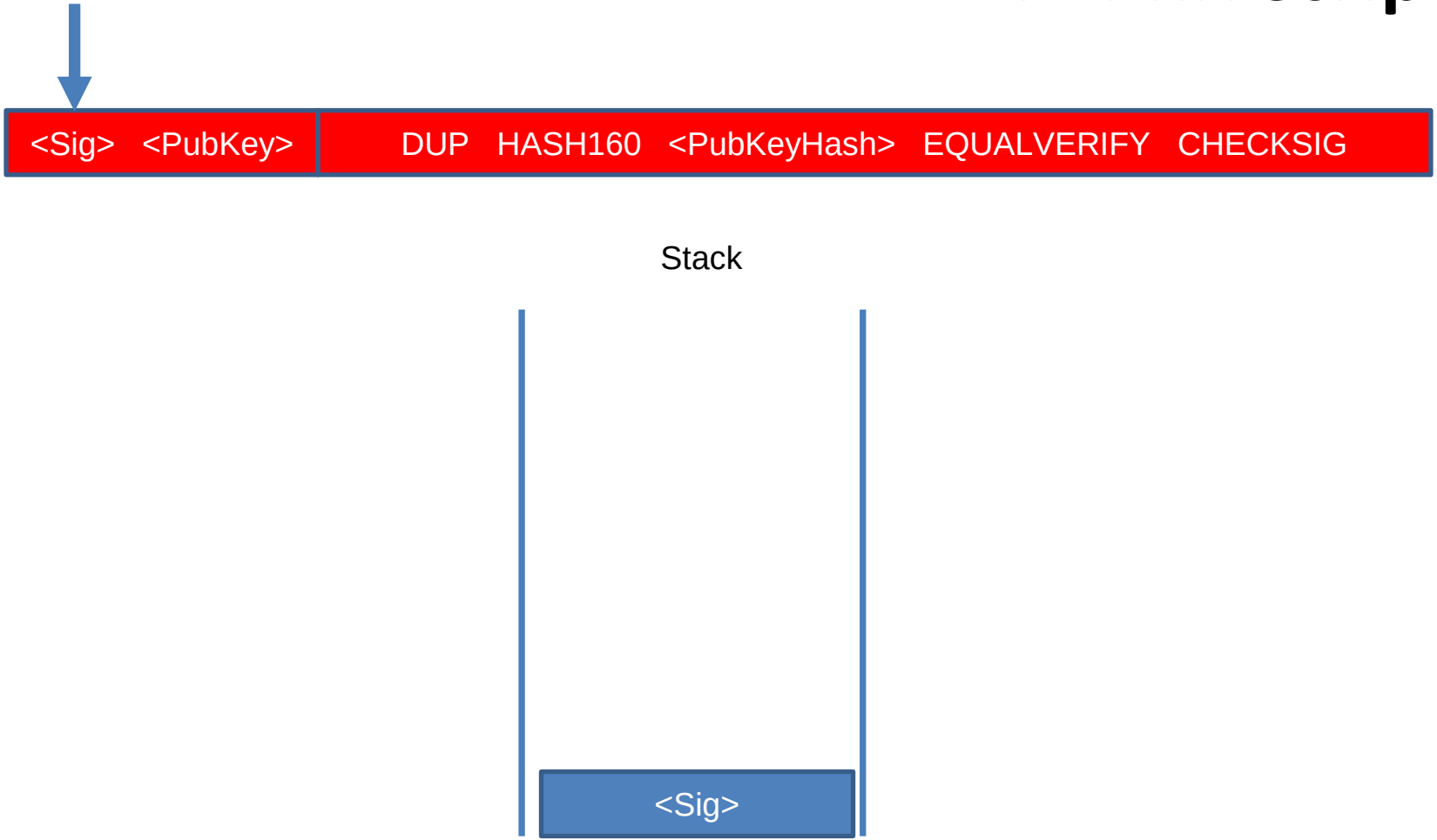
P2PKH script



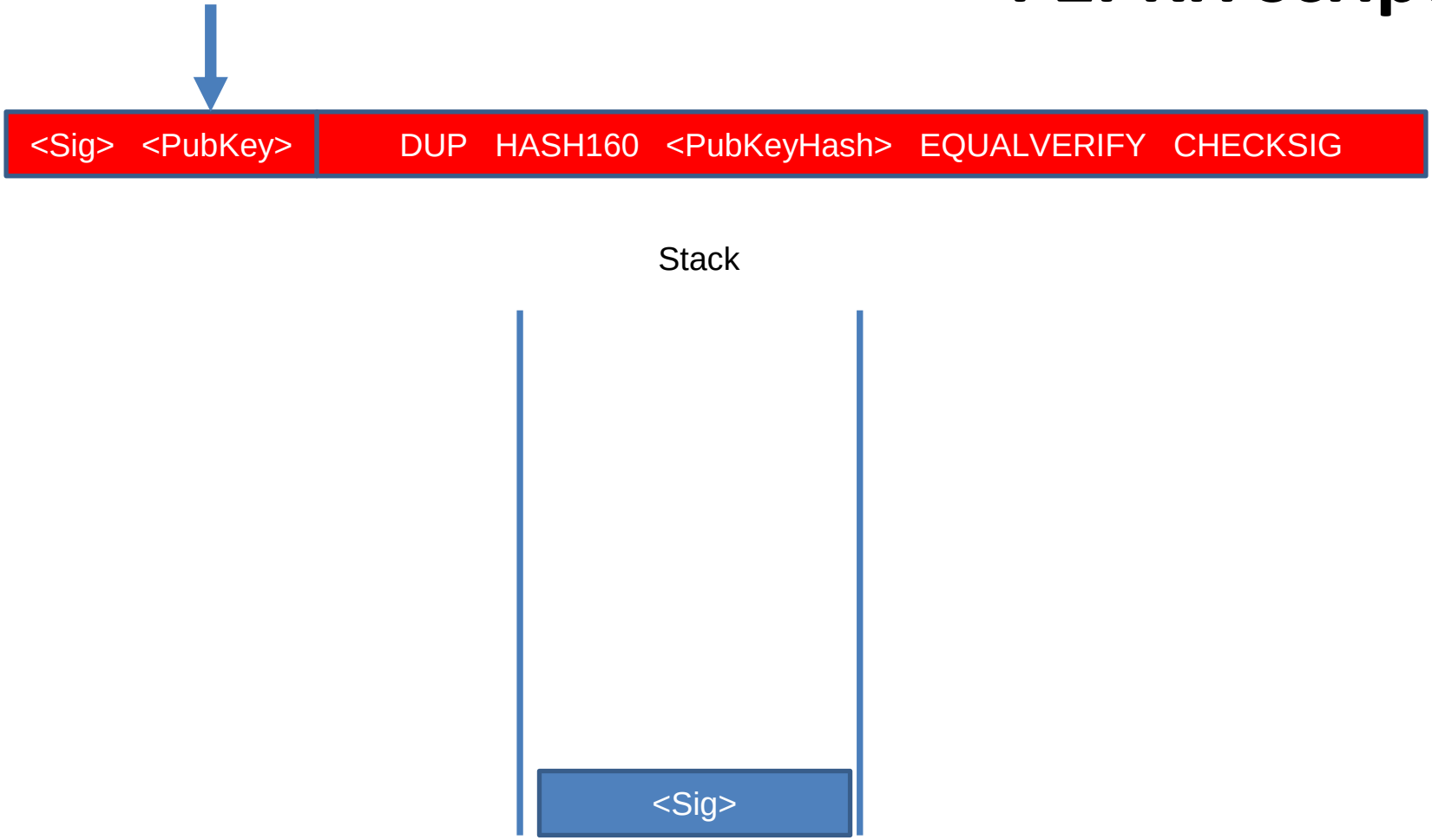
P2PKH script



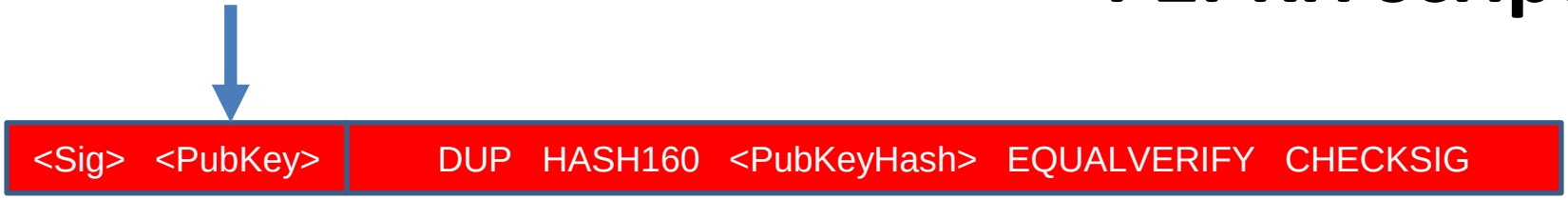
P2PKH script



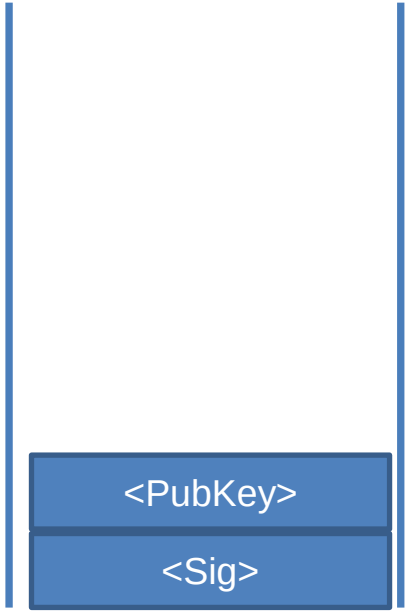
P2PKH script



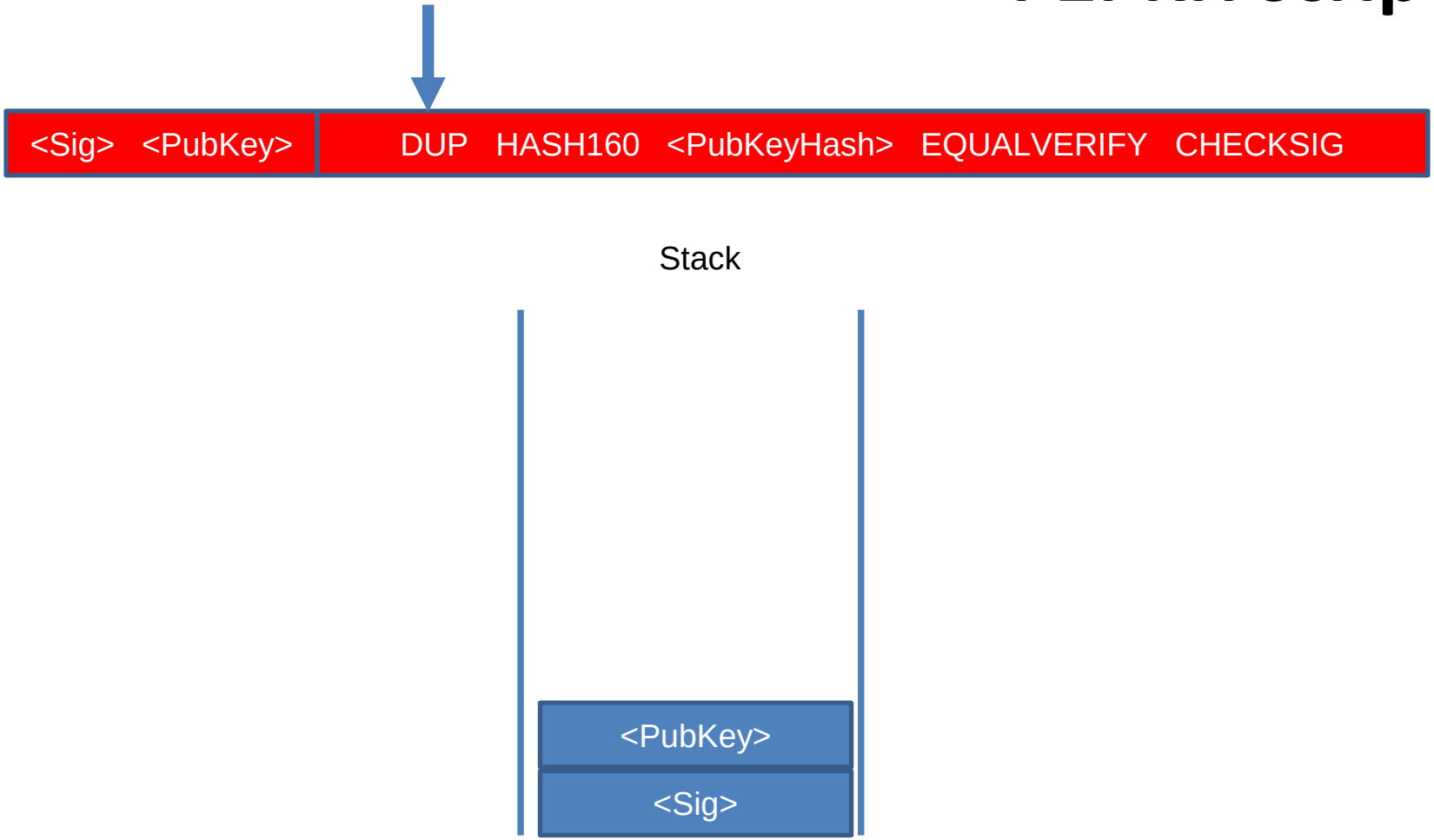
P2PKH script



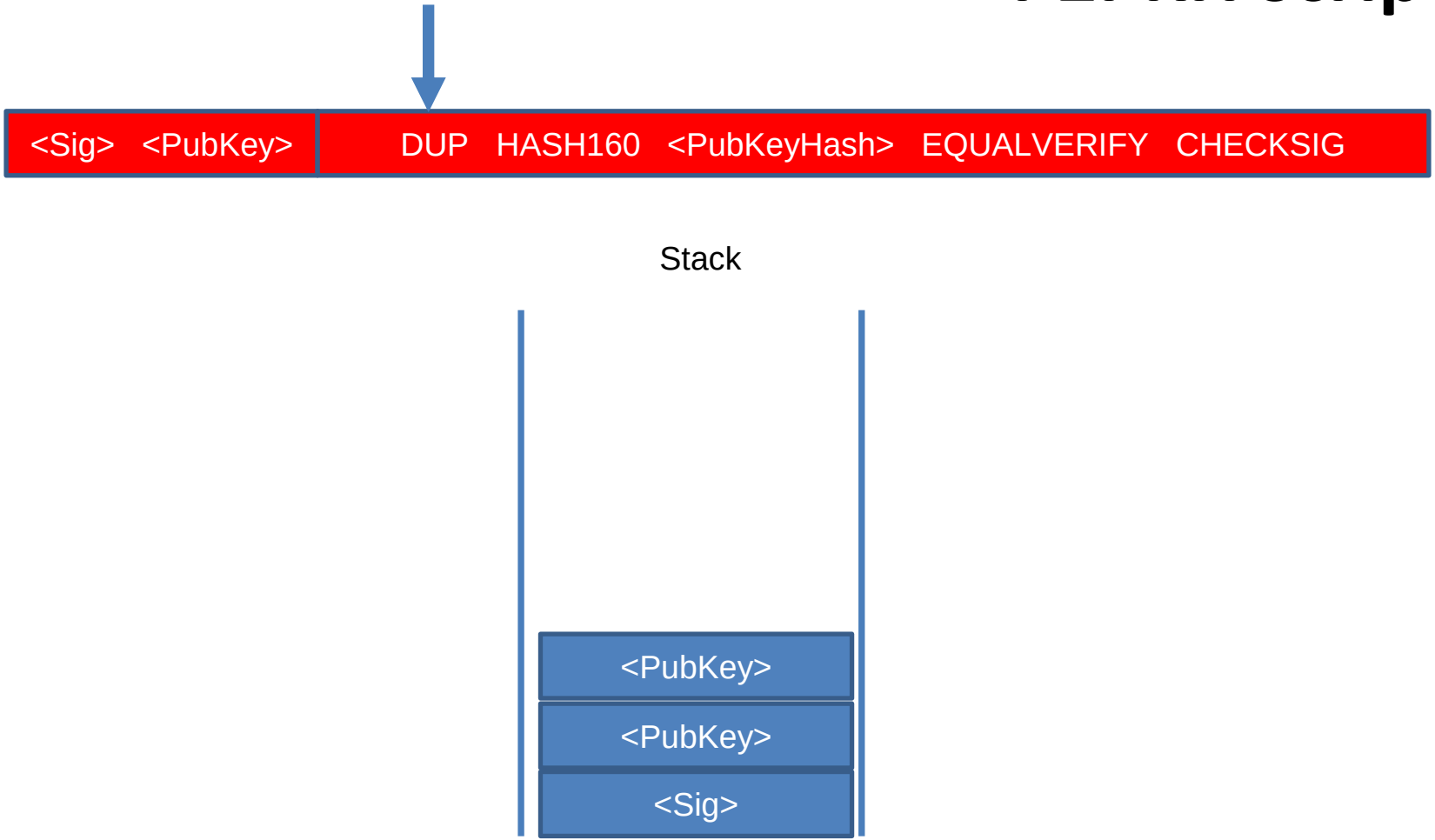
Stack



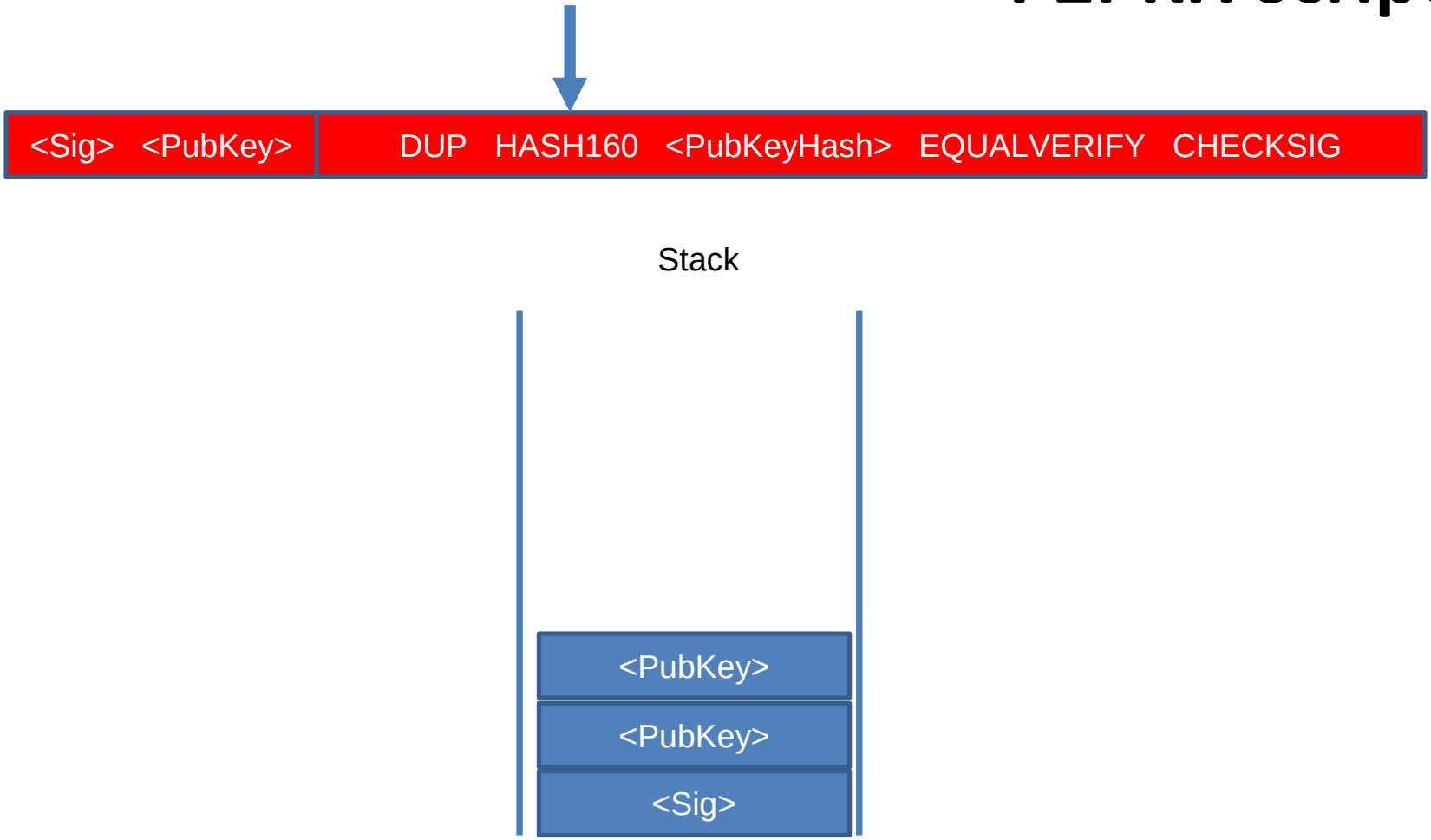
P2PKH script



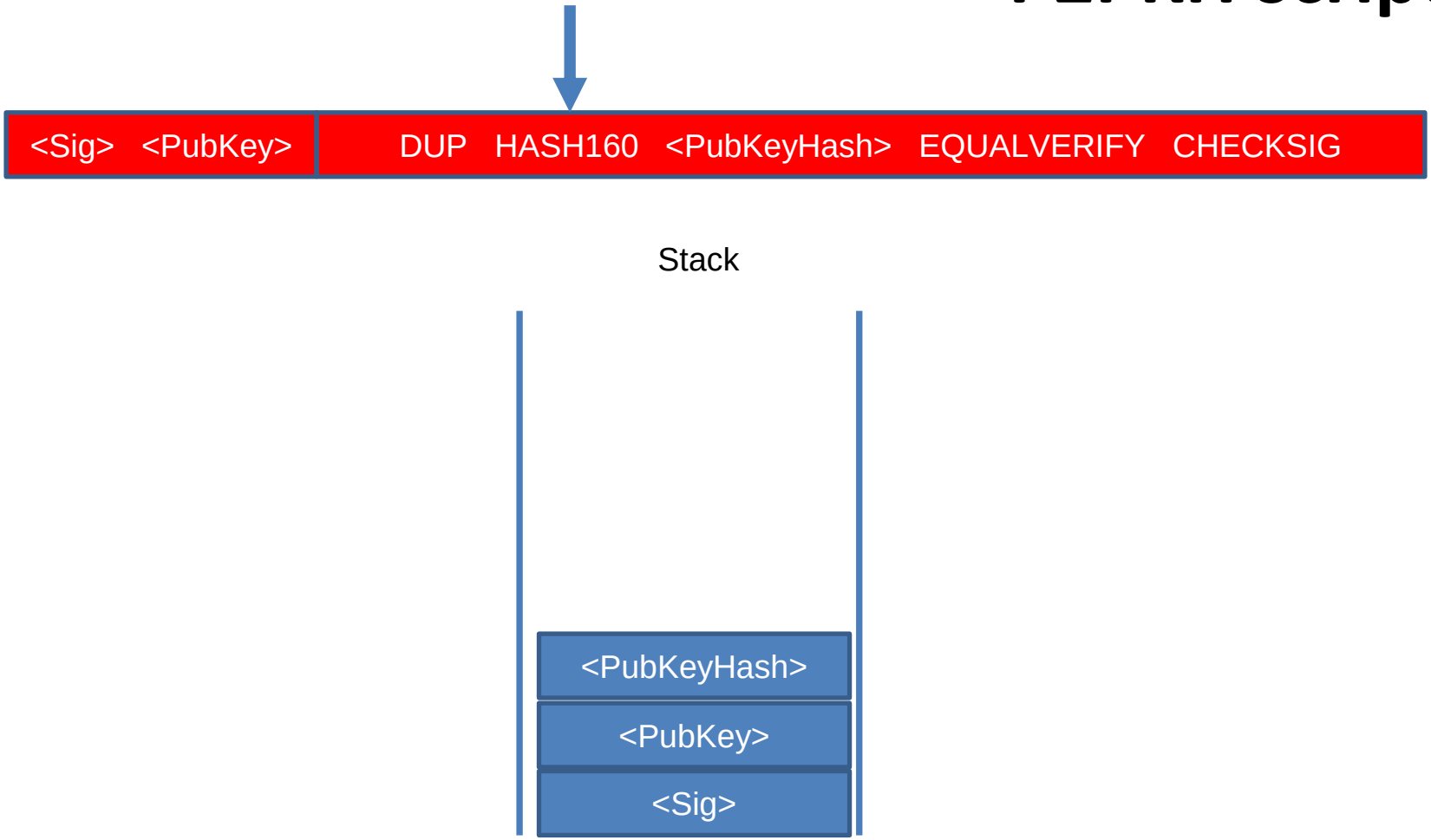
P2PKH script



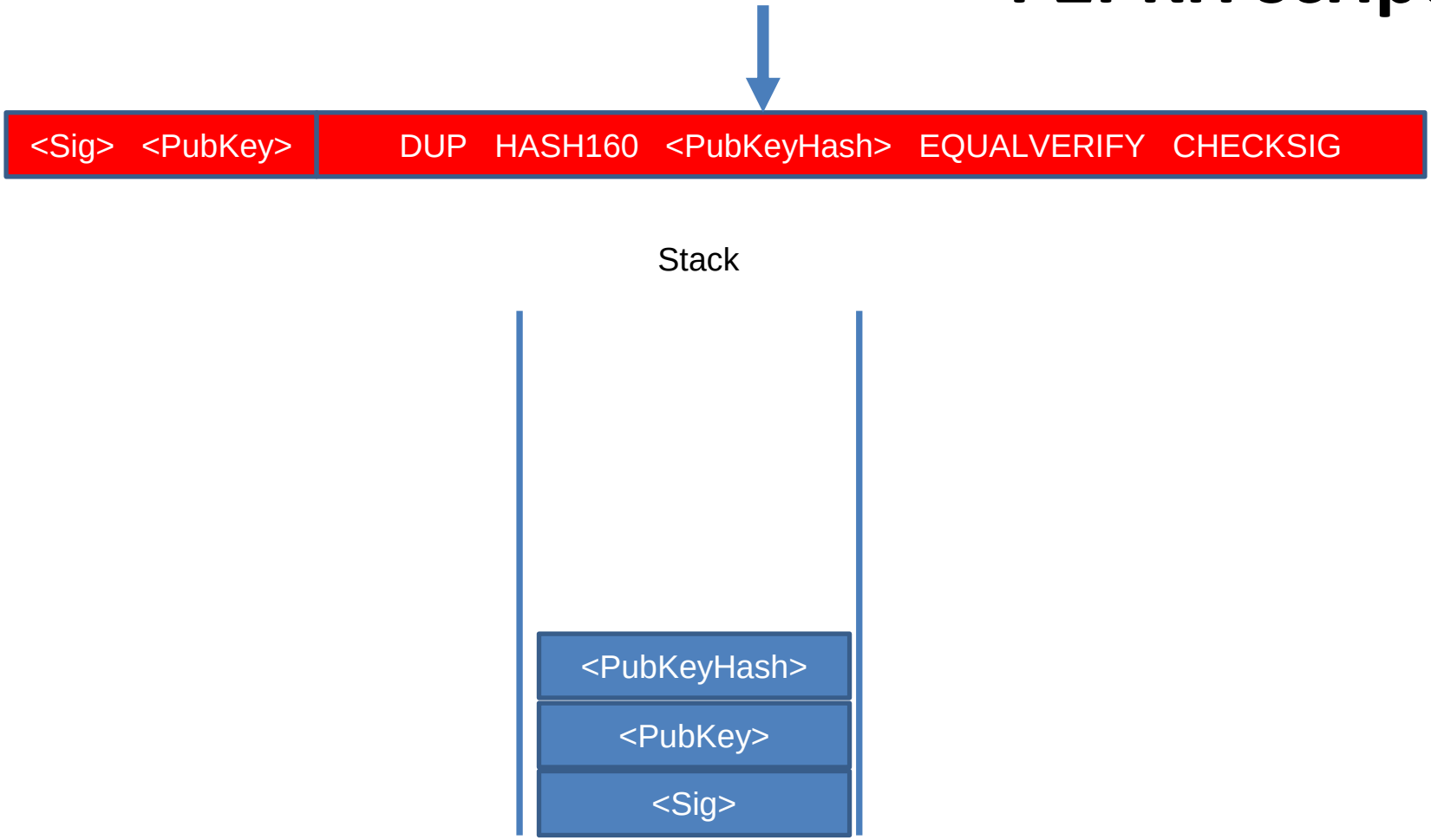
P2PKH script



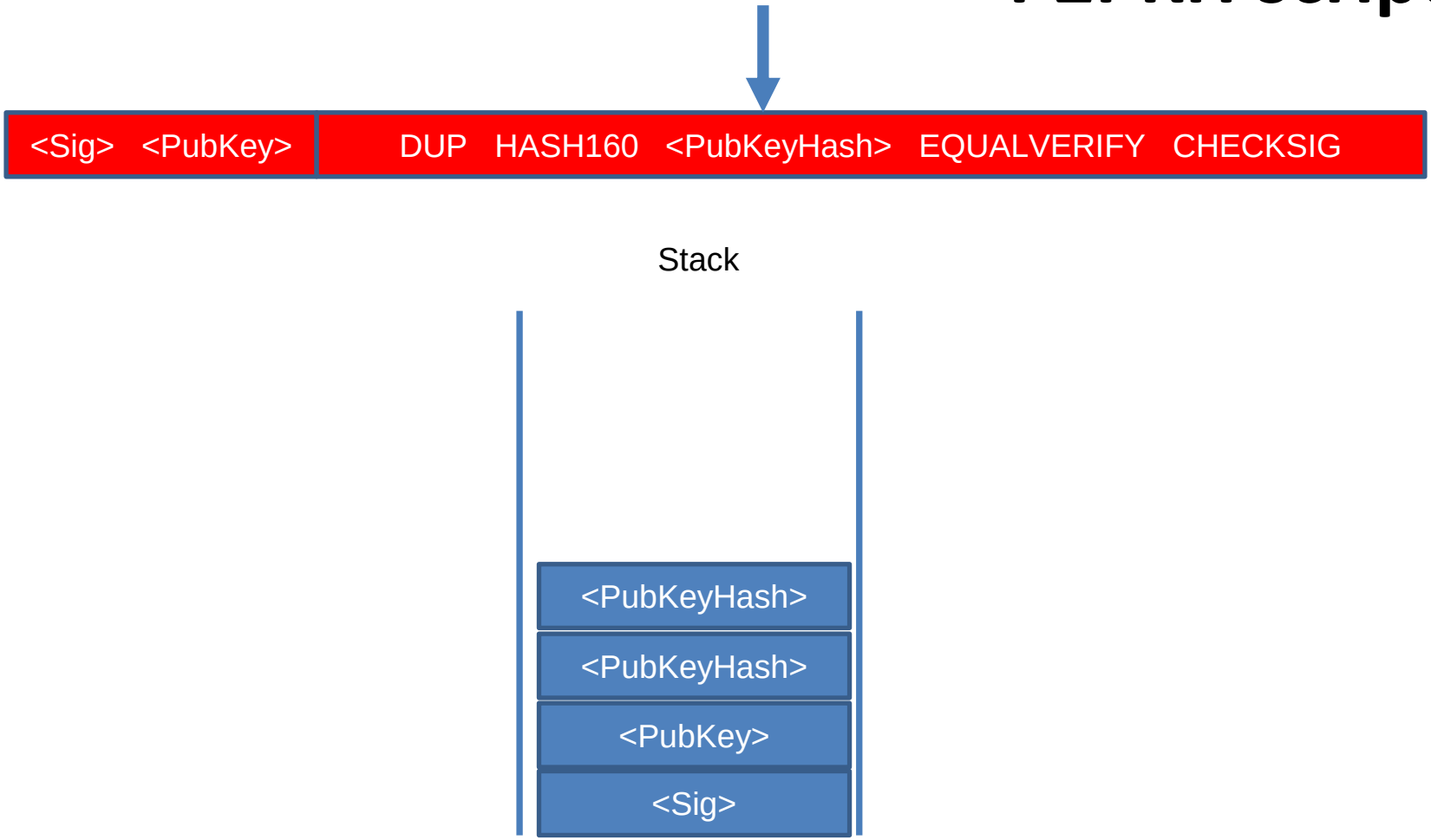
P2PKH script



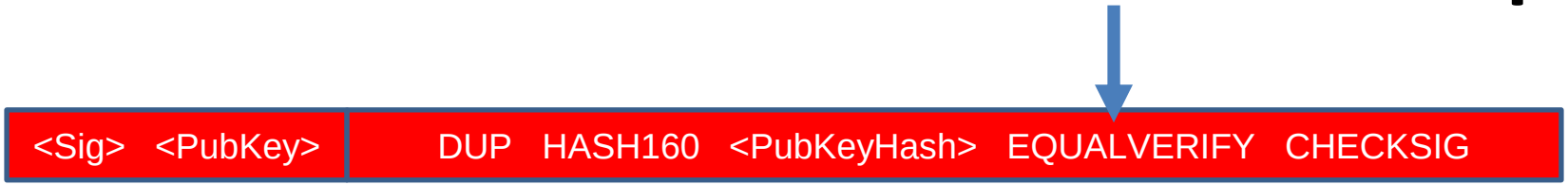
P2PKH script



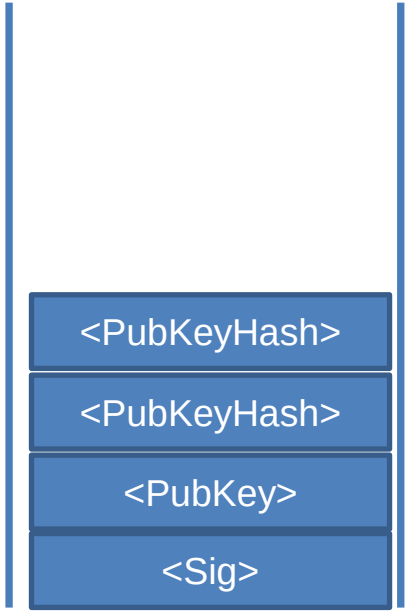
P2PKH script



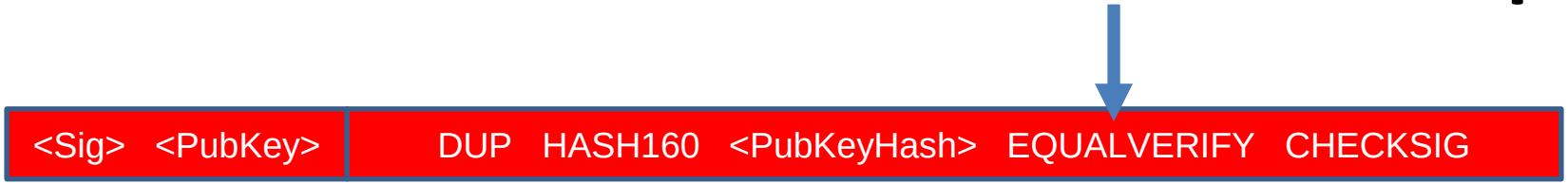
P2PKH script



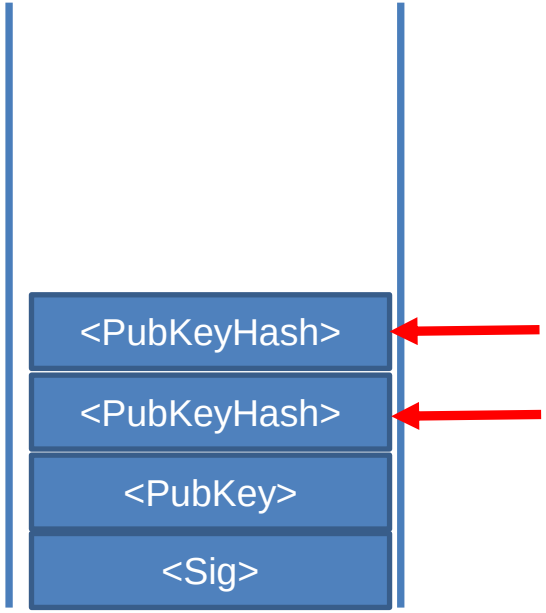
Stack



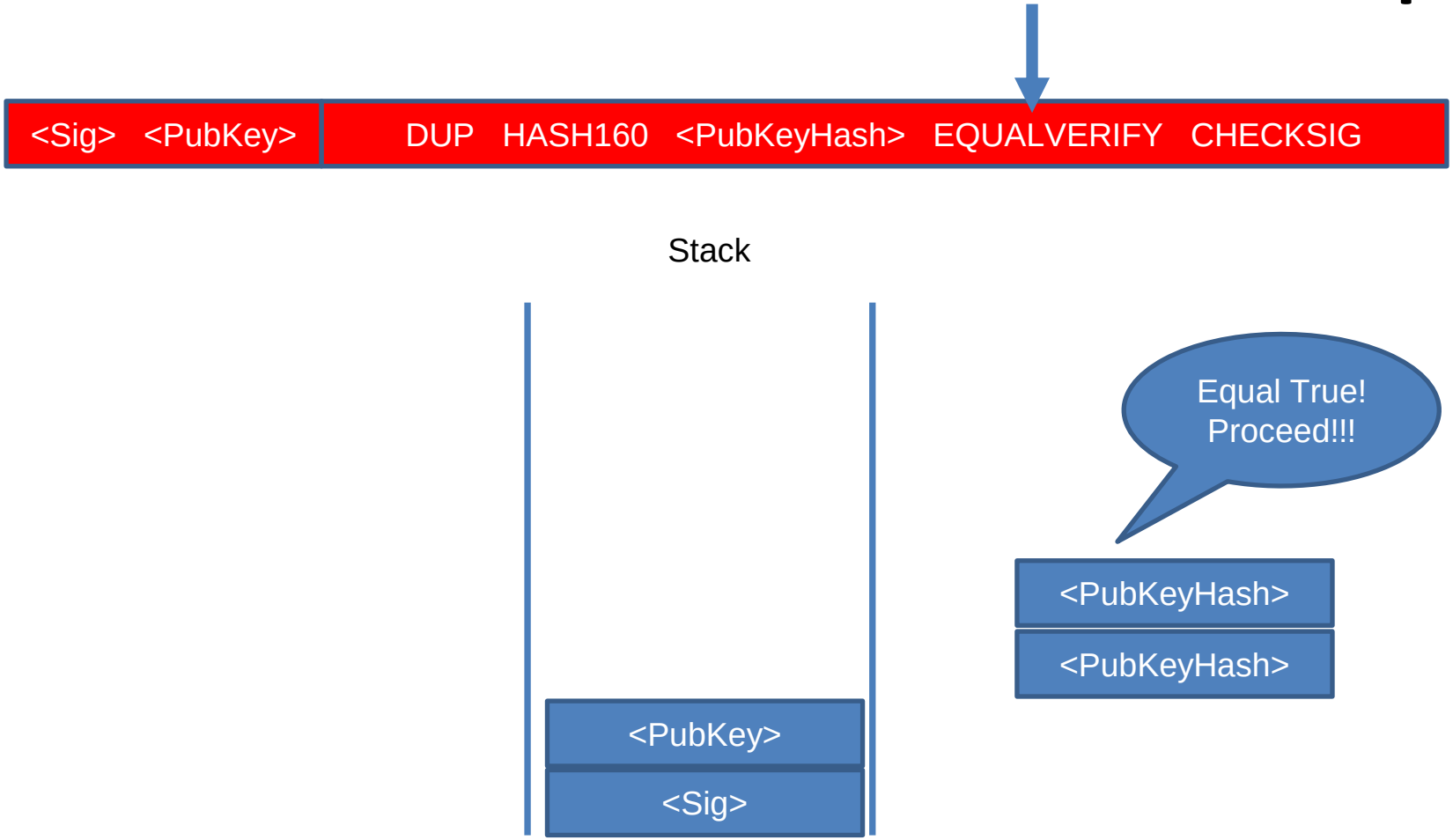
P2PKH script



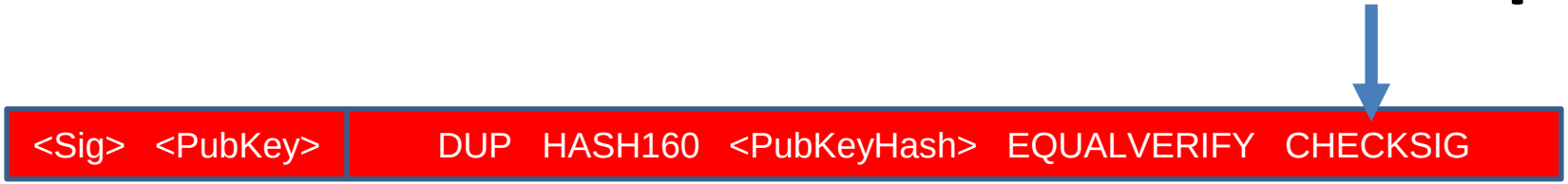
Stack



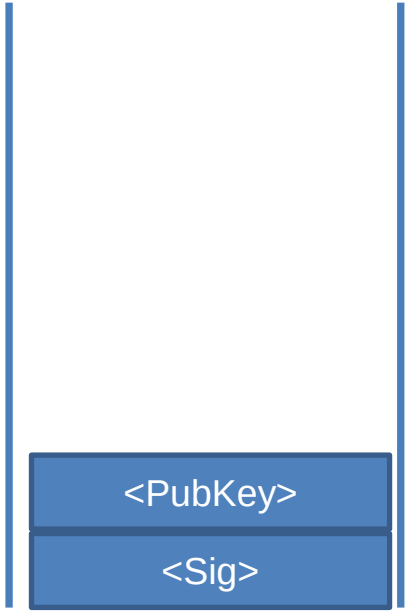
P2PKH script



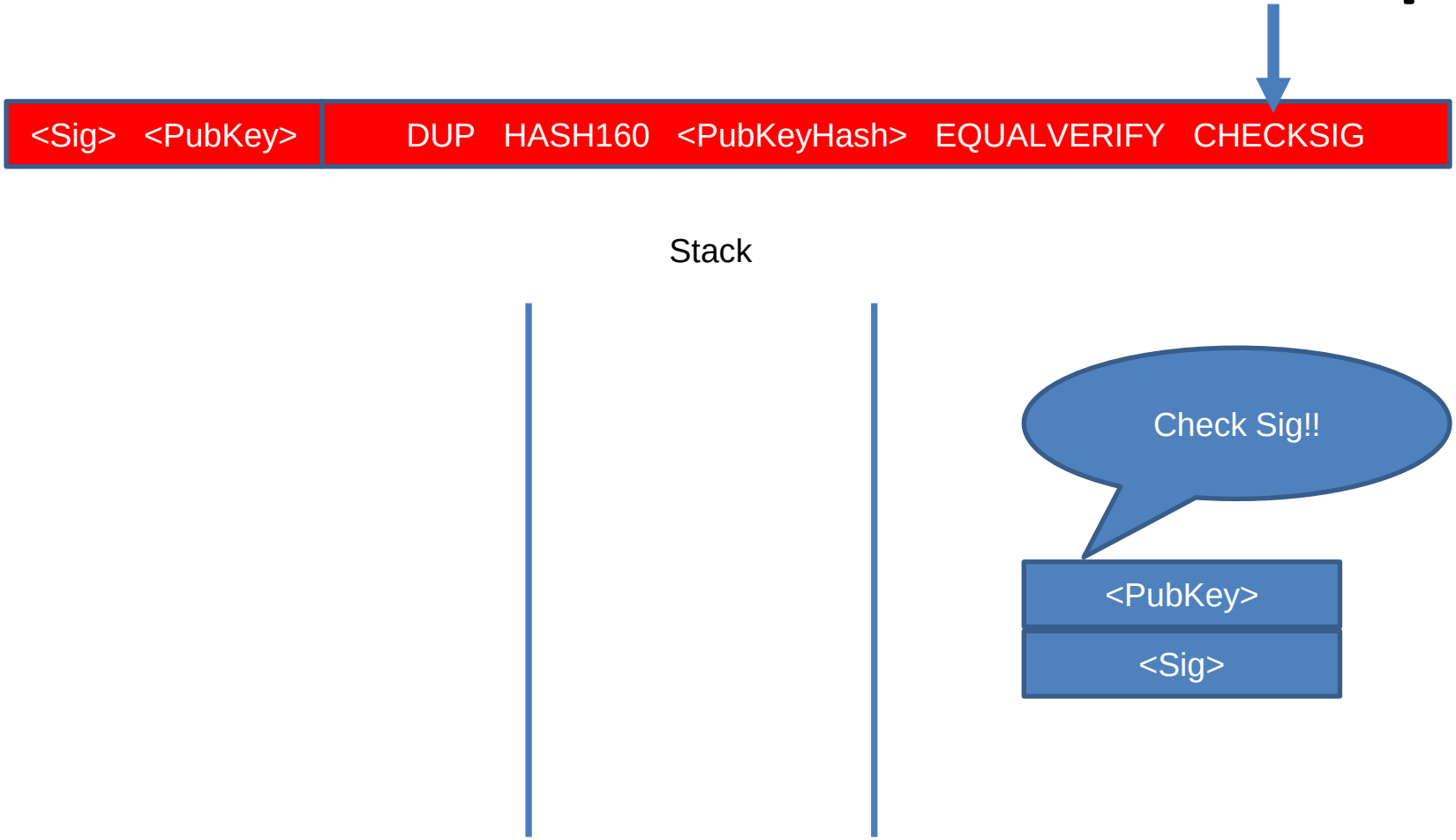
P2PKH script



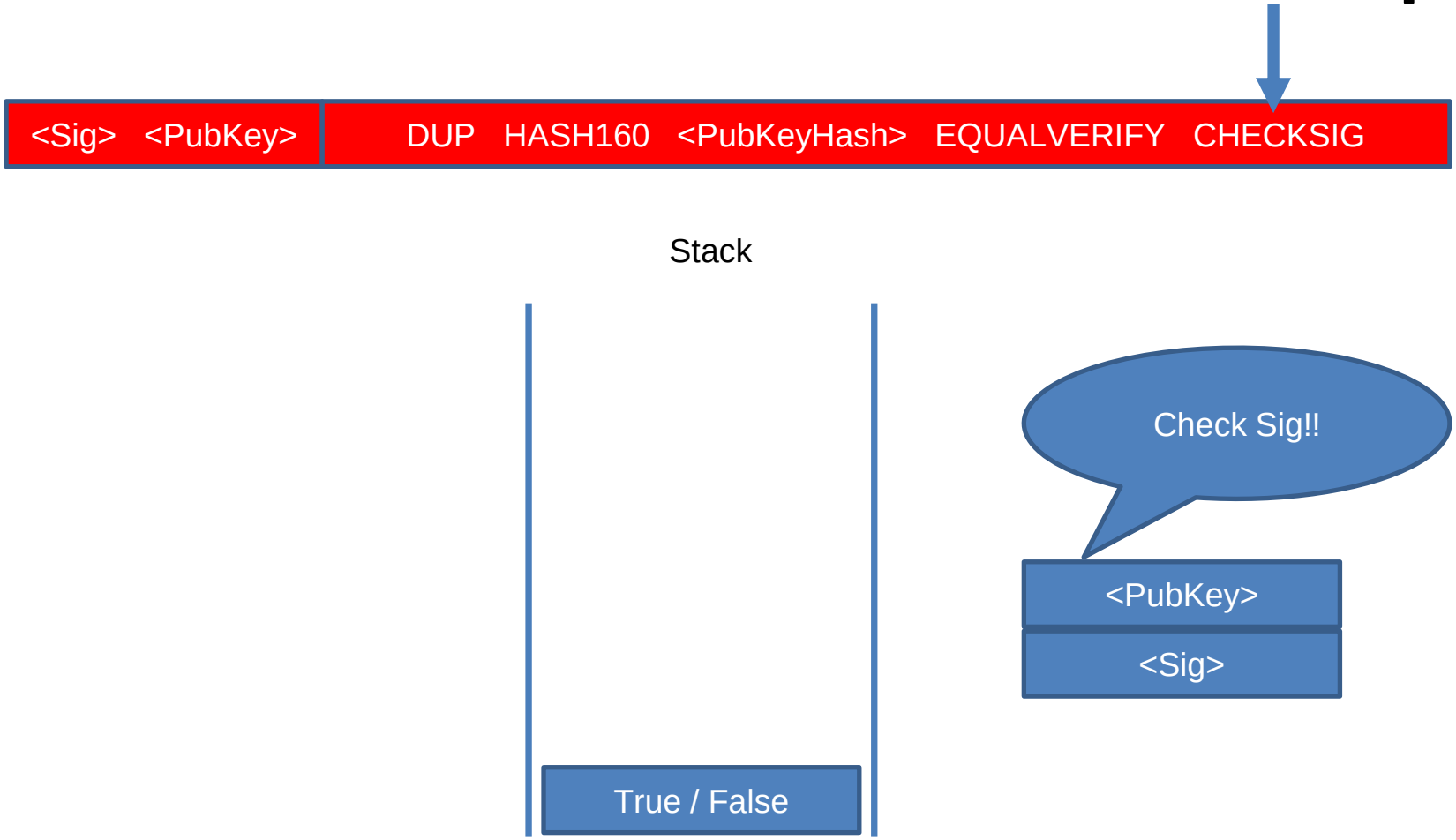
