Bitcoin Mechanics

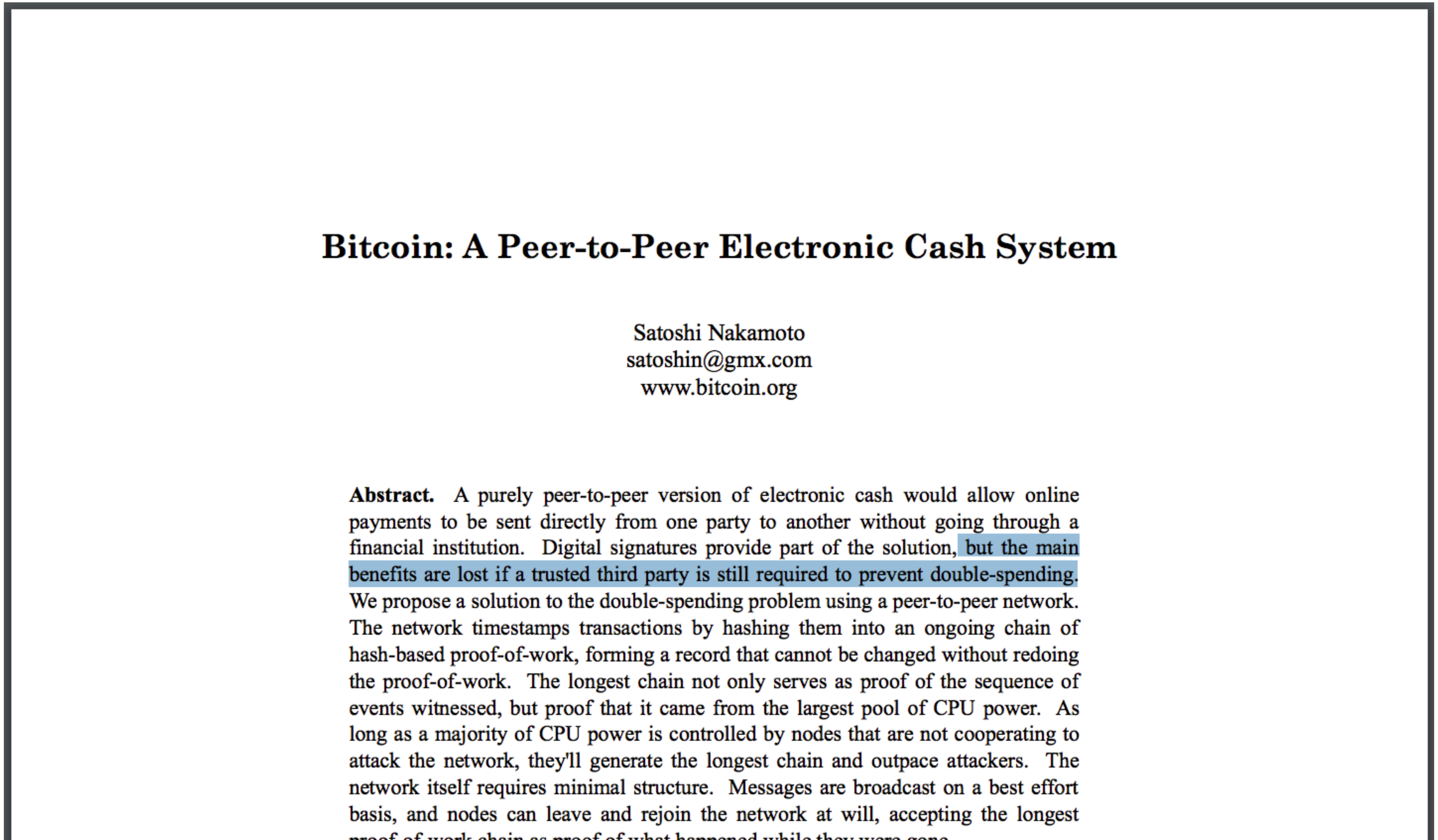
Ronghui Gu

Fall 2024

Columbia University

Course website: https://verigu.github.io/6998Fall2024/

Bitcoin

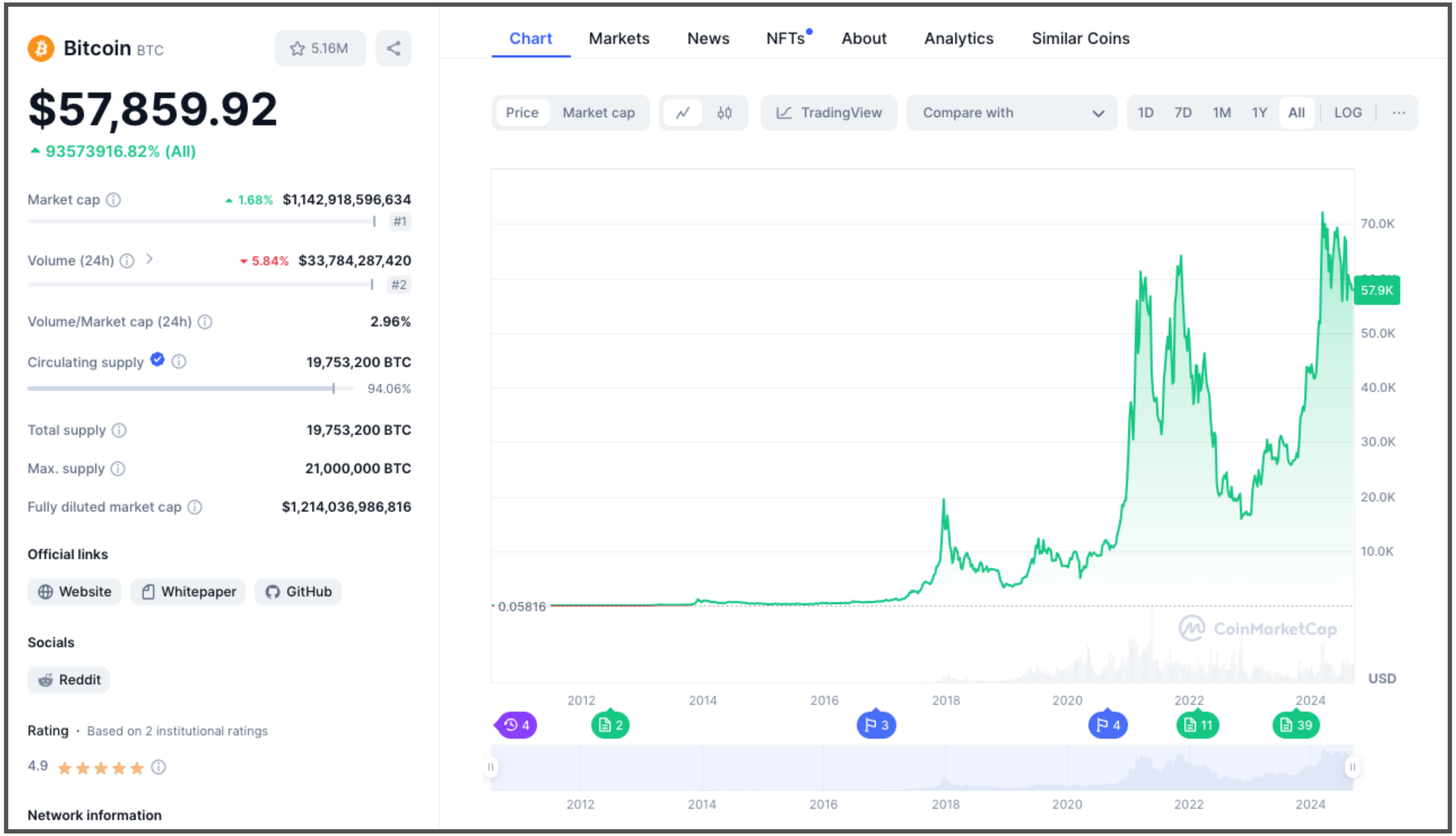


Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin MarketCap



Bitcoin BTC

$57,859.92

▲ 93573916.82% (All)

Market cap	▲ 1.68%	$1,142,918,596,634 #1
Volume (24h)	▼ 5.84%	$33,784,287,420 #2
Volume/Market cap (24h)		2.96%
Circulating supply		19,753,200 BTC 94.06%
Total supply		19,753,200 BTC
Max. supply		21,000,000 BTC
Fully diluted market cap		$1,214,036,986,816

Official links

Website Whitepaper GitHub

Socials

Reddit

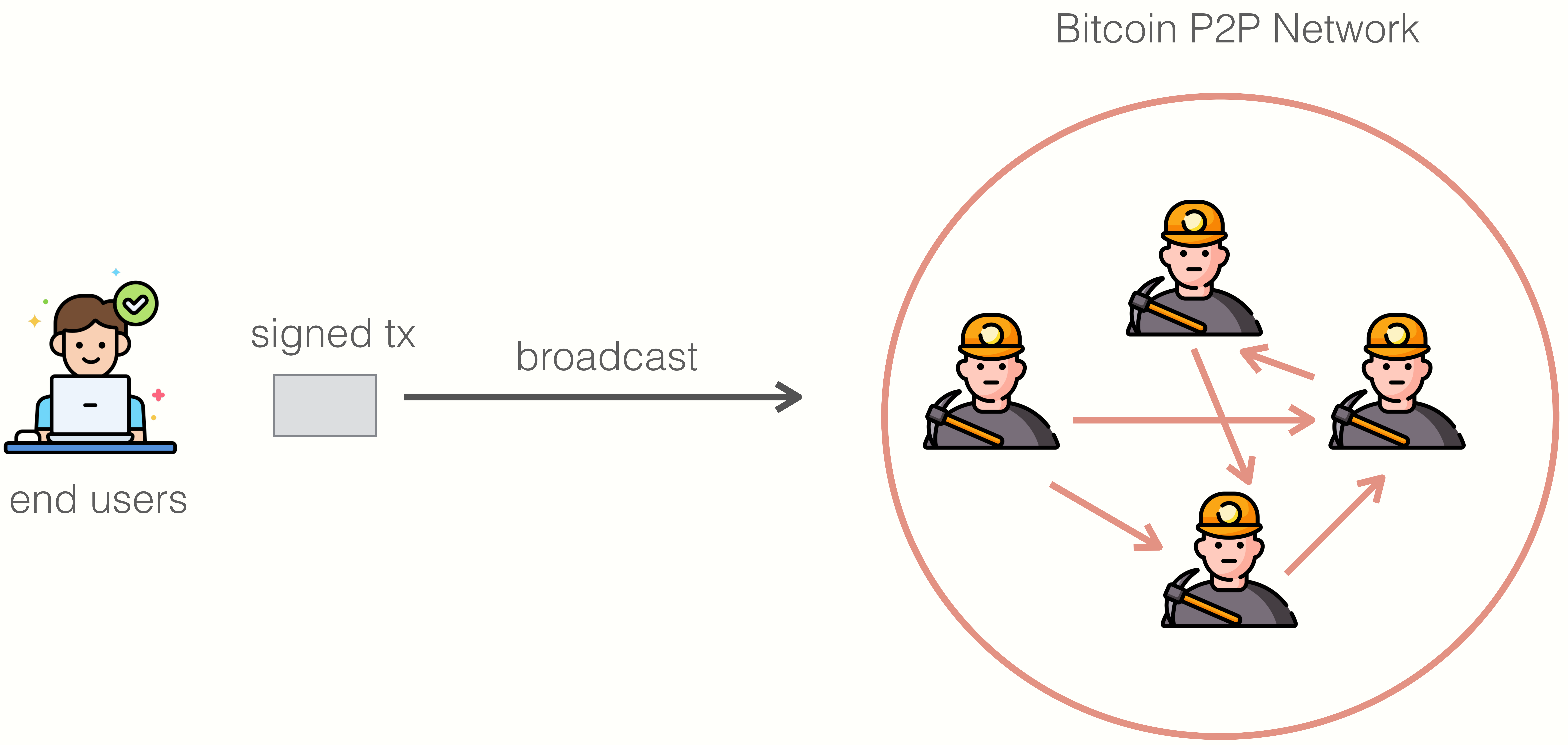
Rating · Based on 2 institutional ratings

