TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

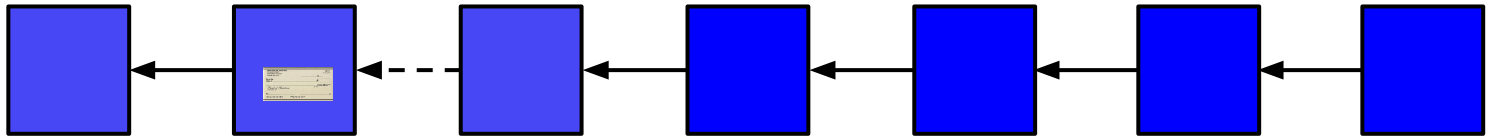
FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

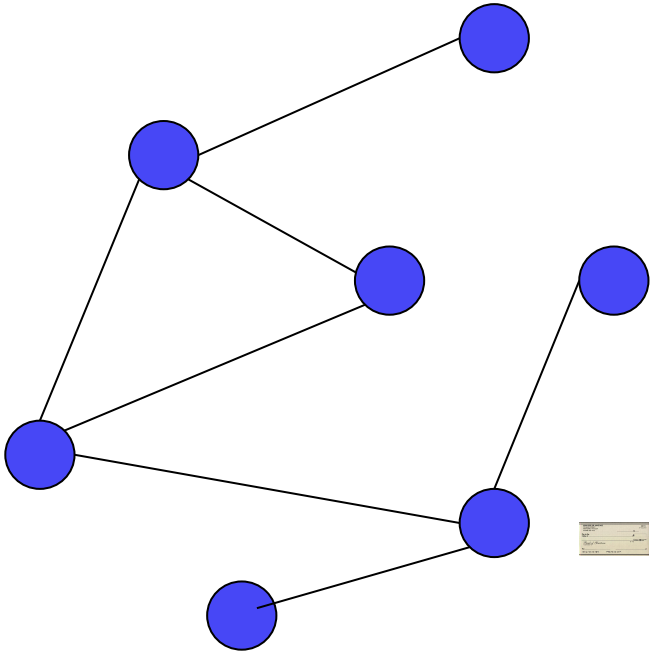
S&P SECURITY & PRIVACY GROUP

Divide & Scale:
Formalization and Roadmap to Secure Sharding

Zeta Avarikioti, Antoine Desjardins, Eleftherios Kokoris-Kogias, Roger Wattenhofer

What is a blockchain?





A blockchain is a protocol run among nodes in a *permissionless* network to reach *probabilistic* agreement on the order of transactions.

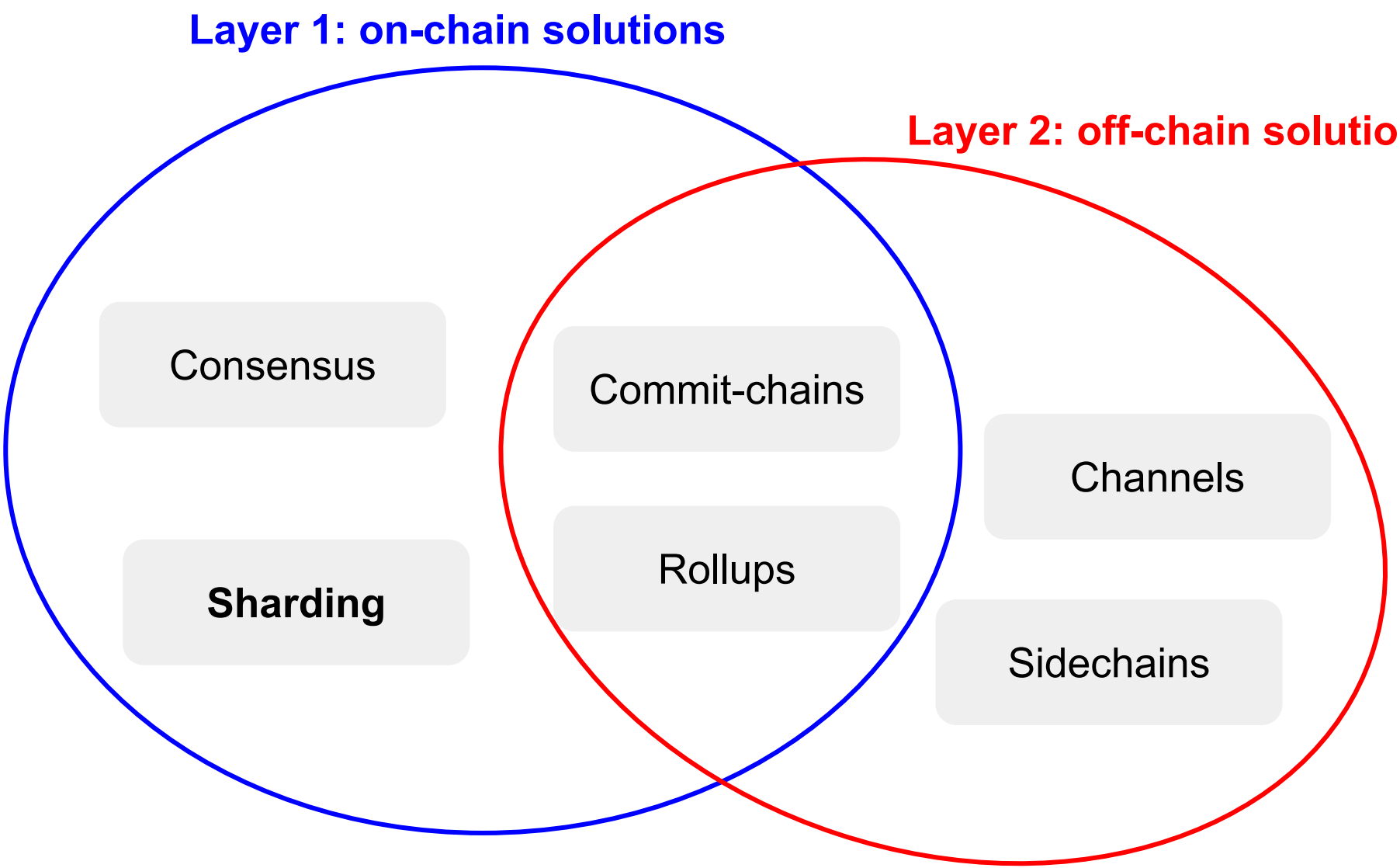
Can cryptocurrencies scale?

