Entanglements and why I think they are a good feature for Swarm (and other systems)

Presentation · May 2019

DOI: 10.13140/RG.2.2.11453.92641

1 author:

Vero Estrada-Galinanes
University of Stavanger (UiS)
19 PUBLICATIONS **31** CITATIONS

SEE PROFILE

Universitetet
i Stavanger

Entanglements

and why I think they are a good feature for Swarm (and other systems)

Vero Estrada-Galiñanes, PhD
@galinanesvero
Research scientist
Resilient Systems Lab, UiS

SWARM ORANGE SUMMIT 2019
May 23-25, Madrid

swarm

Universitetet i Stavanger

UiT / THE ARCTIC UNIVERSITY OF NORWAY

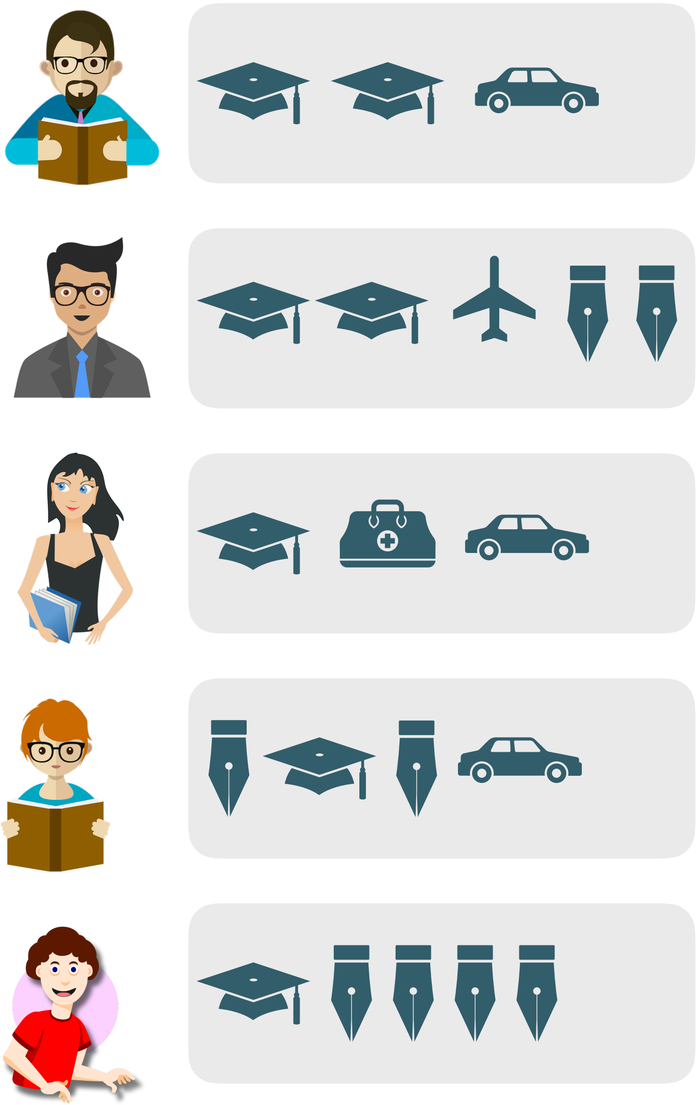
BBCHAIN (Brief recap)

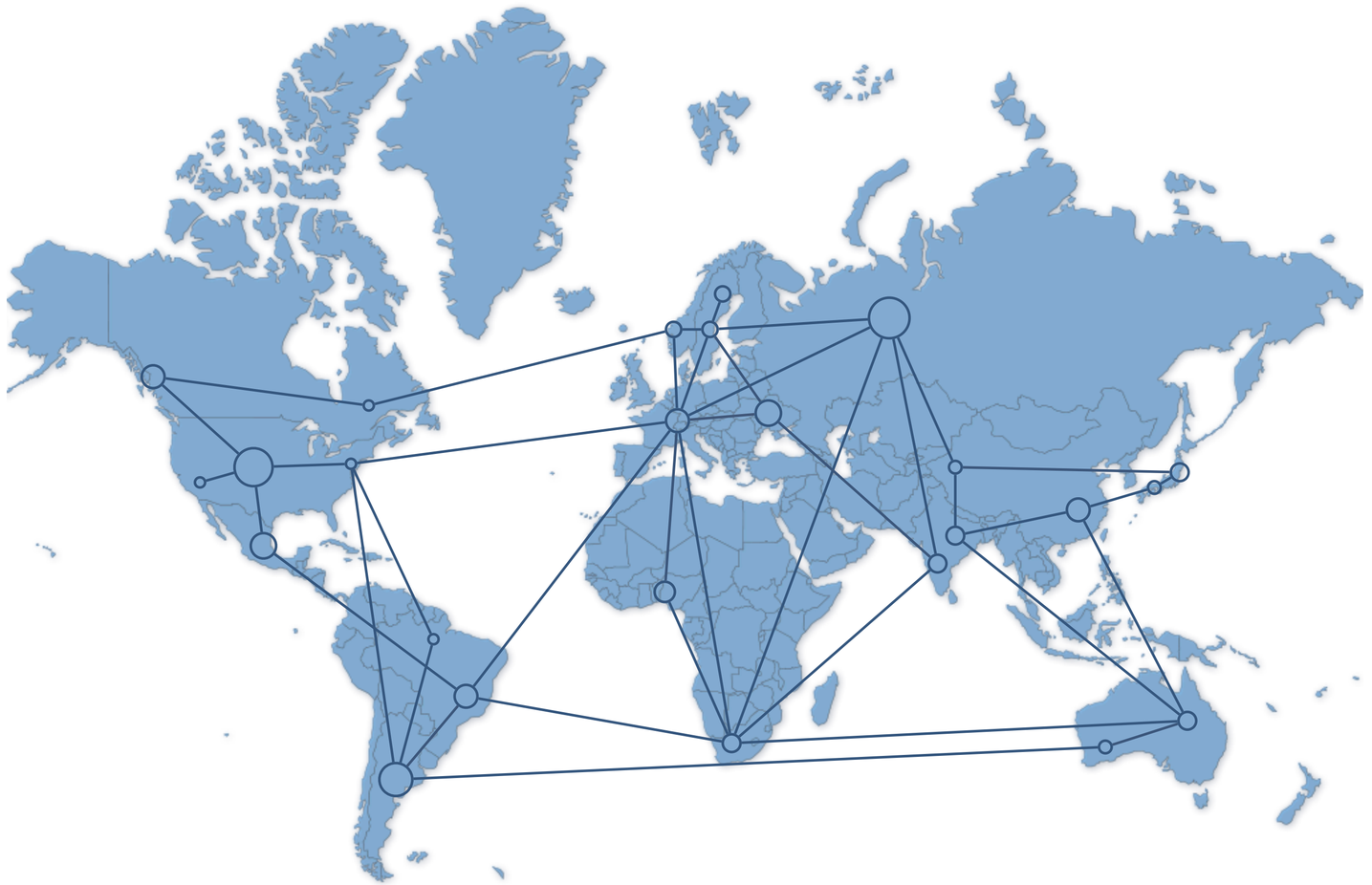
We expect to have a fault-tolerant and trusted authentication system, that can be used to build a public/private database of digitally authenticated documents, allowing for example, that academic degree certificates can be issued and verified from any place in the world with a high degree of trust.

Funded by The Research Council of Norway

Efficient Trustworthy Computing with Blockchains and Biometrics

Public/private database of digitally authenticated documents





Swarm features

- Fault tolerant
- Censorship resistant
- DDoS resistant
- Zero downtime
- Self-sustaining

[https://swarm.ethereum.org/]
[https://swarm-gateways.net/bzz:/theswarm.eth/]

Challenges in decentralised storage systems

Alice pays for storing a file redundantly

Challenges in decentralised storage systems

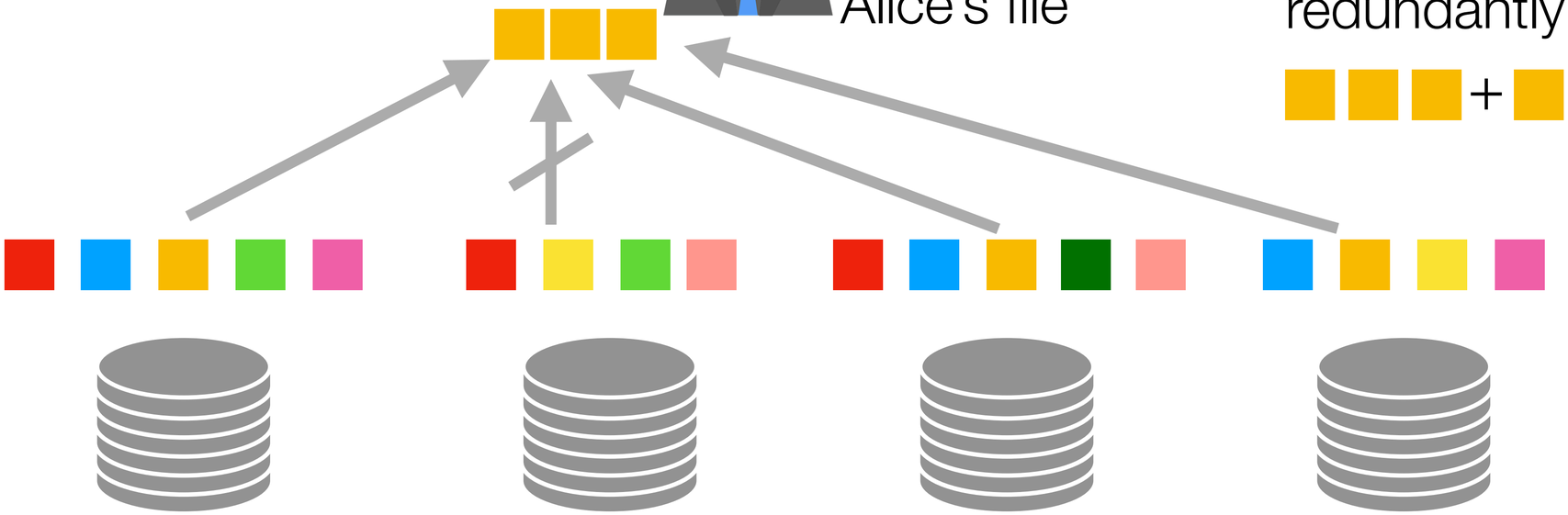
Alice pays for storing a file redundantly

