Ecclesiastes (Eccl) 12:13

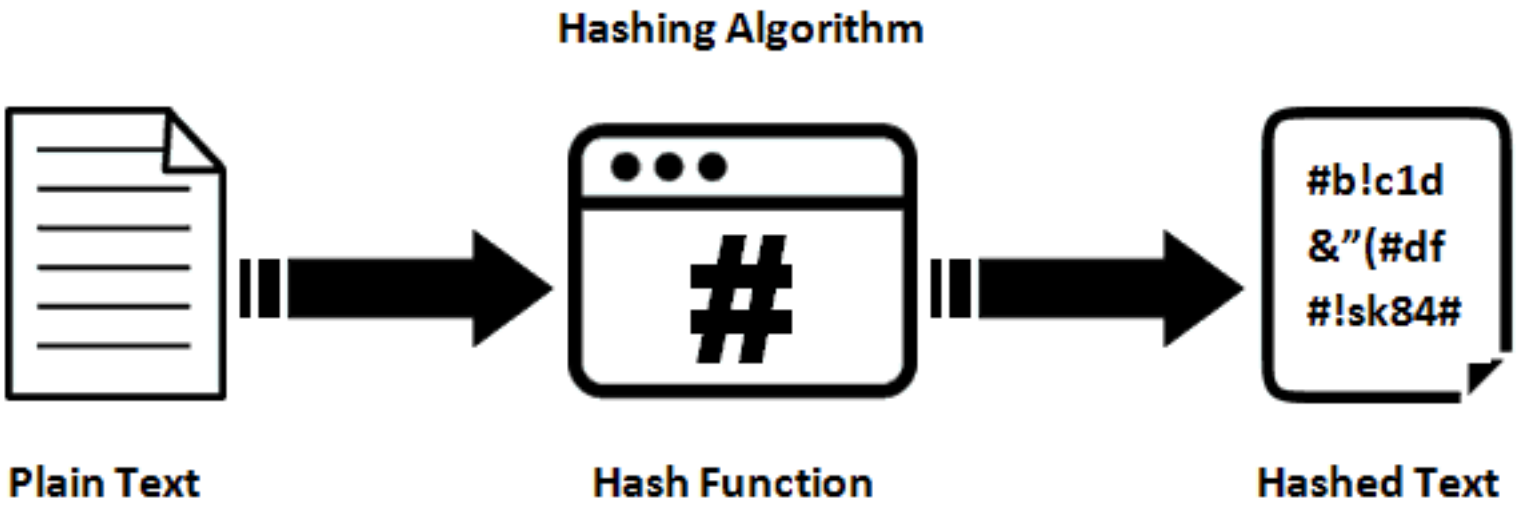
Now all has been heard;
here is the conclusion of the matter :

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

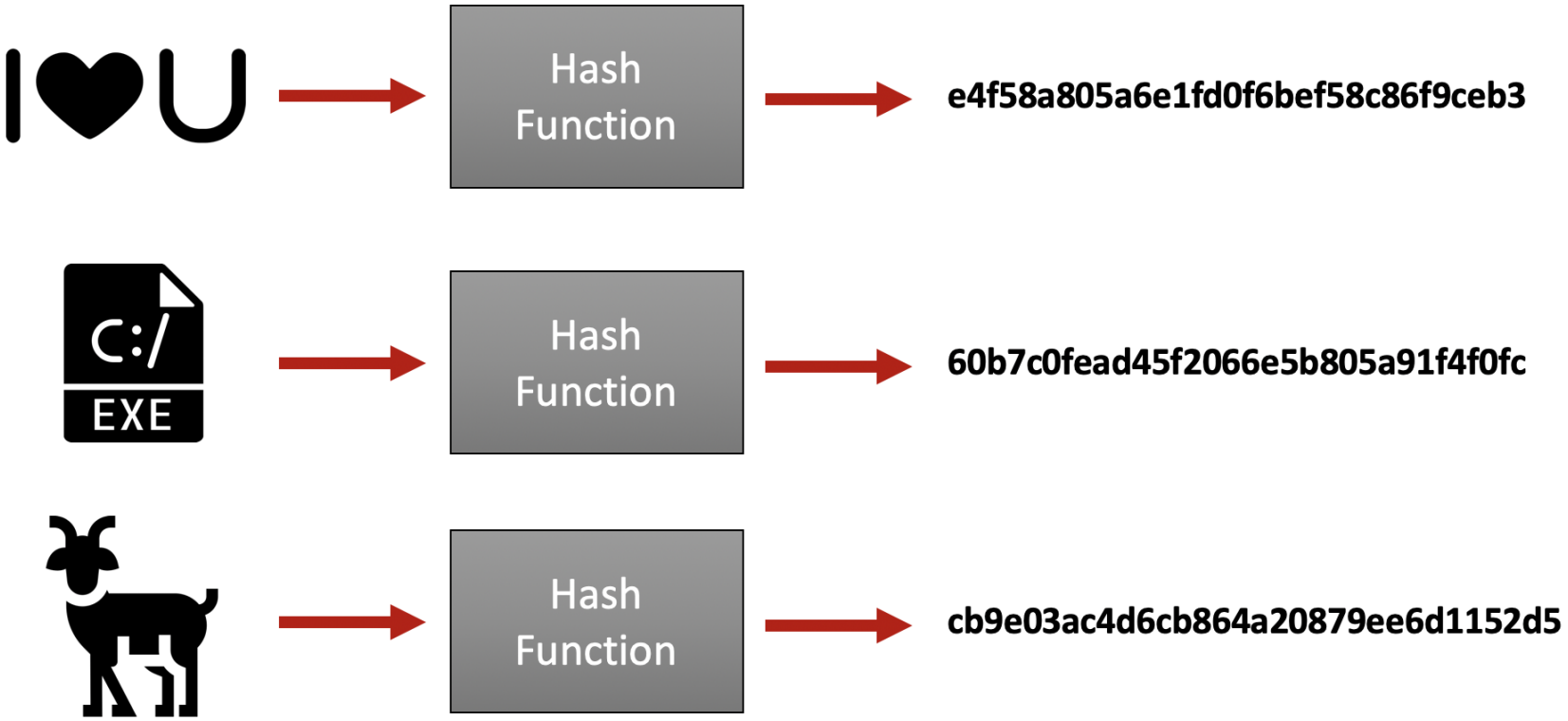
Fear God and keep his commandments,
for this is the whole duty of man.

Block and Chain ?

Hash Function

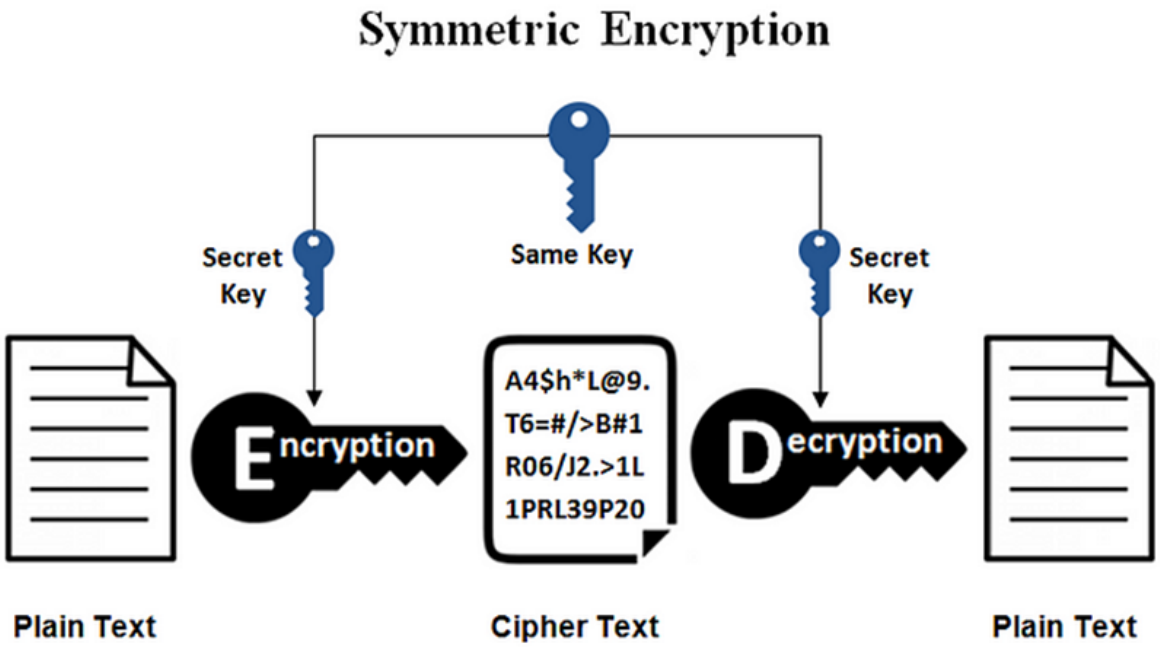


✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)



