Ecclesiastes (Eccl) 12:13

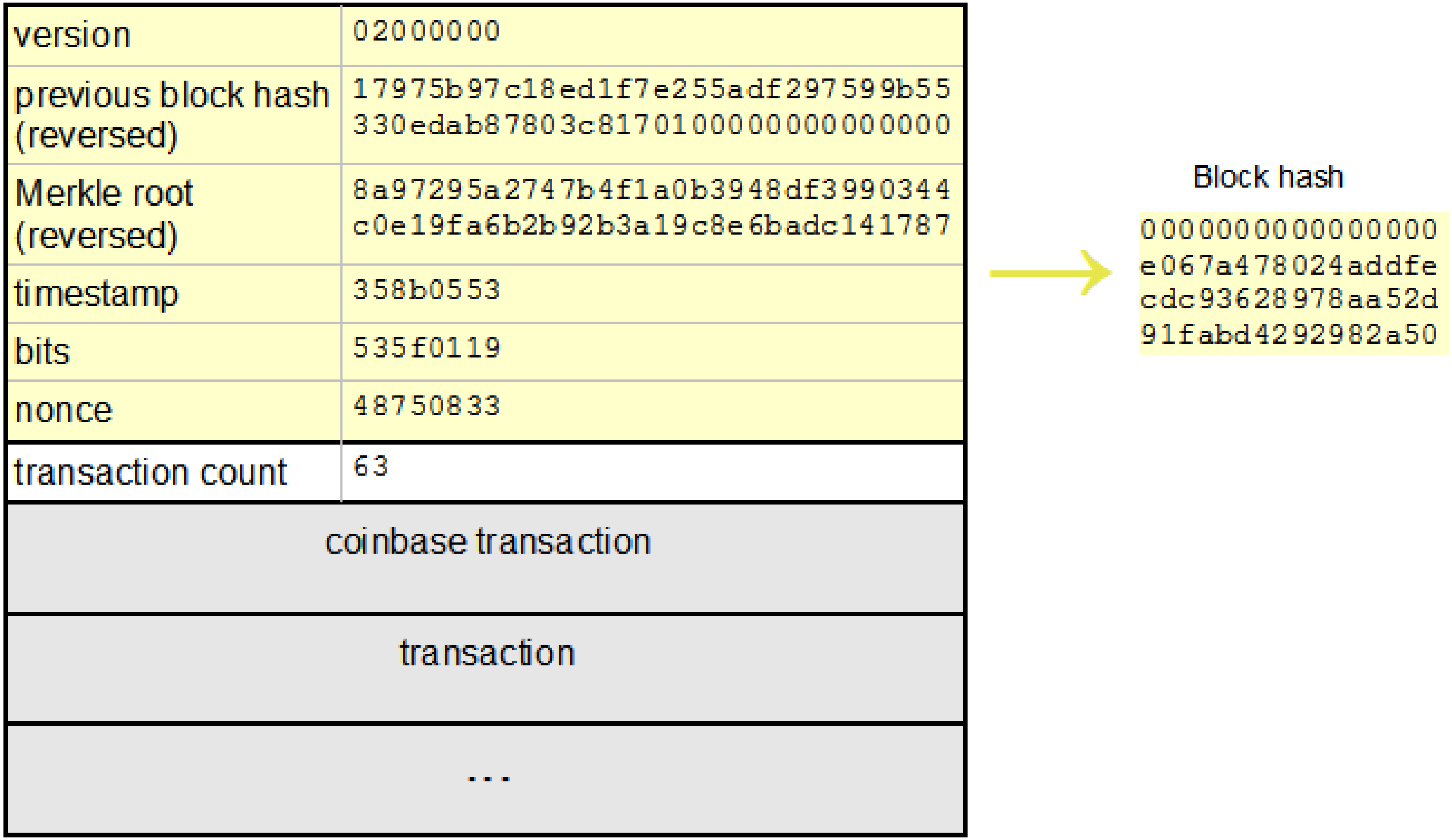
Now all has been heard;
here is the conclusion of the matter :

Have reverence for God, and obey his commands,
because this is all that man was created for.

Fear God and keep his commandments,
for this is the whole duty of man.

Bitcoin Transaction

Calculation Hash for Block Header



version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63

coinbase transaction

transaction

...

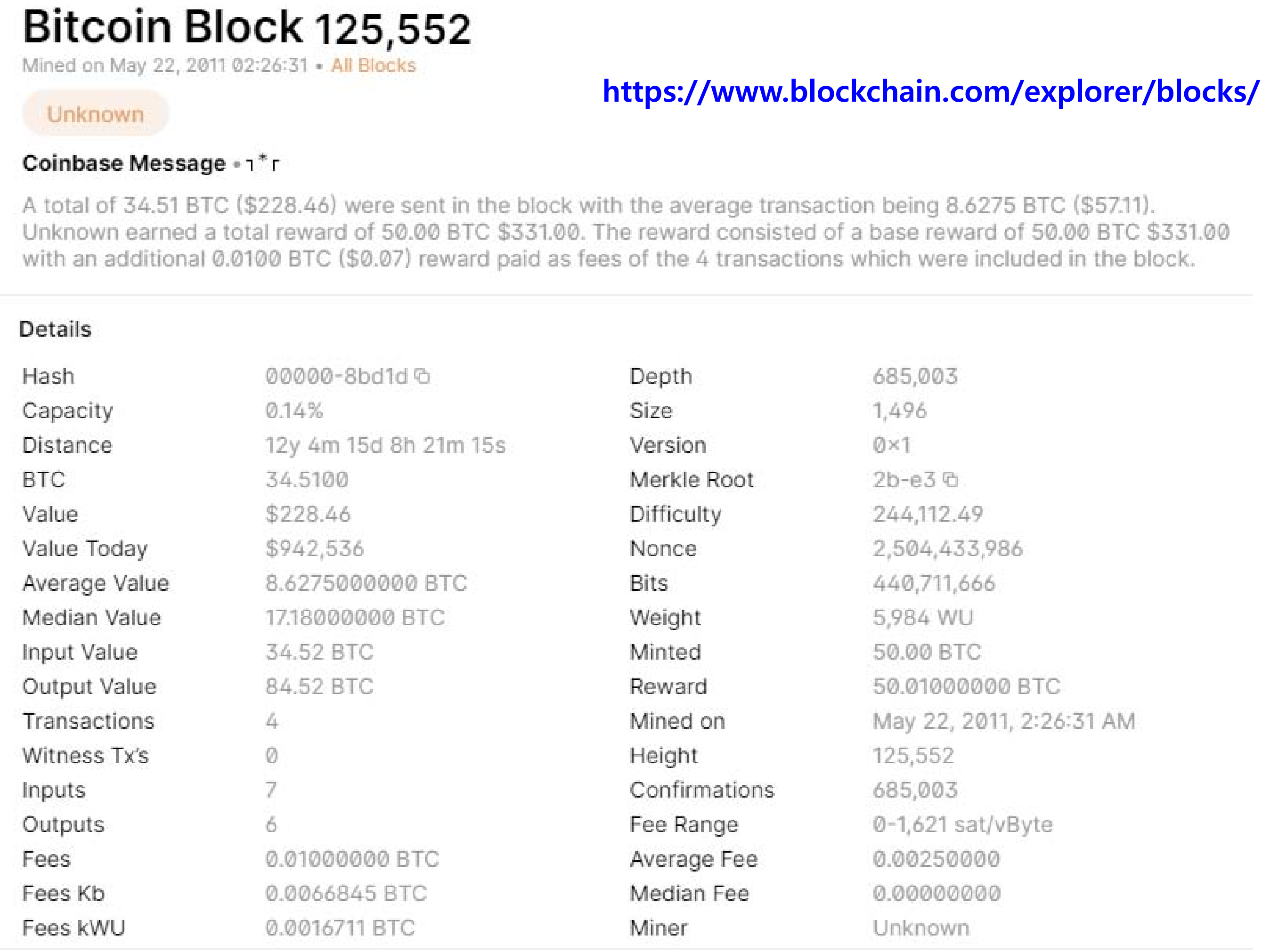
Block hash

0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Block (125552) Information

https://www.blockchain.com/explorer/blocks/btc/125552



Bitcoin Block 125,552

Mined on May 22, 2011 02:26:31 • All Blocks

Unknown

Coinbase Message • ˥*r

A total of 34.51 BTC ($228.46) were sent in the block with the average transaction being 8.6275 BTC ($57.11). Unknown earned a total reward of 50.00 BTC $331.00. The reward consisted of a base reward of 50.00 BTC $331.00 with an additional 0.0100 BTC ($0.07) reward paid as fees of the 4 transactions which were included in the block.

Details

Hash	00000-8bd1d	Depth	685,003
Capacity	0.14%	Size	1,496
Distance	12y 4m 15d 8h 21m 15s	Version	0×1
BTC	34.5100	Merkle Root	2b-e3
Value	$228.46	Difficulty	244,112.49
Value Today	$942,536	Nonce	2,504,433,986
Average Value	8.6275000000 BTC	Bits	440,711,666
Median Value	17.18000000 BTC	Weight	5,984 WU
Input Value	34.52 BTC	Minted	50.00 BTC
Output Value	84.52 BTC	Reward	50.01000000 BTC
Transactions	4	Mined on	May 22, 2011, 2:26:31 AM
Witness Tx's	0	Height	125,552
Inputs	7	Confirmations	685,003
Outputs	6	Fee Range	0-1,621 sat/vByte
Fees	0.01000000 BTC	Average Fee	0.00250000
Fees Kb	0.0066845 BTC	Median Fee	0.00000000
Fees kWU	0.0016711 BTC	Miner	Unknown

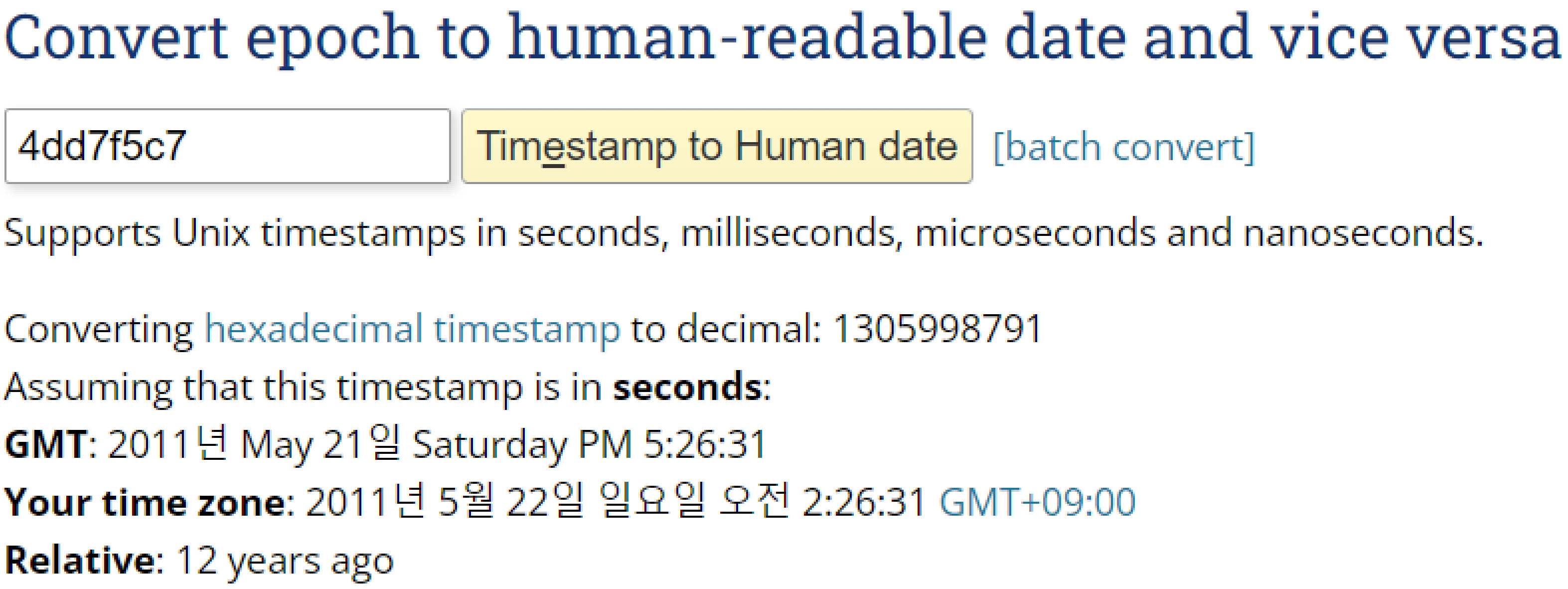
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Calculation Hash for Block (125552) Header

```
>>> import hashlib
>>> from binascii import unhexlify, hexlify

>>> header_hex = ("01000000" +
 "81cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a308000000000000" +       # Prev BlkHash (125551)
 "e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b" +       # Merkel Root
 "c7f5d74d" +                                         # Timestamp
 "f2b9441a" +                                         # Bits = 0x1A44B9F2 = 440,711,666
 "42a14695")                                          # Nonce = 0x9546A142 = 2,504,433,986

>>> header_bin = unhexlify(header_hex)

>>> hash = hashlib.sha256(hashlib.sha256(header_bin).digest()).digest()

>>> hexlify(hash).decode("utf-8")
'1dbd981fe6985776b644b173a4d0385ddc1aa2a829688d1e0000000000000000'

>>> hexlify(hash[::-1]).decode("utf-8")
'00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d'          # hash for Block 125552
```

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

https://www.epochconverter.com/



Convert epoch to human-readable date and vice versa

4dd7f5c7

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Converting hexadecimal timestamp to decimal: 1305998791

Assuming that this timestamp is in **seconds**:

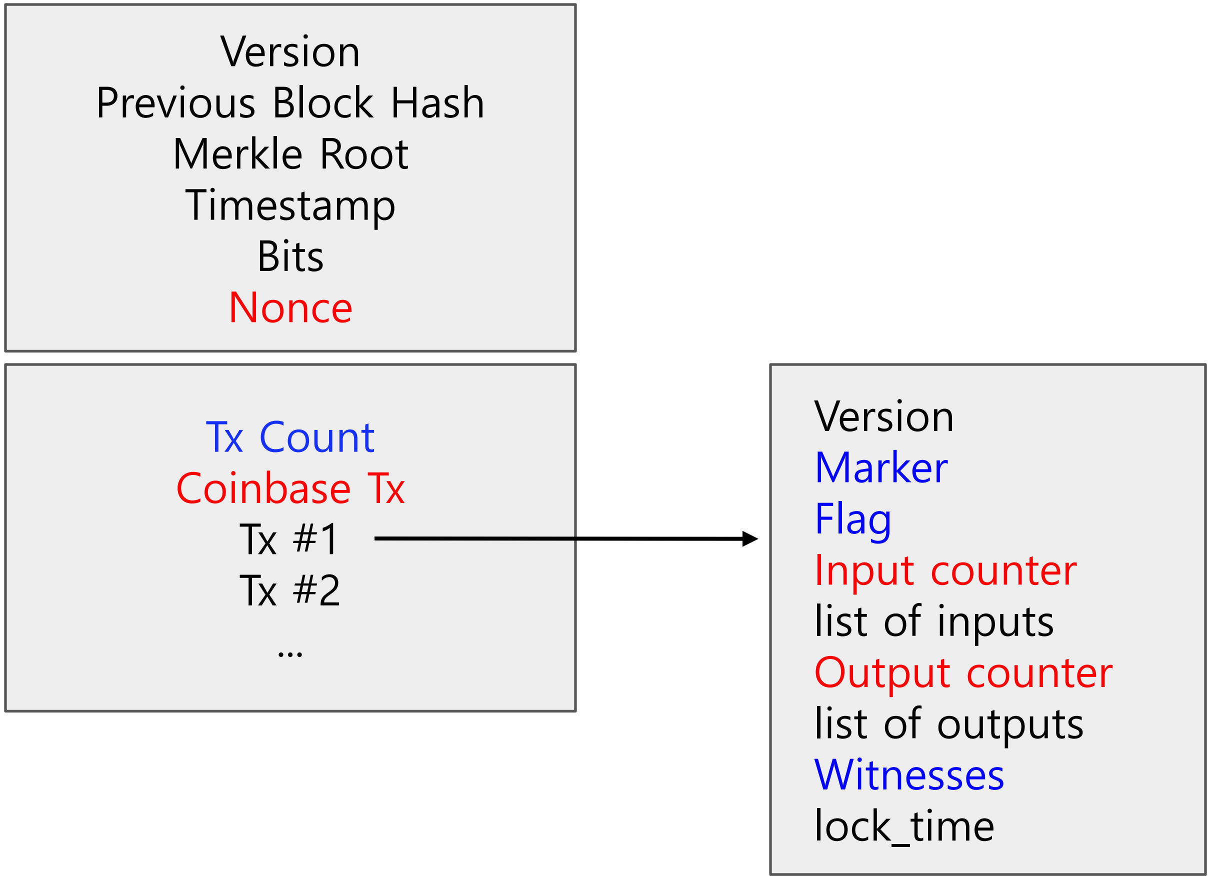
GMT: 2011년 May 21일 Saturday PM 5:26:31

Your time zone: 2011년 5월 22일 일요일 오전 2:26:31 GMT+09:00

Relative: 12 years ago

Bitcoin Block Structure

- Block = Block Header + Transaction List



Version
Previous Block Hash
Merkle Root
Timestamp
Bits
Nonce

Tx Count
Coinbase Tx
Tx #1
Tx #2
…

Version
Marker
Flag
Input counter
list of inputs
Output counter
list of outputs
Witnesses
lock_time

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Block Search in Bitcoin

- https://blockchain.com/explorer/blocks/btc/$block_number
- https://blockchain.info/rawblock/$block_hash
- https://blockchain.info/rawblock/$block_hash?format=hex
- https://api.blockchair.com/bitcoin/raw/block/$block_hash

- https://www.blockchain.com/explorer/blocks/btc/0
  - 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
- https://blockchain.info/rawblock/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
- https://blockchain.info/rawblock/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f?format=hex
- https://api.blockchair.com/bitcoin/raw/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Lab : Block Search

- Serch Bitcoin Block 538,695

- https://www.blockchain.com/explorer

  538695
- https://www.blockchain.com/explorer/search?search=538695
- https://www.blockchain.com/explorer/blocks/btc/538695

- https://www.blockchain.com/explorer/blocks/btc/0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda

https://www.blockchain.com/explorer

* https://www.blockchain.com/explorer/blocks/btc/538695

```
Depth      268,649
Size       1,241,455 kB
Version    0x20000000
MerkleRoot e0-d7 (e0e5c1e24465805b97c359d9f0f5271a014b766853073f516bc6bc4f3be29bd7)
Difficulty 6,727,225,469,722.53
Nonce      664,909,101
Bits       388,618,029
Minted     12.50 BTC
Reward     12.58705715 BTC
Mined on   Aug 27, 2018, 5:37:26 PM
Height     538,695
Confirm    268,649
Miner      BTC.TOP

Hash       00000-7dcda (0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda)
Txs        1,614
Wit Tx's   653        // Number of Segwit Txs
Inputs     6,406
Outputs    3,623
```

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

https://blockchain.info/rawblock/$block_hash

- Get block hash for block number 538695
- https://www.blockchain.com/explorer/blocks/btc/538695
  - 0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda

- https://blockchain.info/rawblock/$block_hash
  - https://blockchain.info/rawblock/0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda

- https://blockchain.info/rawblock/$block_hash?format=hex
  - https://blockchain.info/rawblock/0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda?format=hex

- https://api.blockchair.com/bitcoin/raw/block/$block_hash
  - https://api.blockchair.com/bitcoin/raw/block/0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

https://blockchain.info/rawblock/0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda

```
{
    "hash": "0000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda",
    "ver": 536870912,
    "prev_block": "0000000000000000002669a90eec10c534c158eabe4ef8bd7f6133601f0ab116",
    "mrkl_root": "e0e5c1e24465805b97c359d9f0f5271a014b766853073f516bc6bc4f3be29bd7",
    "time": 1535359046,
    "bits": 388618029,
    "next_block": [
        "00000000000000000009ef223af6652bbc8736e756e1b276dd429298eb4a3198"
    ],
    "fee": 8705715,
    "nonce": 664909101,
    "n_tx": 1614,
    "size": 1241455,
    "block_index": 538695,
    "main_chain": true,
    "height": 538695,
    "weight": 3993181,
    "tx": [
        {
            "hash": "6d67c652ee4e12f85d2ead3c4ba1030ff821f243633f6347aa5ee5aa5c7f6eda",
            "ver": 1,
            "vin_sz": 1,
            "vout_sz": 2 ...
```

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

https://www.blockchain.com/explorer/blocks/btc/0
https://api.blockchair.com/bitcoin/raw/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

```
{
    "data": {
        "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f": {
            "raw_block":
   "0100000000000000000000000000000000000000000000000000000000000000000000003ba3edfd7a7b12b27ac72c3e67768f617fc81b
   c3888a51323a9fb8aa4b1e5e4a29ab5f49ffff001d1dac2b7c01010000000100000000000000000000000000000000000000000000000000
   000000000000000ffffffff4d04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e
   206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73ffffffff0100f2052a01000000434104678afdb0fe5
   548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6b
   f11d5fac00000000",
            "decoded_raw_block": {
                "hash": "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
                "confirmations": 809429,
                "height": 0,
                "version": 1,
                "versionHex": "00000001",
                "merkleroot": "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
                "time": 1231006505,
                "mediantime": 1231006505,
                "nonce": 2083236893,
                "bits": "1d00ffff",
                "difficulty": 1,
                "chainwork": "0000000000000000000000000000000000000000000000000000000100010001",
                "nTx": 1,
                "nextblockhash": "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048",
                ...
```

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

https://www.arcblock.io/blog/en/post/2018/08/16/index-bitcoin

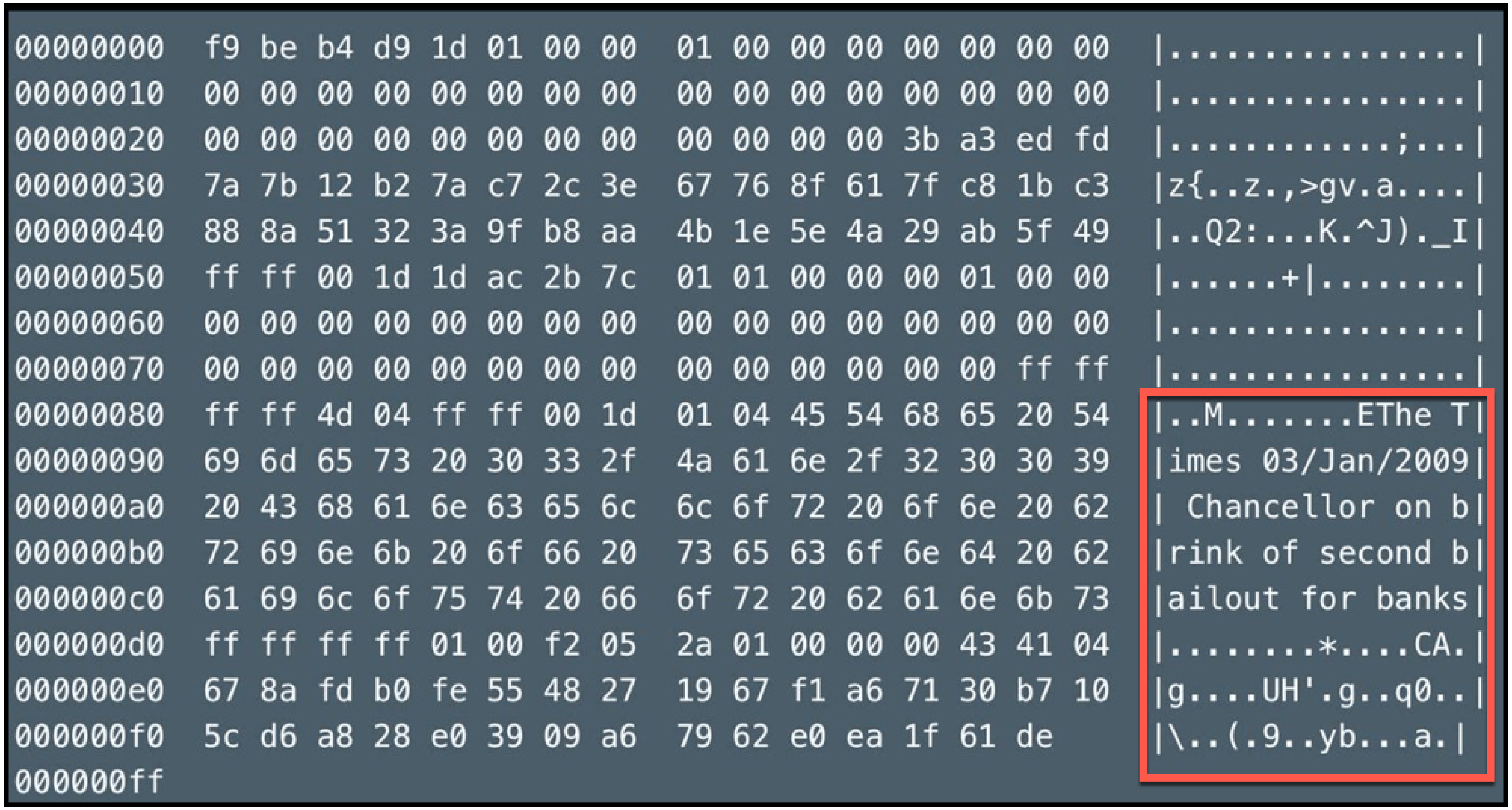
- `$HOME/.bitcoin/blocks`
- `od -x --endian=big -N 297 blk00000.dat`

od -x --endian=big -N 297 -An blk00000.dat

```
000   f9be b4d9 1d01 0000 0100 0000 0000 0000
010   0000 0000 0000 0000 0000 0000 0000 0000
020   0000 0000 0000 0000 0000 0000 3ba3 edfd
030   7a7b 12b2 7ac7 2c3e 6776 8f61 7fc8 1bc3
040   888a 5132 3a9f b8aa 4b1e 5e4a 29ab 5f49
050   ffff 001d 1dac 2b7c 0101 0000 0001 0000
060   0000 0000 0000 0000 0000 0000 0000 0000
070   0000 0000 0000 0000 0000 0000 0000 ffff
080   ffff 4d04 ffff 001d 0104 4554 6865 2054
090   696d 6573 2030 332f 4a61 6e2f 3230 3039
0A0   2043 6861 6e63 656c 6c6f 7220 6f6e 2062
0B0   7269 6e6b 206f 6620 7365 636f 6e64 2062
0C0   6169 6c6f 7574 2066 6f72 2062 616e 6b73
0D0   ffff ffff 0100 f205 2a01 0000 0043 4104
0E0   678a fdb0 fe55 4827 1967 f1a6 7130 b710
0F0   5cd6 a828 e039 09a6 7962 e0ea 1f61 deb6
100   49f6 bc3f 4cef 38c4 f355 04e5 1ec1 12de
110   5c38 4df7 ba0b 8d57 8a4c 702b 6bf1 1d5f
120   ac00 0000 00f9 beb4 d900
```

