原语里弄
PRIMITIVES LANE

# A Brief History of Difficulty Bomb

2021.07

Winky

# London Hard Fork and Difficulty Bomb

EIP-3554

## Simple Summary

Delays the difficulty bomb to show effect the first week of December 2021.

## Abstract

Starting with `FORK_BLOCK_NUMBER` the client will calculate the difficulty based on a fake block number suggesting to the client that the difficulty bomb is adjusting 9,700,000 blocks later than the actual block number.

## Motivation

Targeting for the Shanghai upgrade and/or the Merge to occur before Decemember 2021. Either the bomb can be readjusted at that time, or removed all together.

## Specification

Relax Difficulty with Fake Block Number

For the purposes of `calc_difficulty`, simply replace the use of `block.number`, as used in the exponential ice age component, with the formula:

```
    fake_block_number = max(0, block.number - 9_700_000) if block.number >= FORK_
```

## Rationale

The following script predicts a .1 second delay to blocktime the first week of december and a 1 second delay by the end of the month. This gives reason to address because the effect will be seen, but not so much urgency we don't have space to work around if needed.

```
def predict_diff_bomb_effect(current_blknum, current_difficulty, block_adjustment
    '''
    Predicts the effect on block time (as a ratio) in a specified amount of month
    Vars used in last prediction:
    current_blknum = 12382958
    current_difficulty = 7393633000000000
    block adjustment = 9700000
    months = 6
    '''
    blocks_per_month = (86400 * 30) // 13.3
    future_blknum = current_blknum + blocks_per_month * months
    diff_adjustment = 2 ** ((future_blknum - block_adjustment) // 100000 - 2)
    diff_adjust_coeff = diff_adjustment / current_difficulty * 2048
    return diff_adjust_coeff


diff_adjust_coeff = predict_diff_bomb_effect(12382958,7393633000000000,9700000,6)
```

## Backwards Compatibility

No known backward compatibility issues.

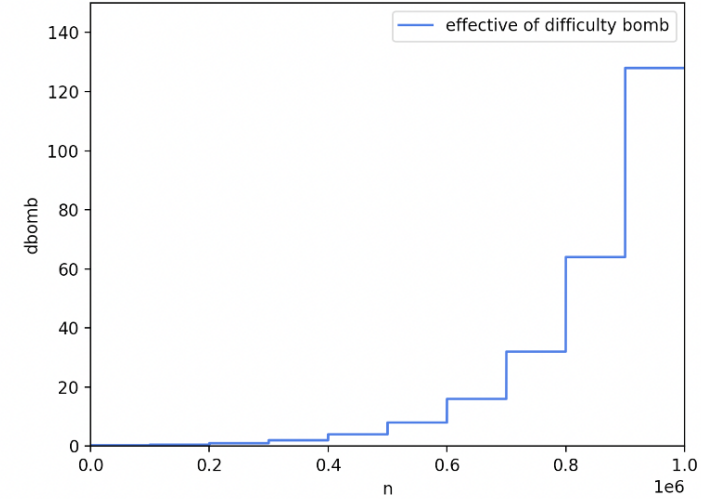
## Security Considerations

Misjudging the effects of the difficulty can mean longer blocktimes than anticipated until a hardfork is released. Wild shifts in difficulty can affect this number severely. Also, gradual changes in blocktimes due to longer-term adjustments in difficulty can affect the timing of difficulty bomb epochs. This affects the usability of the network but unlikely to have security ramifications.

