Fundamentals of the Stellar Consensus Protocol

Alexander Steinhoff

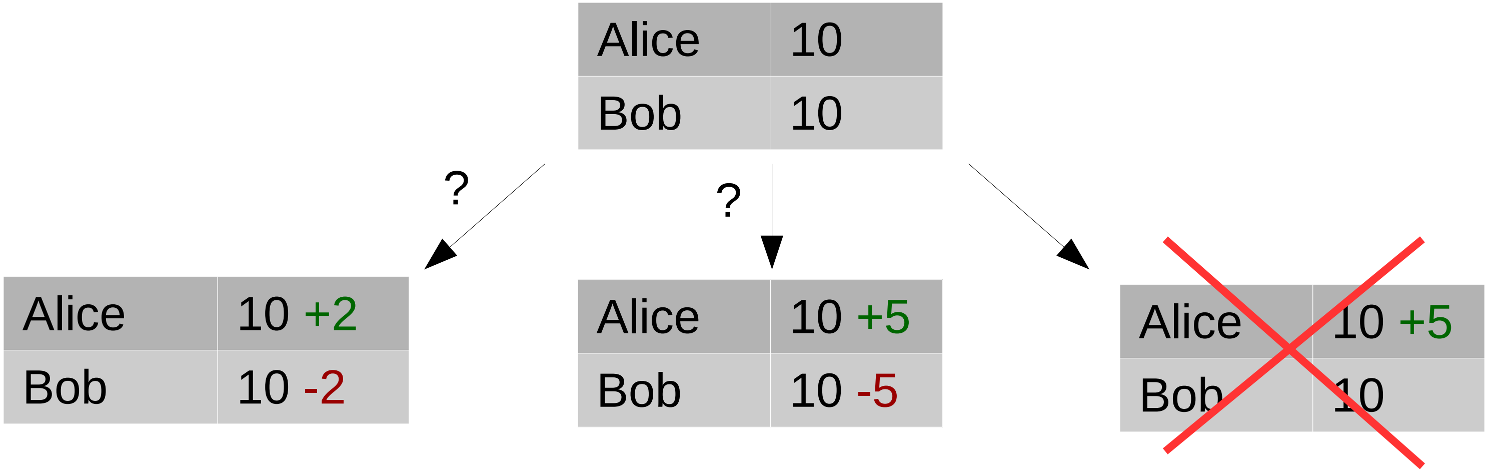
Stellar-Meetup, Munich, March 26, 2019

Agenda

- Blockchain Consensus
- Byzantine Agreement
- Federated Byzantine Agreement
  - Quorums and quorum slices
  - Federated Voting
- Quorum slice selection
  - Theory
  - Practice
- Conclusion

The Blockchain-Consensus Problem

- Collectively decide on the next (valid) state of a distributed database/ledger
- No designated leader
- Participants might not be trustworthy or even unknown



Alice	10
Bob	10

Alice	10 +2
Bob	10 -2

Alice	10 +5
Bob	10 -5

Alice	10 +5
Bob	10

Distributed Consensus Approaches

- **Proof of Work** (Bitcoin, Ethereum, Monero, ...)
  - basically a lottery where tickets are bought with hash power
- **Proof of Stake** (NXT, maybe Ethereum in the future)
  - rich people have more lottery tickets
- **Delegated Proof of Stake** (EOS, Bitshares, ...)
  - rich people vote leaders
- **Byzantine Agreement** (Ripple)
  - negotiate among closed set of participants
- **Federated Byzantine Agreement (FBA)** (Stellar)

Byzantine Agreement

- Closed system of nodes
- Robustness against „Byzantine failure“ of a subset of nodes
- Typically $N = 3f + 1$ where N is the number of nodes and f the number of failures
- e.g. 16 nodes and 5 may fail

Safety and Liveness

Liveness

There are no deadlocks

Safety

No two honest nodes reach different conclusions about the new state

Maximizing either property conflicts with the other

Federated Byzantine Agreement

- The attempt to „open up“ Byzantine agreement
- No fixed set of participants
- No fixed quorums: Each nodes decides for itself which other nodes to trust

