



TECHNISCHE
UNIVERSITÄT
WIEN
Vienna | Austria



FAKULTÄT FÜR
INFORMATIK

Faculty of Informatics

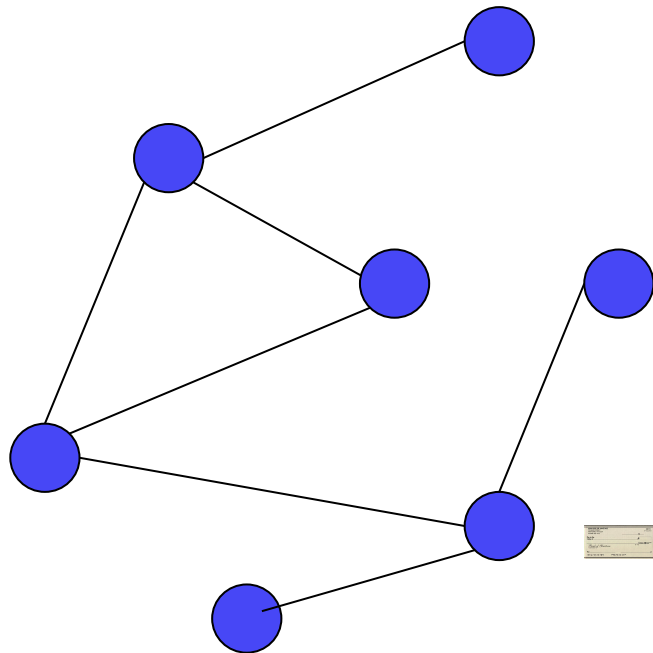
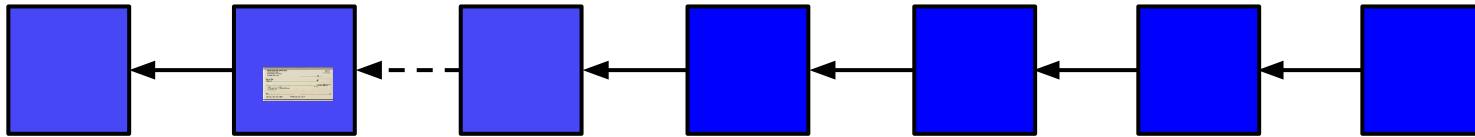


SECURITY &
PRIVACY
GROUP

Divide & Scale: Formalization and Roadmap to Secure Sharding

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

What is a blockchain?

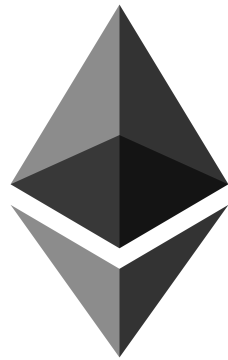


A blockchain is a protocol run among nodes in a *permissionless* network to reach *probabilistic agreement on the order of transactions*.

Can cryptocurrencies scale?