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

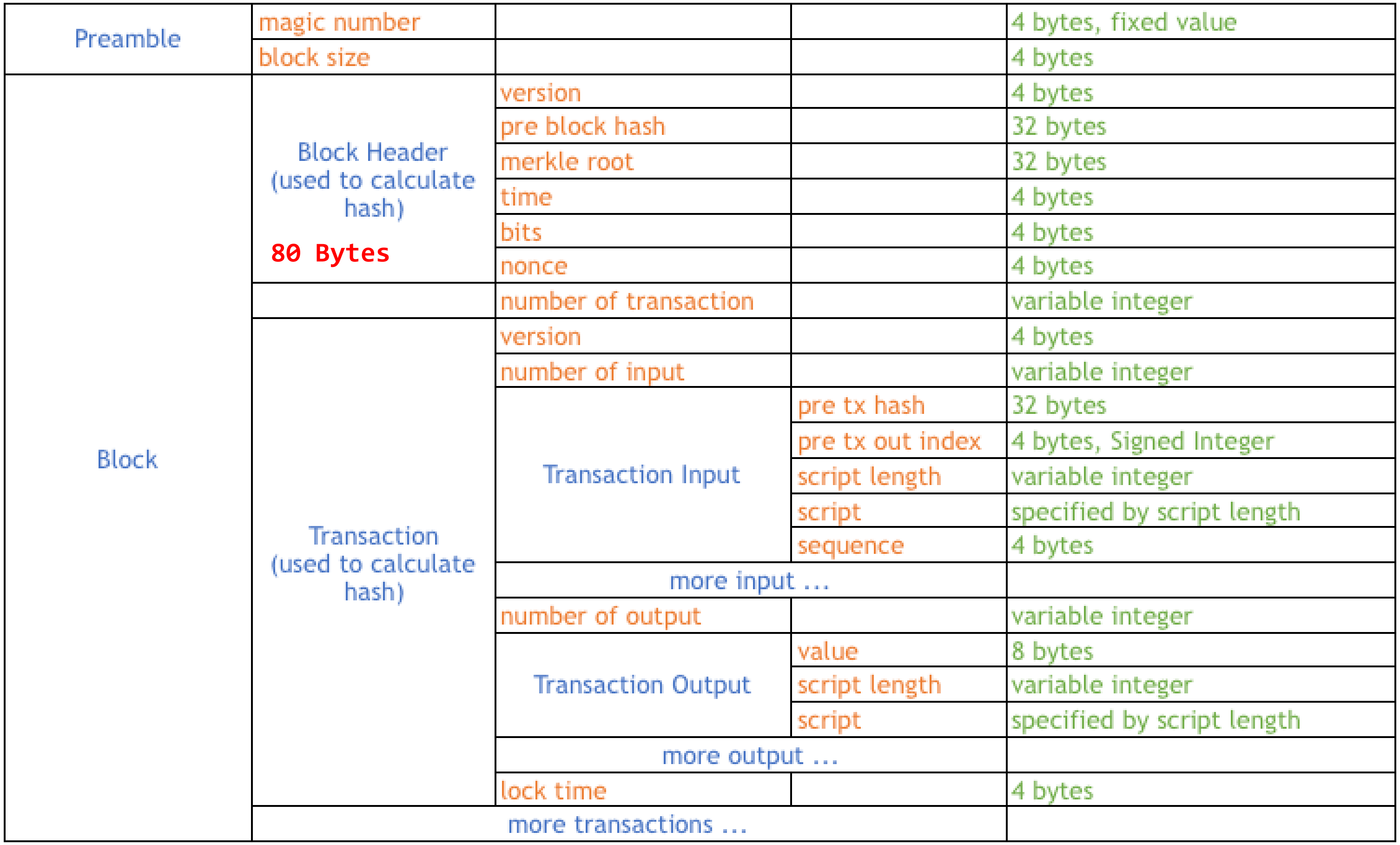
Genesis Block



```
00000000  f9 be b4 d9 1d 01 00 00  01 00 00 00 00 00 00 00  |................|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 3b a3 ed fd  |............;...|
00000030  7a 7b 12 b2 7a c7 2c 3e  67 76 8f 61 7f c8 1b c3  |z{..z.,>gv.a....|
00000040  88 8a 51 32 3a 9f b8 aa  4b 1e 5e 4a 29 ab 5f 49  |..Q2:...K.^J)._I|
00000050  ff ff 00 1d 1d ac 2b 7c  01 01 00 00 00 01 00 00  |......+|........|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff ff  |................|
00000080  ff ff 4d 04 ff ff 00 1d  01 04 45 54 68 65 20 54  |..M.......EThe T|
00000090  69 6d 65 73 20 30 33 2f  4a 61 6e 2f 32 30 30 39  |imes 03/Jan/2009|
000000a0  20 43 68 61 6e 63 65 6c  6c 6f 72 20 6f 6e 20 62  | Chancellor on b|
000000b0  72 69 6e 6b 20 6f 66 20  73 65 63 6f 6e 64 20 62  |rink of second b|
000000c0  61 69 6c 6f 75 74 20 66  6f 72 20 62 61 6e 6b 73  |ailout for banks|
000000d0  ff ff ff ff 01 00 f2 05  2a 01 00 00 00 43 41 04  |........*....CA.|
000000e0  67 8a fd b0 fe 55 48 27  19 67 f1 a6 71 30 b7 10  |g....UH'.g..q0..|
000000f0  5c d6 a8 28 e0 39 09 a6  79 62 e0 ea 1f 61 de     |\..(.9..yb...a.|
000000ff
```

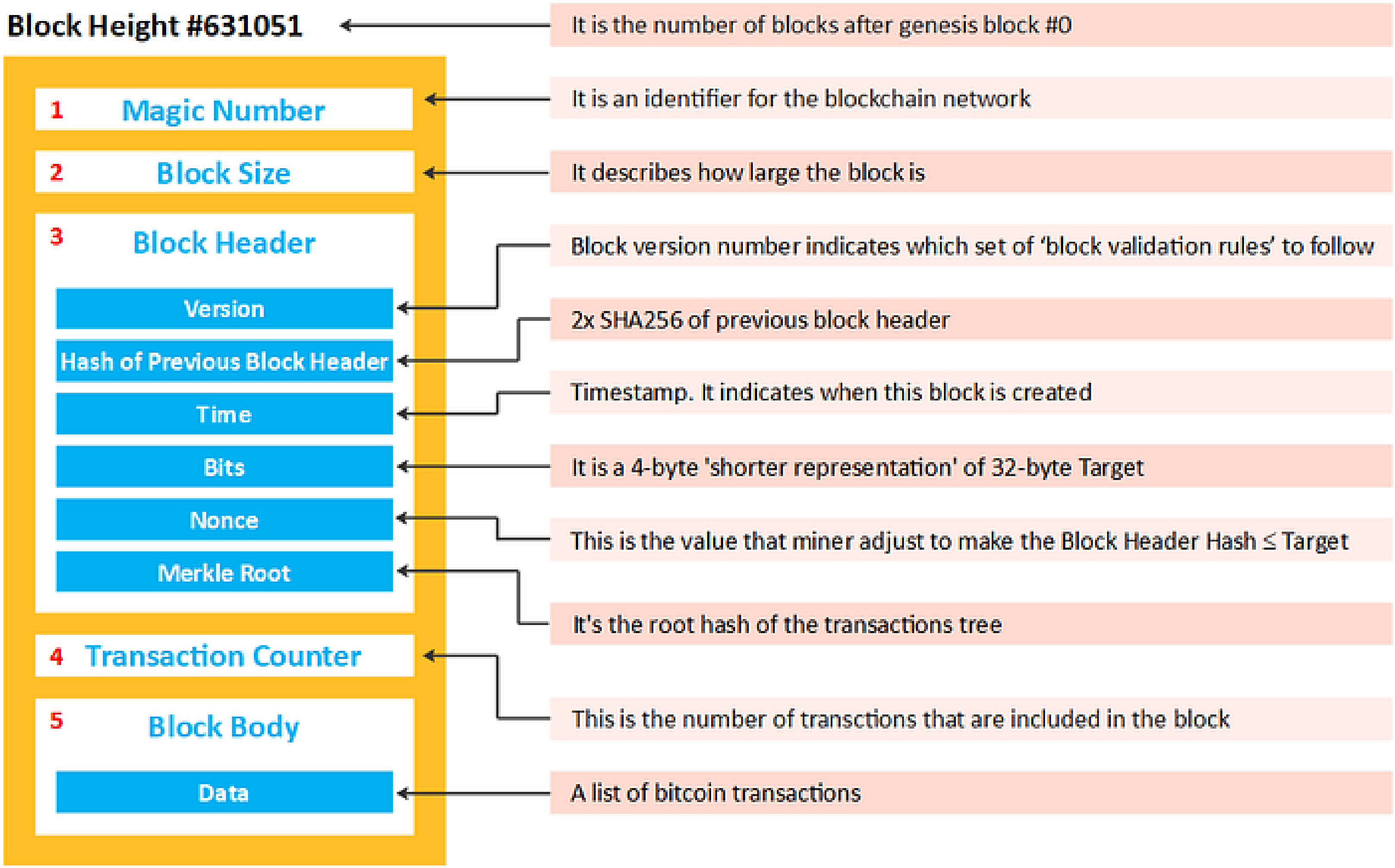
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Block Format in Bitcoin



Preamble	magic number			4 bytes, fixed value
	block size			4 bytes
Block	Block Header (used to calculate hash) 80 Bytes	version		4 bytes
		pre block hash		32 bytes
		merkle root		32 bytes
		time		4 bytes
		bits		4 bytes
		nonce		4 bytes
		number of transaction		variable integer
	Transaction (used to calculate hash)	version		4 bytes
		number of input		variable integer
		Transaction Input	pre tx hash	32 bytes
			pre tx out index	4 bytes, Signed Integer
			script length	variable integer
			script	specified by script length
			sequence	4 bytes
		more input …		
		number of output		variable integer
		Transaction Output	value	8 bytes
			script length	variable integer
			script	specified by script length
		more output …		
		lock time		4 bytes
	more transactions …			

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**



Block Height #631051 — It is the number of blocks after genesis block #0

1 Magic Number — It is an identifier for the blockchain network

2 Block Size — It describes how large the block is

3 Block Header

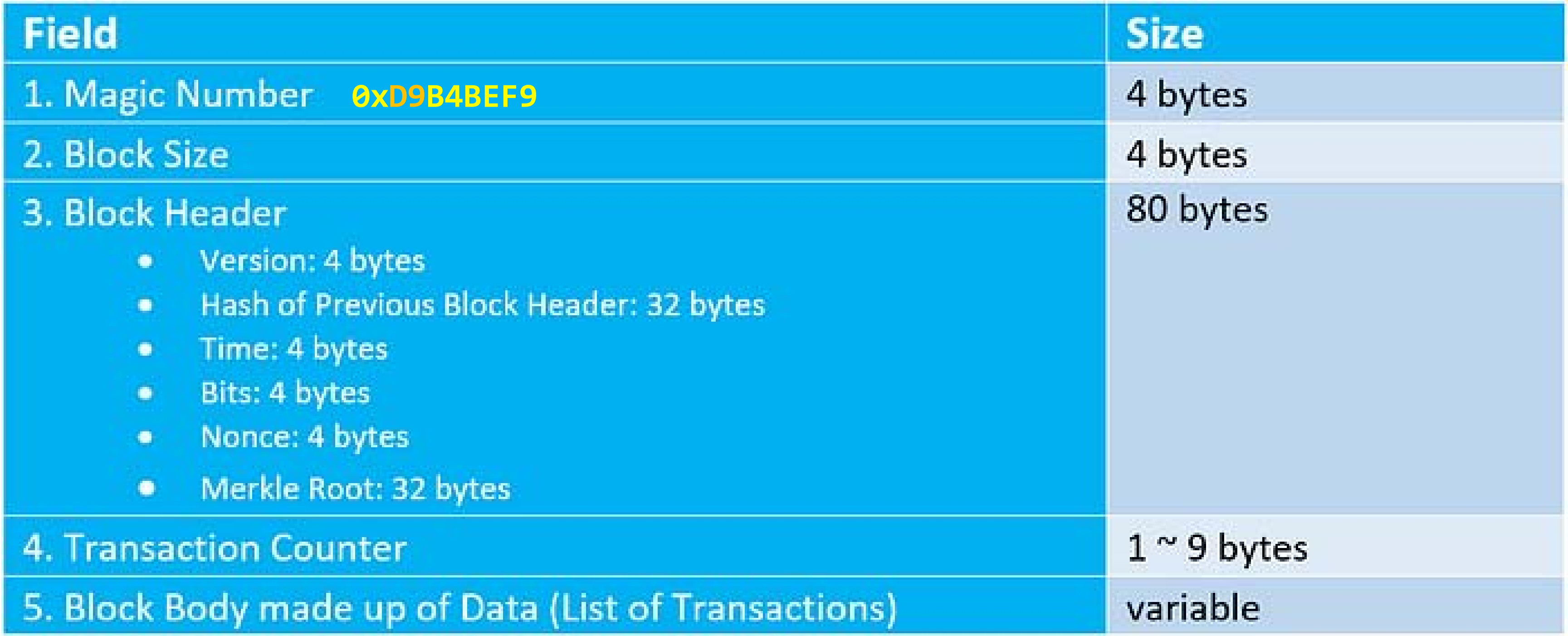
- Version — Block version number indicates which set of 'block validation rules' to follow
- Hash of Previous Block Header — 2x SHA256 of previous block header
- Time — Timestamp. It indicates when this block is created
- Bits — It is a 4-byte 'shorter representation' of 32-byte Target
- Nonce — This is the value that miner adjust to make the Block Header Hash ≤ Target
- Merkle Root — It's the root hash of the transactions tree

4 Transaction Counter — This is the number of transctions that are included in the block

5 Block Body

- Data — A list of bitcoin transactions

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

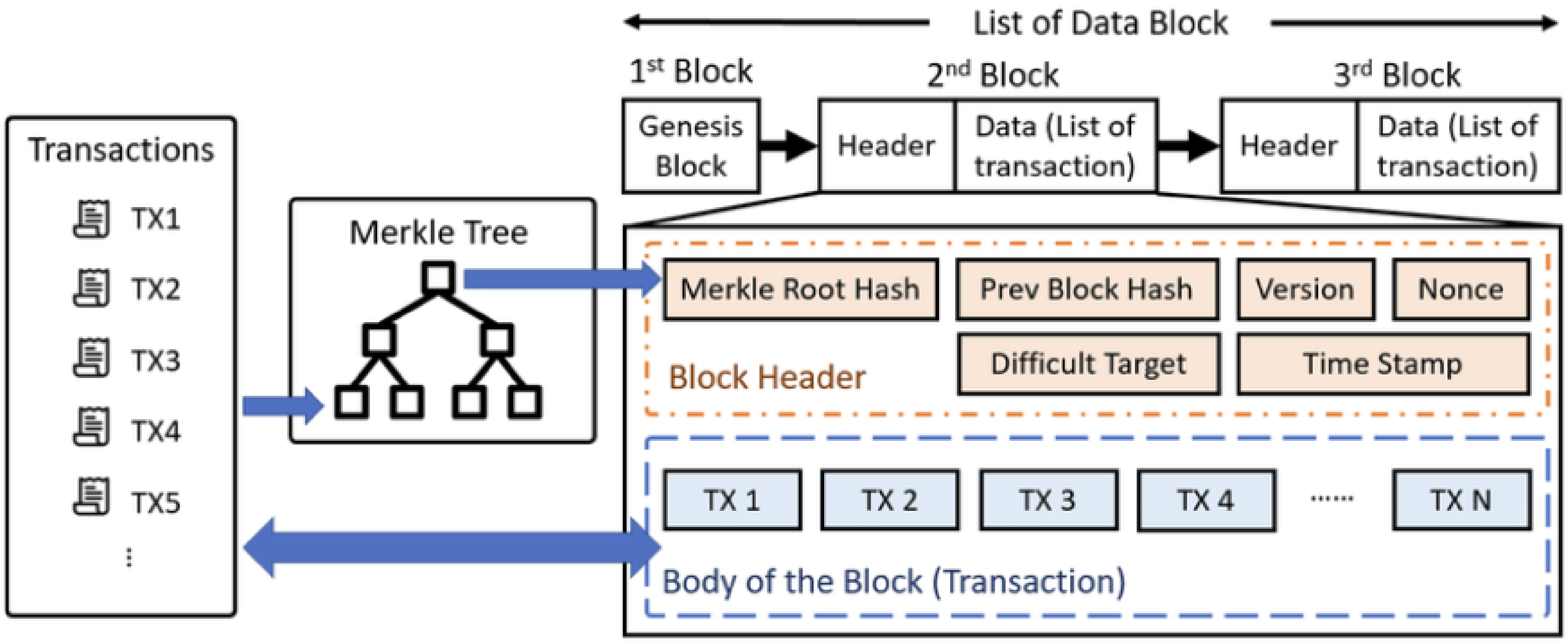


Field	Size
1. Magic Number 0xD9B4BEF9	4 bytes
2. Block Size	4 bytes
3. Block Header • Version: 4 bytes • Hash of Previous Block Header: 32 bytes • Time: 4 bytes • Bits: 4 bytes • Nonce: 4 bytes • Merkle Root: 32 bytes	80 bytes
4. Transaction Counter	1 ~ 9 bytes
5. Block Body made up of Data (List of Transactions)	variable

Magic Number

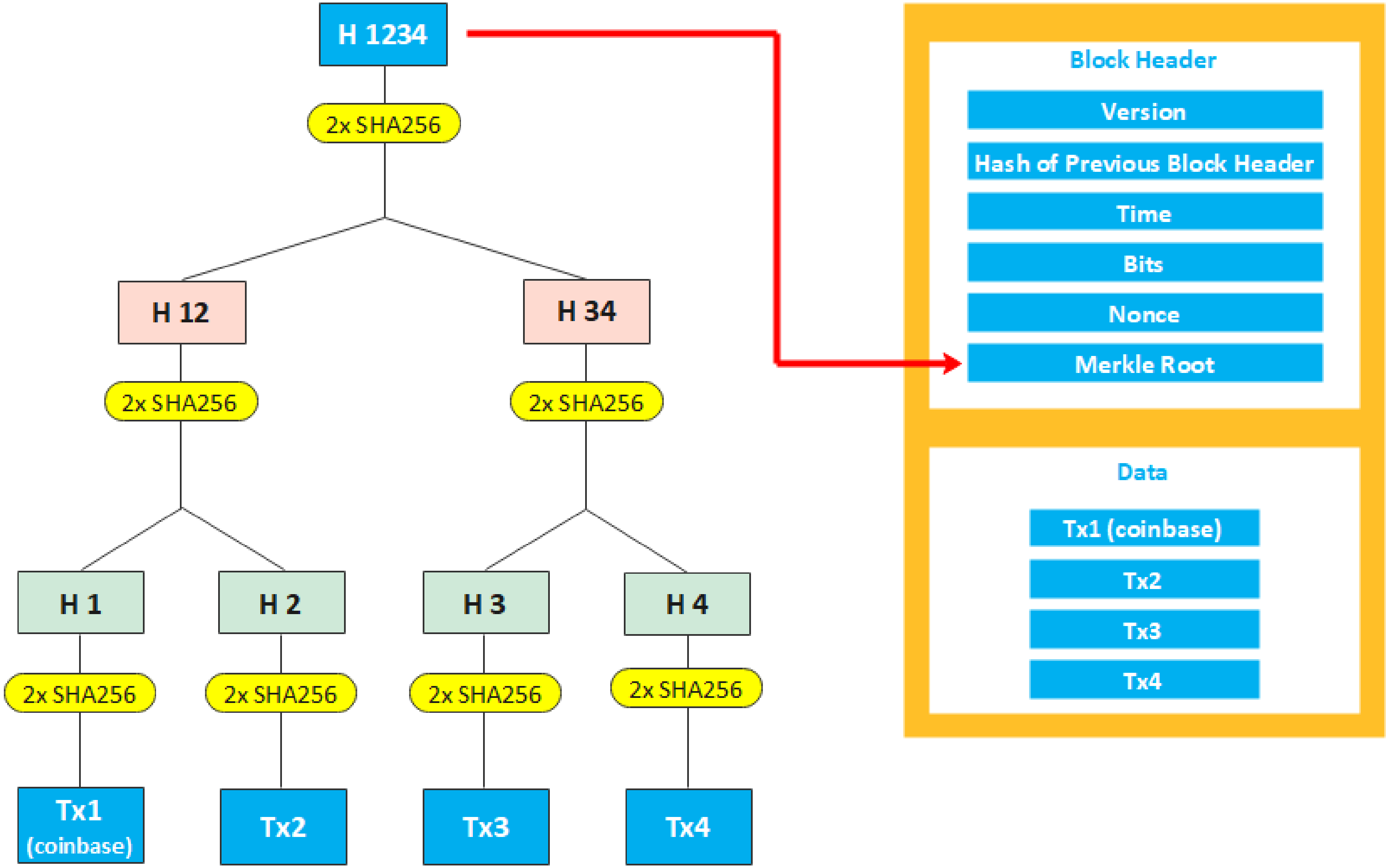
- Refers to a specific value that is included in the block's header
  - It serves as a unique identifier to help network nodes and miners recognize and interpret **start of a new block** when it is received over the Bitcoin network
- **0xD9B4BEF9** : Used to distinguish mainnet Bitcoin blocks from blocks on other networks or testnets
  - Different Bitcoin test networks, such as the testnet and regtest, have their own magic numbers to differentiate their blocks from those on the main network
  - 0xD9: indicates start of a message or data packet on the Bitcoin network
  - 0xB4 0xBE 0xF9 : These bytes form the unique identifier for main network
- When a Bitcoin node receives data from the network
  - it checks the magic number in the header to ensure that the incoming data is indeed a valid Bitcoin block or message for the correct network
  - If the magic number doesn't match the expected value for the network, the data is typically discarded
  - The use of a magic number helps maintain network integrity and security by preventing nodes from mistakenly processing data meant for other networks and ensuring that Bitcoin nodes only interact with the Bitcoin main network or the appropriate test networks

