Consensus Cleanup

Antoine Poinsot (@darosior)

MIT - 04/25

590B7292695AFFA5B672CBB2E13FC145CD3F4304

Timeline

- **01/19** – Great Consensus Cleanup (Matt Corallo)
- **11/19** – GCC abandoned
- **03/24** – GCC Revival (Antoine Poinsot)
- **03/24** – Worst Block Inquiry (Antoine Poinsot)
- **03/25** – Consensus Cleanup BIP

Vulnerabilities

- Timewarp (and other timestamp games)
- Expensive blocks
- Merkle tree malleability
- Duplicate transactions

Impact

- Timewarp
  - 38 days to reset difficulty
  - Changes the threat model of a 51% attacker
  - Perverse incentive to exploit to a small extent
- Expensive blocks
  - Accessibility to full validation
  - Miners attacking their competition

Impact

- Merkle tree malleability
  - Fake a block inclusion proof for a transaction with arbitrary number of confirmations
- Duplicate transactions
  - Resume BIP30 validation
  - Utreexo nodes can’t perform full validation

Mitigations

- Timewarp
  - Restrict timestamp at diff adjustment boundaries
- Expensive blocks
  - Restrict the number of legacy signature operations per transaction
- Merkle tree malleability
  - Invalidate 64-byte transactions
- Duplicate transactions
  - Commit to block height in coinbase nLockTime

Zoom-in on Timewarp

- As everyone knows:
  - Difficulty adjustment compares 2016 blocks vs 2 weeks
  - Expected time between blocks is 10 minutes

Zoom-in on Timewarp

- Right?

Zoom-in on Timewarp

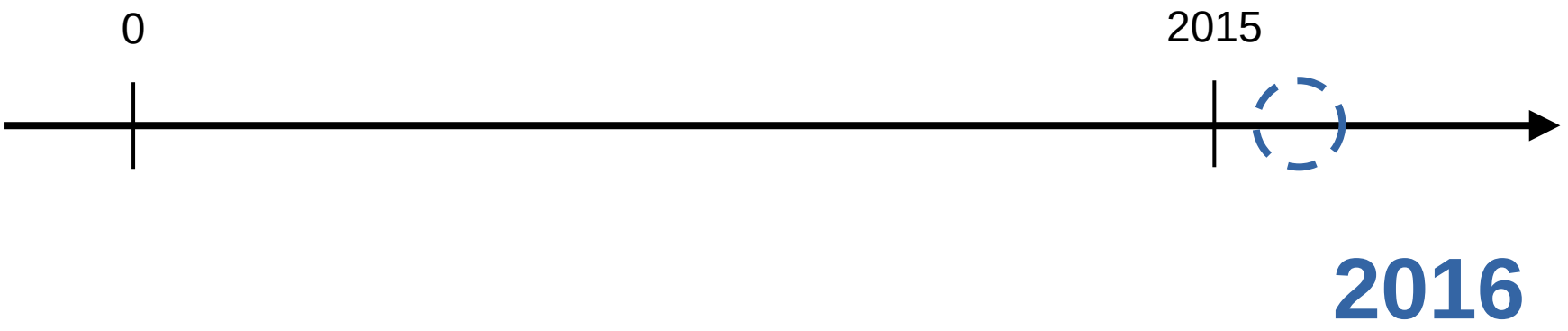
- Right?

Zoom-in on Timewarp

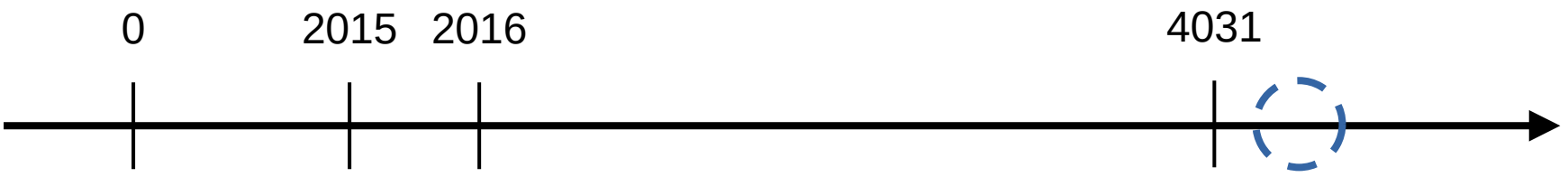
Zoom-in on Timewarp

- Not exactly.

