

Bitcoin: Programming the Future of Money

Topics in Computer Science - ITCS 4010/5010, Spring 2025

Dr. Christian Kümmerle

Lecture 21

Consensus & Forks



**What determines the consensus
of what Bitcoin is?**

THE DECENTRALIZED CONSENSUS OF THE BITCOIN NETWORK

We distinguish:

- **Technical Consensus:**

Does this transaction follow the rules? Is this block a valid Bitcoin block? If there are multiple branches of the Bitcoin blockchain, which is the right one?

- **Social Consensus:**

What are “the rules” in the first place?

“Emergent Consensus”

TECHNICAL CONSENSUS

- Independent **validation** of each **transaction** by all full nodes
- Independent **aggregation** of (mempool) **transactions** into new blocks by miners
- Independent **validation** of each **new block** by all full nodes
- Independent **selection of the chain with the most cumulative proof-of-work** enforced by all full nodes

VALIDATION OF (NEW) TRANSACTIONS

For a Tx to be valid, the following rules need to be satisfied:

- Tx's syntax and data structure must be correct.
- **No inputs** nor **outputs** are **empty**.
- Transaction is **not too large** (in vbytes) to fit in a block.
- Each **output** value needs to be **in range of values** ($0 < \text{value} < 21,000,000$).
- Lock time is INT_MAX or follows rules of [BIP68](#) (correct abs. or rel. lock time).
- **Scripts** of each **input must validate against respective output script** of referred UTXO.
- Not more **signature operations** than the set limit (up to 80000 per block).
- All rel. or abs. lock times are fulfilled, if Coinbase input, 100 confirmations until spendable

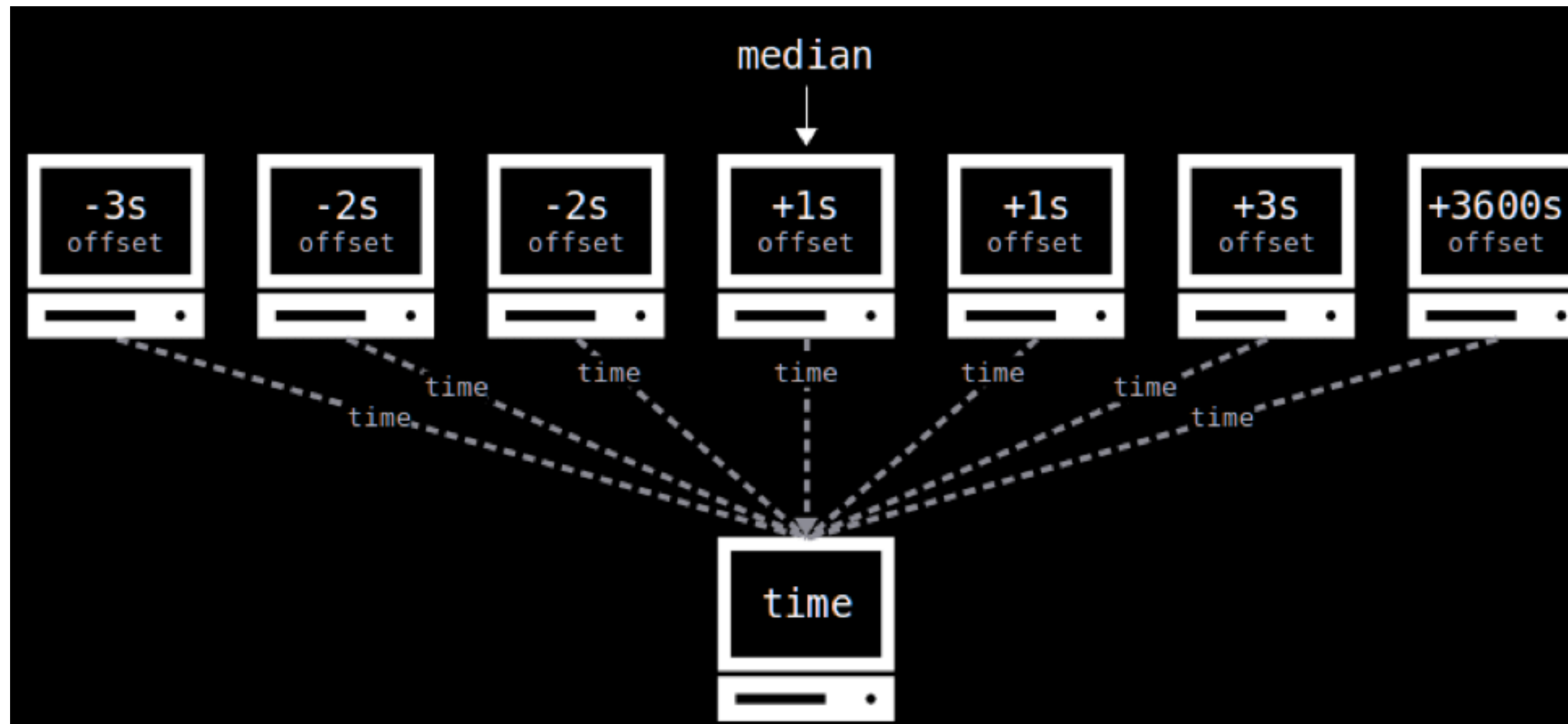
VALIDATION OF BLOCKS

For a block to be valid, the following rules need to be satisfied:

- Syntax of the block data structure needs to be correct (see also [here](#)).
- Block header hash is less than the [target](#).
- Block time stamp is above the **Median Time Past** (See [BIP113](#)) (median time last 11 blocks in the chain).
- Block time stamp is below **Network Adjusted Time** plus two hours.
- Block size is below 1,000,000 vbytes.
- (Only) first transaction in transaction Merkle tree is the **coinbase transaction**.
- All transactions in block are valid.

