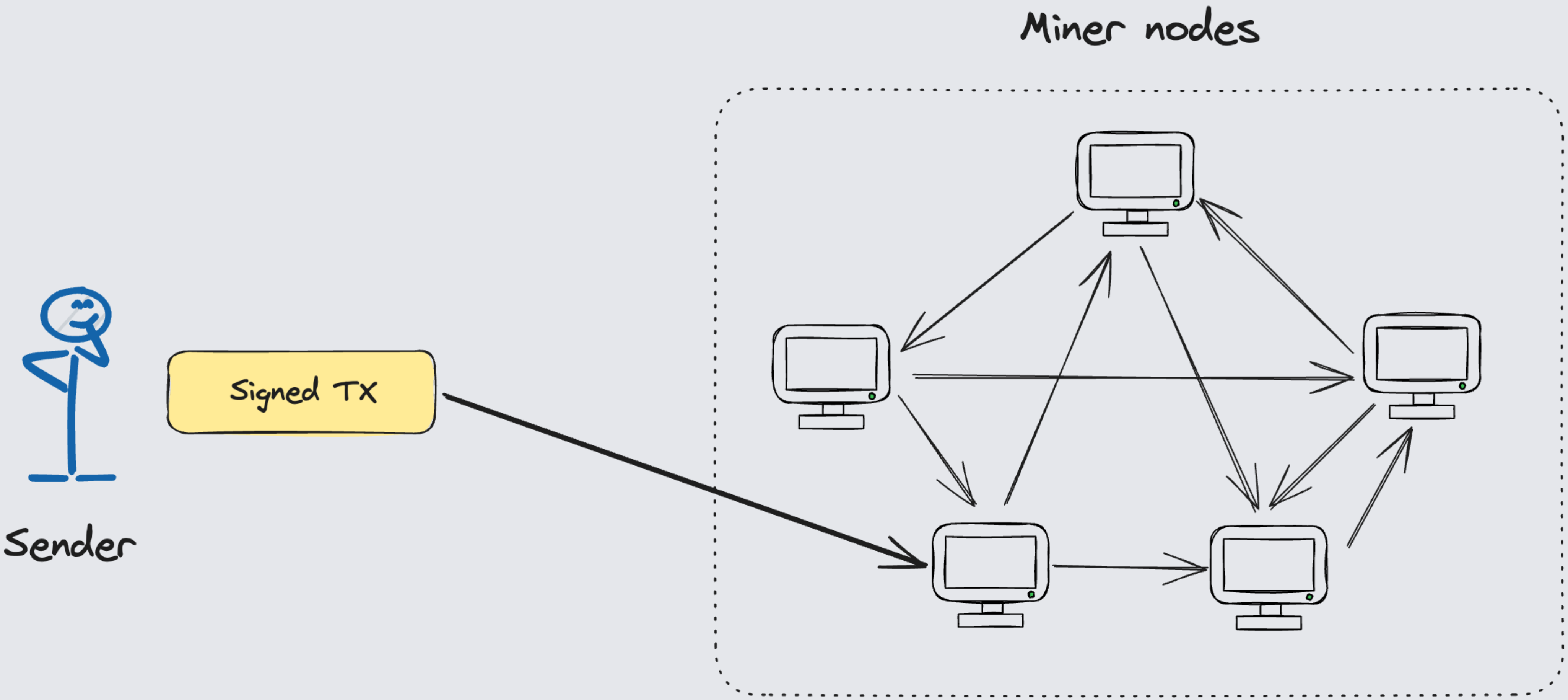
Bitcoin

Prepared by Kirill Sizov

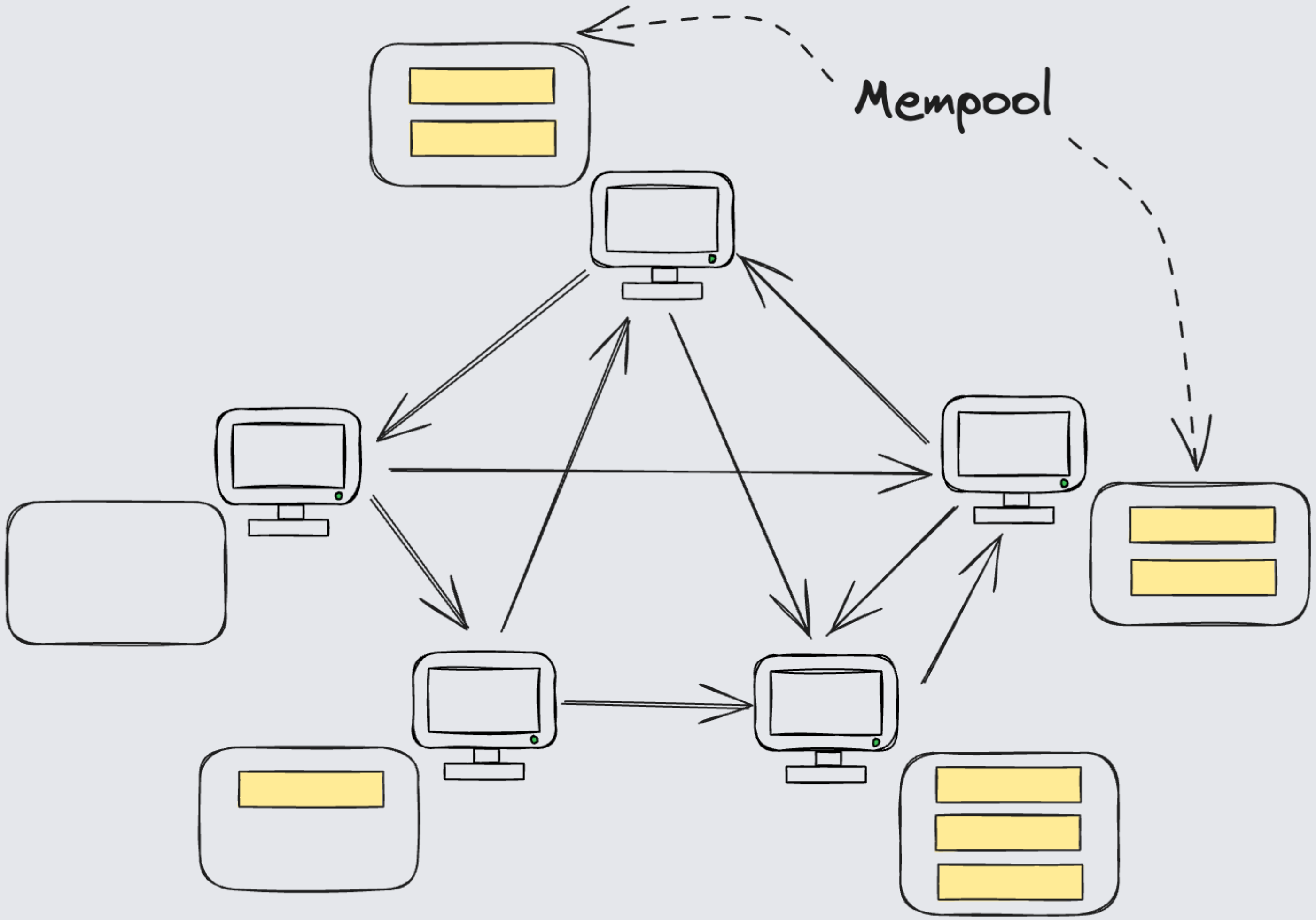
Agenda

- Transaction path
- Block structure
- Transaction structure
- Bitcoin script
- Segwit
- Visual demo

