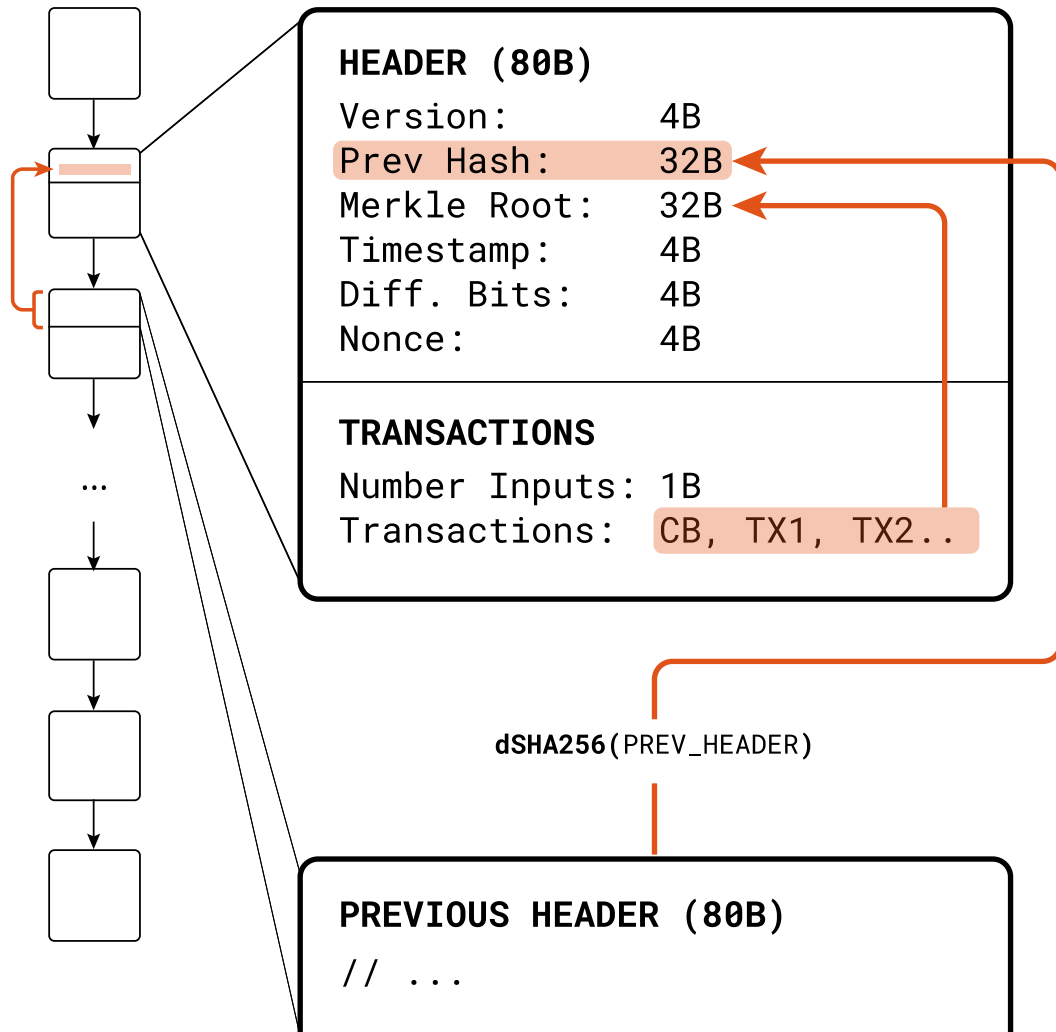


Bitcoin Block Headers



Version:

- Version 2: Height in Coinbase Input Script (BIP34)
- Version 3: Strict DER (BIP66)
- Version 4: CLTV support (BIP65)
- BIP9 signalling: Up to 29 different signals

Merkle Root:

- Commits all transactions and their order.

Timestamp:

- POSIX time (seconds since 1.1.1970, overflows in 2106 :))
- Must be higher than median of previous 11 blocks
- Cannot more than 2hrs higher than local peer clock

Difficulty Bits:

- Defines target for POW
- Block hash must be below target

Nonce:

- Iterated for POW

Block Hash:

- Double sha256 of serialised 80B header

Genesis Block



HEADER (80B)

//...

Diff. Bits: **ffff001d**

//...