NETWORK ADJUSTED TIME

Definition: Local time of node + median offset of all connected nodes



Rule: Block time stamp is below **Network Adjusted Time** plus two hours.

Q: How could this be manipulated?

THE DIFFICULTY ADJUSTMENT

Part of the Bitcoin consensus rules.

Every 2016 blocks, mining difficulty is adjusted by updating value for “target” in the subsequent 2016 blocks based on:

$$\text{new target} = \text{old target} \cdot \frac{(\text{time of current block}) - (\text{time of (current - 2015th) block})}{20160 \text{ minutes}}$$

THE DIFFICULTY ADJUSTMENT

Every 2016 blocks, mining difficulty is adjusted by updating value for “target” in the subsequent 2016 blocks based on:

$$\text{new target} = \text{old target} \cdot \frac{(\text{time of current block}) - (\text{time of (current - 2015th) block})}{20160 \text{ minutes}}$$

Q: What if a lot of miners stop working for two weeks?

THE DIFFICULTY ADJUSTMENT

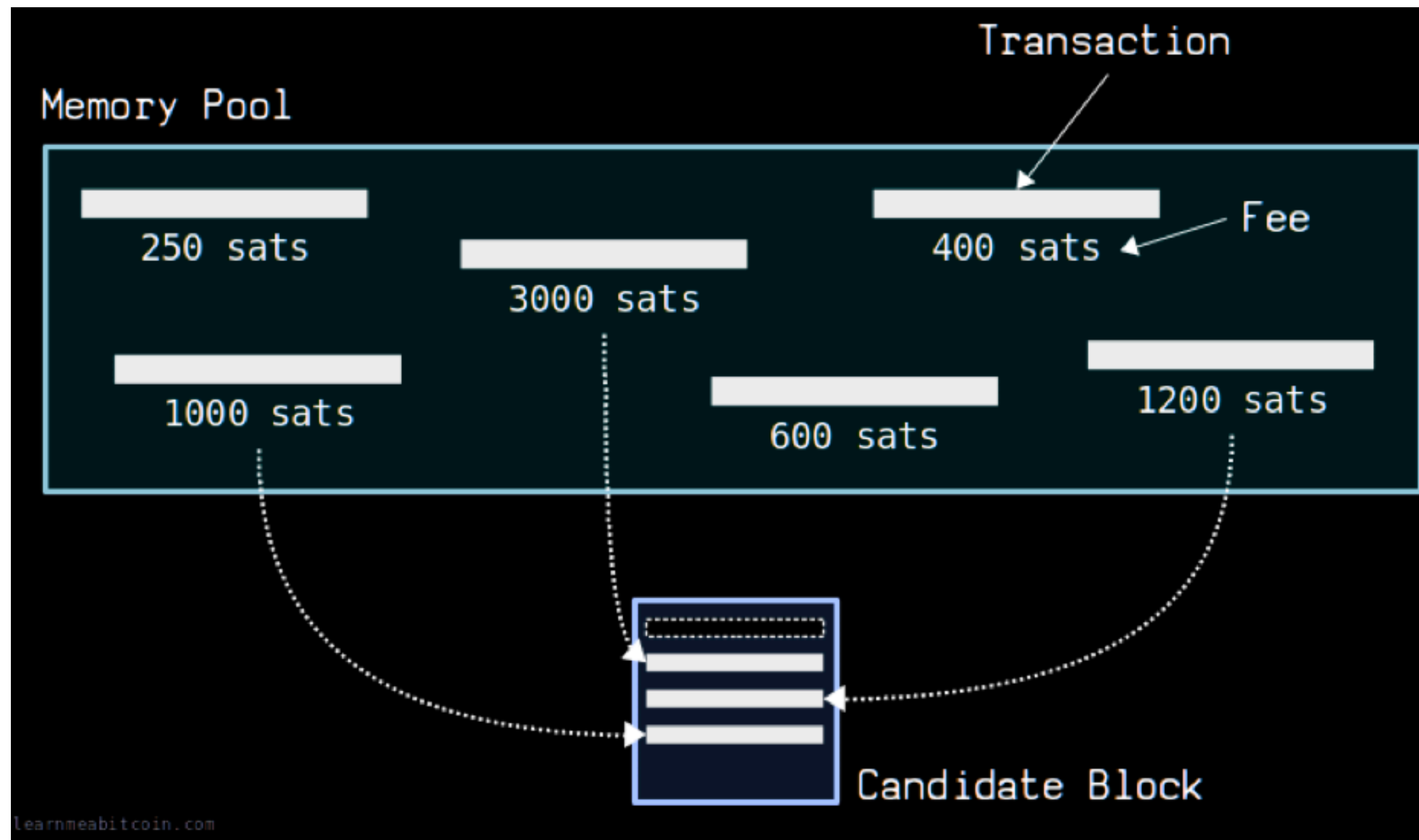
Every 2016 blocks, mining difficulty is adjusted by updating value for “target” in the subsequent 2016 blocks based on:

$$\text{new target} = \text{old target} \cdot \frac{(\text{time of current block}) - (\text{time of (current} - 2015\text{th) block})}{20160 \text{ minutes}}$$

- The target cannot increase by more than 400% in each adjustment period.
- The target cannot decrease by more than 75% in each adjustment period.

