Bitcoin:
Programming the Future of Money

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

Dr. Christian Kümmerle

Lecture 23

Attacks

RECAP: 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”

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.**

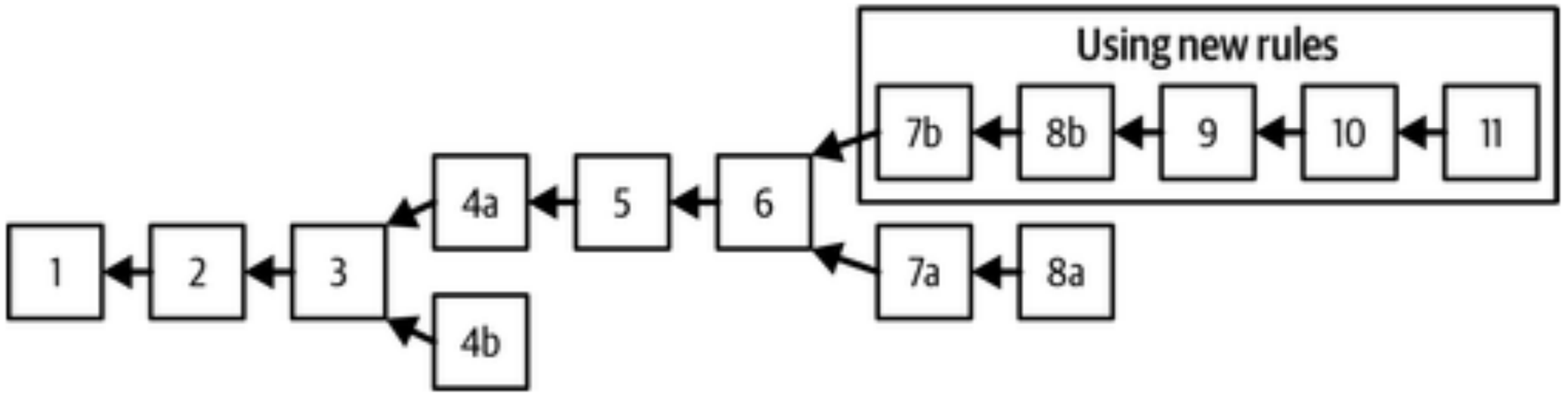
-> Typically leads to chain split

- **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

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



Some important soft forks of Bitcoin

- April 2012: Activation of P2SH format (BIP16)
- 2016/2017: SegWit Update
- November 2021: Taproot Update (BIP 340,BIP 341,BIP 342)
  Schnorr Signatures, Merklized Alternative Script Trees, Taproot Scripts

EXAMPLE SOFTFORK: ACTIVATION OF P2SH (BIP16)

Standard script validation rule before BIP16:

- ScriptPubKey

```
OP_HASH160 [20-byte-hash-value] OP_EQUAL
```

can be satisfied by providing the script whose hash160 image is [20-byte-hash-value]

Script validation rule after BIP16:

- As above, but also execute script <RedeemScript> and interpret remaining of ScriptSig information as Stack elements that need to successfully execute <RedeemScript>

How do we implement a soft fork?

STAKE HOLDERS IN THE SOCIAL CONSENSUS

- **Economic Nodes**: Nodes that **validate and rely transactions** and **send and receive substantial amount** of bitcoin payments.
  Examples: Exchanges, custody providers, large merchants accepting bitcoin
- **Investors: Hold, buy and sell bitcoin** (maybe without self-custody, w or w/o node)
- **Media Influencers: Have reputation/following**. E.g., media, press organization, organizer of conferences
- **Miners: Users or producers of specialized hardware** to find new blocks and earn block reward and transaction fees.
- **Protocol Developers: Propose and implement consensus changes**, maintain client
- **Users and Application Developers:** Start-ups using bitcoin e.g. for remittances, NFT platforms, wallet providers, users of bitcoin as store of value

To understand this better, check paper:
"Analyzing Bitcoin Consensus: Risks in Protocol Upgrades", Ren Crypto Fish, Steve Lee, Lyn Alden, November 2024, also available at https://github.com/bitcoin-cap/bcap
Linked in Readings of Week 12

THE BITCOIN IMPROVEMENT PROPOSAL PROCESS

See: https://github.com/bitcoin/bips/tree/master

People wishing to submit BIPs, first should propose their idea or document to the bitcoindev@googlegroups.com mailing list (do *not* assign a number - read BIP 2 for the full process). After discussion, please open a PR. After copy-editing and acceptance, it will be published here.

We are fairly liberal with approving BIPs, and try not to be too involved in decision making on behalf of the community. The exception is in very rare cases of dispute resolution when a decision is contentious and cannot be agreed upon. In those cases, the conservative option will always be preferred.

Having a BIP here does not make it a formally accepted standard until its status becomes Final or Active.