# Design Objectives and Principles of Difficulty Bomb

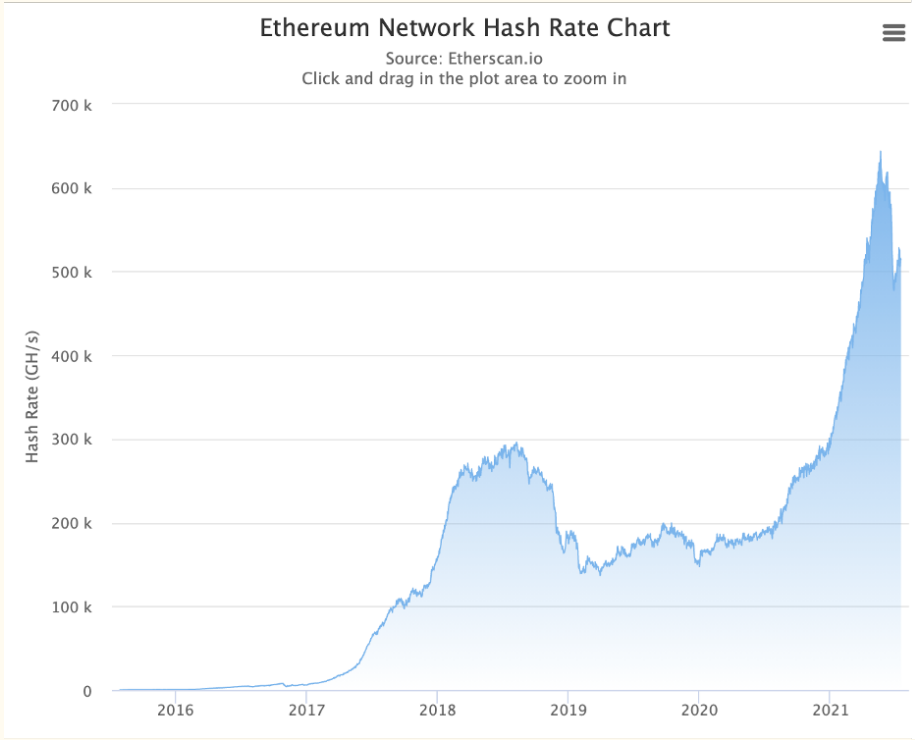
POW → POS

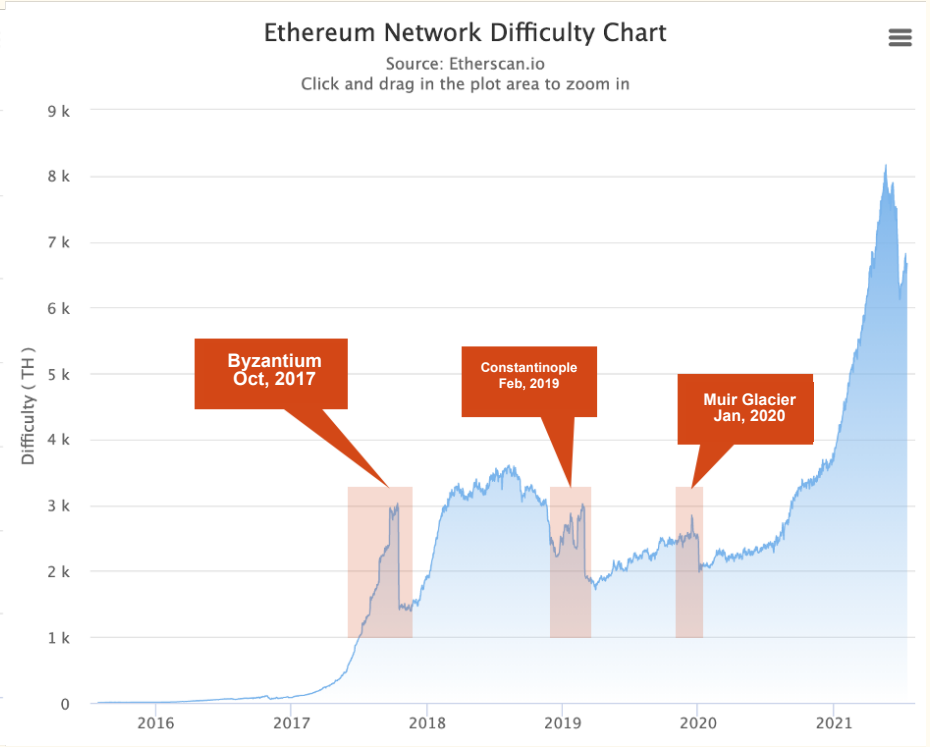
$$d_c = d_p + \underbrace{\frac{d_p}{2048} * \max\left(1 - \left\lfloor \frac{ts_c - ts_p}{10} \right\rfloor, -99\right)}_{\text{Regular Block Production Time}} + \underbrace{2^{\left(\left\lfloor \frac{n_p + 1}{100{,}000} \right\rfloor - 2\right)}}_{\text{Difficulty Bomb}}$$