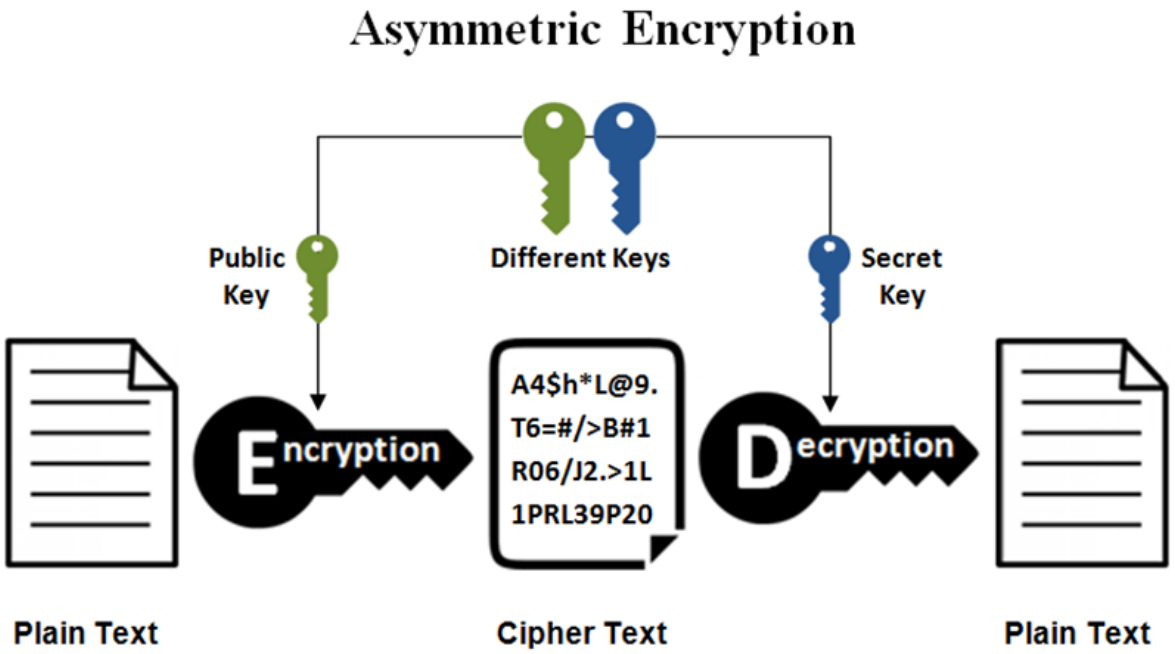
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

Symmetric Key Cryptography



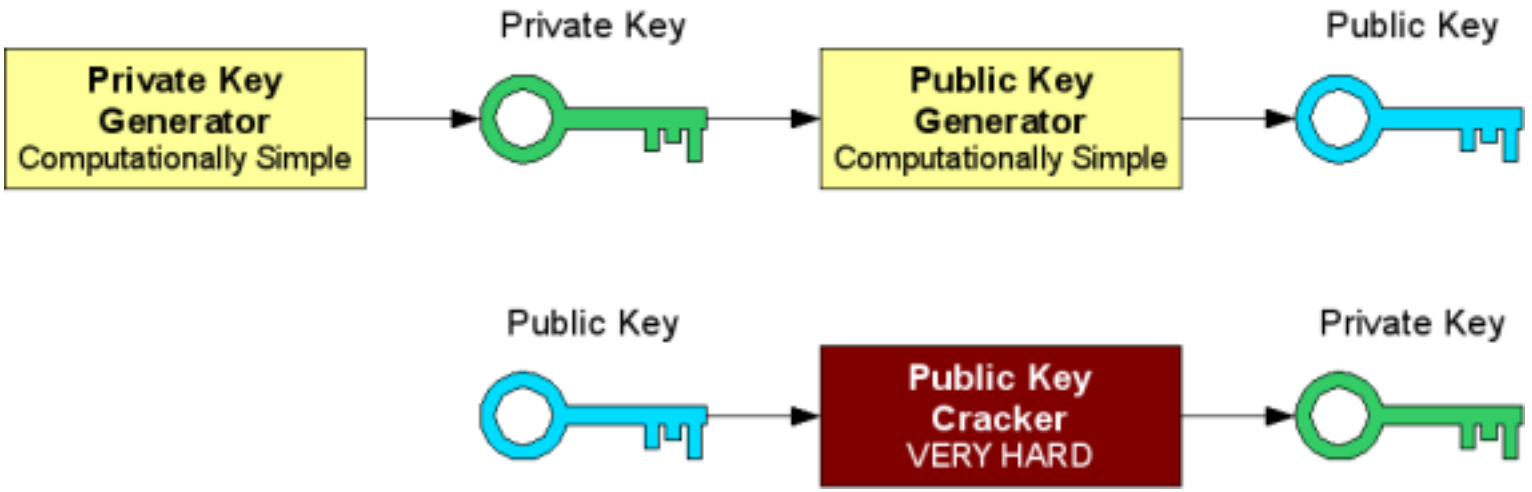
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Asymmetric (Public) Key Cryptography



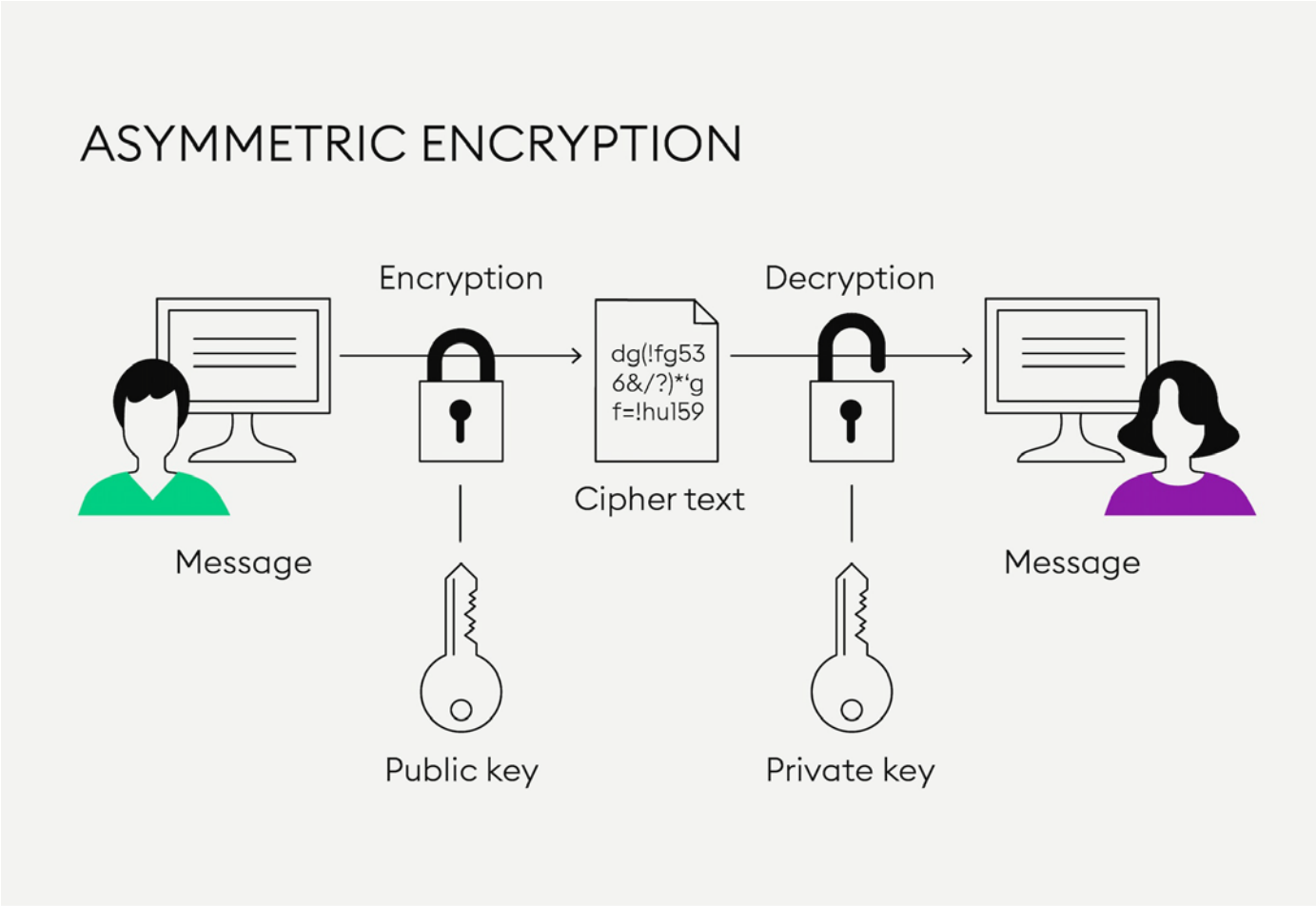
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Private Key vs Public Key



