Byzantine Fault Tolerance

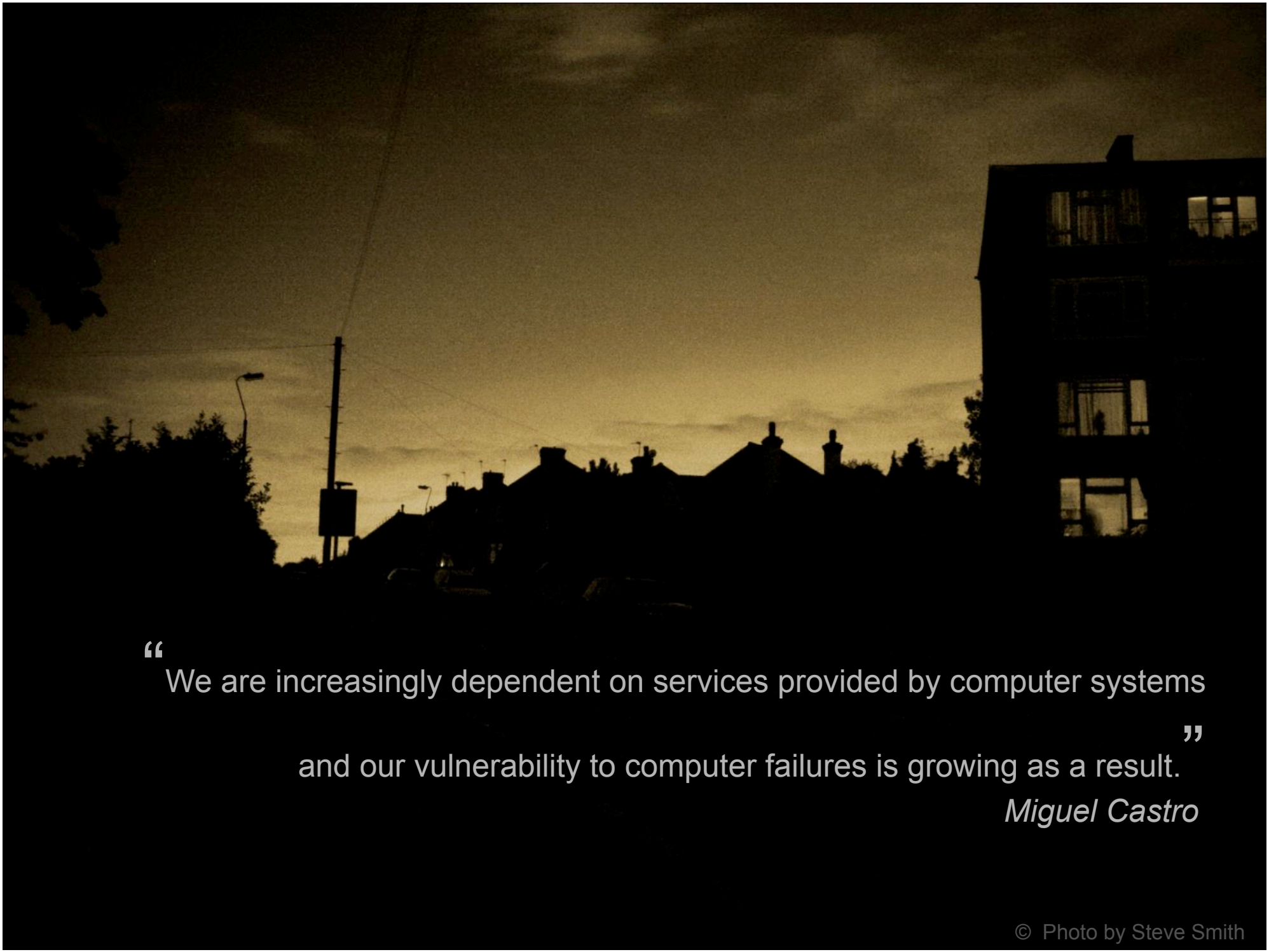
© Photo by James Case (Flickr)

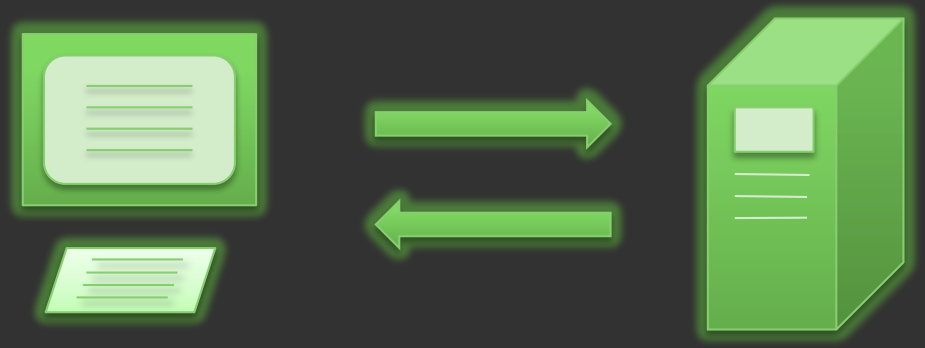
The Swiss Army Knife to hacks and crashes?