TRANSACTIONS

Number of TXs: 01

Version: 01000000

Inputs: 01

Prev TX hash: 00000000..00

UTXO Index: ffffffff

Input Script: [**ffff001d**][04][**The Times
03/Jan/2009 Chancellor on
brink of second bailout for
banks**]

Outputs: 0x01

Output Script: [0467...5f] [checksig]

Value: 5000000000

Locktime: 00000000

Block header:

- No previous block hash.
- Timestamp:
 - 6:15:05 PM, Jan 3rd, 2009
- Difficulty bits:
 - Lowest accepted difficulty bits.

Transactions:

- First TX is always coinbase.
- Coinbase input script:
 - Version 1: Arbitrary data
 - Genesis block:
 - Difficulty bits.
 - Times heading proves block originated afterwards.
- Difficulty Bits:
 - Lowest accepted difficulty bits.
- [Genesis Tx Demo](#)

Difficulty & Target

Difficulty Bits:

0xffff001d

Target:

coefficient $\times 2^{(8 \times (\text{exponent} - 3))}$

00ffff $\times 2^{(8 \times (\underbrace{29}_{26} - 3))}$

0x00000000ffff0000...00
26B

\leq

Header Hash:

0x00000000839a8e68...48

Valid Header Hash must be \leq target

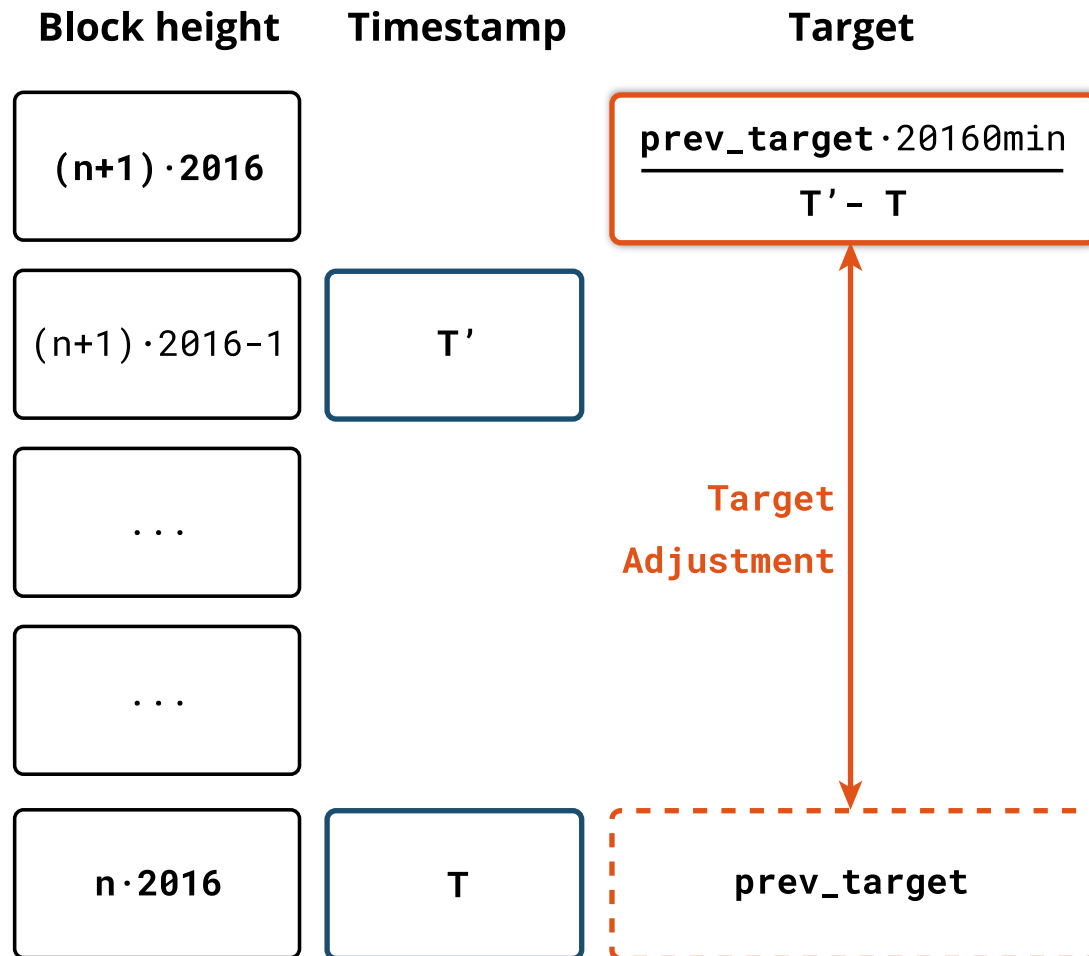
Miner can iterate following data in block:

- Nonce.
- Unused version bits.
- Timestamp.
- Coinbase (Merkle Root).
 - Version bits.
 - Input script.
- Merkle root(TX set/order)

Hashes required to achieve target:

- Example: 0x800...00: Every 2nd Hash...
- Example: 0x400...00: Every 4th Hash...

