Thanks to Mustafa Al-Bassam (@musalbas), Ismail Khoffi (@ismail), and Mikerah Quintyne-Collins (@mikerah) for review.

HackMD mirror: https://hackmd.io/Vyor9g4kTquybdJSK1DOPw

Resolving the Nothing-at-Stake problem in permissionless consensus protocols using Proof-of-Stake can be accomplished with slashing. Common knowledge tells us that slashing is required

to solve Nothing-at-Stake, but is it? This post analyzes slashing and Nothing-at-Stake, and proposes an alternative to slashing that can provide exactly the same guarantees.

Prerequisite Reading

- Slasher: A Punitive Proof-of-Stake Algorithm, Buterin
- On Stake and Consensus, Poelstra
- Nakamoto Consensus Requires Social Coordination and Subjectivity, Adler

Proof-of-Stake and Nothing-at-Stake

Permissionless consensus protocols based on Proof-of-Stake generally work by having a set of bonded coin-holders (stakers) vote on blocks, with new blocks being added to the chain once a quorum is met. When a staker wishes to cease their involvement in staking, they must remain in an unbonding

(but still bonded) state for a period of time, after which they can completely unbond their coins, freeing them from any rights or responsibility associated with staking.

There are two issues that arise that are not present in Nakamoto Consensus: short-range attacks and long-range attacks. In the former, individual stakers vote for two conflicting chains (equivocate) while still bonded. This can be resolved by slashing still-bonded stakers, introducing a cost for equivocating, much like how there is a cost to working on two different chains in Nakamoto Consensus. The latter attack can be resolved with a weak subjectivity assumption.

This post dives further into short-range attacks, another name for which is Nothing-at-Stake

. Without a penalty for voting for different (conflicting) chains, there is no real cost to voting for any number of different chains (typically only a single digital signature is needed to vote for a chain, which is trivial to produce). In Nakamoto Consensus, work must be done on all chains a miner wishes to “vote” on.

Slashing is one way of solving the Nothing-at-Stake problem and short-range attacks: if a still-bonded staker equivocates, inclusion of cryptographic proof of equivocation into a chain causes the staker to be slashed on that chain, i.e. a fraction of their coins are burned. The exact fraction is a system parameter, and choosing a good value for this parameter is outside to scope of this post. We see that slashing does indeed introduce a cost to voting for two conflicting chains, and thus solves the Nothing-at-Stake problem.

One important thing to note is that Nothing-at-Stake is a game-theoretical issue that only concerns individually rational actors

, and is not related to a history reversion with a large fraction of staking power (usually > 1/3 for most stake-based permissionless consensus protocols). Every single staker, even if they have only a single coin, will vote on everything they can without a disincentive to constrain their votes to a single chain.

Staking Model

We consider the model where the blockchain exists in a closed system, whereby the total market capitalization of all coins remains the same. In other words, if new coins are minted, the price of each coin drops proportionally, and if existing coins are burned, the price of each coin rises proportionally. While the real world is not a closed system, other causes of movements in coin price independent of the mechanisms discussed in this post affect all cases equally, and can thus be safely ignored. We assume that staking rewards in the form of issuance of new coins are permanently positive and non-zero.

Slashing

Since market capitalization is fixed, in order to have any effect penalties must reduce the fraction of coins of an offending staker. Given a staker with c

coins and total number of coins C

, their original fraction of coins \mathcal{F} is $\frac{c}{C}$

. We can calculate their new fraction of coins $\mathcal{F}'$

after being slashed as

$\mathcal{F}' = \frac{c - c \sigma}{C - c \sigma}$

, where $0 < \sigma \leq 1$

is the slashing rate

, a system parameter.

For a small staker with $c \ll C$

, we can simplify the above equation as

$\mathcal{F}' = \frac{c - c \sigma}{C - c \sigma} \approx \frac{c - c \sigma}{C}$

As an example, let us consider the case where $\sigma = \frac{1}{32}$

, e.g. if a staker has 32 coins, they will lose 1 coin if slashed. Their new fraction of coins is

$\mathcal{F}' = \frac{\frac{31 c}{32}}{C} = \frac{31}{32}\frac{c}{C} = \frac{31}{32}\mathcal{F}$

We can see that slashing reduces the fraction of coins of an offending staker primarily by reducing their number of coins.

A Rose By Any Other Name

In this section we propose an alternative equivalent to slashing: blacklisting. If a slashable offense is detected, rather than being slashed, the still-bonded (i.e. actively-bonded or unbonding-but-not-yet-unbonded) staker is blacklisted

. In this state, they are set to unbonding (or remain as unbonding) for a period of time, a system parameter. The blacklisting duration is added on top of the regular unbonding duration. During this time, they cannot do anything with their coins, and cannot collect staking rewards as they are not actively bonded.

We note that since staking rewards are positive and non-zero, not staking results in dilution, as the total number of coins increases. Assuming a fixed issuance rate, and given a staker with c

coins and total number of coins C

, their new fraction of coins after being blacklisted is

$\mathcal{F}' = \frac{c}{(C - c) \rho + c}$

, where $\rho > 1$

is the reward rate

, the issuance rate for staking coins for the duration of a blacklisting

. As the name suggests, the issuance rate only counts issuance of new coins, not transaction fees. This post only considers the case of a fixed issuance rate, but more complex issuance rate equations can be modeled as well and are left as an exercise for the reader.

Note that issuance of new coins should generally greatly outweigh transaction fees in order to avoid consensus instability.

For a small staker with $c \ll C$

, we can simplify the above equation as

$\mathcal{F}' = \frac{c}{(C - c) \rho + c} \approx \frac{c}{C \rho}$

to simplify analysis. Note that performing analysis on the full equation ultimately yields the same conclusions, and is left as an exercise for the reader.

Can this penalty—that is not slashing—produce the exact same results as slashing? Consider the same example as the previous section, $\sigma = \frac{1}{32}$

. We can equate the RHS of both equations and compute a value for ρ

:

\begin{align} \frac{31}{32} \frac{c}{C} = & \frac{c}{C \rho} \ \rho = & \frac{32}{31} \ \end{align}

In other words, a value of \rho \approx 103\%

produces the exact same end result as slashing with \sigma = \frac{1}{32}

.

As another example, consider

\lim\limits_{\rho \to \infty} \frac{c}{(C - c) \rho + c} = 0

The equivalent slashing rate would clearly be 100\%

, i.e. \sigma = 1

.

Penalties to Solve Nothing-at-Stake

We see that it is always possible to compute a value for \rho

given \sigma

(or \sigma

given \rho

) with the equation

\frac{c - c \sigma}{C - c \sigma} = \frac{c}{(C - c) \rho + c}

, and therefore the two penalties can be parametrized to be completely functionally equivalent. However, without changing the reward rate, blacklisting can only be parametrized using the duration of blacklisting. Given contemporary deployments of Proof-of-Stake protocols, and their reward and slashing rates, this in practice could result in blacklisting durations on the order to several months to a year or more to achieve the same effect as slashing.

Slashing and blacklisting are two elements from a generic class of penalties that can be applied to introduce a cost to equivocating and other staker offenses. With proper parameter choice, these two schemes can produce identical results. There may be other penalties that can be applied to offending stakers, and exploration to the possibility space is left as future research.

Conclusion

We demonstrate that slashing

is not necessary to resolve Nothing-at-Stake in permissionless consensus protocols using Proof-of-Stake, but instead a generic class of penalties, which includes blacklisting

—locking bonded coins that have equivocated for a period of time—is sufficient. In fact, we show that blacklisting is functionally identical to slashing, and provides the same guarantees under our model.