XtreemOS
Enabling Linux for the Grid

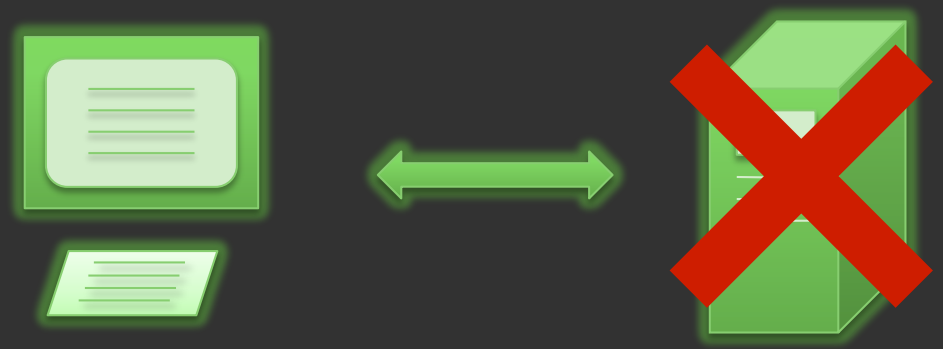
LGFG

Christian Spann
Ulm University

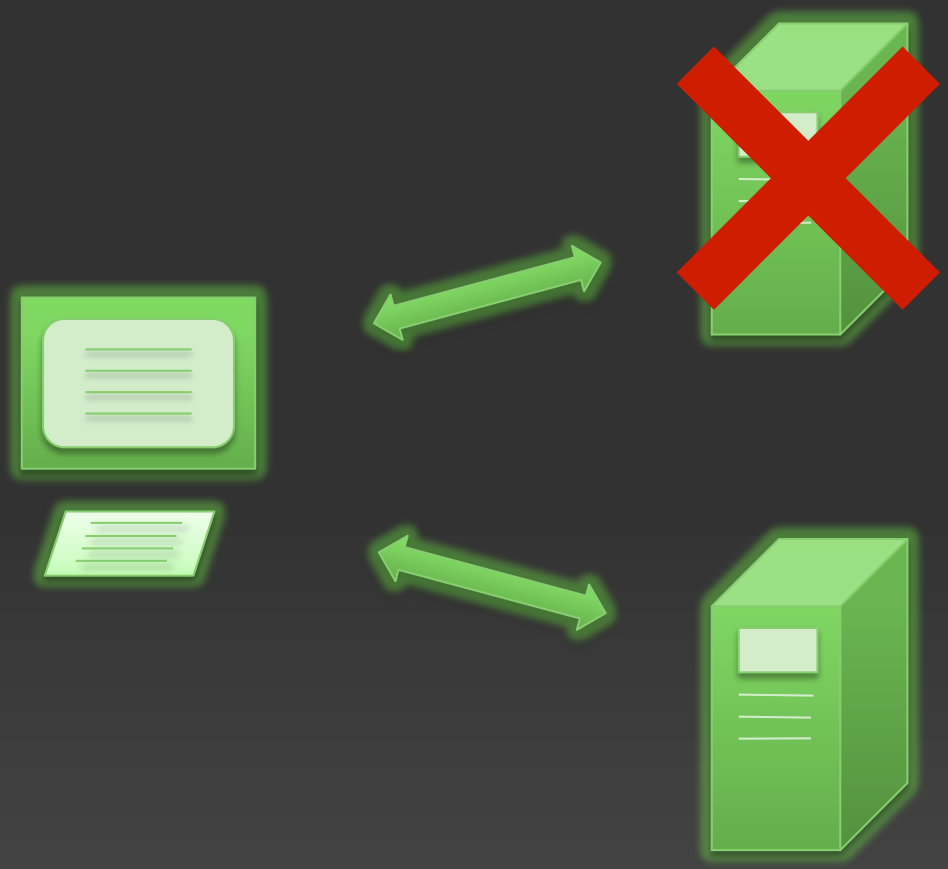

“We are increasingly dependent on services provided by computer systems and our vulnerability to computer failures is growing as a result.”
Miguel Castro
© Photo by Steve Smith