Challenges in decentralised storage systems

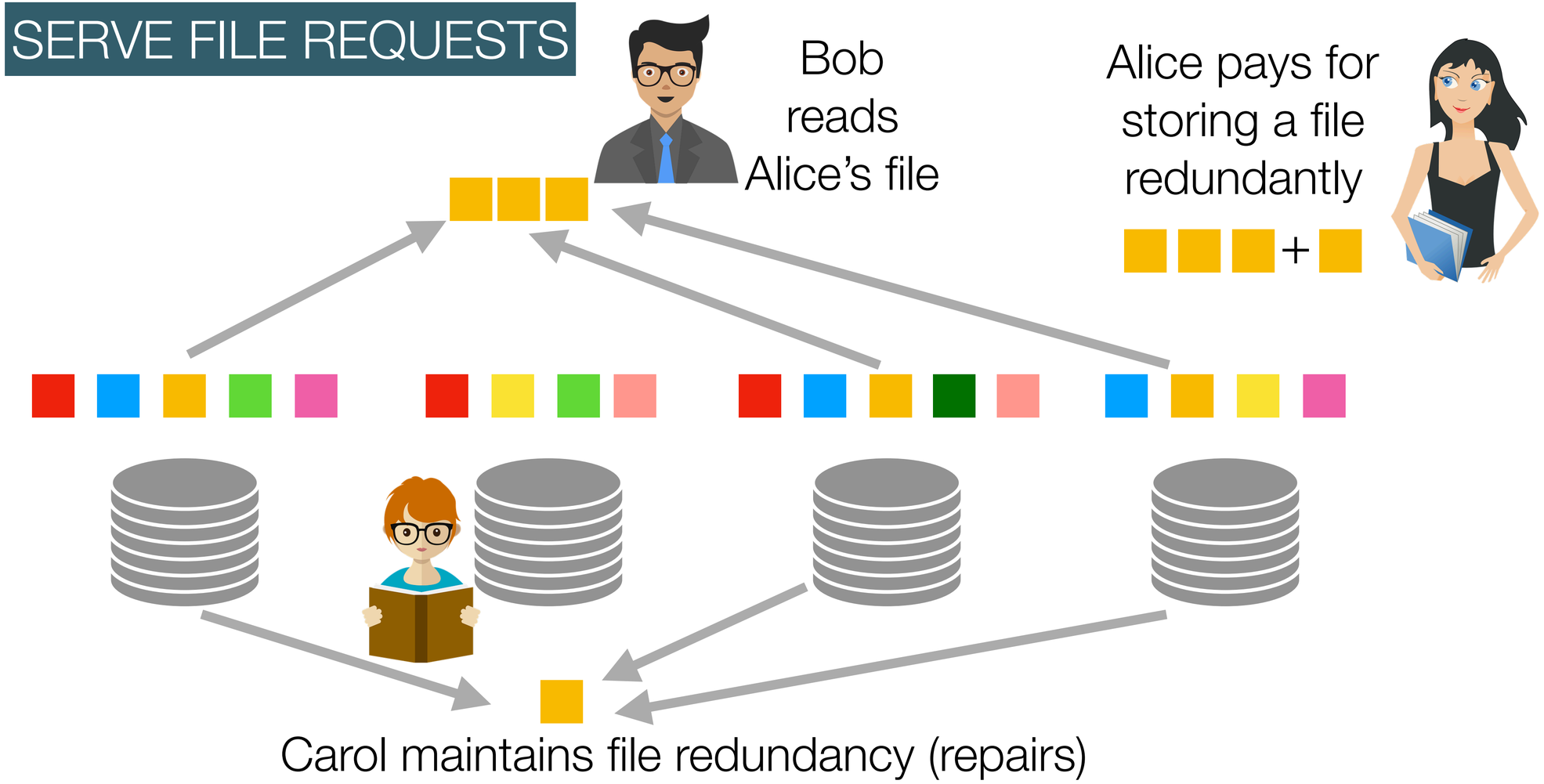
SERVE FILE REQUESTS

Bob reads Alice's file

Alice pays for storing a file redundantly



Challenges in decentralised storage systems

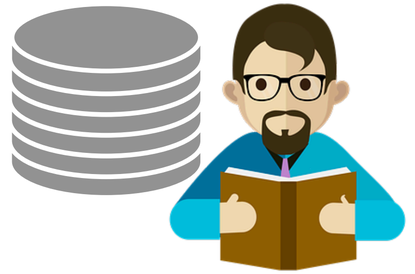


Challenges in decentralised storage systems

SERVE FILE REQUESTS

Bob
reads
Alice's file

Alice pays for
storing a file
redundantly



Carol wishes to maintain file redundancy

Mallory
saves bandwidth
and not cooperates

~~MAINTENANCE PROCESS~~

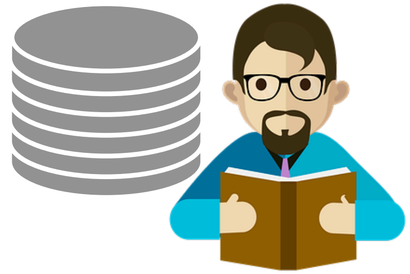
Challenges in decentralised storage systems

SERVE FILE REQUESTS

Bob
wishes to read
Alice's file

Alice pays for
storing a file
redundantly

Oscar
saves space
by deleting
blocks



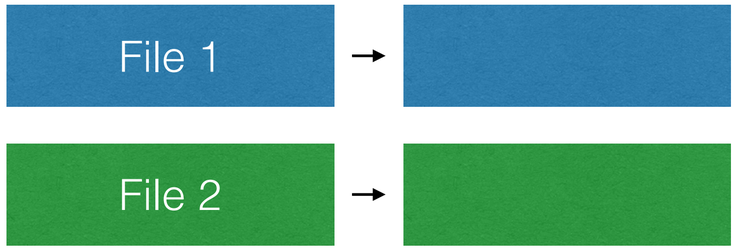
Carol wishes to maintain file redundancy

Mallory
saves bandwidth
and not cooperates

MAINTENANCE PROCESS

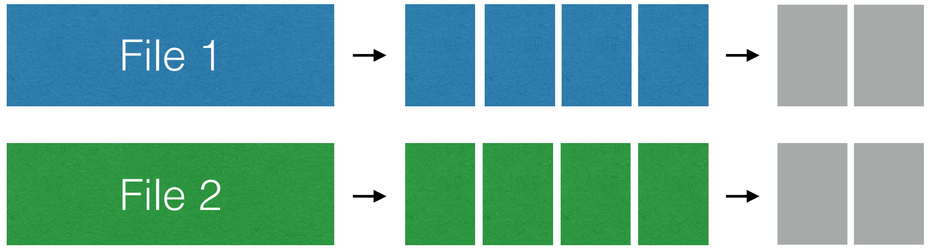
Overheads of redundancy schemes

REPLICATION



copy

RS(k,m) ERASURE CODE



split(k) expand (m)

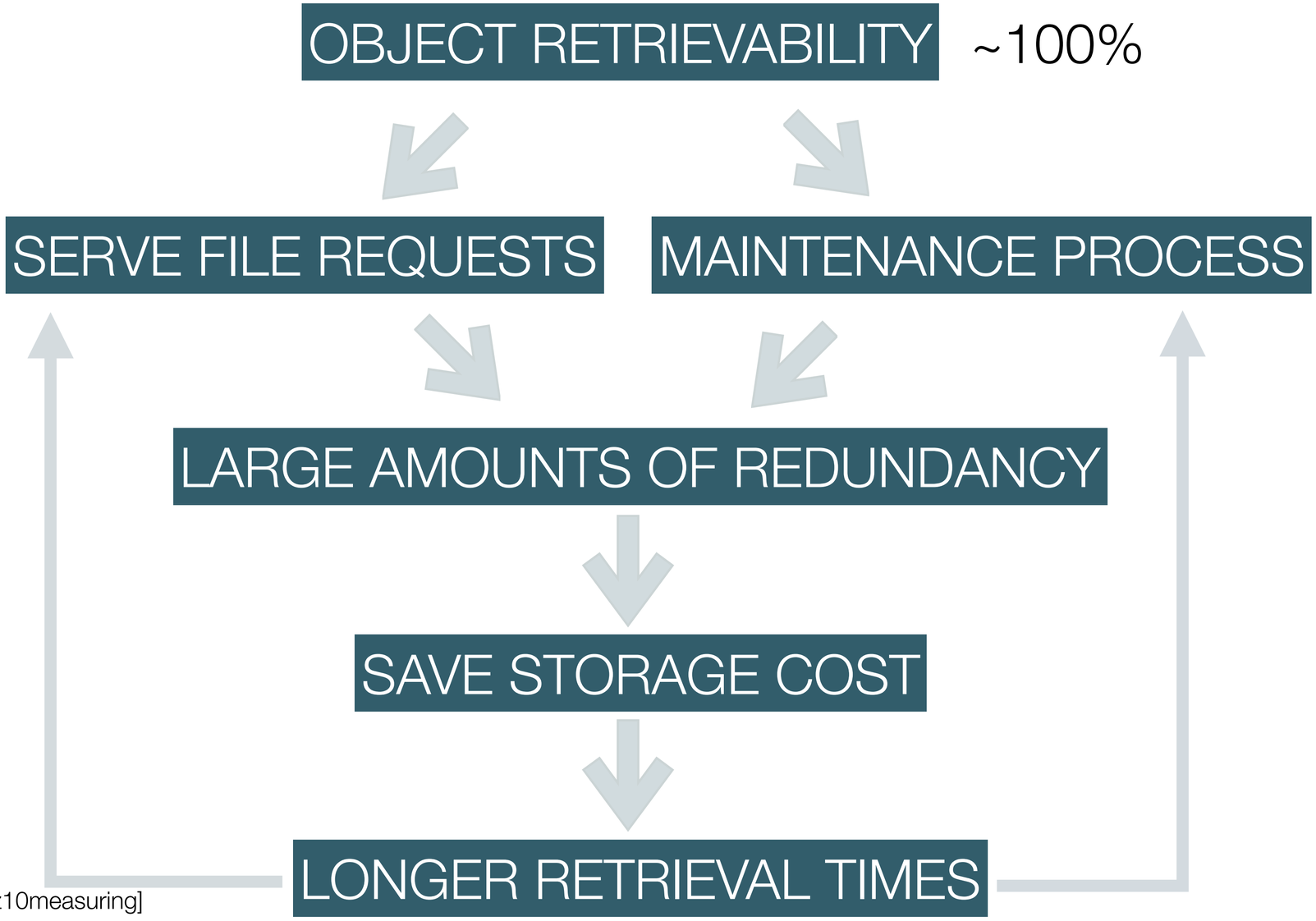
Tolerates “m” failures

REDUNDANCY

STORAGE CAPACITY

COMMUNICATION OVERHEAD

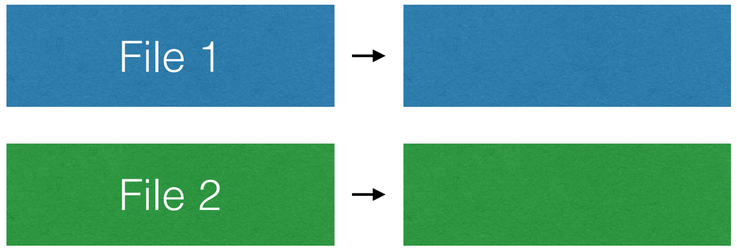
Dimensioning redundancy levels in a decentralised system is difficult



[Pamies-Juarez10measuring]

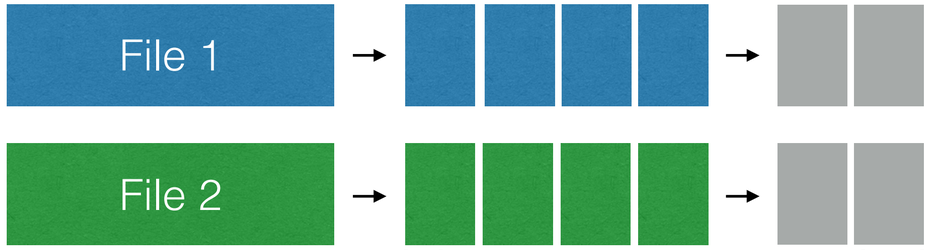
Rethinking redundancy schemes

REPLICATION



copy

RS(k,m) ERASURE CODE



split(k) expand (m)