7 tx/s

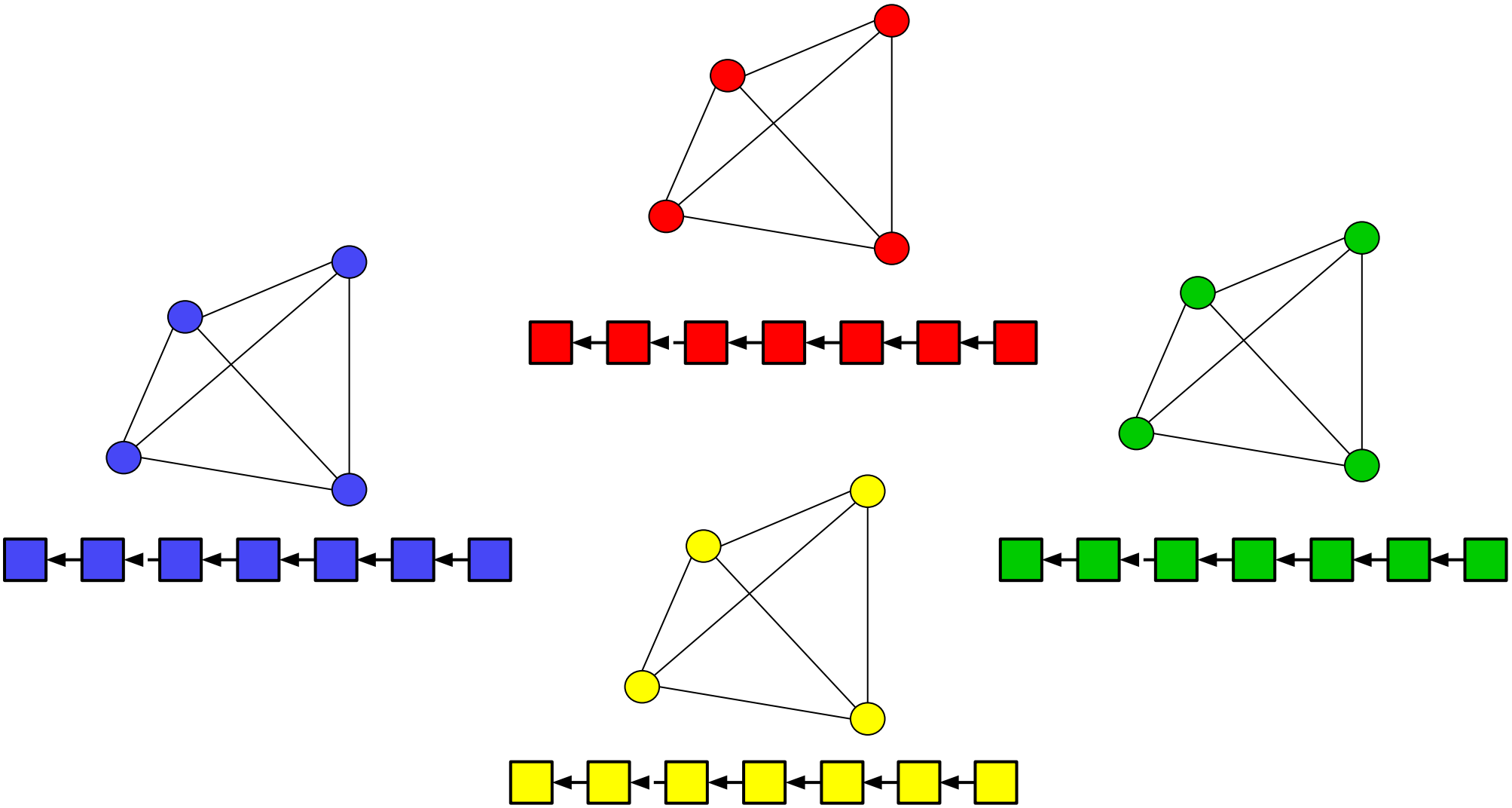
30 tx/s

65.000 tx/s

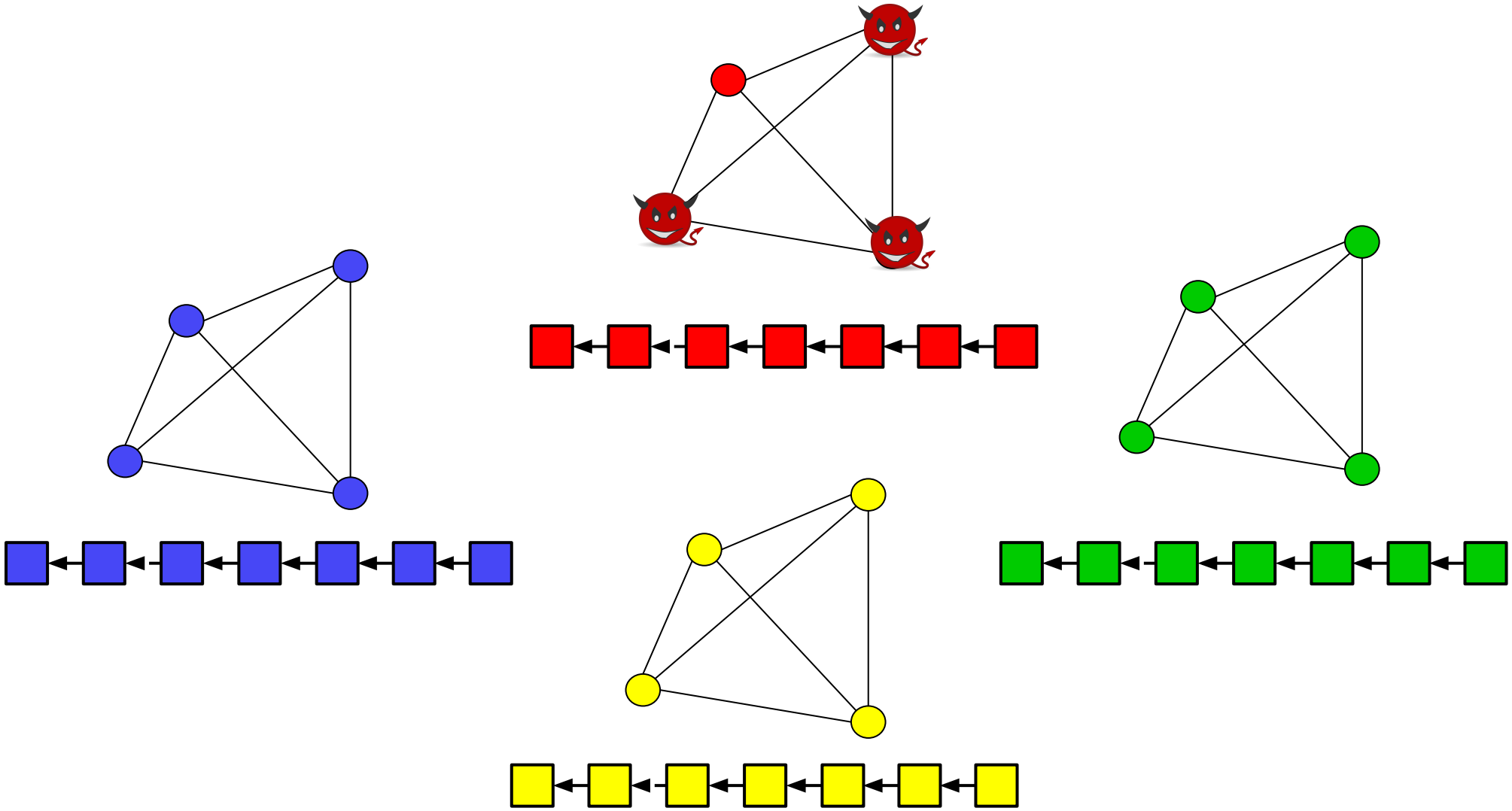
Scaling solutions



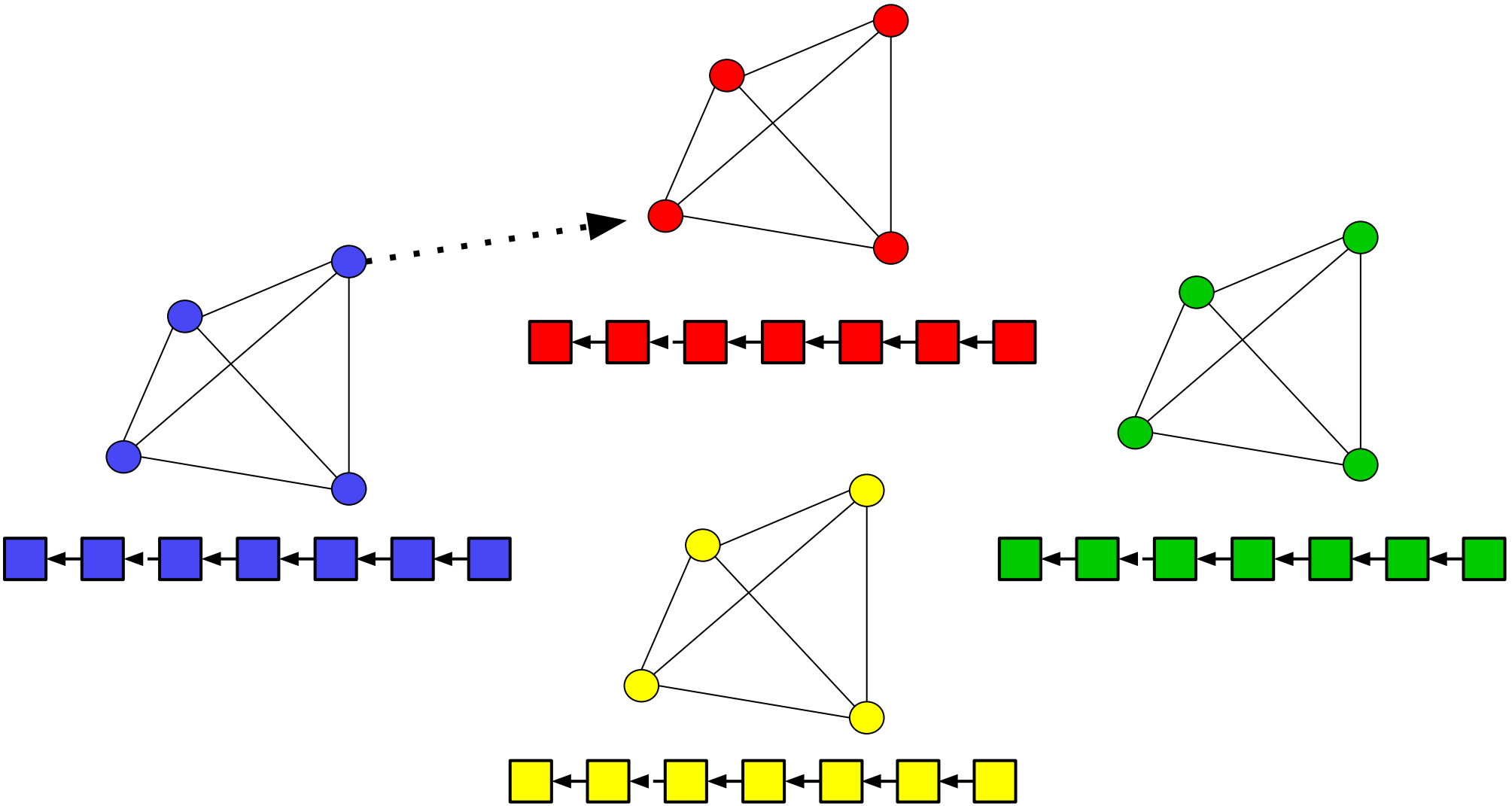
What is sharding?



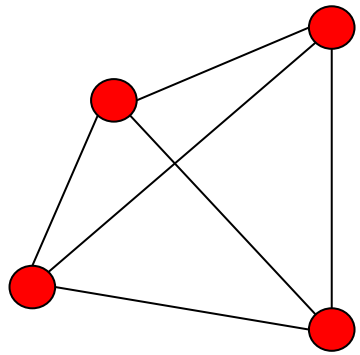
What is sharding?

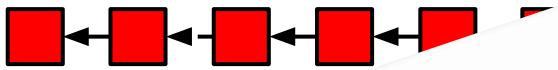


What is sharding?



What is sharding?





A Secure Sharding Protocol For Open Blockchains

Loi Luu
National University of Singapore
loiluu@comp.nus.edu.sg

Kunal Baweja
National University of Singapore
kbaweja@comp.nus.edu.sg

Viswesh Narayanan
National University of Singapore
visweshn@comp.nus.edu.sg

Seth Gilbert
National University of Singapore
seth.gilbert@comp.nus.edu.sg

RapidChain: Scaling Blockchain via Full Sharding

Mahdi Zamani
Visa Research
Palo Alto, CA

Mahnush Movahedi†
Dfinity
Palo Alto, CA

Mariana Raykova
Yale University