Request / Reply

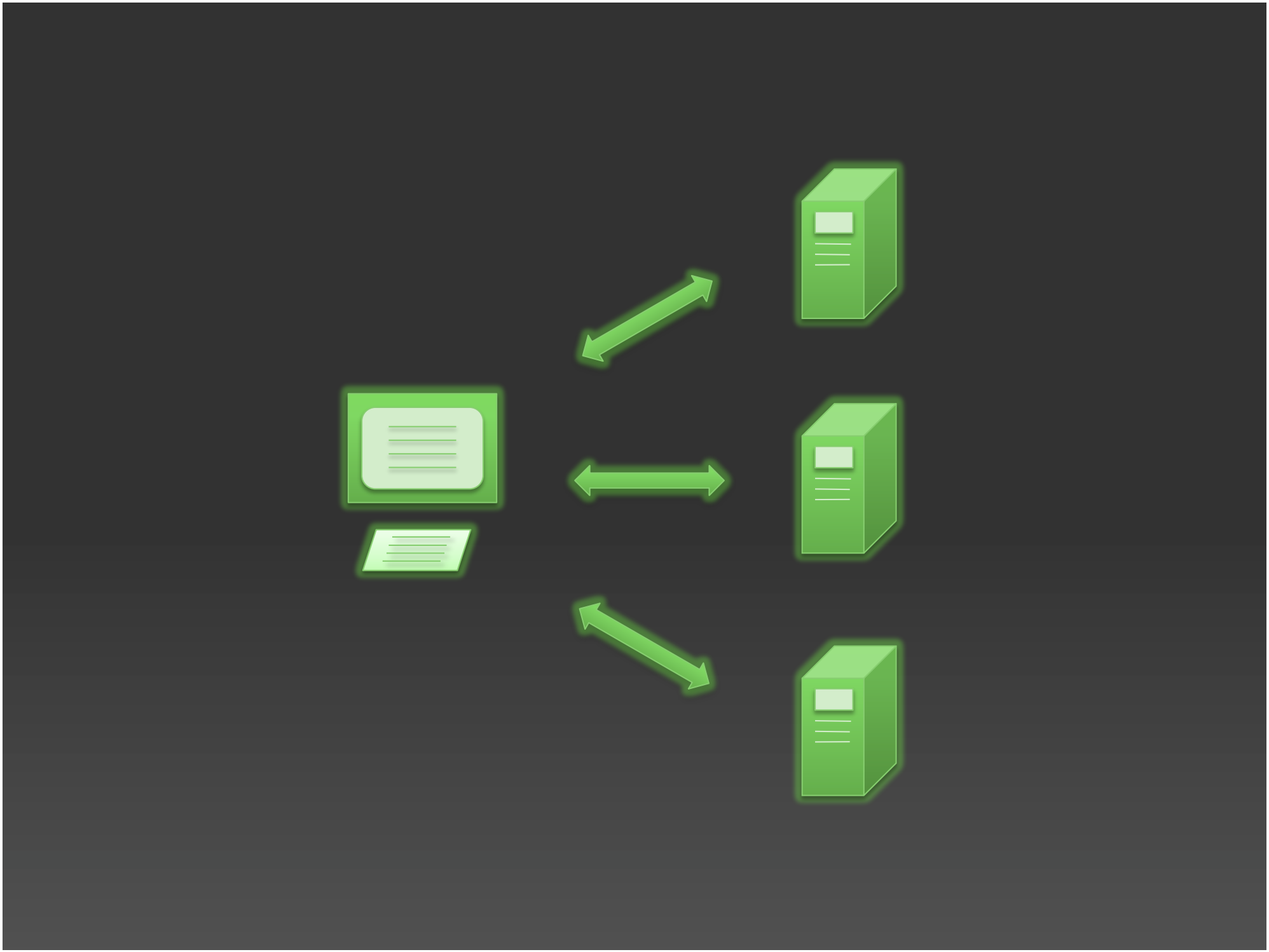


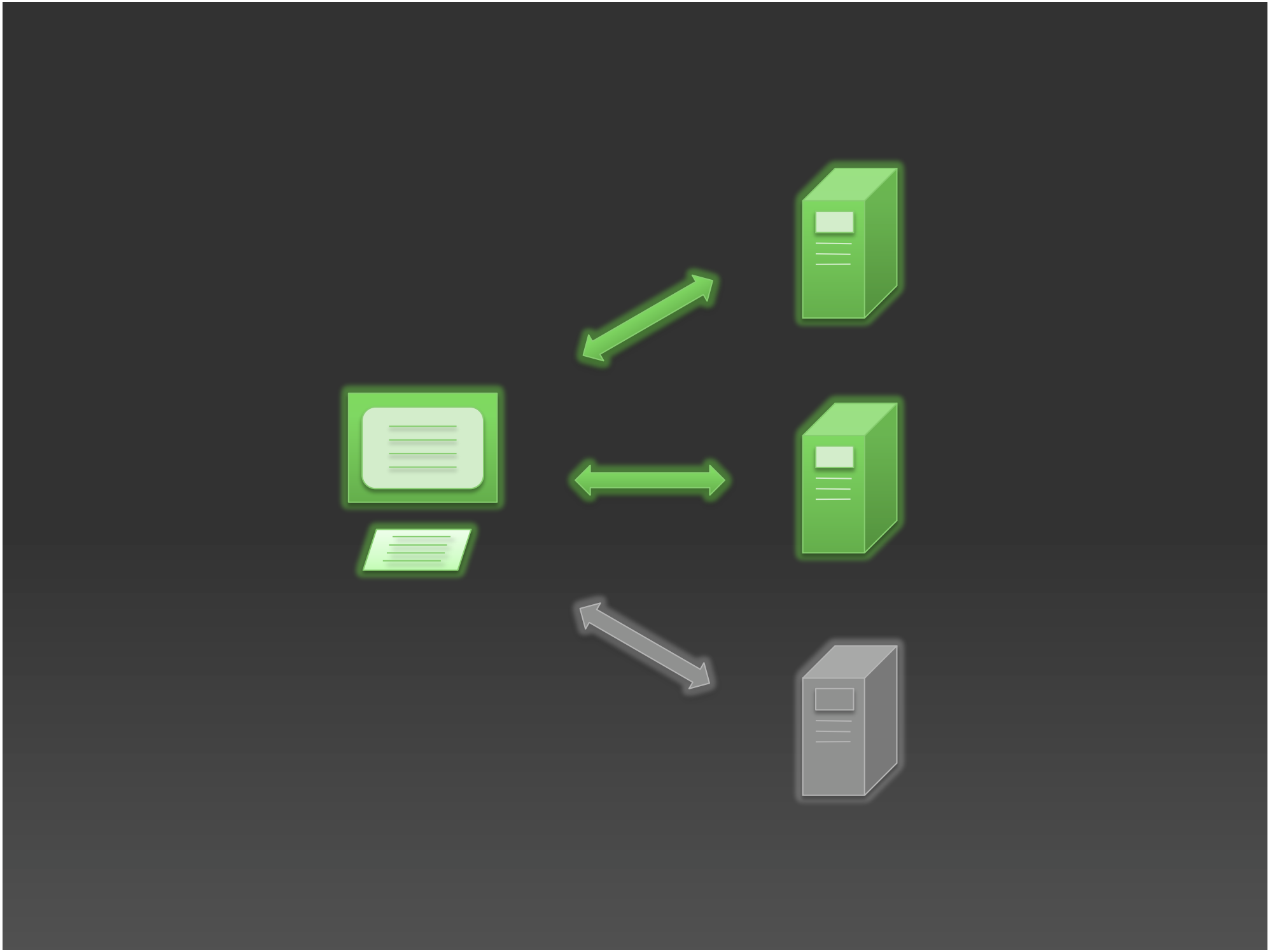
Failure

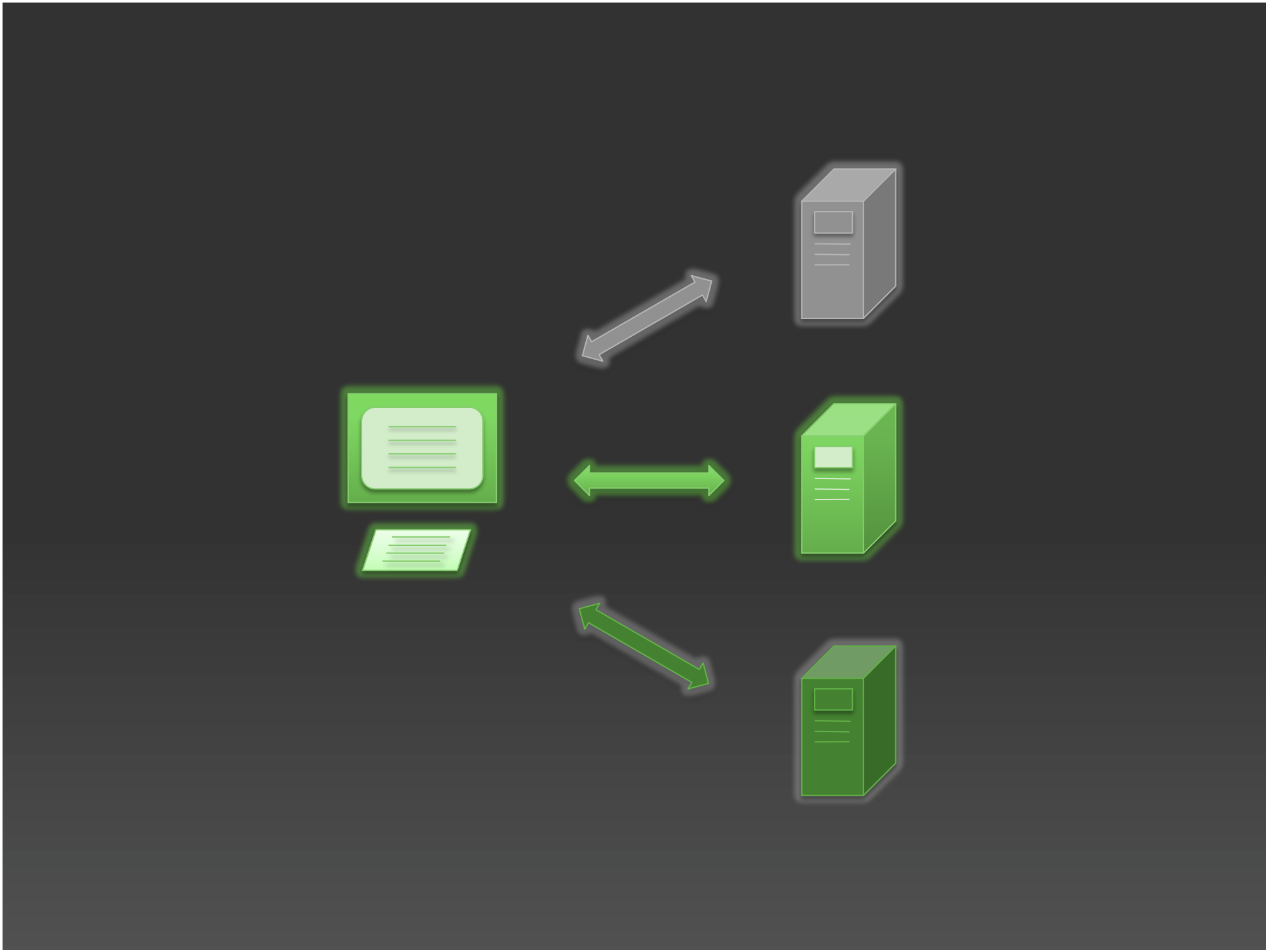


The Network
is unreliable!

© Photo by William Grootonk on Flickr





