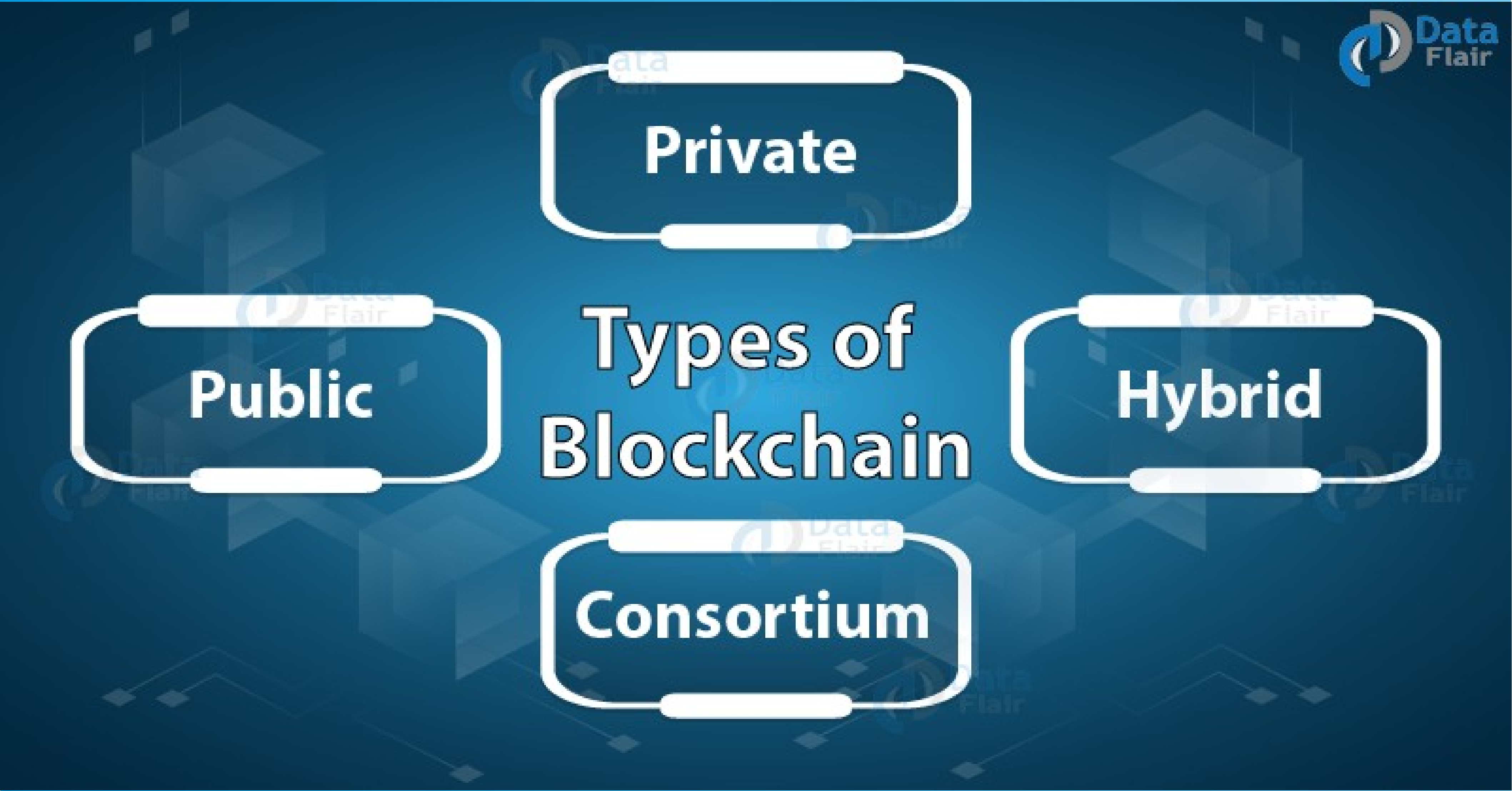
Blockchain Fundamentals Part 2

Types of Blockchain, Blocks, Transactions



Types of Blockchain

Private

Public

Hybrid

Consortium

Public and Private Blockchains

- **Public Blockchains**

A Public Blockchain is a permissionless blockchain. Anyone can join the blockchain network, meaning that they can read, write, or participate with a public blockchain. Public blockchains are decentralised, no one has control over the network, and they are secure in that the data can’t be changed once validated on the blockchain.

- Anonymous
- Total Transparent
- Secure
- Examples – Ethereum, Bitcoin

Cons

Usually uses POW

Problems with scalability

Energy Inefficient

Public and Private Blockchains

- **Private Blockchains**

A Private Blockchain is a permissioned blockchain.

Permissioned networks place restrictions on who is allowed to participate in the network and in what transactions.

- Anonymous
- More scalable
- More Efficient in cost
- Can use exotic consensus alg

- Cons
- Lack of trust
- Security
- Centralized

Examples – Hyperledger, Quorum

Public and Private Blockchains

A public network is more secure due to decentralization and active participation. Due to the higher number of nodes in the network, it is nearly impossible for ‘bad actors’ to attack the system and gain control over the consensus network.

In a private blockchain, there is no chance of minor collision. Each validator is known and they have the suitable credentials to be a part of the network. But in a public blockchain, no one knows who each validator is and this increases the risk of potential collusion or a 51% attack

Both function as an append-only ledger where the records can be added but cannot be altered or deleted. Hence, these are called immutable records.

Hybrid Blockchains

- Hybrid Blockchains

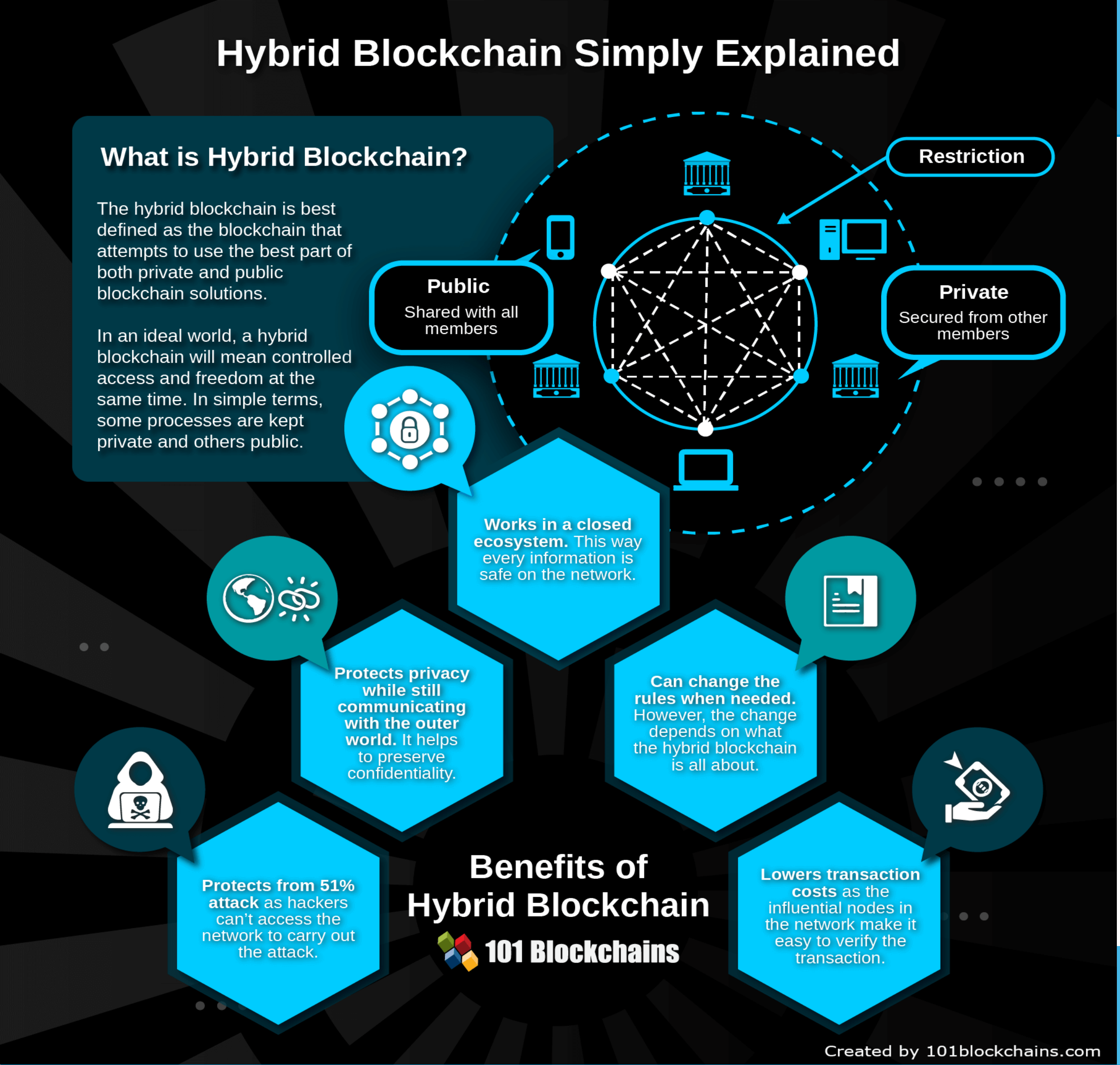
They combines the privacy benefits of a permissioned and private blockchain with the security and transparency benefits of a public blockchain. That gives businesses significant flexibility to choose what data they want to make public and transparent and what data they want to keep private.

