BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2024

Blockchain Resistant to Quantum Attack

Michal Ľaš, supervised by Mgr. Kamil Malinka, Ph.D.

Goals

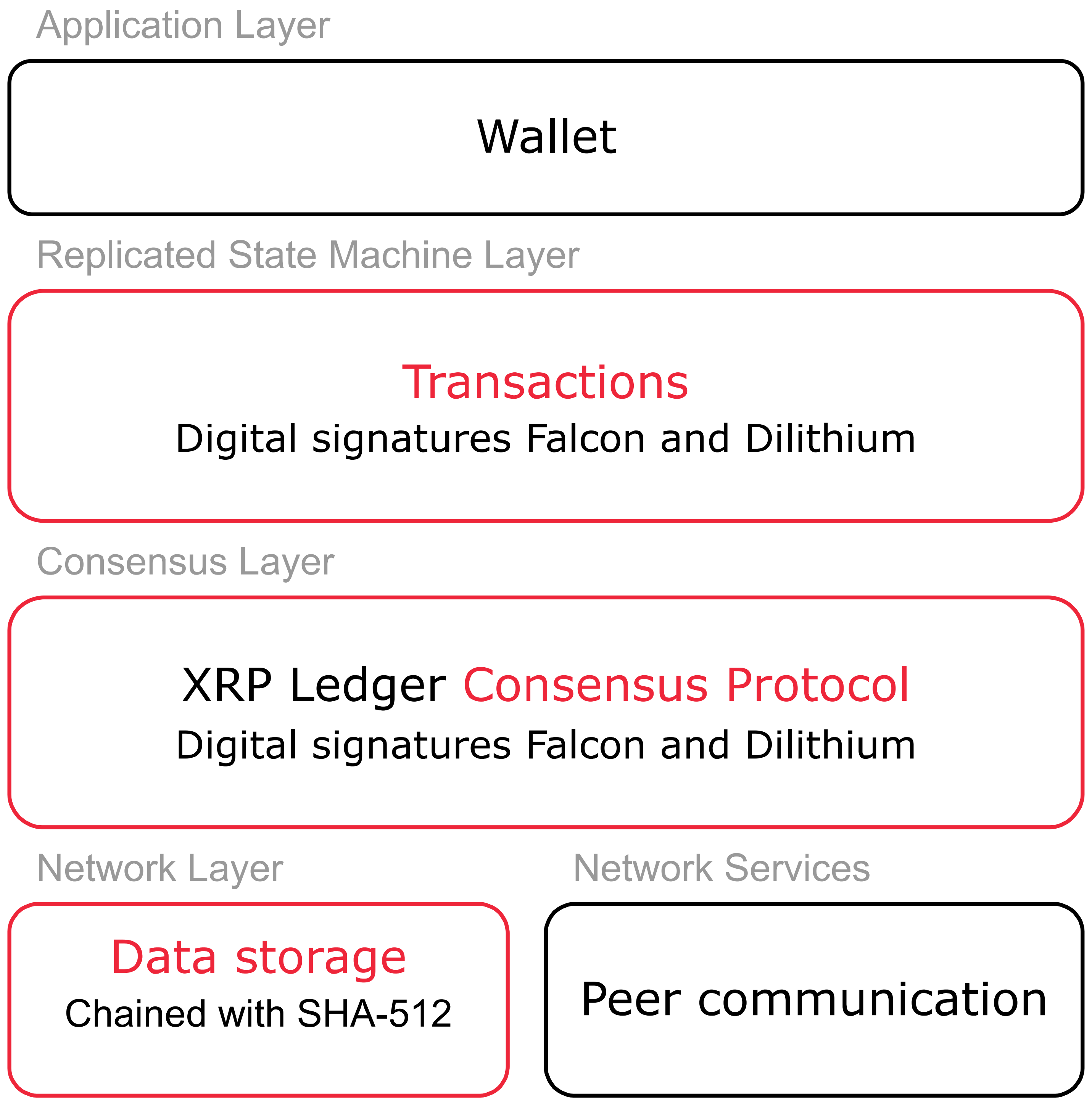
- Analyze blockchain components vulnerable to quantum attacks
- Identify appropriate post-quantum cryptography algorithms for use in a blockchain
- Design and implement a post-quantum blockchain
- Test implementation performance with different post-quantum cryptography algorithms