7 tx/s



30 tx/s

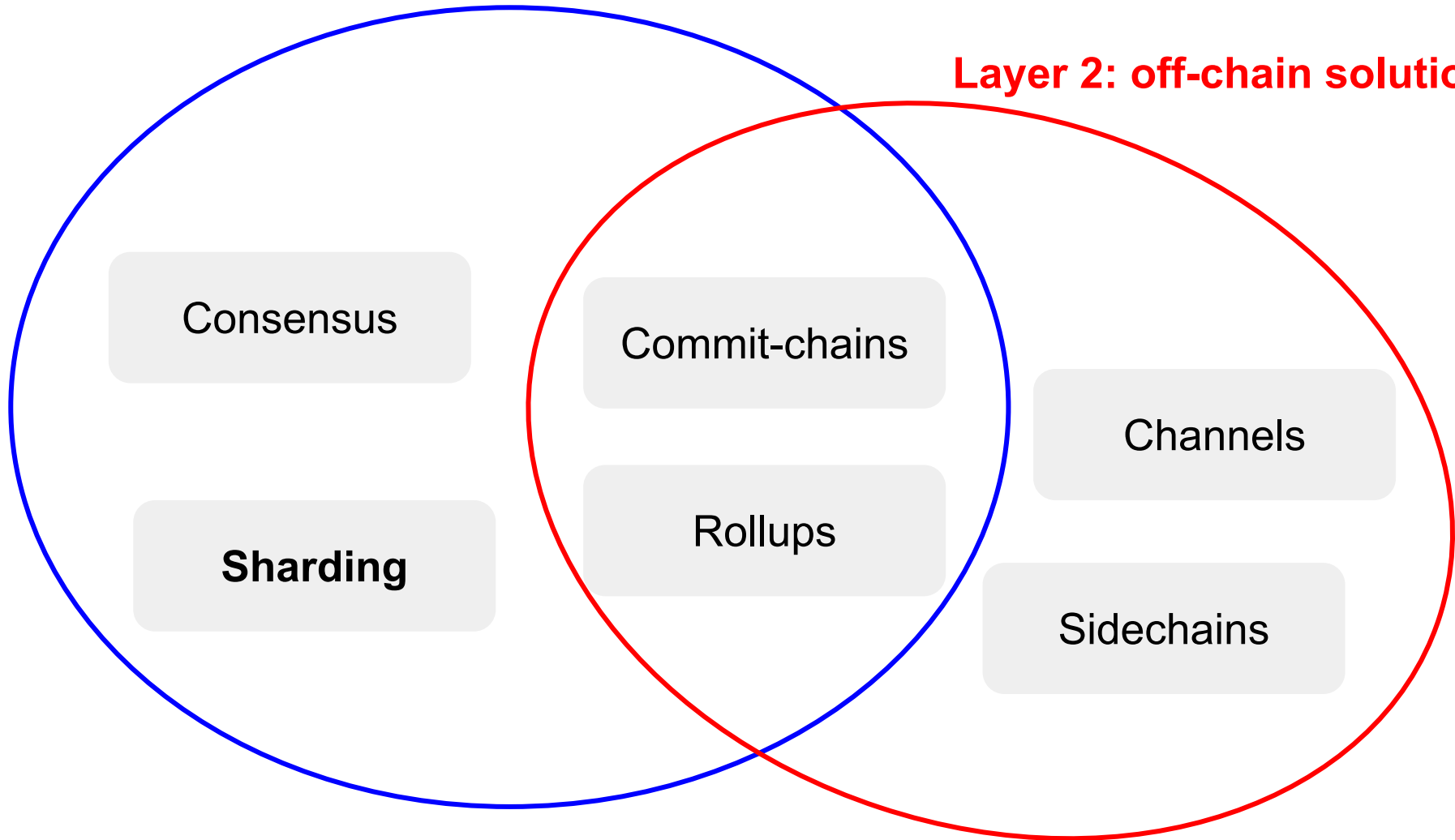


65.000 tx/s

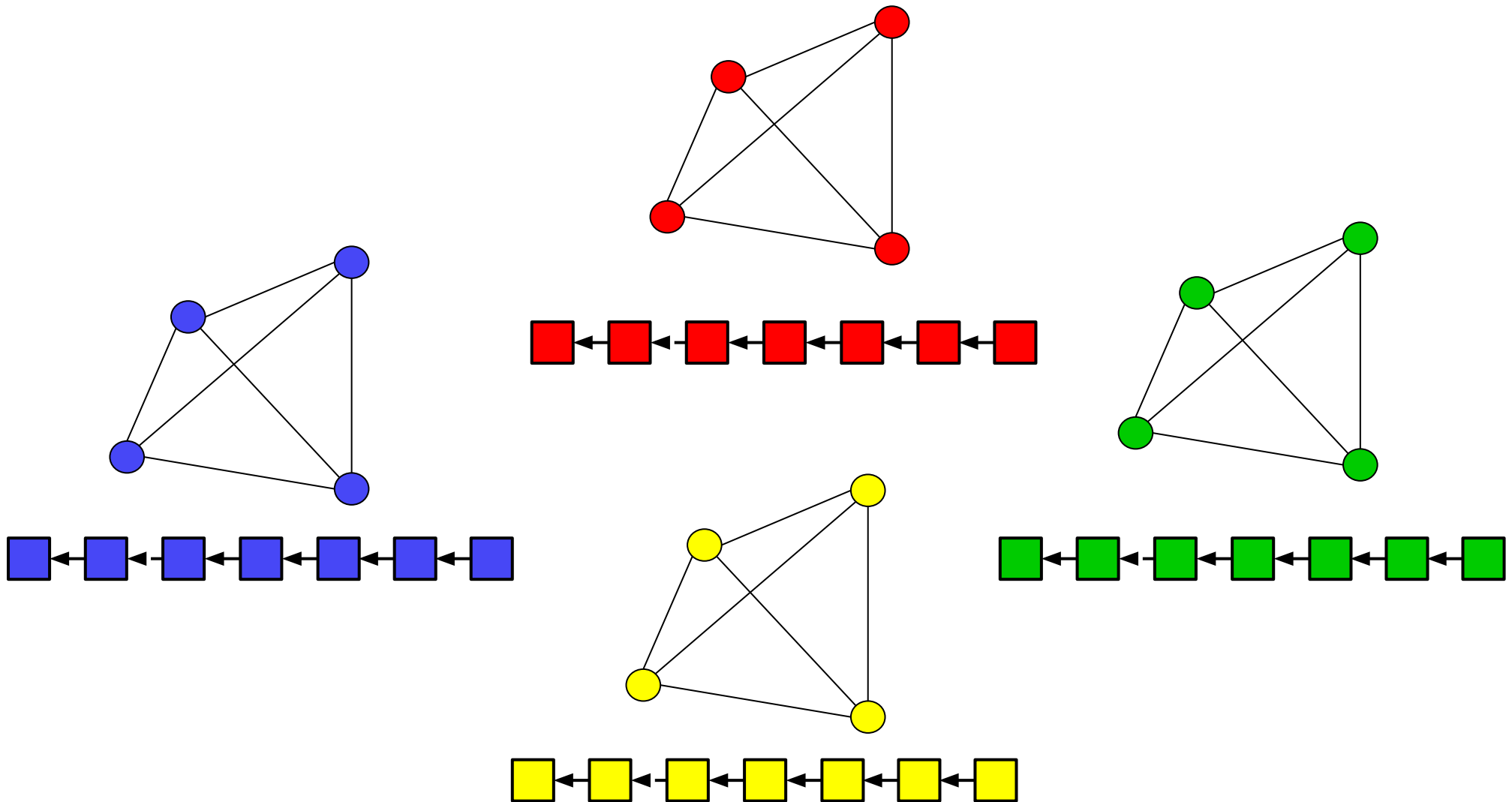
Scaling solutions

Layer 1: on-chain solutions

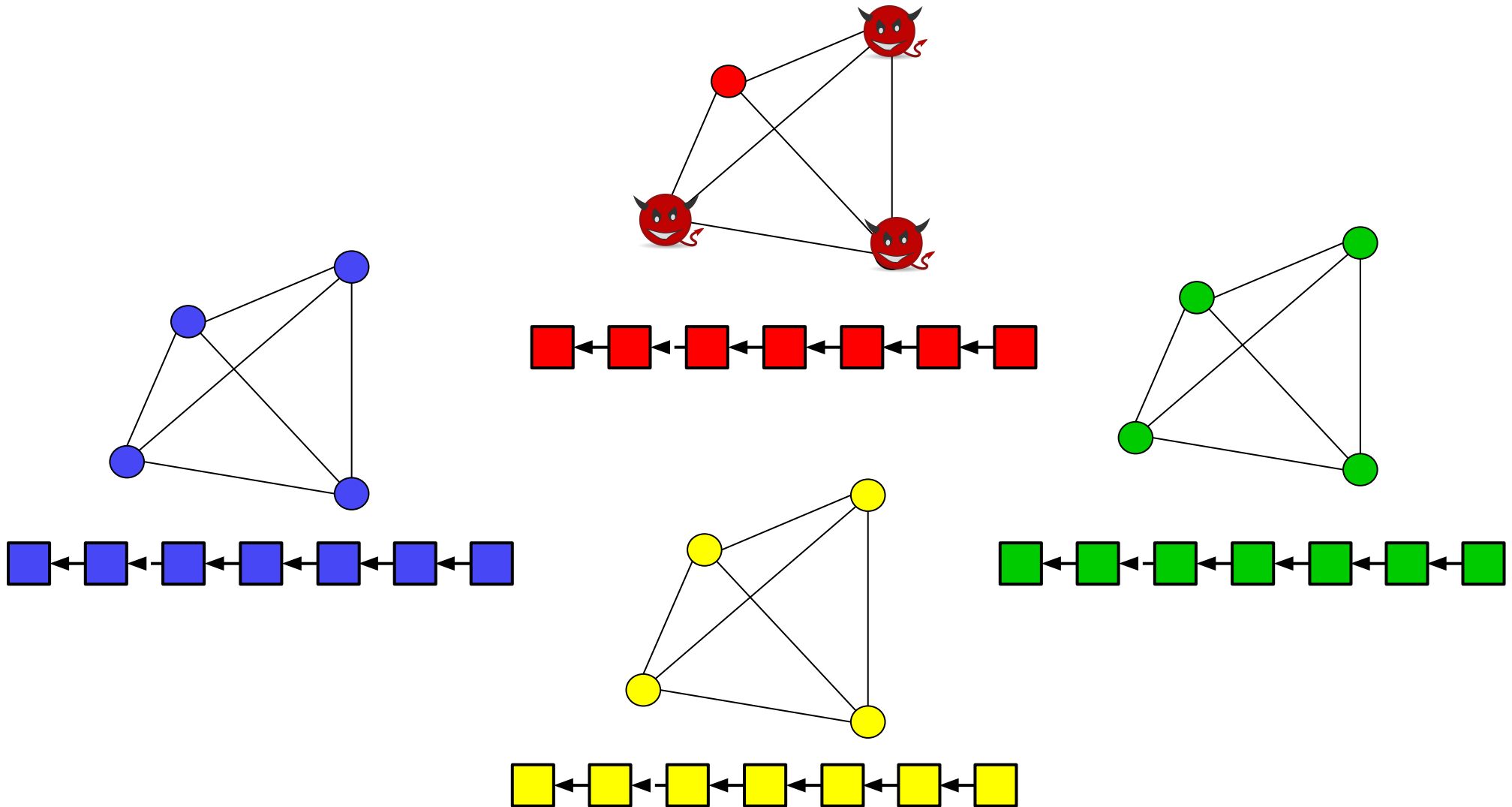
Layer 2: off-chain solutions



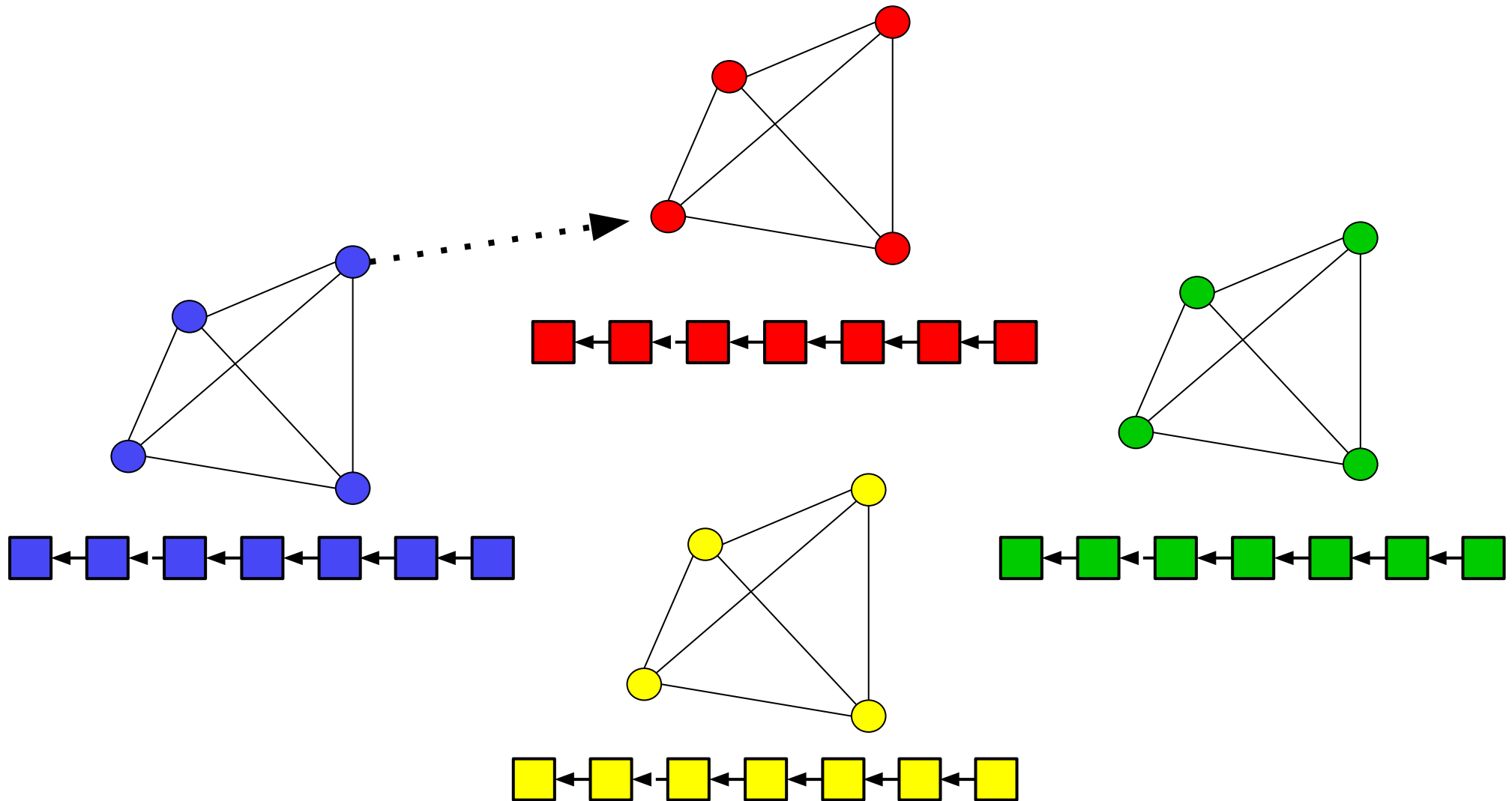
What is sharding?



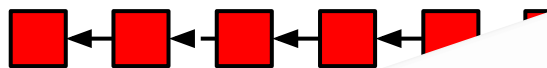
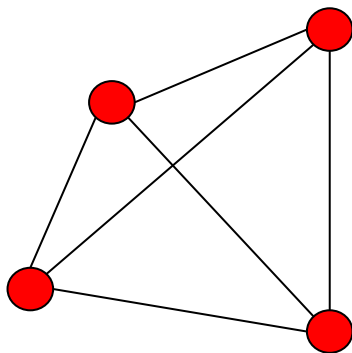
What is sharding?



What is sharding?



What is sharding?



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

Abstract—Designing a secure permissionless distributed ledger (blockchain) that performs on par with centralized payment processors, such as Visa, is a challenging task. Most existing distributed ledgers are unable to scale-out, *i.e.*, to grow their total processing capacity with the number of validators; and those that do, compromise security or decentralization. We present OmniLedger, a novel scale-out distributed ledger that preserves long-term security under permissionless operation. It ensures security and correctness by using a bias-resistant public-randomness protocol for choosing large, statistically representative shards that process transactions, and by introducing an efficient cross-shard commit protocol that atomically handles transactions affecting multiple shards. OmniLedger also optimizes performance

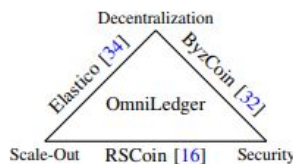


Fig. 1: Trade-offs in current DL systems.

permissionless decentralization. To achieve this goal, OmniLedger

A Secure Sharding Protocol For Open Blockchains

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

Kunal Baweja
National University of Singapore
kwejaku@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

National University of Singapore
Chan...
chaok...
Nations...
pratee...

RapidChain: Scaling Blockchain via Full Sharding

Mahdi Zamani
Visa Research
Palo Alto, CA

Mahmush Movahedi[†]
Dfinity
Palo Alto, CA

Mariana Raykova
Yale University
New Haven, CT

Abstract
performance and scalability limitations of current l...
the overheads of processing transactions among...
in parallel to maximize performance while requi...
m, and storage per node, allowing the system to...
ed blockchain protocols still require a linear amou...
per transaction, and hence, attain only partiall...
introduces a major bottleneck to the throughpu...
scalability, these protocols achieve weak security...
1/8 and 1/4) or high failure probability, or th...