Sending a TX

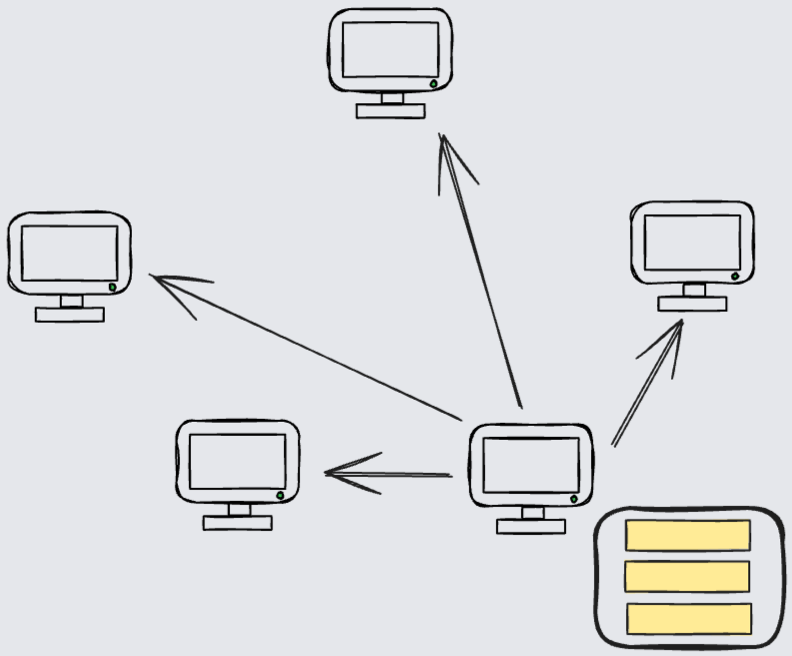


TX propagation



Block creation

- Each miner select TXs and build their own block.
- PoW consensus mechanism select a node.
- Selected node propagates their block to other nodes.
- Other nodes validate this block.

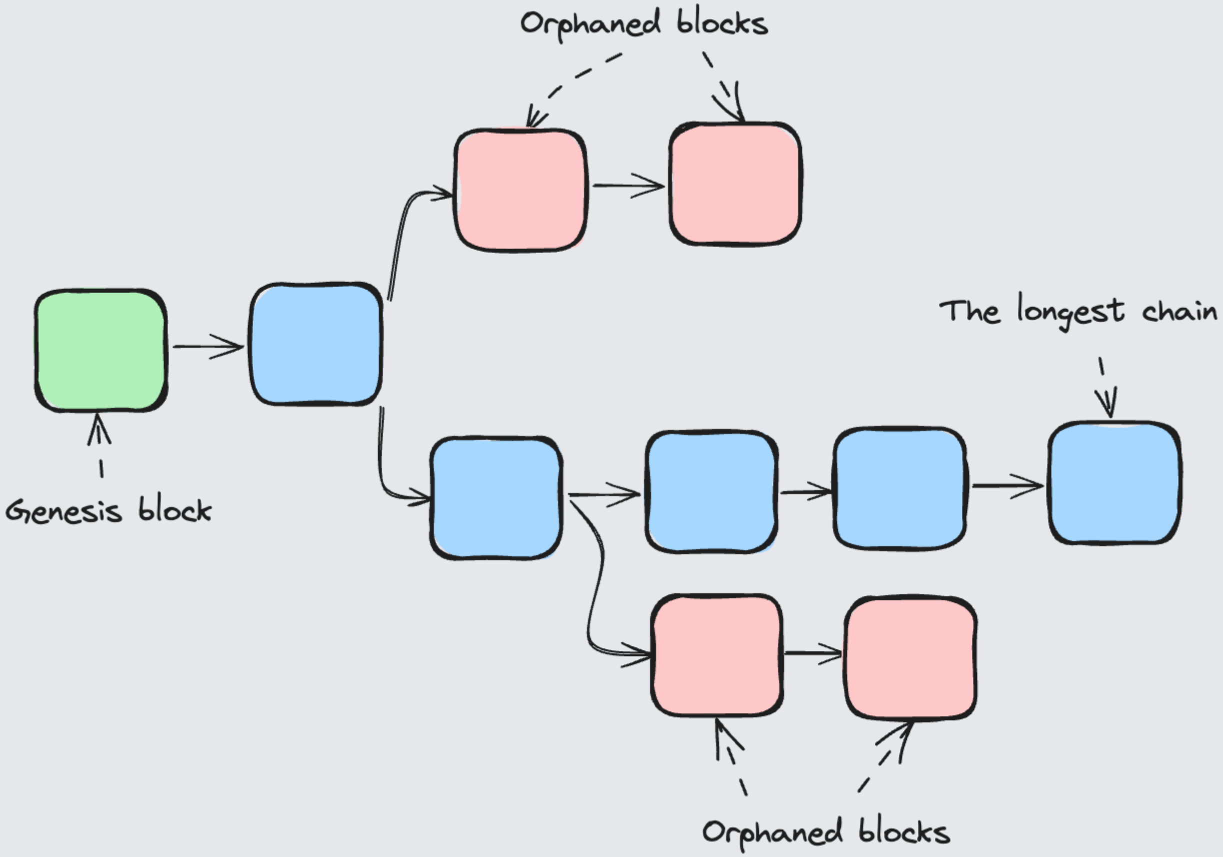


Choosing a winner

- Each node brute force the nonce of the block to find the smallest possible hash.
- The size of the minimum acceptable hash is determined by the difficulty target.
- Difficulty target is adjusted every 2016 blocks (~14 days).