Tolerates “m” failures

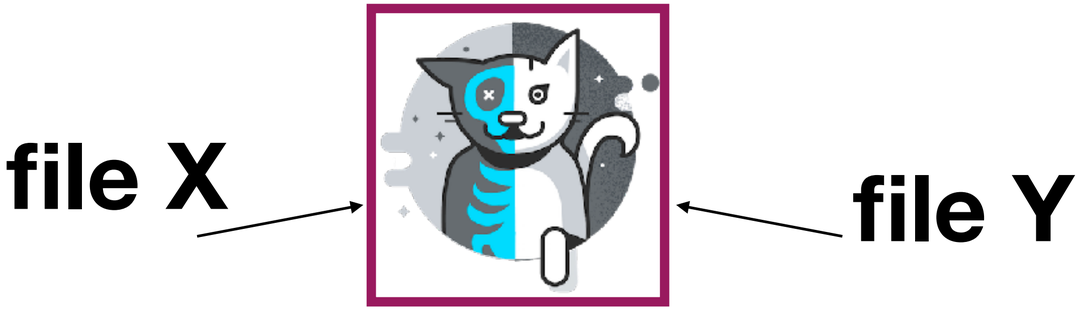
ENTANGLEMENTS

shared redundancy

Entanglements: Design requirements

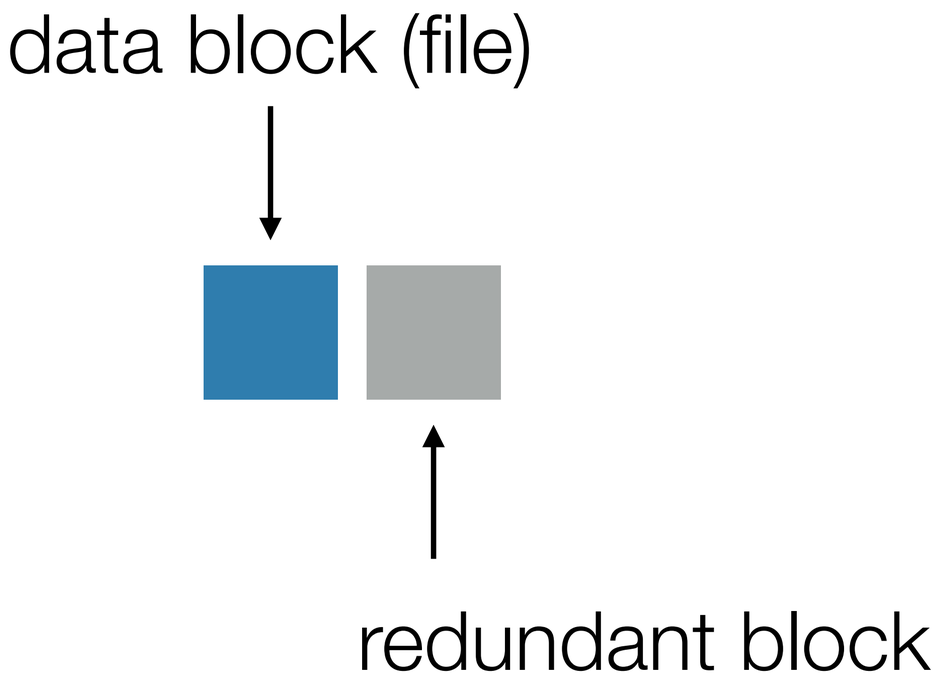
- General-purpose practical code for storage systems
- High fault-tolerance
- Fair protection to all files
- Low encoding/decoding complexity
- Data integrity
- Some protection against censorship is desired too

TANGLE BLOCKS



A chain of entangled blocks ($\alpha = 1$)

Storage: equivalent to 2 replicas (data block + redundant block)

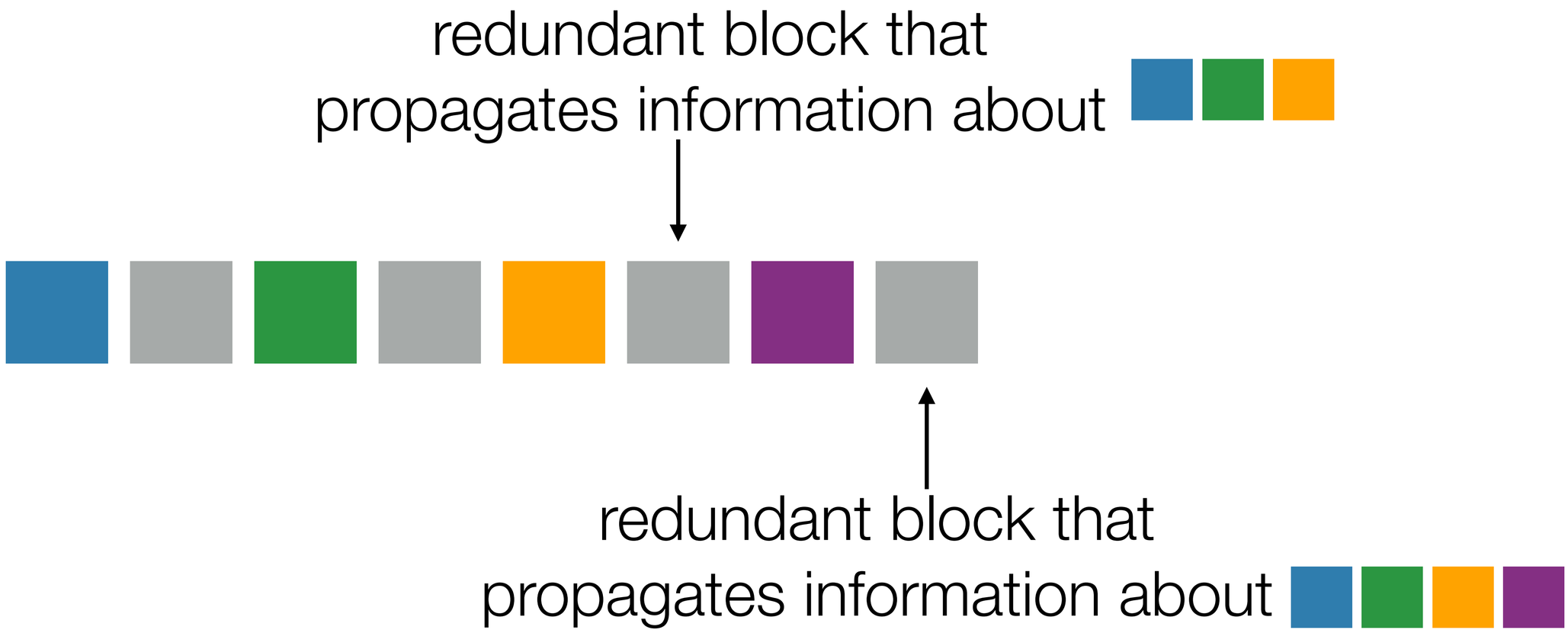


A chain of entangled blocks ($\alpha = 1$)

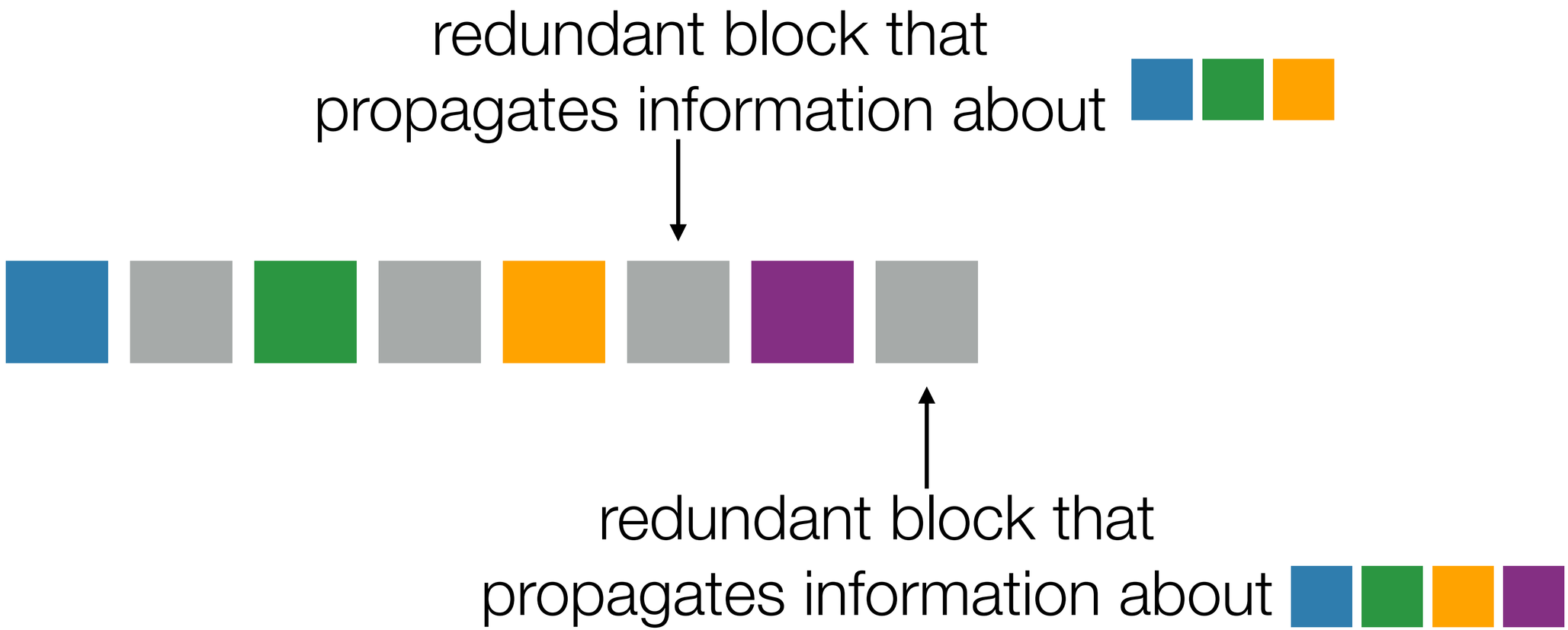
A chain of entangled blocks ($\alpha = 1$)

redundant block that
propagates information about

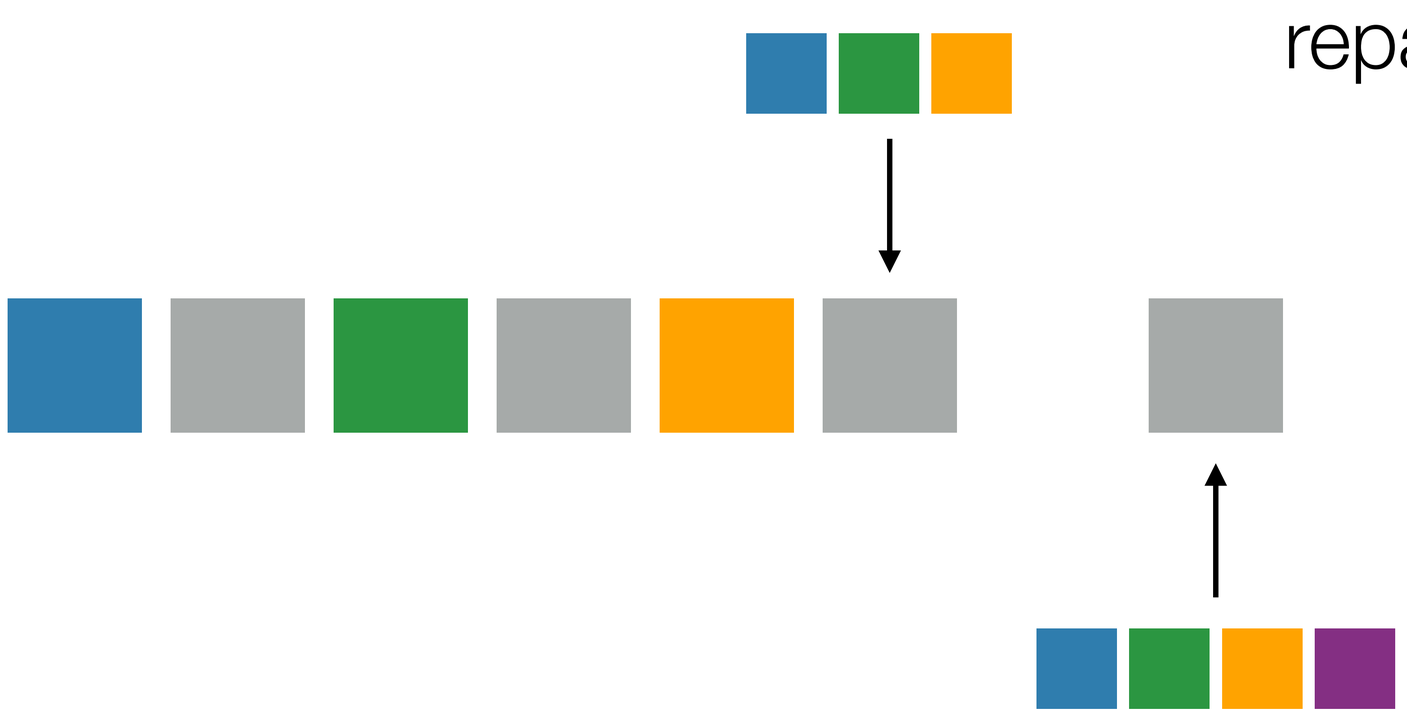
A chain of entangled blocks ($\alpha = 1$)