Difficulty adjustment

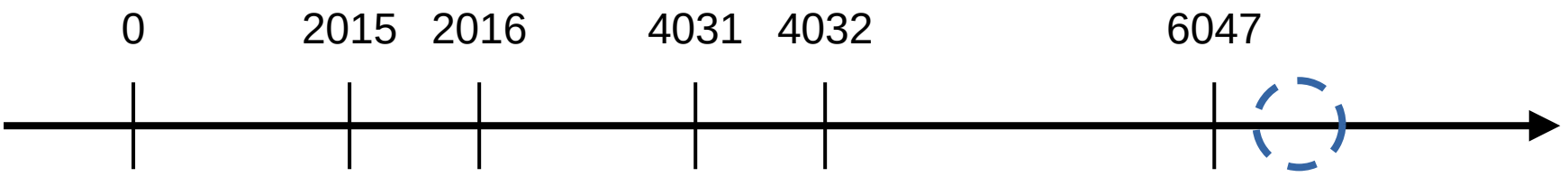


Difficulty adjustment



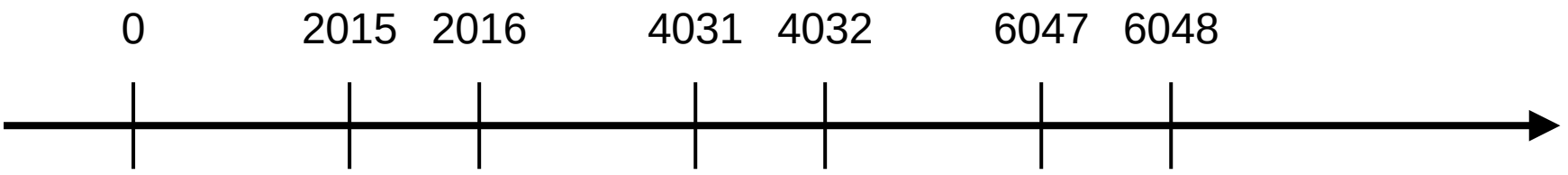
4032

Difficulty adjustment

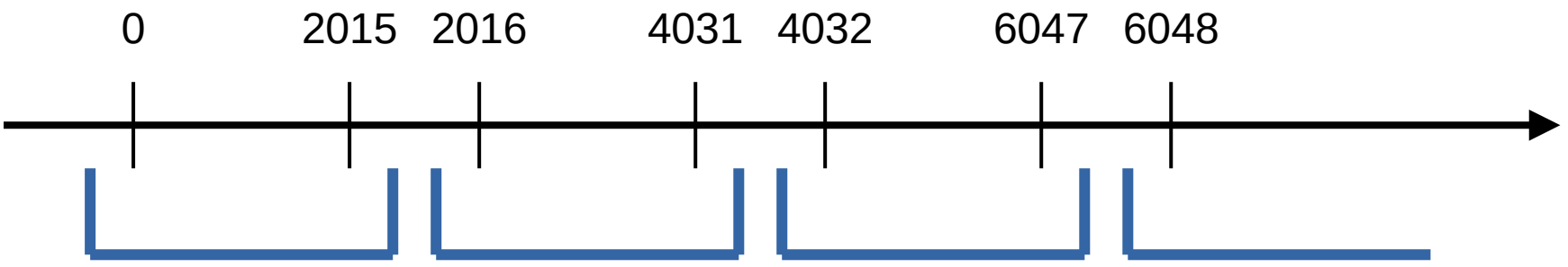


6048

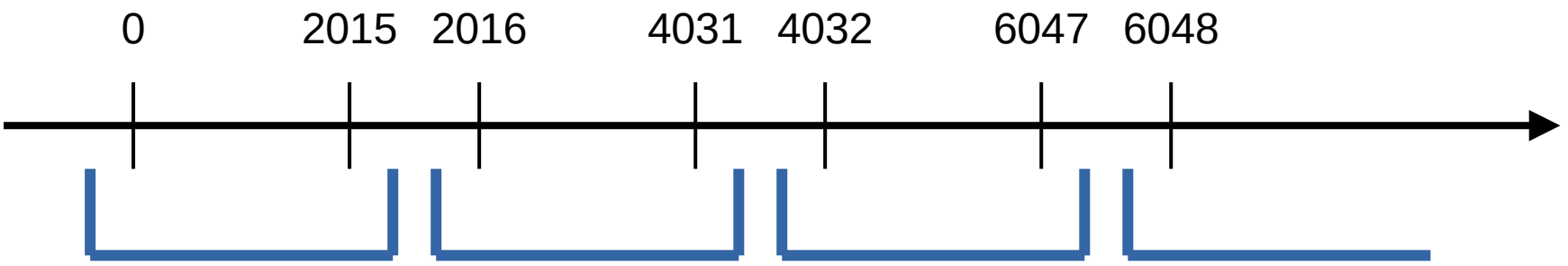