Uses of Hybrid Blockchains:

IoT - The internet of things can be a tricky thing to manage with complete public blockchain solution as it will give hackers free data to map nodes or even hack into them.

Supply Chains – IBM Food Trust - https://www.ibm.com/blockchain/solutions/food-trust

Governments



Hybrid Blockchain Simply Explained

What is Hybrid Blockchain?

The hybrid blockchain is best defined as the blockchain that attempts to use the best part of both private and public blockchain solutions.

In an ideal world, a hybrid blockchain will mean controlled access and freedom at the same time. In simple terms, some processes are kept private and others public.

Works in a closed ecosystem. This way every information is safe on the network.

Protects privacy while still communicating with the outer world. It helps to preserve confidentiality.

Can change the rules when needed. However, the change depends on what the hybrid blockchain is all about.

Protects from 51% attack as hackers can't access the network to carry out the attack.

Benefits of Hybrid Blockchain

101 Blockchains

Lowers transaction costs as the influential nodes in the network make it easy to verify the transaction.

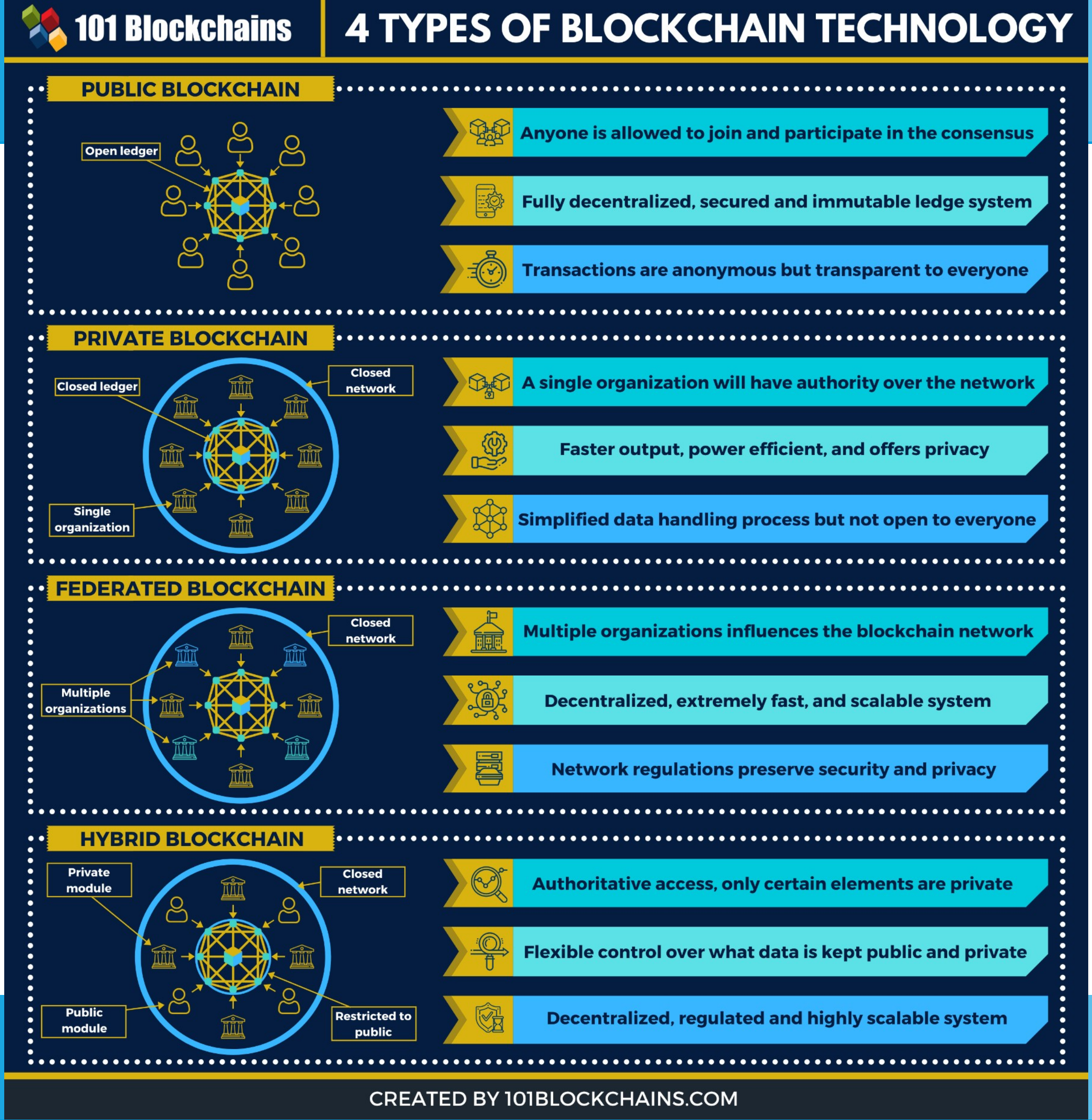
Created by 101blockchains.com

Consortium (Federated) Blockchain

A consortium blockchain is a semi-decentralized type where more than one organization manages a blockchain network. This is contrary to what we saw in a private blockchain, which is managed by only a single organization. More than one organization can act as a node in this type of blockchain and exchange information or do mining. Consortium blockchains are typically used by banks, government organizations, etc.

Examples of consortium blockchain are; Energy Web Foundation, R3, etc.

Explain R3 Corda States



101 Blockchains

4 TYPES OF BLOCKCHAIN TECHNOLOGY

PUBLIC BLOCKCHAIN

Open ledger

- Anyone is allowed to join and participate in the consensus
- Fully decentralized, secured and immutable ledge system
- Transactions are anonymous but transparent to everyone

PRIVATE BLOCKCHAIN

Closed ledger

Closed network

Single organization

- A single organization will have authority over the network
- Faster output, power efficient, and offers privacy
- Simplified data handling process but not open to everyone

FEDERATED BLOCKCHAIN

Closed network

Multiple organizations

- Multiple organizations influences the blockchain network
- Decentralized, extremely fast, and scalable system
- Network regulations preserve security and privacy

HYBRID BLOCKCHAIN

Private module

Closed network

Public module

Restricted to public

- Authoritative access, only certain elements are private
- Flexible control over what data is kept public and private
- Decentralized, regulated and highly scalable system

CREATED BY 101BLOCKCHAINS.COM

Blockchain Blocks Definition

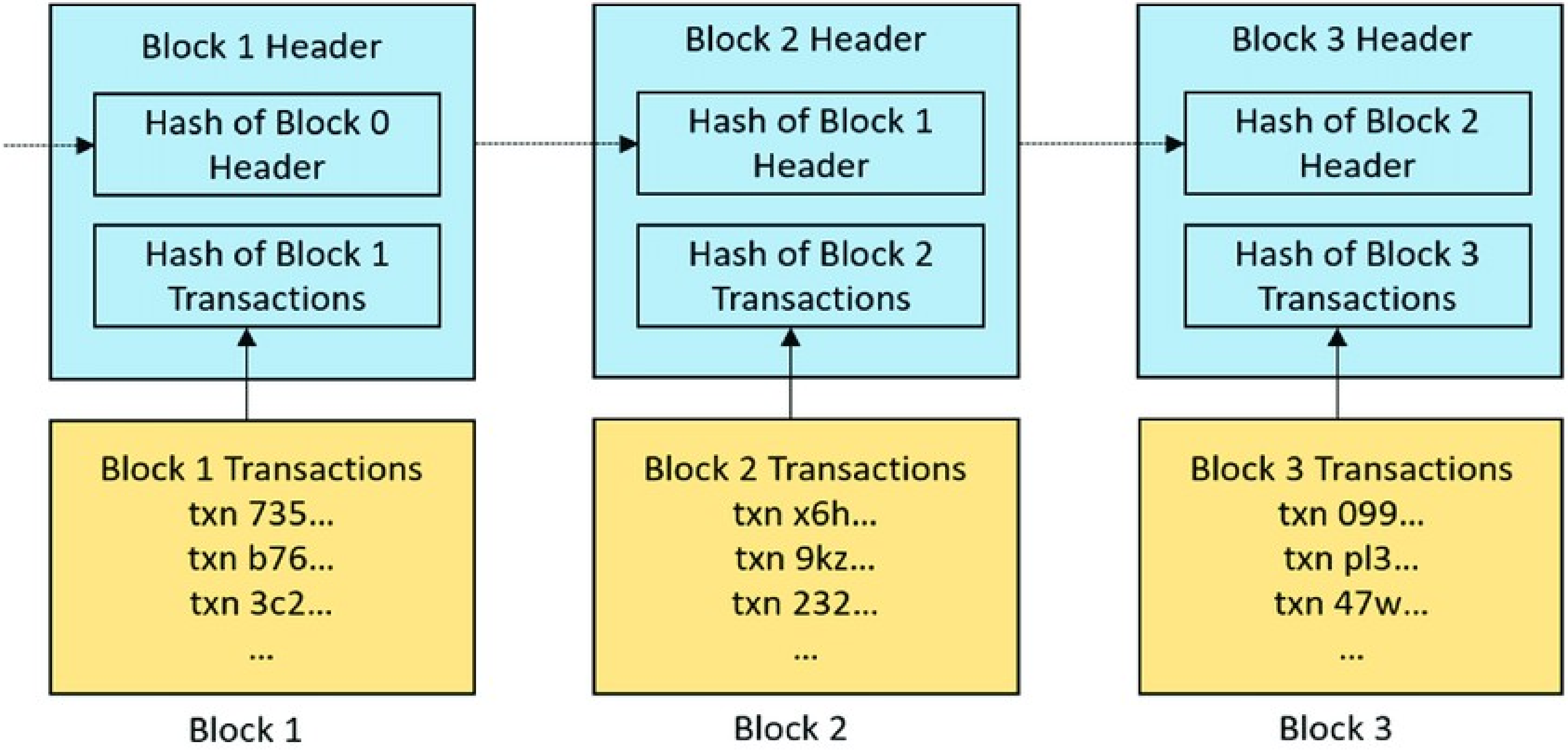
What is a Blockchain Block ?