limit their applicability to mainstream payment...
sharding-based public blockchain protocol that is...
on of its participants, and achieves complete sha...
ge overhead of processing transactions without a...
optimal intra-committee consensus algorithm that...
sure robustness. Using an efficient cross-shar...
gossiping transactions to the entire network. C...
process (and confirm) more than 7,300 tx/sec w...
seconds in a network of 4,000 nodes with an over...

es, such as Bitcoin and 250 similar alt-coins, em...
a blockchain protocol — a mechanism for a dis...
of computational nodes to periodically agree on...
challenge in security, that of designing a *highly*...
protocol open to manipulation by byzantine or...
les. Bitcoin's blockchain agreement proto...
does not scale: it processes 3–7 transac...
irrespective of the available computa...
a new distributed agreement proto...
ains called ELASTICO. ELASTICO...
nearly with available computation...
blocks selected per unit time, the...
total computational power, the...
ions and tolerates byzan...
ites, each of which min...
ards"). While sharding...
ICO is the first candi...
nce of byzantine ad...
on EC2 with up to...
ing properties.

the fraction of malicious processors is...
Processors have no inherent identities, a...
infrastructure to establish identities for p...
can choose a set (e.g. block) of transac...
the blockchain; the goal of the protocol is t...
processors agree on one set of transac...
At a high level, the blockchain protocol is...
selects one processor per epoch (say 10 minutes...
proposal that everyone adopts, thus requir...
cast to reach agreement [1]. There may be tempo...
ment if two proposals occur at the same time...
high probability, one proposal will be estab...
longest blockchain. Nakamoto consensus uses a pro...
(PoW) mechanism to probabilistically elect the leader...
a fair choice of leaders. In terms of scale, Bitcoin emp...
ions of CPUs worth of computational power today (by obser...
systems [2]), and is one of the largest completely decentral...
of such scale.
Unfortunately, Bitcoin's transaction throughput does not...
well. The Bitcoin network consumes massive computati...
and presently processes up to 7 transactions per computati...
centralized fiat payment processing systems...
Visa are reported to processing 1,200...
second [4, 5]. The demand fre...
orders of magnitude high...

