
its of Bitcoin
A tale of Cryptography, Finance and Mystery
Ben April - Sr. Threat Researcher
DCC March 2014
CARPE
CERVIXIA
TREND
MICRO

It’s about hash value

0000000000000272ff16617011170d1bc92562175411095eb5e2467a1e72e9a

What is that hash worth? Think about this for a moment Bitcoin is using the value of the hash as more than =/!= operator. One of the most novel elements is that Bitcoin uses a < operator on a SHA256. If you have a function that will tell me how to change the input to find a smaller SHA256 value, let me know I’ll show you how to turn that into cash!

It’s about hash value

00000000000000272ff16617011170d1bc92562175411095eb5e2467a1e72e9a

25.20695016 BTC

What is that hash worth? Think about this for a moment Bitcoin is using the value of the hash as more than =/!= operator. One of the most novel elements is that Bitcoin uses a < operator on a SHA256. If you have a function that will tell me how to change the input to find a smaller SHA256 value, let me know I’ll show you how to turn that into cash!

It’s about hash value

00000000000000272ff16617011170d1bc92562175411095eb5e2467a1e72e9a

25.20695016 BTC

$13K USD

$9.5K EUR

What is that hash worth? Think about this for a moment Bitcoin is using the value of the hash as more than =/!= operator. One of the most novel elements is that Bitcoin uses a < operator on a SHA256. If you have a function that will tell me how to change the input to find a smaller SHA256 value, let me know I’ll show you how to turn that into cash!

Meet: Satoshi Nakamoto

- Author of first bitcoin client.
- Paper published 2008. First TX 2009.
- Satoshi vanished in 2010.
- Satoshi can mean "wisdom" or "reason"
- Naka = Center Moto = cause

No Japanese references in the bitcoin code. Samples of writing seems to alternate between British and American English.

Checks and balances

- Difficulty level.
- Controlled Supply/Transaction fees
- Non-recovery/Write only.

Bitcoin Addresses

1LuckyY9fRzcJre7aou7ZhWVXktxjjBb9S

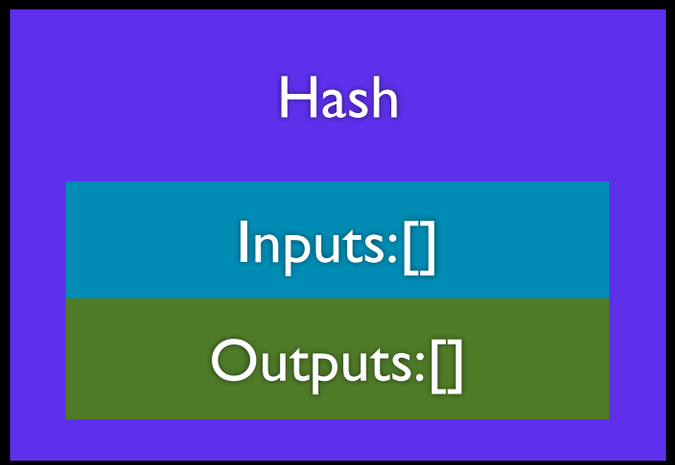
- EC-DSA keypair.
- Curve: Secp256k1
- RIPEMD-160(SHA256(pubkey))
- Encoded in base58-Check
- Loose the Private Key, loose the BTC.
- Disposable/cheap.
- Lapses in Address hygiene reduce anonymity.

Address is public key.
public key (64 Bytes) -> maps to 20 Bytes.

Base58check

- Like Base64 but without I,l,O,0 or punctuation.
- 1 Byte Preamble. (0x00 in Bitcoin)
- 4 Byte Checksum suffix.
- Designed for human transcription.

Anatomy of a TX



Do we have to bring Alice and Bob into this?

Alice Sends 25 BTC to Bob


```
{
  "hash":"fb7a14659b6c156daac45082821ec60b1cb8e218809707dae4cab742d9a8d919",
  "ver":1,
  "vin_sz":1,
  "vout_sz":2,
  "lock_time":0,
  "size":258,
  "in":[
    {
      "prev_out":{
        "hash":"6dc904afcc7817e56a0ead3965497bff4031de948f2d88a2c4d2ec57566d0b5",
        "n":0
      },

"scriptSig":"3045022100d942844c8148c4f61cc4a3786b8601a9786e1df19cee377e1863f8dea63490ae02207a88c839163b808054e
61445d949cd9afdfee122102eaf1561dd880fcfaa97f381
040117609 8c1cb7b4637f5476338cc426933f9130d10013d6f848be3842ac67522743308c563137a4509b5fcda7237adc12b00a5b197c1
37c8f9de272556c58f7a"
    }
  },
  "out":[
    {
      "value":"10.21727524",
      "scriptPubKey":"OP_DUP OP_HASH160 0709df684fed4e1d6e5def8f5698537b86183abf OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value":"25.00000000",
      "scriptPubKey":"OP_DUP OP_HASH160 0a637345368864f49b9fa801d32025e55a03e1647 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```


Couple of caveats:
1) randomly selected transaction, May or may not be between alice and bob.
2)This transaction is displayed in JSON, showing it in the internal binary format would be unhelpful.

Incoming TX

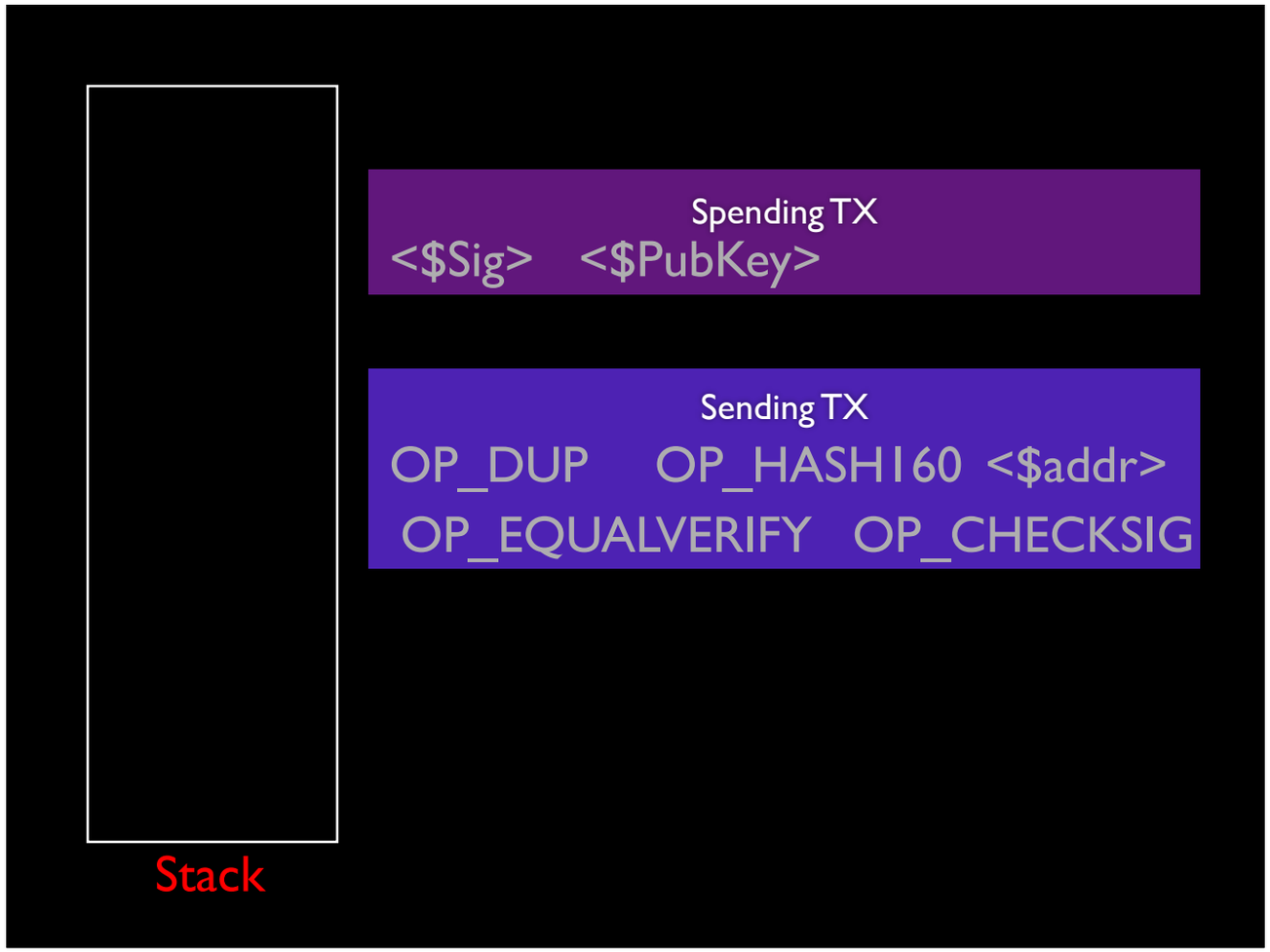

