

Ecclesiastes (Eccl) 12:13

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

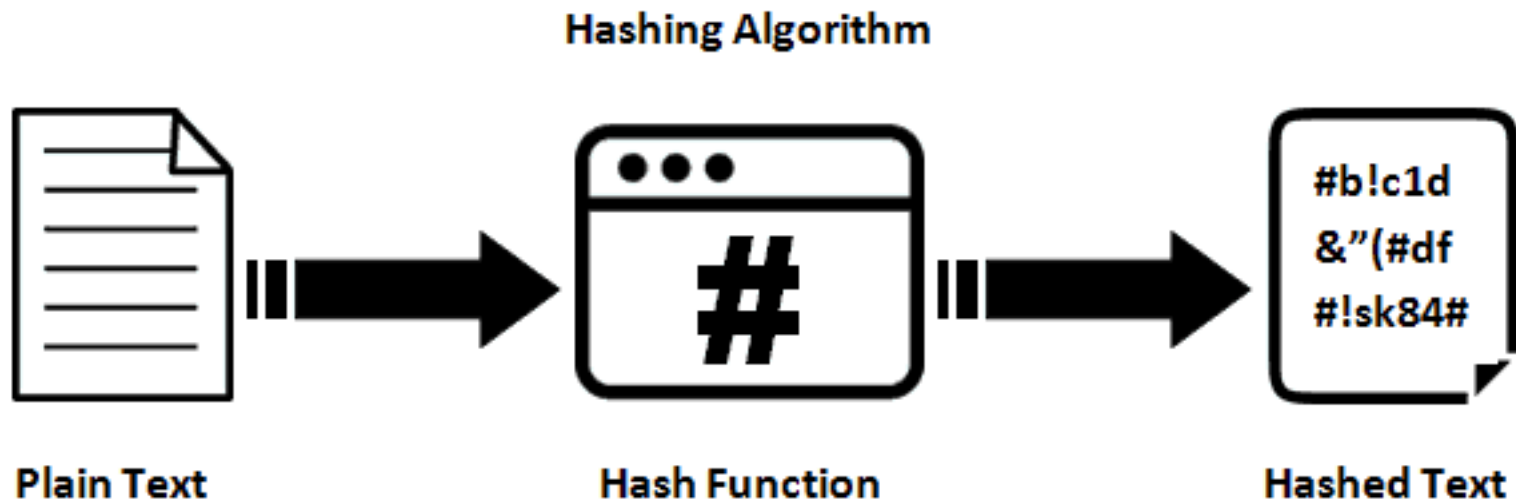
**Have reverence for God, and obey his commands,
because this is all that man was created for.**

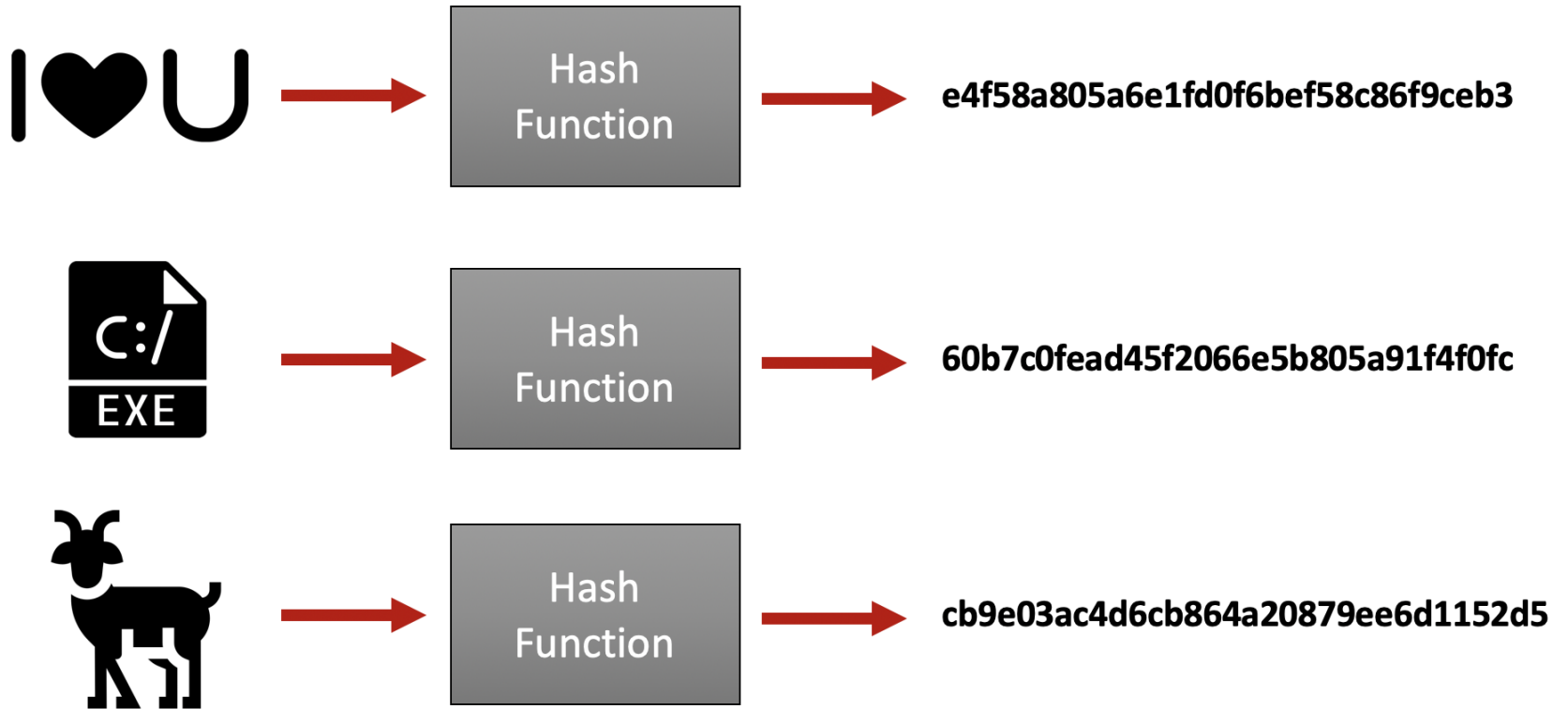
**Fear God and keep his commandments,
for this is the whole duty of man.**



Block and Chain ?

