Correct By Costruction (Casper) -Implementation in Chain

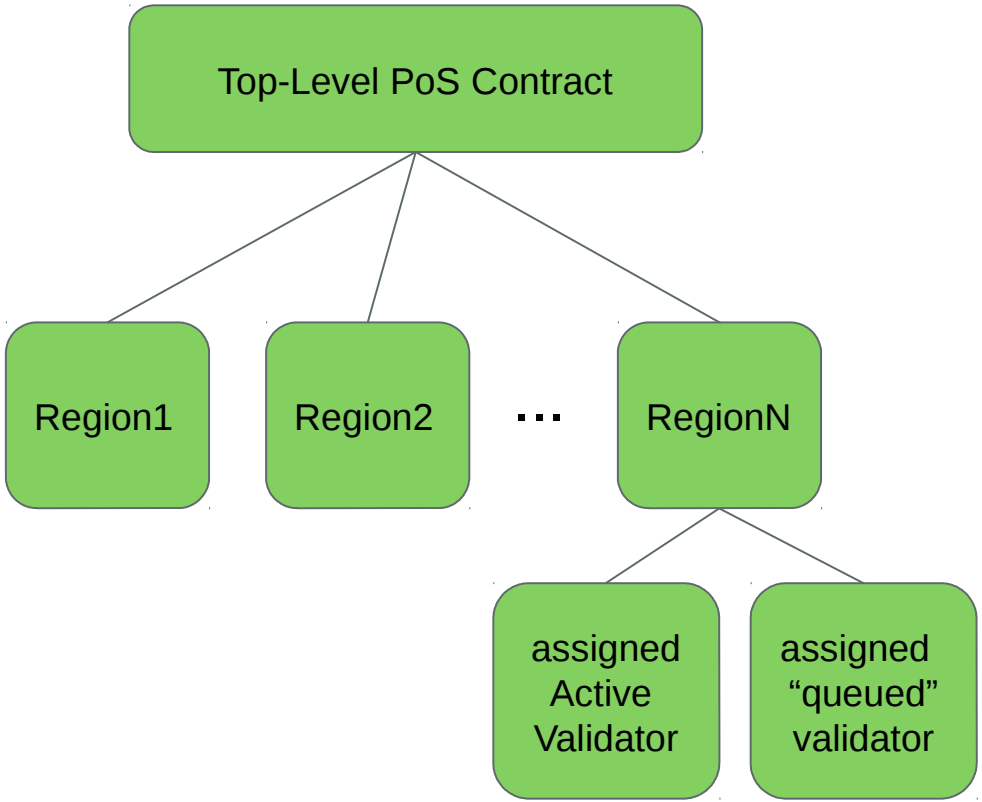
by Patrick Udo Kranenzien

Disclaimer

I Am only a Messenger

The Correct by Construction Casper Protokoll:
(short intro)

- Introduced By **Vlad Zamfir's** intententionally ment
  For the Ethereum Network
- Belongs to family of Proof-of-Stake protocols
- Validators bet on new blocks with their stake
- Introduces Slashing as punishment
- Solves the “Nothing at Stake” Problem by
  - Punishing validators with malicious betting behavior get by slashing there Stake
  - Punishing none-perfoming (offline) validators



- Bonding
- Unboding
- Slashing

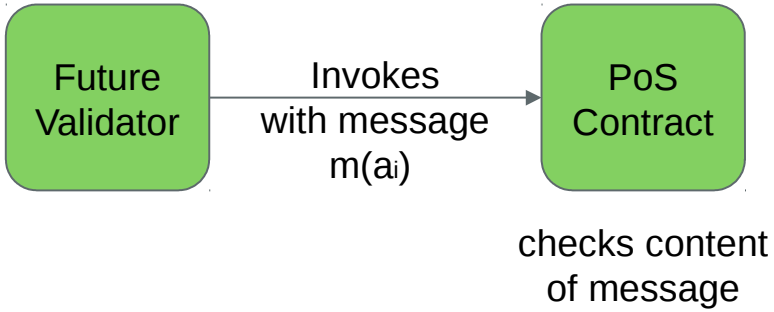
- Distribution of Rewards

Region

Regions are self defined at creation by:

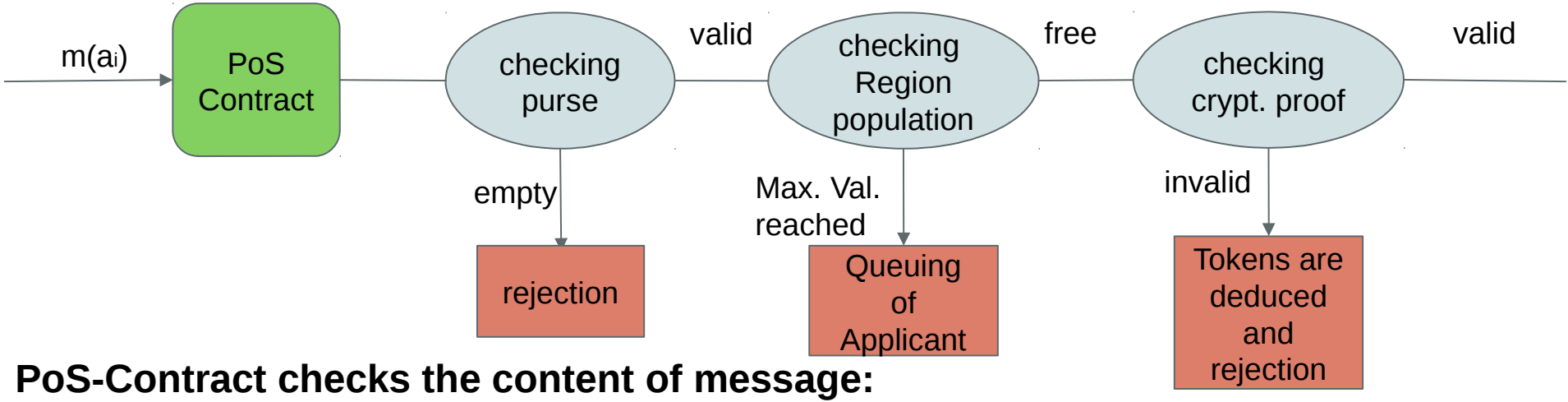
- The max. number of active validators
- The max. number of “queued” validators
- The max unbounding rate (N validators per 100 blocks)
- The post-unbounding stake holding time (in blocks)
- The minimum bond amount
- The maximum bond amount
- Cryptographic evidence for Proof-of Performance (joining and slashing

This information is known by the PoS-Contract



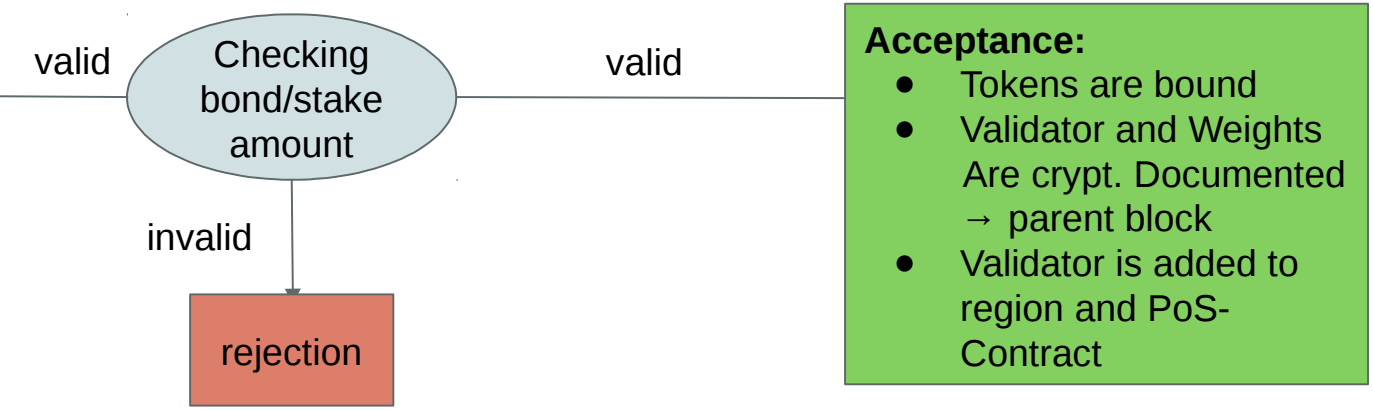
Future Validator invokes the PoS-Contract by providing:

- The region they want to join
- A form of cryptographic ID (e.g. public key)
- A purse
- Cryptographic evidence as needed by region



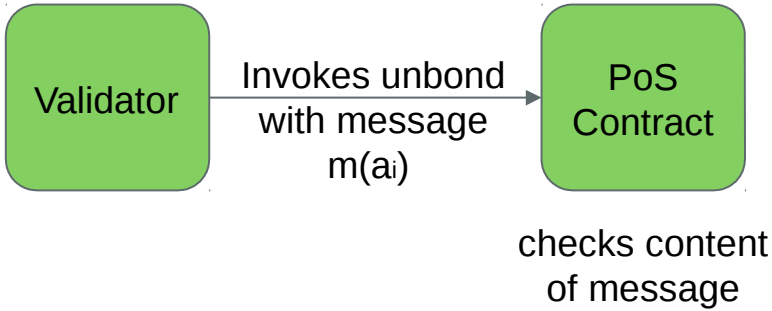
PoS-Contract checks the content of message:

- Autom. rejects if purse is empty
- “Queues” Validator if number of max. Validators is reached
  → stops evaluation
- Evaluates cryptographic evidence
  → rejects & deduces tokens if invalid



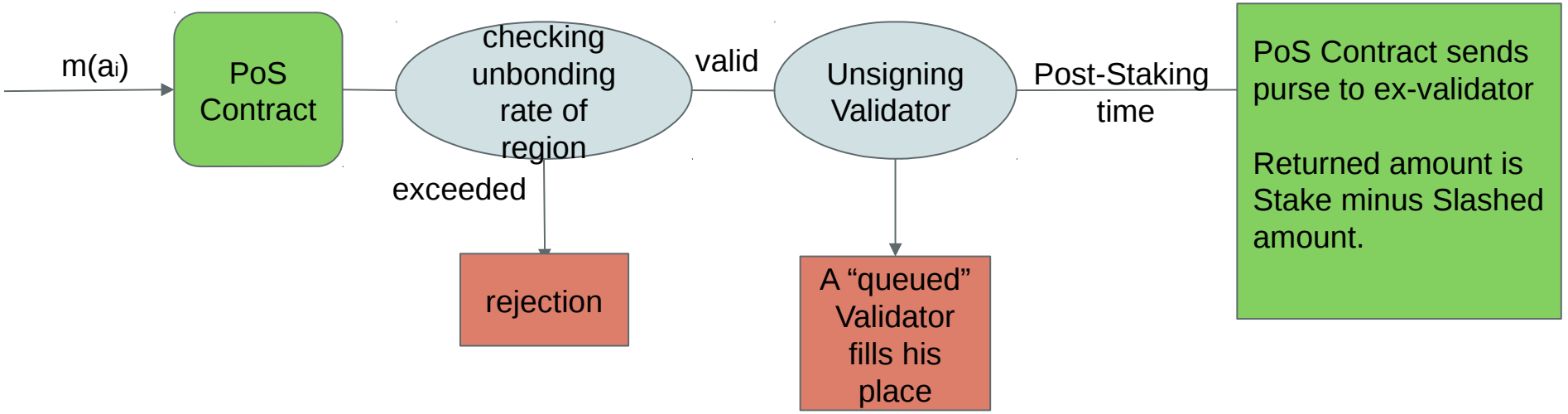
When bond amount is within the defined limit of the region (min./max. bound)the validator is accepted.