In this work

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

The model

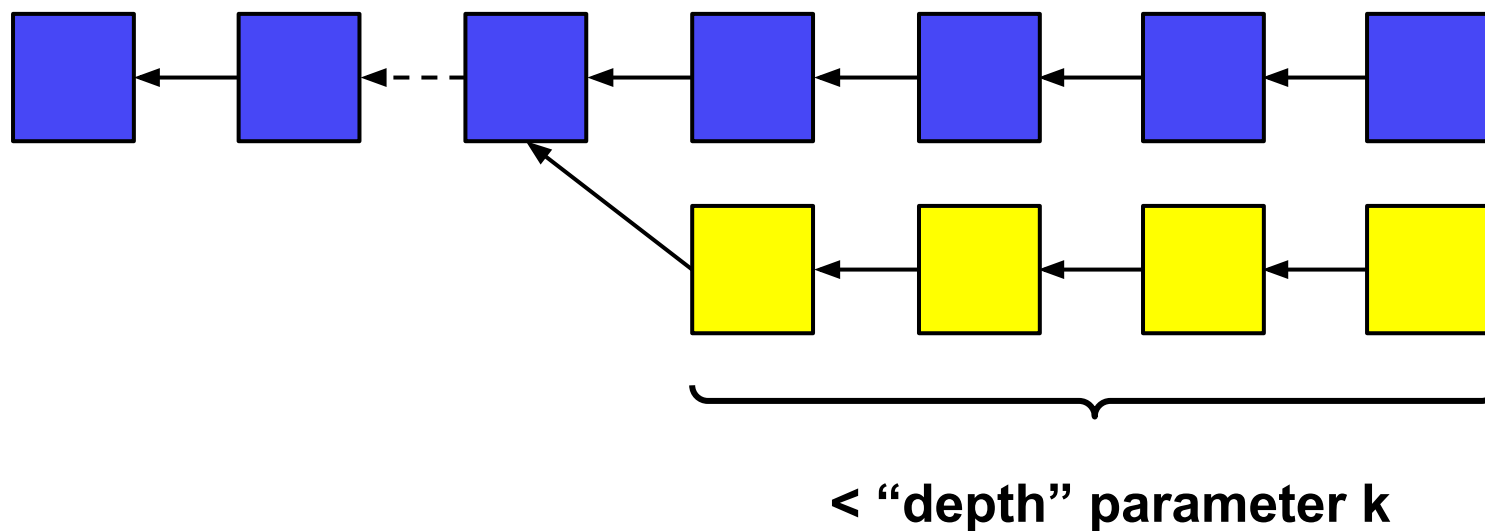
Synchrony

f corruptions

**Slowly adaptive
adversary**

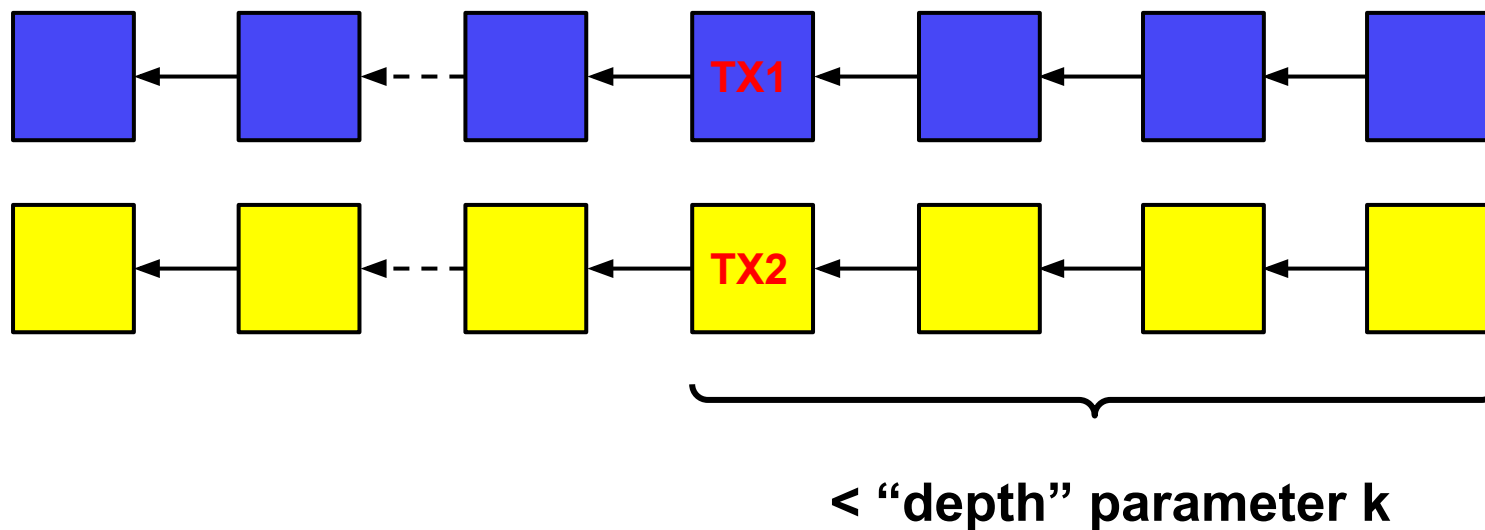
What is sharding?

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.



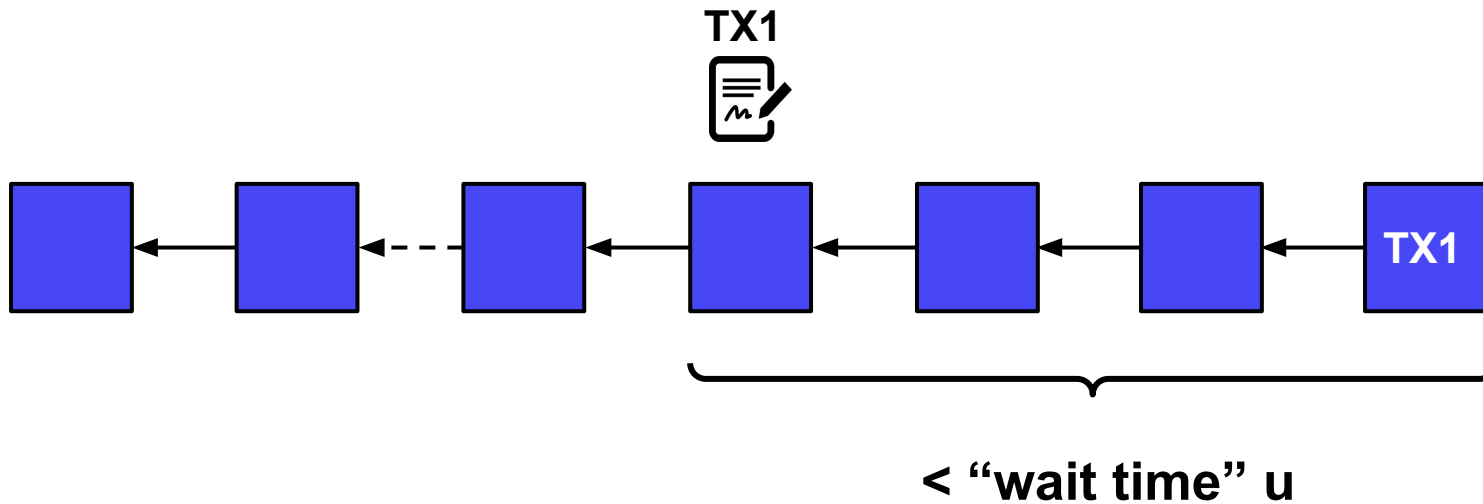
What is sharding?