Those proposing changes should consider that ultimately consent may rest with the consensus of the Bitcoin users (see also: economic majority).

Number	Layer	Title	Owner	Type	Status
1		BIP Purpose and Guidelines	Amir Taaki	Process	Replaced
2		BIP process, revised	Luke Dashjr	Process	Active
3		Updated BIP Process	Murch	Process	Proposed
8		Version bits with lock-in by height	Shaolin Fry, Luke Dashjr	Informational	Draft

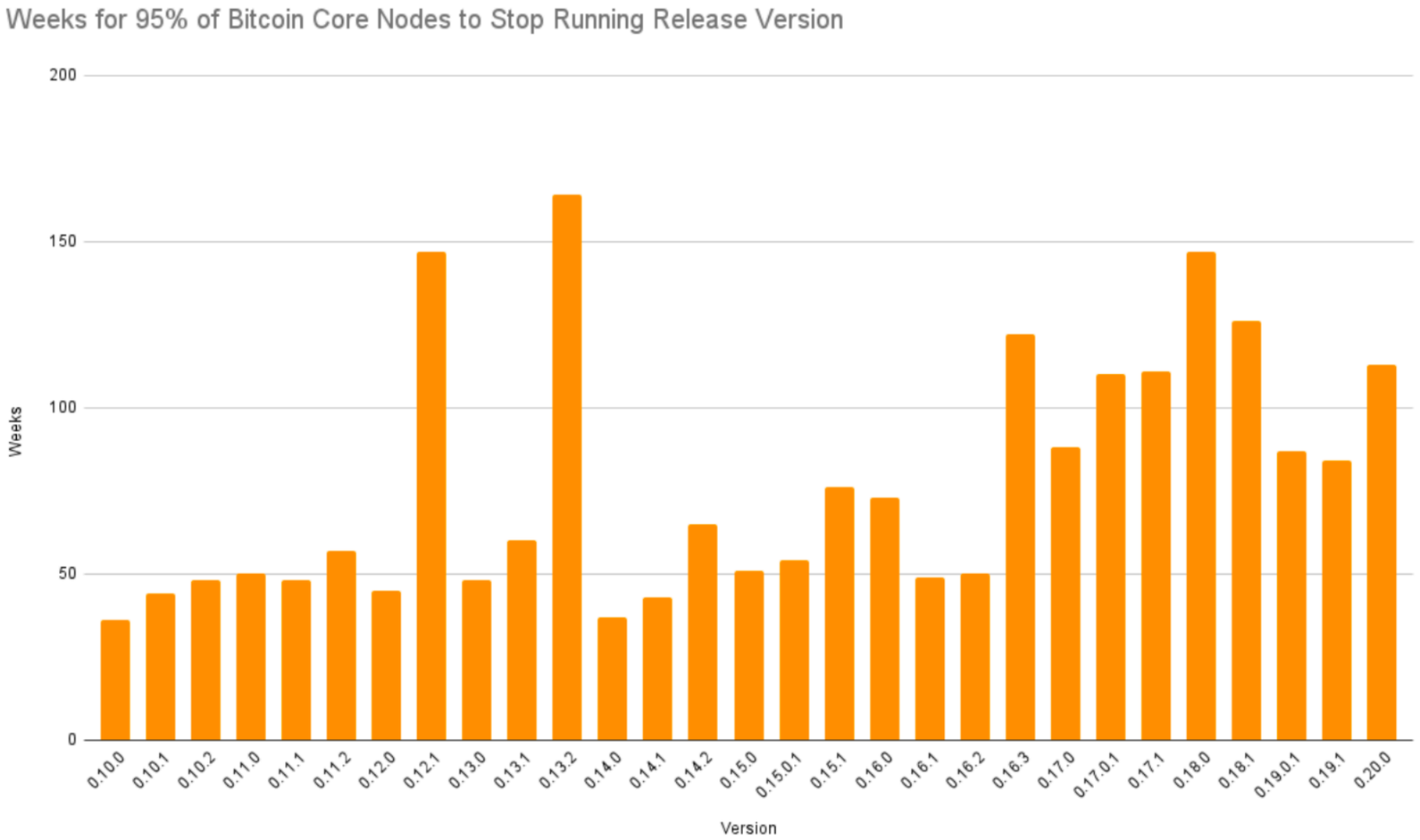


Figure 1: Weeks taken for 95% of Bitcoin Core Nodes to Upgrade

THE BITCOIN IMPROVEMENT PROPOSAL PROCESS

Type of BIPs:

- **Process BIP**
- **Standard BIP**:
  Propose useful convention standard that does not involve consensus change
  (e.g.: BIP 39 on mnemonic backup phrase standard)
- **Consensus BIP**:
  Change of consensus rules, activation by network necessary

A NEW STAKEHOLDER GROUP?