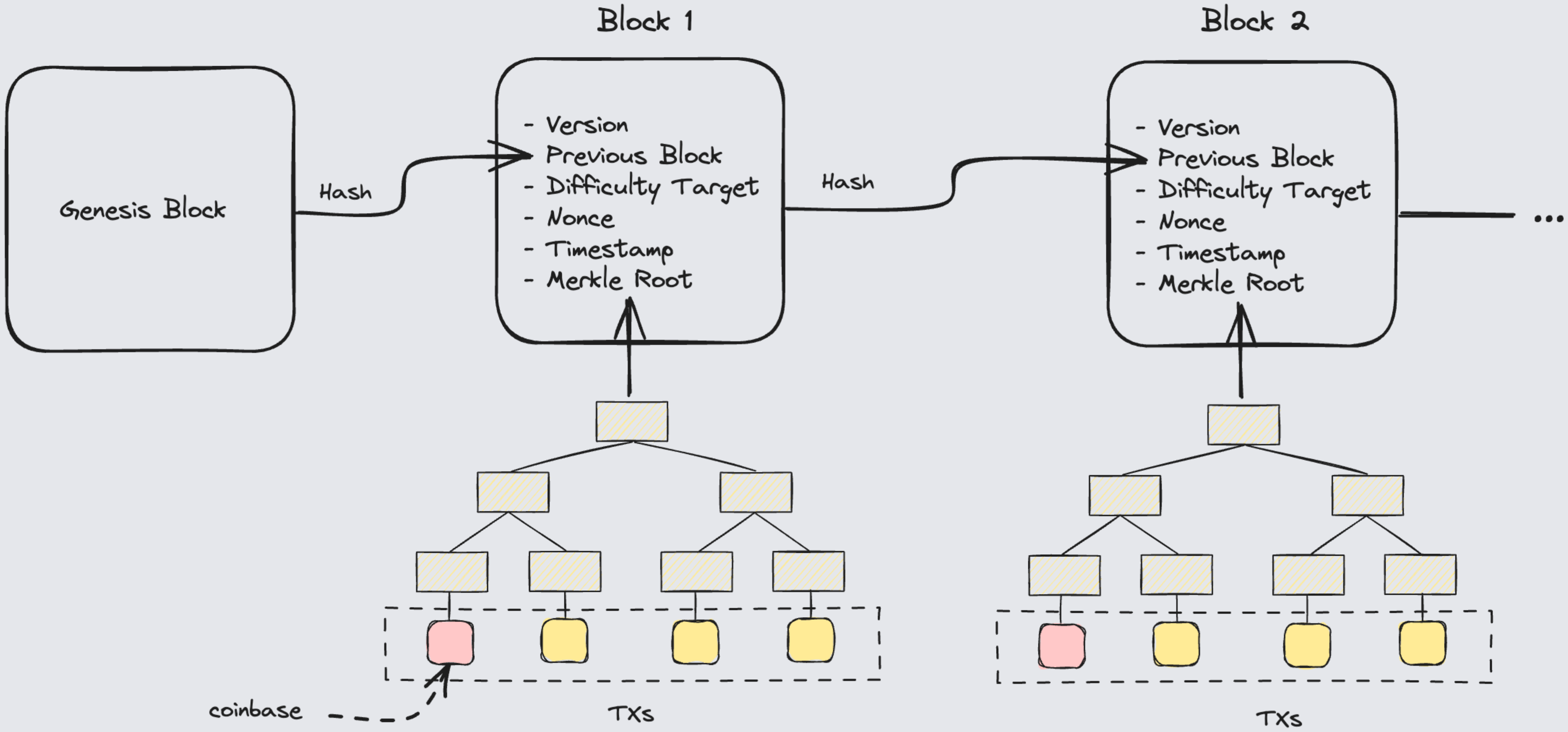
Bitcoin consensus

- The longest chain is considered the valid one.
- When temporary forks occur, nodes follow the chain with the most accumulated work (typically the longest).



Block

Bitcoin: sequence of block headers



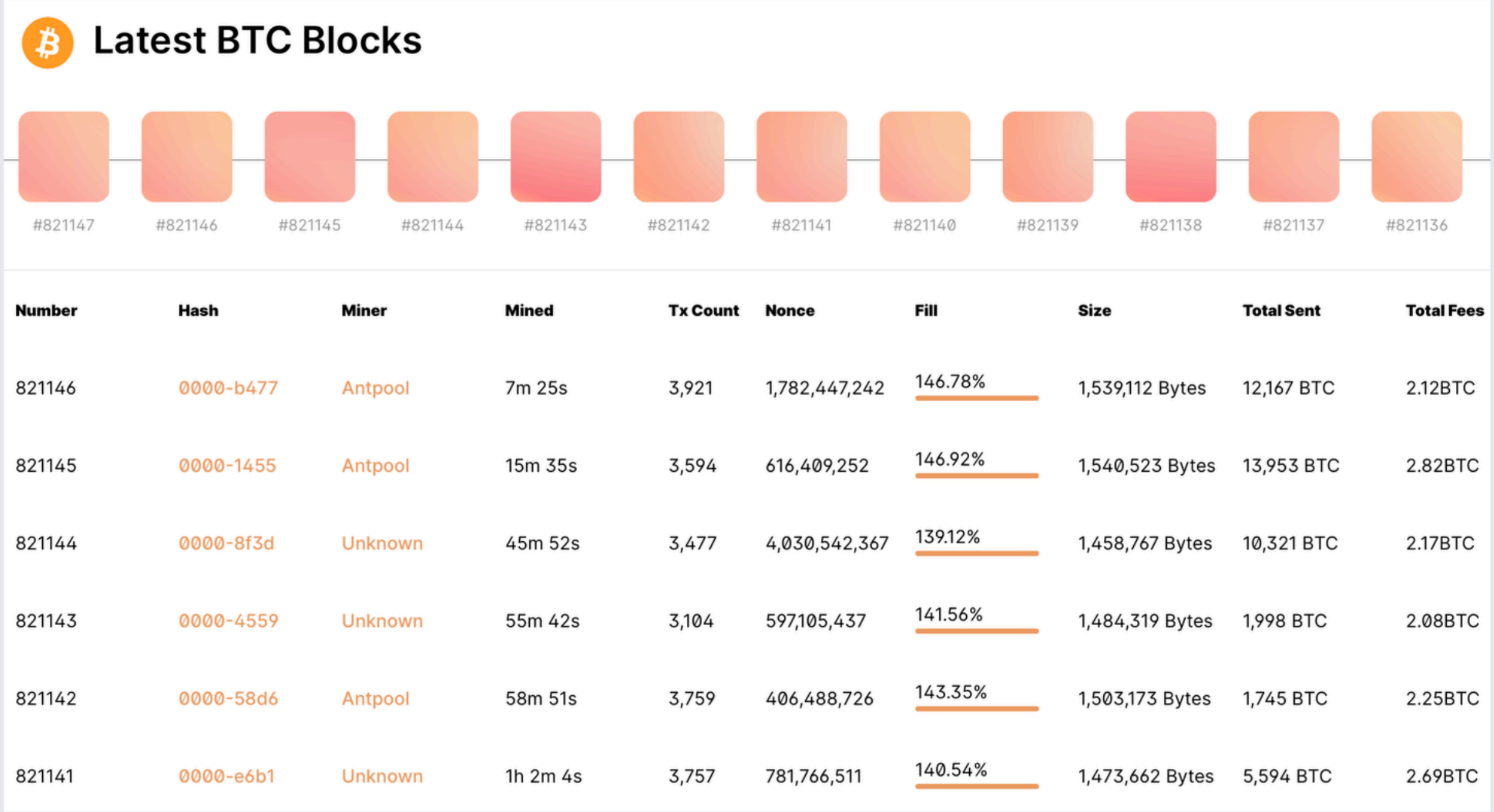
Block structure

Parameter	Description
`Block Size`	The size of the block in bytes.
`Block Header`	A 80-byte header of the block.
`Transaction Counter`	The number of transactions.
`Transactions`	The list of transactions included in the block.