Quorums Slices and Quorums

Quorum

Informally: A set of nodes that can agree on the outcome of a vote

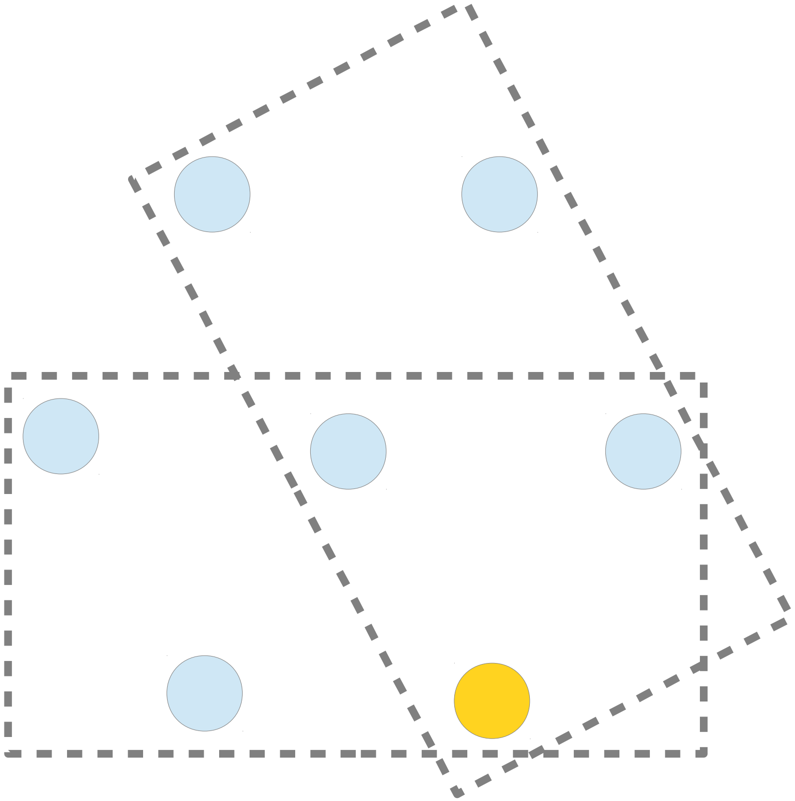
Quorum slice

A set of nodes that one node thinks should be part of the quorum.

Several alternative slices per node.