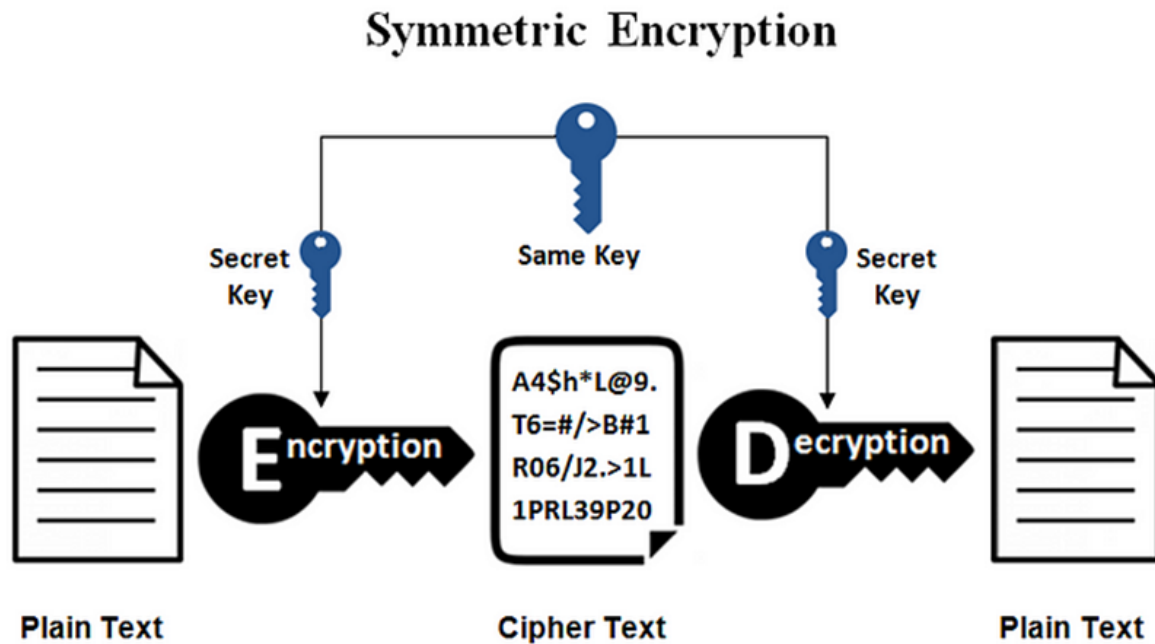
Hash Function



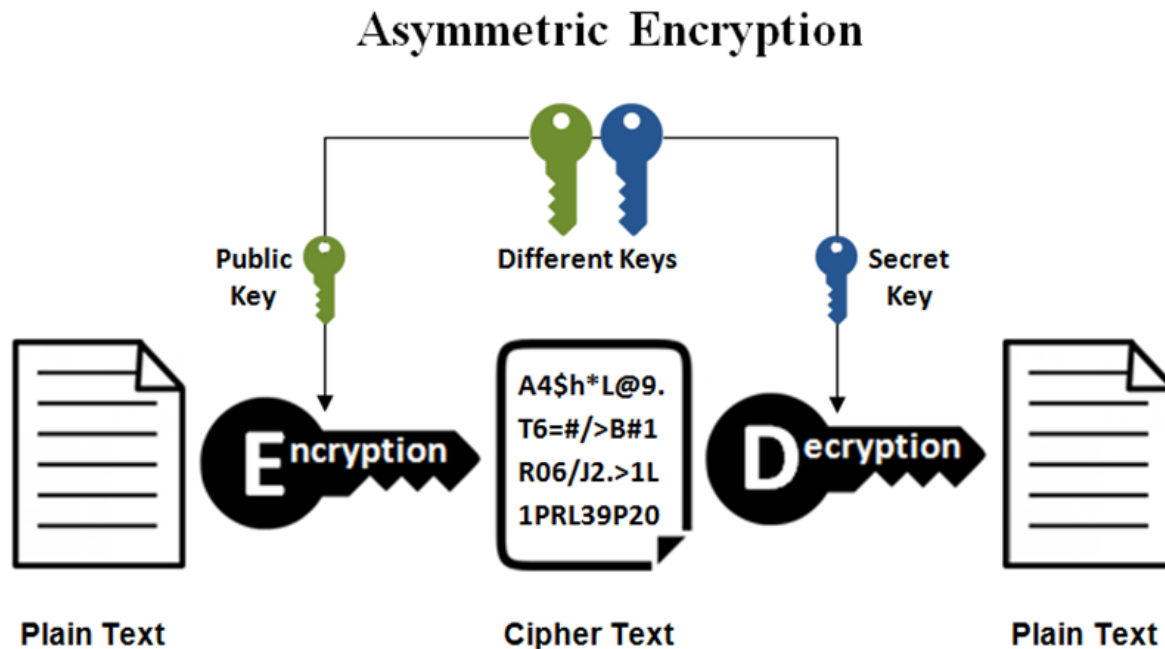


† Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

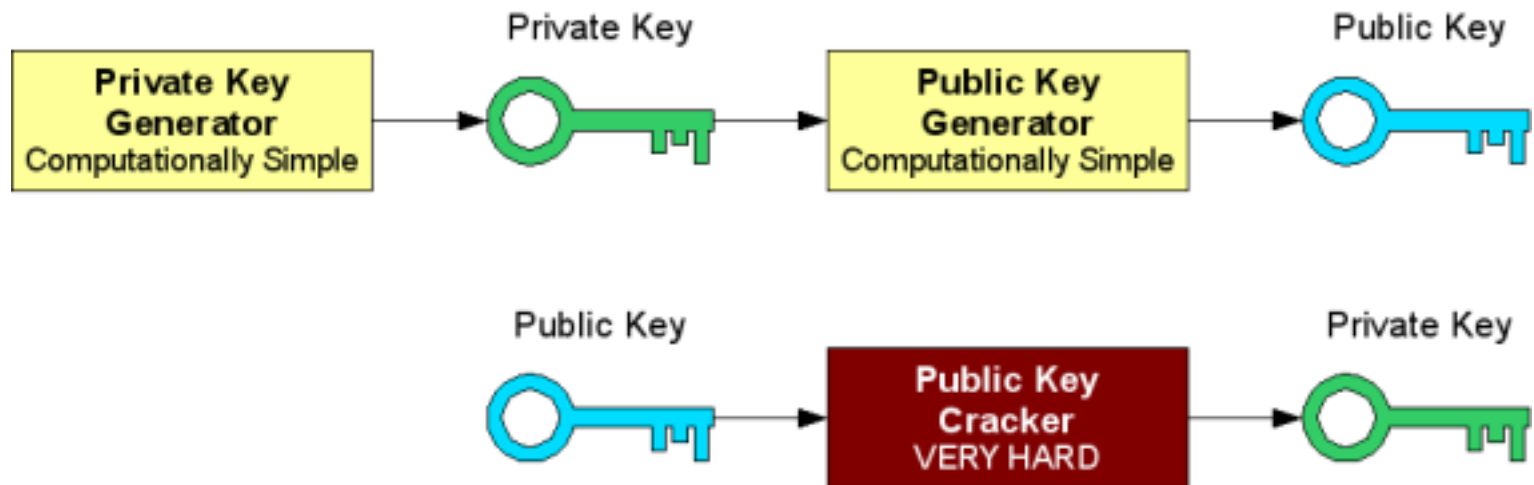
Symmetric Key Cryptography



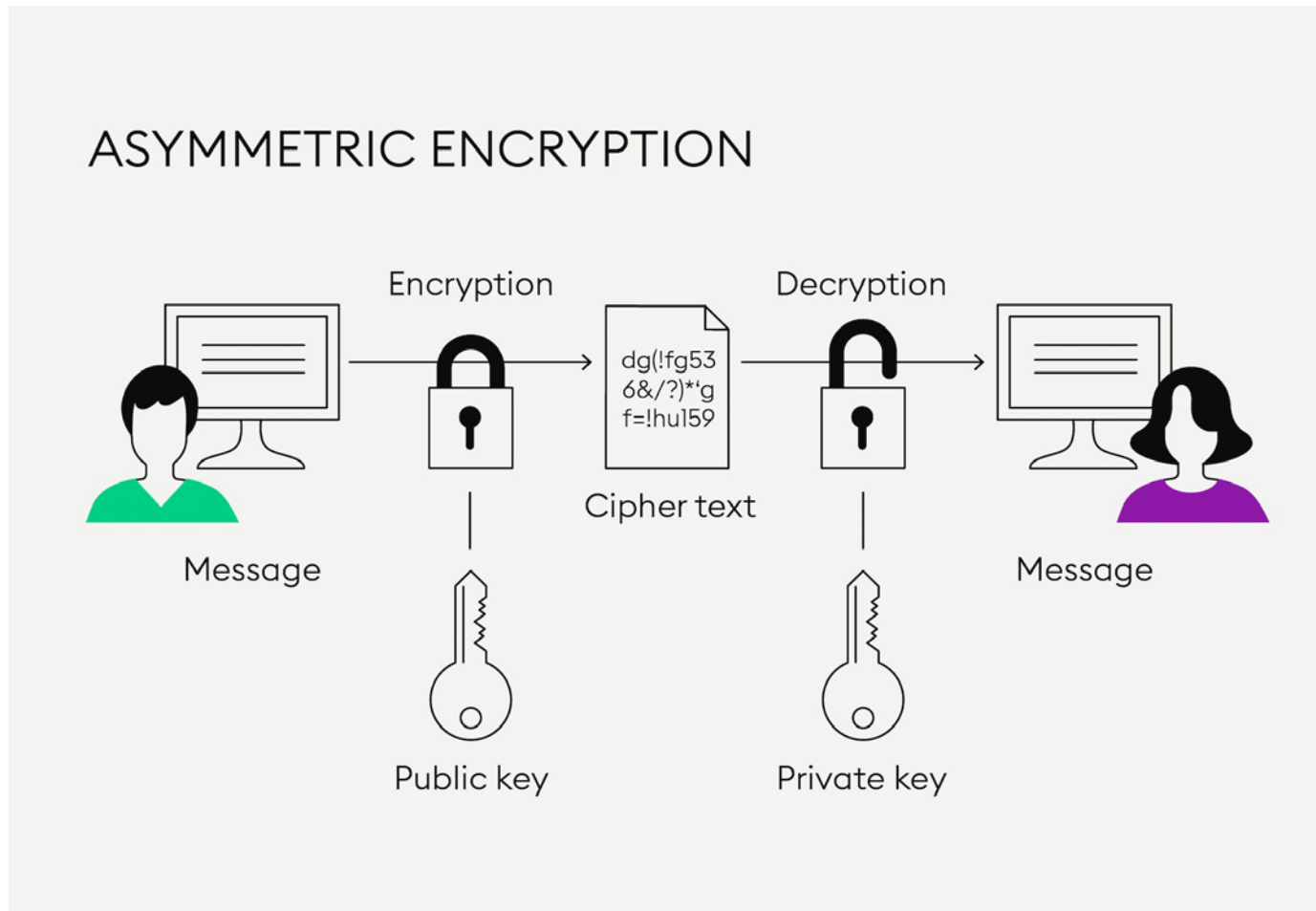
Asymmetric (Public) Key Cryptography



Private Key vs Public Key

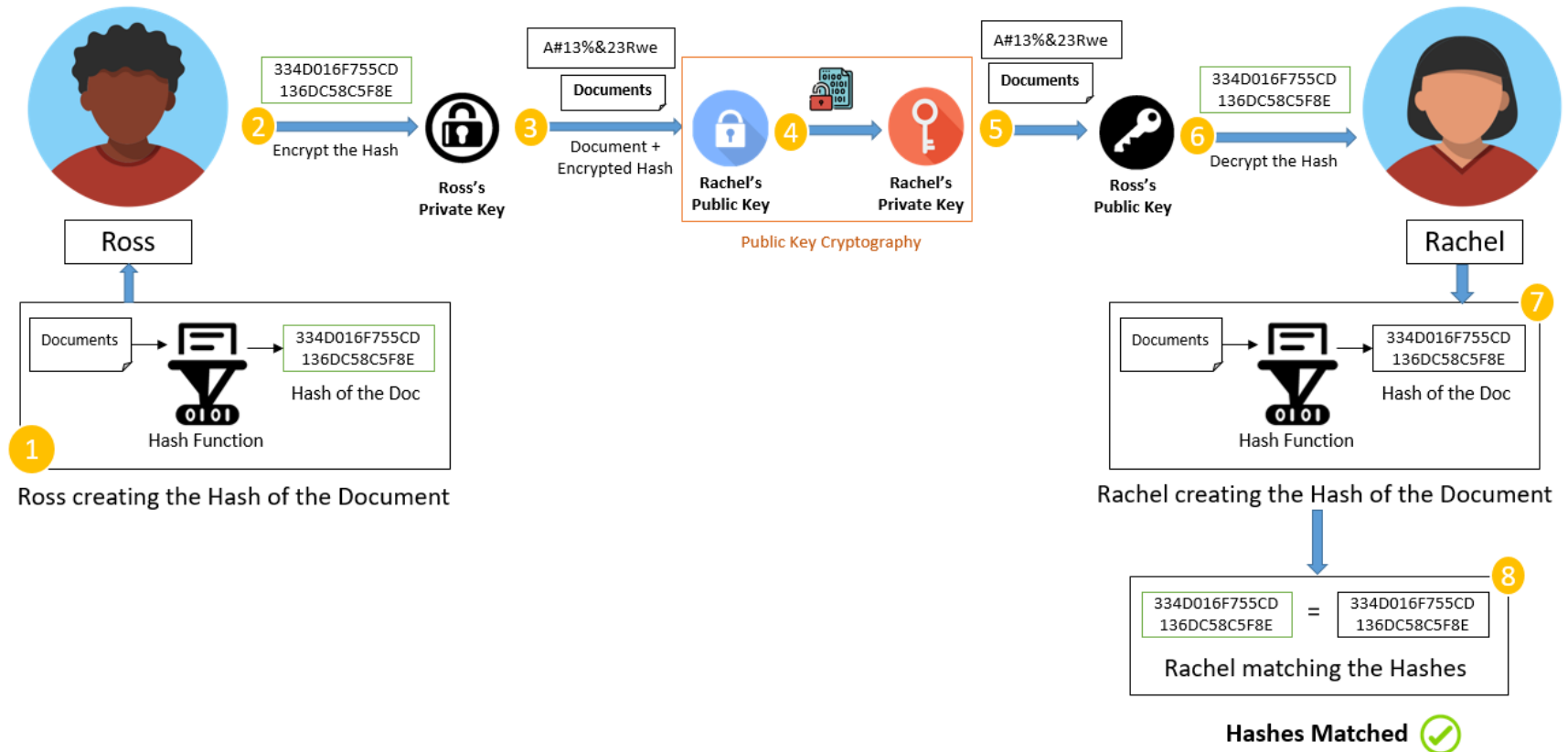


How to Share a Key in Symmetric Cryptography



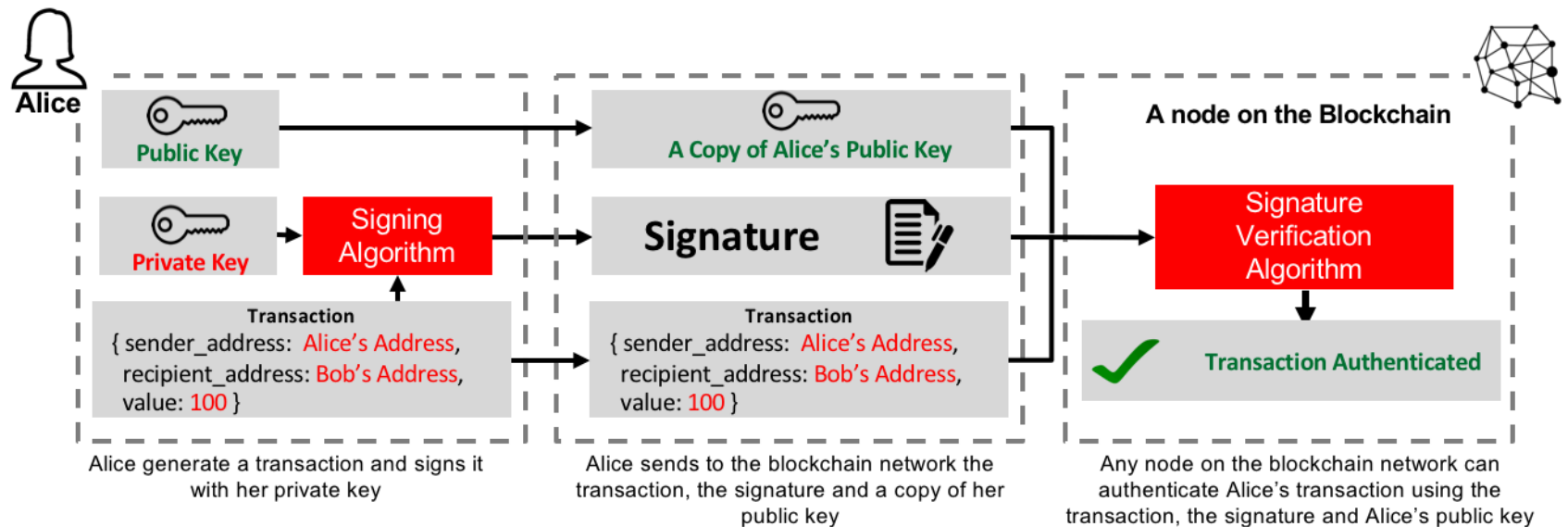
† Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Digital Signature



