MAgiCS '26 Workshop (affiliated with Eurocrypt 2026)

10 May 2026, Rome

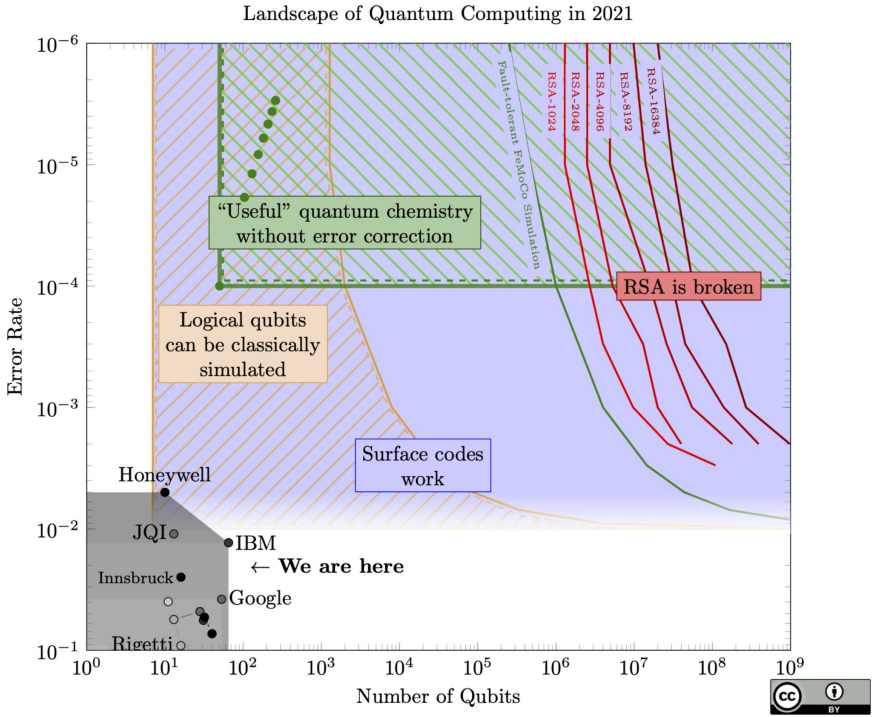
Post-Quantum Blockchains with Agility in Mind

Manuel B. Santos[1*], Danno Ferrin[2], Ron Kahat[2], Michael Lodder[2]

[1] Quantum, [2] Tectonic Labs

[*] Work done while at Tectonic Labs.