Block header structure

Parameter	Description
`Version`	4-byte version number.
`Previous Block`	32-byte hash of the previous block in the blockchain.
`Merkle Root`	32-byte hash based on all of the transactions in the block.
`Timestamp`	4-byte timestamp recording when this block was created.
`Difficulty Target`	4-byte number used in PoW
`Nonce`	4-byte number used in PoW

Explore blocks (screen from blockchain.com)

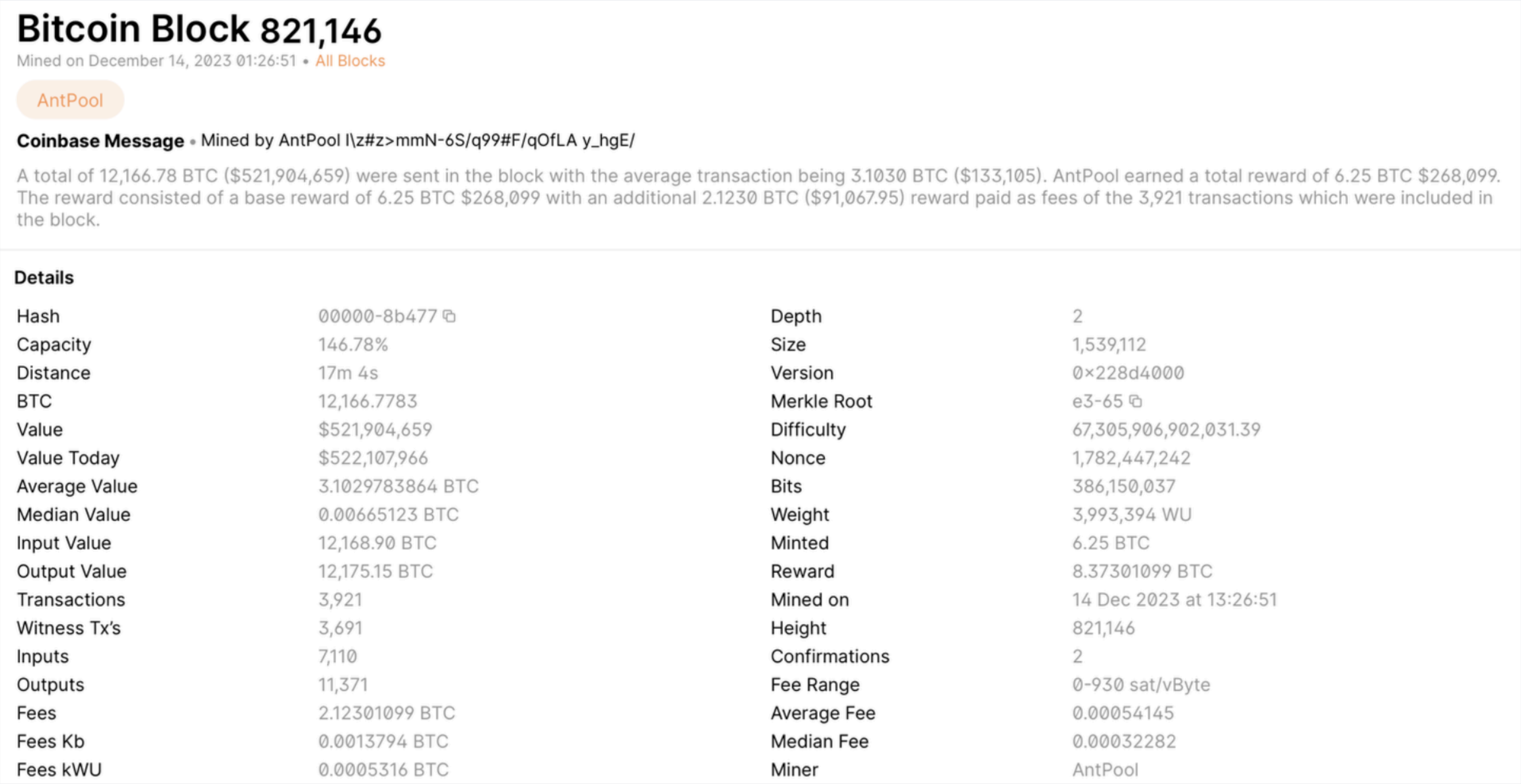


Latest BTC Blocks

#821147 #821146 #821145 #821144 #821143 #821142 #821141 #821140 #821139 #821138 #821137 #821136

Number	Hash	Miner	Mined	Tx Count	Nonce	Fill	Size	Total Sent	Total Fees
821146	0000-b477	Antpool	7m 25s	3,921	1,782,447,242	146.78%	1,539,112 Bytes	12,167 BTC	2.12BTC
821145	0000-1455	Antpool	15m 35s	3,594	616,409,252	146.92%	1,540,523 Bytes	13,953 BTC	2.82BTC
821144	0000-8f3d	Unknown	45m 52s	3,477	4,030,542,367	139.12%	1,458,767 Bytes	10,321 BTC	2.17BTC
821143	0000-4559	Unknown	55m 42s	3,104	597,105,437	141.56%	1,484,319 Bytes	1,998 BTC	2.08BTC
821142	0000-58d6	Antpool	58m 51s	3,759	406,488,726	143.35%	1,503,173 Bytes	1,745 BTC	2.25BTC
821141	0000-e6b1	Unknown	1h 2m 4s	3,757	781,766,511	140.54%	1,473,662 Bytes	5,594 BTC	2.69BTC

Explore blocks (screen from blockchain.com)



Bitcoin Block 821,146

Mined on December 14, 2023 01:26:51 • All Blocks

AntPool

Coinbase Message • Mined by AntPool I\z#z>mmN-6S/q99#F/qOfLA y_hgE/

A total of 12,166.78 BTC ($521,904,659) were sent in the block with the average transaction being 3.1030 BTC ($133,105). AntPool earned a total reward of 6.25 BTC $268,099. The reward consisted of a base reward of 6.25 BTC $268,099 with an additional 2.1230 BTC ($91,067.95) reward paid as fees of the 3,921 transactions which were included in the block.

Details

Hash	00000-8b477	Depth	2
Capacity	146.78%	Size	1,539,112
Distance	17m 4s	Version	0x228d4000
BTC	12,166.7783	Merkle Root	e3-65
Value	$521,904,659	Difficulty	67,305,906,902,031.39
Value Today	$522,107,966	Nonce	1,782,447,242
Average Value	3.1029783864 BTC	Bits	386,150,037
Median Value	0.00665123 BTC	Weight	3,993,394 WU
Input Value	12,168.90 BTC	Minted	6.25 BTC
Output Value	12,175.15 BTC	Reward	8.37301099 BTC
Transactions	3,921	Mined on	14 Dec 2023 at 13:26:51
Witness Tx's	3,691	Height	821,146
Inputs	7,110	Confirmations	2
Outputs	11,371	Fee Range	0-930 sat/vByte
Fees	2.12301099 BTC	Average Fee	0.00054145
Fees Kb	0.0013794 BTC	Median Fee	0.00032282
Fees kWU	0.0005316 BTC	Miner	AntPool

