Orchestrating a brighter world NEC

MITOSIS: Practically Scaling Permissioned Blockchains

Giorgia Marson Sebastien Andreina Lorenzo Alluminio Konstantin Munichev Ghassan Karame

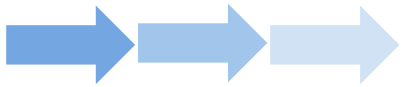
NEC Labs Europe
Heidelberg, Germany

ACSAC 2021

Towards improving blockchain scalability

~7 tx/sec

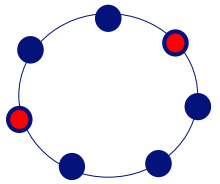
~20 tx/sec



>10.000 tx/sec

Layer-2		Payment channels	Sidechains	Cross-chain techniques	...
Layer-1	Proof of X	Hybrid consensus	DAG-based protocols	Blockchain sharding	...

Motivation



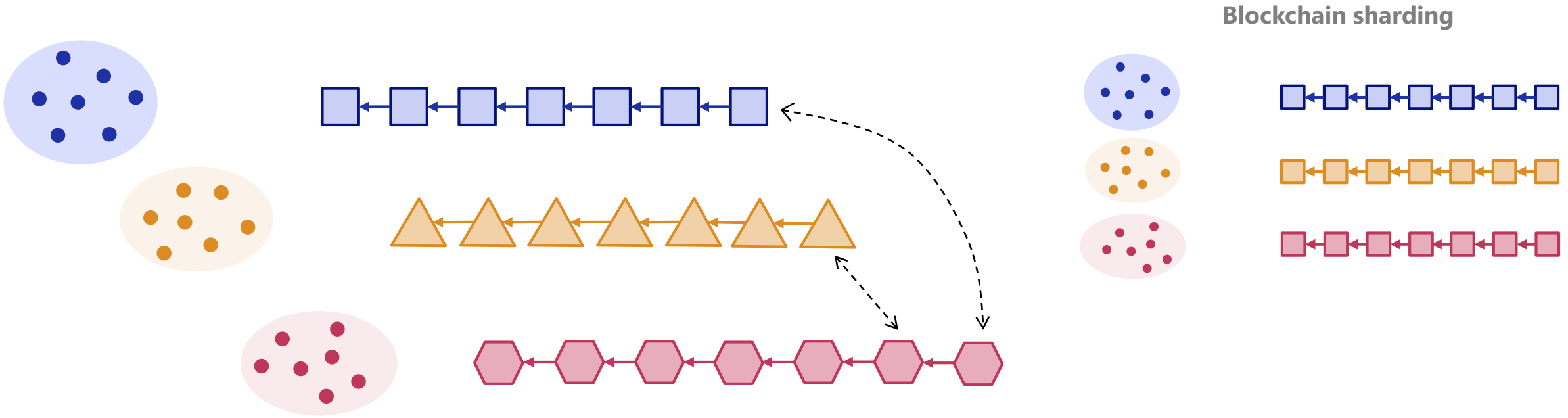
Permissionless blockchains

- Fully decentralized
- **Large-scale deployments**
- Low throughput
- High latency

Permissioned blockchains

- Limited decentralization
- Small/medium-scale deployments
- **High throughput**
- **Low latency**

