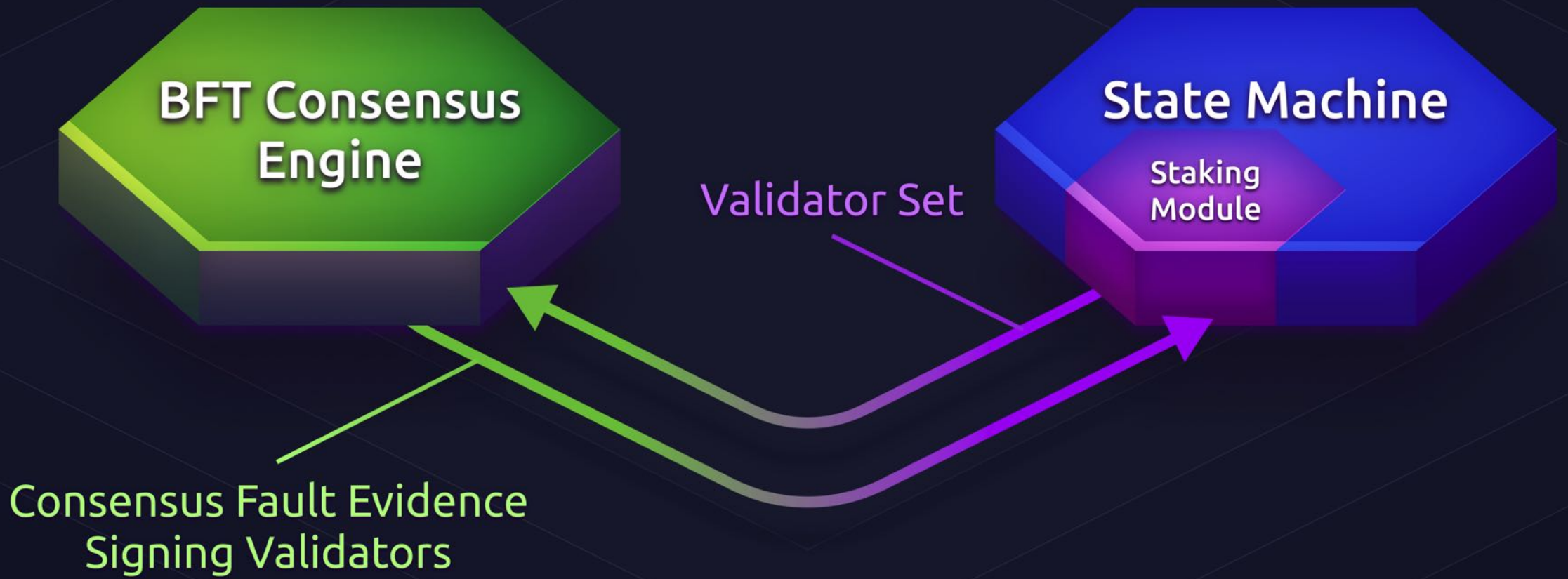
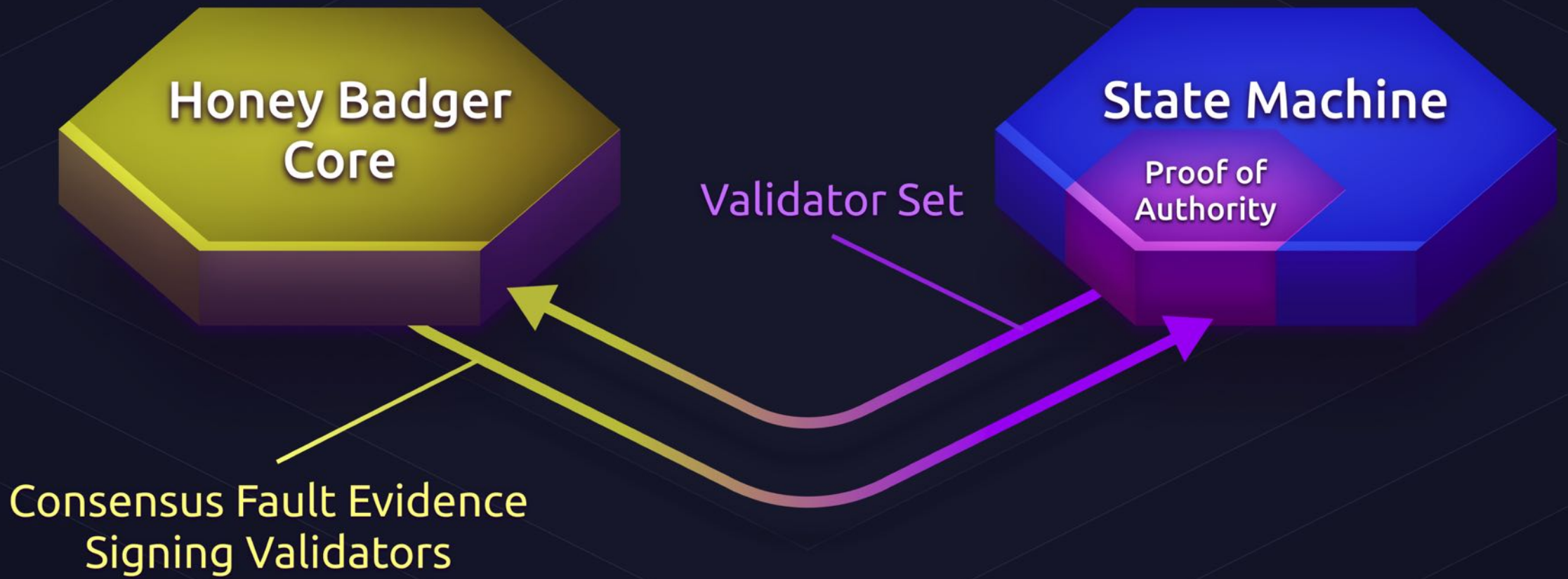
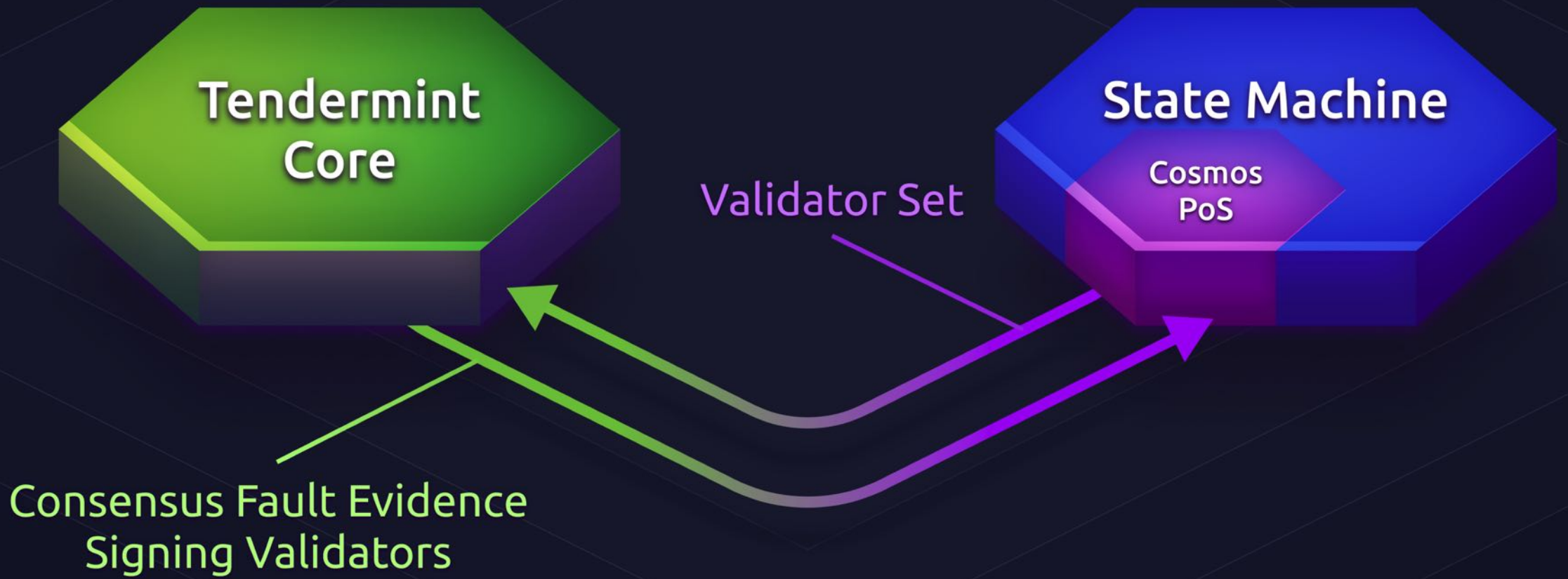
# COSMOS

# PROOF-OF-STAKE

Sunny Aggarwal
Researcher & Core Developer at Cosmos

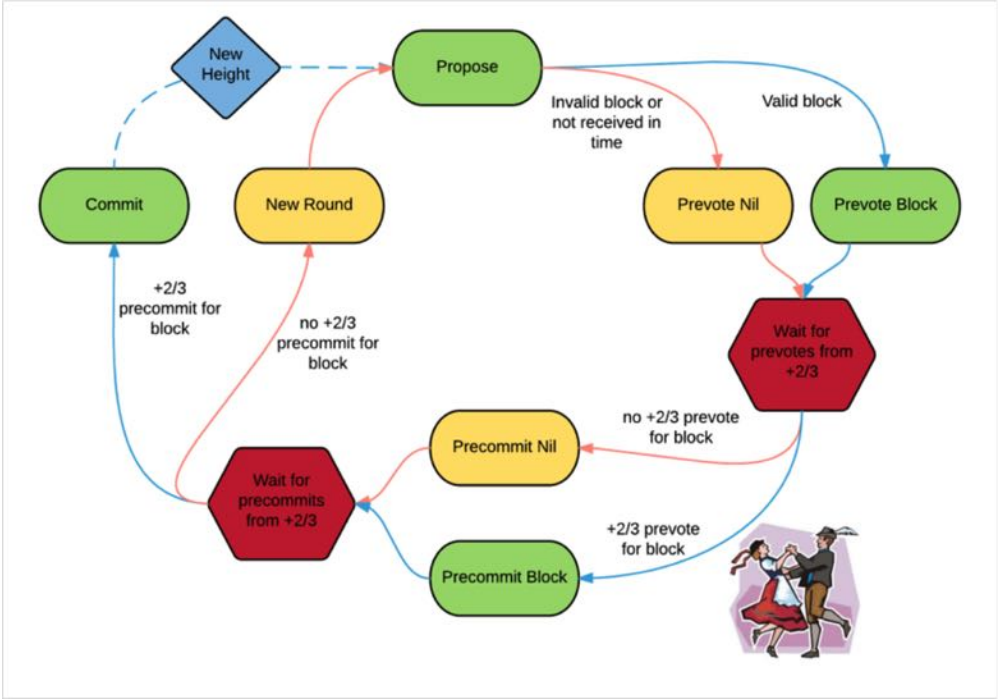

BFT Consensus Engine
State Machine
Staking Module
Validator Set
Consensus Fault Evidence
Signing Validators

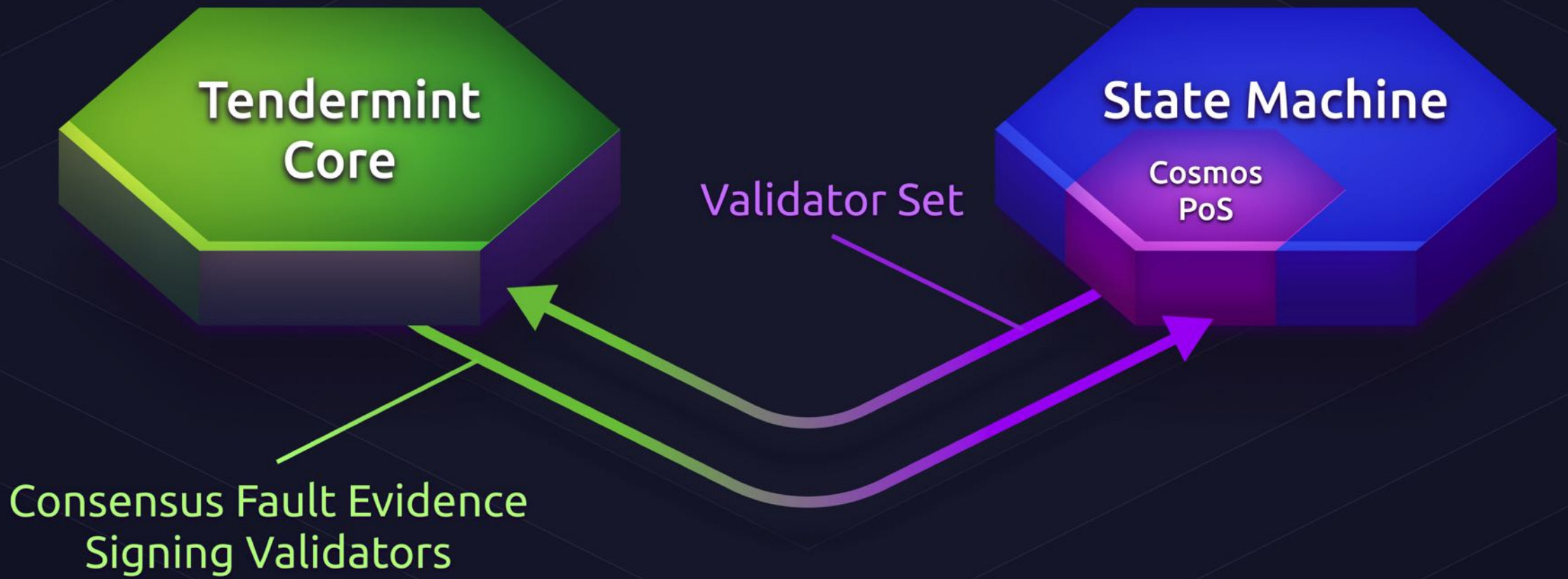

Honey Badger
Core
State Machine
Proof of
Authority
Validator Set
Consensus Fault Evidence
Signing Validators


