Byzantine Generals walk into a Quantum Bar

Distributing the Power of Qubits

Chandrashekar Radhakrishnan
https://sites.google.com/view/chandrashekar/

Olivier Marin
https://wp.nyu.edu/omarin/

This work is an ongoing collaboration; read more at https://arxiv.org/abs/2411.04629

What This Talk is About

Quantum Computing
Qubits
Superposition
Entanglement

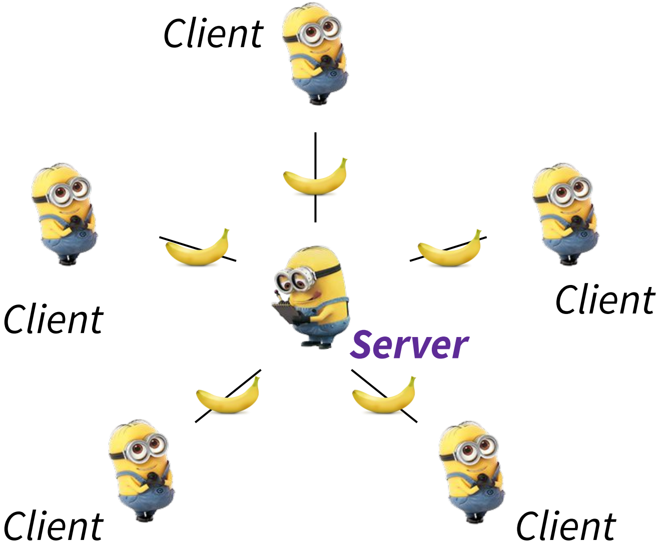
???

Distributed Computing
Scalability
Consensus
Asynchrony

=> Distributed Quantum Computing! <=

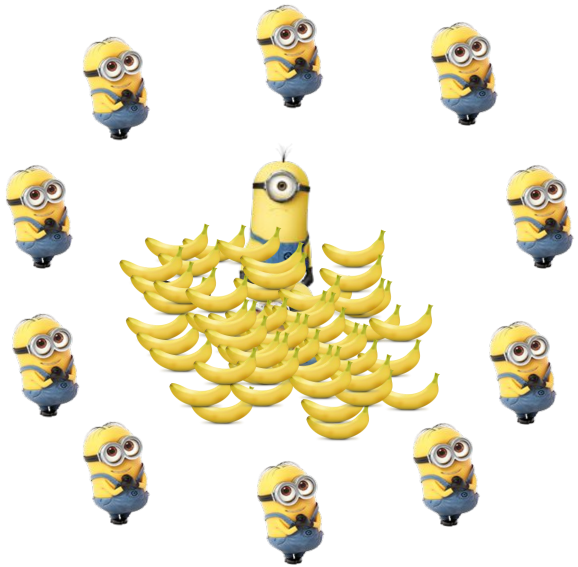
Centralized Computing System

Centralized computational tools work on a limited scale



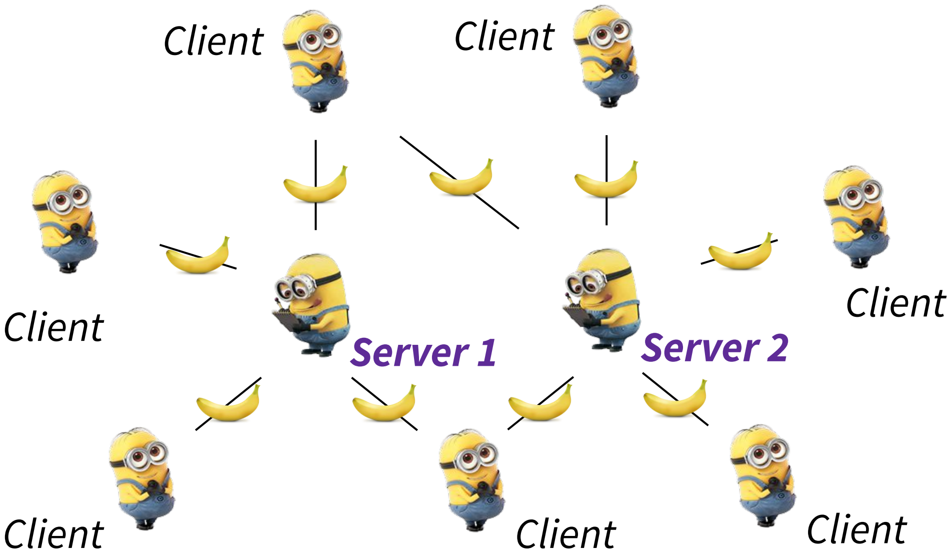
Centralized Computing System

Billions of digital transactions every day



Distributed Computing

Distributing the computation is a way of applying "brute" force to scale up



Powers many fields of science, eg. ML ([federated learning]()), Neuroscience ([brainlife.io]())

