Is Stellar As Secure As You Think?

Minjeong Kim Yujin Kwon Yongdae Kim

Stellar

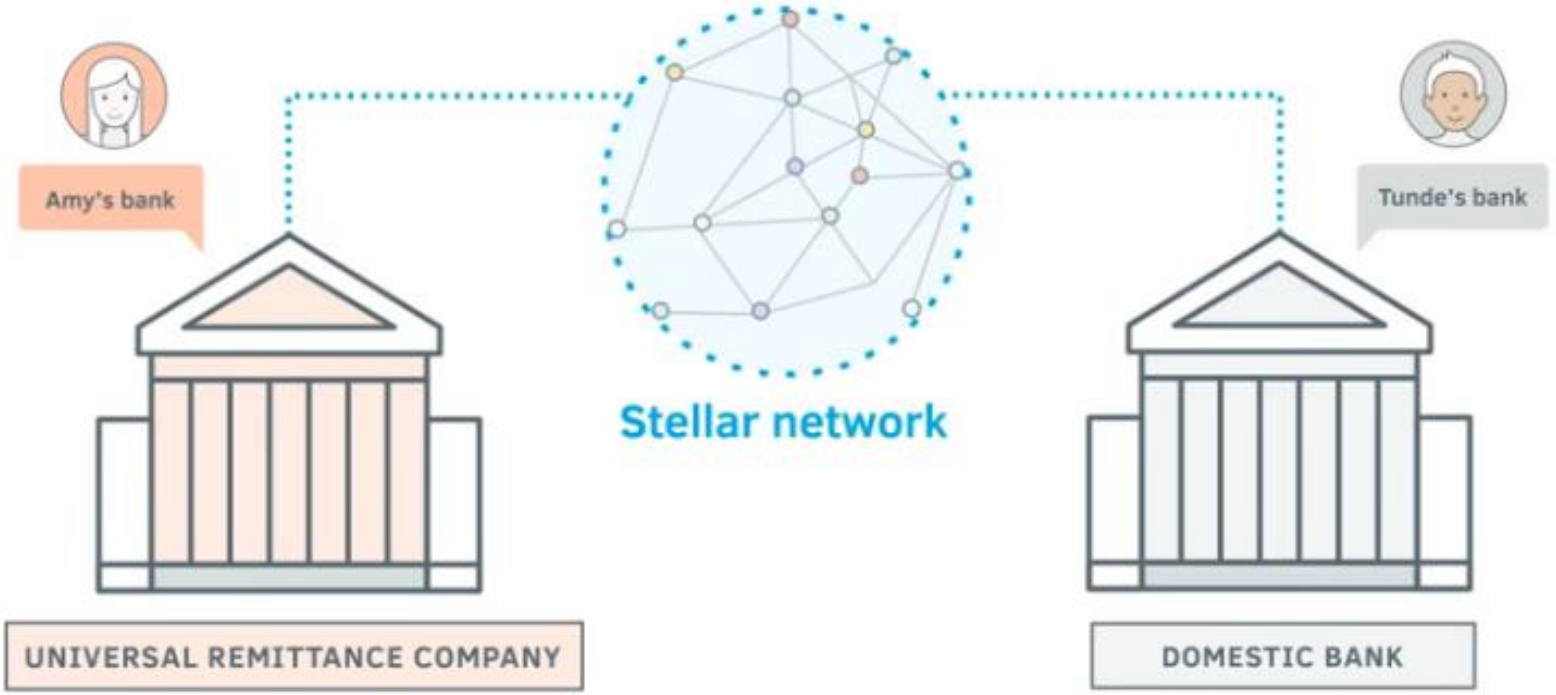
1	Bitcoin	$5,161.43	2.38%	$91.01 B	17.63 M BTC	$17.82 B	
2	Ethereum	$167.92	1.73%	$17.73 B	105.56 M ETH	$7.64 B	
3	XRP	$0.359681	1.02%	$15.01 B	41.74 B XRP *	$1.58 B	
4	Bitcoin Cash	$321.99	10.78%	$5.70 B	17.72 M BCH	$2.78 B	
5	Litecoin	$92.90	3.05%	$5.69 B	61.23 M LTC	$4.11 B	
6	EOS	$5.44	1.45%	$4.93 B	906.25 M EOS *	$3.23 B	
7	Binance Coin	$19.08	-1.22%	$2.69 B	141.18 M BNB *	$152.11 M	
8	Stellar	$0.128513	1.80%	$2.48 B	19.27 B XLM *	$339.73 M	
9	Cardano	$0.090394	0.70%	$2.34 B	25.93 B ADA	$109.84 M	
10	Tether	$1.00	-0.13%	$2.09 B	2.08 B USDT *	$18.45 B	

Stellar

- Problem of central authority
- **Cross-border Payment is too slow and costly**
- Try to solve those problems with blockchain

Stellar

Open platform that connects people, bank or payment systems



History

- Jed McCaleb
  - created Mt.Gox, peer-to-peer eDonkey, Overnet networks …
  - co-founder of Ripple
  - co-founder of Stellar

ripple	STELLAR
To allow banks to transfer money internationally	To allow citizens from developing countries to transfer money internationally
Private blockchain	Blockchain with open membership
XRP	Lumens
Proof of correctness	Stellar Consensus Protocol (SCP)
Fixed membership list	Flexible membership list

Background

Federated Byzantine Agreement (FBA)

❖ Advantages of PBFT
- high transaction throughput
- no waste of energy …

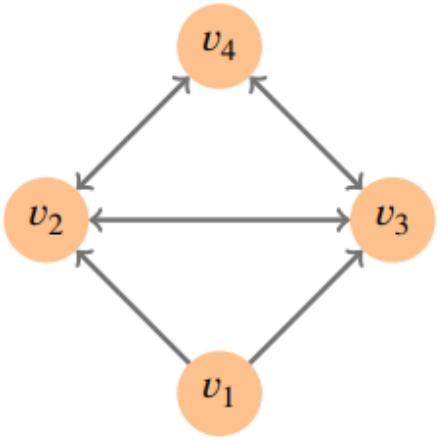
❖ Disadvantages of PBFT
- fixed set of membership list in advance by central authority
  → not suitable for public blockchain

❖ **Federated Byzantine Agreement (FBA)**
- **PBFT + open membership**
- Stellar consensus protocol (SCP) is a construction for FBA
- Trust model
- Quorum slice, Quorum

Quorum Slice / Quorum

❖ Quorum Slice

- A set of nodes that you trust.



QS(node) = Quorum Slice of node

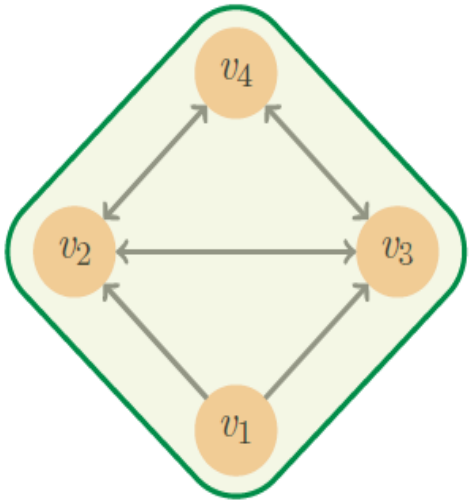
QS (v1) = { { v1, v2, v3 } }
QS (v2) = QS (v3) = QS (v4) = { { v2, v3, v4 } }

- Threshold value
  ex) { t : 2, v_1, v_2, v_3 }
- Nested quorum slice
  ex) { t : 2, v_1, v_2,{ t : 1, v_1, v_2, v_3 }}
- Several quorum slices
- Can have the same slice
- User configurable

Quorum Slice / Quorum

❖ **Quorum**

- A quorum U ⊆ V is a set of nodes that encompasses at least one slice of each of its members.