```
{
  "hash":"6dc904afcc78317e56a0ead3965497bff4031de948f2d88a2c4d2ec57566d0b5",
  "ver":1,
  "vin_sz":1,
  "vout_sz":2,
  "lock_time":0,
  "size":258,
  "in":[
    {
      "prev_out":{
        "hash":"7da6d66ac908b46782917c3fd16deaff1f9a7483f2e4bc38d63d98108cd48148",
        "n":0
      },

"scriptSig":"3045022033f48baf99e6240ba983de98a4433cc87fcf7bf451f6a965516e0dbcfe4c7349022100e8e754446e61595d86f
de5a139e788cdbbd209f330f244a5a6db91daccb27d2101
0401176098c1cb7b4637f5476338cc426933f9130d10013d6f848be3842ac67522743308c563137a4509b5fcda7237adc12b00a5b197c1
37e8f9de272556c58f7a"
    }
  ],
  "out":[
    {
      "value":"35.21727524",
      "scriptPubKey":"OP_DUP OP_HASH160 07090f684fed4e1d6e5def8f569853fb86183abf OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value":"9.80000000",
      "scriptPubKey":"OP_DUP OP_HASH160 cb9d0fadcc7b1210772486b3a95e99fe649bf2fc OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

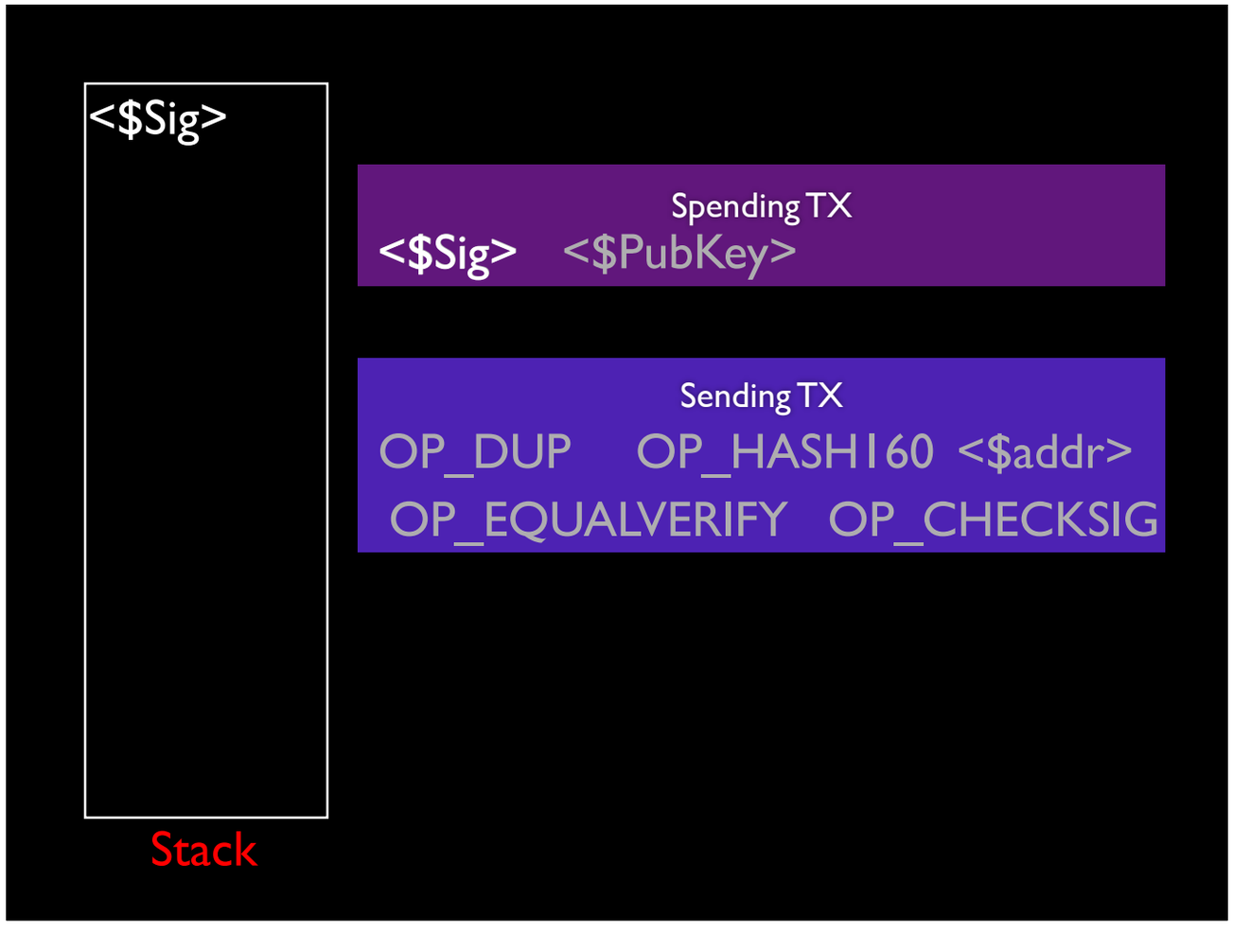
Transaction Script

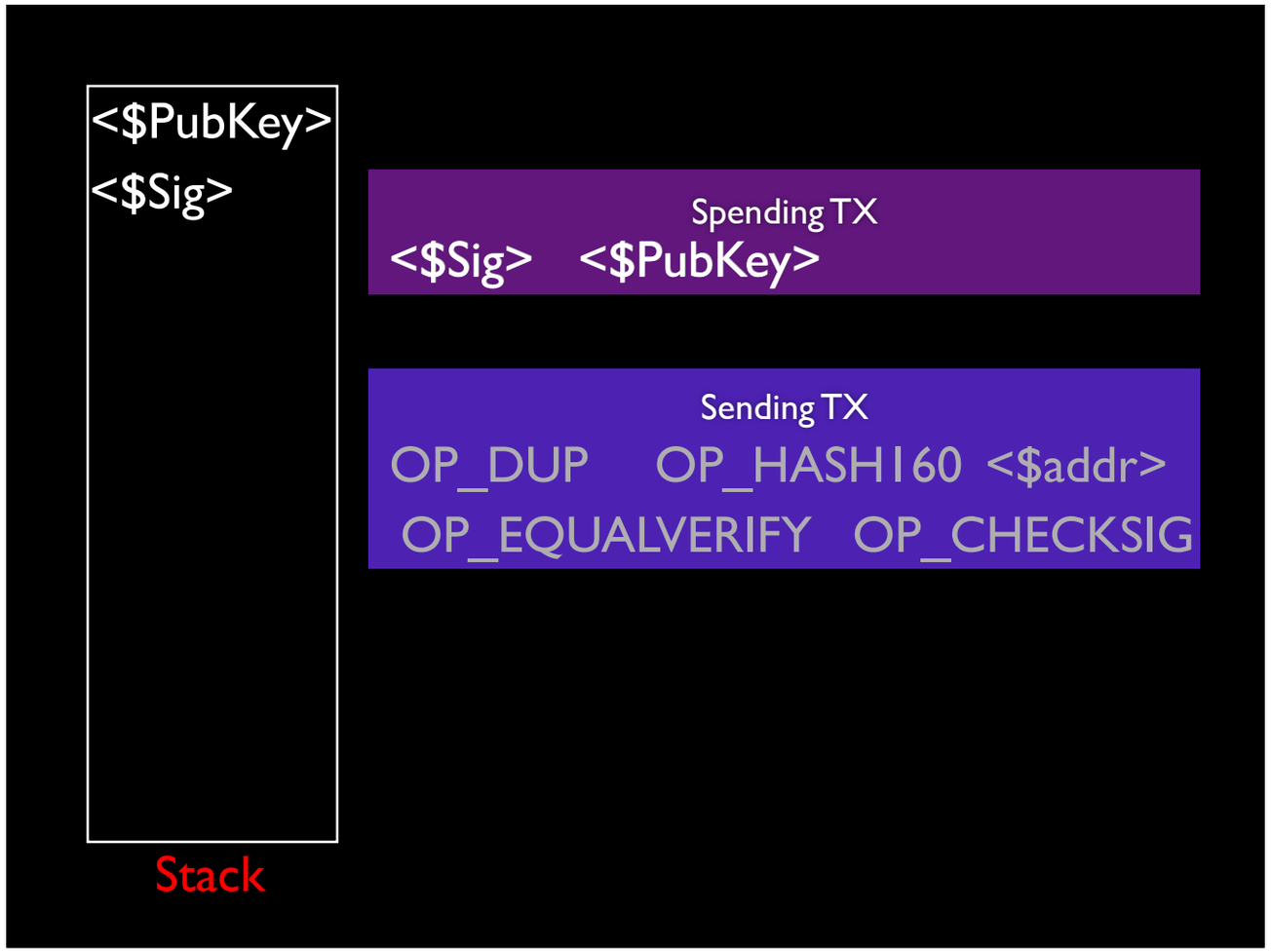
- Stack-based forth-like language.
- Dest script is appended to the source script and executed, if it evaluates true the transaction is accepted.
- Most common script confirms sig by Address key.

