COMPARING SLASHING PENALTIES ON STAKED BLOCKCHAIN NETWORKS

Eric Alston, CU Boulder

William Lehr, MIT

Bryce Bugge, CU Boulder

AUTOMATED PENALTIES

- Penalties uncommon in private coordinative contexts prior to staked blockchain networks

- Threat of discretionary termination serves as a hanging penalty to which any employee is subject; Rewards also discretionary to induce effort (end of year bonuses, etc)

- But if blockchain meant to eliminate a centralized discretionary intermediary → Automated rewards and penalties more important

- Simple rewards for narrowly scoped joint production, but what about more complex joint coordinative purposes (Turing complete systems)?

- Economic organizational logic for the emergence of slashing penalties

Category	Description of Typology
PENALTY CONDITIONS	Validator behaviors that result in the application of penalties
- Malicious Signal	Actions committed on chain that demonstrate malicious intent when validating transactions on the blockchain
-- Conflicting actions	Any form of sending/validating conflicting information to a network that could be a signal of malicious intent
--- Double Signing	When a validator attempts to sign two blocks/transactions simultaneously for the same height/position
--- Double Attestation	Validator equivocation as to the validity of a proposed set of transactions: "double attestation" or "double voting"
--- Transaction Omission	Omission of transactions in a proposed block
- Non-Participation	Failure to participate in validating transactions on the blockchain due to "downtime" or "missed blocks"
PENALTY TYPES	Possible penalties predicated on one of the above slashing conditions being met
- Economic Penalties	Penalty affecting a validators stake and/or rewards being received for validating transaction on a network
-- Percentage Penalty	Validator's stake is reduced by a percentage, a penalty which tends to be uniformly present for all infractions in cases where applied
-- Fixed Penalty	Validator's stake is reduced by a fixed amount, regardless of the amount that they have staked to the network
-- Forgone Rewards	Loss of potentially earned rewards due to temporary or permanent removal from validator set
- Enhanced Penalties	Additional penalties applied as a function of other harmful behaviors in a contemporaneous period as one validator's infraction
- Validator Removal	Penalty involving a validator being involuntarily removed from the validator set
-- Permanent Removal	Validator is involuntarily removed from the validator set permanently - often seen with conflicting actions (i.e. "Tombstoning" or "Slashing")
-- Temporary Removal	Validator is involuntarily removed from the validator set temporarily - often seen with downtime slashing infractions (i.e. "Jailing")
- Forgone Governance	Ability of validator to participate in protocol update decisions is absent or reduced in cases of temporary or permanent removal
PENALTY APPLICATION	The process by which behaviors are assessed and penalties are applied
- Automatic	Behavior is automatically identified and penalty is automatically applied
- Conditional	Additional penalties applied conditional on the automatically assessed contemporaneous behavior of other validators
- Discretionary	Assessment of infractions can be human-initiated, or level of penalties can be defined by a human authority

SUMMARY STATISTICS

- 46 of 69 staked blockchain networks (in the top 100 by market cap) have penalty regimes ($1.62 to $375k for double-sign; <$0.01 to $36k for downtime)

- 8 of 46 penalty regime networks have original codebase; majority either EVM or Cosmos SDK

- Withdrawal queues range from instantaneous to 28 days, with a rough average among 54 staked networks of 11.5 days of waiting to withdraw

- Temporary removal from validator set more common than permanent removal (perhaps due to inability to bar from reentry due to pseudonymity?)

- Offline penalties range from forgone rewards to a small fraction of pledged stake

- Notably hard to obtain this information for a significant percentage of the networks → average users are not a key audience for this information?

Why should Ethereum care?

I don't think about you at all.