Difficulty Retargeting



Difficulty Adjustment:

- Every 2016 blocks.
- Adjusted to maintain 10min block interval.
- Adjustment maximum bound: 4x.

"Inflation" Bug:

- Considers interval between 2015 blocks.
- Slightly faster block/inflation schedule.
- Requires hardfork to fix.

Block interval distribution

Which distribution? Crucial fact:

- Every small Δt , there is a constant probability a block will be found
- Directly leads to exponential distribution: $\Pr(t) \propto e^{-t/600s}$
 - Also known from: Radioactive decay, queueing theory
- $\text{CDF}(t) = 1 - e^{-t/600s}$, $\text{CDF}(1\text{hr}) = 1 - e^{-6} \approx 0.9975$


Some surprising facts:

- What is the most likely block interval?
 - $t \rightarrow 0$
- What is the median block interval?
 - $\ln(2)10\text{min} \approx 6.9\text{min}$
- Given you have already waited 10 minutes, what is the expected remaining time?
 - 10 minutes, "memoryless"
- What is the expected block interval you find yourself in right now?
 - 20 minutes

Coinbase Transaction

Coinbase Transaction

Version: 02000000
Inputs: 01
Prev TX hash: 00000000..00
UTXO Index: ffffffff
Input Script: [blockheight(4B)][...]
Outputs: 02
Output Script: [OP_RETURN][aa21a9ed|
dsha256(witness root|coinbase witness)]
[...]
Value: 0000000000000000
Output Script: Miner spendable
Value: Fees + Inflation
Witness: 32B arbitrary data
Locktime: 00000000



A red arrow originates from the 'Witness: 32B arbitrary data' line and points upwards to the 'coinbase witness' parameter within the 'dsha256(witness root|coinbase witness)' function in the 'Output Script'.

Single input script:

- V1: Arbitrary data.
- Beginning V2: Commits to blockheight (BIP34).
 - Solves coinbase overwriting (identical txid).
- Up to 100B total.

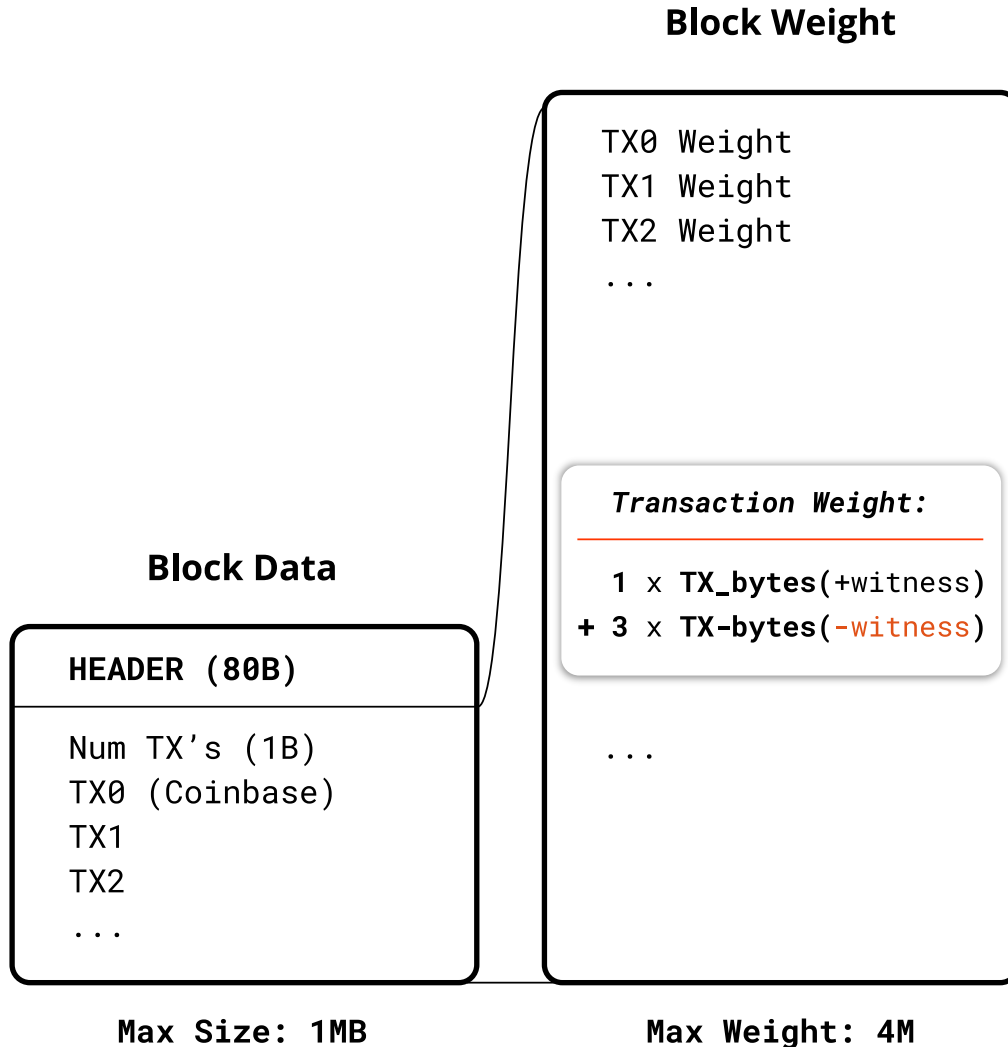
Output script:

- Witness block (BIP141):
 - Witness root and coinbase witness commitment.
 - For witness root: coinbase wtxid = 0x00..00
- Non-witness block:
 - No output committing to witness root required.

Multiple outputs possible:

- Fees from transactions.
- Block subsidy.

Block Size & Weight



Transaction Weight (BIP141):

- Weight equals byte size sum of:
 - 1 x TX serialised (BIP144, with witness).
 - 3 x TX serialised (Pre-BIP144, no witness).

Witness Blocks:

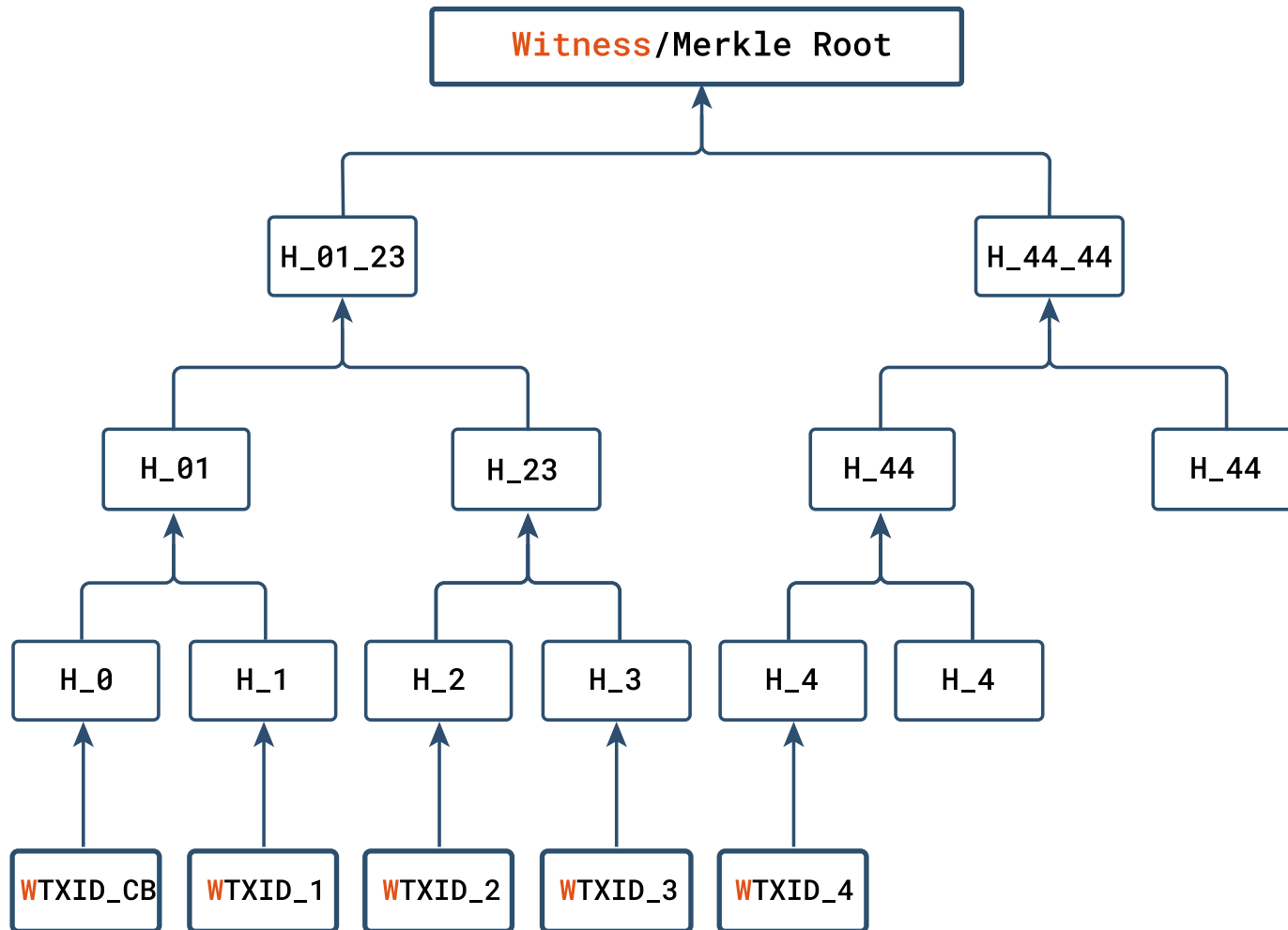
- Maximum weight of 4 Million.
- Actual data size depends on witness data ratio in block