Difficulty adjustment



Difficulty adjustment

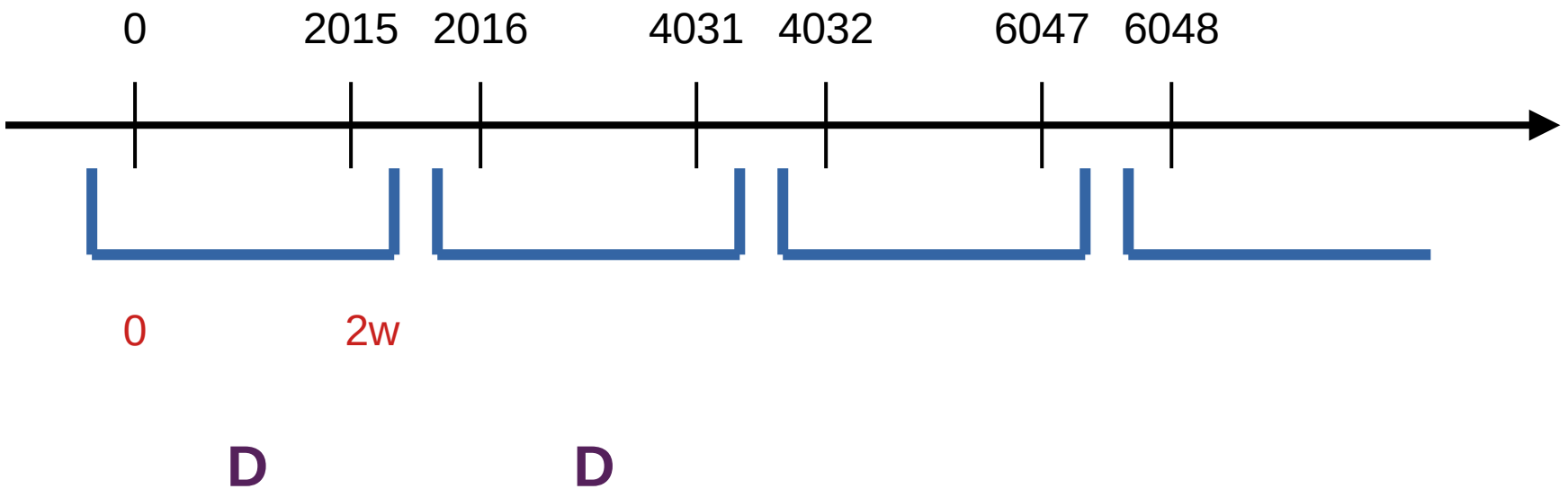


Difficulty adjustment

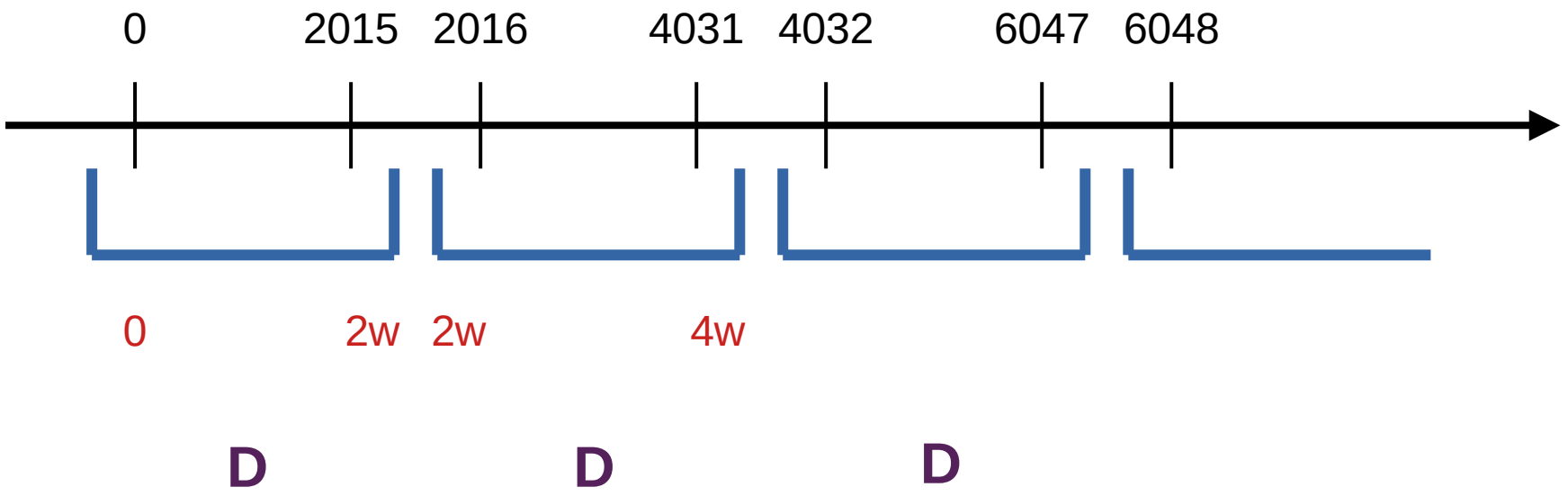


D

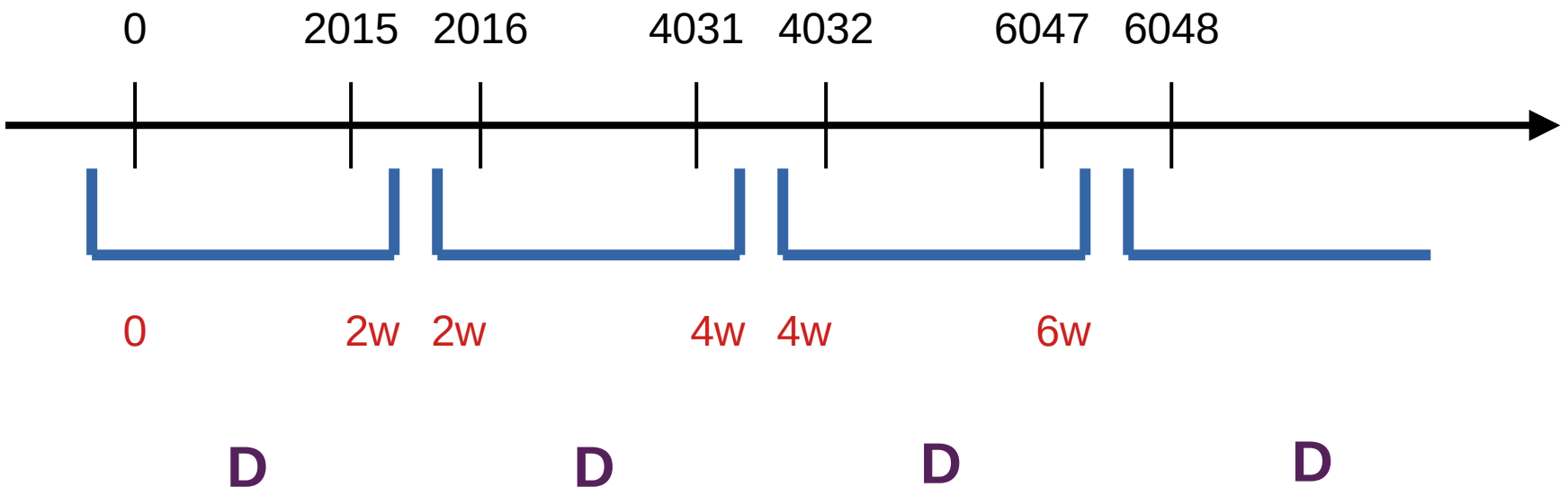
Difficulty adjustment



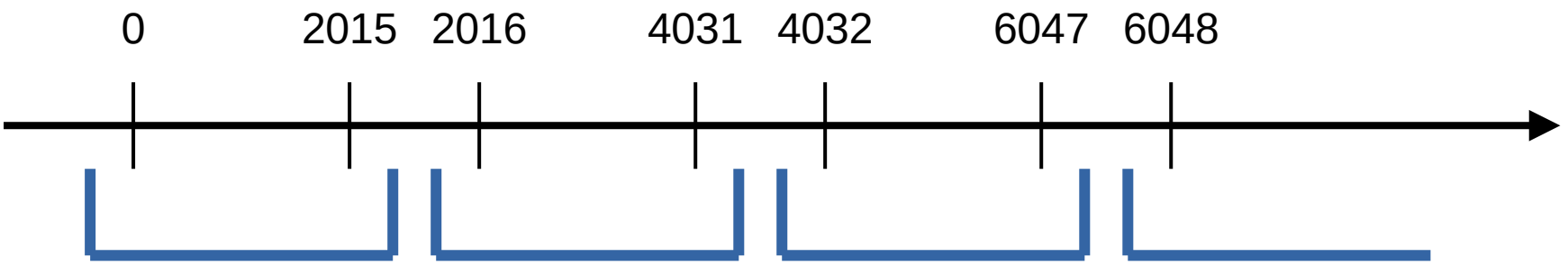