Merkle Tree



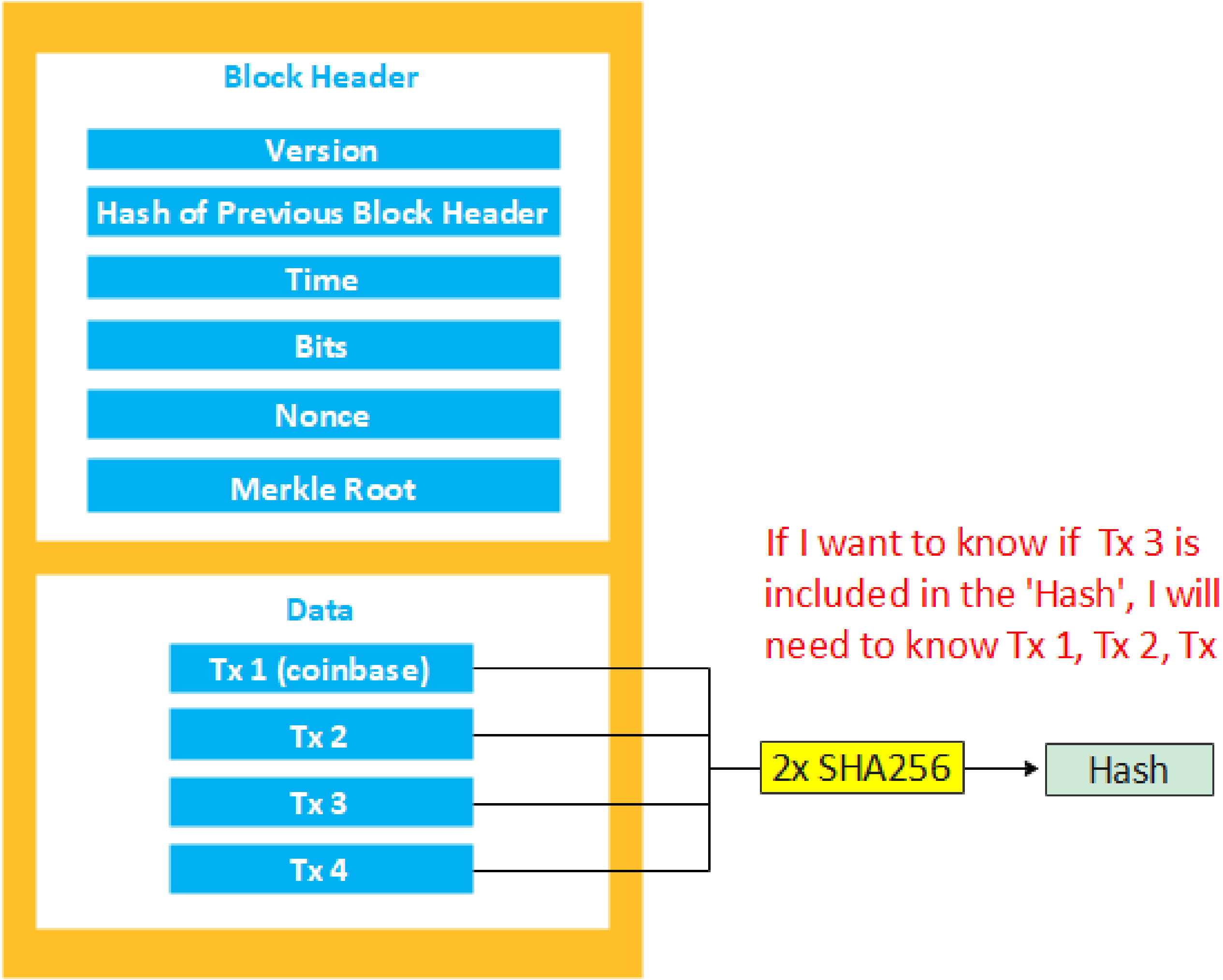
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Ch11: Something on Transaction Merkle Tree
https://medium.com/@ackhor/ch11-something-on-transaction-merkle-tree-f3a65dcfca00



✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Calculation of Tx Hash

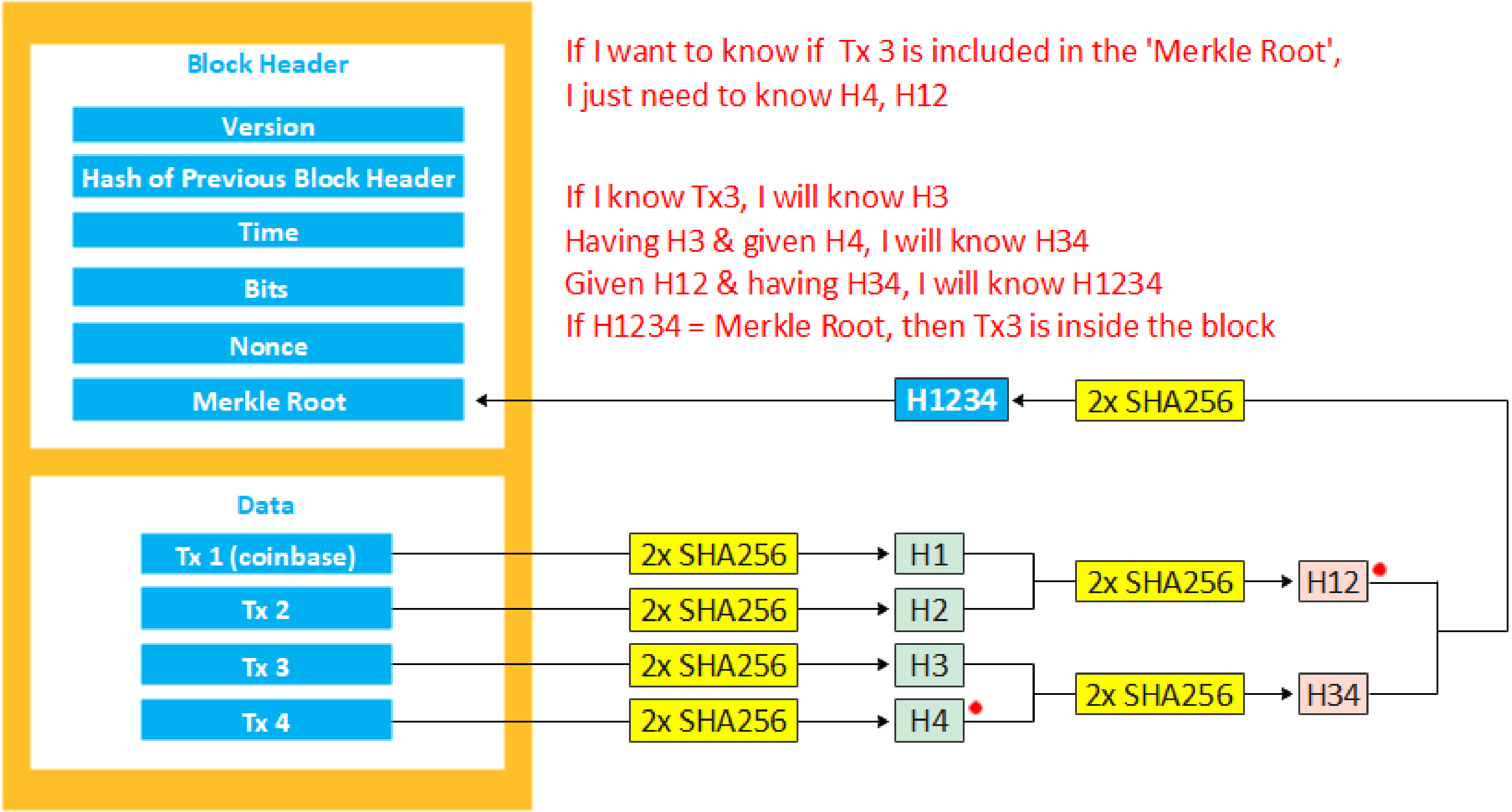


If I want to know if Tx 3 is included in the 'Hash', I will need to know Tx 1, Tx 2, Tx 4

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

If I want to know if Tx 3 is included in the 'Merkle Root',
I just need to know H4, H12

If I know Tx3, I will know H3
Having H3 & given H4, I will know H34
Given H12 & having H34, I will know H1234
If H1234 = Merkle Root, then Tx3 is inside the block



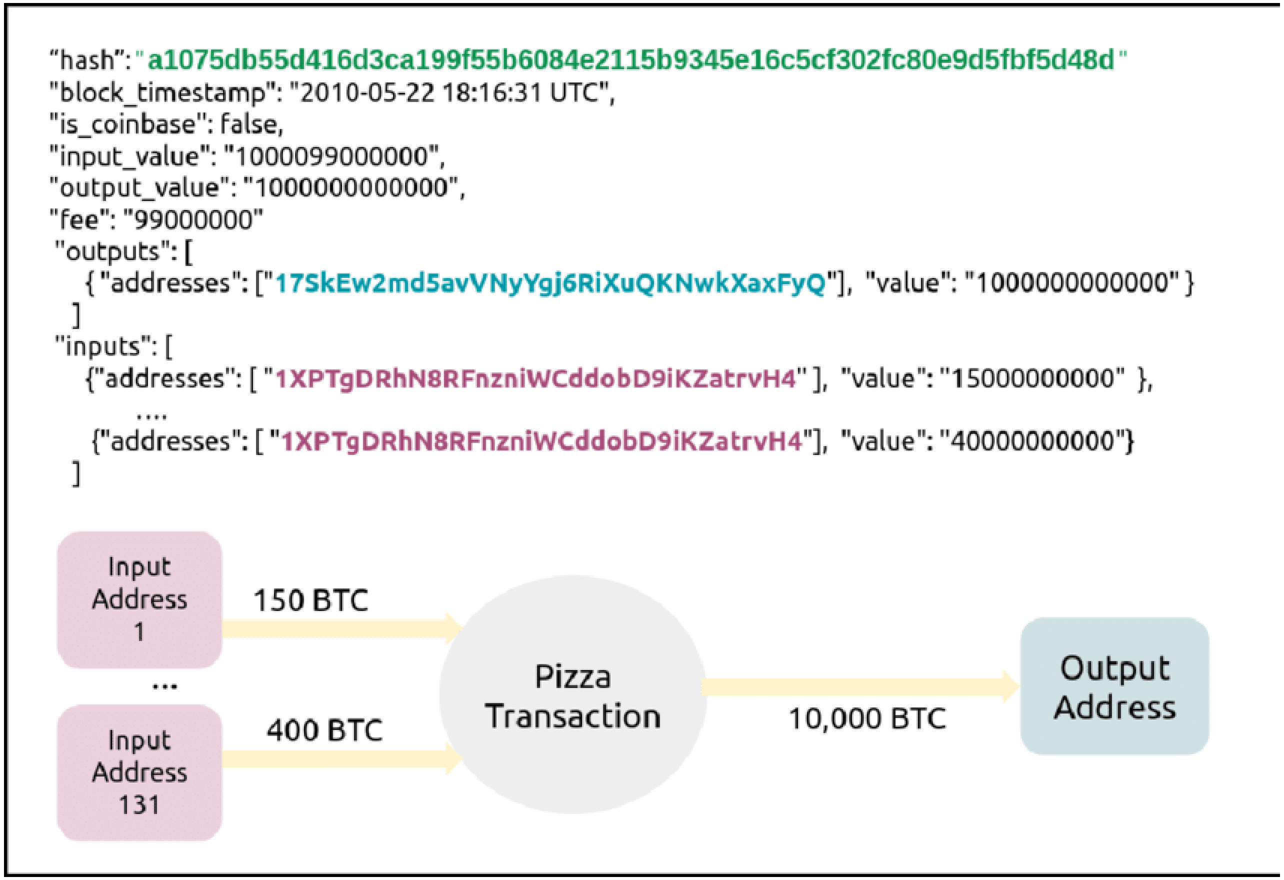
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Block number : 57043

- Pizza Tx
- https://www.blockchain.com/explorer/blocks/btc/57043

- On May 22, 2010 Laszlo Hanyecz paid Jeremy Sturdivant 10,000 bitcoins (BTC) for two Papa John's pizzas which were delivered to Hanyecz's home.
- This exchange is widely celebrated because it is viewed as the first use of bitcoin in a commercial transaction with bitcoin as the medium of exchange

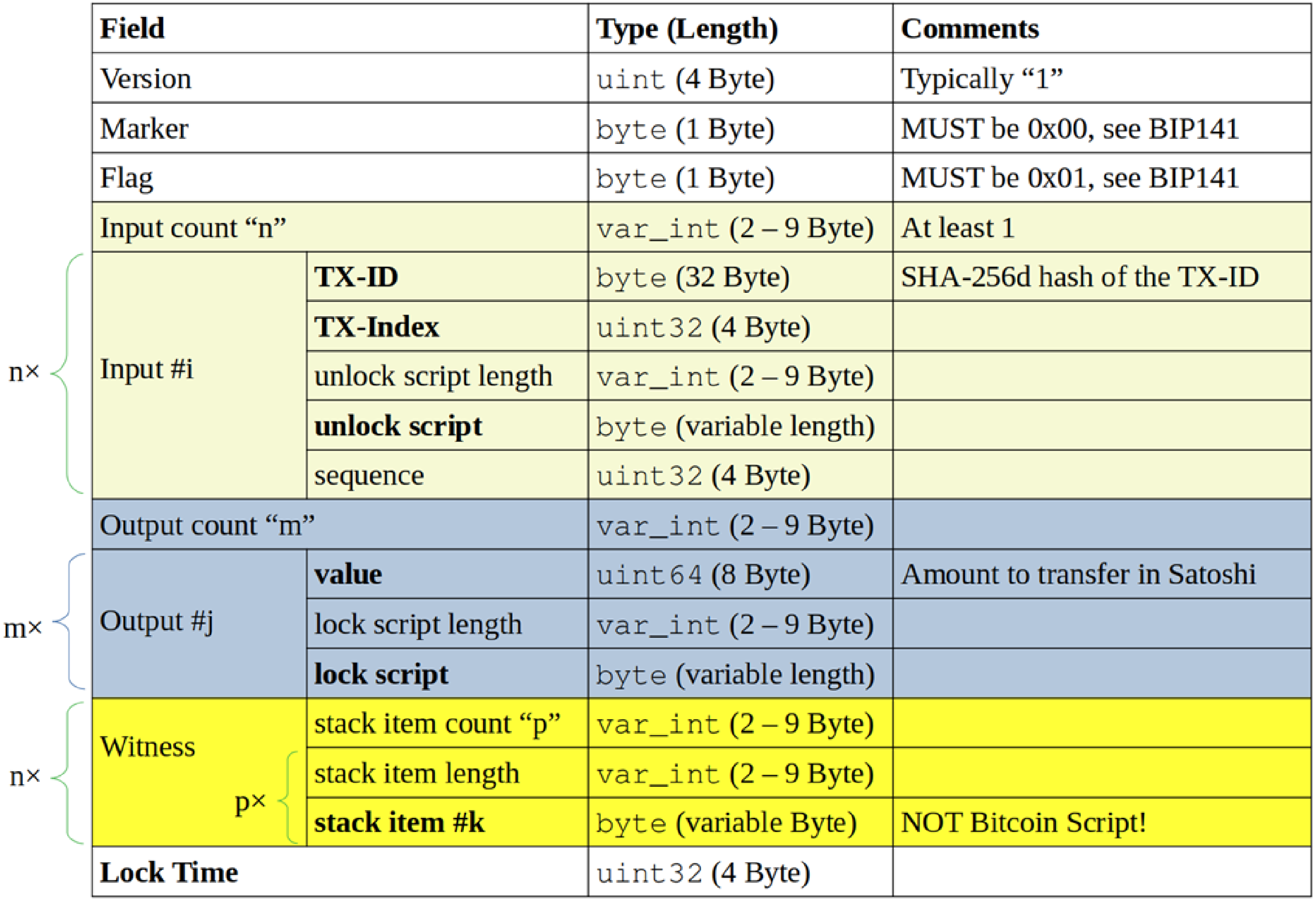
Pizza Transaction



```
“hash”:"a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d"
"block_timestamp": "2010-05-22 18:16:31 UTC",
"is_coinbase": false,
"input_value": "1000099000000",
"output_value": "1000000000000",
"fee": "99000000"
 "outputs": [
   { "addresses": ["17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ"],  "value": "1000000000000" }
  ]
 "inputs": [
   {"addresses": [ "1XPTgDRhN8RFnzniWCddobD9iKZatrvH4" ],  "value": "15000000000"  },
         ....
    {"addresses": [ "1XPTgDRhN8RFnzniWCddobD9iKZatrvH4"],  "value": "40000000000"}
  ]
```

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

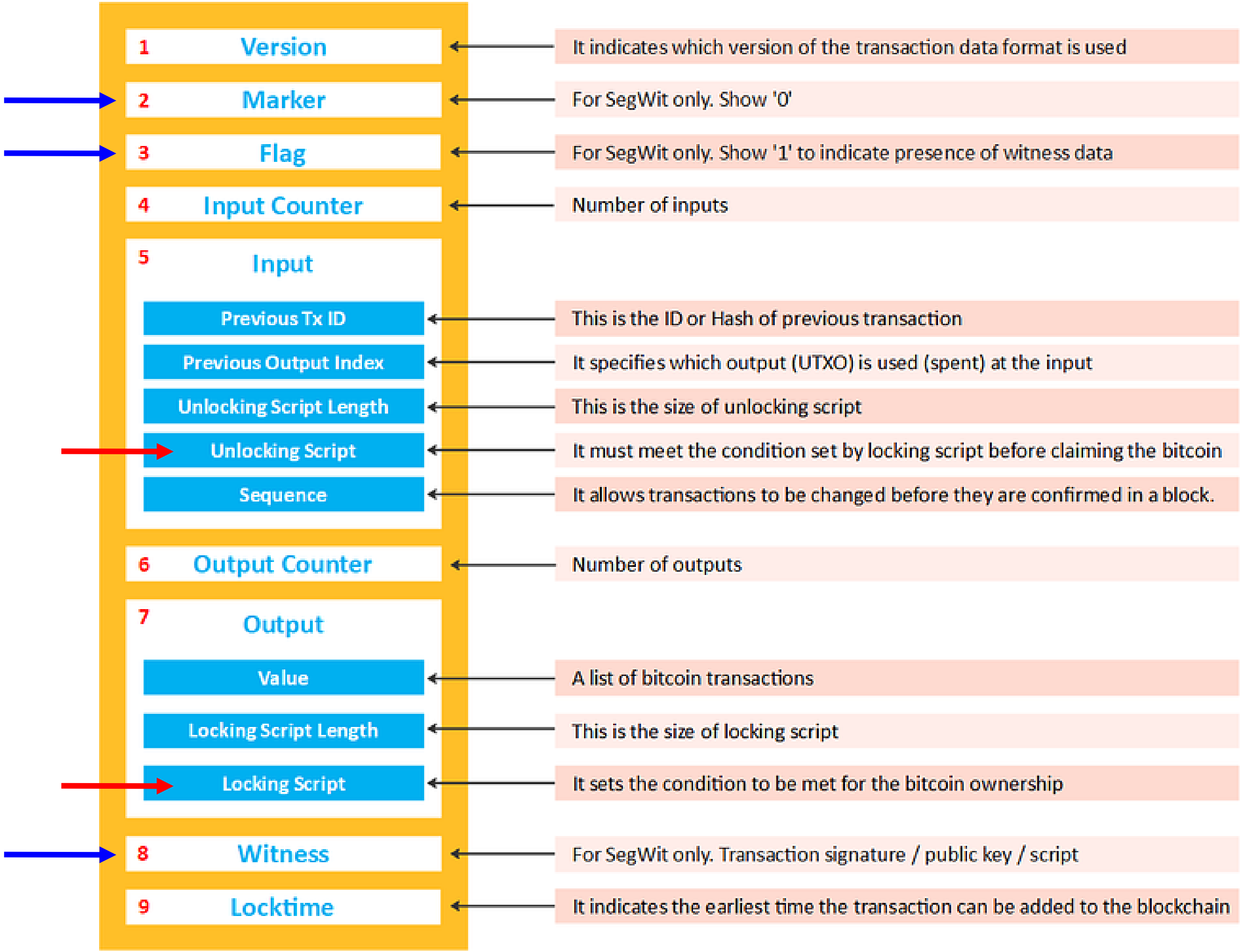
Bitcoin Transaction Format



	Field		Type (Length)	Comments
	Version		`uint` (4 Byte)	Typically “1”
	Marker		`byte` (1 Byte)	MUST be 0x00, see BIP141
	Flag		`byte` (1 Byte)	MUST be 0x01, see BIP141
	Input count “n”		`var_int` (2 – 9 Byte)	At least 1
n×	Input #i	**TX-ID**	`byte` (32 Byte)	SHA-256d hash of the TX-ID
		TX-Index	`uint32` (4 Byte)	
		unlock script length	`var_int` (2 – 9 Byte)	
		unlock script	`byte` (variable length)	
		sequence	`uint32` (4 Byte)	
	Output count “m”		`var_int` (2 – 9 Byte)	
m×	Output #j	**value**	`uint64` (8 Byte)	Amount to transfer in Satoshi
		lock script length	`var_int` (2 – 9 Byte)	
		lock script	`byte` (variable length)	
n×	Witness	stack item count “p”	`var_int` (2 – 9 Byte)	
	p×	stack item length	`var_int` (2 – 9 Byte)	
		stack item #k	`byte` (variable Byte)	NOT Bitcoin Script!
	Lock Time		`uint32` (4 Byte)	

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Transaction Structure



1 Version — It indicates which version of the transaction data format is used

2 Marker — For SegWit only. Show '0'

3 Flag — For SegWit only. Show '1' to indicate presence of witness data

4 Input Counter — Number of inputs

5 Input

- Previous Tx ID — This is the ID or Hash of previous transaction
- Previous Output Index — It specifies which output (UTXO) is used (spent) at the input
- Unlocking Script Length — This is the size of unlocking script
- Unlocking Script — It must meet the condition set by locking script before claiming the bitcoin
- Sequence — It allows transactions to be changed before they are confirmed in a block.