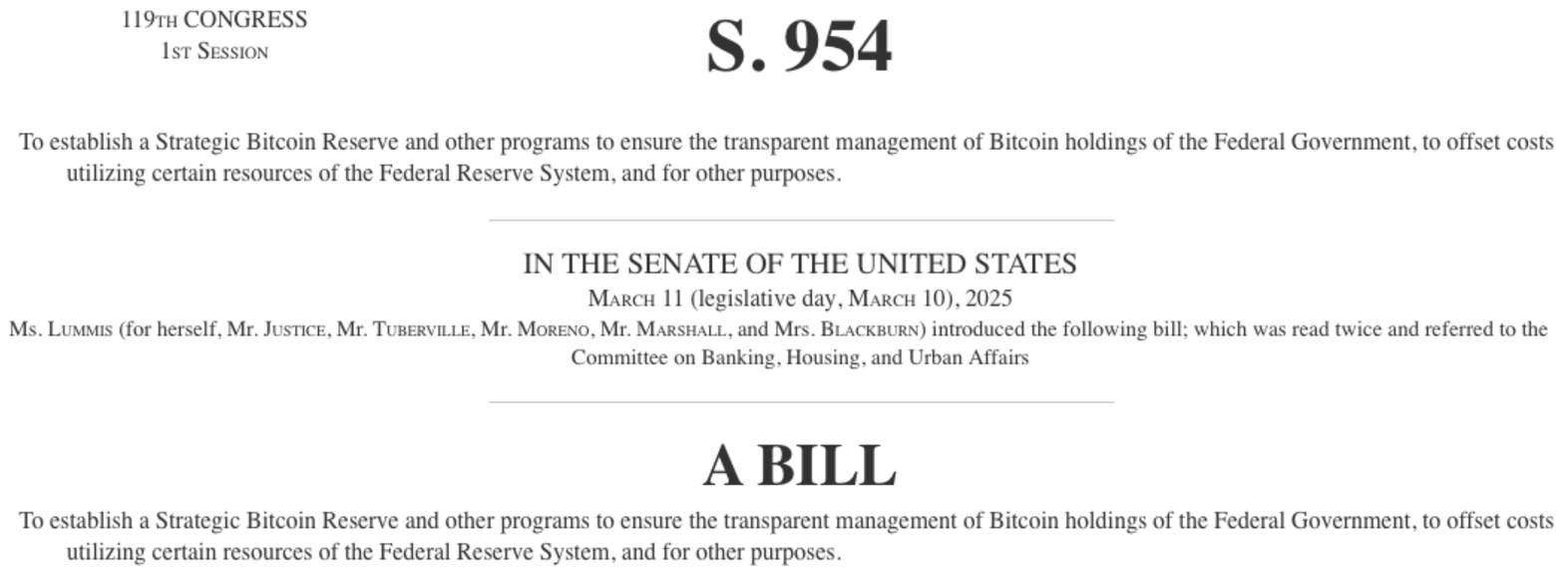
- **Governments:** So far mostly acting as investors.

THE BITCOIN ACT OF 2025: IN U.S. SENATE BANKING COMMITTEE

Proposed by Sen. Cynthia Lummis (R.): “Boosting Innovation, Technology, and Competitiveness through Optimized In Nationwide (BITCOIN) Act of 2025”

Goals:

- **Strategic Bitcoin Reserve**:
  Secured across geographically distributed storage facilities, holding period of 20 years
- **Bitcoin Purchase Program:**
  Purchase 200,000 Bitcoins per year for 5 years, total of 1,000,000 BTC



119TH CONGRESS
1ST SESSION

S. 954

To establish a Strategic Bitcoin Reserve and other programs to ensure the transparent management of Bitcoin holdings of the Federal Government, to offset costs utilizing certain resources of the Federal Reserve System, and for other purposes.

IN THE SENATE OF THE UNITED STATES
MARCH 11 (legislative day, MARCH 10), 2025
Ms. LUMMIS (for herself, Mr. JUSTICE, Mr. TUBERVILLE, Mr. MORENO, Mr. MARSHALL, and Mrs. BLACKBURN) introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

A BILL

To establish a Strategic Bitcoin Reserve and other programs to ensure the transparent management of Bitcoin holdings of the Federal Government, to offset costs utilizing certain resources of the Federal Reserve System, and for other purposes.

Source: https://www.congress.gov/bill/119th-congress/senate-bill/954/text

STAKE HOLDERS IN THE SOCIAL CONSENSUS

(f) RETENTION OF FORKS AND AIRDROPS.—

(1) IN GENERAL.—The Secretary shall ensure that, with respect to Bitcoins controlled by the Strategic Bitcoin Reserve, all digital assets resulting from forks of the Bitcoin distributed ledger and digital assets distributed via airdrops to Bitcoin addresses are accounted for and reasonably stored in the Strategic Bitcoin Reserve.