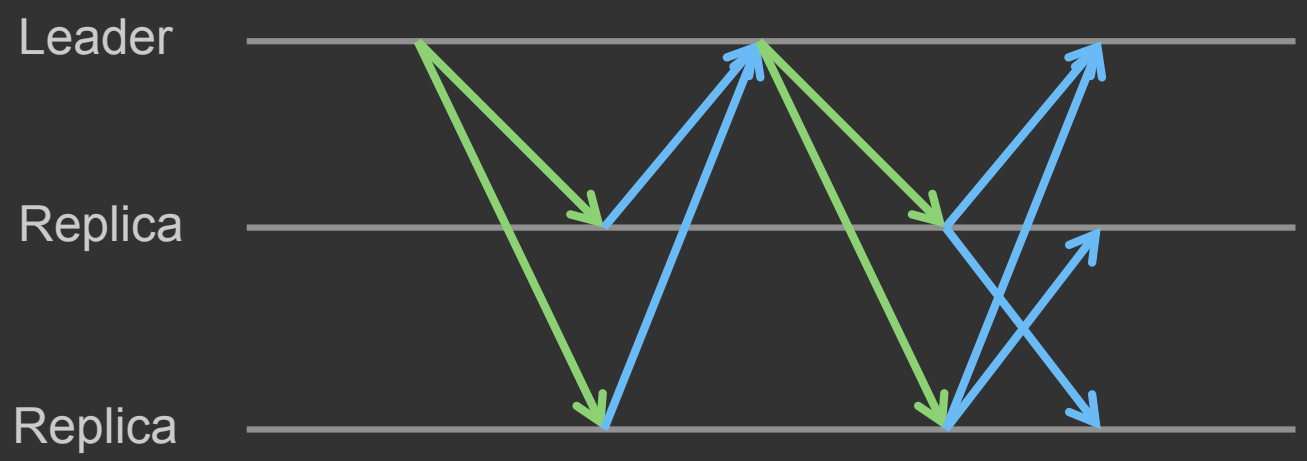


Conclusion

- 2 f + 1 Replicas
- Can cope with max f benign failures
- Inconsistent states possible
- But can be fixed

Paxos Algorithm by L. Lamport

“A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable”



