

Bitcoin

Part 1 – Network and Data Structure

Prof. Marco Comuzzi

Department of Industrial Engineering
Ulsan National Institute of Science and Technology (UNIST)
mcomuzzi@unist.ac.kr

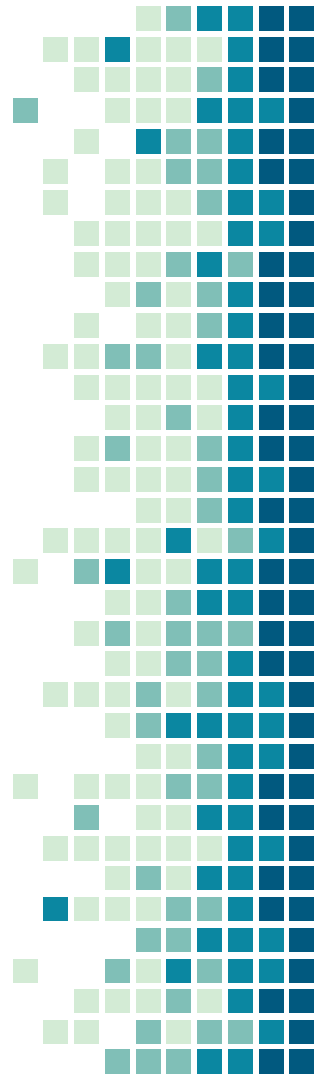
What is Bitcoin?

It is a public blockchain

It is a cryptocurrency: it is used by its users to record the exchange of digital “tokens”, denominated BTC

Conceptually, the “state” of the Bitcoin blockchain is given by the BTC balance of all its nodes (accounts)

White paper published at the end of 2008



Bitcoin: A Peer-to-Peer Electronic Cash System

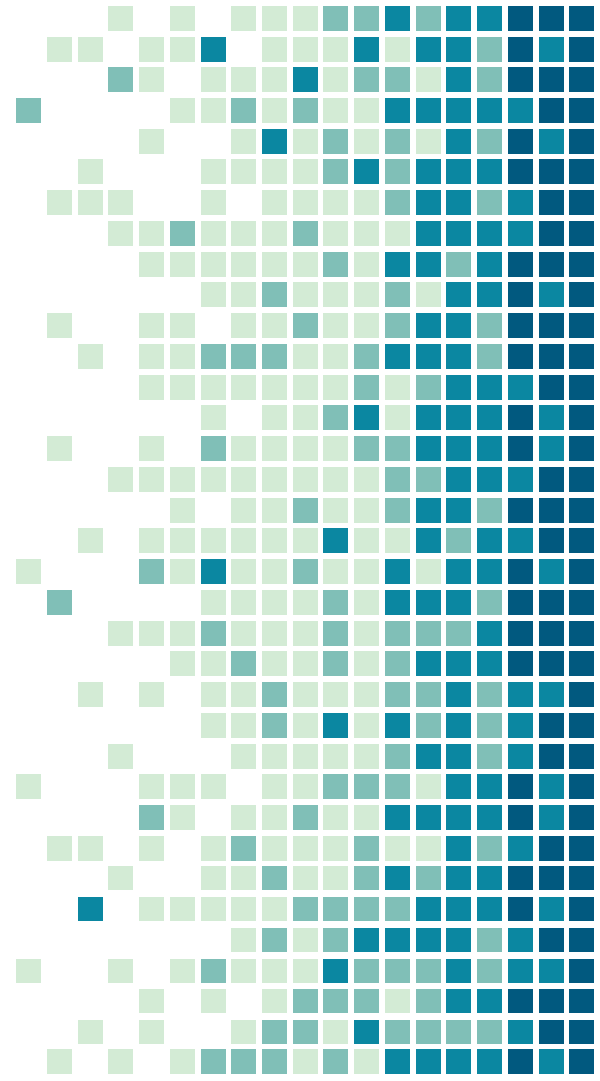
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

Introduction

1.

The Bitcoin Network

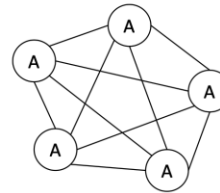


Bitcoin as a P2P Network

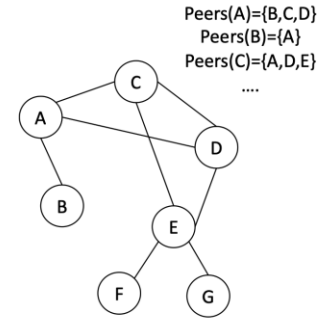
Bitcoin is a P2P network of computational nodes connected to the Internet

Anybody can download the Bitcoin client from <https://bitcoin.org> and run a Bitcoin node

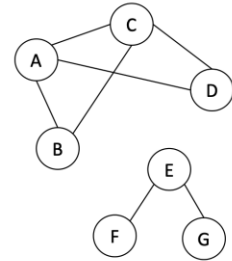
There exists also a Bitcoin “test” network, where BTC are “fake” (used for testing)



Fully connected graph



Connected graph
(Blockchain network)



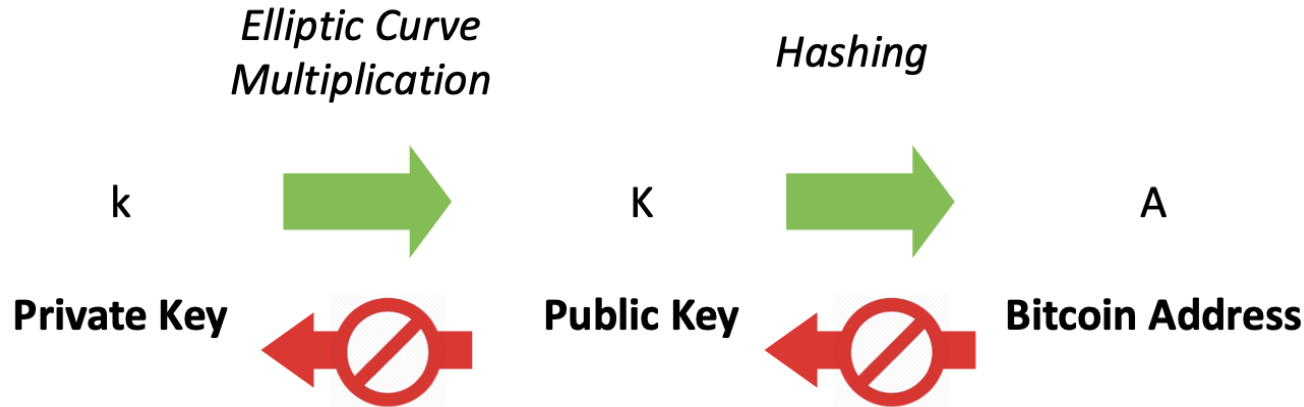
Disconnected graph

What is a Bitcoin address?