(2) PROHIBITION ON IMMEDIATE SALE.—No digital asset stored in the Strategic Bitcoin Reserve that is the result of a fork or airdrop may be sold or otherwise disposed of during the 5-year period beginning on the date of the fork or airdrop, unless explicitly authorized by law.

ACTIVATION MECHANISMS FOR CONSENSUS BIPS

Different activation mechanisms have been used / might be used:

- **Flag Day**
- **Miner-Activated Soft Forks**
- **User-Activated Soft Forks**
- **User-Resisted Soft Forks**

ACTIVATION MECHANISM: FLAG DAY

A hard-coded timestamp or block height triggers activation of soft fork.

Example: Roll-out of Pay-to-Script-Hash (P2SH) address format in April 2012
Bitcoin Core 0.6.0 version published on March 30, activated on April 1

Advantages:

- Simple to understand and implement
- Predictable change time-line for stakeholders

Risks and Considerations:

- **Risk of chain splits** if significant part of network doesn't upgrade in time
- **Lack of flexibility**: No mechanism to gauge network readiness, adjust timeline

ACTIVATION MECHANISM: MINER-ACTIVATED SOFT FORK

Miners indicate support of soft fork in version field of block. Once a threshold percentage of blocks in time period indicate support (e.g., 75% or 95%), activation starts (example process BIP 9)

Examples: SegWit upgrade in 2017. 80% of last 336 blocks were required to signal (see BIP 91); Taproot upgrade in 2021 (“Speedy trial” variant)

Advantages:

- Flexibility, allows for miner coordination
- Tends to allow for quicker upgrades if consensus is large

Risks and Considerations:

- **Potential for Miner Veto** of soft fork
- **Complexity**
- **Potential for “False” signaling**
- **Lack of user input**

ACTIVATION MECHANISM: USER-ACTIVATED SOFT FORK

As miner-activated, but with option that users start rejecting blocks that are not compliant to upgrade after certain block height

Examples: Not yet used, but influential UASF proposal during SegWit activation discussion

Advantages:

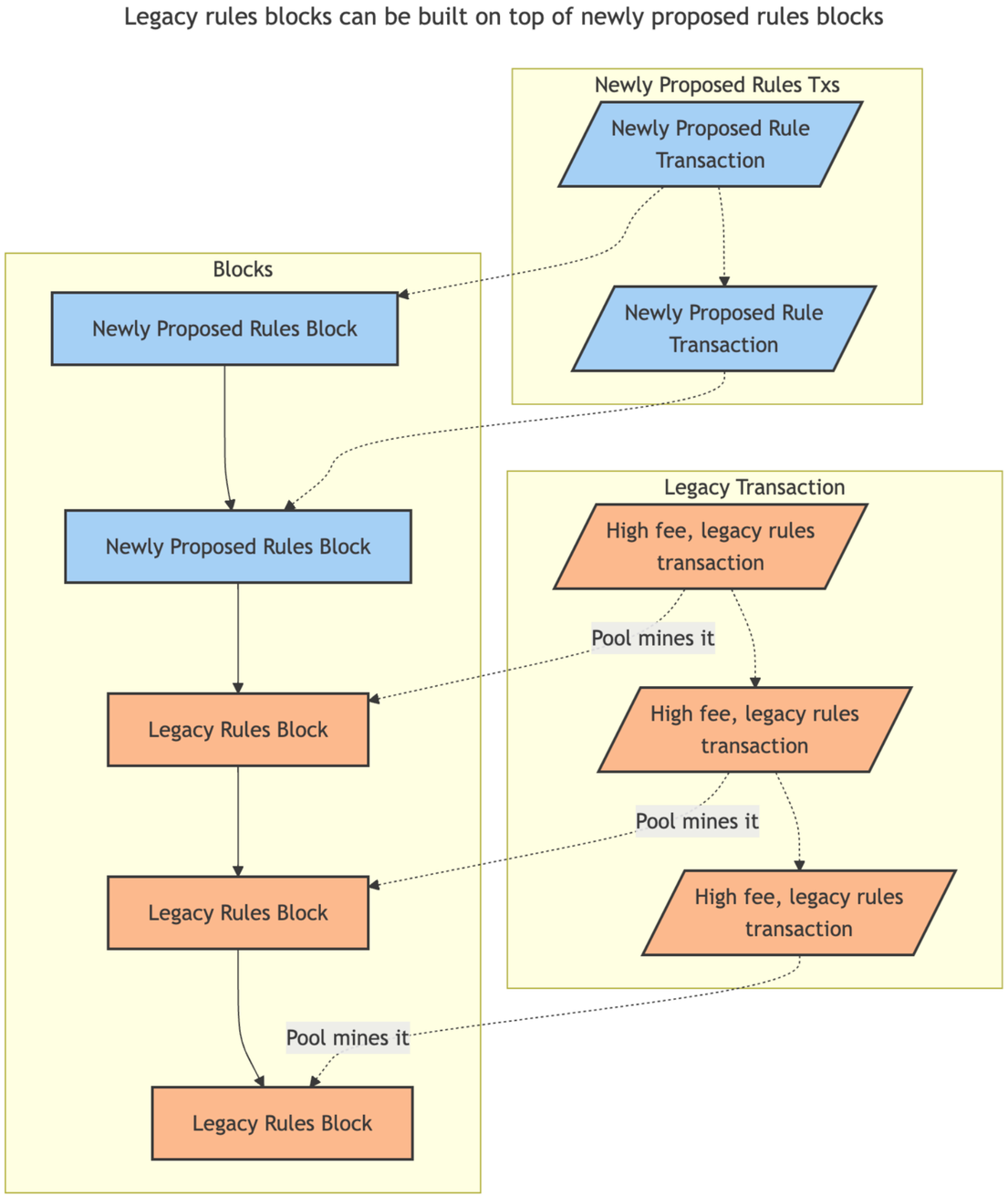
- Prevents **overarching power of miners**
- **Flexibility** of activation