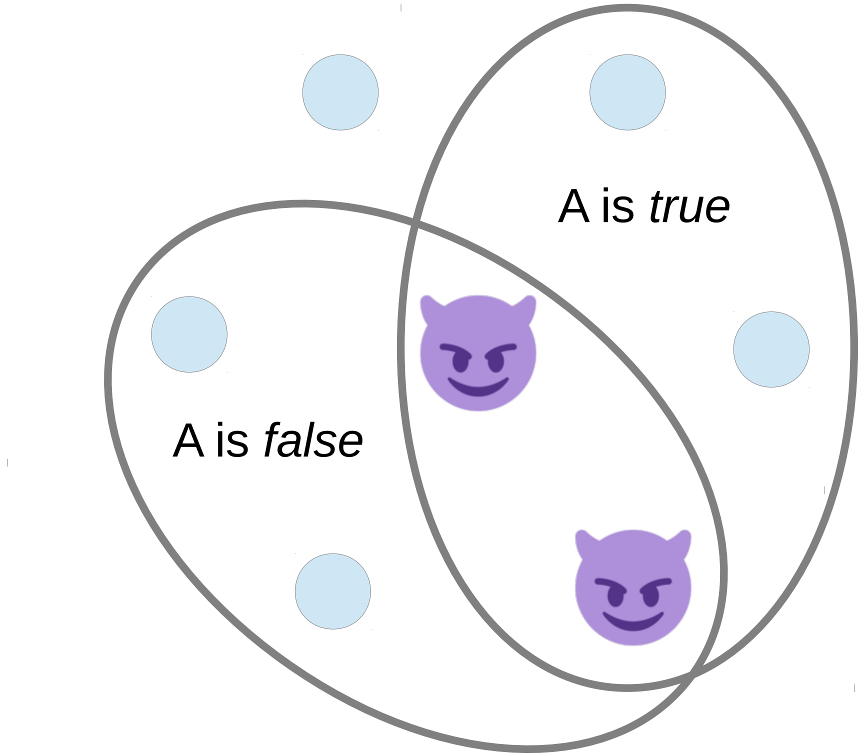
Classic Byzantine Consensus Quorums

Implicitly defined by quorum size of 2f + 1



2 example quorum slices of the yellow node for N = 7

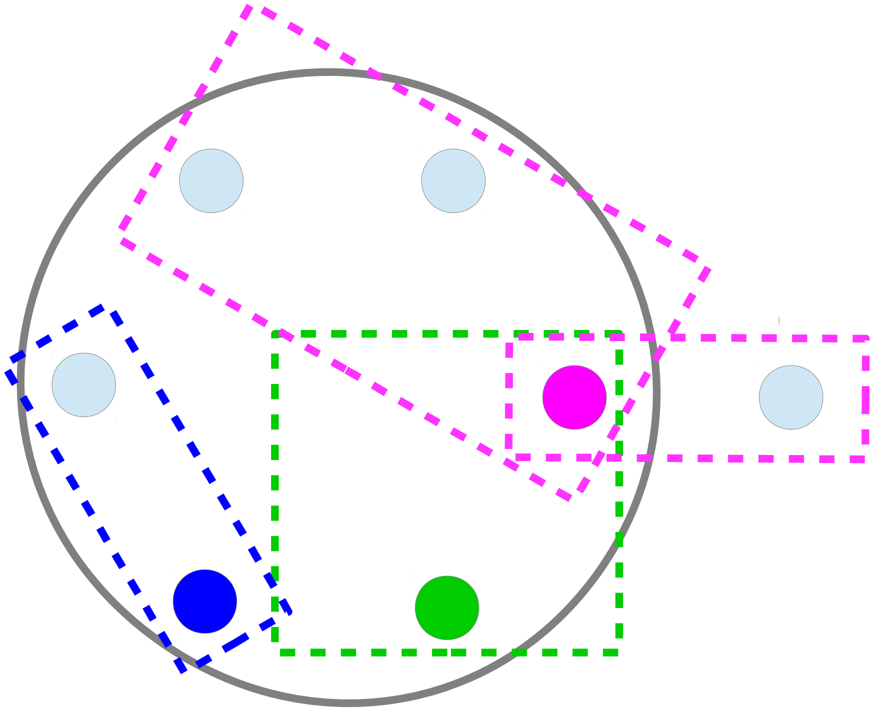
Byzantine Consensus Failure Example



Safety is lost if quorum slices are too small

Quorums in FBA

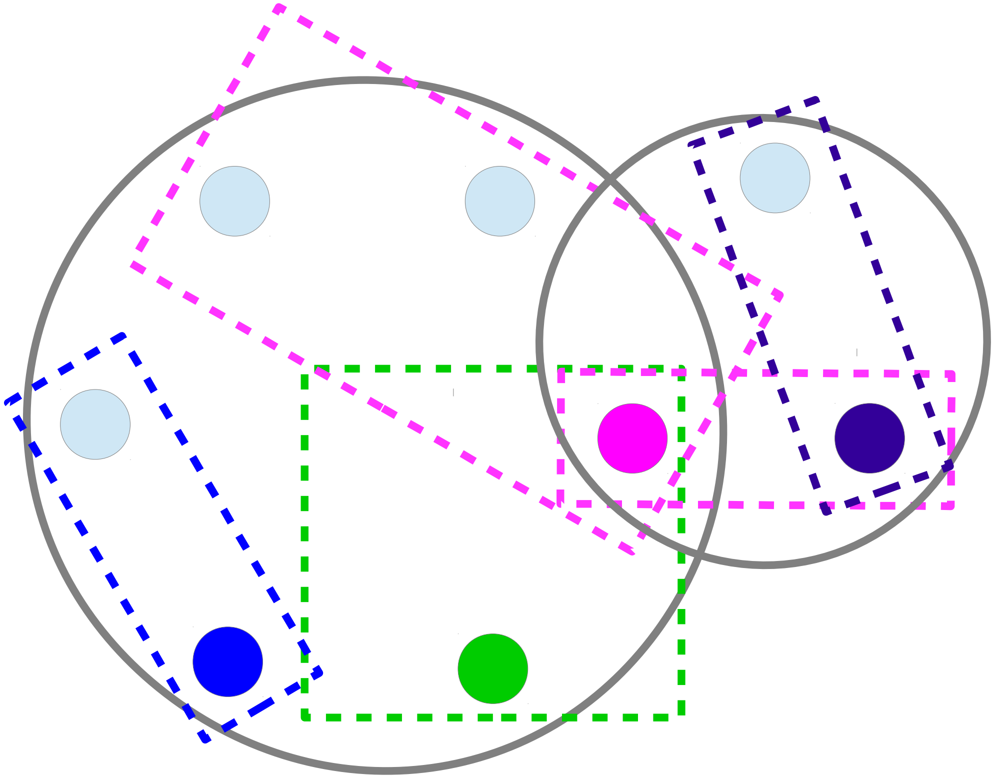
Definition: A set of nodes *U* is a quorum if for each node a complete slice is contained in *U*