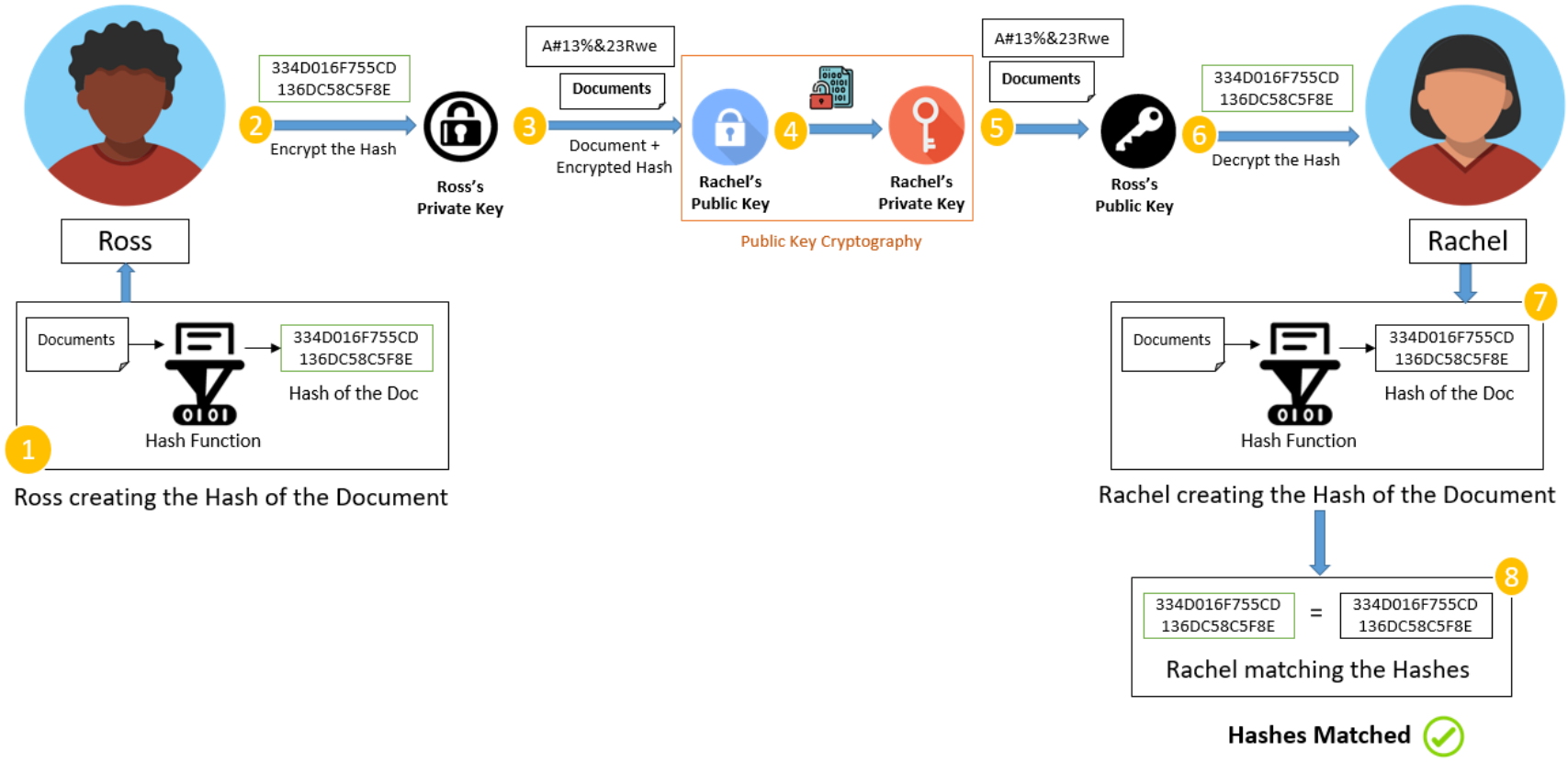
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

How to Share a Key in Symmetric Cryptography



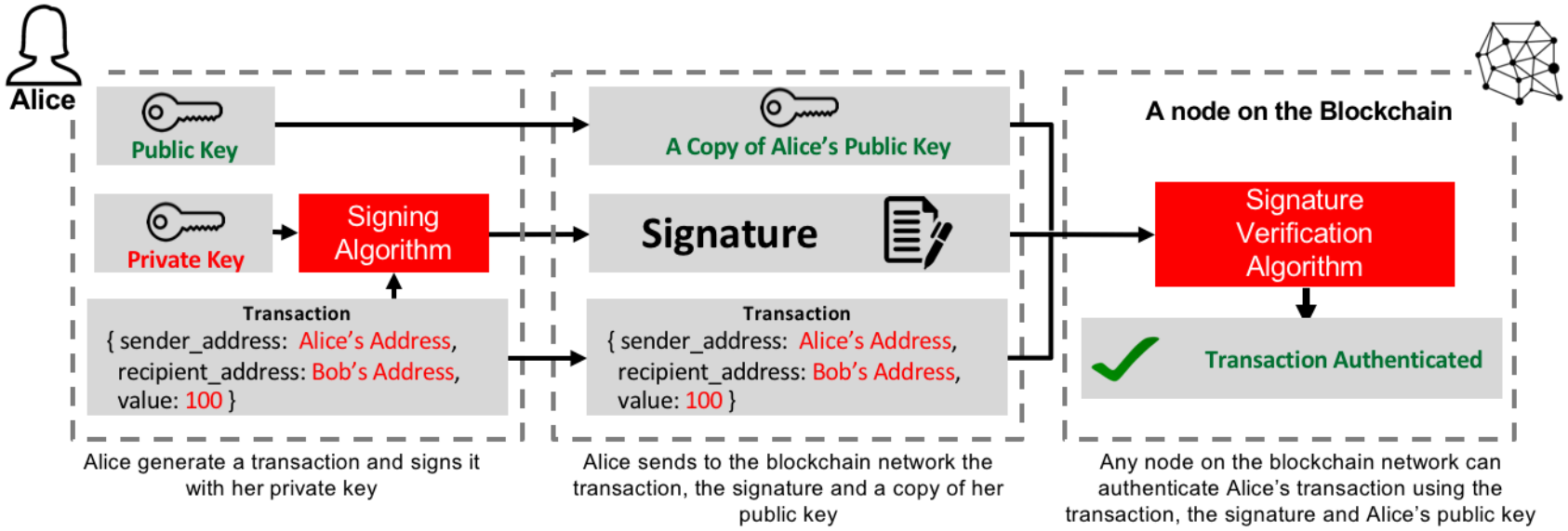
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

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

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

Ledger

BITCOIN TRANSACTION REQUEST MESSAGE

"David sends 5 BTC to Sandra"

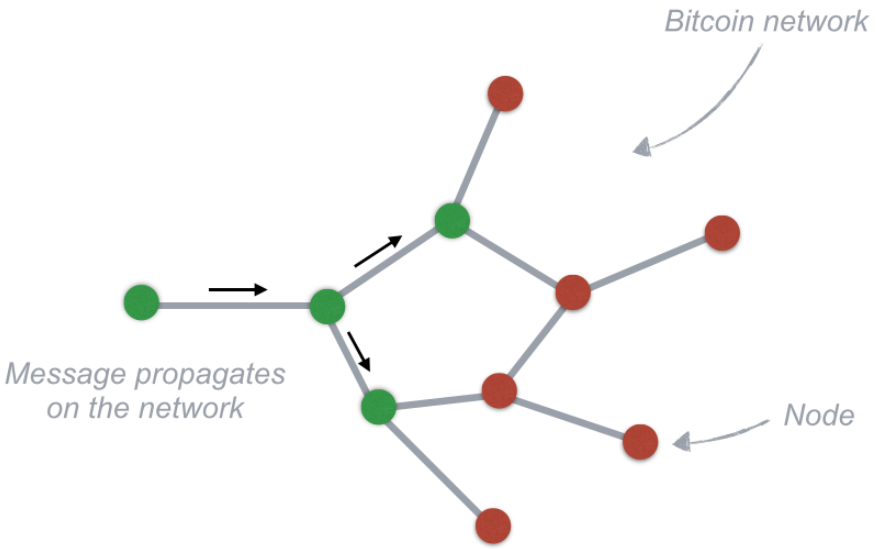
David → Sandra 5 BTC

LEDGER

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23

LEDGER

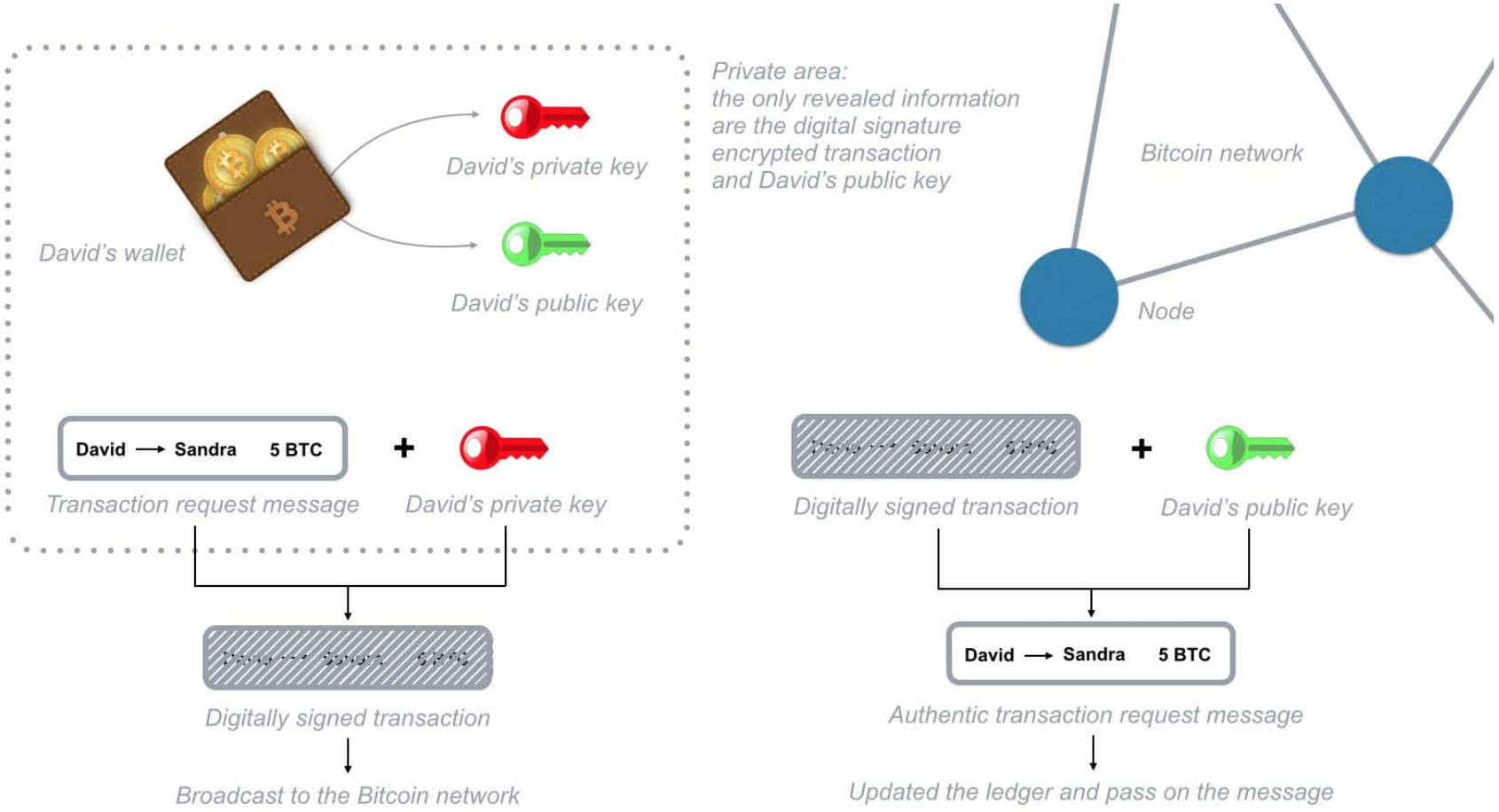
Account owner	Value
Mary	4
John	56
Sandra	88
Lisa	16
David	182
Brian	23