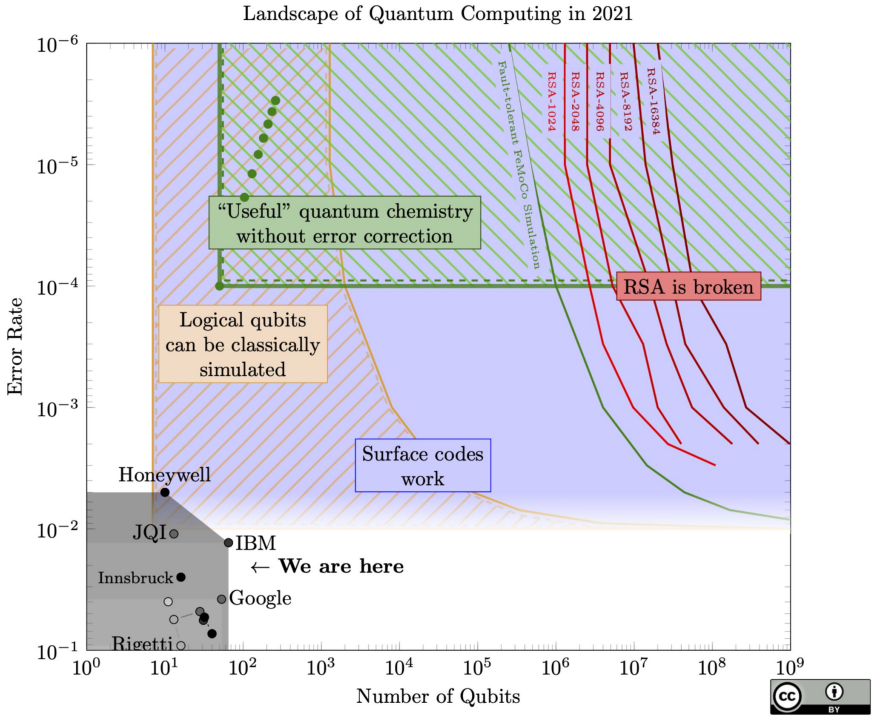
Motivation



By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

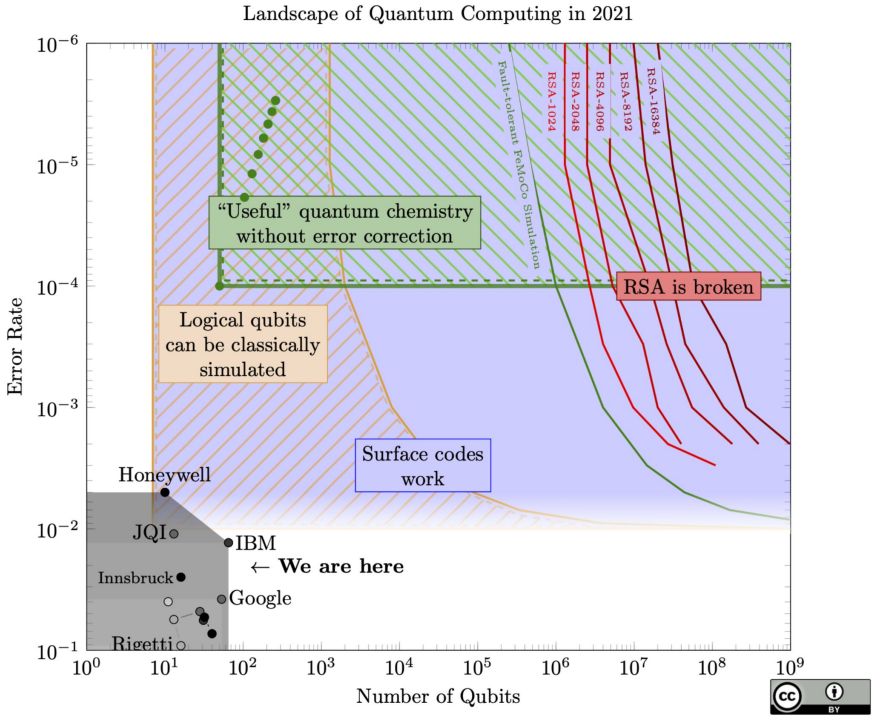


By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

Fidelity of two qubit gate

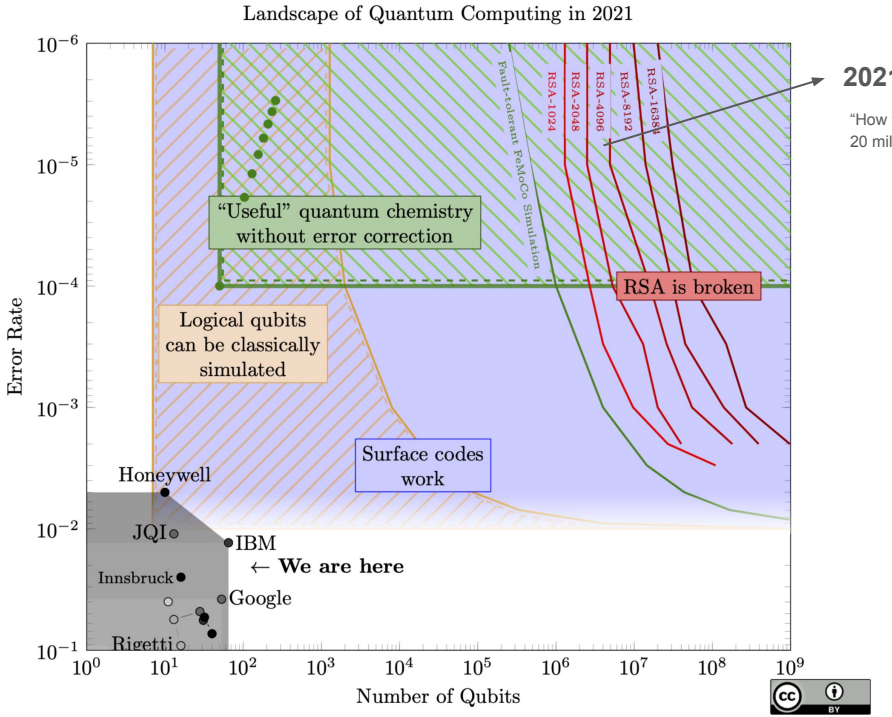


By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

Fidelity of two qubit gate



2021: 20 million qubits

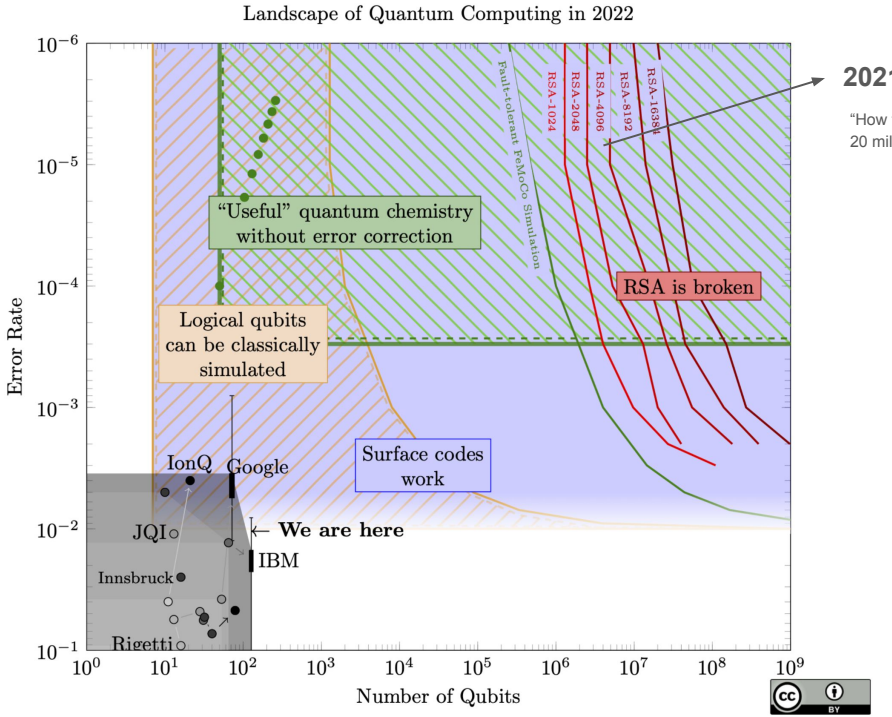
"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Gidney and Ekerå