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

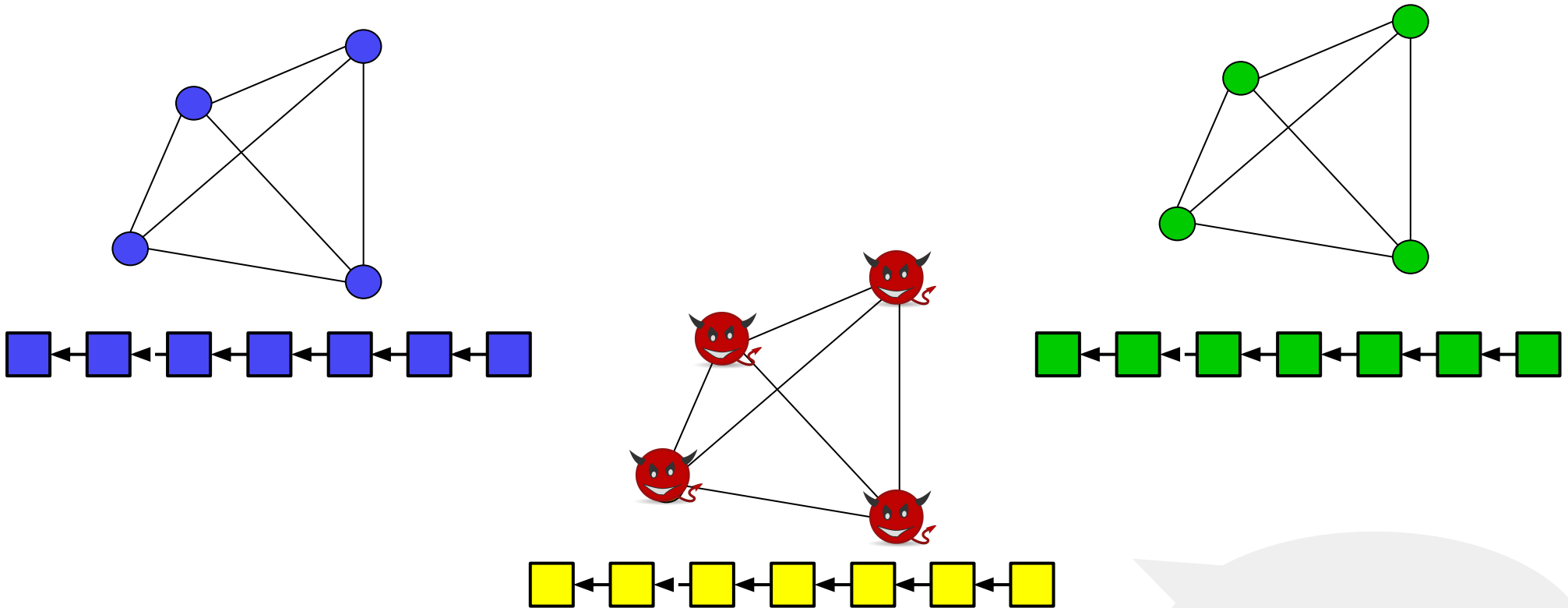
f corruptions

**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 $f \geq n/m$.



n: number of parties
m: number of shards

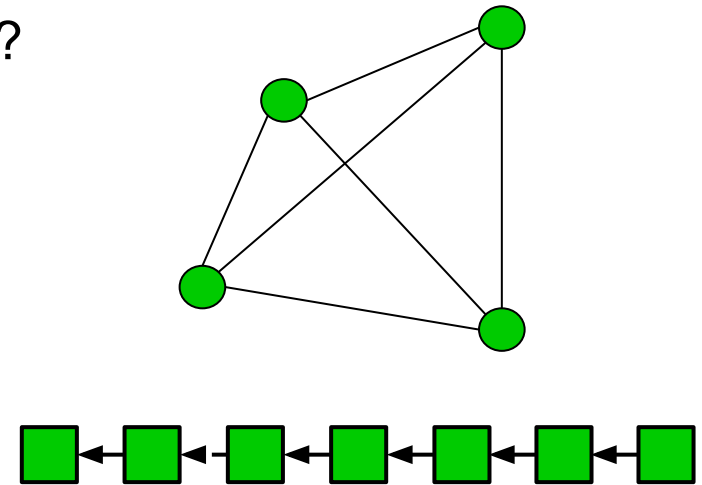
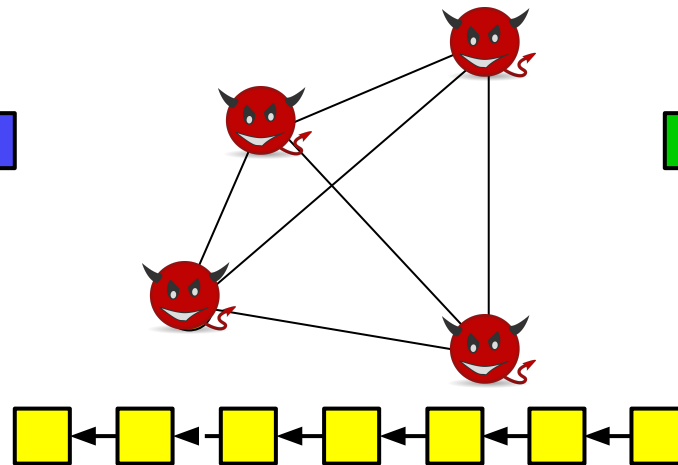
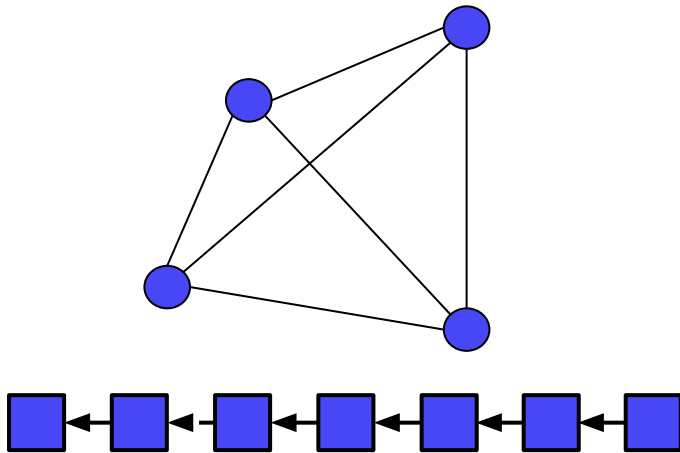
double spend
Consistency!

The boundaries of sharding

There is no sharding protocol that tolerates an **adaptive adversary** with $f \geq n/m$.

What if every node verifies cross-shard transactions?

Storage!

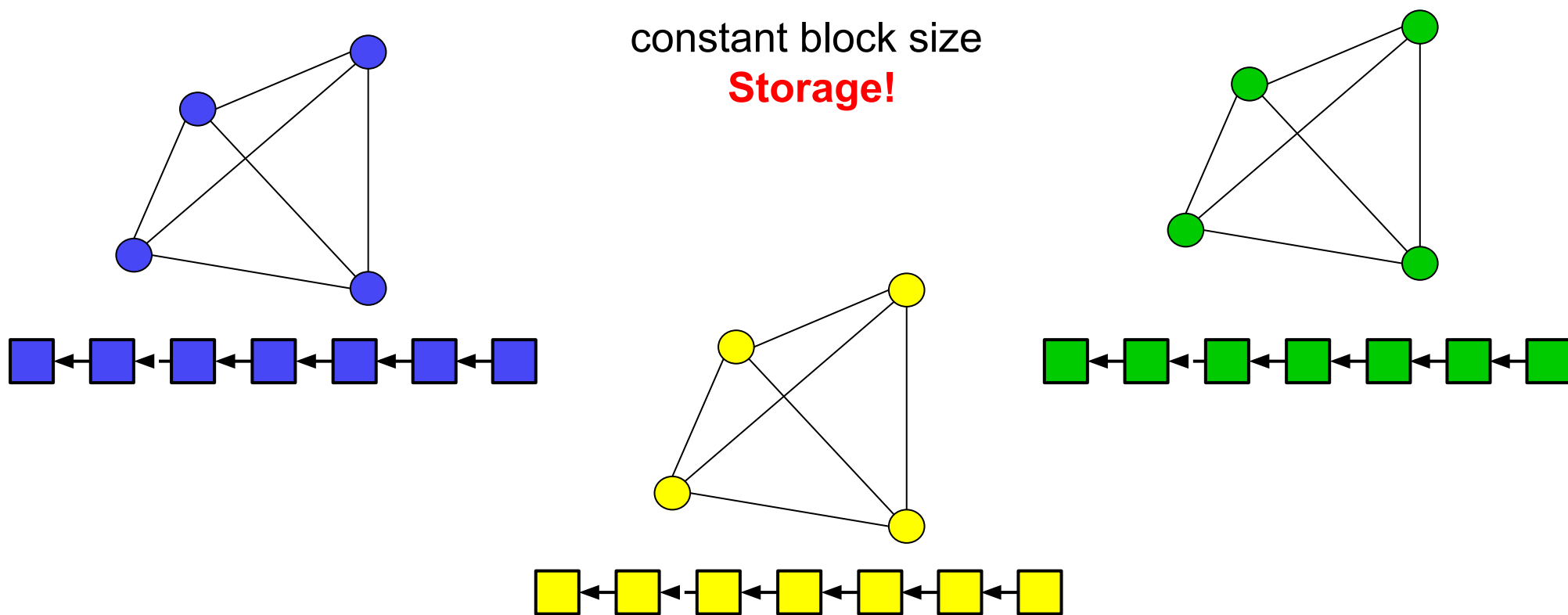


double spend
Consistency!