4.9 ★★★★★

Network information

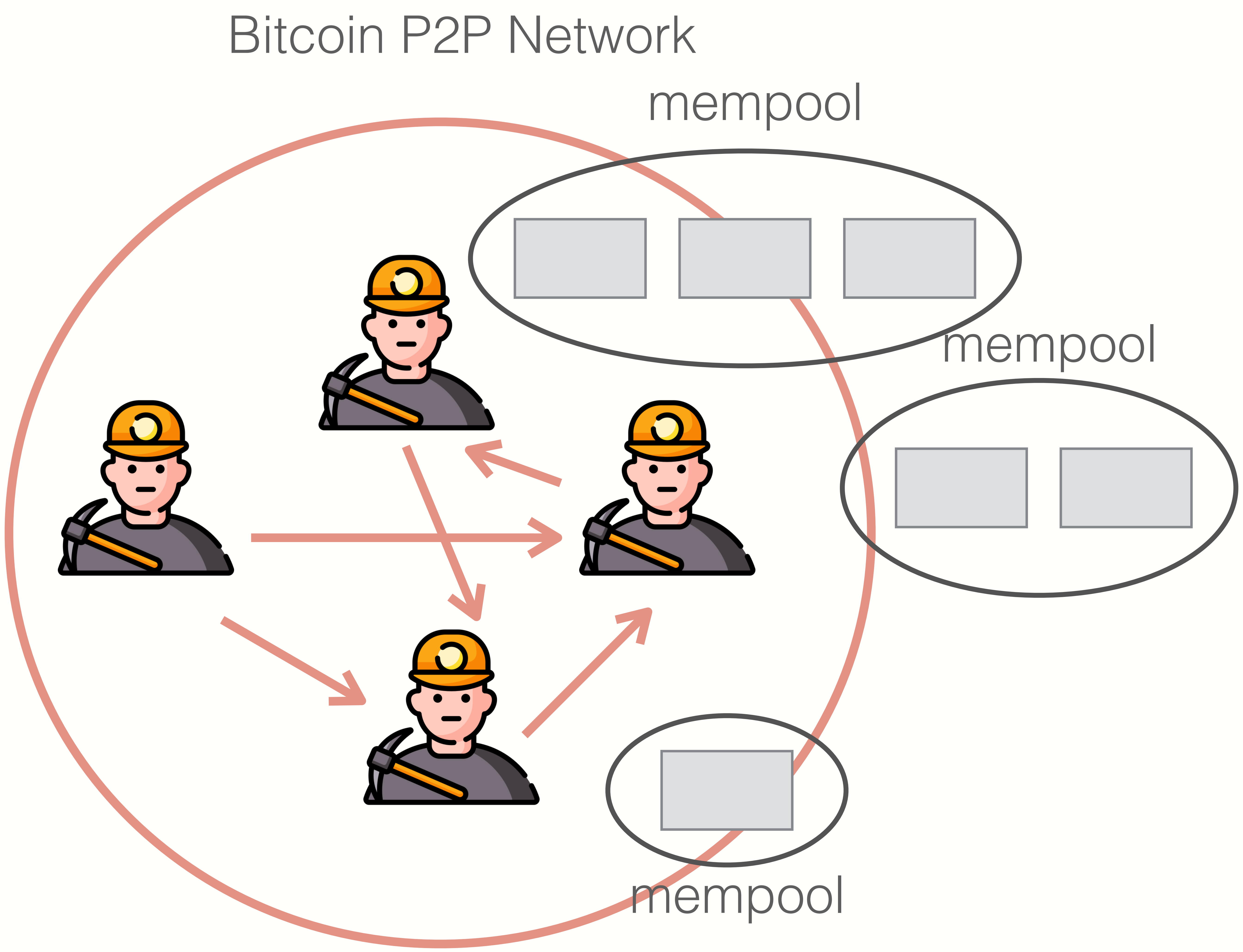
1 Bitcoin Network Overview

Bitcoin Network



Bitcoin Network

- Miners broadcast received Tx
- Every miner
  - Validates Tx
  - Stores them in its mempool

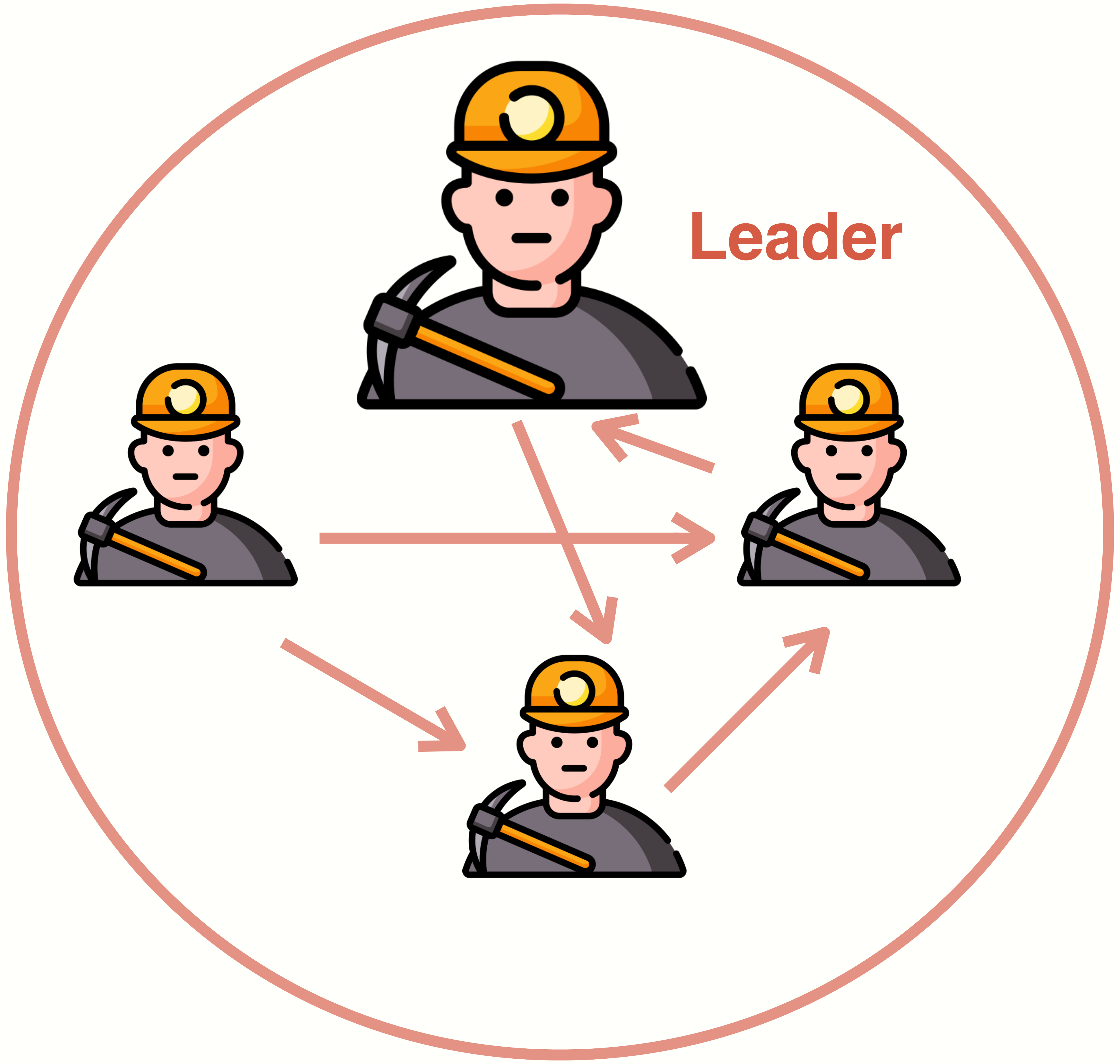


Bitcoin Network

Every 10 minutes:

- Miners create candidate blocks from Tx in its mempool
- A miner is selected (how?) and broadcasts it to P2P network
- All minters validate new block

Bitcoin P2P Network

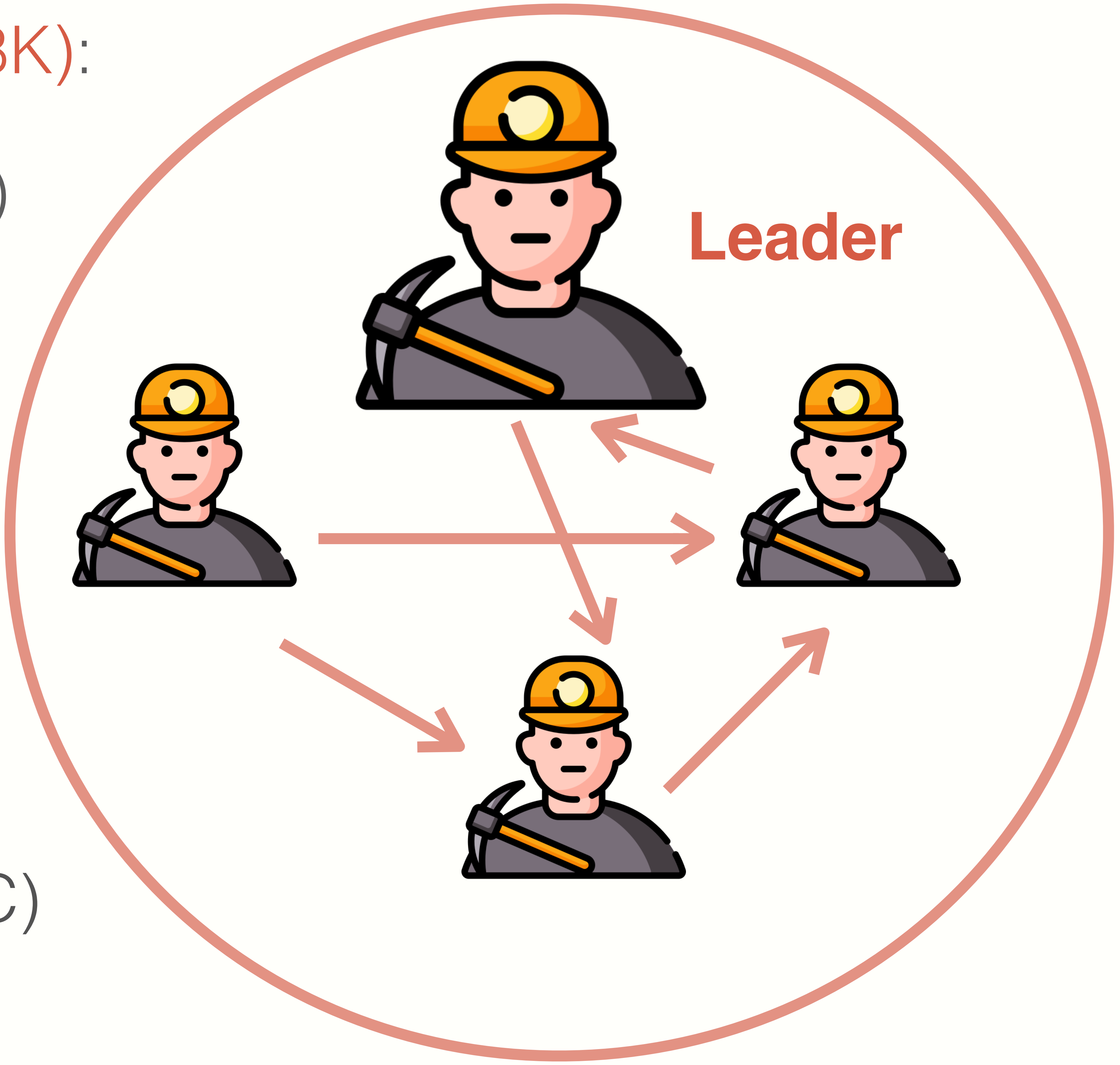


Bitcoin Network

Selected leader is paid 3.125 BTC ($178K):