Stack



P2PKH script



P2PKH script



Script

What do we sign in sig?

- In Bitcoin you can sign only one thing: **the entire transaction**


```
{
  "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",
    }
  ]
}
```

Script

What do we sign in sig?

- In Bitcoin you can sign only one thing: **the entire transaction**


```
{
  "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",
    }
  ]
}
```

What do we sign in sig?

- In reality it is this:


```
{
  "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 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

What do I sign?

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...

Already has the signature!!!

What do I sign?

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...

I leave it empty and sign this.

ScriptSig, ScriptPubKey

Where does the name come from?

A basic transaction

- Pay 1 BTC to X

In reality:

- This creates an output that says
- ‘’This output can be spent by provinding a signature of X"

X is a public key

ScriptSig, ScriptPubKey

Where does the name come from?

A basic transaction

- Pay 1 BTC to X

In reality:

- ‘’This output can be spent by provinding a signature of X"

X is a public key

The majority of coinbase transactions made by Satoshi are like this

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",
        }
    ]
}
```

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"
            }

    ]
}
```



```
{
    "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",
        }
    ]
}
```


<Sig>

<PubKey>

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",
        }
    ]
}
```


<Sig>

<PubKey>
OP_CHECKSIG

A real transaction

P2PK is not in use any more:

- For privacy reasons
- And really because it weight a lot (many bytes)

  (originally uncompressed SEC == 65 bytes contra 20 bytes of P2PKH)

Script

P2PKH script:

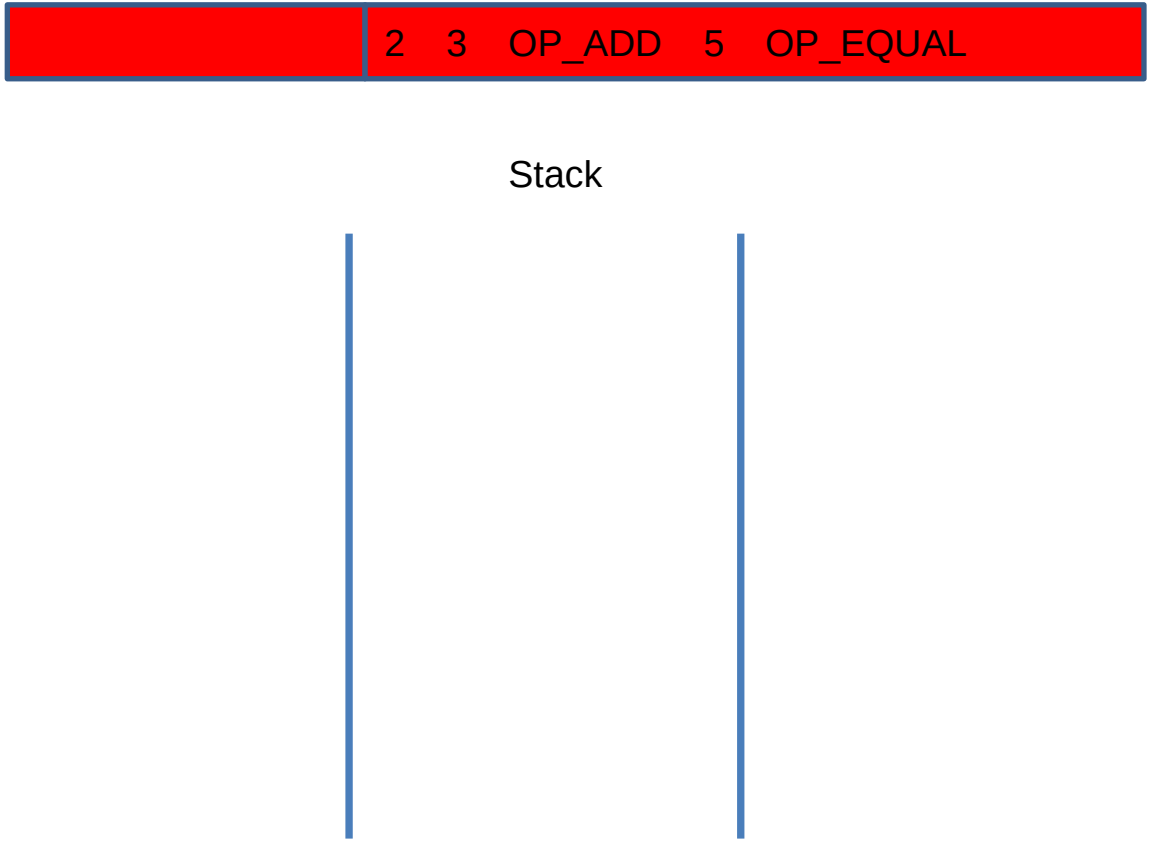
- More than 90% of all the transactions

But scripts can be very different:

2 3 OP_ADD 5 OP_EQUAL

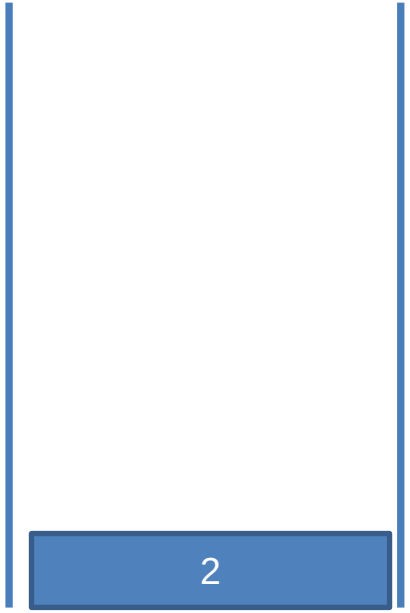
What happens if this is my locking script?