TRANSACTION FEES IN BITCOIN

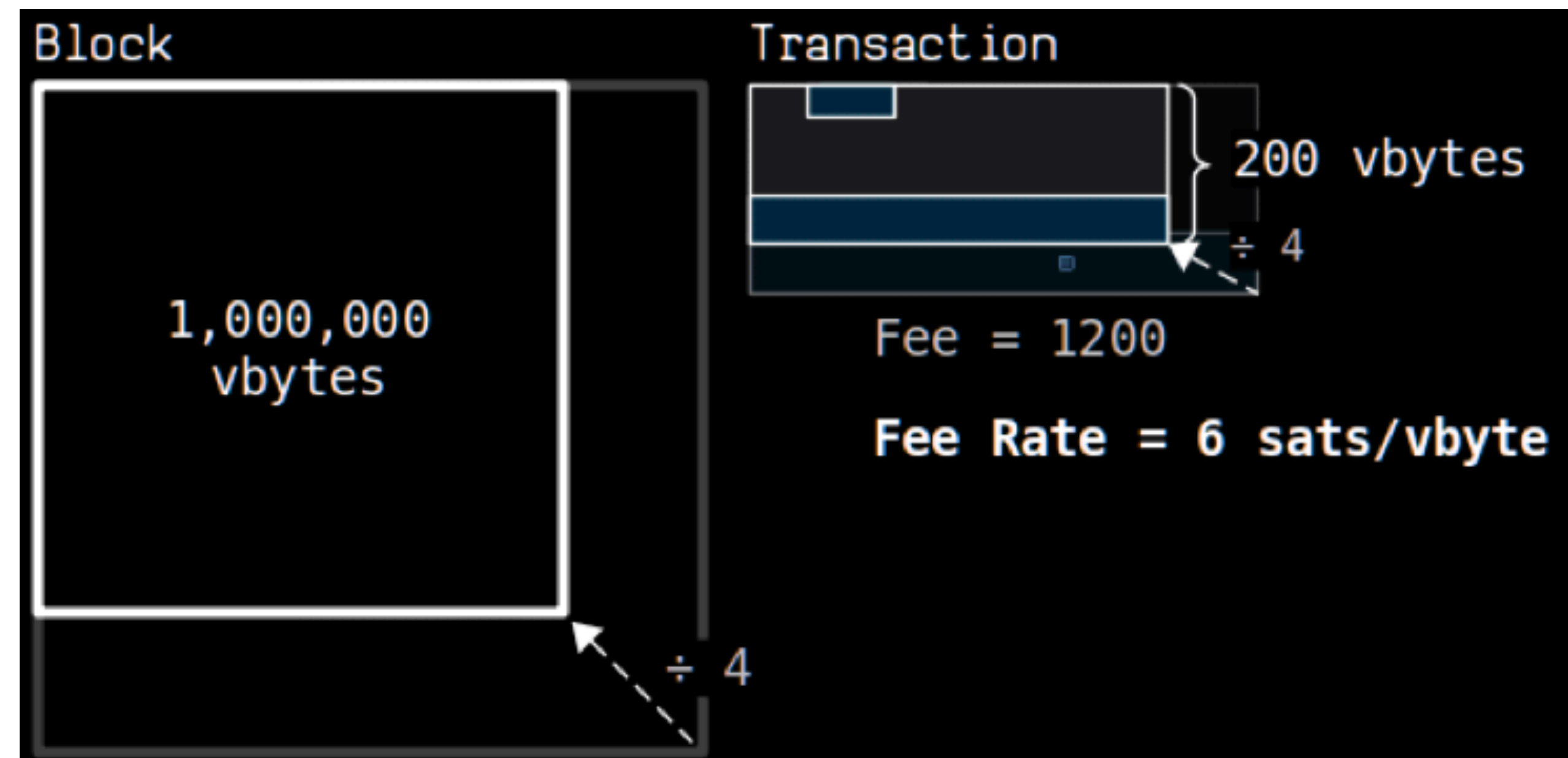
- Transactions in mempool are all eligible to be included in the next block by any miner.



FEES AND FEE RATES (CALCULATION BEFORE 2017 SEGWIT SOFT FORK)

- Sender of transaction can choose a “fee rate” that is measured in “sats/byte”
(1 BTC = 100,000,000 satoshis (sats))
- Transaction fee is computed such that

$$\text{Fee} = (\text{Bytes of transaction}) \cdot (\text{fee rate in sats/byte})$$