- In coinbase Tx (first Tx in the block)
- Only way new BTC is created
- Block reward halves every 4 years
  - Now: 3.125 BTC
  - Initially: 50 BTC ($3M)
  - Max: 21M BTC (now 19.75M BTC)

Bitcoin P2P Network



Properties

Persistence

- To remove a block, need to convince 51% of mining power

Liveness

- To block a Tx from being posted, need to convince 51% of mining power

2 Bitcoin Blockchain

Bitcoin Blockchain: a sequence of block headers

Genesis Block

THE TIMES

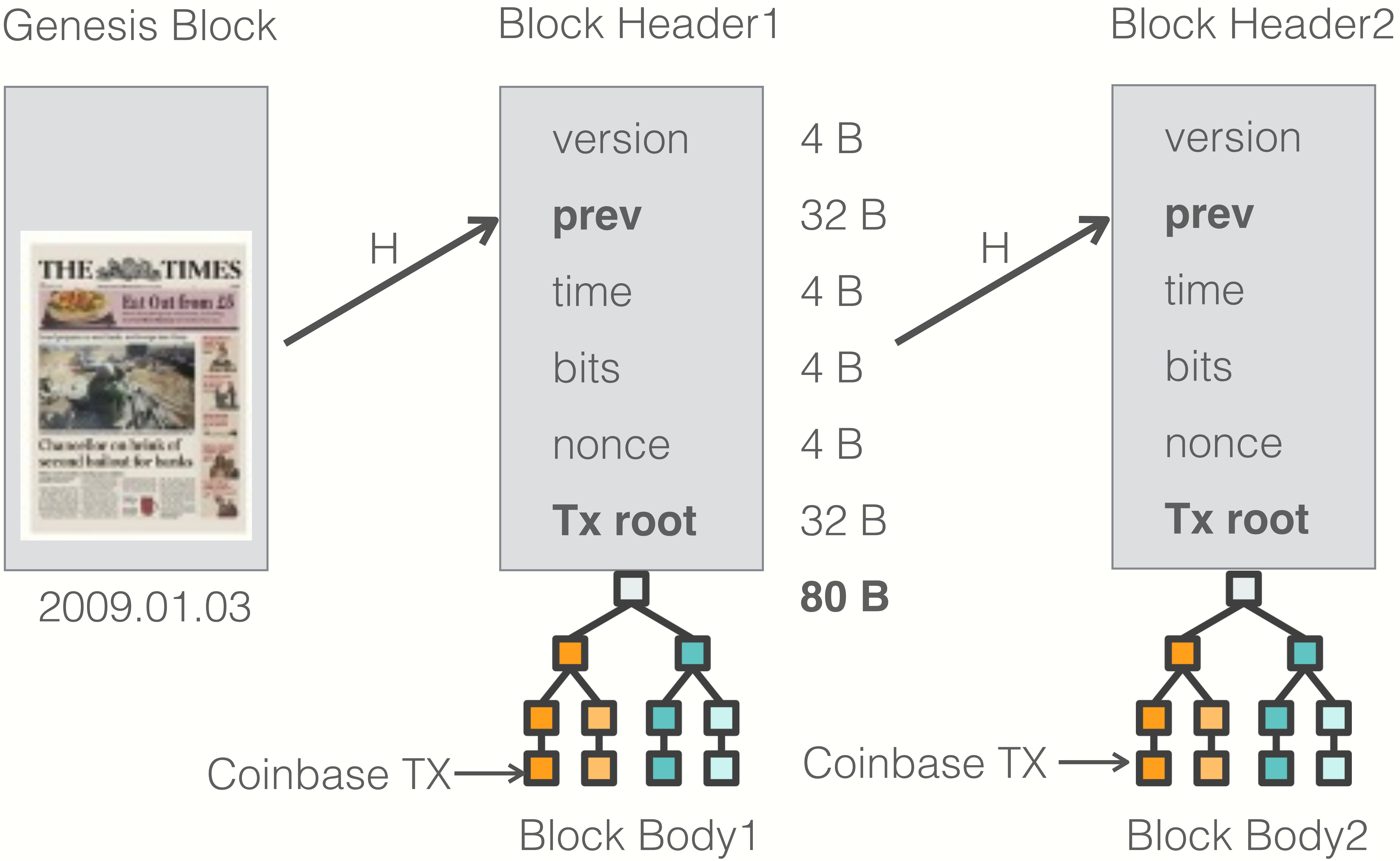
Eat Out from £5

Chancellor on brink of second bailout for banks

2009.01.03

> The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.
>
> — The Bitcoin Genesis Block

Bitcoin Blockchain: a sequence of block headers



Genesis Block

2009.01.03

H

Block Header1

version 4 B

prev 32 B

time 4 B

bits 4 B

nonce 4 B

Tx root 32 B

80 B

H

Block Header2

version

prev

time

bits

nonce

Tx root

Coinbase TX

Block Body1

Coinbase TX

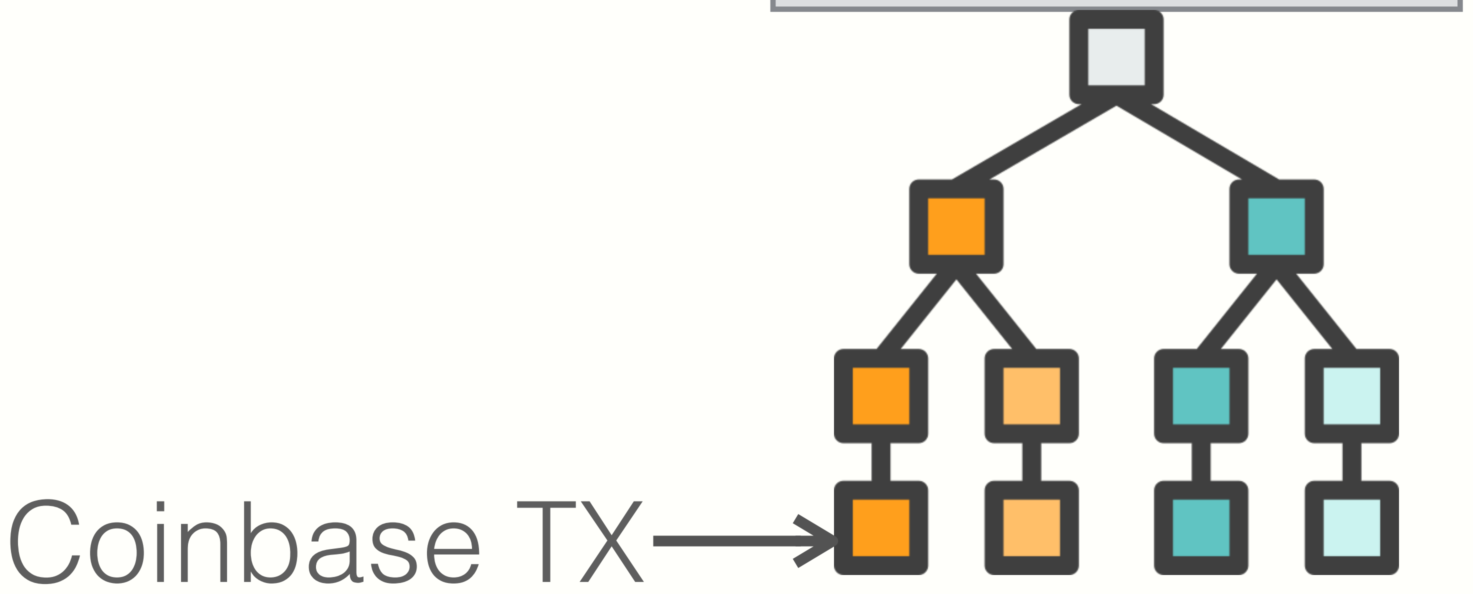
Block Body2

Bitcoin Blockchain: a sequence of block headers

- **time**: time miner assembled the block. Self reported. (block rejected if too far in past or future)
- **bits**: proof of work difficulty
  nonce: proof of work solution
- **Merkle tree**: payer can give a short proof that Tx is in the block

BH1

version	4 B
prev	32 B
time	4 B
bits	4 B
nonce	4 B
Tx root	32 B
	80 B



Bitcoin Blockchain: a sequence of block headers

Hash(

version

prev

time

bits

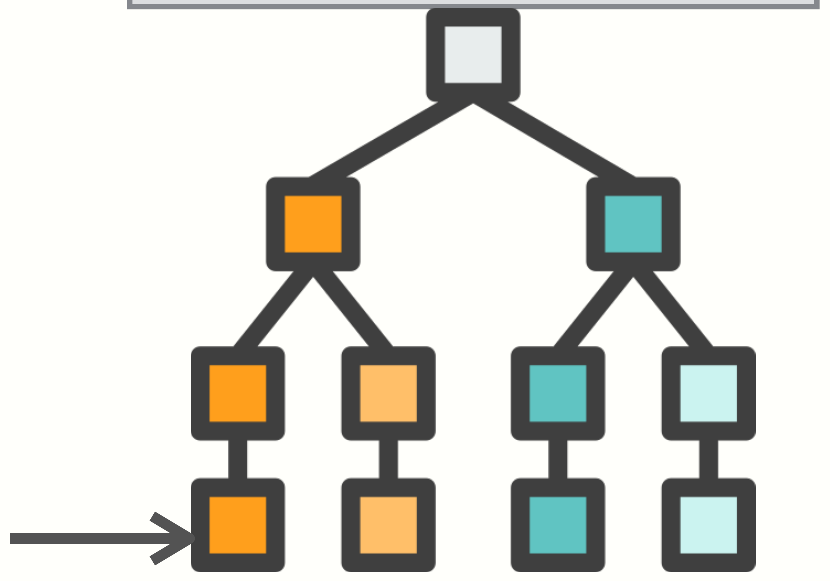
nonce

Tx root

) = 001BD63A

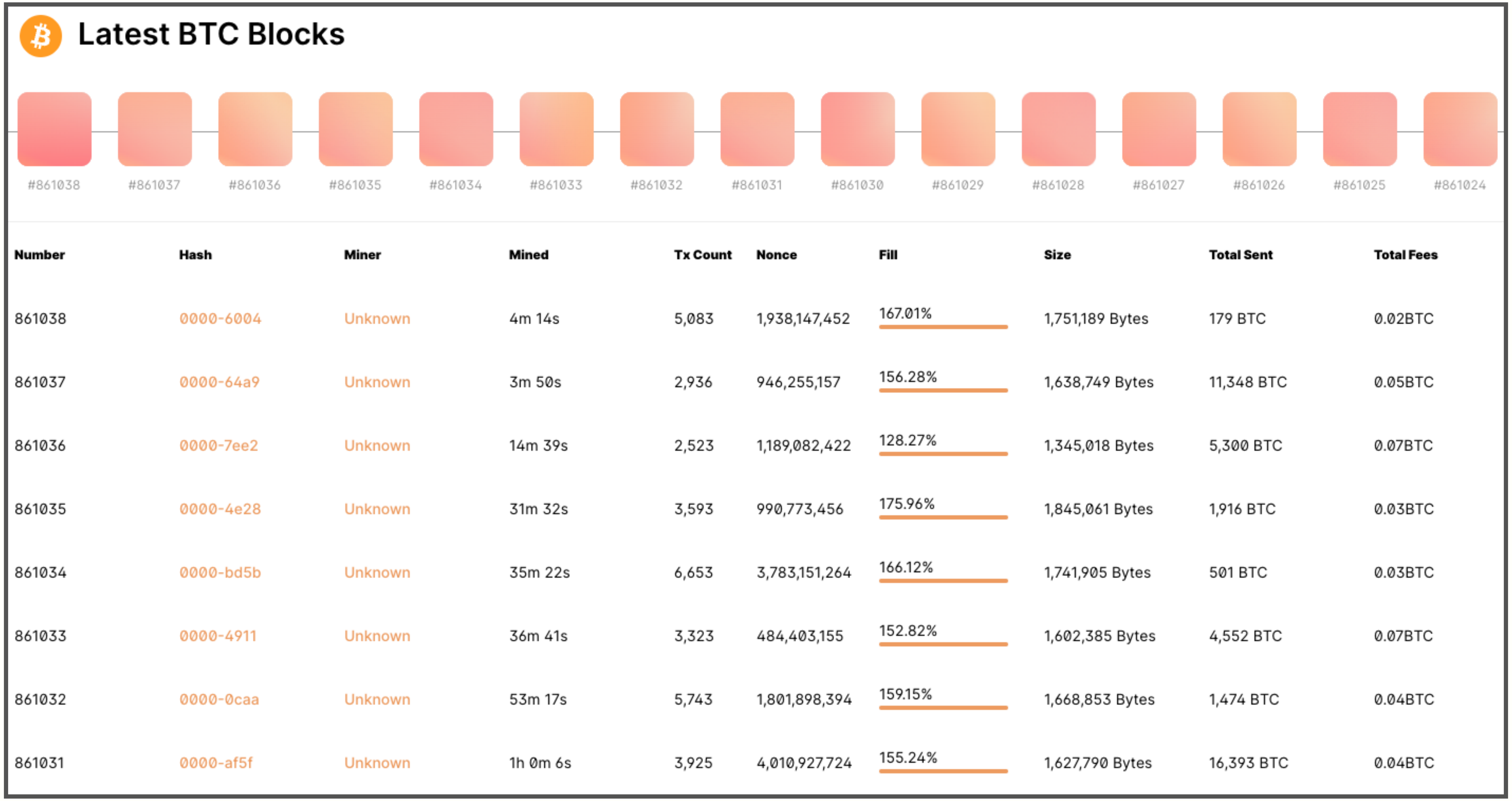
< 001FFFFF

Indicated by “**bits**”