Note: The second evaluation of the purse compares amount to the local contract -the first not. → avoidance of DoS-Attacks



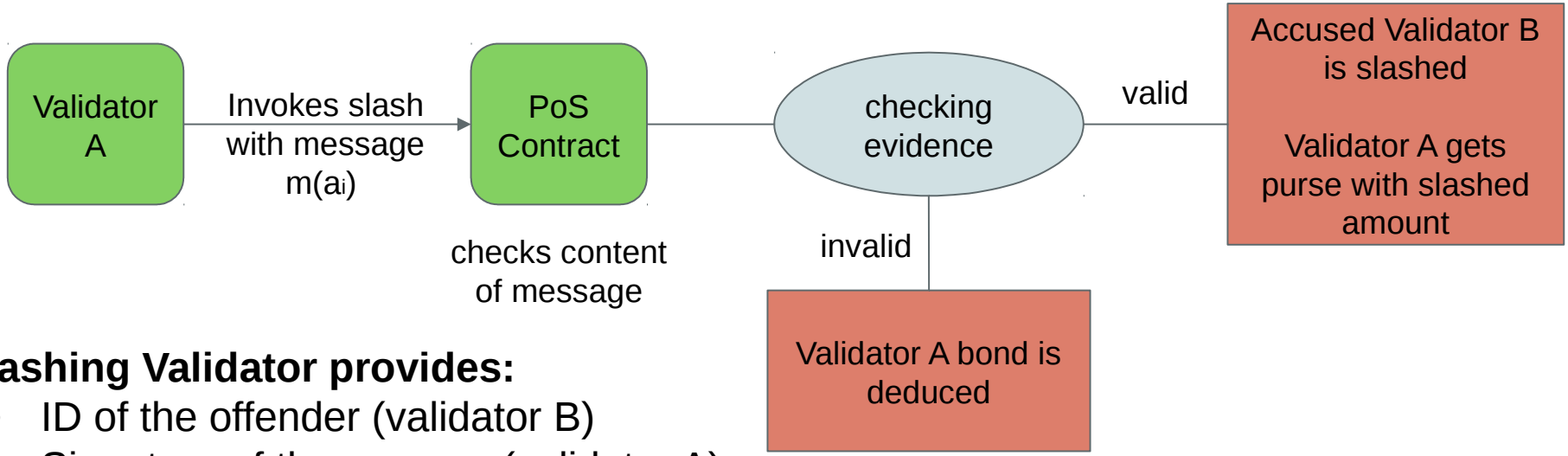
Future Validator invokes the PoS-Contract by providing:

- A signature with the block after which he wants to unbond
- A channel at which he will later receive His stake back



Note:

- During the Post-Stake time the ex-validator’s stake is still slashable
- If Bond of validator is 0 or out of the local’s contract range an automatic Unbonding is triggered
- Rewards are not paid out by the top level PoS-Contract
- The Post-Stake time reduces the risk of “long range attacks”

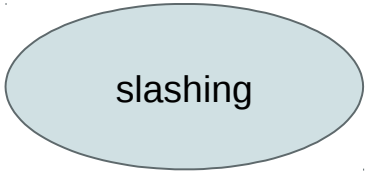


Slashing Validator provides:

- ID of the offender (validator B)
- Signature of the accusor (validator A)
- Offence descriptor
- Cryptographic evidence of the offence
- A purse return channel