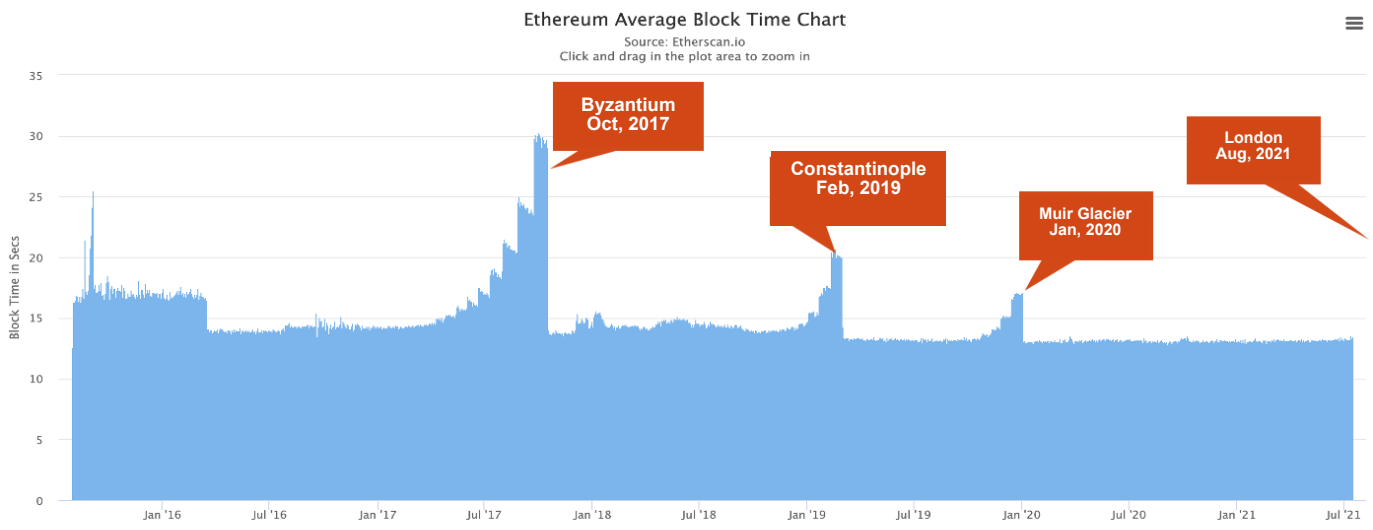
# The History of Difficulty Bomb

$$d_c = d_p + \frac{d_p}{2048} * \max\left(1 - \left\lfloor \frac{ts_c - ts_p}{10} \right\rfloor, -99\right) + 2^{\left(\left\lfloor \frac{n_p + 1}{100{,}000} \right\rfloor - 2\right)}$$



