难度炸弹简史

赵文琦 Winky

伦敦分叉与难度炸弹

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.

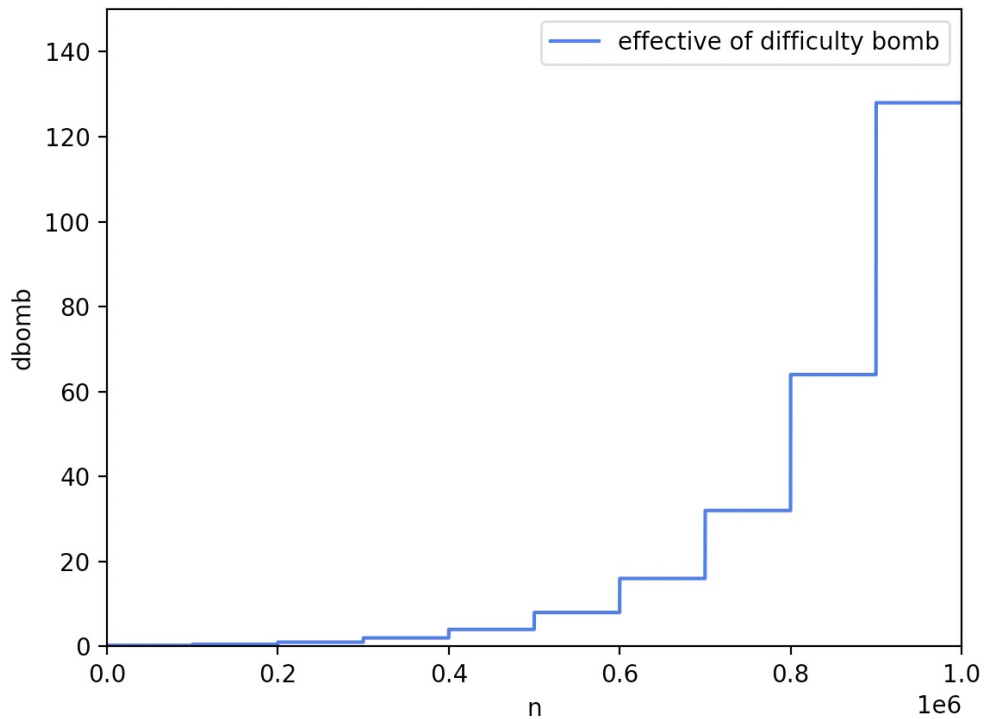
Security Considerations

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.