n: number of parties
m: number of shards

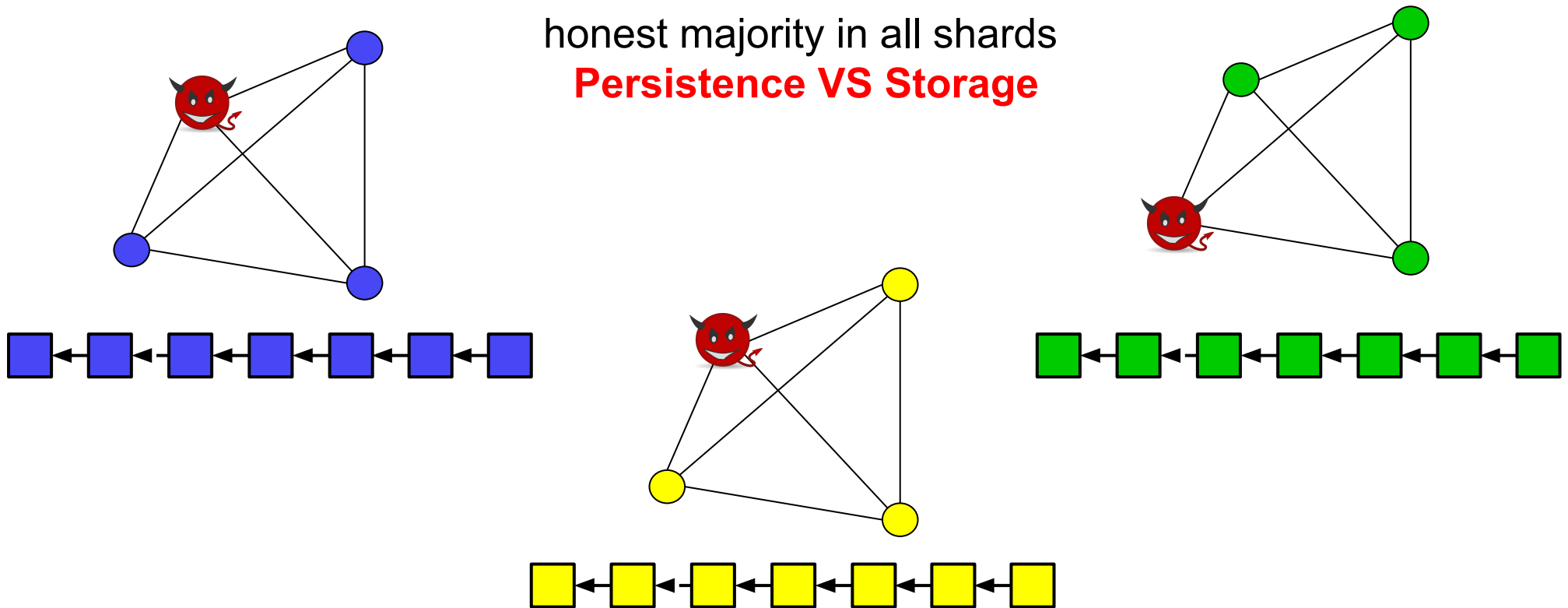
The boundaries of sharding

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



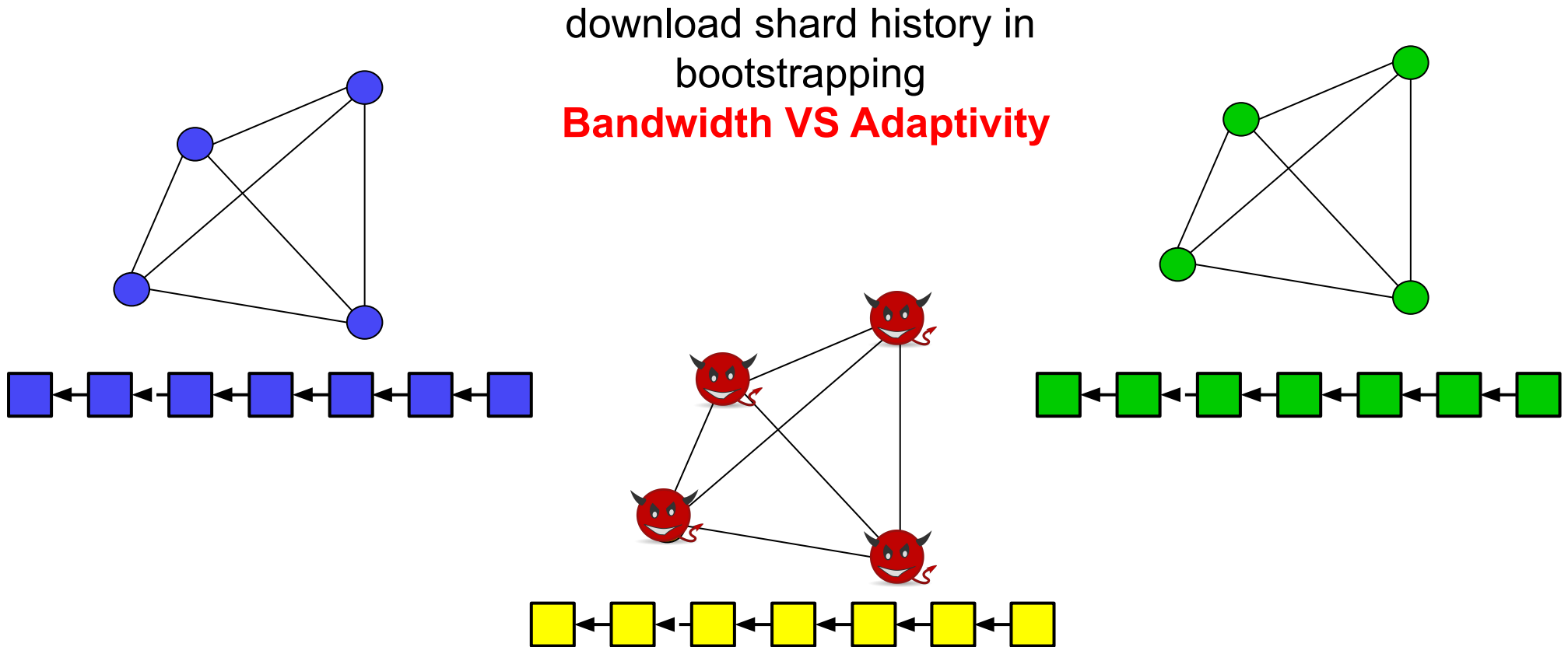
The boundaries of sharding

Any sharding protocol can **scale up to m shards**, where **$n = cm \log m$** , c constant, when nodes are randomly shuffled.