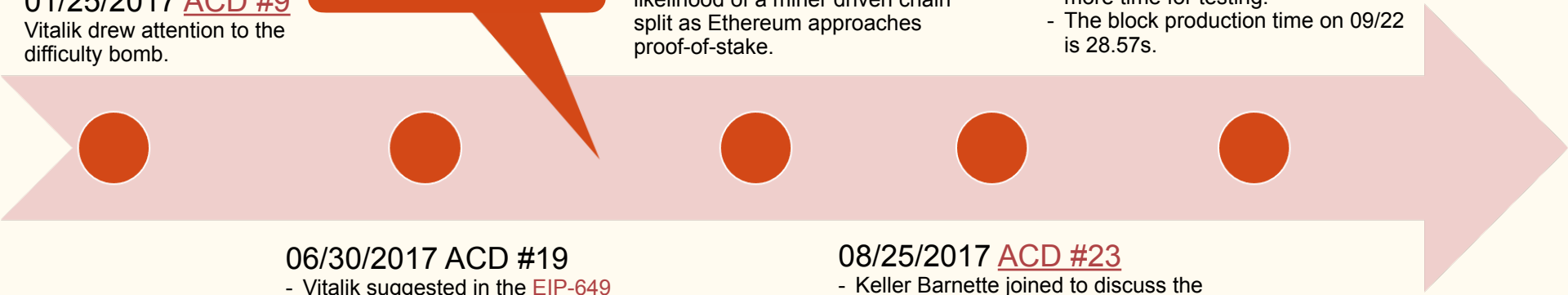



# The History of Difficulty Bomb




| Date | Hard Fork | EIP | Block Number | Set Back | Fake Block | Difficulty Level Increased |
|---|---|---|---|---|---|---|
| Sep, 2015 | Frontier thawing | EIP-2 | 200,000 | - | - | - |
| Oct, 2017 | Byzantium | EIP-649 | 4,370,000 | 3,000,000 | 1,370,000 | 13 |
| Feb, 2019 | Constantinople | EIP-1234 | 7,280,000 | 5,000,000 | 2,280,000 | 22 |
| Jan, 2020 | Muir Glacier | EIP-2384 | 9,200,000 | 9,000,000 | 200,000 | 2 |
| Aug, 2021 | London | EIP-3554 | 12,965,000 | 9,700,000 | 3,265,000 | 32 |
| Dec, 2021 | Arrow Glacier | EIP-4345 | 13,773,000 | 10,700,000 | 3,073,000 | 30 |

# The History of Difficulty Bomb——Byzantium(Oct,17th,2017 | EIP-649)



01/25/2017 ACD #9
Vitalik drew attention to the difficulty bomb.

Besides:
A miner from China argue against the block reward reduction in EIP-649 discussion.

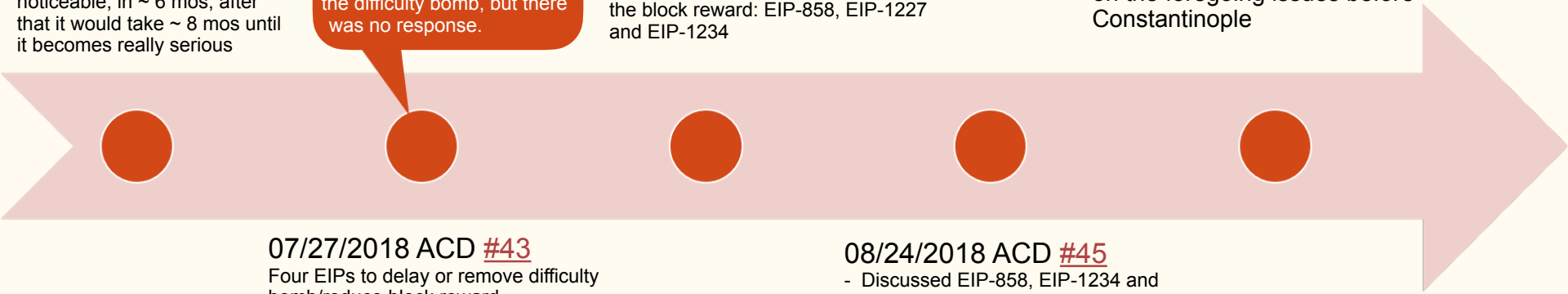
06/30/2017 ACD #19
- Vitalik suggested in the EIP-649 discussion that the gake block number be reduced by 3m and the block reward be reduced.

08/11/2017 ACD #22
- Discussed that reducing block reward to 3 ETH
- Reason: a). With the delay of the ice age, there is a desire to not suddenly also increase miner rewards. b). decreases the likelihood of a miner driven chain split as Ethereum approaches proof-of-stake.

08/25/2017 ACD #23
- Keller Barnette joined to discuss the issuance reduction and to argue for a further reduction.
- Reason: Miners are still overpaid
- Result: keep the issuance reduction for the Byzantium hard fork to 3 ETH in accordance with EIP 649.