难度炸弹的设计目的、设计原理

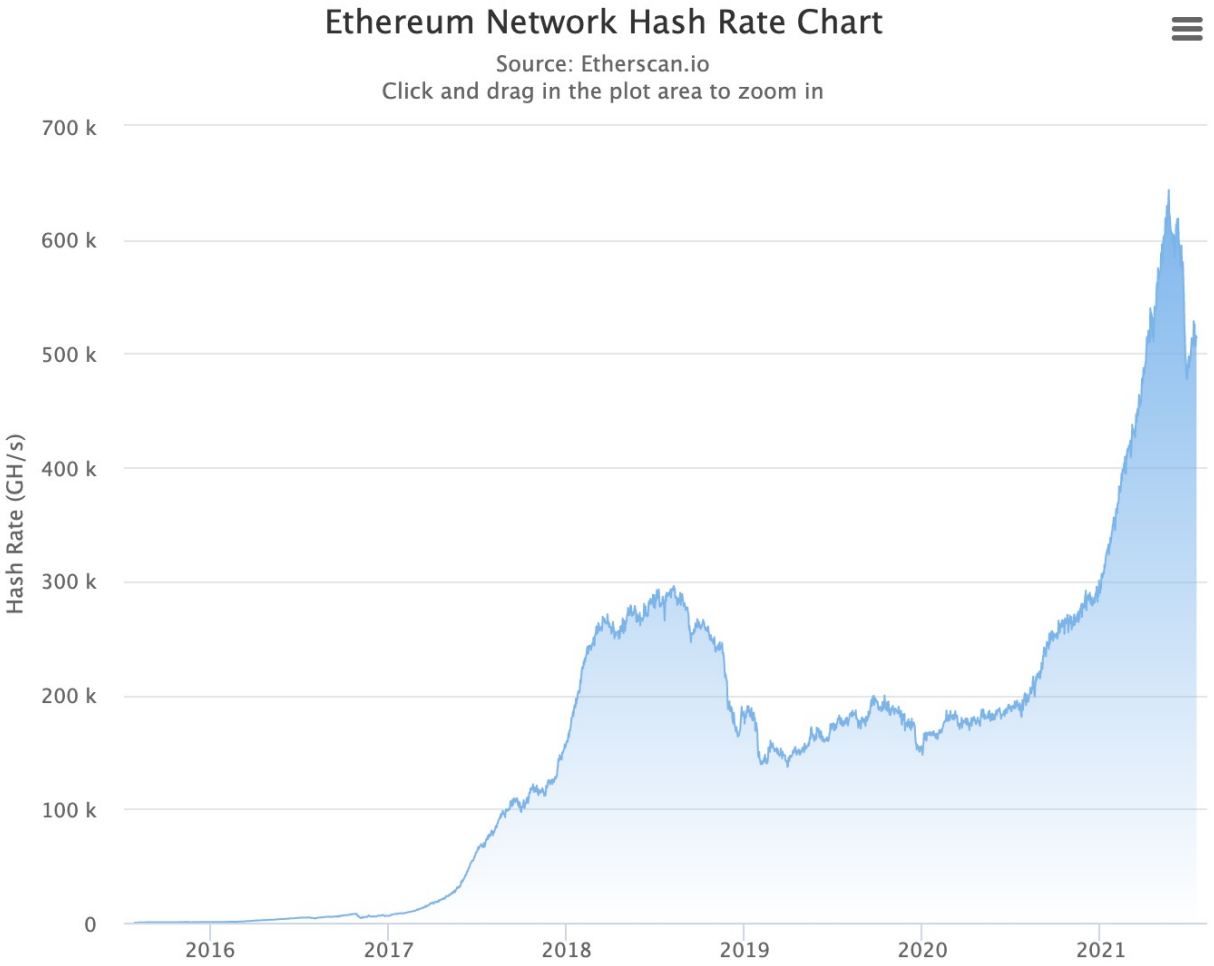
POW → POS

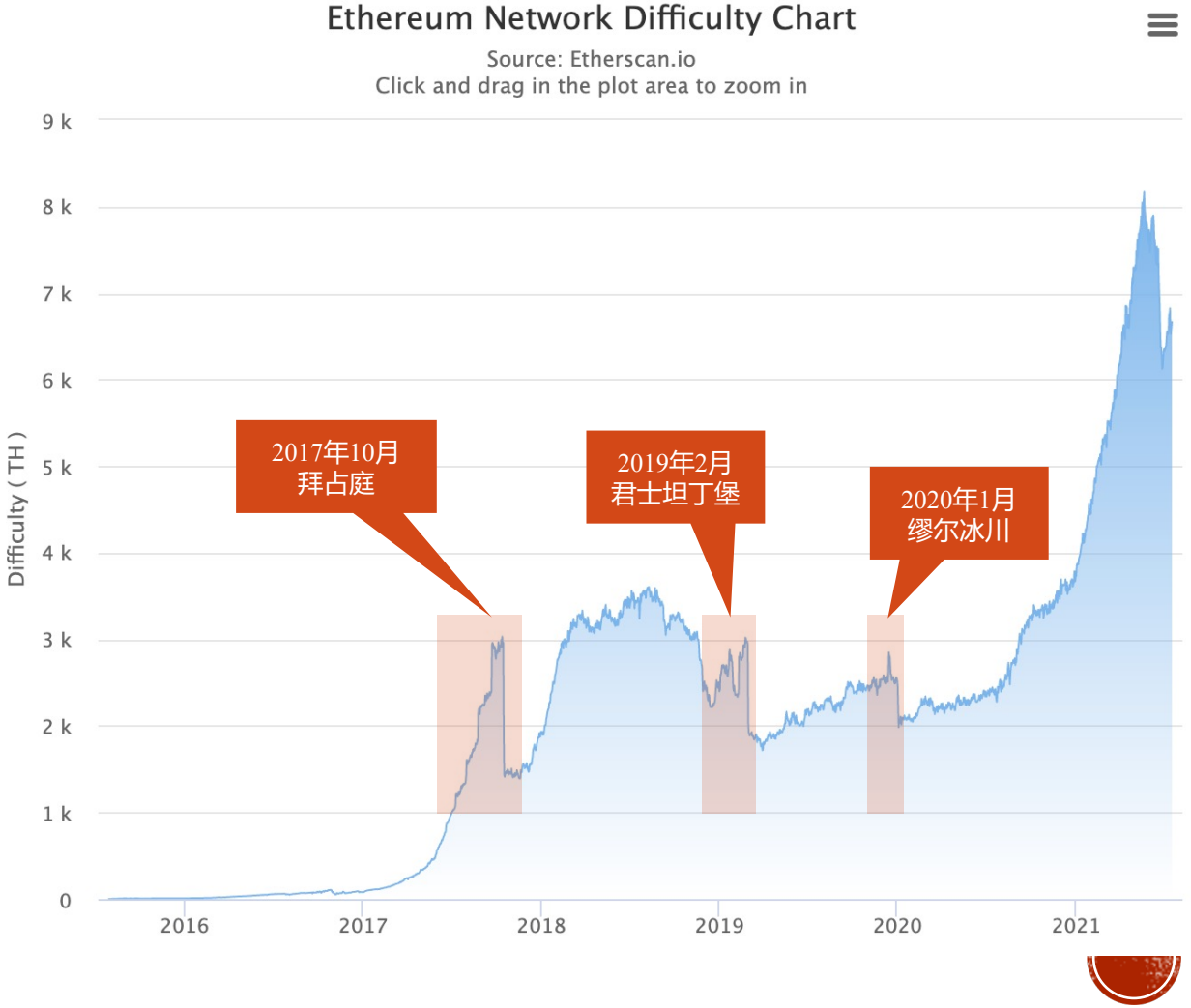
$$d_c = d_p + \underbrace{\frac{d_p}{2048} * \max\left(1 - \left\lfloor \frac{ts_c - ts_p}{10} \right\rfloor, -99\right)}_{\text{稳定出块时间}} + \underbrace{2^{\left(\left\lfloor \frac{n_p + 1}{100{,}000} \right\rfloor - 2\right)}}_{\text{难度炸弹}}$$