Risks and Considerations:

- **Potential for chain splits**
- **Chain reorganizations are likely**
- **Complexity**
- **Pressure on miners**

Attacks

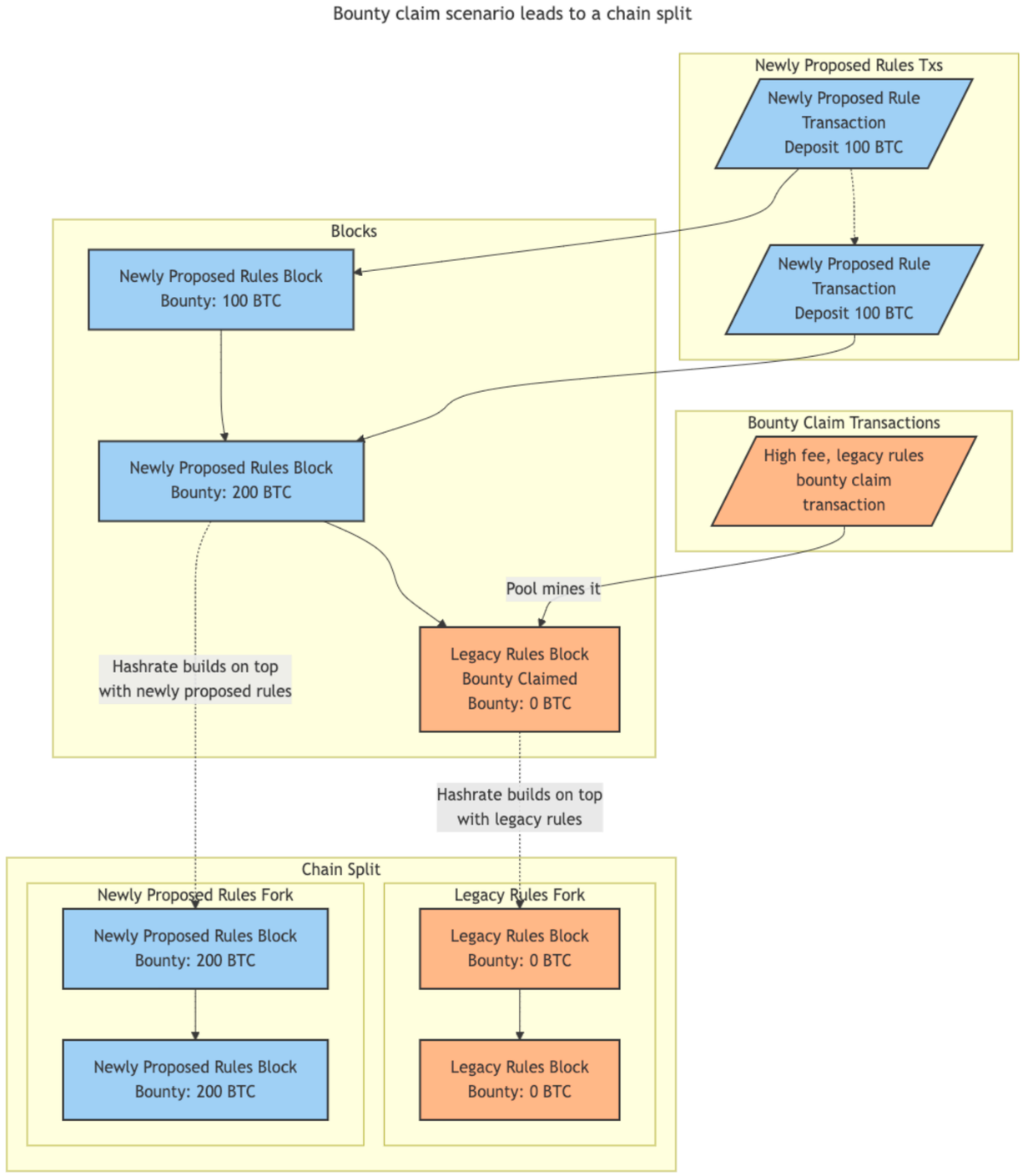
Risks of partially adopted Soft forks



Scenario: Partially adopted Soft Fork

“Bounty Claim”: Assets locked by new type of scripts that are freely spendable in old rule set.

