TLDR

: We discuss strategies to address proposer equivocation when proposal headers are kept off the main chain.

Discussion

Proposer equivocation is when an eligible proposer (or an eligible collator acting as top-level proposer) makes two or more conflicting proposals for a given shard and period. Proposer equivocation was addressed in the retired phase 1 spec by having proposal headers posted to the main chain, and having the SMC enforce proposal uniqueness.

Posting proposal headers on the main chain comes with drawbacks (main chain processing bottleneck, gas costs, censorship, slow and high-variance periods, etc). We can push proposal headers offchain but that doesn't immediately address proposer equivocation. Proposer equivocation is actually the main failure case leading to temporary forks in Dfinity-style full-notorisation schemes.

Below we suggest three strategies to address proposer equivocation with offchain proposal headers.

Strategies

1. Proposer slashing

: Proposer equivocation is an easily attributable fault. A whistleblower can present two equivocated proposals to the SMC to have the corresponding proposer slashed. This may be a significant deterrent if proposers have a corresponding significant minimum deposit (e.g. if they are also executors).

1. Notary honesty

: We can add as a protocol rule that individual notaries should not notarise two equivocated proposals. Assuming honest-majority committees this is sufficient to avoid two equivocated proposals from both getting fully notarised.

1. Notary slashing

: As a strengthening of the notary rule above we can slash dishonest notaries that do sign off on two equivocated proposals. Individual notary slashing requires individually attributable signatures (aggregated BLS signatures are insufficient evidence).