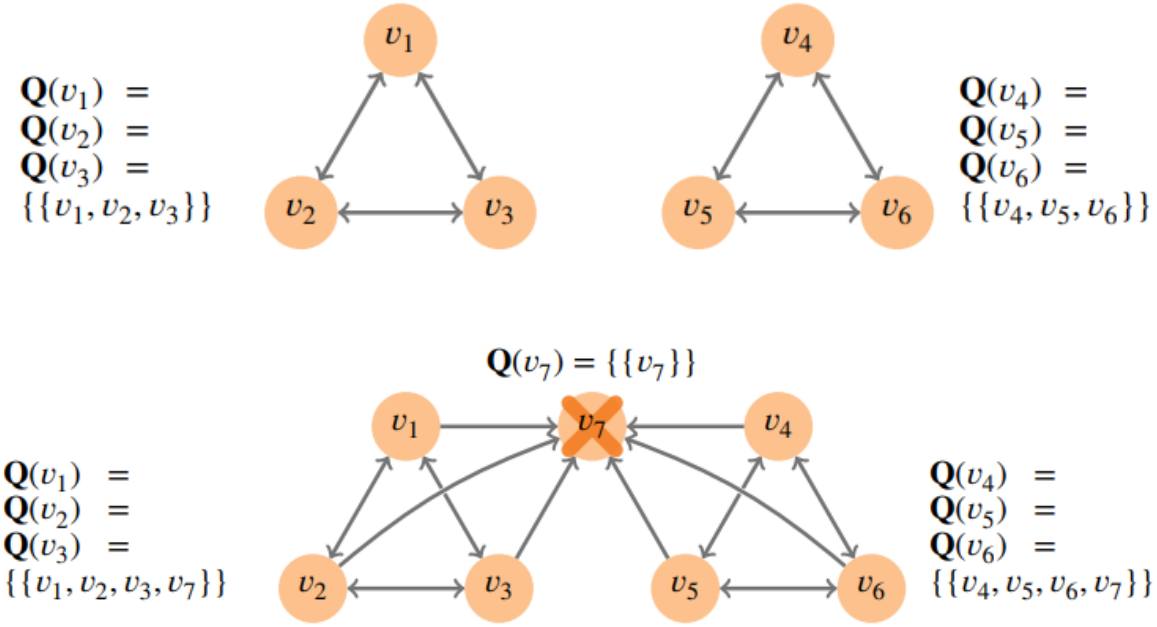
QS(node) = Quorum Slice of node

QS (v1) = { { v1, v2, v3 } }
QS (v2) = QS (v3) = QS (v4) = { { v2, v3, v4 } }

Quorum Slice / Quorum

❖ Quorum Formation Conditions

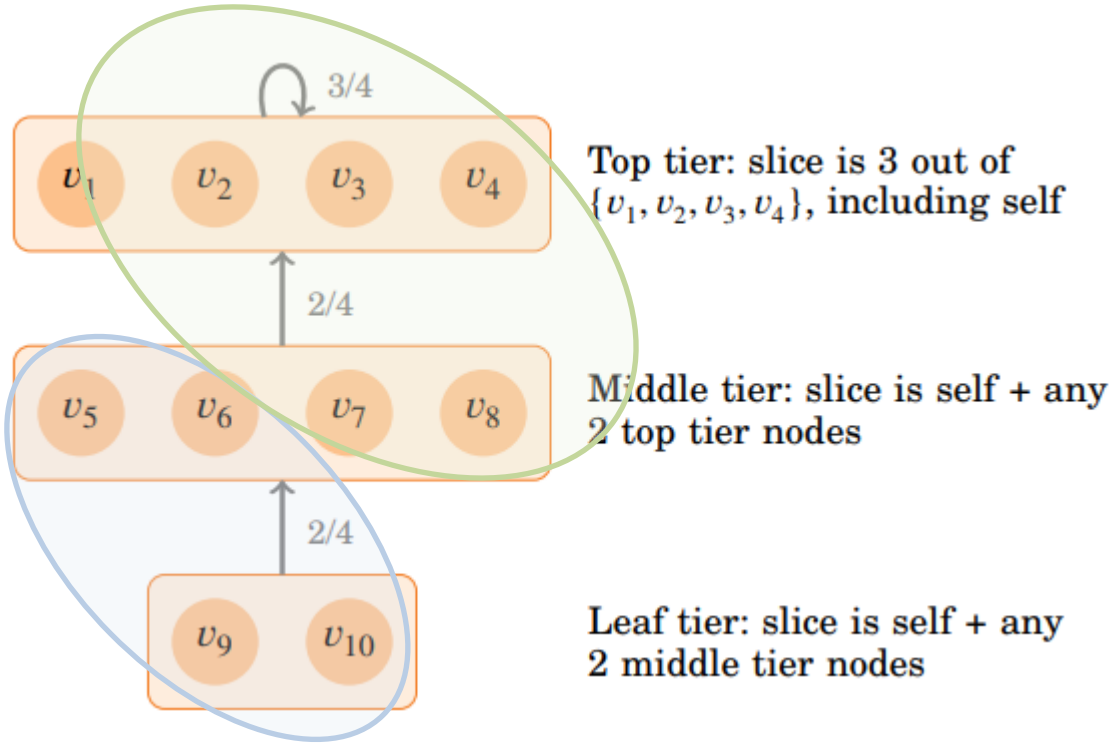
- **Condition 1** : Any two quorums should contain an intersection even after deleting byzantine nodes in the quorums (safety)



Quorum Slice / Quorum

❖ Quorum Formation Conditions

- **Condition 2** : Quorum still exists after deleting byzantine nodes (liveness) (Dispensable Set)