A block is a container data structure, which brings together transactions for inclusion in the public ledger, known as the blockchain. The block is made up of a header; containing metadata, followed by a long list of transactions. A block can be identified in two ways, either by referencing the block hash, or through referencing the block height.

Blocks

- Blocks are the constructive part of the Blockchain
- The transaction information that consist in blocks forms the Blockchain Ledger
- Block has Header and a Body (List of transactions)
- Blocks has Height – the number of the block chronologically in the Blockchain
- Block has Reward – the amount of cryptocurrency issued to the miner / validator of the block

Scheme of Block



Block 1 Header

Hash of Block 0 Header

Hash of Block 1 Transactions

Block 1 Transactions
txn 735...
txn b76...
txn 3c2...
...

Block 1

Block 2 Header

Hash of Block 1 Header

Hash of Block 2 Transactions

Block 2 Transactions
txn x6h...
txn 9kz...
txn 232...
...

Block 2

Block 3 Header

Hash of Block 2 Header

Hash of Block 3 Transactions

Block 3 Transactions
txn 099...
txn pl3...
txn 47w...
...

Block 3

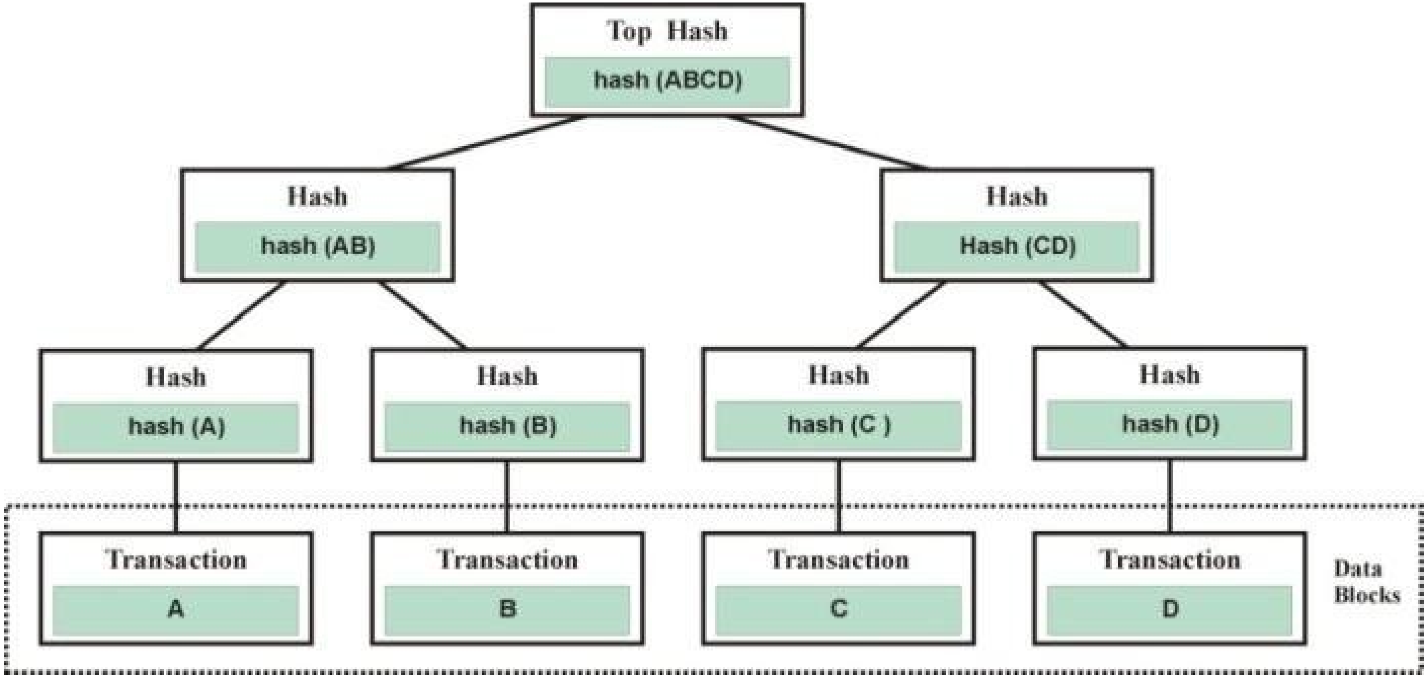
Blocks’s structure

Block header information

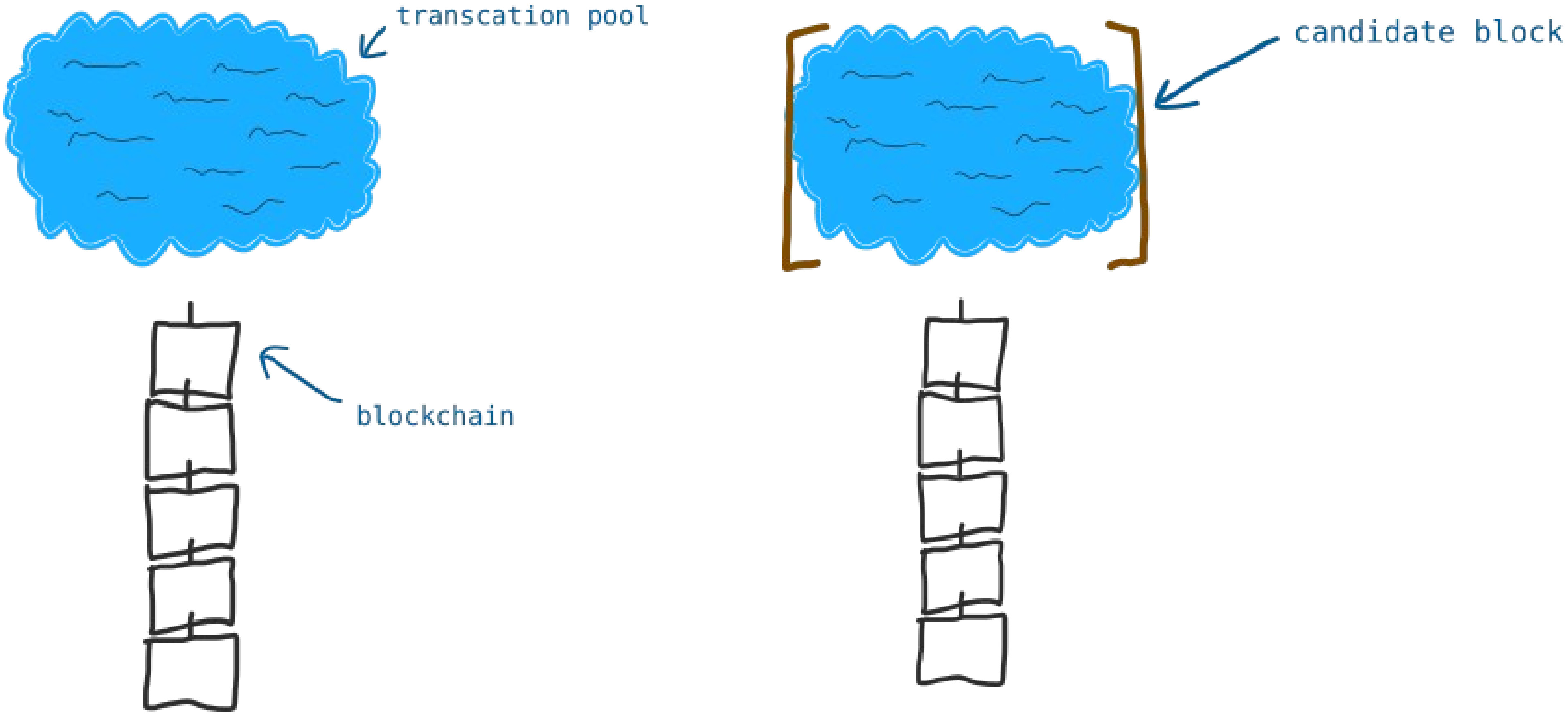
- Version – version number to track software / protocol upgrades
- Previous Block Hash – reference to the previous (parent) block in the chain
- Merkle Root – result of the Merkle-Tree of this block’s transaction
- TimeStamp
- Difficulty Target (Target Hash) – POW difficulty target for this block
- Nonce – number only used once (the result required from the POW algorithm)