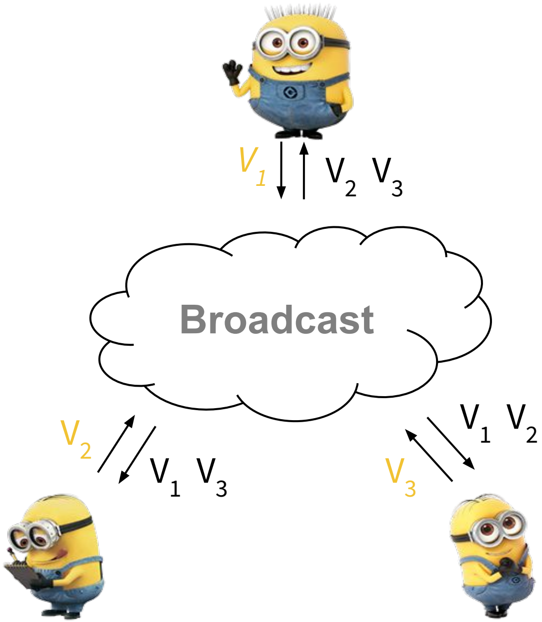
Consensus

Everyone pitches in towards the common computation

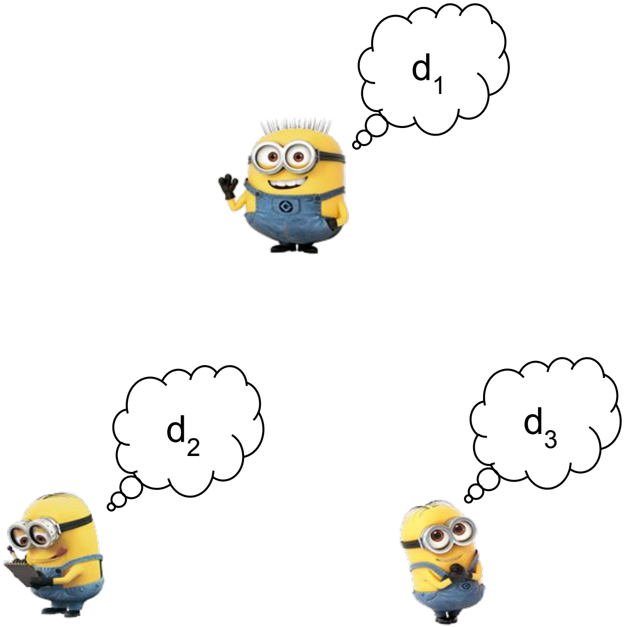
Computer nodes agree on:

- the input each node processes
- the common output

Anatomy of a Consensus



Step 1: Propose



Step 2: Decide

Properties of a Consensus

Agreement

D is the same for all servers

Termination

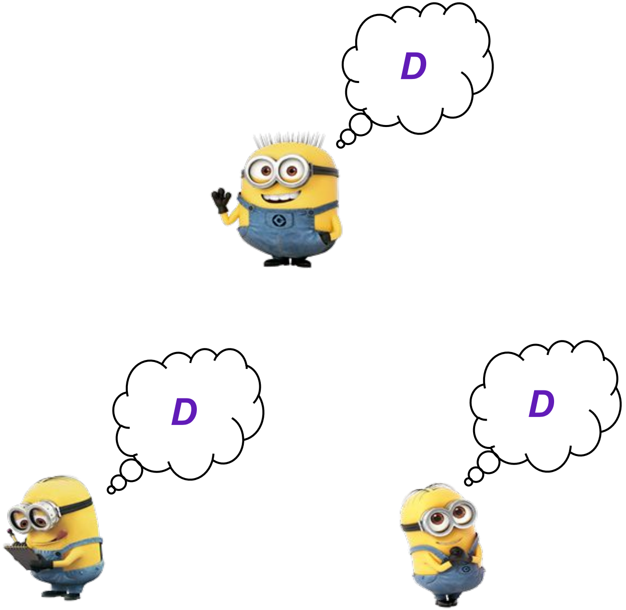
All servers eventually decide on a result ***D***