More details in Section 3.5 of
"Analyzing Bitcoin Consensus: Risks in Protocol Upgrades",
Ren Crypto Fish, Steve Lee, Lyn Alden, November 2024



Are “NFTs on Bitcoin” an attack?

WHAT IS AN NFT?

A **non-fungible token** (short: NFT) is

- a **unique digital identifier recorded on a blockchain**, which is used to certify authenticity and ownership (as of a specific digital asset and specific rights relating to it), or

- the **asset** that is **represented by an NFT**.

Source: https://www.merriam-webster.com/dictionary/NFT

EXAMPLES OF IMAGES ASSOCIATED WITH NFTS

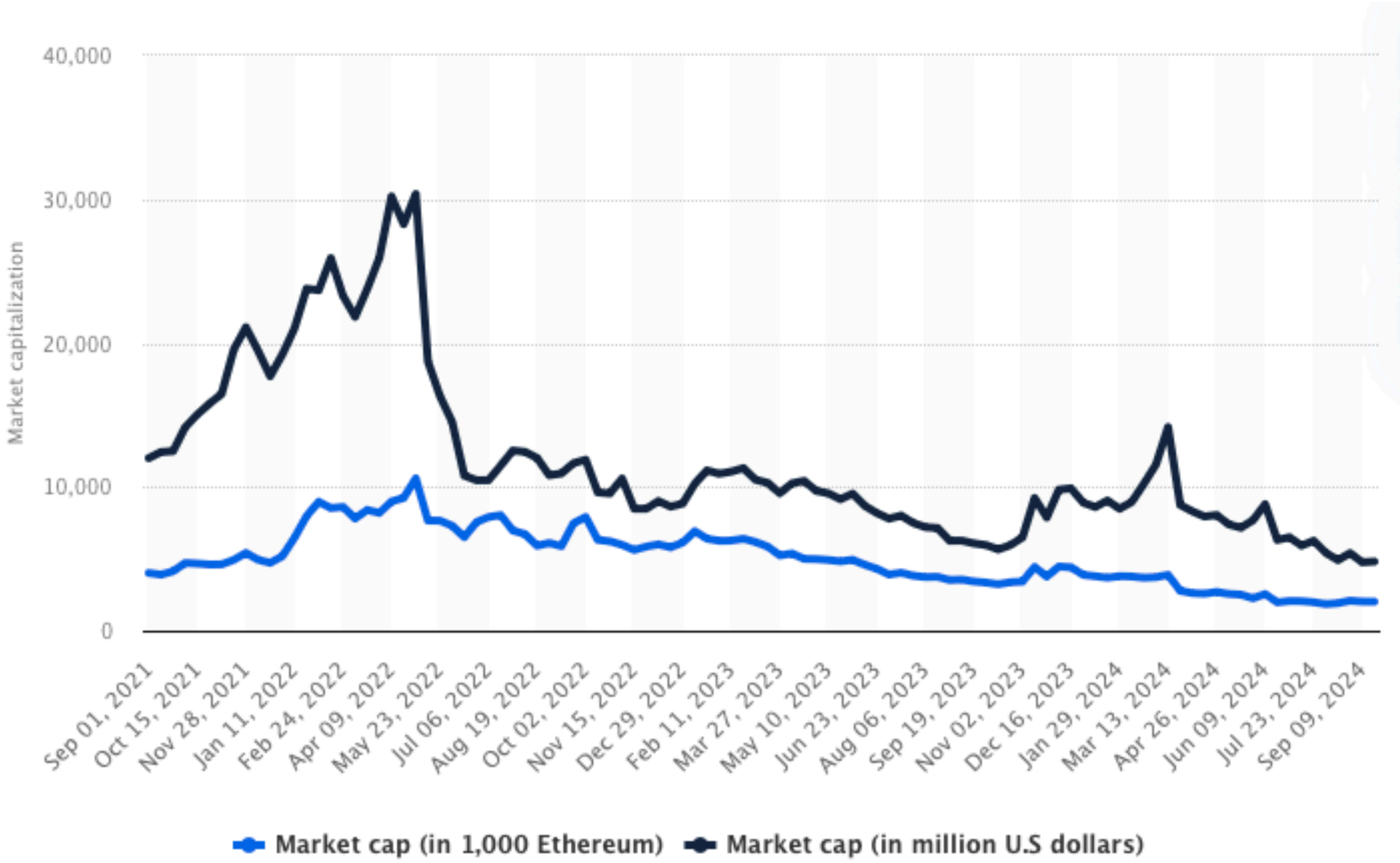
SELLING ALL MY RARE CATS CHEAP

BEST BREEDER: CHECK PROFIL

SHORT HISTORY OF NFTS