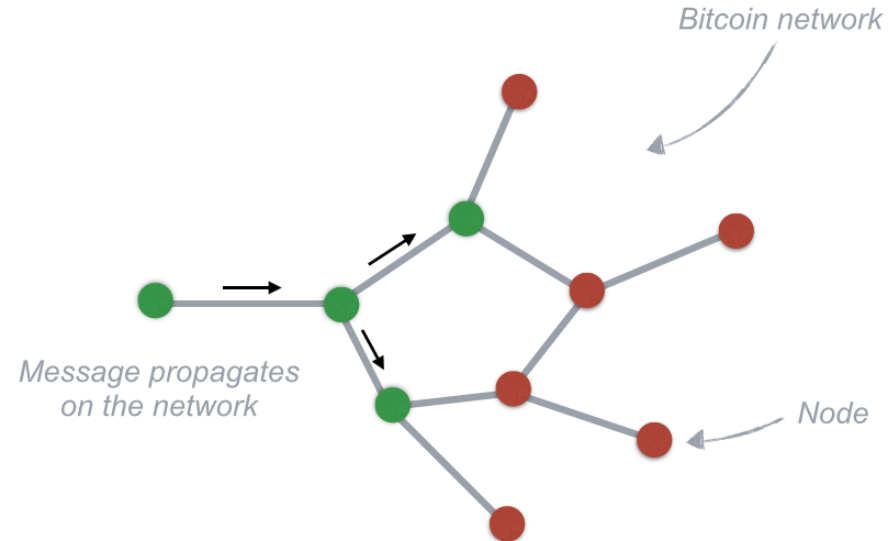
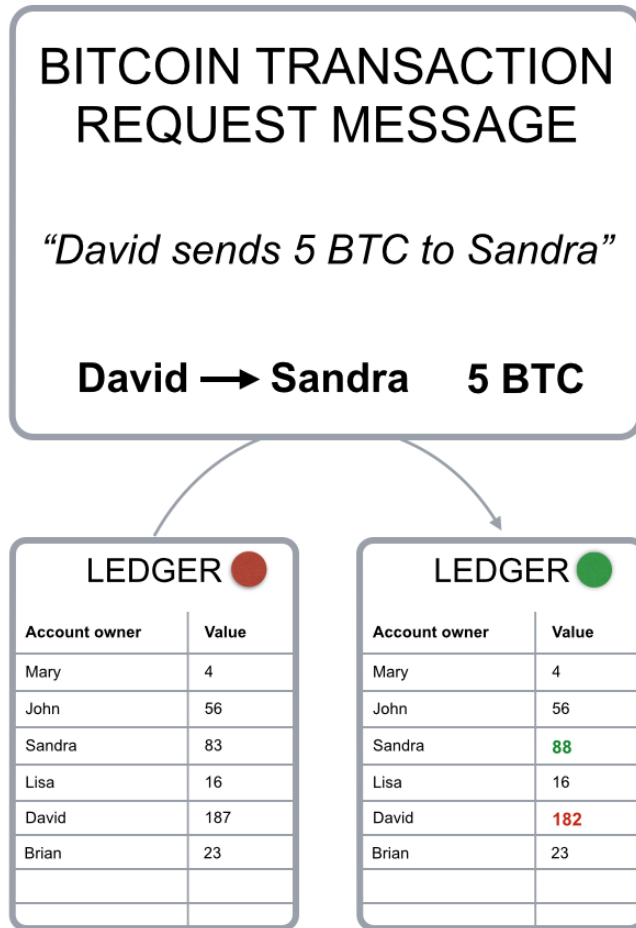
† Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Bitcoin Transaction



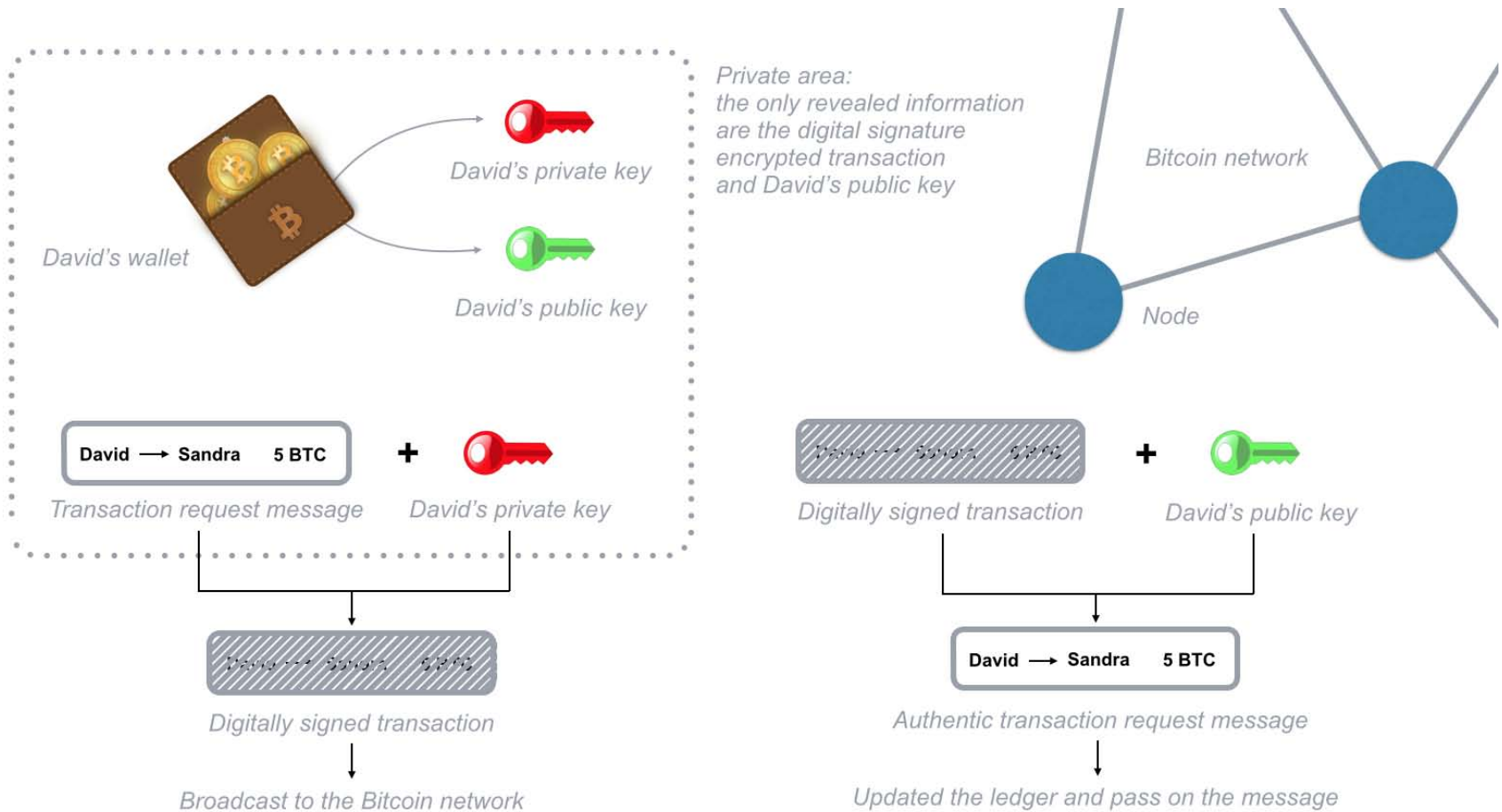
Authentication Process for Transactions on the Blockchain

Ledger



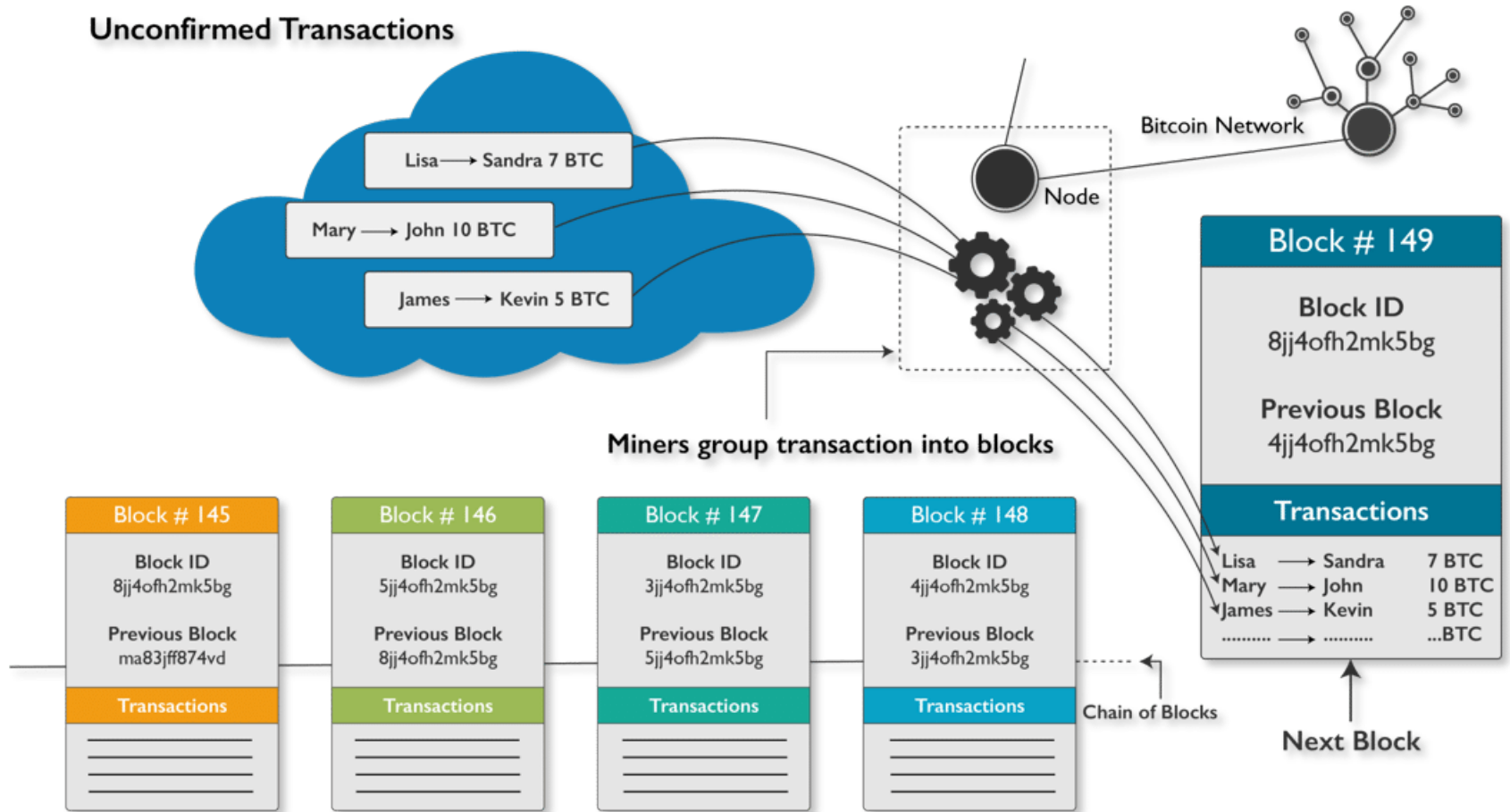
Each *node* receives the transaction request message, updates its own copy of the *ledger* and passes on the message to the nearby *nodes*.

