Description

Instant Redelegation is when an account A is proxying its stake to B, and then wants to switch its proxy from B to C. Instant Redelegation allows A to switch proxys from B to C without waiting for a thawing period to complete. The funds will enter a fake thawing period with B, where if B commits a slashing offense during the thawing period, the funds will be slashed and C's stake will no longer contain the proxied funds.

Motivation

The motivation is to allow users to be able to change their proxied stake without having to wait an entire thawing period (3 weeks) without receiving rewards. If users have to wait an entire thawing period to change their proxy, whilst giving up any rewards, users will be hesitant to change their proxy. We want the proxied stake to be dynamic and constantly adjusting/rebalancing in Logos.

Purpose of staking

Investment in the network

Consider the purpose of staking. First consider staking without slashing. Staking is based on the idea that those who have a lot of "stake" in the network (have a lot of Logos), have the network's best interest in mind. If I have a large stake in logos, I have invested quite a bit in Logos; I want to see the currency do well, and if the currency crashes, I will lose a lot of money. Therefore, the thinking goes, I will not be approving malicious activities or engaging in them if I have a large stake, or investment, in logos.
This type of staking does not require my stake to be "locked" and doesn't require a thawing period (waiting 3 weeks after retiring to claim my stake). However, locking my stake makes my investment in the network larger, because if the currency does crash, I cannot immediately sell off my logos.

Slashing and Nothing-at-stake

Slashing came about because the "investment in the network" argument contains assumptions. One would assume that if I have a million logos, I will not be malicious or approve malicious activities, like double spends, but this is an assumption about human behavior and the price of the currency, and not a protocol level guarantee.
Slashing solves the nothing-at-stake problem. The nothing-at-stake problem is the situation where, as a validator in a PoS network, there is nothing stopping me from approving double spends or attempting them myself. I am not burning any extra resources by approving or attempting a double spend, the way I would be expending extra resources in a PoW network. In fact, if there is a non-zero chance the double spend succeeds, and there is no penalty for attempting a double spend, a rational agent would always attempt double spends, as the

expected value is positive. With Logos' consensus mechanism, if the byzantine assumption is not violated, these double spend attempts should never succeed. However, allowing delegates to vote for invalid requests without any penalty allows delegates to eat up bandwidth and performance space with no repercussions.

Thawing and Long-Range Attack

Slashing combined with locking (keeping stake locked after the validator/delegate is no longer validating), prevents something called the long range attack. Consider a situation where stake is released to a delegate immediately after the delegate stops validating. Now consider a light client who was offline while this delegate was actively validating. When this light client attempts to sync with the network, the delegate who is no longer validating can send the light client fake blocks that have a timestamp during this delegates active period. The light client will see from everyone else in the network that this delegate was active during that period, and if enough old delegates collude together, they can create blocks that have enough signatures to be post-committed. The light client has no way of knowing these blocks are fake. However, the other nodes on the network, who are up to date, do know that these blocks are fake. If the malicious delegate's staked funds are locked in a "thawing" state, these other up-to-date nodes can slash the malicious delegate/s. If the funds are not locked in a "thawing" state, the malicious delegate is free to attempt these attacks without consequence (another version of the nothing-at-stake problem).

Staking and Representatives

In Logos, accounts can only proxy stake to representatives, not delegates, so it is worth exploring these attack vectors from a representative's point of view. The slashing condition for a representative is submitting two conflicting votes during an election period (one epoch). It is important to note that election votes are processed through consensus and post-committed by the delegates. Therefore, submitting conflicting election votes during an election is no different than attempting to spend funds you don't have, send tokens you don't have, declare candidacy when you are ineligible or submit any other type of invalid request. The delegates will simply reject one or both of the election votes.

Representatives that have a lot of stake, or investment, in the network are more likely to vote for delegate candidates that they trust and believe are healthy for the network.

The nothing-at-stake problem, in it's vanilla form, does not fully apply to representatives. Reps cannot approve double spends, and there is no clear benefit to submitting conflicting election votes.

The long-range attack problem also does not fully apply to representatives.

Security of Instant Redelegation

So staking with slashing and thawing serves 3 purposes:

1. Validators (and Representatives) are invested in the network
2. Solve nothing-at-stake problem
3. Prevent long-range-attack

To determine if instant redelegation of proxied stake is safe, we will consider each of the 3 purposes staking serves.

1. Investment in the network
    a. Instant Redelegation does not take any stake out of the network. Therefore, this security aspect of staking is not compromised.
2. Nothing-at-stake
    a. If I instantly redelegate from B to C, there is no new situation where either B or C will have nothing at stake. If C gets slashed, B will still have the stake of other accounts that proxied to B, as well as its own minimum stake (delegates and reps must stake to themselves, in addition to any stake proxied to them). The same applies if C gets slashed.
3. Long-range-attack
    a. The same argument as the general nothing-at-stake problem applies to the long range attack.

One burning question about instant redelegation is in the event that I proxy to B, and then redelegate from B to C, then B and C both act malicious. My proxied stake deserves to be slashed twice (for B and for C), but it can only be slashed once. However, this is no different than I proxy to B, B acts malicious, my stake is slashed, and then B acts malicious again. Here my proxied stake deserves to be slashed twice, but can only be slashed once.

Instant redelegation maintains a useful invariant: if I commit a slashable offense, after that offense my stake will be slashed. There is a possibility my stake was already slashed prior to this offense, but regardless, my stake will be slashed if I commit a slashable offense.

My proxied stake is only ever active with one rep at a given time, so if I redelegate from B to C, and B acts malicious and gets slashed, my proxied stake is no longer available to C. Therefore, no one ever is able to use my proxied stake for free, without the possibility of slashing.

What is the purpose of slashing proxied stake in the first place? Slashing proxied stake makes me as the proxying account select well-behaved reps to proxy to. Also, if proxied stake is not slashed, I could create a rep, put all of my funds in another account, proxy to the rep account, and then behave maliciously with no consequences. This is a form of the nothing-at-stake

problem. Instant redelegation does not provide an avenue for me to select less well-behaved reps, and does not provide a loophole for the nothing-at-stake problem.