Consensus Cleanup

Antoine Poinsot (@darosior)

OPNEXT - 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

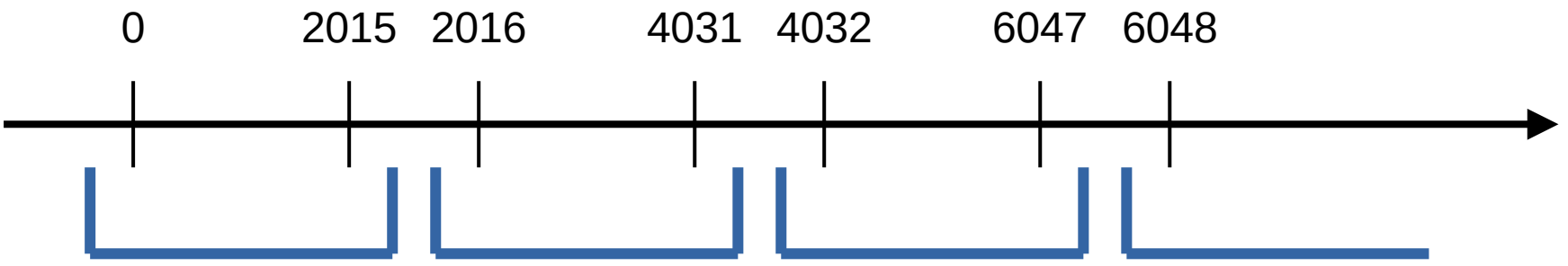
Vulnerabilities

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

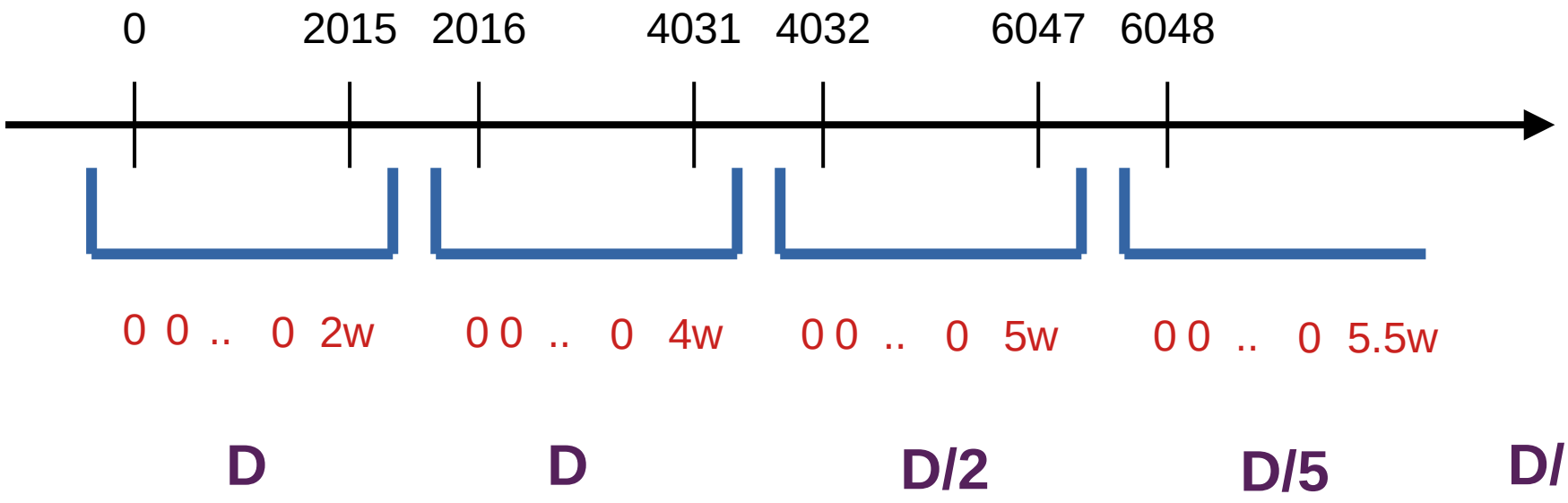
Timewarp

- 38 days to reset difficulty
- Changes the threat model of a 51% attacker
- Perverse incentive to exploit to a small extent

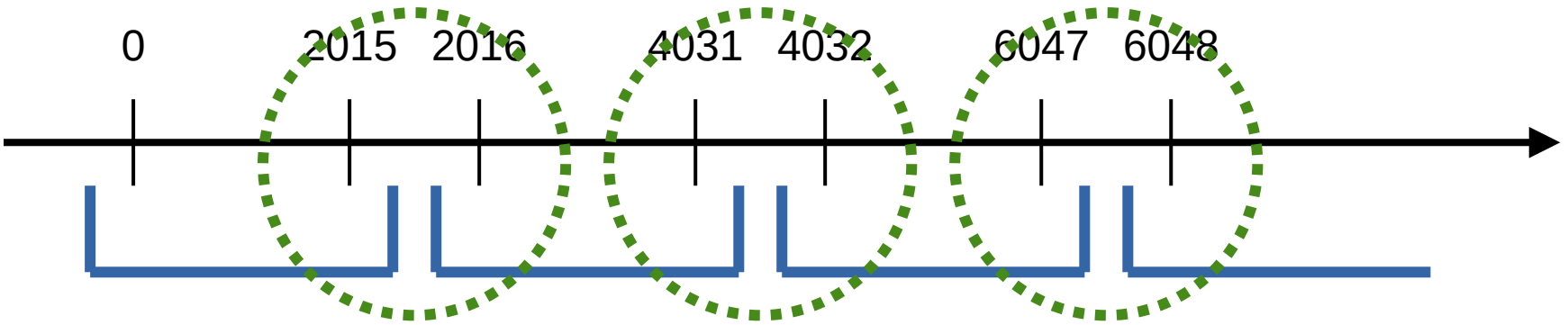
Timewarp



Timewarp


0
2015
2016
4031
4032
6047
6048
0 0 .. 0 2w
0 0 .. 0 4w
0 0 .. 0 5w
0 0 .. 0 5.5w
D
D
D/2
D/5
D/13.75

Timewarp attack



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

Vulnerabilities

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

Expensive blocks

- Accessibility to full validation
  - Worst case: 1h30 to validate on rpi
- Perverse incentive for miners to attack competition
  - Worst case: a few minutes on high-end hardware

Expensive blocks

→ Limit the amount of legacy sigops per transaction.

Vulnerabilities

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

Merkle tree malleability

- CVE-2017-12842
- Has been an issue for full nodes
- Fake block inclusion Merkle proofs

Merkle tree malleability

→ Make 64-byte transactions invalid

Vulnerabilities

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

Duplicate transactions

- Was possible to duplicate Bitcoin transactions
- BIP30 validation will have to be resumed
  - Unnecessary work
  - Utreexo can’t do it

Duplicate transactions

- Commit to the block height (minus 1) in the coinbase’s nLockTime
- Mandate timelock be active

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