New Haven, CT

OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding

Eleftherios Kokoris-Kogias†, Philipp Jovanovic†, Linus Gasser†, Nicolas Gailly†, Ewa Syta*, Bryan Ford†

†École Polytechnique Fédérale de Lausanne, Switzerland, *Trinity College, USA

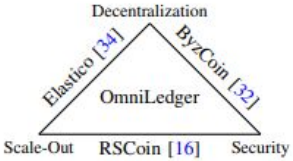


Fig. 1: Trade-offs in current DL systems.

In this work

- ➔ Formally define sharding
- ➔ Explore boundaries of sharding
- ➔ Roadmap to sharding → Divide & Scale
- ➔ Evaluate existing sharding protocols

The model

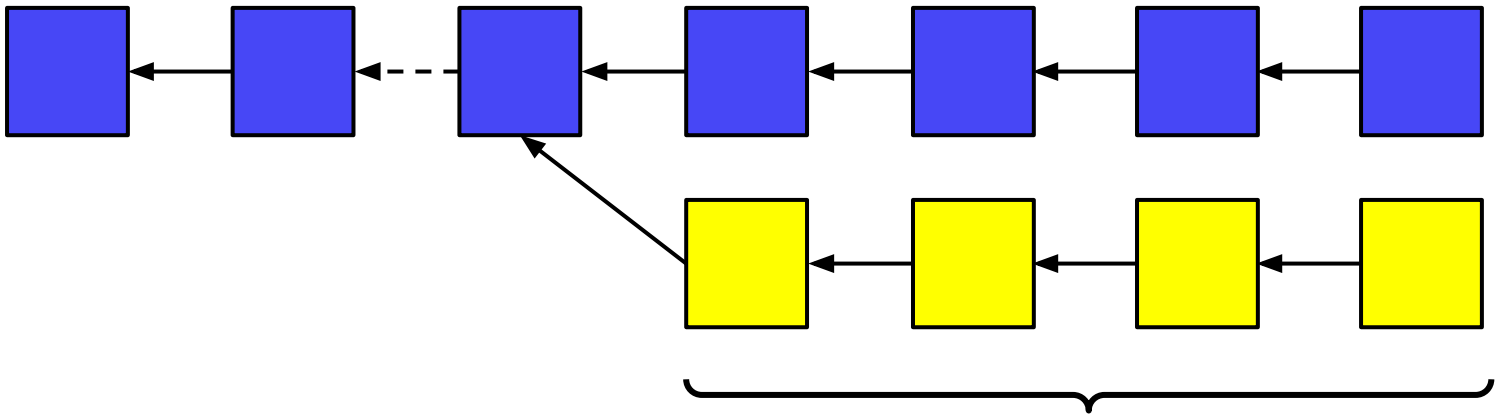
Synchrony

f corruptions

Slowly adaptive adversary

What is sharding?

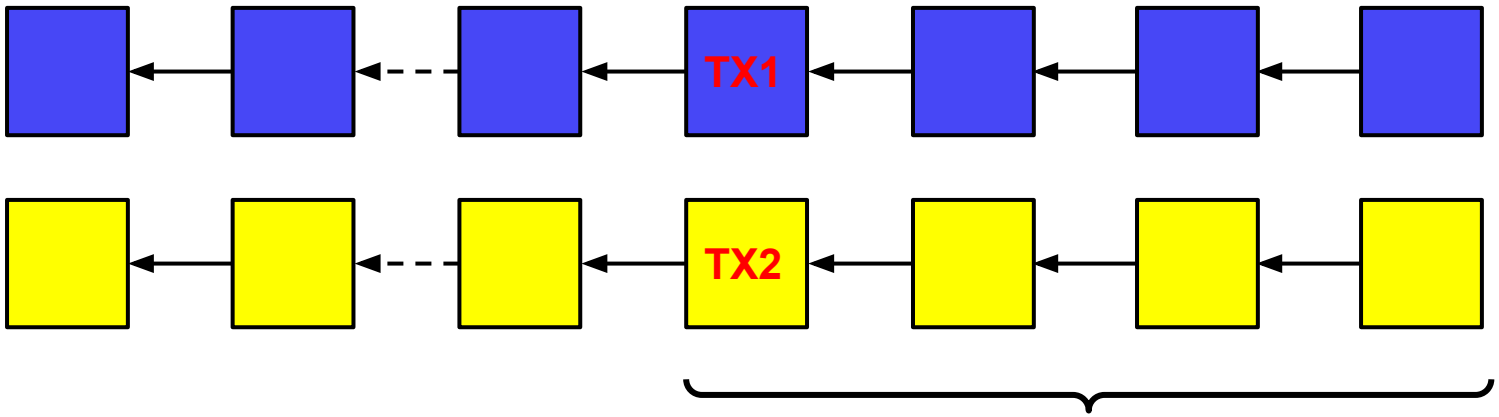
Persistence: **If a transaction is confirmed by an honest party (as “stable”), no honest party will ever disagree about the position of the transaction in the sharded ledger.**