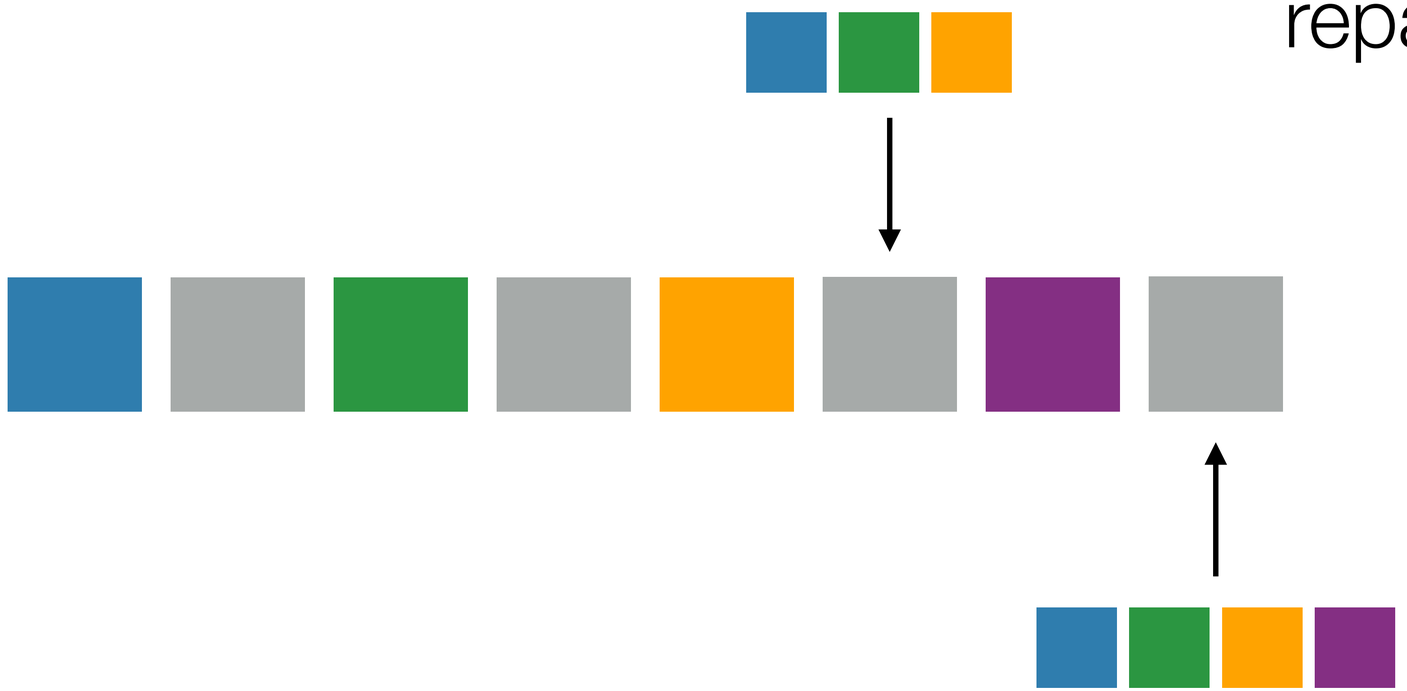
A chain of entangled blocks ($\alpha = 1$)



A chain of entangled blocks ($\alpha = 1$)



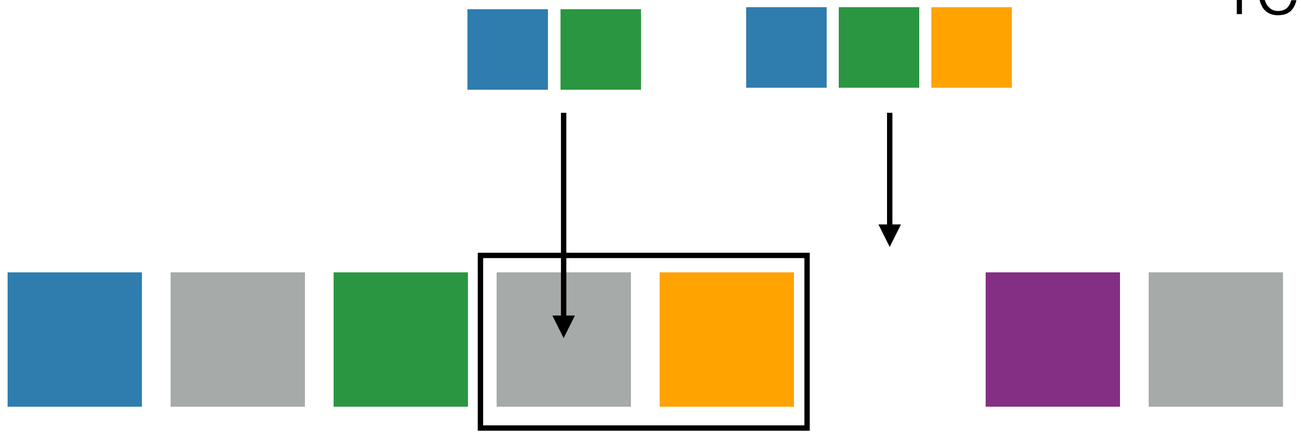
A chain of entangled blocks ($\alpha = 1$)



repair data blocks

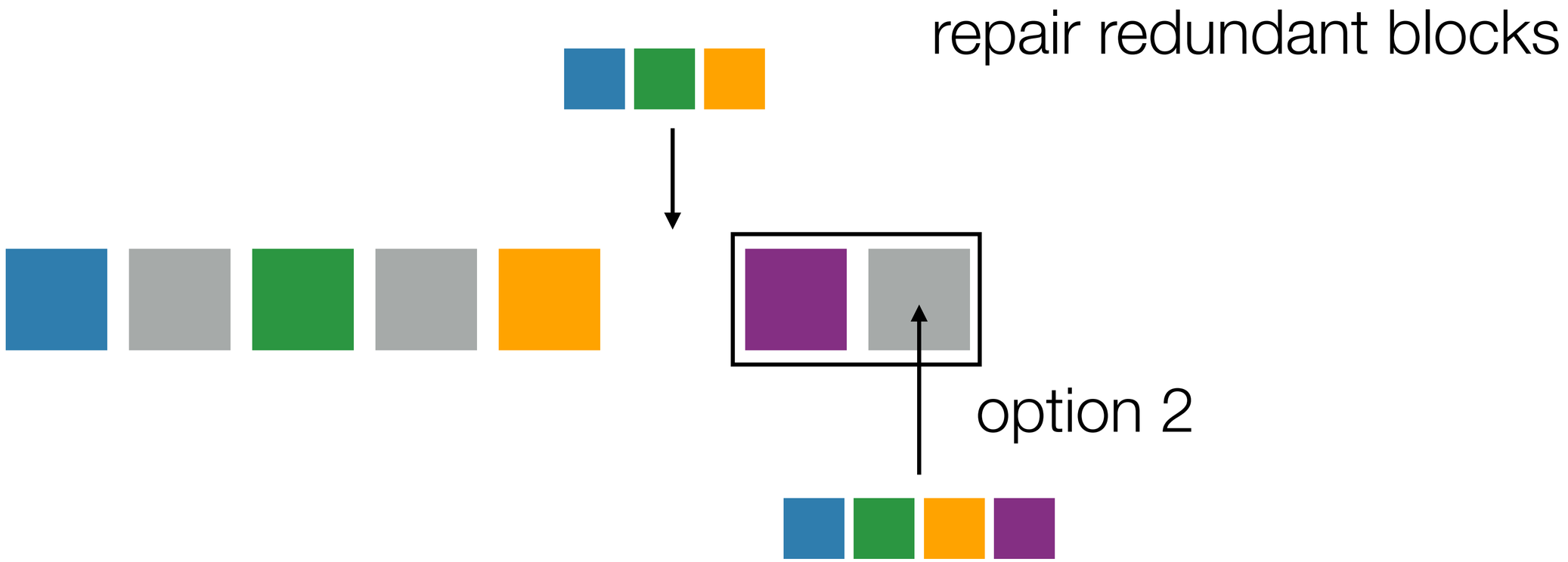
A chain of entangled blocks ($\alpha = 1$)

repair redundant blocks



option 1

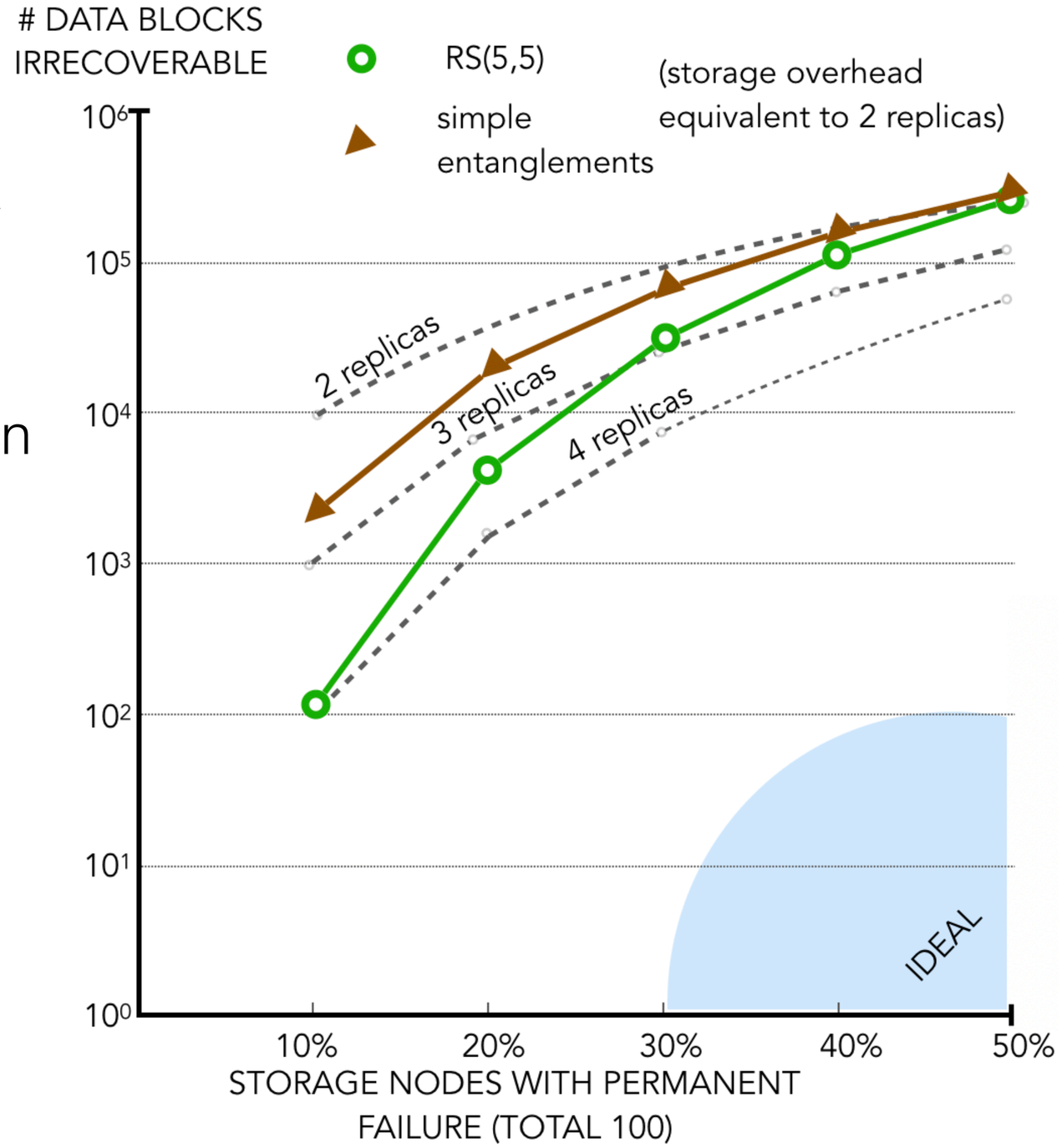
A chain of entangled blocks ($\alpha = 1$)