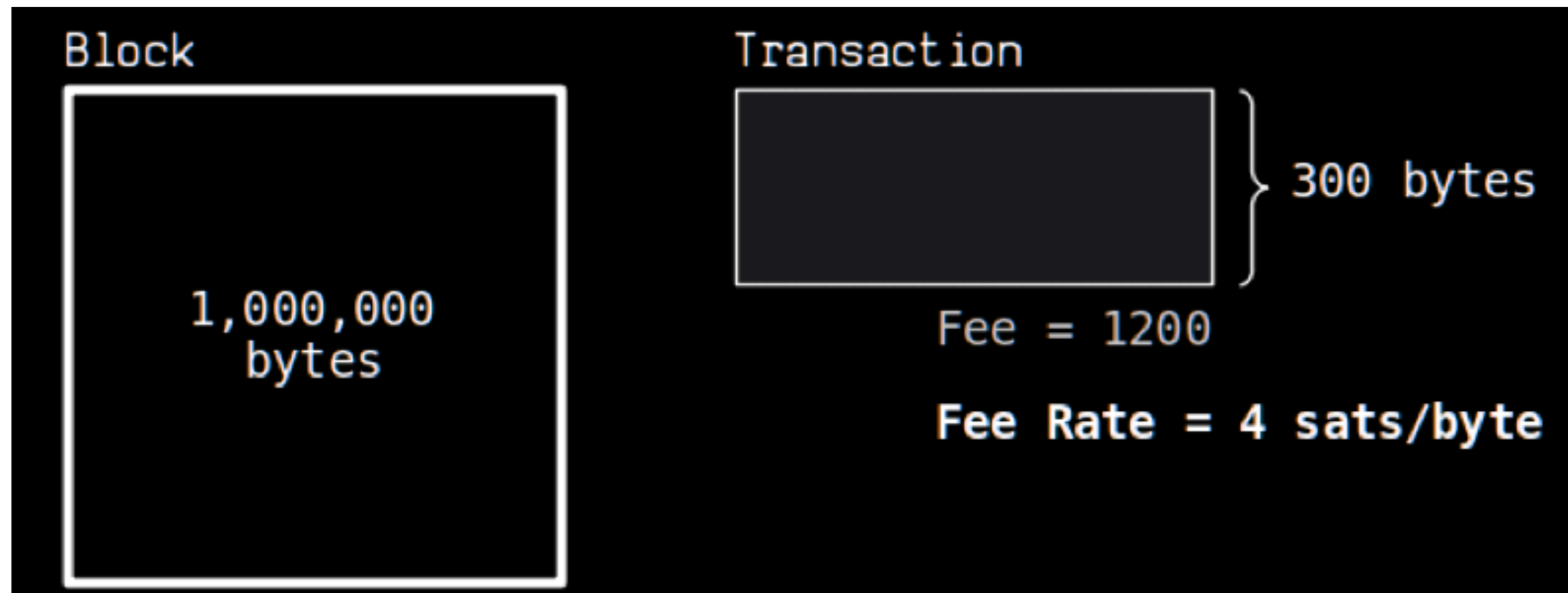


- Size of a block is upper bounded by 1 MB (or 1,000,000 bytes)

FEES AND FEE RATES (CALCULATION AFTER 2017 SEGWIT SOFT FORK)

- Sender of transaction can choose a “fee rate” that is measured in “sats/**vbyte**” where “vbyte” stands for a “virtual byte” unit.
- Transaction fee is computed such that

$$\text{Fee} = (\text{VBytes of transaction}) \cdot (\text{fee rate in sats/vbyte})$$

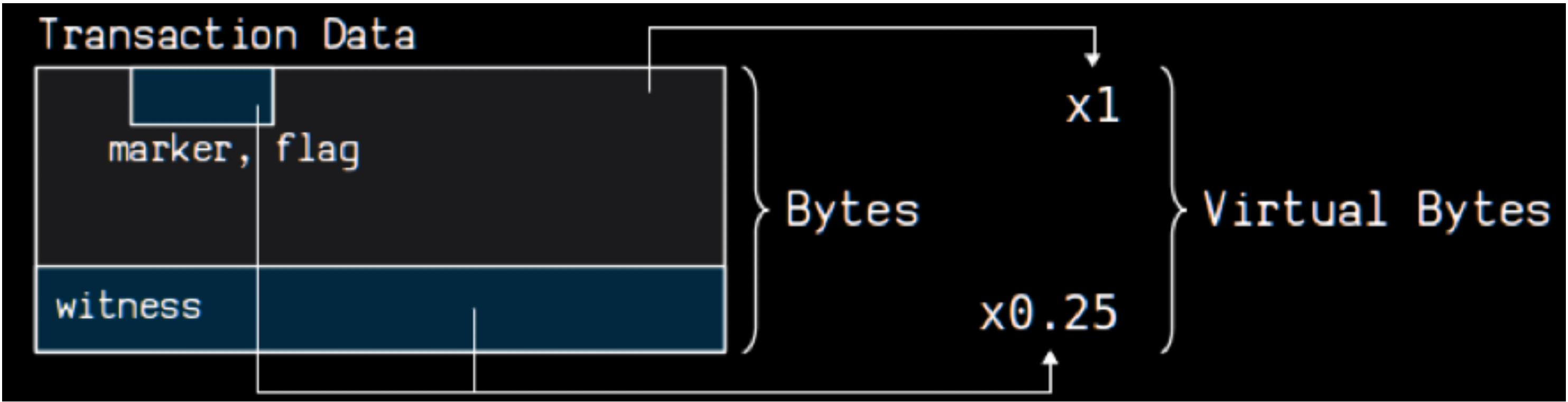


- Size of a block is upper bounded by 1,000,000 “vbytes” (can be more than 1 MB)

WHAT IS A VIRTUAL BYTE (VBYTE)?

- A vbyte unit corresponds to a byte in most transaction fields, but to one quarter of a byte for the “Marker”, “Flag” and “Witness” fields.

