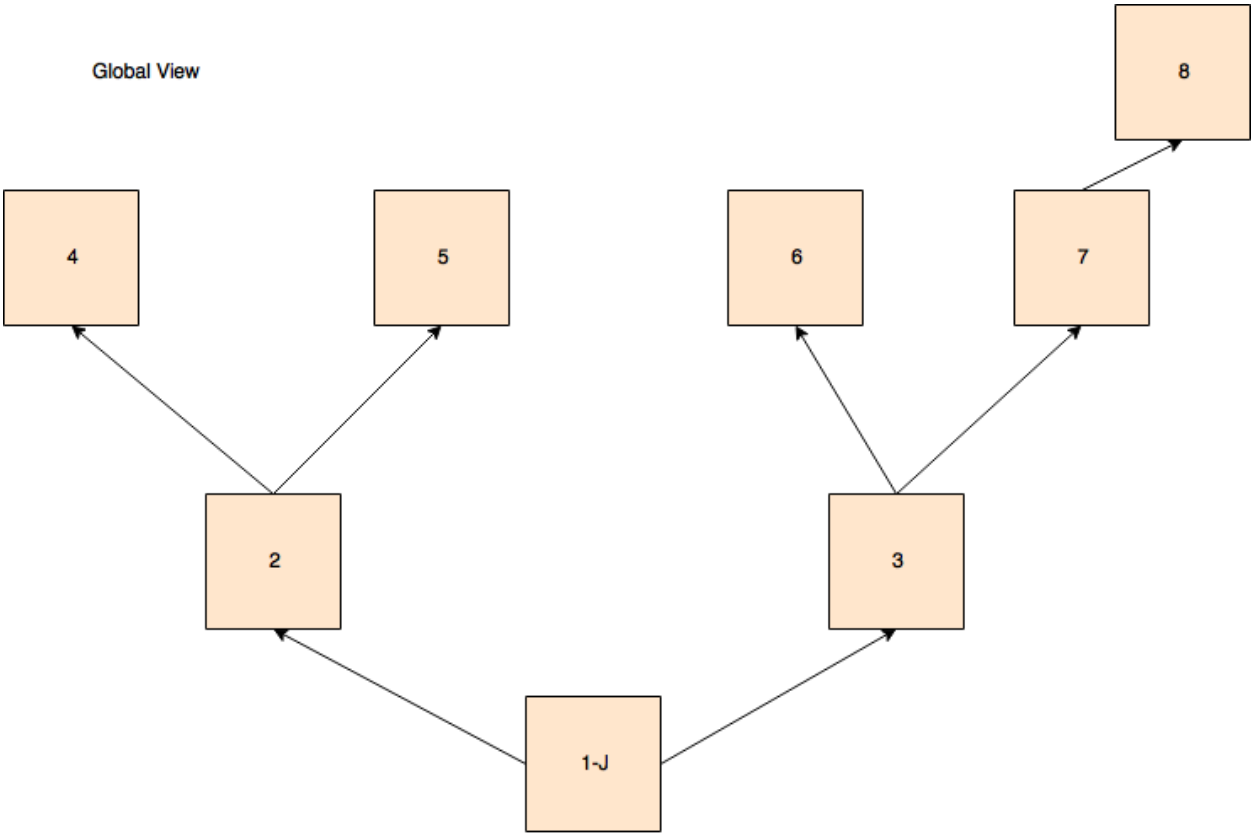
Premature justification/voting leads to deadlock.

- We can show that premature justification schemes will lead to confirmed deadlock if the forking scheme is given by: vote from highest Semi-Justified Checkpoint.
- If the voting scheme is changed to vote from highest(highest justified checkpoint, highest semi justified checkpoint) there is still a chance that a deadlock might take place.