Wallet and Transaction (Tx)

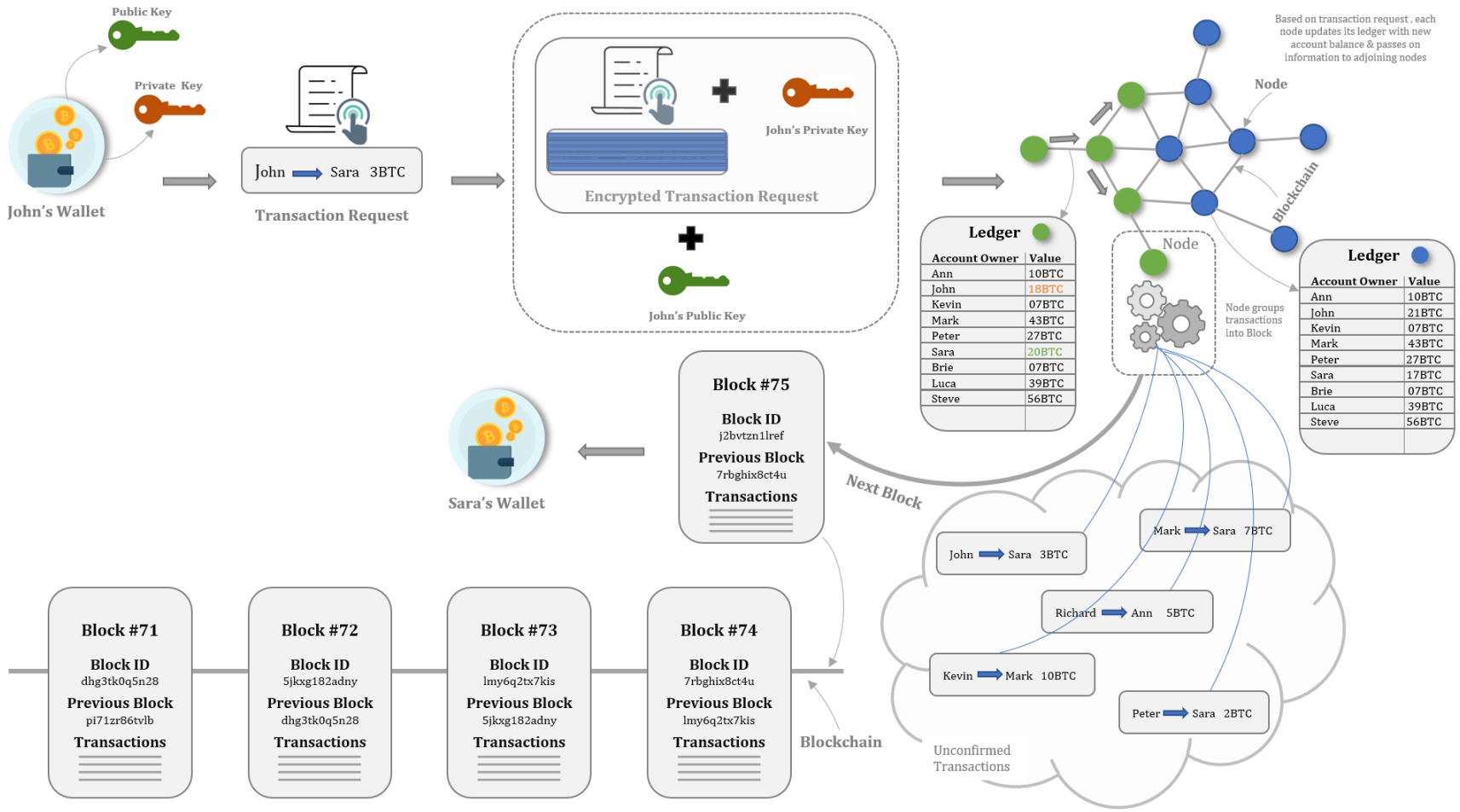


† Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Unconfirmed Txs and Block



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

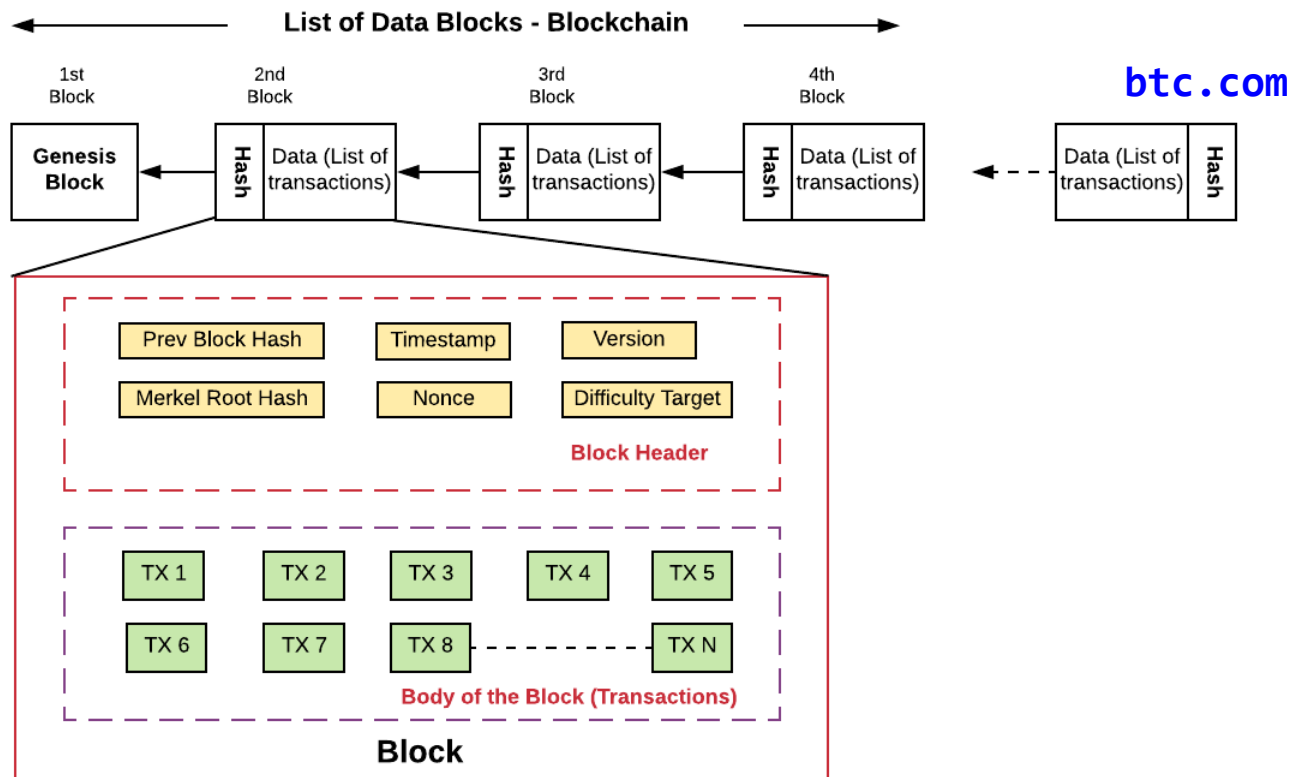


† Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

<https://andersbrownworth.com/blockchain/>

- Block
- Blockchain

Genesis Block and Blockchain





† 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://www.blockchain.com/explorer>

Details

Hash	000000-ce26f 	Depth	809,428
Capacity	0.03%	Size	285
Distance	14y 8m 21d 18h 16m 28s	Version	0×1
BTC	0.0000	Merkle Root	4a-3b 
Value	\$0.00	Difficulty	1.00
Value Today	\$0.00	Nonce	2,083,236,893
Average Value	0.000000000000 BTC	Bits	486,604,799
Median Value	50.0000000000 BTC	Weight	1,140 WU
Input Value	0.00 BTC	Minted	50.00 BTC
Output Value	50.00 BTC	Reward	50.0000000000 BTC
Transactions	1	Mined on	Jan 04, 2009, 3:15:05 AM
Witness Tx's	0	Height	0
Inputs	1	Confirmations	809,428
Outputs	1	Fee Range	0-0 sat/vByte
Fees	0.0000000000 BTC	Average Fee	0.0000000000
Fees Kb	0.00000000 BTC	Median Fee	0.0000000000
Fees kWU	0.00000000 BTC	Miner	Satoshi

† 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](https://blockchain.info/rawblock/$block_hash)

- `Hash(block0) = 00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`
- `blockchain.info/rawblock/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`

```

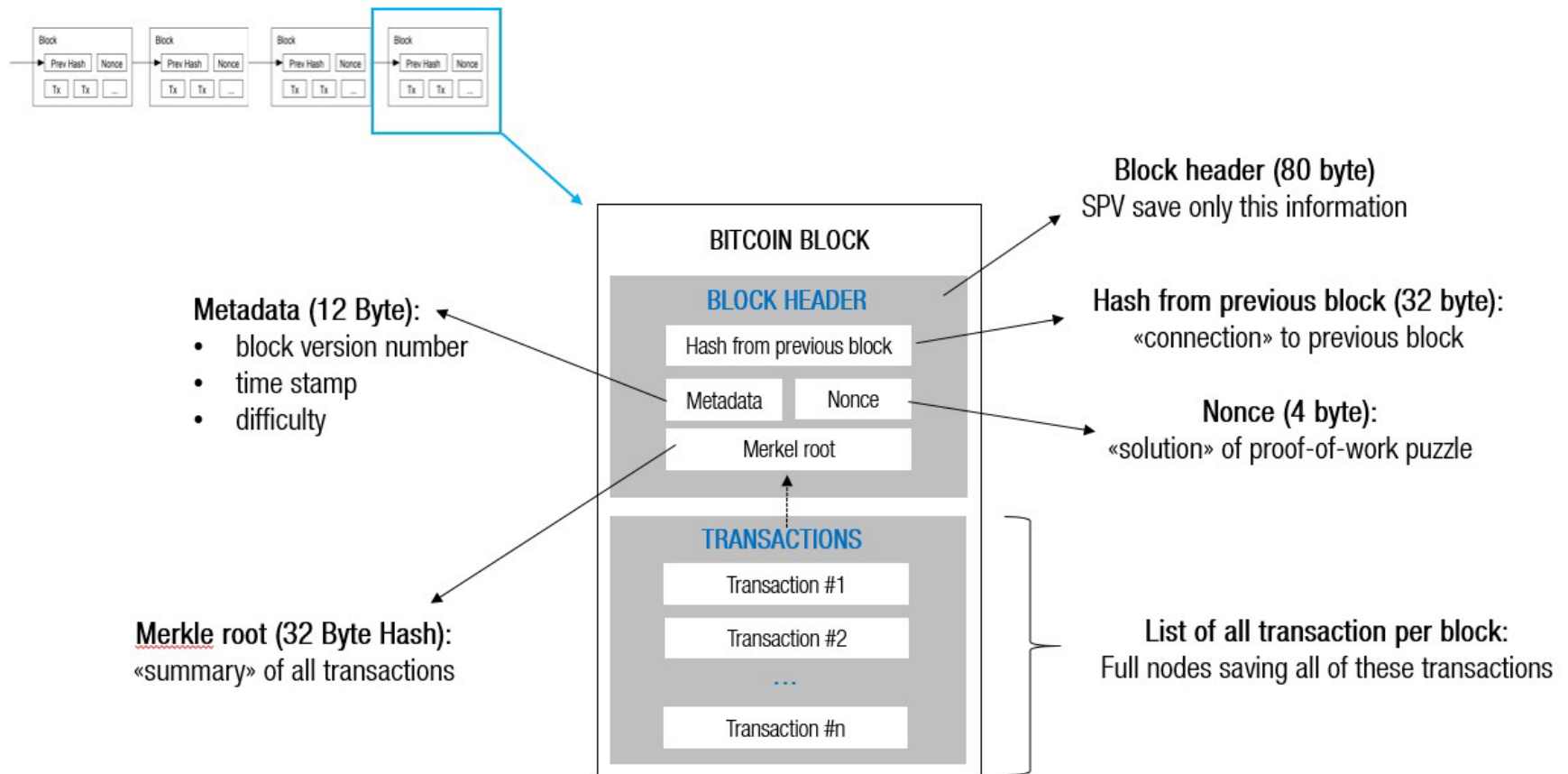
{
  "hash": "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
  "ver": 1,
  "prev_block": "0000000000000000000000000000000000000000000000000000000000000000",
  "mrkl_root": "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
  "time": 1231006505,
  "bits": 486604799,
  "next_block": [
    "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048"
  ],
  "fee": 0,
  "nonce": 2083236893,
  "n_tx": 1,
  "size": 285,
  "block_index": 0,
  "main_chain": true,
  "height": 0,
  "weight": 1140,
  "tx": [
    {
      "hash": "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
      "ver": 1 ...
    }
  ]
}