1 Threats

The main threat is the ability of quantum computers to break the currently used cryptography. For blockchains, it indicates:

- Threat for transactions integrity
- Threat to consensus mechanisms, mainly PoW
- Theoretical threat to the entire integrity of a blockchain

2 Solution & Design



Application Layer

Wallet

Replicated State Machine Layer

Transactions
Digital signatures Falcon and Dilithium

Consensus Layer

XRP Ledger Consensus Protocol
Digital signatures Falcon and Dilithium

Network Layer

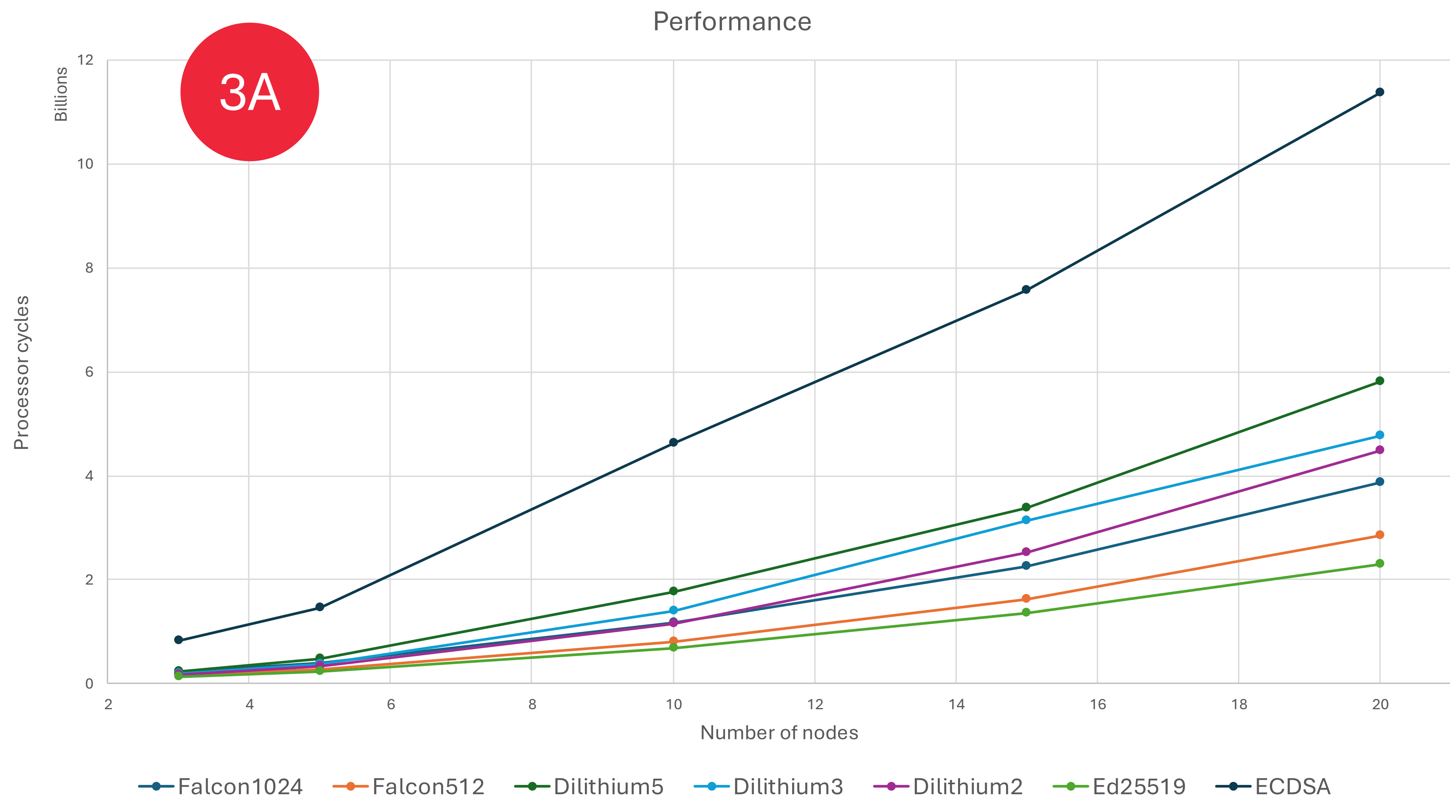
Data storage
Chained with SHA-512

Network Services

Peer communication

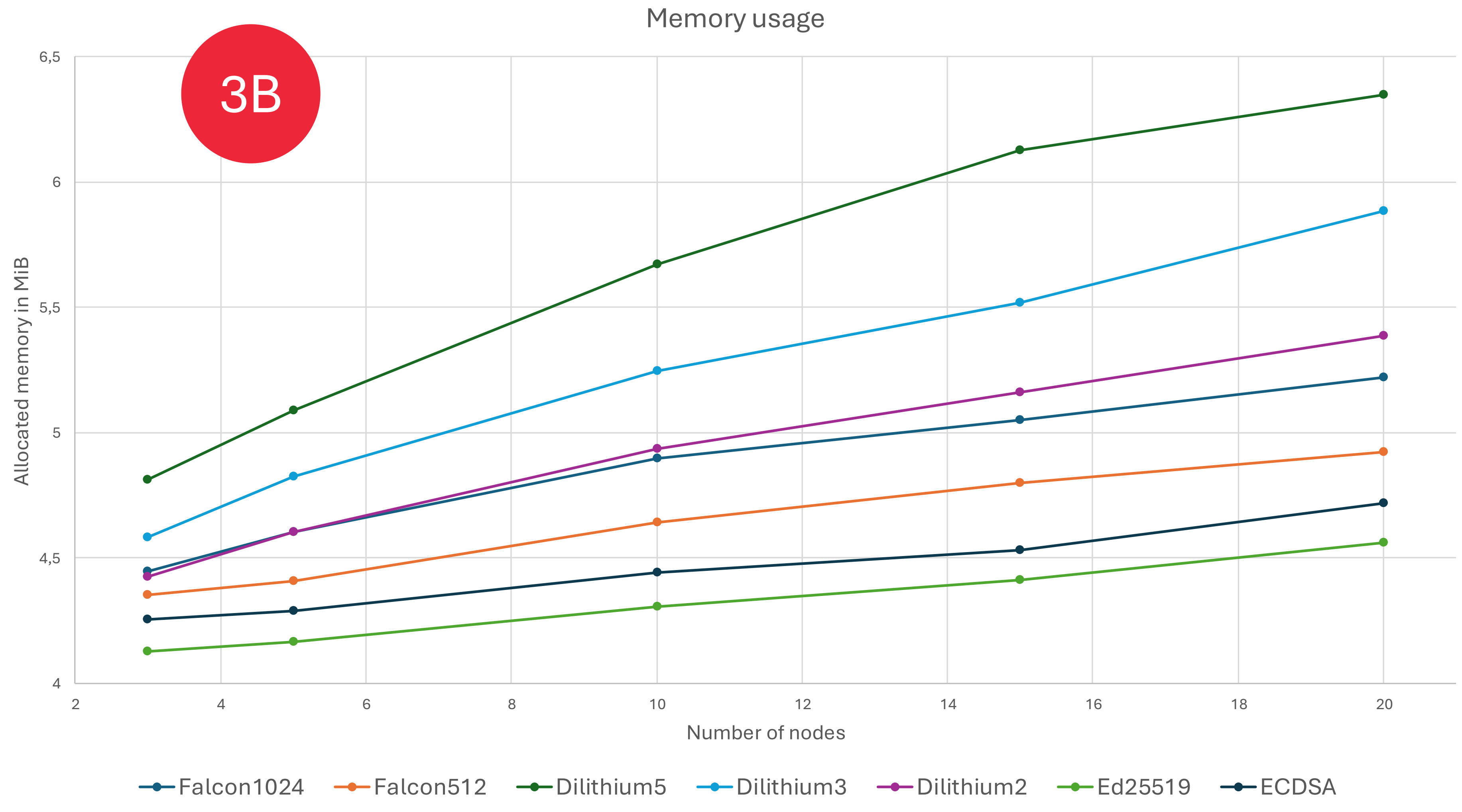
Results

- The performance of PQ algorithms compared to the currently utilized ones is actually quite sufficient
- Faster consensus mechanism can reduce demands on allocated memory
- The primary issue is the size of PQ signatures and keys



