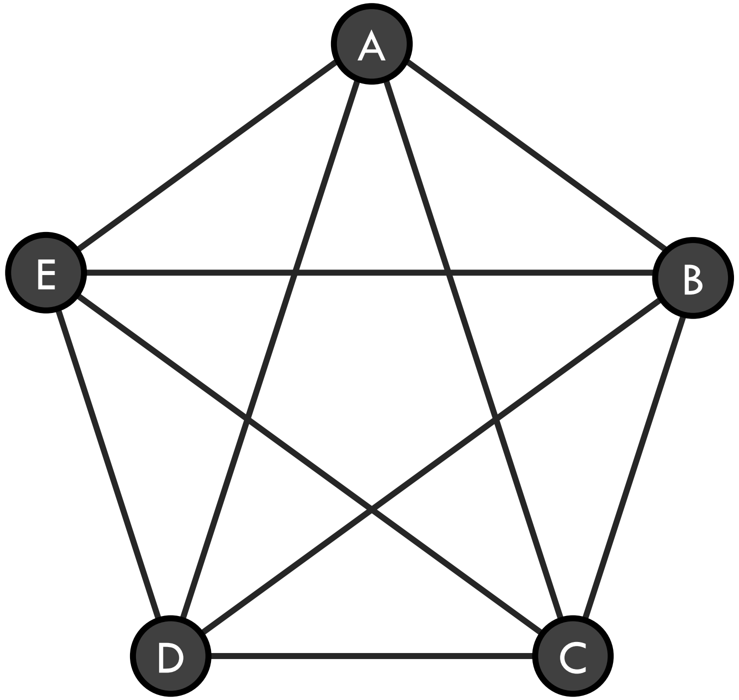
MULTILEVEL VOTING BASED CONSENSUS ALGORITHM FOR PRIVATE BLOCKCHAIN

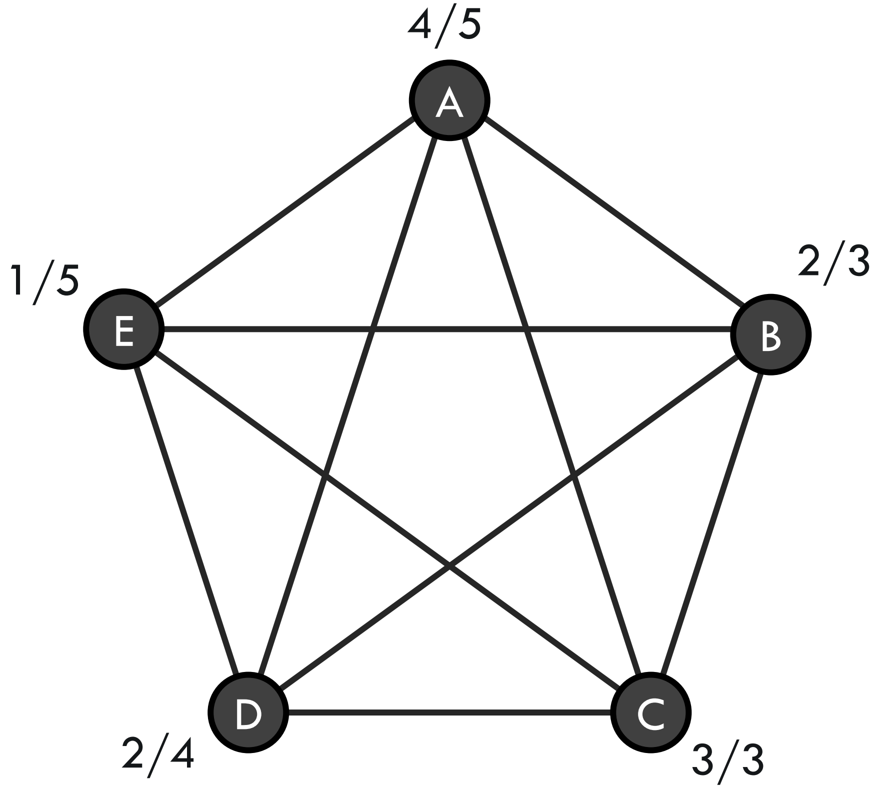
Guided By-
Dr. Kiran Manjappa

Ayush Hemnani – 222IT012
Shubhranshu Dubey – 222IT031

VOTING PROCEDURE



#nodes = 5
#messages exchanged = 5*5
= 25



#nodes = 5
#messages exchanged = 5*5
= 25

- Vote value based on the history of the node.
- Total vote value also changes.