- 2016-2018: First NFTs, “Rare Pepe” trading card images referred to on the Bitcoin blockchain
- 2021: Boom of NFTs issued on the Ethereum blockchain
- Since 2023 (Taproot soft fork): Bitcoin Ordinals

NFTS ON ETHEREUM: MARKET CAPITALIZATION



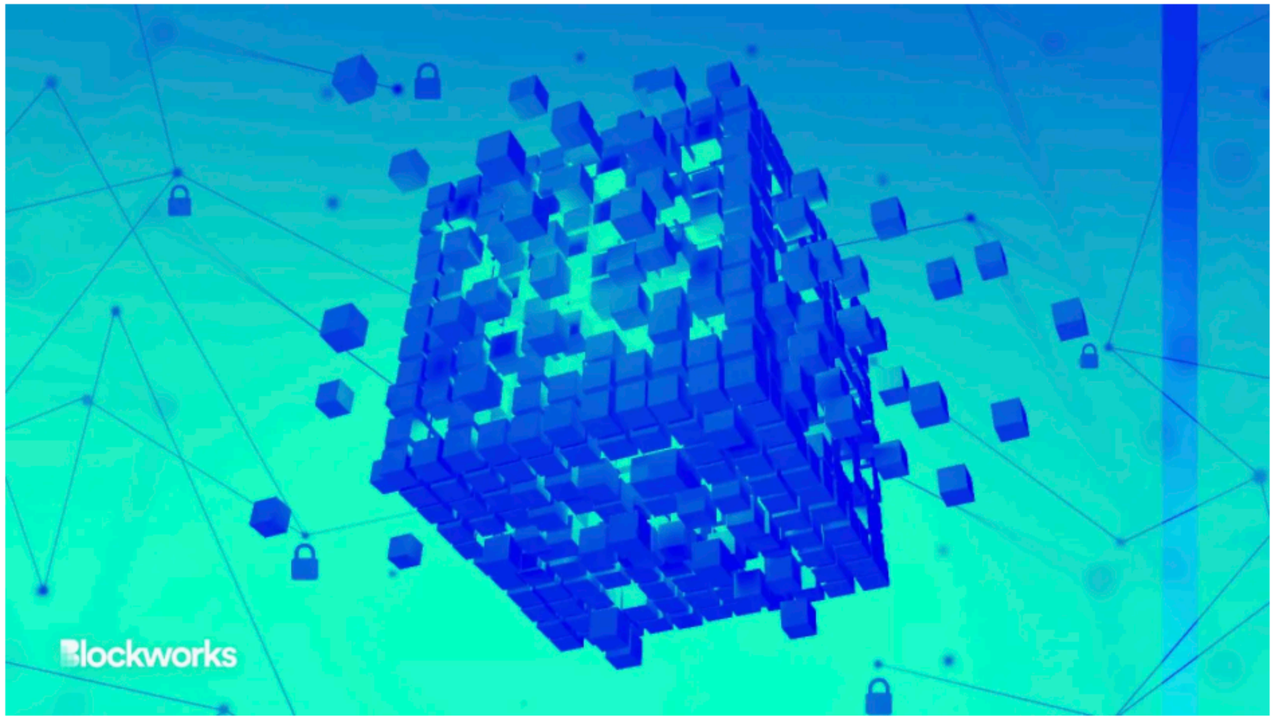
BITCOIN ORDINALS

Source: https://blockworks.co/news/inside-bitcoin-biggest-block

What Was Inside Bitcoin's Biggest Block?

In support of bitcoin NFT project Ordinals, Luxor Mining and crypto developer Udi Wertheimer mined the largest-ever bitcoin block

BY CASEY WAGNER & DAVID CANELLIS / FEBRUARY 2, 2023 12:02 PM



Yurchanka Siarhei/Shutterstock.com modified by Blockworks

NFTS ON BITCOIN

Q: Should NFTs on Bitcoin be allowed, or should they actively be prevented?