Tendermint
Core
State Machine
Cosmos
PoS
Validator Set
Consensus Fault Evidence
Signing Validators

# Tendermint BFT

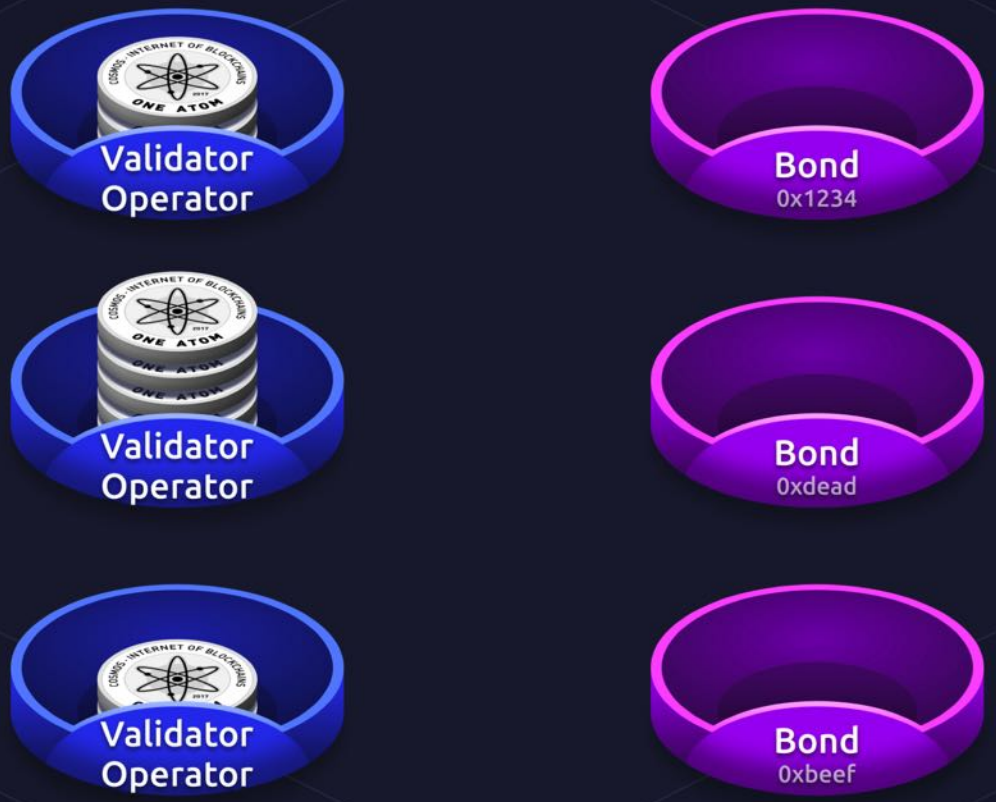
- 1 Block Finality
- Requires +2/3 of the validator set to sign on a block to commit
- Proposer changes every round
- Doesn’t scale as # of validators increases

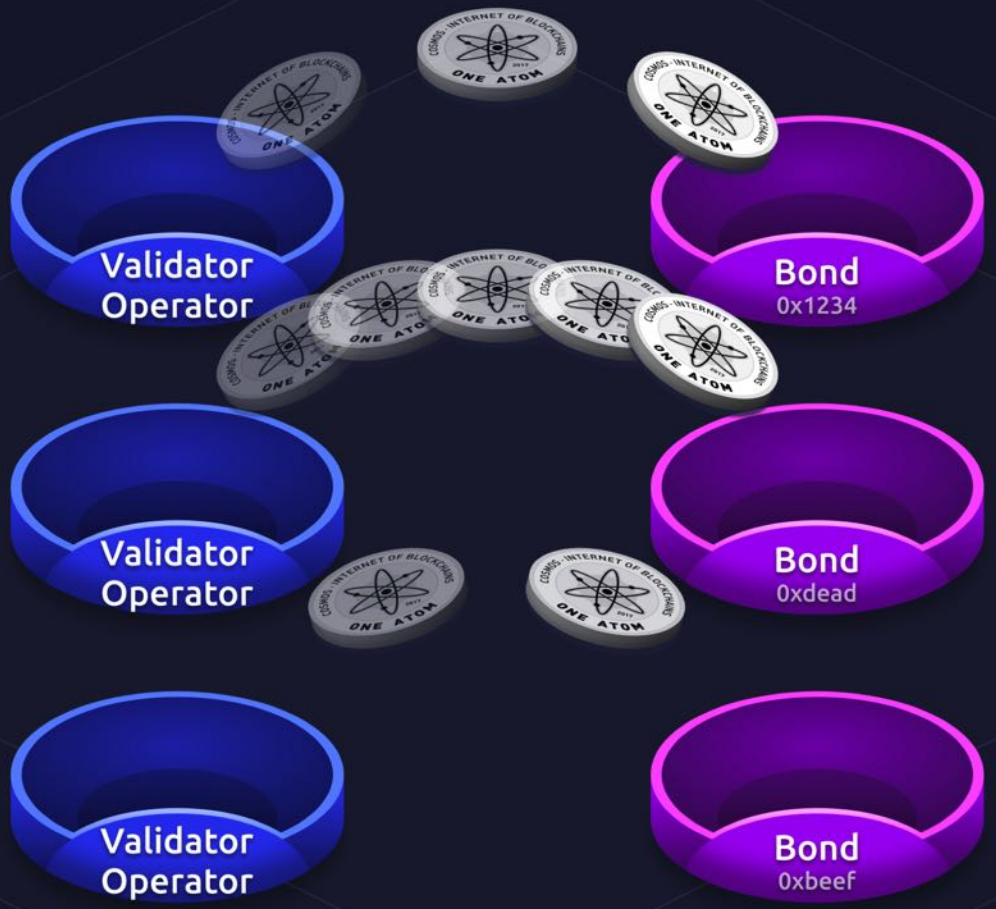


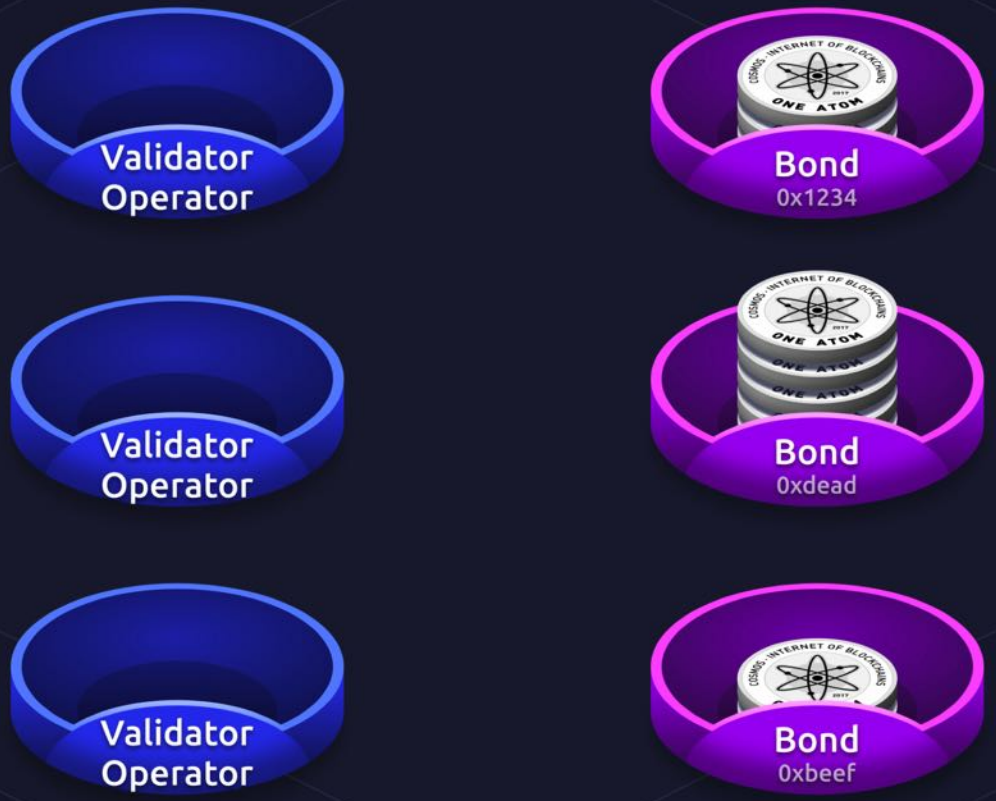

Tendermint
Core
State Machine
Cosmos
PoS
Validator Set
Consensus Fault Evidence
Signing Validators

# Why Proof of Stake?

# Basics of Proof of Stake


Validator
Operator
Bond
0x1234
Validator
Operator
Bond
0xdead
Validator
Operator
Bond
0xbeef


Validator
Operator
Validator
Operator
Validator
Operator
Bond
0x1234
Bond
0xdead
Bond
0xbeef


Validator
Operator
Validator
Operator
Validator
Operator
Bond
0x1234
Bond
0xdead
Bond
0xbeef


Validator
Operator
Bond
0x1234
30%
Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
20%

# Slashing


Validator
Operator
Bond
0x1234
30%
Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
20%


SLASH
Validator Operator
Bond
0x1234
30%
Validator Operator
Bond
0xdead
50%
Validator Operator
Bond
0xbeef
20%


SLASH
Validator Operator
Bond
0x1234
Validator Operator
Bond
0xdead
71%
Validator Operator
Bond
0xbeef
29%