Coinbase TX

An example

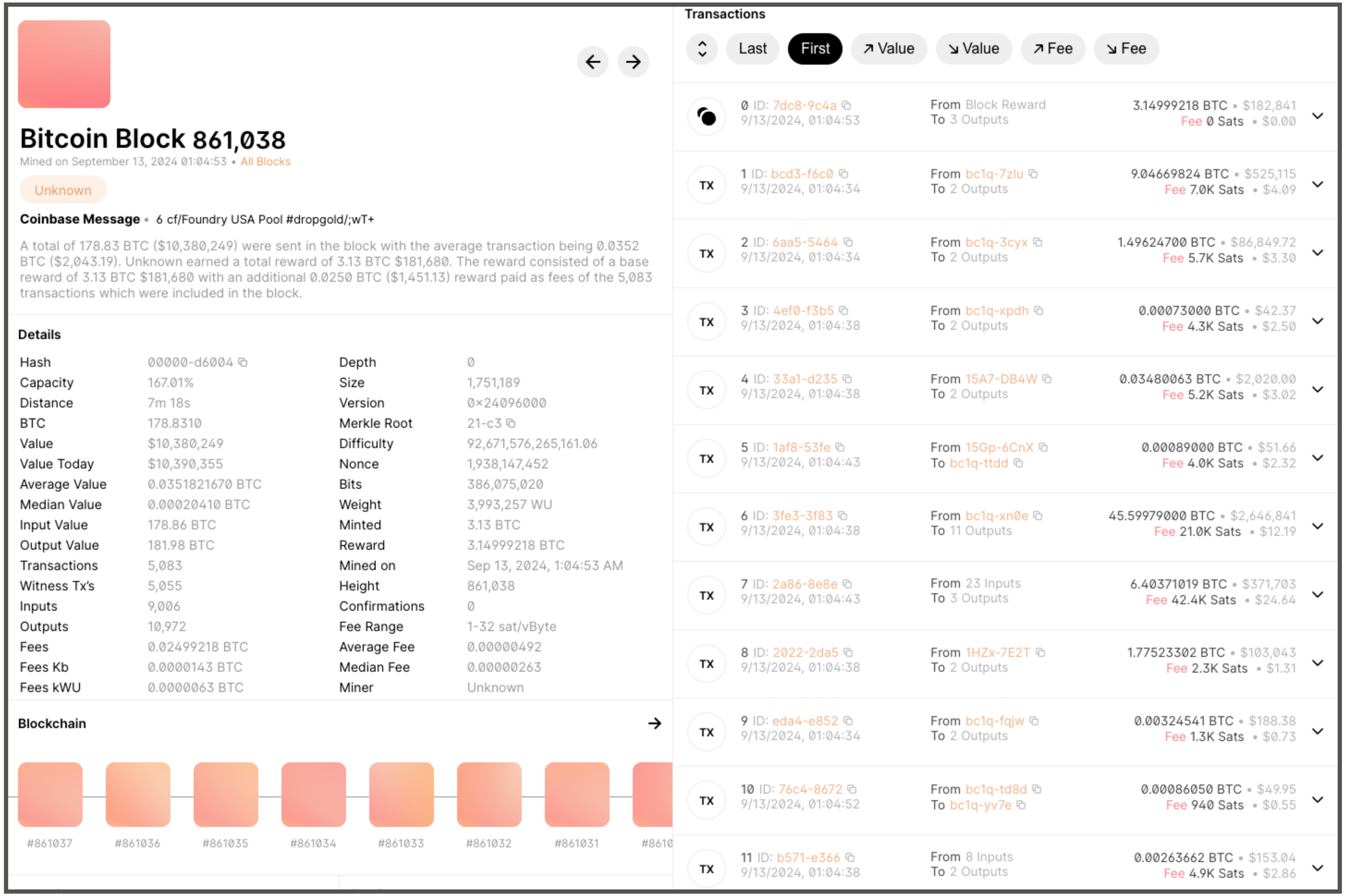


Latest BTC Blocks

#861038 #861037 #861036 #861035 #861034 #861033 #861032 #861031 #861030 #861029 #861028 #861027 #861026 #861025 #861024

Number	Hash	Miner	Mined	Tx Count	Nonce	Fill	Size	Total Sent	Total Fees
861038	0000-6004	Unknown	4m 14s	5,083	1,938,147,452	167.01%	1,751,189 Bytes	179 BTC	0.02BTC
861037	0000-64a9	Unknown	3m 50s	2,936	946,255,157	156.28%	1,638,749 Bytes	11,348 BTC	0.05BTC
861036	0000-7ee2	Unknown	14m 39s	2,523	1,189,082,422	128.27%	1,345,018 Bytes	5,300 BTC	0.07BTC
861035	0000-4e28	Unknown	31m 32s	3,593	990,773,456	175.96%	1,845,061 Bytes	1,916 BTC	0.03BTC
861034	0000-bd5b	Unknown	35m 22s	6,653	3,783,151,264	166.12%	1,741,905 Bytes	501 BTC	0.03BTC
861033	0000-4911	Unknown	36m 41s	3,323	484,403,155	152.82%	1,602,385 Bytes	4,552 BTC	0.07BTC
861032	0000-0caa	Unknown	53m 17s	5,743	1,801,898,394	159.15%	1,668,853 Bytes	1,474 BTC	0.04BTC
861031	0000-af5f	Unknown	1h 0m 6s	3,925	4,010,927,724	155.24%	1,627,790 Bytes	16,393 BTC	0.04BTC

An example



Bitcoin Block 861,038

Mined on September 13, 2024 01:04:53 • All Blocks

Unknown

Coinbase Message • 6 cf/Foundry USA Pool #dropgold/;wT+

A total of 178.83 BTC ($10,380,249) were sent in the block with the average transaction being 0.0352 BTC ($2,043.19). Unknown earned a total reward of 3.13 BTC $181,680. The reward consisted of a base reward of 3.13 BTC $181,680 with an additional 0.0250 BTC ($1,451.13) reward paid as fees of the 5,083 transactions which were included in the block.

Details

Hash	00000-d6004	Depth	0
Capacity	167.01%	Size	1,751,189
Distance	7m 18s	Version	0×24096000
BTC	178.8310	Merkle Root	21-c3
Value	$10,380,249	Difficulty	92,671,576,265,161.06
Value Today	$10,390,355	Nonce	1,938,147,452
Average Value	0.0351821670 BTC	Bits	386,075,020
Median Value	0.00020410 BTC	Weight	3,993,257 WU
Input Value	178.86 BTC	Minted	3.13 BTC
Output Value	181.98 BTC	Reward	3.14999218 BTC
Transactions	5,083	Mined on	Sep 13, 2024, 1:04:53 AM
Witness Tx's	5,055	Height	861,038
Inputs	9,006	Confirmations	0
Outputs	10,972	Fee Range	1-32 sat/vByte
Fees	0.02499218 BTC	Average Fee	0.00000492
Fees Kb	0.0000143 BTC	Median Fee	0.00000263
Fees kWU	0.0000063 BTC	Miner	Unknown

Blockchain

#861037 #861036 #861035 #861034 #861033 #861032 #861031 #8610

Transactions

0 ID: 7dc8-9c4a
9/13/2024, 01:04:53
From Block Reward
To 3 Outputs
3.14999218 BTC • $182,841
Fee 0 Sats • $0.00

TX 1 ID: bcd3-f6c0
9/13/2024, 01:04:34
From bc1q-7zlu
To 2 Outputs
9.04669824 BTC • $525,115
Fee 7.0K Sats • $4.09

TX 2 ID: 6aa5-5464
9/13/2024, 01:04:34
From bc1q-3cyx
To 2 Outputs
1.49624700 BTC • $86,849.72
Fee 5.7K Sats • $3.30

TX 3 ID: 4ef0-f3b5
9/13/2024, 01:04:38
From bc1q-xpdh
To 2 Outputs
0.00073000 BTC • $42.37
Fee 4.3K Sats • $2.50

TX 4 ID: 33a1-d235
9/13/2024, 01:04:38
From 15A7-DB4W
To 2 Outputs
0.03480063 BTC • $2,020.00
Fee 5.2K Sats • $3.02

TX 5 ID: 1af8-53fe
9/13/2024, 01:04:43
From 15Gp-6CnX
To bc1q-ttdd
0.00089000 BTC • $51.66
Fee 4.0K Sats • $2.32

TX 6 ID: 3fe3-3f83
9/13/2024, 01:04:38
From bc1q-xn0e
To 11 Outputs
45.59979000 BTC • $2,646,841
Fee 21.0K Sats • $12.19

TX 7 ID: 2a86-8e8e
9/13/2024, 01:04:43
From 23 Inputs
To 3 Outputs
6.40371019 BTC • $371,703
Fee 42.4K Sats • $24.64

TX 8 ID: 2022-2da5
9/13/2024, 01:04:38
From 1HZx-7E2T
To 2 Outputs
1.77523302 BTC • $103,043
Fee 2.3K Sats • $1.31

TX 9 ID: eda4-e852
9/13/2024, 01:04:34
From bc1q-fqjw
To 2 Outputs
0.00324541 BTC • $188.38
Fee 1.3K Sats • $0.73

TX 10 ID: 76c4-8672
9/13/2024, 01:04:52
From bc1q-td8d
To bc1q-yv7e
0.00086050 BTC • $49.95
Fee 940 Sats • $0.55