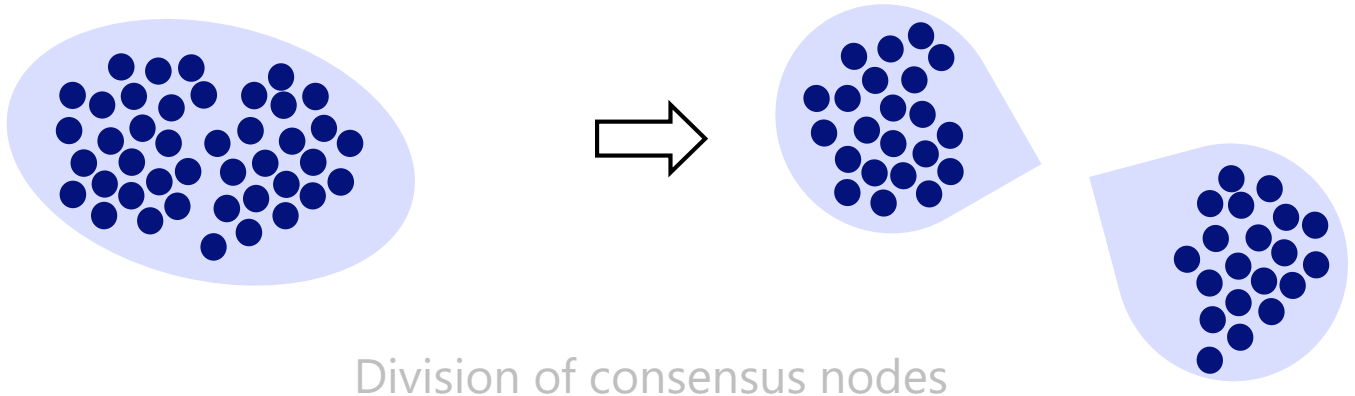
Our proposal: MITOSIS



Ecosystem of autonomous **permissioned blockchains**

- **Dynamic**: blockchains are created and evolve as the need comes
- **Flexible**: each blockchain can run its own consensus protocol
- **Interoperable**: blockchains can interact with each other