6 Output Counter — Number of outputs

7 Output

- Value — A list of bitcoin transactions
- Locking Script Length — This is the size of locking script
- Locking Script — It sets the condition to be met for the bitcoin ownership

8 Witness — For SegWit only. Transaction signature / public key / script

9 Locktime — It indicates the earliest time the transaction can be added to the blockchain

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Transaction Structure

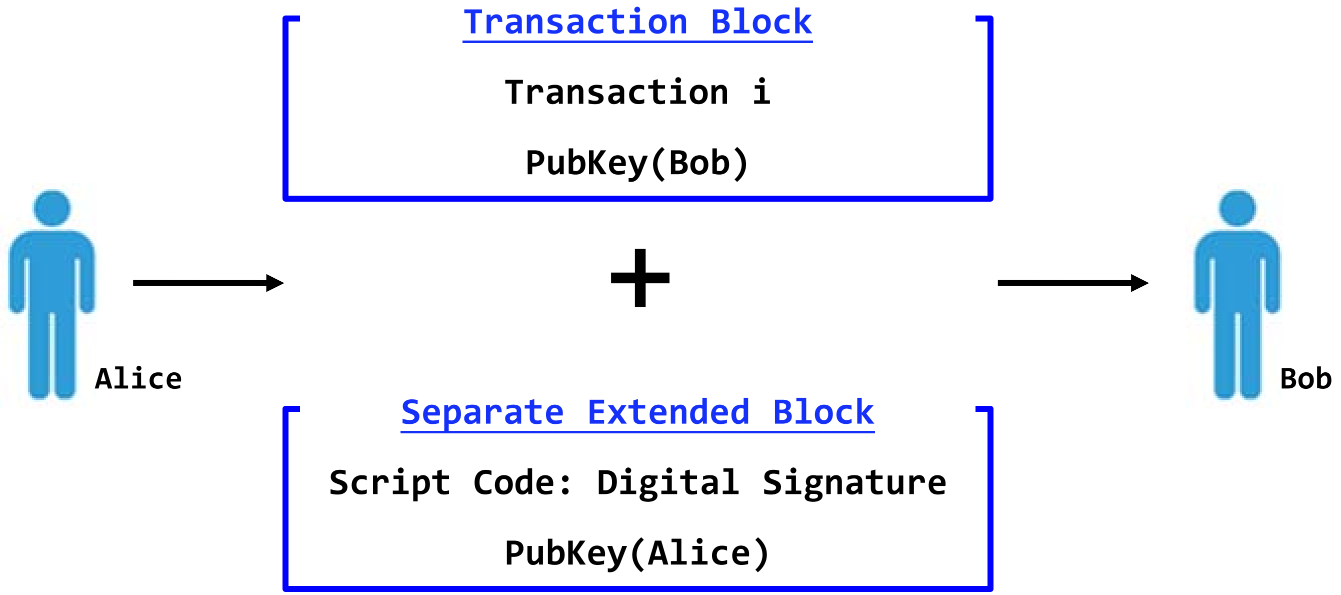
- BIP141 (Bitcoin Improvement Proposal)

- Legacy transaction
  - [nVersion] [txIns] [txOuts] [nLockTime]
  - Signature is stored in the 'unlocking script'

- SegWit transaction
  - [nVersion] [marker] [flag] [txIns] [txOuts] [witness] [nLockTime]
  - Signature is stored in the 'witness'

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

SegWit Tx



Transaction Block

Transaction i

PubKey(Bob)

+

Alice

Bob

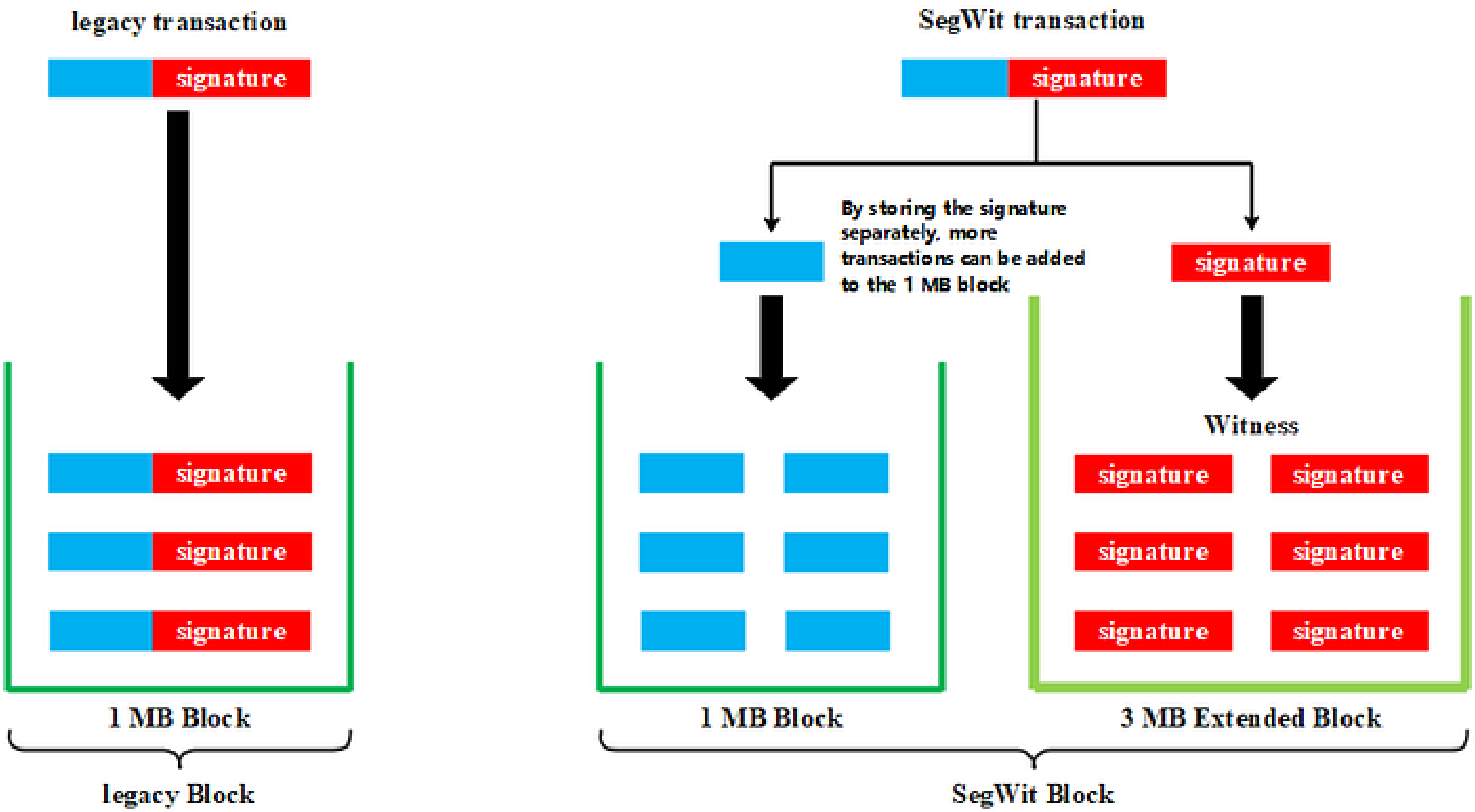
Separate Extended Block

Script Code: Digital Signature

PubKey(Alice)

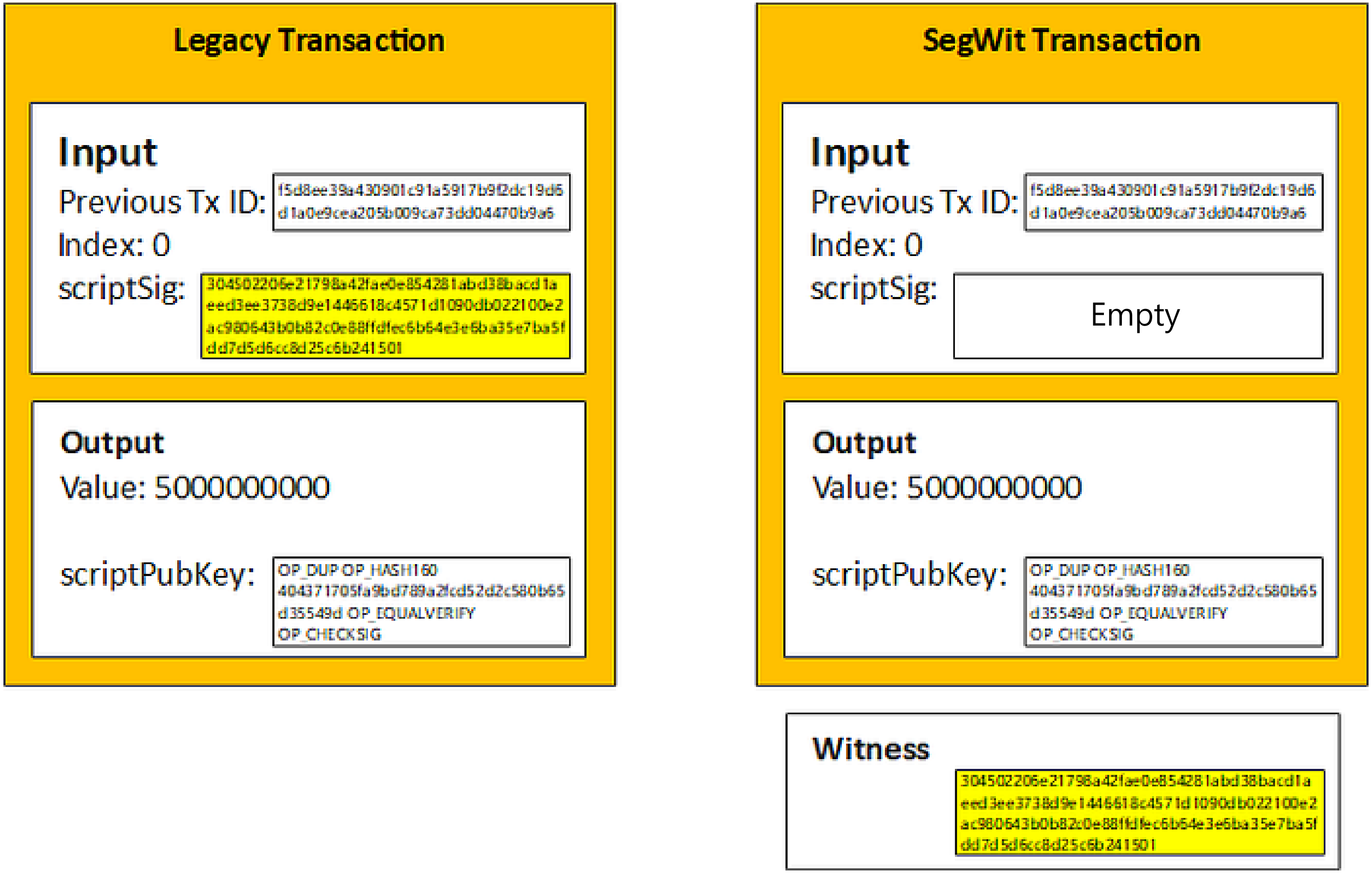
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Legacy vs SegWit Transaction



✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Legacy vs SegWit



Legacy Transaction

Input

Previous Tx ID: f5d8ee39a430901c91a5917b9f2dc19d6
d1a0e9cea205b009ca73dd04470b9a6

Index: 0

scriptSig: 304502206e21798a42fae0e854281abd38bacd1a
eed3ee3738d9e1446618c4571d1090db022100e2
ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5f
dd7d5d6cc8d25c6b241501

Output

Value: 5000000000

scriptPubKey: OP_DUP OP_HASH160
404371705fa9bd789a2fcd52d2c580b65
d35549d OP_EQUALVERIFY
OP_CHECKSIG

SegWit Transaction

Input

Previous Tx ID: f5d8ee39a430901c91a5917b9f2dc19d6
d1a0e9cea205b009ca73dd04470b9a6

Index: 0

scriptSig: Empty

Output

Value: 5000000000

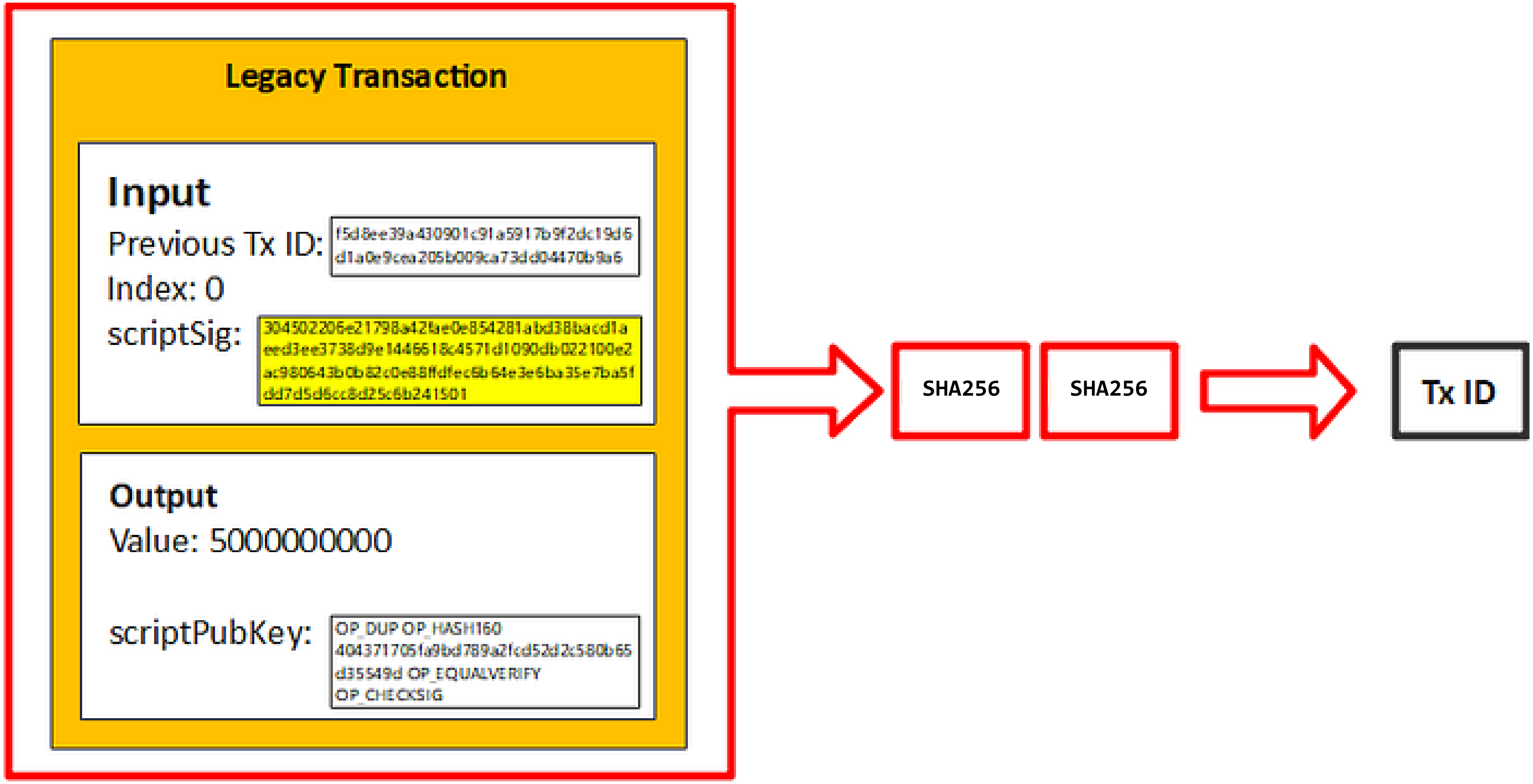
scriptPubKey: OP_DUP OP_HASH160
404371705fa9bd789a2fcd52d2c580b65
d35549d OP_EQUALVERIFY
OP_CHECKSIG

Witness

304502206e21798a42fae0e854281abd38bacd1a
eed3ee3738d9e1446618c4571d1090db022100e2
ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5f
dd7d5d6cc8d25c6b241501

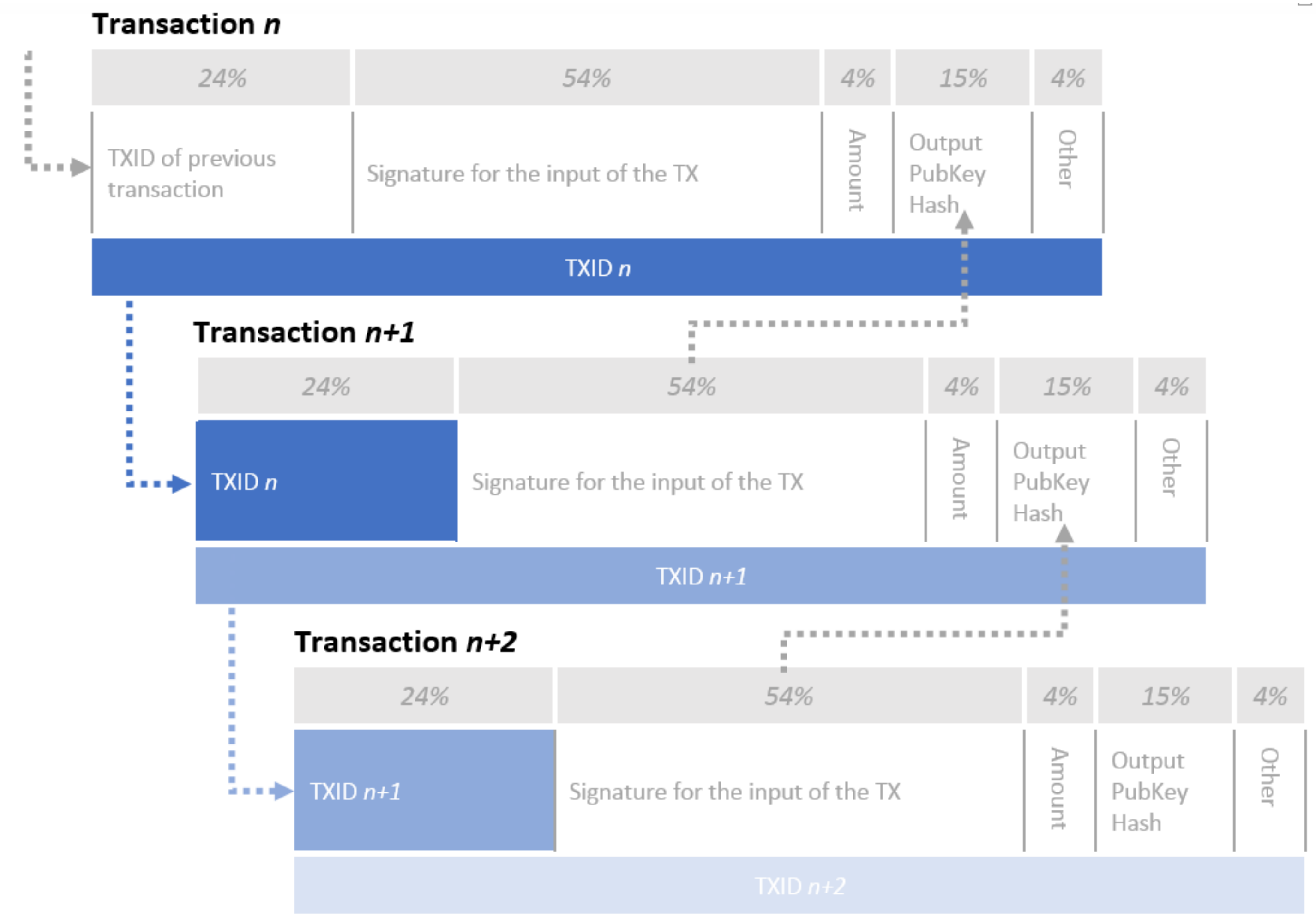
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Legacy Tx


Legacy Transaction
Input
Previous Tx ID:
f5d8ee39a430901c91a5917b9f2dc19d6
d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig:
304502206e21798a42fae0e854281abd38bacd1a
eed3ee3738d9e1446618c4571d1090db022100e2
ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5f
dd7d5d6cc8d25c6b241501
Output
Value: 5000000000
scriptPubKey:
OP_DUP OP_HASH160
404371705fa9bd789a2fcd52d2c580b65
d35549d OP_EQUALVERIFY
OP_CHECKSIG
SHA256
SHA256
Tx ID

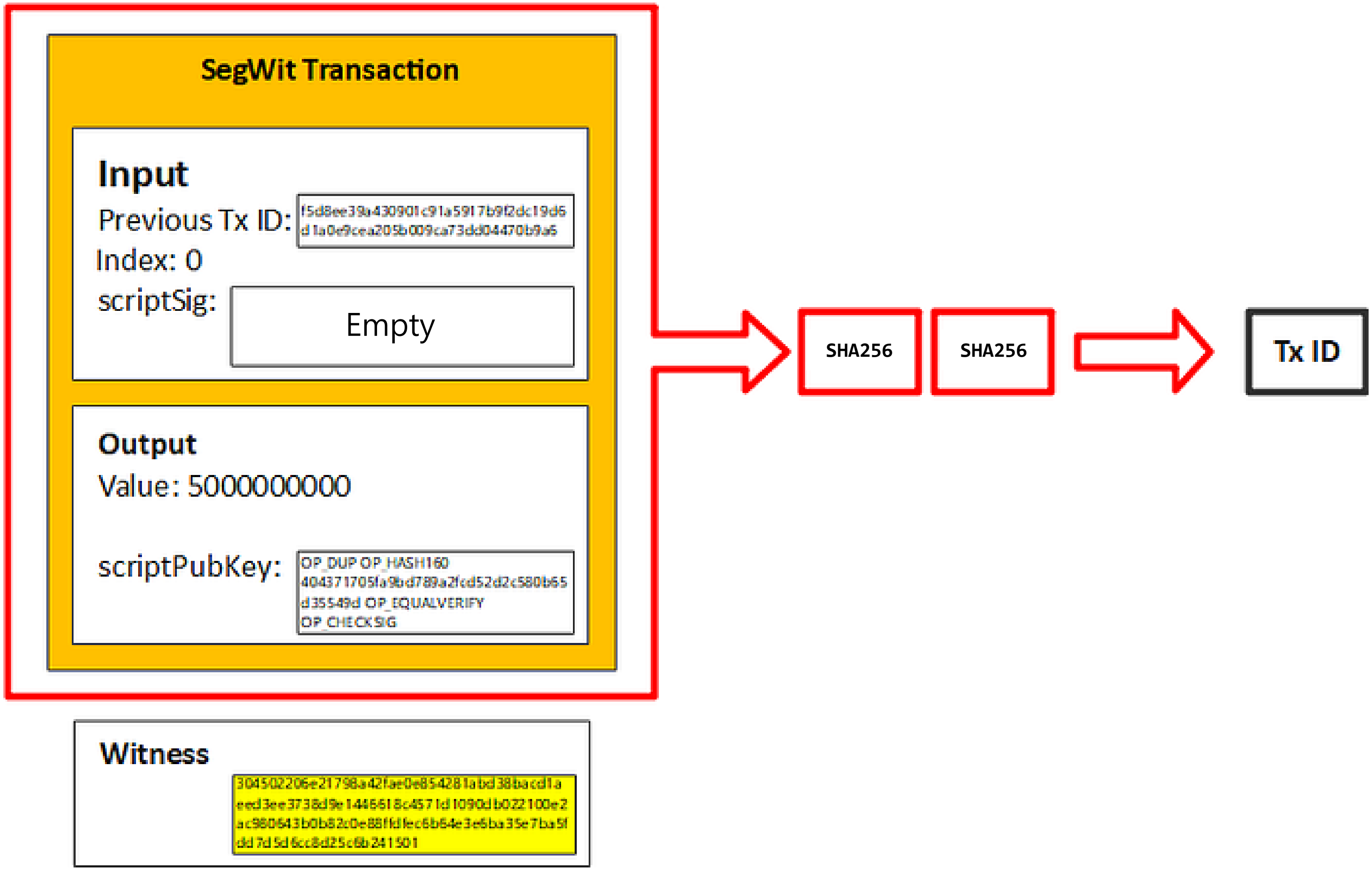
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Legacy Tx



✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

SegWit Tx



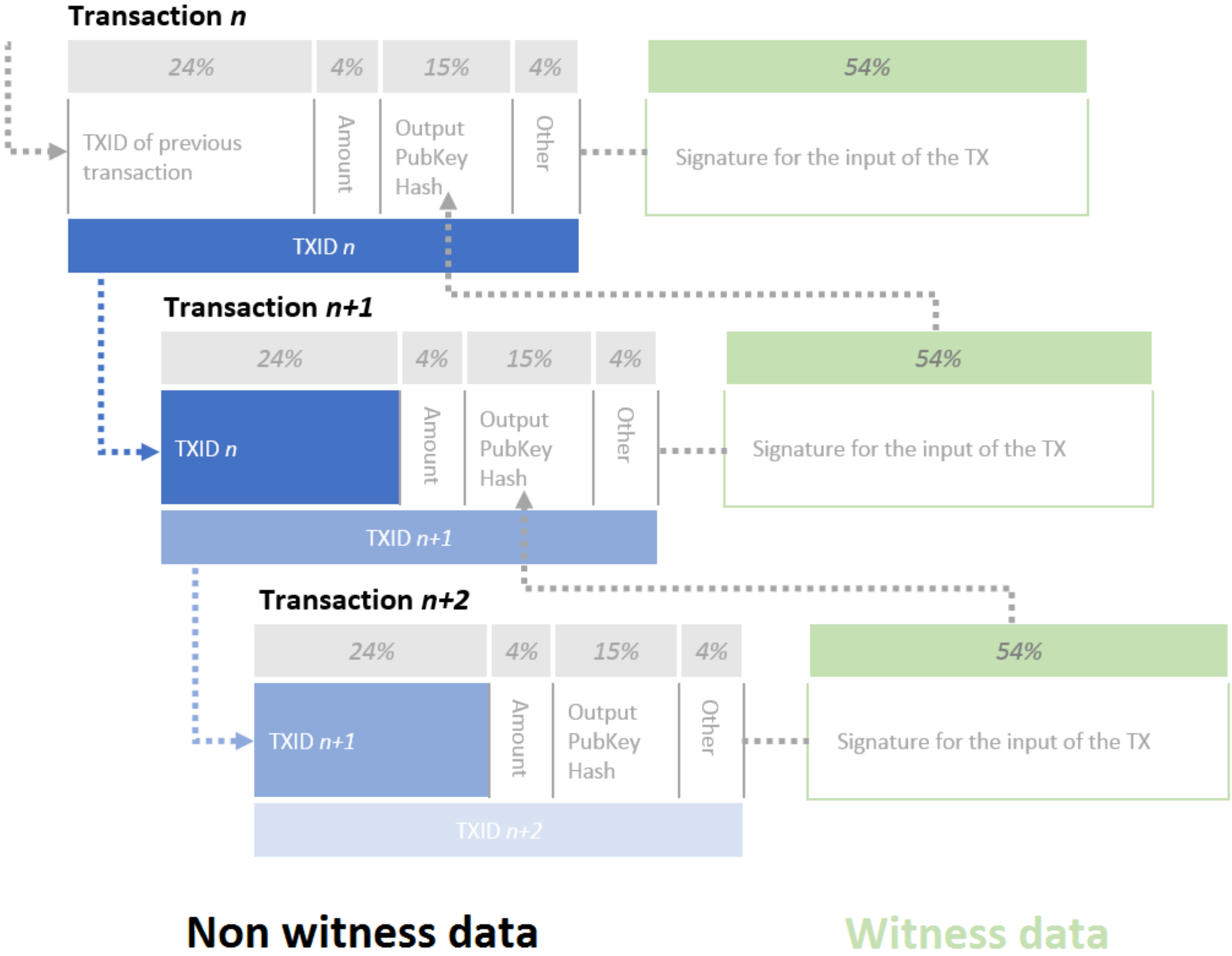
Previous Tx ID: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6

scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d OP_EQUALVERIFY OP_CHECKSIG