A node (account) in the Bitcoin network is associated with a unique private key, public key, and address.

A new account is initialized by creating a random private key.

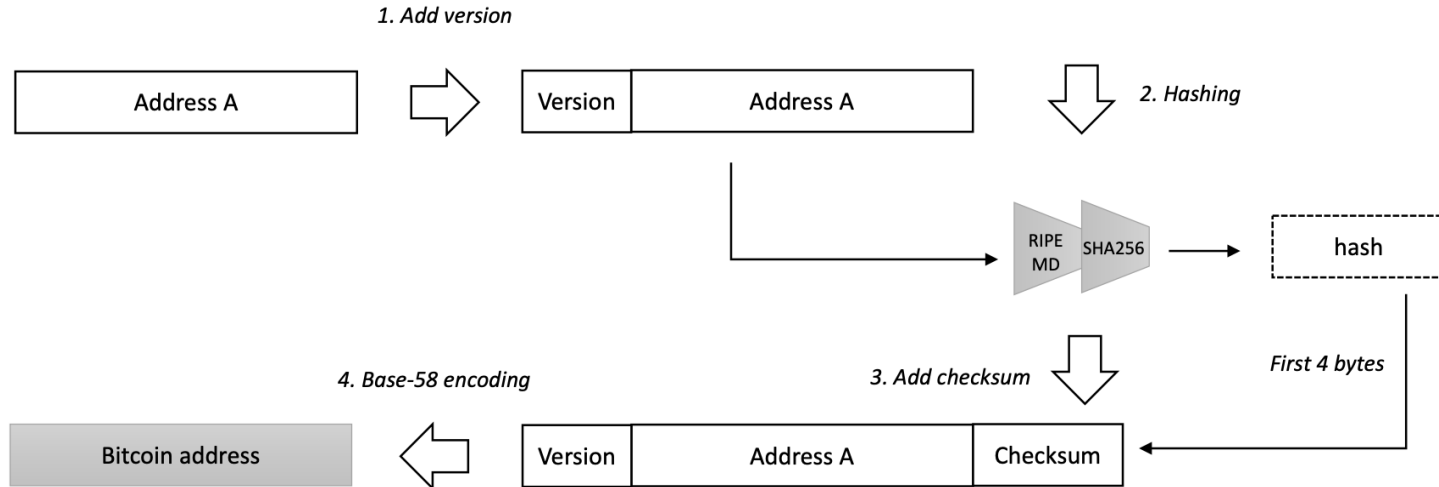
Private, public key and Bitcoin address are mathematically linked



Format of Bitcoin addresses

Addresses are obtained by encoding the hash of the public key using the Base58check encoding

Base58check is more human readable and can be easily verified, thanks to the checksum



Bitcoin Address

1FYdZfNwQjmHgoxzXVcUSK2XAXNg7MY4W2



Address 1FYdZfNwQjmHgoxzXVcUSK2XAXNg7MY4W2 has 1 transaction on the Bitcoin blockchain. Last balance change was 2022-09-28 13:02:38 GMT +9. It has received a total of 0.00265247 BTC and has sent a total of 0 BTC. The current balance of this address is 0.00265247 BTC.



Bitcoin Address

16Vmt96W4psGeUbqPLjzmCr9jKnTbxjNig

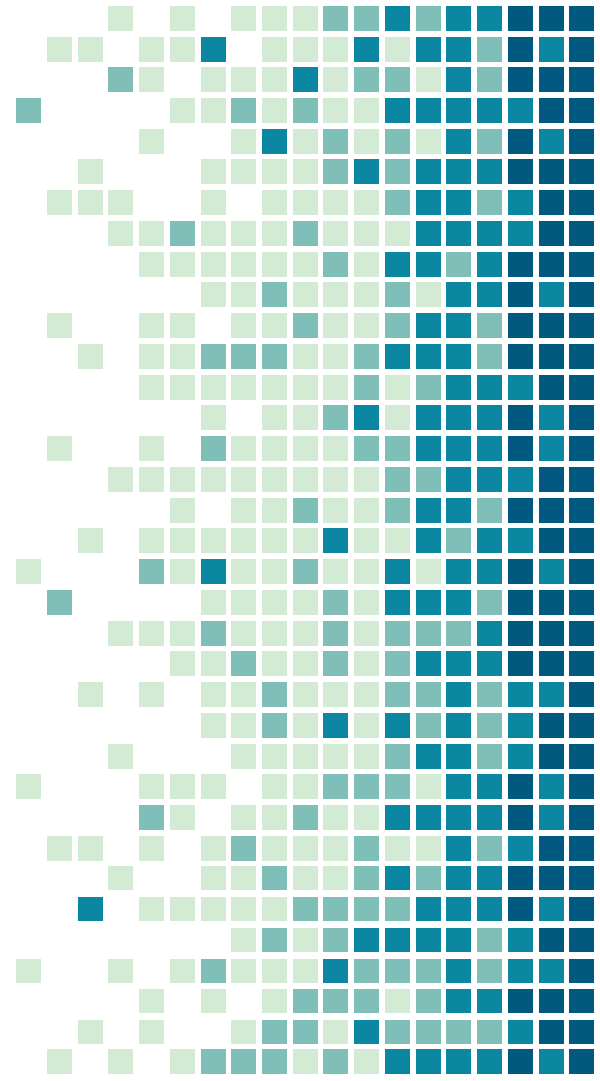


Address 16Vmt96W4psGeUbqPLjzmCr9jKnTbxjNig has 517 transactions on the Bitcoin blockchain. Last balance change was 2022-09-28 13:02:38 GMT +9. It has received a total of 940.82917105 BTC and has sent a total of 940.82917105 BTC. The current balance of this address is 0 BTC.



2.

Bitcoin Transactions and Ledger

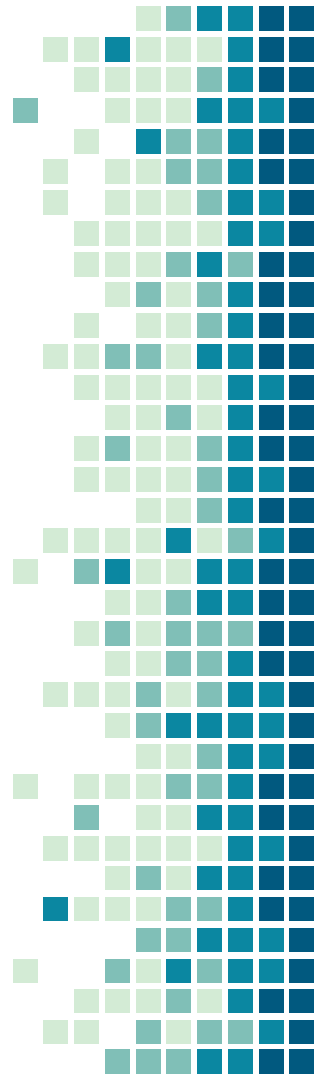


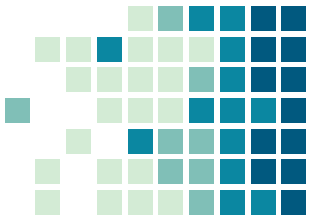
Transactions in Bitcoin

The state of the Bitcoin network is determined by the BTC balance of all nodes (conceptually)