MITOSIS core idea

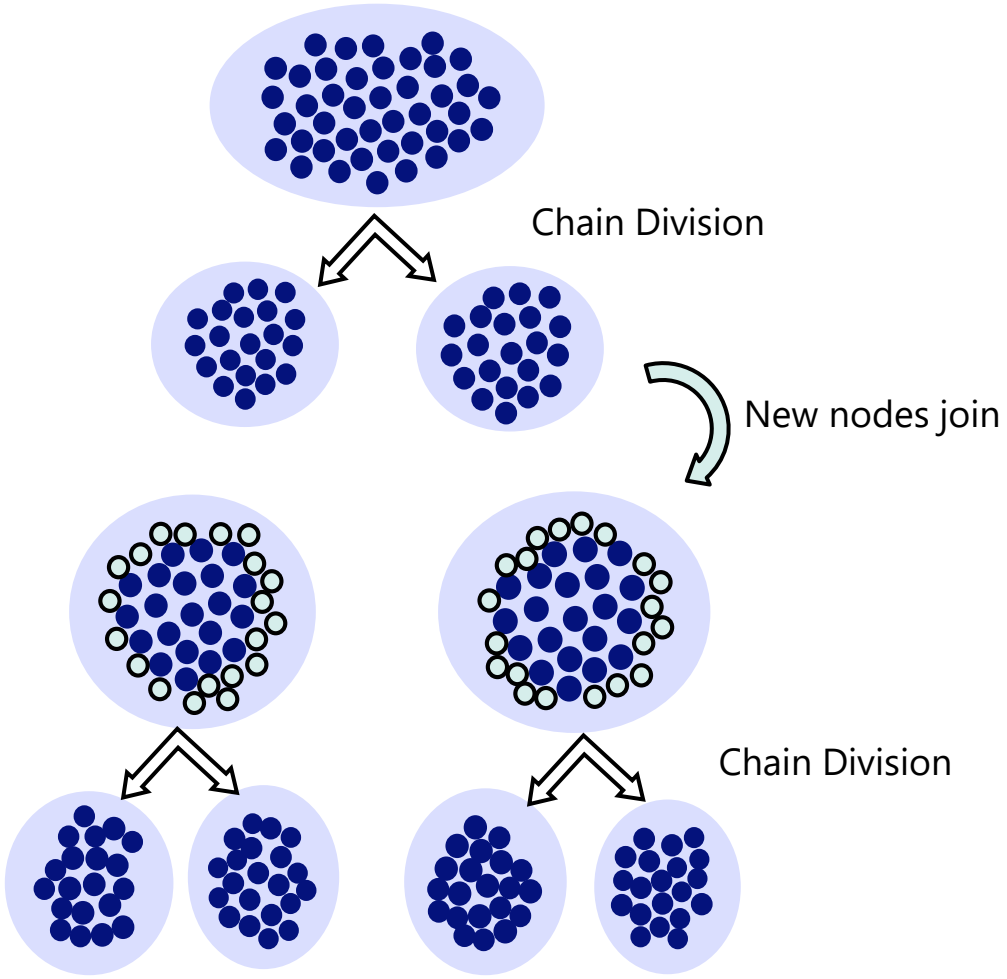


Division of consensus nodes

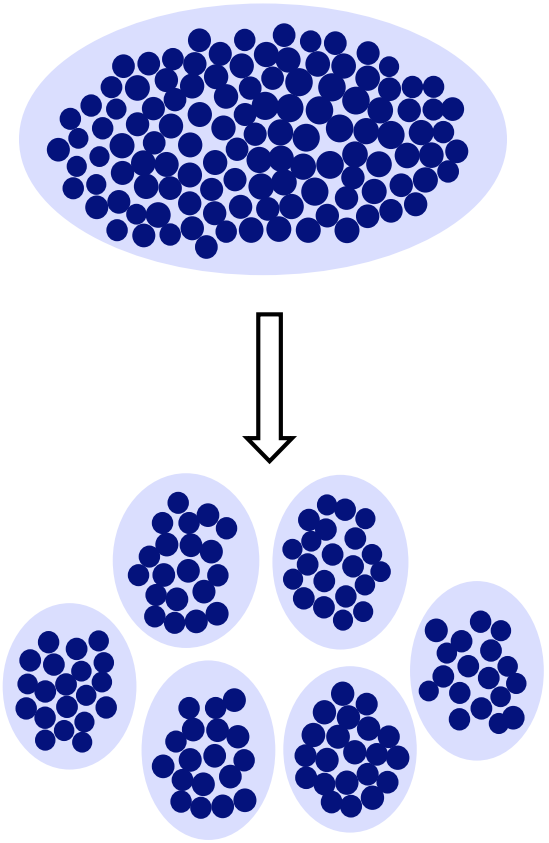
Chain Division (akin *cell division* in Biology)

- Enable existing blockchain to “give birth” to new chains
- Trigger chain division when performance reaches bottleneck (e.g., too many nodes)
- Evolve reactively to meet optimal performance

MITOSIS Chain division

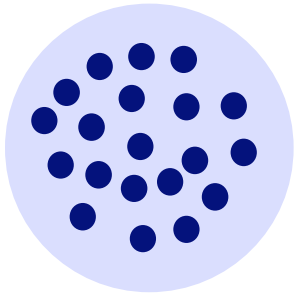


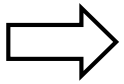
Blockchain sharding



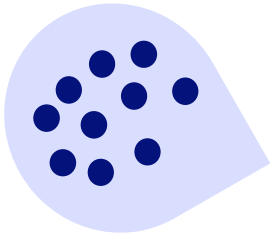
Security risks of chain division

Example: $n = 20$

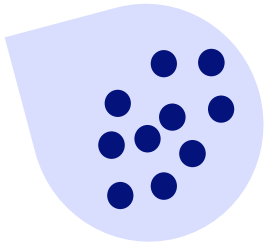




$n_1 = 10$

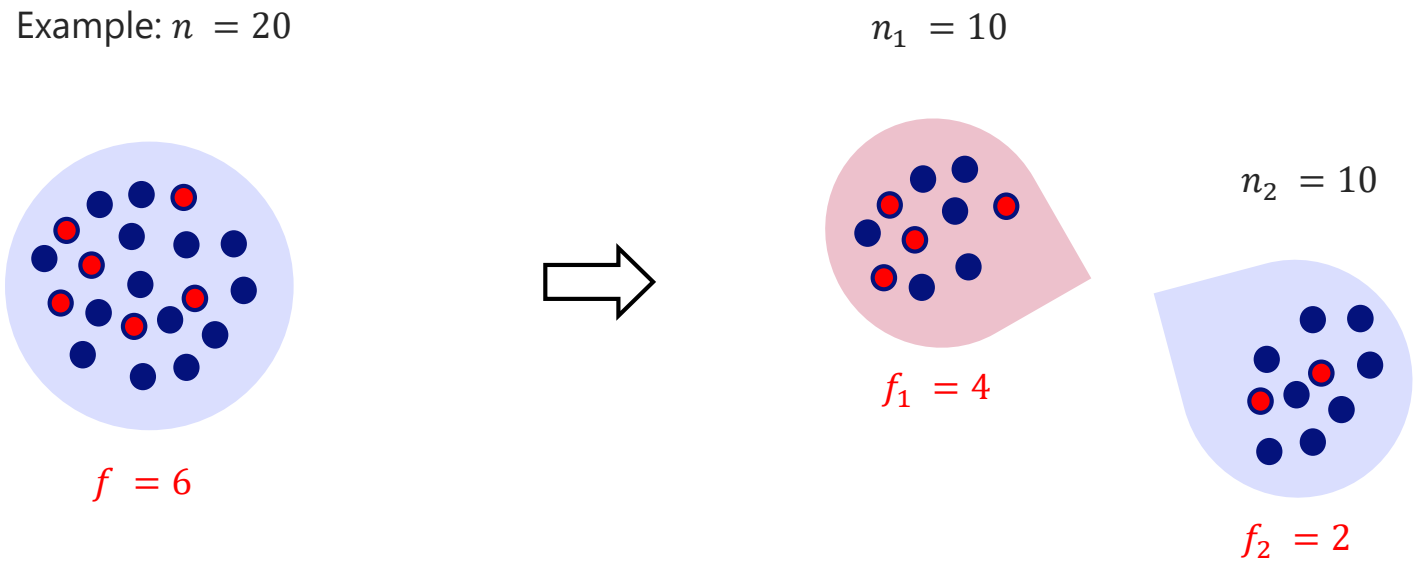


$n_2 = 10$



- Consensus protocols can tolerate limited faults

Chain division introduces security risks



- Consensus protocols can tolerate limited faults
- Splitting may cause imbalanced # faults among child chains
  - E.g., Byzantine nodes might exploit chain division to take over a child chain