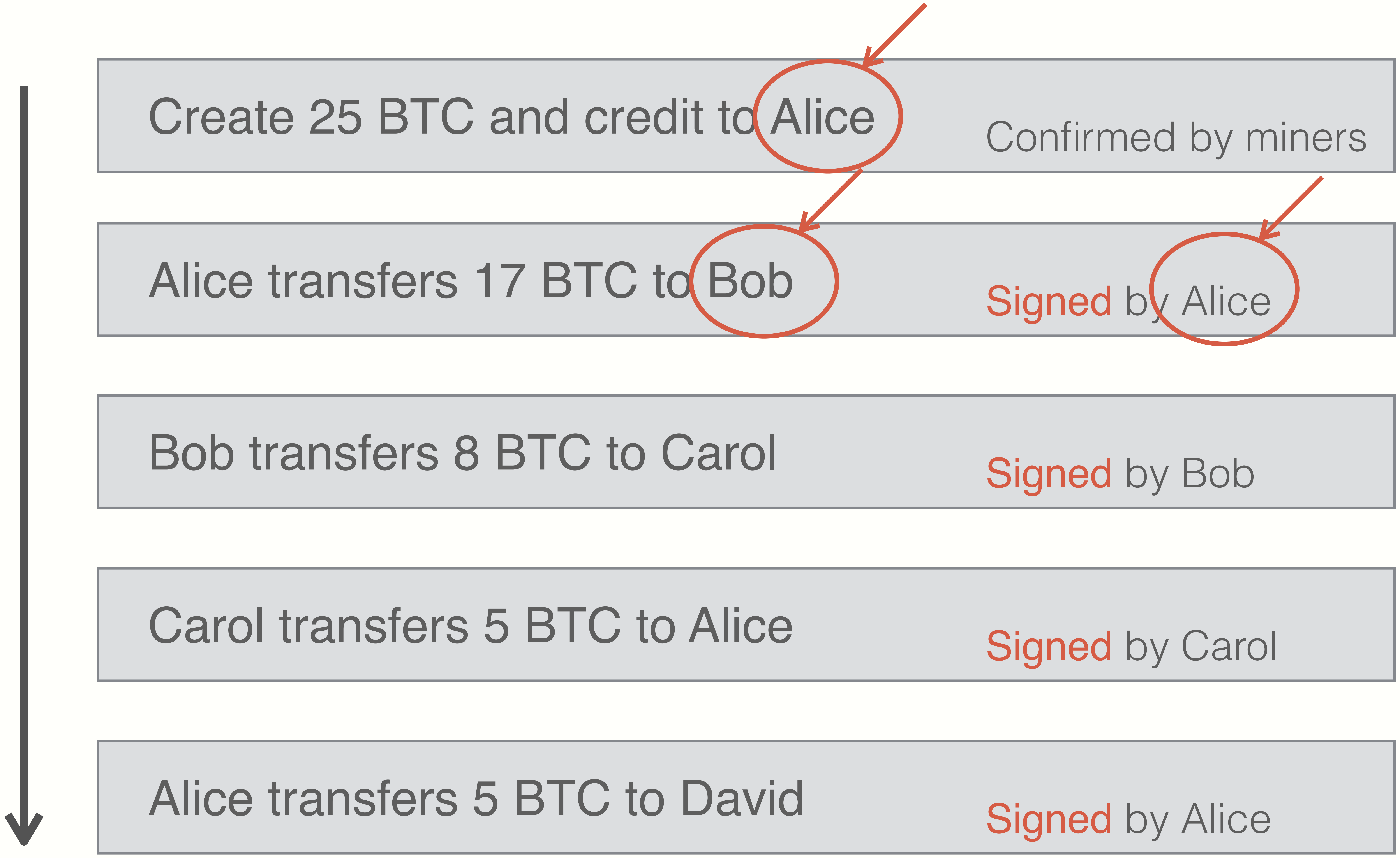
TX 11 ID: b571-e366
9/13/2024, 01:04:38
From 8 Inputs
To 2 Outputs
0.00263662 BTC • $153.04
Fee 4.9K Sats • $2.86

3 Bitcoin Transactions

Bitcoins exist as records of Bitcoin transactions

> We define a bitcoin as **a chain of digital signatures**. Each owner transfers bitcoin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.
>
> — Satoshi Nakamoto

Bitcoins exist as records of Bitcoin transactions



Create 25 BTC and credit to Alice — Confirmed by miners

Alice transfers 17 BTC to Bob — Signed by Alice

Bob transfers 8 BTC to Carol — Signed by Bob

Carol transfers 5 BTC to Alice — Signed by Carol

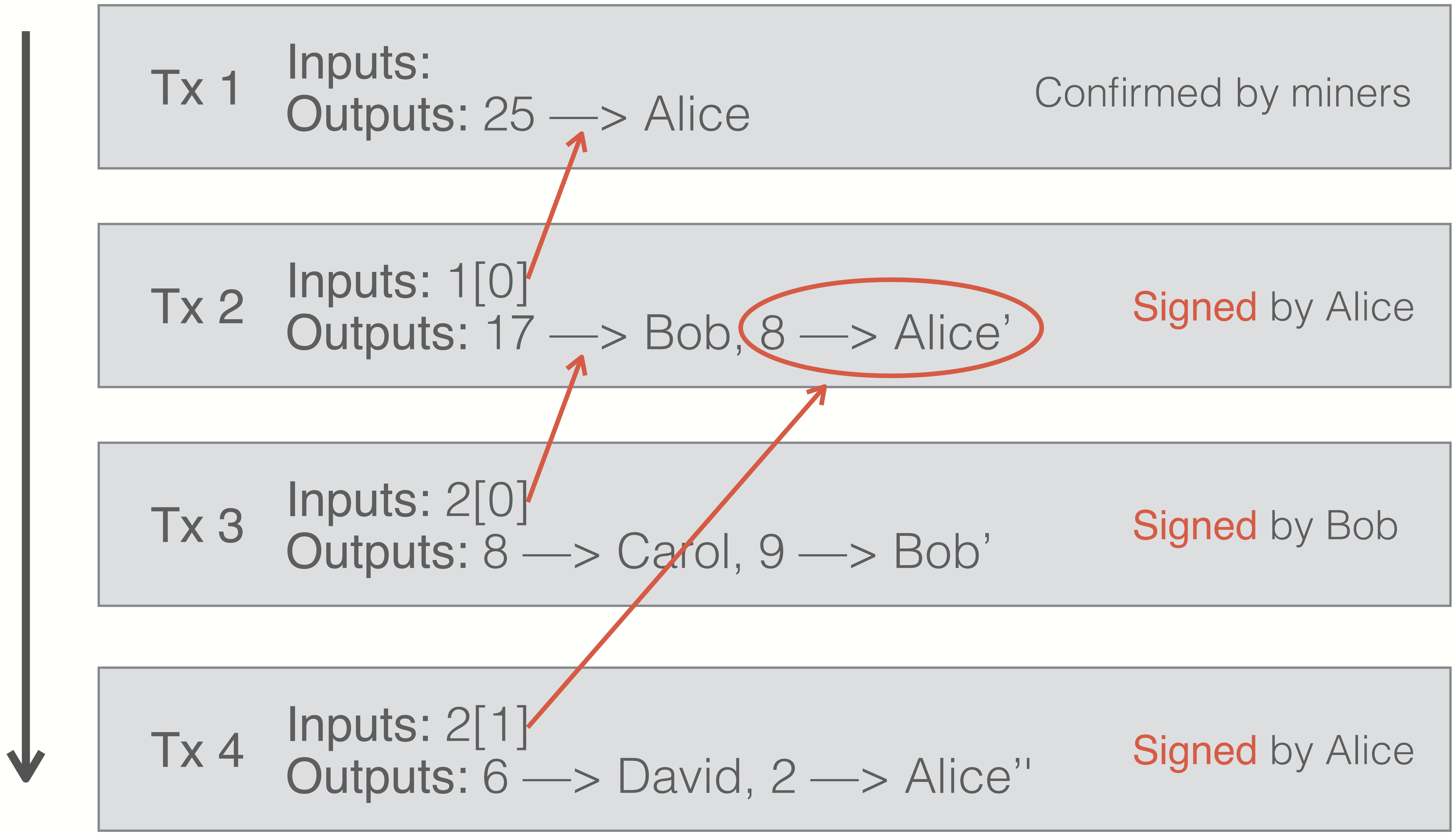
Alice transfers 5 BTC to David — Signed by Alice

Is this valid?

Bitcoins exist as records of Bitcoin transactions

> We define a bitcoin as **a chain of digital signatures**. Each owner transfers bitcoin to the next by digitally **signing** a hash of the **previous** transaction and the **public key of the next owner** and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.
>
> — Satoshi Nakamoto

Bitcoins exist as records of Bitcoin transactions



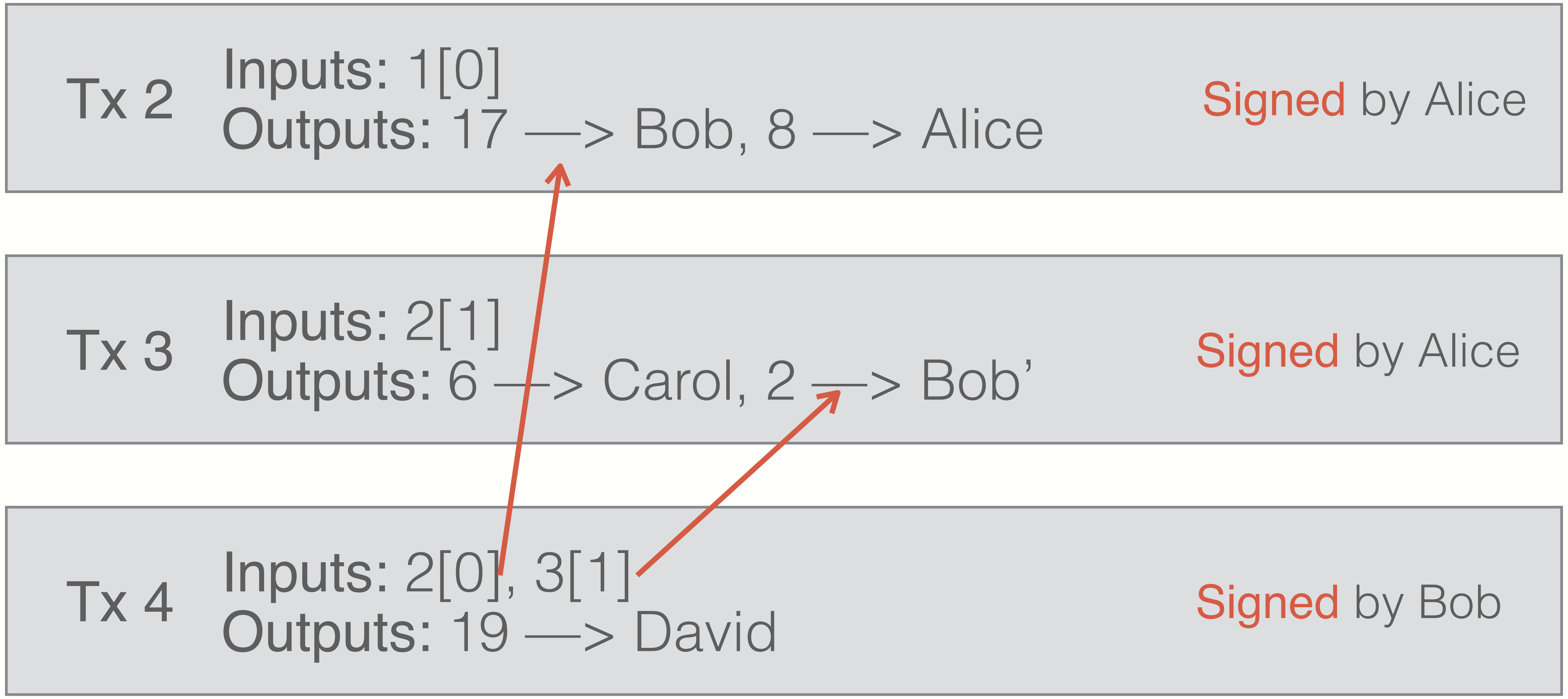
Tx 1
Inputs:
Outputs: 25 —> Alice
Confirmed by miners