By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

Fidelity of two qubit gate



2021: 20 million qubits

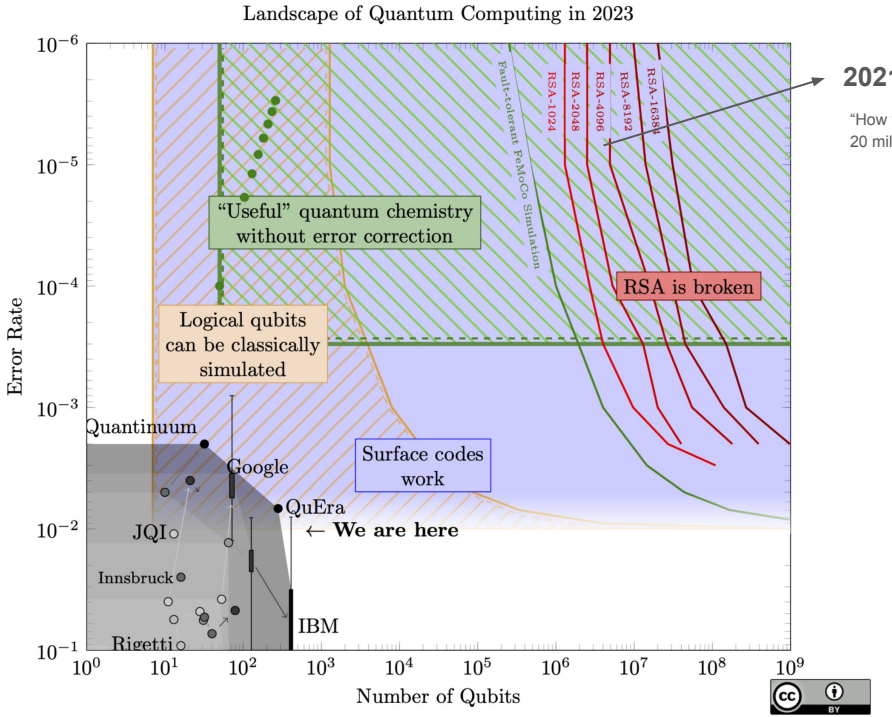
"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Gidney and Ekerå

By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

Fidelity of two qubit gate



2021: 20 million qubits

"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Gidney and Ekerå

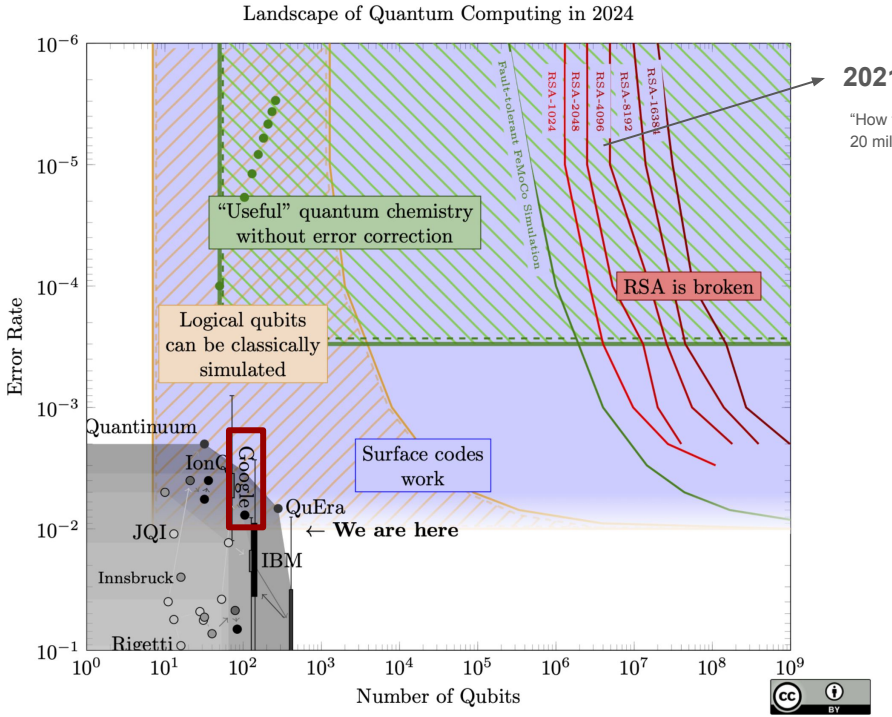
By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