Script



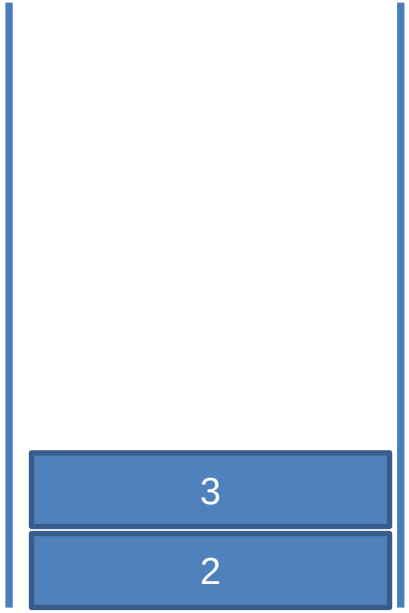
Script

Stack

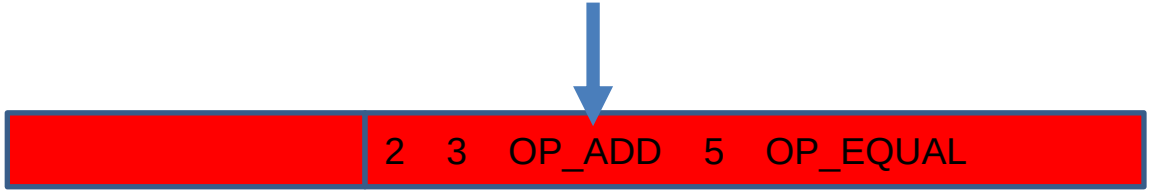


Script

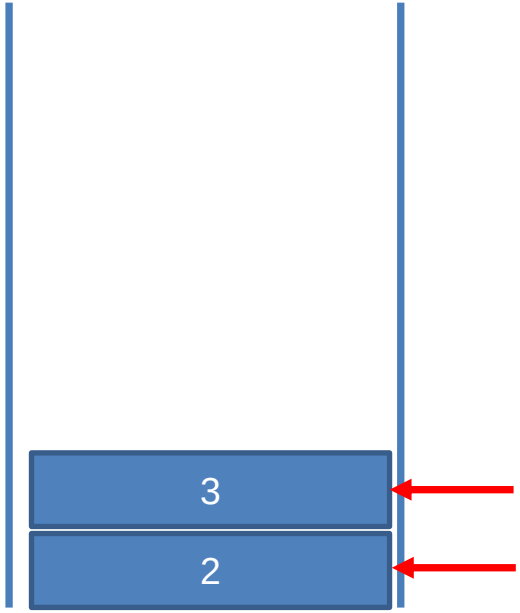
Stack



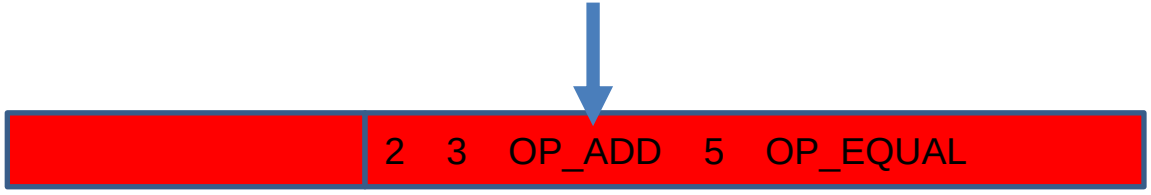
Script



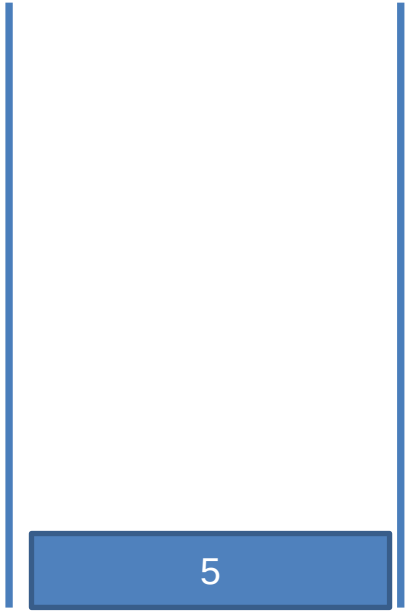
Stack



Script

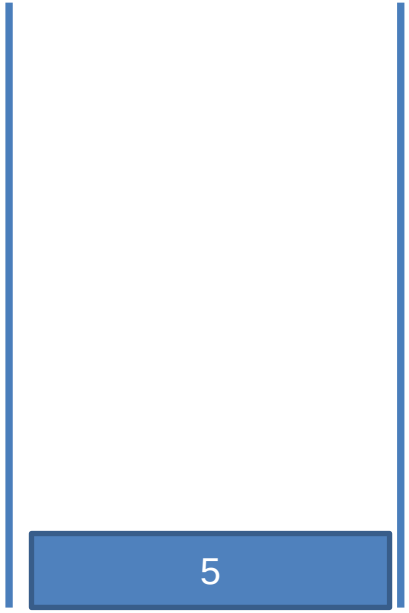


Stack

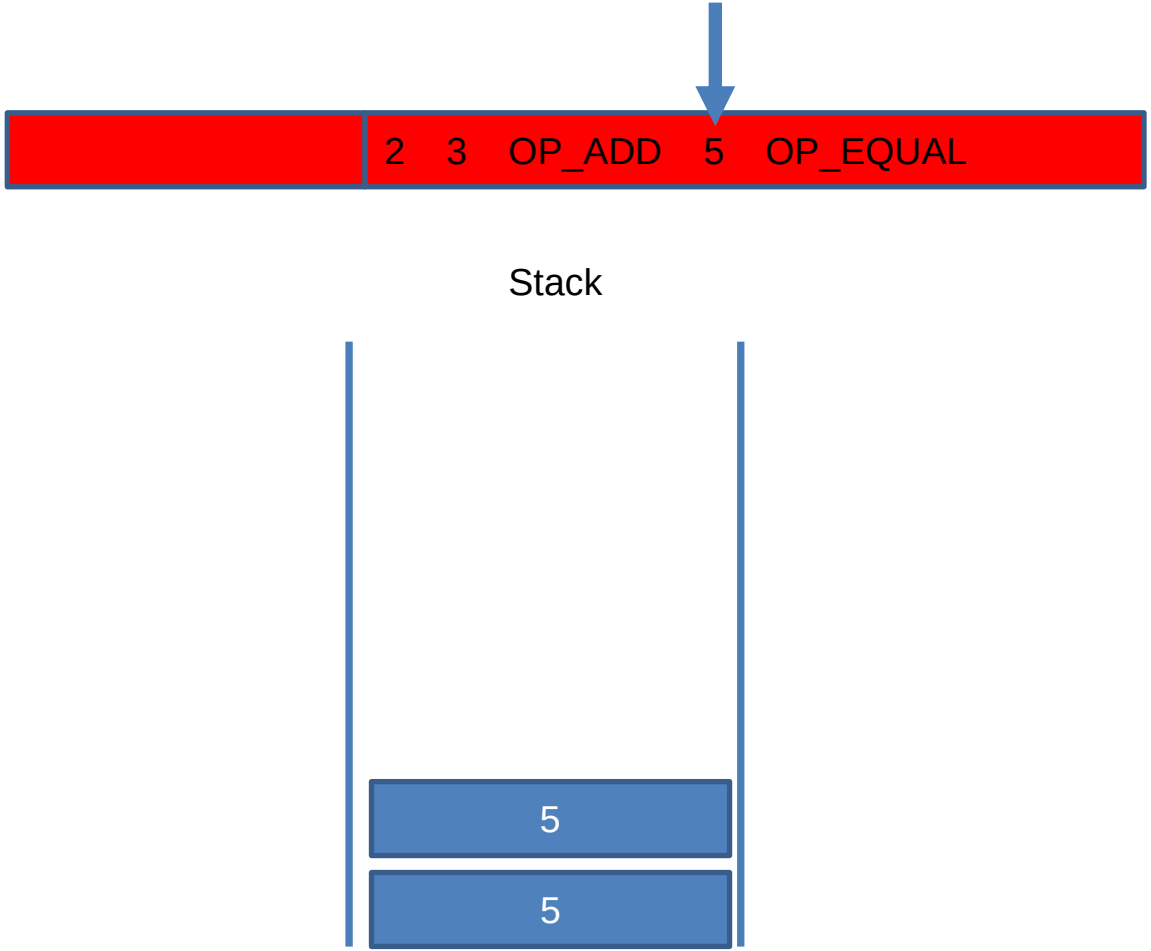


Script

Stack

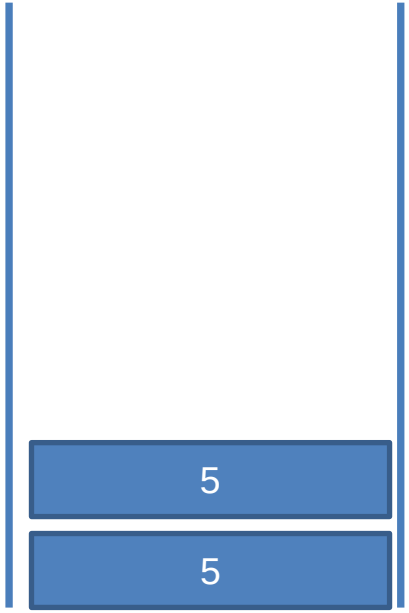


Script

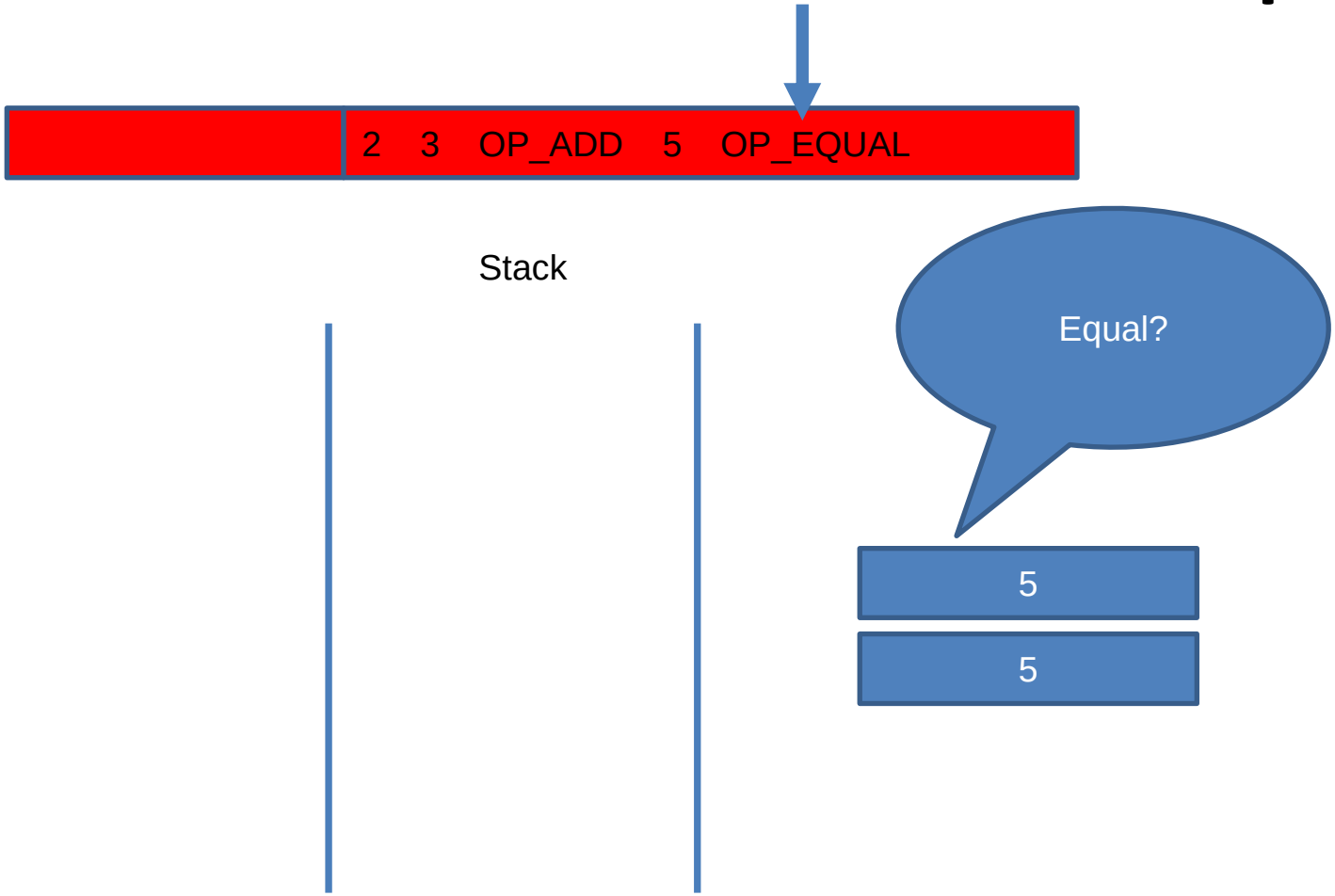


Script

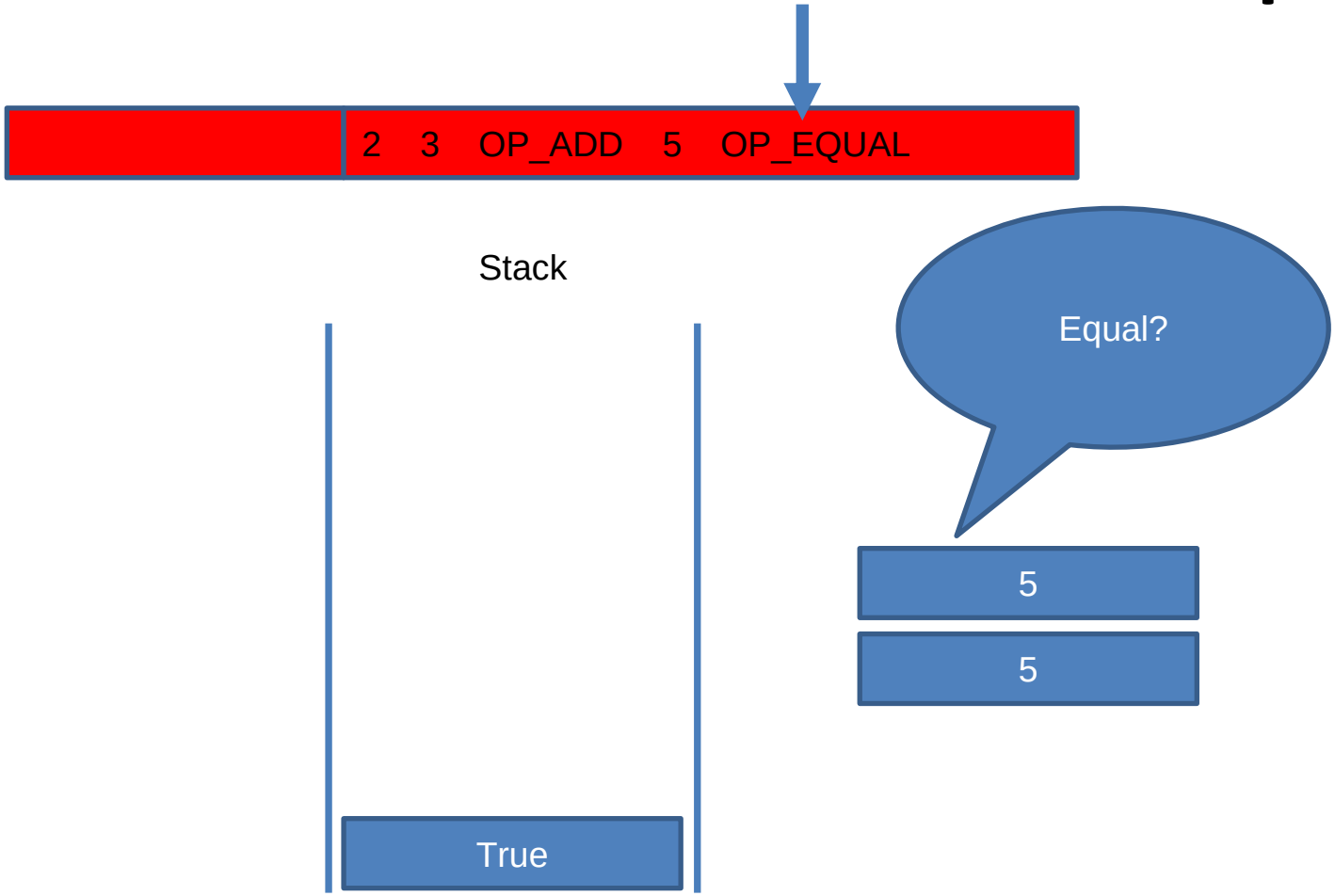
Stack



Script



Script



Coinbase


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "coinbase": "03323b04040001bb1844124d696e6564206279204254432047756 96c642cfabe6d6d1e910cc21520338a2e
            a55b3ad96e37206a19ab19bc28664cca85697f26ed1b0100000000000000000800134cd50000066c",
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 25.00526000,
            "n": 0,
            "scriptPubKey": "OP_DUP OP_HASH160 27a1f12771de5cc3b73941664b2537c15316be43 OP_EQUALVERIFY OP_CHECKSIG"
        }
    ]
}
```

Coinbase

extra nonce

block reward + transaction fee