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

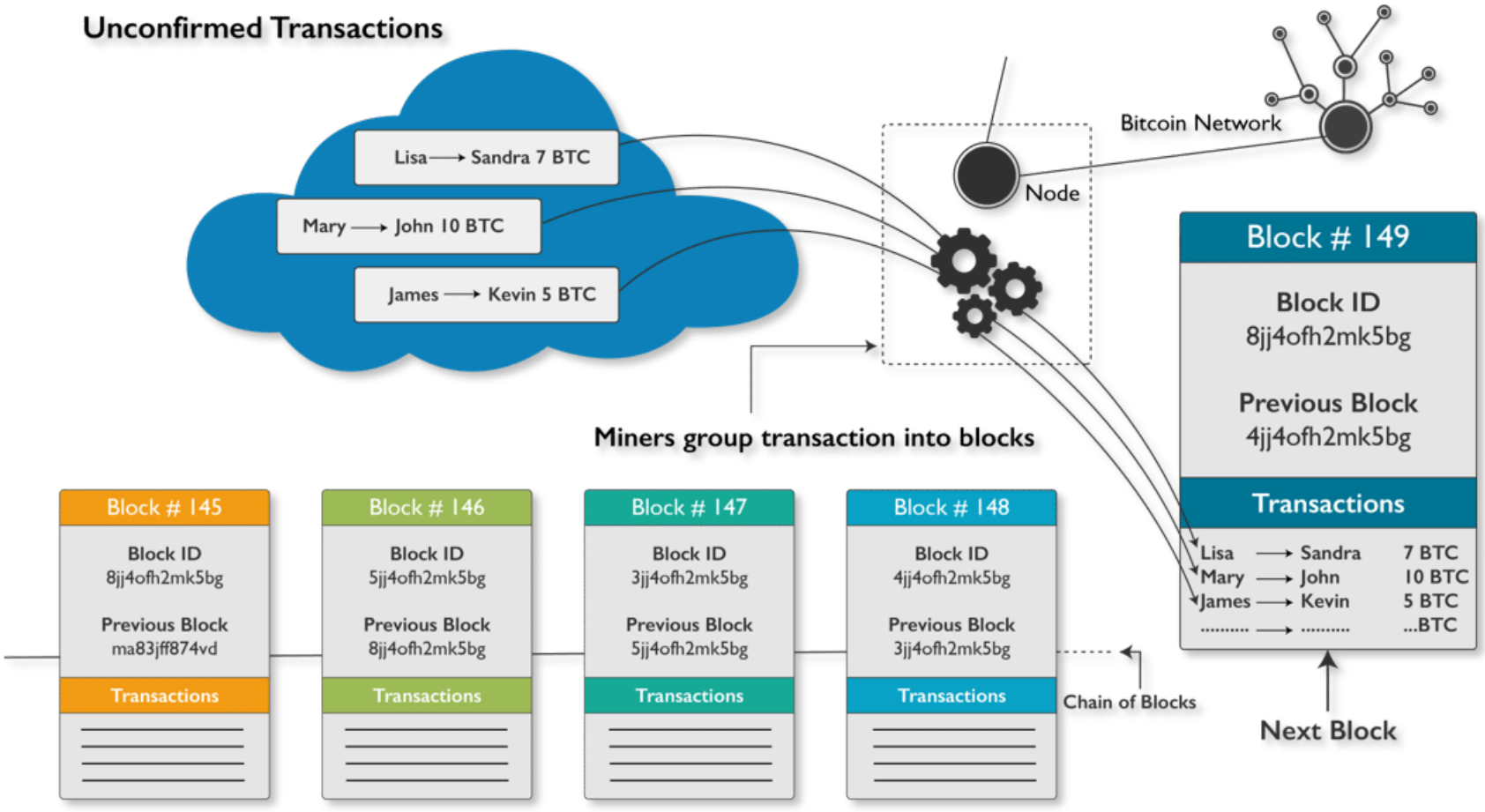
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