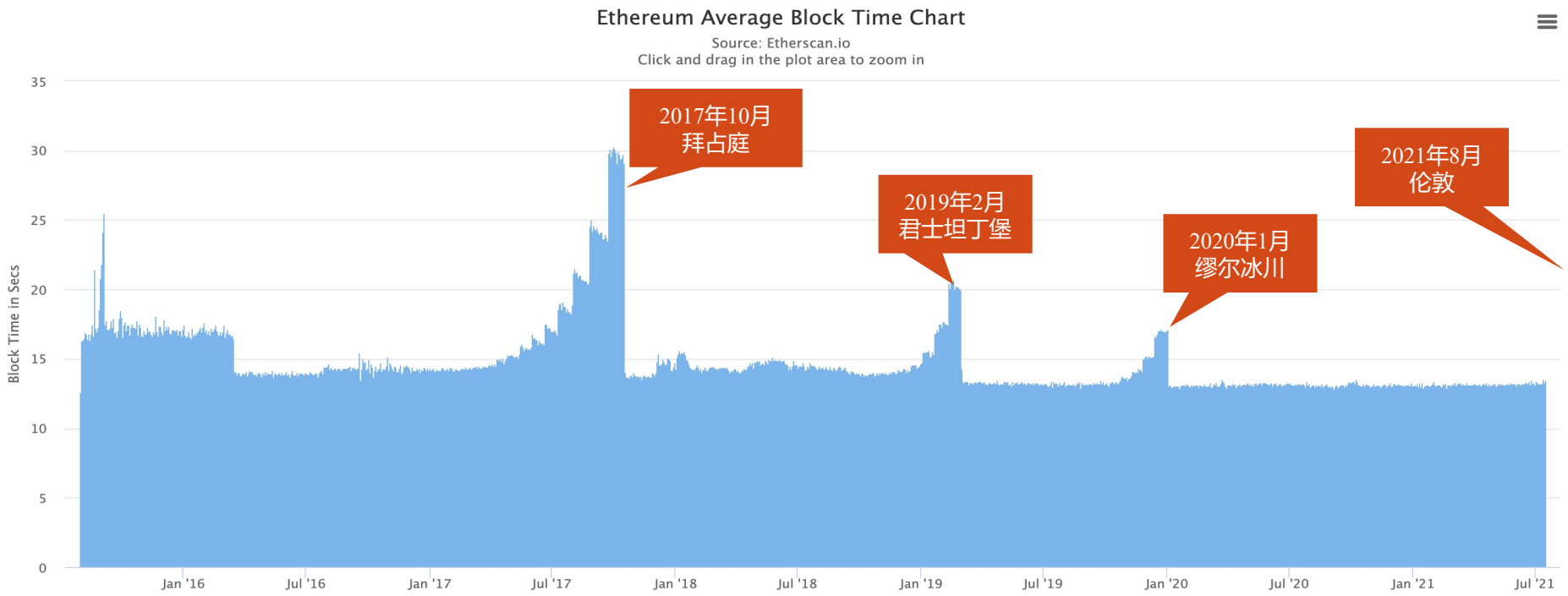
难度炸弹发展历程

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





难度炸弹发展历程



时间	硬分叉	EIP	区块号	回退	伪块号	难度增加级别
2015年9月	前沿解冻	EIP-2	200,000	-	-	-
2017年10月	拜占庭	EIP-649	4,370,000	3,000,000	1,370,000	13
2019年2月	君士坦丁堡	EIP-1234	7,280,000	5,000,000	2,280,000	22
2020年1月	缪尔冰川	EIP-2384	9,200,000	9,000,000	200,000	2
2021年8月	伦敦	EIP-3554	12,965,000	9,700,000	3,265,000	32