The nodes of the Bitcoin network issue transactions

Transactions signify the exchange of BTC among nodes
(not only 1-to-1 exchange)





A Bitcoin transaction

Fee

0.00007874 BTC
(41.010 sat/B - 10.253 sat/WU - 192 bytes)

Hash

e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e

15TUAasp5G8k18gXBdJA7jdMvPEaPr2KxLx

0.11847874 BTC

1CTtPA5hCgtydSCMbcWWnNTfdTRLBm1rVG

0.11840000 BTC

0.11840000 BTC

2018-09-26 00:56

0.11840000 BTC

Details

Hash

e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e

Status

Confirmed

Received Time

2018-09-26 00:56

Size

192 bytes

Weight

768

Included in Block

543028

Confirmations

195,651

Total Input

0.11847874 BTC

Total Output

0.11840000 BTC

Fees

0.00007874 BTC



Another one...

Fee

0.00061812 BTC
(108.986 sat/B - 38.705 sat/WU - 562 bytes)
(154.530 sat/vByte - 400 virtual bytes)

Hash

578fa2731059bde959e2418903e2c717f81bc9bf883b10560fff9a66c3f20428

bc1q7cyrfmck2ffu2ud3m5i5a8yv6f0chkp0zpemf
bc1q7cyrfmck2ffu2ud3m5i5a8yv6f0chkp0zpemf

0.12912465 BTC
11.10650236 BTC

bc1qtj2n6d6k89ph9y5me6c3eyms2na3xwwdipd...
bc1qsucikyuuuffyq0cg2cjvt075hk92sglky3v44
15yQZN6LHWzkc7KHCPJV8dTAzhgRgBxbXn
36QH3zJgM6XqkdtUyzYvez6gg4yMe8Ce5U
bc1q4pf23addqat02jy9hx4syn3trmnv50suueywkf
3DV4FgWhrUTbKb18XPNjmdfO2EBL49y3s
bc1q7hwvq489wdphk772ha2g45qvmzkgp03stfpyt
bc1q7cyrfmck2ffu2ud3m5i5a8yv6f0chkp0zpemf

0.00940000 BTC
0.00810000 BTC
4.51802168 BTC
0.02494350 BTC
0.00479958 BTC
0.11250000 BTC
0.01400000 BTC
6.54324413 BTC

Details

Hash

578fa2731059bde959e2418903e2c717f81bc9bf883b10560fff9a66c3f20428

Status

Confirmed

Received Time

2022-05-31 15:31

Size

562 bytes

Weight

1,597

Included in Block

738680

Confirmations

6

Total Input

11.23562701 BTC

Total Output

11.23500889 BTC

Fee

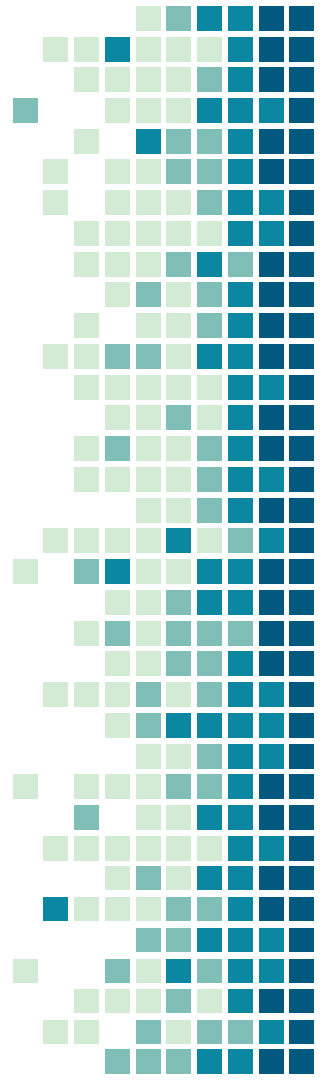
0.00061812 BTC

Bitcoin explorers and reality

Explorers make Bitcoin information easy to consult by anybody

To really understand how Bitcoin works, we need to look “under the hood”, that is, at the “machine-readable” representation of Bitcoin transactions

Here we study the “JSON” representation



```

{
  "txid": "e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e",
  "hash": "e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e",
  "version": 1,
  "size": 192,
  "vsize": 192,
  "weight": 768,
  "locktime": 0,
  "vin": [
    {
      "txid": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
      "vout": 1,
      "scriptSig": {
        "asm": "3045022100ea ( ",
        "hex": "483045022100ea( "
      },
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.1184,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 ( ",
        "hex": "76a9147dbf17155ee3019b0ca180ec0e8f9bdf43d5e4e88ac",
        "address": "1CTtPA5hCgtydSCMbcWWnNTfdTRLBm1rVG",
        "type": "pubkeyhash",
        "addresses": [
          "1CTtPA5hCgtydSCMbcWWnNTfdTRLBm1rVG"
        ],
        "reqSigs": 1
      }
    }
  ]
}

```

A “real” Bitcoin transaction

Fee	0.00007674 BTC (81.070 sat/B - 10.253 sat/WU - 192 bytes)	0.11840000 BTC
Hash	e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e	2018-09-26 00:58
	157c4up5D6k16g8baJk7ykmP6uH2KdLx	0.11847674 BTC
		1CTtPA5hCgtydSCMbcWWnNTfdTRLBm1rVG
		0.11840000 BTC
Details		
Hash	e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e	
Status	Confirmed	
Received Time	2018-09-26 00:58	
Size	192 bytes	
Weight	768	
Included in Block	543028	
Confirmations	195,851	
Total Input	0.11847674 BTC	
Total Output	0.11840000 BTC	
Fees	0.00007674 BTC	

```
{
  "txid": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
  "hash": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
  "version": 1,
  .(
  "vin": [
    {
      "txid": "785397b83f201e50db8154e93e5996bb698cfef20c10fb6ff1a63f46d3e51b31",
      "vout": 0,
      "scriptSig": {
        "asm": .( .
        "hex": -( . },
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01986368,
      "n": 0,
      "scriptPubKey": {
        (
        "address": "3FdkDy6xaKvaugDtCaEiXqXW6oDt5hw9NC",
        "type": "scripthash",
        ( .
      }
    },
    {
      "value": 0.11847874,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 30e1ffaddbf133ead74cb356b77c7698412e3817 OP_EQUALVERIFY OP_CHECKSIG",
        "hex": "76a91430e1ffaddbf133ead74cb356b77c7698412e381788ac",
        "address": "15TUAsp5G8k18gXBdJA7jdMvPEaPr2KxLx",
        "type": "pubkeyhash",
        "addresses": [
          "15TUAsp5G8k18gXBdJA7jdMvPEaPr2KxLx"
        ],
        "reqSigs": 1
      }
    }
  ]
}
```