```

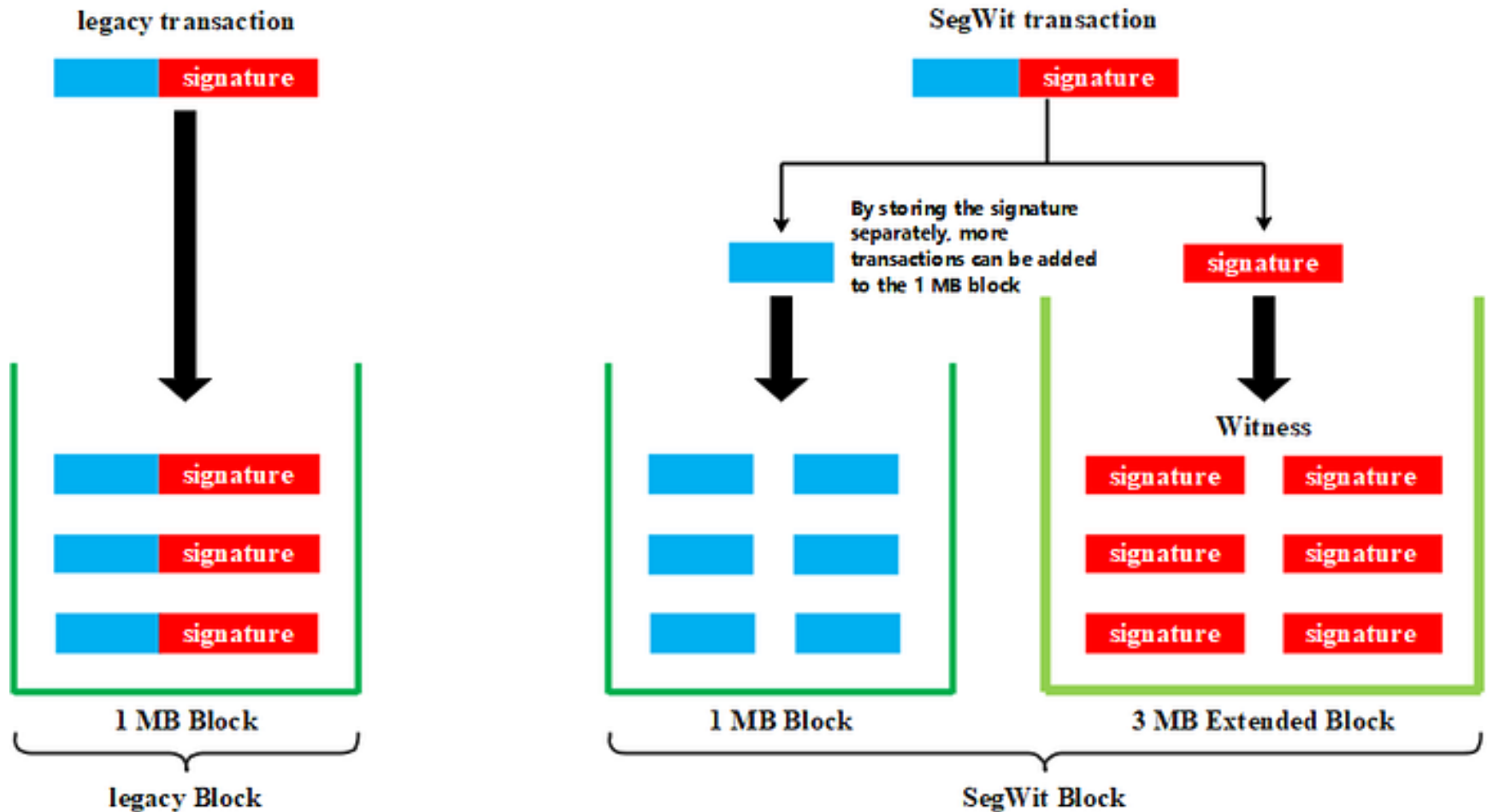
† Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

[**https://www.blockchain.com/explorer/blocks/btc/1**](https://www.blockchain.com/explorer/blocks/btc/1)

