# Secure Vote Signing

A validator receives entries from the current leader and submits votes confirming those entries are valid. This vote submission presents a security challenge, because forged votes that violate consensus rules could be used to slash the validator's stake.

The validator votes on its chosen fork by submitting a transaction that uses an asymmetric key to sign the result of its validation work. Other entities can verify this signature using the validator's public key. If the validator's key is used to sign incorrect data(e.g. votes on multiple forks of the ledger), the node's stake or its resources could be compromised.

## Validators, Vote Signers, and Stakeholders

When a validator receives multiple blocks for the same slot, it tracks all possible forks until it can determine a "best" one. A validator selects the best fork by submitting a vote to it.

A stakeholder is an identity that has control of the staked capital. The stakeholder can delegate its stake to the vote signer. Once a stake is delegated, the vote signer's votes represent the voting weight of all the delegated stakes, and produce rewards for all the delegated stakes.

## Validator voting

A validator node, at startup, creates a new vote account and registers it with the cluster via gossip. The other nodes on the cluster include the new validator in the active set. Subsequently, the validator submits a "new vote" transaction signed with the validator's voting private key on each voting event. Previous Turbine Block Propagation Next Runtime Native Programs