2024 Google: Willow with below threshold QEC

Fidelity of two qubit gate



2021: 20 million qubits

"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Gidney and Ekerå

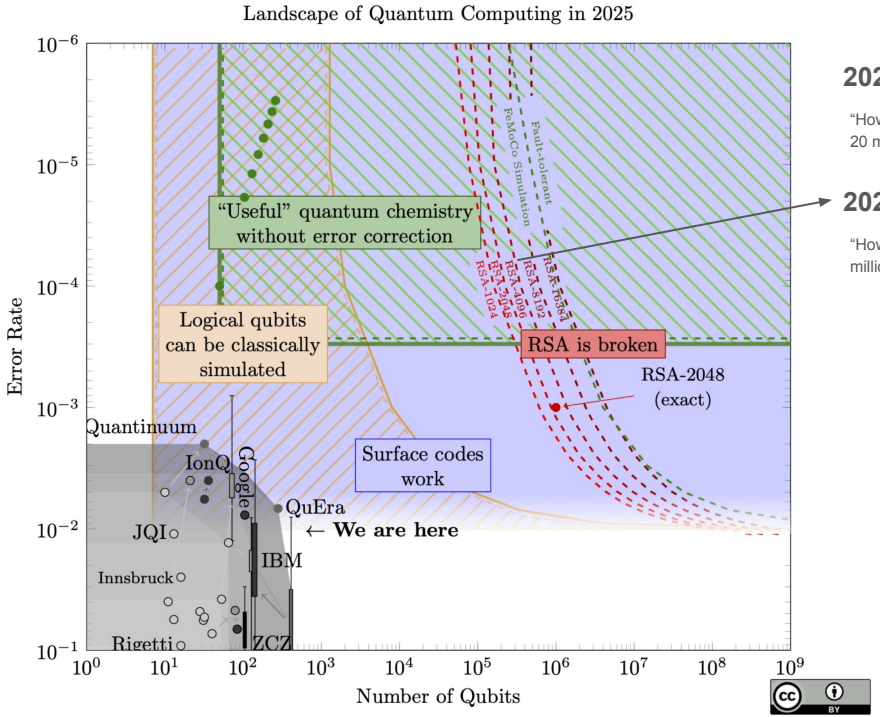
By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

2024 Google: Willow with below threshold QEC

Fidelity of two qubit gate



2021: 20 million qubits

"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Gidney and Ekerå

2025: 1 million qubits

"How to factor 2048 bit RSA integers with less than a million noisy qubits", Gidney

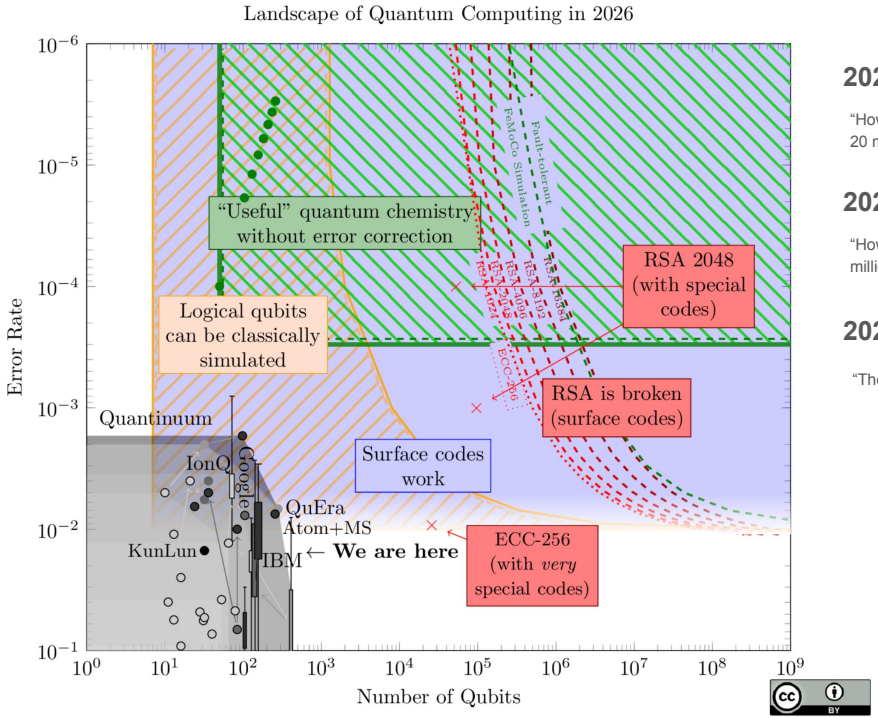
By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

Motivation

Quantum Error Correction

2024 Google: Willow with below threshold QEC

Fidelity of two qubit gate



By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

2021: 20 million qubits

"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Gidney and Ekerå

2025: 1 million qubits

"How to factor 2048 bit RSA integers with less than a million noisy qubits", Gidney

2026: 100 thousand qubits

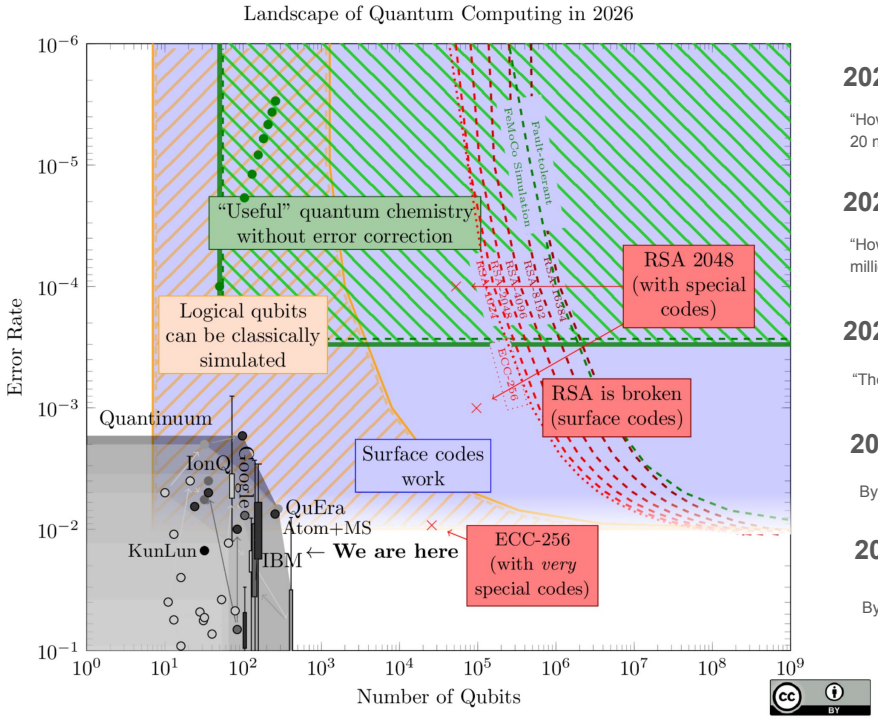
"The Pinnacle Architecture", Iceberg Quantum

Motivation

Quantum Error Correction

2024 Google: Willow with below threshold QEC

Fidelity of two qubit gate



By Samuel Jaques, https://sam-jaques.appspot.com/quantum_landscape

2021: 20 million qubits

"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Gidney and Ekerå

2025: 1 million qubits

"How to factor 2048 bit RSA integers with less than a million noisy qubits", Gidney

2026: 100 thousand qubits

"The Pinnacle Architecture", Iceberg Quantum

2026: 10 thousand qubits

By Oratomic

2026: 1 thousand qubits

By Google quantum AI, Berkeley, Ethereum Foundation, Stanford

Motivation

Challenges (NIST CSWP 39):