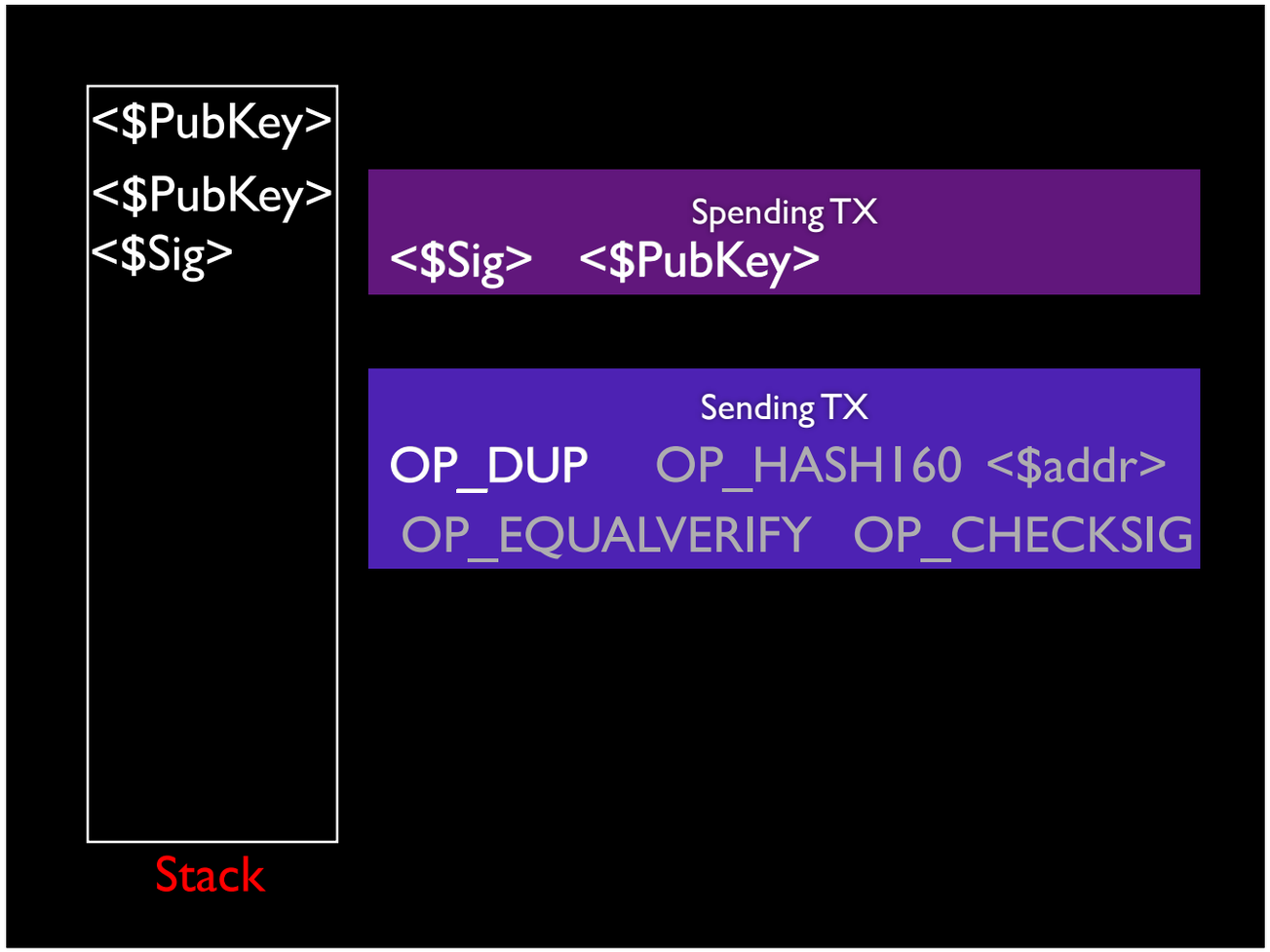
“Standard” TX

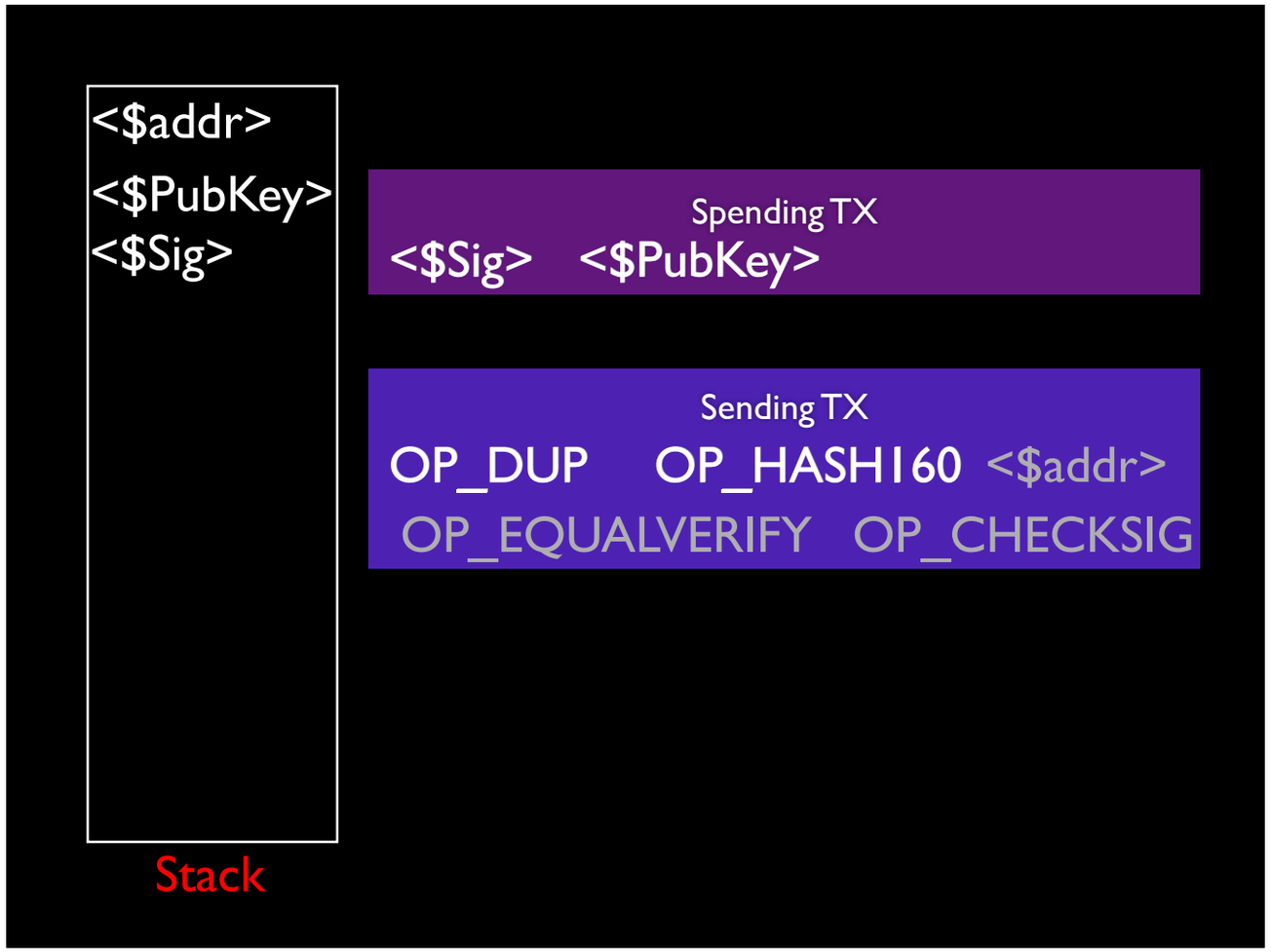
- Spender: <$Sig> <$PubKey>
- Sender: OP_DUP OP_HASH160 <$addr> OP_EQUALVERIFY OP_CHECKSIG