Another one

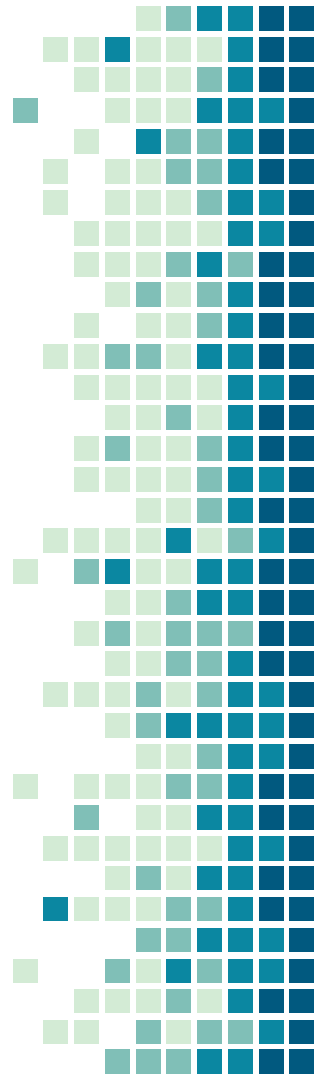
Bitcoin transactions

Transactions in Bitcoin "produce" transaction outputs

As input, a transaction consumes one or more outputs produced by other transactions

The sum (in BTC) of all transaction inputs must be greater than the sum (in BTC) of all the outputs

The difference (in BTC) between transaction inputs and outputs is the fee

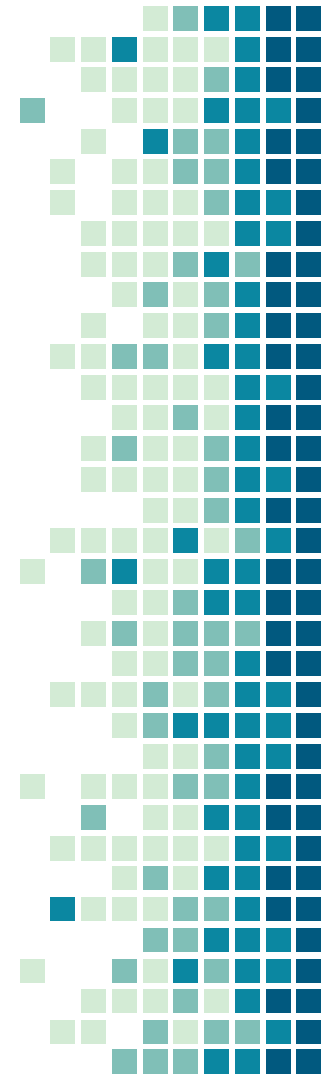


UTXOs

A UTXO (Unspent TX Output) is an output produced by a transaction and not yet used as input by any other transaction

A transaction can only use UTXOs as input

The state of the Bitcoin blockchain (= balance of all nodes) at a given time is fully determined by the list of UTXOs