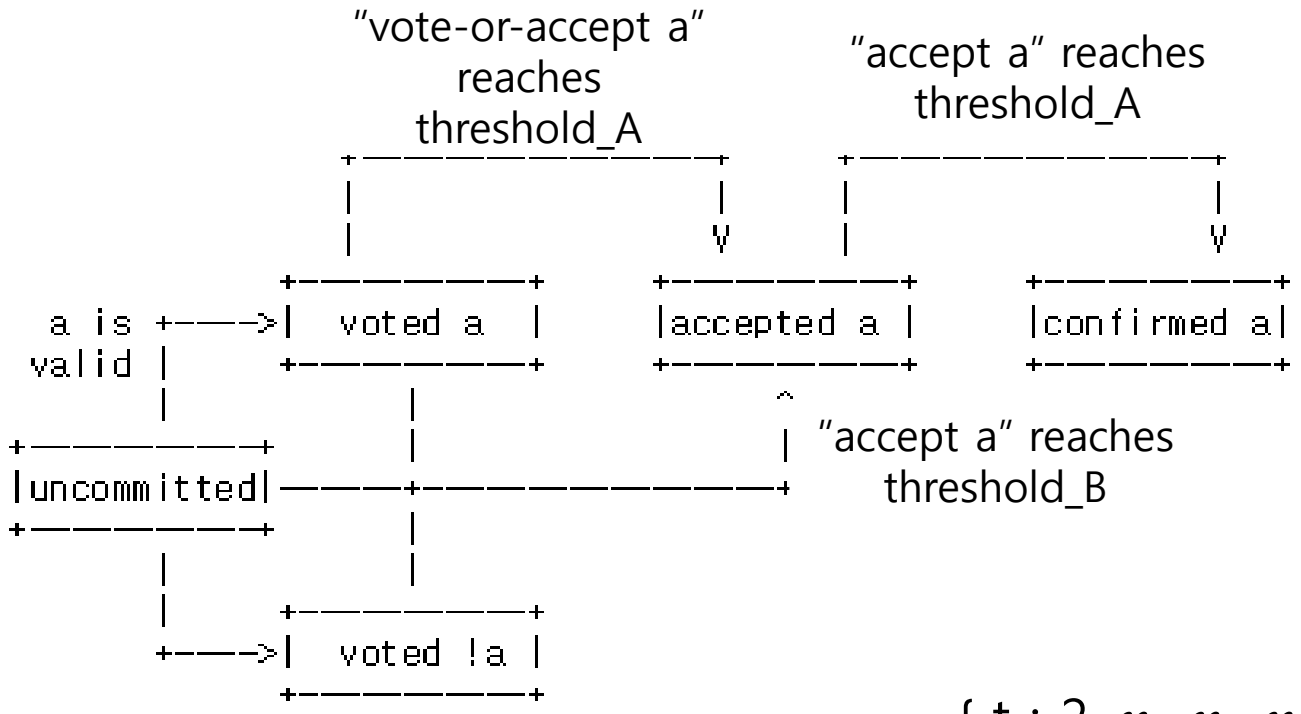


Stellar Consensus Protocol (SCP)

- A construction for FBA
- Nomination, Ballot
- Federated voting

Stellar Consensus Protocol (SCP)

❖ **Federated Voting**



$\{ t : 2, v_1, v_2, v_3 \}$

- **threshold_A** : threshold of each quorum slice
- **threshold_B** : number of nodes in slice – threshold1 + 1

Stellar Consensus Protocol (SCP)

❖ **Nomination**

- **nodes converge on a set of candidate values**
- NOMINATE x : states that x is a valid candidate consensus value
- nodes can take the union of sets, the largest set, or the set with the highest hash …
- federated leader selection : to reduce the number of different values in NOMINATE statements

❖ **Ballot**

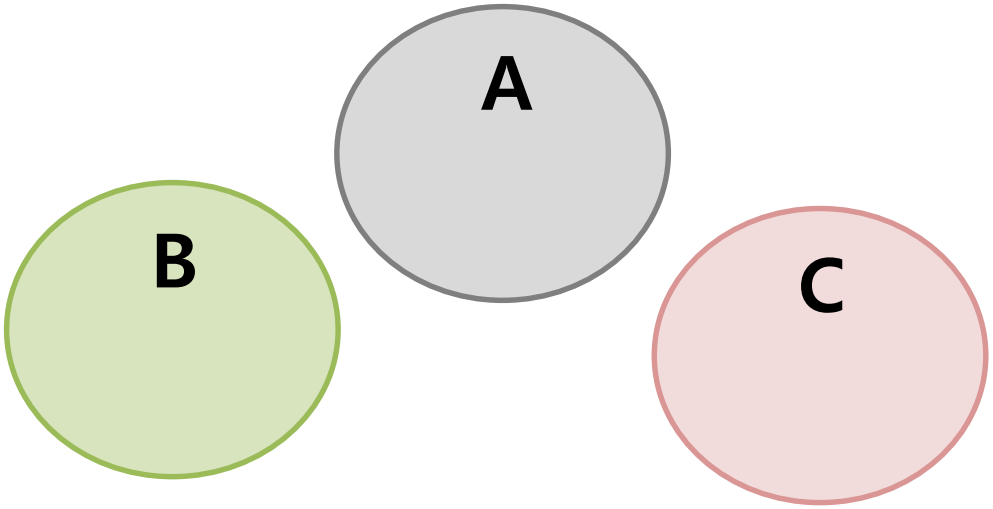
- SCP votes on a series of numbered ballots
- If stuck, we can time out and try again with ballot n+1

Some terminologies…

- **Well-behaved** node
  : It chooses acceptable quorum slice and responds properly
- **Ill-behaved** node
  : It suffers from byzantine failure
- **Validator**
  : Node that participates in the consensus protocol by broadcasting vote messages
- **Safety**
  : A set of nodes satisfy safety if no two of them ever reach an agreement on different values at the same time
- **Liveness**
  : A node satisfies liveness if it can reach an agreement on a new value even without the participation of faulty nodes

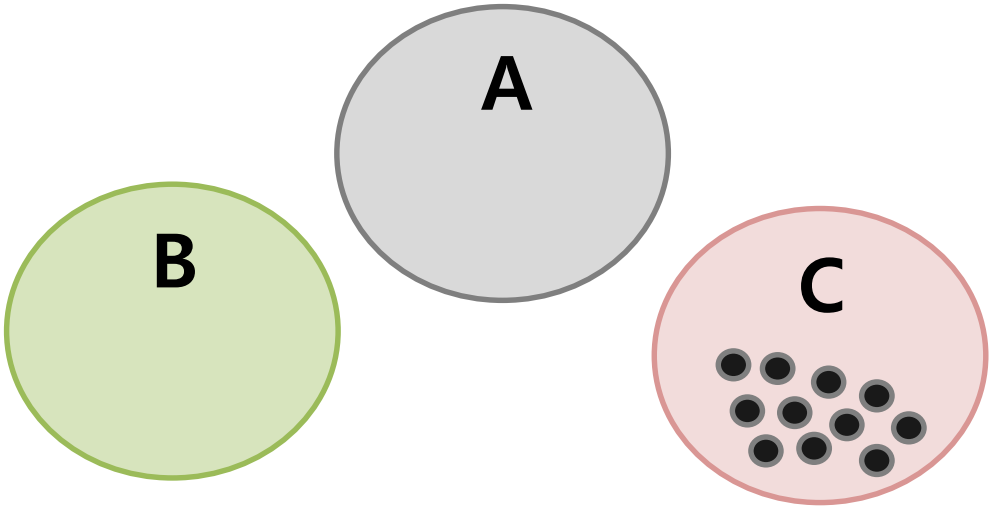
FBA Analysis

Brief diagram of FBA



Group A : ill-behaved nodes
Group B : well-behaved nodes that are affected by the ill-behaved nodes
Group C : remaining well-behaved nodes

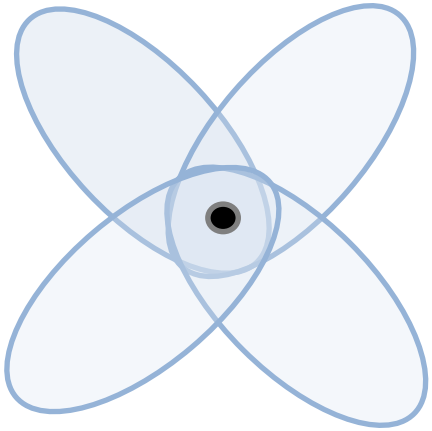
Brief diagram of FBA

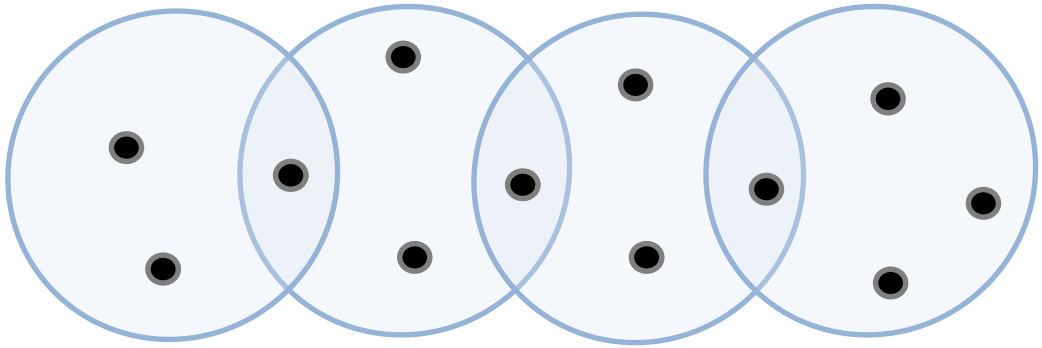


Group A : ill-behaved nodes
Group B : well-behaved nodes that are affected by the ill-behaved nodes
Group C : remaining well-behaved nodes