Difficulty adjustment



Difficulty adjustment

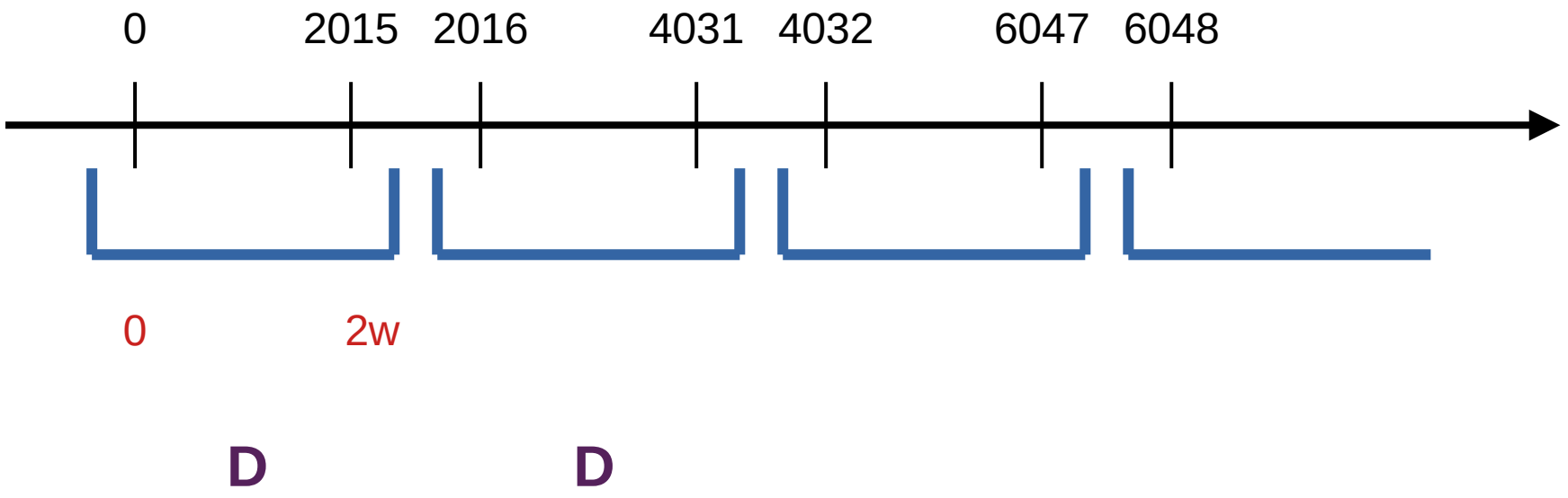


Difficulty adjustment

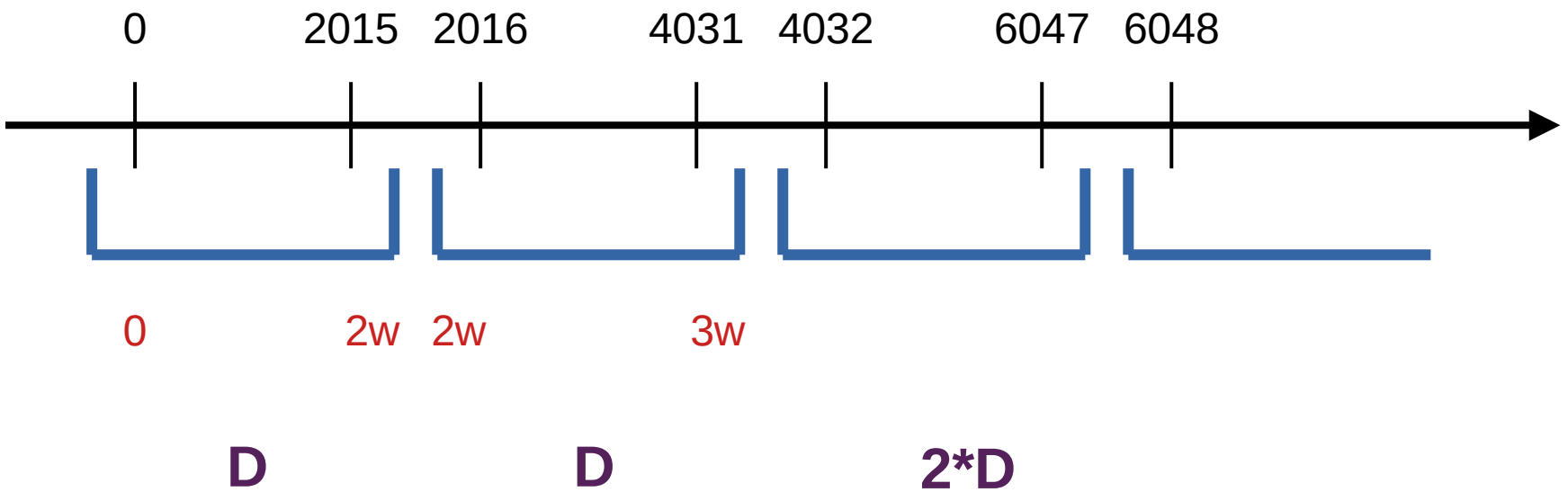


D

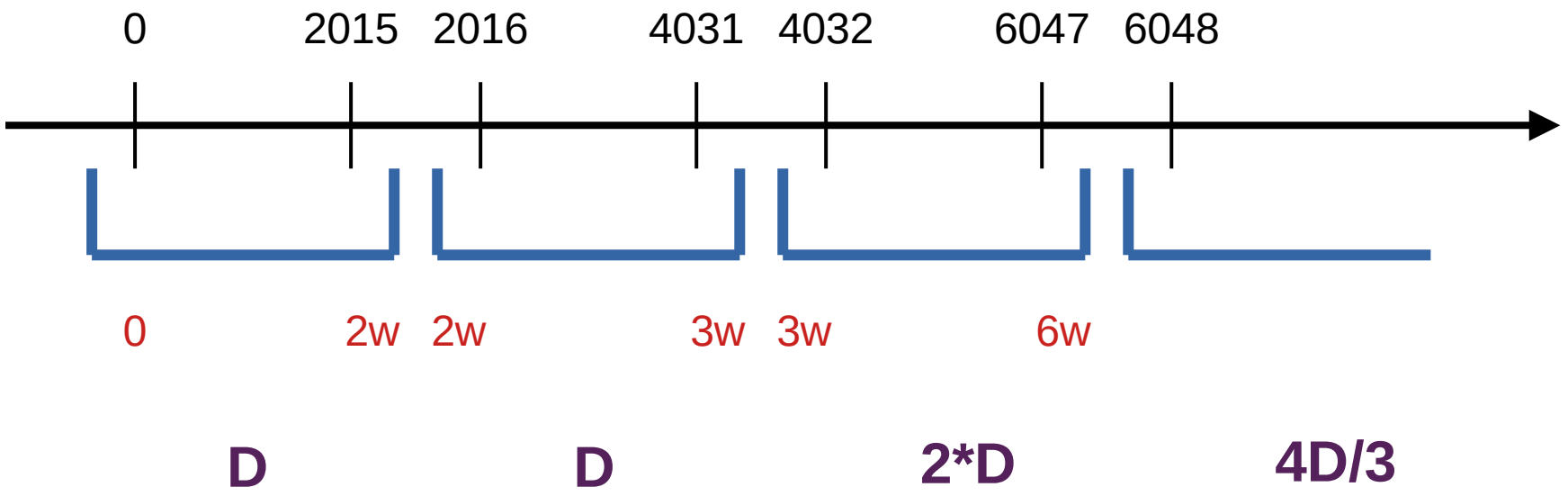
Difficulty adjustment



Difficulty adjustment