# Unbonding


Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
20%


Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
50%

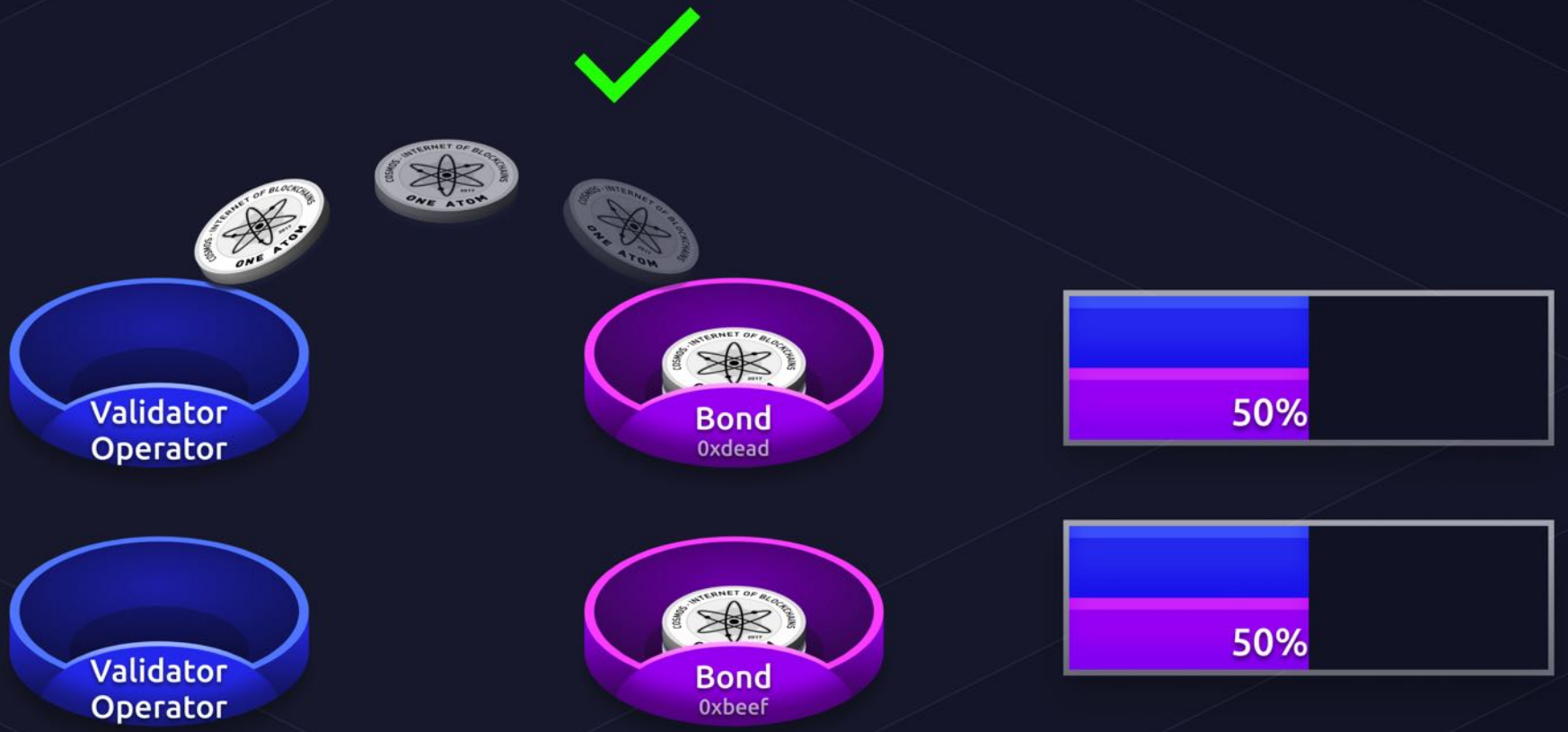

Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
50%


SLASH
Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
50%


Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
20%


Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
50%


Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
50%

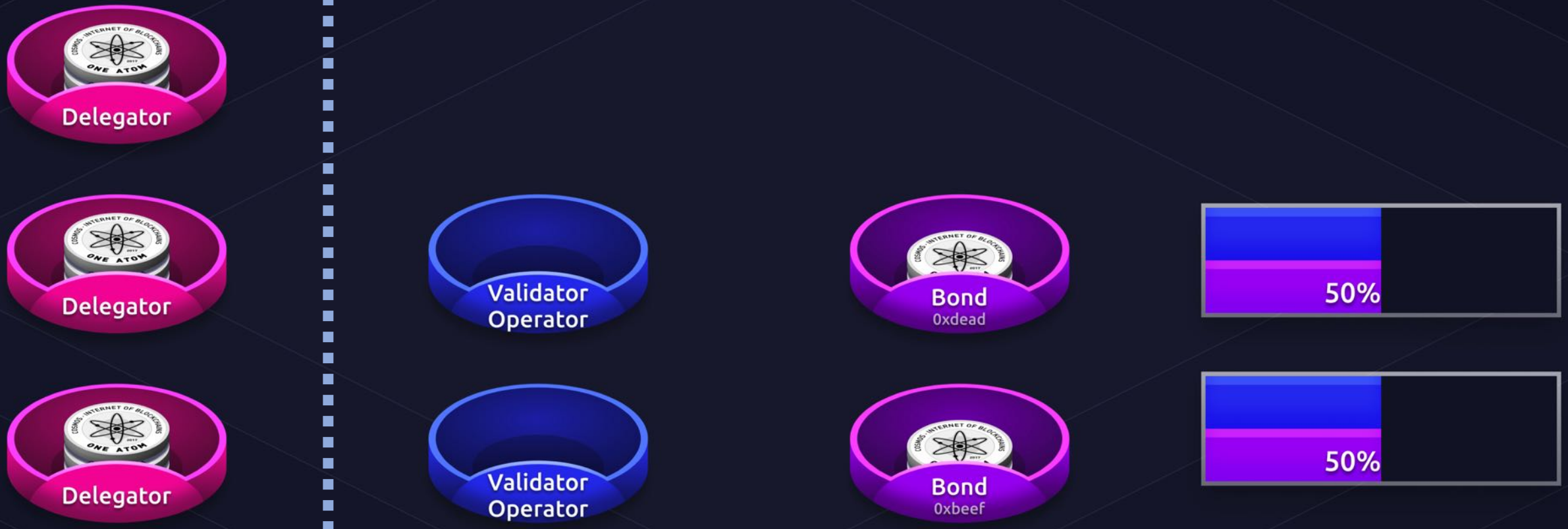

Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
50%


Validator
Operator
Bond
0xdead
50%
Validator
Operator
Bond
0xbeef
50%

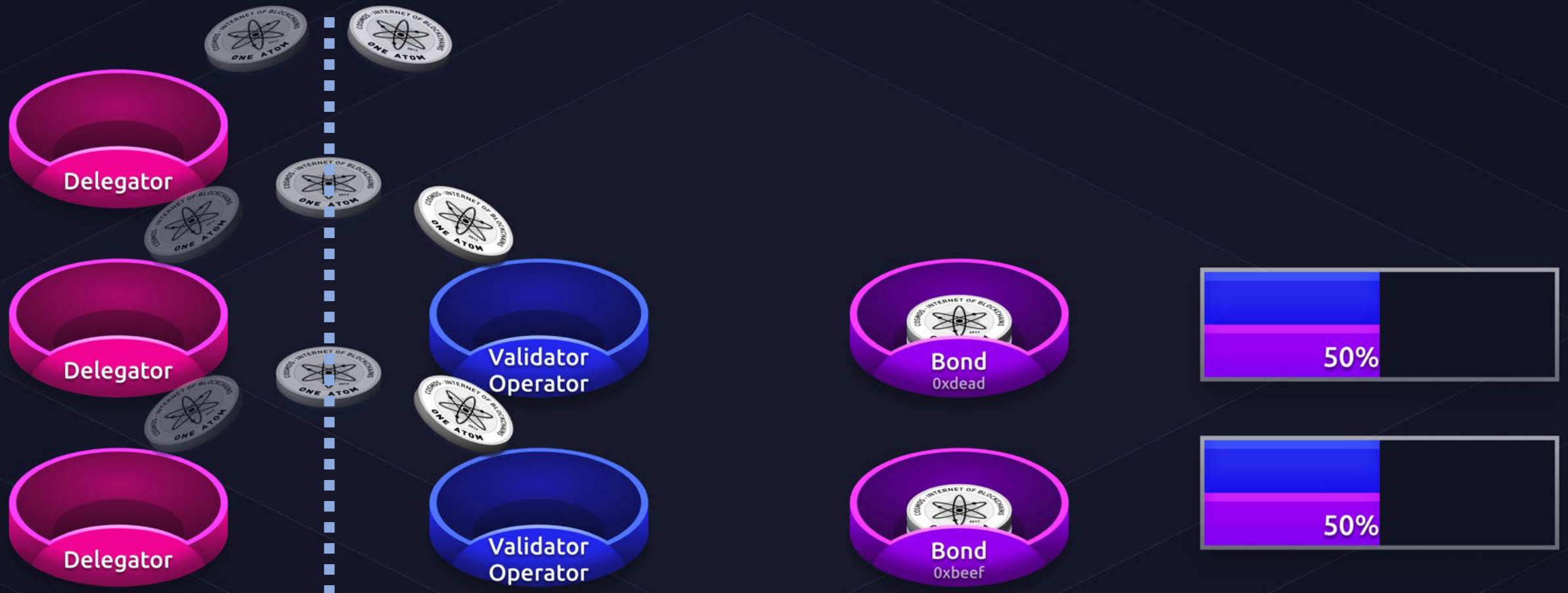
# Out of Band Delegation

# Out of Protocol

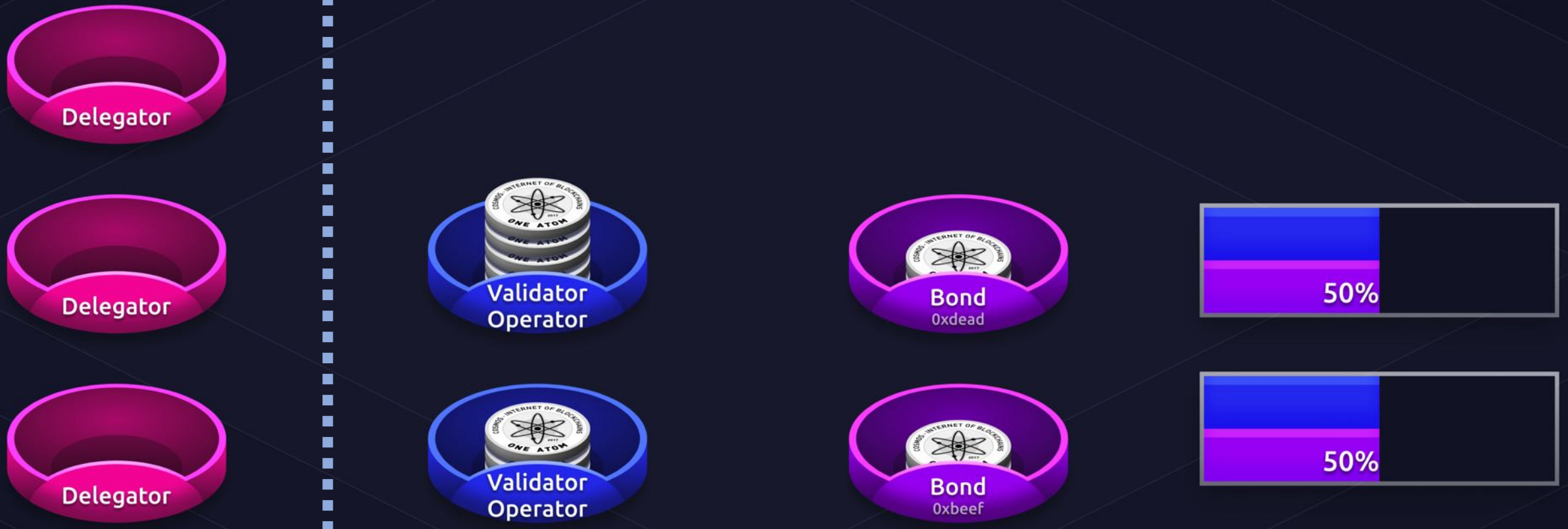
# Out of Protocol



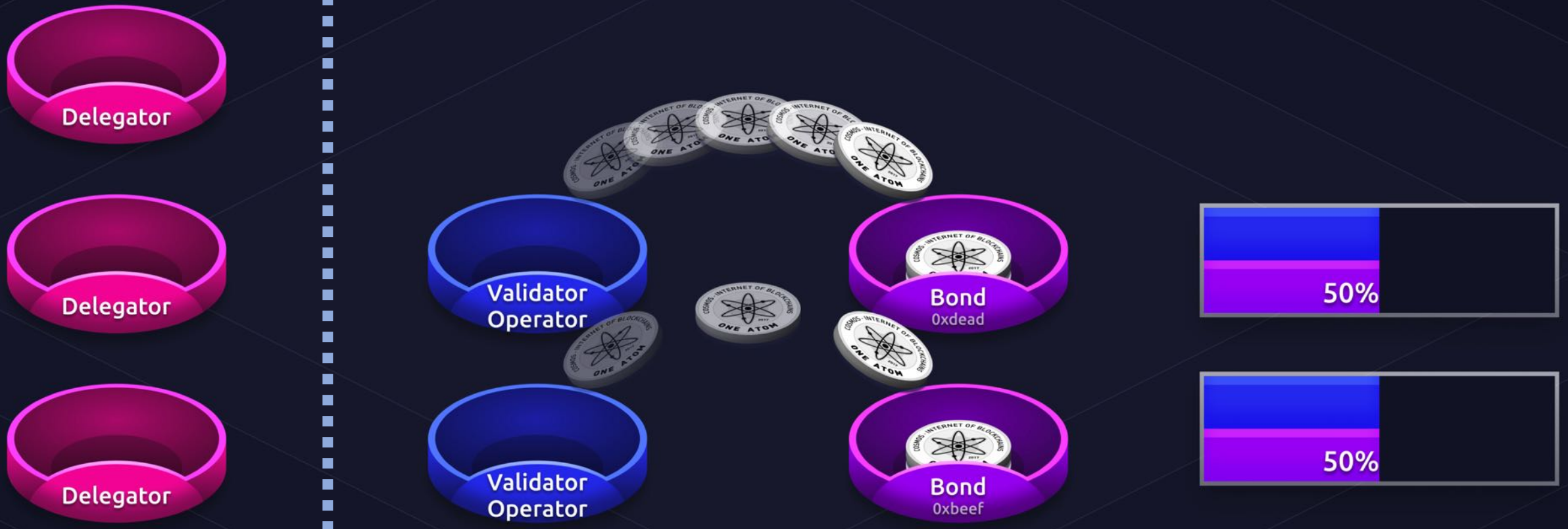
# Out of Protocol



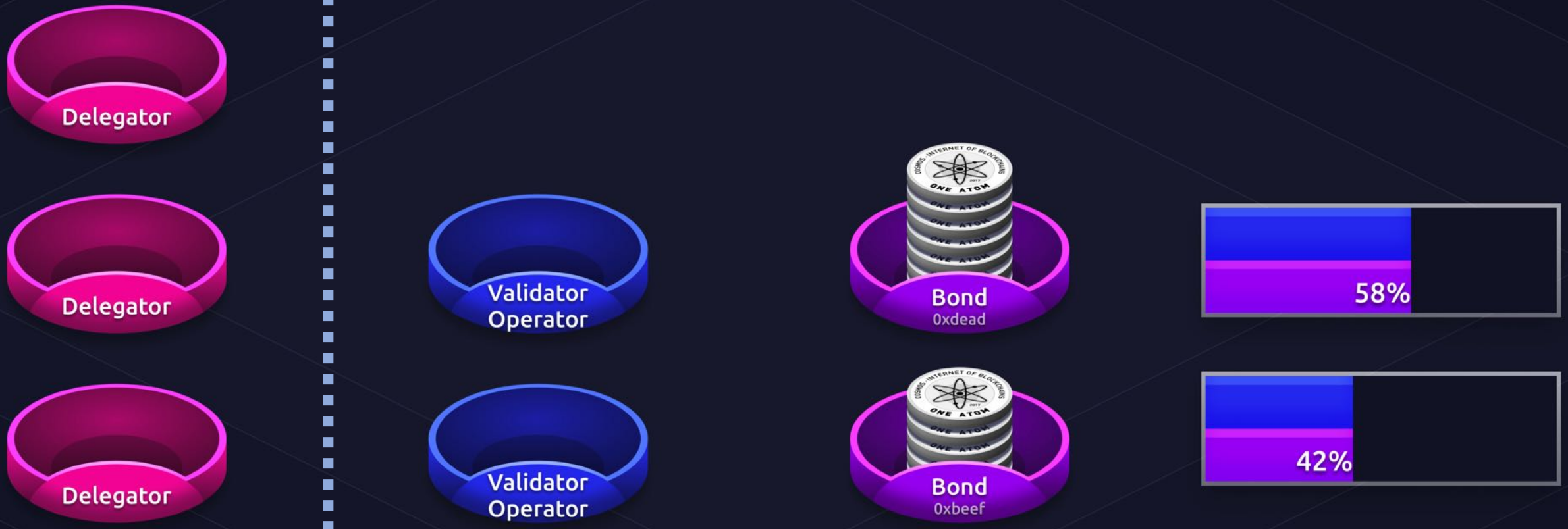
# Out of Protocol



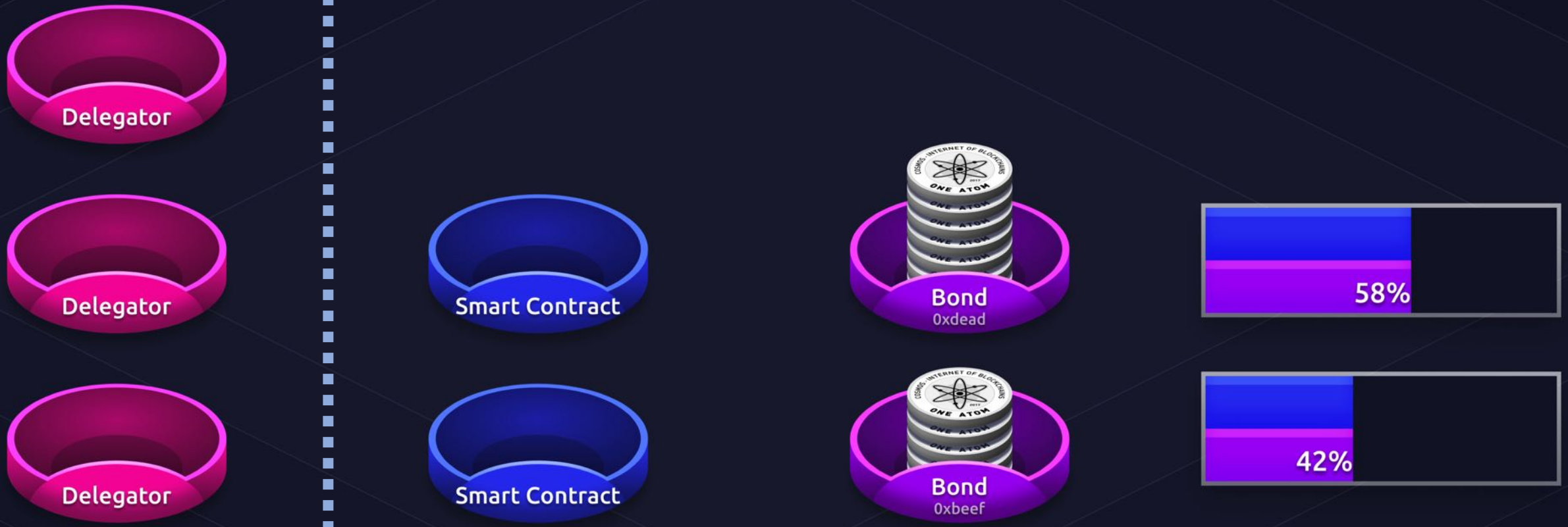
# Out of Protocol



# Out of Protocol



# Out of Protocol



# Delegation in Protocol


Delegator
Validator
Operator
Validator
0x1234
Delegator
Validator
Operator
Validator
0xbeef
Delegator


Delegator


Validator
Operator

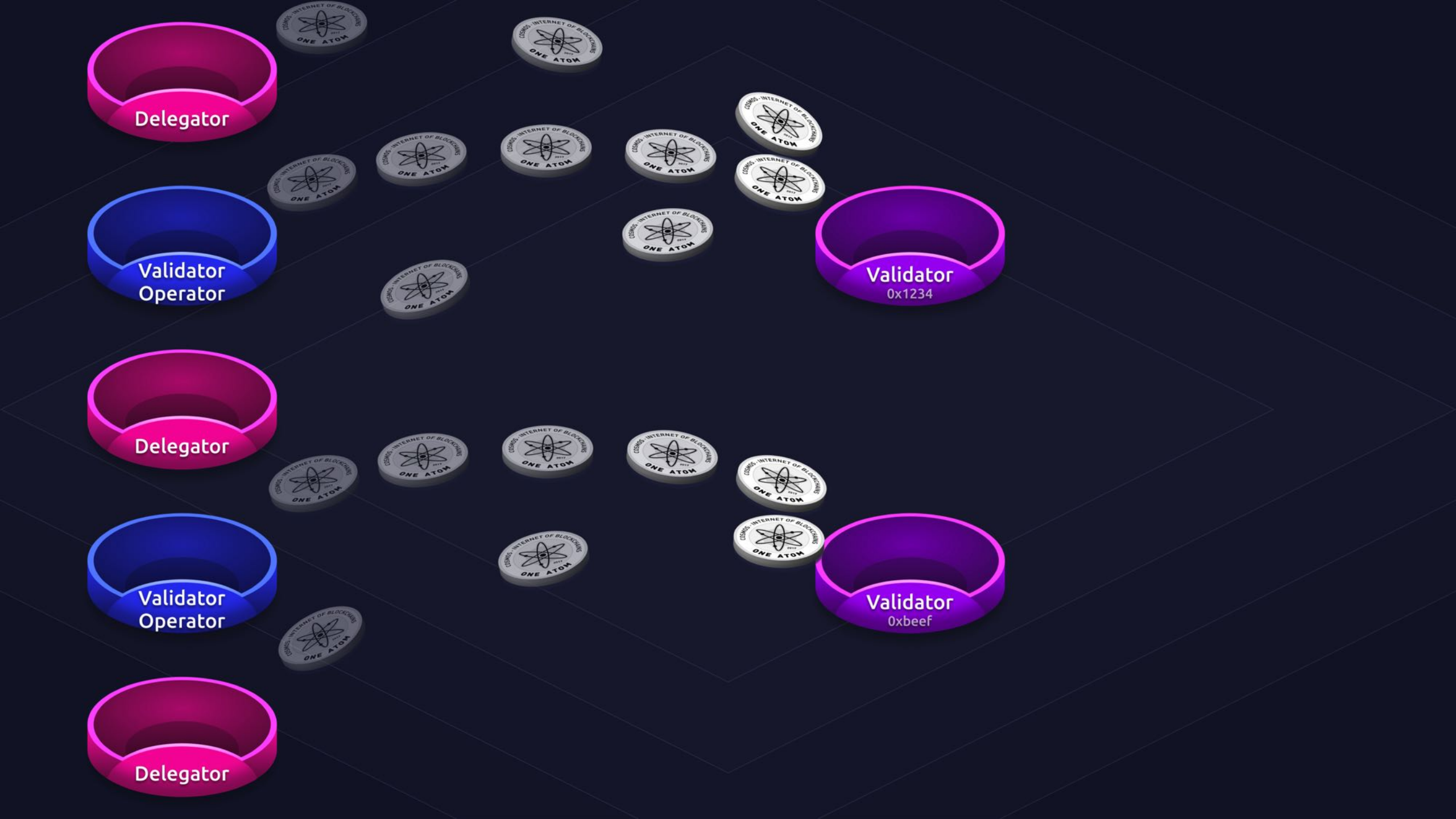

Validator
0x1234


Delegator


Validator
Operator


Validator
0xbeef


Delegator


Delegator
Validator Operator
Validator
0x1234
Delegator
Validator Operator
Validator
0xbeef
Delegator


Delegator
Validator
Operator
Delegator
Validator
Operator