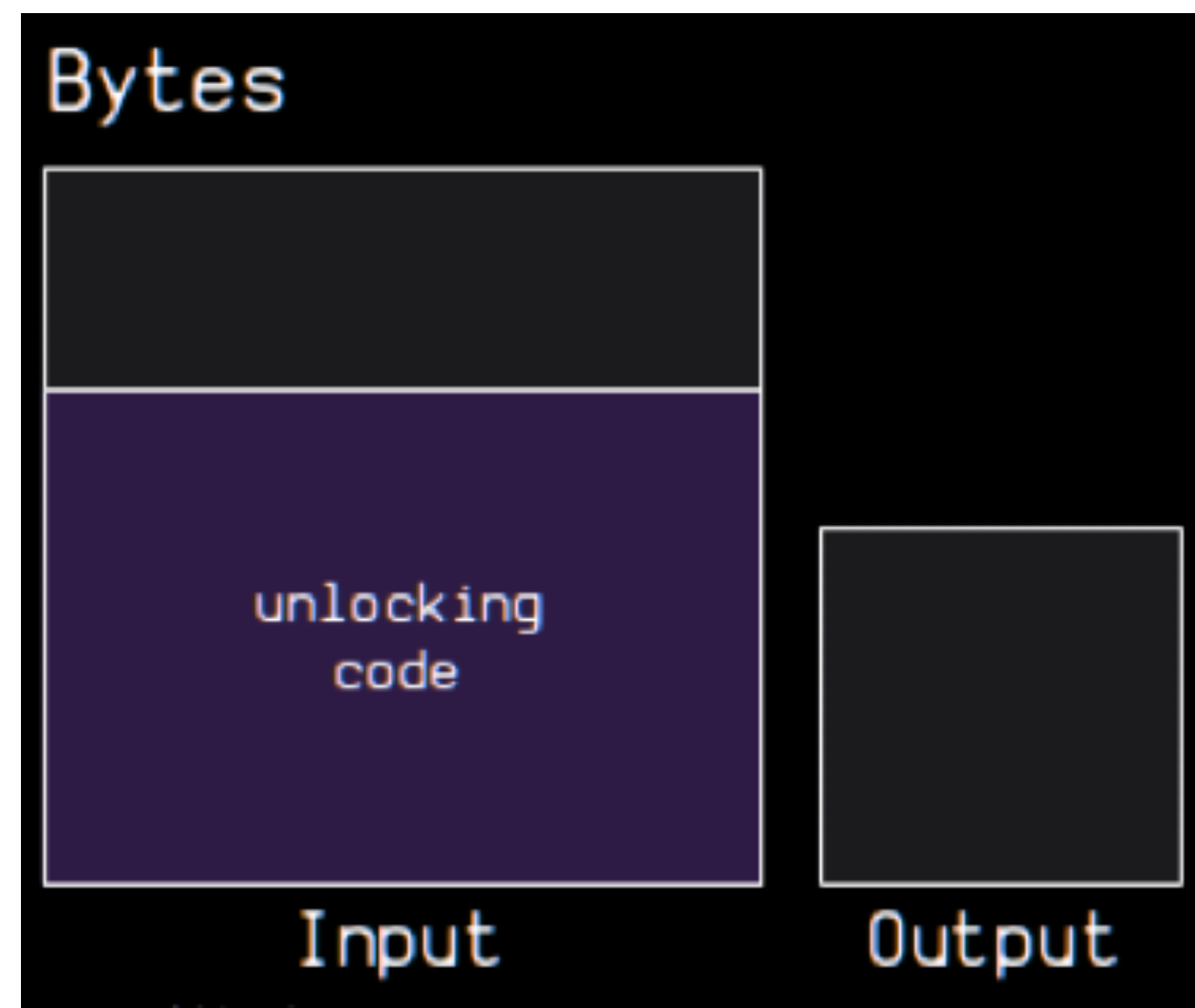
Field	Multiplier
version	x1
marker	x0.25
flag	x0.25
input	x1
output	x1
witness	x0.25
locktime	x1