难度炸弹历次推迟——拜占庭(2017年10月，EIP-649)

难度炸弹历次推迟——君士坦丁堡(2019年2月，EIP-1234)

2018.07.13

ACD 42

•V提示注意难度炸弹，6-8个月后有显著影响

场外：
1227作者在论坛强调其提案核心是移除难度炸弹，未被理睬

2018.07.27

ACD 43

•EIP-858，奖励1ETH
•EIP-1227，奖励5ETH
•EIP-1234，奖励2ETH
•EIP-1240，移除难度炸弹
•结果：移除难度炸弹遭全体反对

2018.08.10

ACD 44

•EIP-858、EIP-1227、EIP-1234

2018.08.24

ACD 45

•EIP-858、EIP-1234，新增EIP-1295(3ETH，更改激励结构)
•邀请相关方讨论，包括矿工，不包括1227、1240作者
•结果：未在会议上形成结论

•上线前，没有会议再集中讨论前述问题

难度炸弹历次推迟——伊斯坦布尔(2019年12月)&缪尔冰川(2020年1月，EIP-2384)

2019.08.23

ACD 69

- Danno提示关注难度炸弹

2019.10.04

ACD 72

- James称难度炸弹会在明年4-7月爆炸
- 受Danno质疑
- James改称3月爆炸

2019.10.25

ACD 73

- 未有进一步数据支撑，但确定伊斯坦布尔不包括难度炸弹

2019.11.15

ACD 75

- Danno在会议结束时，提到难度炸弹问题
- James表示还在算

2019.11.29

ACD 76

- 讨论缪尔冰川的回退区块数、流程问题和命名问题

场外：
发现难度炸弹预测出错，Thomas Jay Rush帮忙测算并发文《It’s not that difficult》

难度炸弹历次推迟——伦敦(2021年8月，EIP-3554)

2020.11.27

ACD 101

•Danno提示难度炸弹6-9个月后开始爆炸

2021.01.22

ACD 104

•再次确认难度炸弹大概在7月爆炸

•Artem Vorotnikov提出拆除难度炸弹

•被强烈反对

2021.02.19

ACD 106

•V建议merge前的每一次硬分叉都推迟难度炸弹，也就意味着每次不推迟很多

2021.03.05

ACD 107

•Tim: Difficulty bomb delay must be packaged with 1559 as miners could elect not to upgrade otherwise