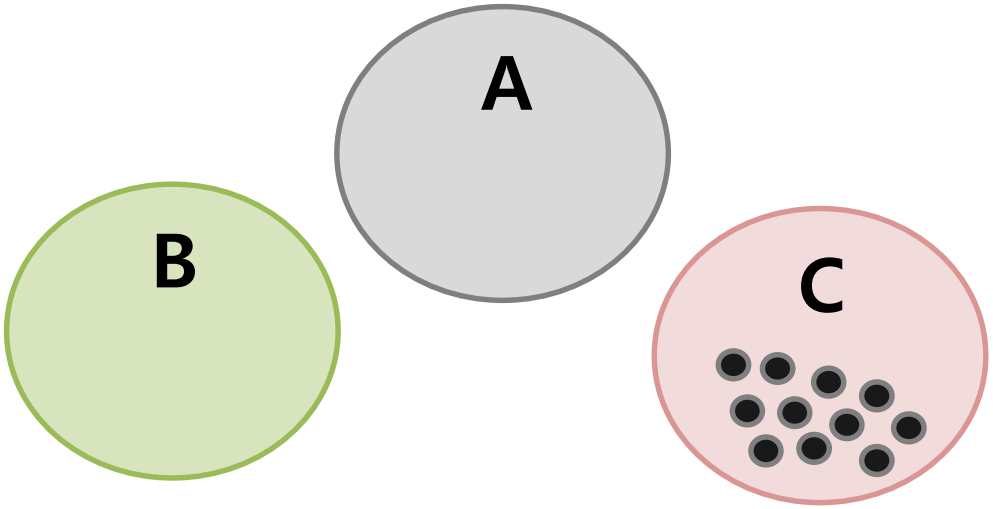
It depends on the **structure of quorum slices!**

Depends on Structure of Quorum Slice?





Brief diagram of FBA



Group A : ill-behaved nodes
Group B : well-behaved nodes that are affected by the ill-behaved nodes
Group C : remaining well-behaved nodes

It depends on the **structure of quorum slices!**

(f, x)-FT (Fault Tolerant) System

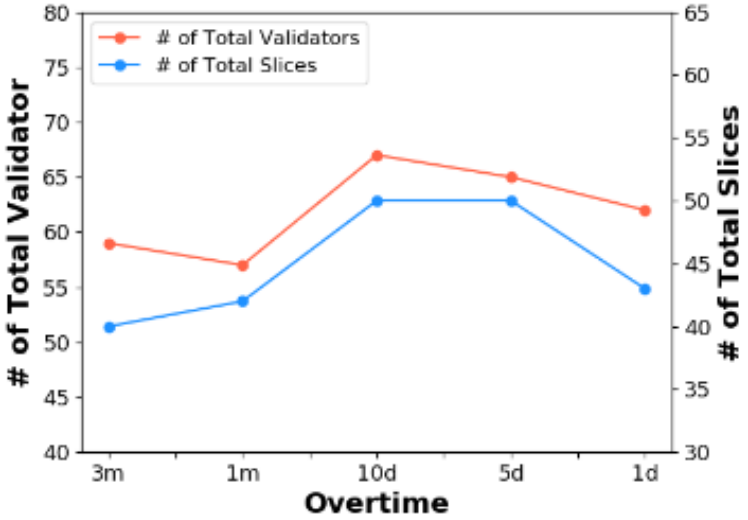
❖ **(f, x)-FT System**

- It represents how much the system is tolerant of ill-behaved nodes
- " If less than f nodes are ill-behaved, where account for x% of the total active validators, all nodes eventually can agree on the same value that are not contradictory to history in process of consensus. "
- f and x value in FBA can be changed depending on the structure of quorum slices
- A value of x in FBA ranges from 0 to $\frac{100}{3}$
- x value of PBFT is $\frac{100}{3}$
- FBA is less than or equal to PBFT in terms of x value

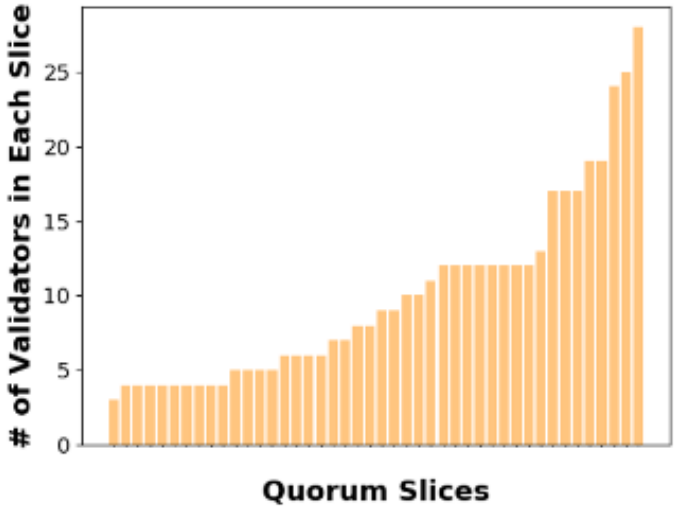
Data Analysis

Characteristics of Quorum Slices

- Number of validators and quorum slices in the current Stellar system



(a) The number of total validators and quorum slices in the system over time



(b) The number of validators in each quorum slice

Characteristics of Quorum Slices

❖ Why is it so small??

