Validator Economics: Variable min validator deposit size

EF Academic Grant ID: FY23-1030

SLASHING & PENALTIES - MILESTONE 6

Sandra Johnson
Consensys Software R&D

May 2, 2024

1 Slashing penalty analysis

The main motivation for this post is the concern of large stakers regarding slashing penalties for consolidated validators. The proposal consists of two parts:

1. Changes to existing penalties:
    - Changing the *initial penalty* to be either fixed, or scaled sublinearly
    - Changing the *correlation penalty* to scale quadratically rather than linearly.
2. Unchanged penalties:
    - *Attestation penalties*
    - *Inactivity leak penalties*

1.1 Validator slashing and penalties

Slashing

The situations that lead to a validator being slashed are few, but they are severe violations of protocol rules that may be considered as a potential solo or coordinated attack on the system. Regardless of the reason for the slashing event, they are all handled in the same way. There is an initial slashing penalty, which is currently set at 1 ETH (or $\frac{1}{32}$ of the stake) and this is followed 18 days after the slashing event by another penalty, known as the correlation penalty. The purpose of the latter is to penalise what may be a coordinated attack on the chain. Therefore the correlation penalty takes into account slashings 18 days before and after the slashing event.

A validator gets slashed when they are reported and evidence of the violation of the rules is included in a beacon block. For the valid reporting of a slashing event, the reporting validator receives a reward. The intention is that this will help incentivise the reporting of slashable events. Only one proposer slashing can be included in a report, whereas multiple attestation violations can be included in a report. When the slashing is included in a block, the proposer gets a reward which is a fraction of the effective balance of the validator being slashed (currently $\frac{1}{512}$). Up to 16 proposer slashings can be included in a block and up to 2 attester slashing reports. Therefore,

if several slashings have occurred, including these reports in a block can generate a generous reward for the proposer.

For more detailed information on slashing and calculations, please refer to the latest version of Edgington's *Upgrading Ethereum* book [17] which incorporates the updates included in the Capella hard fork. In summary the events that lead to slashing are:

1. "making two differing attestations for the same target checkpoint"
2. "making an attestation whose source and target votes 'surround' those in another attestation from the same validator.
3. "proposing more than one distinct block at the same height"
4. "attesting to different head blocks, with the same source and target checkpoints"

The first two relate to Casper Friendly finality gadget (FFG) consensus, and the latter two are related to Latest message driven (LMD) Greedy Heaviest-Observed Sub-Tree (GHOST) consensus.

Edgington points out that 'slashable behaviours relate to "equivocation", which is when a validator contradicts something it previously advertised to the network'. Hence it is important for validators to ensure that they do not 'accidentally' equivocate. This could theoretically happen as a result of bugs in client software, but the vast majority of slashings have been due to node operators running two different nodes using the same validator keys. The reason may have been to improve uptime, but the risk of slashing is too great compared to any potential benefit in uptime [17]. There was also an incident where a validator exploited a vulnerability in a relay operator running mev-boost, an open source proposer-builder separation protocol. Flashbots posted a detailed post-mortem of the event.

Apart from the slashing penalties, a slashed validator accrues attestation penalties until such time as they exit, which is not until 2^{13} $epochs = 8,192$ $epochs \approx 36$ $days$ after being slashed. Moreover, if there is an inactivity leak at the time, the penalties imposed on slashed validators will be higher. Slashed validators cannot earn any attestation rewards while waiting to exit. It seems rather odd, but a slashed validator can still be elected to be the proposer for the next block. However, their block will be deemed to be invalid. The only duty for which they could receive a small reward is if they are selected to be in the sync committee, but the probability of this happening is very small.

Penalties

Slashing is the most severe penalty a validator is subjected to and as explained they can accrue several extra penalties while they wait to exit. However, there are a number of smaller, less serious 'misdemeanours', or failure to perform their duties that can result in penalties for validators. The validator's stake is reduced by the penalty and the ETH is burnt, thereby reducing net issuance [17].

Attestation penalties

- Missed source and target votes (i.e. missed Casper FFG votes), but no penalty for a missed head vote.
- Incorrect source vote, then target vote is missed.
- Incorrect source or target vote, then head vote is missed.