Merkel Tree

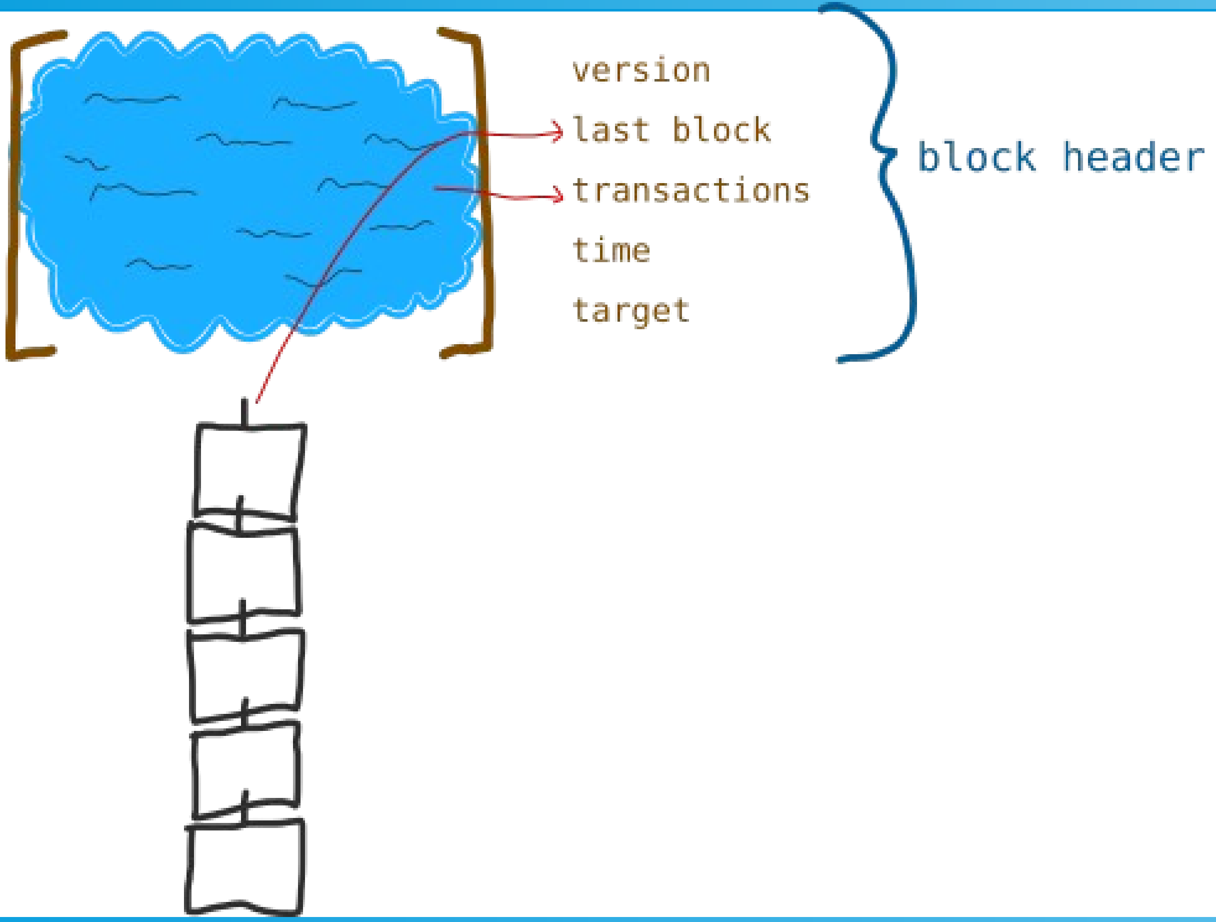
- All the transactions in the block are hashed by the Merkel Tree algoritm
- The final result of the hash is keeped in the block's header



How Blocks are formed



Forming candidate block



version

last block

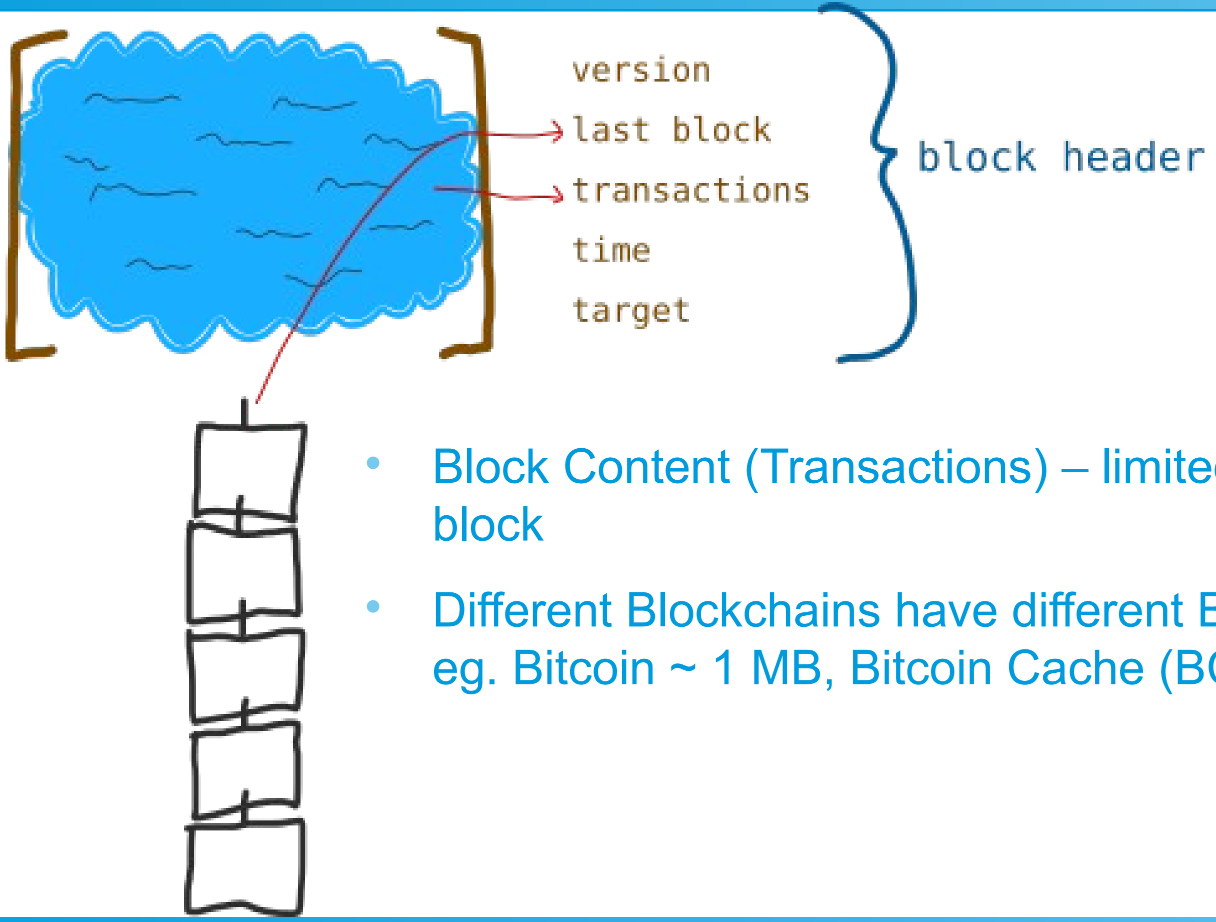
transactions

time

target

block header

Forming candidate block



- Block Content (Transactions) – limited by the size of the block
- Different Blockchains have different Block sizes – eg. Bitcoin ~ 1 MB, Bitcoin Cache (BCH) – 8 MB

Validating the new Block

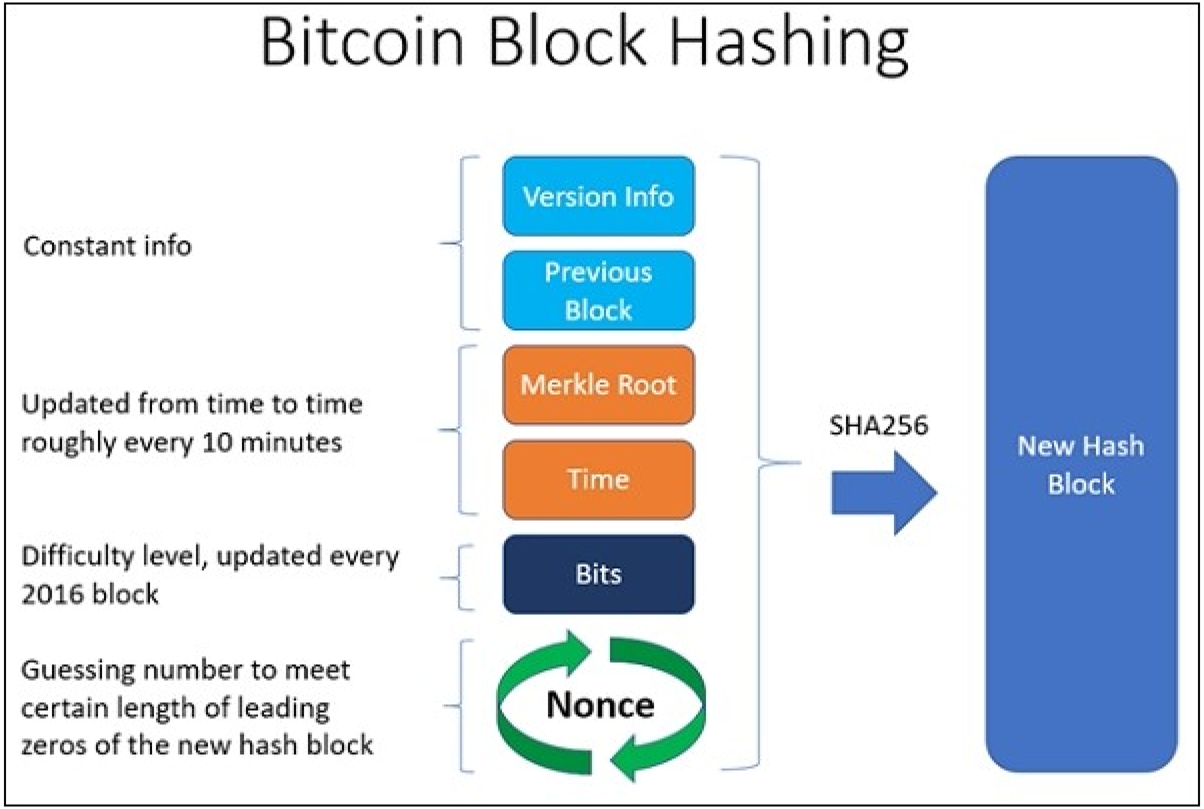
- What is Nonce ?