Motivation

Challenges (NIST CSWP 39):

- Transitions take a long time

Motivation

Challenges (NIST CSWP 39):

- Transitions take a long time
- Backward compatibility

Motivation

Challenges (NIST CSWP 39):

- Transitions take a long time
- Backward compatibility
- PQC increases resource pressure

Motivation

Challenges (NIST CSWP 39):

- Transitions take a long time
- Backward compatibility
- PQC increases resource pressure
- Downgrade attacks become a risk

Motivation

Challenges (NIST CSWP 39):

- Transitions take a long time
- Backward compatibility
- PQC increases resource pressure
- Downgrade attacks become a risk

Blockchains

Motivation

Challenges (NIST CSWP 39):

- Transitions take a long time
- Backward compatibility
- PQC increases resource pressure
- Downgrade attacks become a risk

Blockchains

decentralization

long-term integrity

Overview

- Intro to EVM-based blockchains
- Flexibility framework
- CATX
- Experiments

EVM-based blockchains

World state: σ_t

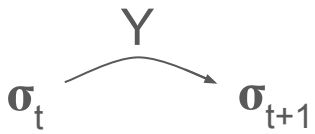
Address	Balance
0x742d3	0.1 ETH
0x841a7	2.1 ETH

EVM-based blockchains

World state: σ_t →

Address	Balance
0x742d3	0.1 ETH
0x841a7	2.1 ETH

Transition function: Y →

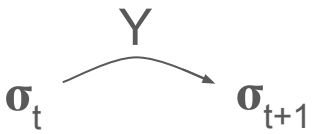


EVM-based blockchains

World state: σ_t →

Address	Balance
0x742d3	0.1 ETH
0x841a7	2.1 ETH

Transition function: Y →



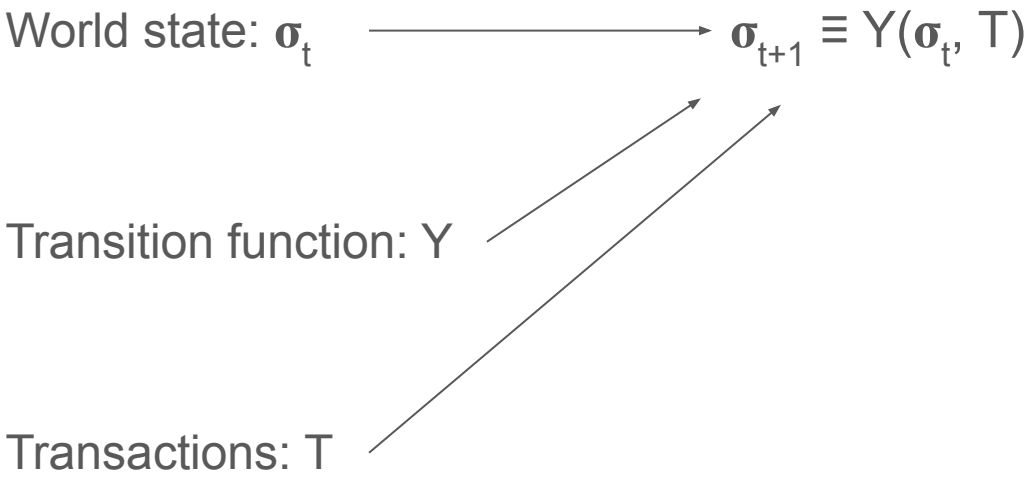
Transactions: T →

From: 0x742d3

To: 0x841a7

Amount: 0.01 ETH

EVM-based blockchains



EVM-based blockchains

Quantum vulnerable: ECDSA signature

$$\sigma_{t+1} \equiv Y(\sigma_t, T)$$

EVM-based blockchains