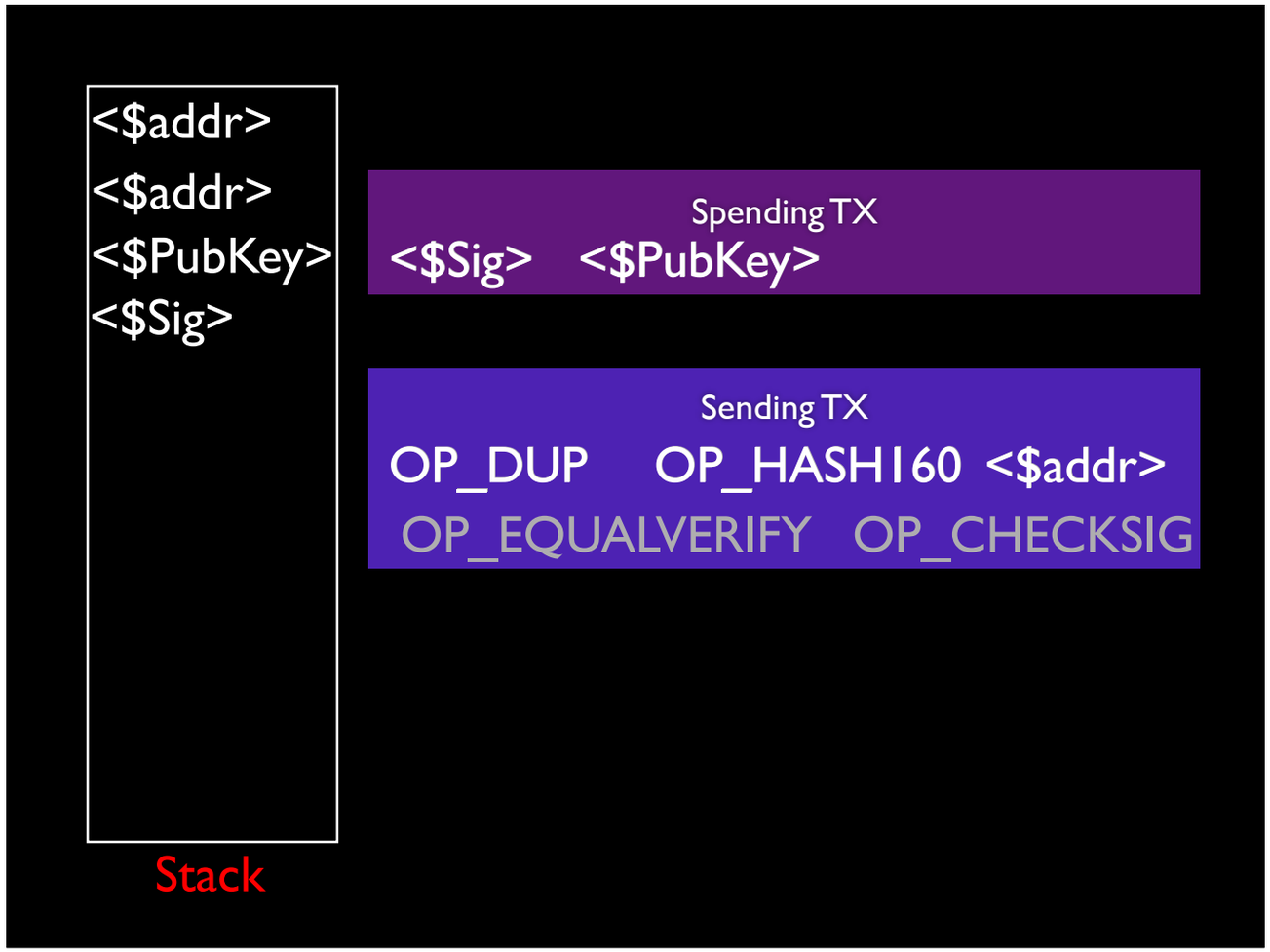

Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG
Stack

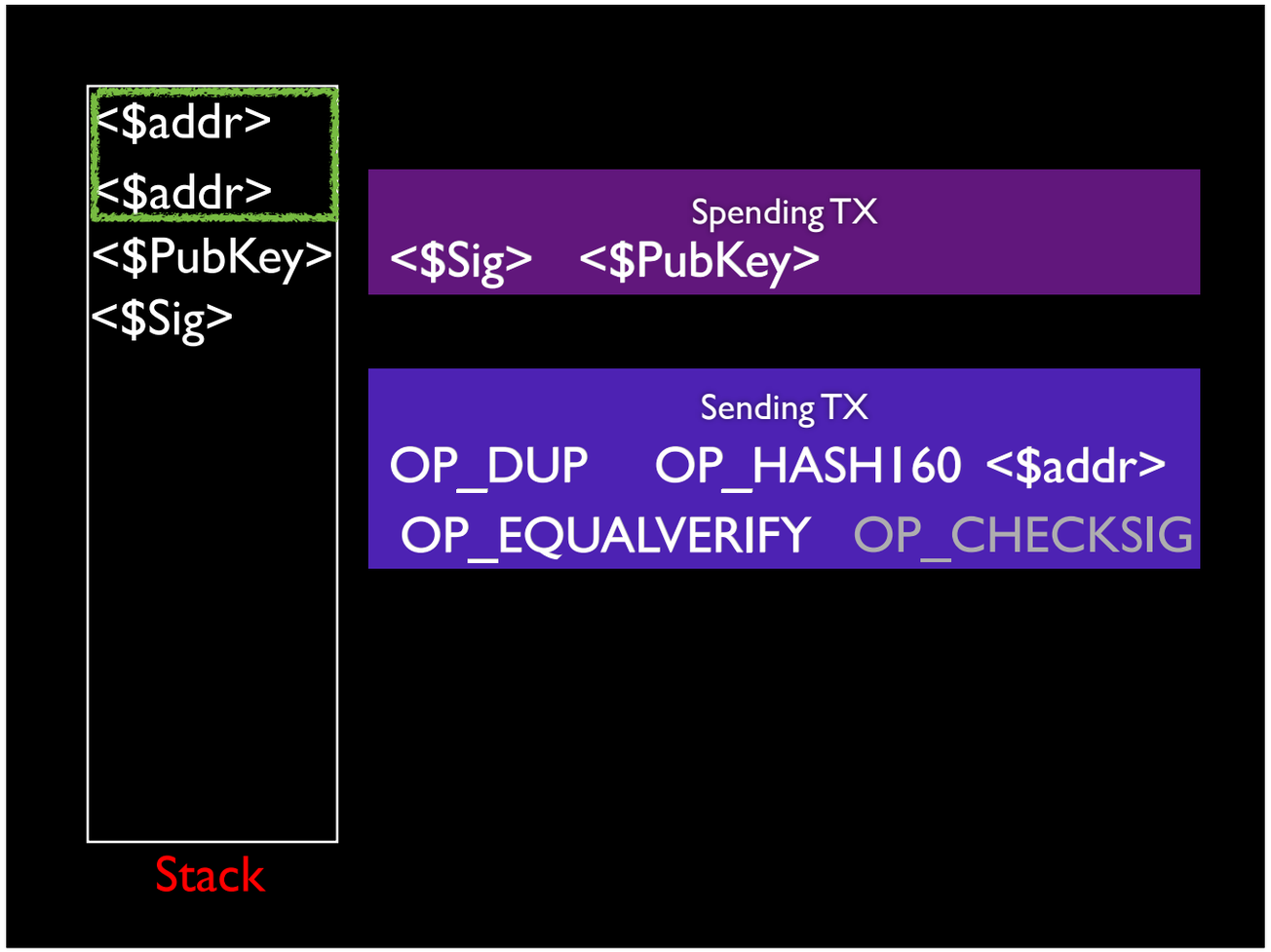

<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG

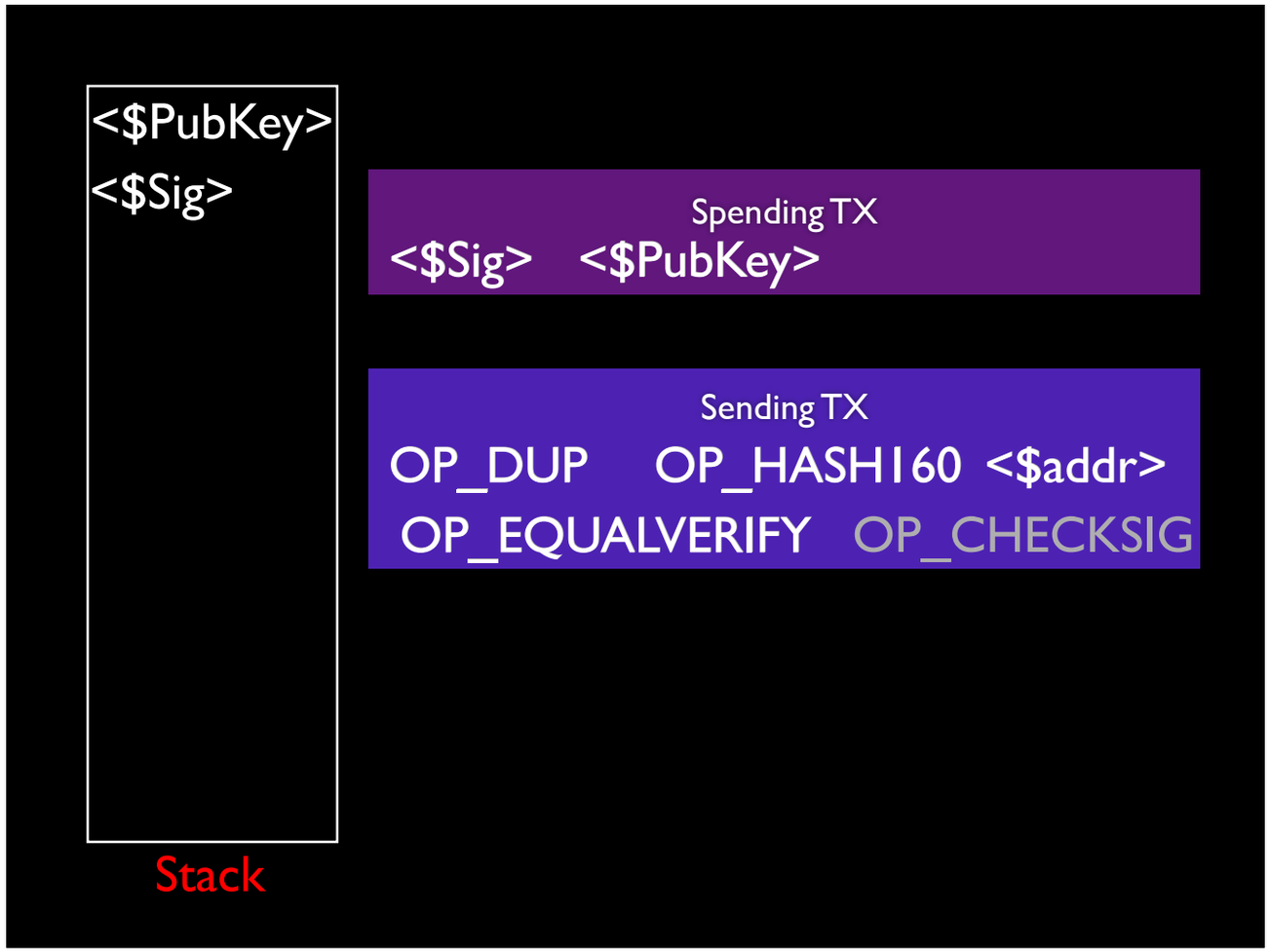

<$PubKey>
<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG

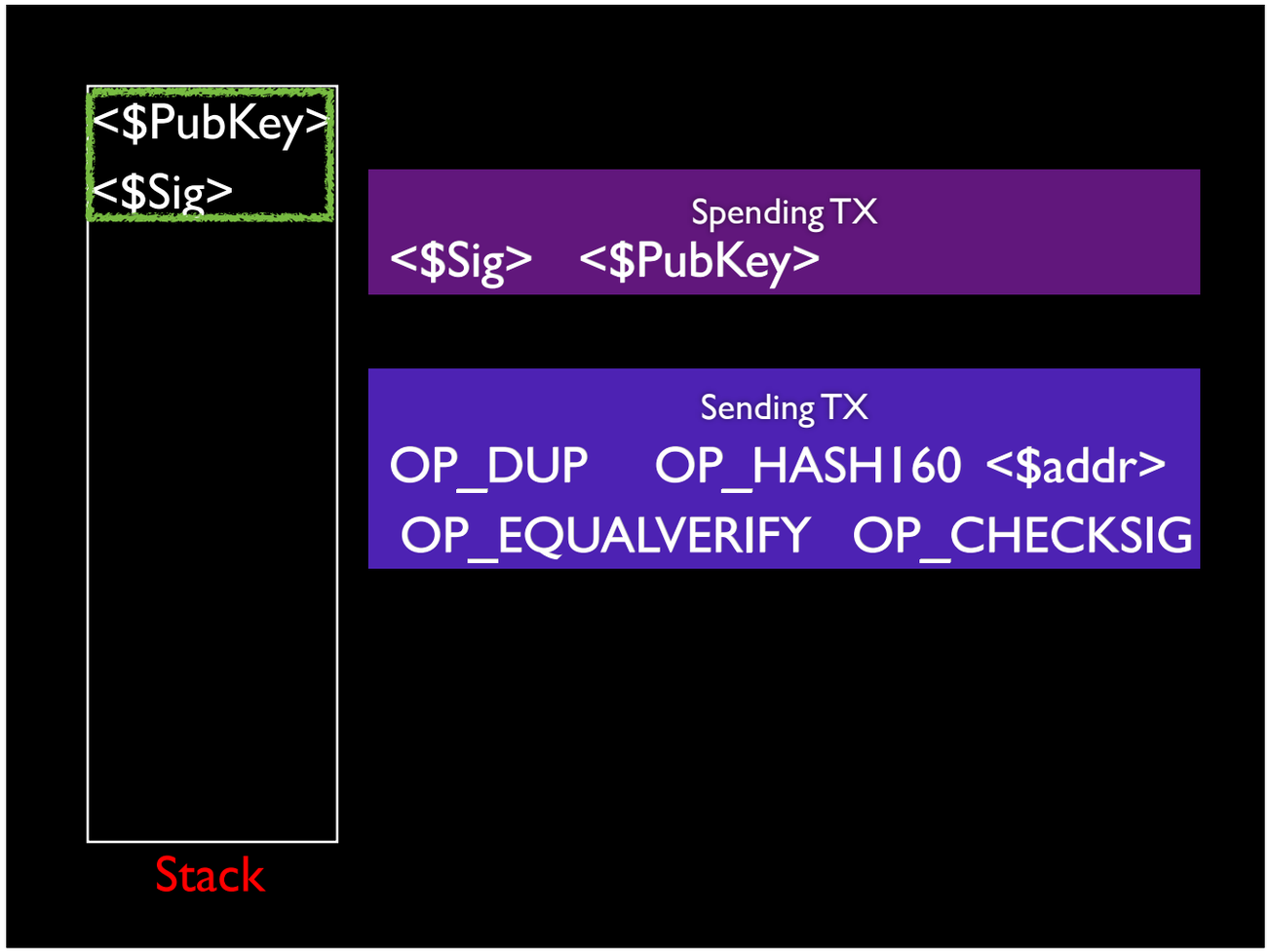

<$PubKey>
<$PubKey>