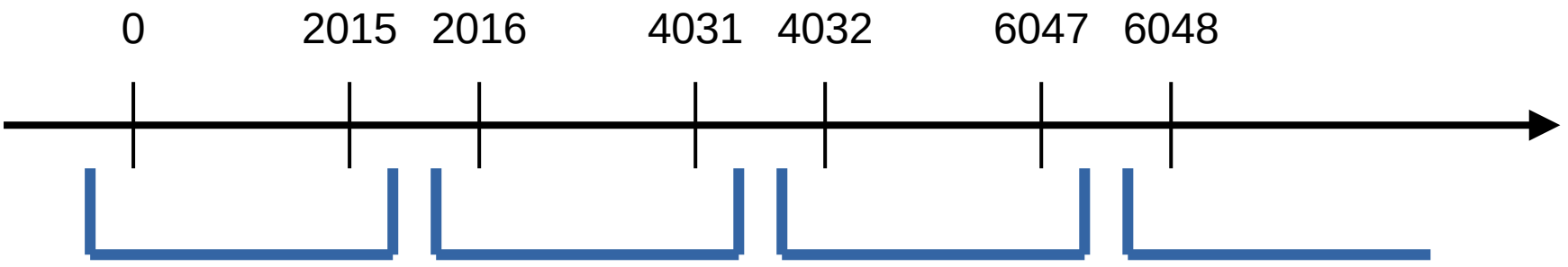
Difficulty adjustment



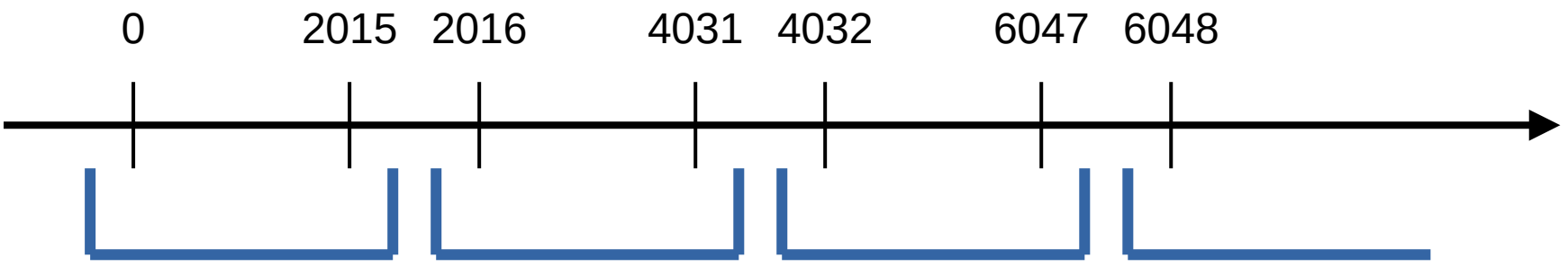
Difficulty adjustment

- Timestamp restrictions
  - MTP: $t_n > \text{median}([t_{n-11} .. t_{n-1}])$
  - Future: $t_n <=$ wall clock + 2 hours