A chain of entangled blocks ($\alpha = 1$)

Simple entanglements

- Better fault-tolerance than duplication
- Fair protection to all files
- Low encoding/decoding complexity
- Data integrity

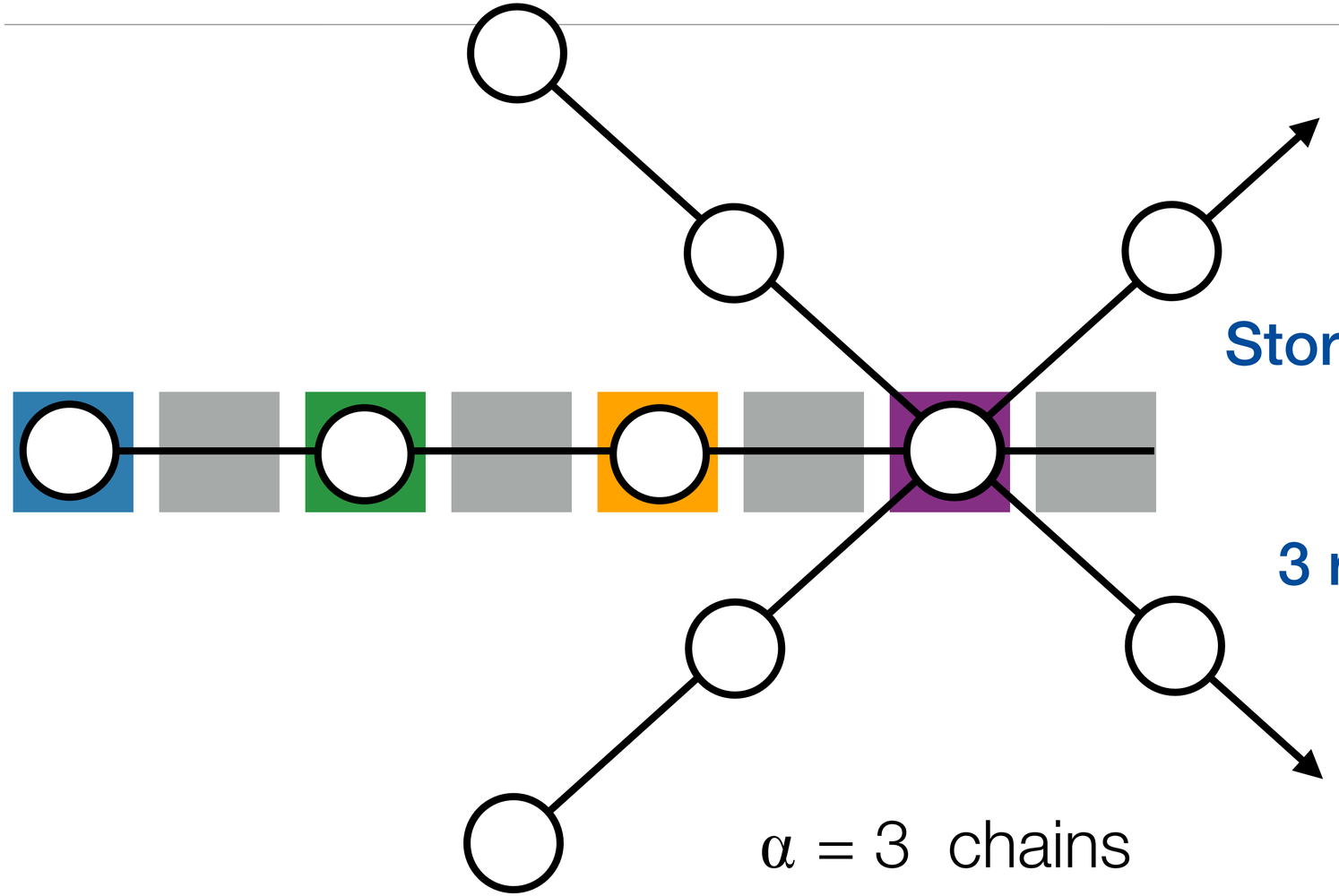


Vero Estrada-Galiñanes, Jehan-François Pâris, Pascal Felber
Simple data entanglement layouts with high reliability. *Proceedings of the 35th International Performance of Computers and Communication Conference (*IPCCC 2016), Las Vegas, Dec 2016

How can we improve fault-tolerance?

How can we improve fault-tolerance?

How can we improve fault-tolerance?



$\alpha = 3$ chains

Storage cost equivalent to 4 replicas (data block + 3 redundant blocks)

Alpha entanglements (AE) codes

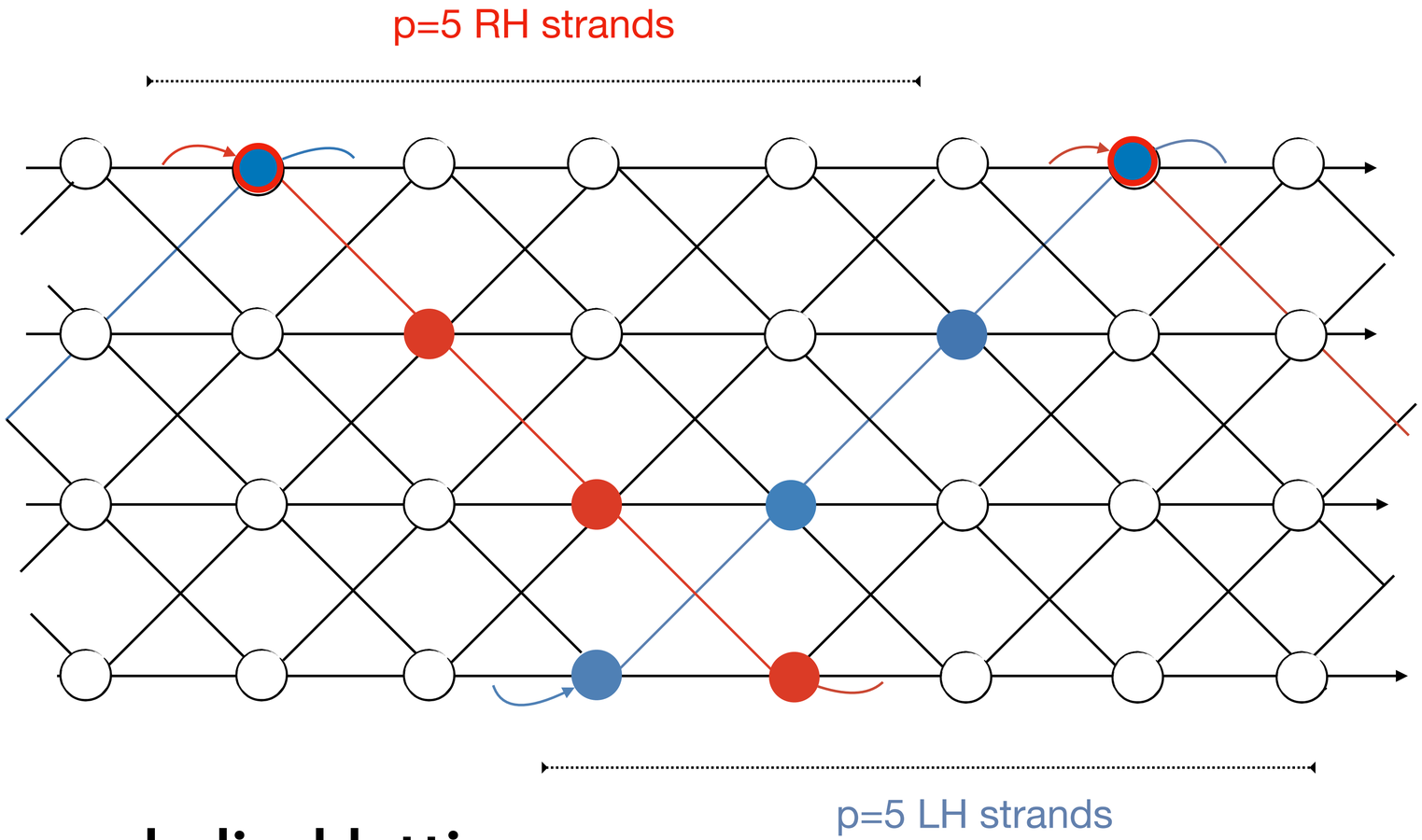
Every data block

belongs to α chains

This lattice configuration

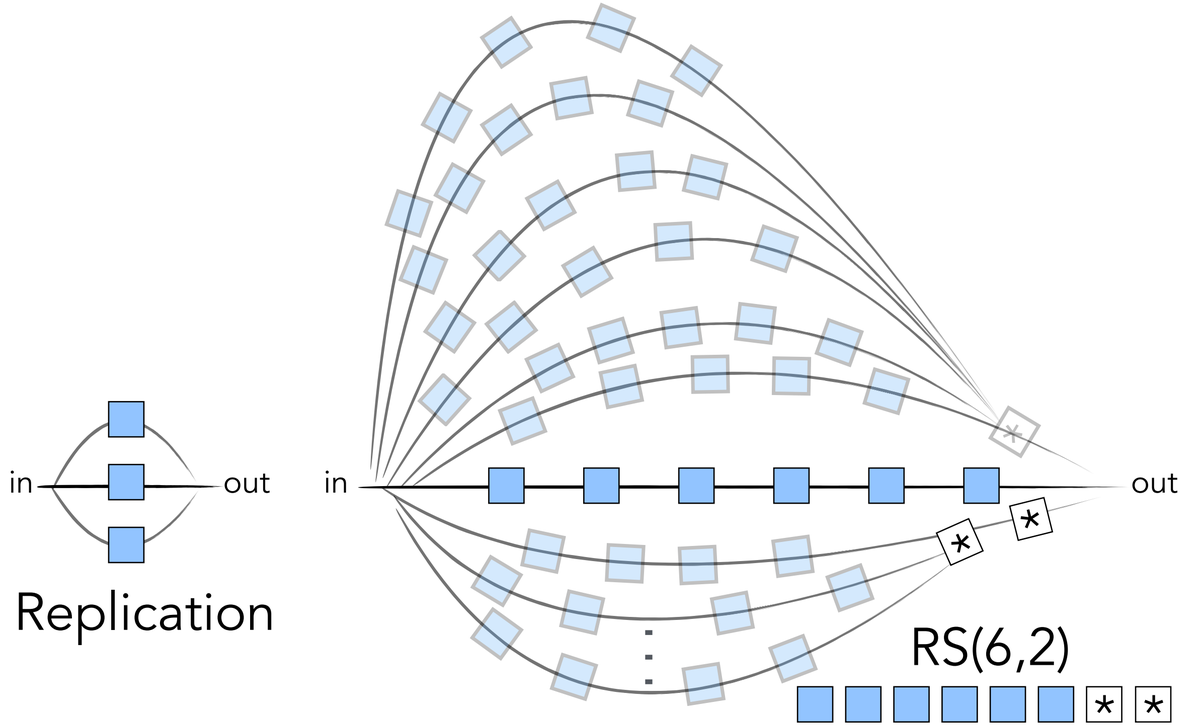
is built with 14 chains

(strands)