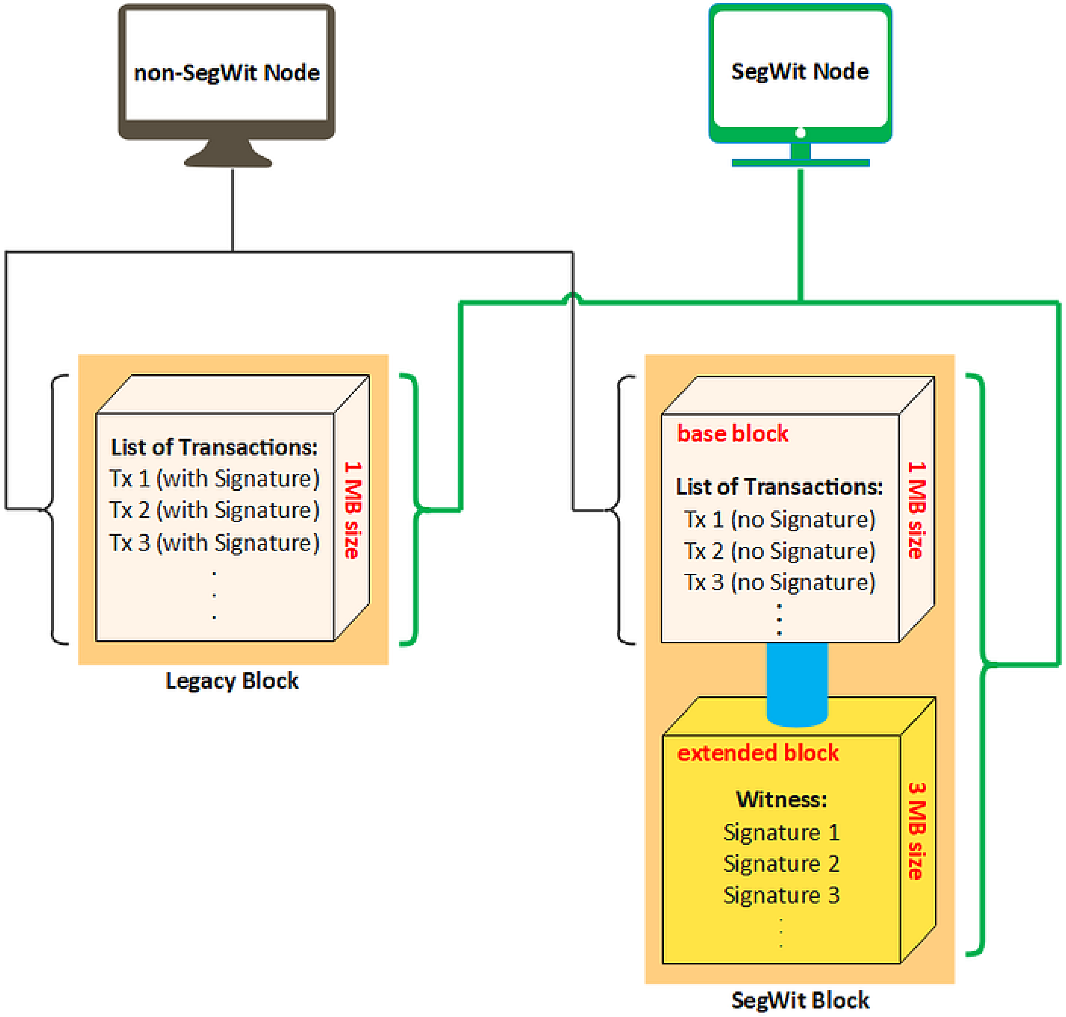
Witness: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

SegWit Tx

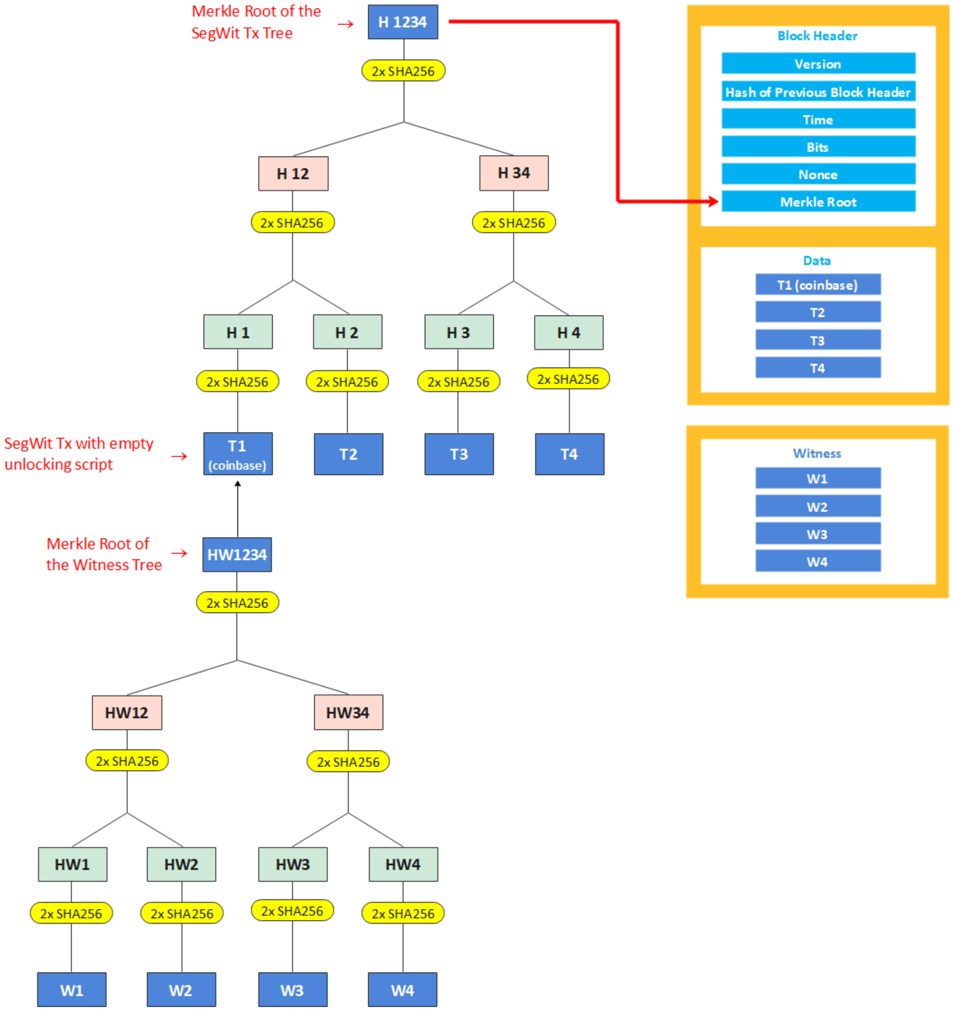


✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**



✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Merkle Root for SegWit Transaction



Merkle Root of the SegWit Tx Tree →

H 1234

2x SHA256

H 12

2x SHA256

H 34

2x SHA256

H 1

2x SHA256

H 2

2x SHA256

H 3

2x SHA256

H 4

2x SHA256

SegWit Tx with empty unlocking script →

T1 (coinbase)

T2

T3

T4

Merkle Root of the Witness Tree →

HW1234

2x SHA256

HW12

2x SHA256

HW34

2x SHA256

HW1

2x SHA256

HW2

2x SHA256

HW3

2x SHA256

HW4

2x SHA256

W1

W2

W3

W4

Block Header

Version

Hash of Previous Block Header

Time

Bits

Nonce

Merkle Root

Data

T1 (coinbase)

T2

T3

T4

Witness

W1

W2

W3

W4

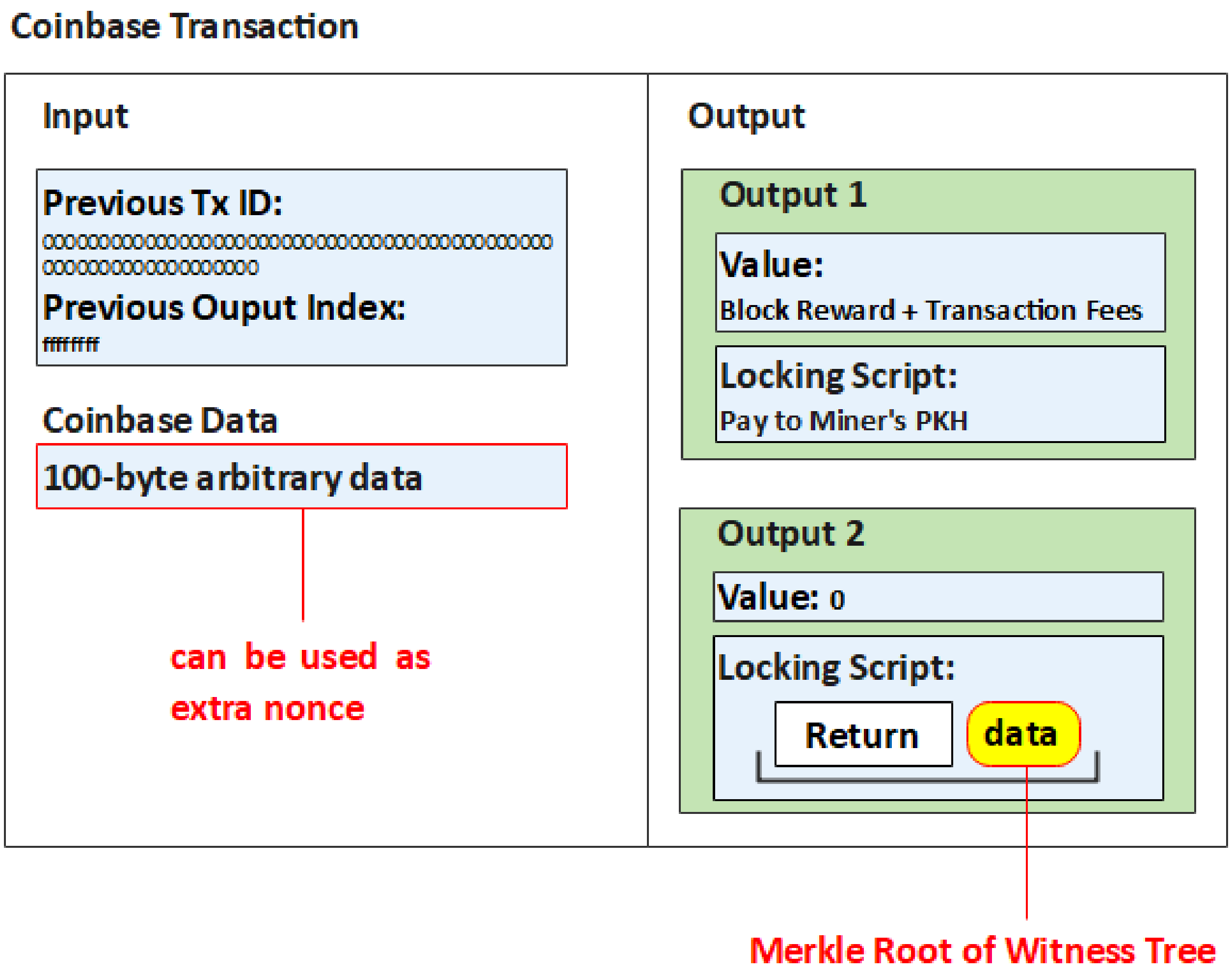
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

- Merkle tree
  - Transaction Merkle tree
  - Witness Merkel tree : SegWit (Segregated Witness) data

Coinbase Tx or Generation Tx

- There is no unlocking script
- The unlocking script is replaced by 'coinbase data', which is a 100-byte arbitrary data
  - This 100-byte arbitrary data can be used as an 'extra nonce'
- for SegWit transaction
  - its Merkle root of witness tree is stored as 'data' in the null data locking script.

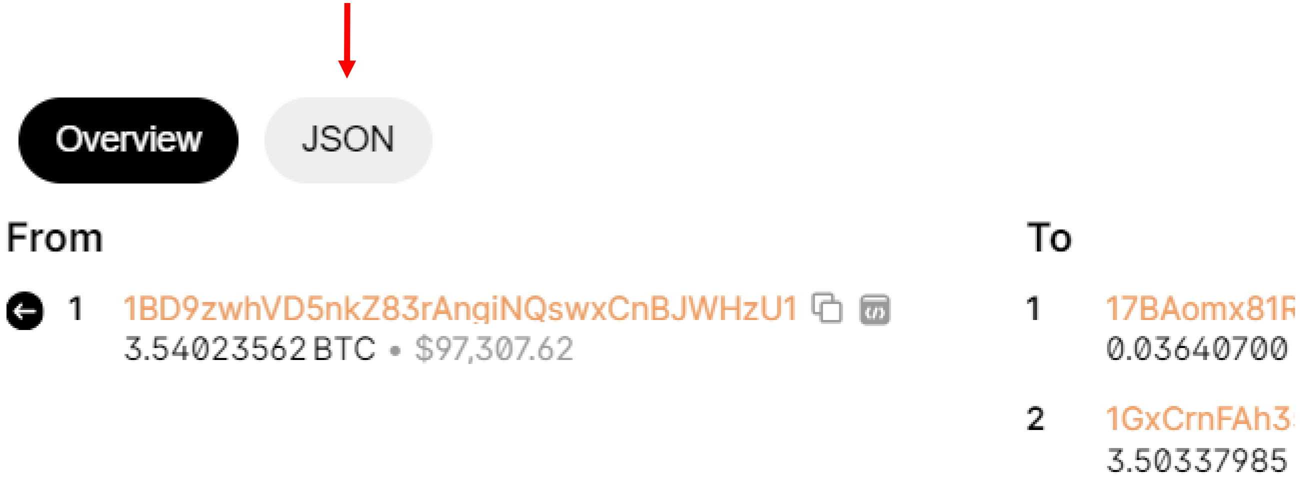
Coinbase Tx



✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

JSON

- https://www.blockchain.com/explorer/transactions/btc/82d62d5f4e69ae8338c39b7ae2e1d33db59bdf62c869ded7344adc936bab8653



From

1 1BD9zwhVD5nkZ83rAngiNQswxCnBJWHzU1
3.54023562 BTC • $97,307.62

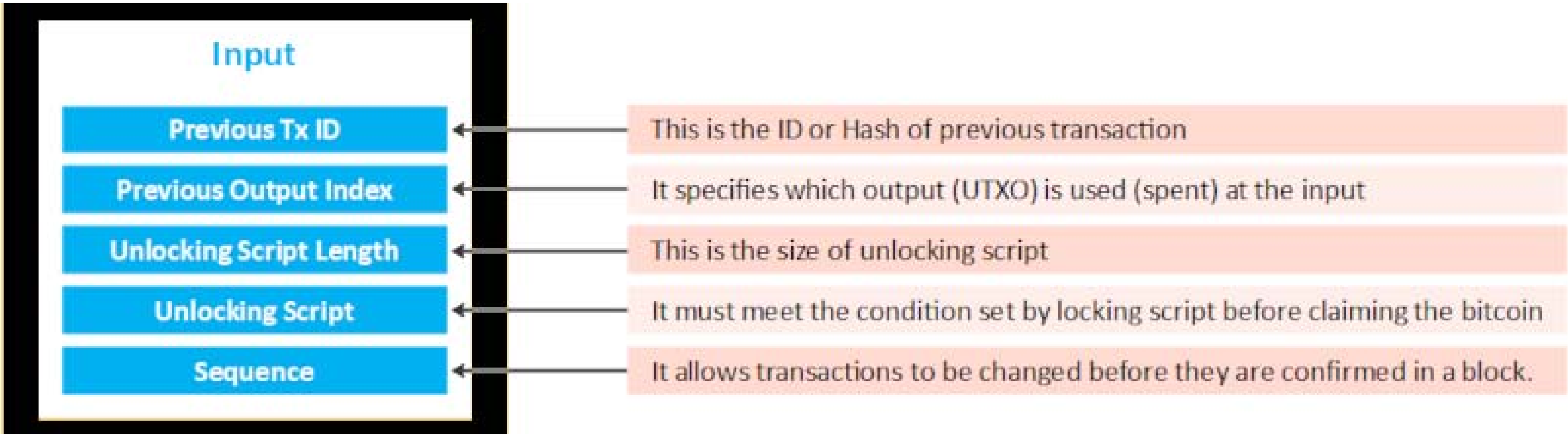
To

1 17BAomx81F
0.03640700

2 1GxCrnFAh3
3.50337985

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Transaction Inputs



Previous Tx ID — This is the ID or Hash of previous transaction

Previous Output Index — It specifies which output (UTXO) is used (spent) at the input

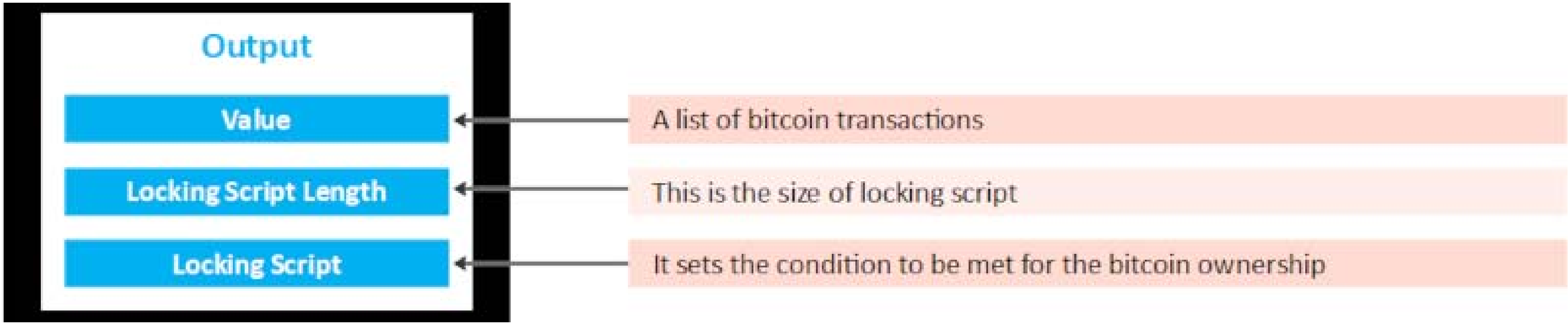
Unlocking Script Length — This is the size of unlocking script

Unlocking Script — It must meet the condition set by locking script before claiming the bitcoin

Sequence — It allows transactions to be changed before they are confirmed in a block.

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Transaction Outputs



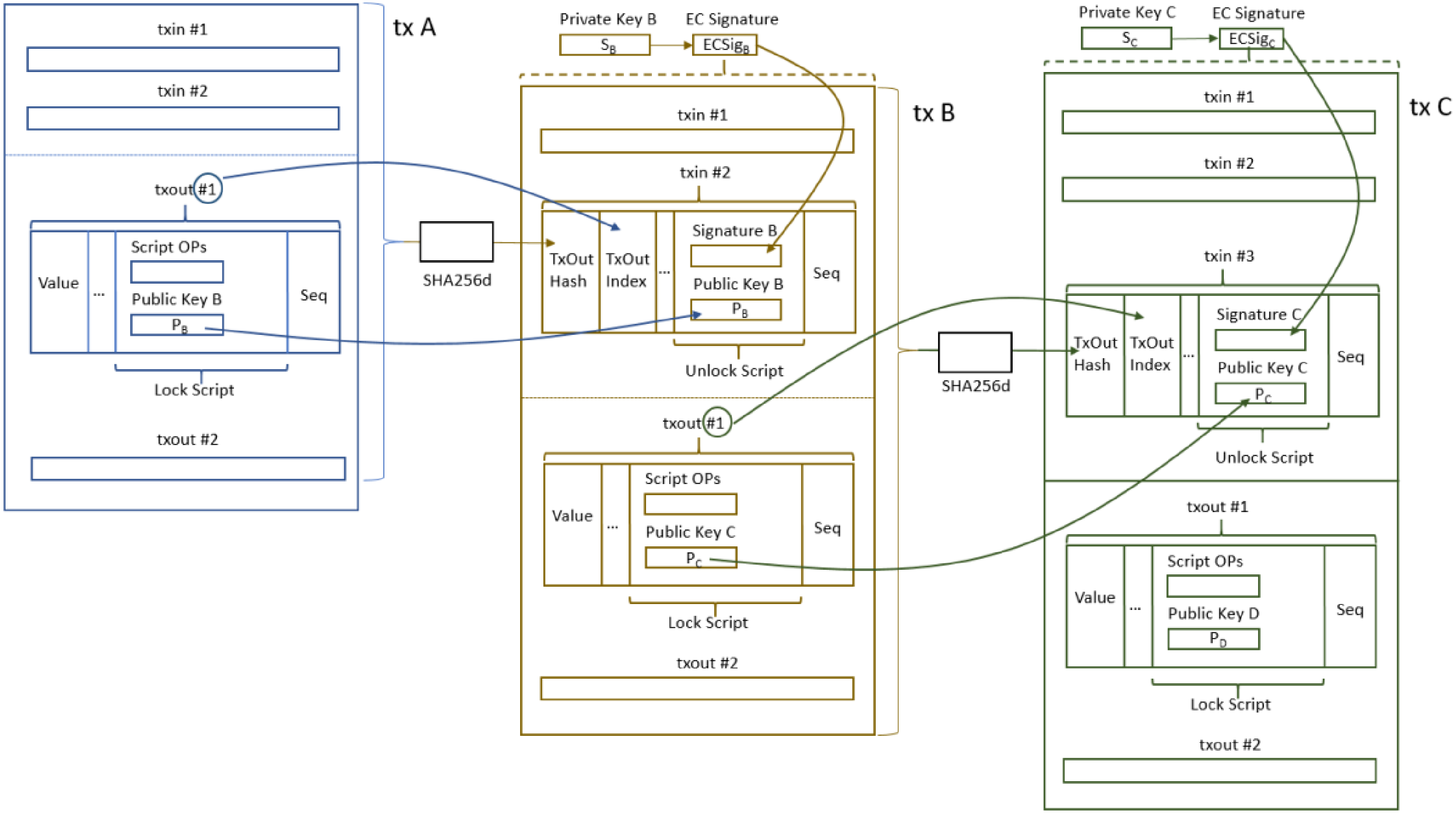
A list of bitcoin transactions

This is the size of locking script

It sets the condition to be met for the bitcoin ownership

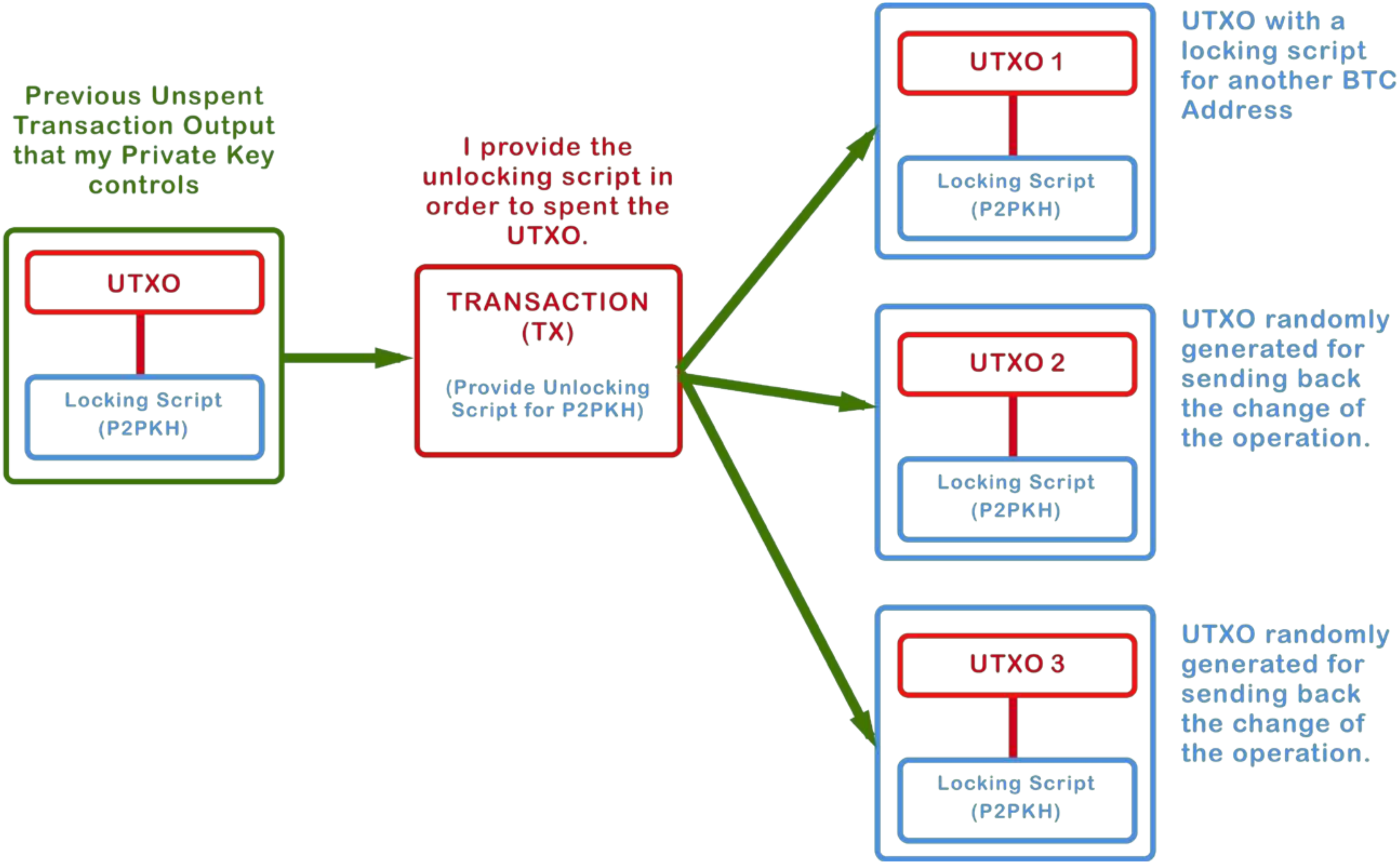
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