< “depth” parameter k

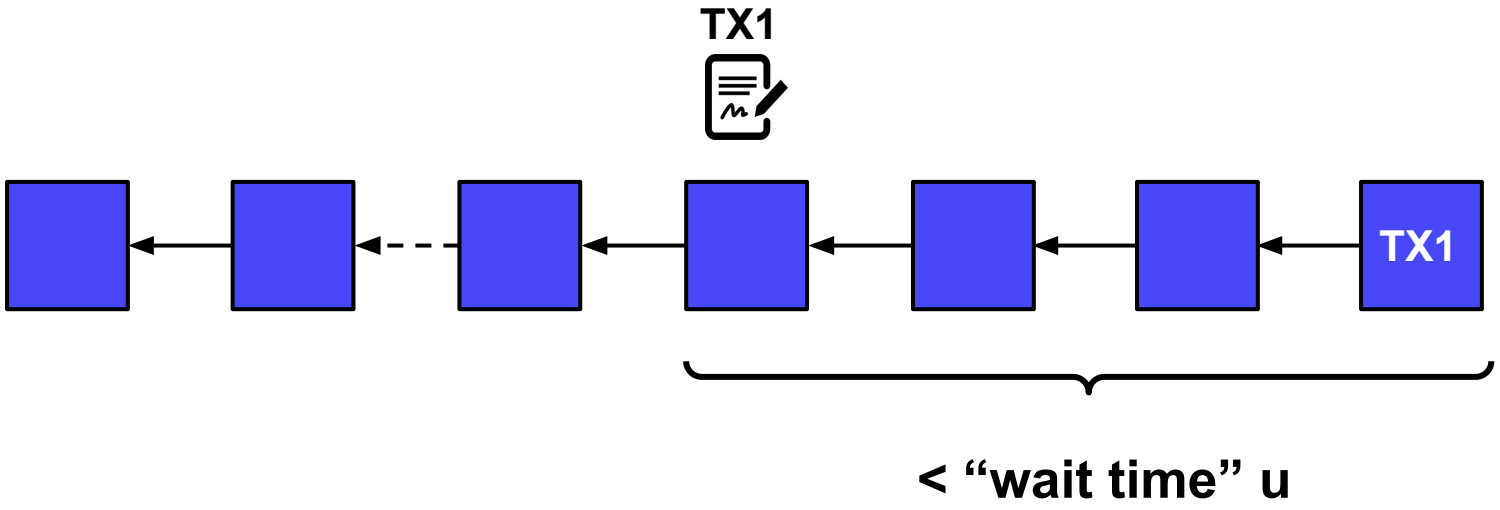
What is sharding?

Consistency: **There is no round in which two honest parties confirm two stable conflicting transactions.**



What is sharding?

Liveness: **If a transaction is broadcast, it will eventually be confirmed by all honest parties.**



What is sharding?

Scalability: A sharded protocol must scale well in bandwidth, computation and storage.

1. **Bandwidth** → Average number of messages per party.

2. **Computation** → Total number of times all parties perform transaction verifications.

3. **Storage** → The total stored data by all parties in comparison to a single database.

What is sharding?

Synchrony

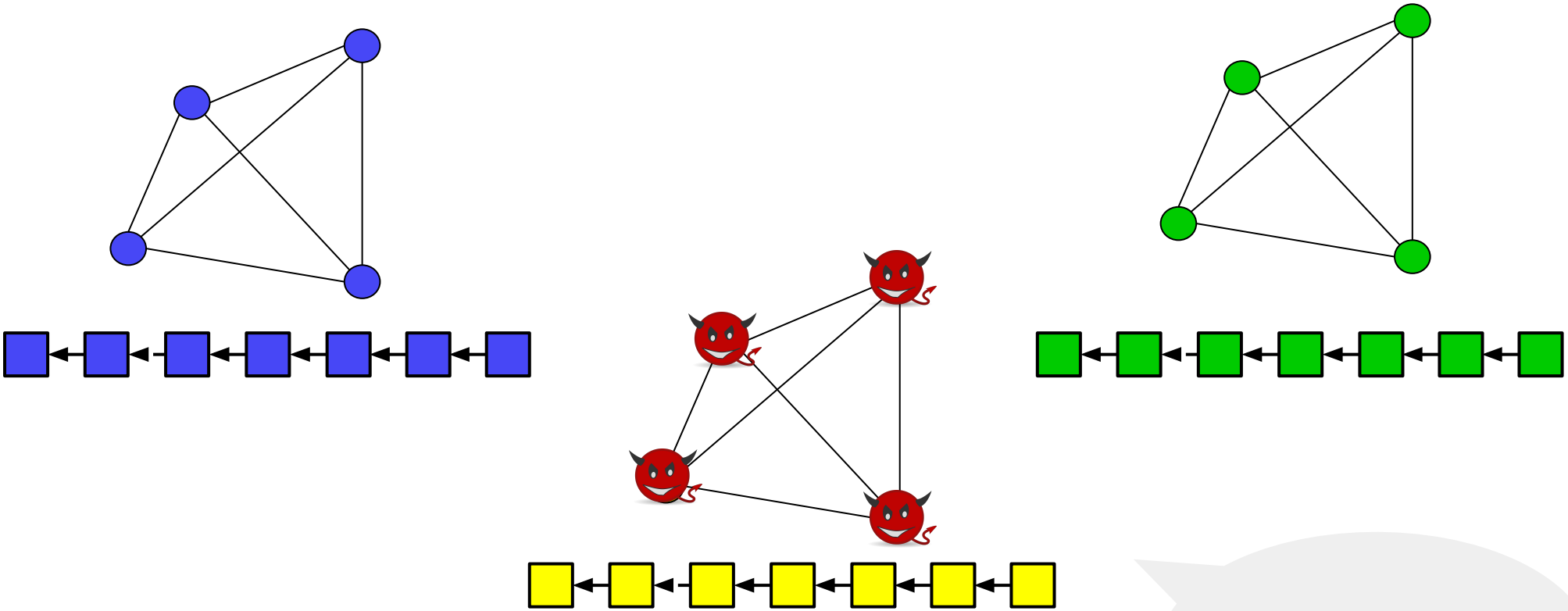
f corruptions

Slowly adaptive adversary

A sharding protocol satisfies persistence, consistency, liveness, and scalability.

The boundaries of sharding

There is no sharding protocol that tolerates an adaptive adversary with f ≥ n/m.