Only part of the slices are shown

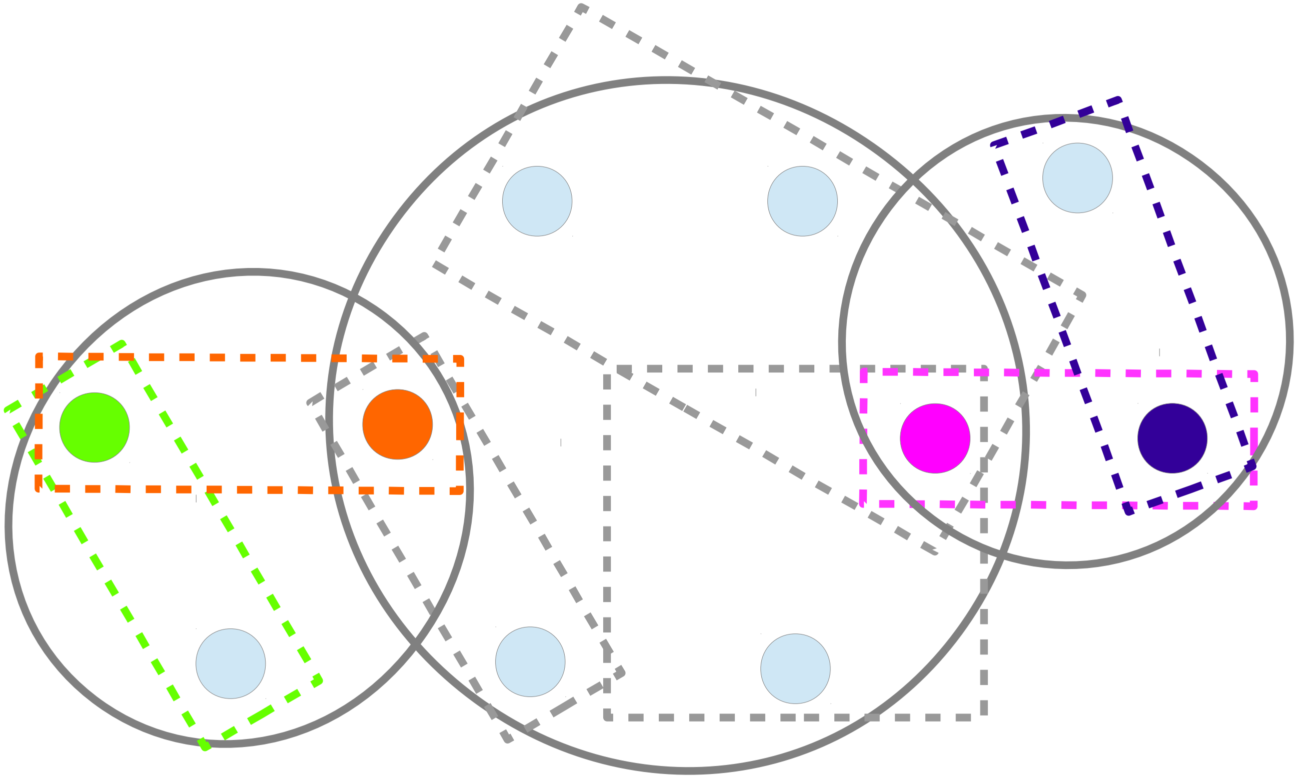
Quorum intersection (1)

All pairs of quorums must share at least one node



Quorum intersection (2)

Safety is lost if there are disjoint quorums



Federated voting

Three stage process

- Voting
- Acceptance
- Confirmation

Voting

Nodes may cast a vote to assert that they deem a statement *a* true.

A node may not contradict itself.

A statement *a* is **ratified** (not accepted or confirmed!) by a quorum if all nodes in the quorum vote for it.

Acceptance

A node accepts statement *a* if it has not accepted a contradicting statement and either

1) there exists a quorum of nodes either having voted for *a* or accepting it, or

2) in all of its quorum slices there is a node accepting *a*

Confirmation

A node confirms *a* if all members of a quorum accept it. One can also say it ratifies the statement *accept(a).*

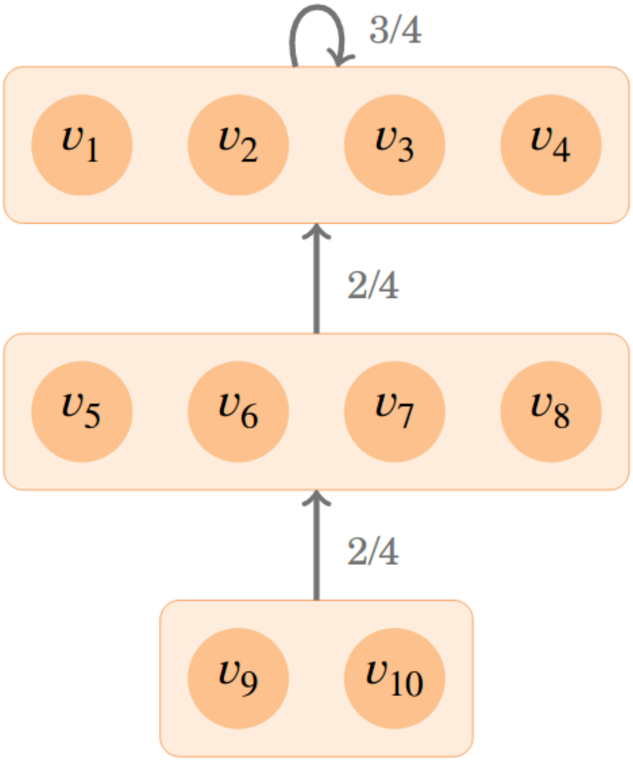
The node can from now on assume *a* is true.