<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG


<$addr>
<$PubKey>
<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG


<$addr>
<$addr>
<$PubKey>
<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG

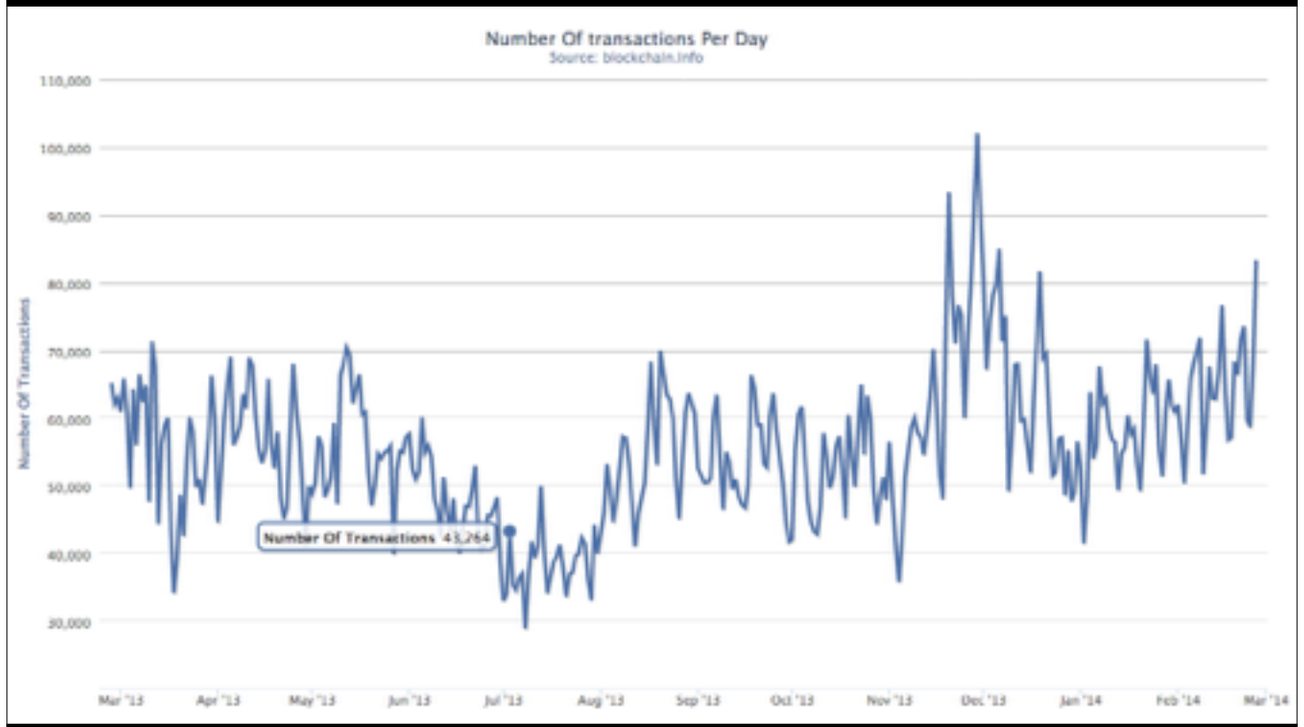

<$addr>
<$addr>
<$PubKey>
<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG


<$PubKey>
<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG

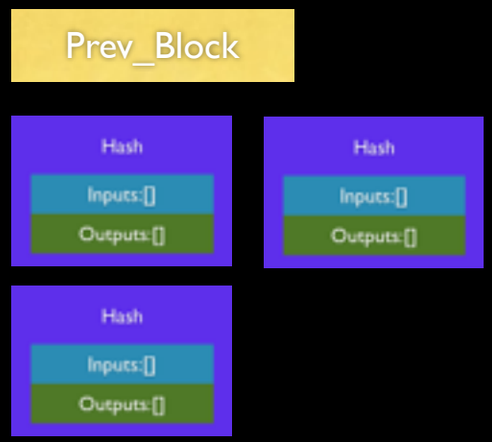

<$PubKey>
<$Sig>
Stack
Spending TX
<$Sig> <$PubKey>
Sending TX
OP_DUP OP_HASH160 <$addr>
OP_EQUALVERIFY OP_CHECKSIG

Stupid Script tricks

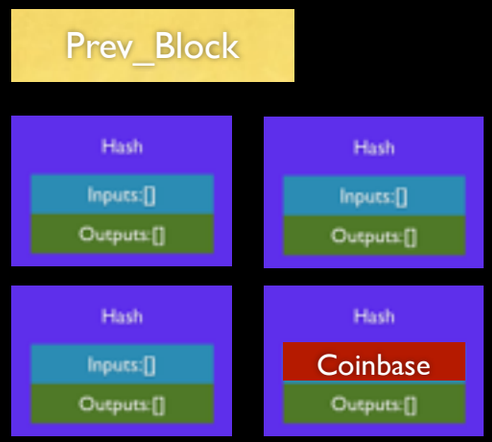
- Accept a password instead of a key.
- Inject ASCII art... (Dan Kaminsky)
- Require 2 or more Keys to redeem.
- Some are just flat broken. (> 2900 BTC)