Number only used once. Nonce is the central part of this Proof of Work. The Nonce is a random whole number, which is a 32-bit (4 byte) field, which is adjusted by the miners, so that it becomes a valid number to be used for hashing the value of block. Nonce is the number which can be used only once. Once the perfect Nonce is found, it is added to the hashed block.

It is compared to the existing target, whether it is lower or equal to the current target. Miners test and discard millions of Nonce per second until they find that Golden Nonce which is valid. Once the Golden Nonce is found, they can complete the Block and add it to the Block Chain and there by receive the Block reward.

Validating the new Block

New Hash Block is compared to It is compared to the existing Target, whether it is lower or equal to the current target.



Bitcoin Block Hashing

Constant info
Updated from time to time roughly every 10 minutes
Difficulty level, updated every 2016 block
Guessing number to meet certain length of leading zeros of the new hash block
Version Info
Previous Block
Merkle Root
Time
Bits
Nonce
SHA256
New Hash Block

Block Confirmation time

- What is Block confirmation time?
  Where is used – is it related to security?

Definition – Confirmation time is defined as the time elapsed between the moment a blockchain transaction is submitted to the network and the time it is finally recorded into a confirmed block.

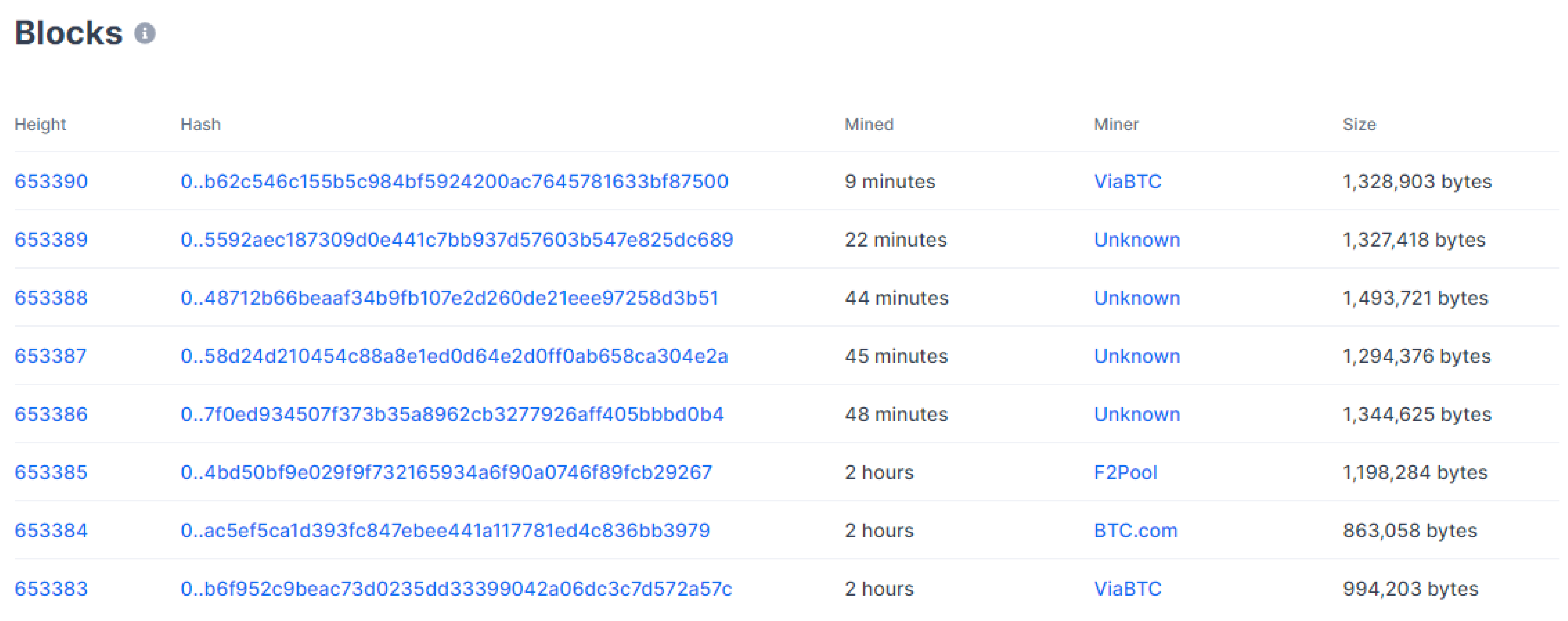
This is the duration between the validation of two blocks. The block confirmation time has a relative value, but is not fixed.

Merchants can use higher confirmation times.

Every public Blockchain has public visible Block Explorer

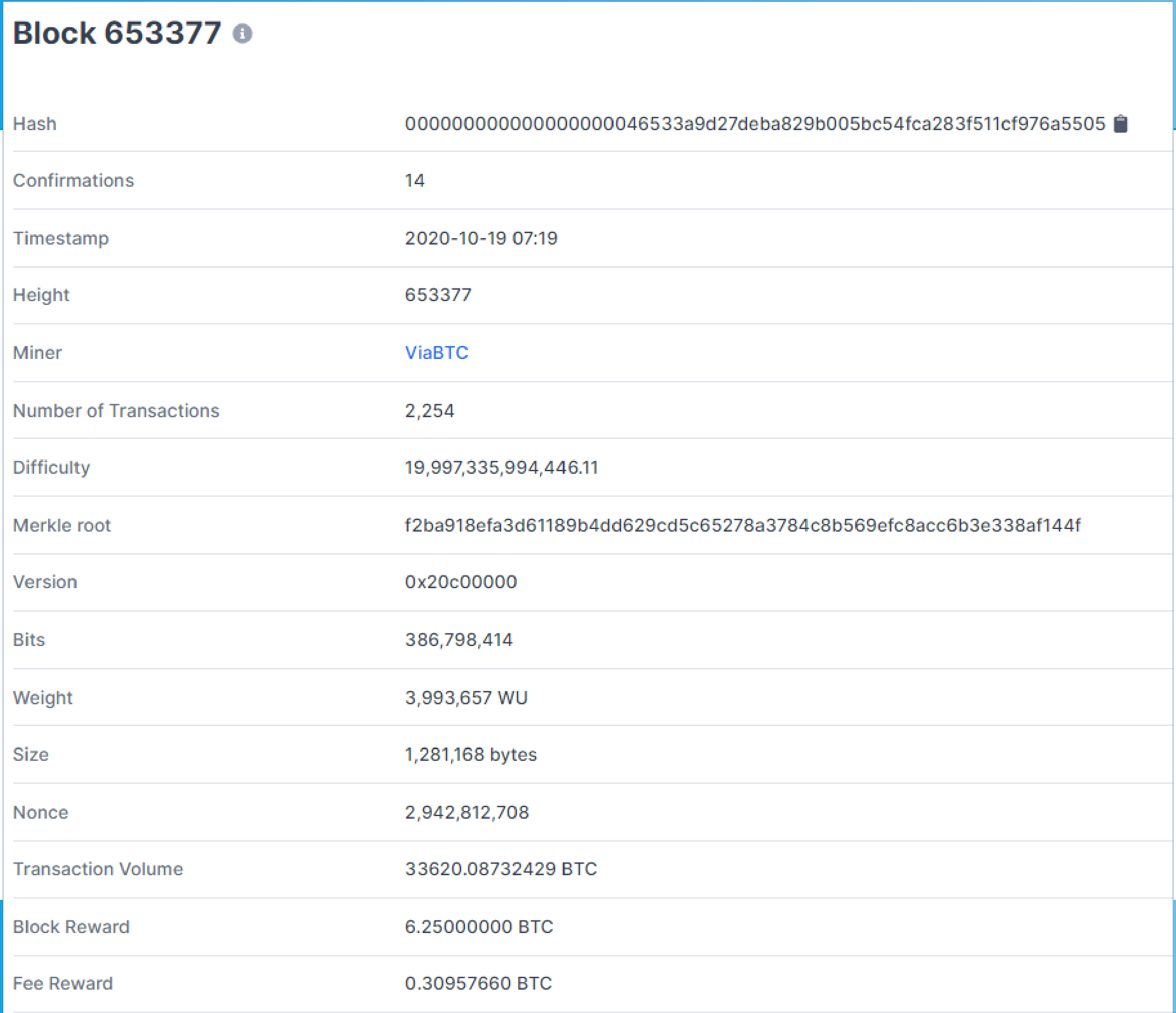
- BTC Block Explorers -
  - https://btc.com/
  - https://www.blockchain.com/btc/blocks
- Ethereum Block Explorer
  - https://etherscan.io/blocks