Delegator
Validator
0x1234
Validator
0xbeef


Delegator

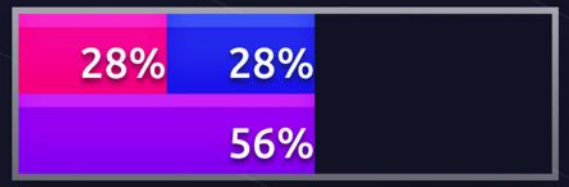

Validator
Operator


Delegator


Validator
Operator


Delegator


Validator
0x1234


28%
28%
56%


Validator
0xbeef


17%
28%
44%


Delegator


Validator
Operator

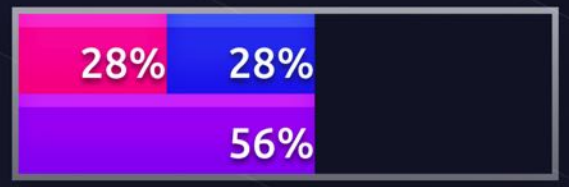

Delegator


Validator
Operator


Delegator

40% SLASH


Validator
0x1234


28%
28%
56%


Validator
0xbeef


17%
28%
44%


Delegator


Validator
Operator


Delegator

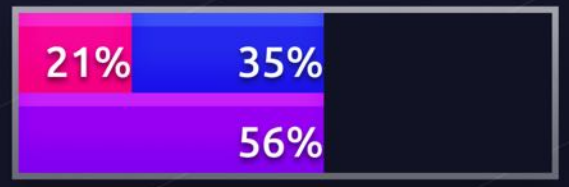

Validator
Operator


Delegator


Validator
0x1234


22%
22%
44%


Validator
0xbeef


21%
35%
56%

# Delegation Criteria

Delegators will choose validators off of criteria such as:

- Validator track record
- Validator’s security setup
- Self-declared, protocol-enforced minimum self-bond
- Commission rate on fees/rewards

# Classical Redelegation


Delegator

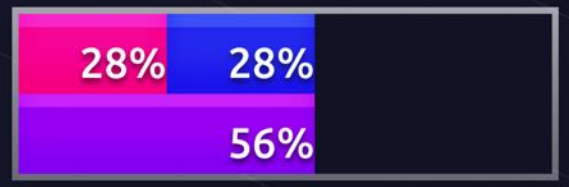

Validator
Operator


Delegator


Validator
Operator


Delegator


Validator
0x1234


28%
28%
56%


Validator
0xbeef


17%
28%
44%


Delegator
Validator Operator
Delegator
Validator Operator
Delegator
Validator
0x1234
Validator
0xbeef
19%
31%
50%
19%
31%
50%


Delegator


Validator
Operator


Delegator


Validator
Operator

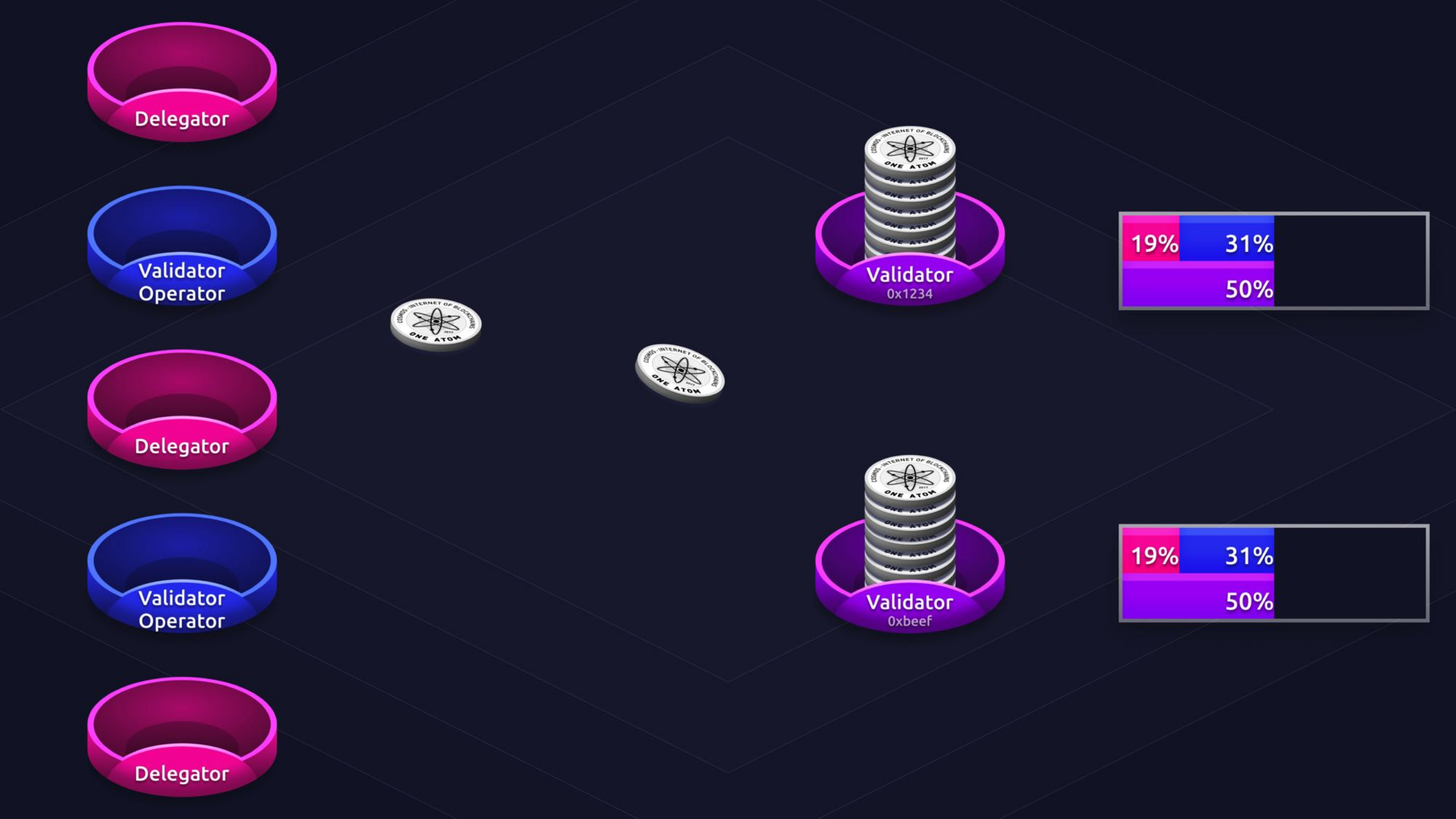

Delegator


Validator
0x1234


19%
31%
50%


Validator
0xbeef


19%
31%
50%


Delegator
Validator Operator
Delegator
Validator Operator
Delegator
Validator
0x1234
19%
31%
50%
Validator
0xbeef
19%
31%
50%