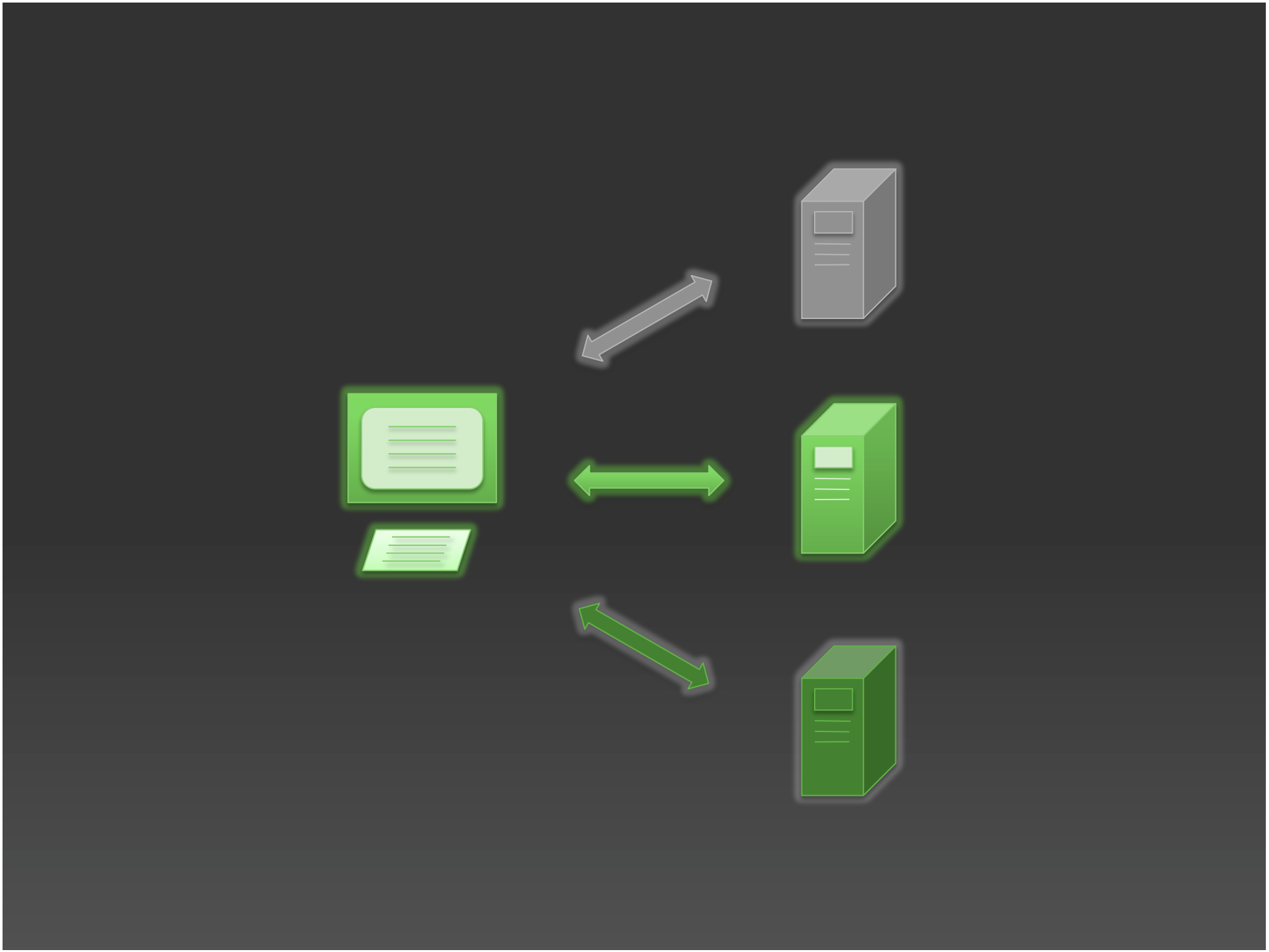
Paxos visualised

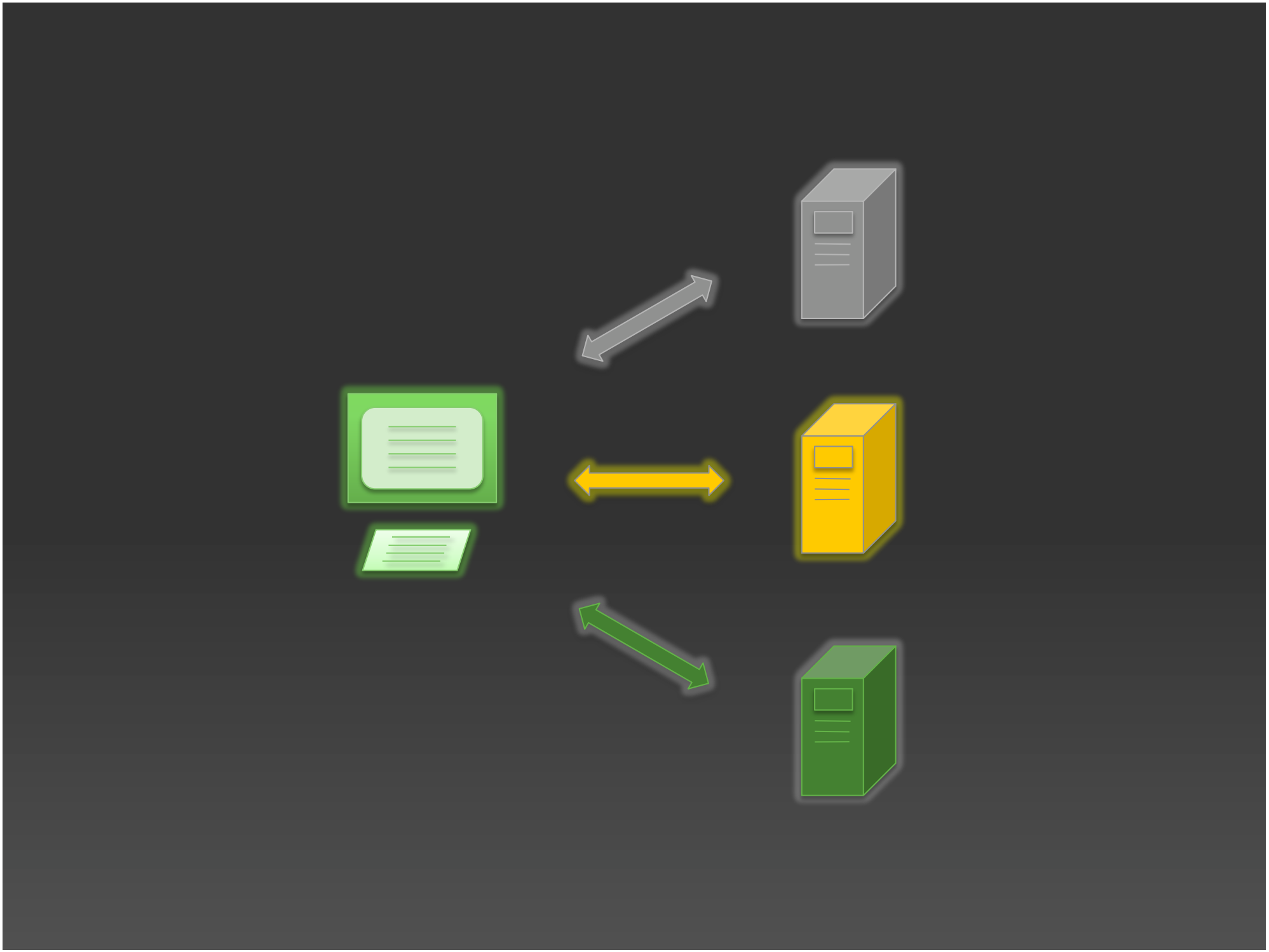
Sometimes
something is wrong

The Byzantine Generals Problem

We only trust the Mailsystem