Timewarp attack

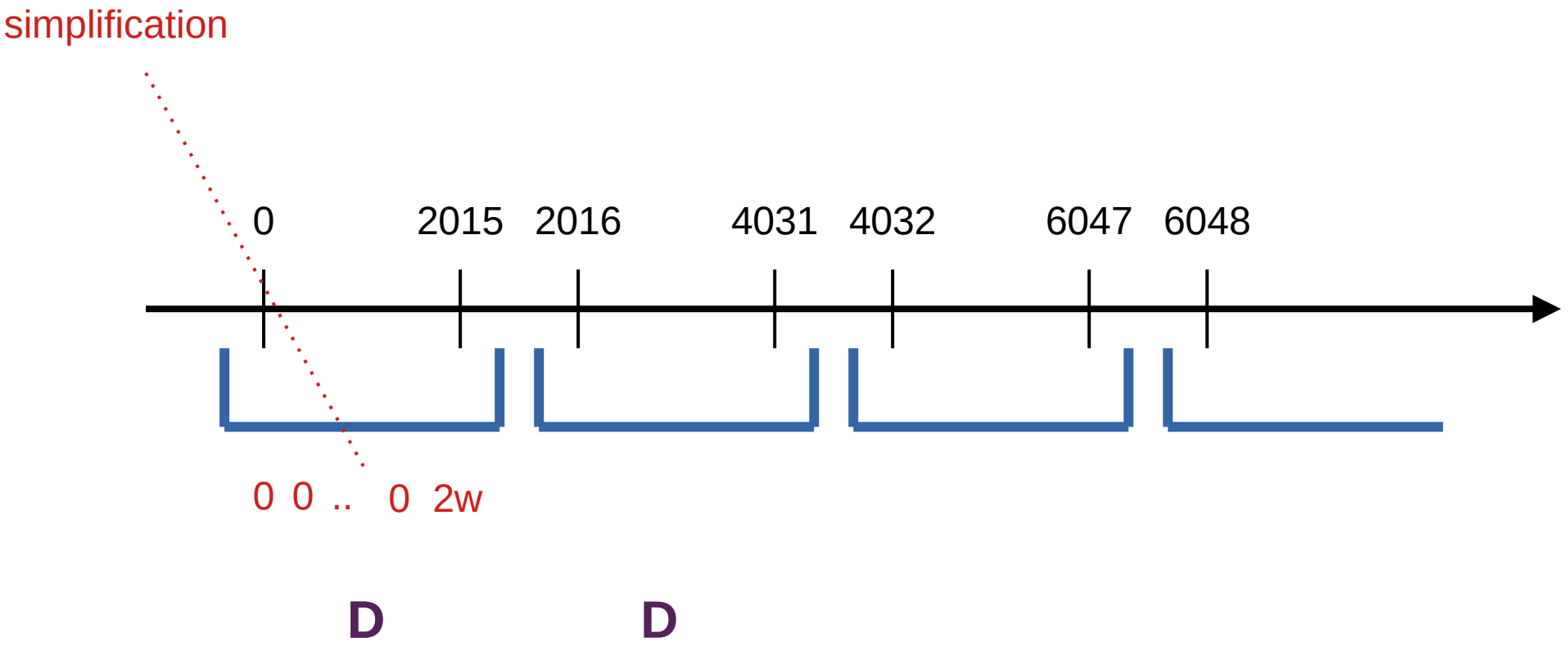


Timewarp attack

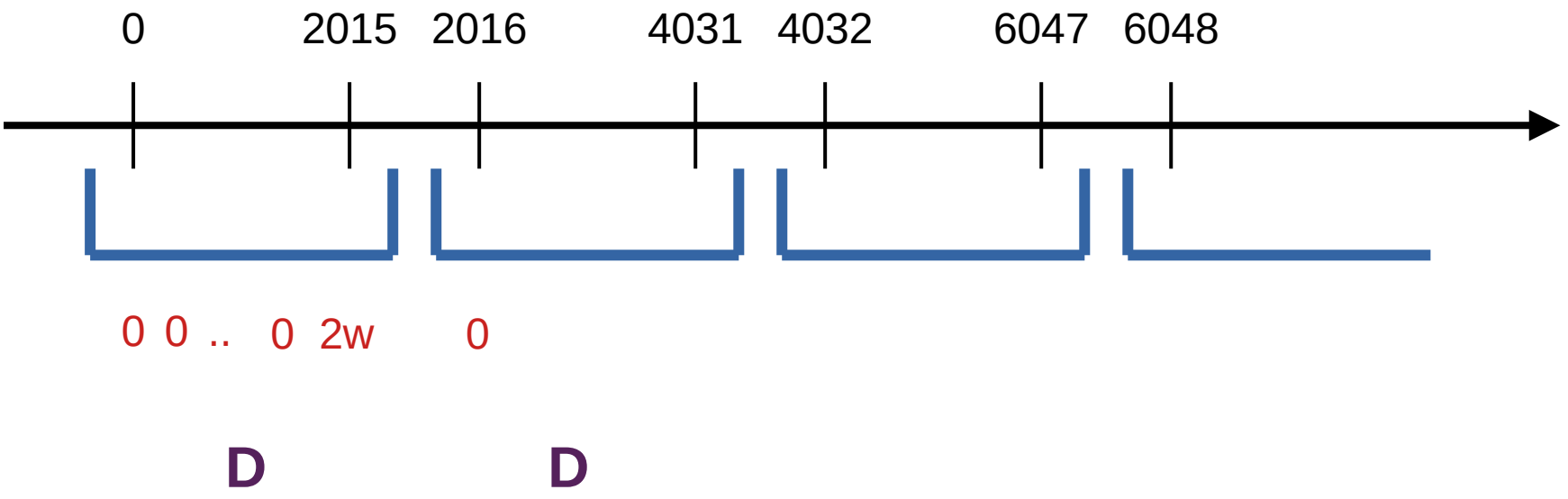


D

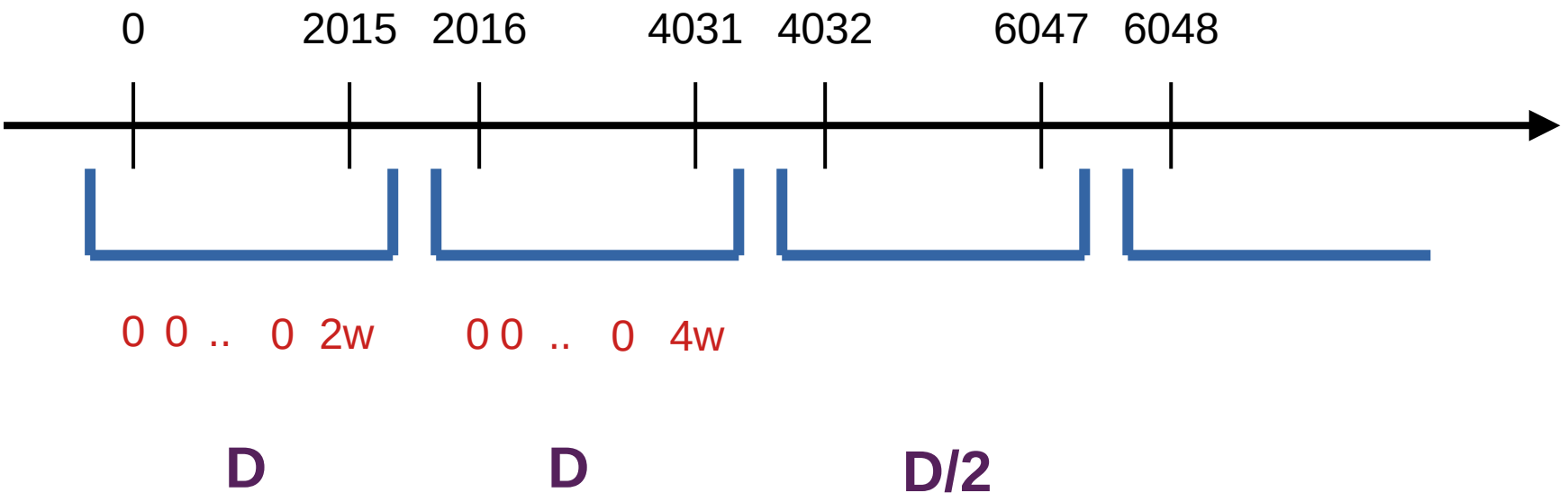
Timewarp attack



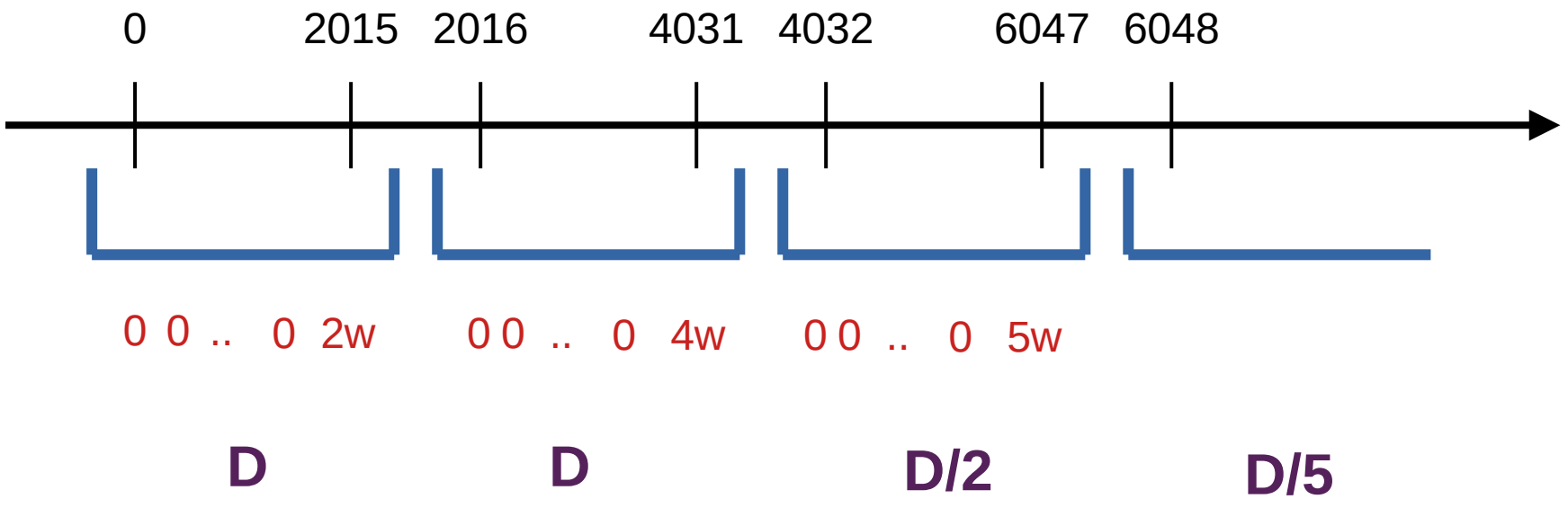