Tx 2
Inputs: 1[0]
Outputs: 17 —> Bob, 8 —> Alice’
Signed by Alice

Tx 3
Inputs: 2[0]
Outputs: 8 —> Carol, 9 —> Bob’
Signed by Bob

Tx 4
Inputs: 2[1]
Outputs: 6 —> David, 2 —> Alice’’
Signed by Alice

Merging Value

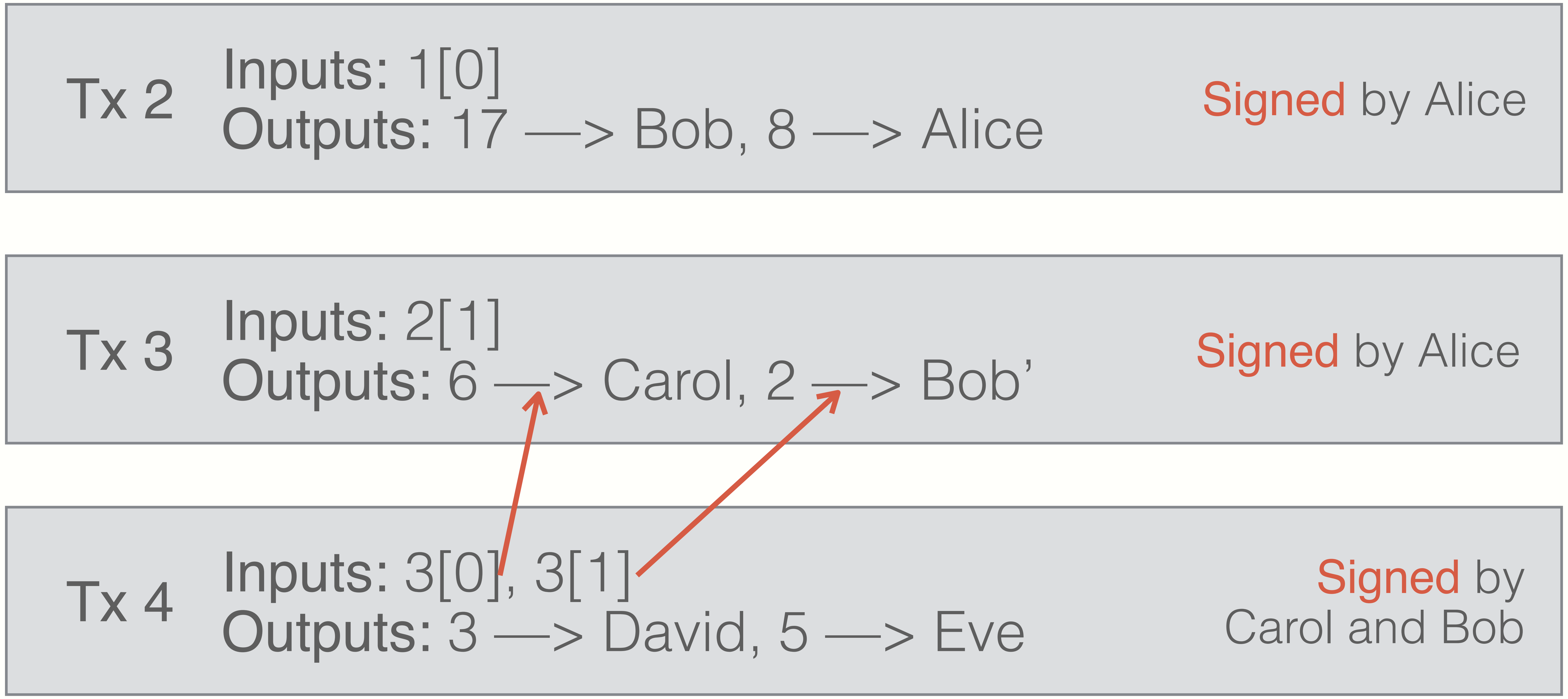


Tx 2 Inputs: 1[0]
Outputs: 17 —> Bob, 8 —> Alice
Signed by Alice

Tx 3 Inputs: 2[1]
Outputs: 6 —> Carol, 2 —> Bob'
Signed by Alice

Tx 4 Inputs: 2[0], 3[1]
Outputs: 19 —> David
Signed by Bob

Joint Payment

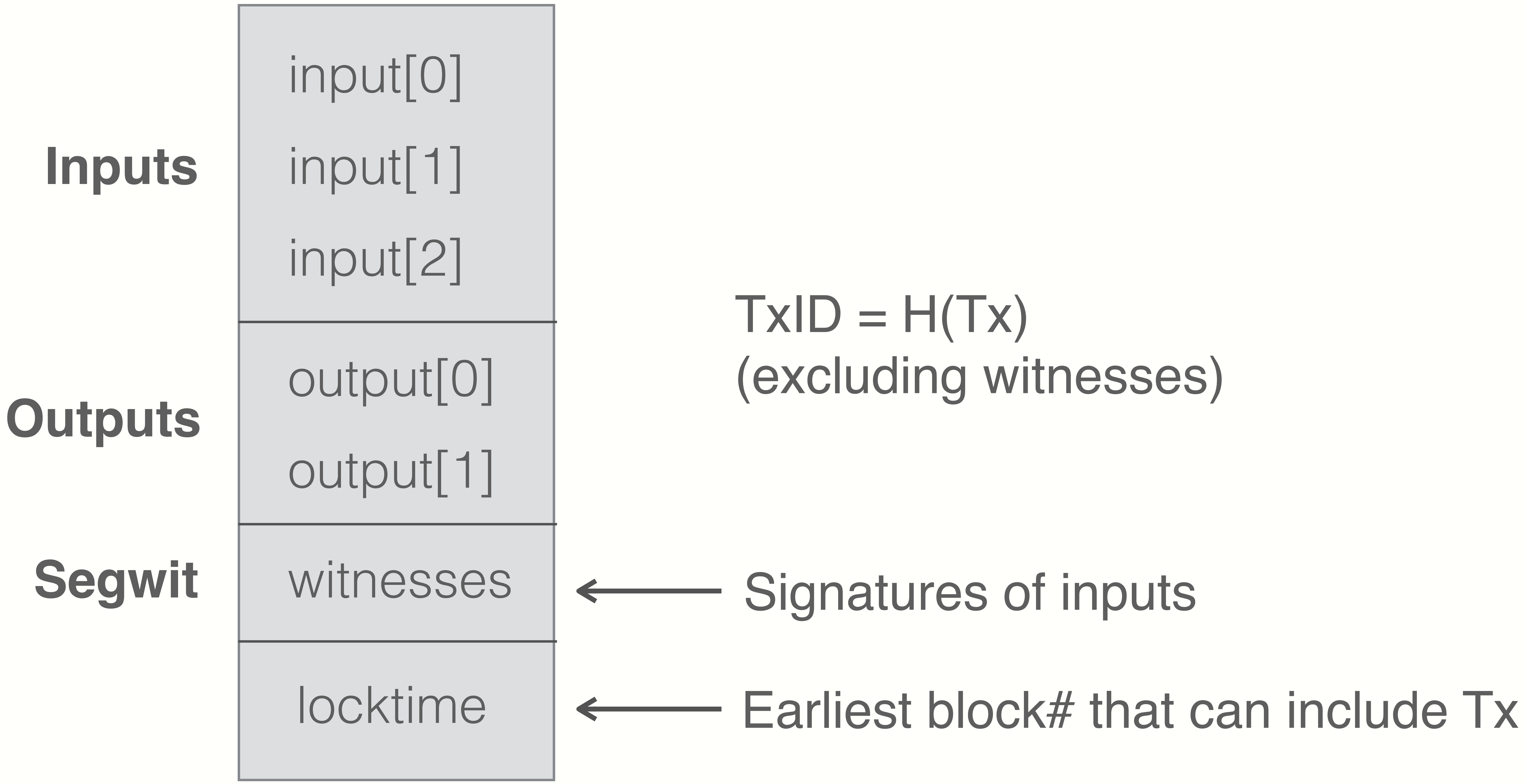


Tx 2 Inputs: 1[0]
Outputs: 17 —> Bob, 8 —> Alice
Signed by Alice

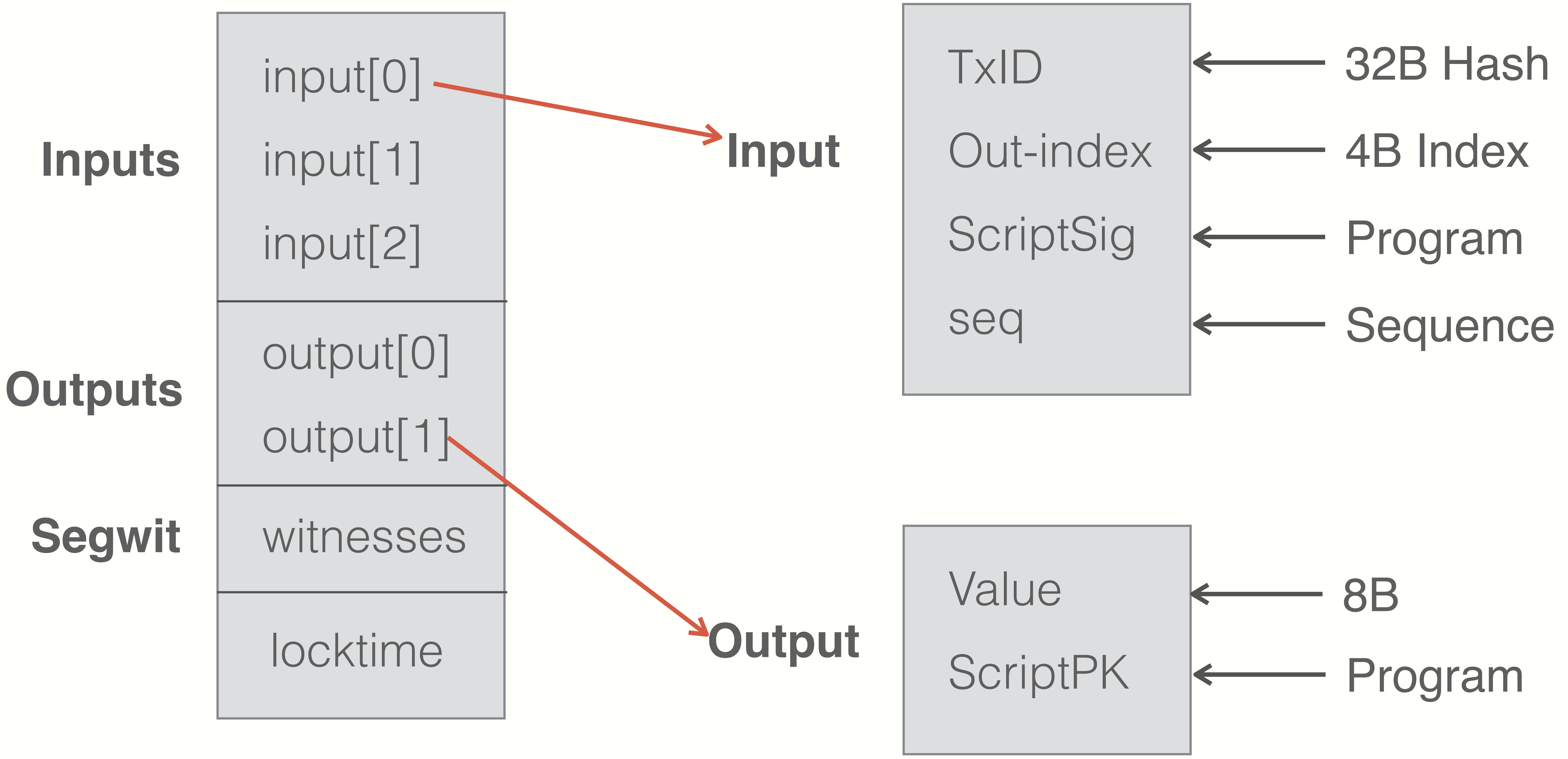
Tx 3 Inputs: 2[1]
Outputs: 6 —> Carol, 2 —> Bob'
Signed by Alice