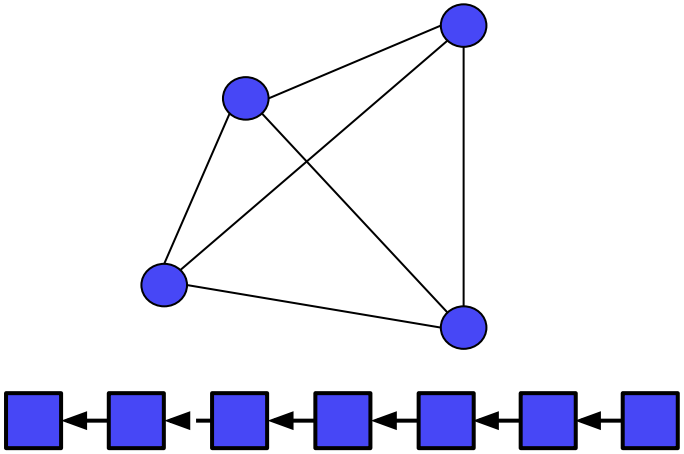
n: number of parties
m: number of shards

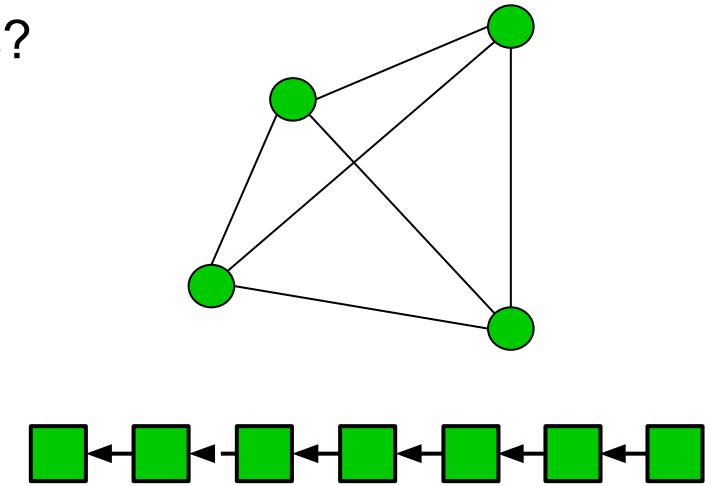
double spend
Consistency!

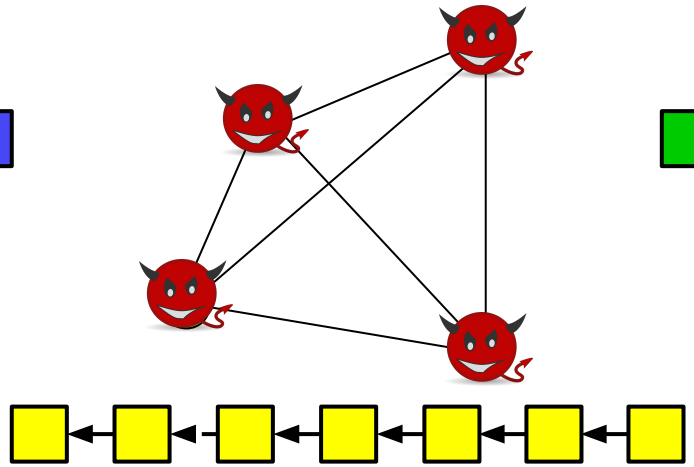
The boundaries of sharding

There is no sharding protocol that tolerates an adaptive adversary with f ≥ n/m.

What if every node verifies cross-shard transactions?
Storage!





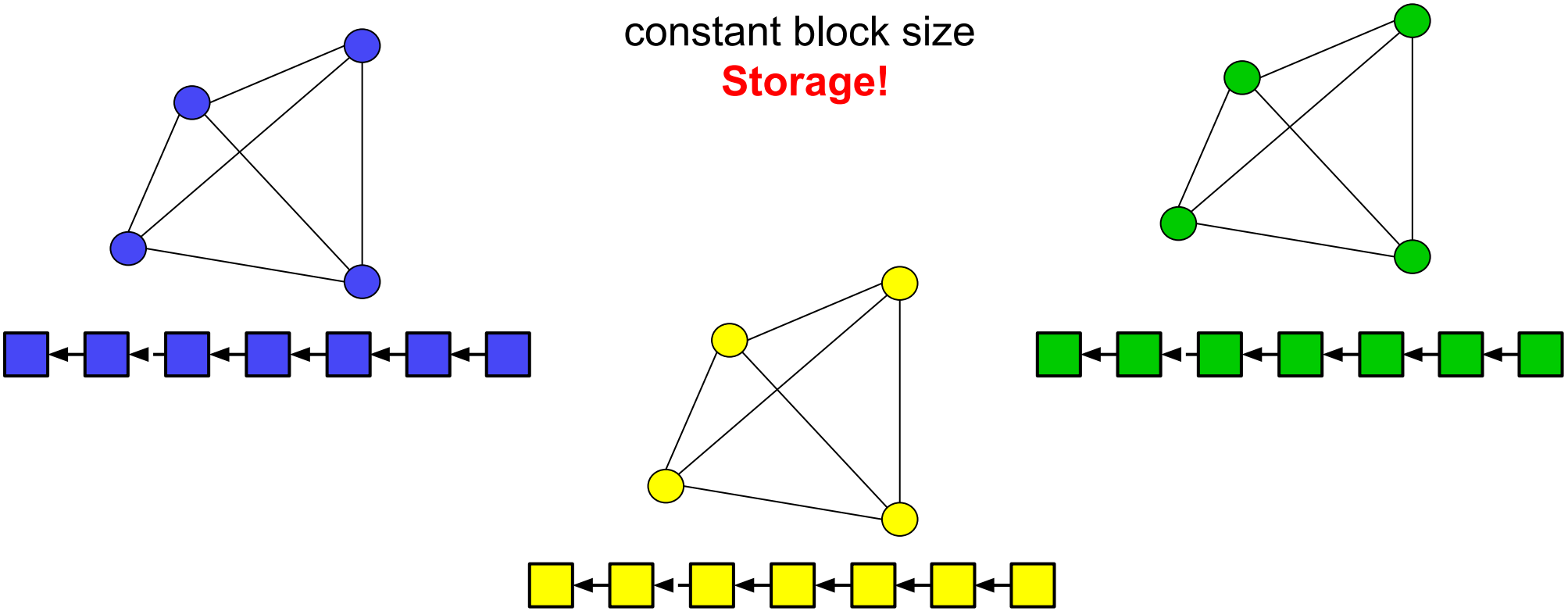


double spend
Consistency!