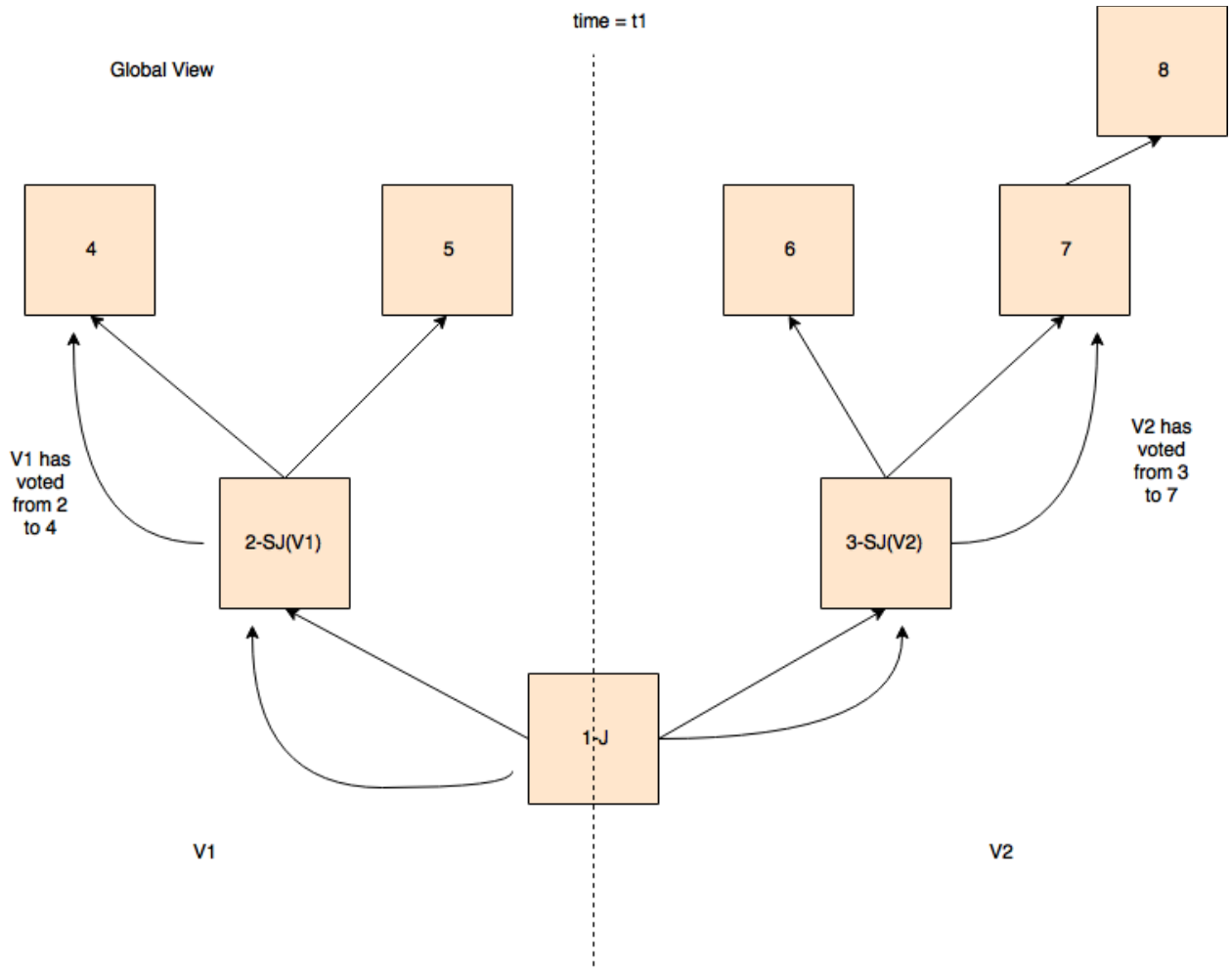


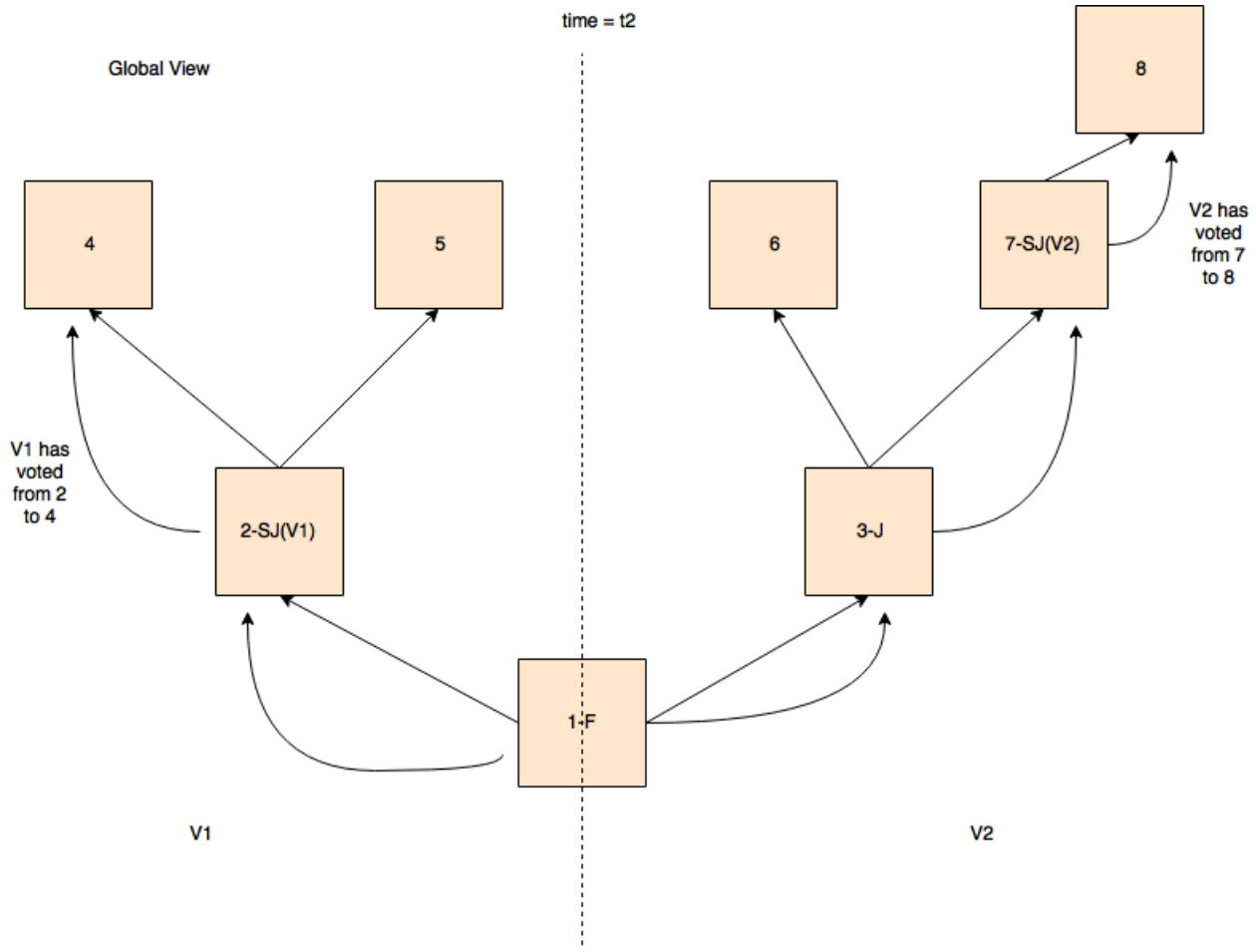
- Let us call a premature justified block as semi-justified block(SJ).