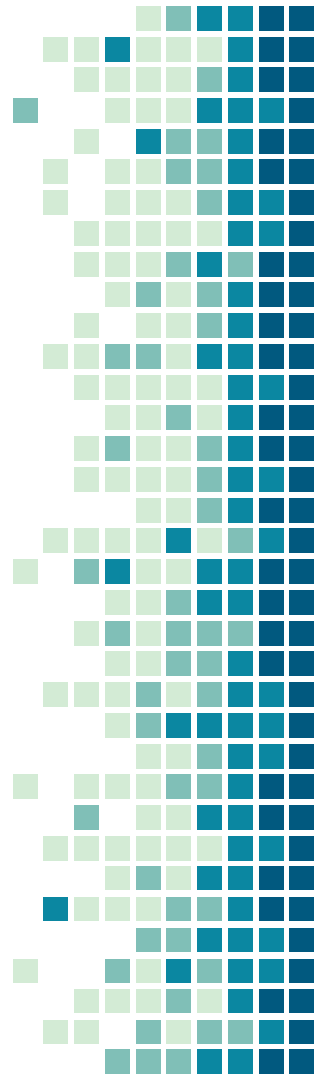


UTXOs as magic banknotes

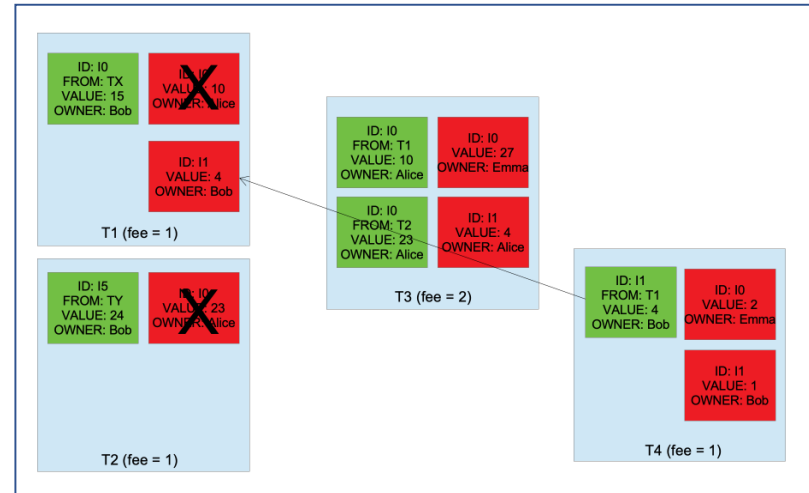
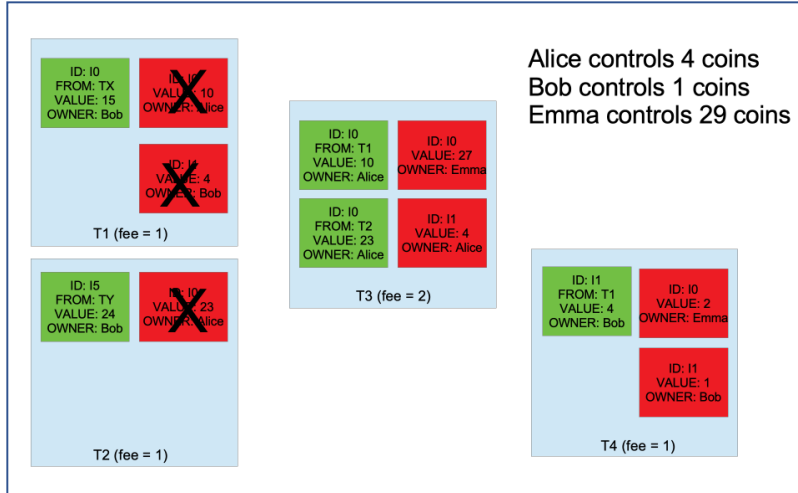
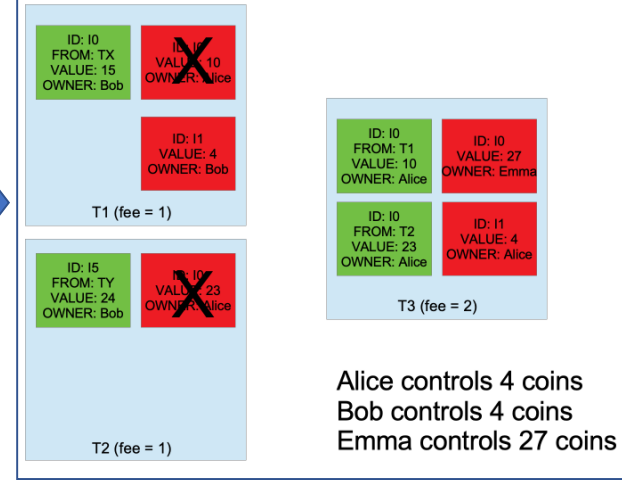
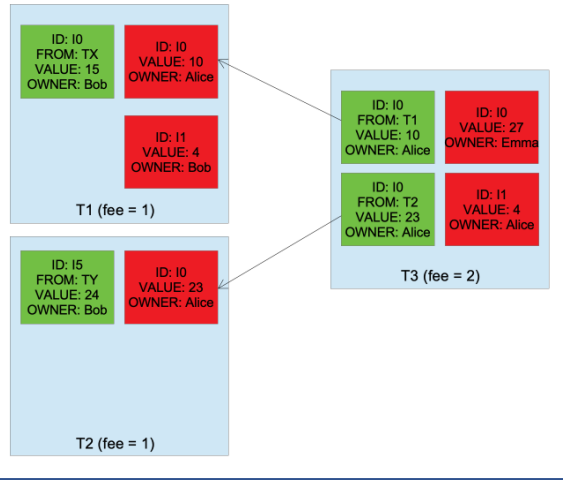
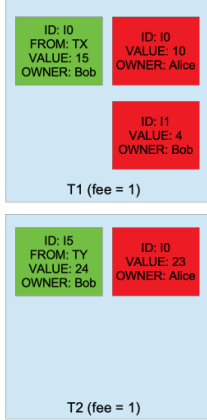
A UTXO controlled by a user (Alice) can be seen as a banknote owned by that user. For example, if Alice controls a UTXO valued 20 Bitcoins, it is like if she has a banknote worth 20 Bitcoins in her wallet.

Let us assume that Alice now wants to transfer 6 Bitcoins to Bob. Alice issues a new transaction that uses as input the 20 Bitcoins UTXO that she controls and produces two UTXOs as output: one controlled by Bob, valued 6 Bitcoins and one controlled again by Alice, valued 14 Bitcoins (actually a little less, because Alice also needs to pay a small fee!).

So, somehow, UTXOs are like magic banknotes that can be split by the owner into as many other banknotes as necessary.



Alice controls 33 coins
Bob controls 4 coins
(Emma controls 0 coins)



```

"result": {
  "txid": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
  "hash": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
  "version": 1,
  "size": 223,
  "vsize": 223,
  "locktime": 0,
  "vin": [
    {
      "txid": "785397b83f201e50db8154e93e5996bb698cfef20c10fb6ff1a63f46d3e51b31",
      "vout": 0,
      "scriptSig": {
        "asm": "3044022078efb490291a33b4c08783f7139de49444fc0e67c1fa20c4407
          hex": "473044022078efb490291a33b4c08783f7139de49444fc0e67c1fa20c44
        },
        "sequence": 4294967295
      },
      "value": 0.01986368,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 98f368618454272590d63e430898d53fdaeb3573 OP_EQUA
          hex": "a91498f368618454272590d63e430898d53fdaeb357387",
          reqSigs": 1,
          type": "scripthash",
          addresses": [
            "3FdkDy6xaKvaugDtCaF4XqXW6oDt5hw9NC"
          ]
        },
        "value": 0.11847874,
        "n": 1,
        "scriptPubKey": {
          "asm": "OP_DUP OP_HASH160 30e1ffadbbf133ead74cb356b77c7698412e3817
            hex": "76a91430e1ffadbbf133ead74cb356b77c7698412e381788ac",
            reqSigs": 1,
            type": "pubkeyhash",
            addresses": [
              "15TUA5p5G8k18gXBdJA7jdMvPeaPr2KxLx"
            ]
          }
        }
      ],
      "vout": [
        {
          "value": 0.11840000,
          "n": 0,
          "scriptPubKey": {
            "asm": "OP_DUP OP_HASH160 7dbf17155ee3019b0ca180ec
              hex": "76a9147dbf17155ee3019b0ca180ec0e8f9bdfdf43d
              reqSigs": 1,
              type": "pubkeyhash",
              addresses": [
                "1CTtPA5hCgtydSCMbcWwNNTfdTRLBm1rVG"
              ]
            }
          }
        ],
        "hex": "01000000155f4955c00b192ce9aeaa71420314b5659d7a0865609a7f6e40a1c88
          blockhash": "000000000000000000000000a318feb2fc7c2c9dc43c2d1de1606bb5f0cc6dc1
          confirmations": 19915,
          time": 1537890970,
          blocktime": 1537890970
        },
        "error": null,
        "id": null
      }
    }
  ]
}

```

```

"result": {
  "txid": "e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e",
  "hash": "e27824e8c9a8f2fdd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e",
  "version": 1,
  "size": 192,
  "vsize": 192,
  "locktime": 0,
  "vin": [
    {
      "txid": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ac
      vout": 1,
      "scriptSig": {
        "asm": "3045022100ea2f8df5a63197a1a521408d3839cc78
          hex": "483045022100ea2f8df5a63197a1a521408d3839cc
        },
        "sequence": 4294967295
      },
      "value": 0.11840000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 7dbf17155ee3019b0ca180ec
          hex": "76a9147dbf17155ee3019b0ca180ec0e8f9bdfdf43d
          reqSigs": 1,
          type": "pubkeyhash",
          addresses": [
            "1CTtPA5hCgtydSCMbcWwNNTfdTRLBm1rVG"
          ]
        },
        "hex": "01000000155f4955c00b192ce9aeaa71420314b5659d7a0865609a7f6e40a1c88
          blockhash": "000000000000000000000000a318feb2fc7c2c9dc43c2d1de1606bb5f0cc6dc1
          confirmations": 19915,
          time": 1537890970,
          blocktime": 1537890970
        },
        "error": null,
        "id": null
      }
    }
  ]
}

```

Digital signature of Bitcoin transactions

<https://www.blockchain.com/btc/tx/15ce5e5b522519b6bc931472ef93ccf1c051b477b81fc0240088237e50fcd42>

A Bitcoin transaction can also capture a N-to-M Bitcoin exchange

Fee 0.00003281 BTC
(4.026 sat/B - 1.006 sat/WU - 815 bytes)

Hash 15ce5e5b522519b6bc931472ef93ccf1c051b477b81fc0240088...