- Total vote = 5
- Vote/node = 1

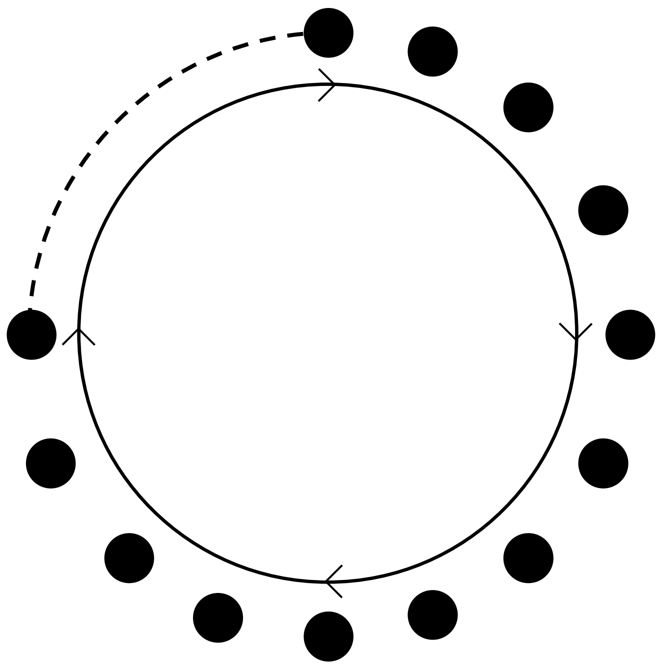
- $hf = history\ factor$
- $d = denominator$

- Total vote(t) = $\sum hf\ *$ LCM(d)
- Votes values = LCM(d) * hf

- LCM = 60
- t = (190/60)*60 = 190
- A = 4/5 * 60 = 48
- B = 2/3 * 60 = 40
- C = 3/3 * 60 = 60
- D = 2/4 * 60 = 30
- E = 1/5 * 60 = 12