Tx 4 Inputs: 3[0], 3[1]
Outputs: 3 —> David, 5 —> Eve
Signed by
Carol and Bob

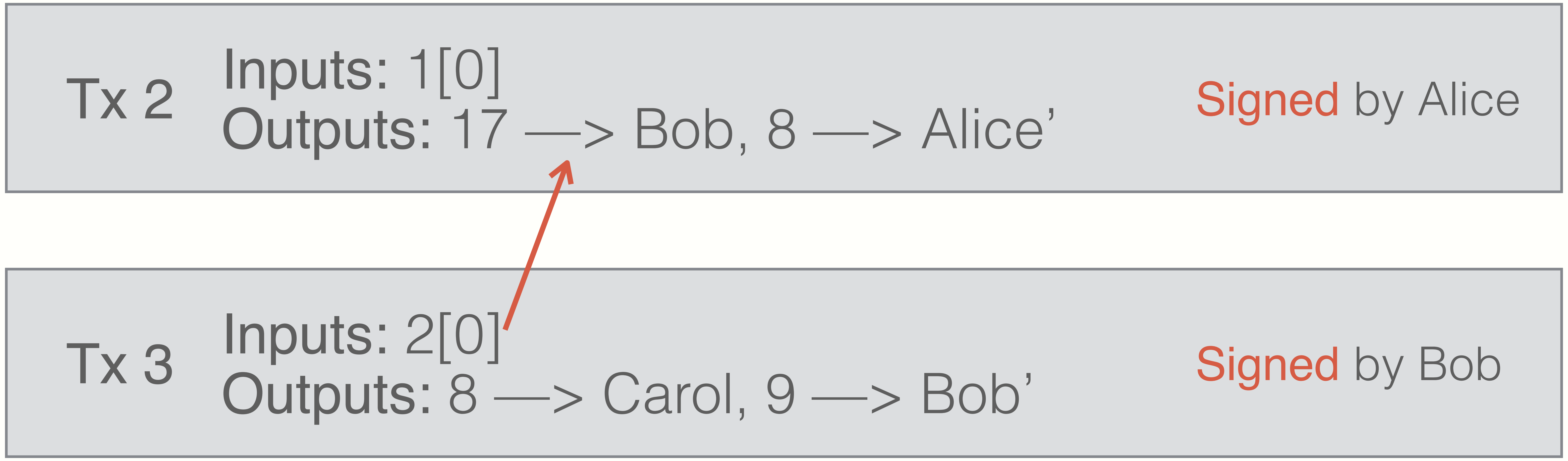
Transaction Structure



Transaction Structure



Example

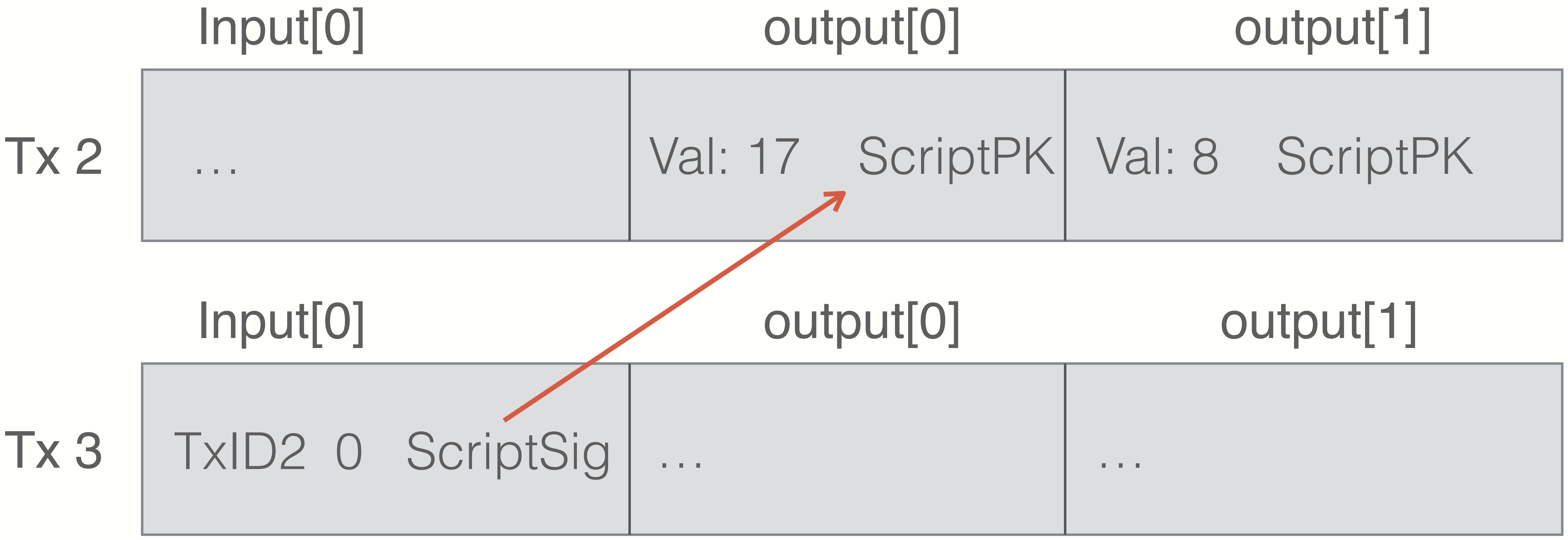


Tx 2 Inputs: 1[0]
Outputs: 17 —> Bob, 8 —> Alice’
Signed by Alice

Tx 3 Inputs: 2[0]
Outputs: 8 —> Carol, 9 —> Bob’
Signed by Bob

Example

Tx 2 Inputs: 1[0]
Outputs: 17 —> Bob, 8 —> Alice’
Signed by Alice



	Input[0]	output[0]	output[1]
Tx 2	…	Val: 17 ScriptPK	Val: 8 ScriptPK
Tx 3	TxID2 0 ScriptSig	…	…

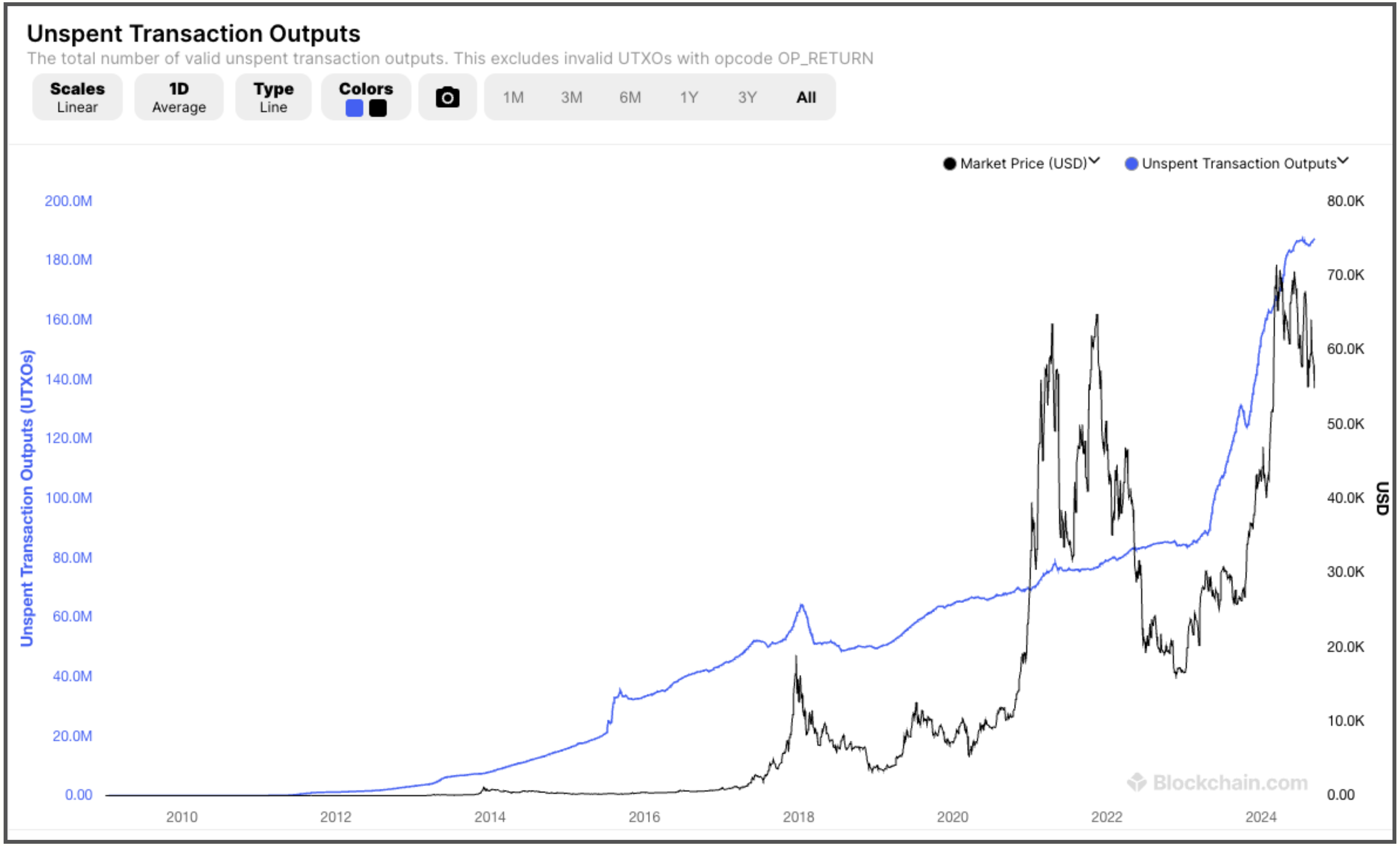
Tx 3 Inputs: 2[0]
Outputs: 8 —> Carol, 9 —> Bob’
Signed by Bob

Validating Transactions

Miners check (for each input):

- The program ScriptSig | ScriptPK returns true
- TxId | Index is in the current UTXO (unspent TX output) set
- Sum input values >= sum output values

Validating Transactions



Unspent Transaction Outputs

The total number of valid unspent transaction outputs. This excludes invalid UTXOs with opcode OP_RETURN

Scales: Linear

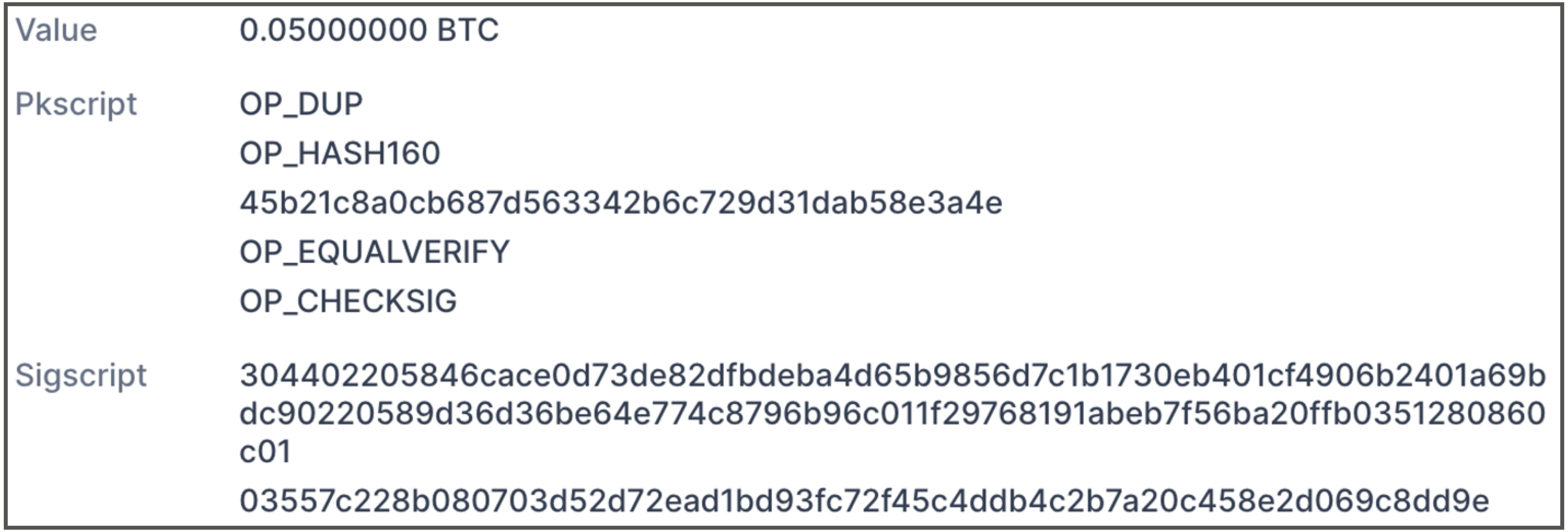
1D: Average

Type: Line

Colors: 🟦 ■

4 Bitcoin Script

Example



Value	0.05000000 BTC
Pkscript	OP_DUP OP_HASH160 45b21c8a0cb687d563342b6c729d31dab58e3a4e OP_EQUALVERIFY OP_CHECKSIG
Sigscript	304402205846cace0d73de82dfbdeba4d65b9856d7c1b1730eb401cf4906b2401a69bdc90220589d36d36be64e774c8796b96c011f29768191abeb7f56ba20ffb0351280860c01 03557c228b080703d52d72ead1bd93fc72f45c4ddb4c2b7a20c458e2d069c8dd9e

Bitcoin Script

A stack machine (and a stack-based scripting language) .