- No incentivization

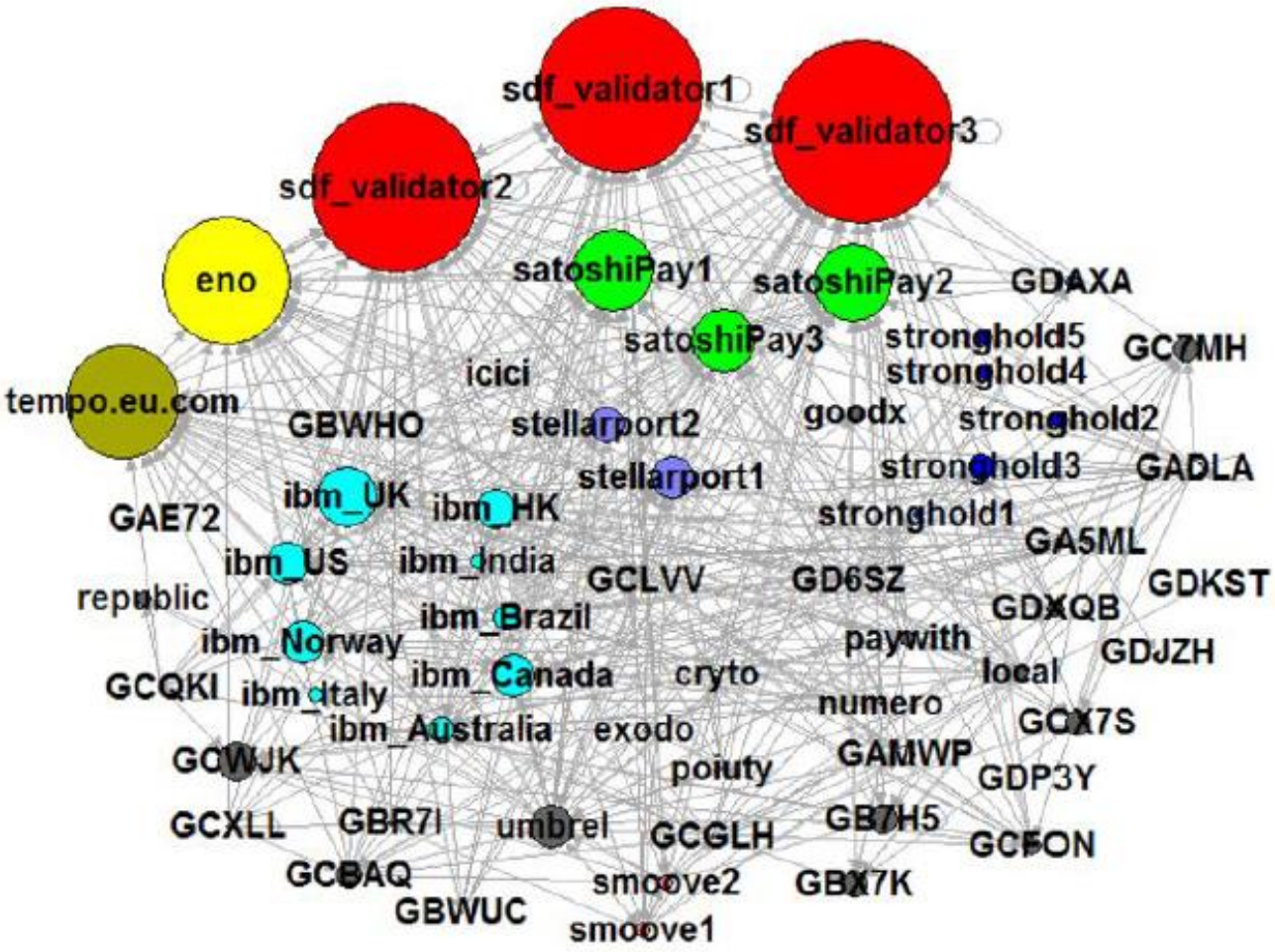
Table I
WHY PLAYER PARTICIPATES IN STELLAR AS A VALIDATOR.

Purpose	Type	Number of players	Rate (%)
For-profit	Business with Stellar	23	74.2
	Stellar Foundation	3	9.7
Non-profit	Individual	1	3.2
Unknown		4	12.9

- Based on the trust model

ex) satoshipay → {sdf_validator1, sdf_validator2, sdf_validator3, eno}

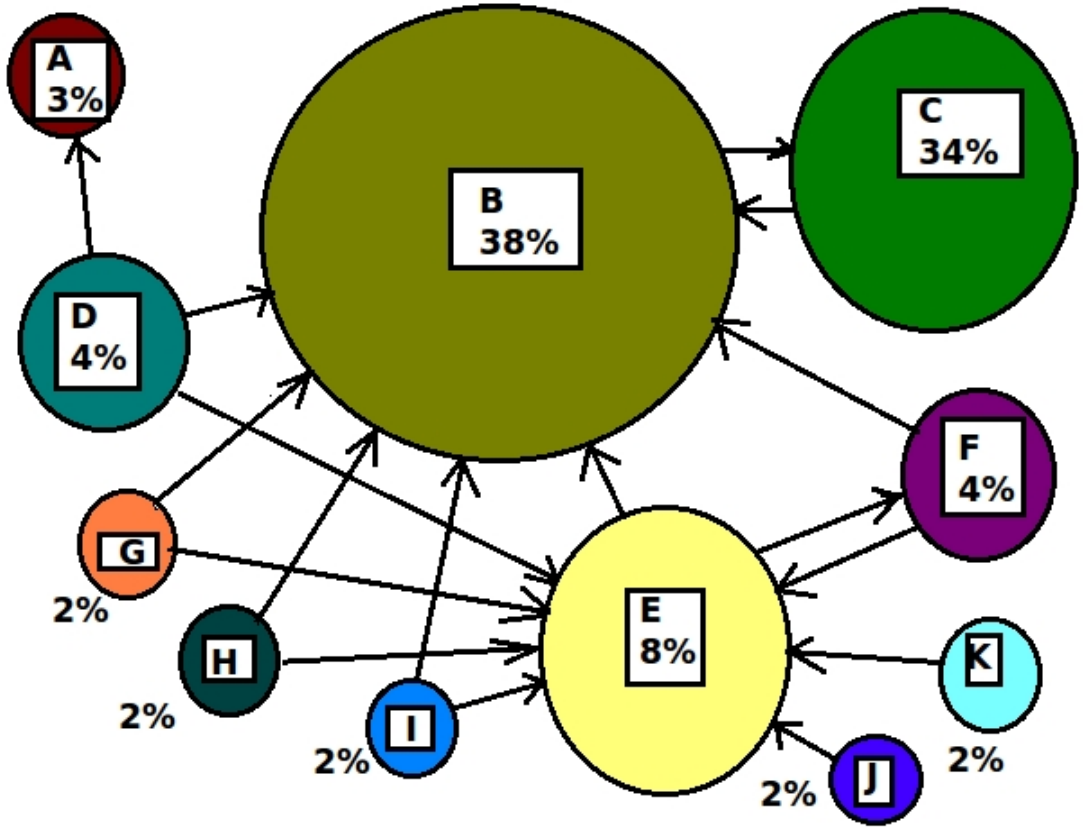
Visualization of Quorum Slices



Node Influence

❖ Evaluation of Node Influence

- PageRank (PR)



Node Influence

❖ Evaluation of Node Influence

- NodeRank (NR)

1) How many times the node is included in slices
2) Whether an influential node chooses the node in its slice
3) Whether the threshold of slice containing the node is high or low

$$n_1 \rightarrow \{t: 3, n_1, n_2, n_3\}$$
$$n_4 \rightarrow \{t: 2, n_4, n_5, n_6\}$$