Block Structure



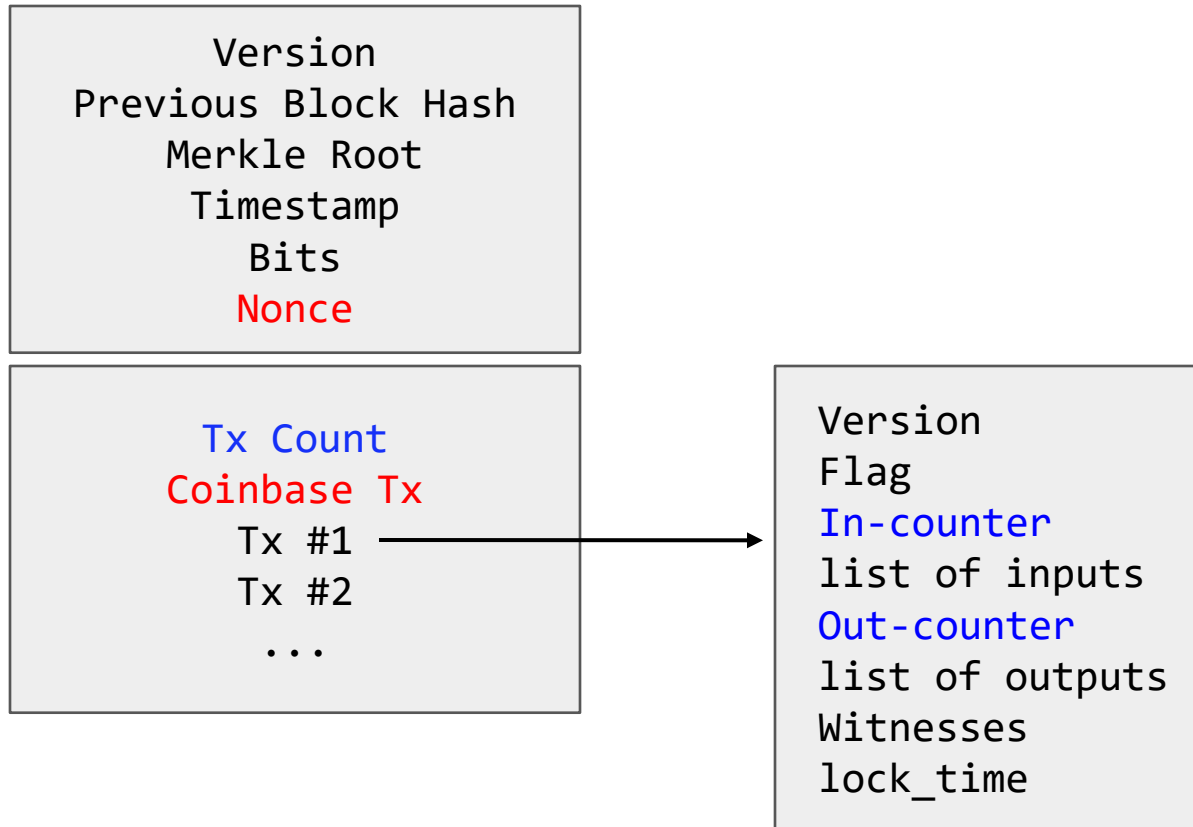
Legacy vs SegWit Block





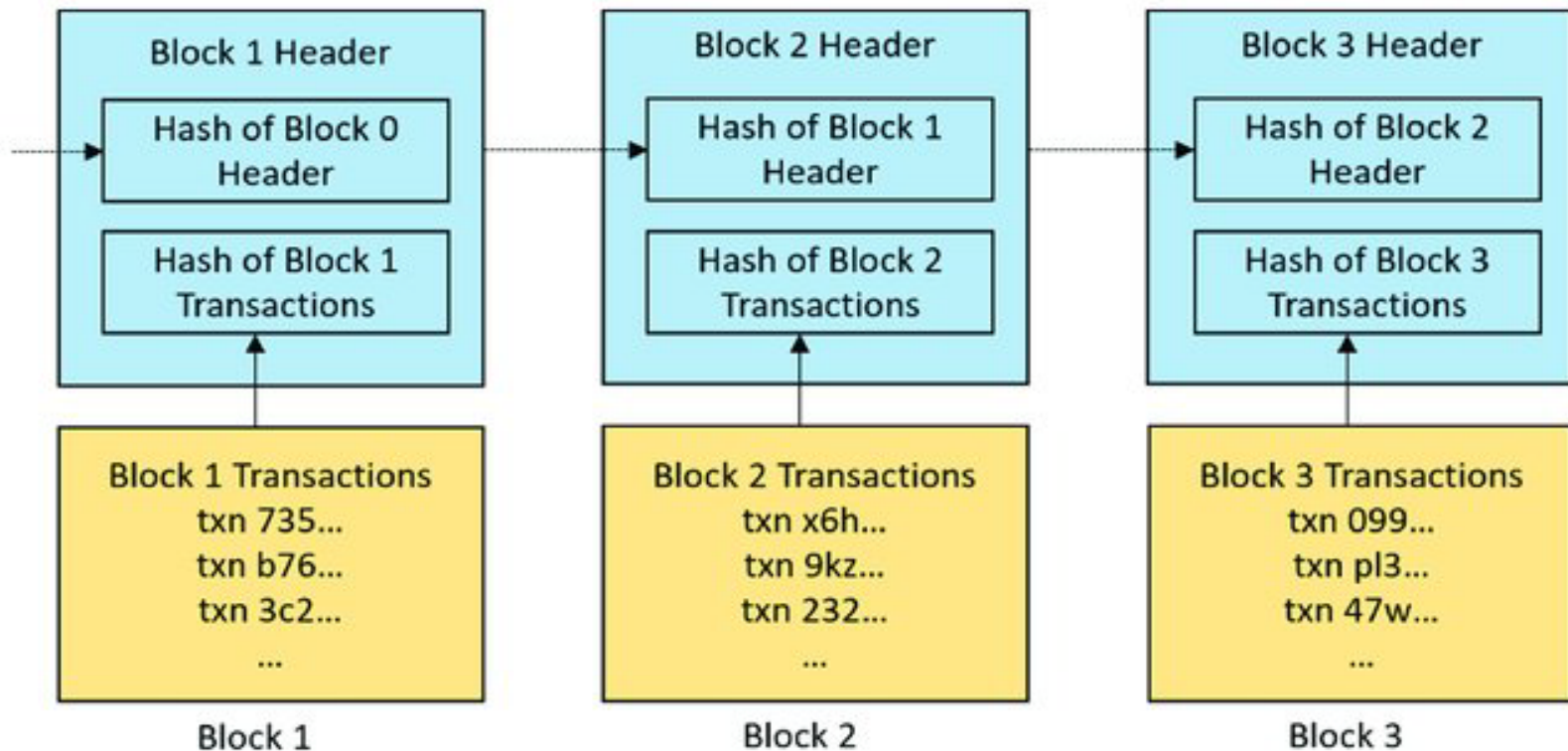
Bitcoin Block Structure

- Block = Block Header + Transaction List



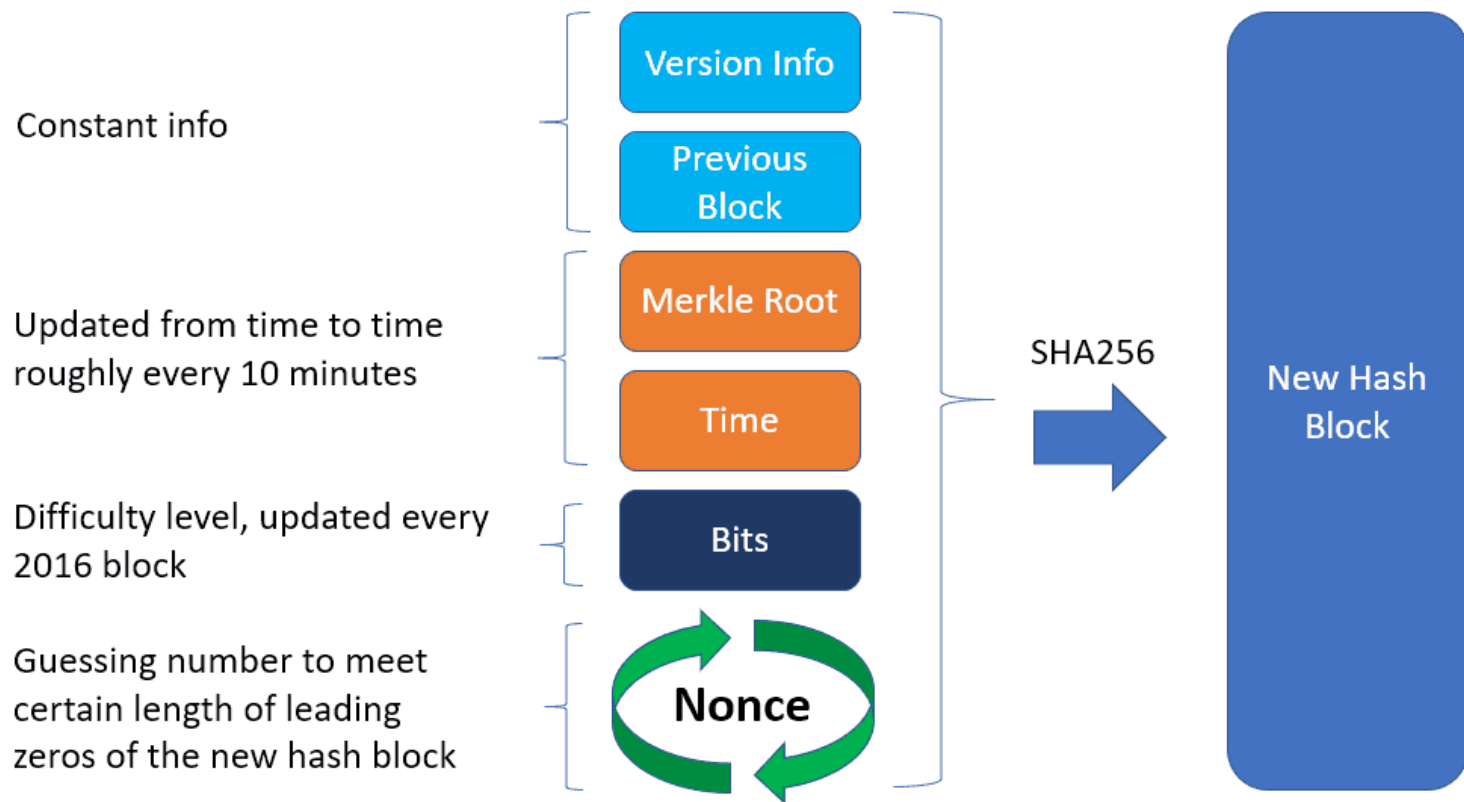
Chain ? Hash of Previous Block Header

Hash = SHA256(Version, Prev BlockHash, Merkle Root, Time, Bits, Nonce)