Selecting quorum slices

- Nodes are responsible for selecting slices
- Resilience of the system depends on it
- Tradeoff between safety and liveness
- It might be sensible to include anchor nodes

Theoretic example (1)

An example from the whitepaper:



Top tier: slice is 3 out of $\{v_1, v_2, v_3, v_4\}$, including self

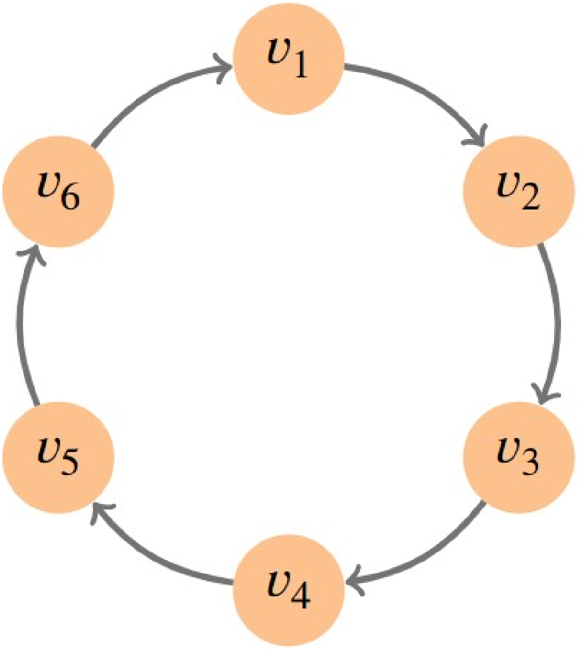
Middle tier: slice is self + any 2 top tier nodes

Leaf tier: slice is self + any 2 middle tier nodes

Fig. 3. Tiered quorum structure example

Theoretic example (2)

An unrealistic but possible example:

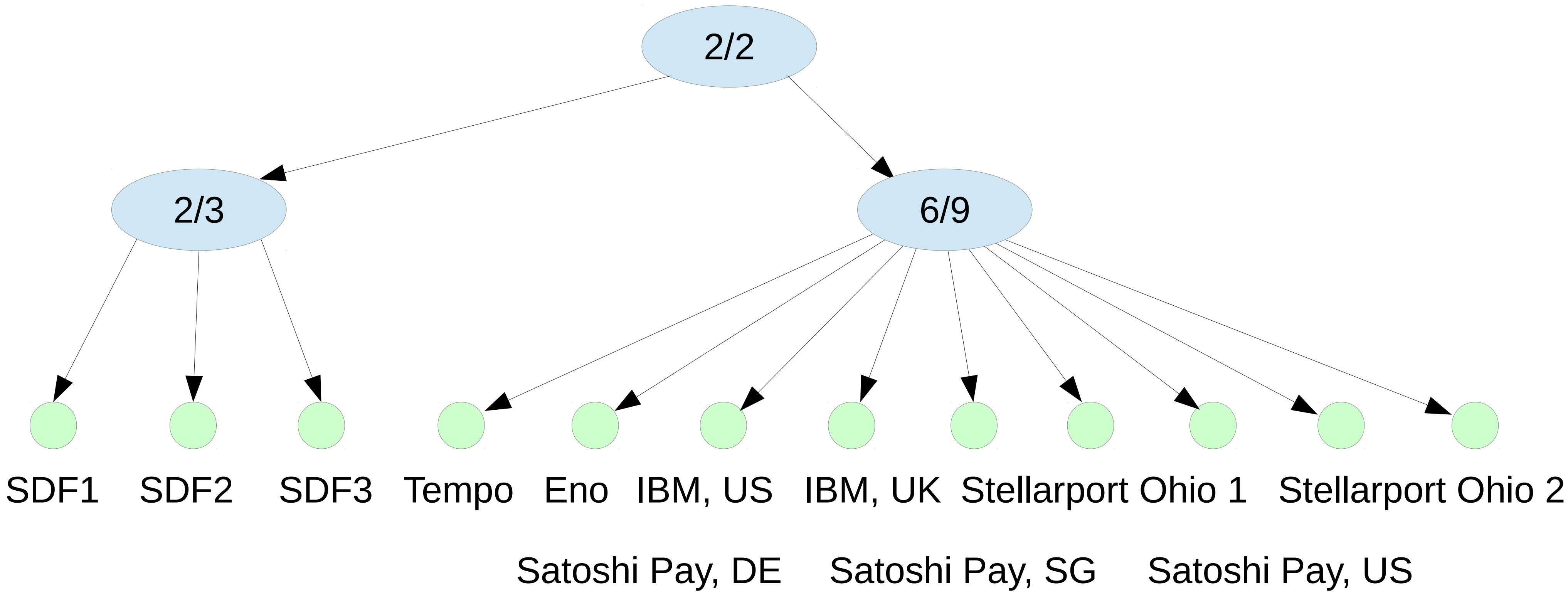


$$\mathbf{Q}(v_i) = \big\{\{v_i, v_{(i \bmod 6)+1}\}\big\}$$

Specifying quorum slices

Definition is based on quorum sets.