https://privatekeys.org/2018/04/17/anatomy-of-a-bitcoin-transaction/



✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

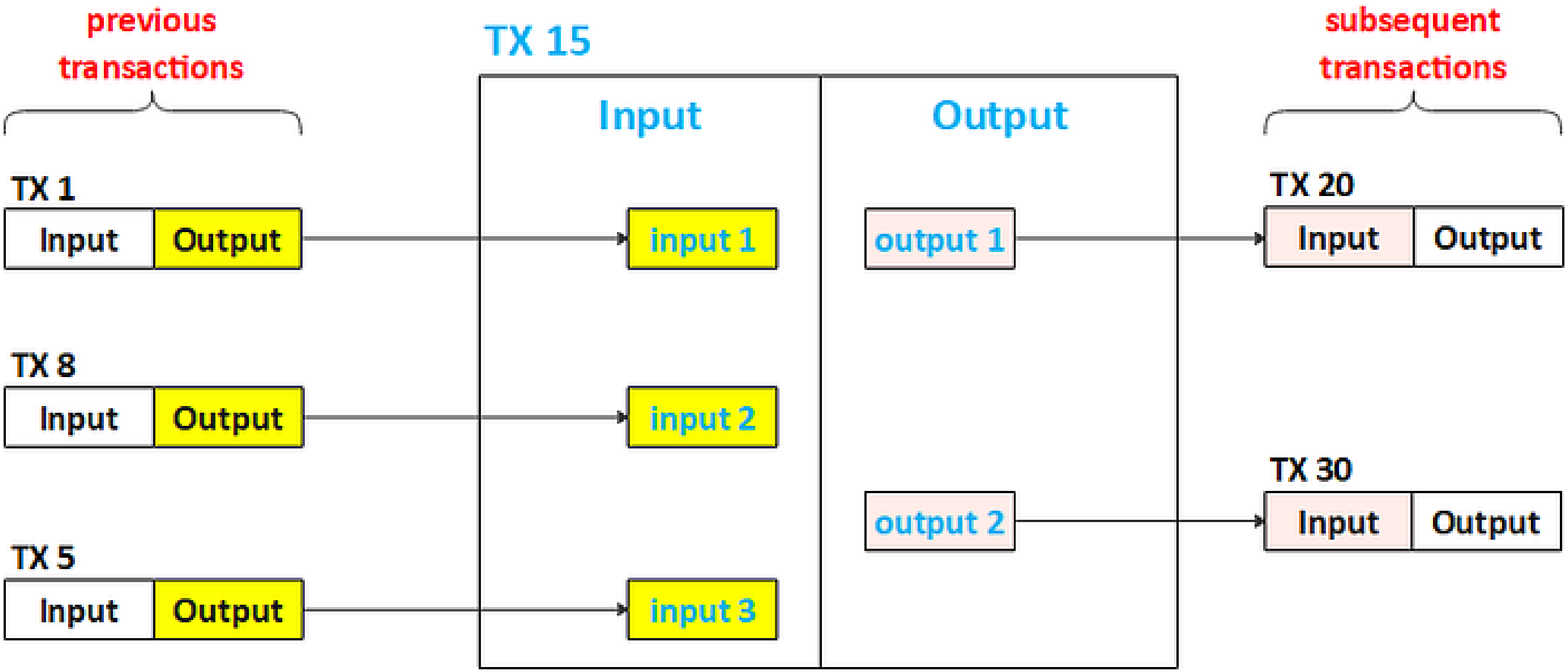
UTXO (Unspent Transaction Output)



Previous Unspent Transaction Output that my Private Key controls
UTXO
Locking Script (P2PKH)
I provide the unlocking script in order to spent the UTXO.
TRANSACTION (TX)
(Provide Unlocking Script for P2PKH)
UTXO 1
Locking Script (P2PKH)
UTXO with a locking script for another BTC Address
UTXO 2
Locking Script (P2PKH)
UTXO randomly generated for sending back the change of the operation.
UTXO 3
Locking Script (P2PKH)
UTXO randomly generated for sending back the change of the operation.

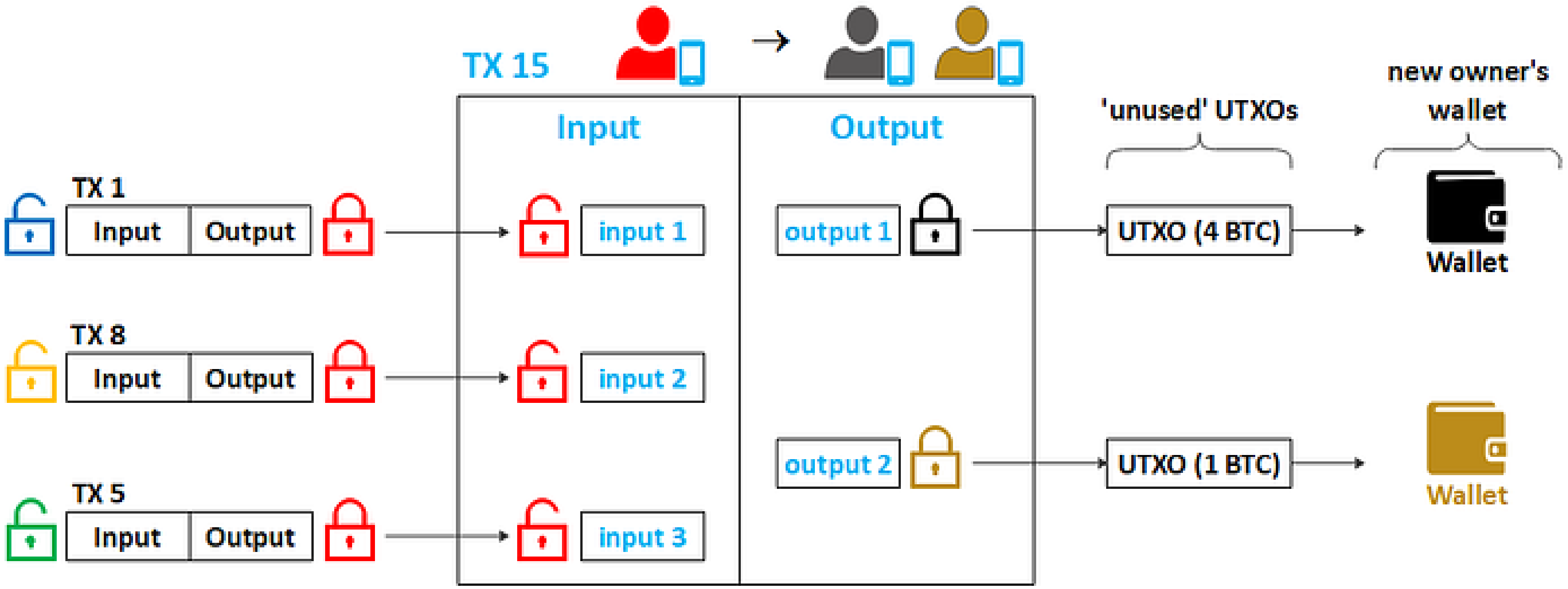
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Tx Chain ?



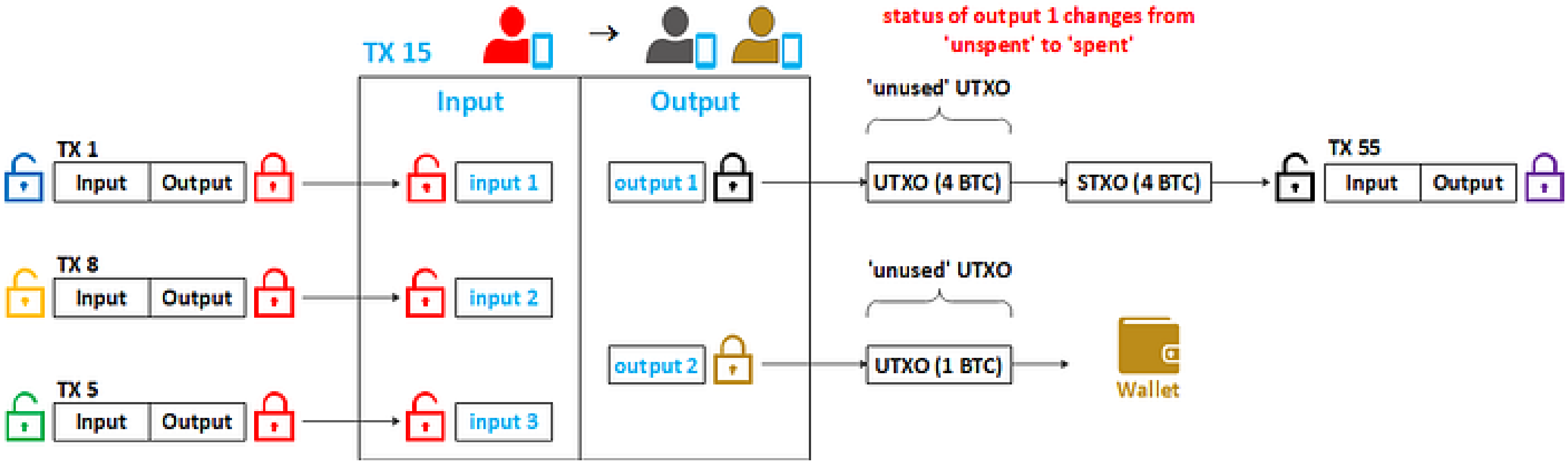
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

UTXO

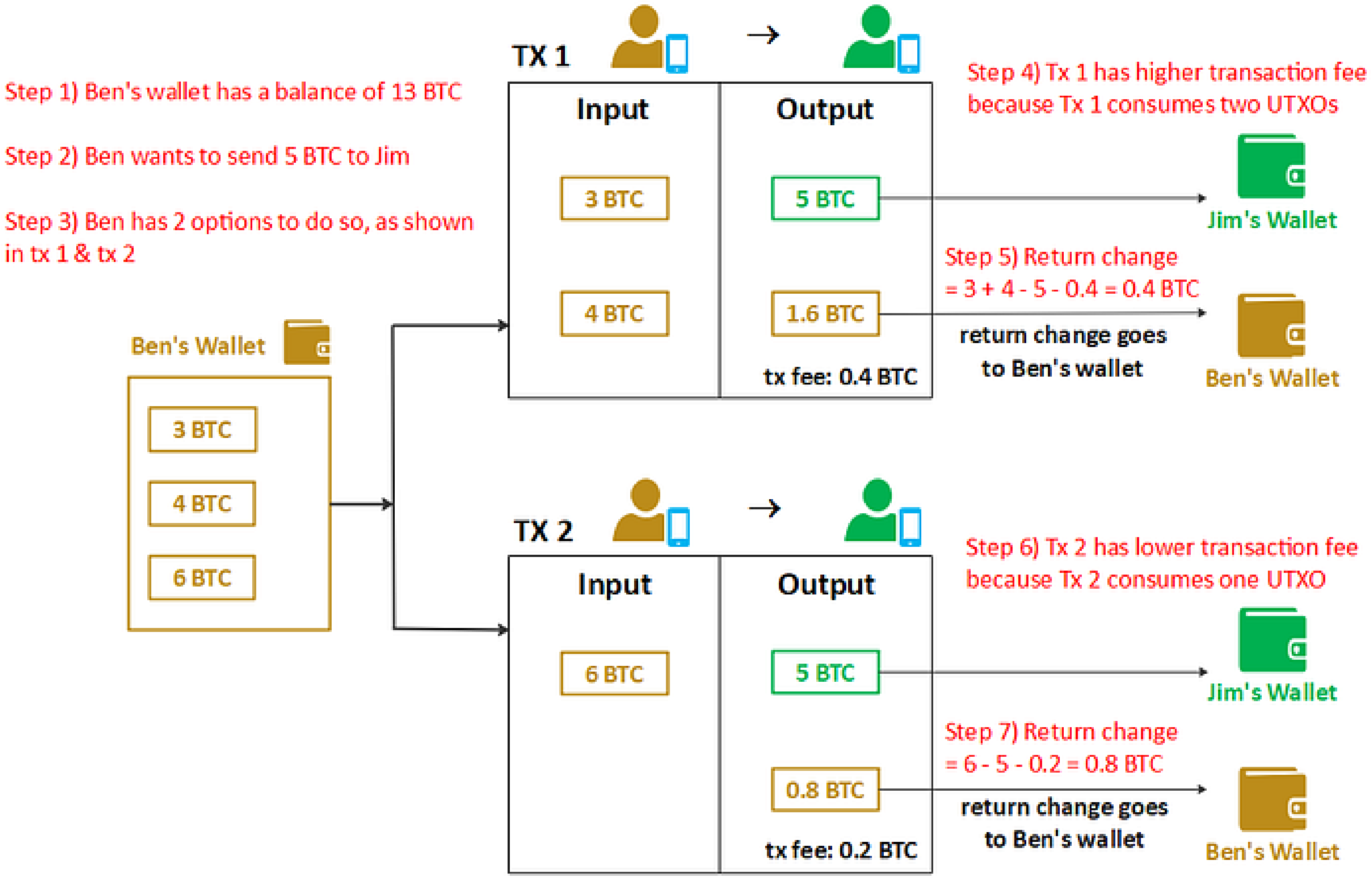


✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Unspent vs Spent Transaction



✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)



Step 1) Ben's wallet has a balance of 13 BTC

Step 2) Ben wants to send 5 BTC to Jim

Step 3) Ben has 2 options to do so, as shown in tx 1 & tx 2

Ben's Wallet

3 BTC

4 BTC

6 BTC

TX 1

Input	Output
3 BTC	5 BTC
4 BTC	1.6 BTC
	tx fee: 0.4 BTC

Step 4) Tx 1 has higher transaction fee because Tx 1 consumes two UTXOs

Jim's Wallet

Step 5) Return change = 3 + 4 - 5 - 0.4 = 0.4 BTC

return change goes to Ben's wallet

Ben's Wallet

TX 2

Input	Output
6 BTC	5 BTC
	0.8 BTC
	tx fee: 0.2 BTC

Step 6) Tx 2 has lower transaction fee because Tx 2 consumes one UTXO

Jim's Wallet

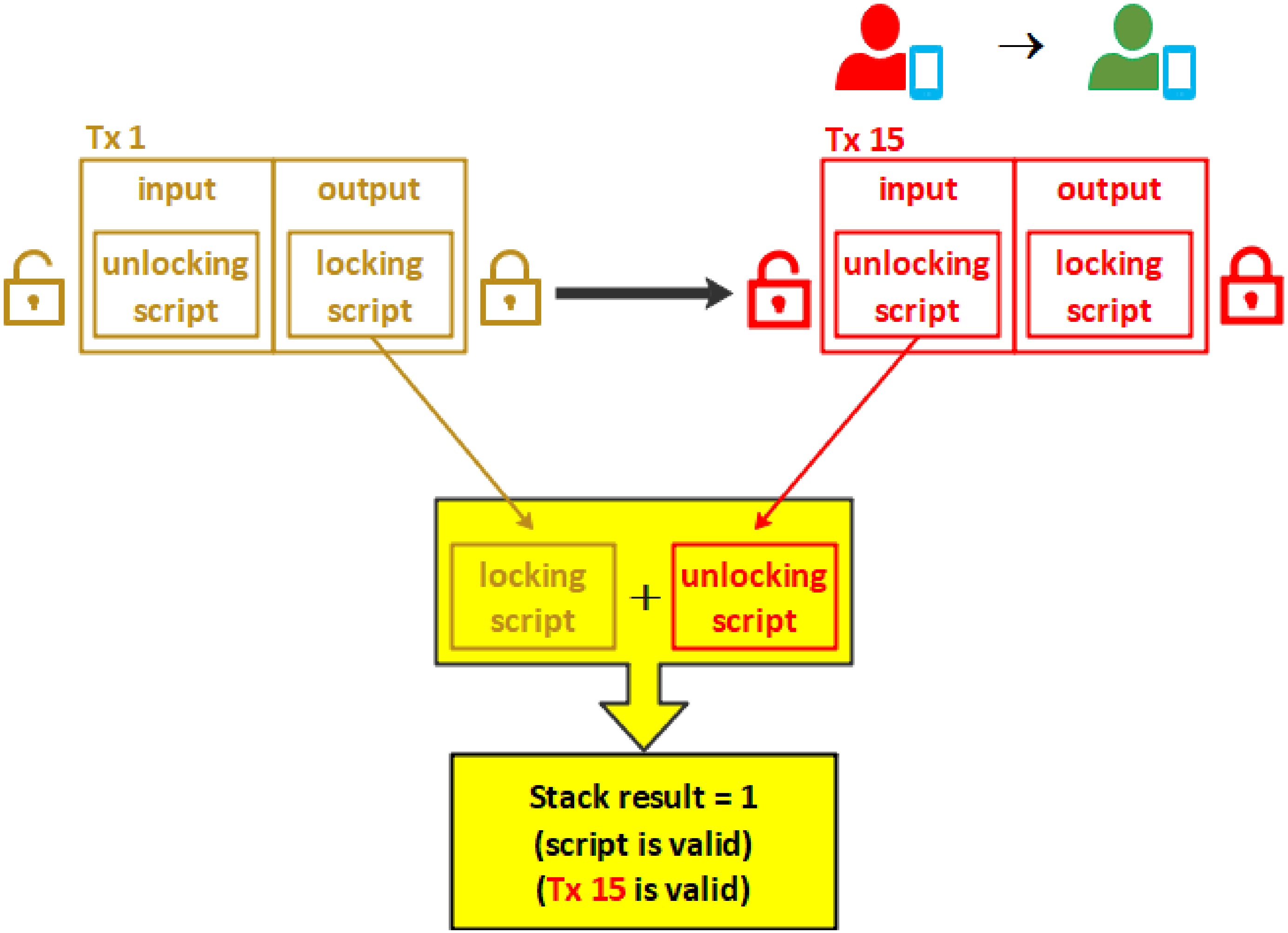
Step 7) Return change = 6 - 5 - 0.2 = 0.8 BTC

return change goes to Ben's wallet

Ben's Wallet

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

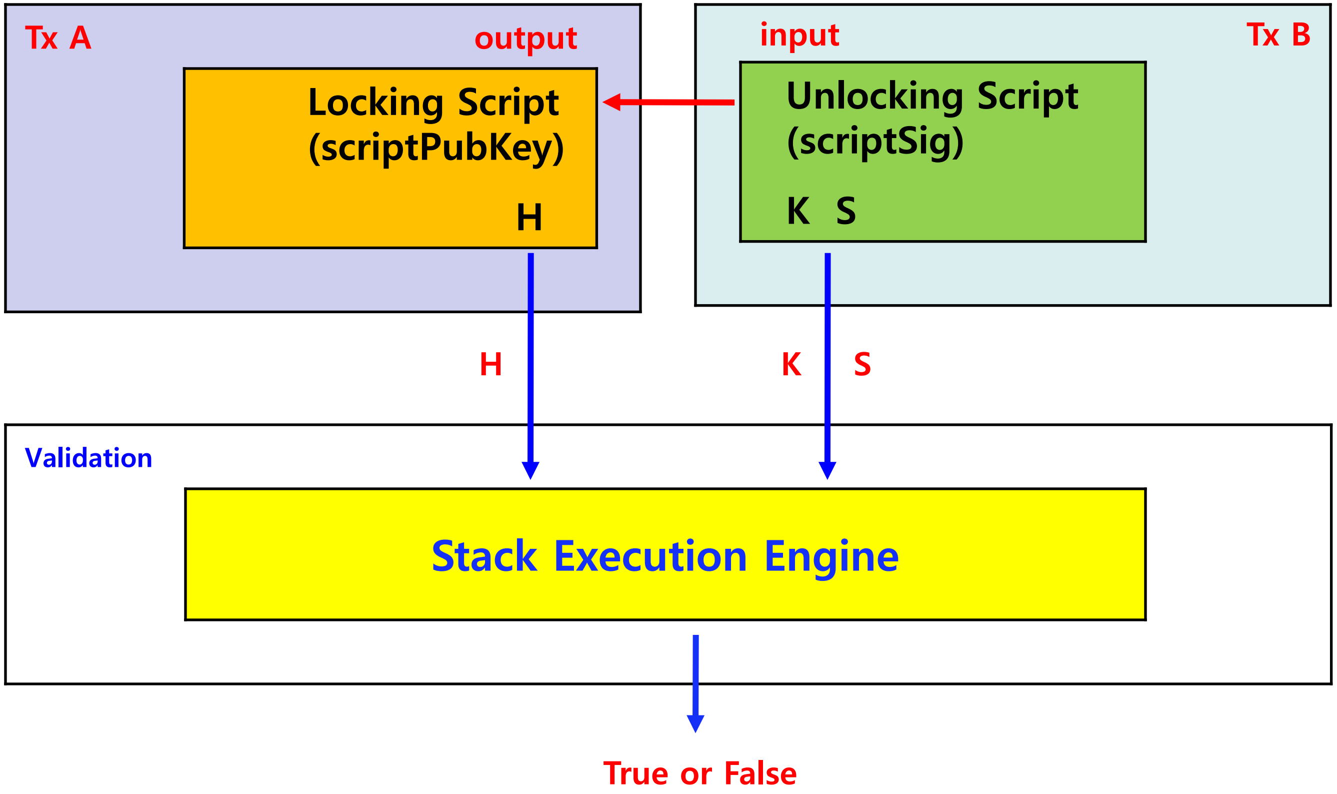
Scripts in Tx



✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

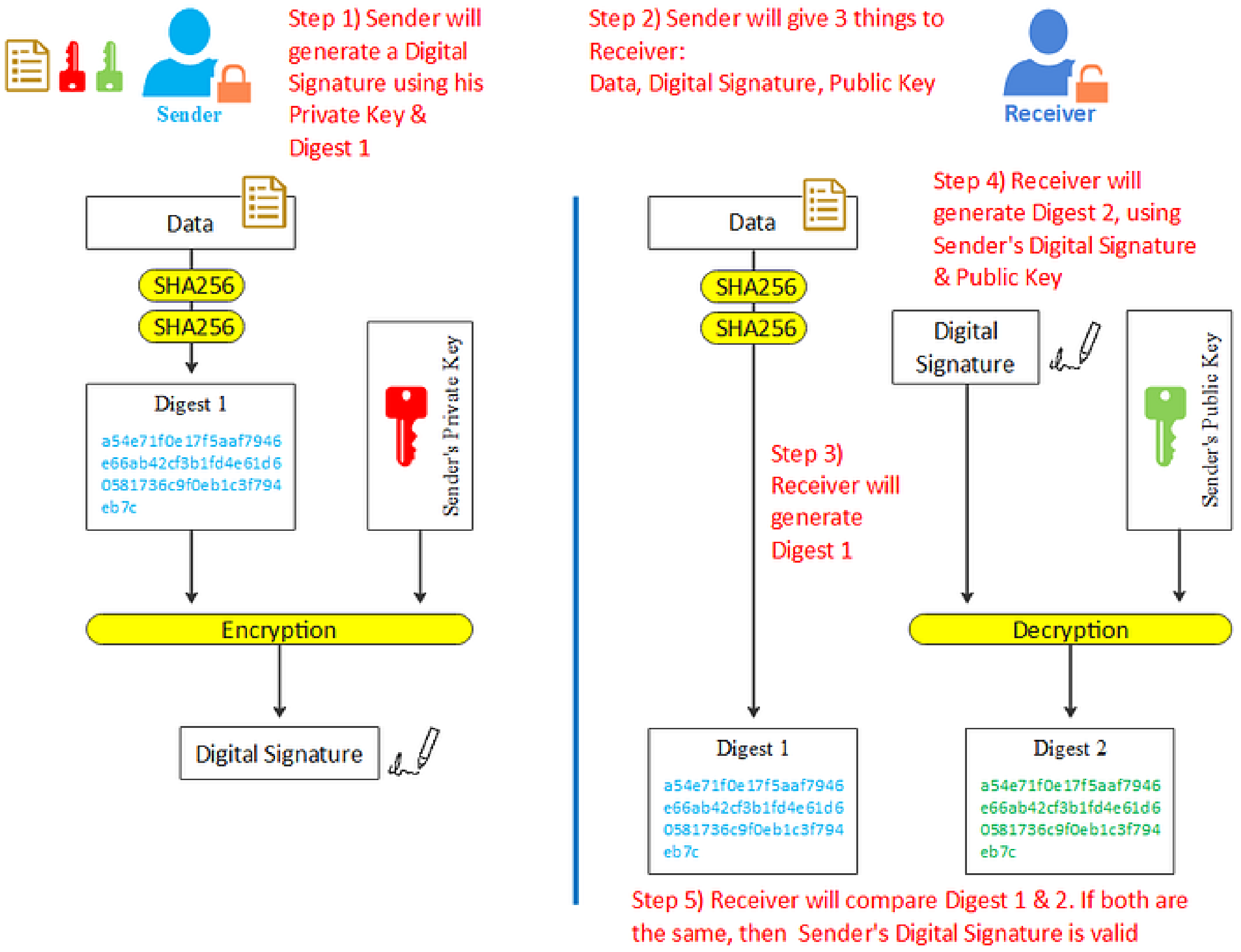
Locking and Unlocking Script

- Input : Unlocking script (scriptSig) is located
- Output : Locking script (scriptPubKey) is located



✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Signature



Step 1) Sender will generate a Digital Signature using his Private Key & Digest 1

Step 2) Sender will give 3 things to Receiver:
Data, Digital Signature, Public Key

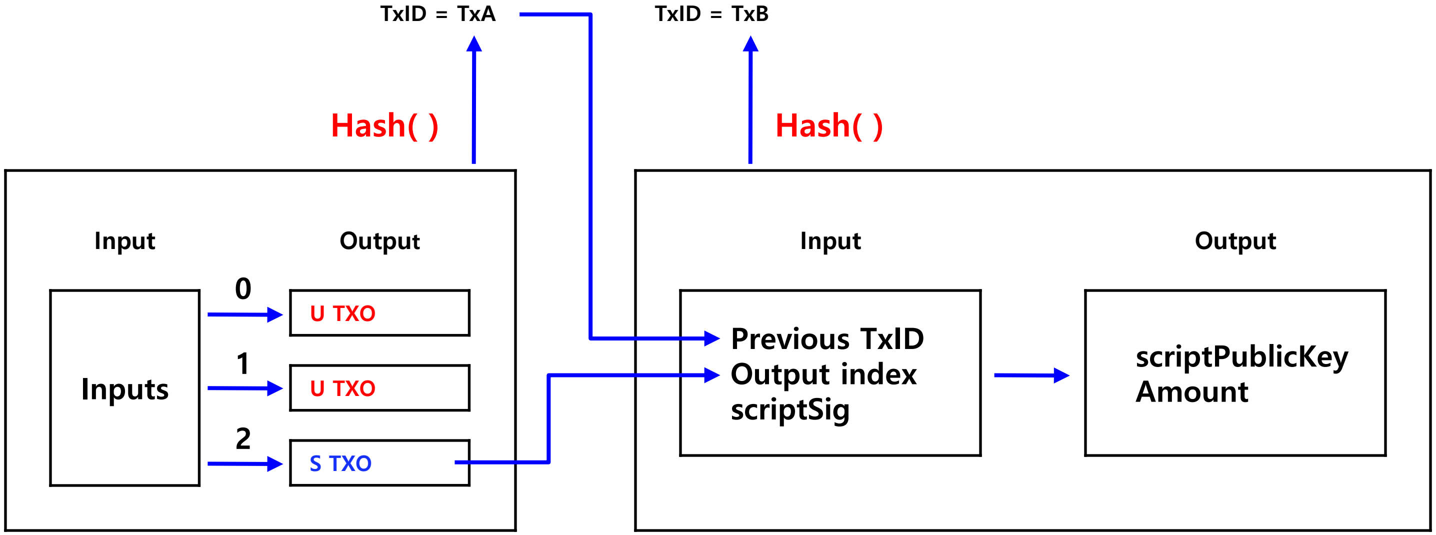
Step 3) Receiver will generate Digest 1

Step 4) Receiver will generate Digest 2, using Sender's Digital Signature & Public Key

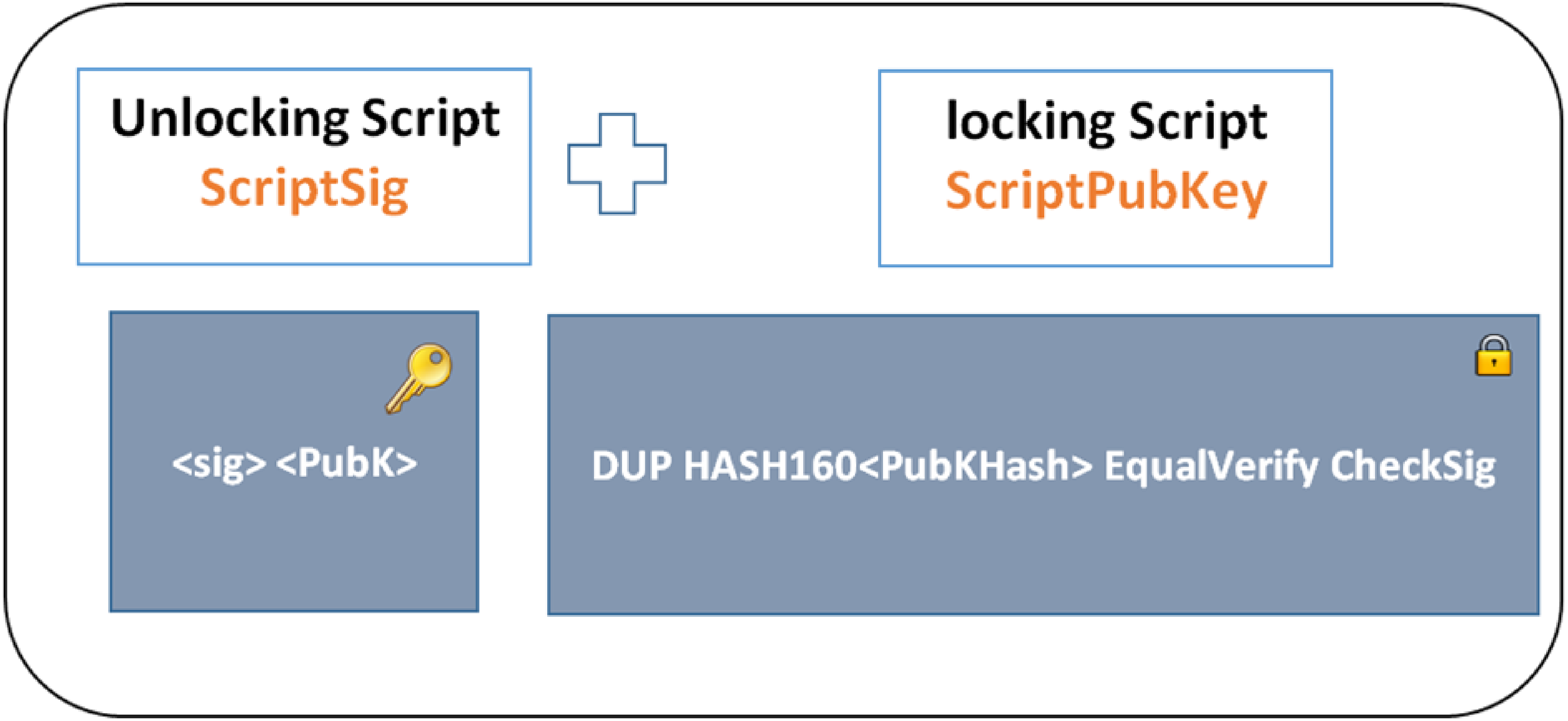
Step 5) Receiver will compare Digest 1 & 2. If both are the same, then Sender's Digital Signature is valid

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

U (UnSpent) vs S (Spent) TXO



✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)



Unlocking Script

ScriptSig

locking Script

ScriptPubKey

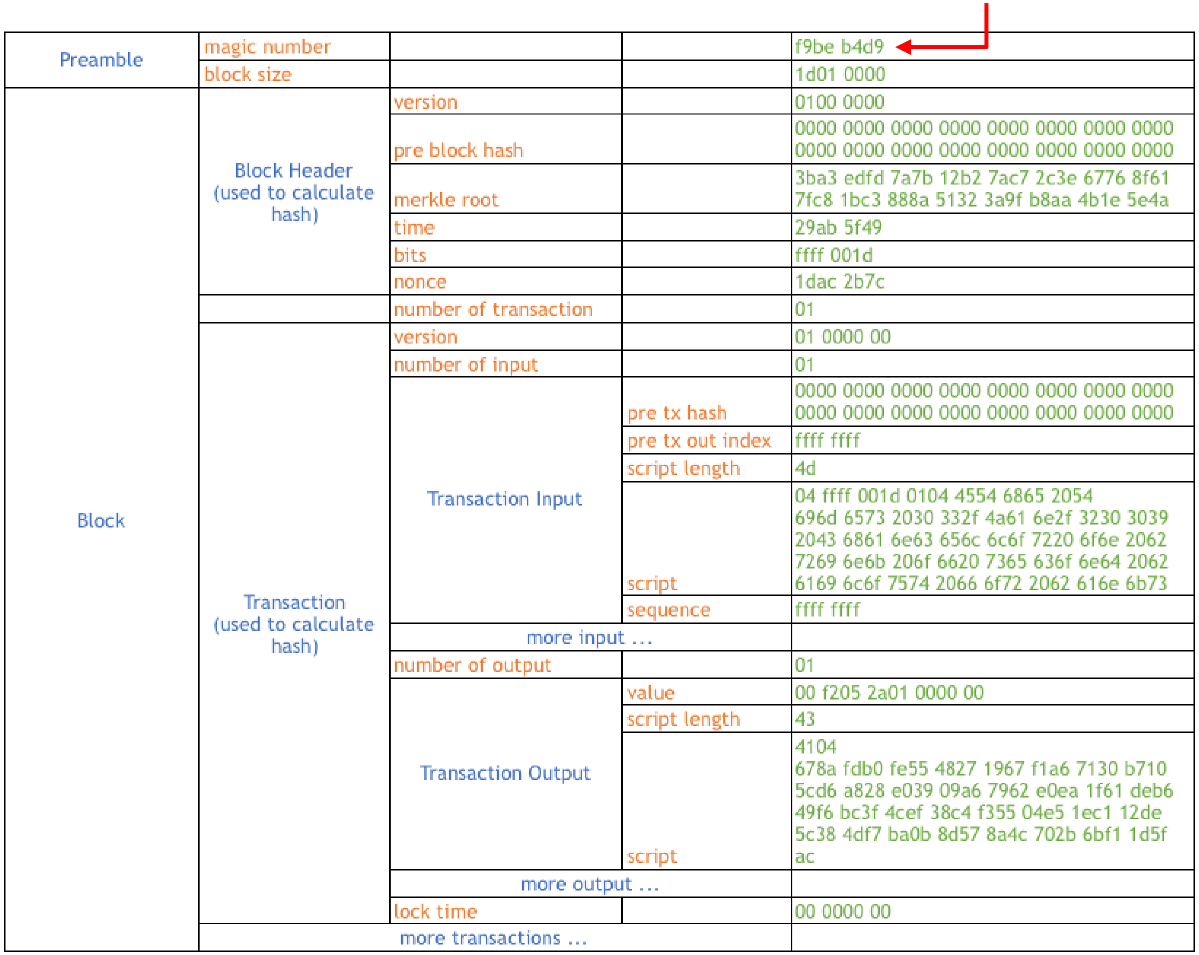
<sig> <PubK>

DUP HASH160<PubKHash> EqualVerify CheckSig

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Bitcoin Genesis Block

Start of a new block



Preamble	magic number			f9be b4d9
	block size			1d01 0000
Block	Block Header (used to calculate hash)	version		0100 0000
		pre block hash		0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
		merkle root		3ba3 edfd 7a7b 12b2 7ac7 2c3e 6776 8f61 7fc8 1bc3 888a 5132 3a9f b8aa 4b1e 5e4a
		time		29ab 5f49
		bits		ffff 001d
		nonce		1dac 2b7c
		number of transaction		01
	Transaction (used to calculate hash)	version		01 0000 00
		number of input		01
		Transaction Input	pre tx hash	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
			pre tx out index	ffff ffff
			script length	4d
			script	04 ffff 001d 0104 4554 6865 2054 696d 6573 2030 332f 4a61 6e2f 3230 3039 2043 6861 6e63 656c 6c6f 7220 6f6e 2062 7269 6e6b 206f 6620 7365 636f 6e64 2062 6169 6c6f 7574 2066 6f72 2062 616e 6b73
			sequence	ffff ffff
		more input …		
		number of output		01
		Transaction Output	value	00 f205 2a01 0000 00
			script length	43
			script	4104 678a fdb0 fe55 4827 1967 f1a6 7130 b710 5cd6 a828 e039 09a6 7962 e0ea 1f61 deb6 49f6 bc3f 4cef 38c4 f355 04e5 1ec1 12de 5c38 4df7 ba0b 8d57 8a4c 702b 6bf1 1d5f ac
		more output …		
		lock time		00 0000 00
	more transactions …			

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

api.blockchair.com/bitcoin/raw/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

```
{
    "data": {
        "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f": {
            "raw_block":
   "0100000000000000000000000000000000000000000000000000000000000000000000003ba3edfd7a7b12b27ac72c3
   e67768f617fc81bc3888a51323a9fb8aa4b1e5e4a29ab5f49ffff001d1dac2b7c0101000000010000000000000000000
   000000000000000000000000000000000000000000000ffffffff4d04ffff001d0104455468652054696d65732030332
   f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f7574206
   66f722062616e6b73ffffffff0100f2052a01000000434104678afdb0fe5548271967f1a67130b7105cd6a828e03909a
   67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac00000000",
            "decoded_raw_block": {
                "hash": "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
                "confirmations": 810130,
                "height": 0,
                "version": 1,
                "versionHex": "00000001",
                "merkleroot": "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
                "time": 1231006505,
                "mediantime": 1231006505,
                "nonce": 2083236893,
                "bits": "1d00ffff",
...
```

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Raw Block Data for Genesis Block

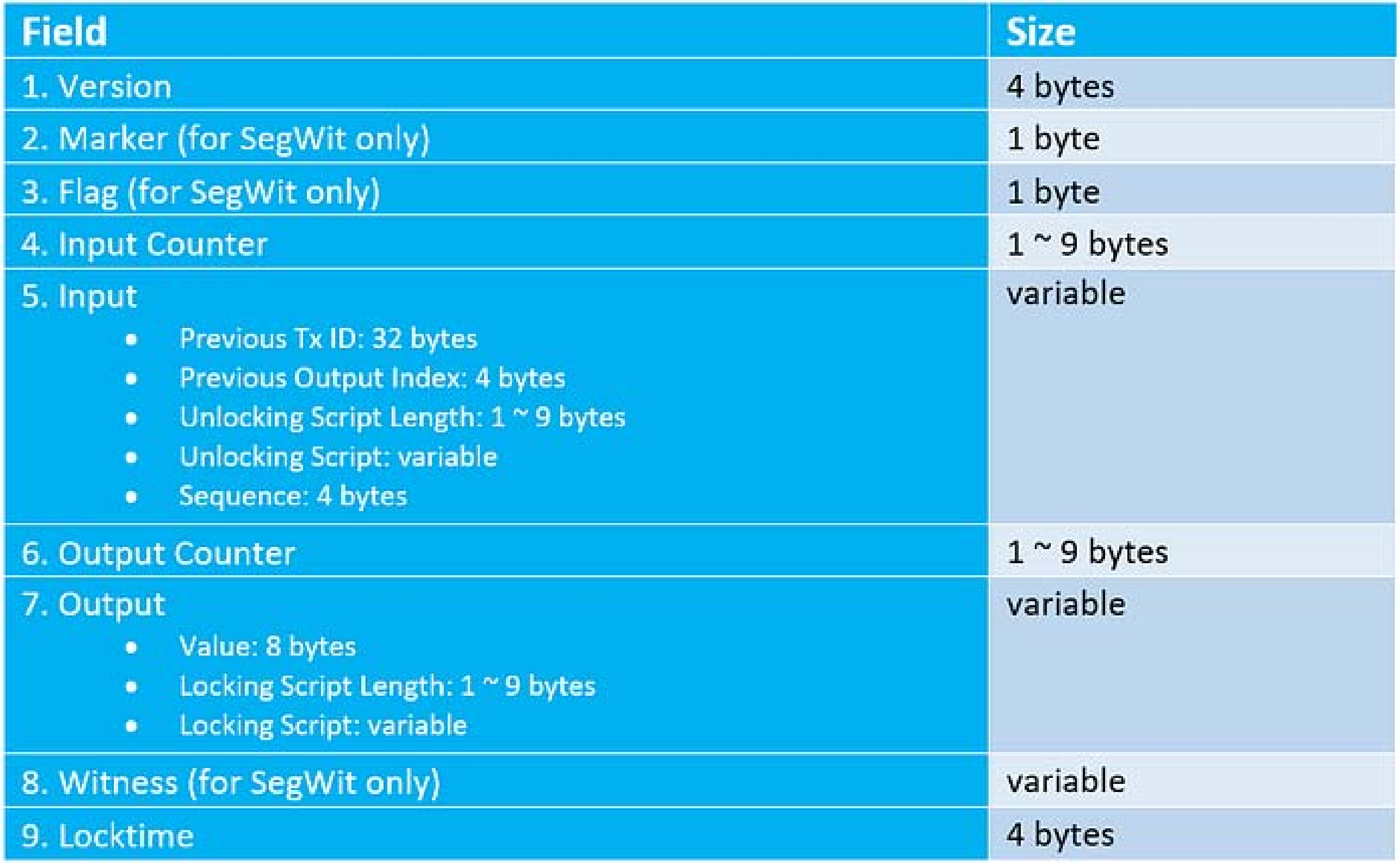
```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.E.A??Q2:?¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iyy...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......yyyyM.yy..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksyyyy..o.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.g?y°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gn|q0·.\O¨(a9.|
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybae.aÞ¶Io¼?Li8A
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   oU.a.A.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ?Lp+kn._¬....
```

Block Header and Transaction

```
01000000 : version
0000000000000000000000000000000000000000000000000000000000000000 : prev block
3BA3EDFD7A7B12B27AC72C3E67768F617FC81BC3888A51323A9FB8AA4B1E5E4A : merkle root
29AB5F49 : timestamp
FFFF001D : bits
1DAC2B7C : nonce
01 : number of transactions
01000000 : version
01 : input
0000000000000000000000000000000000000000000000000000000000000000FFFFFFFF : prev output
4D : script length
04FFFF001D0104455468652054696D65732030332F4A616E2F32303039204368616E63656C6C6F72206F6E206272696
   E6B206F66207365636F6E64206261696C6F757420666F722062616E6B73 : scriptSig
FFFFFFFF : sequence
01 : outputs
00F2052A01000000 : 50 BTC
43 : pk_script length
4104678AFDB0FE5548271967F1A67130B7105CD6A828E03909A67962E0EA1F61DEB649F6BC3F4CEF38C4F35504E51EC
   112DE5C384DF7BA0B8D578A4C702B6BF11D5FAC : pk_script
00000000 : lock time
```

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Transaction Format

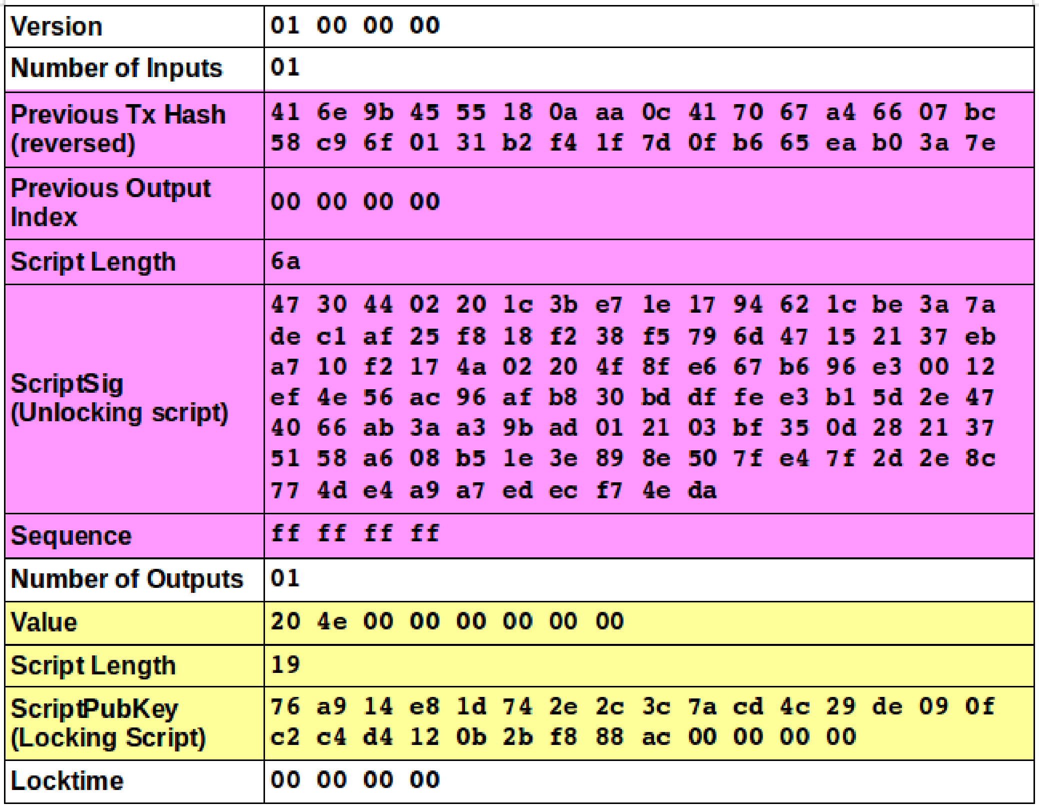


Field	Size
1. Version	4 bytes
2. Marker (for SegWit only)	1 byte
3. Flag (for SegWit only)	1 byte
4. Input Counter	1 ~ 9 bytes
5. Input • Previous Tx ID: 32 bytes • Previous Output Index: 4 bytes • Unlocking Script Length: 1 ~ 9 bytes • Unlocking Script: variable • Sequence: 4 bytes	variable
6. Output Counter	1 ~ 9 bytes
7. Output • Value: 8 bytes • Locking Script Length: 1 ~ 9 bytes • Locking Script: variable	variable
8. Witness (for SegWit only)	variable
9. Locktime	4 bytes

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

- 0100000001416e9b4555180aaa0c417067a46607bc58c96f0131b2f41f7d0fb665eab03a7e000000006a47304402201c3be71e1794621cbe3a7adec1af25f818f238f5796d47152137eba710f2174a02204f8fe667b696e30012ef4e56ac96afb830bddffee3b15d2e474066ab3aa39bad012103bf350d2821375158a608b51e3e898e507fe47f2d2e8c774de4a9a7edecf74edaffffffff01204e000000000000001976a914e81d742e2c3c7acd4c29de090fc2c4d4120b2bf888ac00000000