Timewarp attack



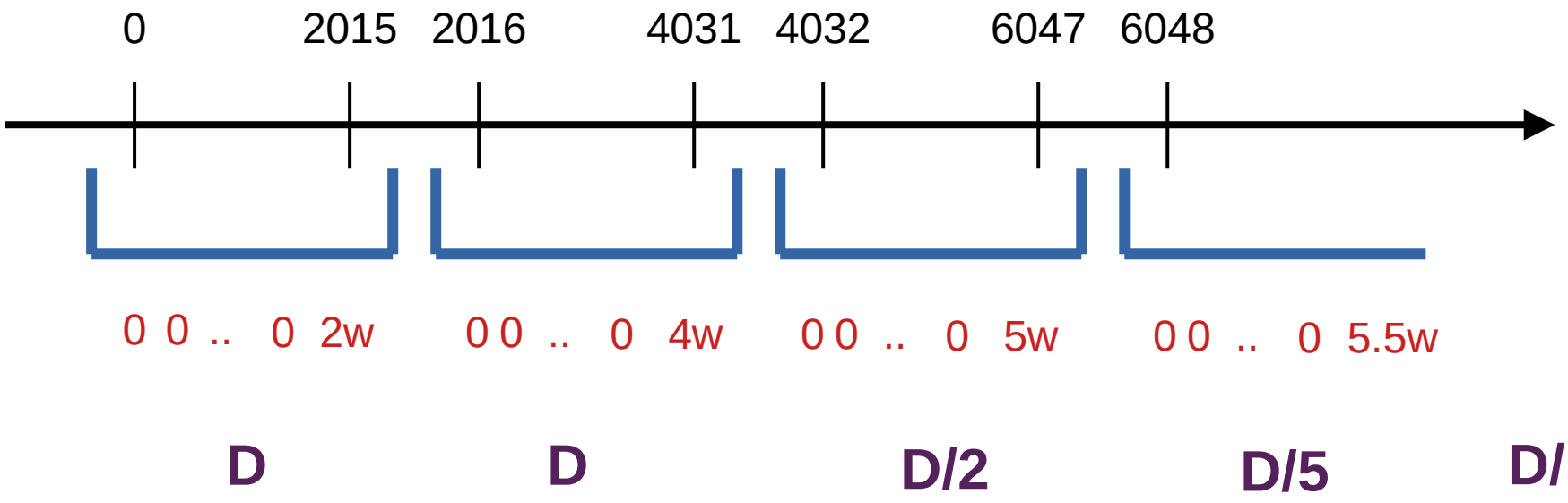
Timewarp attack



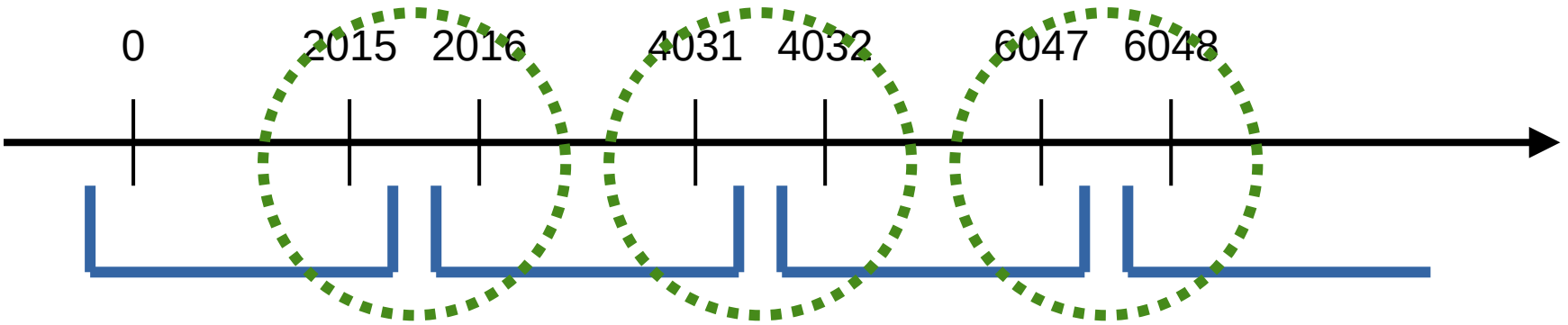
Timewarp attack



Timewarp attack



Timewarp attack



$t_n >= t_{n-1} - 2h$

Consensus Cleanup

- BIP: https://github.com/bitcoin/bips/pull/1800
- Delving:
  - https://delvingbitcoin.org/t/great-consensus-cleanup-revival
  - https://delvingbitcoin.org/t/worst-block-validation-time-inquiry
- Twitter/Bluesky: @darosior