© Photo by Dani Sardà i Lizaran on Flickr





The Byzantine Generals Problem

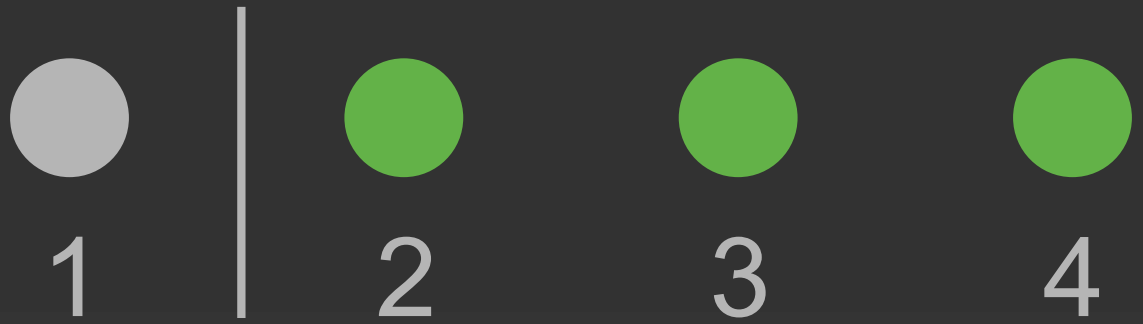
Can only be solved with a majority of 2/3 of correct nodes!

Why?