UNSUCCESSFUL ELECTIONS

ODD NODES



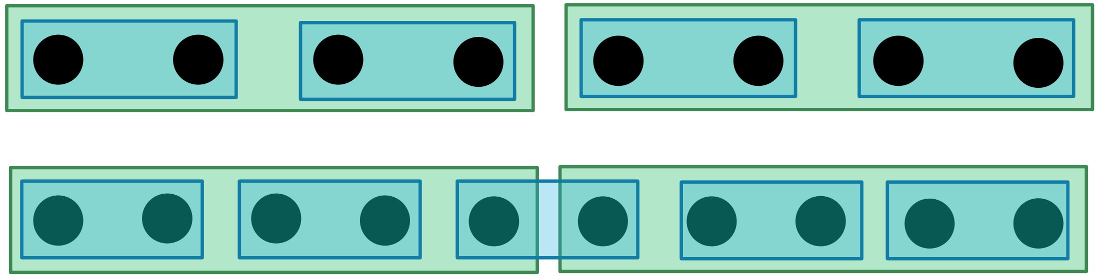
#possible voting = $(n-1)^n$

#possible chains = $(n-1)!$

Unsuccessful Election Probability

$$= \frac{(n-1)!}{(n-1)^n}$$

EVEN NODES



#possible voting = $(n-1)^n$

let a non-trivial factor of n be f_i

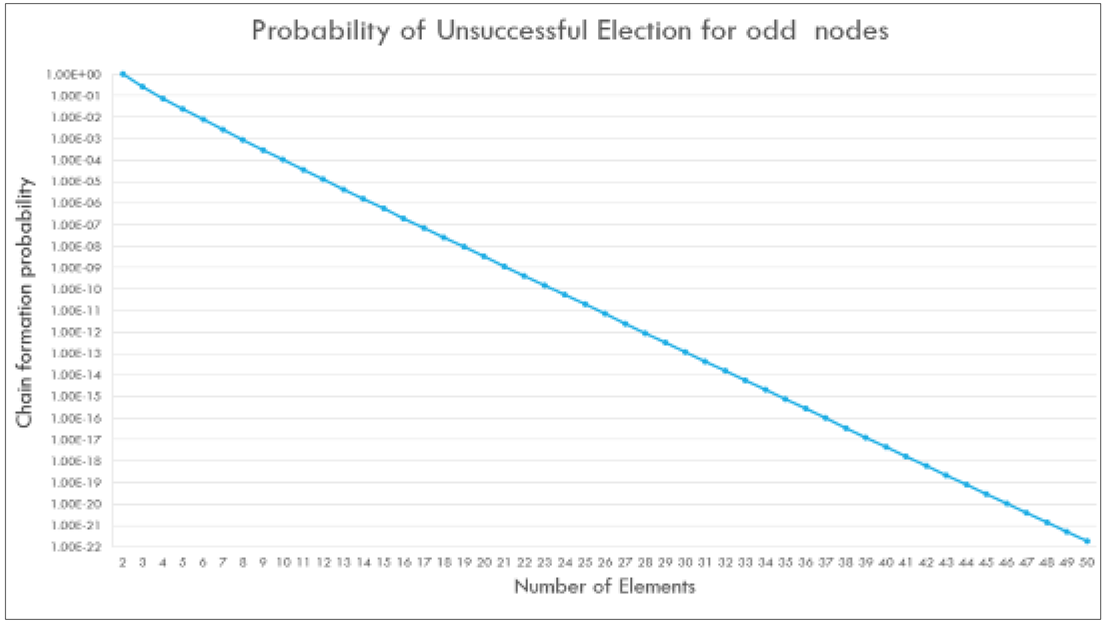