Delegator


Validator
Operator


Delegator

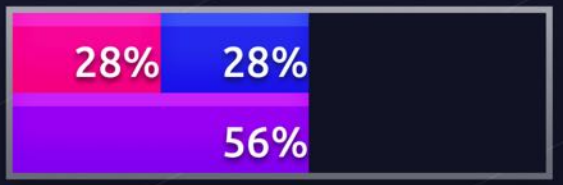

Validator
Operator


Delegator


Validator
0x1234


17%
28%
44%


Validator
0xbeef


28%
28%
56%

# Instant Redelegation


Delegator

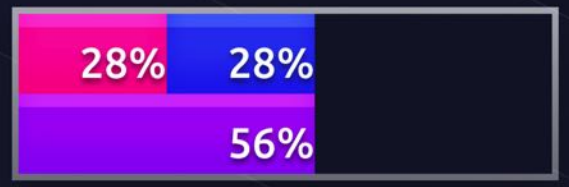

Validator
Operator


Delegator


Validator
Operator

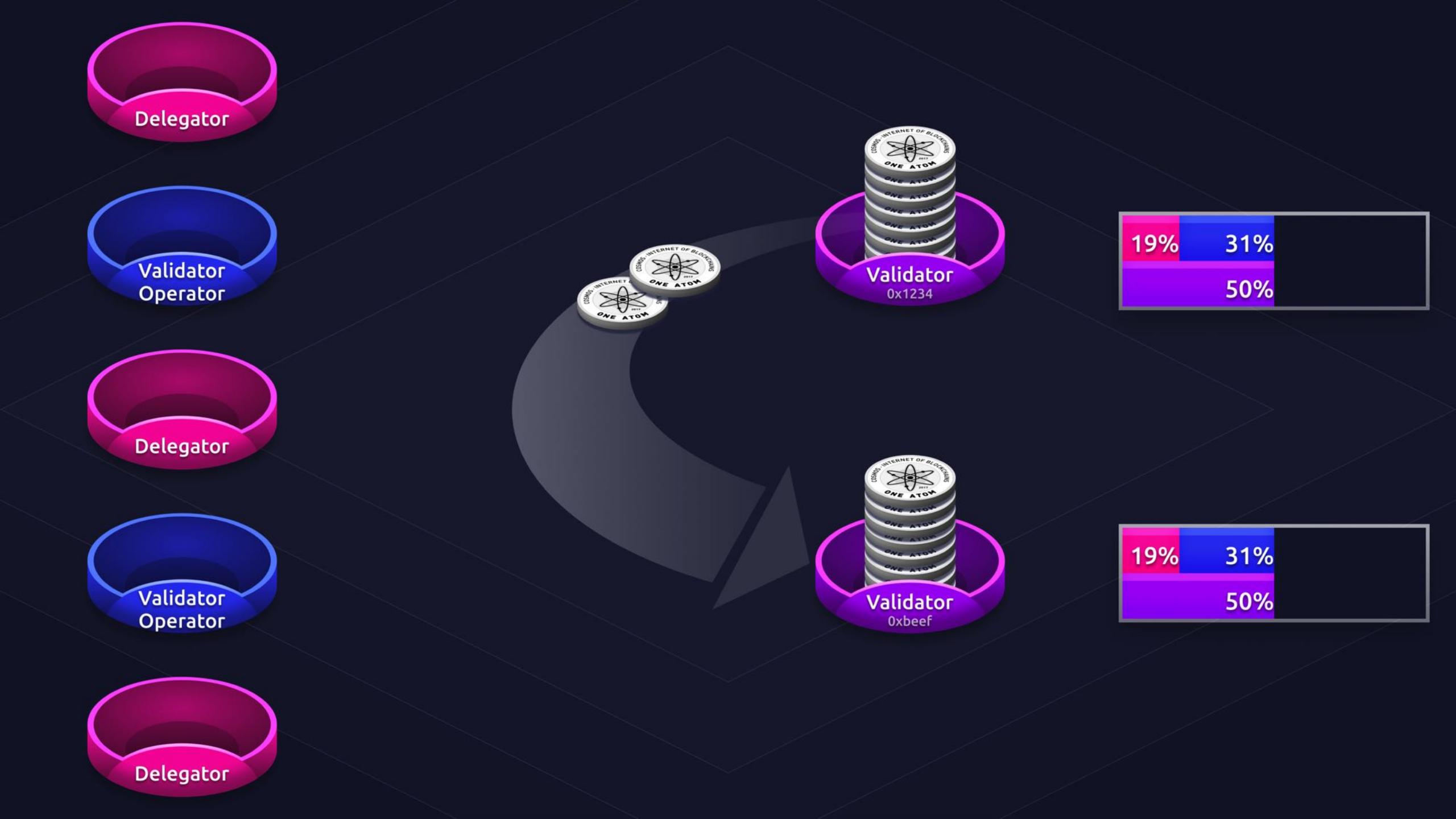

Delegator

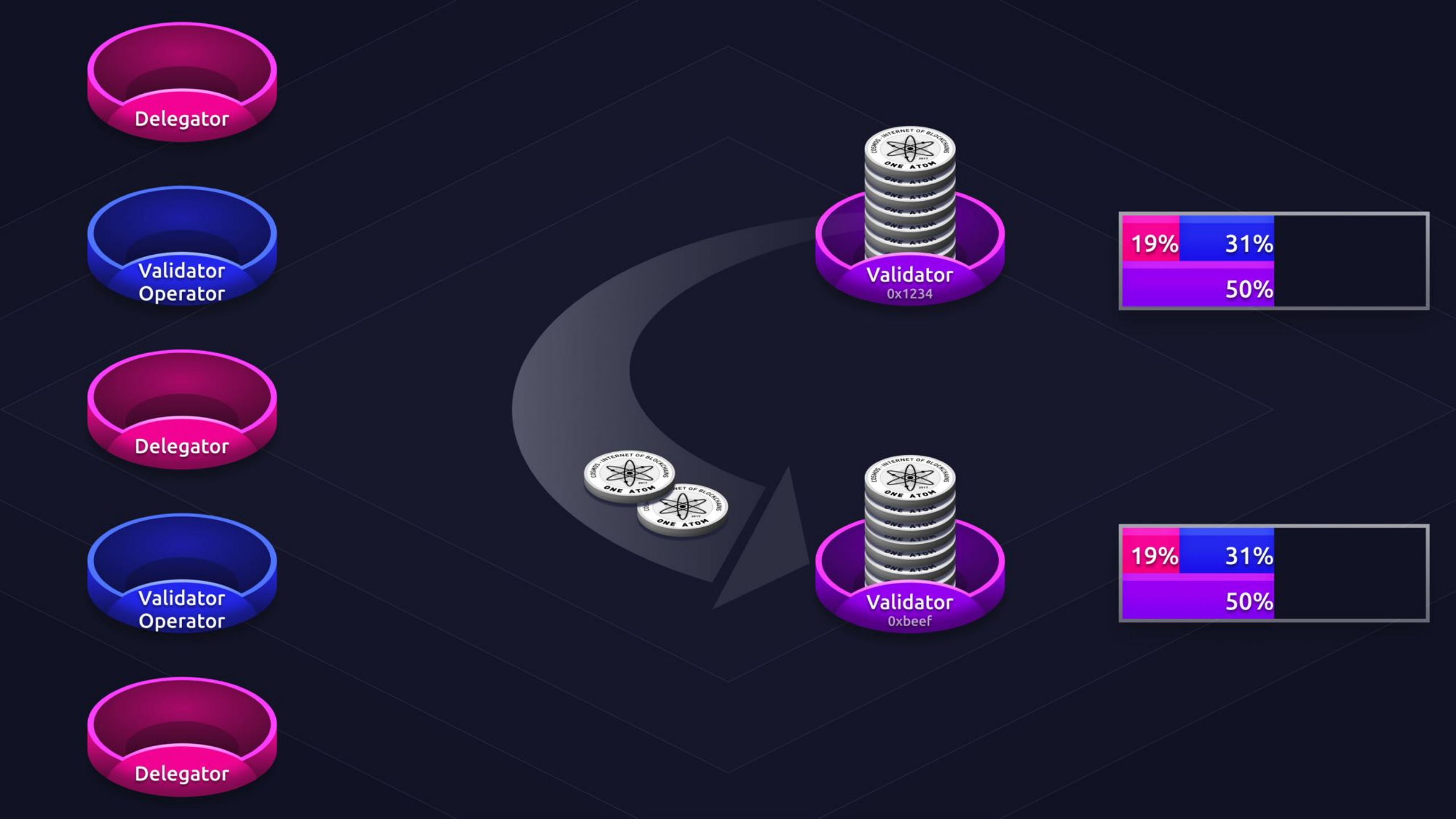

Validator
0x1234


28%
28%
56%


Validator
0xbeef


17%
28%
44%


Delegator
Validator Operator
Delegator
Validator Operator
Delegator
Validator
0x1234
Validator
0xbeef
19%
31%
50%
19%
31%
50%


Delegator
Validator Operator
Delegator
Validator Operator
Delegator
Validator
0x1234
Validator
0xbeef
19%
31%
50%
19%
31%
50%



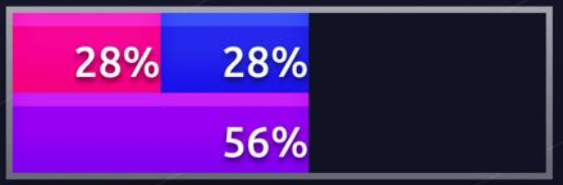



## Unbonding Queue

**Redelegation** - 8:07pm
delegator2 from 0xbeef

**Unbonding** - 8:32pm
delegator1 from 0x1234



Validator A
0x1234

Delegated to
0x1234

Validator B
0xbeef

JAN FEB MAR APR MAY

Validator A
0x1234

Delegated to
0x1234

Validator B
0xbeef

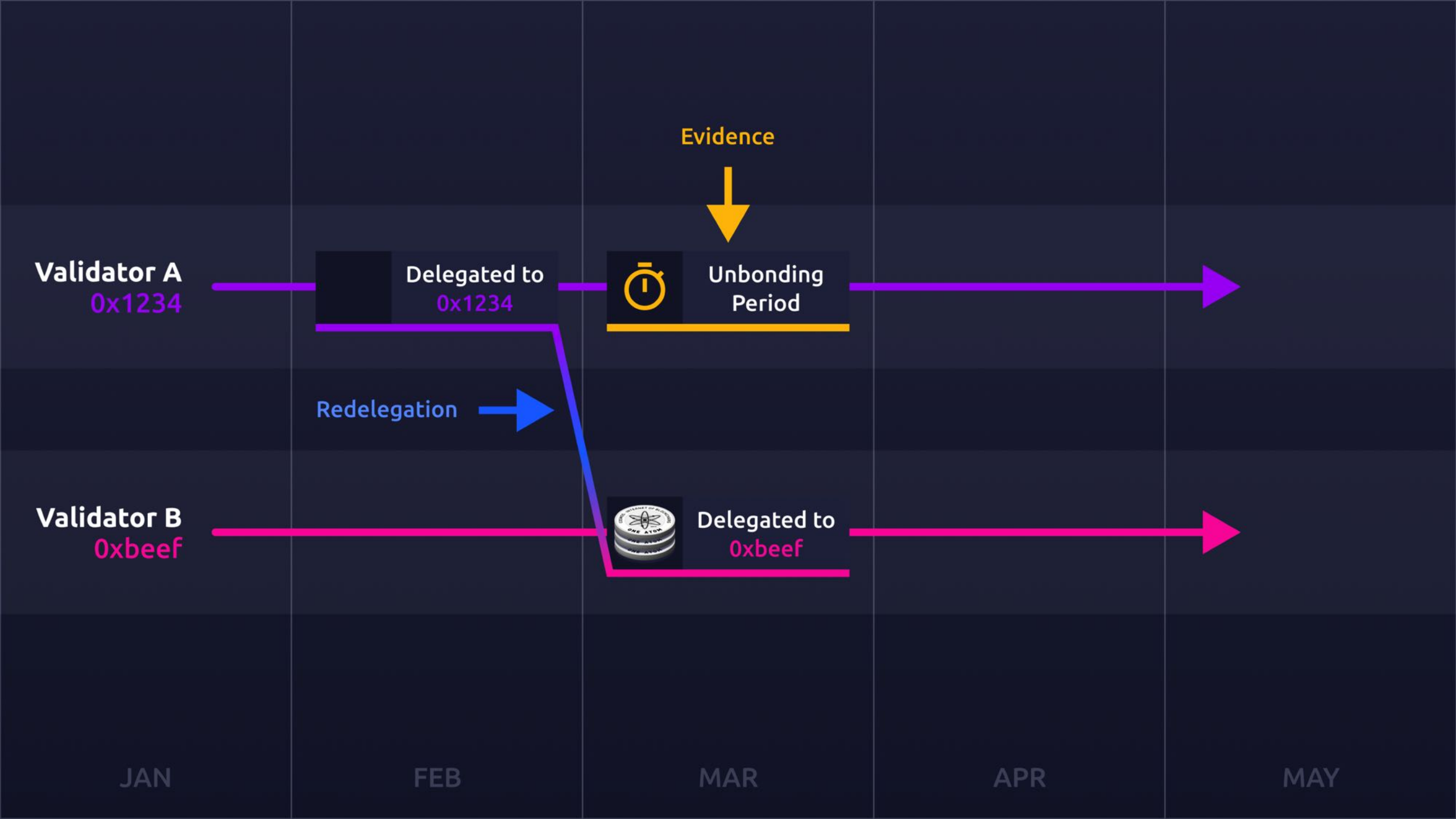
JAN FEB MAR APR MAY


Validator A
0x1234
Delegated to
0x1234
Validator B
0xbeef
JAN
FEB
MAR
APR
MAY


Validator A
0x1234
Delegated to
0x1234
Redelegation
Validator B
0xbeef
JAN
FEB
MAR
APR
MAY

