Enhancing Blockchain-based Federated Learning

UPPSALA UNIVERSITET

Project in Computational Science 2020

Project Members

Fredrik Örn
Fredrik.Orn.6328@student.uu.se

Jacob Tiensuu
Jacob.Tiensuu.4776@student.uu.se

Jialun Song
Jialun.Song.4857@student.uu.se

Maja Linderholm
Maja.Linderholm.6920@student.uu.se

Supervisors

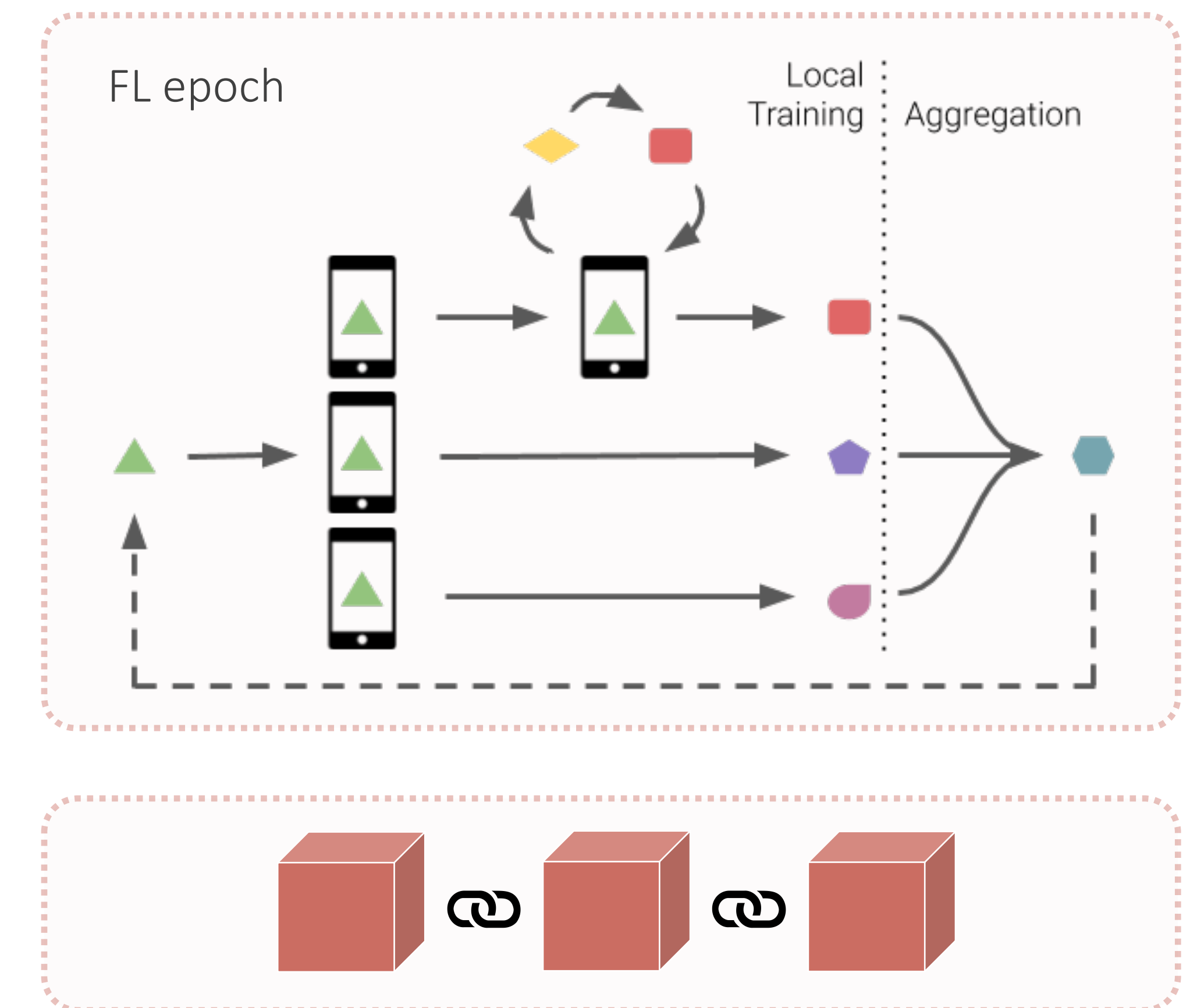Salman Toor

Felix Morsbach

Federated Learning & Blockchain

Federated Learning (FL)