#possible unsuccessful elections =

$$(n-1)! + \sum \frac{(n-1)!}{f_i!} = c$$

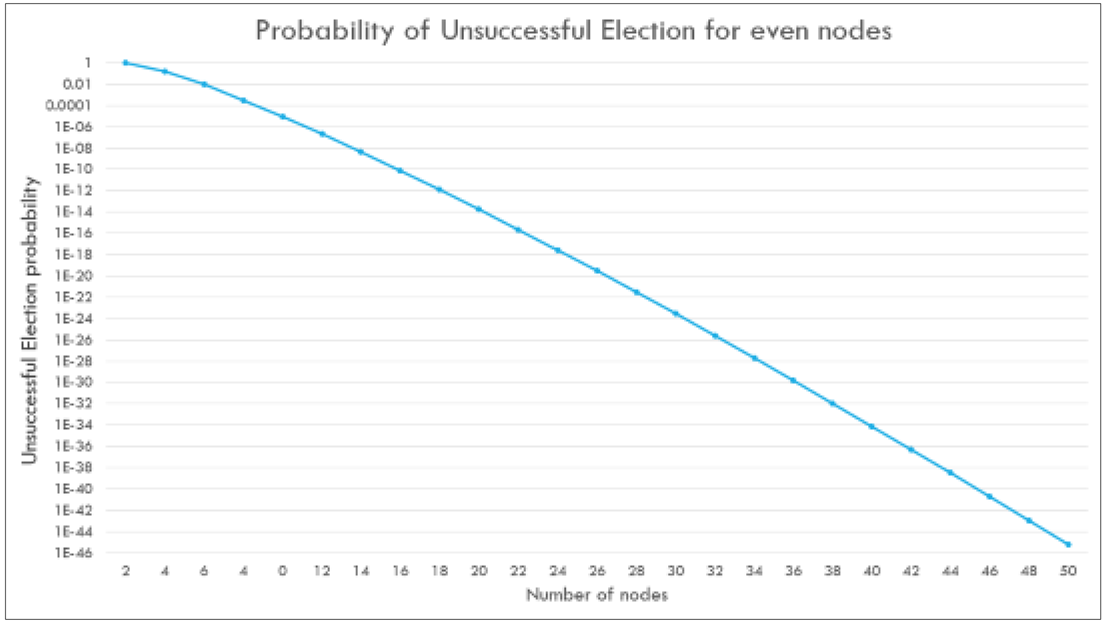
Unsuccessful Election Probability

$$= \frac{c}{(n-1)^n}$$

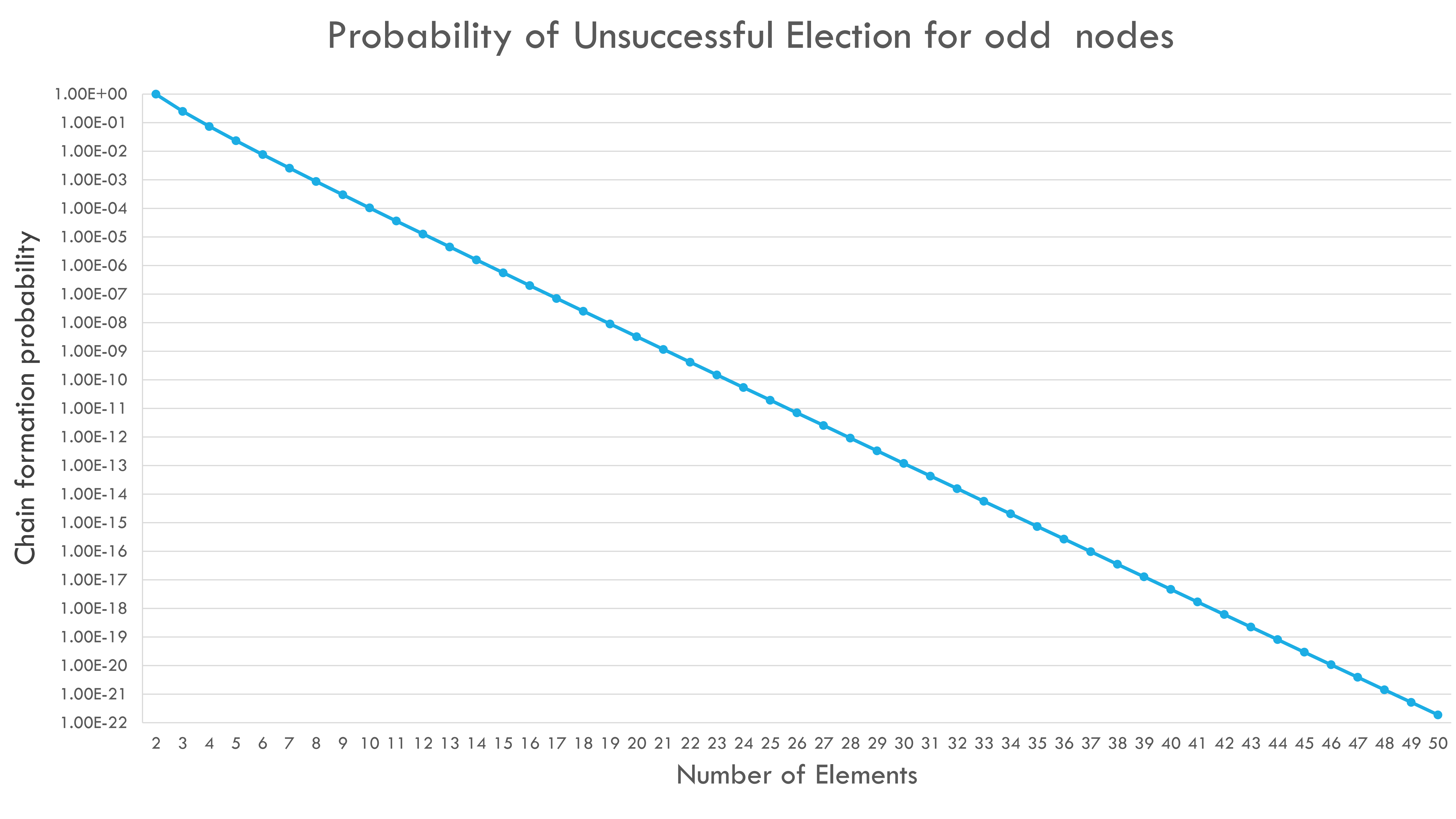
- ➢ BOTH THE PROBABILITIES DECREASES EXPONENTIALLY AS THE NUMBER OF NODES INCREASES.