Validity

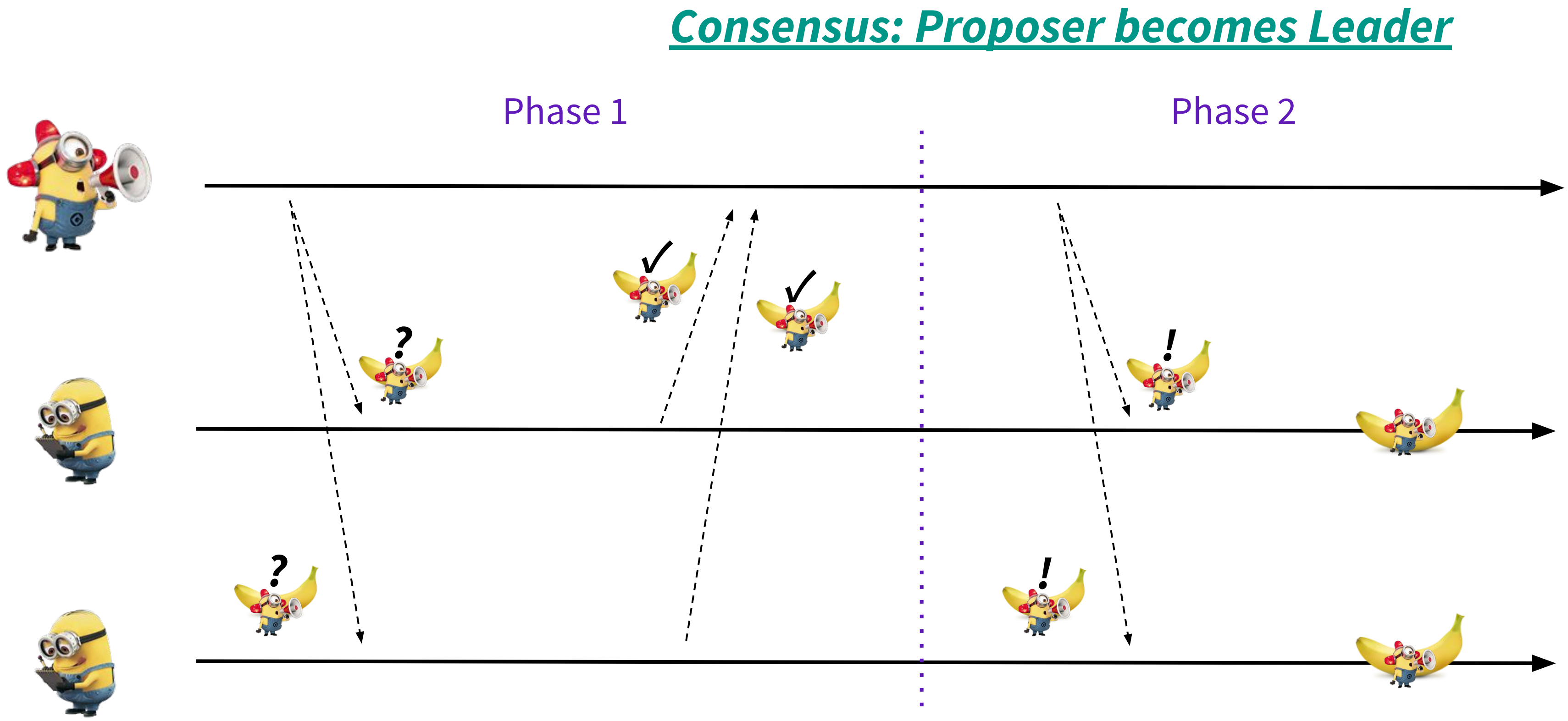
D is a proposed value

Integrity

Once a server decides ***D***, it cannot switch to ***D'***

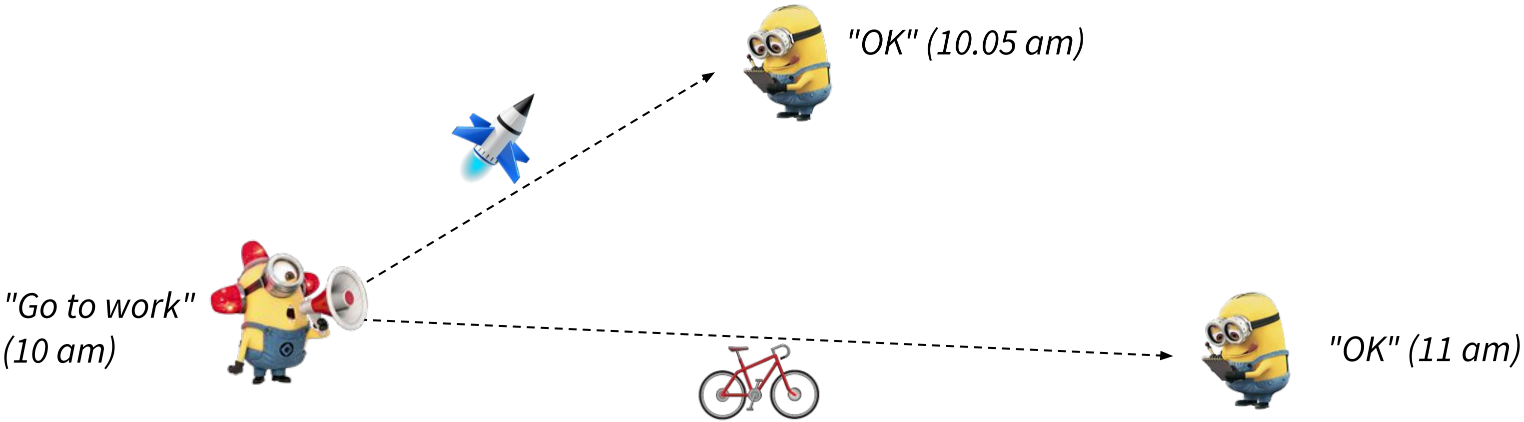


Leader Election



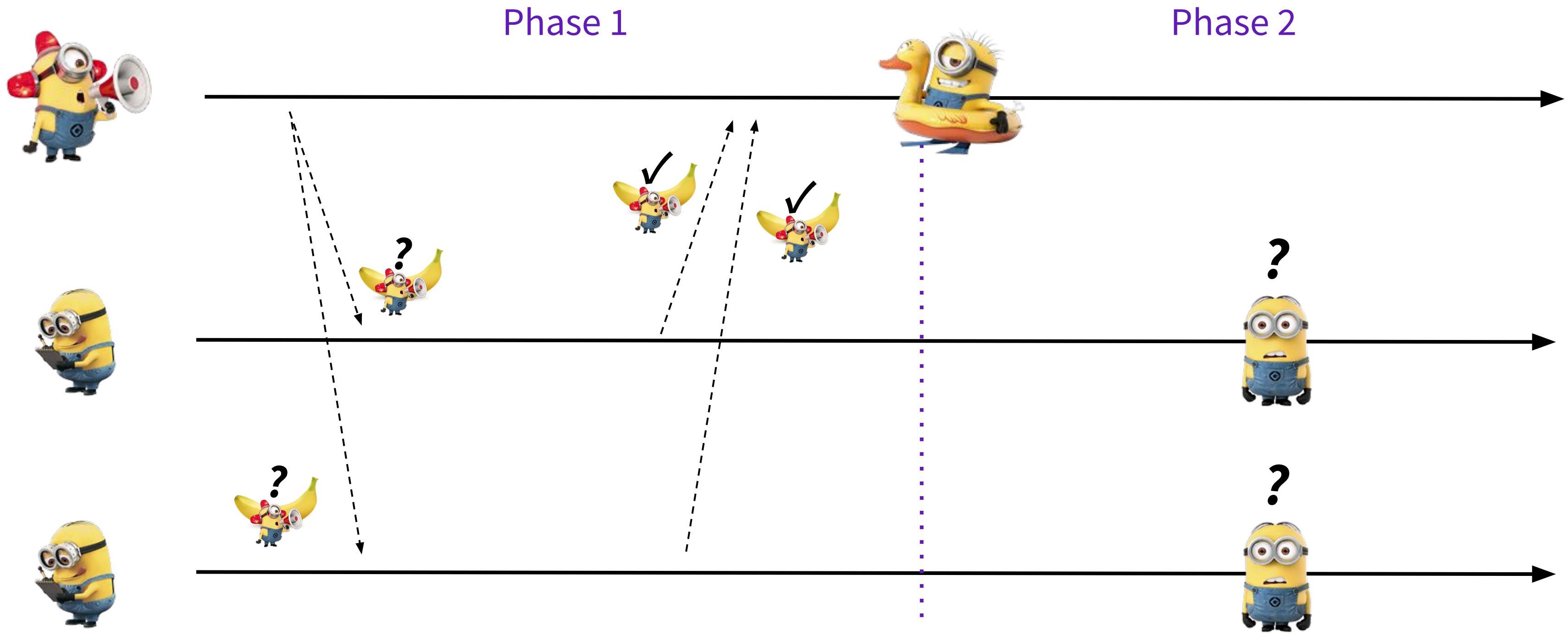
Time is Relative!

Message transfer introduces delays (latency)
Every communication channel incurs a different latency that changes over time
Consensus: *Termination affected by the slowest server!*



Leader Election

Proposer crashes - Consensus?

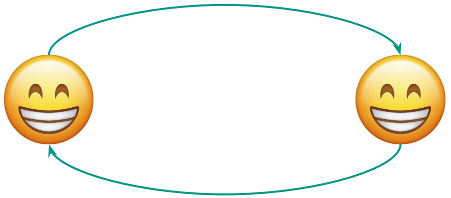


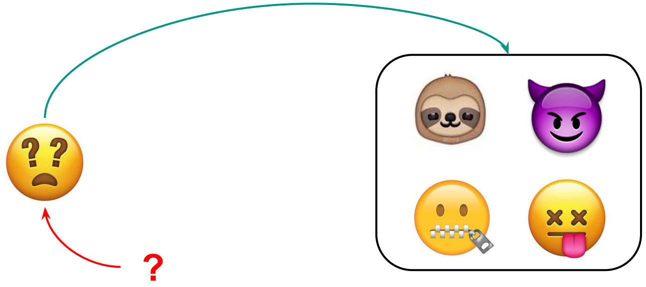
The Internet Can't Exist: Here's Why!