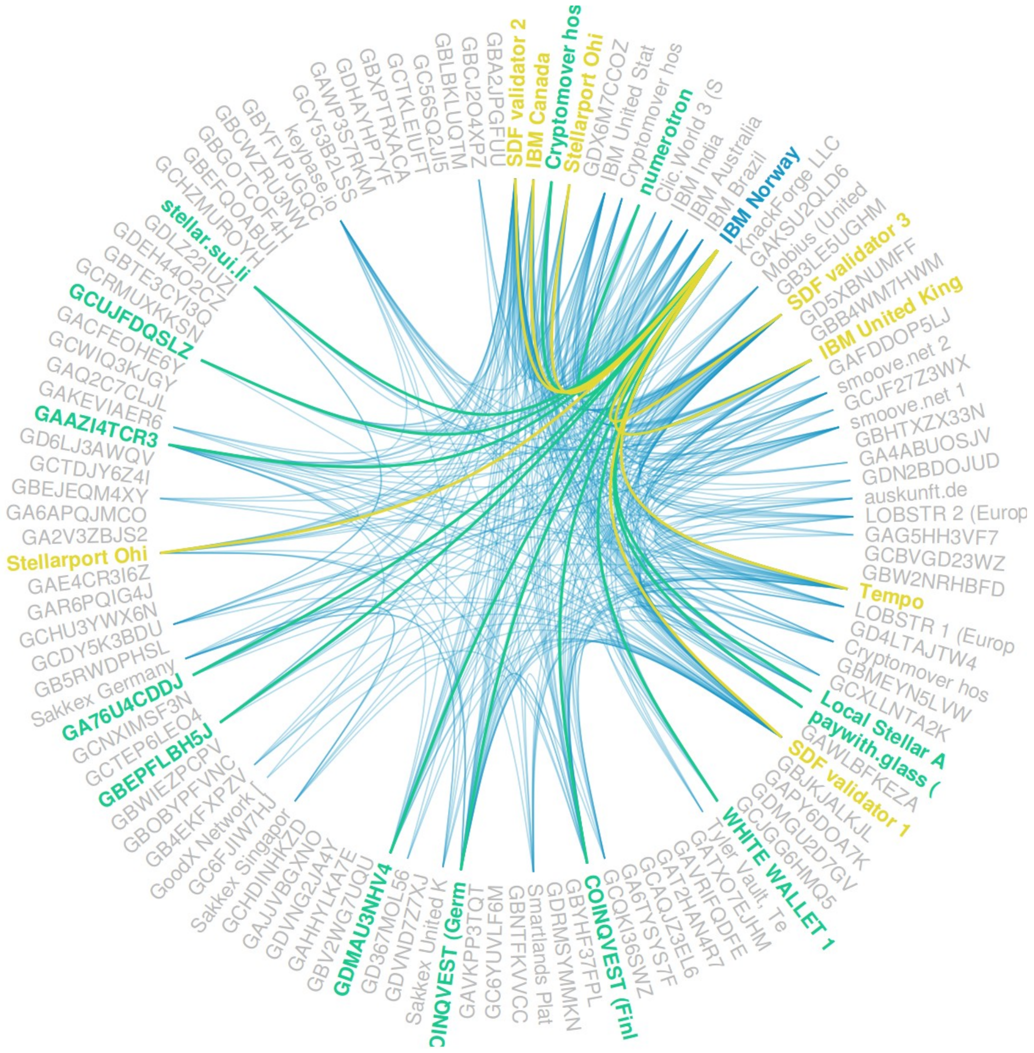
Example: IBM UK



Quroums in practice (1)