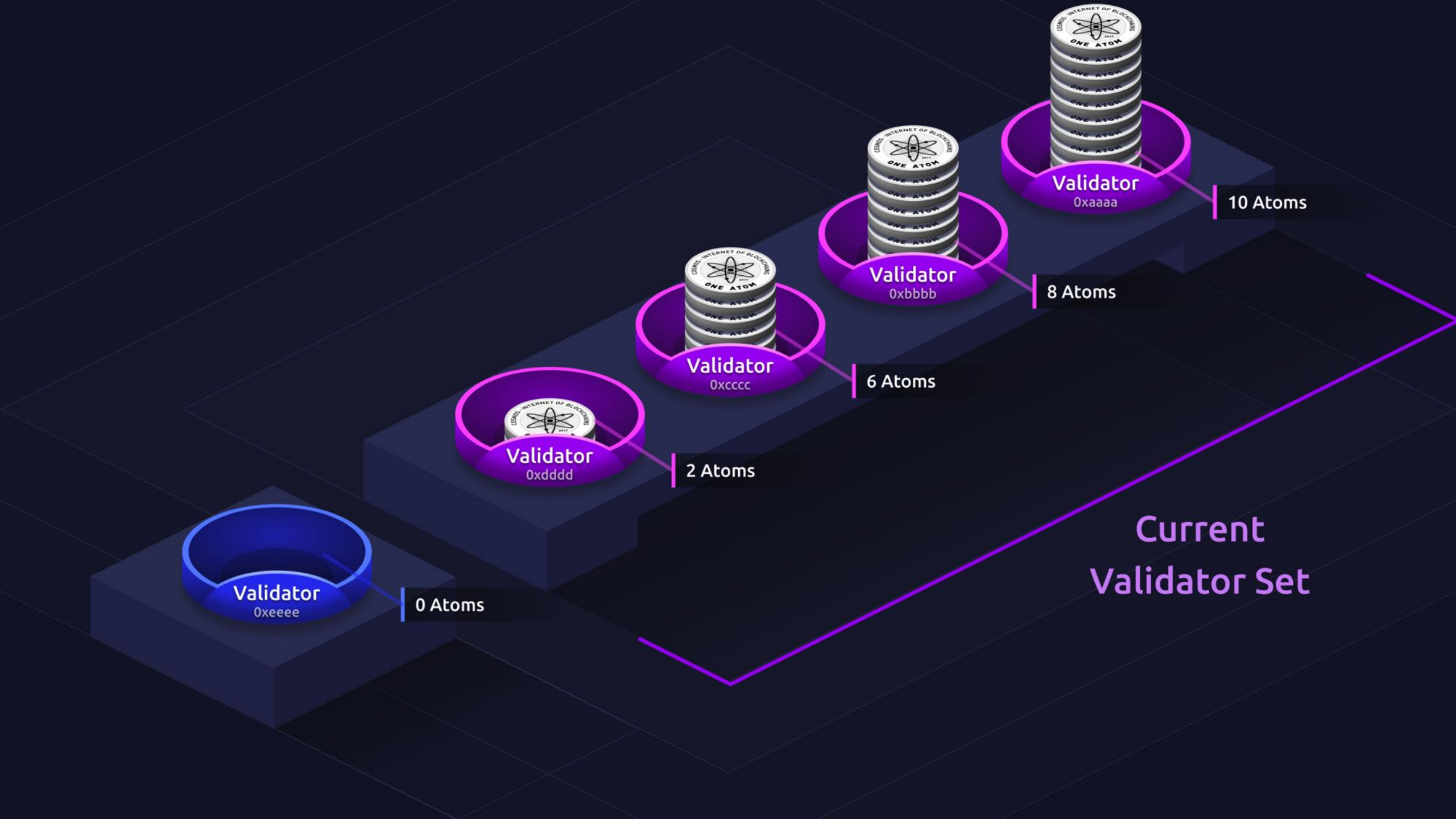

Validator A
0x1234
Delegated to
0x1234
Unbonding
Period
Redelegation
Validator B
0xbeef
Delegated to
0xbeef
JAN
FEB
MAR
APR
MAY

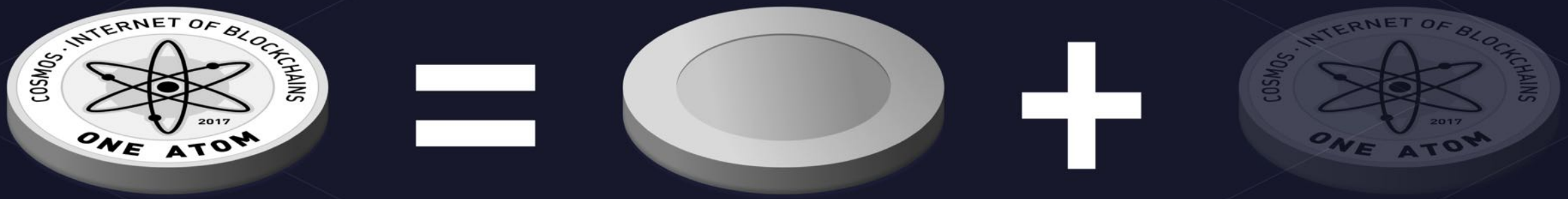

Validator A
0x1234
Delegated to
0x1234
Unbonding
Period
Redelegation
Validator B
0xbeef
Delegated to
0xbeef
JAN
FEB
MAR
APR
MAY


Evidence
Validator A
0x1234
Delegated to
0x1234
Unbonding
Period
Redelegation
Validator B
0xbeef
Delegated to
0xbeef
JAN
FEB
MAR
APR
MAY


Evidence
Validator A
0x1234
Delegated to
0x1234
Unbonding
Period
Redelegation
SLASH
Validator B
0xbeef
Delegated to
0xbeef
JAN
FEB
MAR
APR
MAY

# Delegation Commitments

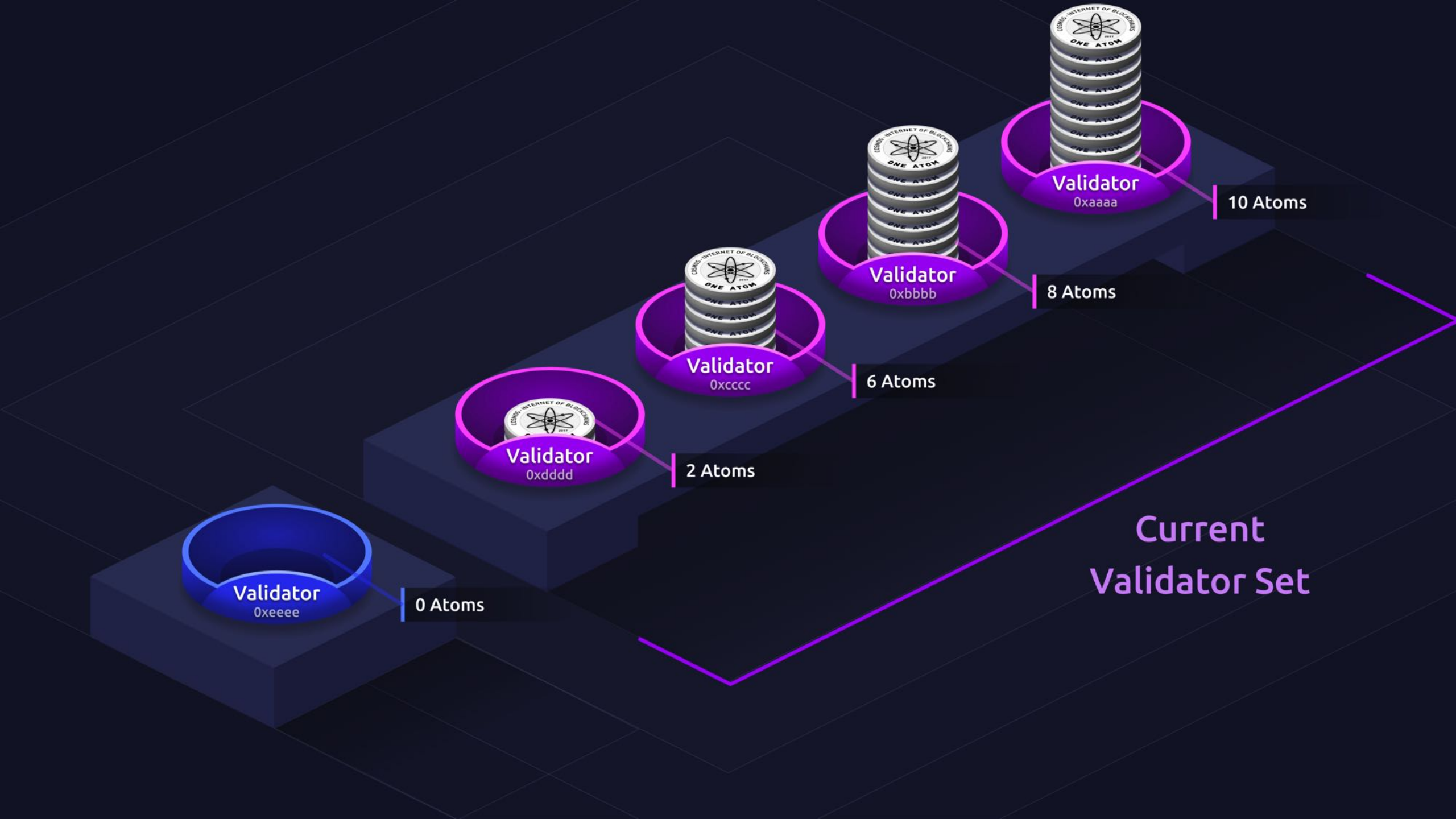

Validator
0xeeee
0 Atoms
Validator
0xdddd
2 Atoms
Validator
0xcccc
6 Atoms
Validator
0xbbbb
8 Atoms
Validator
0xaaaa
10 Atoms
Current
Validator Set