2021.04.30

ACD 112

•Alexey建议拆除难度炸弹

•被Tim直接建议下次讨论，下次没有再讨论

•下次直接确定回退9.7m个区块

难度炸弹核心问题——是否能预测炸弹爆炸时间？

粗略预测简单，精准预测难

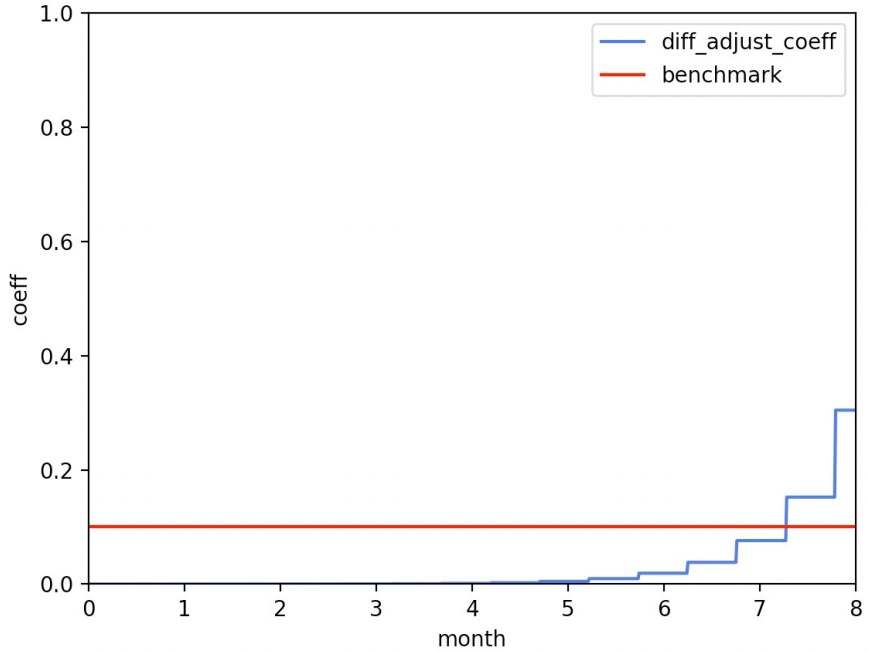
- 粗略预测：预测时长 = 回退序号差*出块时间/86400

时间	硬分叉	区块号	回退	出块时间	时长预测(天)	日期预测
2015年09月07日	前沿解冻	200,000	0	-	-	
2017年10月16日	拜占庭	4,370,000	3,000,000	14.0	486	2019年02月14日
2019年02月28日	君士坦丁堡	7,280,000	5,000,000	14.0	324	2020年01月18日
2020年01月01日	缪尔冰川	9,200,000	9,000,000	13.0	602	2021年08月24日
2021年08月04日	伦敦	12,965,000	9,700,000	13.5	109	2021年11月21日

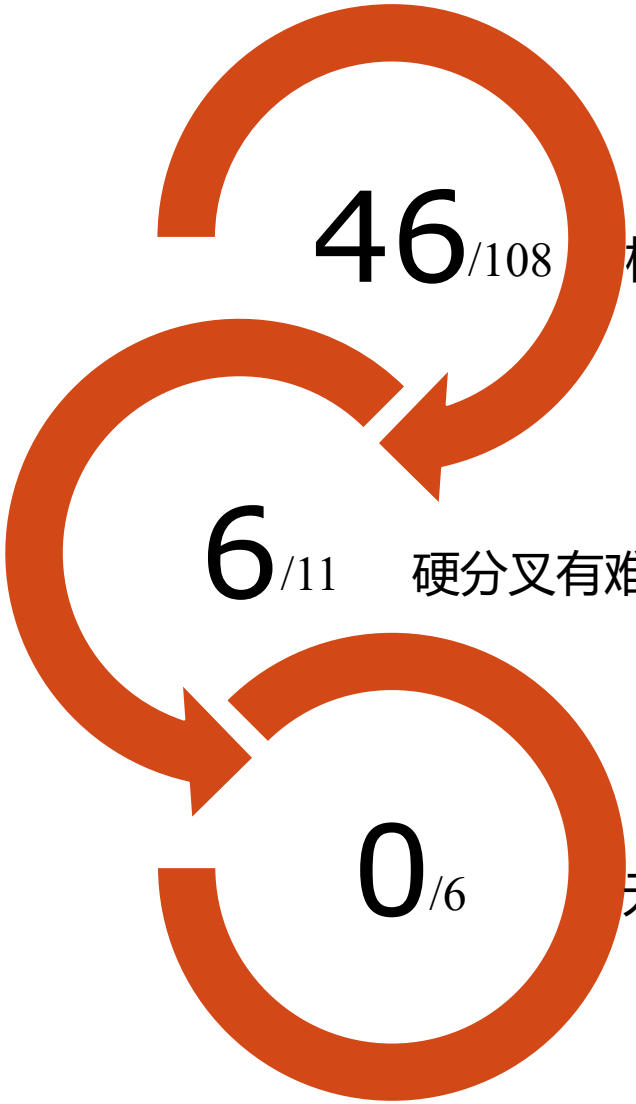
- EIP中给出的预测方案：

diff_adjust_coeff >= 0.1，标志着难度炸弹开始爆炸

测算基准日期	时长预测(月)	日期预测
2021年05月07日	7.28	2021年12月11日
2021年07月20日	6.35	2022年01月26日



难度炸弹核心问题——为治理带来哪些问题？



46/108 核心开发者会议提及

6/11 硬分叉有难度炸弹EIP

0/6 无争议通过

- 时间
- 经济模型
- 拆弹

难度炸弹核心问题——为什么不拆除难度炸弹？

时间	名称	背景	提出地点	结果
2017年7月	zhoujianwei	中国矿工	EIP-649讨论区	未被回复
2018年7月	SmeargleUsedFly	不明	EIP-1227	未被直视
2018年7月	Micah Zoltu	Serv.eth Support	EIP-1240	撤回EIP
2021年1月	Artem Vorotnikov	EF	ACD 104	直接被否定
2021年4月	Alexey Akhunov	前高盛、花旗开发	ACD 112	未被直接回答

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."

难度炸弹存在是否合理？