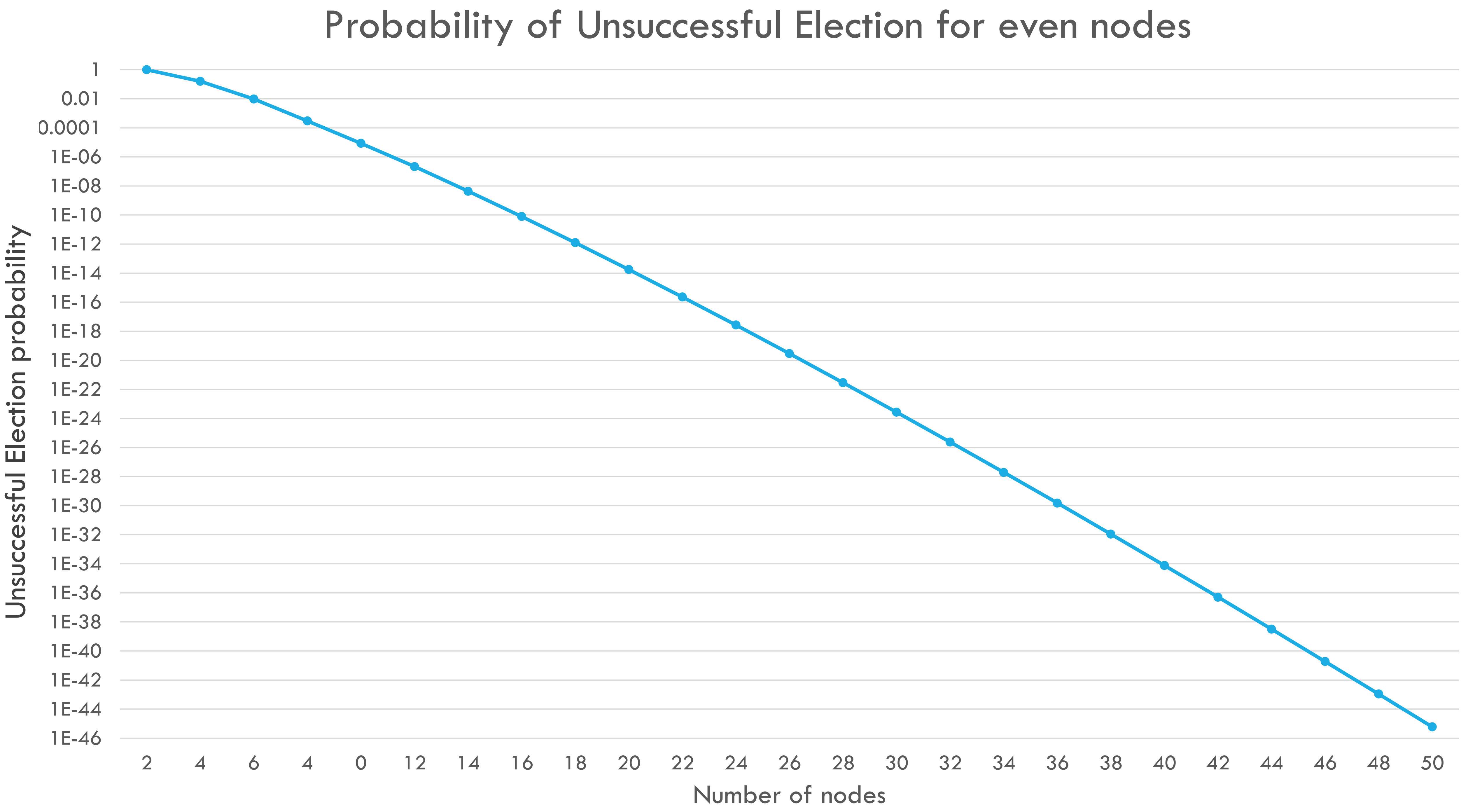
Probability of Unsuccessful Election for odd nodes