Scaling paradox

1. Probability of failures increases with the number of nodes
2. Dead nodes can bring down the entire system

FLP85: Theoretical proof that two nodes may never reach consensus





Can quantum computing break this impossibility?

Proof of concept: Quantum Leader Election

Quantum Computing 101: The Qubit

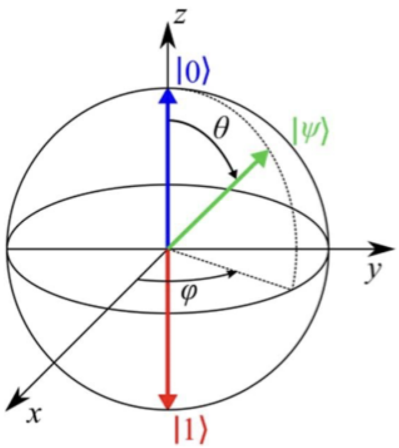
Classical bit (binary integer):

State can be 0 or 1

Qubit (quantum bit):

State can be 0, 1, or a *superposition* of both

$\alpha|0\rangle+\beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2+|\beta|^2=1$



Quantum Magic #1: Superposition

Superposition enables *processing multiple states at once!*

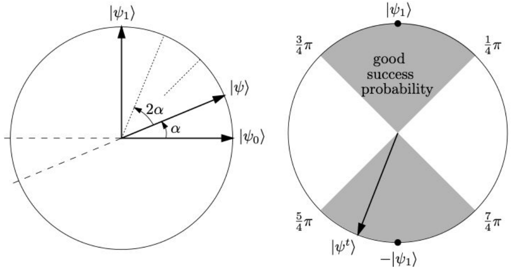
$(|0\rangle + |1\rangle)/\sqrt{2}$ =>

$|\alpha|^2 = 0.5$

$|\beta|^2 = 0.5$

Quantum gates allow to impose rules on the outcome of the measurement

$(|0\rangle + |1\rangle)/\sqrt{2}$



source: Spalek, R. (2006). Quantum Algorithms, Lower Bounds, and Time-Space Tradeoffs. Amsterdam: ILLC.

$1/2|0\rangle + \sqrt{3}/2|1\rangle$

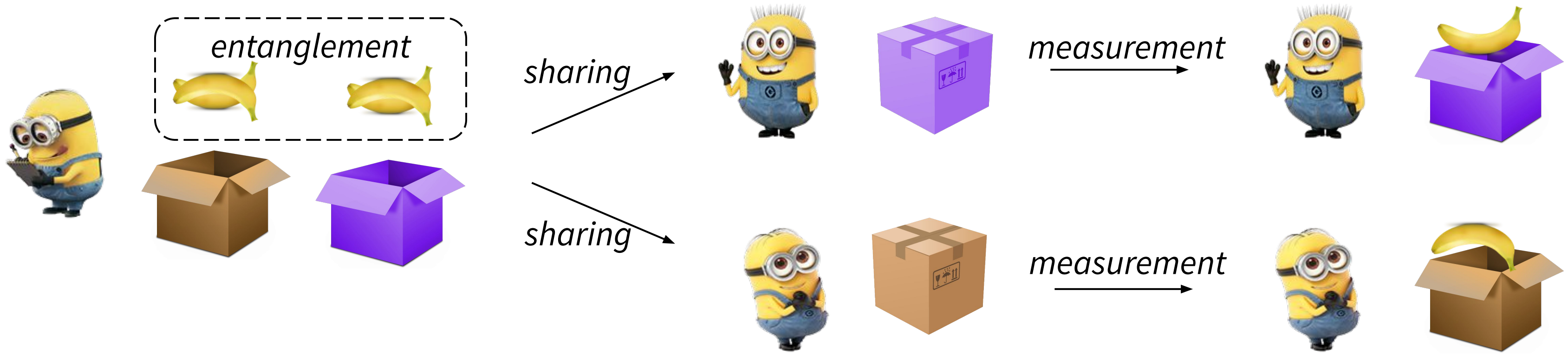
$|\alpha|^2 = 0.25$

$|\beta|^2 = 0.75$

Quantum Magic #2: Entanglement

Entanglement links qubits

- Even at a distance!
- Measuring one instantly determines the state of the other
- => synchronized states across separate quantum processors



Quantum Advantage

Grover's Algorithm (1997)

Given: Oracle access to a black-box function $f: \{0,1\}^n \rightarrow \{0,1\}$

Goal: Output a marked input x such that $f(x) = 1$, if one exists

(*Application example*: break a secret code by guessing it…)