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

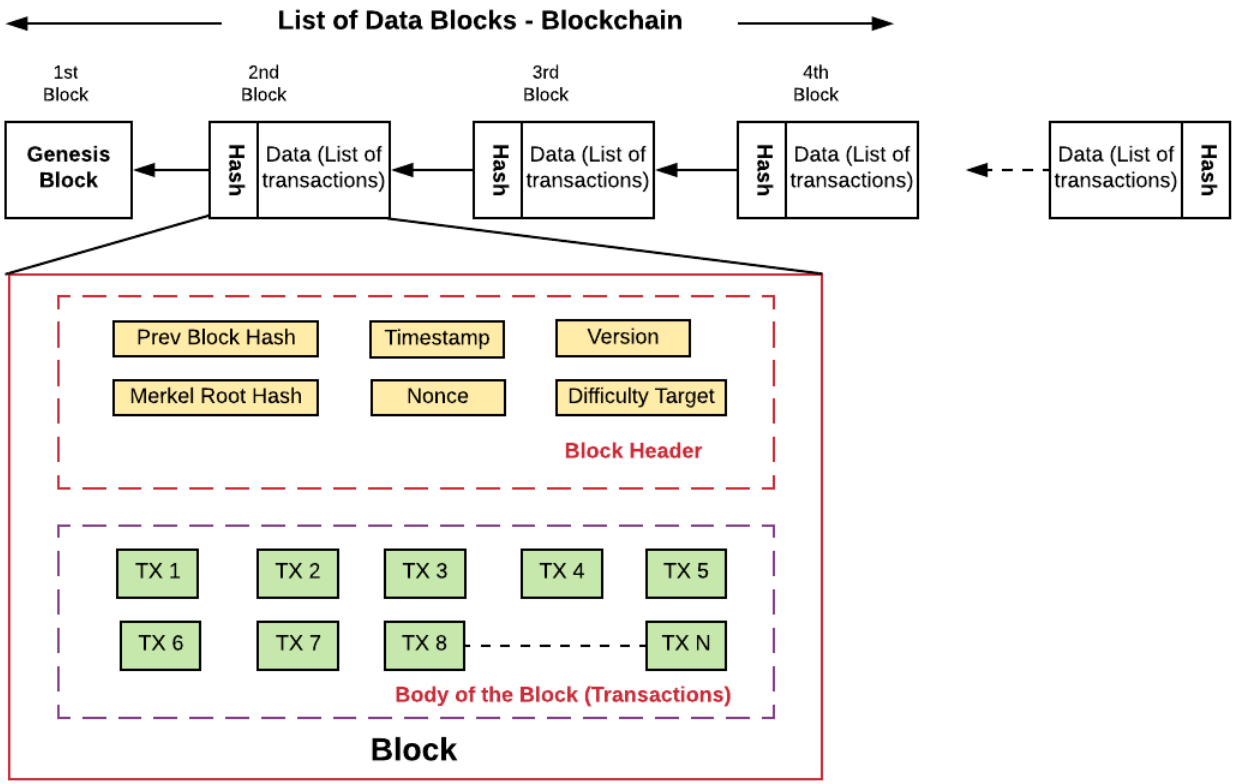


✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

https://andersbrownworth.com/blockchain/

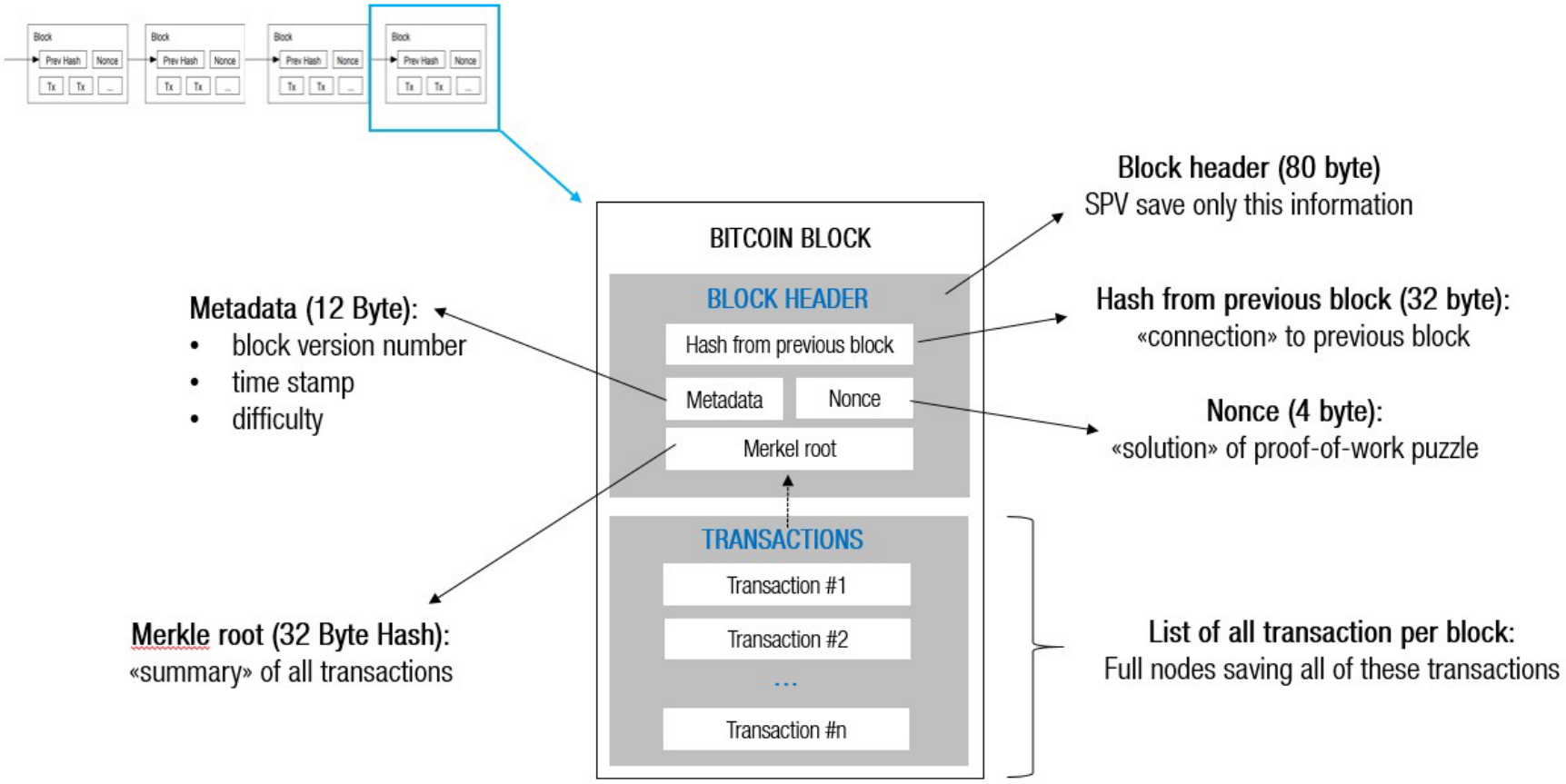
- `Block`
- `Blockchain`

Genesis Block and Blockchain



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

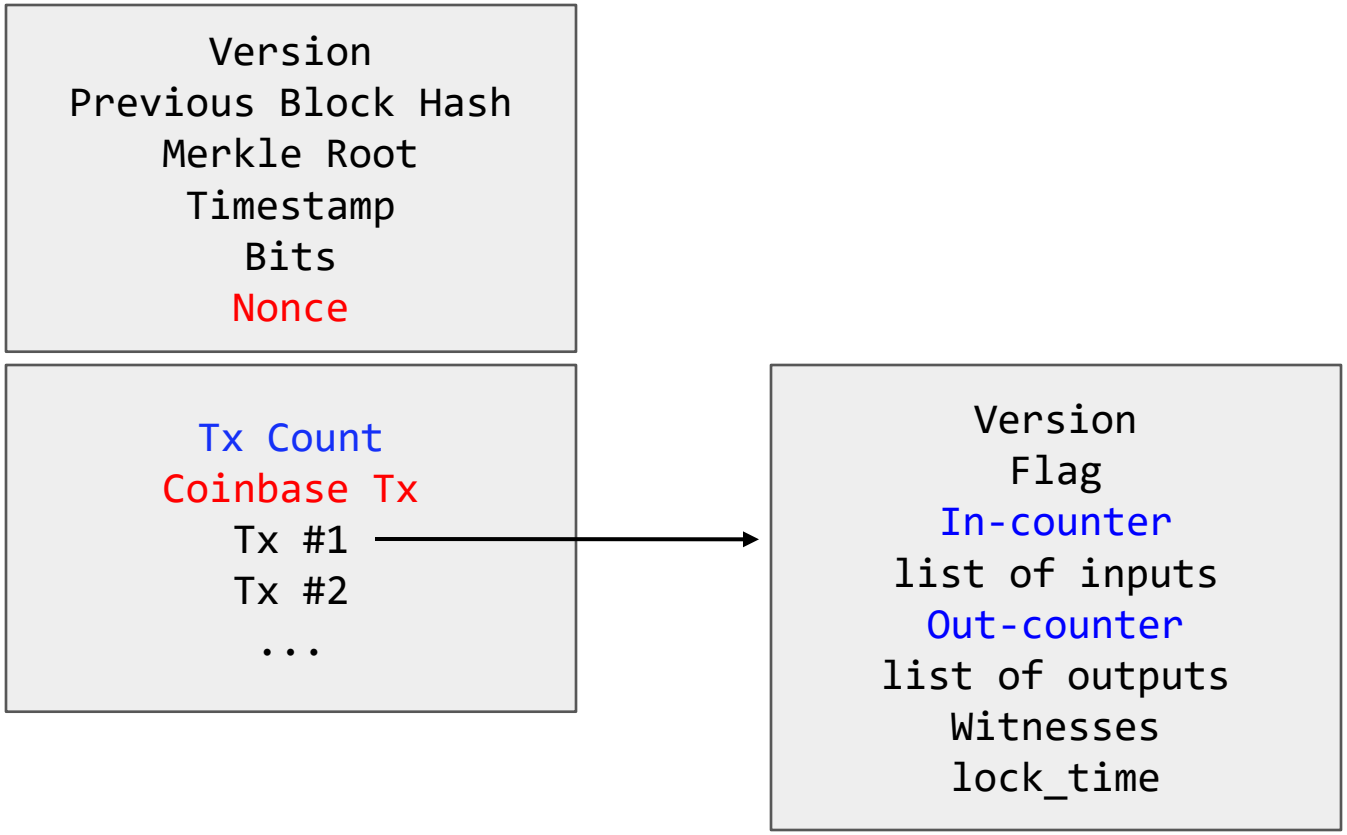
Block Structure



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

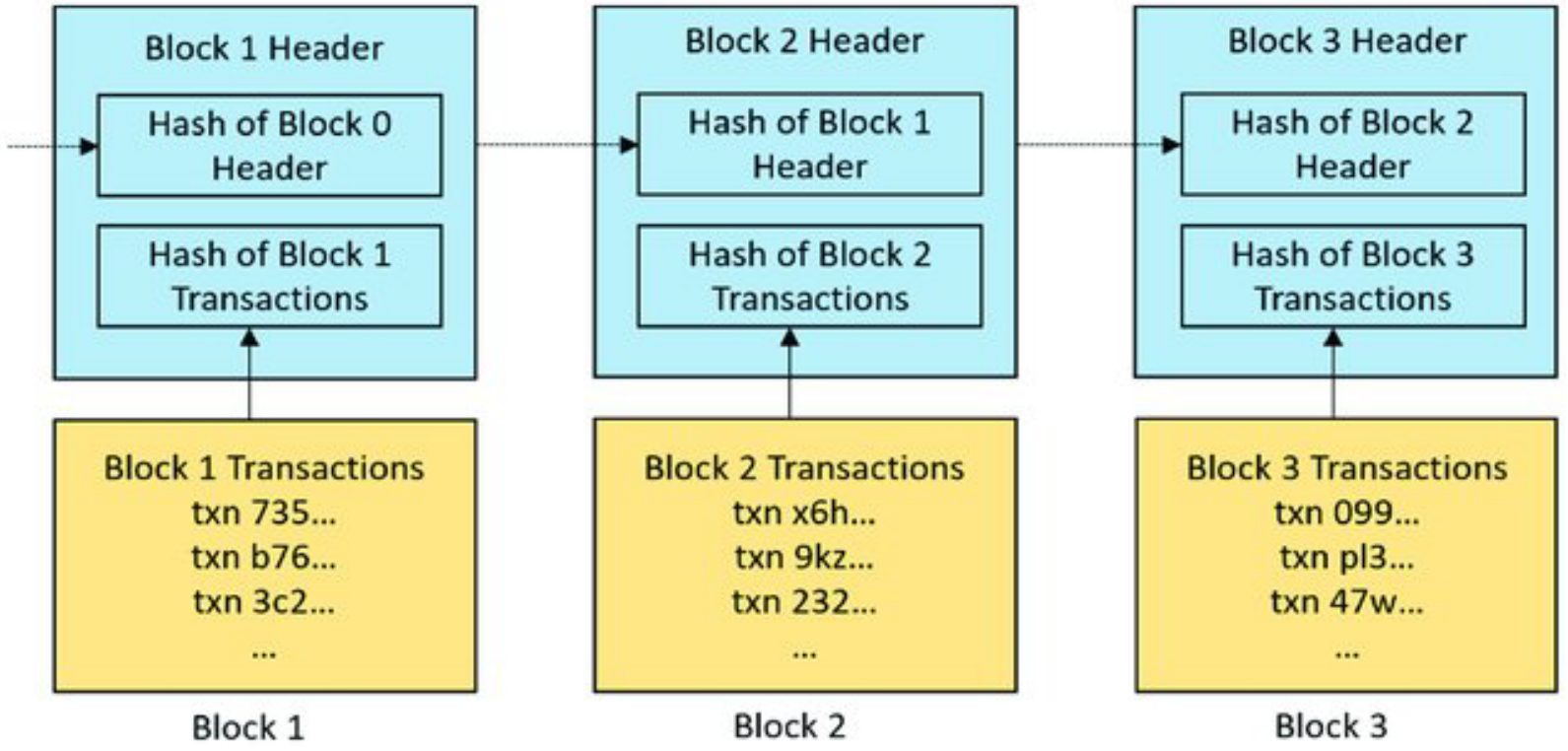
Block Structure

- Block Header + Block Body : Payload