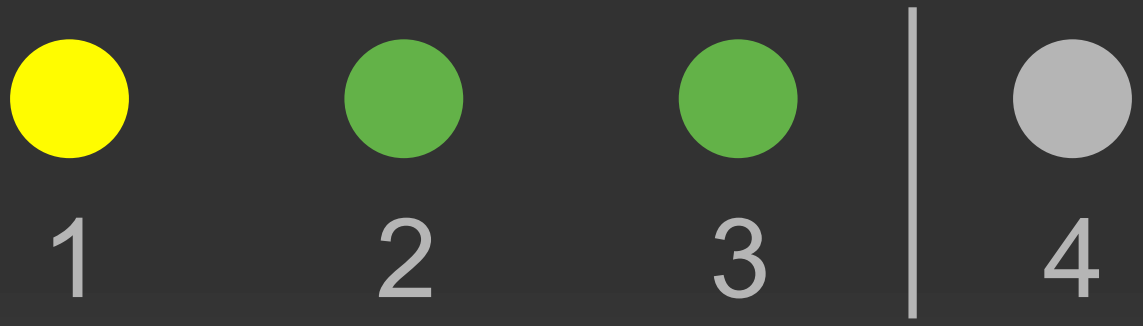
Byzantine Agreement

Replicated service with
read/write operations on a variable

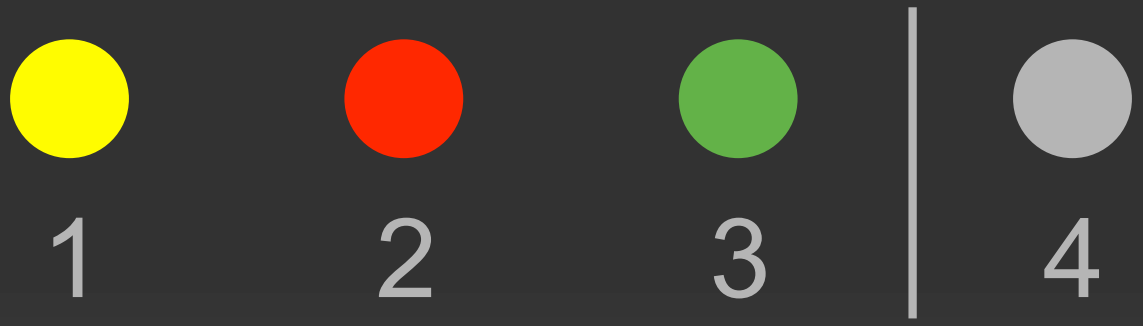
Byzantine Agreement



Byzantine Agreement

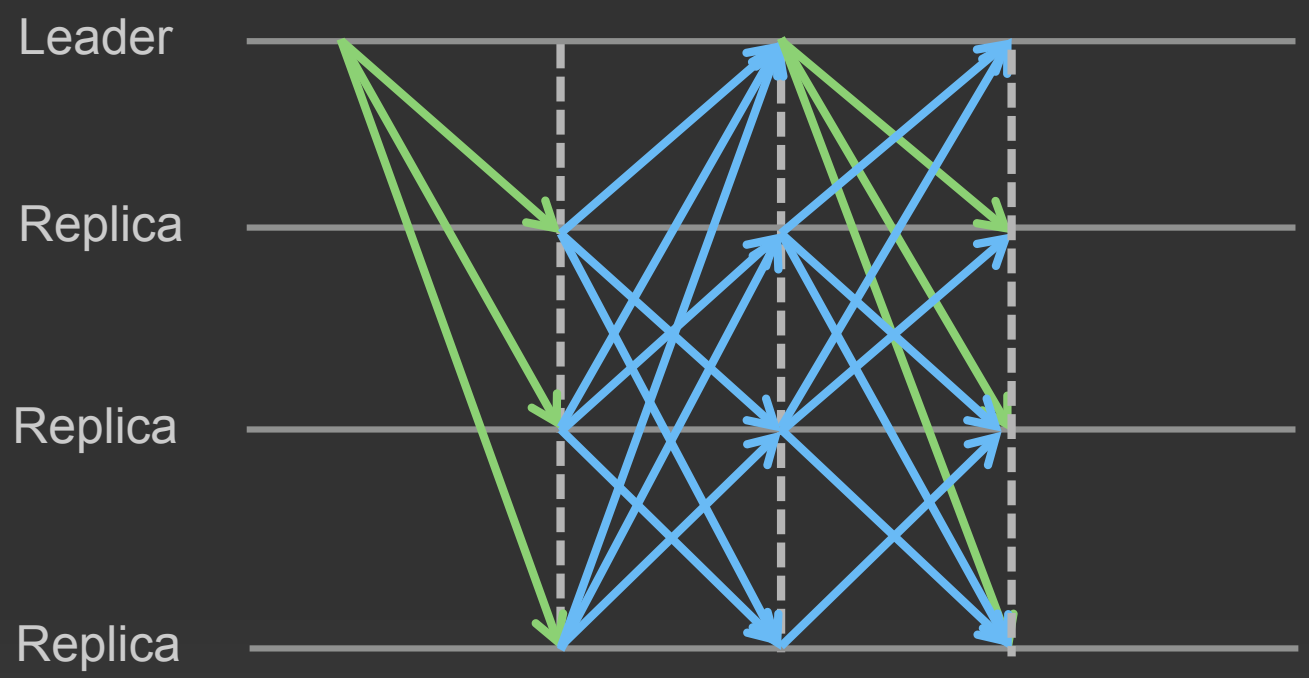


Byzantine Agreement



PBFT by Castro und Liskov

- Leader – Backup algorithm
- Mutual Authentication
- 3 phase commit protocol
- Leader proposes ordering of requests
- Backups validate that leader is correct



BFT visualised

More facts on PBFT

- View Change – protocol for leader election
- Optimized through MACs
- Proactive recovery (PBFT)