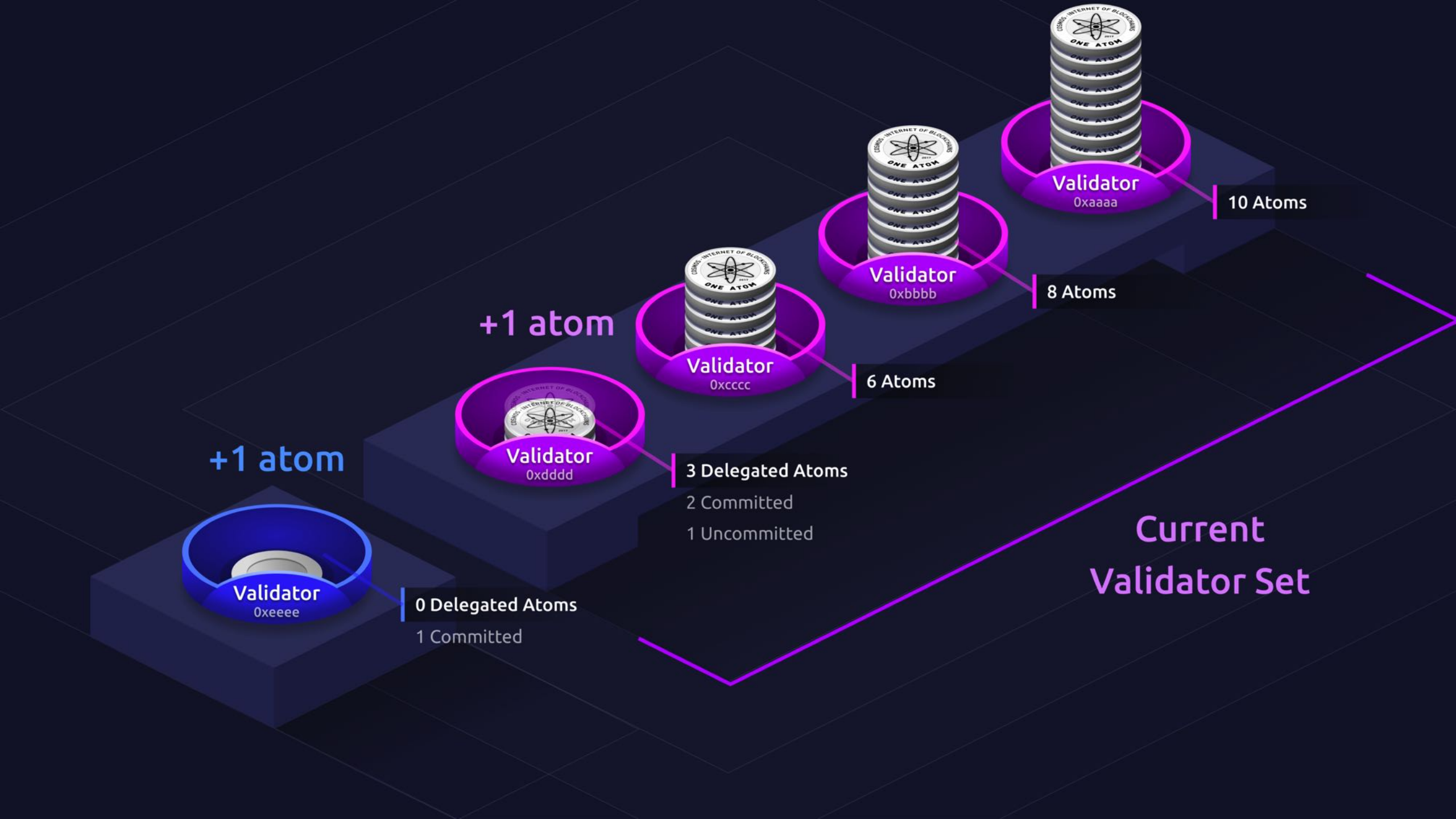


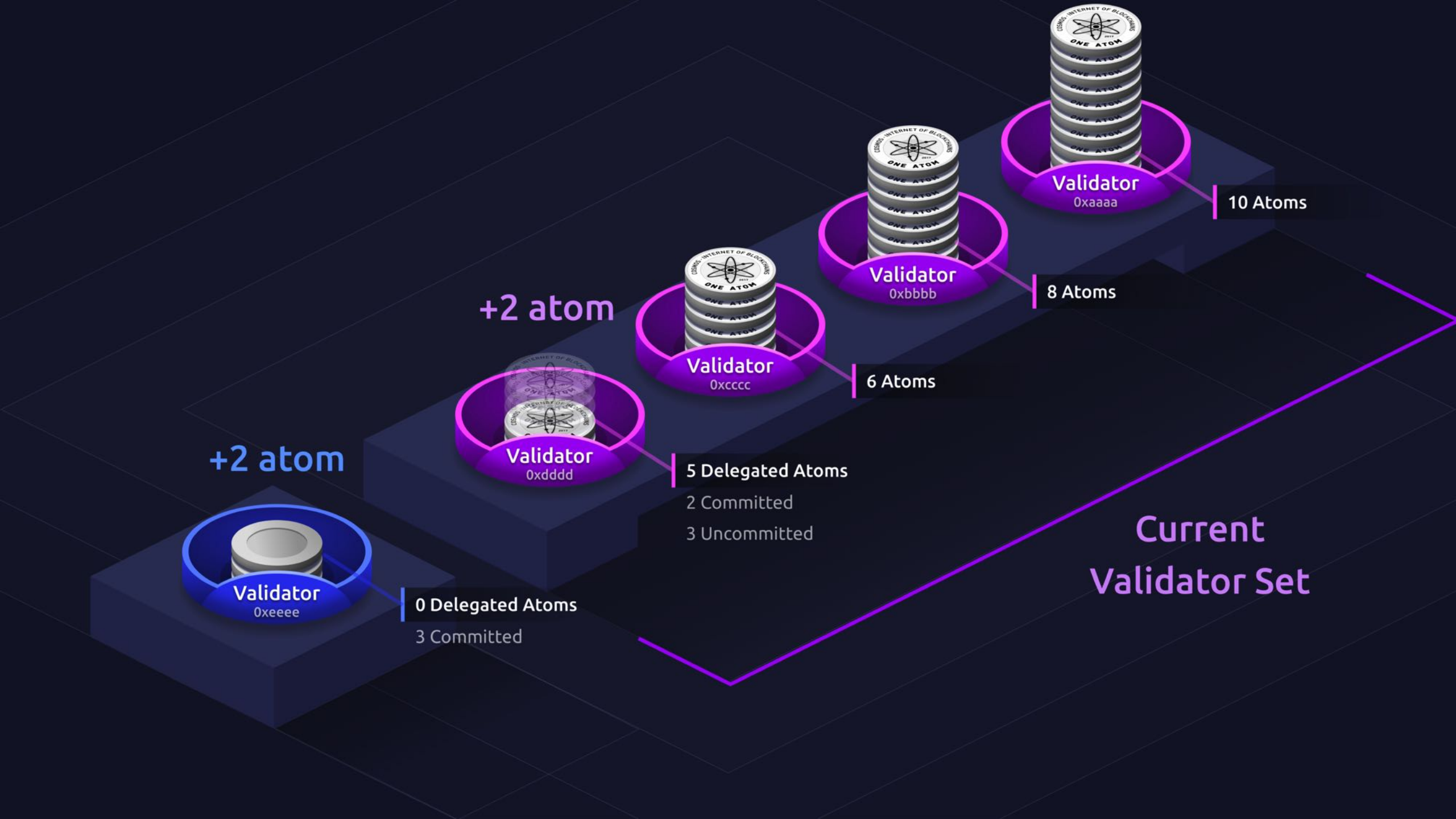

Normal Atom

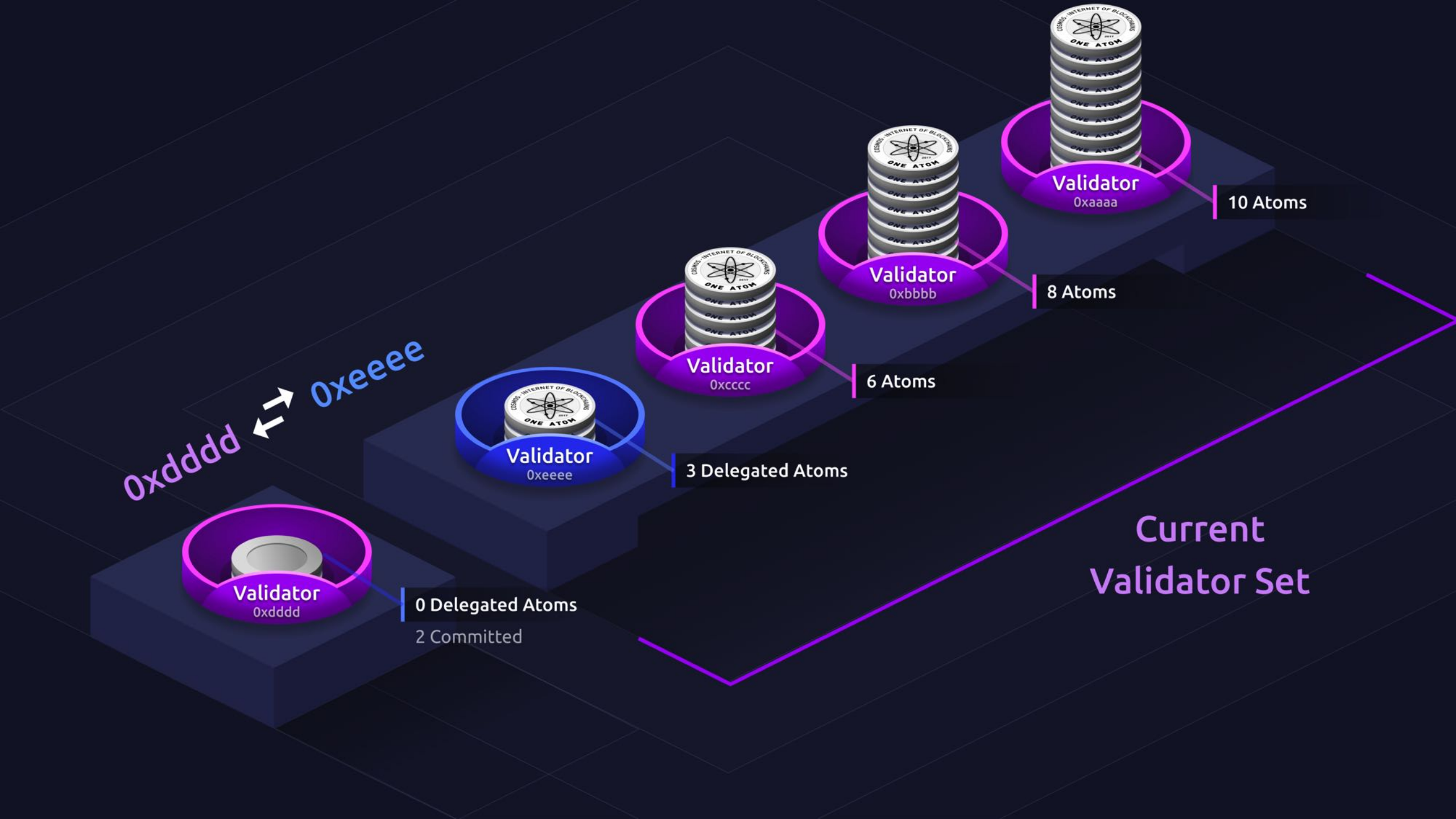
Commitment Token

Ghost Atom


Validator
0xeeee
0 Atoms
Validator
0xdddd
2 Atoms
Validator
0xcccc
6 Atoms
Validator
0xbbbb
8 Atoms
Validator
0xaaaa
10 Atoms
Current
Validator Set


Validator
0xeeee
0 Delegated Atoms
1 Committed
+1 atom
Validator
0xdddd
+1 atom
3 Delegated Atoms
2 Committed
1 Uncommitted
Validator
0xcccc
6 Atoms
Validator
0xbbbb
8 Atoms
Validator
0xaaaa
10 Atoms
Current
Validator Set


Validator
0xaaaa
10 Atoms
Validator
0xbbbb
8 Atoms
+2 atom
Validator
0xcccc
6 Atoms
Validator
0xdddd
5 Delegated Atoms
2 Committed
3 Uncommitted
+2 atom
Validator
0xeeee
0 Delegated Atoms
3 Committed
Current
Validator Set


0xdddd
0xeeee
Validator
0xdddd
0 Delegated Atoms
2 Committed
Validator
0xeeee
3 Delegated Atoms
Validator
0xcccc
6 Atoms
Validator
0xbbbb
8 Atoms
Validator
0xaaaa
10 Atoms
Current
Validator Set

# Incentives

# Rewards

# Staking Token

- Atoms are just a staking token for the Cosmos Hub
- Staking tokens are similar to ASICs
- Capital you need in order to be able to be a validator, and thus earn transaction fees

# Multi Fee Tokens

- Governance can maintains a whitelist of fee tokens
- Each validator maintains a local relative weighting of values of the different whitelisted tokens
- Validators can choose to order transactions based on this ordering.
- Can also require these to be submitted to the chain in order to enforce a global min fee (using the median)

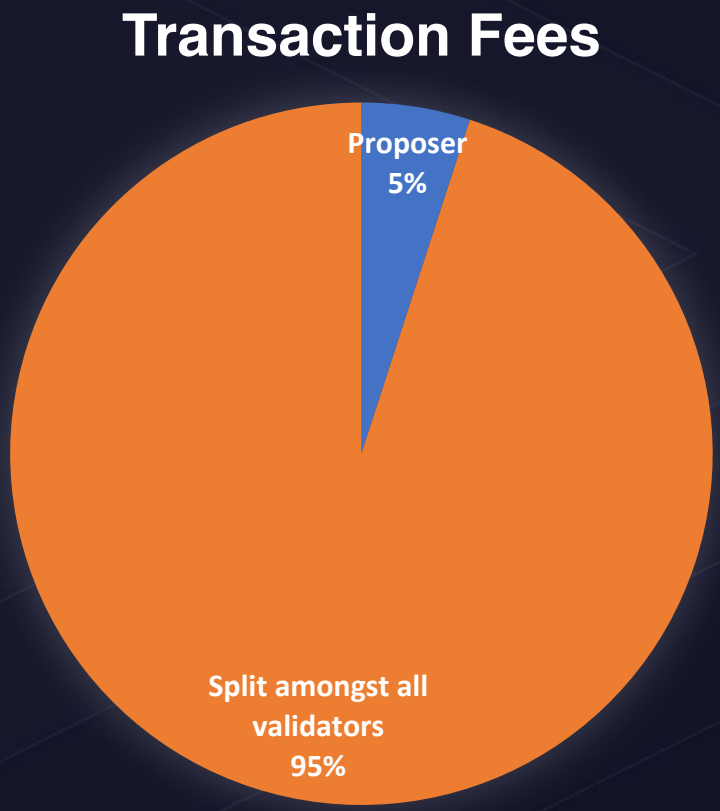
Atom: 5
Photon: 3
BTC: 5000
ETH: 0.2
DAI: 1

# Block Rewards

- Inflation schedule is designed to encourage staking (the lower the percentage of staked atoms, the higher the inflation rate)
- Block rewards split amongst all staked validators
- Block rewards start off unbonded

# Proposer Reward

- Majority of collected fees gets split amongst the validators
- Proposer gets a special dedicated percentage in order to incentivize them to not produce empty blocks



# Proposer Reward

$$P = 0.01 + 0.02 * S + 0.02\ (0.9^R)$$

$P$ = Proposers dedicated percentage

$S$ = Percentage of stake whose precommits from previous block were included in the proposal

$R$ = Round number that a proposal was first proposed

# Distribution

- Passive Accounting to avoid iterating over the entire set of stakers every block
- Transaction Fees and block rewards are added to a pool
- Shares in the pool are distributed to validators, who themselves have shares distributed to delegators
- Validators can charge commission rate on fees/rewards