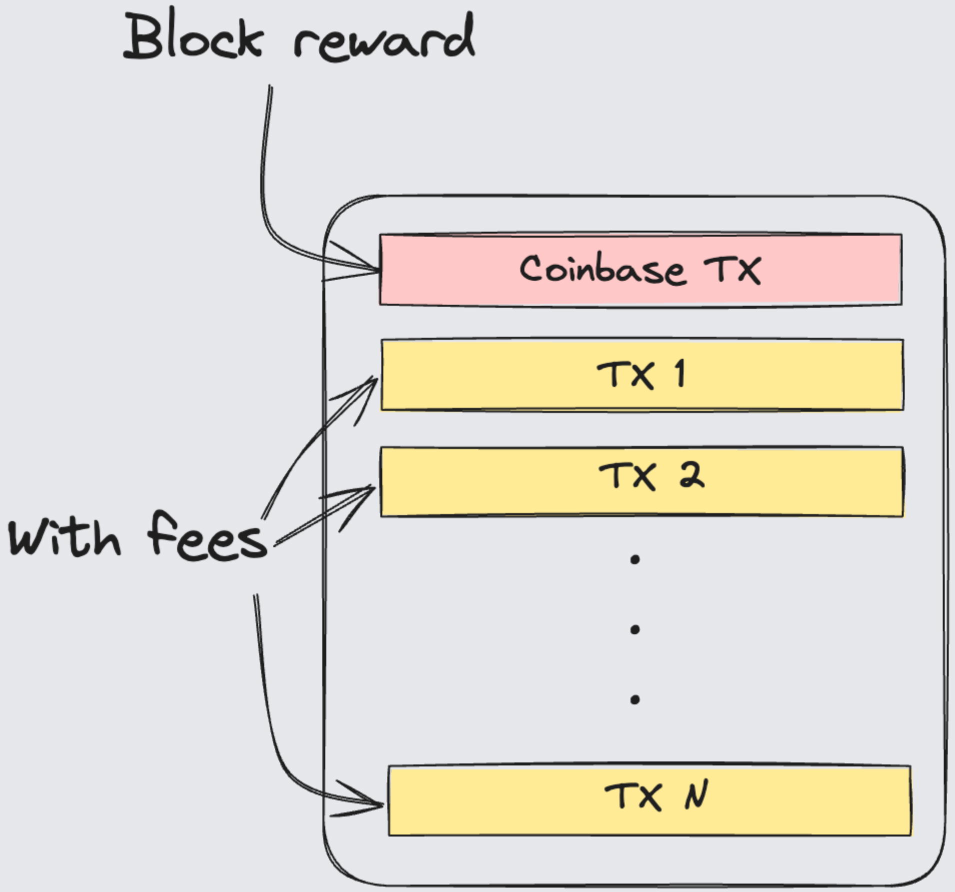
Visual demo

Let's play with Blockchain demo

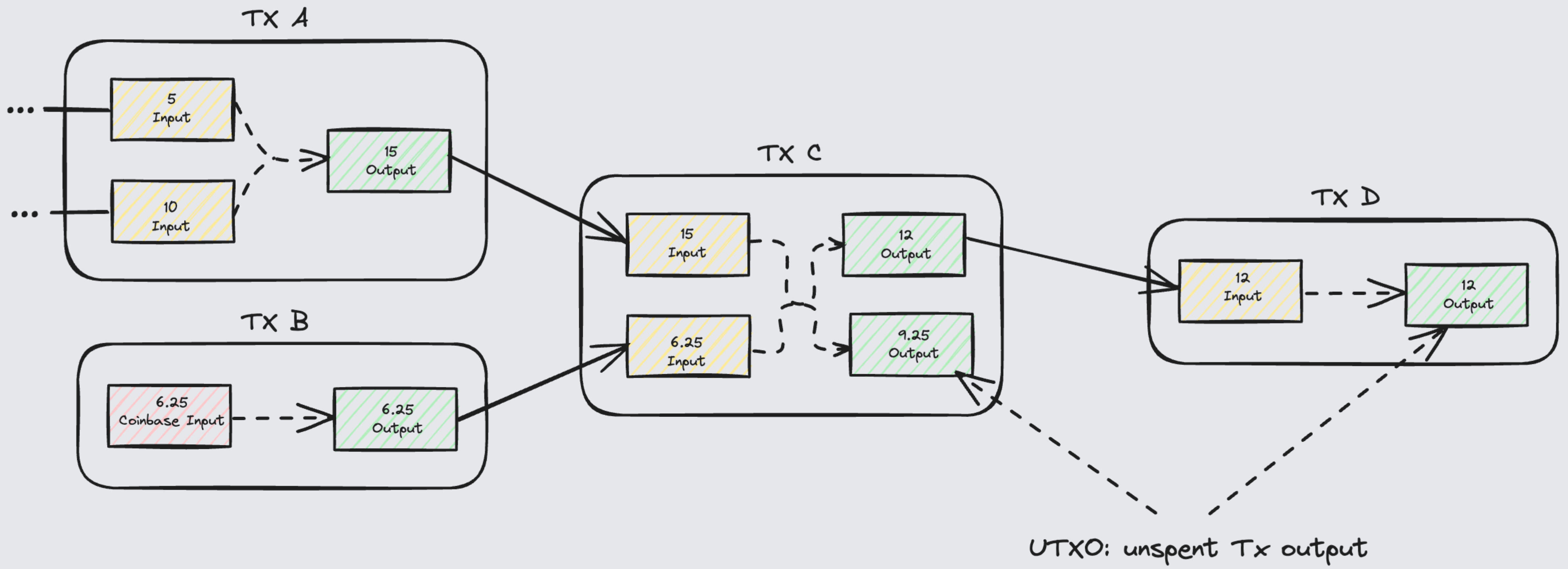
Transactions

Coinbase

- Miner reward consists of a block reward (coinbase) and tx fees.
- Block reward is halved after every 210,000 blocks (~4 years).
- Current reward is 3.125 BTC.



UTXO (Unspent Transaction Output)



TX structure

Parameter	Description
`Version`	Transaction data format version.
`Input Counter`	Number of transaction inputs.
`Inputs`	The list of transaction inputs.
`Output Counter`	Number of transaction outputs.
`Outputs`	The list of transaction outputs.
`Locktime`	Earliest block number that can include Tx

TX input

Parameter	Description
`Previous TX`	The hash of the transaction containing spending output
`Output Index`	The index of the spending output in the TX outputs
`Script Length`	The length of the input script.
`Signature Script`	A script which provides data to the previous output's scriptPubKey.
`Sequence`	A sequence number, currently disabled but reserved for future use.

TX output

Parameter	Description
`Value`	The number of Satoshis to spend to this output.
`Script Length`	The length of the output script.
`Pubkey Script`	A script which dictates the conditions required to spend this output.

TX validation

For each input in transaction, a miner node check:

- `Signature script | Pubkey script` returns true.
- `Previous TX | Output Index` is in the UTXO set.
- Previous TX is in the block.
- $\sum inputs \geq \sum outputs$

After a tx is executed, all its inputs are removed from UTXO set.

Script language

Bitcoin Script

- Programming language that is used to define the conditions under which UTXO can be spent.
- Stack-based, composed of opcodes.
- Intentionally not Turing-complete, with no loops.
- https://en.bitcoin.it/wiki/Script

Pay-to-Pubkey Hash (P2PKH)

One of the most common form of transaction on the Bitcoin.