Classical algorithms need $\Omega(2^n)$ queries solve

Grover's Algorithm does it with $O(\sqrt{(2^n)})$ queries

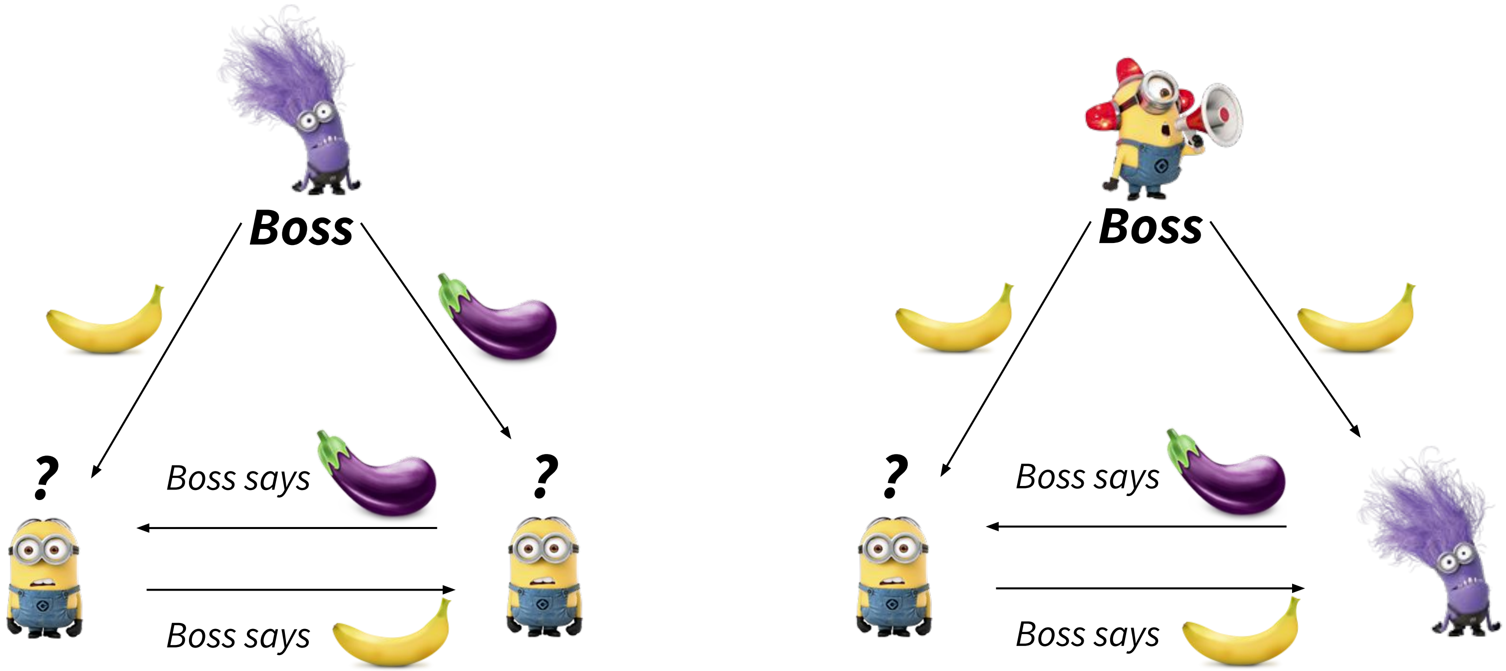
Quadratic speedup

1 billion seconds ≈ 31.7 years

√(1 billion) seconds ≈ 9 hours

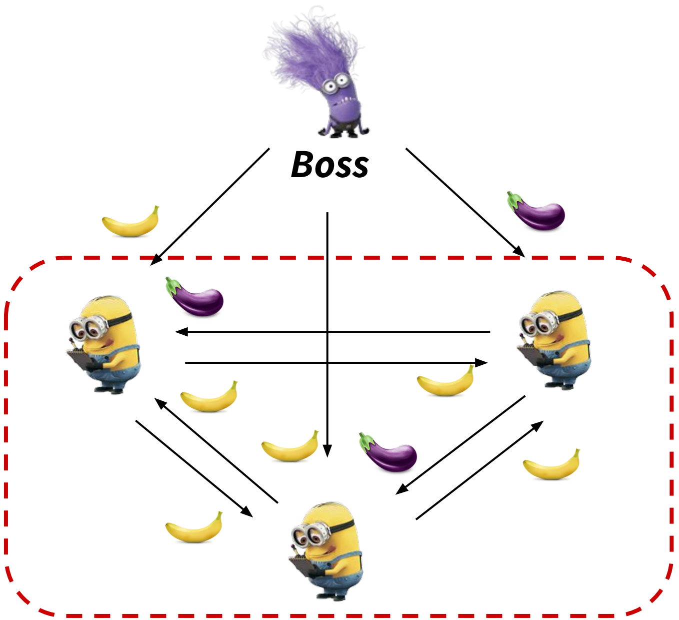