```
{
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "coinbase": "03323b04040001bb1844124d696e6564206279204254432047756 96c642cfabe6d6d1e910cc21520338a2e
            a55b3ad96e37206a19ab19bc28664cca85697f26ed1b0100000000000000000800134cd50000066c",
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 25.00526000,
            "n": 0,
            "scriptPubKey": "OP_DUP OP_HASH160 27a1f12771de5cc3b73941664b2537c15316be43 OP_EQUALVERIFY OP_CHECKSIG"
        }
    ]
}
```

Tracking transactions

https://www.blockchain.com/en/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

https://blockchain.info/tx/b657e22827039461a9493ede7bdf55b01579254c1630b0bfc9185ec564fc05ab?format=json

Advanced scripting

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.

Multisig

Multisig locking script:

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

Multisig

Multisig locking script:

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

For example

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
                044f09a164267c635c6991f7a96bc7901d035c07161a0074d719be723f6a9c50bc72b900092cffec
                5f3c3484dae35d04a5a2fa2e75f3a99e17577537c1227b44ba
                04971e5b8b222fe47f742fa07d3327d36a6cd37088656ce29842ed82e1dc8bffaa81848b3219359f
                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>

Multisig

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>

MSIG

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	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

MSIG

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	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>

MSIG

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	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

MSIG

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

tx: 0x20ff1…

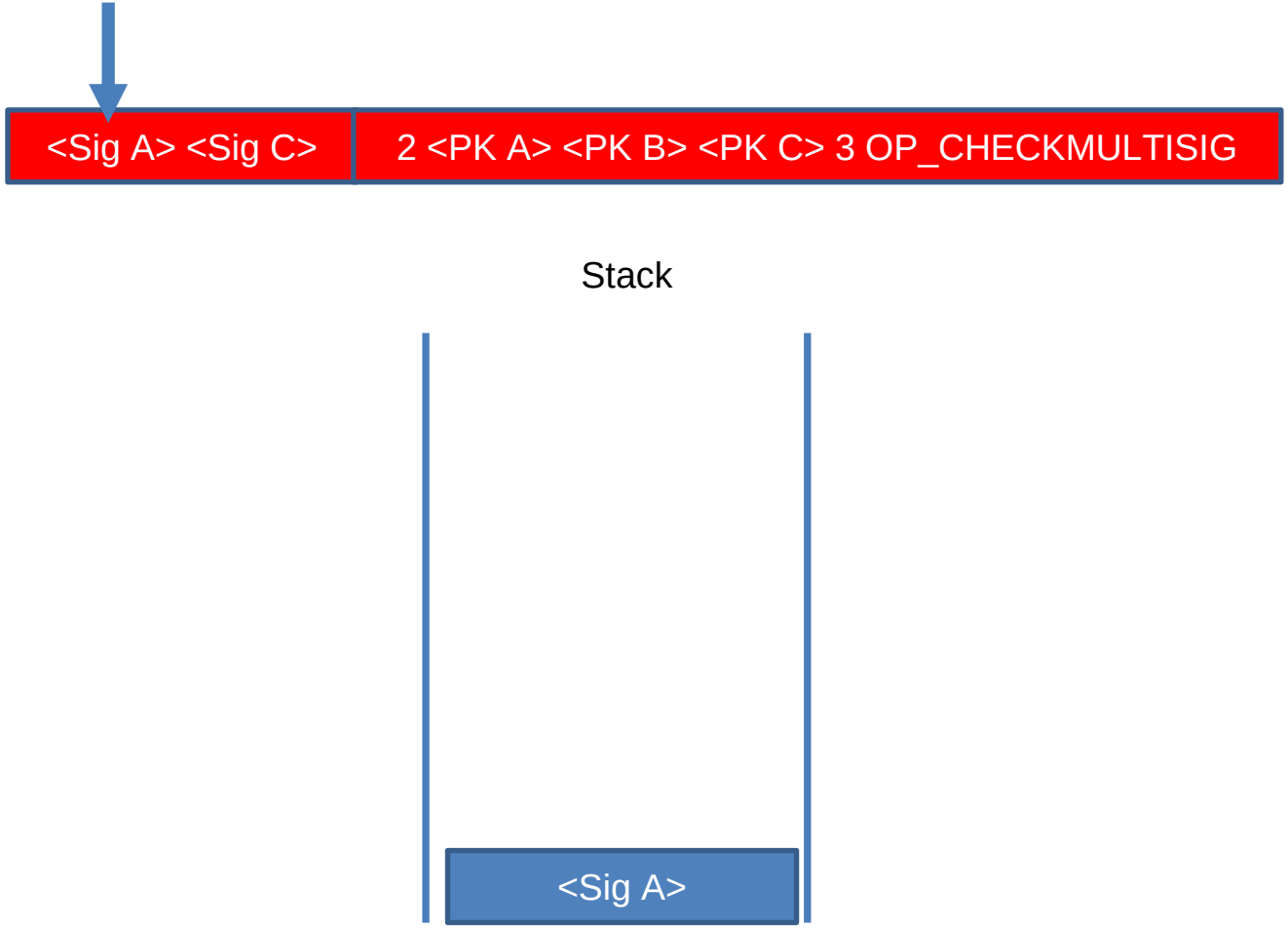
Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff…	1	<Sig A> <Sig C>

Outputs		
num	value	Locking script

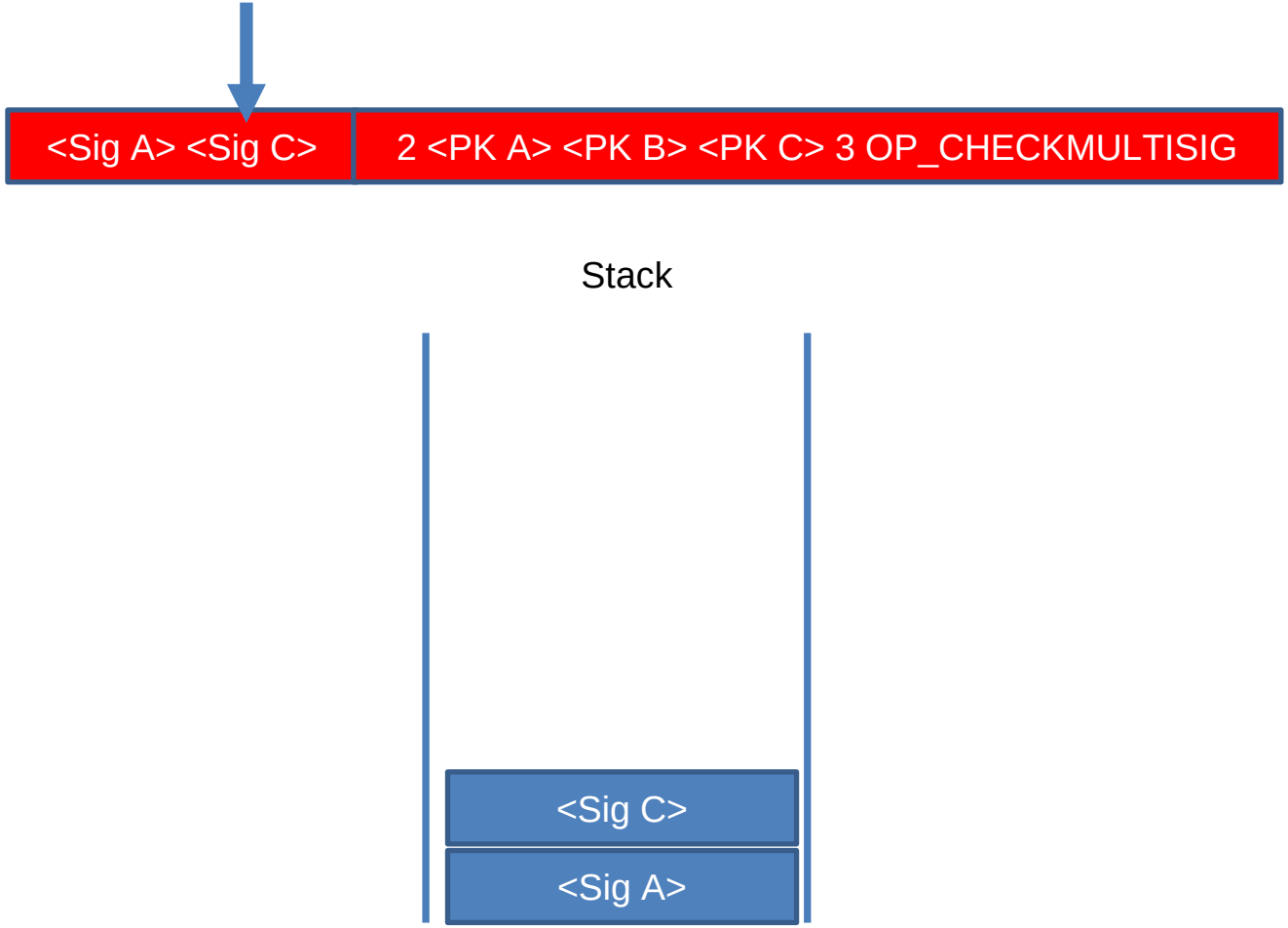
<Sig A> <Sig C>	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

run this

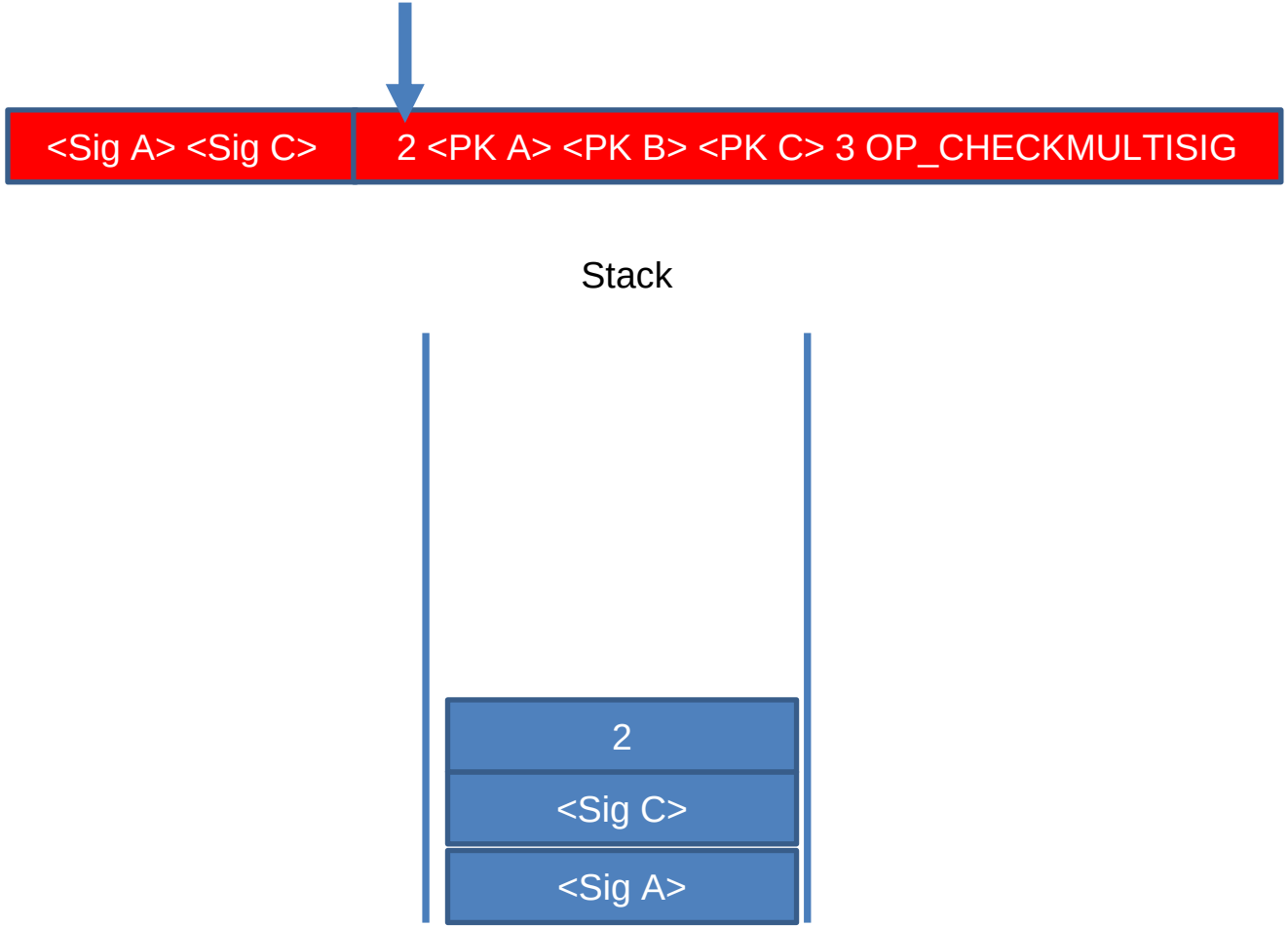
Multisig



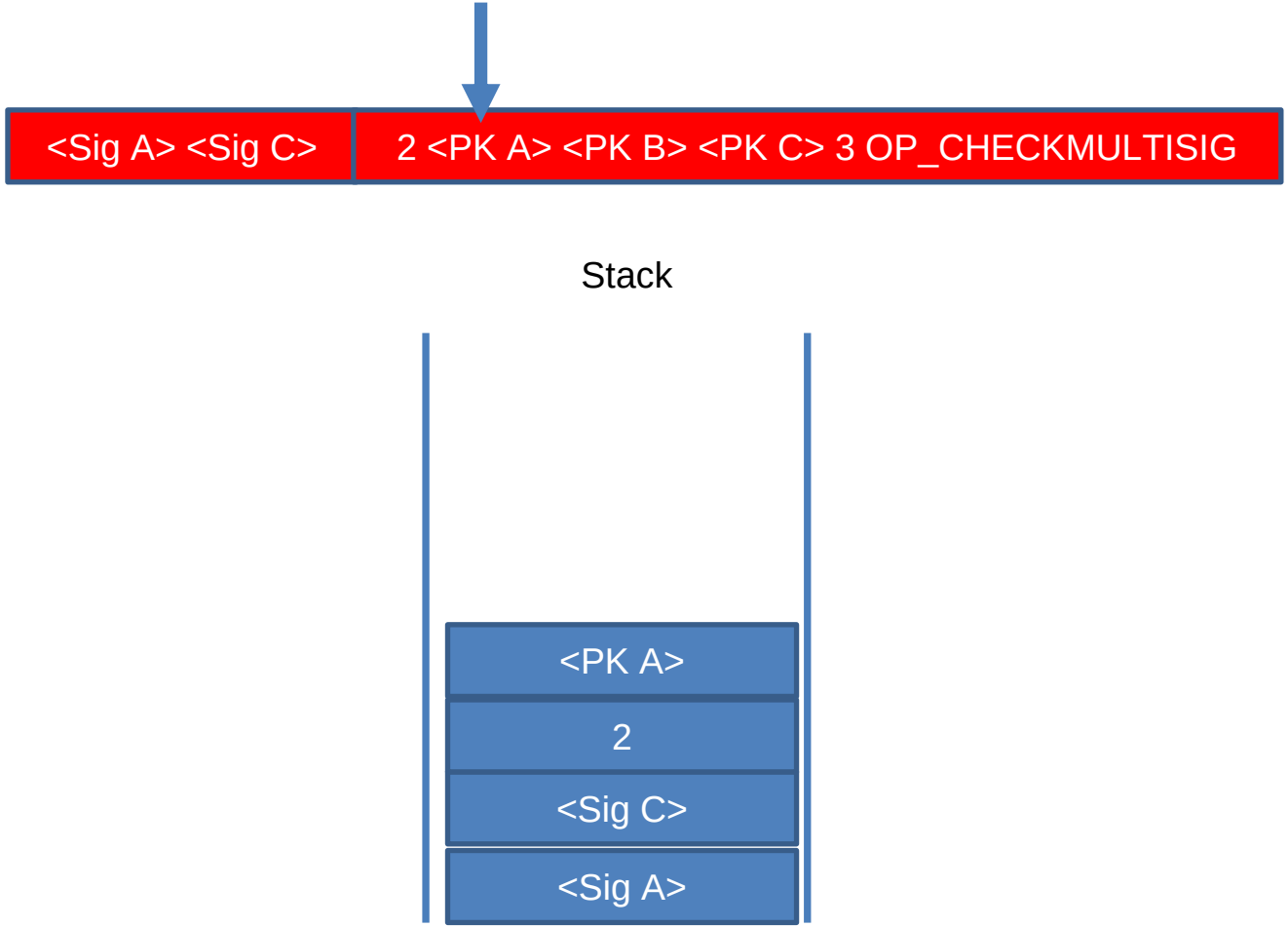
Multisig



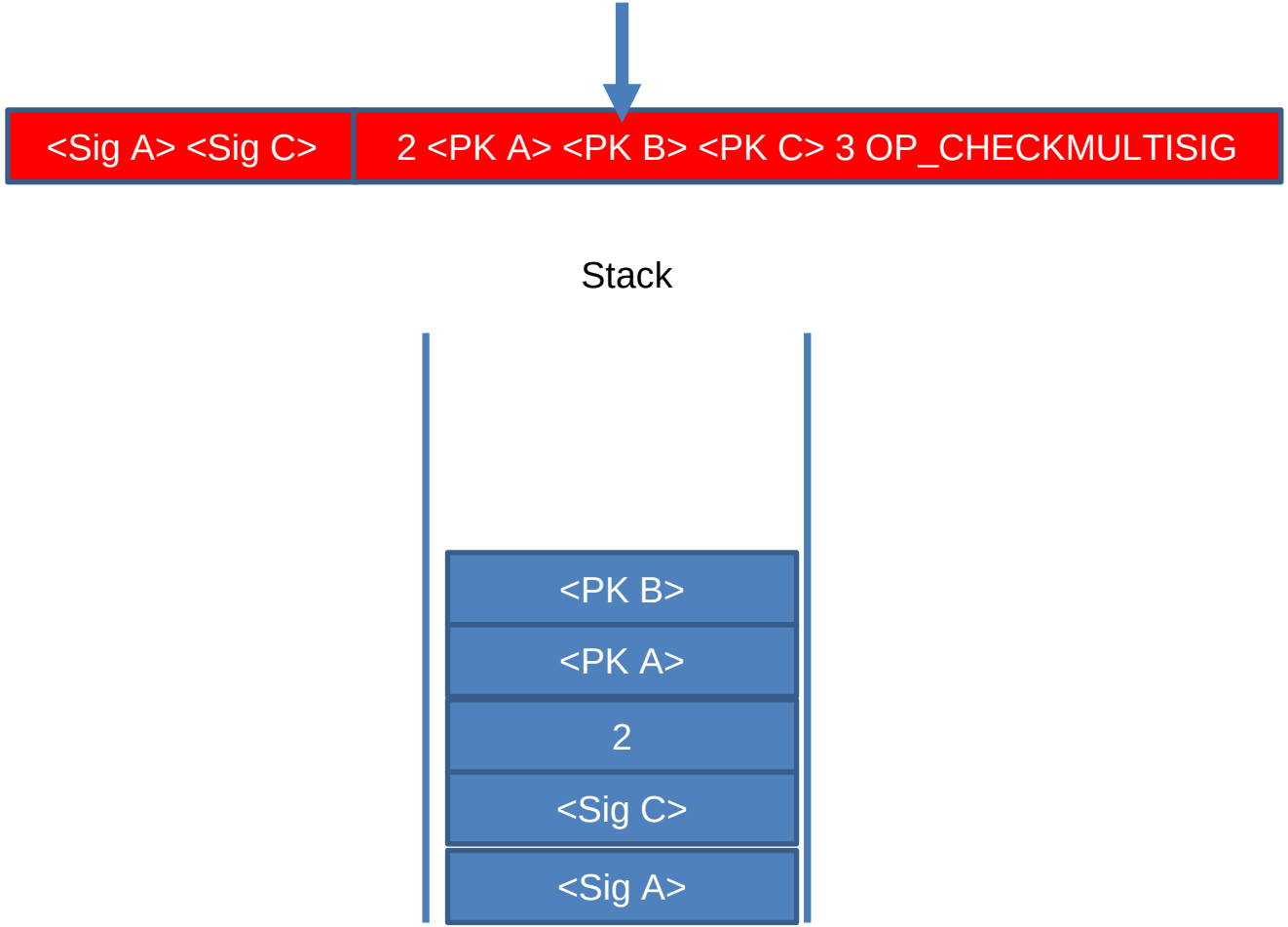
Multisig



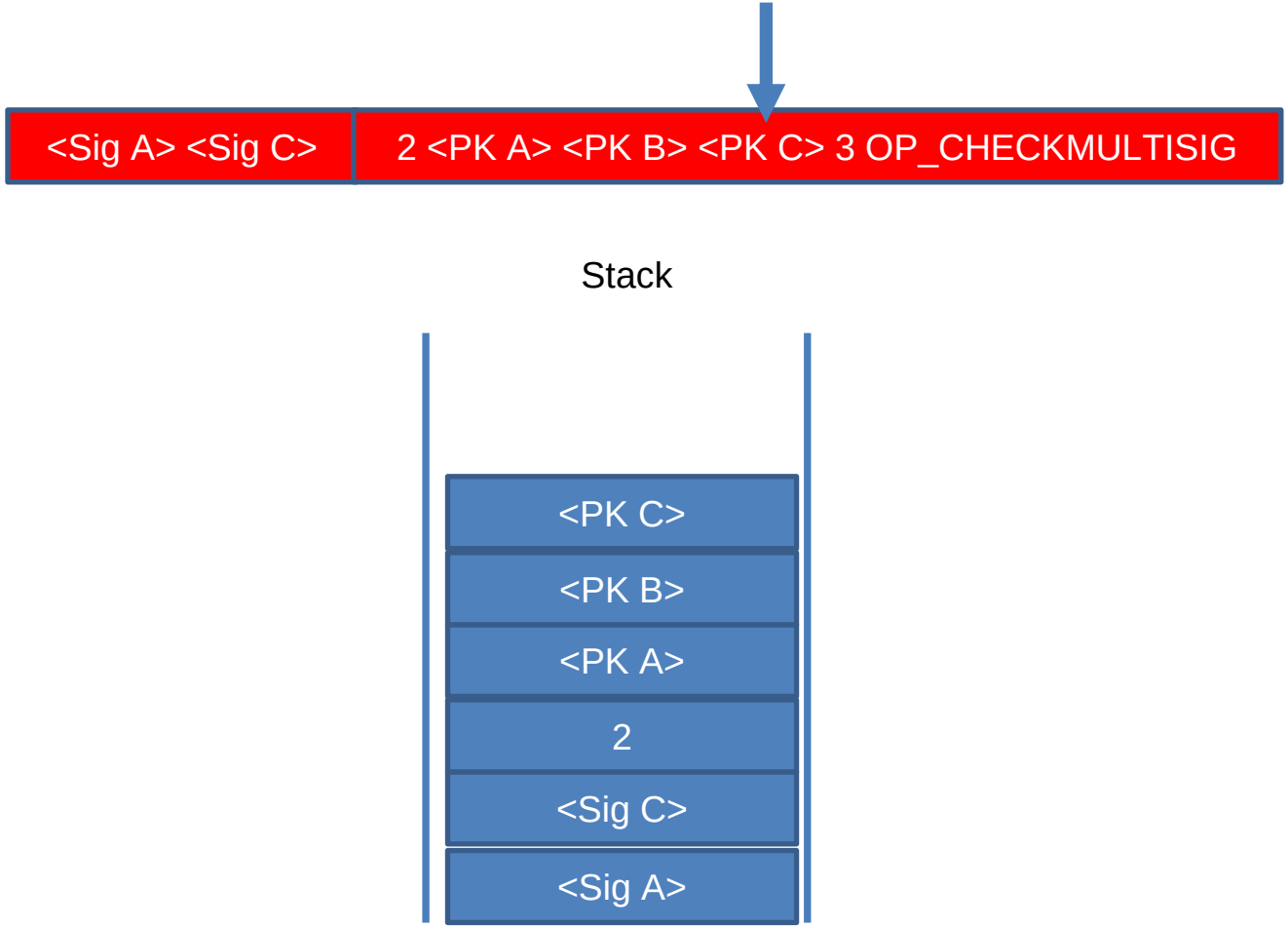
Multisig


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

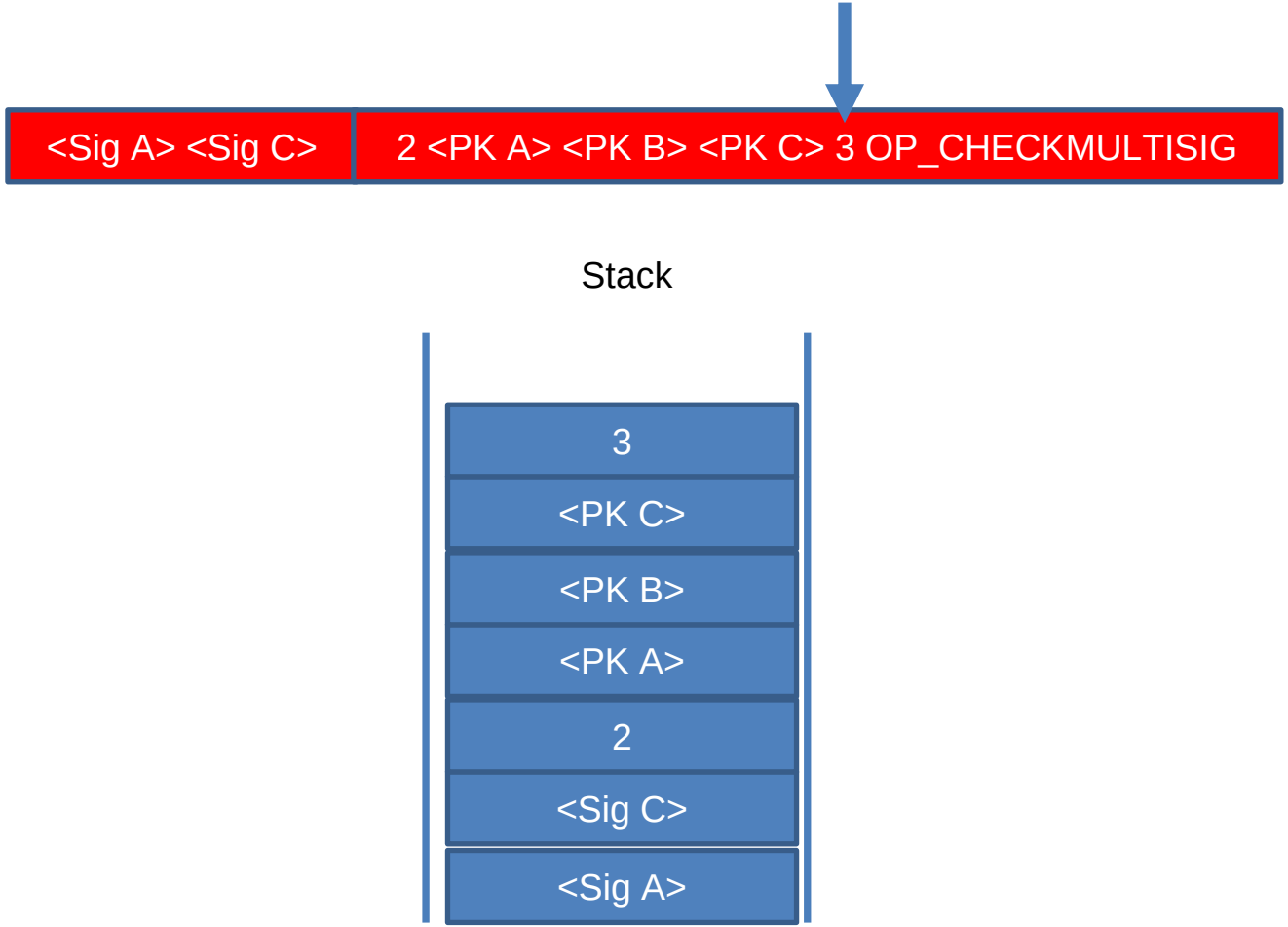
Multisig


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

Multisig


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

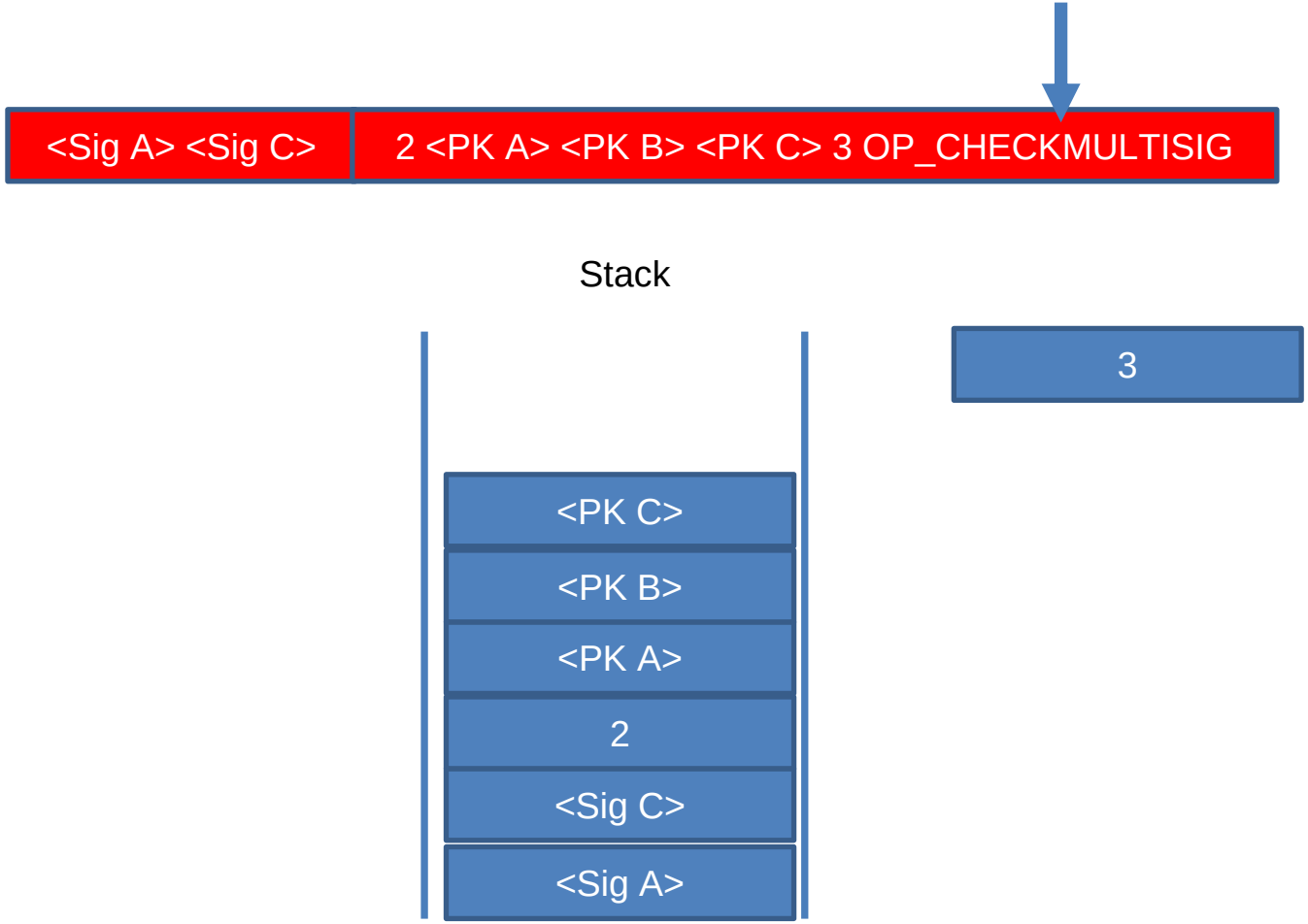
Multisig


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

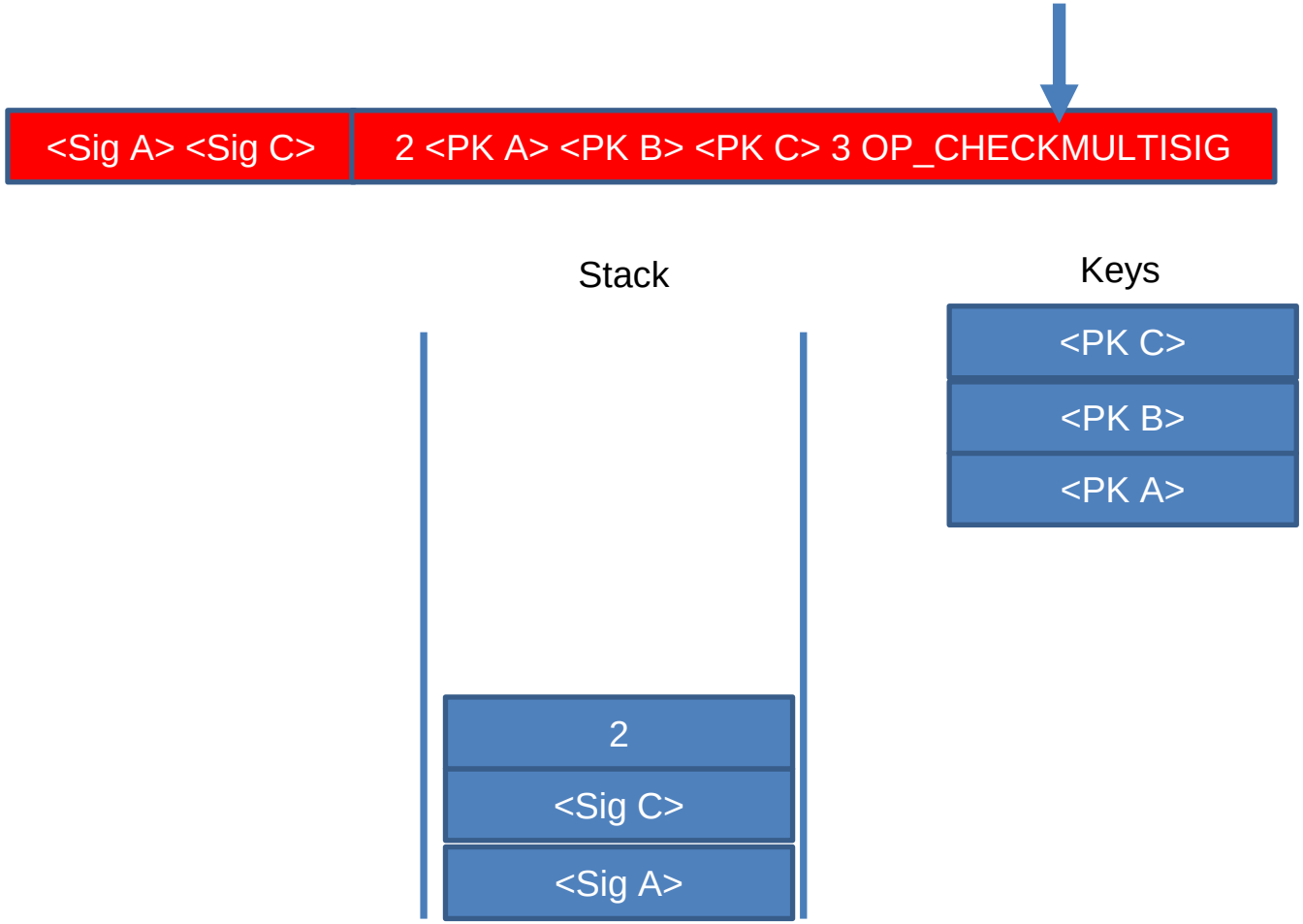
Multisig

Stack

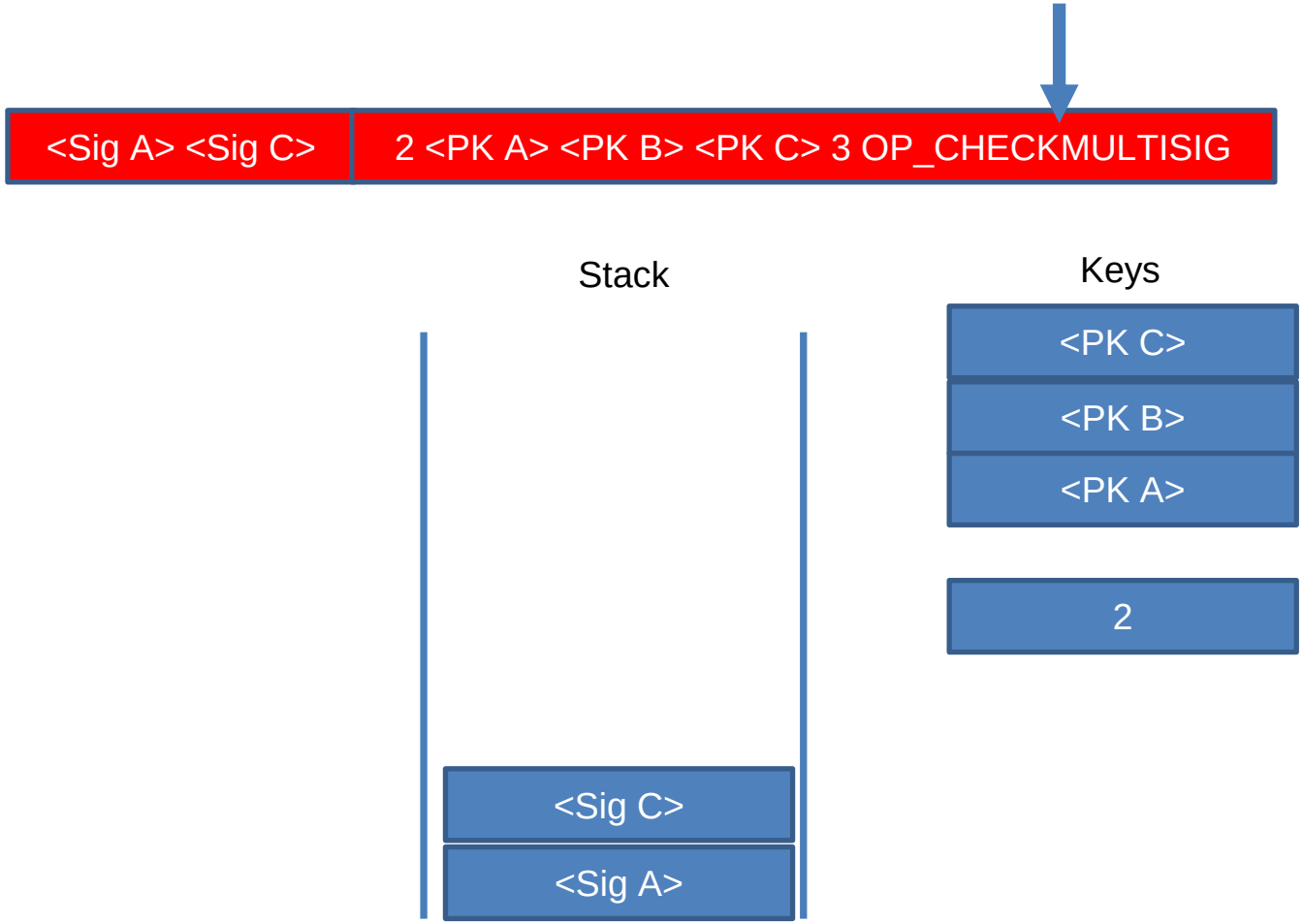
Multisig


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

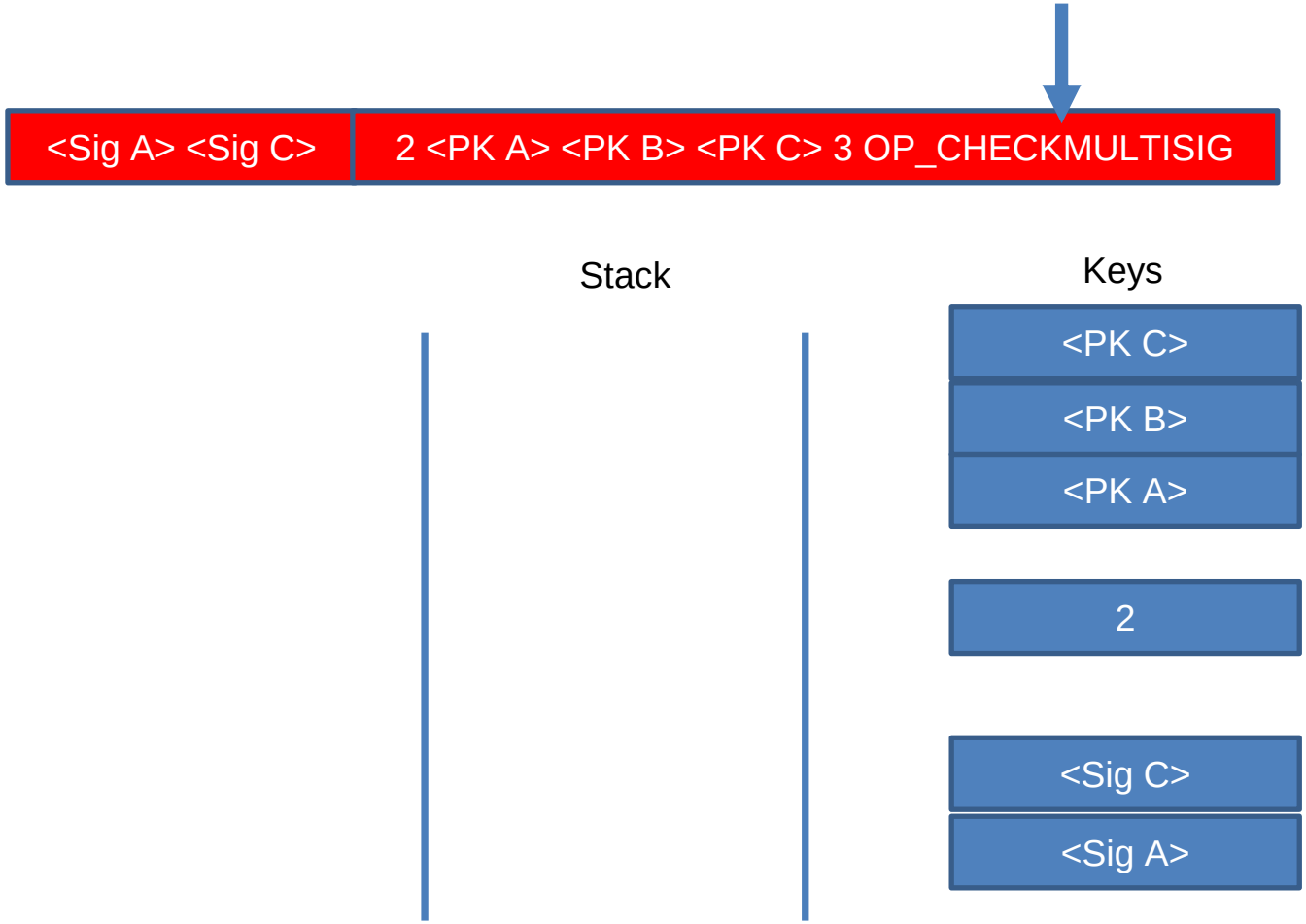
Multisig


<Sig A> <Sig C>
2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG
Stack
Keys
<PK C>
<PK B>
<PK A>
2
<Sig C>
<Sig A>

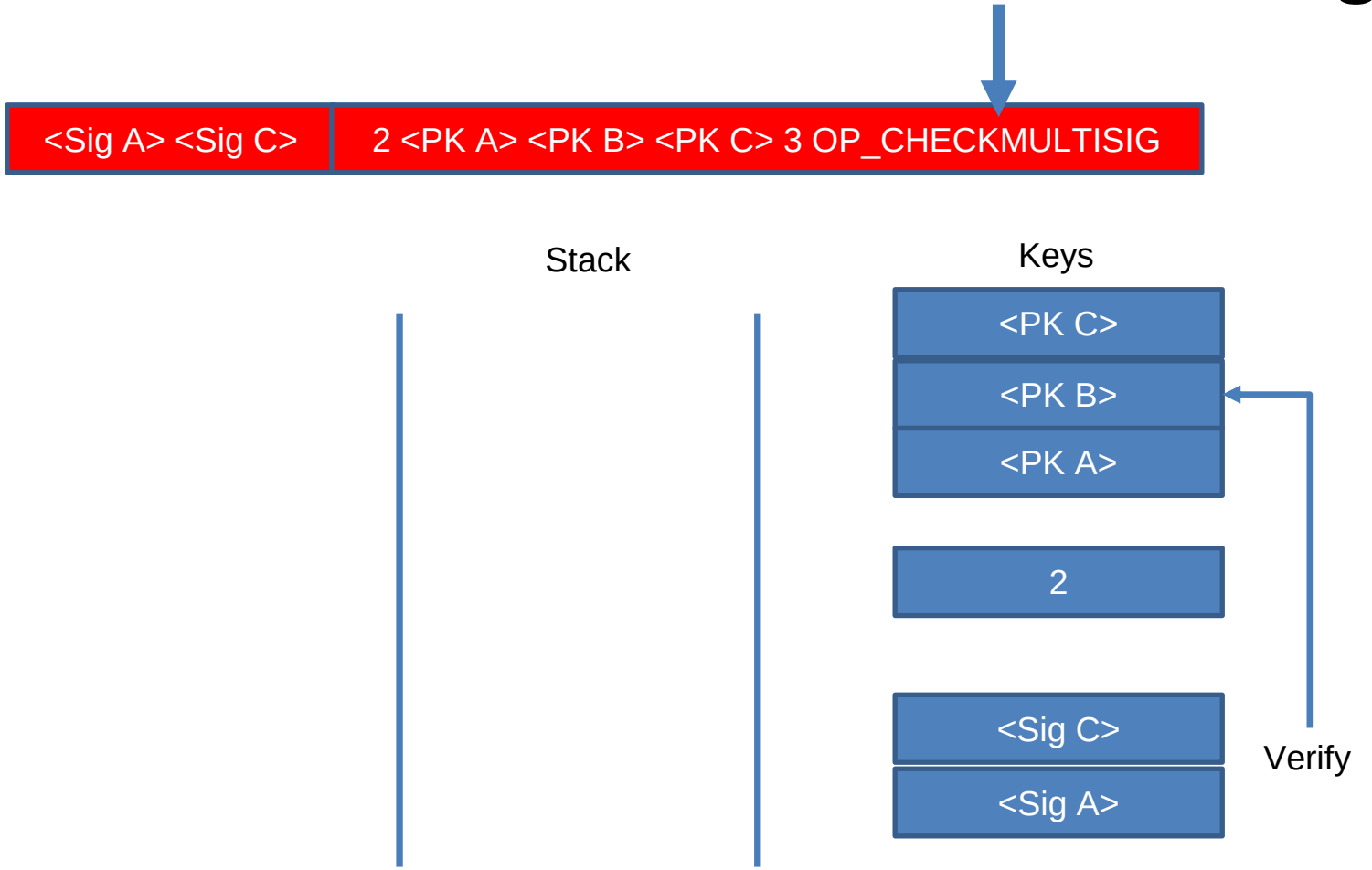
Multisig


<Sig A> <Sig C>
2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG
Stack
Keys
<PK C>
<PK B>
<PK A>
2
<Sig C>
<Sig A>

Multisig


<Sig A> <Sig C>
2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG
Stack
Keys
<PK C>
<PK B>
<PK A>
2
<Sig C>
<Sig A>

Multisig


<Sig A> <Sig C>
2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG
Stack
Keys
<PK C>
<PK B>
<PK A>
2
<Sig C>
<Sig A>
Verify

Multisig

In practice:

- **CHECKMULTISIG makes an extra pop**

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

Escrow transactions

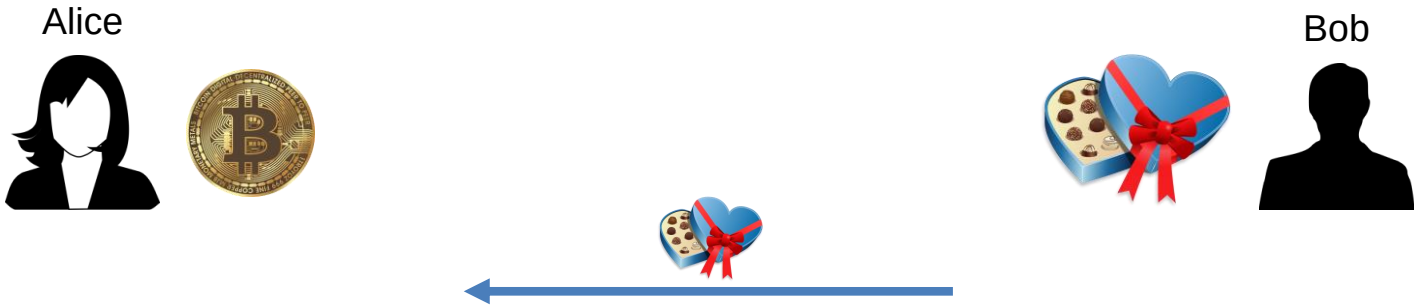
A use case for MULTISIG

Alice

Bob

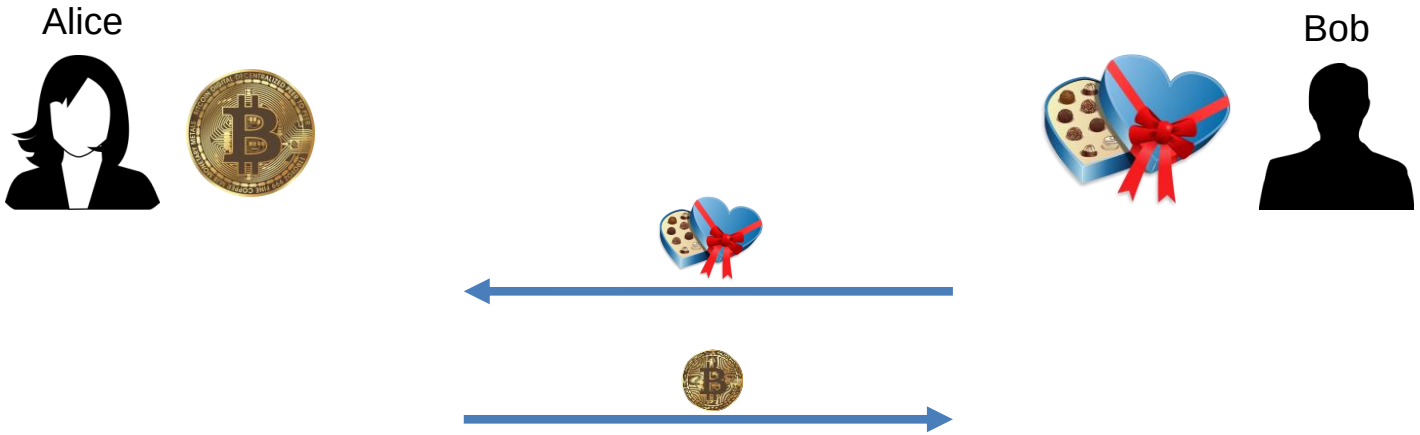
Escrow transactions

A use case for MULTISIG