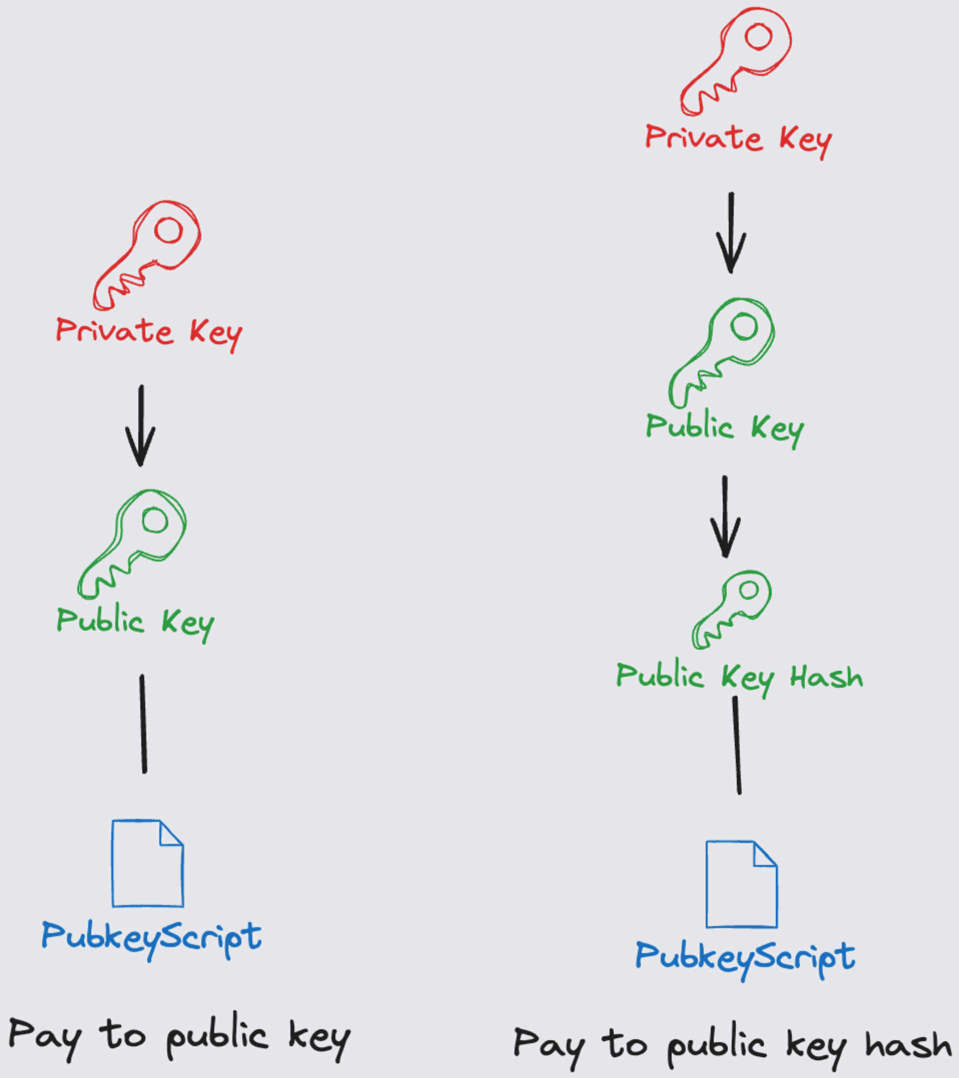
- https://en.bitcoinwiki.org/wiki/Pay-to-Pubkey_Hash

Pubkey script:

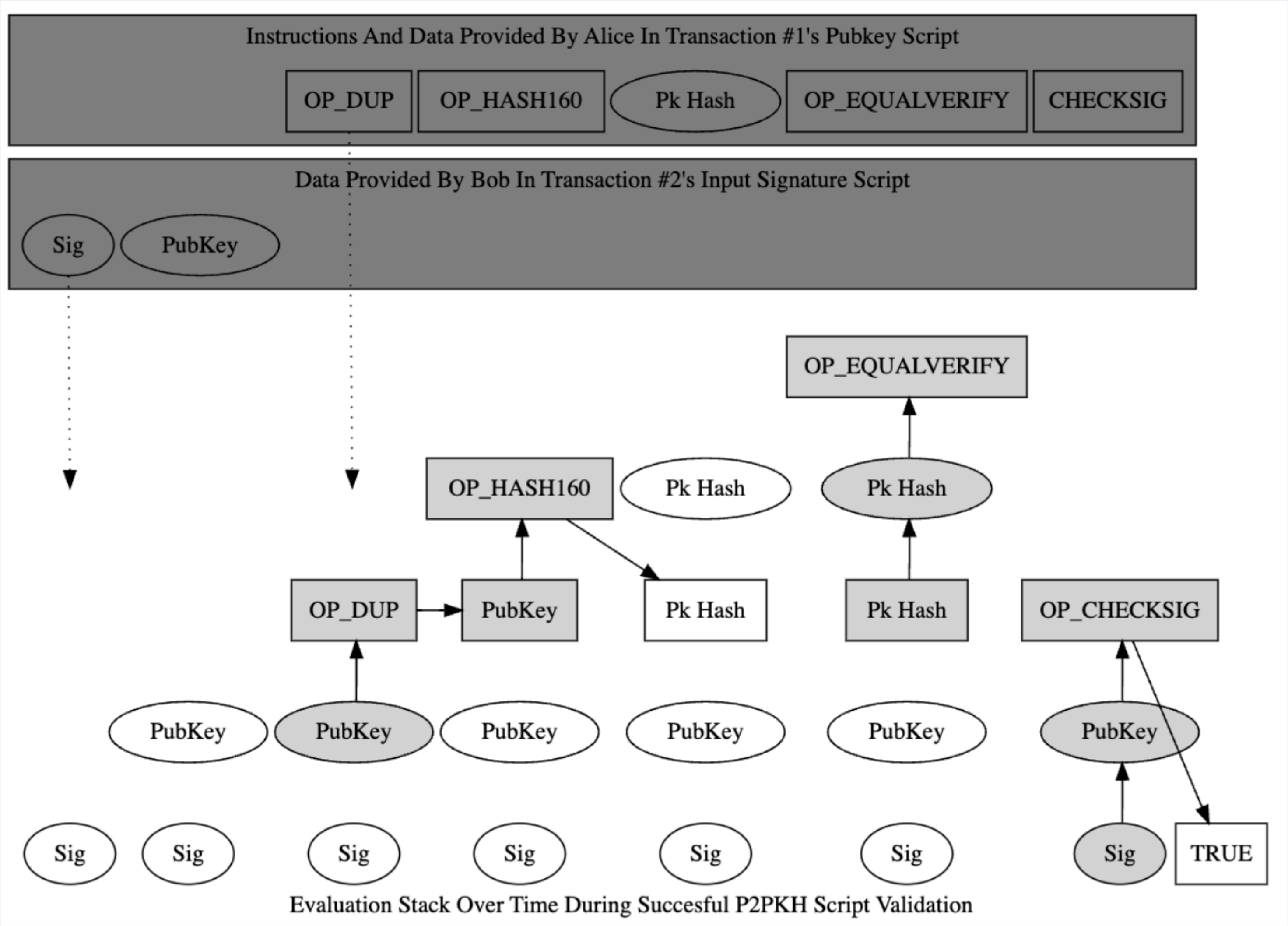
```
OP_DUP OP_HASH160 <PubkeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

Signature script:

```
<Sig> <PubKey>
```



P2PKH explained


Instructions And Data Provided By Alice In Transaction #1's Pubkey Script
OP_DUP
OP_HASH160
Pk Hash
OP_EQUALVERIFY
CHECKSIG
Data Provided By Bob In Transaction #2's Input Signature Script
Sig
PubKey
OP_EQUALVERIFY
OP_HASH160
Pk Hash
Pk Hash
OP_DUP
PubKey
Pk Hash
Pk Hash
OP_CHECKSIG
PubKey
PubKey
PubKey
PubKey
PubKey
PubKey
Sig
Sig
Sig
Sig
Sig
Sig
Sig
TRUE
Evaluation Stack Over Time During Succesful P2PKH Script Validation

Pay-to-Script Hash (P2SH)

Payer can specify a redeem script.

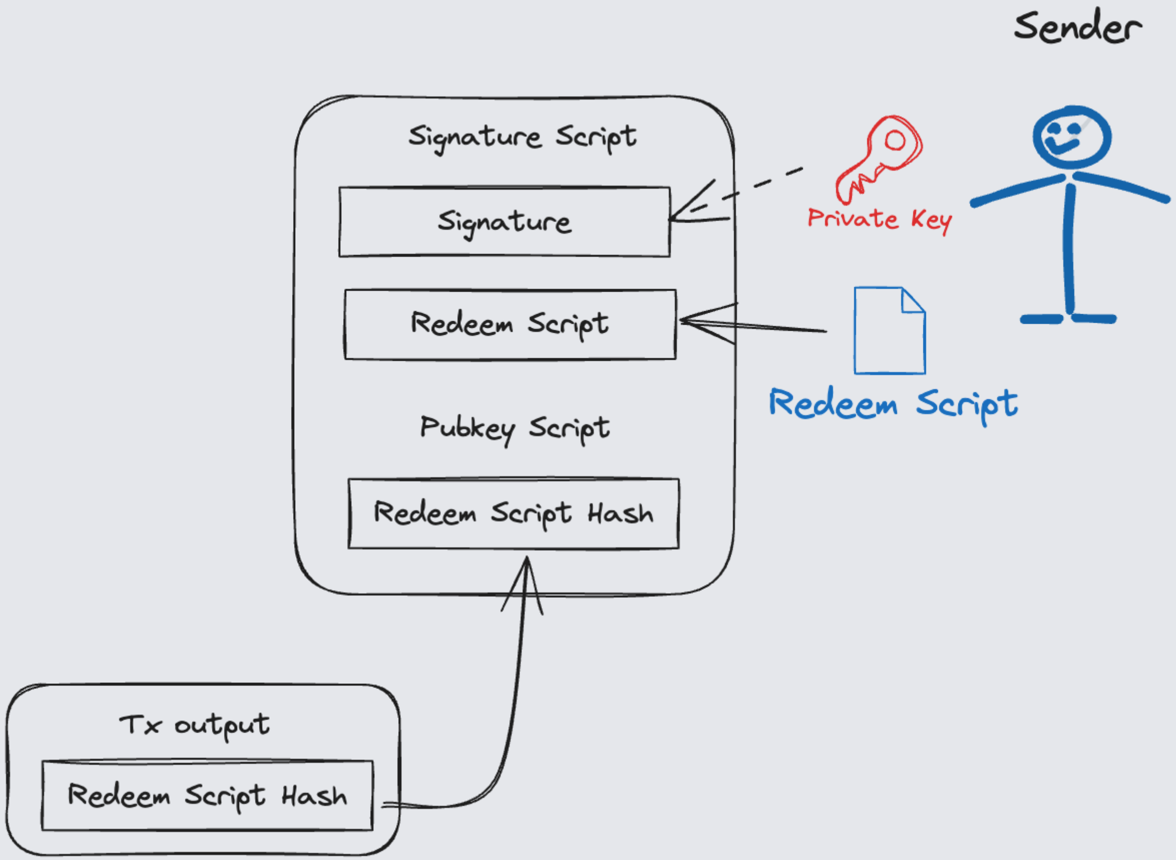
- https://en.bitcoinwiki.org/wiki/Pay-to-Script_Hash

Pubkey script:

```
HASH160 <H(Redeem Script)> EQUAL
```

Signature script:

```
<Sigs> <Redeem Script>
```



Segregated Witness (Segwit)

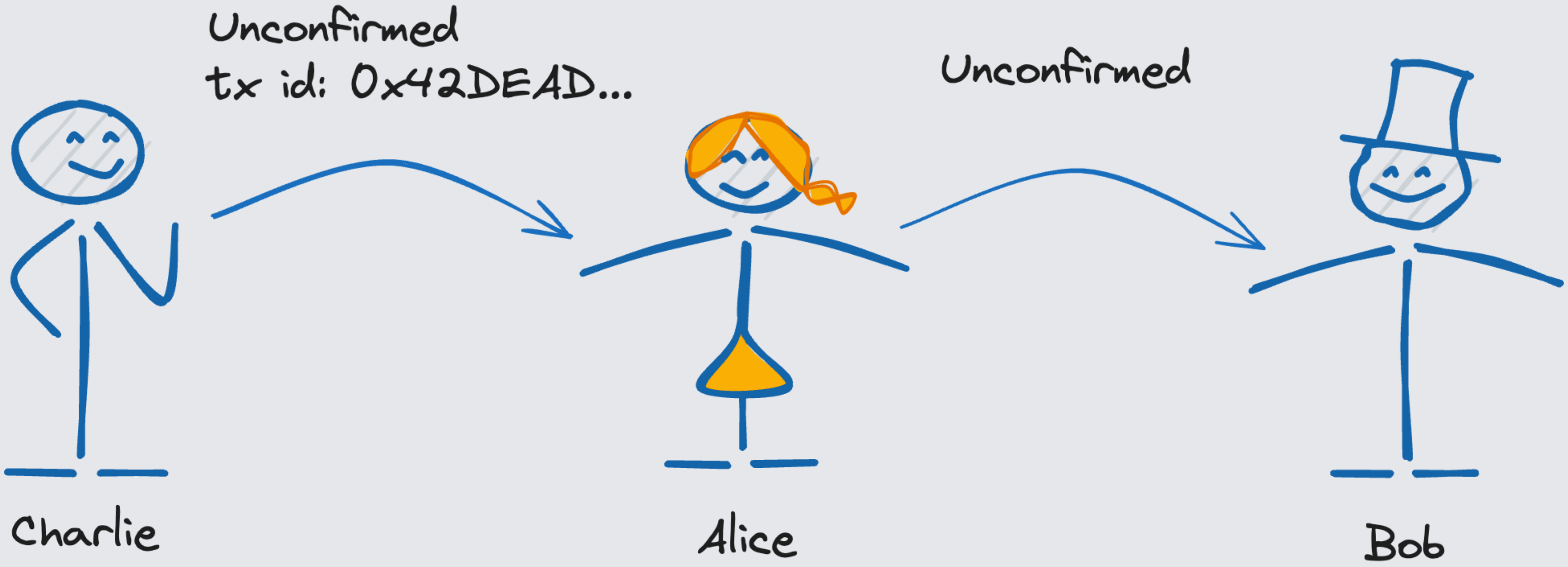
Problem

- Bitcoin has the block size limit of 1 Mb, which can't be changed without hard-fork.
- SegWit aims at reducing the size of transactions by separating the signature information (witness data) from the transaction data.

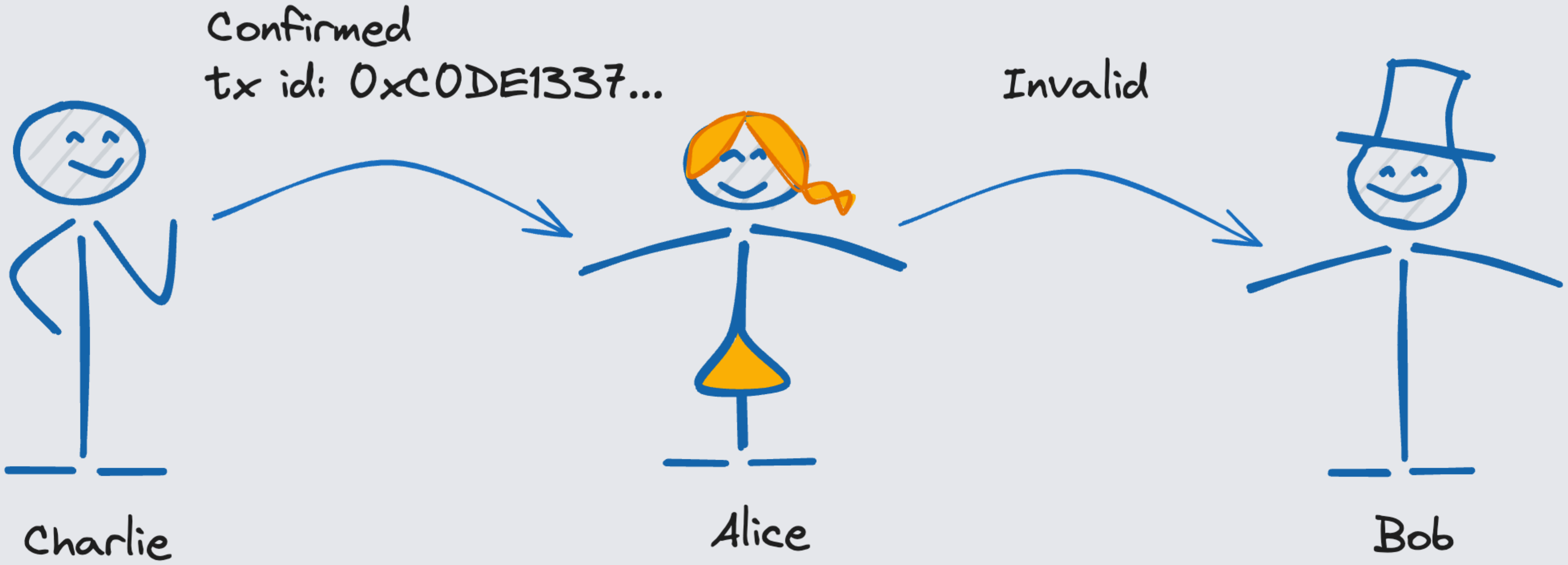
Signature alteration

Element	Original transaction	Altered transaction
Signature	`333...`	`0333...`
Mathematical value	`333...`	`333...`
Transaction id	`42DEAD...`	`C0DE1337...`

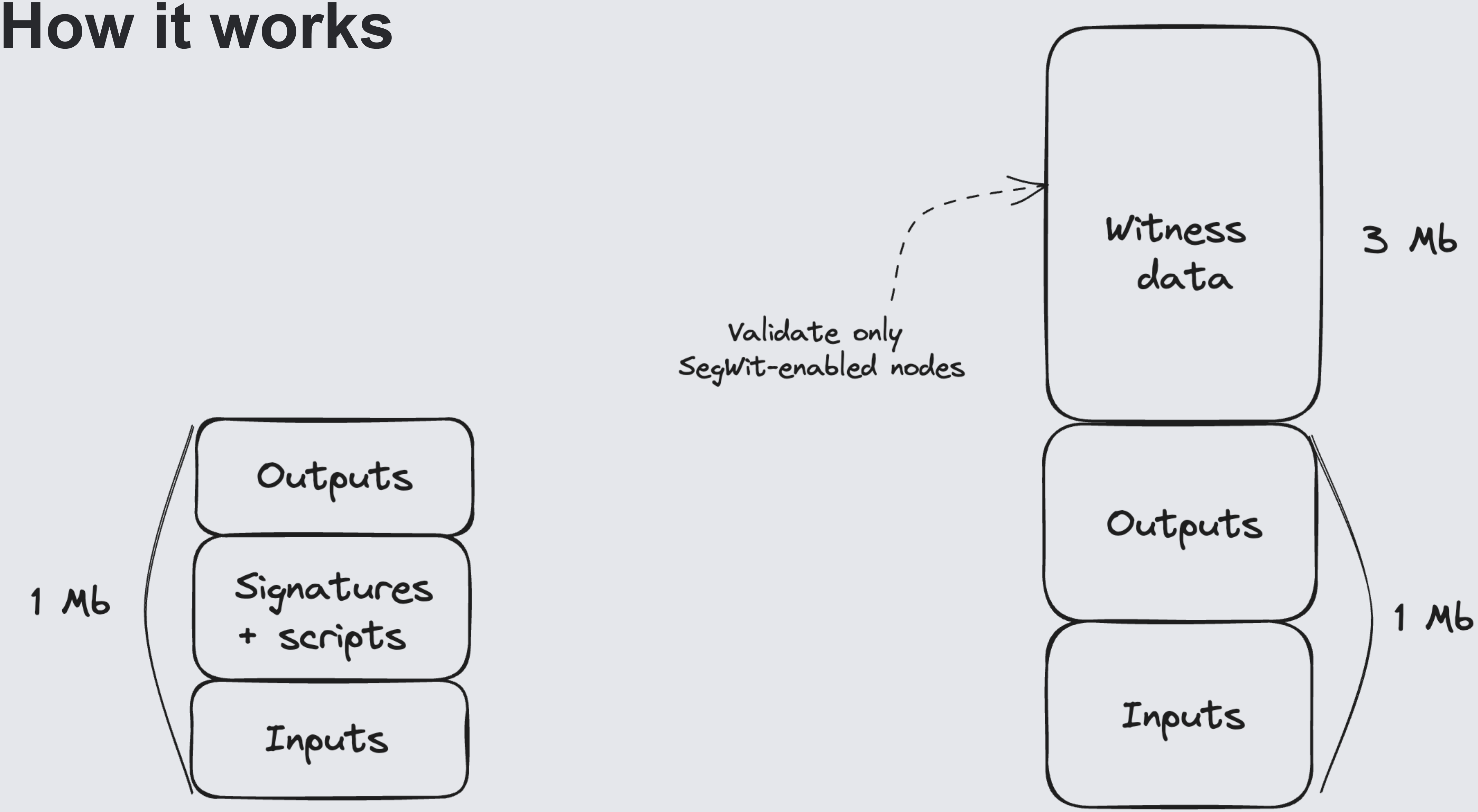
Signature alteration



Signature alteration



How it works



Outputs

Signatures + scripts

Inputs

1 Mb

Witness data

3 Mb

Validate only SegWit-enabled nodes

Outputs

Inputs

1 Mb

Quiz time!