helical lattice

In context with traditional methods

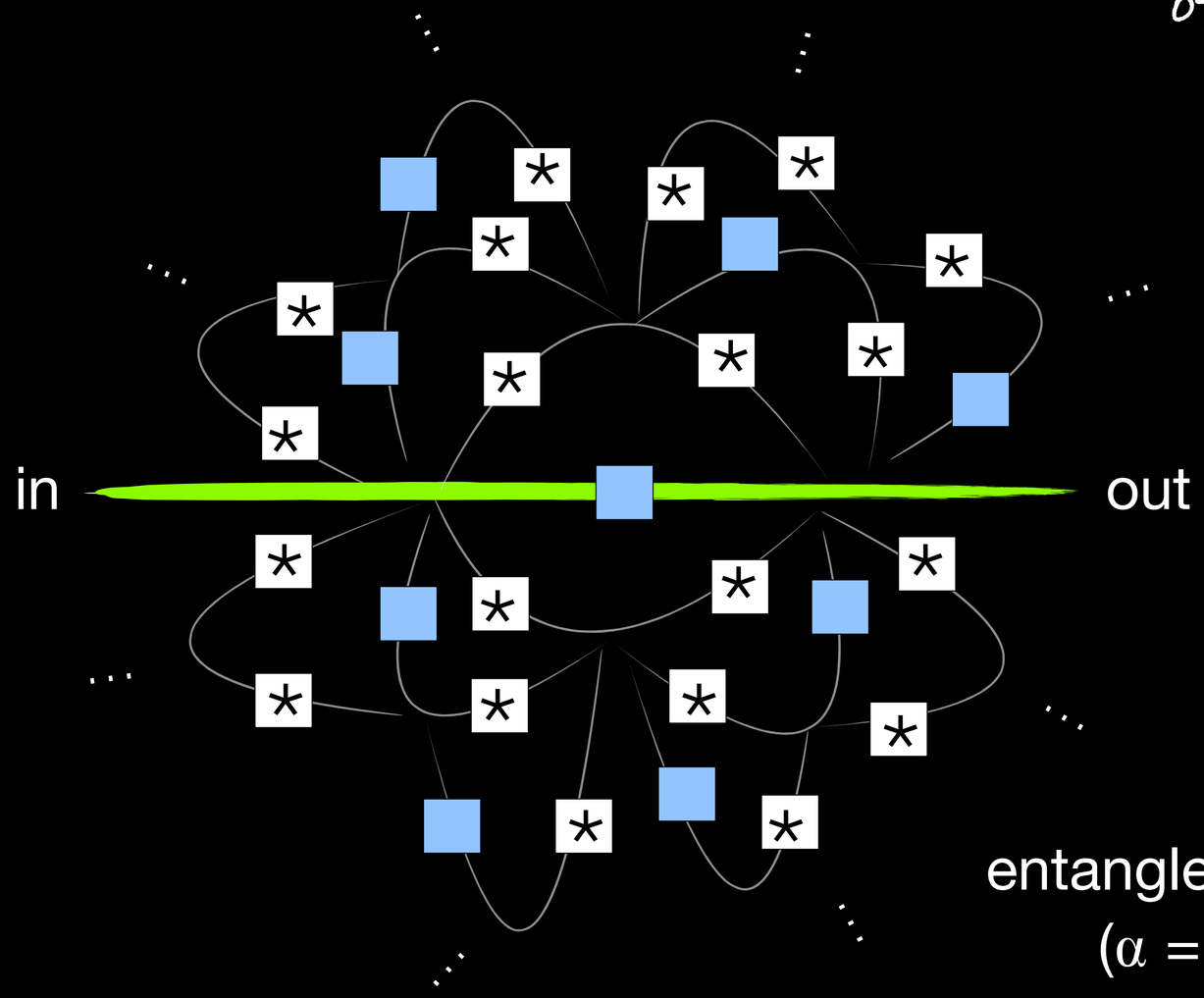


virtual data block
data block
virtual redundant block
redundant block

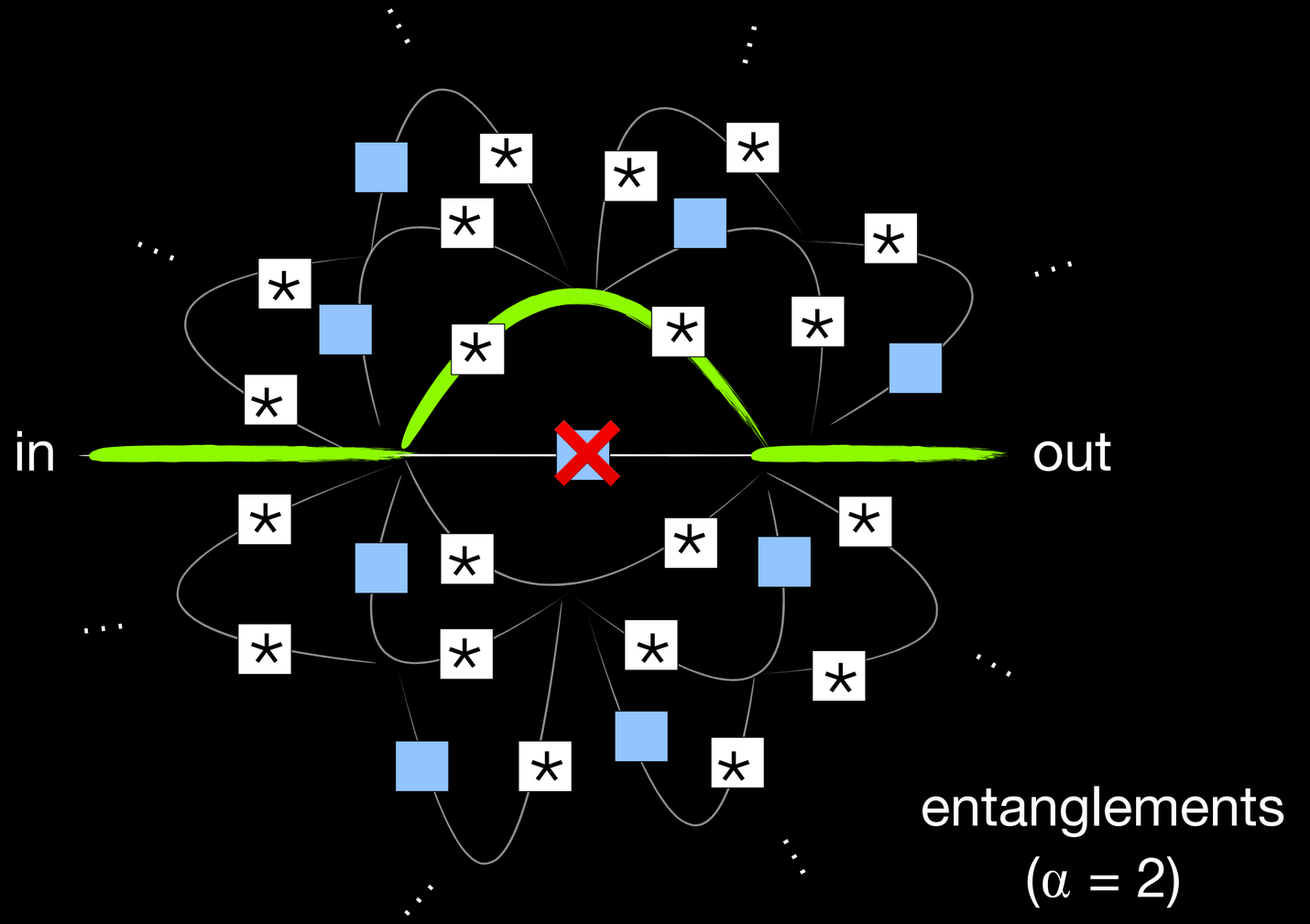
in: get(block id)

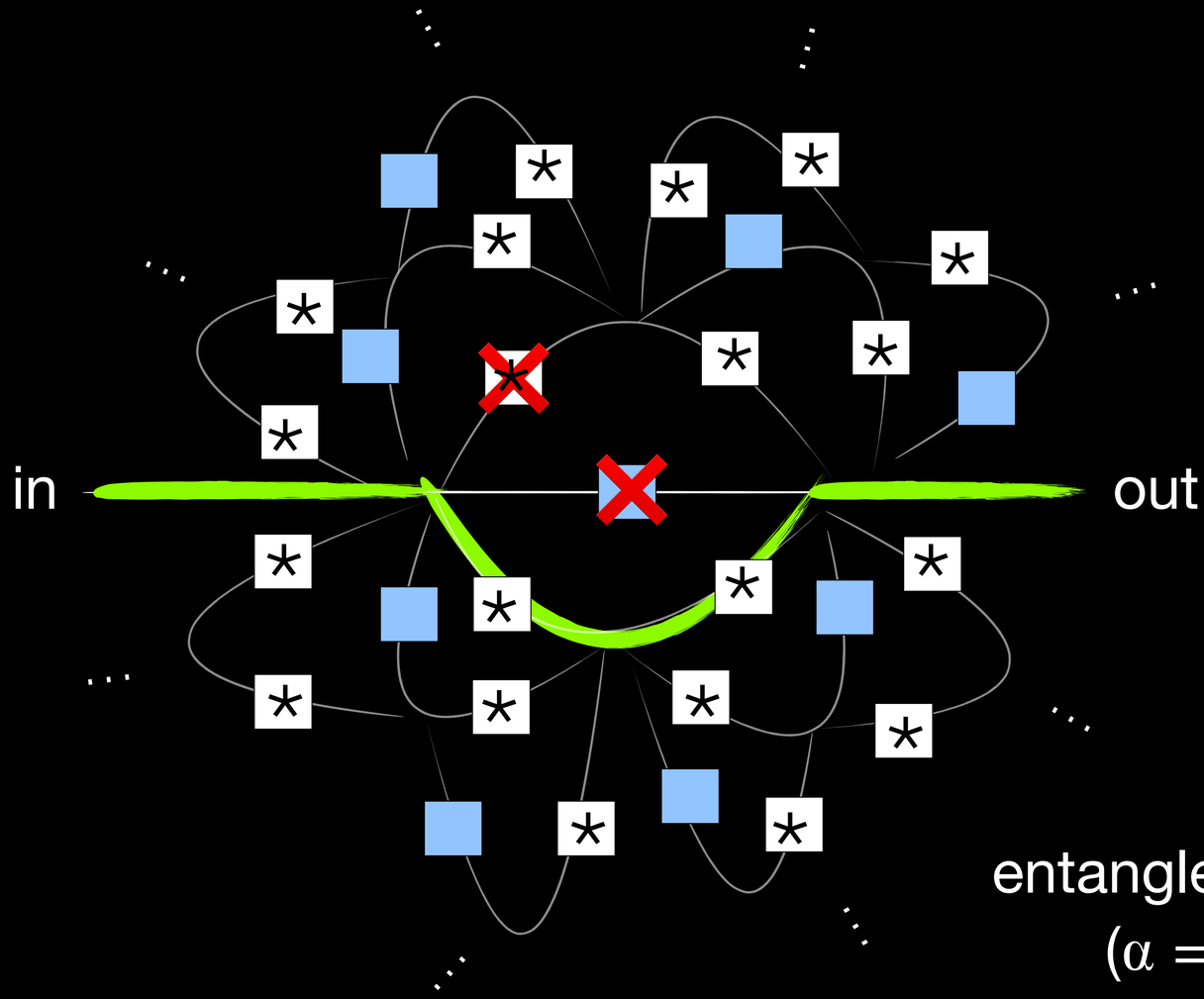
out: the requested block

(a different view
of the helical lattice)