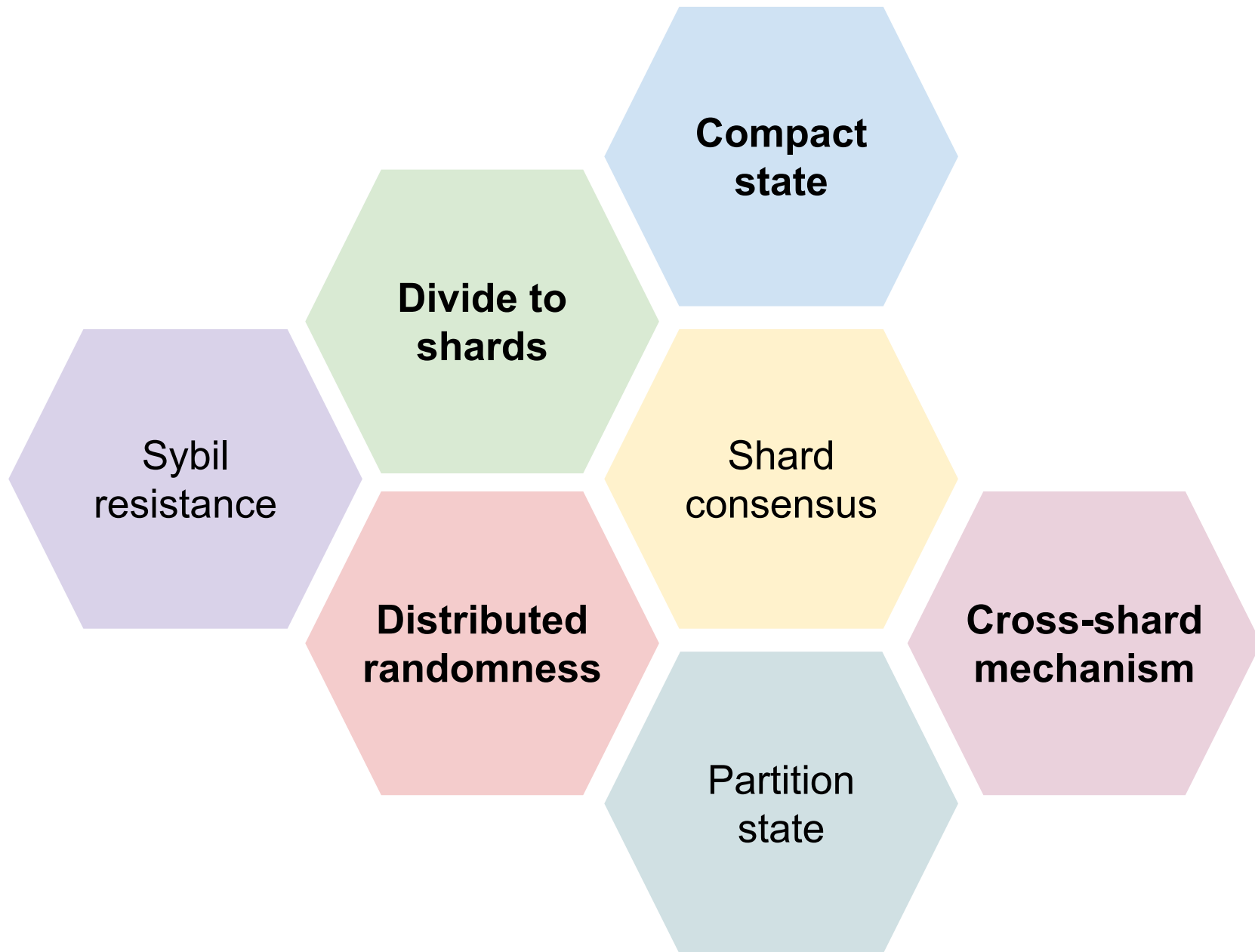


The boundaries of sharding

Any sharding protocol must employ **verifiable compaction of the state.**

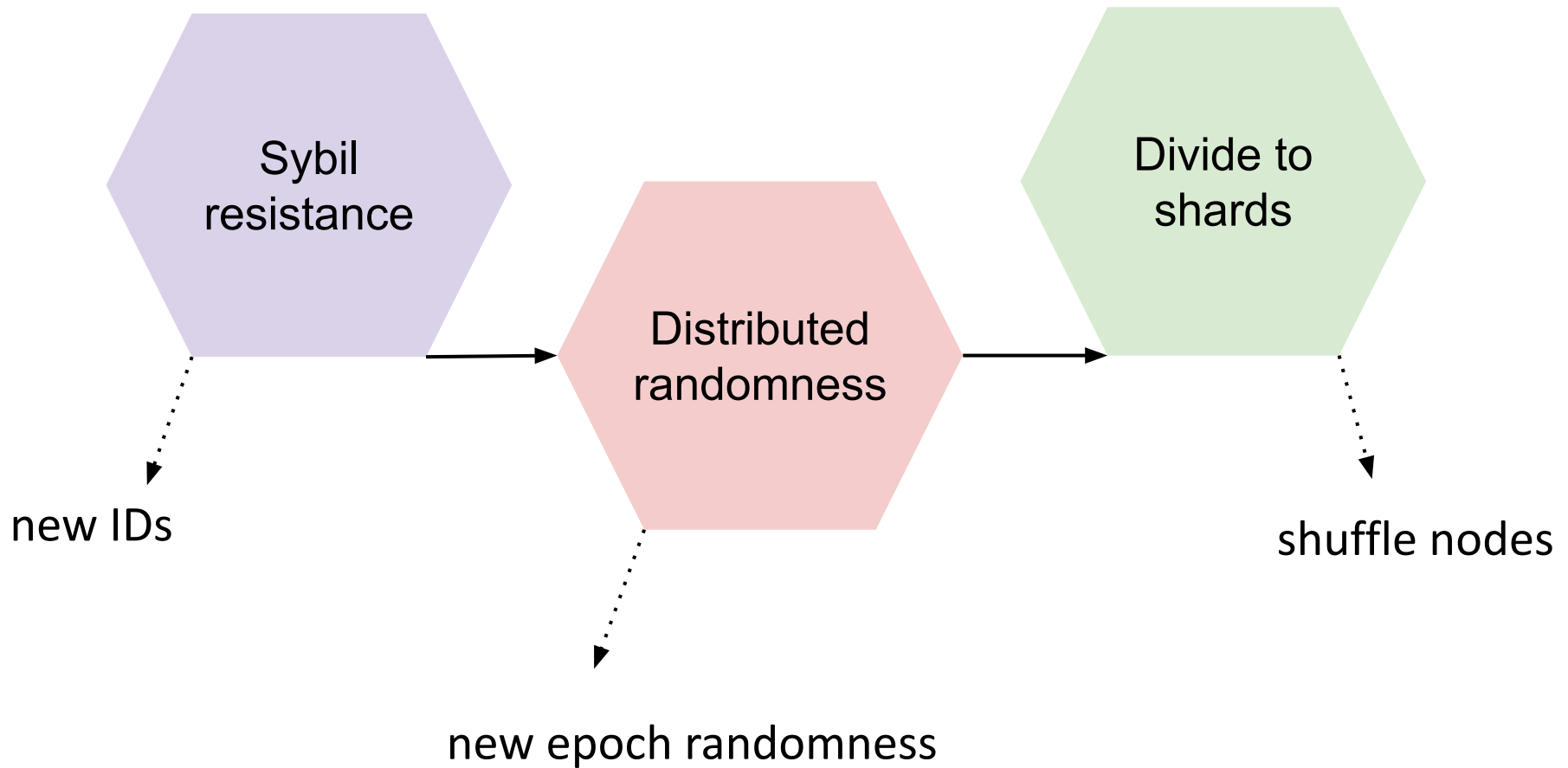


Roadmap to sharding



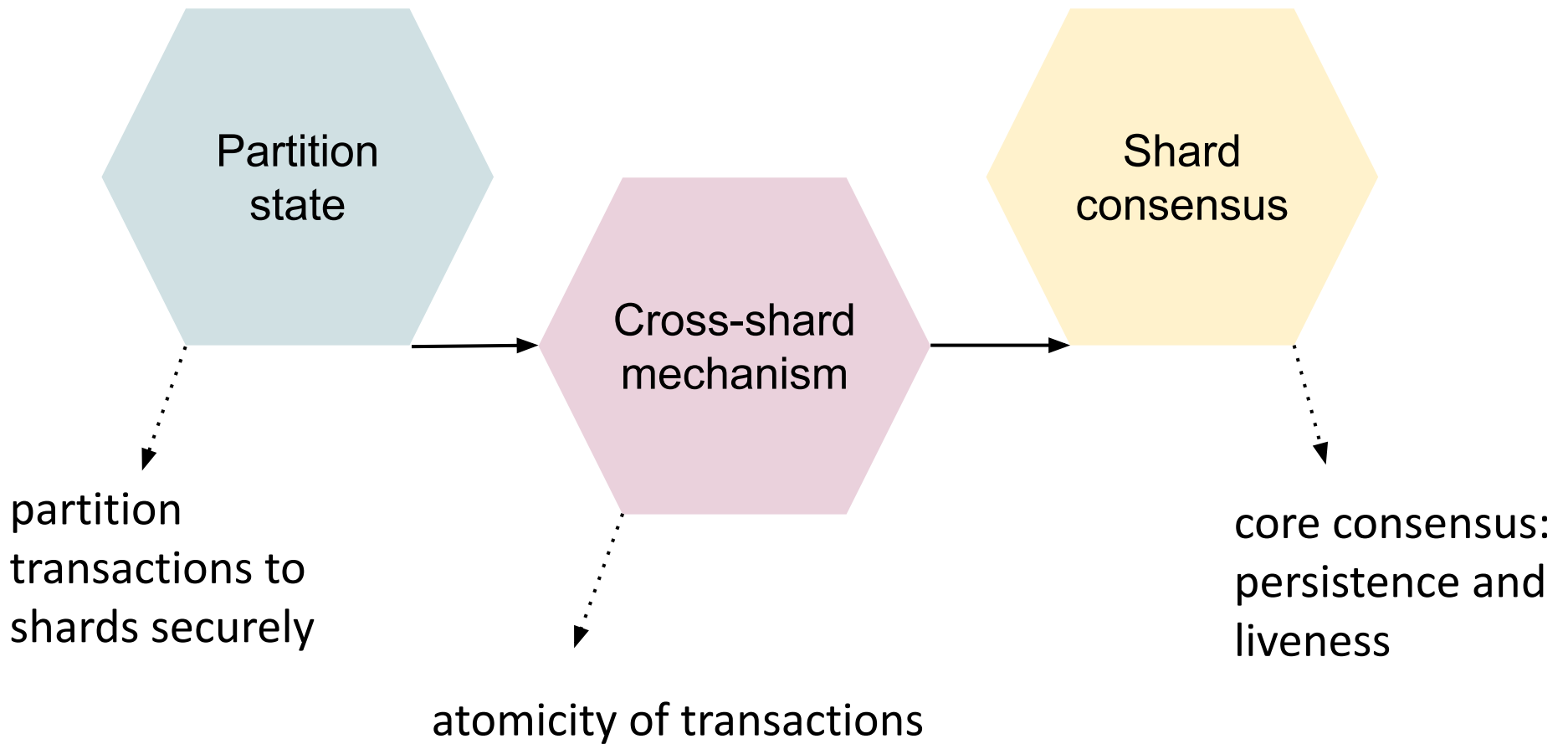
Divide & Scale

Beginning of epoch:



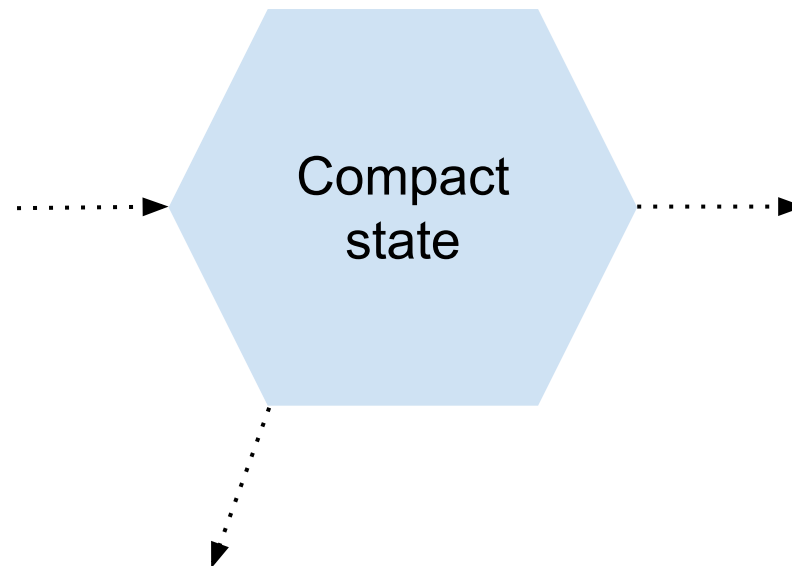
Divide & Scale

Within an epoch:



Divide & Scale