# Punishments

# Liveness Slashing

= Signed

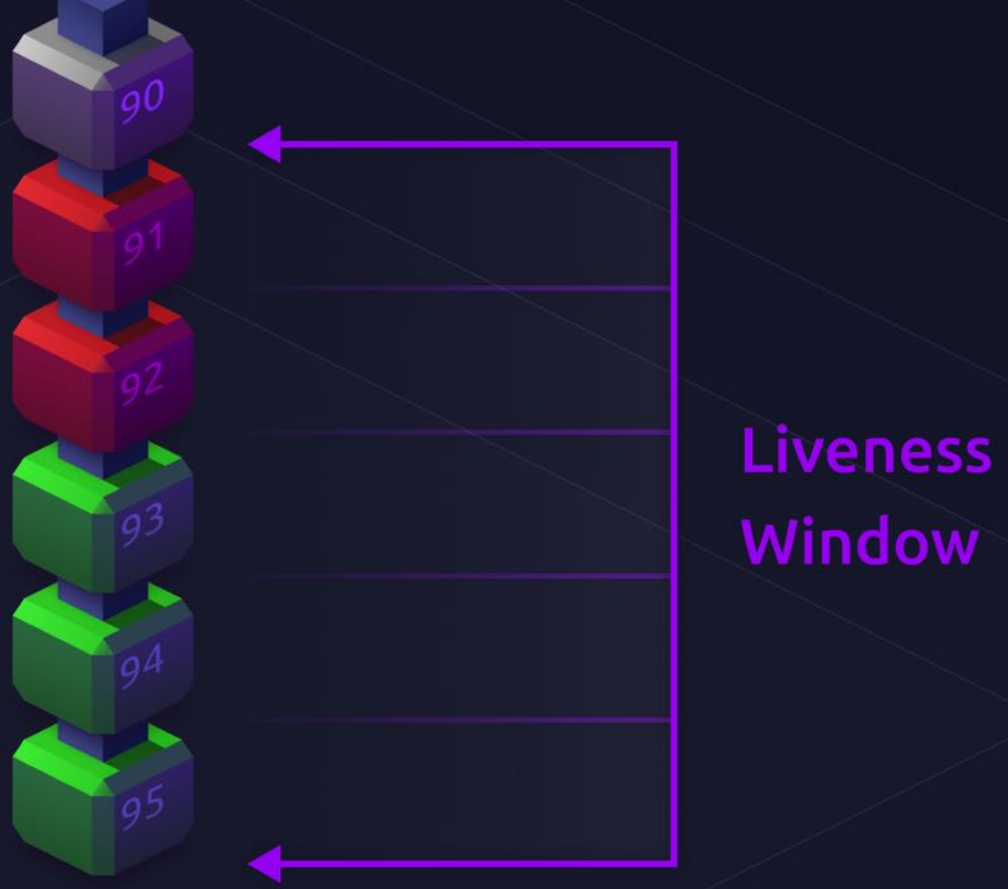
= Unsigned

= Signed

= Unsigned

= Signed

= Unsigned



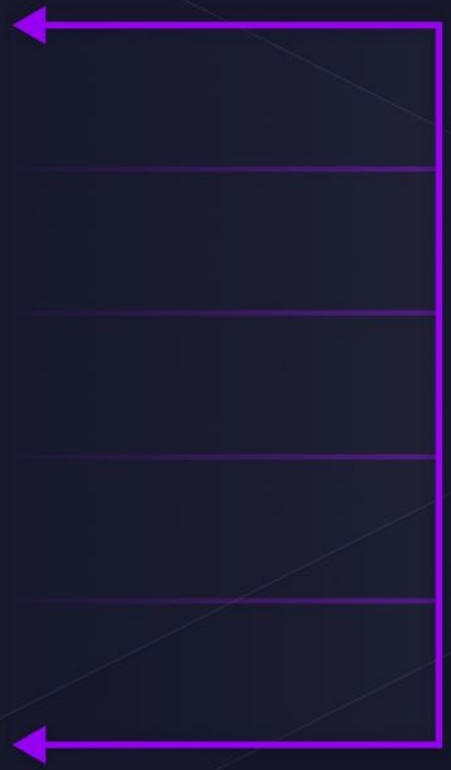
= Signed

= Unsigned


Liveness Window

= Signed

= Unsigned

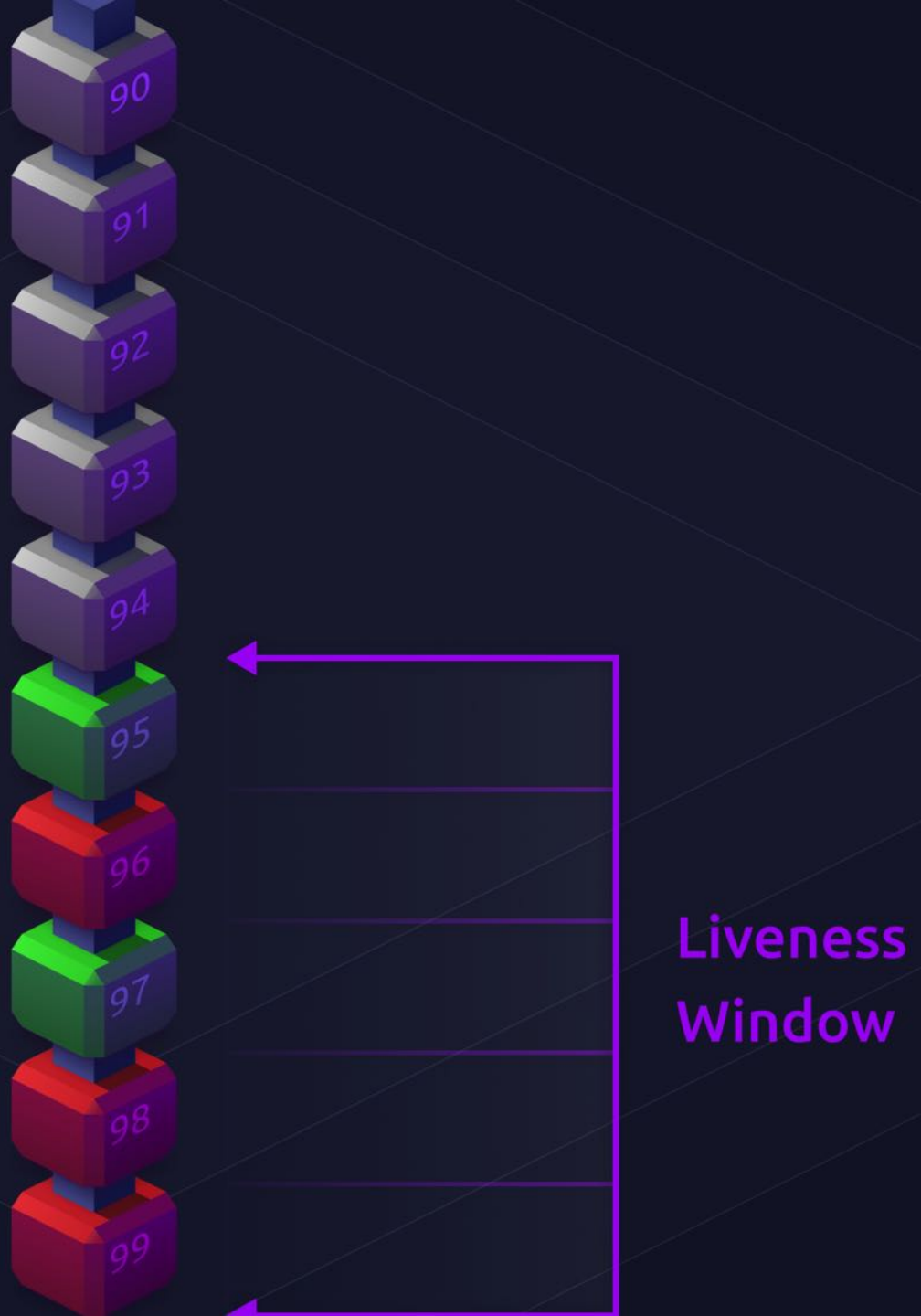
Liveness
Window

= Signed

= Unsigned

= Signed

= Unsigned



= Signed

= Unsigned

LIVENESS SLASH


Liveness Window

# Liveness Slashing

- Validator gets a slight slash and is automatically put in an jail period of 2 days
- After a jail period (2 days) the validator can choose to rebond
- Unless delegators redelegated or unbonded, they will be delegated to the validator when he gets out of jail
- The jail period time gets credited to the unbonding period, for both validator operators and delegators

# Byzantine Slashing

# Consensus Fault Slashing

- The consensus engine tracks and generates evidence for BFT faults
  - Double signing on a block
  - Breaking a Tendermint locking condition
  - Signing a block while you're in the unbonding period

- There can be a delay between the time an infraction occurs and the time that evidence is found

# Consensus Fault Slashing

- At time of evidence, the validator is slashed and killed.
- A killed validator has all of his delegators unbonded and the validator cannot revive itself
- Only the worst slash infraction is tracked
  - Compromised key can’t be used to slash 100% of a validator’s funds
  - Prevents evidence DoS attacks


Validator A
Validating
Evidence A - 30%
Validator Killed
Total Slash: 30%
WEEK 1
WEEK 2
WEEK 3
WEEK 4
WEEK 5


Total Slash: 30%

WEEK 1 WEEK 2 WEEK 3 WEEK 4 WEEK 5


**Total Slash: 40%**

WEEK 1 WEEK 2 WEEK 3 WEEK 4 WEEK 5


CAPPED

**Total Slash: 40%**

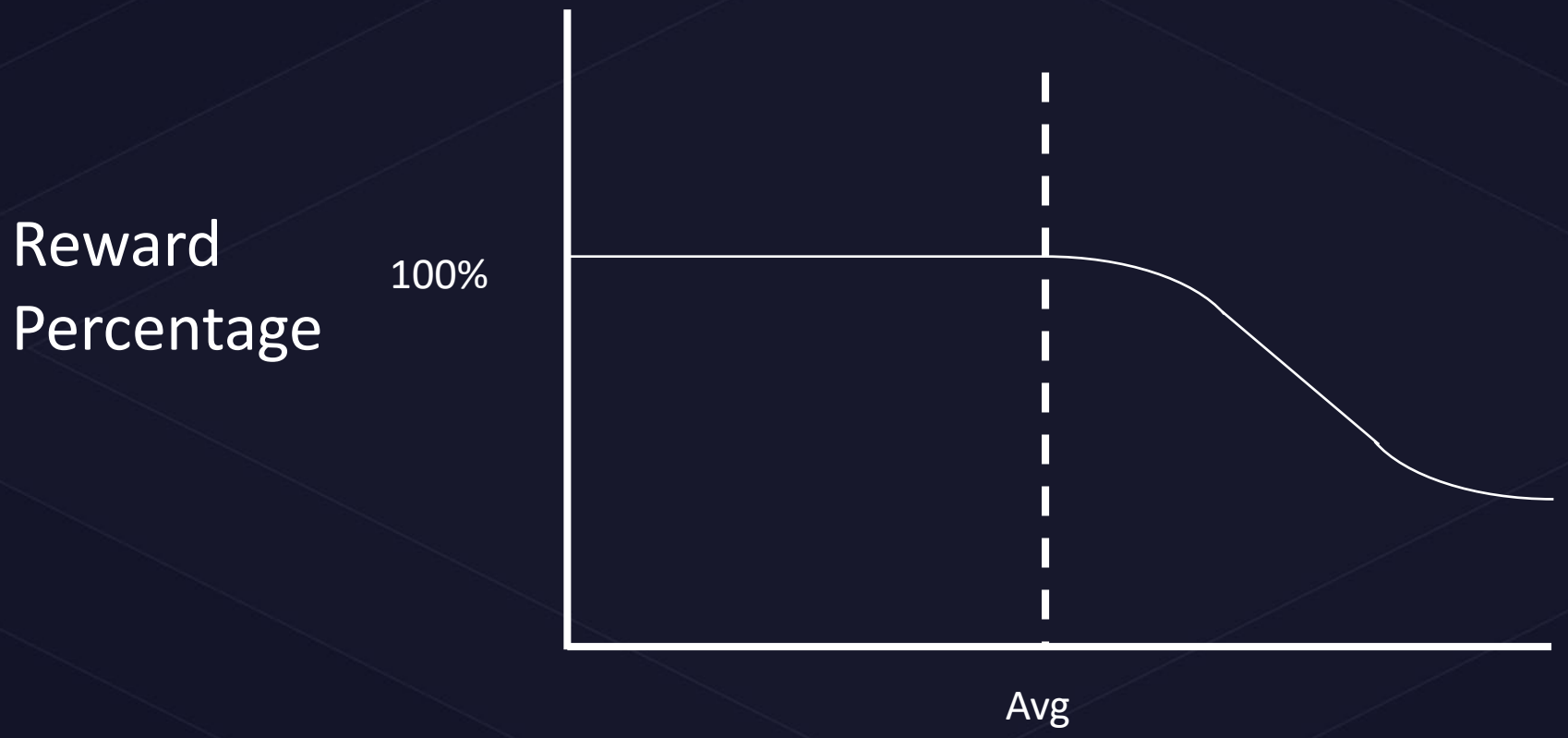
WEEK 1 WEEK 2 WEEK 3 WEEK 4 WEEK 5

# Incentivizing Decentralization


Delegation
Self-Bond
Validator
0x1234
Validator
0xdead
Validator
0xbeef
5 atoms
7 atoms
15 atoms


Delegation
Self-Bond
Validator
0x1234
Validator
0xdead
Validator
0xbeef
3:2
4:3
12:3


Delegation
Self-Bond
Validator
0x1234
Validator
0xdead
Validator
0xbeef
1.5
1.3333
4


Reward
Percentage
100%
Avg
Self Bond Ratio

# Further Work

# Help us!

- Attack and improve our economic and theoretical models
- Properly parameterize constants
- Help simulate real world attacks in Game of Stakes
- Test and contribute to the open source codebase
- Come up with a name for Cosmos Proof of Stake


CØSMOS
GAME OF STAKES
FOR THE
VALIDATOR CANDIDATES
BOB

# Help us!

- Attack and improve our economic and theoretical models
- Properly parameterize constants
- Help simulate real world attacks in Game of Stakes
- Test and contribute to the open source codebase
- Come up with a name for Cosmos Proof of Stake

cosmos / cosmos-sdk

Unwatch 96 | Star 614 | Fork 206

Code | Issues 310 | Pull requests 21 | Projects 5 | Wiki | Insights

Branch: develop — cosmos-sdk / x / stake / — Create new file | Upload files | Find file | History

**sunnya97** and **cwgoes** Merge PR #2405: Unbonding and Redelegations Queue — Latest commit cd21427 6 hours ago

| | | |
|---|---|---|
| .. | | |
| client | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |
| keeper | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |
| querier | Merge PR #2394: Split up UpdateValidator into distinct state transiti... | 5 days ago |
| simulation | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |
| tags | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |
| types | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |
| app_test.go | Merge PR #2365: Validator Commission Model | 14 days ago |
| genesis.go | Merge PR #2450: Add ValidateGenesis to staking, add more tests | 7 hours ago |
| genesis_test.go | Merge PR #2450: Add ValidateGenesis to staking, add more tests | 7 hours ago |
| handler.go | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |
| handler_test.go | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |
| stake.go | Merge PR #2405: Unbonding and Redelegations Queue | 6 hours ago |

# Help us!

- Attack and improve our economic and theoretical models
- Properly parameterize constants
- Help simulate real world attacks in Game of Stakes
- Test and contribute to the open source codebase
- Come up with a name for Cosmos Proof of Stake

**Ethan Buchman**
@buchmanster

Following

Officially advocating for @cosmos #proofofstake to be called BDSM-PoS. It's "Bonding, Delegation, Slashing, Merkle Proof of Stake". Because, as @juddkeppel notes, "everyone loves a good slashing!" #blockchain

11:15 AM - 29 Aug 2018

**24** Retweets **85** Likes

11 24 85

# Help us!

- Attack and improve our economic and theoretical models
- Properly parameterize constants
- Help simulate real world attacks in Game of Stakes
- Test and contribute to the open source codebase
- Come up with a name for Cosmos Proof of Stake

# Thank You!

@cosmos

@sunnya97