Consensus with byzantine failures

Impossibility: solving byzantine generals with 3 processes

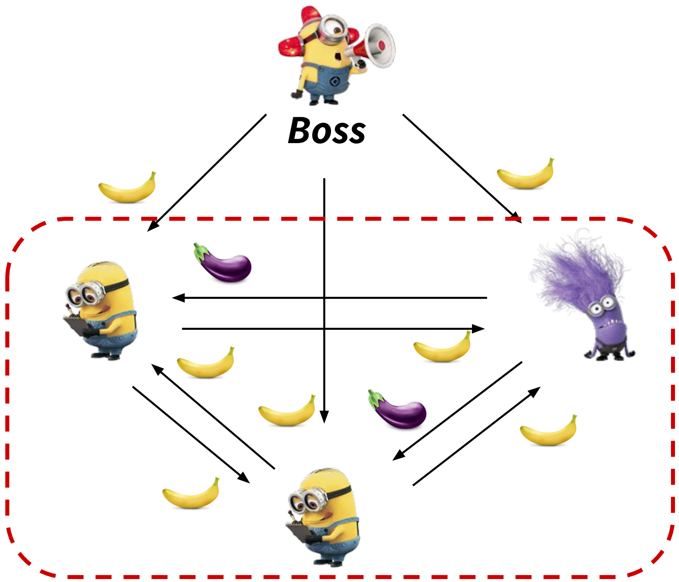


Consensus with byzantine failures

4-process solution for byzantine generals

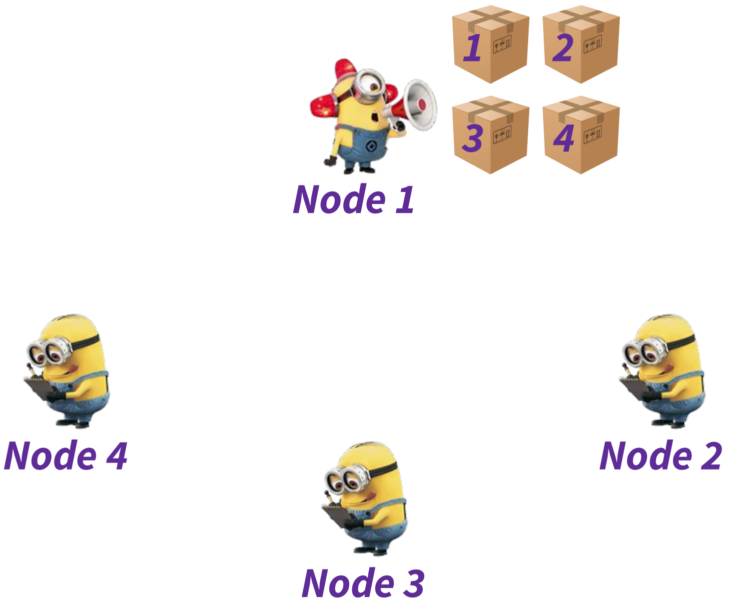


number of messages = N^2!