Number Of transactions Per Day
Source: blockchain.info
110,000
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
Number Of Transactions
Number Of Transactions 43,264
Mar '13
Apr '13
May '13
Jun '13
Jul '13
Aug '13
Sep '13
Oct '13
Nov '13
Dec '13
Jan '14
Feb '14
Mar '14

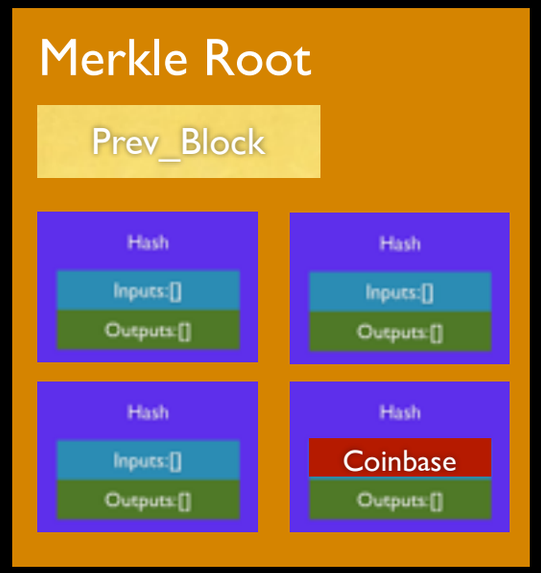
Blocks


Prev_Block
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]

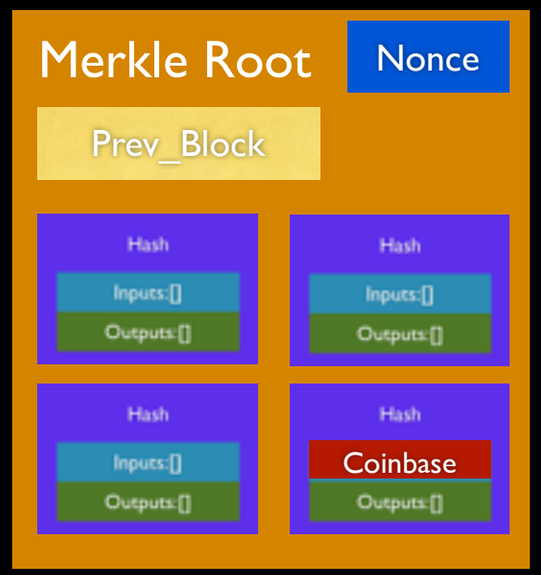
Blocks


Prev_Block
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Coinbase
Outputs:[]

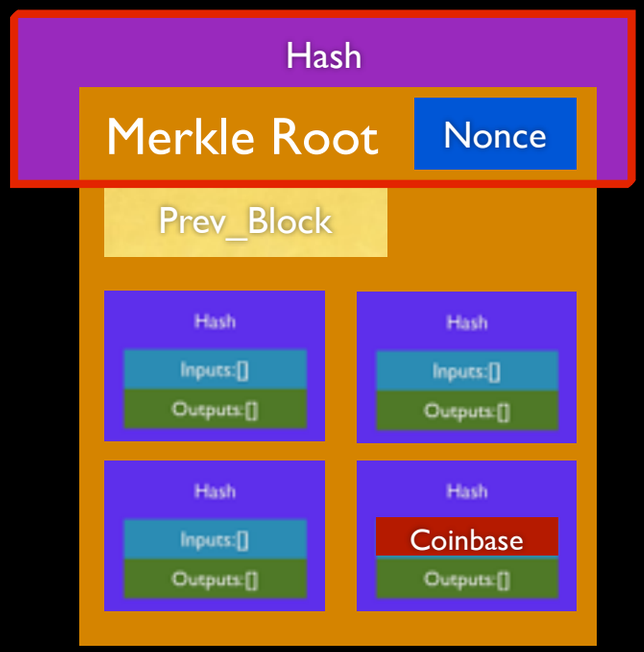
Blocks


Merkle Root
Prev_Block
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Coinbase
Outputs:[]

Blocks

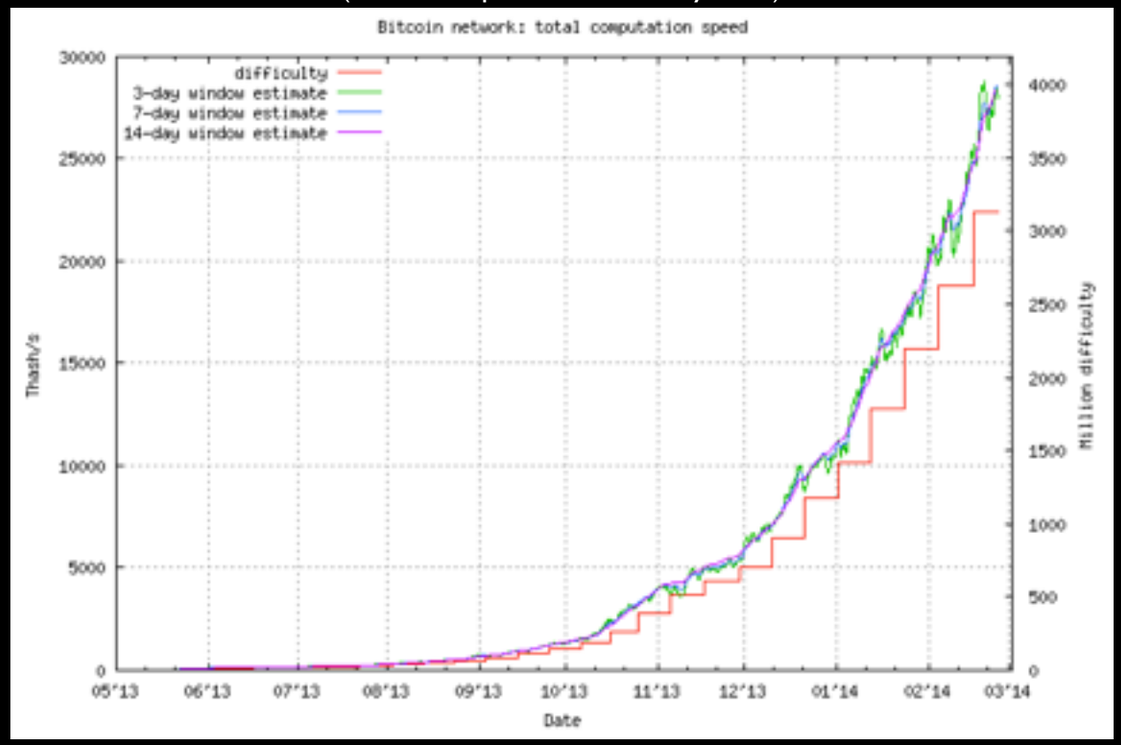

Merkle Root
Nonce
Prev_Block
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Coinbase
Outputs:[]

Blocks


Hash
Merkle Root
Nonce
Prev_Block
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Inputs:[]
Outputs:[]
Hash
Coinbase
Outputs:[]

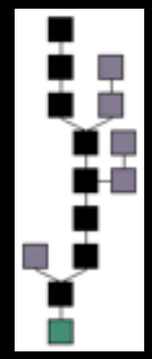
Target/Difficulty

(Source: http://bitcoindifficulty.com/)



Difficulty is re-calculated every 2016 blocks
That's 2 weeks @ the ideal rate of 1 block per 10 min)
Easiest target is a sha256 with 8 leading "0"s

Block Chain



- Solves the mining race-condition.
- Detours can be up to 120 blocks long.
- May mean you loose that block you won.
- In practice doesn't get beyond 3-4 blocks.