Not Turing Complete: no loops

OP codes:

- **OP_TRUE (OP_1), OP_2, .., OP_16**: push x onto stack
- **OP_DUP**: duplicate and push top of stack onto stack
- **Control**:
  - **OP_IF** <statements> **OP_ELSE** <statements> **OP_ENDIF**
  - **OP_VERIFY:** abort and fail if "top = false"
  - **OP_RETURN:** abort and fail
    - What is: "ScriptPK = [**OP_RETURN**, <data>]"

Bitcoin Script

- **OP_EQVERIFY**: pop two items, abort fail if not equal
- **Arithmetic**:
  - **OP_ADD, OP_SUB, OP_AND, …:** pop two items, add, push
- **Crypto**:
  - **OP_HASH256:** pop, hash, push
  - **OP_CHECKSIG:** pop sig, pop pk, verify sig on Tx, push 0 or 1

Example: A Common Script

<sig> <pk> **DUP HASH256** <pkhash> **EQVERIFY CHECKSIG**

Stack	
[ ]	Init
[<sig> <pk>]	Push data
[<sig> <pk> <pk>]	**DUP**
[<sig> <pk> <hash>]	**HASH256**
[<sig> <pk> <hash> <pkhash>]	Push data
[<sig> <pk>]	**EQVERIFY**
[1]	**CHECKSIG**

P2PKH (Pay to Public Key Hash)

Alice want to pay Bob 5 BTC

- **Step1**: Bob generates key pair (pk_B, sk_B)
- **Step2**: Bob computes his BTC address as addr_B <— H(pk_B)
- **Step3**: Bob sends addr_b to Alice
- **Step4**: Alice broadcasts TX:

	Input[0]	output[0]	output[1]
Tx 2	TxID1 0 ScriptSig_A	Val: 5 ScriptPK_B	…

ScriptPK_B = **DUP HASH256** < addr_B > **EQVERIFY CHECKSIG**

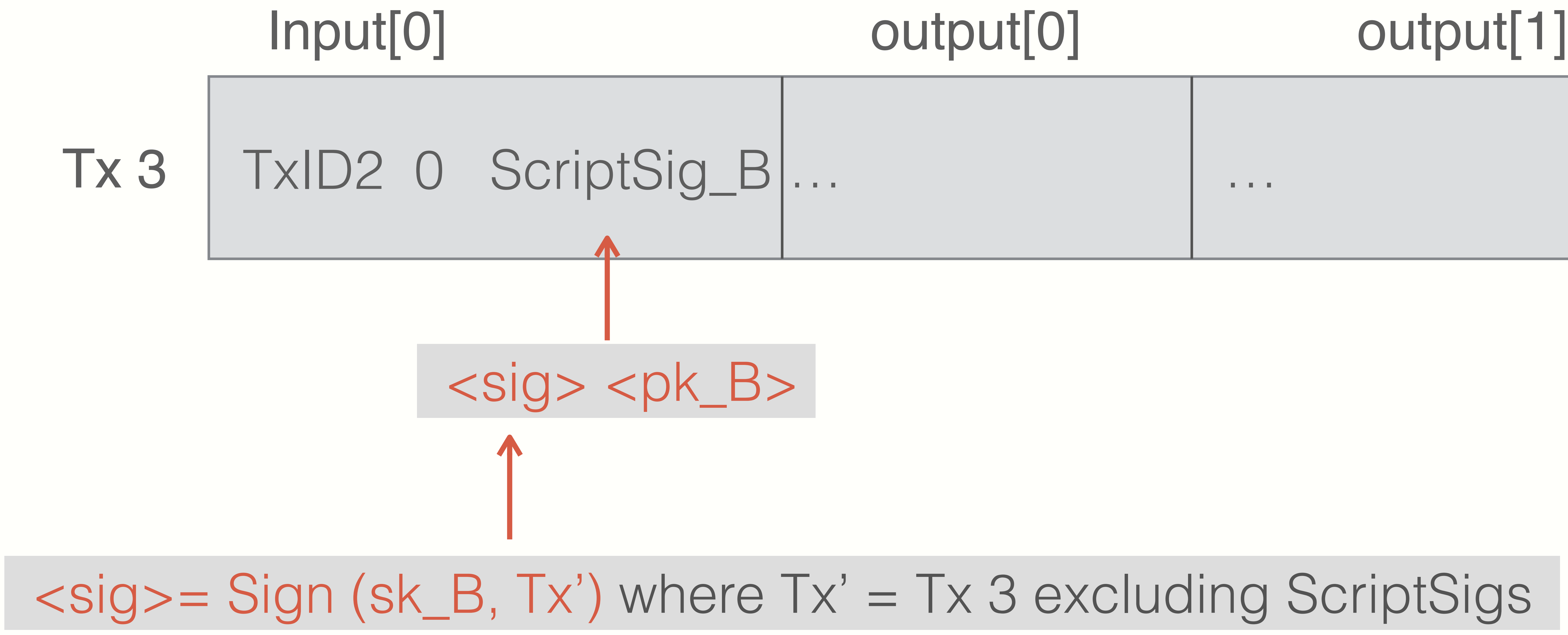
P2PKH (Pay to Public Key Hash)

Input contains ScriptSig_A, i.e., Alice's signature of **Tx 2**, such that information in outputs cannot be modified by miners.

	Input[0]	output[0]	output[1]
Tx 2	TxID1 0 ScriptSig_A	Val: 5 ScriptPK_B	…

P2PKH (Pay to Public Key Hash)

Later, when Bob wants to spend his UTXO, he creates **Tx 3**

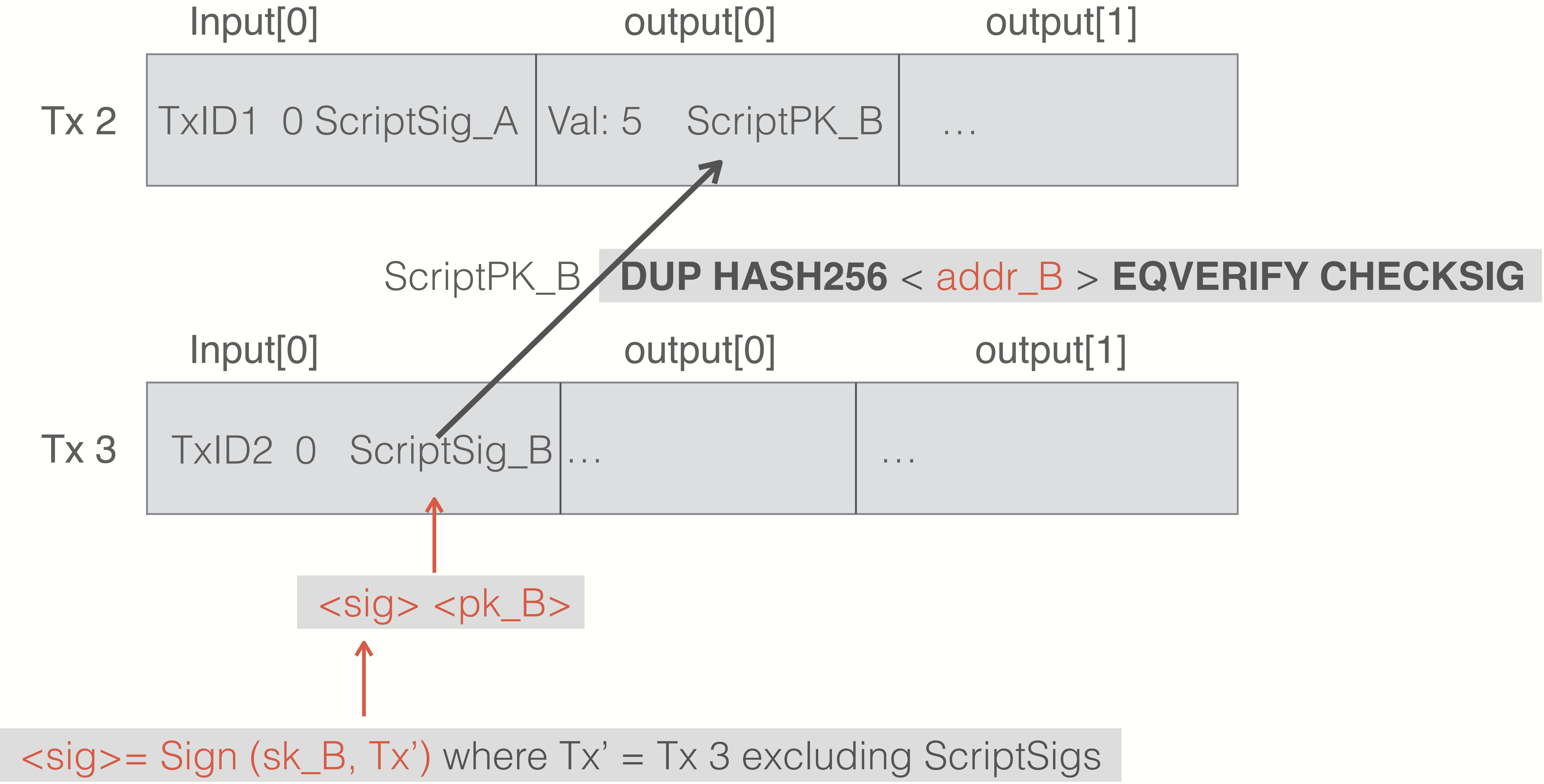


	Input[0]	output[0]	output[1]
Tx 3	TxID2 0 ScriptSig_B	…	…

<sig> <pk_B>

<sig>= Sign (sk_B, Tx’) where Tx’ = Tx 3 excluding ScriptSigs

P2PKH (Pay to Public Key Hash)



	Input[0]	output[0]	output[1]
Tx 2	TxID1 0 ScriptSig_A	Val: 5 ScriptPK_B	…

ScriptPK_B **DUP HASH256** < addr_B > **EQVERIFY CHECKSIG**

	Input[0]	output[0]	output[1]
Tx 3	TxID2 0 ScriptSig_B	…	…

<sig> <pk_B>

<sig>= Sign (sk_B, Tx’) where Tx’ = Tx 3 excluding ScriptSigs

P2PKH (Pay to Public Key Hash)

<sig> <pk_B> **DUP HASH256** <addr_B> **EQVERIFY CHECKSIG**

Stack	
[ ]	Init
[<sig> <pk_B>]	Push values
[<sig> <pk_B> <pk_B>]	**DUP**
[<sig> <pk_B> <addr_B>]	**HASH256** addr_B <— H(pk_B)
[<sig> <pk_B> <addr_B> <addr_B>]	Push values
[<sig> <pk_B>]	**EQVERIFY**
[1]	**CHECKSIG** <sig>= Sign (sk_B, Tx’)

P2PKH (Pay to Public Key Hash)

- Bob’s Public Key is not revealed until UXTO is spent
  - Alice only specifies Bob’s PK hash
- Miner Cannot change addr_B and steal funds
  - Invalidates Alice’s signature

	Input[0]	output[0]	output[1]
Tx 2	TxID1 0 ScriptSig_A	Val: 5 ScriptPK_B	…

5 Discussion Session

How to start a startup?