Examples:

- TX Data 1000B / Witness Data 0B:
 - TX Weight: 1000 + 3000 = 4000
- TX Data 1000B / Witness Data 500B:
 - TX Weight: 1000 + 1500 = 2500
- TX Data 1000B / Witness Data 900B:
 - TX Weight: 1000 + 300 = 1300

As Witness data size approaches total tx size, effective block size approaches 4MB.

Merkle Root



Commits to every tx

- With small inclusion proofs
- SPV

Merkle Root:

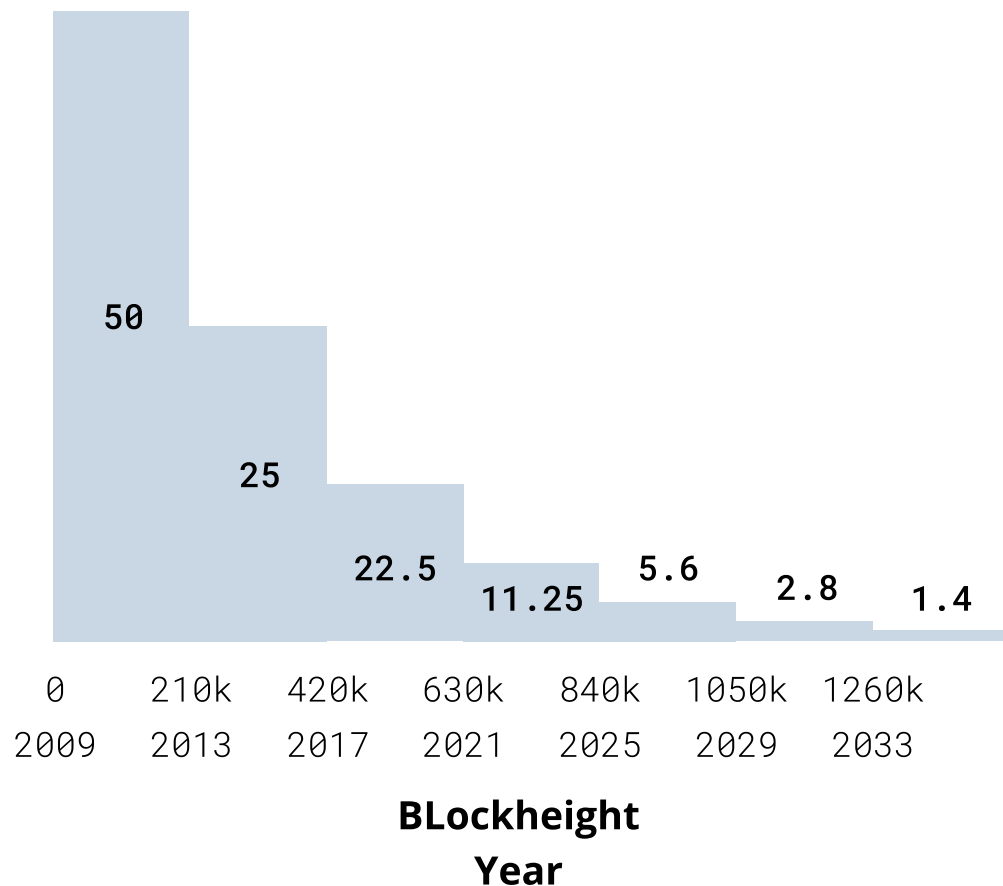
- Bitcoin256: dsha256 -> LE Encoding.
- At each level, duplicate last leaf if uneven.