blockchain.com block explorer



Blocks

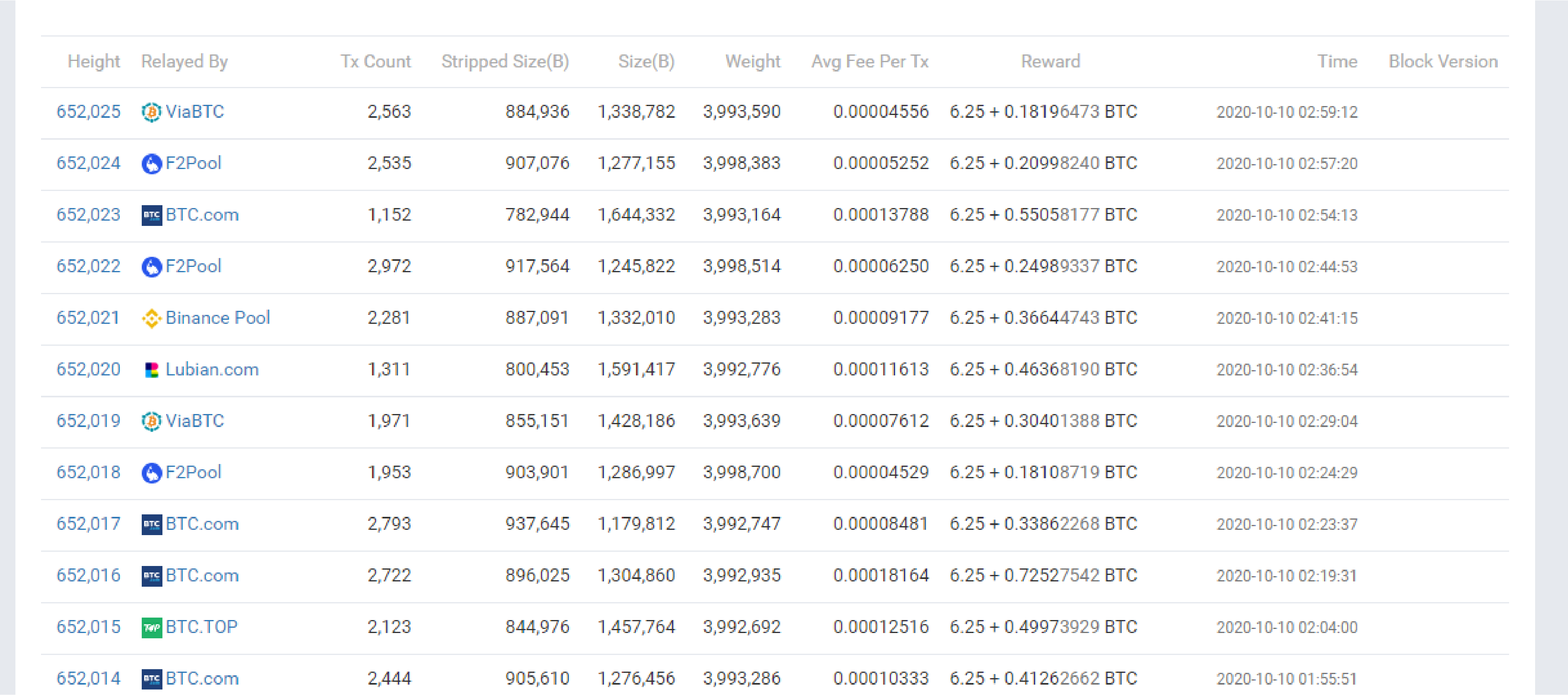
Height	Hash	Mined	Miner	Size
653390	0..b62c546c155b5c984bf5924200ac7645781633bf87500	9 minutes	ViaBTC	1,328,903 bytes
653389	0..5592aec187309d0e441c7bb937d57603b547e825dc689	22 minutes	Unknown	1,327,418 bytes
653388	0..48712b66beaaf34b9fb107e2d260de21eee97258d3b51	44 minutes	Unknown	1,493,721 bytes
653387	0..58d24d210454c88a8e1ed0d64e2d0ff0ab658ca304e2a	45 minutes	Unknown	1,294,376 bytes
653386	0..7f0ed934507f373b35a8962cb3277926aff405bbbd0b4	48 minutes	Unknown	1,344,625 bytes
653385	0..4bd50bf9e029f9f732165934a6f90a0746f89fcb29267	2 hours	F2Pool	1,198,284 bytes
653384	0..ac5ef5ca1d393fc847ebee441a117781ed4c836bb3979	2 hours	BTC.com	863,058 bytes
653383	0..b6f952c9beac73d0235dd33399042a06dc3c7d572a57c	2 hours	ViaBTC	994,203 bytes



Block 653377

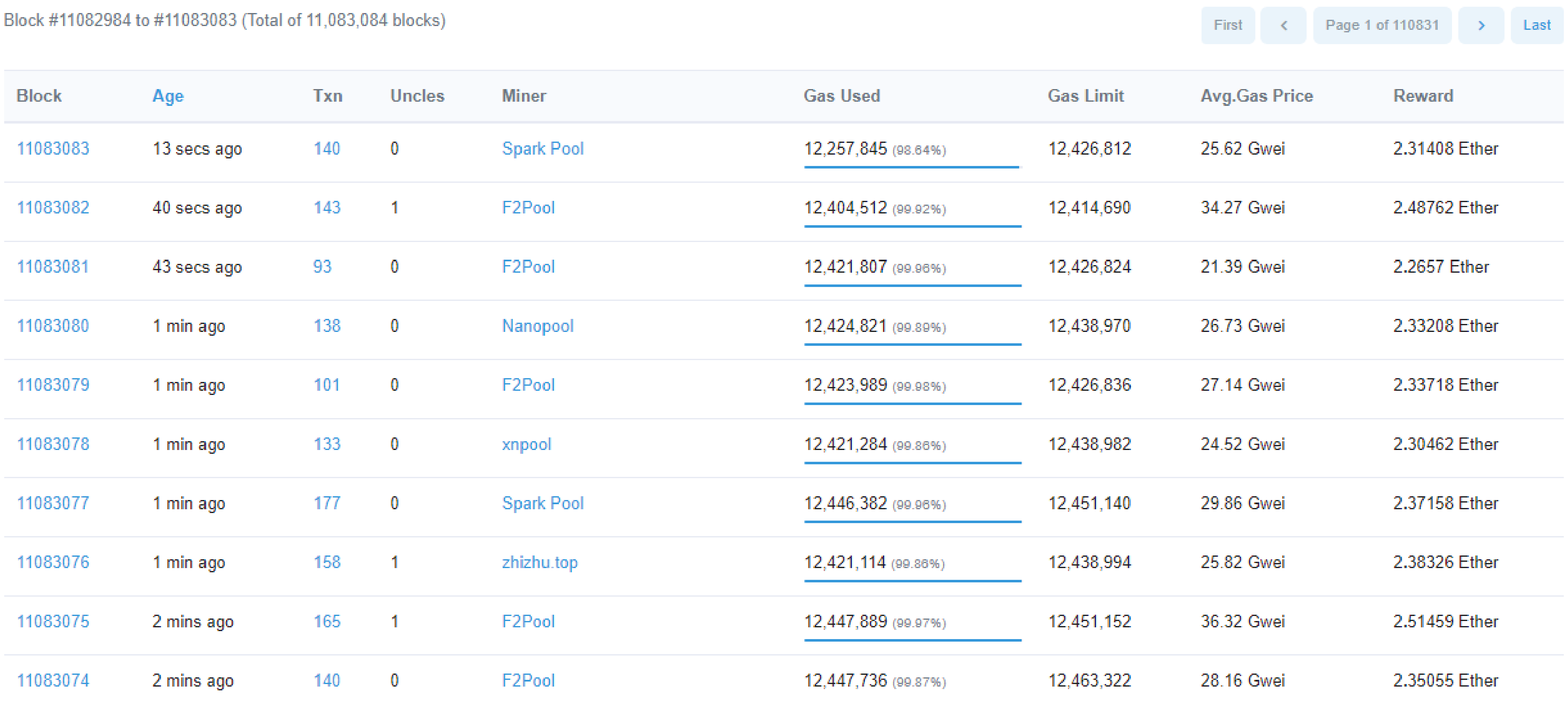
Hash	0000000000000000000046533a9d27deba829b005bc54fca283f511cf976a5505
Confirmations	14
Timestamp	2020-10-19 07:19
Height	653377
Miner	ViaBTC
Number of Transactions	2,254
Difficulty	19,997,335,994,446.11
Merkle root	f2ba918efa3d61189b4dd629cd5c65278a3784c8b569efc8acc6b3e338af144f
Version	0x20c00000
Bits	386,798,414
Weight	3,993,657 WU
Size	1,281,168 bytes
Nonce	2,942,812,708
Transaction Volume	33620.08732429 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.30957660 BTC

btc.com block explorer



Height	Relayed By	Tx Count	Stripped Size(B)	Size(B)	Weight	Avg Fee Per Tx	Reward	Time	Block Version
652,025	ViaBTC	2,563	884,936	1,338,782	3,993,590	0.00004556	6.25 + 0.18196473 BTC	2020-10-10 02:59:12	
652,024	F2Pool	2,535	907,076	1,277,155	3,998,383	0.00005252	6.25 + 0.20998240 BTC	2020-10-10 02:57:20	
652,023	BTC.com	1,152	782,944	1,644,332	3,993,164	0.00013788	6.25 + 0.55058177 BTC	2020-10-10 02:54:13	
652,022	F2Pool	2,972	917,564	1,245,822	3,998,514	0.00006250	6.25 + 0.24989337 BTC	2020-10-10 02:44:53	
652,021	Binance Pool	2,281	887,091	1,332,010	3,993,283	0.00009177	6.25 + 0.36644743 BTC	2020-10-10 02:41:15	
652,020	Lubian.com	1,311	800,453	1,591,417	3,992,776	0.00011613	6.25 + 0.46368190 BTC	2020-10-10 02:36:54	
652,019	ViaBTC	1,971	855,151	1,428,186	3,993,639	0.00007612	6.25 + 0.30401388 BTC	2020-10-10 02:29:04	
652,018	F2Pool	1,953	903,901	1,286,997	3,998,700	0.00004529	6.25 + 0.18108719 BTC	2020-10-10 02:24:29	
652,017	BTC.com	2,793	937,645	1,179,812	3,992,747	0.00008481	6.25 + 0.33862268 BTC	2020-10-10 02:23:37	
652,016	BTC.com	2,722	896,025	1,304,860	3,992,935	0.00018164	6.25 + 0.72527542 BTC	2020-10-10 02:19:31	
652,015	BTC.TOP	2,123	844,976	1,457,764	3,992,692	0.00012516	6.25 + 0.49973929 BTC	2020-10-10 02:04:00	
652,014	BTC.com	2,444	905,610	1,276,456	3,993,286	0.00010333	6.25 + 0.41262662 BTC	2020-10-10 01:55:51	

etherscan.io Ethereum block explorer



Block #11082984 to #11083083 (Total of 11,083,084 blocks)