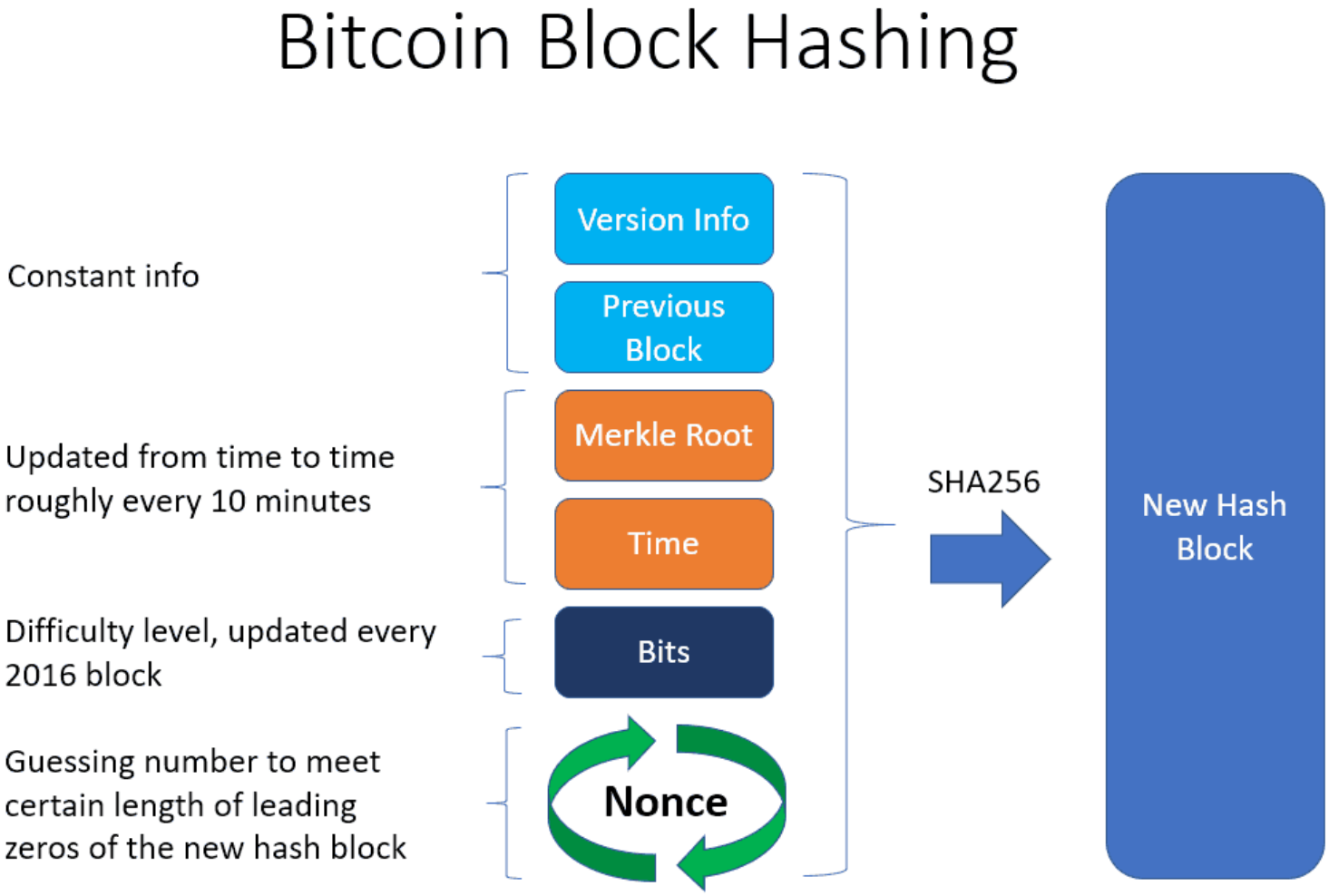
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

Chain : Hash of Previous Block Header



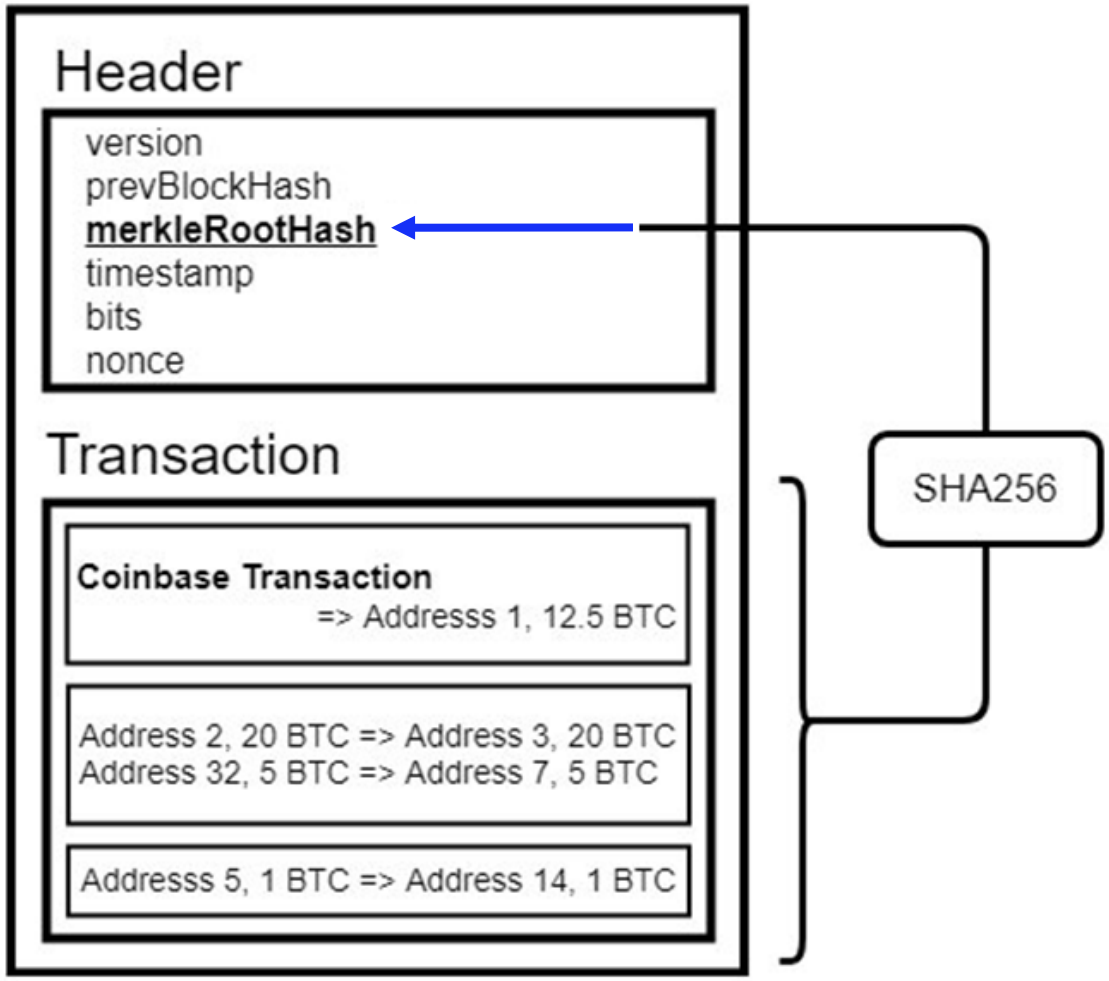
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

SHA256



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

Merkle Root



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

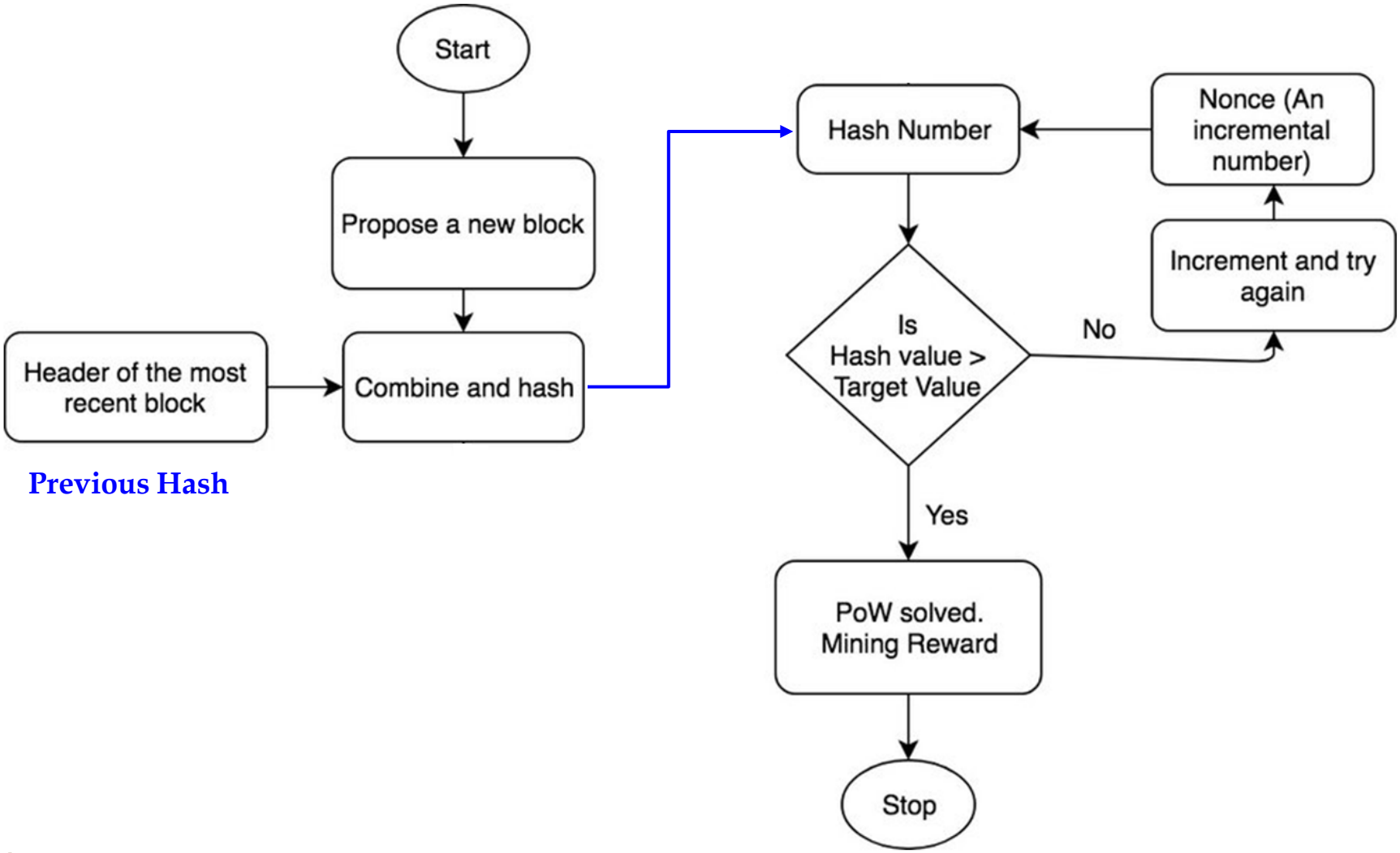
Mining Procedure in Bitcoin Core

- 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, and more.
- 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.