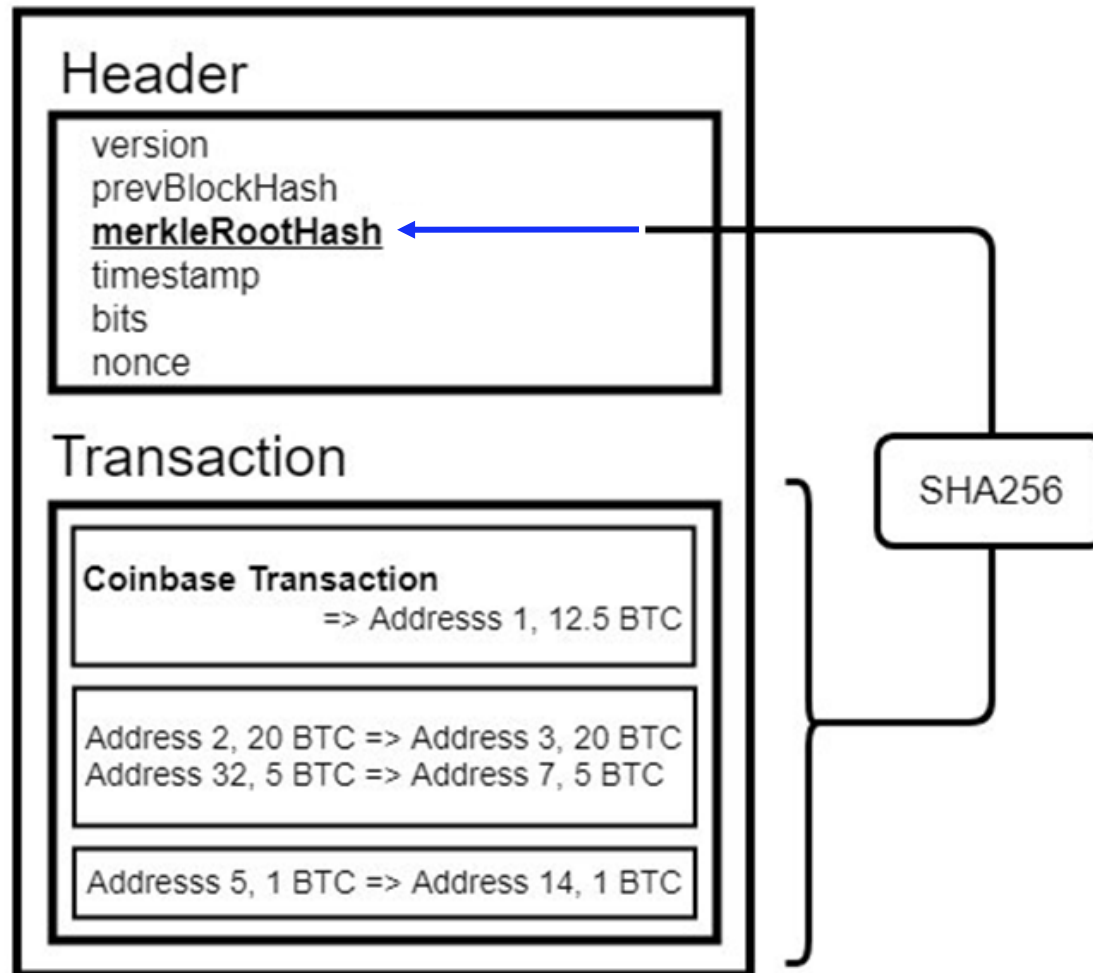


SHA256

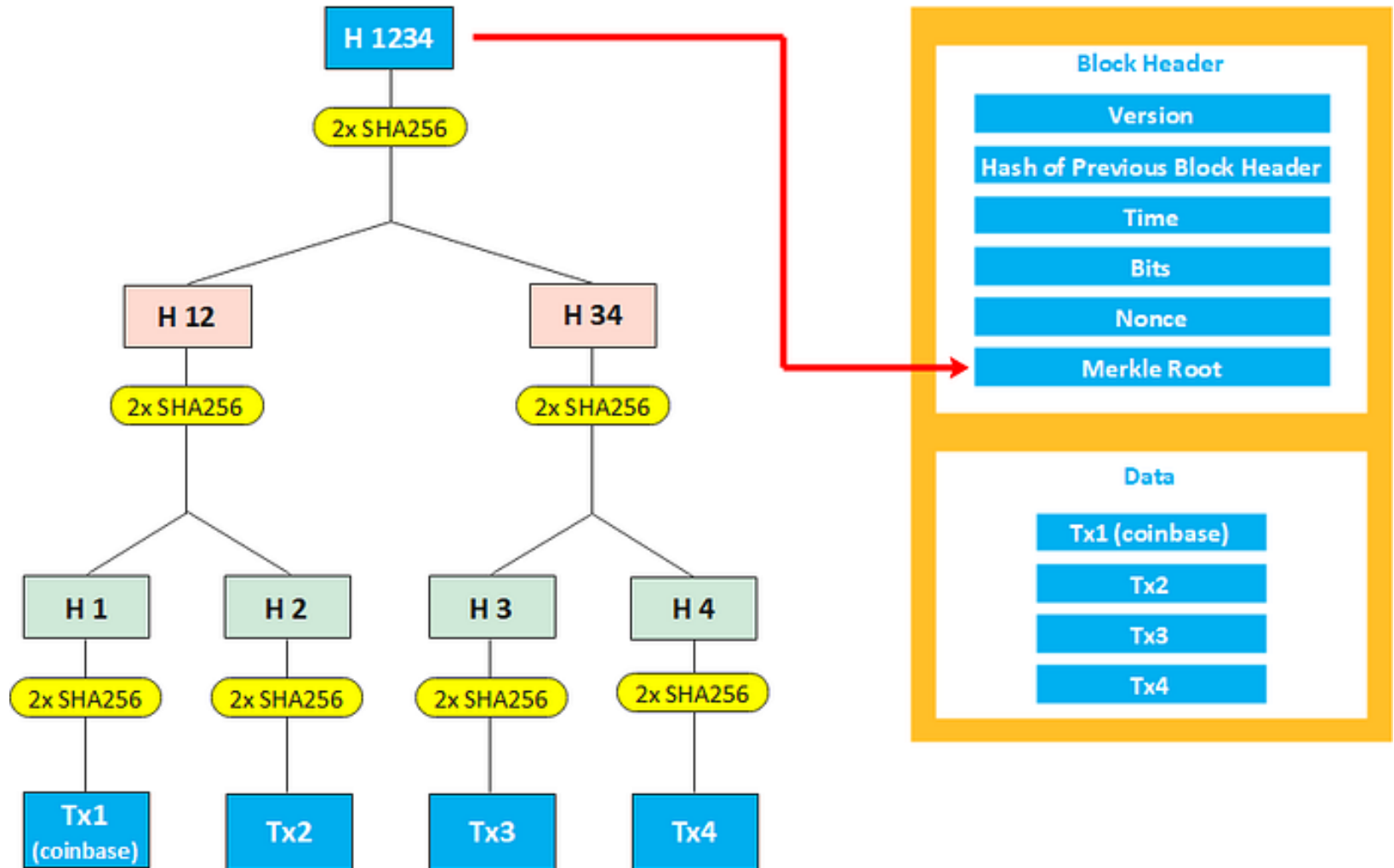
Bitcoin Block Hashing



Merkle Root



How to get Merkle Root

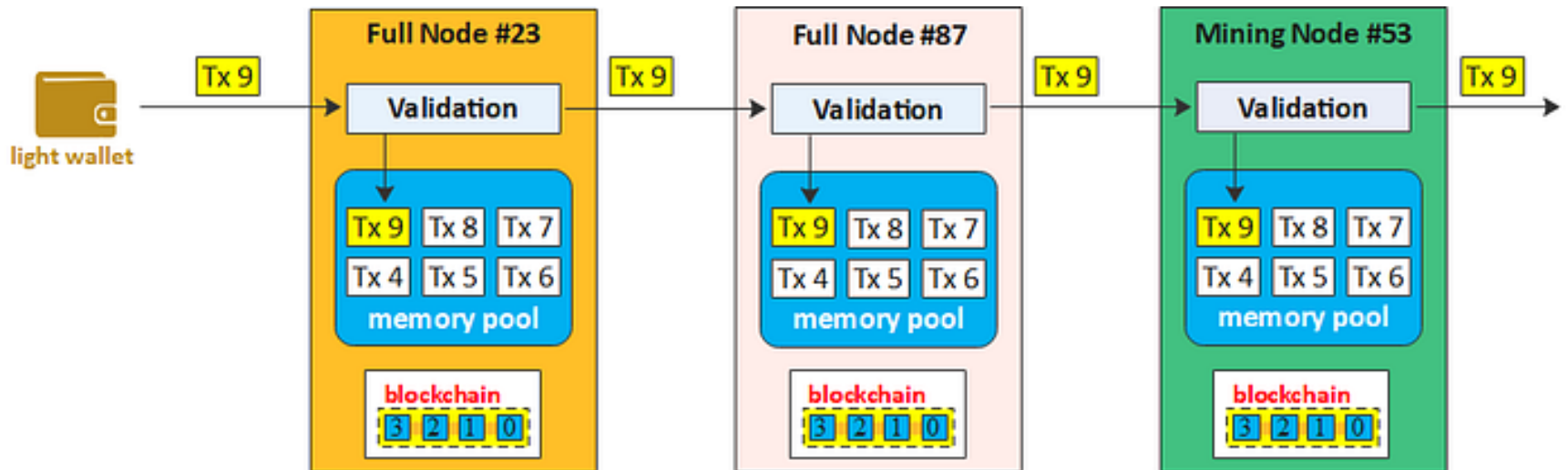


† Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

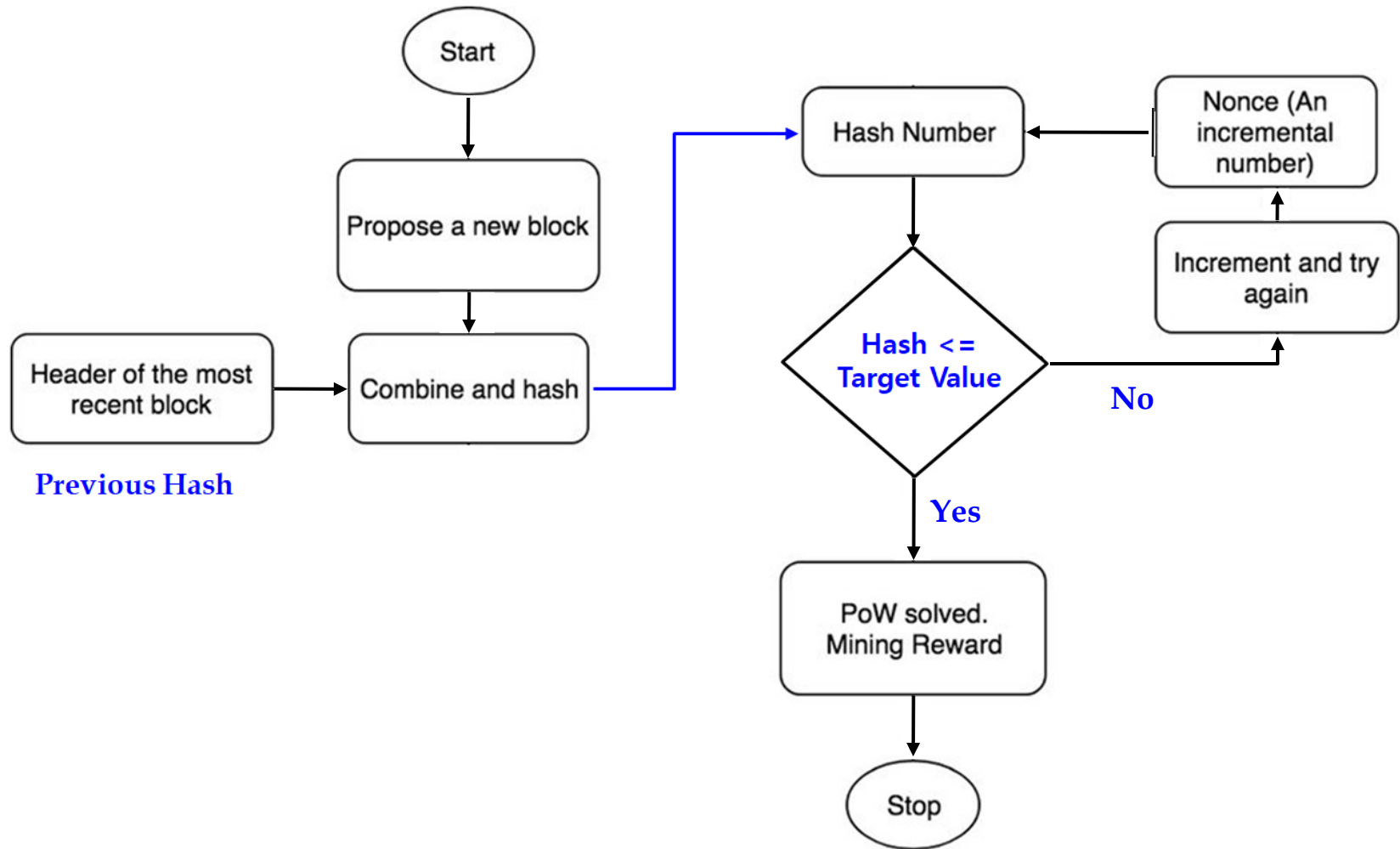
Mining Procedure in Bitcoin Core

- Transaction Collection
 - First, miners gather all valid transactions received from the network.
 - These transactions are stored in the memory pool
- Block Header Creation
 - a block header is created
 - It includes information such as the previous block's hash, mining difficulty, timestamp ...
- Nonce Value Alteration
 - Miners repeatedly change the nonce value in the block header while calculating the hash of the header
- Hash Validation
 - Miners verify whether the hash of the block header meets the difficulty level set by the network
 - Miners continue to change the nonce value and perform calculations until they find a hash that satisfies the difficulty
- Block Generation
 - Once a valid hash is found, the miner assembles a new block using the valid block header and the list of selected transactions
- Block Broadcasting
 - The newly mined block is broadcast to the network, notifying other nodes
- Reward Collection
 - Miners receive block rewards and transaction fees as compensation for mining the new block

Memory Pool



PoW (Proof of Work)

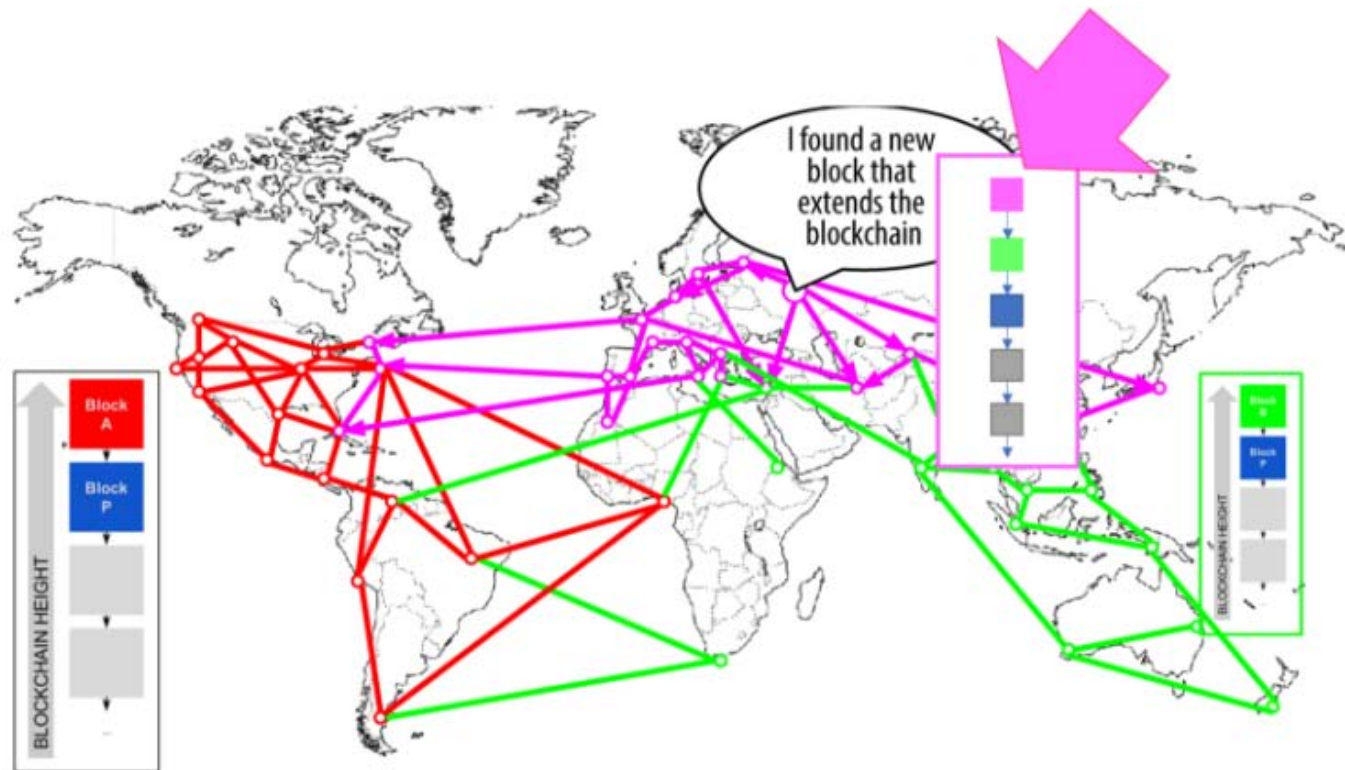


Two blocks are mined simultaneously ?

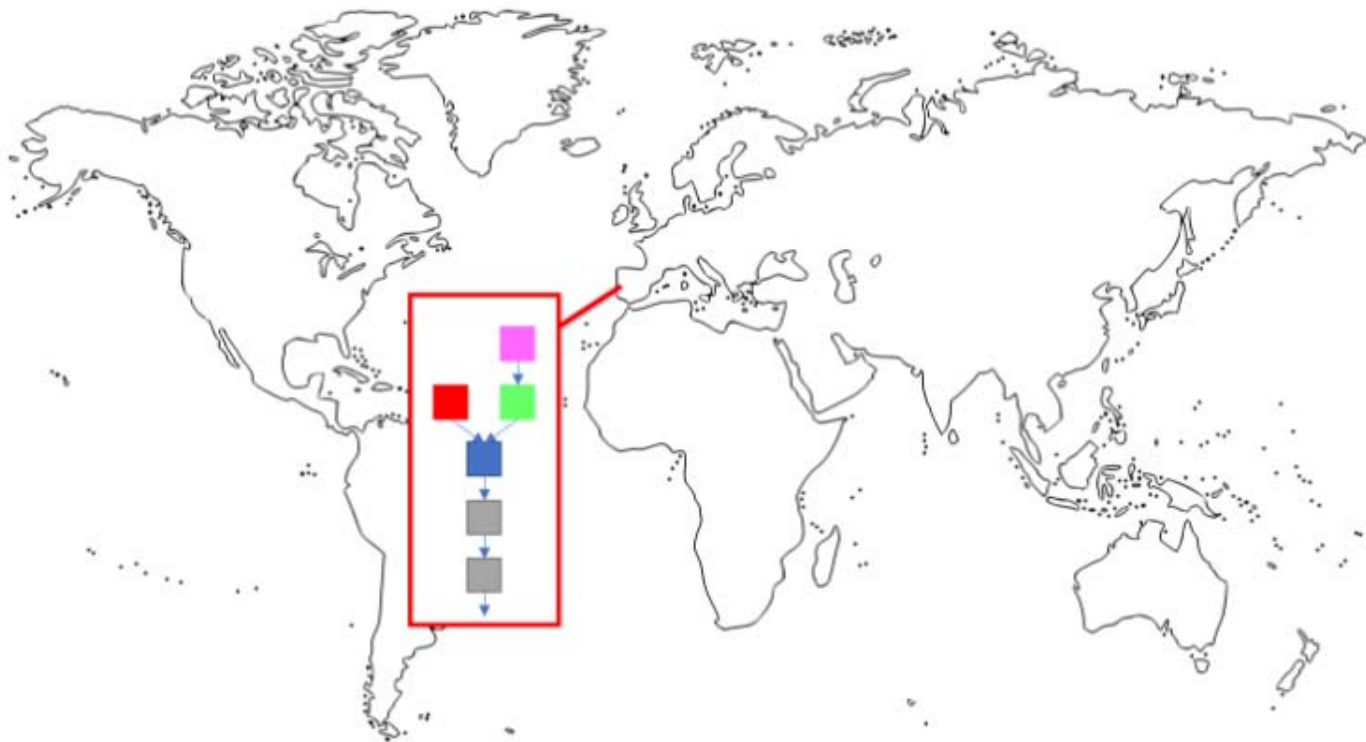








The decision on which block will be chosen ?