Sync committee penalties

- Non-participation of a member incurs a penalty equivalent to the reward they would have received if it was correct

1.2 Initial slashing penalty

Currently this penalty is proportional to the validator's effective balance, and this would result in a penalty of 1 ETH if the validator had 32 ETH. However, if a fully consolidated validator with 2,048 ETH effective balance would incur an initial penalty of 64 ETH.

One proposal is to make this penalty a constant value of 1 ETH, but "If we decide that a constant penalty is insufficient, ..." it can be adjusted so that it monotonically increases with effective balance, e.g. by choosing from the family of polynomials.

How do the authors propose to check whether the initial penalty is sufficient?

The authors demonstrate the increase in initial penalty such that
$initial\ penalty = \frac{EB^x}{32},\ \ x \leqslant 1$

and generate graphs for $x = 1, \frac{15}{16}, \frac{7}{8}, \frac{3}{4}, \frac{1}{2}$ with respect to the graph of a constant initial penalty of 1 ETH [37].

The authors conclude that visually it appears that $x = \frac{3}{4}\ \ \frac{7}{8}$ are good choices in terms of balancing the size of the initial slashing penalty and the risk for a consolidated validator.

1.3 Correlation penalty

This penalty is incurred roughly 18 days (4,096 epochs) after the slashing event, half way between its exit epoch and the slashing event. The correlation penalty is important in assessing whether there appears to have been a coordinated attack on the chain.

The penalty for a *slashed validator,* v_j, is then calculated as follows by looking at the previous 36 days from this "half-way" epoch:

$$correlation\ penalty = \frac{(\sum_{i=1}^{n} v_i) \cdot b \cdot v_j}{T},\ \ where$$

v_j = *effective balance of validator j slashed 18 days ago*

v_i = *effective balance of* i^{th} *validator slashed during previous 36 days*

n = *number of validators that were slashed during last 36 days*

$b = 3$ *(multiplier changed to 3 in Bellatrix, from 1 in Phase 0, and 2 in Altair)*

T = *total effective balance of the beacon chain*

For simplicity this is represented as:

$$correlation\ penalty\ (penalty) = \frac{3 \cdot EB \cdot SB}{TB},\ \ where$$

3 = *Bellatrix multiplier*

EB = *slashed validator's effective balance*

SB = *total slashable balance*

TB = *total effective balance of the beacon chain*

$$\therefore if\ SB = \frac{1}{3} \cdot TB \implies penalty = EB$$

$$Similarly,\ if\ 3 \cdot EB \cdot SB < TB \implies penalty = 0\ due\ to\ integer\ division$$

As designed, there is no correlation penalty for isolated slashing events. The authors point out that this continues to be the case for a fully consolidated validator with 2,048 ETH effective balance.

They based their calculation on the current staked ETH at the time of writing which is 24 million ETH.

$$
\begin{aligned}
&SB = EB \text{ for an isolated slashing} \\
&\therefore 3 \cdot EB \cdot SB = 3 \cdot EB \cdot EB \\
&\text{Assuming } EB = \text{2,048 \& } TB = 2.4 \cdot 10^7, \text{ then} \\
&3 \cdot EB \cdot EB = 1.2582912 \cdot 10^7 < 2.4 \cdot 10^7 \\
&\therefore penalty = 0
\end{aligned}
$$

The authors include two graphs to demonstrate how the correlation penalty increases for solo (32 ETH), partially consolidated (256 ETH) and fully consolidated (2,048 ETH) validators. It is important to ensure that any modifications to the function for calculating the correlation penalty satisfies the requirement that when the total slashed balance is $\frac{1}{3}^{rd}$ of the total balance, the entire balance of the validator is slashed.

The authors propose a function that preserves this requirement if the MaxEB proposal is implemented:

$$
\begin{aligned}
penalty' &= \frac{3^2 \cdot EB \cdot SB^2}{TB^2} \\
\therefore \text{if } SB &= \frac{TB}{3}, \text{ then} \\
penalty' &= \frac{3^2 \cdot EB \cdot \left(\frac{TB}{3}^2\right)}{TB^2} \\
\therefore penalty' &= EB
\end{aligned}
$$

Moreover, the new correlation penalty function scales quadratically as opposed to the current function that scales linearly. Clearly with the proposed new function, the slashing penalties are substantially reduced, not only for fully consolidated validator, but also for partially consolidated and solo validators. The authors demonstrate the comparative correlated slashing penalties for these three types of validators using both the current and the proposed functions [37].