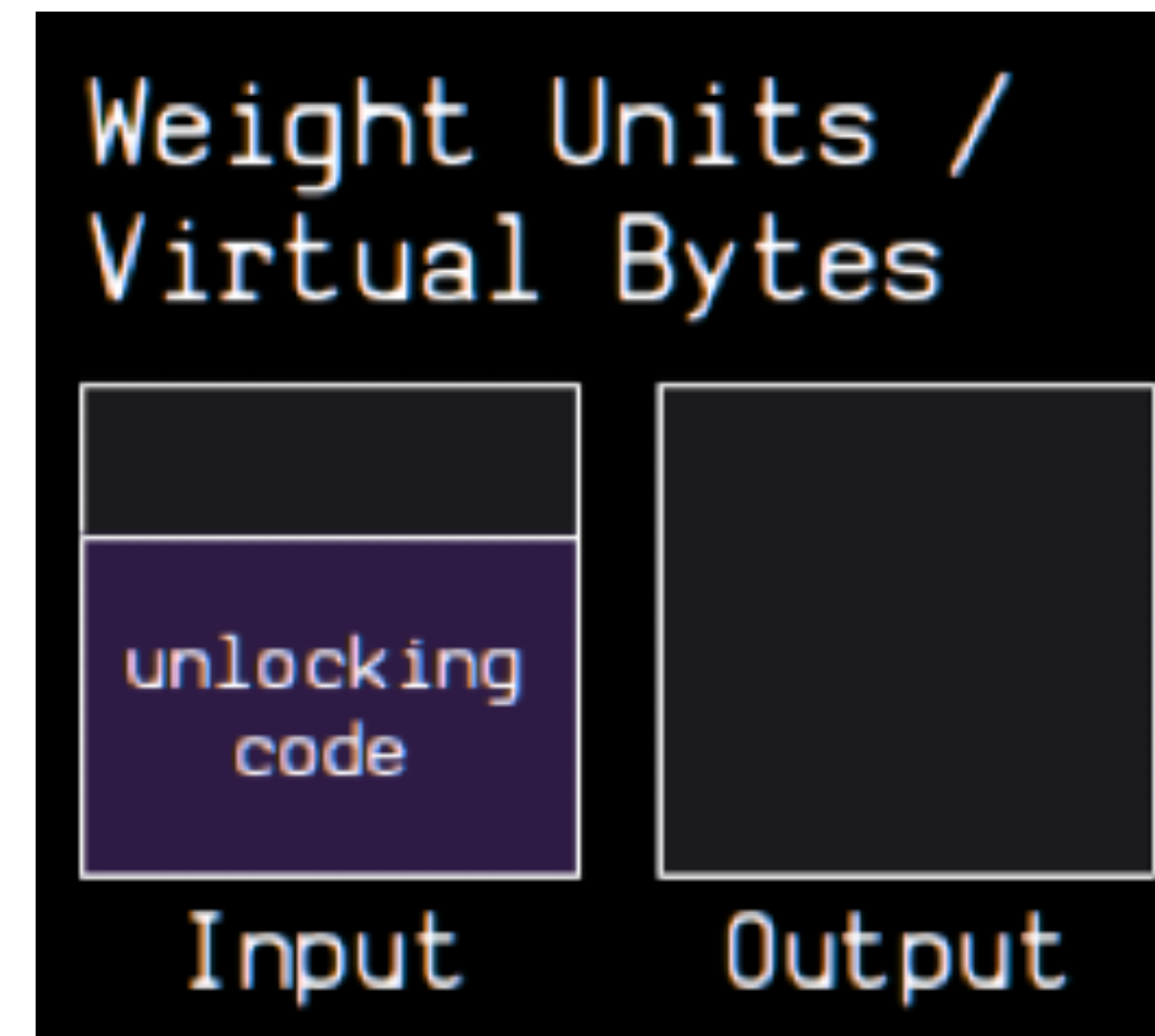
- Size of a block is upper bounded by 1,000,000 “vbytes” (can be more than 1 MB)

PURPOSE OF SATS/VBYTE FEE RATES IN SEGWIT SOFT FORK

- Implicit way of slightly increasing the block size limit of 1 MB (higher amount of transactions / block supported)
- Fairer distribution of fees between spender & recipient



Byte sizes before SegWit



VByte sizes after SegWit

WHAT IF YOU CHOSE A TRANSACTION FEE THAT IS TOO LOW?

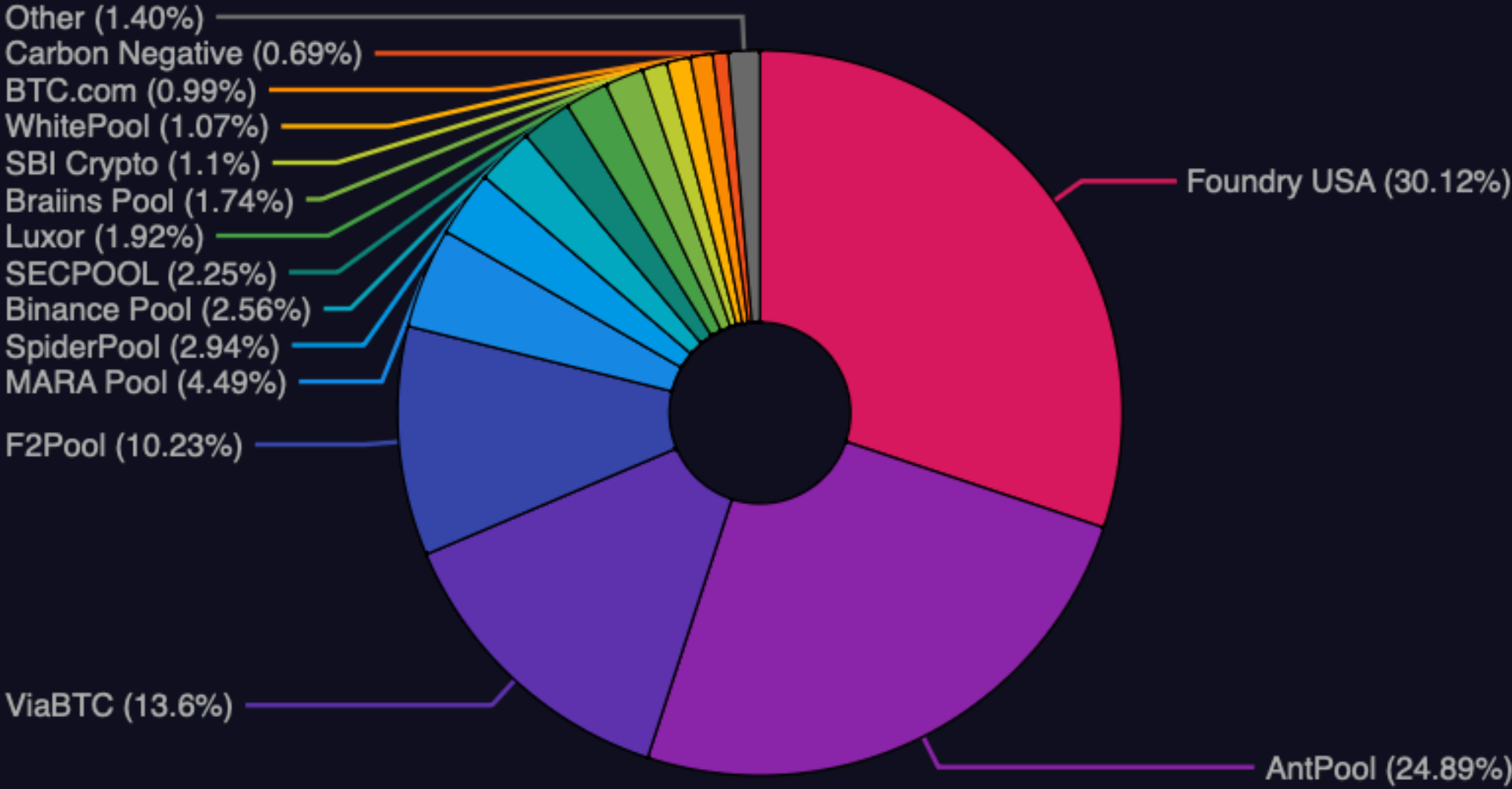
- **Replace by Fee Bumping**
- **Child Pays for Parent (CPFP) Fee Bumping**
- **Pay mining pool directly**