Escrow transactions

A use case for MULTISIG



Escrow transactions

A use case for MULTISIG

Alice

Bob

Charlie

Escrow transactions

A use case for MULTISIG

Alice

Bob

0xff…

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

Charlie

Escrow transactions

A use case for MULTISIG

Alice

Bob

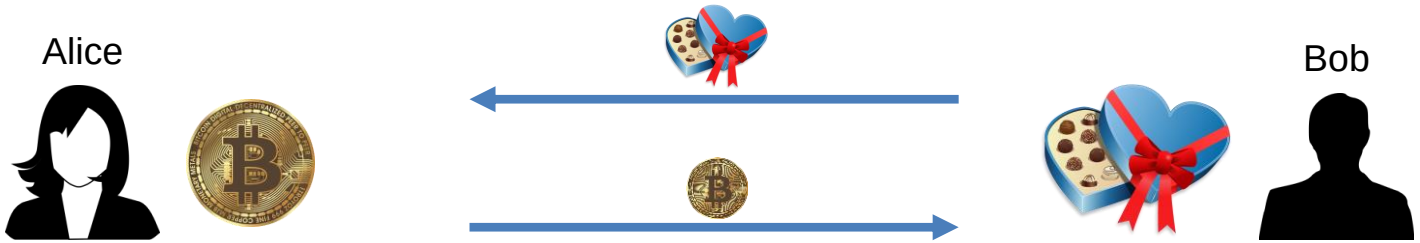
0xff…

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

Charlie

Escrow transactions

A use case for 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

A use case for MULTISIG

Alice

Bob

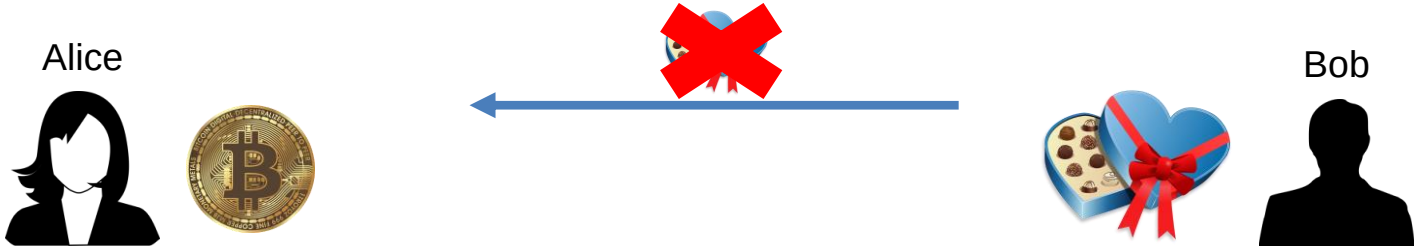
0xff…

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

Charlie

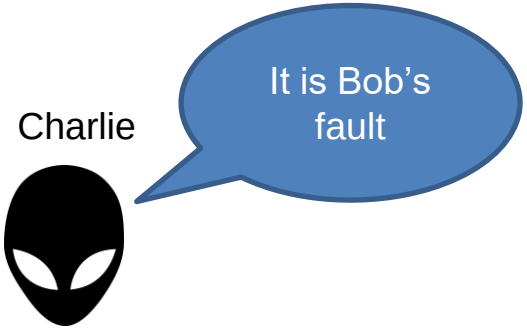
Escrow transactions

A use case for MULTISIG



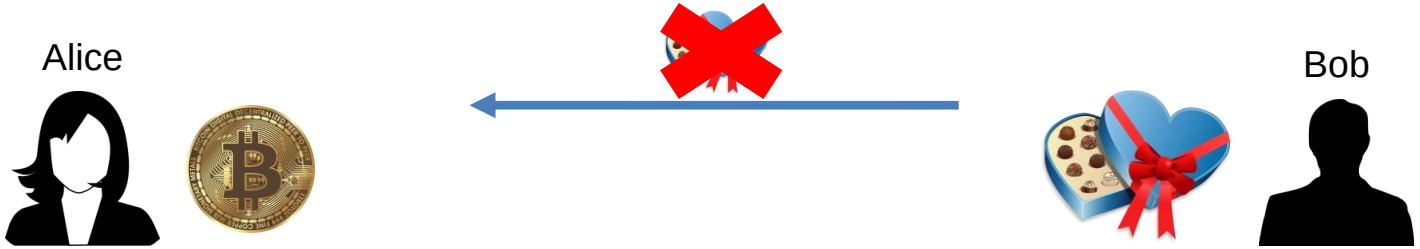
0xff…

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



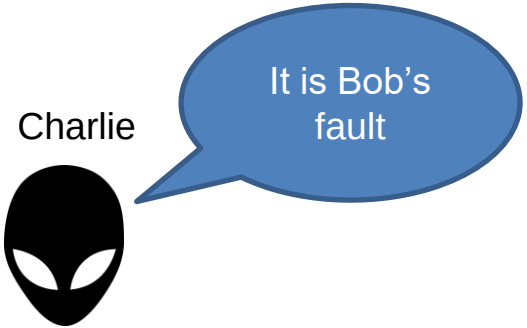
Escrow transactions

A use case for MULTISIG



0xff…

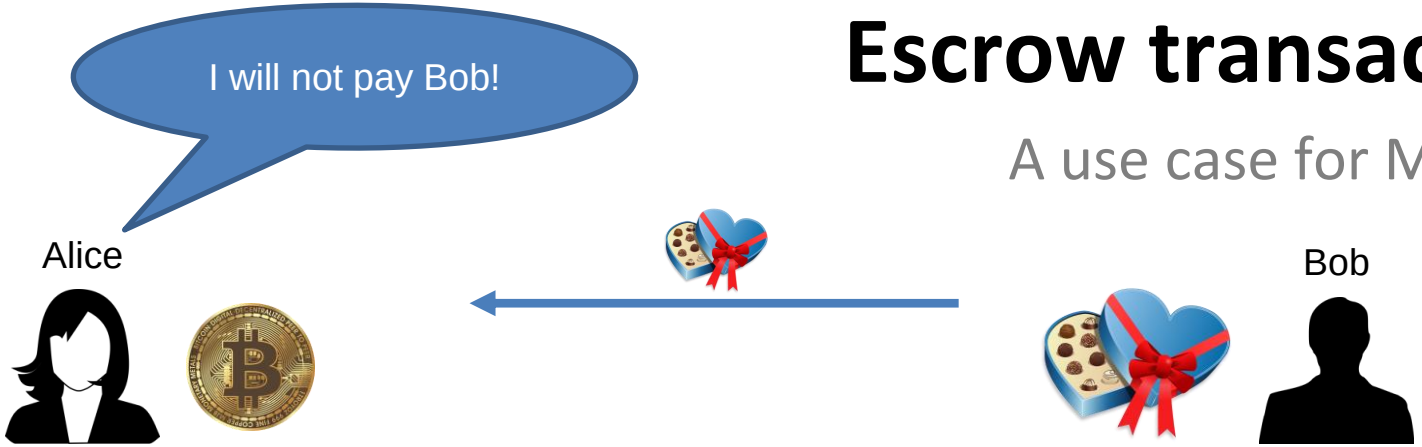
Value	Locking Script
1 BTC	2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG



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

A use case for MULTISIG



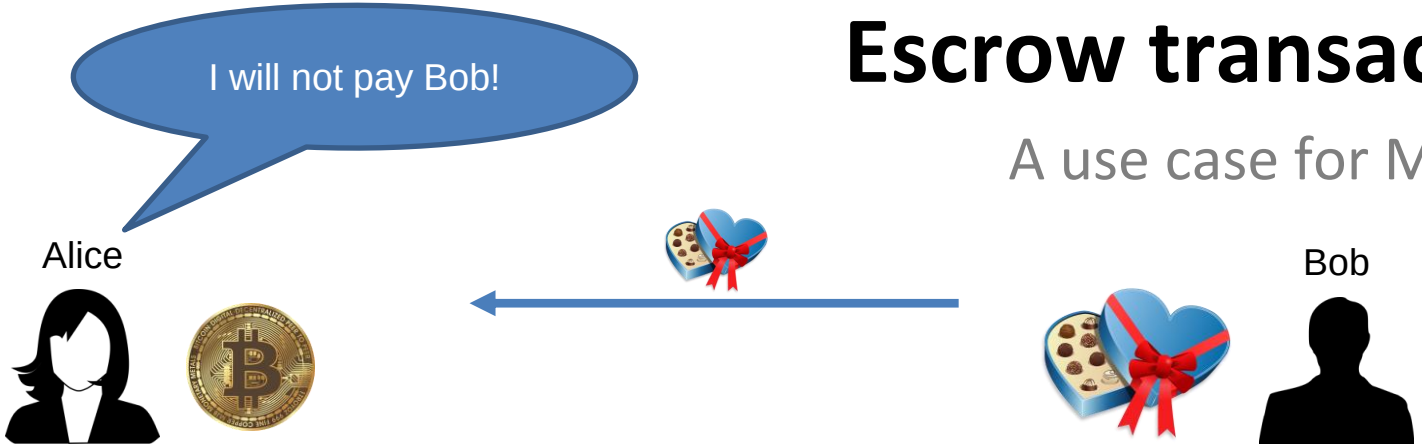
0xff…

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

Charlie

Escrow transactions

A use case for MULTISIG

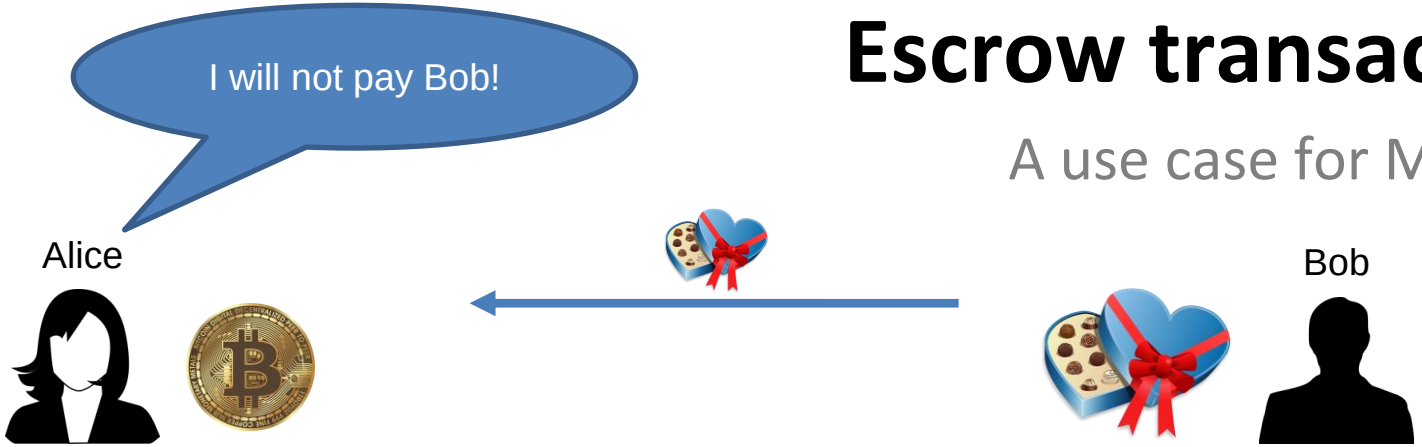


0xff…

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

Escrow transactions

A use case for MULTISIG



0xff…

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

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

Disadvanatges of MULTISIG:

- Difficult for the paying party (needs to construct a custom script)
- Example of a big script (the payer has extra cost for tx fee)
- Example of a big script (stays in the UTXO pool and uses a lot of RAM for nodes in the network)

Pay to script hash (P2SH)