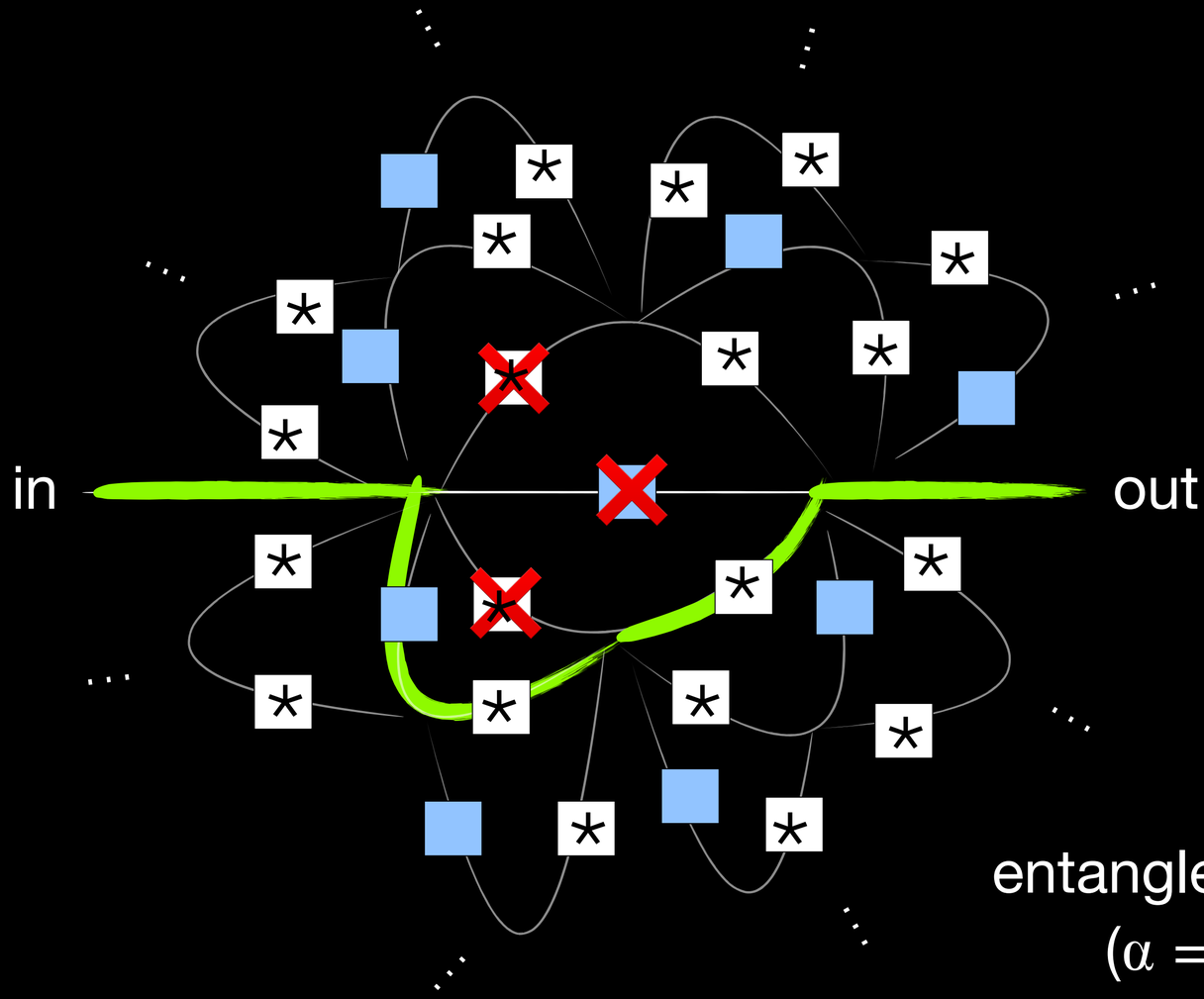


entanglements
($\alpha = 2$)

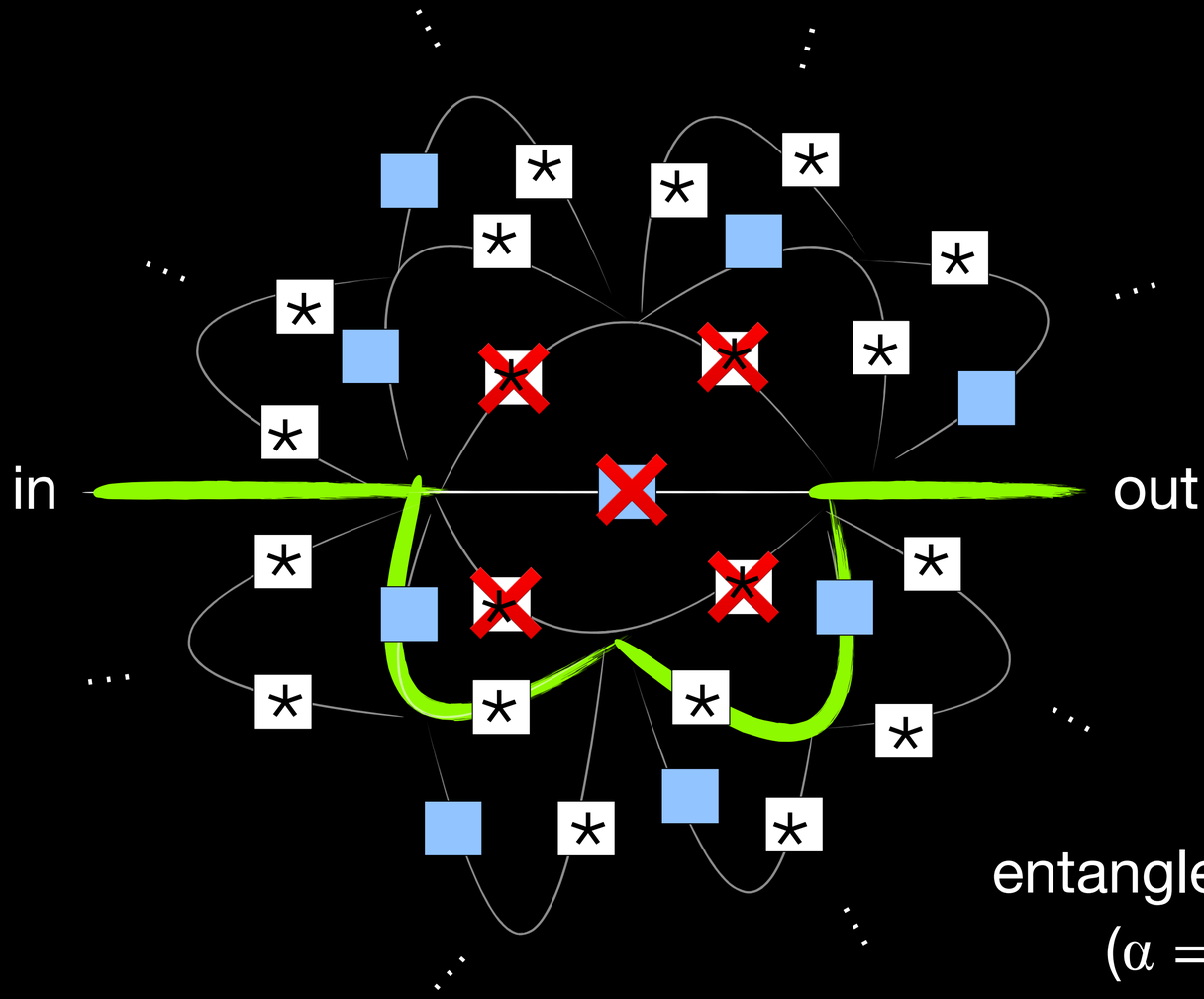

in
out
entanglements
(α = 2)



entanglements
($\alpha = 2$)



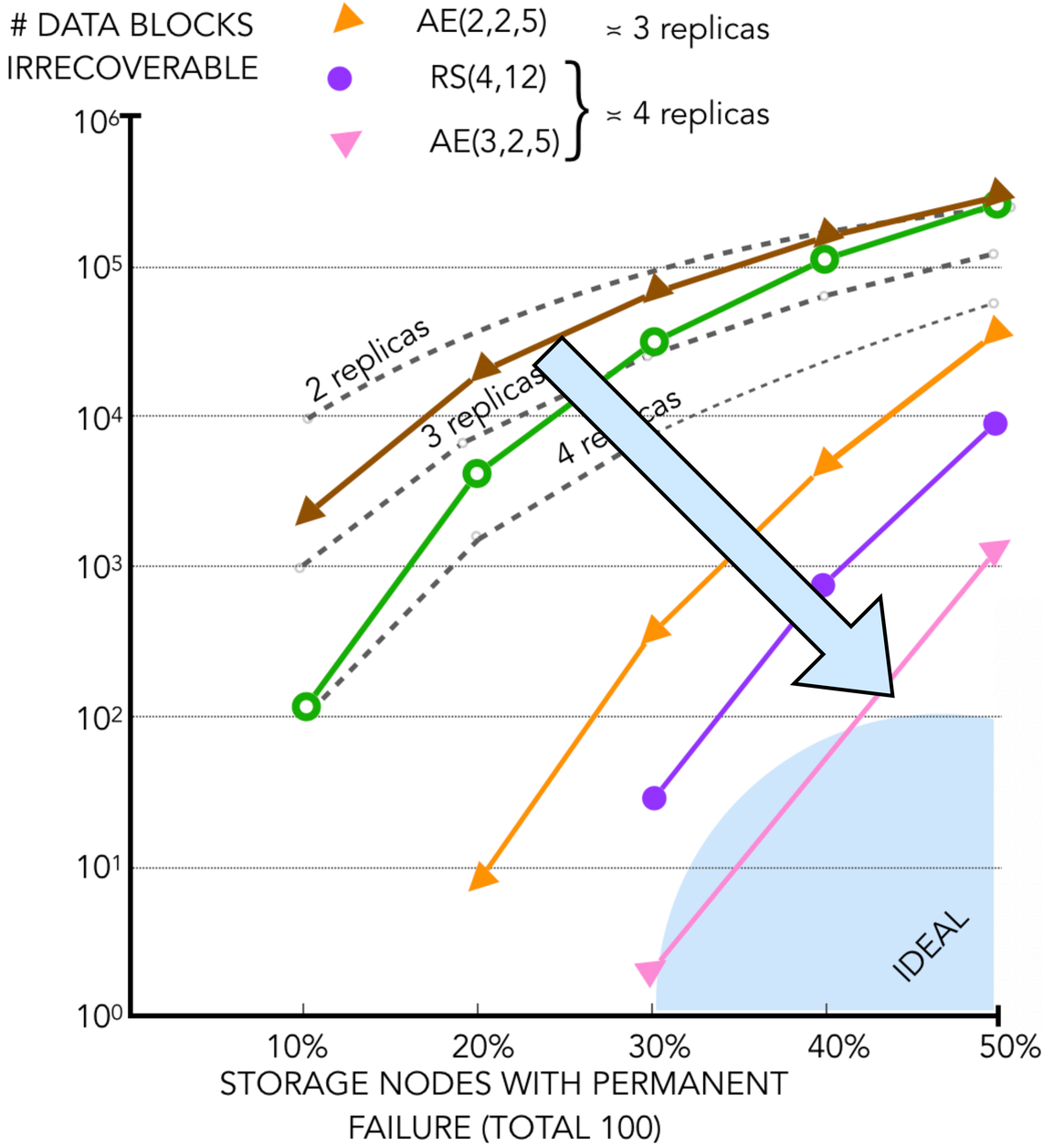
entanglements
($\alpha = 2$)



entanglements
($\alpha = 2$)