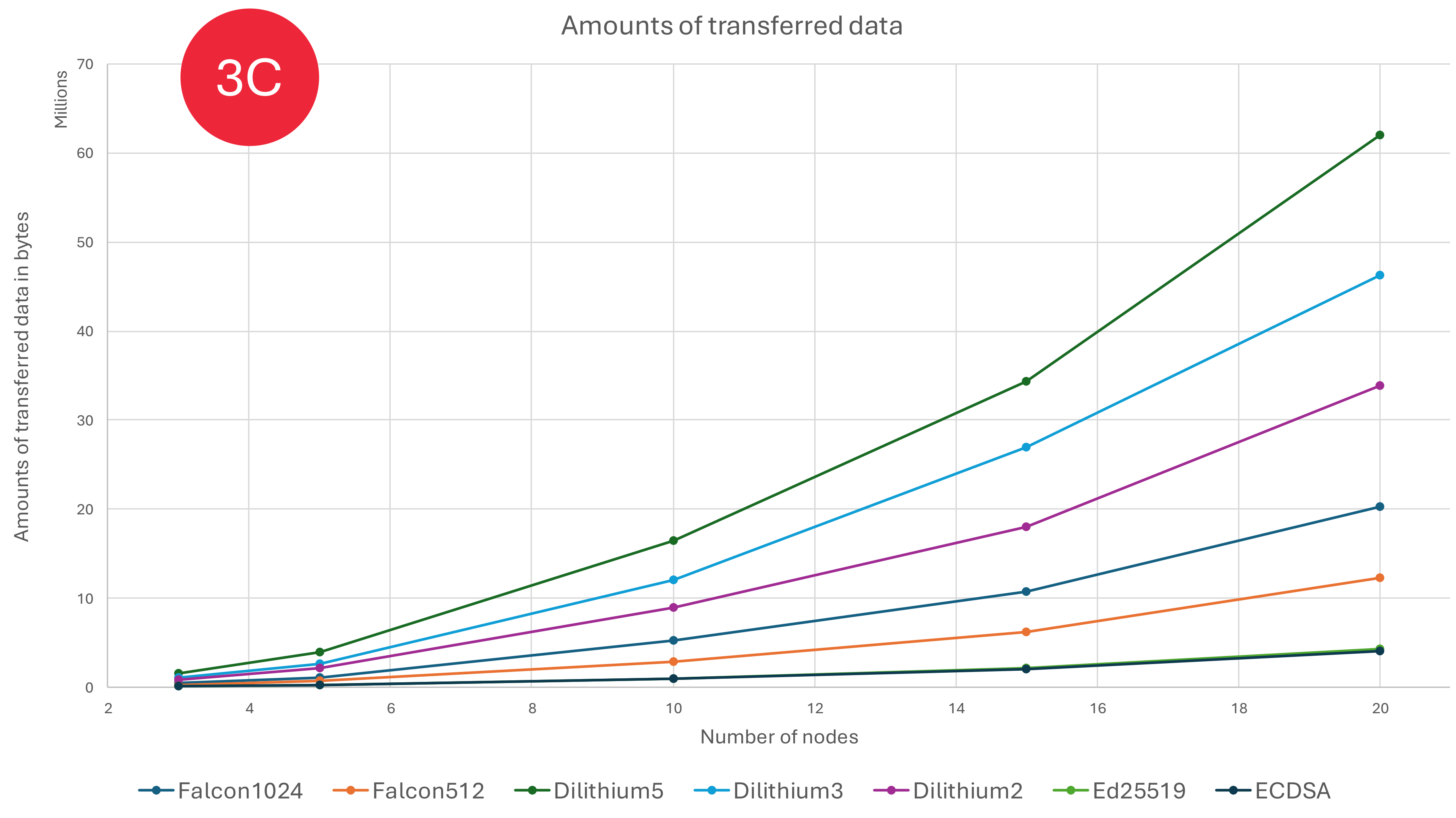
3A

Performance



3B

Memory usage



3C

Amounts of transferred data