1.4 Attestation penalty

Once a validator is slashed, their attestations (source, target and head votes) are deemed to be invalid and hence they incur attestation penalties for the 8,192 epochs until their exit epoch.

Different weights are attached to each vote, but only the source (weight = 14) and target (weight = 26) votes incur penalties. For each of the 8,192 epochs the slashed validator will incur:

$$Given:$$

$$base\ reward = \frac{64}{\left\lfloor \sqrt{TB} \right\rfloor},\ weight\ denominator = 64,$$

$$source\ weight = 14\ \&\ target\ weight = 26$$

$$\therefore epoch\ attestation\ penalty = \frac{base\ reward \cdot EB \cdot (14 + 26)}{64}$$

$$\therefore\ if\ TB \approx 24 million\ ETH = 2.4 \cdot 10^6 \cdot 10^9\ Gwei$$

$$the\ integer\ square\ root\ of\ 2.4 \cdot 10^6\ ETH = 4,898,\ and$$

$$the\ integer\ square\ root\ of\ 2.4 \cdot 10^6 \cdot 10^9\ Gwei = 154,919,333$$

$$base\ reward = \frac{64 \cdot 10^9}{154,919,333} = 413\ Gwei$$

$$\therefore for\ a\ \textbf{solo staker}\ with\ 32\ ETH:$$

$$total\ attestation\ penalty\ for\ 8{,}092\ epochs = 8192 \cdot \frac{413 \cdot 32 \cdot 40}{64}\ Gwei$$

$$\therefore total\ attestation\ penality \approx 6.767 \cdot 10^7\ Gwei \approx 0.06767\ ETH$$

$$for\ a\ \textbf{fully consolidated}\ validator\ with\ 2{,}048\ ETH:$$

$$total\ attestation\ penalty\ for\ 8{,}092\ epochs = 8192 \cdot \frac{413 \cdot 2048 \cdot 40}{64} \approx 4.331\ ETH$$

This attestation penalty for a large slashed staker seems acceptable, but could potentially be adjusted by changing the number of epochs that the validator is deemed as being "offline".The size of this penalty needs to be such that the security model is not compromised. In other words it should never be a better option to self-slash to avoid inactivity penalties. Therefore, it needs to be greater than the inactivity penalties for an unslashed validator that is exiting and offline [37].

1.5 Inactivity leak penalty

An inactivity leak is currently defined as the situation when the chain has not been finalising for 4 epochs (this value is set by the protocol). Online validators are not penalised when this happens, i.e. no rewards are earned but the penalty is 0. On the other hand, offline validators, which includes slashed validators waiting to exit, start 'leaking' state. The loss of stake means that the relative weight of the online validators will increase, which helps the chain to start finalising again. The inactivity penalty can be quite severe.

Using the current method of calculating inactivity leaks, the authors worked out the penalty for validators with three different effective balances: 32 ETH (solo validator), 256 ETH (partially consolidated validator), and 2,048 ETH (fully consolidated validator).

Table 1: inactivity leak penalties

validator size	16 epoch leak	128 epoch leak	1024 epoch leak
32 ETH	0.000259 ETH	0.0157 ETH	1.00 ETH
256 ETH	0.00208 ETH	0.126 ETH	8.01 ETH
2048 ETH	0.0166 ETH	1.01 ETH	64.1 ETH

1.6 Griefing/discouragement attacks

According to Buterin a griefing attack is when a validator acts maliciously inside a consensus mechanism to reduce other validators' revenue even at some cost to themselves to encourage the victims to drop out of the mechanism [8].