n: number of parties
m: number of shards

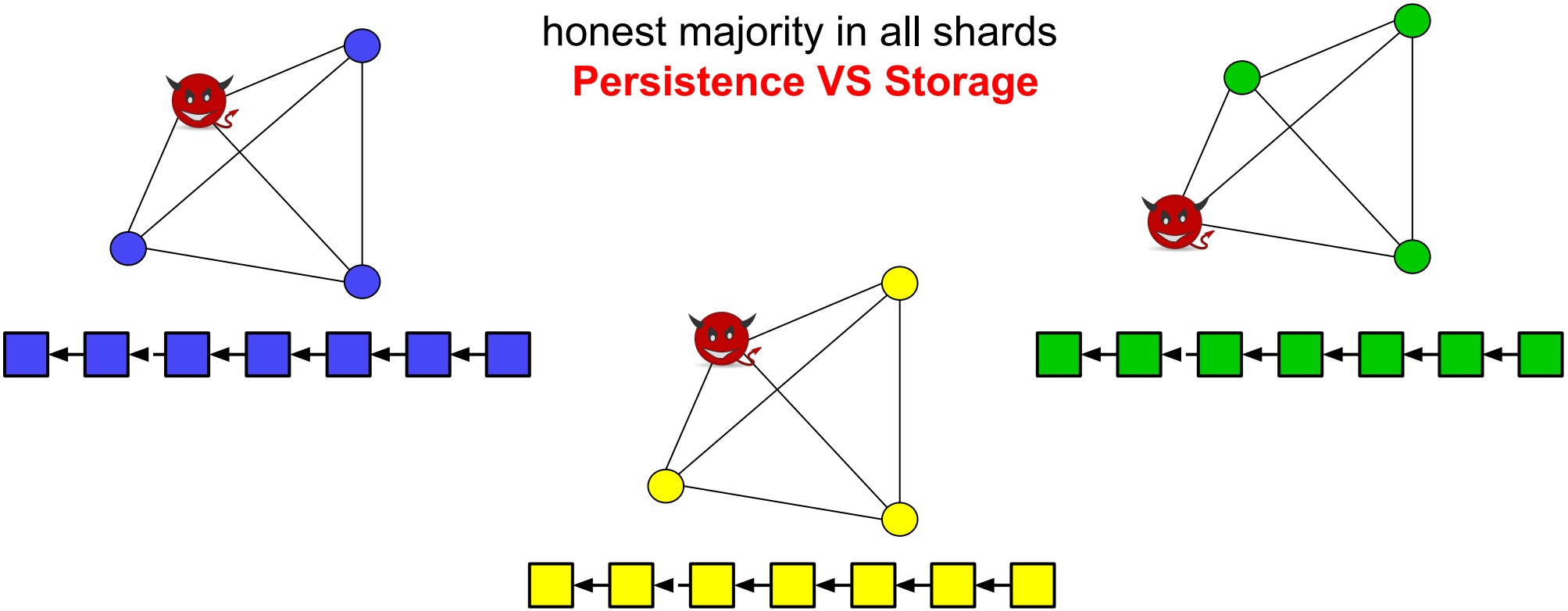
The boundaries of sharding

There is no sharding protocol that requires participants to be light nodes on the shards involved in cross-shard transactions.



The boundaries of sharding

Any sharding protocol can scale up to m shards, where n=cmlogm, c constant, when nodes are randomly shuffled.

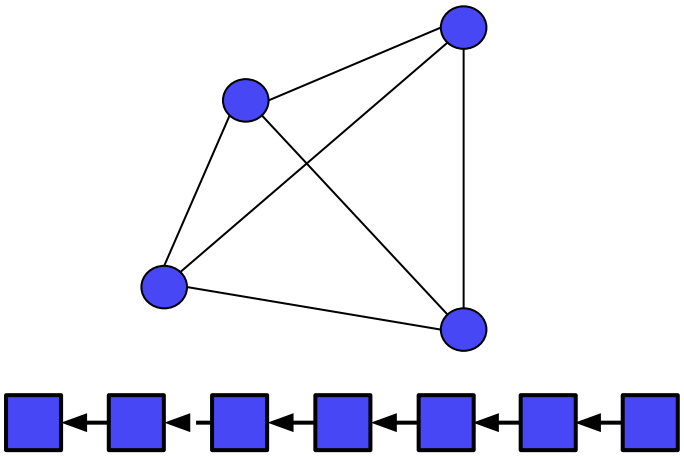


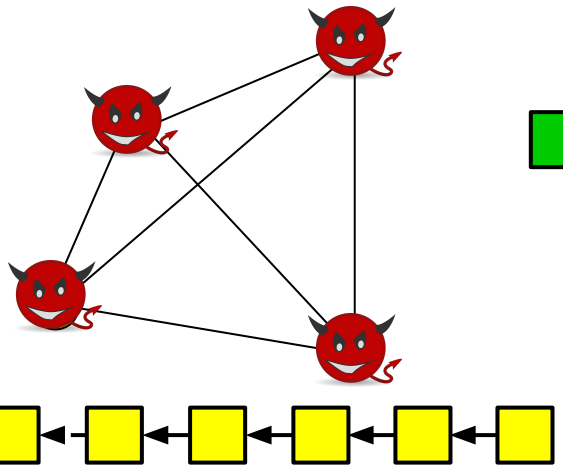
The boundaries of sharding

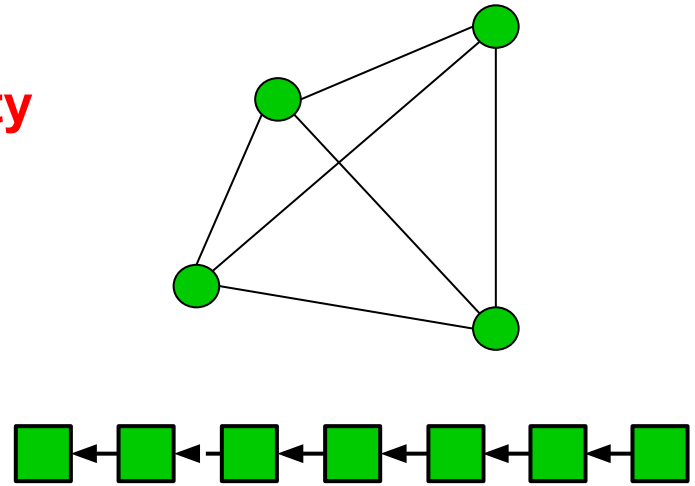
Any sharding protocol must employ verifiable compaction of the state.