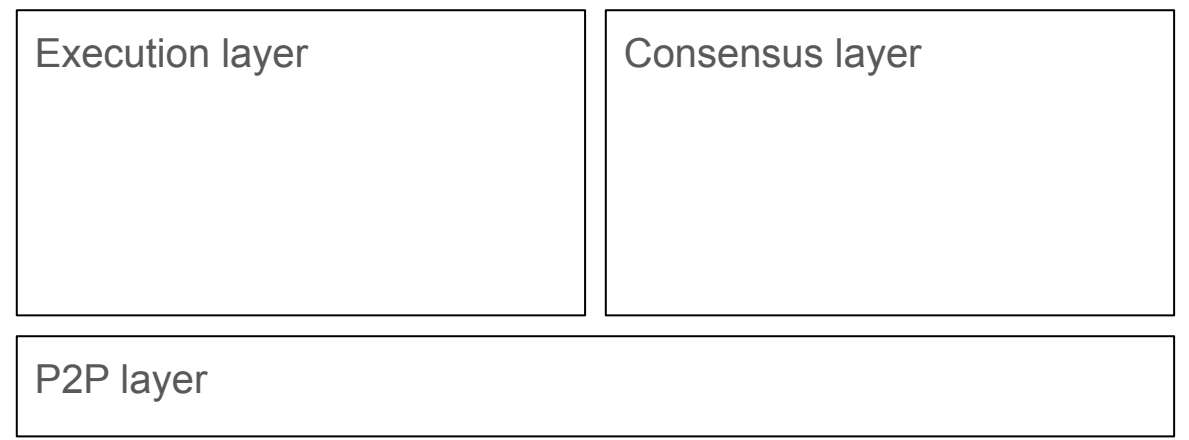
Quantum vulnerable: ECDSA signature

$$\sigma_{t+1} \equiv Y(\sigma_t, T)$$

EVM-based blockchains

Quantum vulnerable: ECDSA signature

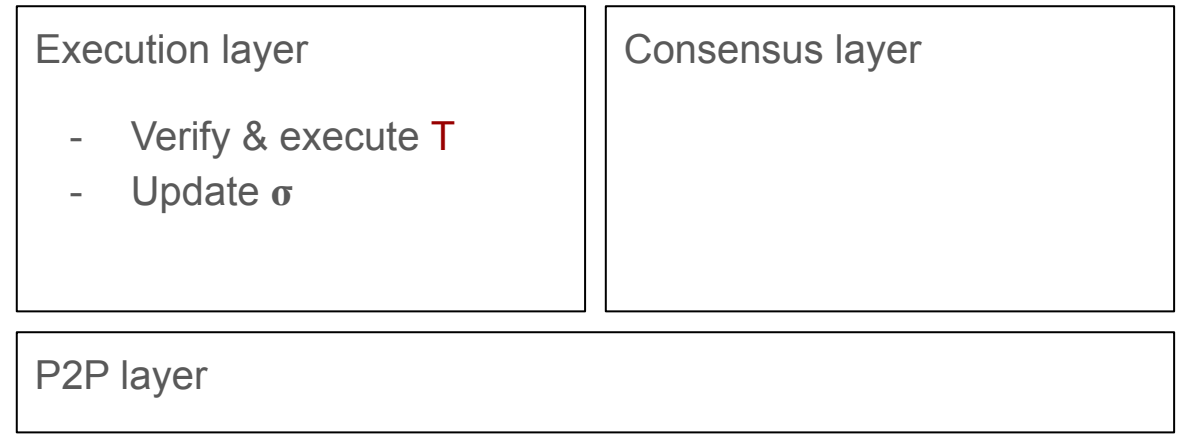
$$\sigma_{t+1} \equiv Y(\sigma_t, T)$$



EVM-based blockchains

Quantum vulnerable: ECDSA signature

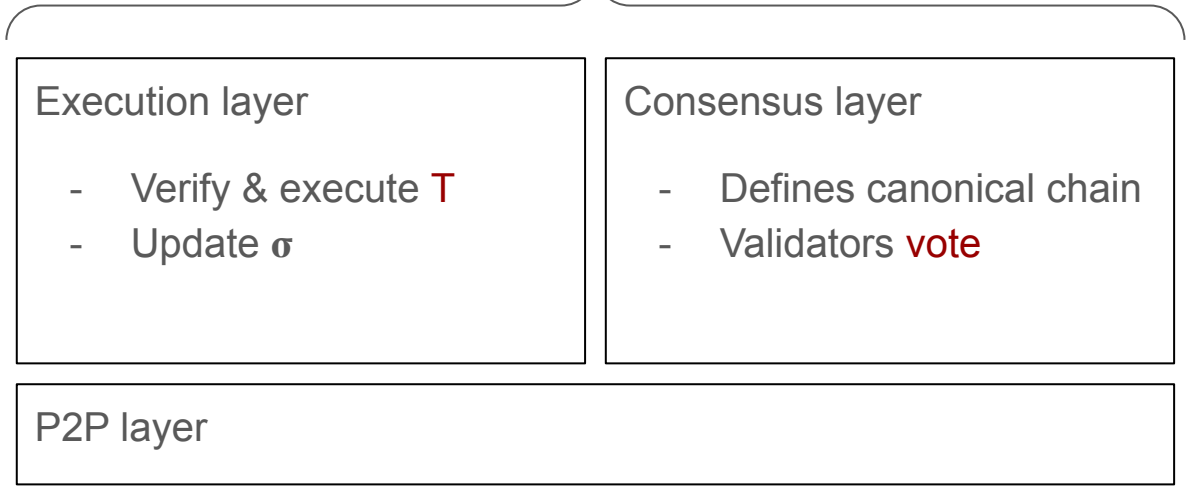
$$\sigma_{t+1} \equiv Y(\sigma_t, T)$$



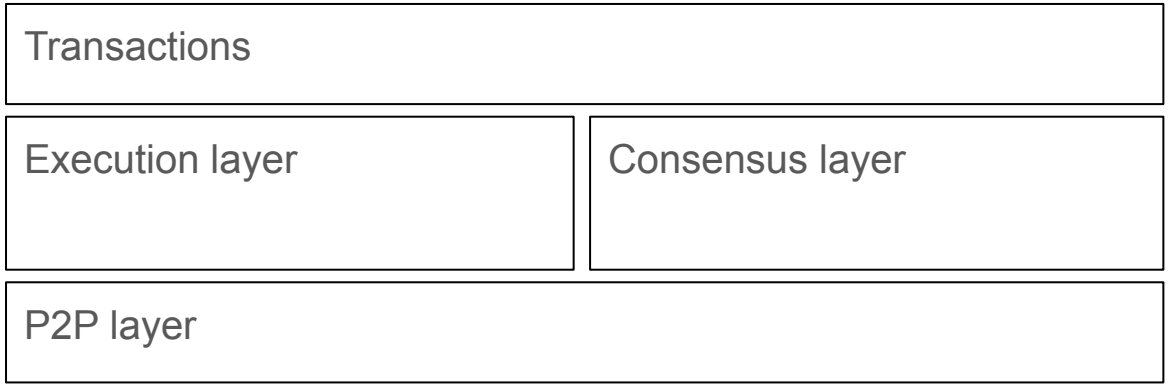
EVM-based blockchains

Quantum vulnerable: ECDSA signature

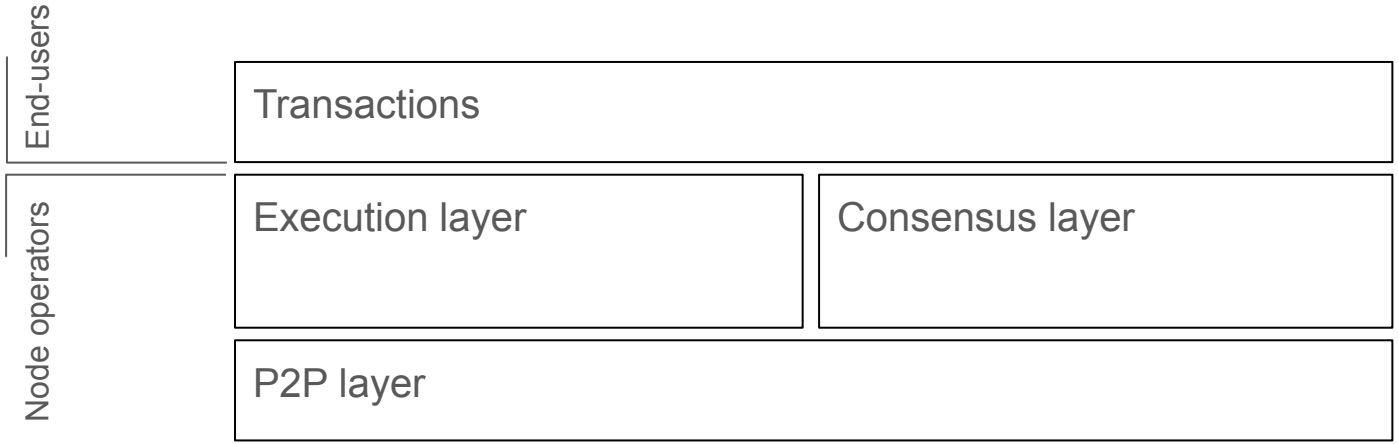
$$\sigma_{t+1} \equiv Y(\sigma_t, T)$$



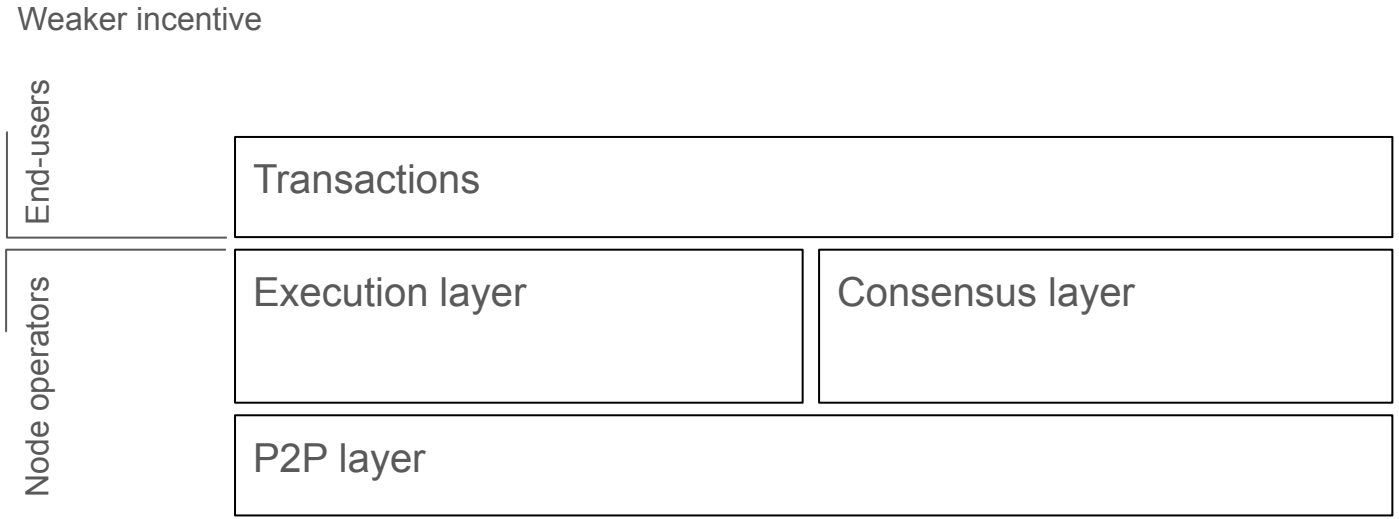
Flexibility framework



Flexibility framework | Coordination

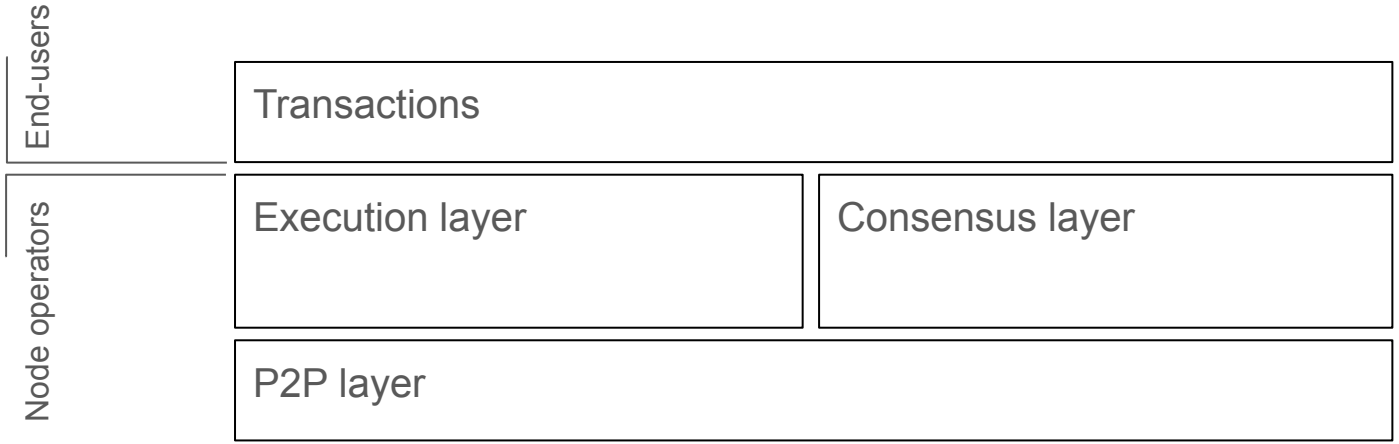


Flexibility framework | Coordination



Flexibility framework | Coordination

Weaker incentive



Stronger incentive

HSM

Flexibility framework | Types

- Singular

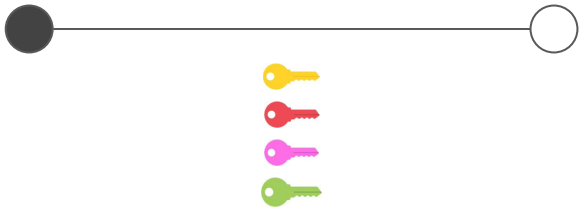
Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular

- Selected



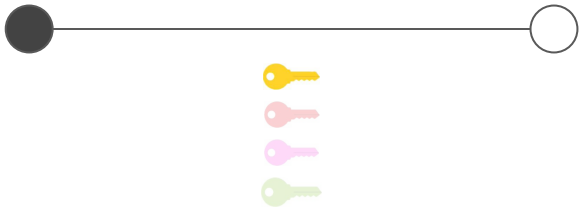
Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular

- Selected



Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular

- Selected

Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular

- Selected

- Negotiated

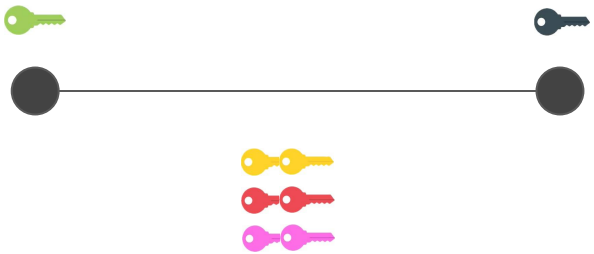
Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular

- Selected



- Negotiated

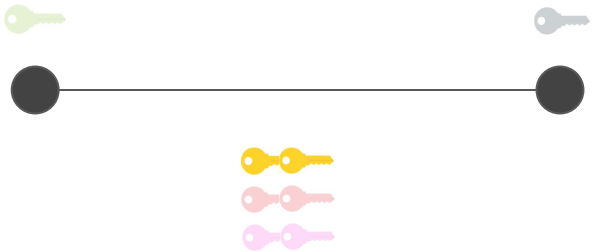
Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular

- Selected



- Negotiated

Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular

- Selected

- Negotiated

Legend:

: cryptographic scheme

Flexibility framework | Types

- Singular 
- Selected 
- Negotiated 

Flexibility framework | Types

- Singular 

  Simple

- Selected 

- Negotiated 

Flexibility framework | Types

- Singular

Simple

- Selected

- Negotiated

Flexibility framework | Types

- Singular

Simple

Synchronous upgrade

- Selected

- Negotiated

Flexibility framework | Types

- Singular

Simple

Synchronous upgrade

- Selected

Support multiple schemes

- Negotiated

Flexibility framework | Types

- Singular

Simple

Synchronous upgrade

- Selected

Support multiple schemes

- Negotiated

Flexibility framework | Types

- Singular

Simple

Synchronous upgrade

- Selected

Support multiple schemes

- Negotiated

Flexibility framework | Types

- Singular

Simple

Synchronous upgrade

- Selected

Support multiple schemes

Asynchronous upgrade

- Negotiated

Flexibility framework | Types

- Singular

Simple

Synchronous upgrade

- Selected

Support multiple schemes

Asynchronous upgrade

- Negotiated

Support multiple schemes

Communication

Flexibility framework | Types

- Singular

Simple

Synchronous upgrade

- Selected

Support multiple schemes

Asynchronous upgrade

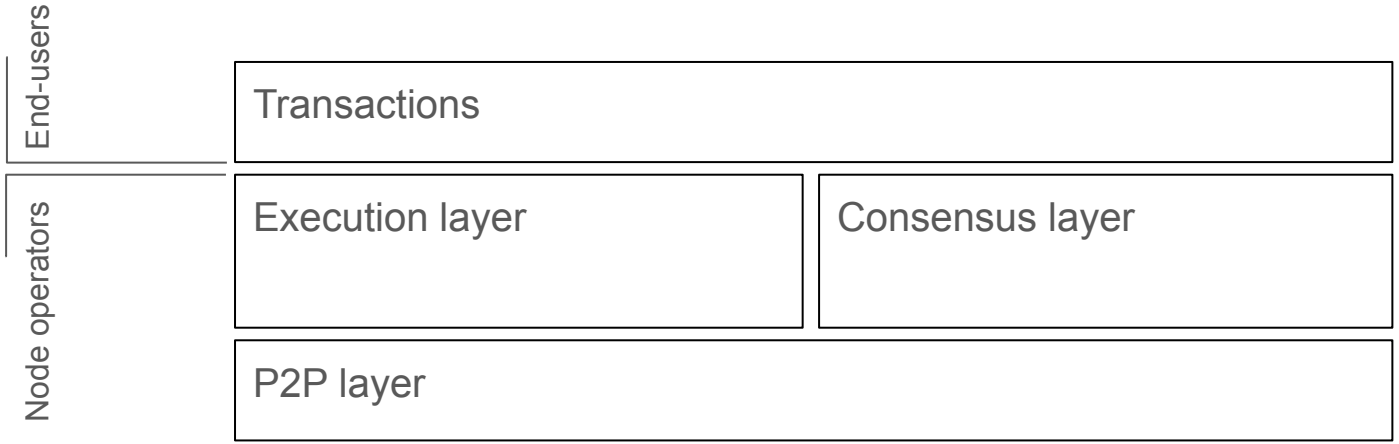
- Negotiated

Support multiple schemes

Communication

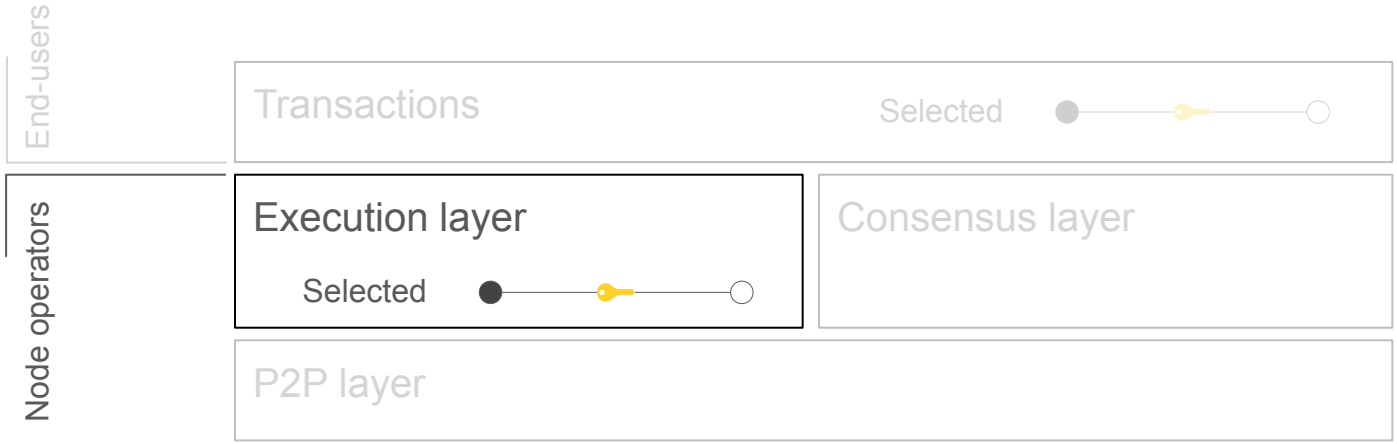
Asynchronous upgrade

Flexibility framework

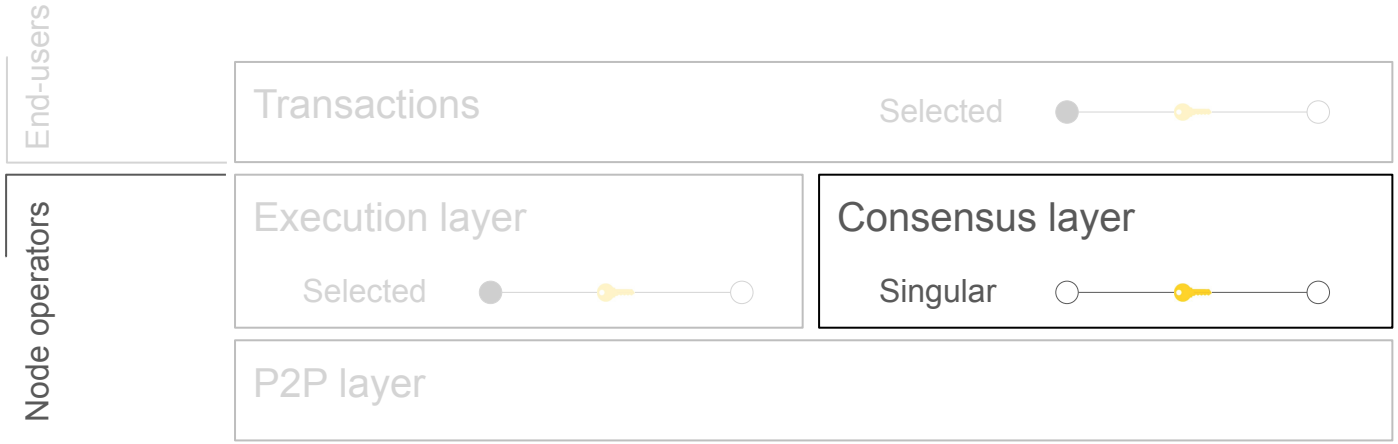


Flexibility framework

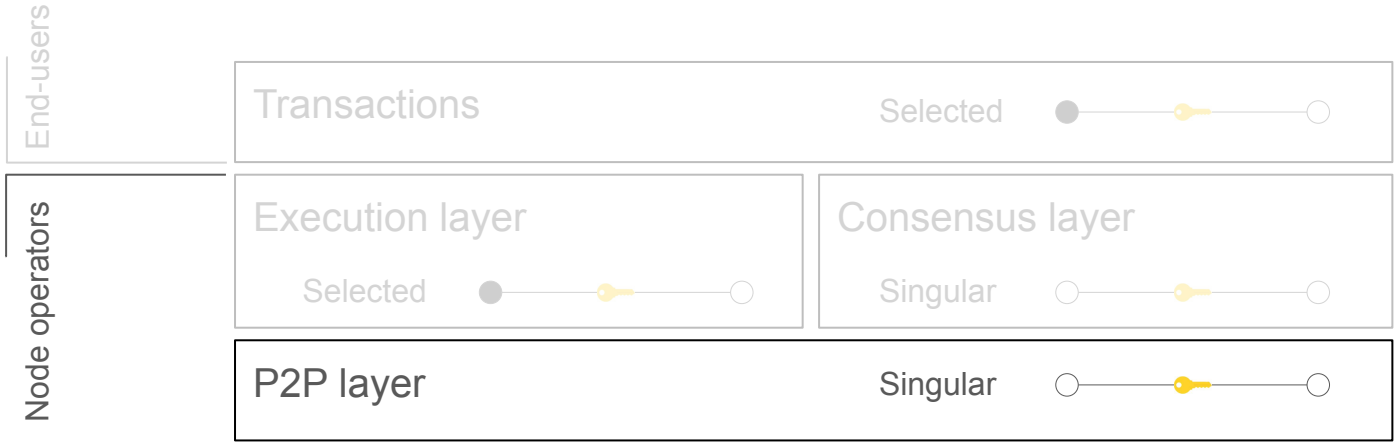
Flexibility framework



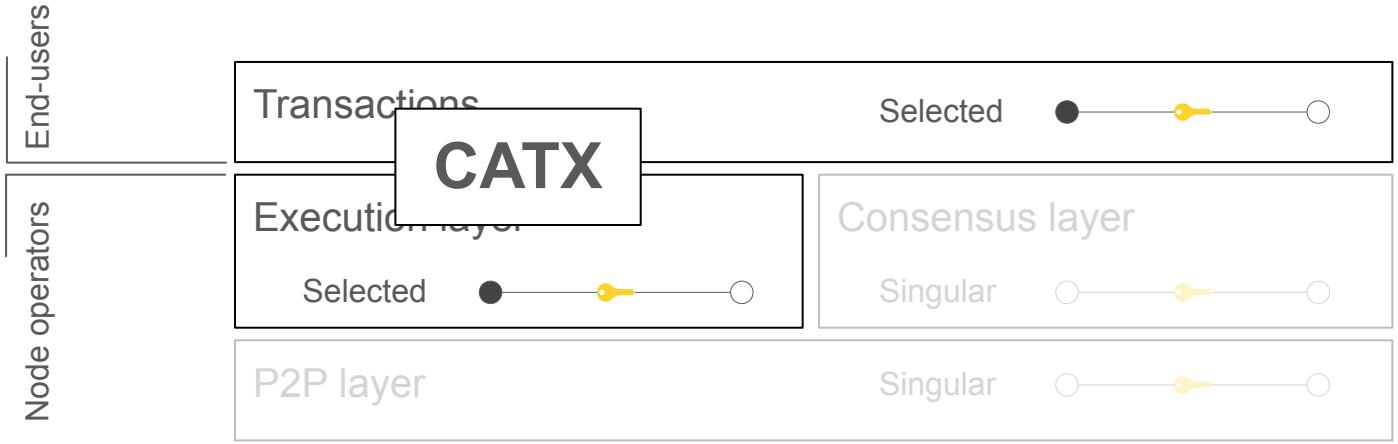
Flexibility framework