- These steps describe how miners use the Bitcoin Core source code to mine new blocks and contribute to the Bitcoin network.

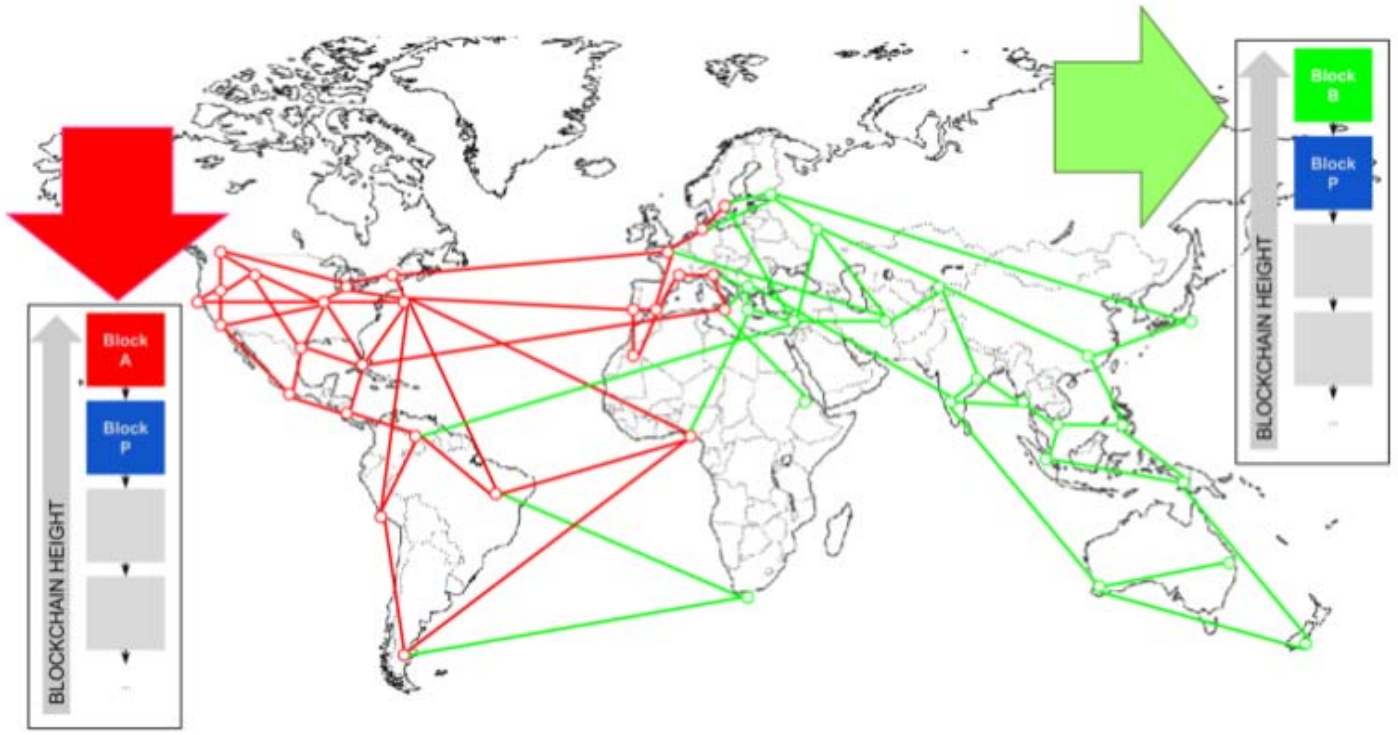
✝ Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)

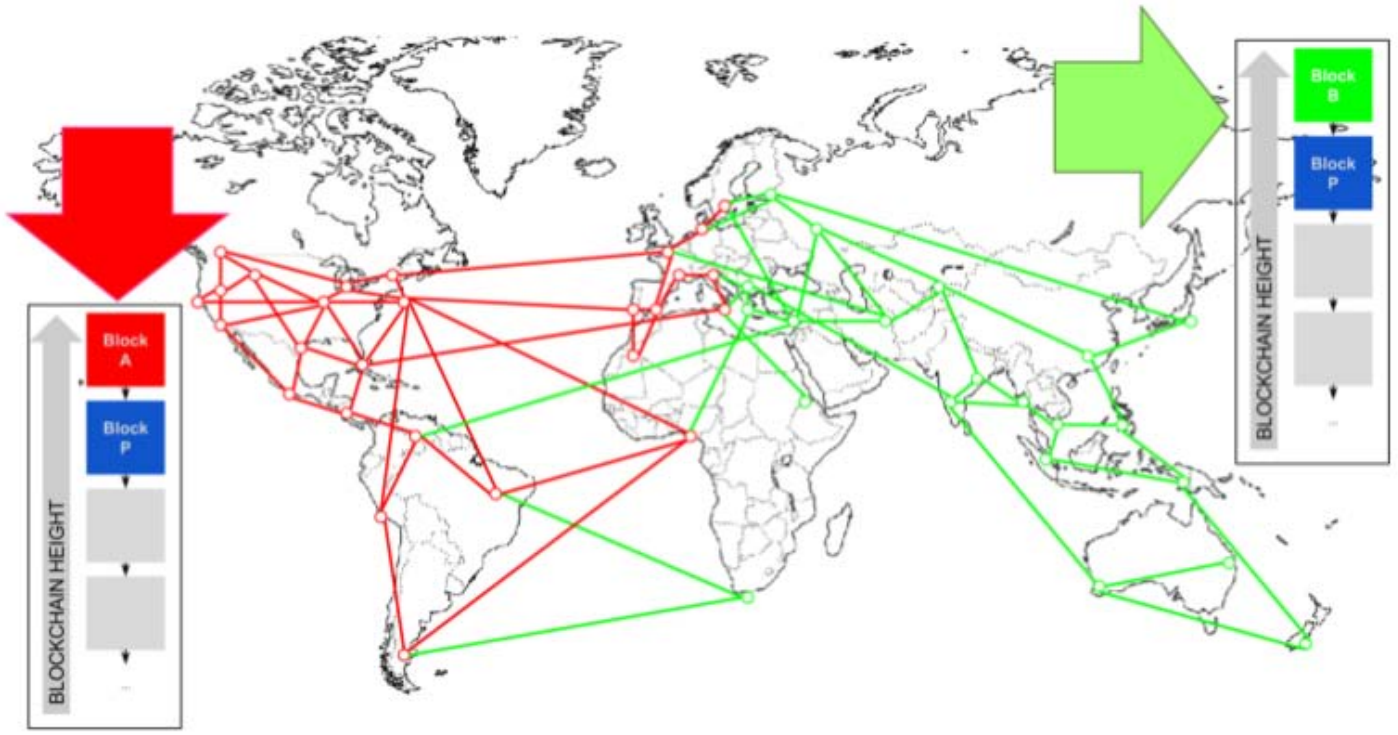
Mining, PoW (Proof of Work)



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

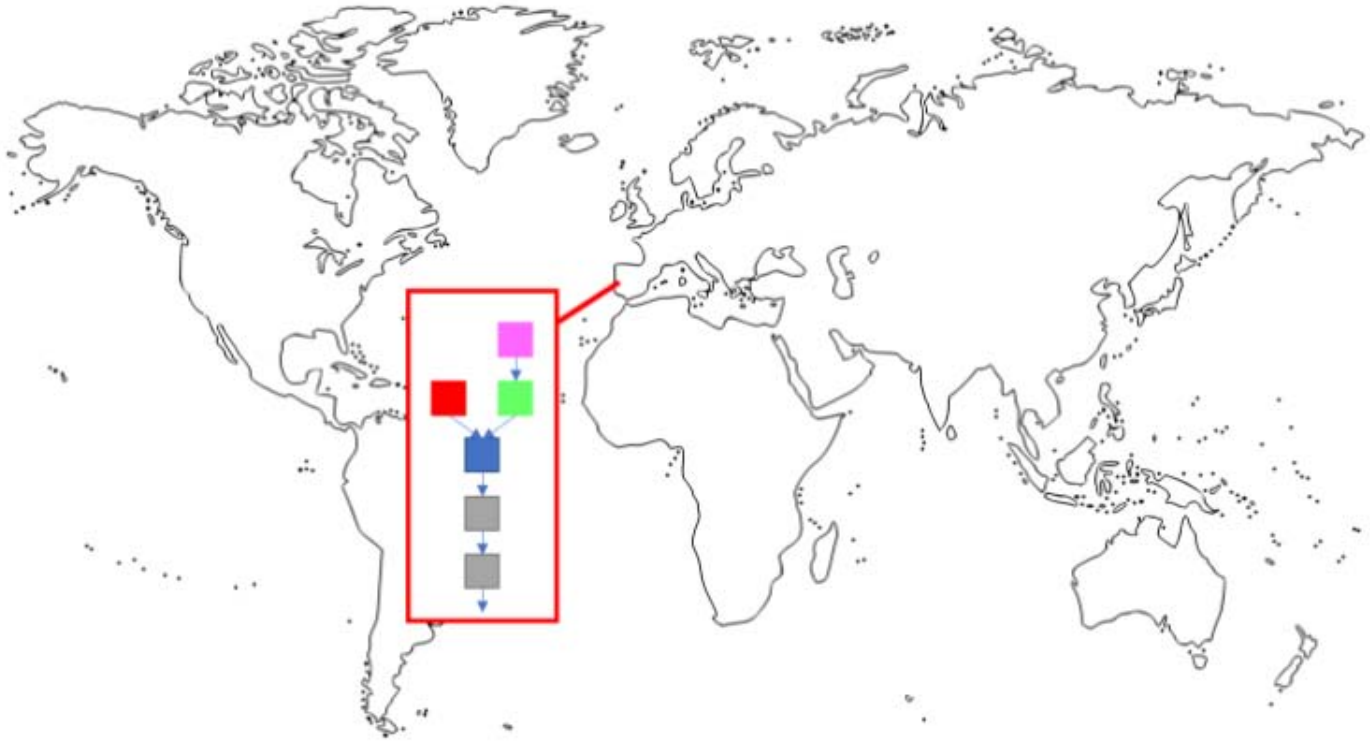
Two blocks are mined simultaneously ?