Block	Age	Txn	Uncles	Miner	Gas Used	Gas Limit	Avg.Gas Price	Reward
11083083	13 secs ago	140	0	Spark Pool	12,257,845 (98.64%)	12,426,812	25.62 Gwei	2.31408 Ether
11083082	40 secs ago	143	1	F2Pool	12,404,512 (99.92%)	12,414,690	34.27 Gwei	2.48762 Ether
11083081	43 secs ago	93	0	F2Pool	12,421,807 (99.96%)	12,426,824	21.39 Gwei	2.2657 Ether
11083080	1 min ago	138	0	Nanopool	12,424,821 (99.89%)	12,438,970	26.73 Gwei	2.33208 Ether
11083079	1 min ago	101	0	F2Pool	12,423,989 (99.98%)	12,426,836	27.14 Gwei	2.33718 Ether
11083078	1 min ago	133	0	xnpool	12,421,284 (99.86%)	12,438,982	24.52 Gwei	2.30462 Ether
11083077	1 min ago	177	0	Spark Pool	12,446,382 (99.96%)	12,451,140	29.86 Gwei	2.37158 Ether
11083076	1 min ago	158	1	zhizhu.top	12,421,114 (99.86%)	12,438,994	25.82 Gwei	2.38326 Ether
11083075	2 mins ago	165	1	F2Pool	12,447,889 (99.97%)	12,451,152	36.32 Gwei	2.51459 Ether
11083074	2 mins ago	140	0	F2Pool	12,447,736 (99.87%)	12,463,322	28.16 Gwei	2.35055 Ether

Block Reward

- Open question - What is block Reward? Is it constant?

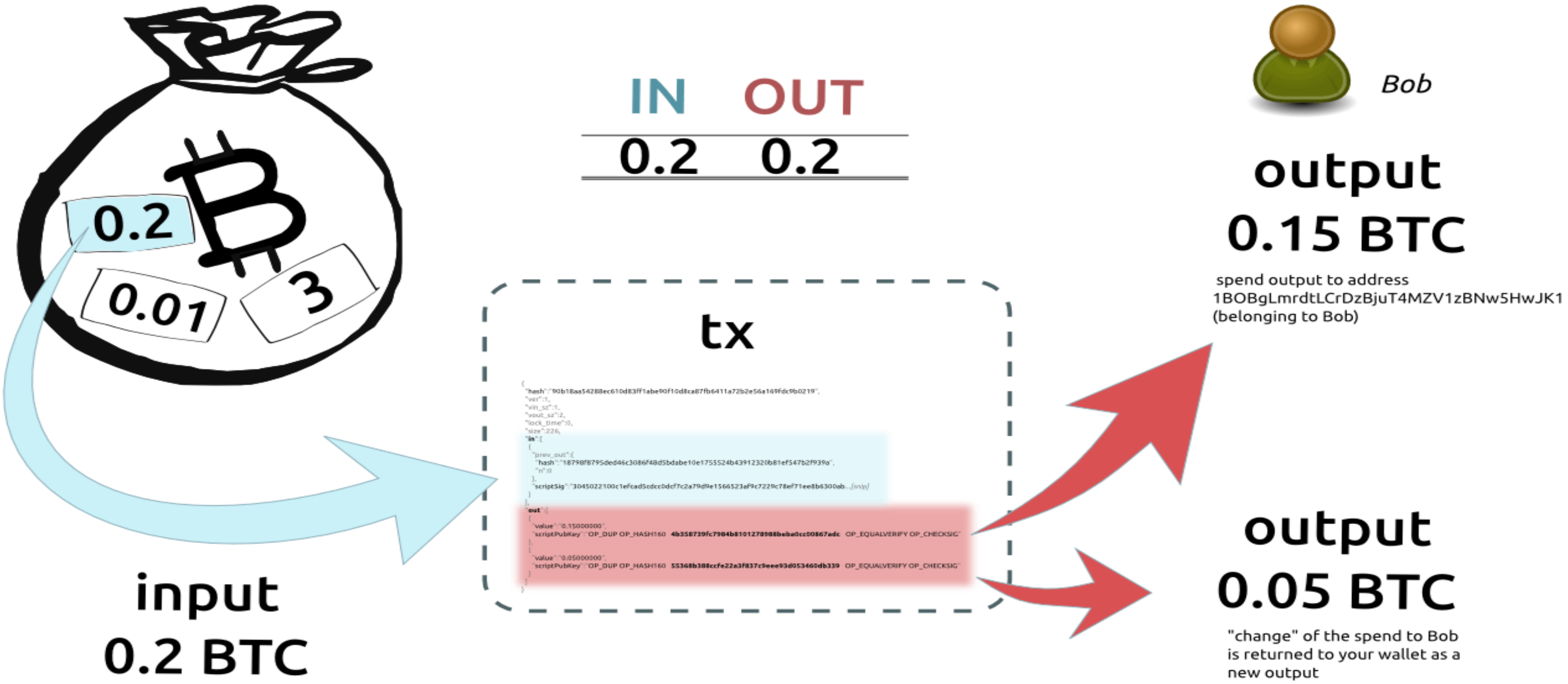
Blockchain Transactions

Blockchain transaction - is a signed piece of data that is broadcast to the network and, if valid, ends up in a block in the blockchain.

Contains Metadata that can be viewed in the block explorer.

- Transaction ID
- Descriptors and meta-data
- Inputs (address from, signature)
- Outputs (address out)

Bitcoin Transaction Input and Outputs



IN	OUT
0.2	0.2

tx

```
{
 "hash":"90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219",
 "ver":1,
 "vin_sz":1,
 "vout_sz":2,
 "lock_time":0,
 "size":226,
 "in":[
  {
   "prev_out":{
    "hash":"18798f8795ded46c3086f48d5bdabe10e1755524b43912320b81ef547b2f939a",
    "n":0
   },
   "scriptSig":"3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab...(snip)
  }
 ],
 "out":[
  {
   "value":"0.15000000",
   "scriptPubKey":"OP_DUP OP_HASH160  4b358739fc7984b8101278988beba0cc00867adc  OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
   "value":"0.05000000",
   "scriptPubKey":"OP_DUP OP_HASH160  55368b388ccfe22a3f837c9eee93d053460db339  OP_EQUALVERIFY OP_CHECKSIG"
  }
 ]
}
```

output

0.15 BTC

spend output to address
1BOBgLmrdtLCrDzBjuT4MZV1zBNw5HwJK1
(belonging to Bob)