REPLACE BY FEE

- **No replace by fee**
- **Opt-In Replace by Fee**
- **Full Replace by Fee**

MINING POOLS

Current market shares
of mining pools



Rank		Pool	Blocks	Avg Health	Avg Block Fees	Empty Blocks
1		Foundry USA	4069 (30.12%)	99.68%	-2.58%	0 (0.00%)
2		AntPool	3362 (24.89%)	99.28%	-2.64%	18 (0.54%)
3		ViaBTC	1837 (13.6%)	99.67%	-1.91%	3 (0.16%)
4		F2Pool	1382 (10.23%)	99.62%	-2.84%	1 (0.07%)
5		MARA Pool	606 (4.49%)	99.72%	-2.37%	0 (0.00%)
6		SpiderPool	397 (2.94%)	95.14%	-8.26%	18 (4.53%)
7		Binance Pool	346 (2.56%)	99.95%	-1.84%	0 (0.00%)

Source:
<https://mempool.space/graphs/mining/pools>

THE HALVING RULE

Part of the Bitcoin consensus rules: [Decrease of block subsidy around every 4 years.](#)

Every 210,000 blocks, the amount of the output of Coinbase transaction is divided by two, starting from 50 BTC in block number 0.

```
CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
{
    int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
    // Force block reward to zero when right shift is undefined.
    if (halvings >= 64)
        return 0;

    CAmount nSubsidy = 50 * COIN;
    // Subsidy is cut in half every 210,000 blocks.
    nSubsidy >>= halvings;
    return nSubsidy;
}
```

THE HALVING RULE

Part of the Bitcoin consensus rules: [Decrease of block subsidy around every 4 years.](#)

Halving	Height	Subsidy (BTC)	Date	Total Mined (BTC)
0	<u>0</u>	50.00000000	03 Jan 2009, 18:15:05	0.00000000
1	<u>210,000</u>	25.00000000	28 Nov 2012, 15:24:38	10,500,000.00000000
2	<u>420,000</u>	12.50000000	09 Jul 2016, 16:46:13	15,750,000.00000000
3	<u>630,000</u>	6.25000000	11 May 2020, 19:23:43	18,375,000.00000000
4	<u>840,000</u>	3.12500000	20 Apr 2024, 00:09:27	19,687,500.00000000
5	1,050,000	1.56250000	15 Apr 2028 (estimate)	20,343,750.00000000
6	1,260,000	0.78125000	12 Apr 2032 (estimate)	20,671,875.00000000
7	1,470,000	0.39062500	10 Apr 2036 (estimate)	20,835,937.50000000
8	1,680,000	0.19531250	07 Apr 2040 (estimate)	20,917,968.75000000
9	1,890,000	0.09765625	04 Apr 2044 (estimate)	20,958,984.37500000
10	2,100,000	0.04882812	02 Apr 2048 (estimate)	20,979,492.18750000
11	2,310,000	0.02441406	30 Mar 2052 (estimate)	20,989,746.09270000

THE HALVING RULE

22	4,620,000	0.00001192	01 Mar 2096 (estimate)	20,999,994.97890000
23	4,830,000	0.00000596	27 Feb 2100 (estimate)	20,999,997.48210000
24	5,040,000	0.00000298	25 Feb 2104 (estimate)	20,999,998.73370000
25	5,250,000	0.00000149	23 Feb 2108 (estimate)	20,999,999.35950000
26	5,460,000	0.00000074	20 Feb 2112 (estimate)	20,999,999.67240000
27	5,670,000	0.00000037	17 Feb 2116 (estimate)	20,999,999.82780000
28	5,880,000	0.00000018	15 Feb 2120 (estimate)	20,999,999.90550000
29	6,090,000	0.00000009	12 Feb 2124 (estimate)	20,999,999.94330000
30	6,300,000	0.00000004	09 Feb 2128 (estimate)	20,999,999.96220000
31	6,510,000	0.00000002	07 Feb 2132 (estimate)	20,999,999.97060000
32	6,720,000	0.00000001	04 Feb 2136 (estimate)	20,999,999.97480000
33	6,930,000	0.00000000	01 Feb 2140 (estimate)	20,999,999.97690000
Total Supply: 20,999,999.9769 BTC				