15ce5e5b522519b6bc931472ef93ccf1c051b477b81fc0240088237e50fcd42
1PGfB81fc0240088237e50fcd42
19sGjJHKGdD21c5qQgm1Q6MBwKyC5nMZ
1KDufTC9mAgxsLxCt7chu9qPF45NMkxmQW
1NHv6qBxu6haWj8rqeLqw9eyJqm4JT26R6
1DHKUjABQyVvkq6d4r2MJ9CCbimL4wibZPd

0.00089505 BTC
0.00009047 BTC
1.50000000 BTC
1.98833513 BTC
0.11905417 BTC

3NcwtFUNsigvGUMyBtMKmmNmBoA5Wm4QRP
1NDyJtNTjmwk5xPNhjqAMu4HDHigtobu1s

0.00996722 BTC
3.59837479 BTC

3.60834201 BTC

2021-10-19 23:30

How can these transactions be digitally signed?

There would be one originator who issued the transaction, but the BTCs moved around are from multiple nodes...

Digital signature of Bitcoin transactions

Originators do not sign transactions
(actually, it does not really matter who the originator is!)

Transactions inputs/outputs are digitally signed by their owners

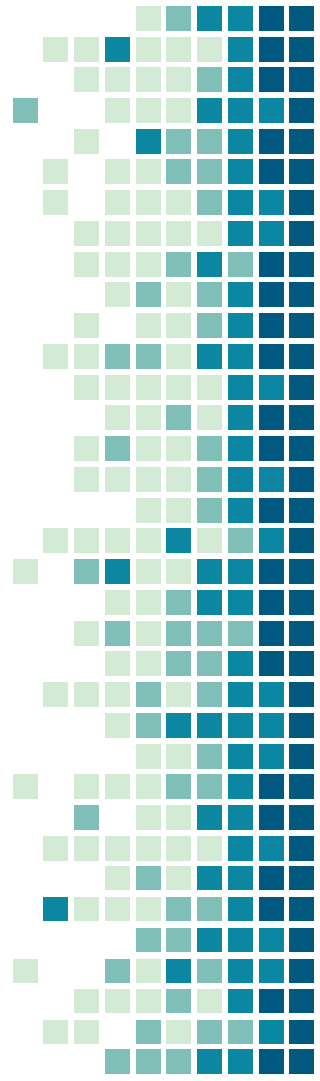
Digital signature of UTXOs

Transaction outputs (UTXOs) are “locked” by the owner using a cryptographic puzzle

A solution of the puzzle can only be given using the private key of the owner.

The solution of the puzzle must be given in order to use a UTXO as input of another transaction

Any other node can verify the correctness of a solution provided using an input's owner public key (when “validating” a transaction)



```

"result": {
  "txid": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
  "hash": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
  "version": 1,
  "size": 223,
  "vsize": 223,
  "locktime": 0,
  "vin": [
    {
      "txid": "785397b83f201e50db8154e93e5996bb698cfef20c10fb6ff1a63f46d3e51b31",
      "vout": 0,
      "scriptSig": {
        "asm": "3044022078efb490291a33b4c08783f7139de49444fc0e67c1fa20c4407",
        "hex": "473044022078efb490291a33b4c08783f7139de49444fc0e67c1fa20c44",
        "sequence": 4294967295
      },
      "value": 0.01986368,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 98f368618454272590d63e430898d53fdaeb3573 OP_EQUAL",
        "hex": "a91498f368618454272590d63e430898d53fdaeb357387",
        "reqSigs": 1,
        "type": "scripthash",
        "addresses": [
          "3FdkDy6xaKvaugDtCaF4xqXW6oDt5hw9NC"
        ]
      }
    },
    {
      "value": 0.11847874,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 30e1ffadbbf133ead74cb356b77c7698412e3817",
        "hex": "76a91430e1ffadbbf133ead74cb356b77c7698412e381788ac",
        "reqSigs": 1,
        "type": "pubkeyhash",
        "addresses": [
          "15TUA5p5G8k18gXBdJA7jdMvPEaPr2KxLx"
        ]
      }
    }
  ],
  "vout": [
    {
      "value": 0.11840000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 7dbf17155ee3019b0ca180ec",
        "hex": "76a9147dbf17155ee3019b0ca180ec0e8f9bdfdf43d",
        "reqSigs": 1,
        "type": "pubkeyhash",
        "addresses": [
          "1CTtPA5hCgtydSCMbcWnNTfdTRLBm1rVG"
        ]
      }
    },
    {
      "hex": "010000000155f4955c00b192ce9aeaa71420314b5659d7a0865609a7f6e40a1c88",
      "blockhash": "000000000000000000000000a318feb2fc7c2c9dc43c2d1de1606bb5f0cc6dc1",
      "confirmations": 19915,
      "time": 1537890970,
      "blocktime": 1537890970
    }
  ],
  "error": null,
  "id": null
}