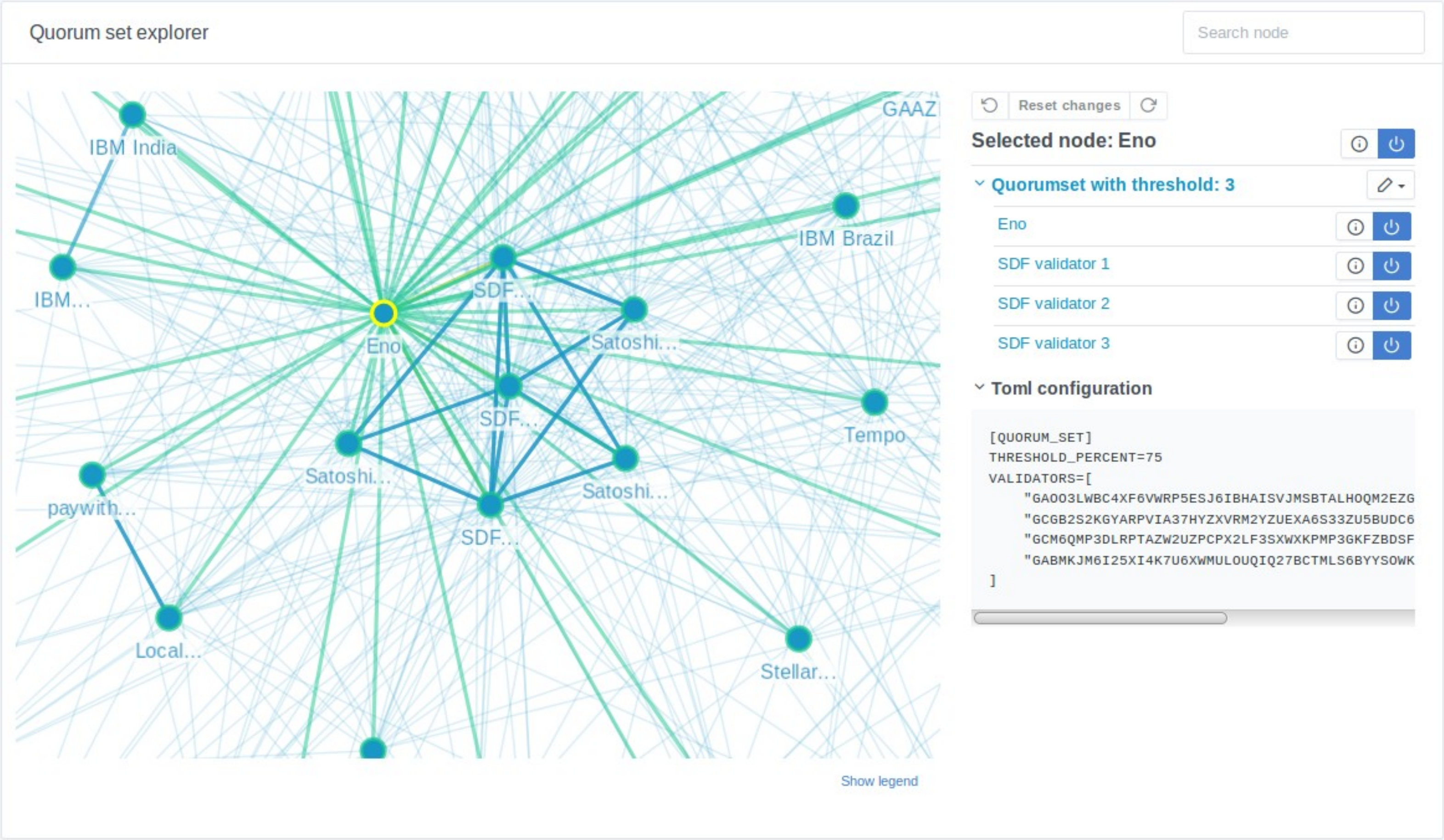
Visualization at stellarbeat.io

- Shows incoming and outgoing trust relations
- Looks nice
- Not very helpful



Quroums in practice (2)