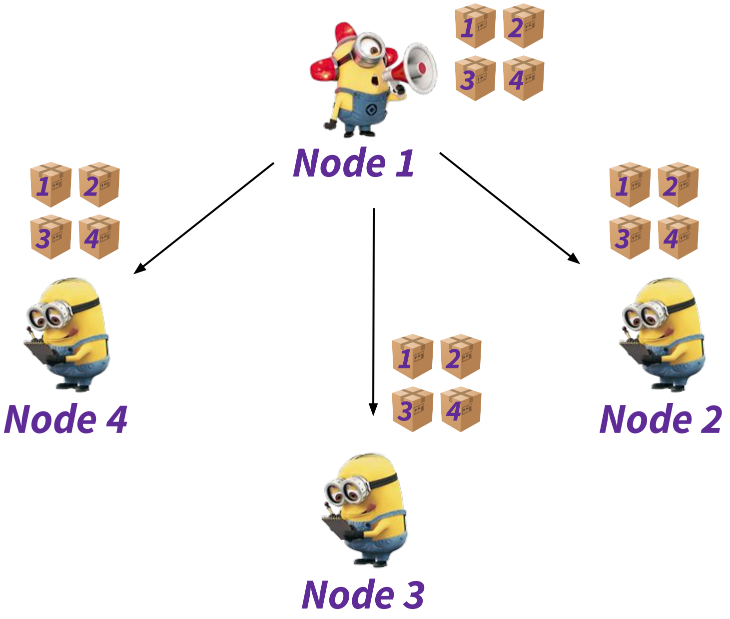
Quantum Leader Election: Step 1

Leader prepares a set of shared quantum states



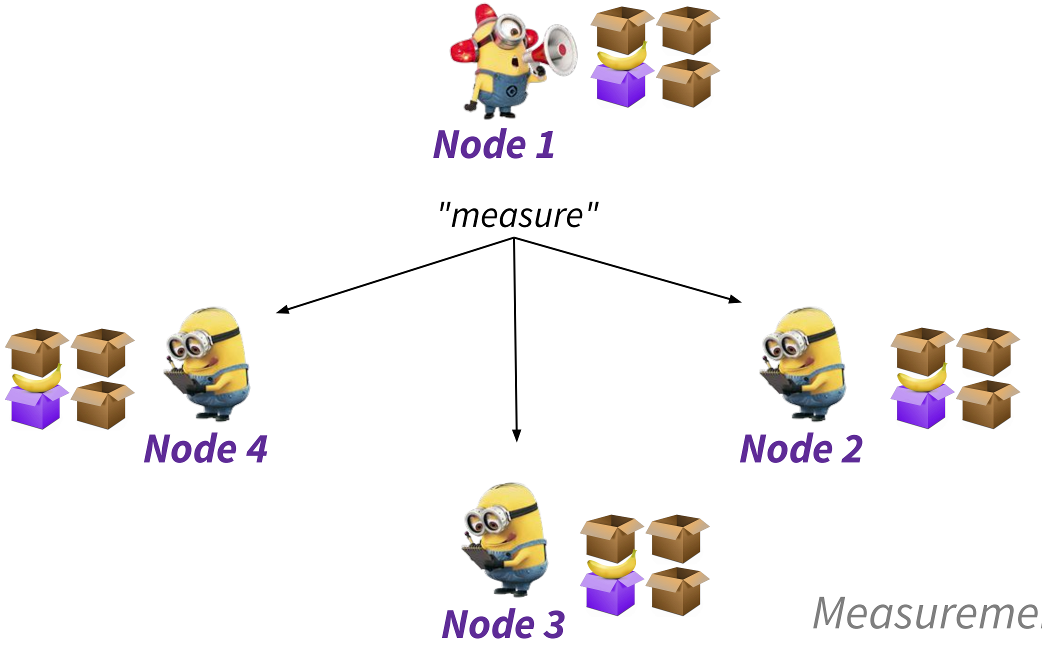
Quantum Leader Election: Step 2

Leader sends an entangled set to each node



Quantum Leader Election: Step 3

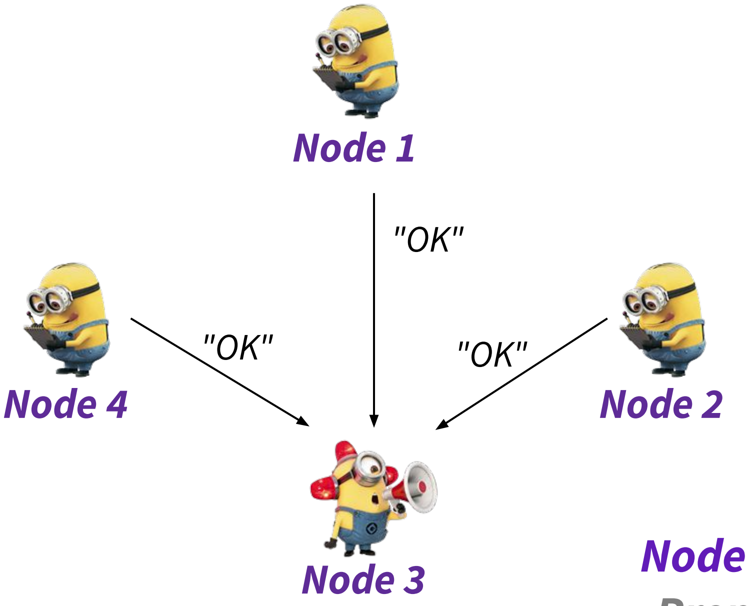
Leader triggers the measurement of the sets on each node



Measurement **=> Node 3 is the new leader**

Quantum Leader Election: Step 4

All nodes acknowledge the new leader



***Node 3* jumps back to step 1**
Prepares the next election

The Strengths and Limits of Entanglement

Entanglement does eliminate delays in the quantum world

- Traditional algorithms for consensus can be very slow and costly
- There is room for significant performance improvements

But *only* in the quantum world

Nodes still need to coordinate through classical channels

- Decide when to measure
- Acknowledge the measurement results to move on

Takeaway points

There is a lot to gain with Distributed Quantum Computing!

Entanglement does make a difference

Message complexity of traditional Leader Elections is O(N^2)

Our Quantum Leader Election algorithm reduces it to O(N)

But the impossibility theorem still stands!

Failures are… ***inevitable***!