End of epoch:



securely compress the epoch's data
and broadcasts

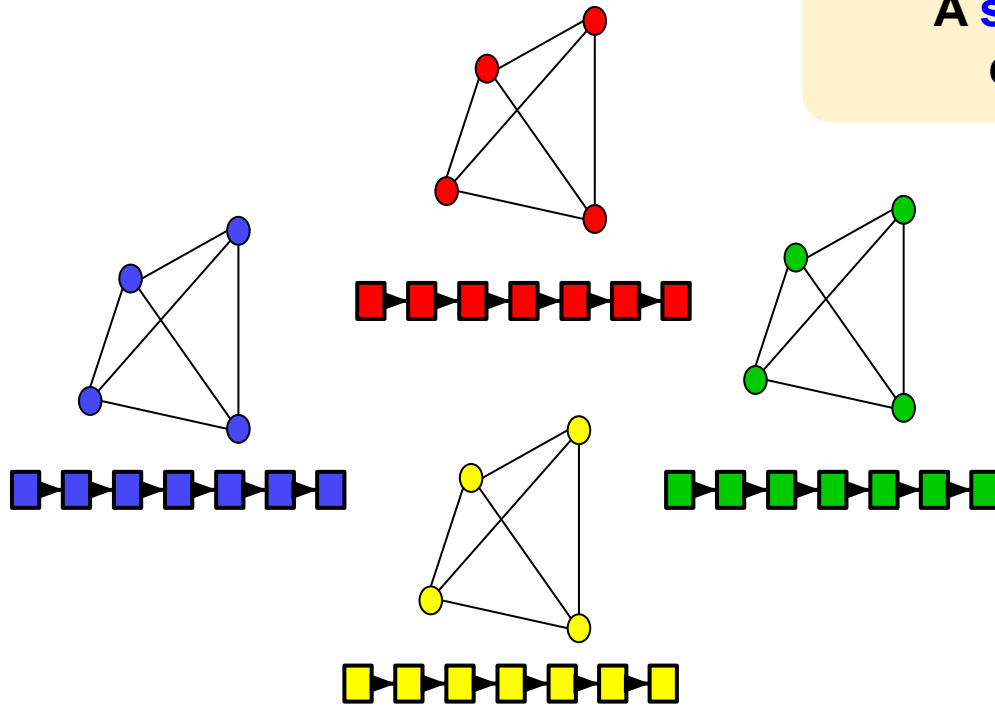
Evaluation of sharding protocols

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

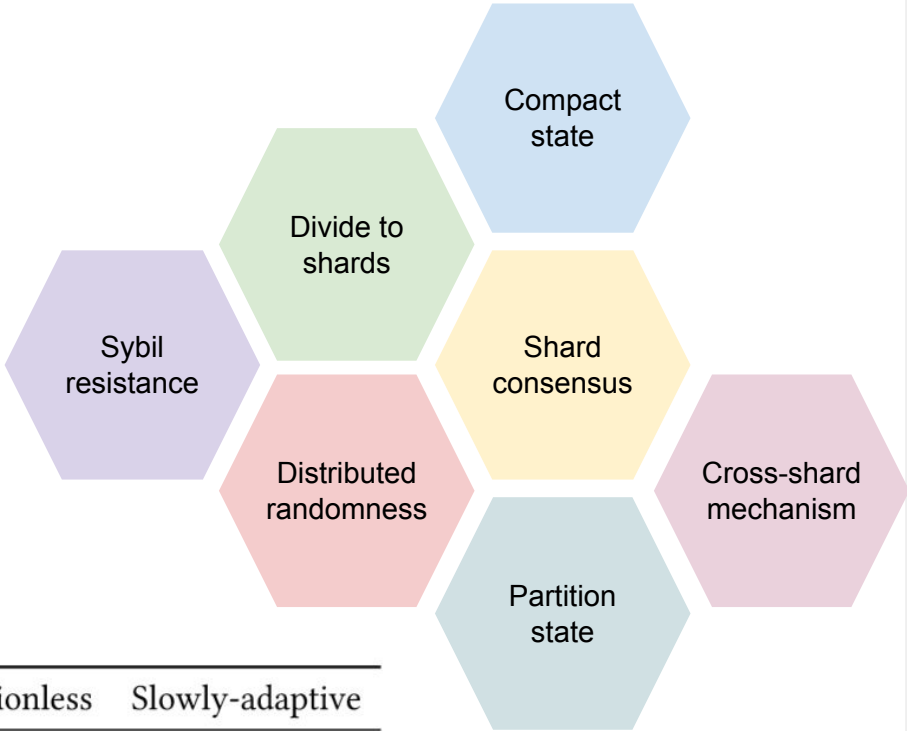
~ constant-adaptive adversary

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
INFORMATIK

Faculty of Informatics



SECURITY &
PRIVACY
GROUP

Thank you!