P2PKH (Pay-To-Public-Key-Hash) Transaction



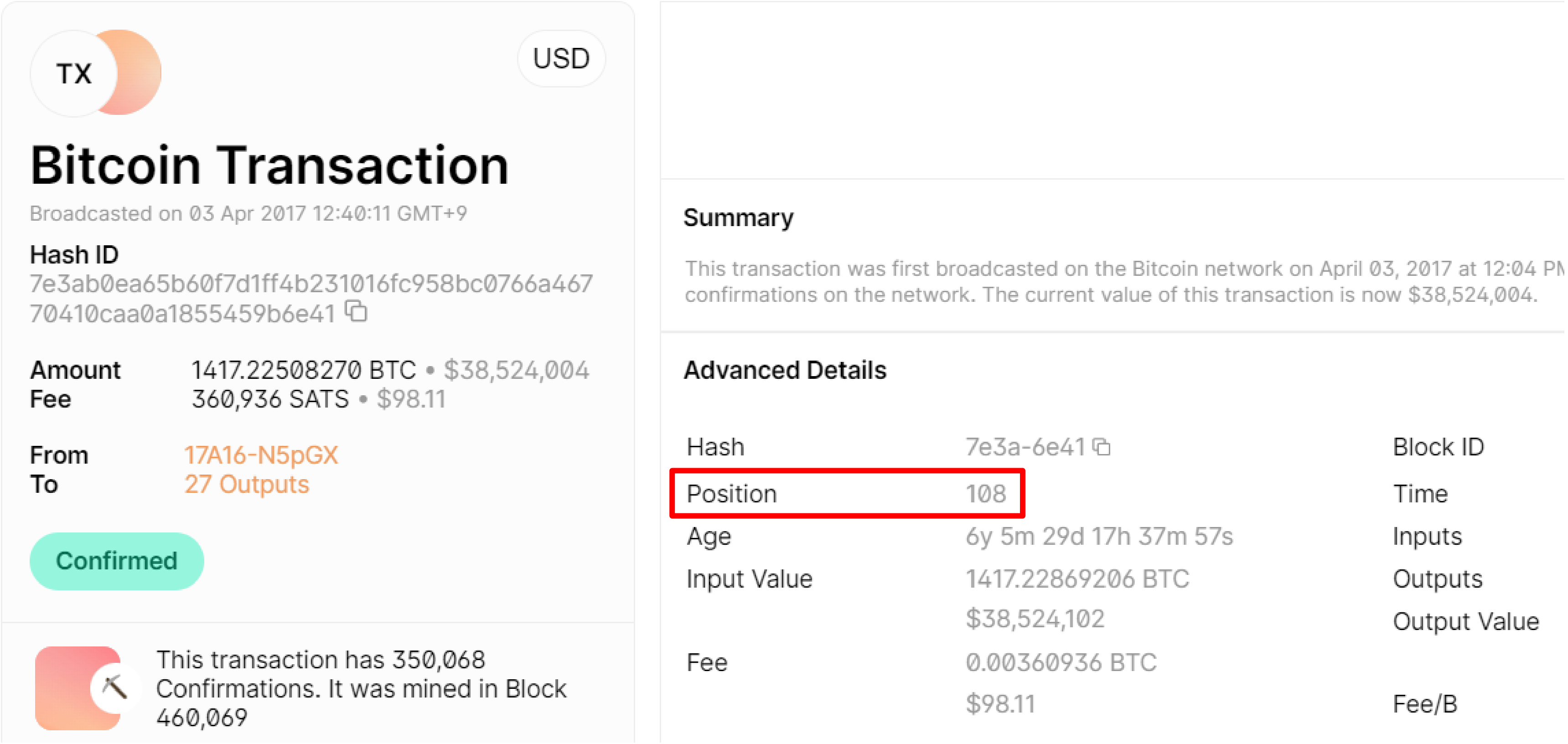
Version	01 00 00 00
Number of Inputs	01
Previous Tx Hash (reversed)	41 6e 9b 45 55 18 0a aa 0c 41 70 67 a4 66 07 bc 58 c9 6f 01 31 b2 f4 1f 7d 0f b6 65 ea b0 3a 7e
Previous Output Index	00 00 00 00
Script Length	6a
ScriptSig (Unlocking script)	47 30 44 02 20 1c 3b e7 1e 17 94 62 1c be 3a 7a de c1 af 25 f8 18 f2 38 f5 79 6d 47 15 21 37 eb a7 10 f2 17 4a 02 20 4f 8f e6 67 b6 96 e3 00 12 ef 4e 56 ac 96 af b8 30 bd df fe e3 b1 5d 2e 47 40 66 ab 3a a3 9b ad 01 21 03 bf 35 0d 28 21 37 51 58 a6 08 b5 1e 3e 89 8e 50 7f e4 7f 2d 2e 8c 77 4d e4 a9 a7 ed ec f7 4e da
Sequence	ff ff ff ff
Number of Outputs	01
Value	20 4e 00 00 00 00 00 00
Script Length	19
ScriptPubKey (Locking Script)	76 a9 14 e8 1d 74 2e 2c 3c 7a cd 4c 29 de 09 0f c2 c4 d4 12 0b 2b f8 88 ac 00 00 00 00
Locktime	00 00 00 00

Magenta: Input Segment

Yellow: Output Segment

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

https://www.blockchain.com/explorer/transactions/btc/7e3ab0ea65b60f7d1ff4b231016fc958bc0766a46770410caa0a1855459b6e41



TX

USD

Bitcoin Transaction

Broadcasted on 03 Apr 2017 12:40:11 GMT+9

Hash ID
7e3ab0ea65b60f7d1ff4b231016fc958bc0766a46770410caa0a1855459b6e41

Amount	1417.22508270 BTC • $38,524,004
Fee	360,936 SATS • $98.11
From	17A16-N5pGX
To	27 Outputs

Confirmed

This transaction has 350,068 Confirmations. It was mined in Block 460,069

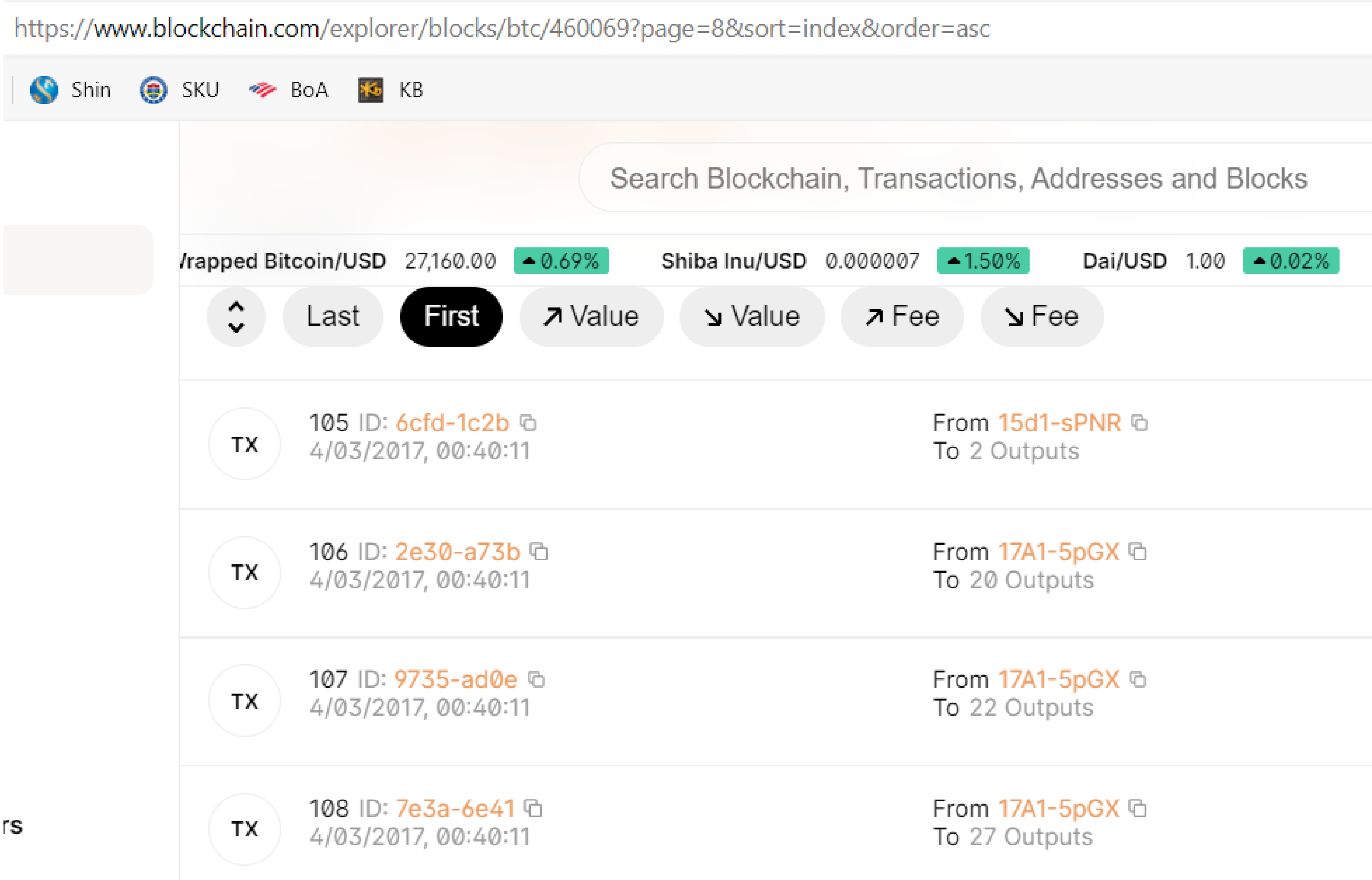
Summary

This transaction was first broadcasted on the Bitcoin network on April 03, 2017 at 12:04 PM
confirmations on the network. The current value of this transaction is now $38,524,004.

Advanced Details

Hash	7e3a-6e41	Block ID
Position	108	Time
Age	6y 5m 29d 17h 37m 57s	Inputs
Input Value	1417.22869206 BTC	Outputs
	$38,524,102	Output Value
Fee	0.00360936 BTC	
	$98.11	Fee/B

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**



https://www.blockchain.com/explorer/blocks/btc/460069?page=8&sort=index&order=asc

/rapped Bitcoin/USD 27,160.00 ▲0.69%   Shiba Inu/USD 0.000007 ▲1.50%   Dai/USD 1.00 ▲0.02%

TX 105 ID: 6cfd-1c2b 4/03/2017, 00:40:11 From 15d1-sPNR To 2 Outputs

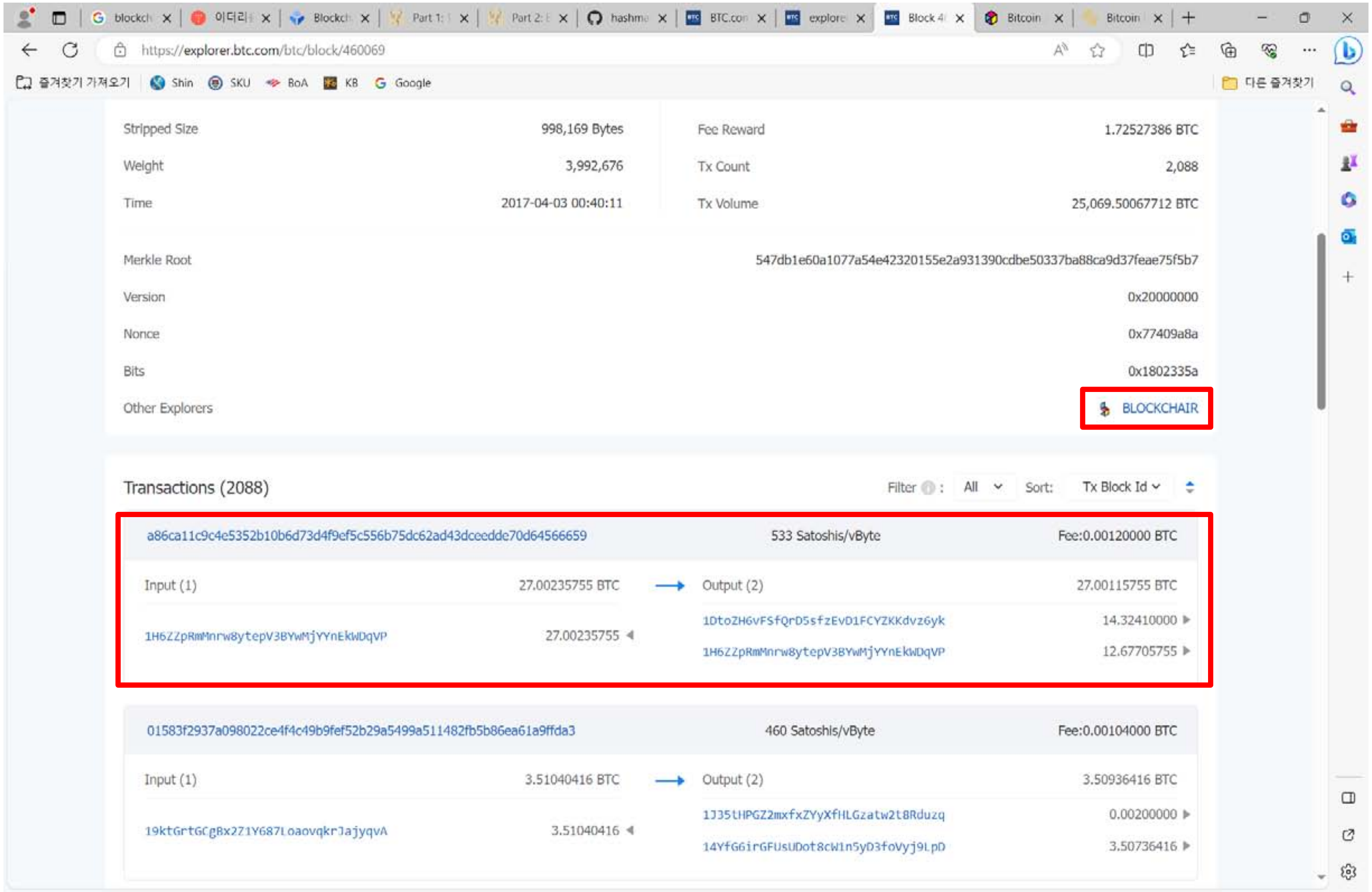
TX 106 ID: 2e30-a73b 4/03/2017, 00:40:11 From 17A1-5pGX To 20 Outputs

TX 107 ID: 9735-ad0e 4/03/2017, 00:40:11 From 17A1-5pGX To 22 Outputs

TX 108 ID: 7e3a-6e41 4/03/2017, 00:40:11 From 17A1-5pGX To 27 Outputs

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

https://explorer.btc.com/btc/



Stripped Size	998,169 Bytes	Fee Reward	1.72527386 BTC
Weight	3,992,676	Tx Count	2,088
Time	2017-04-03 00:40:11	Tx Volume	25,069.50067712 BTC

Merkle Root	547db1e60a1077a54e42320155e2a931390cdbe50337ba88ca9d37feae75f5b7
Version	0x20000000
Nonce	0x77409a8a
Bits	0x1802335a
Other Explorers	BLOCKCHAIR

Transactions (2088)

a86ca11c9c4e5352b10b6d73d4f9ef5c556b75dc62ad43dceedde70d64566659 533 Satoshis/vByte Fee:0.00120000 BTC

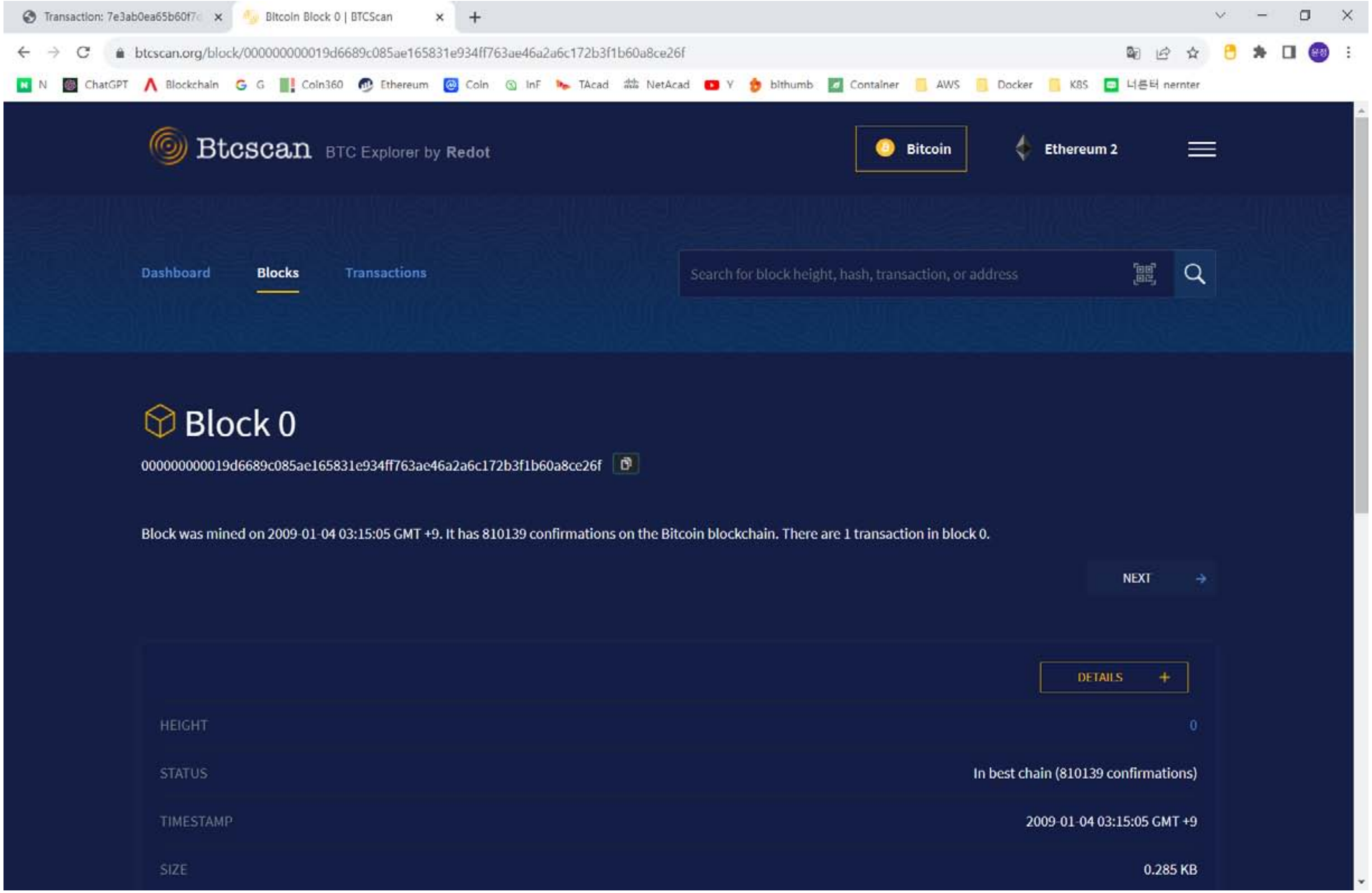
Input (1)	27.00235755 BTC	→	Output (2)	27.00115755 BTC
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	27.00235755 ◀		1DtoZH6vFSfQrD5sfzEvD1FCYZKKdvz6yk	14.32410000 ▶
			1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	12.67705755 ▶

01583f2937a098022ce4f4c49b9fef52b29a5499a511482fb5b86ea61a9ffda3 460 Satoshis/vByte Fee:0.00104000 BTC

Input (1)	3.51040416 BTC	→	Output (2)	3.50936416 BTC
19ktGrtGCgBx2Z1Y687LoaovqkrJajyqvA	3.51040416 ◀		1J35tHPGZ2mxfxZYyXfHLGzatw2t8Rduzq	0.00200000 ▶
			14YfG6irGFUsUDot8cW1n5yD3foVyj9LpD	3.50736416 ▶

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

https://btcscan.org/


Transaction: 7e3ab0ea65b60f7c
Bitcoin Block 0 | BTCScan
btcscan.org/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
N
ChatGPT
Blockchain
G
Coin360
Ethereum
Coin
InF
TAcad
NetAcad
Y
bithumb
Container
AWS
Docker
K8S
너른터 nernter
Btcscan
BTC Explorer by Redot
Bitcoin
Ethereum 2
Dashboard
Blocks
Transactions
Search for block height, hash, transaction, or address
NEXT →
DETAILS +

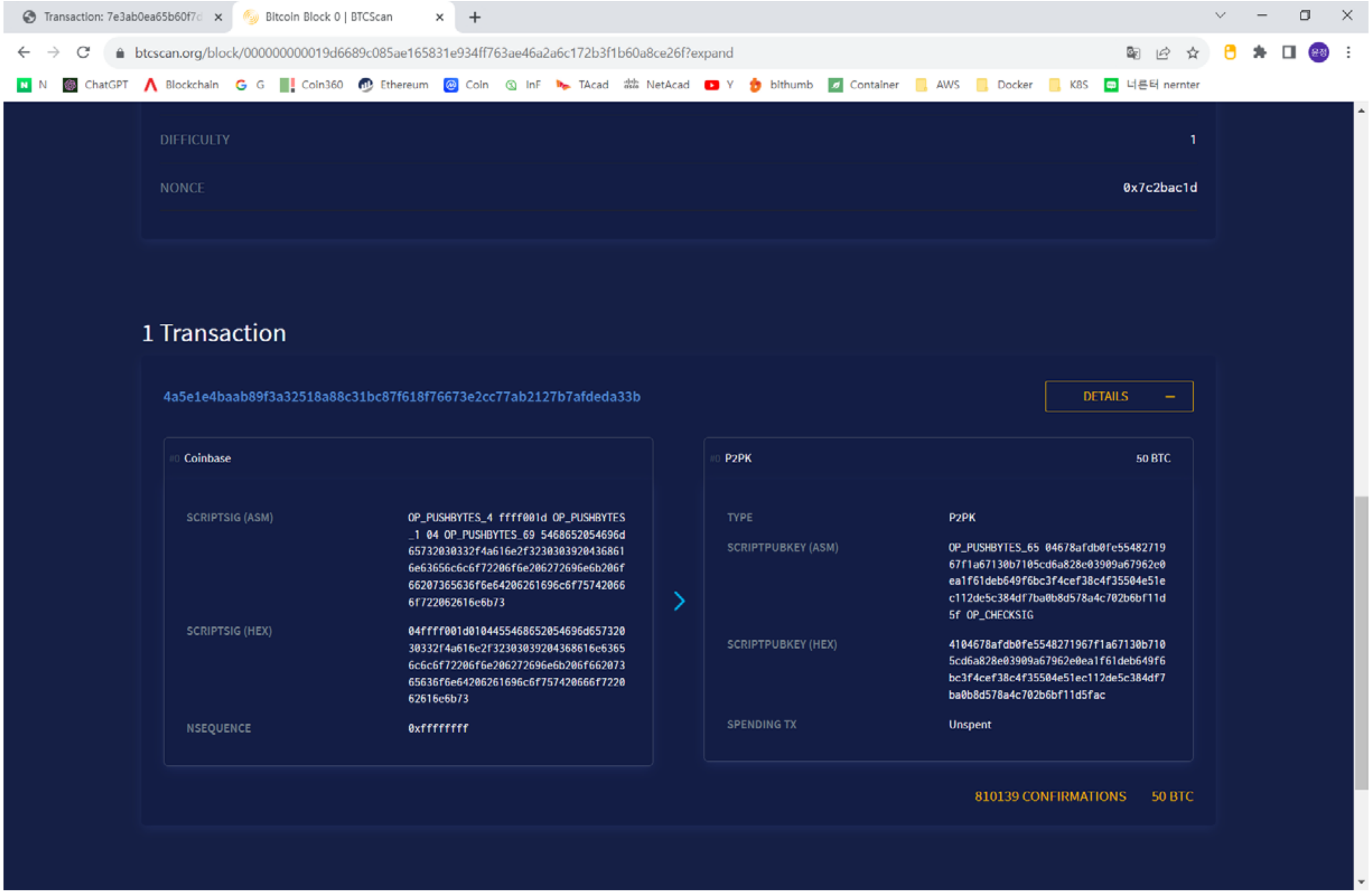
Block 0

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Block was mined on 2009-01-04 03:15:05 GMT +9. It has 810139 confirmations on the Bitcoin blockchain. There are 1 transaction in block 0.

HEIGHT	0
STATUS	In best chain (810139 confirmations)
TIMESTAMP	2009-01-04 03:15:05 GMT +9
SIZE	0.285 KB

✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)



Transaction: 7e3ab0ea65b60f7c
Bitcoin Block 0 | BTCScan
btcscan.org/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f?expand
N
ChatGPT
Blockchain
G
Coin360
Ethereum
Coin
InF
TAcad
NetAcad
Y
bithumb
Container
AWS
Docker
K8S
너른터 nernter

DIFFICULTY 1

NONCE 0x7c2bac1d

1 Transaction

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

#0 Coinbase

SCRIPTSIG (ASM)	OP_PUSHBYTES_4 ffff001d OP_PUSHBYTES_1 04 OP_PUSHBYTES_69 5468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73
SCRIPTSIG (HEX)	04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73
NSEQUENCE	0xffffffff

#0 P2PK 50 BTC

TYPE	P2PK
SCRIPTPUBKEY (ASM)	OP_PUSHBYTES_65 04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG
SCRIPTPUBKEY (HEX)	4104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac
SPENDING TX	Unspent

810139 CONFIRMATIONS 50 BTC

✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**