09/22/2017 ACD #25
- Discussed picking block number 4.35mil (Oct. 9th), 4.36mil (Oct. 13th), 4.37mil (Oct. 17th), or 4.4mil (Oct. 27th) for the mainnet fork, and decided on block number 4.37mil (roughly Oct. 17th) in order to give more time for testing.
- The block production time on 09/22 is 28.57s.

# The History of Difficulty Bomb——Constantinople (Feb,2017 | EIP-1234)



## 07/13/2018 ACD #42

Vitalik: Going by etherscan data on block time previously, if we say it starts when block time reaches 16s, would be ~ block 6.7m, would become noticeable, in ~ 6 mos, after that it would take ~ 8 mos until it becomes really serious

Besides:
The author of EIP-1227 emphasized that the underlying motivation of the proposed change is defusing the difficulty bomb, but there was no response.

## 07/27/2018 ACD #43

Four EIPs to delay or remove difficulty bomb/reduce block reward

a. EIP-858 - Reduce block reward to 1 ETH per block.
b. EIP-1227 - Delay bomb and change rewards to 5 ETH.
c. EIP-1234 - Delay bomb and change rewards to 2 ETH.
d. EIP-1240 - Remove the difficulty bomb entirely.

Result: “We have consensus we don't want to remove it entirely”

## 08/10/2018 ACD #44

Discussed three competing EIPs to delay the difficulty bomb and/or reduce the block reward: EIP-858, EIP-1227 and EIP-1234

## 08/24/2018 ACD #45

- Discussed EIP-858, EIP-1234 and EIP-1295.
- Interested parties were invited to the meeting including miners, excluding EIP-1227 and EIP-1240 authors.
- No clear conclusions

No further meetings focused on the foregoing issues before Constantinople

# The History of Difficulty Bomb——Istanbul (Dec,2019) & Muir Glacier (Jan,2020 | EIP-2384)

### 08/23/2019 ACD #69
- Danno drew attention to the difficulty bomb

### 10/04/2019 ACD #72
- James: So there is a script somewhere floating around that predicts it, alright…..given that it's in the April May June July range that we might see something.
- Danno doubted the time.
- James: it would be still in the March but it should show up slower because the hash rate is so much less than it was last time.

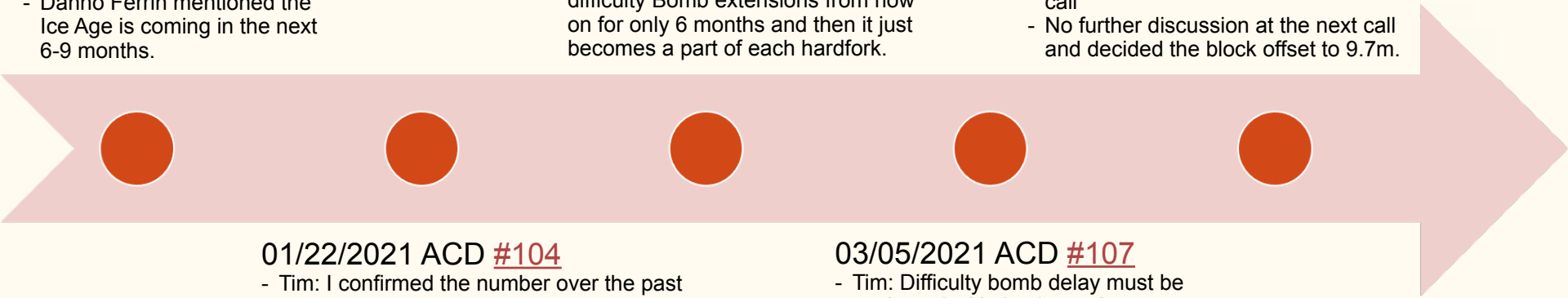
### 10/25/2019 ACD #73
- There is no data analysis to support the decision.
- DECISION 72.1: The Ice Age EIP will not be included in Istanbul. This gives enough time to plan for another fork and not delay Istanbul.