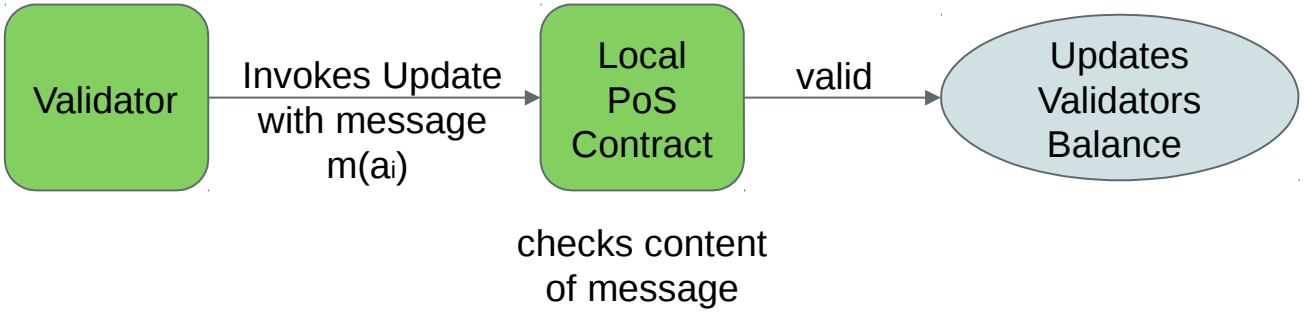
Pro: Economic incentive for slashing other validators

Con: Possible unbonding through backdoor



Slashable Events:

- Breach of Service-Level-Agreement (SLA)
  (SLA's are region-specific)
- Production of an invalid block
- Equivocation
  Validators sends two contradicting (signed), which can not be causally ordered



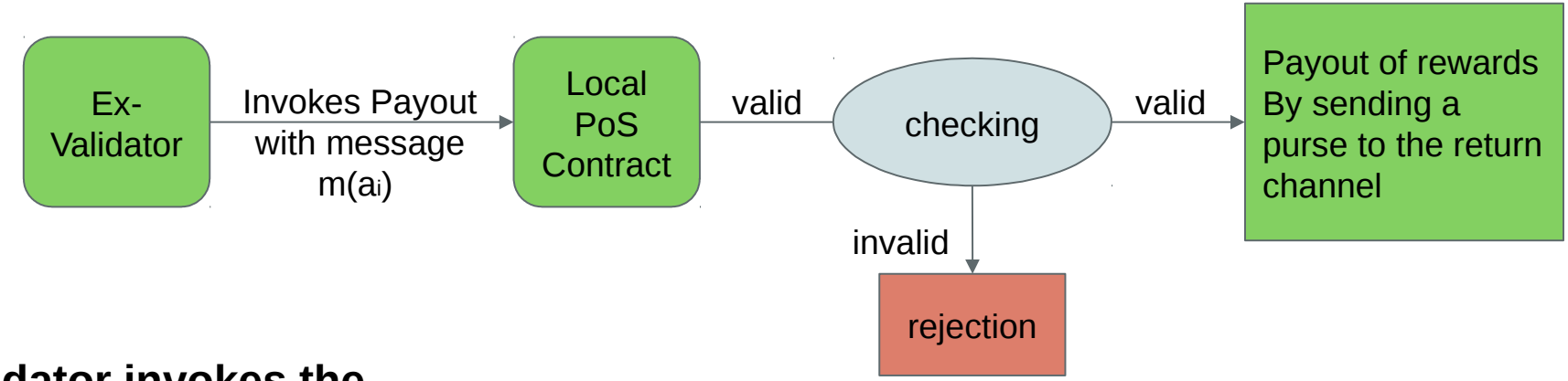
Validator invokes the local PoS-Contract by providing:

- A signature

The Balances are updated byq:

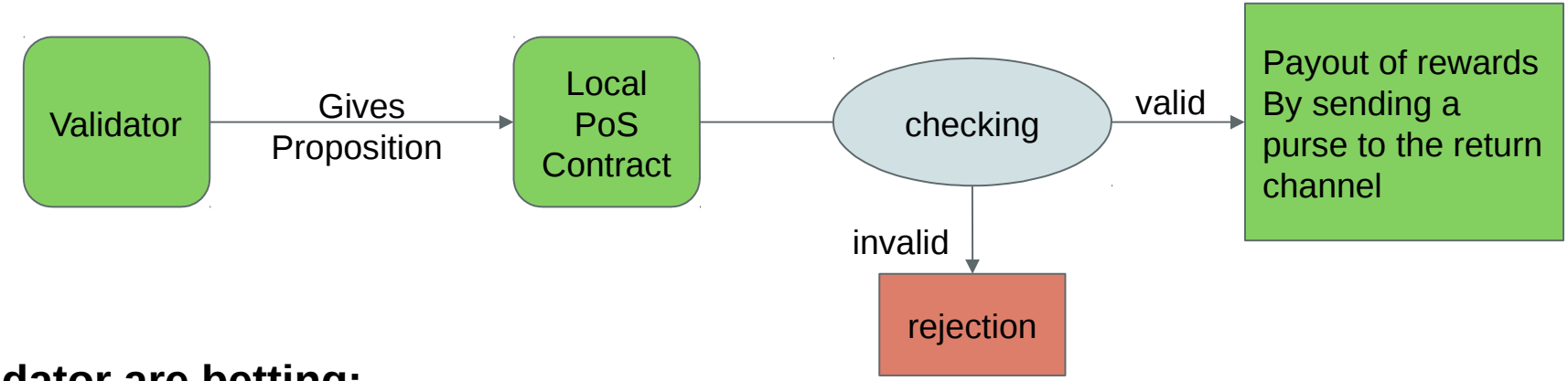
Reward = Discount * transactionFees

The Discount-Faktor **decreases** with **increasing consecutive blocks** pubplished by the validator
→ incentive for cooperation with other validators



Validator invokes the local PoS-Contract by providing:

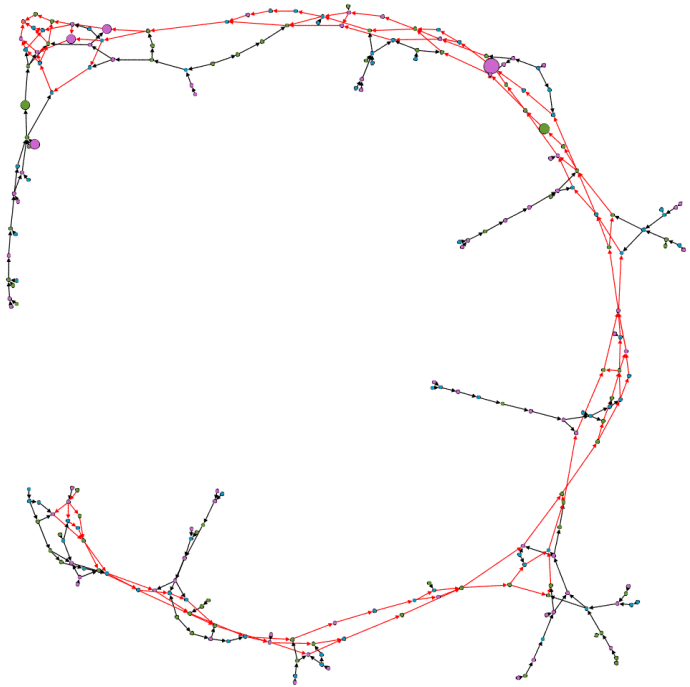
- Validator ID
- Purse Return Channel



Validator are betting:

- Validator ID
- Purse Return Channel

Validators are betting on **propositions**
Like on the sequence/order of blocks
Rather than on single blocks.
→ higher transaction rate



https://medium.com/rchain-cooperative/a-visualization-for-the-future-of-blockchain-consensus-b6710b2f50d6

End