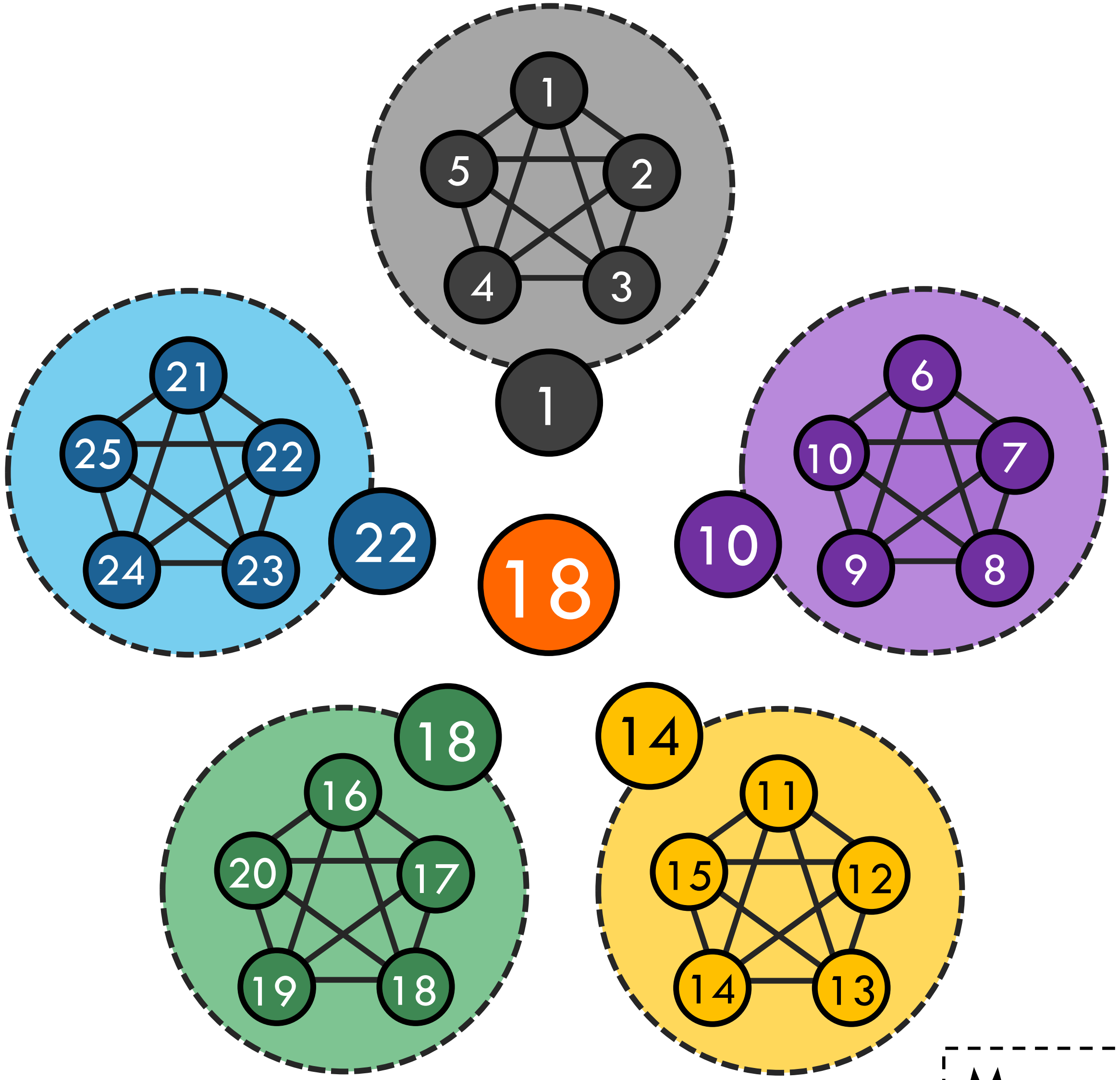
Probability of Unsuccessful Election for even nodes