The two main motivations for reducing the number of participants are most likely because fewer participants:

- mean greater rewards for those remaining in the mechanism
- helps to prepare an attack on the chain by reducing the cost of an attack

Some strategies have already been put in place to avoid discouragement attacks [17]:

- inverse square root scaling of validator rewards
- scaling of rewards with participation (viz. for each "source, target, and head vote, the attester's reward is scaled by the proportion of the total stake that made the same vote")
- zeroing attestation rewards during an inactivity leak
- rate limiting of validator exists, which means that an attacker needs to sustain an attack for longer and at greater cost in order to achieve the same outcome.

2 Bibliography

References

[1] Laurence Aitchison, Nicola Corradi & Peter E Latham (2016): *Zipf's Law Arises Naturally When There Are Underlying, Unobserved Variables. PLoS computational biology* 12(12), p. e1005110, doi:10.1371/journal.pcbi.1005110.

[2] Ether alpha (2023): *Client diversity: Resource site to assist in Ethereum client diversity efforts.* Available at `https://clientdiversity.org/`.

[3] Ether alpha (2023): *Project Sunshine.* Available at `https://ethsunshine.com/`.

[4] Ether alpha (2023): *Validator queue: Dashboard to monitor validator enter/exit queues and wait times.* Available at `https://www.validatorqueue.com/`.

[5] Aditya Asgaonkar (2023): *Removing Unnecessary Stress from Ethereum's P2P Network.* Available at `https://ethresear.ch/t/removing-unnecessary-stress-from-ethereums-p2p-network/15547`.

[6] Andrew Breslin (2022): *What is staking?* Available at https://consensys.net/blog/ethereum-2-0/what-is-staking/.

[7] Vitalik Buterin (2017): *The Meaning of Decentralization.* Available at https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

[8] Vitalik Buterin (2018): *Discouragement Attacks.* Available at https://eips.ethereum.org/assets/eip-2982/ef-Discouragement-Attacks.pdf.

[9] Vitalik Buterin (2020): *Vitalik's Annotated Ethereum 2.0 Spec.* Available at https://notes.ethereum.org/@vbuterin/SkeyEI3xv.

[10] Vitalik Buterin (2023): *Don't overload Ethereum's consensus.* Available at https://vitalik.ca/general/2023/05/21/dont_overload.html.

[11] Vitalik Buterin (2023): *Paths toward single-slot finality.* Available at https://notes.ethereum.org/@vbuterin/single_slot_finality.

[12] Rajan Chattamvelli (2020): *Discrete distributions in engineering and the applied sciences.* Synthesis lectures on mathematics and statistics ; 34, Morgan & Claypool Publishers.

[13] Liquid Collective (2023): *Ethereum's activation and exit queues.* Available at https://liquidcollective.io/eth-activations-and-exits/.

[14] Matt Corva & Bill Hughes (2023): *Staking is Data Validation, Not Investment.* Available at https://consensys.net/blog/news/staking-is-data-validation-not-investment/.

[15] Francesco D'Amato & Mike Neuder (2023): *Security Considerations and Spec Changes for a MAX_EFFECTIVE_BALANCE Increase.* Available at https://notes.ethereum.org/@fradamt/meb-increase-security.

[16] dapplion (2023): *Ethereum specs pull request: Add upper epoch churn limit #3448.* Available at https://github.com/ethereum/consensus-specs/pull/3448.

[17] Benjamin Edgington (2023): *A technical handbook on Ethereum's move to proof of stake and beyond.* Technical Report. Available at https://eth2book.info/latest.

[18] ethereum.org (2022): *Pooled staking.* Available at https://ethereum.org/en/staking/pools/.

[19] ethereum.org (2022): *Solo staking.* Available at https://ethereum.org/en/staking/solo/.

[20] ethereum.org (2022): *Staking as a service (Saas).* Available at https://ethereum.org/en/staking/saas/.

[21] ethereum.org (2022): *Staking with Ethereum.* Available at https://ethereum.org/en/staking/.

[22] Etherscan (2023): *BeaconScan: The Official Etherscan Beacon Chain Ethereum 2.0 Explorer.* Available at https://beaconscan.com/.

[23] Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert Van Renesse & Emin Gün Sirer (2018): *Decentralization in Bitcoin and Ethereum Networks.* Technical Report, Berlin, Heidelberg. arXiv:1801.03998v2.