SELECTION OF VALID BLOCKCHAIN

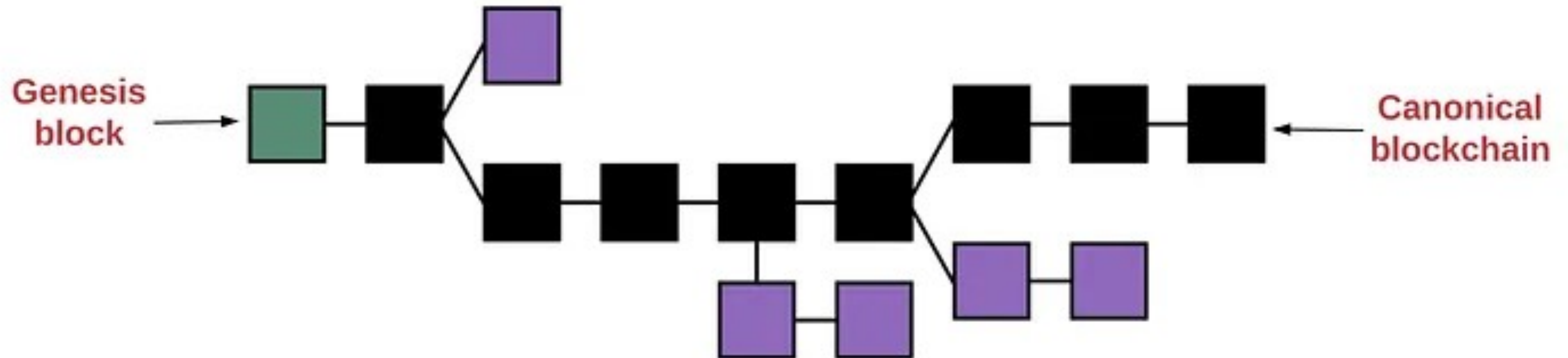
- **Key Rule:**
The chain of blocks with largest cumulative proof-of-work is the valid one.
- Can be checked by adding up the hashes of all blocks.
- Consequence:
It is not uncommon that (short) **chain reorganizations** take place!

HASHRATE ATTACKS

How can malicious (group of) miners endanger the consensus?

- Empty-Block Attack
- Double Spend Attack
- Seesaw Attack

Usually require $>51\%$ of hashrate (or more than 30%).



Changes of Social Consensus

HARD AND SOFT FORKS

We distinguish:

- **Hard forks:**

Change rules such that **new blocks / transaction types are not valid in the old rule set.**

-> Typically leads to chain split

- **Soft forks:**

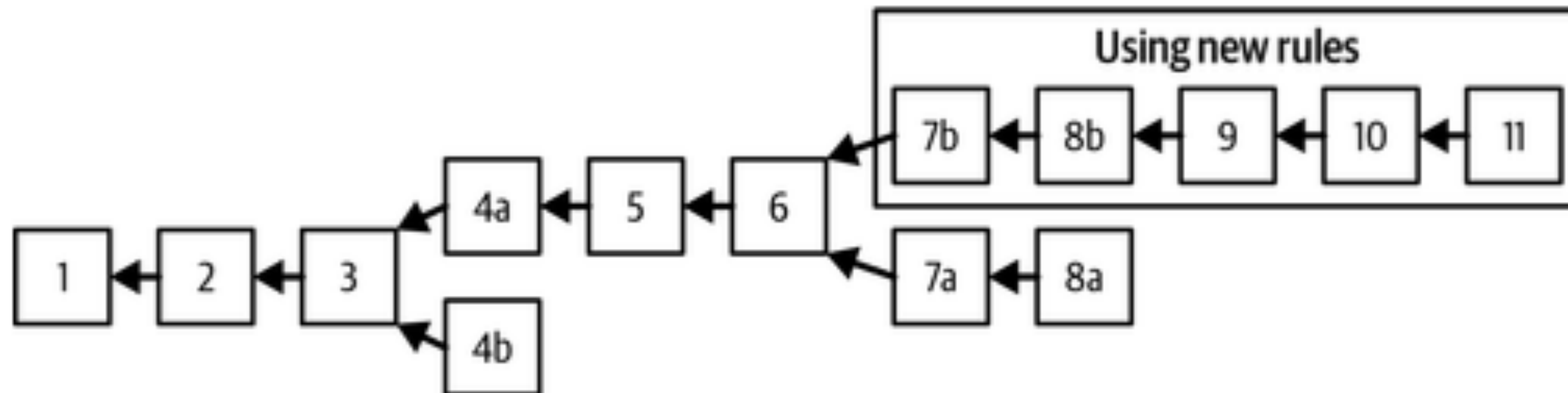
Change rules such that **new blocks / transaction types are still valid in the old rule set, but old transaction/block rules are not (necessarily) valid in the new rule set.**

-> Typically does not lead to chain split

HARD FORKS OF BITCOIN

Some hard forks of Bitcoin

- 2010: Addition of OP_NOP opcodes by Satoshi Nakamoto (no chain split)
- 2016: Bitcoin Classic
- 2017: Bitcoin Cash (“The Blocksize Wars”)
- 2018: Bitcoin-Satoshi’s Vision



MARKET VALUES OF FORK COINS