### 11/15/2019 ACD #75
- General discussion around the Ice Age and calculating when it will occur. Vitalik wrote a script and Lane cleaned it up. It is a fairly manual process and James Hancock is working on it.

### 11/29/2019 ACD #76
- Discussed the block offset, progress and naming issue of Ice Age.

Besides:
Finding out that the difficulty bomb prediction was wrong, Thomas Jay Rush helped measure and publish the article ***It's Not That Difficult***

# The History of Difficulty Bomb——London (Aug,2021 | EIP-3554)



11/27/2020 ACD #101
- Danno Ferrin mentioned the Ice Age is coming in the next 6-9 months.

01/22/2021 ACD #104
- Tim: I confirmed the number over the past work with TJ Rush from QuickBlocks [TrueBlocks], the July 2021 number is accurate.
- Artem Vorotnikov: Can't we just disable the Ice Age once and for all and not bring up this topic in the future? (diagreement from multiple parties, perhaps Danno Ferrin and Tim Beiko, maybe others)

02/19/2021 ACD #106
- Vitalik: One thing we could you could do is we could even just say old difficulty Bomb extensions from now on for only 6 months and then it just becomes a part of each hardfork.

03/05/2021 ACD #107
- Tim: Difficulty bomb delay must be packaged with 1559 as miners could elect not to upgrade otherwise. They could still do this even if the difficulty bomb is pushed back but this would be more work as they'd need to fork a client.

04/30/2021 ACD #112
- Alexey: I do believe that we do not need to reset the difficulty bomb but simply remove it
- Tim: Can we discuss that on the next call
- No further discussion at the next call and decided the block offset to 9.7m.

# Core issues of Difficulty Bomb - Is the triggered time predicable?

Precise predictions are hard to come by when rough predictions are easy

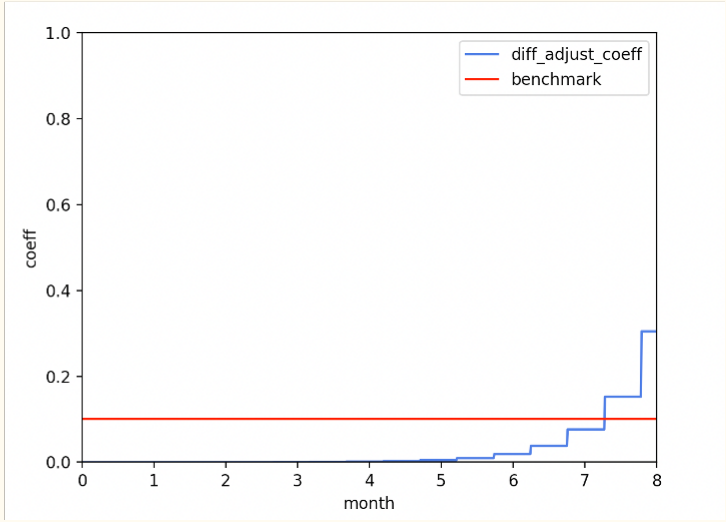
- Rough prediction method: Predicted Time = Set Back Number * Block Production Time / 86400

| Date | Hard Fork | Block Number | Set Back | Block Production Time | Predicted Time(day) | Predicted Date |
|---|---|---|---|---|---|---|
| Sep, 7th, 2015 | Frontier thawing | 200,000 | 0 | - | - | |
| Oct, 16th, 2017 | Byzantium | 4,370,000 | 3,000,000 | 14.0 | 486 | Feb, 24th, 2019 |
| Feb, 28th, 2019 | Constantinople | 7,280,000 | 5,000,000 | 14.0 | 324 | Jan, 18th, 2020 |
| Jan, 1st, 2020 | Muir Glacier | 9,200,000 | 9,000,000 | 13.0 | 602 | Aug, 24th, 2020 |
| Aug, 4th, 2020 | London | 12,965,000 | 9,700,000 | 13.5 | 109 | Nov, 21th, 2021 |