[24] Hex (2023): *Lido on Ethereum Validator & Node metrics*. Available at https://app.hex.tech/8dedcd99-17f4-49d8-944e-4857a355b90a/app/3f7d6967-3ef6-4e69-8f7b-d02d903f045b/latest.

[25] Viet Tung Hoang, Ben Morris & Phillip Rogaway (2014): *An Enciphering Scheme Based on a Card Shuffle*. arXiv:1208.1176.

[26] Charles I Jones (2015): *Pareto and Piketty: The Macroeconomics of Top Income and Wealth Inequality*. *The Journal of economic perspectives* 29(1), pp. 29–46.

[27] Aris Koliopoulos (2023): *Solo stakers: The backbone of Ethereum*. Available at https://blog.rated.network/blog/solo-stakers.

[28] Dániel Kondor, Márton Pósfai, István Csabai & Gábor Vattay (2014): *Do the rich get richer? An empirical analysis of the Bitcoin transaction network*. *PloS one* 9(2), pp. e86197–e86197.

[29] Qinwei Lin, Chao Li, Xifeng Zhao & Xianhai Chen (2021): *Measuring Decentralization in Bitcoin and Ethereum using Multiple Metrics and Granularities*, pp. 1–8. arXiv:2101.10699.

[30] Nansen (2023): *Eth2 Dashboard*. Available at https://pro.nansen.ai/eth2-deposit-contract.

[31] Nansen (2023): *The Ethereum Shanghai (Shapella) Upgrade Dashboard*. Available at https://query.nansen.ai/public/dashboards/Hk93n66vsO0uvycfui8ypF2xcpNhpraxfwX5AWZJ.

[32] U Natale (2022): *Analyzing Ethereum Cryptoeconomics: the validator's perspective*. Technical Report, Chorus. Available at https://docs.google.com/document/d/1r640UQOm2z-Q9nsJzqBq3BVgCtTL1_Yc7WnPp4jEBgk.

[33] Rated network (2023): *Network overview*. Available at https://www.rated.network/overview?network=mainnet&timeWindow=all&rewardsMetric=average.

[34] Mike Neuder (2023): *EIP 7251 Maximum effective balance increase proposal [DRAFT]*. Available at https://github.com/michaelneuder/EIPs/blob/max-eb-increase/EIPS/eip-increase-maxeb.md.

[35] Mike Neuder (2023): *Security Considerations and Spec Changes for a MAX_EFFECTIVE_BALANCE Increase*. Available at https://notes.ethereum.org/nHqON5l7SACkL_nPwz8Vqw.

[36] Mike Neuder, Francesco D'Amato, Aditya Asgaonkar & Justin Drake (2023): *Increase the MAX_EFFECTIVE_BALANCE – a modest proposal*. Available at https://ethresear.ch/t/increase-the-max-effective-balance-a-modest-proposal/15801/3.

[37] Mike Neuder & Barnabé Monnot (2023): *[DRAFT] Slashing penalty analysis; EIP-7251*. Available at https://notes.ethereum.org/@mikeneuder/slashings-eip-7251.

[38] Rocket Pool (2023): *Rocket Pool: How Ethereum Staking Works*. Technical Report. Available at https://docs.rocketpool.net/guides/staking/overview.html#how-ethereum-staking-works.

[39] Roberto Saltini (2023): *Upper bound on the probability of one majority dishonest committee in the context of MAX_EFFECTIVE_BALANCE increase*. Available at `https://notes.ethereum.org/nHqON5l7SACkL_nPwz8Vqw`.

[40] James Smith & Rodrigo Vasquez (2023): *Staking survey: Key trends, take aways, and predictions*. Technical Report, Ethereum Foundation and EthStaker. Available at `https://lookerstudio.google.com/u/0/reporting/cafcee00-e1af-4148-bae8-442a88ac75fa/page/p_ja2srdhh2c`.

[41] Balaji S. Srinivasan & Leland Lee (2017): *Quantifying Decentralization*. Available at `https://news.earn.com/quantifying-decentralization-e39db233c28e`.

[42] Gavin Wood (2016): *Ethereum: a secure decentralized generalised transaction ledger*. Available at `https://github.com/ethereum/yellowpaper`.