Merkle/Witness Root.

- TXID leaves -> merkle root (in block header).
- WTXID leaves -> witness root (in coinbase output)

Block Subsidy

Block Reward (BTC)



Genesis Block:

- 50 BTC Block Reward

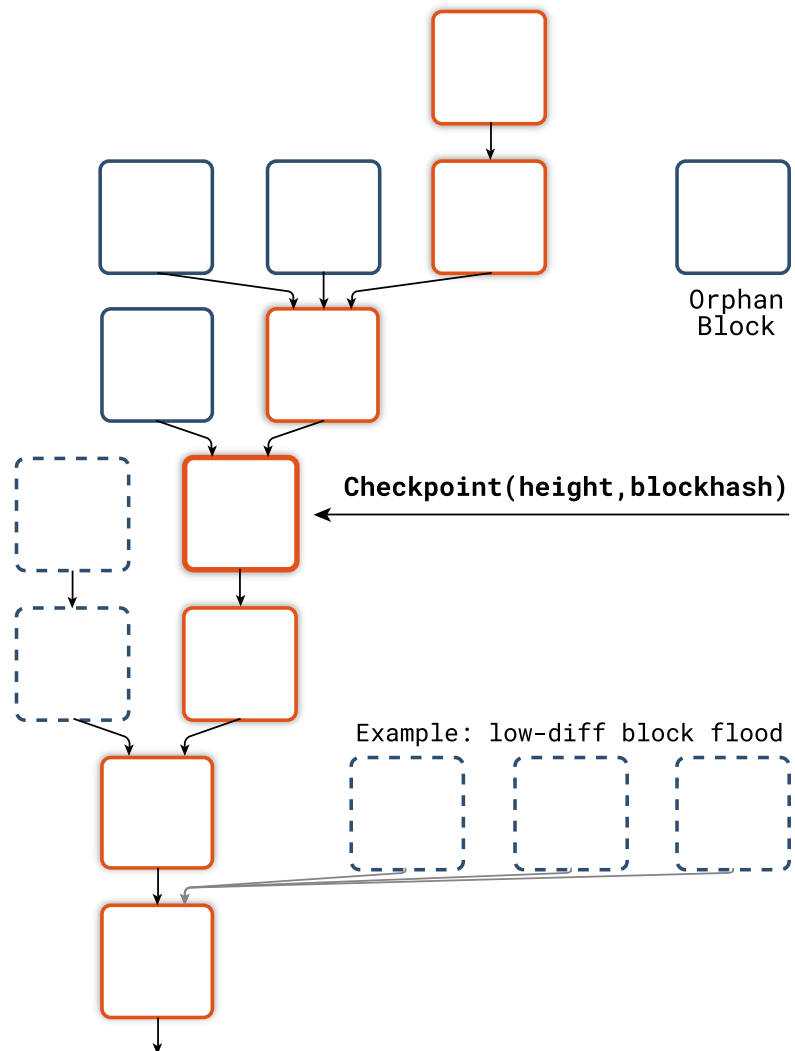
Block reward adjustment:

- Halves every 210,000 blocks/~ 4 years.
- Future Bitcoin supply
 - 90%: Dec. 2021
 - 95%: Mar. 2026
 - 99%: Mar. 2035
- After 33 halvings (in 2140), block reward is removed.

Block subsidy vs fees

- As block rewards decrease, and usage increases, fee market emerges for block inclusion.

Chain Organisation



Forks:

- Different valid blocks of equal height.
- All valid blocks are organised by node.
- Node follows chain with most POW.

Orphan Blocks:

- Node tries to link to main chain.

Checkpoints:

- Forks below checkpoint not organised into chain.
- Does not contribute to security model.
- Legacy: Prevent low-difficulty DOS blocks.
 - Resource exhaustion.
- Currently 13 hardcoded checkpoints.
 - Latest at height 295000.
 - Forks are costly.

Why do we need blocks anyway?