$$\text{Influence}(n_2) > \text{Influence}(n_5)$$

Node Influence

❖ Evaluation of Node Influence

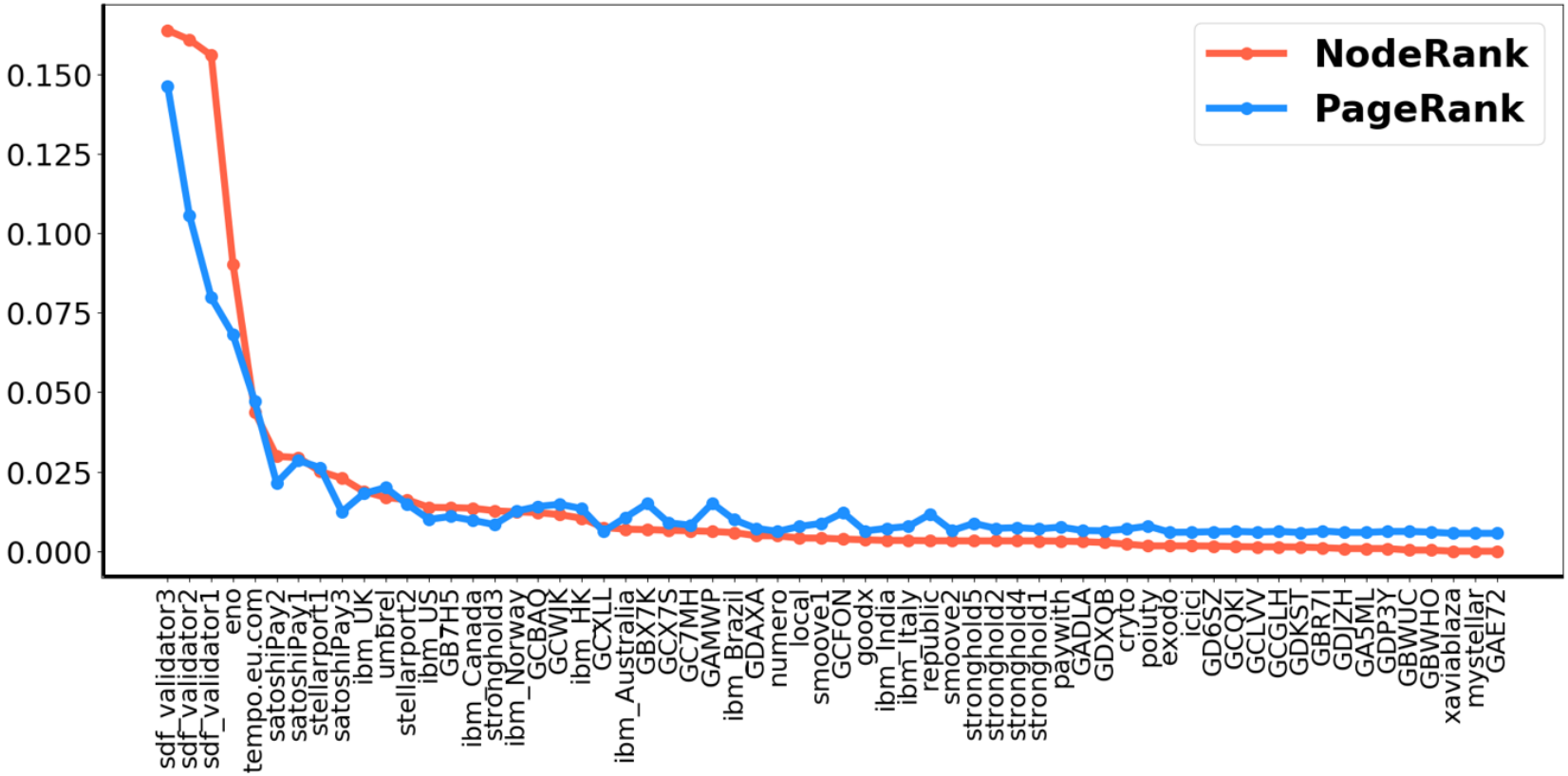
- NodeRank (NR)

1) How many times the node is included in slices
2) Whether an influential node chooses the node in its slice
3) Whether the threshold of slice containing the node is high or low

$$a_0(Q,v) = 1, \quad a_k(Q,v) = \frac{T_Q}{|Q|} \times a_{k-1}(Q,v)$$

$$\mathrm{NR} = \sum_{Q \in \boldsymbol{Q}_v} \sum_{G \in \boldsymbol{G}_Q} \mathrm{PR}_G \times a_{l(Q,v)}(Q,v)$$

Node Influence



- Why is it biased?
  - Based on the trust model
  - small number of validators

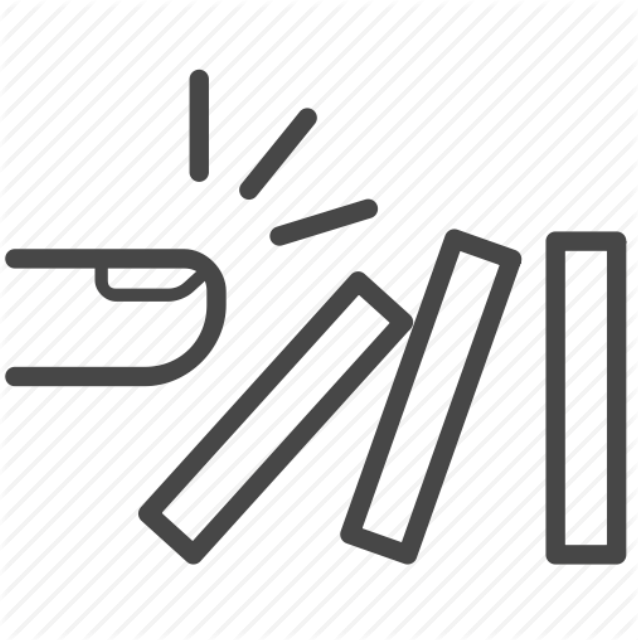
So the current structure of quorum slices in Stellar…

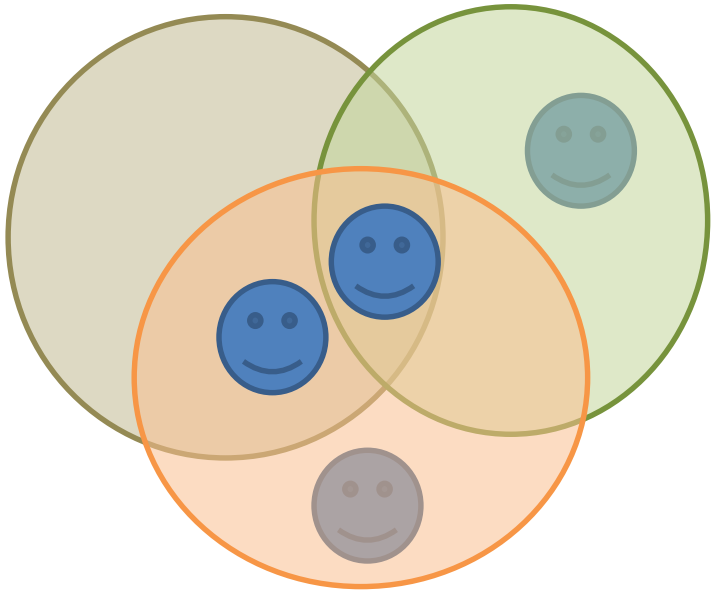
- Small number of validators
- Significantly biased

➔ Centralized!!