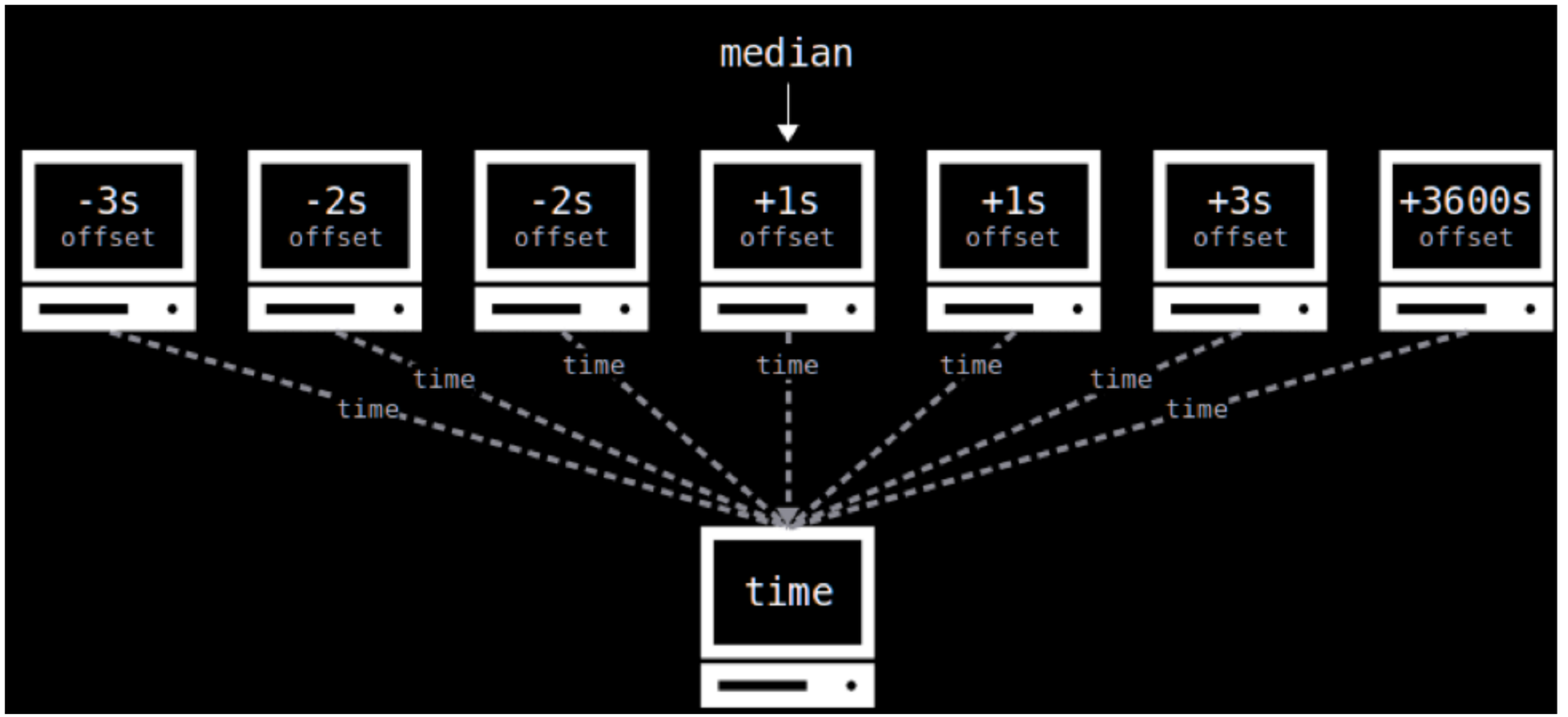
VALIDATION OF BLOCKS

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

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.

THE TIME WARP ATTACK

Assume here: Difficulty adjustment after 4 blocks.

Normal chain (example):

blk#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
time	0	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150

Chain with manipulated time stamps:

blk#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
time	0	1	2	30	4	5	6	70	8	9	10	110	12	13	14	150

- Time passed between #3-#0: 30 min
- Time passed between #7-#4: 66 min
- Time passed between #11-#8: 104 min

Attack strategy:

- Miners set time stamps of blocks in alternating pattern:
  - First three blocks of adjustment period (blk# 0,1,2, 4,5,6, and 8,9,10 etc.) use time stamps **as small as possible** (while still choosing them above the Median Time Past, the median time stamp of last 11 blocks)
  - Last block of adjustment period (blk# 3,6,10) use time stamp that corresponds to actual time (**much larger,** but below Network Adjusted Time)

Chain with manipulated time stamps:

blk#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
time	0	1	2	30	4	5	6	70	8	9	10	110	12	13	14	150

- Time passed between #3-#0: 30 min -> Difficulty in first period: 1 (relative measure)
- Time passed between #7-#4: 66 min -> Difficulty in second period: 1* (66 min / 30 min)$^{-1}$ = 0.4545
- Time passed between #11-#8: 104 min -> Difficulty in third period: 0.4545* (104 min / 30 min)$^{-1}$ = 0.1311

NEXT CLASS

- **Selfish Mining Attack**: Malicious chain reorganizations profitable if mining pool has at least 1/3 of hash power