```
{
    "txid": "40eee3ae1760e3a8532263678cdf64569e6ad06abc133af64f735e52562bccc8",
    "version": 1,
    "locktime": 0,
    "vin": [
        {
            "txid": "42a3fdd7d7baea12221f259f38549930b47cec288b55e4a8facc3c899f4775da",
            "vout": 0,
            "scriptSig": "473044022048d1468895910edafe53d4ec4209192cc3a8f0f21e7b9811f83b5e419bfb57
            e002203fef249b56682dbbb1528d4338969abb14583858488a3a766f609185efe68bca0121031a455dab5e
            1f614e574a2f4f12f22990717e93899695fb0d81e4ac2dcfd25d00",
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 0.00990000,
            "n": 0,
            "scriptPubKey": "OP_HASH160 e9c3dd0c07aac76179ebc76a6c78d4d67c6c160a OP_EQUAL",

        }
    ]
}
```

P2SH

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_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)

Solution: Pay to script hash (P2SH):

- Allows specifying a complex script as if it were a single address
- Idea: **Locking script** does not contain the script, but only its hash
- To spend the funds: **Unlocking script** specifies the script and its input data

P2SH has a special execution:

- Detect that it is a P2SH locking script
- And do a two-phase validation

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

P2SH

Phase 1: run

P2SH

Phase 1: run

P2SH

Phase 1: run

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

Stack

h(<redeem script>)

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

Stack

<script hash>
h(<redeem script>)

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**

Stack

<script hash>

h(<redeem script>)

Proceed if the same!!!

P2SH

Phase 2: run

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

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 <h(redeem script)> OP_EQUAL

redeem script

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

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 <h(redeem script)> OP_EQUAL

Unlocking:

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

P2SH

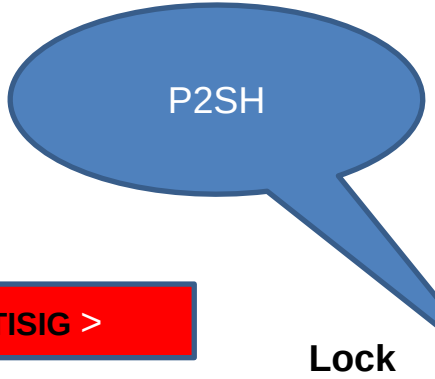
Unlock

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

Lock

OP_HASH160 <h(redeem script)> OP_EQUAL

P2SH



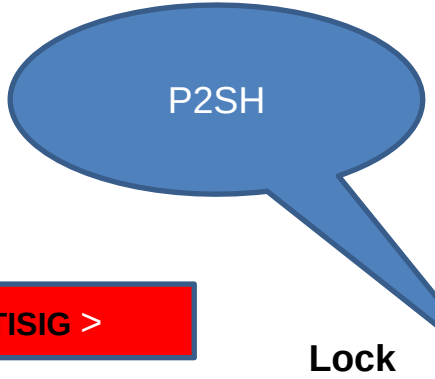
Unlock

<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

h(**2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG**) == <h(redeem script)>

P2SH

P2SH

Unlock

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

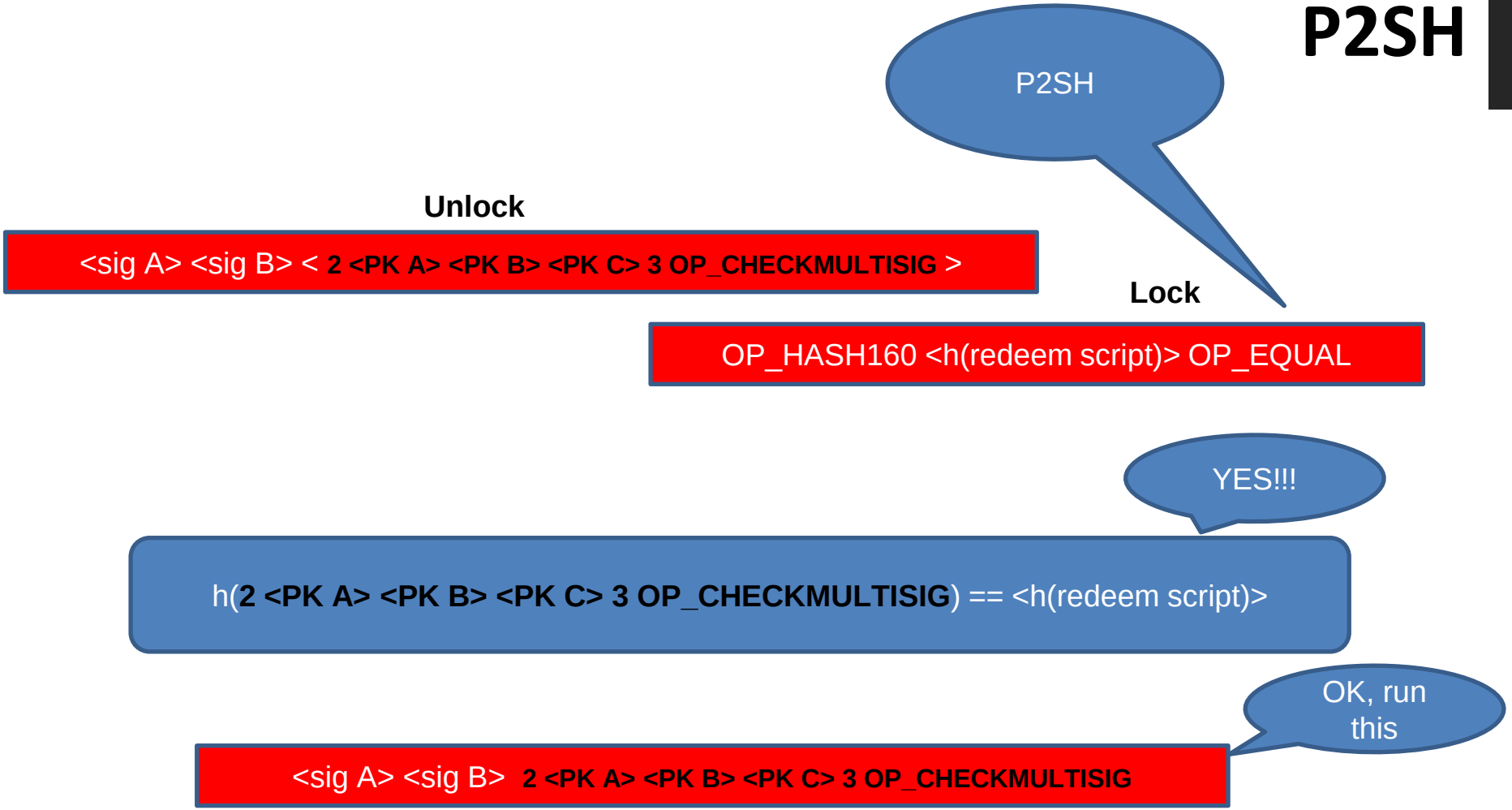
Lock

OP_HASH160 <h(redeem script)> OP_EQUAL

YES!!!

h(**2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG**) == <h(redeem script)>

P2SH

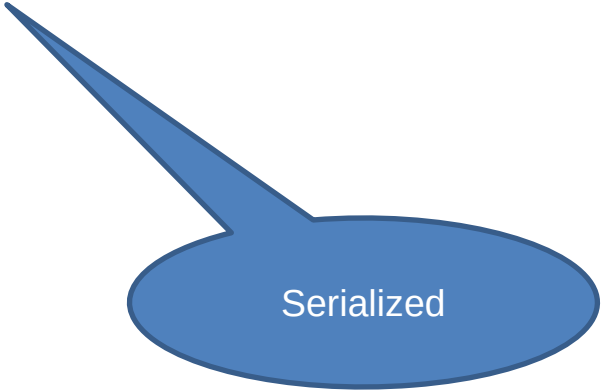

P2SH
Unlock
<sig A> <sig B> < 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG >
Lock
OP_HASH160 <h(redeem script)> OP_EQUAL
YES!!!
h(2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG) == <h(redeem script)>
OK, run this
<sig A> <sig B> 2 <PK A> <PK B> <PK C> 3 OP_CHECKMULTISIG

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>



Pay to script hash (P2SH)

Benefits of P2SH:

- Small input, including for a complicated script (its hash)
- The sender does not pay big fee (work is done when spending the funds)
- The big script is not stored in the UTXO (RAM), but on blockchain (HDD)
- The big script is not stored until the funds are spent
- The seller is responsable of constructing the complicated script

Bitcoin as a tamper proof log

I want to prove that I knew certain information at a specific date:

- I publish the hash of the information on the Bitcoin blockchain
- I.e. I do a transaction to hash of my document in base58 encoding
- Problem: "Blockchain/UTXO bloat"

- E.g. https://proofofexistence.com

Bitcoin as a tamper proof log

Solution: OP_RETURN

- A command making the output unspendable
- Introduced in BicoinCore 0.9 to make UTXO set smaller

Inputs (UTXO referenced)			
num	hash	Nr_output	Unlocking script
0	0xff…	4	012123…
Outputs			
num	value	Locking script	
0	0.000001	OP_RETURN H(”Hi. It’s me, Satoshi!”)	

Bitcoin as a tamper proof log

Use of this idea:

- Digital timestamping
- Proof fo burn

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