```

CRYPTO PUZZLE

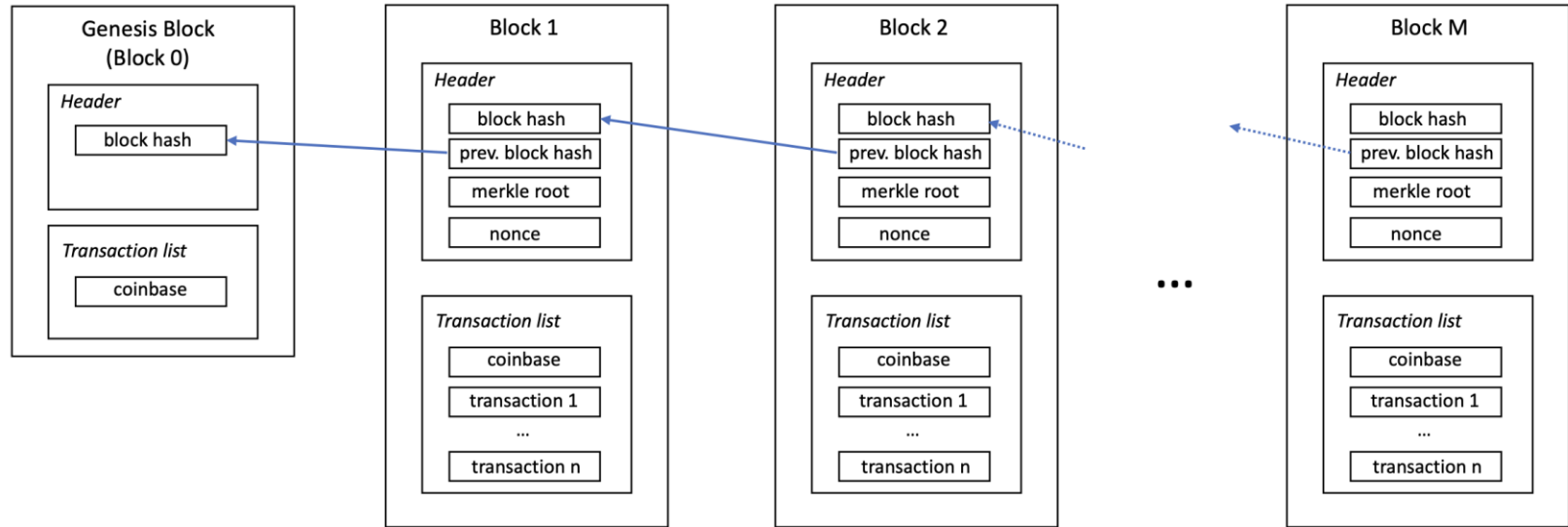
```

"result": {
  "txid": "e27824e8c9a8f2f1dd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e",
  "hash": "e27824e8c9a8f2f1dd4c731c13ea6a057b21d5940a4d0b85473431d10ce6aea9e",
  "version": 1,
  "size": 192,
  "vsize": 192,
  "locktime": 0,
  "vin": [
    {
      "txid": "1d09a97d881c0ae4f6a7095686a0d759564b312014a7ea9ace92b1005c95f455",
      "vout": 1,
      "scriptSig": {
        "asm": "3045022100ea2f8df5a63197a1a521408d3839cc73",
        "hex": "483045022100ea2f8df5a63197a1a521408d3839cc",
        "sequence": 4294967295
      },
      "value": 0.11840000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 7dbf17155ee3019b0ca180ec",
        "hex": "76a9147dbf17155ee3019b0ca180ec0e8f9bdfdf43d",
        "reqSigs": 1,
        "type": "pubkeyhash",
        "addresses": [
          "1CTtPA5hCgtydSCMbcWnNTfdTRLBm1rVG"
        ]
      }
    },
    {
      "hex": "010000000155f4955c00b192ce9aeaa71420314b5659d7a0865609a7f6e40a1c88",
      "blockhash": "000000000000000000000000a318feb2fc7c2c9dc43c2d1de1606bb5f0cc6dc1",
      "confirmations": 19915,
      "time": 1537890970,
      "blocktime": 1537890970
    }
  ],
  "error": null,
  "id": null
}

```

CRYPTO PUZZLE SOLUTION

The Bitcoin Ledger



Header: metadata about a block, including hashes

Transaction list, including the “coinbase” transaction

Header of a block

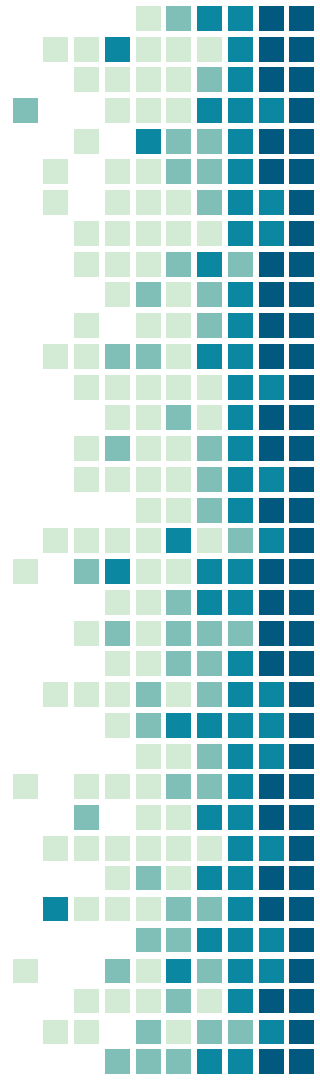
Hash of the block: SHA256 hash of the content of the block, also used as a unique id of the block.

Block height: a progressive number identifying the block. The genesis block has height equal to 0.

Hash of the previous block: including the hash of the previous block in a block guarantees the immutability of the blockchain ledger.

Merkle root: this value is calculated based on the data structure in which the transactions belonging to a block are stored. We do not discuss this aspect of the Bitcoin blockchain in detail in this course. It is important to quickly verify whether a given transaction (identified by its unique id) belongs or not to a block.

Nonce: an integer number. The value of this integer number is set by the 'block mining' process (consensus mechanism). From the point of view of the functioning of the Bitcoin blockchain (i.e., transfers of tokens and state updates), it has no particular meaning.




Block 738656 ⓘ

This block was mined on May 31, 2022 at 11:30 AM GMT+9 by [ViaBTC](#). It currently has 293 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC (\$185,486.63). The reward consisted of a base reward of 6.25000000 BTC (\$185,486.63) with an additional 0.15852069 BTC (\$4,704.55) reward paid as fees of the 1758 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this [address](#).

A total of 43,268.81283562 BTC (\$1,284,125,769.70) were sent in the block with the average transaction being 24.61252152 BTC (\$730,446.97). Learn more about [how blocks work](#).

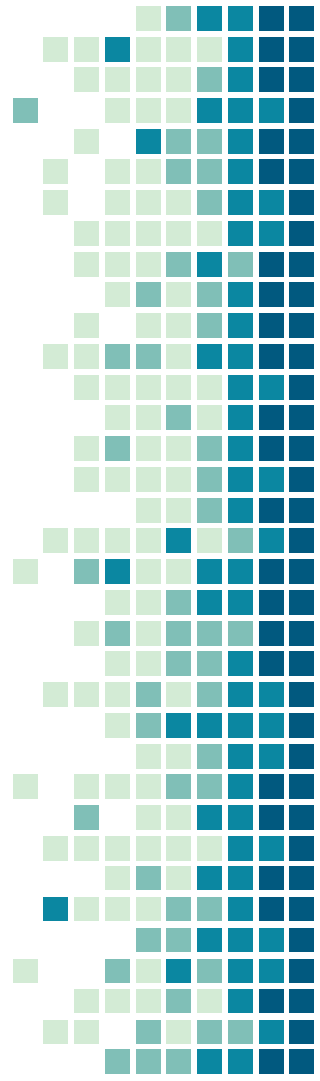
Hash	000000000000000000073ef06543252dce1cc24c9e31a6d6848d892ffc824f71 
Confirmations	293
Timestamp	2022-05-31 11:30
Height	738656
Miner	ViaBTC
Number of Transactions	1,758
Difficulty	29,897,409,688,833.63
Merkle root	0aa51c8d448e8e9e9264449f0a387be3049e69673e9645c79de4b8293ab0fdad
Version	0x20000000
Bits	386,492,960
Weight	3,993,422 WU
Size	1,324,859 bytes
Nonce	1,440,543,490
Transaction Volume	43268.81283562 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.15852069 BTC