BLOCKCHAIN HEIGHT
Block A
Block P
BLOCKCHAIN HEIGHT
Block B
Block P


BLOCKCHAIN HEIGHT
Block A
Block P
BLOCKCHAIN HEIGHT
Block B
Block P


I found a new block that extends the blockchain
BLOCKCHAIN HEIGHT
Block A
Block P
BLOCKCHAIN HEIGHT

The decision on which block will be chosen ?



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/000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda

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

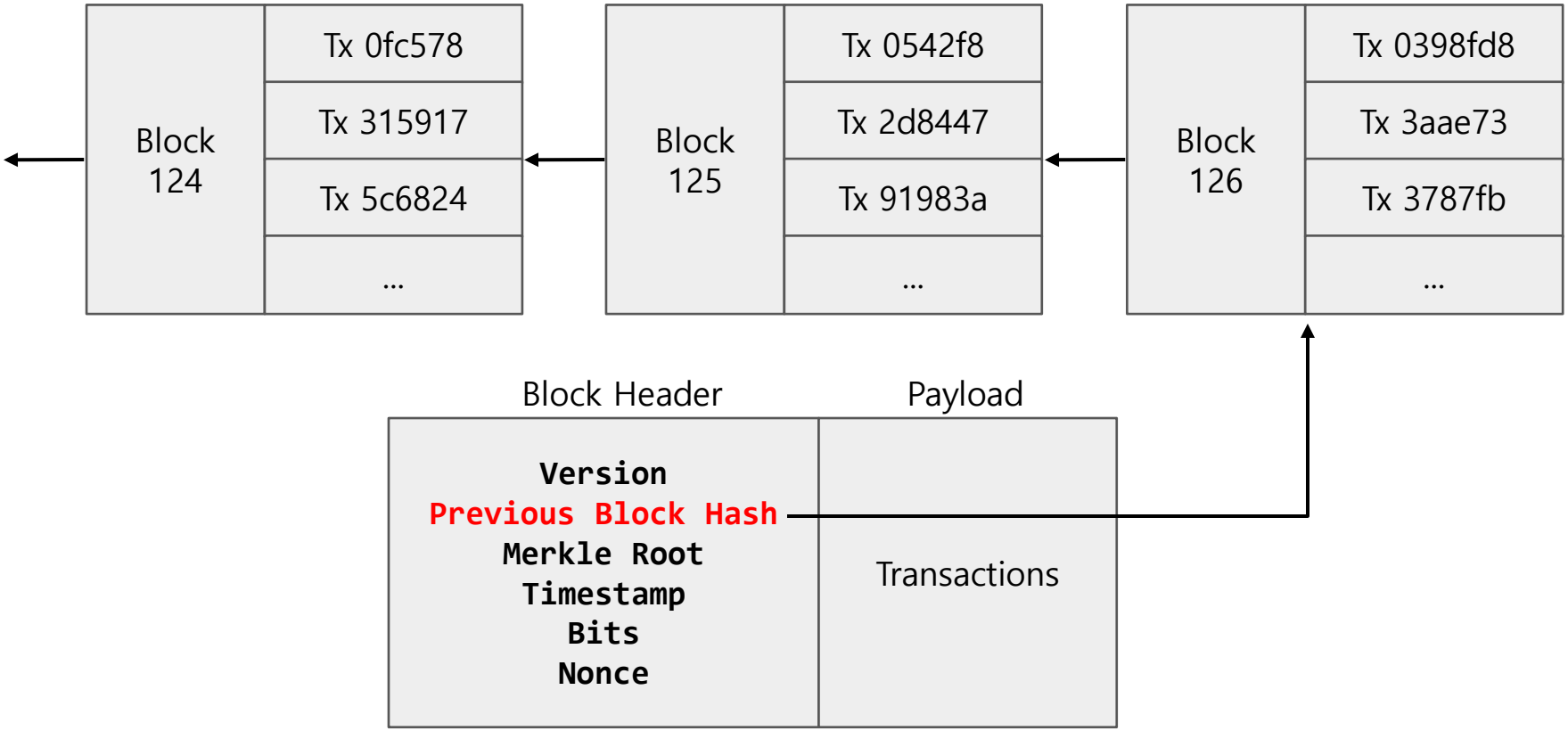
https://www.blockchain.com/explorer

```
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 (00000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda)
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)

Blockchain



Block hash = Sha256(Sha256(Header))

✝ **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

```
/** 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)**

The 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)	

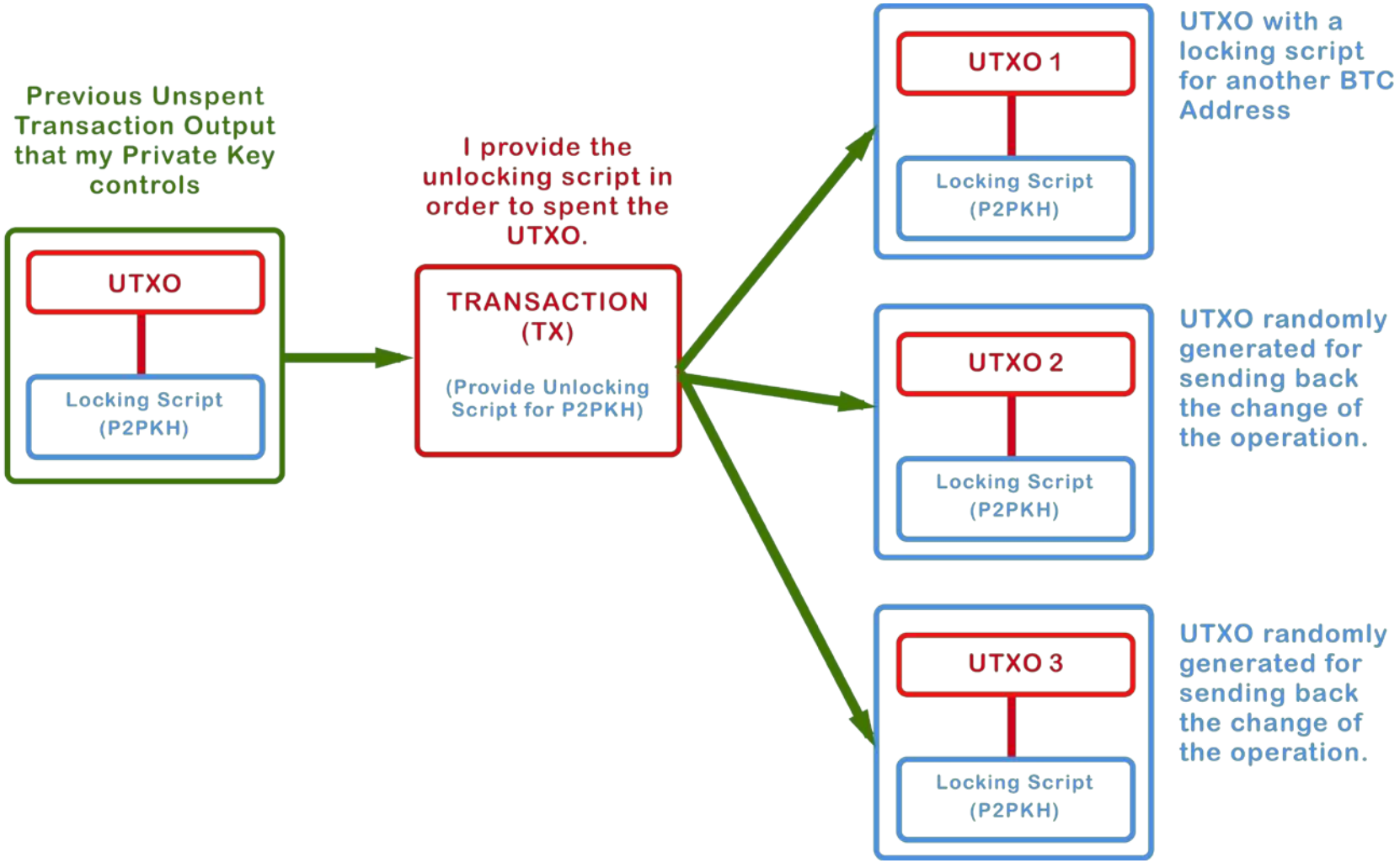
✝ **Have reverence for God, and obey his commands, because this is all that man was created for (Ecclesiastes 12:13)**

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)**

UTXO (Unspent Transaction Output)



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

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**

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