Block Search in Bitcoin

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

- <https://www.blockchain.com/explorer/blocks/btc/0>
 - 00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
- <https://blockchain.info/rawblock/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>
- <https://blockchain.info/rawblock/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f?format=hex>
- <https://api.blockchair.com/bitcoin/raw/block/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>

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/00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda>

<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 (00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda)
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](https://blockchain.info/rawblock/$block_hash)

- Get block hash for block number 538695
- <https://www.blockchain.com/explorer/blocks/btc/538695>
 - 0000000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda
- [https://blockchain.info/rawblock/\\$block_hash](https://blockchain.info/rawblock/$block_hash)
 - <https://blockchain.info/rawblock/00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda>
- [https://blockchain.info/rawblock/\\$block_hash?format=hex](https://blockchain.info/rawblock/$block_hash?format=hex)
 - <https://blockchain.info/rawblock/00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda?format=hex>
- [https://api.blockchair.com/bitcoin/raw/block/\\$block_hash](https://api.blockchair.com/bitcoin/raw/block/$block_hash)
 - <https://api.blockchair.com/bitcoin/raw/block/00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda>

<https://blockchain.info/rawblock/00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda>

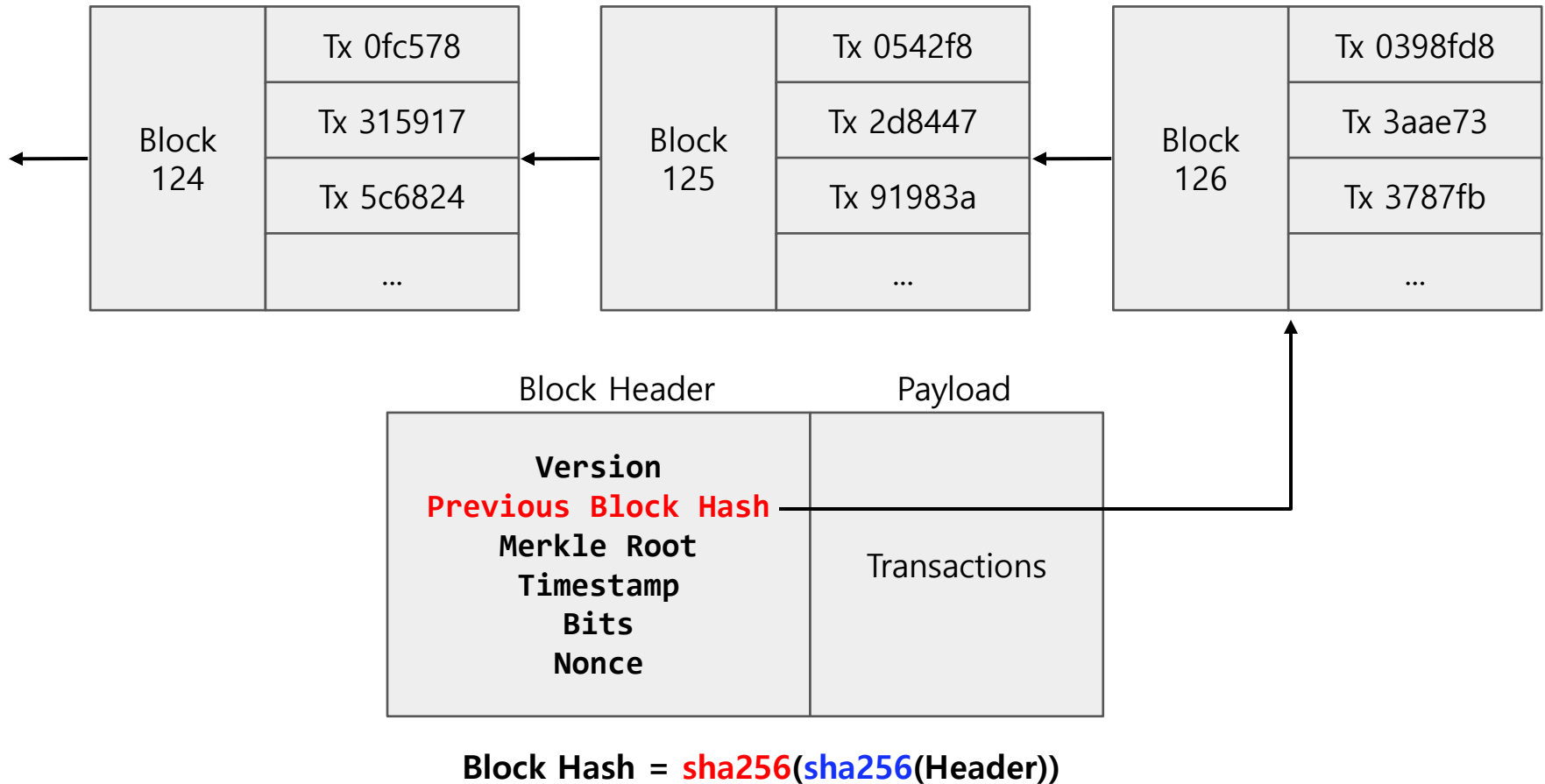
```
{
  "hash": "00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda",
  "ver": 536870912,
  "prev_block": "000000000000000000002669a90eec10c534c158eabe4ef8bd7f6133601f0ab116",
  "mrkl_root": "e0e5c1e24465805b97c359d9f0f5271a014b766853073f516bc6bc4f3be29bd7",
  "time": 1535359046,
  "bits": 388618029,
  "next_block": [
    "000000000000000000009ef223af6652bbc8736e756e1b276dd429298eb4a3198"
  ],
  "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://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)

Blockchain



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

Block Header

- [github.com/bitcoin/bitcoin/src/primitives/block.h](https://github.com/bitcoin/bitcoin/blob/master/src/primitives/block.h)

```
/** The block header is 80 bytes.  
 * (4) version  
 * (32) previous block hash  
 * (32) merkle root  
 * (4) time  
 * (4) bits  
 * (4) nonce  
 */
```

```
class CBlockHeader  
{  
public:  
    // header  
    int32_t nVersion;  
    uint256 hashPrevBlock;  
    uint256 hashMerkleRoot;  
    uint32_t nTime;  
    uint32_t nBits;  
    uint32_t nNonce;  
    ...  
};
```

† 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)	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)

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)	
		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)

Bitcoin Genesis 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)

Bitcoin Genesis Block

```
GetHash()      = 0x0000000000019d6689c085ae165831e934fff763ae46a2a6c172b3f1b60a8ce26f
hashMerkleRoot = 0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
txNew.vin[0].scriptSig      = 486604799 4
    0x736B6E616220726F662074756F6C69616220646E6F63657320666F206B6E697262206E6F20726F6C6C65636E616843203930
    30322F6E614A2F33302073656D695420656854
txNew.vout[0].nValue        = 5000000000
txNew.vout[0].scriptPubKey =
    0x5F1DF16B2B704C8A578D0BBAF74D385CDE12C11EE50455F3C438EF4C3FBCF649B6DE611FEAE06279A60939E028A8D65C10B7
    3071A6F16719274855FEB0FD8A6704 OP_CHECKSIG

block.nVersion = 1
block.nTime     = 1231006505
block.nBits     = 0x1d00ffff
block.nNonce    = 2083236893

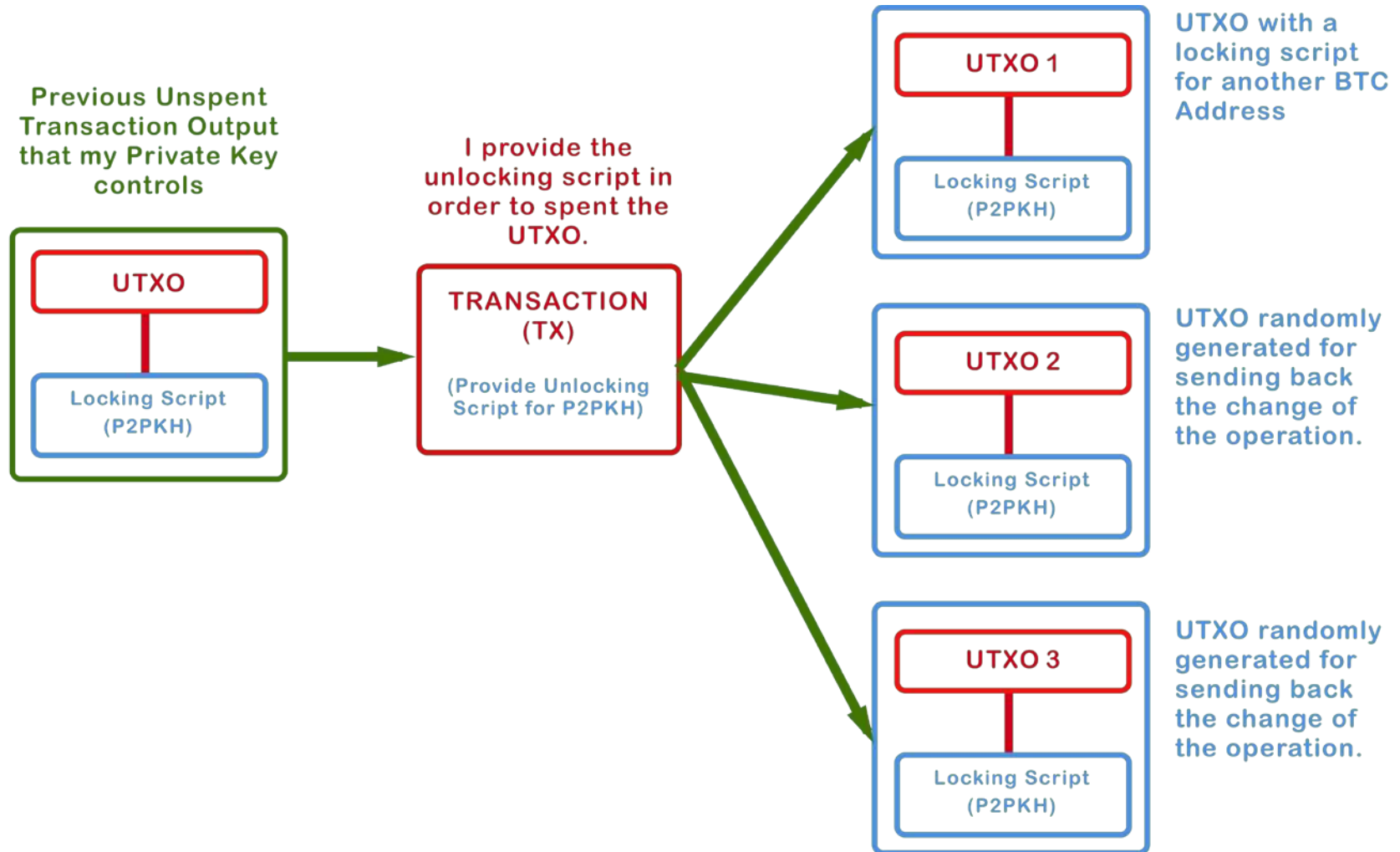
CBlock(hash=0000000000019d6, ver=1, hashPrevBlock=00000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505,
nBits=1d00ffff, nNonce=2083236893, vtx=1)
  CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
    CTxIn(COutPoint(000000, -1), coinbase
04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f
66207365636f6e64206261696c6f757420666f722062616e6b73)
    CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
  vMerkleTree: 4a5e1e
```


Raw Block Data

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; £ iyz{.²zC,>
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 1DyyyyM.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°pUH'
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gn q0°. \0¨(a9.
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybae.ab¶Io%?Li8A
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	oU.a.A.Ð\8M÷º..W
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	?Lp+kn._¬....

01000000 : version
 00 : prev block
 3BA3EDFD7A7B12B27AC72C3E67768F617FC81BC3888A51323A9FB8AA4B1E5E4A : merkle root
 29AB5F49 : timestamp
 FFFF001D : bits
 1DAC2B7C : nonce
 01 : number of transactions
 01000000 : version
 01 : input
 00FFFFFF : 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

UTXO (Unspent Transaction Output)



Bitcoin vs Bitcoin-Core

- <https://bitcoin.org/>
- <https://github.com/bitcoin/bitcoin>
- <https://bitcoincore.org/en/releases/>
- <https://bitcoincore.org/en/download/>
- bitcoin.it
- btc.com