<https://www.blockchain.com/btc/block/000000000000000000073ef06543252dce1cc24c9e31a6d6848d892ffc824f71>

List of transactions

A Bitcoin block contains a variable number of transactions (few thousands)

The first transaction in every block is a special one, called “coinbase”



Summary ⓘ

USD

BTC

Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 318 bytes) (0.000 sat/vByte - 291 virtual bytes)	6.40852069 BTC
Hash	bf9a1aca668b4e825a5434605afee7d74a1479eb082e592294e4793c6d223474 	2022-05-31 11:30
COINBASE (Newly Generated Coins) 		18cBEMRxXHqzWWCzZntU91F5sbUNKhL5PX
		6.40852069 BTC 

Details ⓘ

Hash	bf9a1aca668b4e825a5434605afee7d74a1479eb082e592294e4793c6d223474
Status	Confirmed
Received Time	2022-05-31 11:30
Size	318 bytes
Weight	1,164
Included in Block	738656
Confirmations	293
Total Input	0.00000000 BTC
Total Output	6.40852069 BTC
Fees	0.00000000 BTC

A coinbase
transaction

<https://www.blockchain.com/btc/tx/bf9a1aca668b4e825a5434605afee7d74a1479eb082e592294e4793c6d223474>

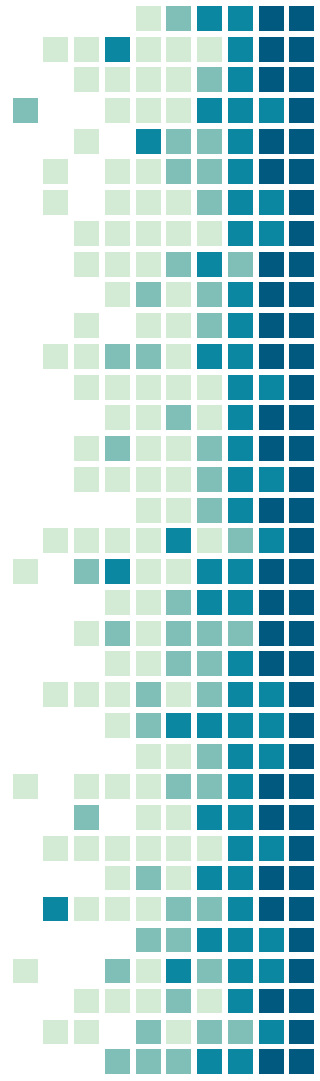
Coinbase transaction

It does not have any input

It has one output equal to
[sum of all the fees of transactions in the block + fixed reward],
controlled by the miner of the block

Fixed reward today: 6.25 BTC per block (>> fees)

Basically, it creates “new” BTCs to reward the miner node
(more about this later...)



Bitcoin halving

The coinbase fixed reward halves every 210,000 blocks (~4 years)

Most recent halving: Spring 2020

Next halving: some time in 2024

Last halving: some time around 2140
At that time, the number of Bitcoins will be 21 million, no more Bitcoins will be created.

First halving

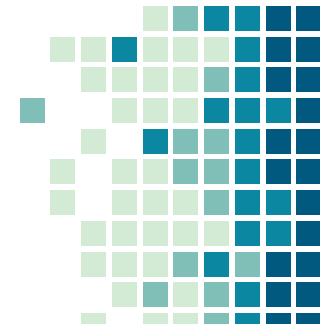
Date	28 November 2012
Block number	210,000
Block reward, BTC	25
BTC created per day	3600
BTC price at the start	\$12
BTC price 100 days later	\$42
BTC price 1 year later	\$964

Second halving

Date	9 July 2016
Block number	420,000
Block reward, BTC	12.5
BTC created per day	1,800
BTC price at the start	\$663
BTC price 100 days later	\$609
BTC price 1 year later	\$2550

Third halving

Date	11 May 2020
Block number	630,000
Block reward, BTC	6.25
BTC created per day	900
BTC price at the start	\$8740
BTC price 100 days later	\$11,950
BTC price 1 year later	N/A



This block was mined on January 04, 2009 at 3:15 AM GMT+9 by Unknown. It currently has 738,953 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 50.00000000 BTC (\$1,491,378.50). The reward consisted of a base reward of 50.00000000 BTC (\$1,491,378.50) with an additional 0.00000000 BTC (\$0.00) reward paid as fees of the 1 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 0.00000000 BTC (\$0.00) were sent in the block with the average transaction being 0.00000000 BTC (\$0.00). [Learn more about how blocks work.](#)

Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f 
Confirmations	738,953
Timestamp	2009-01-04 03:15
Height	0 https://www.blockchain.com/btc/block/0
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Version	0x1
Bits	486,604,799
Weight	1,140 WU
Size	285 bytes

Block Transactions ⓘ

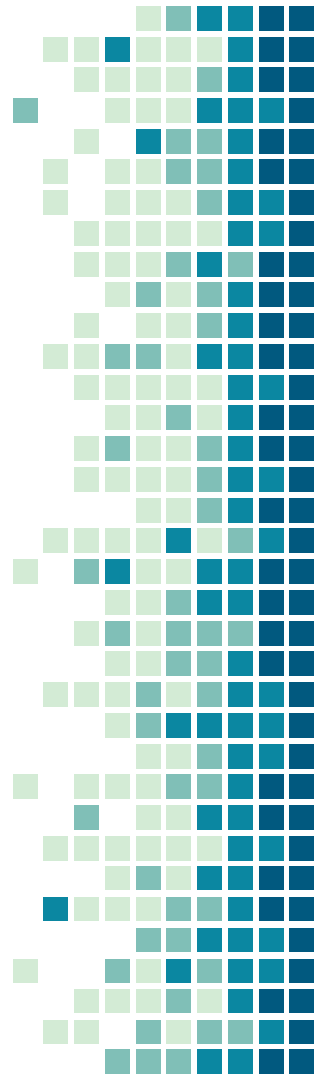
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 204 bytes)	50.00000000 BTC
Hash	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b	2009-01-04 03:15
	COINBASE (Newly Generated Coins)	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa 50.00000000 BTC 

Genesis block

Created on January 4th, 2009

Contained only 1 coinbase transactions

Awarded the first 50 BTC ever minted to the account "1A1zP..."



THANKS!

<https://sites.google.com/site/marcocomuzzi-phd>

<http://iel.unist.ac.kr/>

You can find me at:

@dr_bsad

mcomuzzi@unist.ac.kr