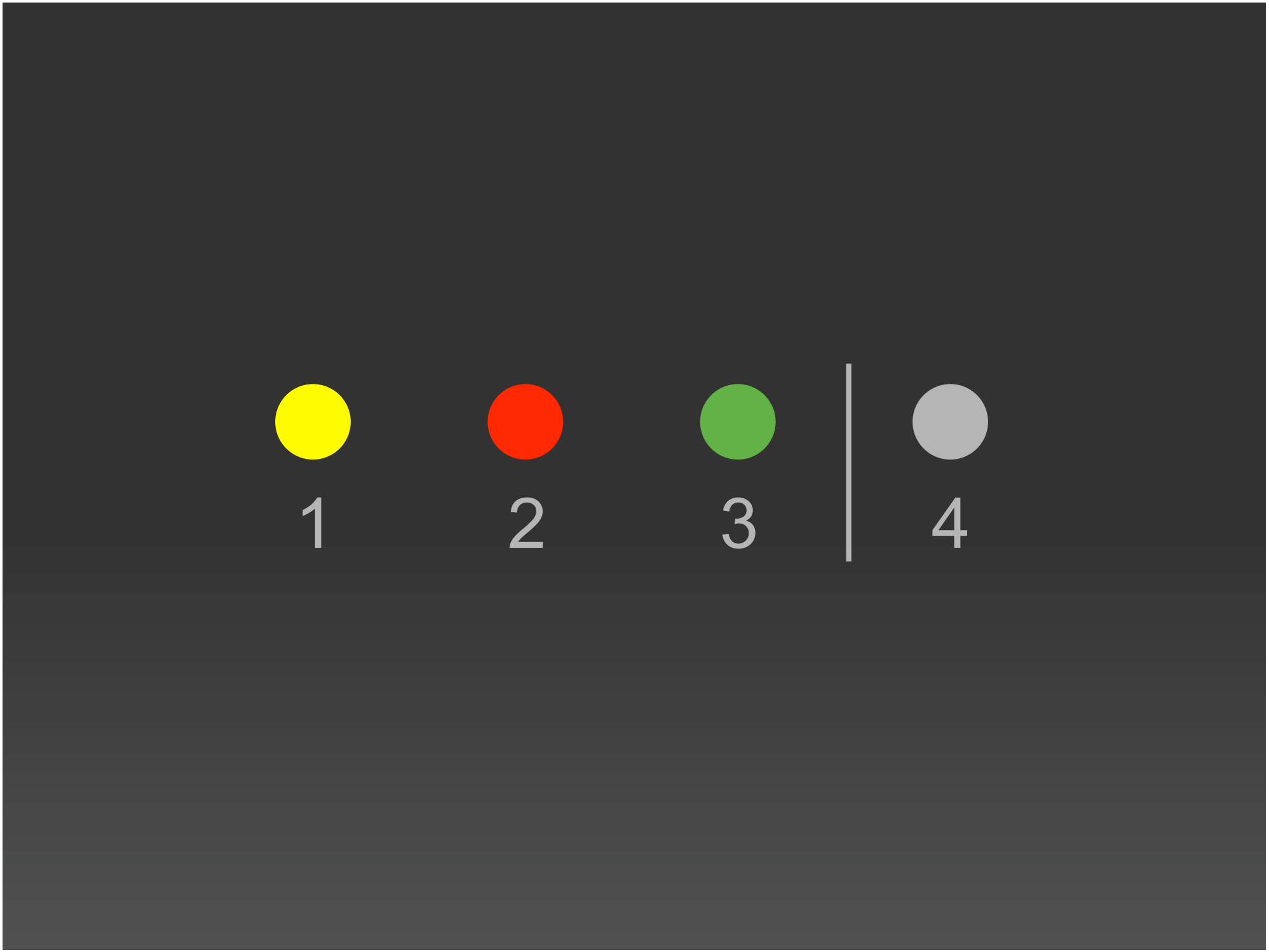
Still we need

3 Steps!

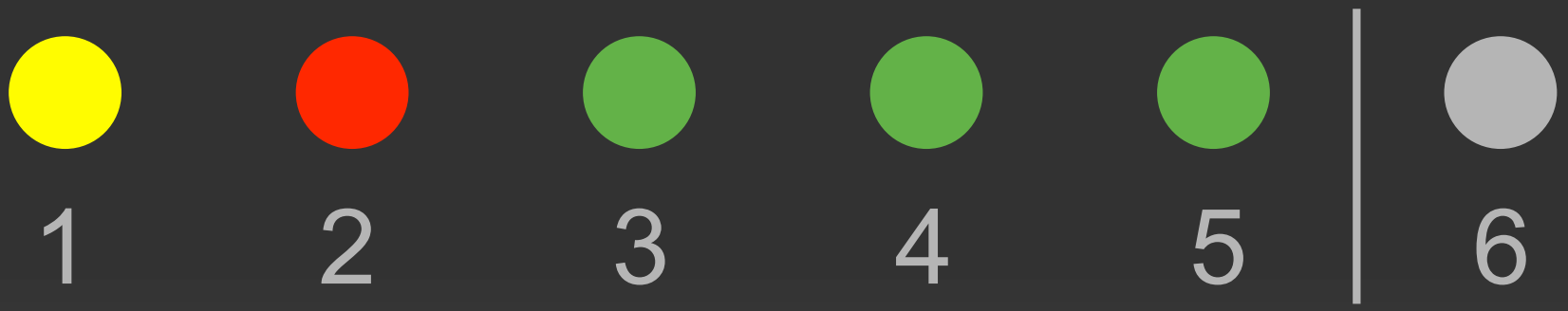
© Photo by AdamKR (Flickr)

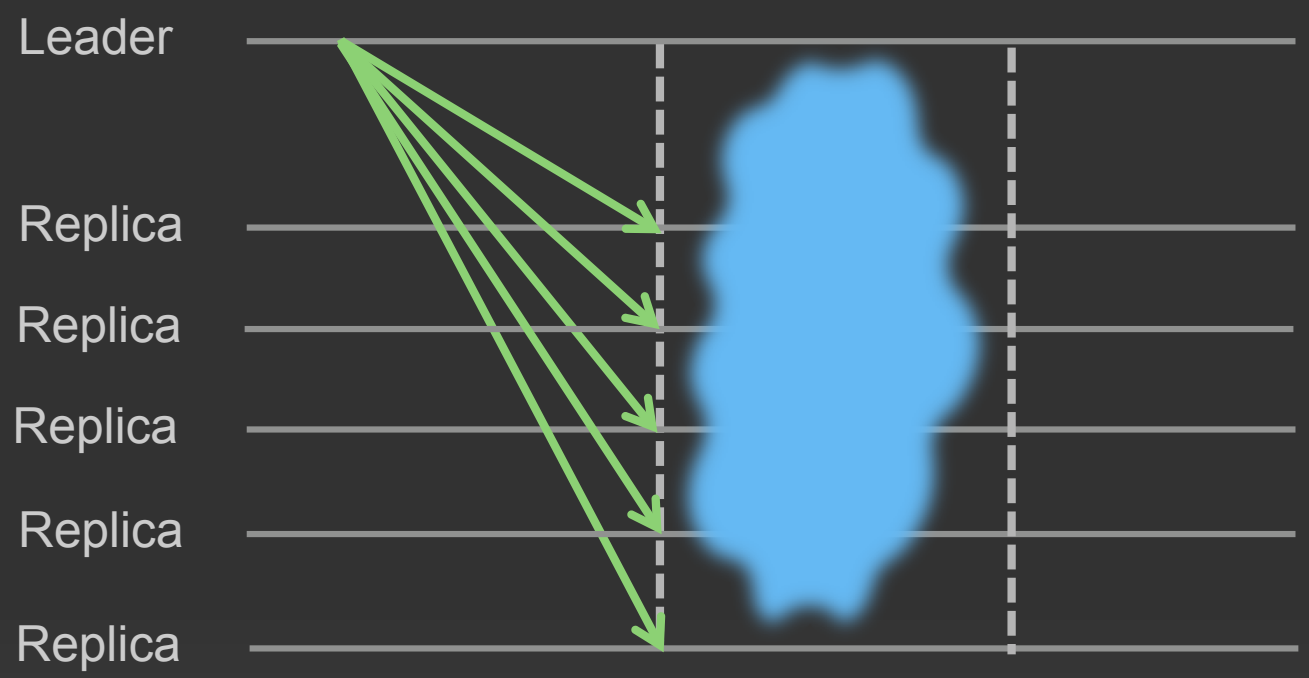
FastBFT

Jean-Philippe Martin, Lorenzo Alvisi


1
2
3
4

FastBFT





FastBFT visualised

Conclusion

- Strict fault-tolerance
- Not scalable
- Quite a few different solutions
- Adaptation could improve performance

Thank you!