download shard history in bootstrapping

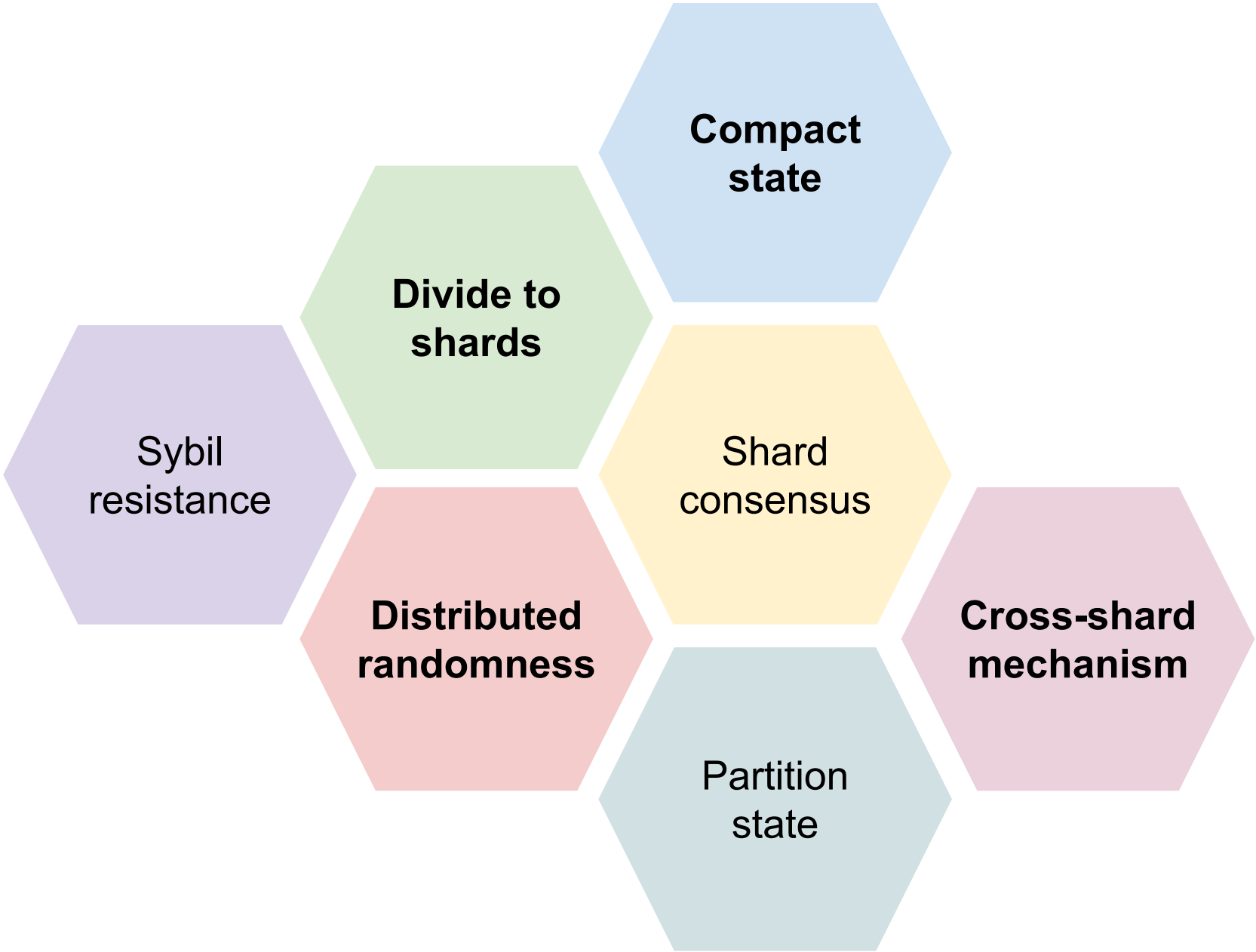
Bandwidth VS Adaptivity





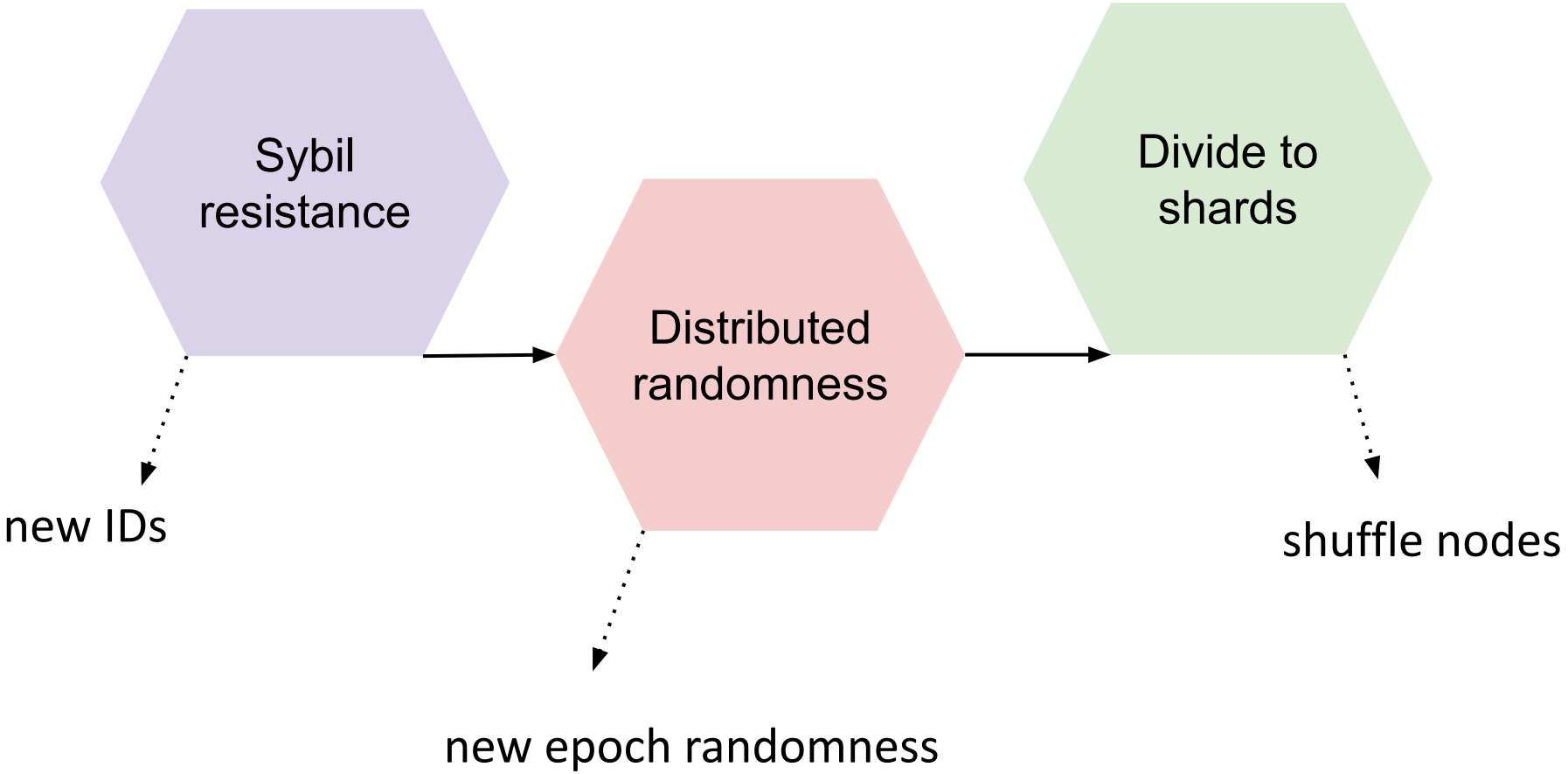


Roadmap to sharding



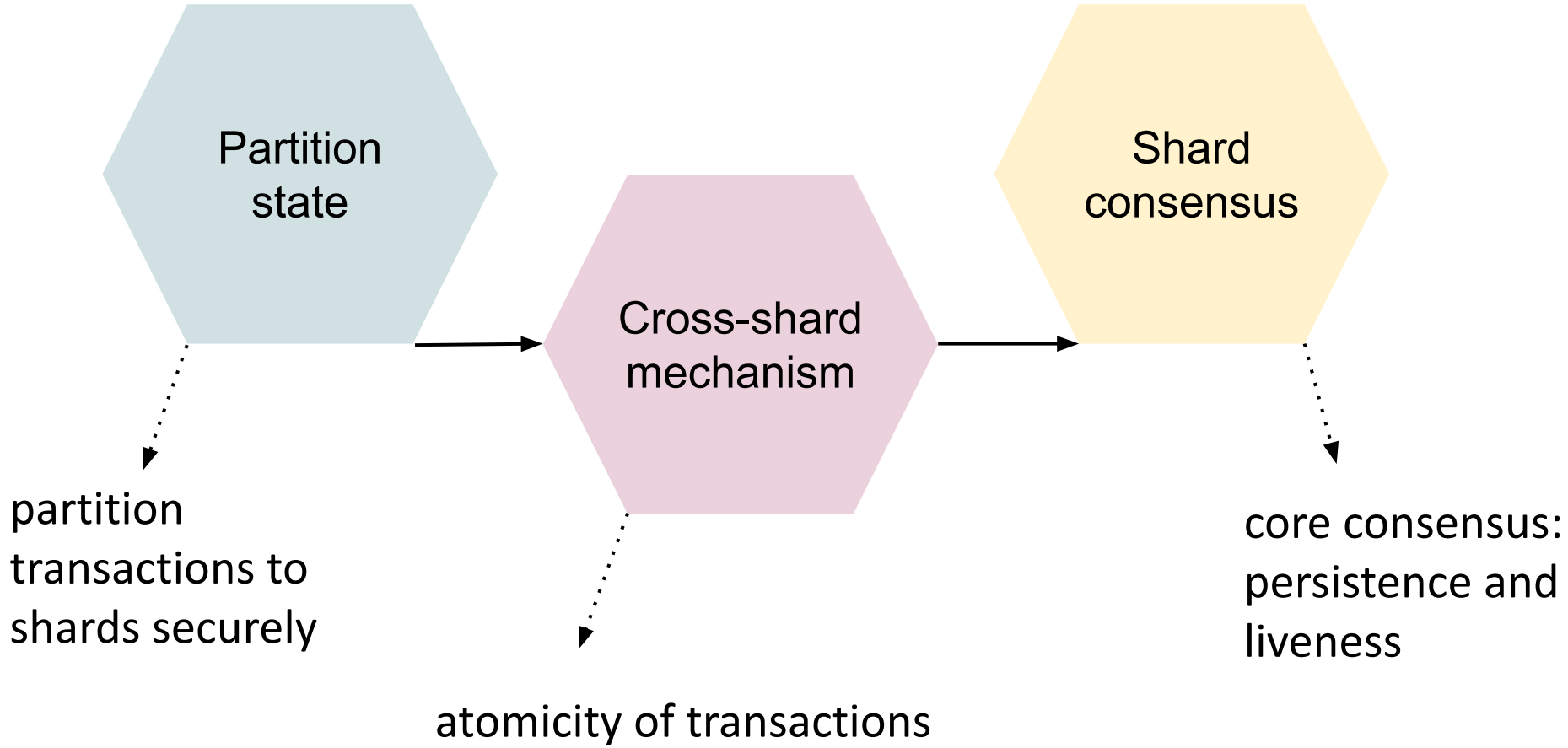
Divide & Scale

Beginning of epoch:



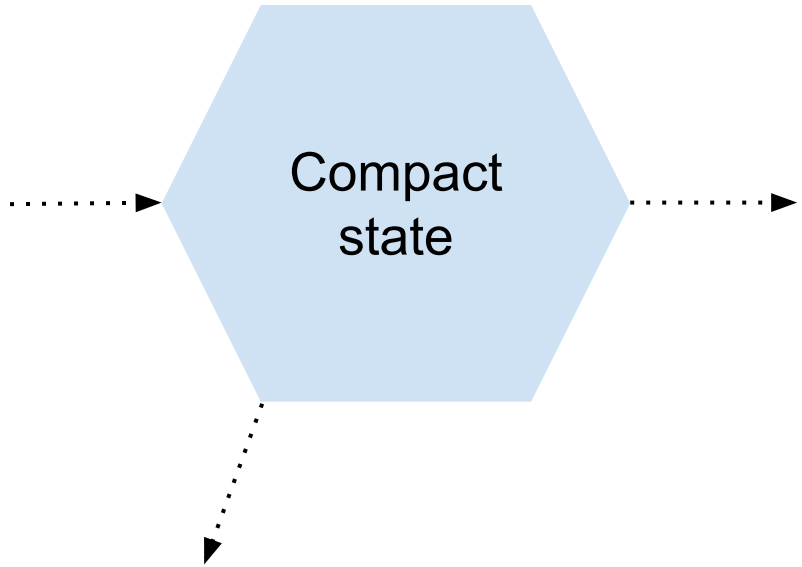
Divide & Scale

Within an epoch:



Divide & Scale

End of epoch:



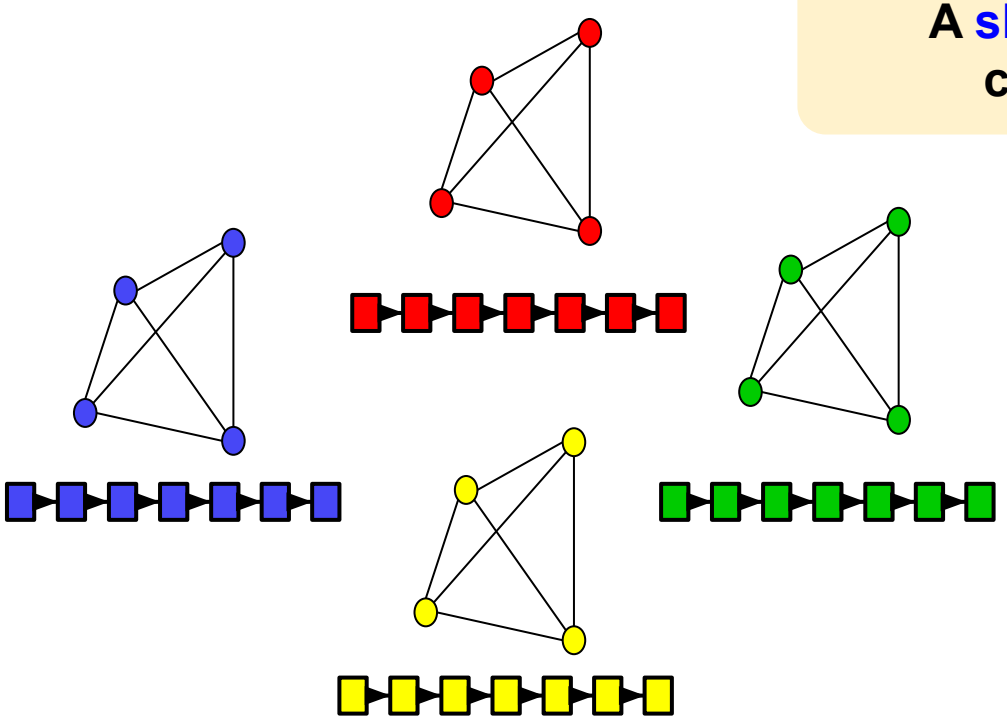
securely compress the epoch’s data and broadcasts

Evaluation of sharding protocols

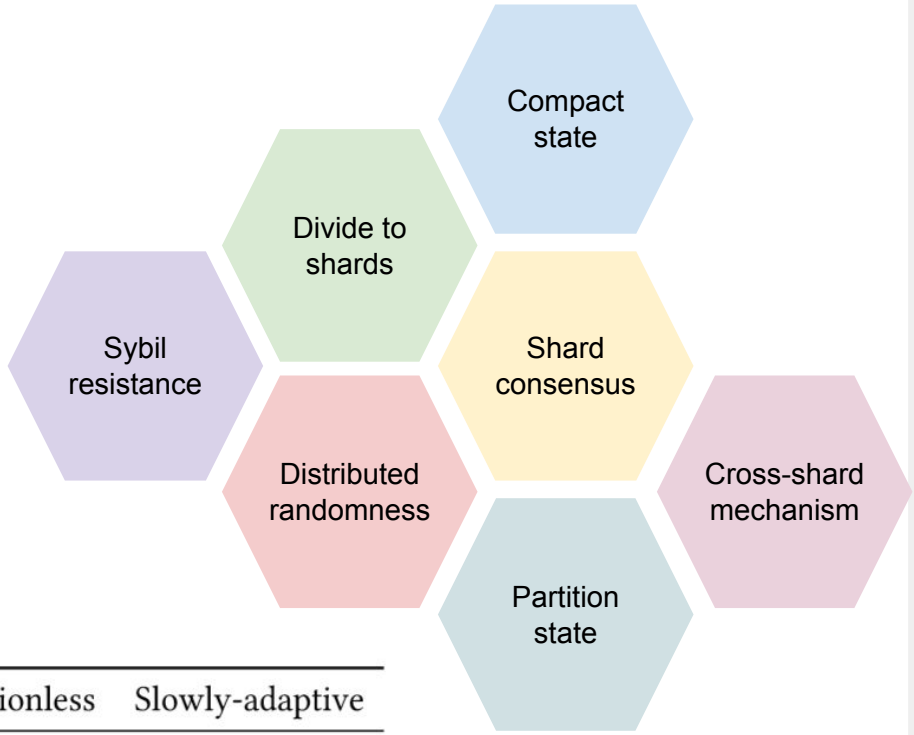
Protocol	Persistence	Consistency	Liveness	Scalability	Permissionless	Slowly-adaptive
Elastico	✓	✗	✓	✗	✓	✓
Monoxide	✓	✓	✓	✗	✓	✓
OmniLedger	✓	✓	✗	✓	✓	✓
RapidChain	✓	✓	✓	✓	✓	~
Chainspace	✓	✓	✓	✓	✗	✗

~ constant-adaptive adversary

Recap



A sharding protocol satisfies persistence, consistency, liveness and scalability.



What is feasible with sharding?

Protocol	Persistence	Consistency	Liveness	Scalability	Permissionless	Slowly-adaptive
Elastico	✓	✗	✓	✗	✓	✓
Monoxide	✓	✓	✓	✗	✓	✓
OmniLedger	✓	✓	✗	✓	✓	✓
RapidChain	✓	✓	✓	✓	✓	~
Chainspace	✓	✓	✓	✓	✗	✗


TECHNISCHE
UNIVERSITÄT
WIEN
Vienna | Austria
FAKULTÄT FÜR
!NFORMATIK
Faculty of Informatics
S&P
SECURITY &
PRIVACY
GROUP

Thank you!