Probability of Unsuccessful Election for odd nodes
Chain formation probability
1.00E+00
1.00E-01
1.00E-02
1.00E-03
1.00E-04
1.00E-05
1.00E-06
1.00E-07
1.00E-08
1.00E-09
1.00E-10
1.00E-11
1.00E-12
1.00E-13
1.00E-14
1.00E-15
1.00E-16
1.00E-17
1.00E-18
1.00E-19
1.00E-20
1.00E-21
1.00E-22
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
Number of Elements


Probability of Unsuccessful Election for even nodes
Unsuccessful Election probability
1
0.01
0.0001
1E-06
1E-08
1E-10
1E-12
1E-14
1E-16
1E-18
1E-20
1E-22
1E-24
1E-26
1E-28
1E-30
1E-32
1E-34
1E-36
1E-38
1E-40
1E-42
1E-44
1E-46
2 4 6 4 0 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50
Number of nodes

2 LEVEL VOTING



Traditional Election:

#nodes = 25

#messages = 25*25 = 625

2 level Election:

#nodes = 25

#groups = 5

#members/group = 5

#messages/group = 5*5 = 25

#messages at 1st level = 25*5 = 125

#messages by group electives = 5*5 = 25

#total messages = 125 + 25 = 150

Messages reduces by a factor of 625/150 = 4.16667

MESSAGE REDUCTION FACTOR FOR N NODES

Traditional Voting

nodes $= n$

messages $= n^2$

$$f = \frac{n^2}{\mathrm{n}(\sqrt{n}+1)}$$

$$= \frac{\mathrm{n}}{\sqrt{n}+1} = \mathrm{O}(\sqrt{n})$$

2 Level Voting

nodes $= n$

groups $= \sqrt{n}$

nodes/group$= \sqrt{n}$

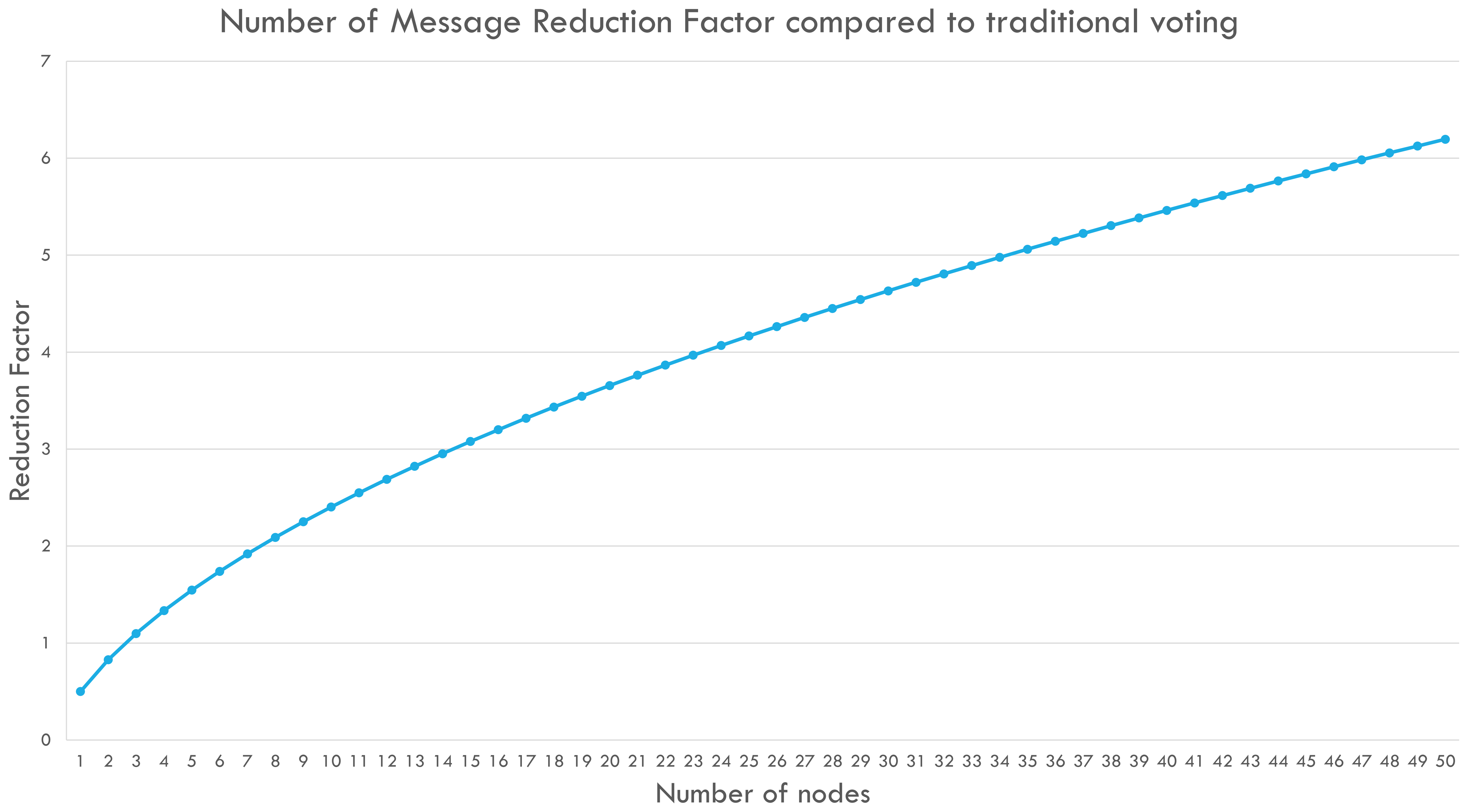
messages/group $=\sqrt{n}^2 = n$