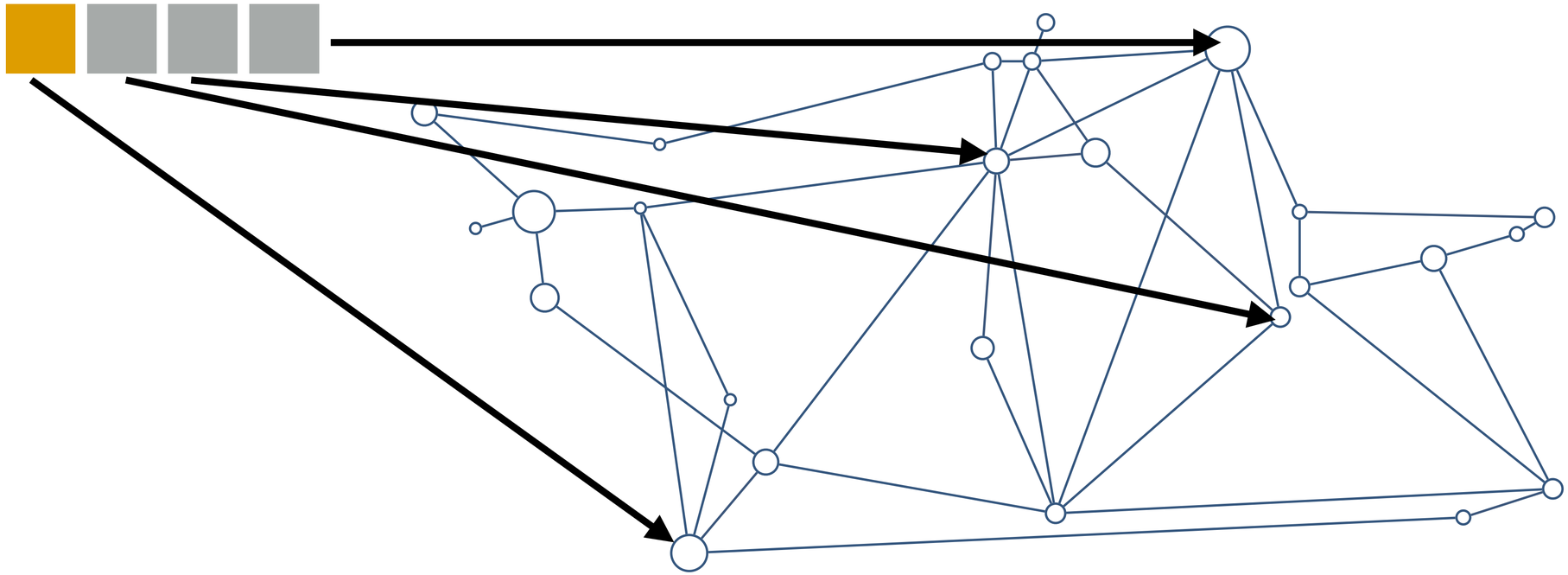
AE codes

- High fault-tolerance
- Fair protection to all files
- Low encoding/decoding complexity
- Data integrity
- Some protection against censorship



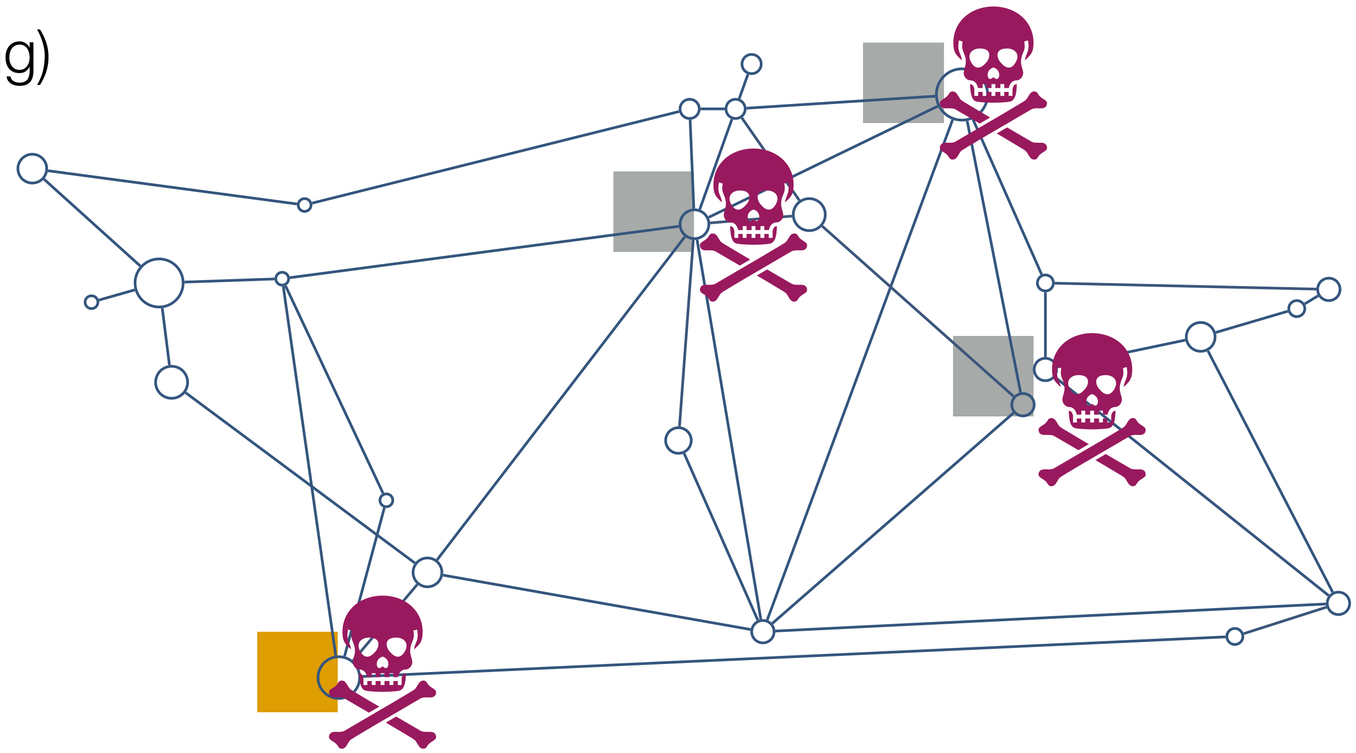
Vero Estrada-Galiñanes, Ethan L. Miller, Pascal Felber, Jehan-François Pâris
Alpha Entanglement Codes: Practical Erasure Codes to Archive Data in Unreliable Environments. 48th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2018), Luxembourg, Jun 2018

Alice, Bob and adversary peers

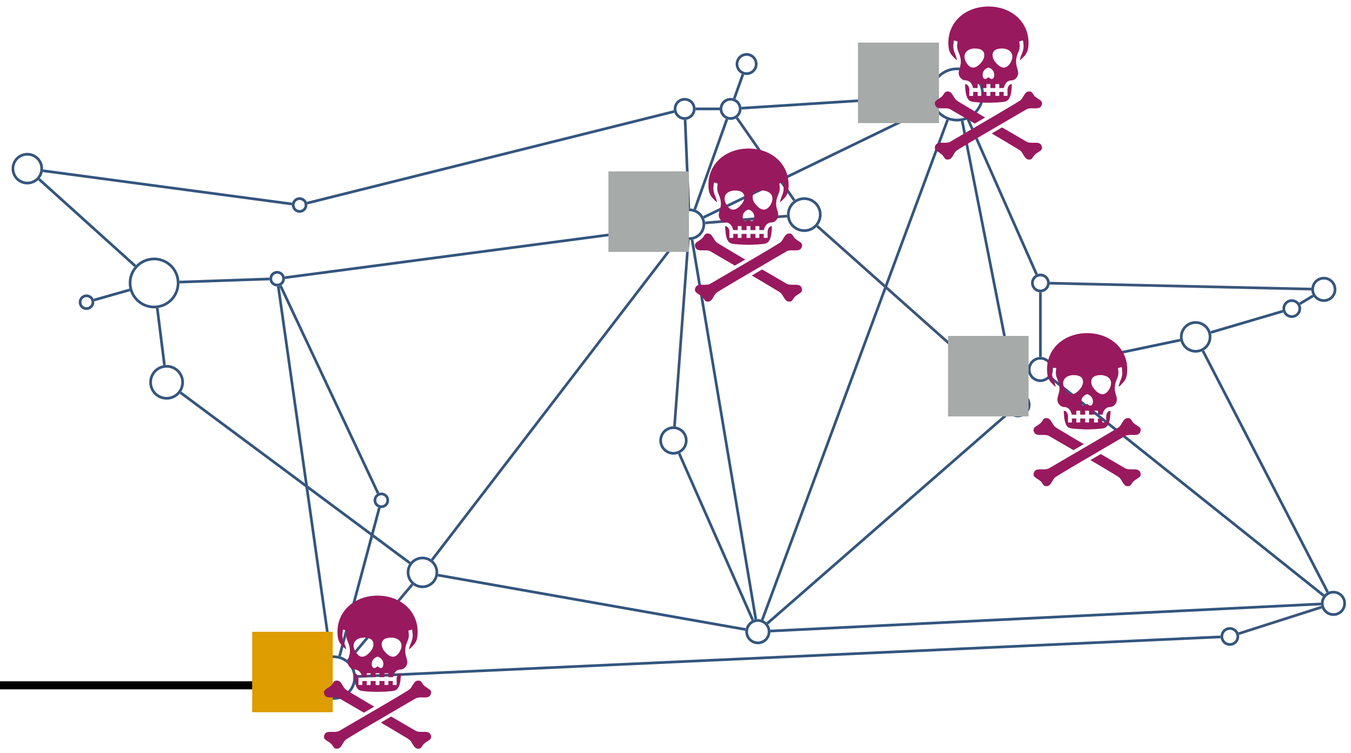


Alice, Bob and adversary peers

Alice (without knowing)
stores the blocks
in untrusted nodes



Alice, Bob and adversary peers



Bob
can try other paths to
read Alice’s file

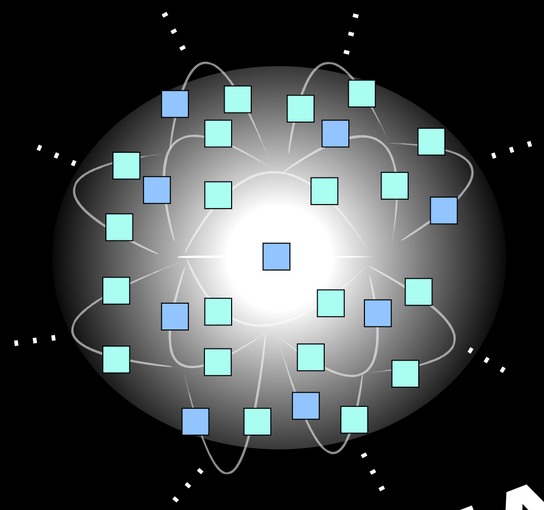
Future Work and Conclusion

- Redundancy is a key part of any fault-tolerance system
- Entanglement codes can provide high fault-tolerance and data integrity guarantees, using a flexible, simple, and efficient algorithm to mix files in a system
- A way to keep off chain data in a chain
- [FUTURE WORK] Build an entangled storage layer in Swarm
- [FUTURE WORK] Framework to compare codes

She ~~He~~ explained that an Aleph is

one of the points in space that contains all other points.

Jorge Luis Borges (1899-1986), Argentinean writer.



THANK YOU!

veg@ieee.org

@GalinanesVero