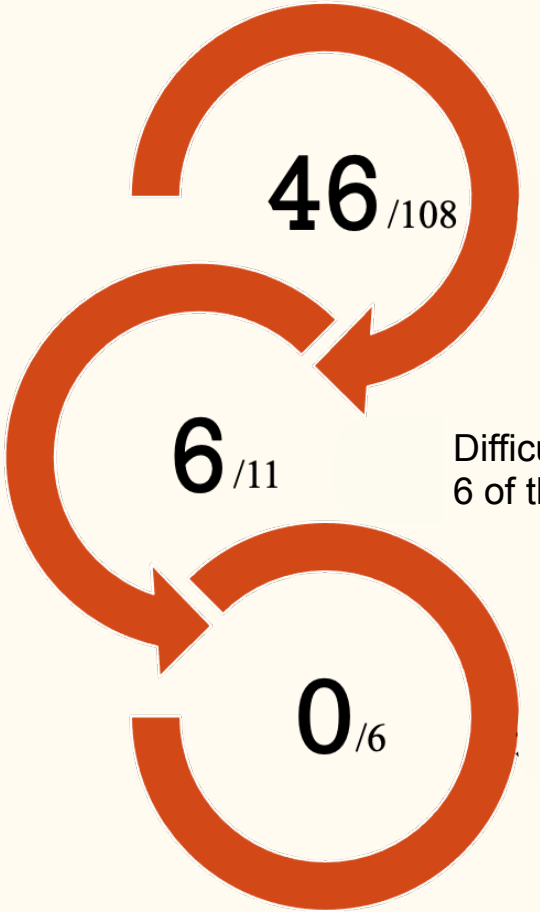
- The prediction scheme provided in EIP:

**diff_adjust_coeff >= 0.1, signalling the difficulty bomb is triggered**

| Prediction Base Date | Predicted Time(M) | Predicted Date |
|---|---|---|
| May, 7th, 2021 | 7.28 | Dec, 11th, 2021 |
| Jul, 20th, 2021 | 6.35 | Jan, 16th, 2022 |



# Core issues of Difficulty Bomb - Does it bring trouble to governance?




Difficulty Bomb was mentioned
46 times out of 108 ACD Meeting

Difficulty Bomb was included in
6 of the 11 Hard Fork EIPs

None of the six were passed
uncontested

- Time
- Economic model
- Delay

# Core issues of Difficulty Bomb - What not remove the Difficulty Bomb?

| Time | Name | Background | Where | Answer |
|---|---|---|---|---|
| Jul, 2017 | zhoujianwei | Miner from China | EIP-649 Discussion | No Answer |
| Jul, 2018 | SmeargleUsedFly | Unknown | EIP-1227 | No Direct Answer |
| Jul, 2018 | Micah Zoltu | Serv.eth Support | EIP-1240 | Withdrawn EIP |
| Jan, 2021 | Artem Vorotnikov | EF | ACD 104 | Denied |
| Apr, 2021 | Alexey Akhunov | Software specialist worked in Goldman Sachs and Citigroup | ACD 112 | No Direct Answer |

Hudson Jameson:
We have consensus we don‘t want to remove it entirely.

Dimitry Khokhlov:
I don't think it was a good idea in the first place.

Peter Szilagyi:
The original purpose of the Ice Age was to force Eth to switch over to Serenity, it seems weird to kill the Ice Age right before actually getting to that point.

Tim Beiko:
I strongly disagree. One, we've found it useful as a forcing function for forks in the past. Two, with the transition to Proof-of-Stake happening in The Merge I think we want it.
Difficulty bomb delay must be packaged with 1559 as miners could elect not to upgrade otherwise.

Thomas Jay Rush:
The forcing function is a reminder that we can do it, and that it benefits us all. It′ s both a carrot and a stick at the same time. Keeping the forcing function is the "working together."

# Is the Difficulty Bomb Reasonable?

Trusted Third Parties are Security Holes

Nick Szabo

Originally published in 2001

原语里弄
PRIMITIVES LANE

# Q&A

2021.07

# THANKS!