Collaborative machine learning: training & aggregation

+ **Privacy**: sensitive data stay at local trainers

− Single point of failure: dependent on a central server
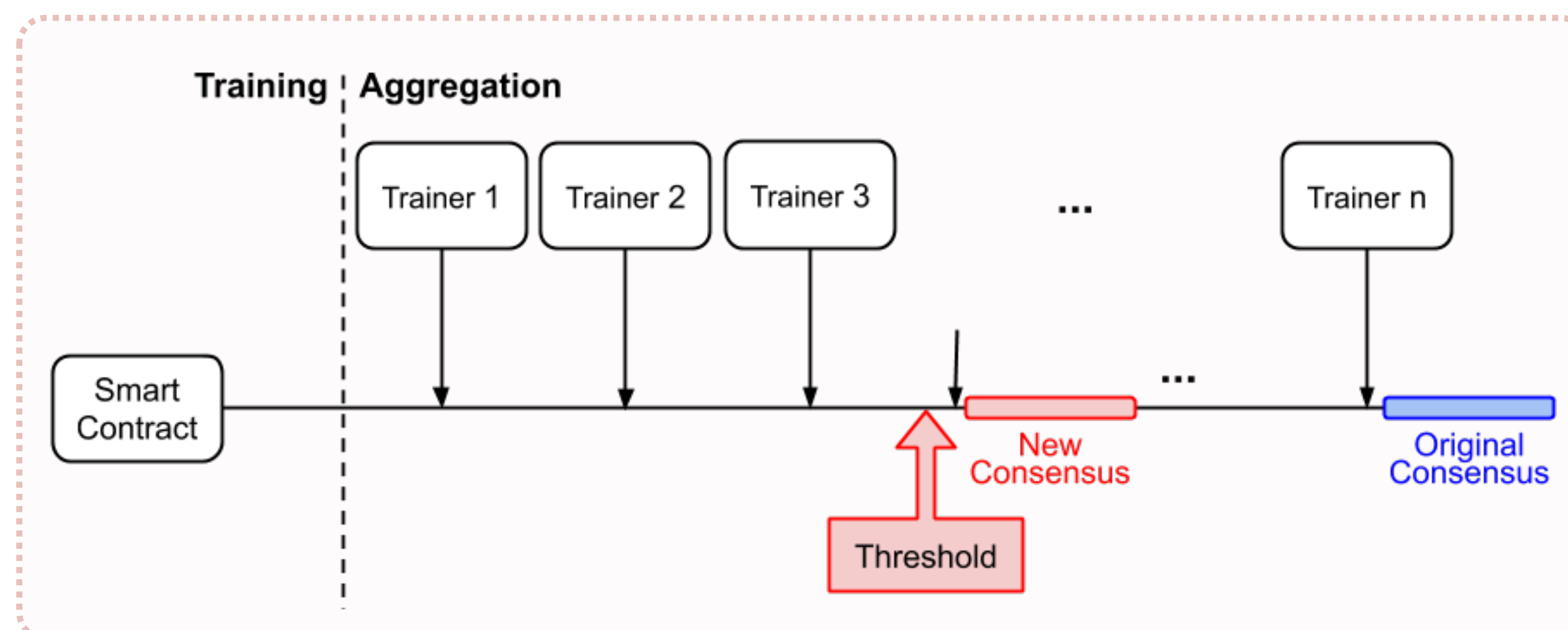
Blockchain-based FL

Smart Contract deployed on blockchain network

+ **Decentralization**: no central authority

+ **Security**: cryptography & immutable blocks

− High transaction costs to get consensus in aggregation

Goal

- Reduce overhead
- Keep FL accuracy
- Keep security

How

Total Costs = Number of transactions × transaction fee [gas]