output

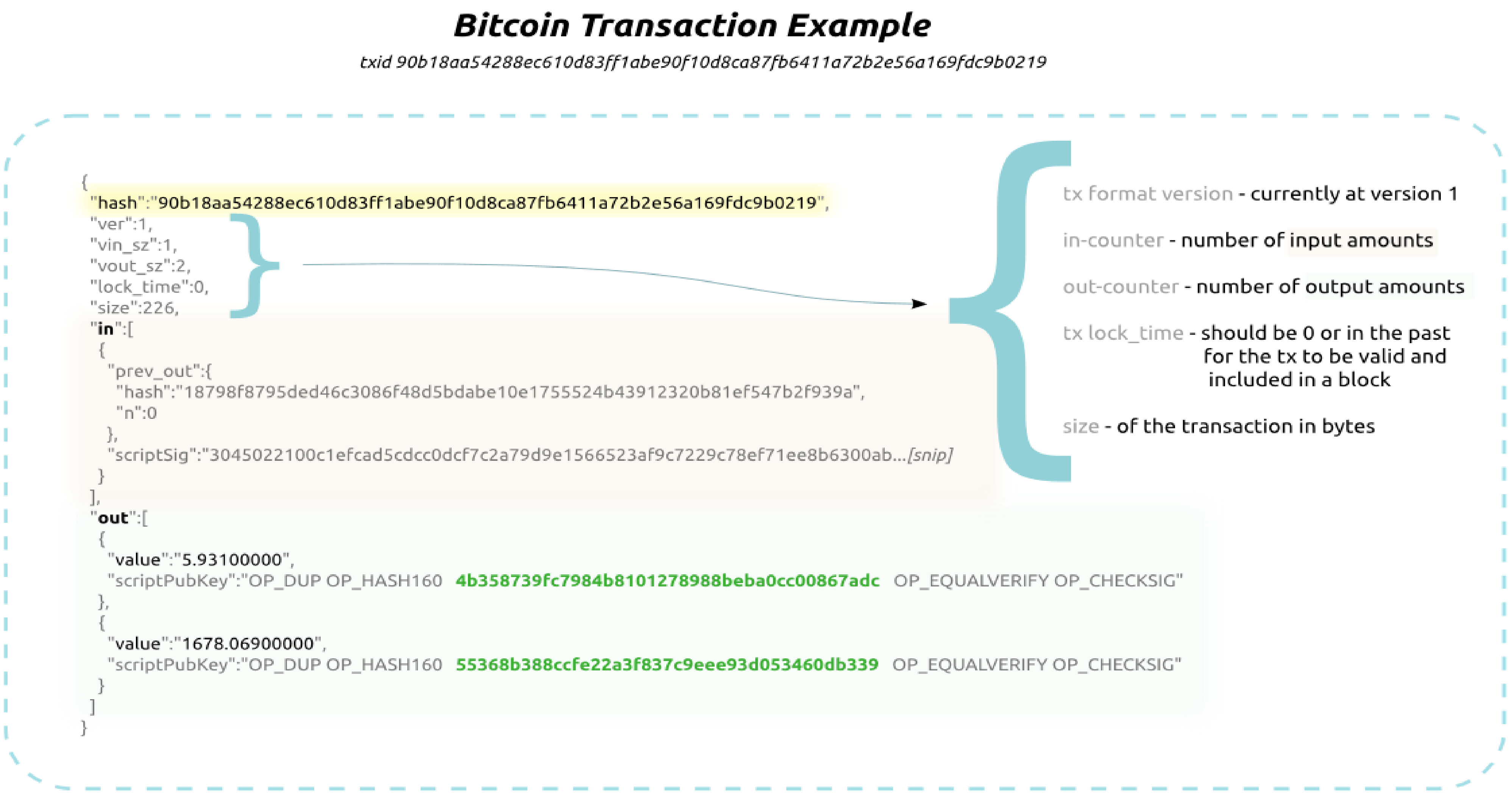
0.05 BTC

"change" of the spend to Bob
is returned to your wallet as a
new output

input

0.2 BTC

image by Venzen <venzen@mail.bihthai.net> 2014 CC SA
conditions of reuse: http://sofala.bihthai.net/works/txinout.htm



Bitcoin Transaction Example

txid 90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219

```
{
 "hash":"90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219",
 "ver":1,
 "vin_sz":1,
 "vout_sz":2,
 "lock_time":0,
 "size":226,
 "in":[
  {
   "prev_out":{
    "hash":"18798f8795ded46c3086f48d5bdabe10e1755524b43912320b81ef547b2f939a",
    "n":0
   },
   "scriptSig":"3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab...[snip]
  }
 ],
 "out":[
  {
   "value":"5.93100000",
   "scriptPubKey":"OP_DUP OP_HASH160  4b358739fc7984b8101278988beba0cc00867adc  OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
   "value":"1678.06900000",
   "scriptPubKey":"OP_DUP OP_HASH160  55368b388ccfe22a3f837c9eee93d053460db339  OP_EQUALVERIFY OP_CHECKSIG"
  }
 ]
}
```

tx format version - currently at version 1

in-counter - number of input amounts

out-counter - number of output amounts

tx lock_time - should be 0 or in the past for the tx to be valid and included in a block

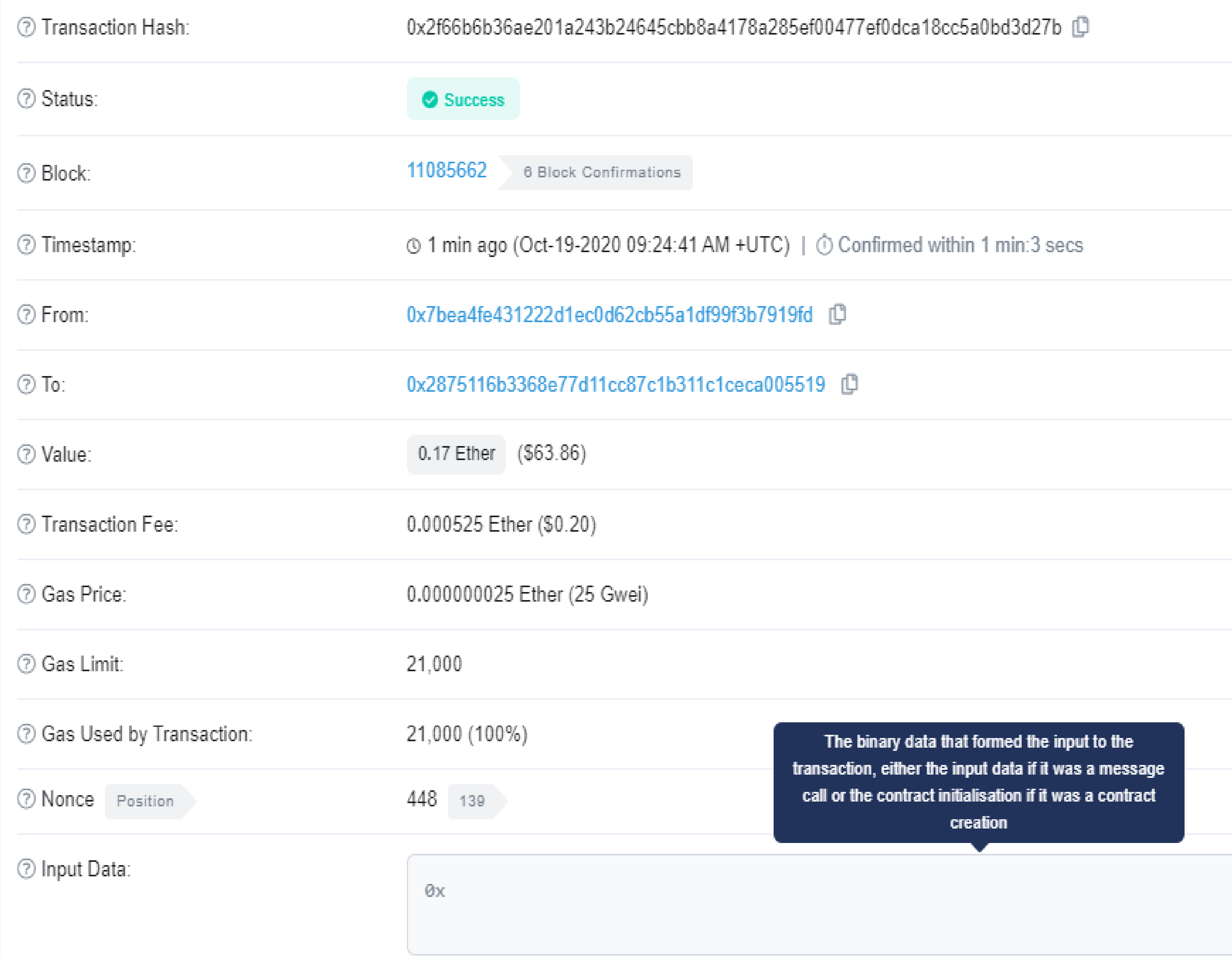
size - of the transaction in bytes

On blockchain:

image by Venzen <venzen@mail.bihthai.net> 2014 CC SA
conditions of reuse: http://sofala.bihthai.net/works/txinout.htm

Ethereum transaction example

https://etherscan.io/tx/



Transaction Hash:	0x2f66b6b36ae201a243b24645cbb8a4178a285ef00477ef0dca18cc5a0bd3d27b
Status:	Success
Block:	11085662 6 Block Confirmations
Timestamp:	1 min ago (Oct-19-2020 09:24:41 AM +UTC) | Confirmed within 1 min:3 secs
From:	0x7bea4fe431222d1ec0d62cb55a1df99f3b7919fd
To:	0x2875116b3368e77d11cc87c1b311c1ceca005519
Value:	0.17 Ether ($63.86)
Transaction Fee:	0.000525 Ether ($0.20)
Gas Price:	0.000000025 Ether (25 Gwei)
Gas Limit:	21,000
Gas Used by Transaction:	21,000 (100%)
Nonce Position	448 139
Input Data:	0x

The binary data that formed the input to the transaction, either the input data if it was a message call or the contract initialisation if it was a contract creation

Transactions Confirmations

After a transaction is broadcast to the Bitcoin network, it may be included in a block that is published to the network. When that happens it is said that the transaction has been mined at a depth of 1 block.

Number of confirmations required

- Varies depending on the Exchange and the volume of the transaction
- 1-6 confirmation times (BTC)
- 20-60 confirmation times (Ethereum)

Transaction bandwidth

How much transactions per second / day can the Blockchain handle?

Bitcoin:

Transactions per day: https://www.blockchain.com/charts/n-transactions

Transactions per second: https://www.blockchain.com/charts/transactions-per-second

Ethereum:

https://blockchair.com/ethereum/charts/transactions-per-second

~ 864 000 transactions per day (ETH)
~ 300 000 (BTC)

More interesting aspects of Blockchain

Block difficulty chart - https://etherscan.io/chart/difficulty

Network Hash Rate - https://etherscan.io/chart/hashrate

BTC Difficulty - https://bitinfocharts.com/comparison/bitcoin-difficulty.html

Block reward

BTC Block reward https://bitcoinvisuals.com/chain-block-reward

Sources

- **Public and private blockchains**
  - https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f
  - https://data-flair.training/blogs/types-of-blockchain/
  - https://101blockchains.com/types-of-blockchain/
- **Blocks**
  - https://learnmeabitcoin.com/beginners/blocks

Questions ?

- Thank you for your attention!