Vote from highest semi-justified checkpoint

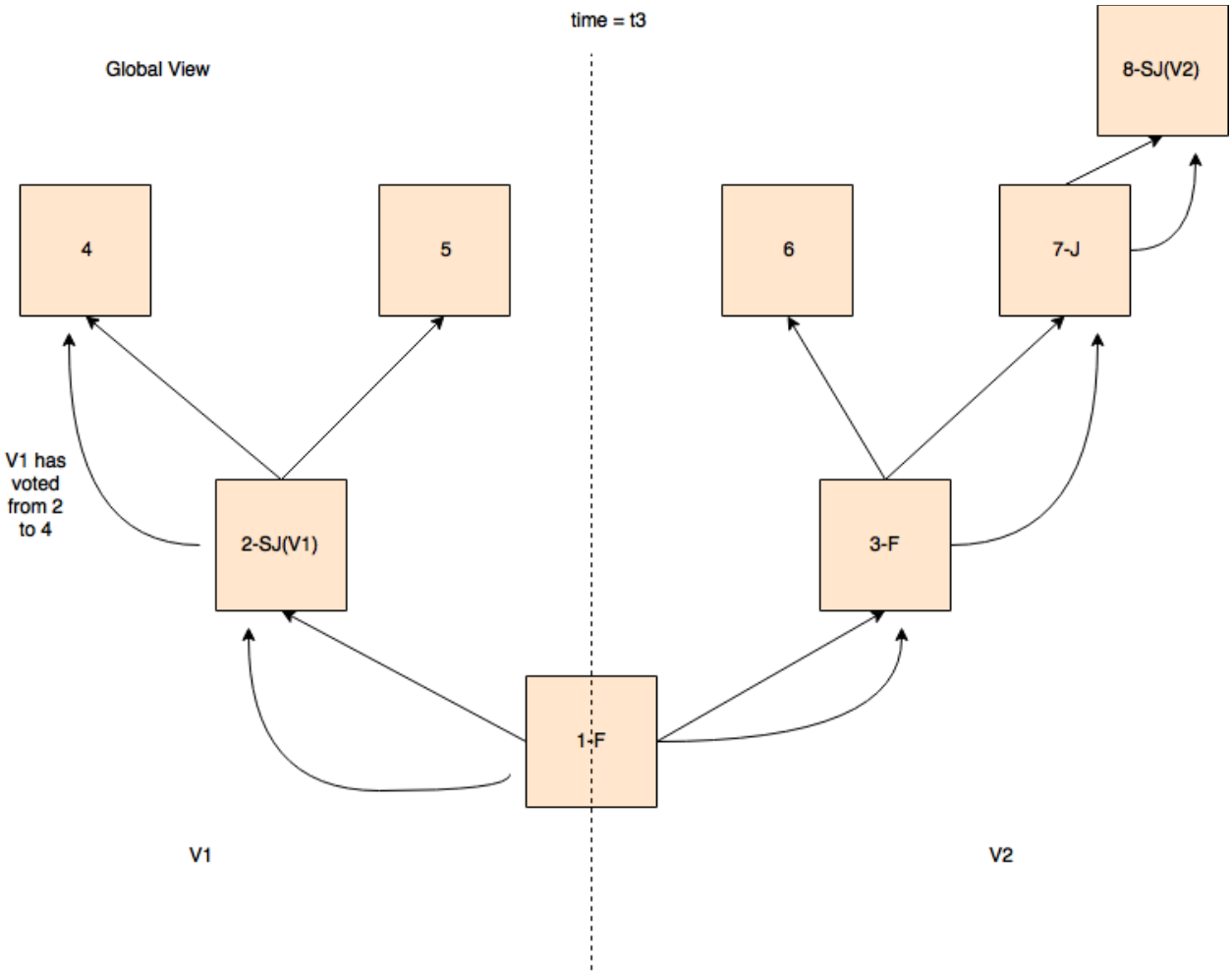
- Consider a diagram bellow.

- This is a global view of all the checkpoints, let checkpoint 1 be Justified at t=t0.
- Let us divide validators in two sets, V1 are validators who semi-justify left branch and V2 are validators who semi-justify right branch(shown in figure below).
- Fraction of V1 = p >0
- Fraction of V2 = 1-p
- p<1/2 w.l.o.g.


time = t1
Global View
8
4
5
6
7
V1 has voted from 2 to 4
2-SJ(V1)
3-SJ(V2)
V2 has voted from 3 to 7
1-J
V1
V2


time = t2
Global View
8
4
5
6
7-SJ(V2)
V2 has voted from 7 to 8
V1 has voted from 2 to 4
2-SJ(V1)
3-J
1-F
V1
V2

- At time = t2, Checkpoint 3 has been justified as shown in the diagram below.
- And checkpoint 7 has been semi justified by V2.
- Eventually at t= t3, checkpoint 3 gets finalized and checkpoint 7 gets justified.



- Now V1 cannot cast a valid vote from its branch as its branch has been left useless by finalization of checkpoint 3.
- Thus the validator set V1 is rendered handicapped from now on and the useful validator set is V2 and its fraction is 1-p.
- Over n such events the fraction of useful sets will be (1-p)^n. Which goes to 0 even if p is very small.
- **Thus this forking scheme will lead to confirmed deadlock**
- Let us move on to forking scheme 2.

Vote from highest(highest justified checkpoint, highest semi-justified checkpoint)

- In this case at time=t2, V1 can shift its voting source from 2 to 3 as both highest justified checkpoint and highest semi-justified checkpoint have the same height. Now V1 can start voting from the right branch and there is no deadlock.
- However, this shift is possible only is there is a valid justification in either of the branch. There is a possibility that there is no justification in either of the branches at height of height(checkpoint 2).
- This can happen if: p>1-SM
- Where SM is supermajority.
- Thus if p>1-SM a permanent fork will occur and neither of the branches will be able to justify any checkpoint in its branch => Deadlock.
- **Thus a confirmed deadlock if p>1-SM**
- This bound may not be strict.