messages within all groups $= \mathrm{n}\sqrt{n}$

messages by group electives $= \sqrt{n}^2 = n$

#total messages $= (n\sqrt{n} + \mathrm{n})$

$= \mathrm{n}(\sqrt{n} + 1)$


Number of Message Reduction Factor compared to traditional voting
Reduction Factor
0
1
2
3
4
5
6
7
Number of nodes
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

FAULT TOLERANCE

A traditional election of n nodes can tolerate $\lfloor n-1 \rfloor/2$ byzantine nodes.

- Let there be n nodes and $m = \sqrt{n}$ groups with each having m nodes.
- At second level there will be m electives from each of the m groups elected from the first level.
- Second level can be considered as a traditional voting mechanism for electives, so we can tolerate at worst $\frac{\lfloor m-1 \rfloor}{2}$ elected byzantine nodes out of m nodes.
- Let us consider all the nodes(m) of these $\frac{\lfloor m-1 \rfloor}{2}$ groups of electives are byzantine, which makes $\frac{m\lfloor m-1 \rfloor}{2}$ nodes byzantine.
- From each of the remaining $\left(m - \frac{\lfloor m-1 \rfloor}{2}\right)$ we can tolerate $\frac{\lfloor m-1 \rfloor}{2}$ nodes, which makes $\left(m - \frac{\lfloor m-1 \rfloor}{2}\right)\left(\frac{\lfloor m-1 \rfloor}{2}\right)$ more byzantine nodes.

$$ft = \left(2m - \frac{\lfloor m-1 \rfloor}{2}\right)\left(\frac{\lfloor m-1 \rfloor}{2}\right)$$

THANKYOU