Interactive quorum monitor at stellarbeat.io



Selected node: Eno

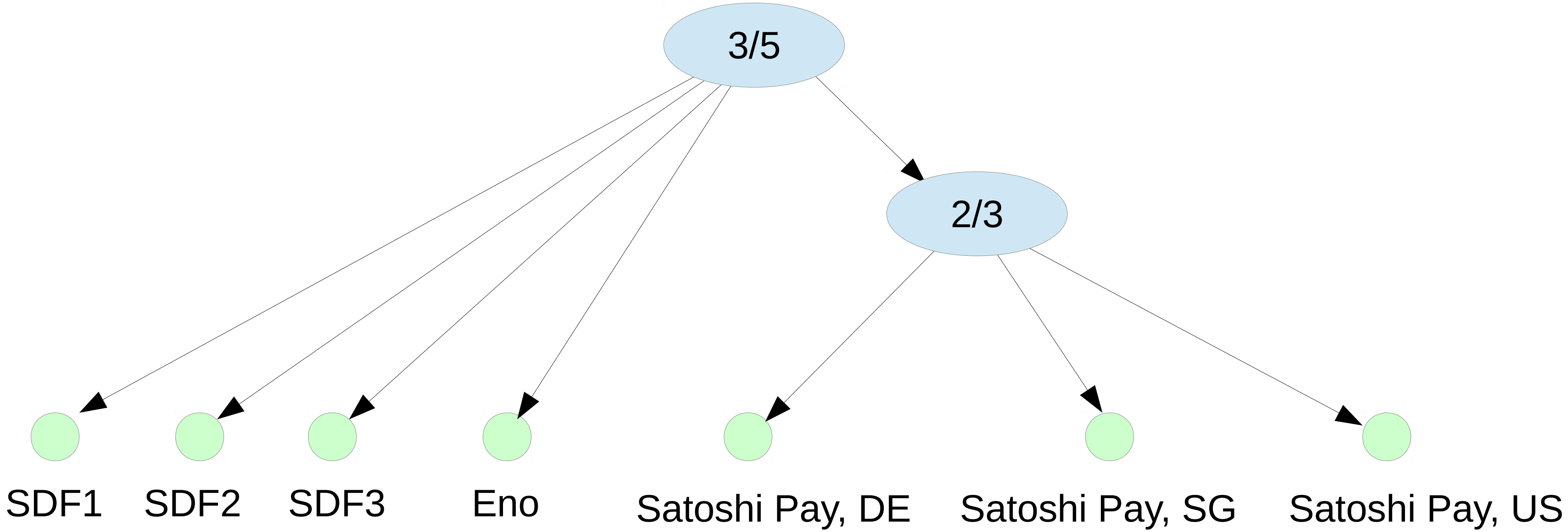
Quorumset with threshold: 3

- Eno
- SDF validator 1
- SDF validator 2
- SDF validator 3

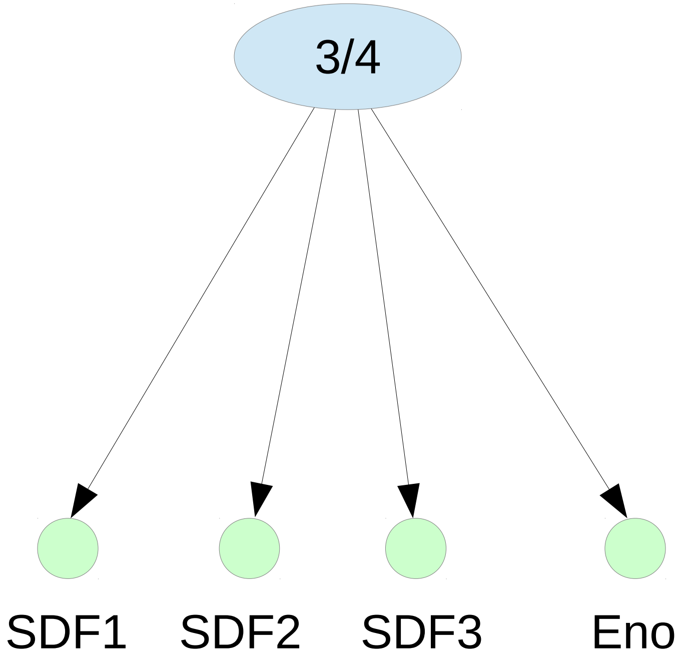
Toml configuration

```
[QUORUM_SET]
THRESHOLD_PERCENT=75
VALIDATORS=[
    "GAOO3LWBC4XF6VWRP5ESJ6IBHAISVJMSBTALHOQM2EZG
    "GCGB2S2KGYARPVIA37HYZXVRM2YZUEXA6S33ZU5BUDC6
    "GCM6QMP3DLRPTAZW2UZPCPX2LF3SXWXKPMP3GKFZBDSF
    "GABMKJM6I25XI4K7U6XWMULOUQIQ27BCTMLS6BYYSOWK
]
```

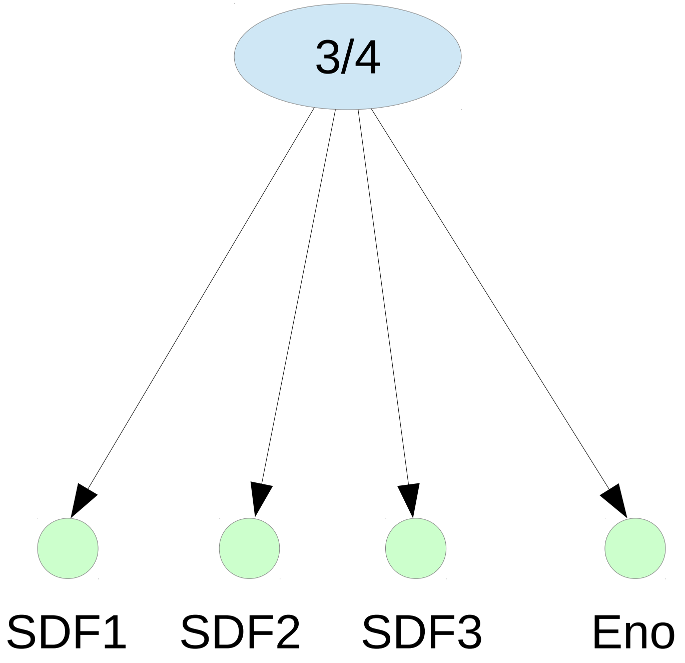
SDF quorum slices



ENO quorum slices



Satoshi pay quorum slices



Conclusion

- Right now Stellar consensus depends on the Stellar Foundation

- Federated Byzantine Agreement facilitates organic growth of the network but it is not clear whether it will actually happen

Resources

- The whitepaper (original and simplified):
  https://www.stellar.org/papers/stellar-consensus-protocol.pdf

  http://www.scs.stanford.edu/~dm/blog/simplified-scp.html
- Helpful blog post:
  https://medium.com/interstellar/understanding-the-stellar-consensus-protocol-423409aad32e
- Quorum explorers
  - stellarbeat.io
  - nodestar.info
  - quorumexplorer.com (broken?)