Introduce an administrator-defined **threshold** in the consensus policy to reduce the number of transactions. In aggregation of each epoch, consensus can be reached as soon as any candidate's votes pass the threshold, it is no longer required to count votes from all trainers.
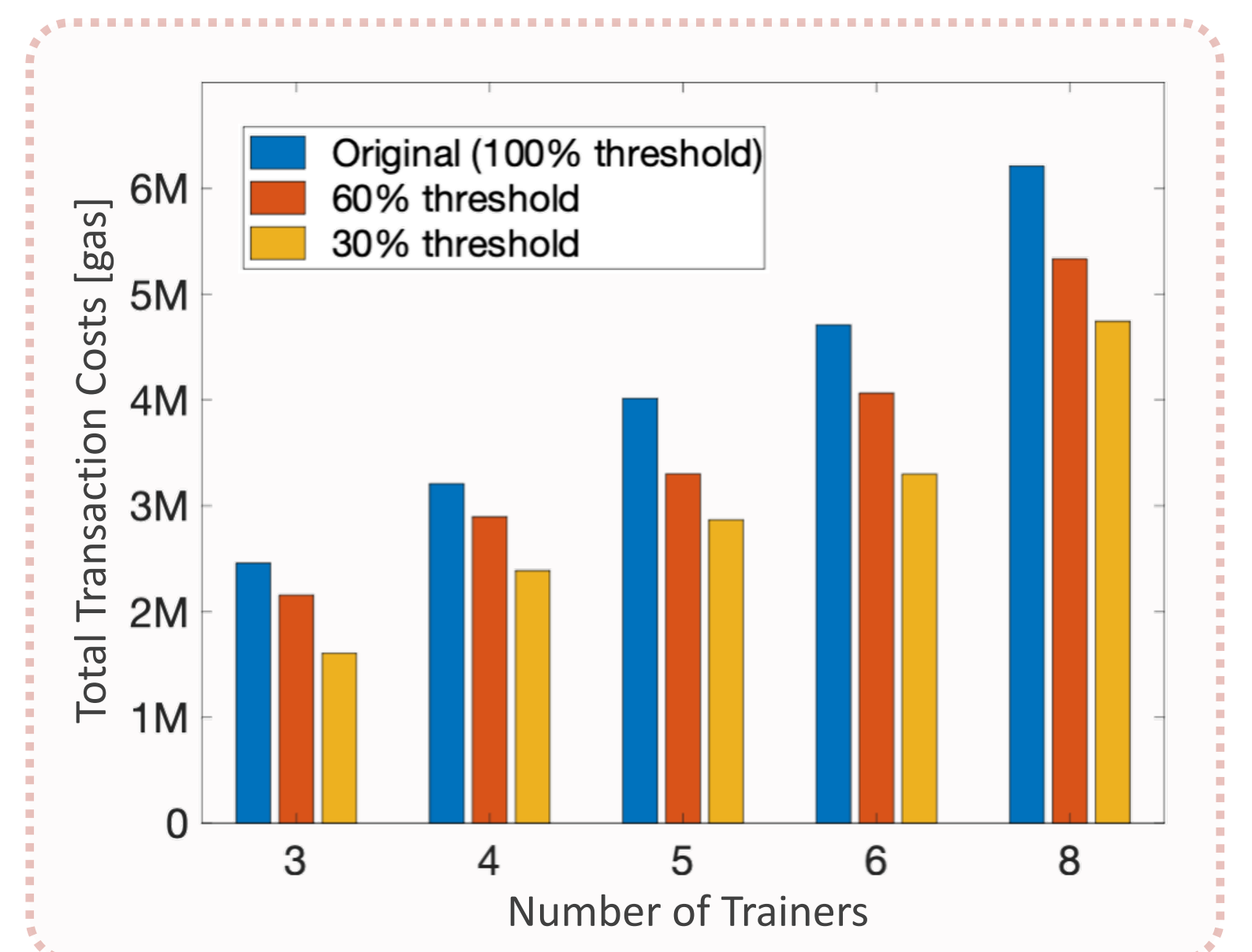

51% threshold & 10 trainers → 6 transactions may get a consensus.
Lower threshold → less transactions, require a more secure set-up.

Result

15 runs, 5 groups
Model: MNIST (IID), 3 epochs

- Transaction costs reduced proportionally to threshold
- Absolute reduction grows with the number of trainers
- Accuracy unaffected

Conclusion

The new consensus policy for blockchain-based federated learning enables a fine control on reducing the transaction costs while retain the training accuracy and a high level of security.