Must wait 120 blocks to spend. ~20 hrs

Controlled supply

- Limit of ~21 Million BTC EVER!
- 12.4 M in circulation today.
- Target of 6 blocks per hour.
- Reward decreases by 1/2 about every 4 years.

Slicing and dicing

- BTC is 1 integer Bitcoin 1.0
- dBTC (decibitcoin) = .1
- cBTC (centibitcoin) = .01
- mBTC (millibitcoin) = .001
- µBTC (microbitcoin) = .000 001
- satoshi = .000 000 01

Currently the satoshi is a code restriction.

- 1 BTC = 100 Million satoshi
- 2.1e+15 units of currency.

That’s 2.1 Quadrillion

Show me the $$$

(Source: http://bitcoincharts.com//)

$230 in late April 2013
Spike to $1200 in Late Nov 2013
Currently ~$500

TX Malleability


Bob Bitcoin
123 Main St
New York, NY 1234
123
March 3 2014
Pay to the Order of
Alice Bitcoin
BTC
25.0
Twenty five BTC
DCC Demo
Bob Bitcoin
& 123456789 & 987654321# 123


Bob Bitcoin
123 Main St
New York, NY 1234
123
March 3 2014
Pay to the Order of
Alice Bitcoin
BTC
25.0
Twenty five BTC
DCC Demo
Bob Bitcoin
& 123456789 & 987654321# 123


Bob Bitcoin
123 Main St
New York, NY 1234
123
March 3 2014
Pay to the Order of
Alice Bitcoin
BTC
25.0
Twenty five BTC
DCC Demo
Bob Bitcoin
& 123456789 & 987654321# 123


Bob Bitcoin
123 Main St
New York, NY 1234
123
March 3 2014
Pay to the Order of
Alice Bitcoin
BTC
25.0
Twenty five BTC
DCC Demo
Bob Bitcoin
& 123456789 & 987654321# 123


Bob Bitcoin
123 Main St
New York, NY 1234
123
March 3 2014
Pay to the Order of
Alice Bitcoin
BTC
25.0
Twenty five BTC
DCC Demo
Bob Bitcoin
& 123456789 & 987654321# 123
Bob Bitcoin
123 Main St
New York, NY 1234
1230
March 3 2014
Pay to the Order of
Alice Bitcoin
BTC
25.0
Twenty five BTC
DCC Demo
Bob Bitcoin
& 123456789 & 987654321# 1230

TX Malleability

FIRST NATIONAL BANK OF BITCOIN

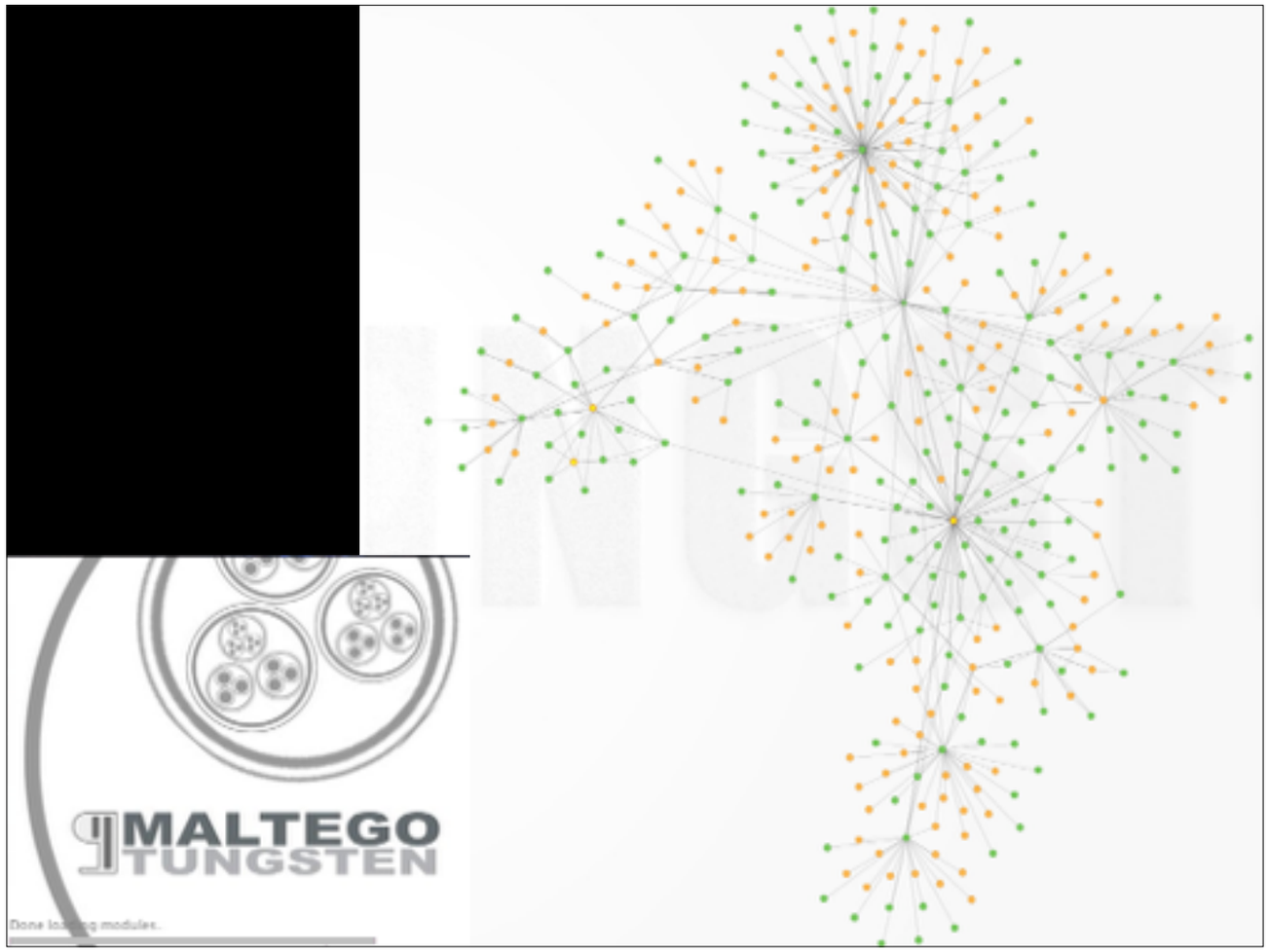
Check No	Pay To	Amount	Date
120	Barry Bitcoin	10.0 BTC	1-March
121	Mike Bitcoin	5.0 BTC	1-March
122	Paul Bitcoin	2.75 BTC	2-March
124	Janet Bitcoin	125.0 BTC	4-March

FIRST NATIONAL BANK OF BITCOIN

Check No	Pay To	Amount	Date
120	Barry Bitcoin	10.0 BTC	1-March
121	Mike Bitcoin	5.0 BTC	1-March
122	Paul Bitcoin	2.75 BTC	2-March
124	Janet Bitcoin	125.0 BTC	4-March
1230	Alice Bitcoin	25.0 BTC	3-March

FIRST NATIONAL BANK OF BITCOIN

Check No	Pay To	Amount	Date
120	Barry Bitcoin	10.0 BTC	1-March
121	Mike Bitcoin	5.0 BTC	1-March
122	Paul Bitcoin	2.75 BTC	2-March
124	Janet Bitcoin	125.0 BTC	4-March
1230	Alice Bitcoin	25.0 BTC	3-March


MALTEGO
TUNGSTEN