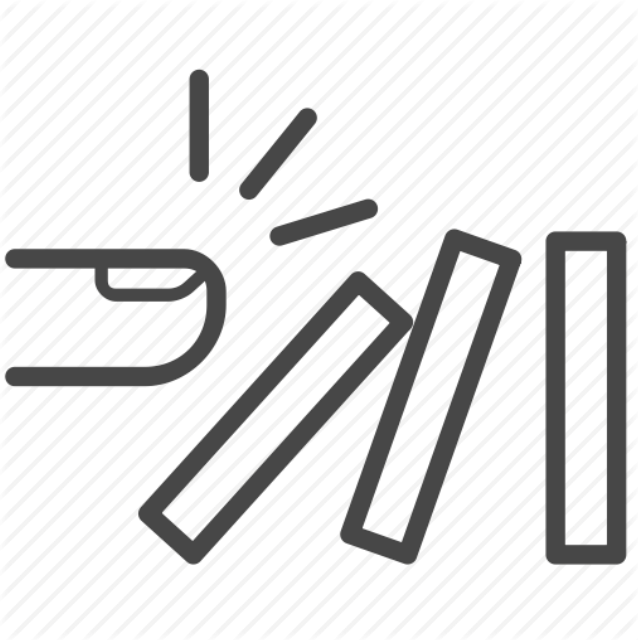
Cascading Failure

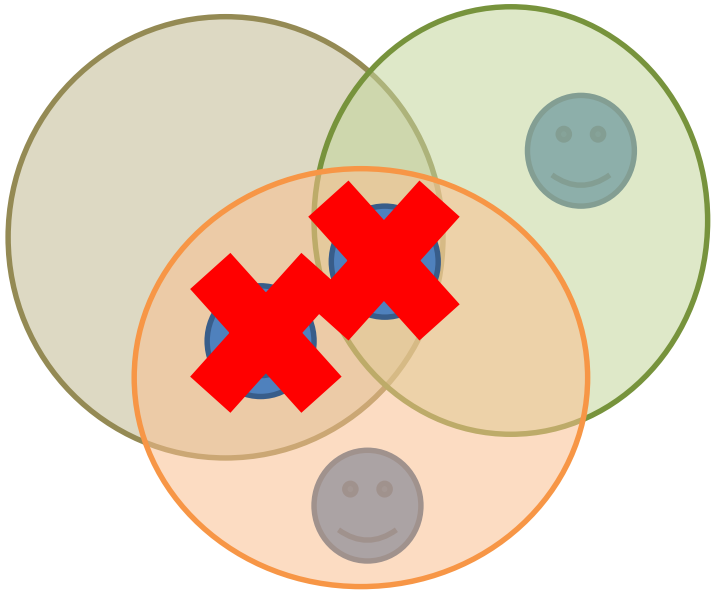
Cascading Failure



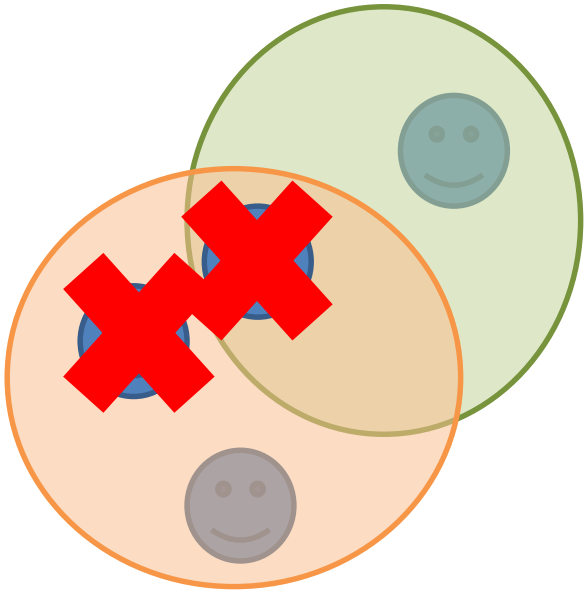


Cascading Failure

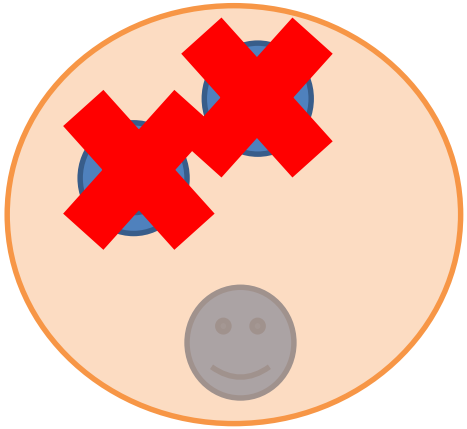




Cascading Failure



Cascading Failure



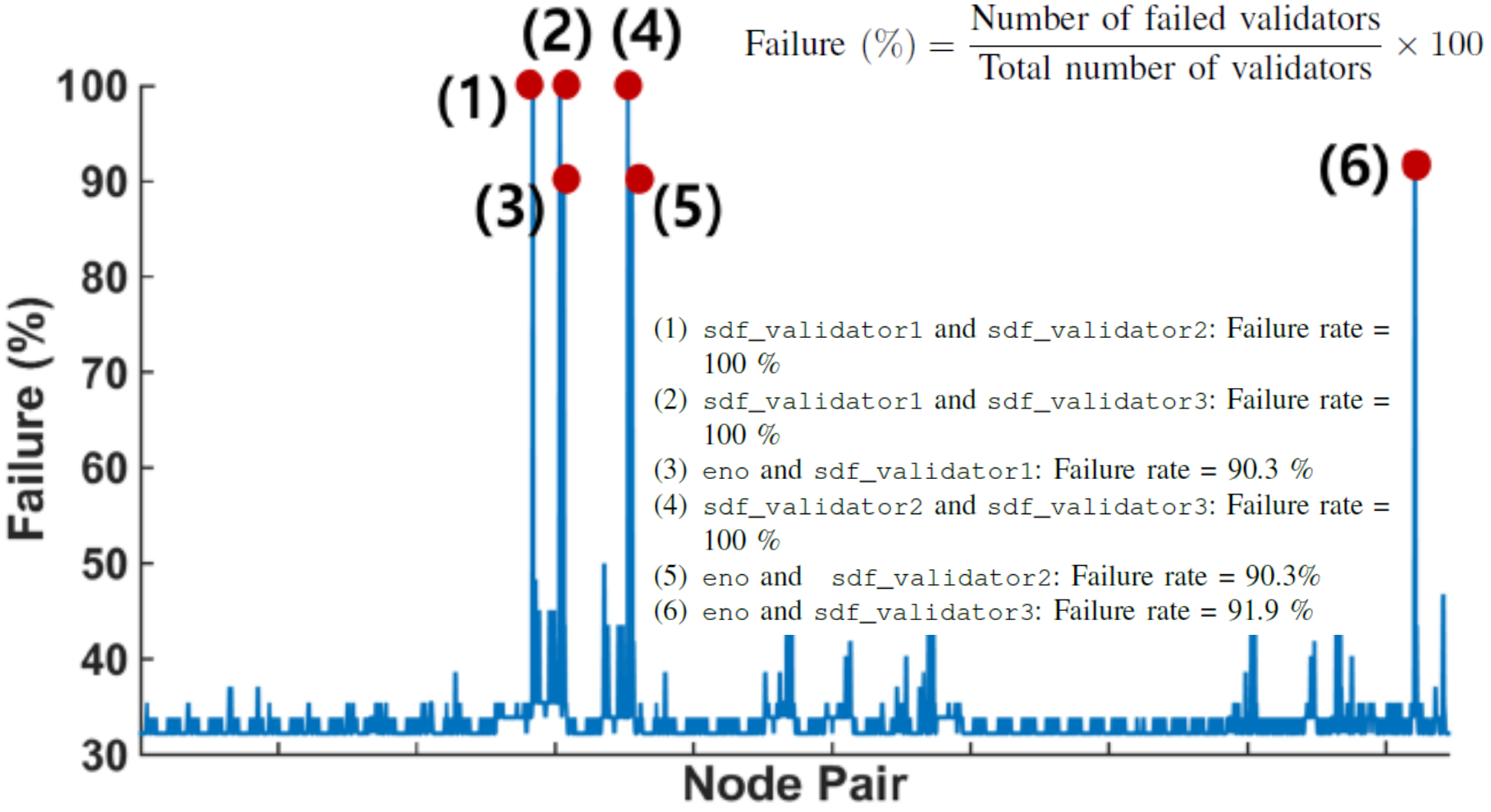
Cascading Failure

Cascading Failure

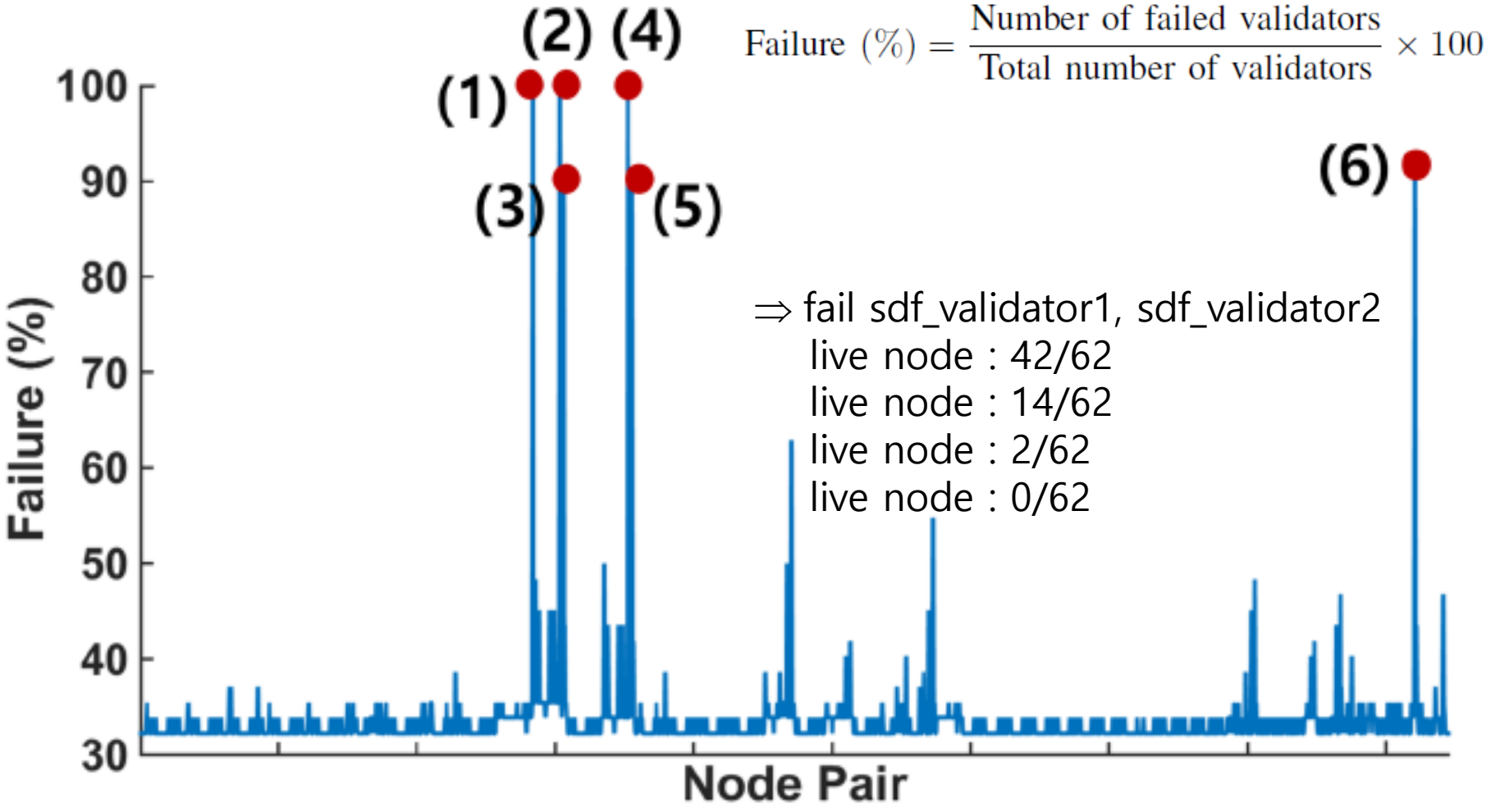
- How is cascading failure possible in Stellar?
  - The protocol is designed to be influenced by other nodes
  - The degree of robustness against cascading failure depends largely on the structure of quorum slices

- Then, what about the current Stellar system?

Cascading Failure

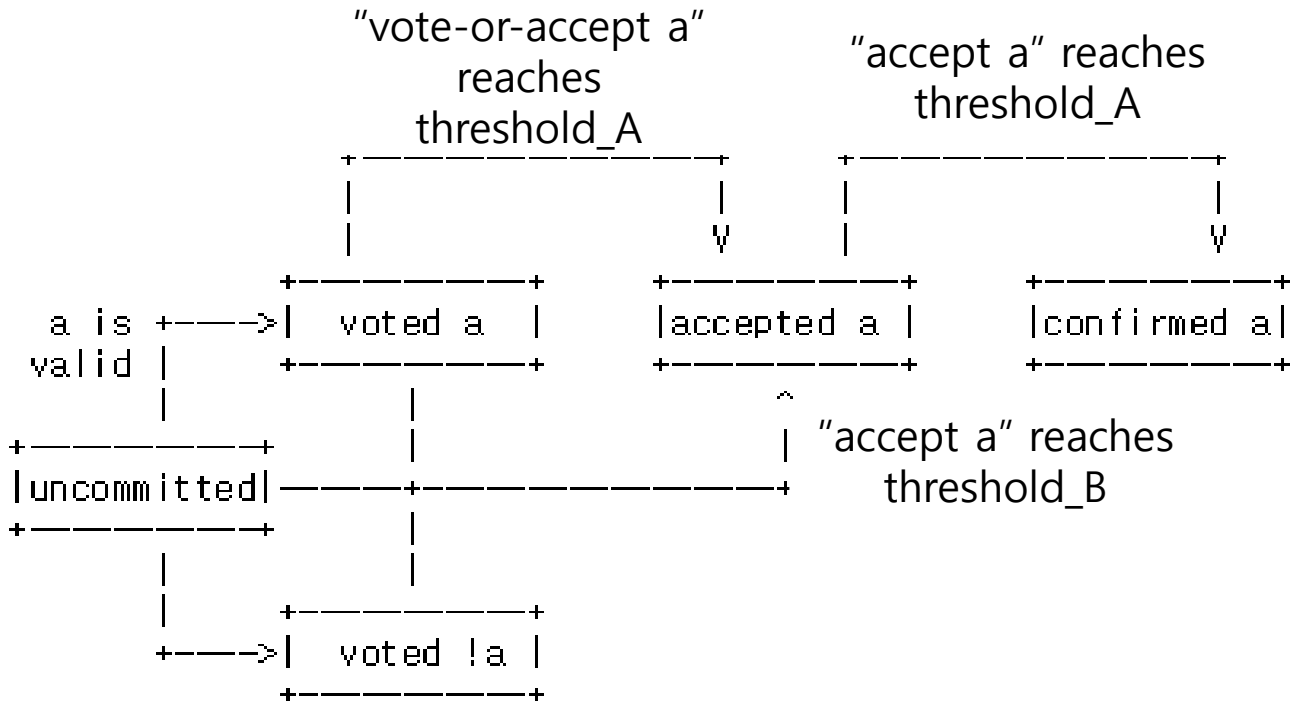


Cascading Failure



Cascading Failure

- Federated Voting



- **threshold_A** : threshold of each quorum slice
- **threshold_B** : number of nodes in slice – threshold1 + 1

Cascading Failure

- Result
  - Stellar is **(2, $\frac{50}{11}$ (≈ 4.5))-FT** System
  - Much smaller than $\frac{100}{3}$ ($\approx$ 33.3)
  - Even those two nodes are all controlled by Stellar Foundation

Discussion

Mitigations & Limitations

- Making Stellar's structure of quorum slices like that of PBFT style?
  - Every user is enforced to have the same slice
  - Must dynamically and securely change their slices

- Change the value of threshold to a lower number?
  - Then, have a safety problem

- What if lots of popular and important financial institutions come in the Stellar system so that user can diversely choose various validators?
  - How to attract such institutions?

Conclusion

Summary

- Analyze FBA and define (f, x)-FT System
- Find that x ranges from 0 to $\frac{100}{3}$
- Analyze the current structure of quorum slices -> centralized
- By cascading failure, (2, $\frac{50}{11}$ (≈ 4.5))-FT System

Thank You!