Security of chain division

1. Given tolerated faults $n_i \geq \alpha_i \cdot f_i + 1$ (child chains)
2. Derive condition on f (parent chain)

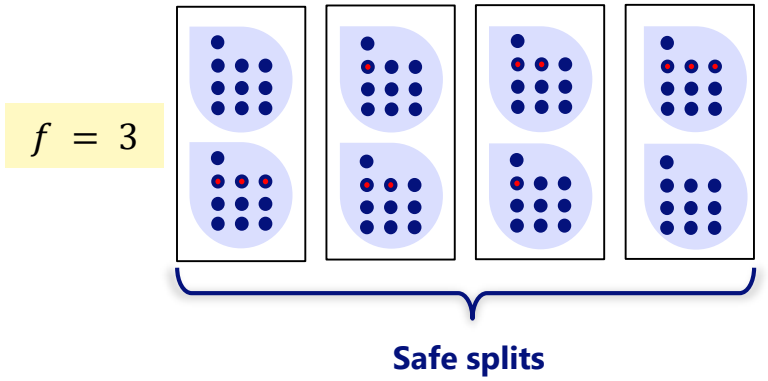
Example:
$n = 20, n_1 = n_2 = 10$
Byz. faults $\Rightarrow f_i \leq 3$
$f \leq$ … ?

Optimistic case:

- Actual # faults in parent chain ≤ # tolerated faults in child chains:

$$f \leq \frac{1}{2} \cdot \frac{n-1}{3}$$

- Security is preserved regardless of node assignment

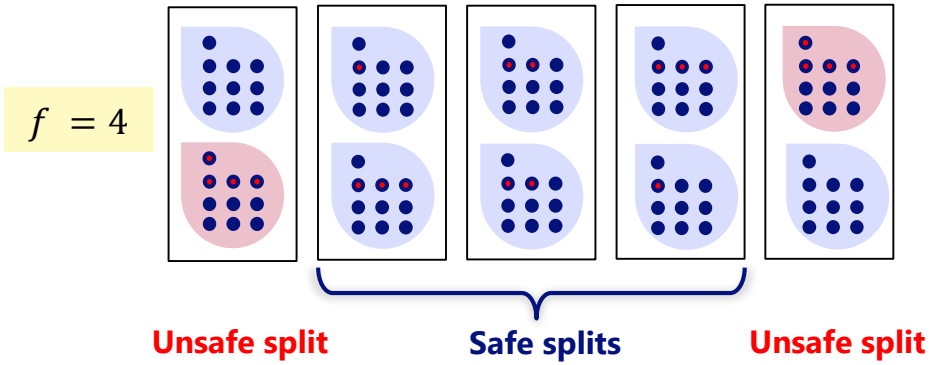


General case:

- Milder bound on tolerated faults:

$$f = \beta \cdot (n-1) \quad \text{with } 0 < \beta \leq \frac{1}{3}$$

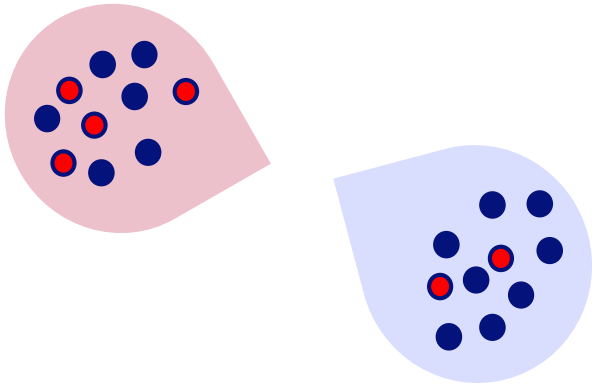
- Safe split increasingly more likely as $\beta \to 1/6$
- Probabilistic security; graceful degradation for increasing β



Summary

MITOSIS

- Scaling permission-based blockchains via secure chain division
- Flexible blockchain ecosystem leveraging “dynamic sharding”
  - Cross-chain protocols for knowledge and asset transfers
  - PoC implementation based on HyperLedger Fabric



Thank you

giorgia.marson@neclab.eu
Security Group - NEC Labs Europe