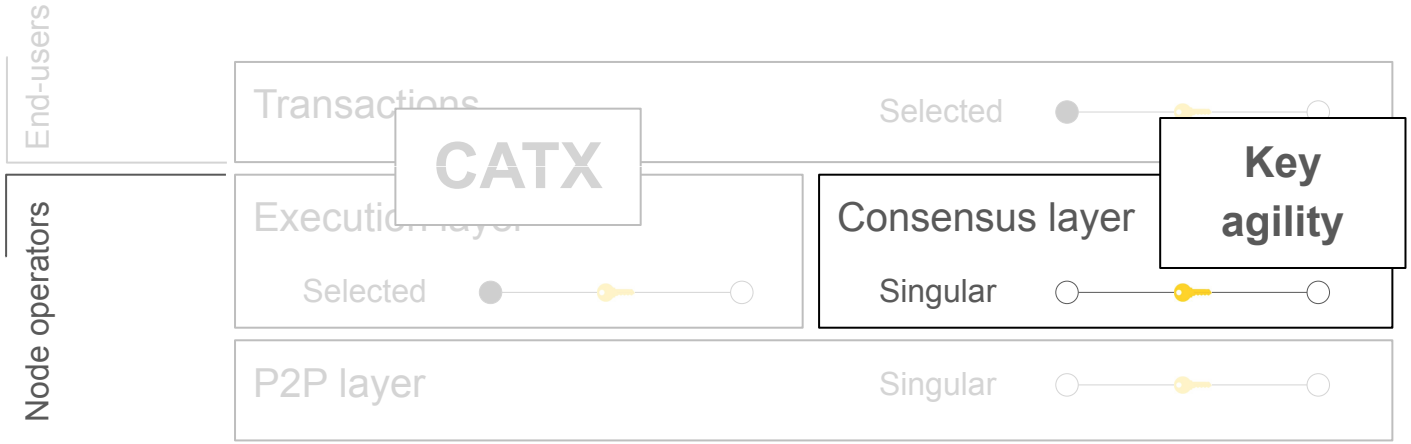
Flexibility framework



Flexibility framework



Flexibility framework



Cryptographically agile transactions (CATX)

Cryptographically agile transactions (CATX)

Legacy typed-transaction:

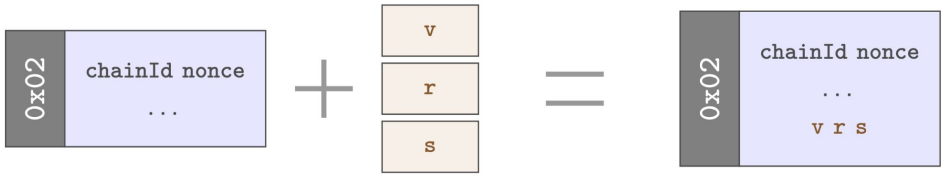
Cryptographically agile transactions (CATX)

Legacy typed-transaction:

$$\mathrm{Tx} = \texttt{0x02} \,\|\, \mathrm{RLP}\left(\begin{array}{c}\texttt{chainId}, \texttt{nonce}, \texttt{maxTip}, \texttt{maxFee}, \texttt{gasLimit}, \\ \texttt{destination}, \texttt{amount}, \texttt{data}, \texttt{accessList}, \texttt{v}, \texttt{r}, \texttt{s}\end{array}\right)$$

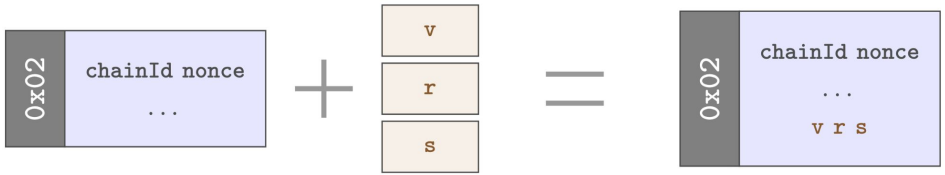
Cryptographically agile transactions (CATX)

Legacy typed-transaction:



Cryptographically agile transactions (CATX)

Legacy typed-transaction:

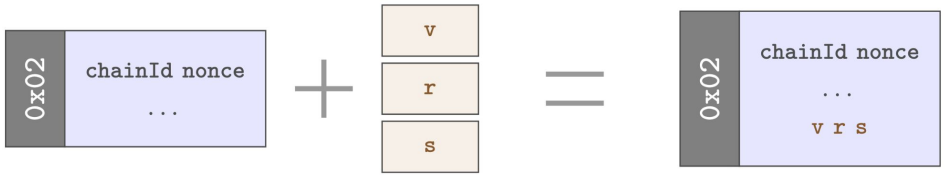


Limitations:

- Assumes pk recovery

Cryptographically agile transactions (CATX)

Legacy typed-transaction:

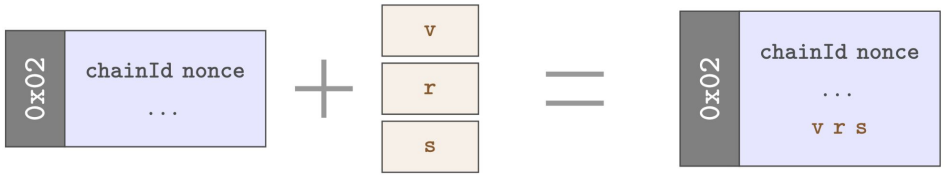


Limitations:

- Assumes pk recovery
- Signature hardcoded inside tx serialization

Cryptographically agile transactions (CATX)

Legacy typed-transaction:



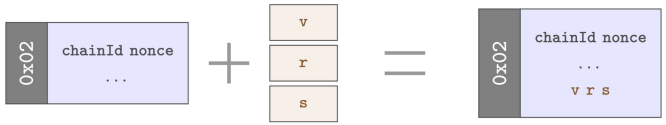
Limitations:

- Assumes pk recovery
- Signature hardcoded inside tx serialization

❌ Modularity

Cryptographically agile transactions (CATX)

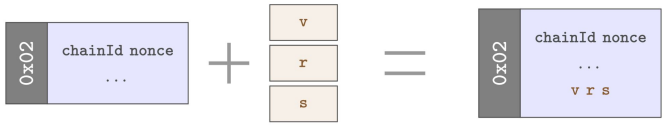
Legacy typed-transaction:



CATX design:

Cryptographically agile transactions (CATX)

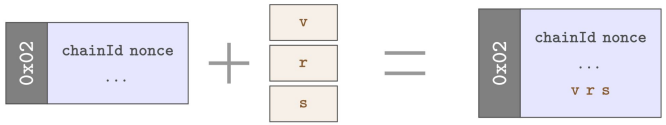
Legacy typed-transaction:



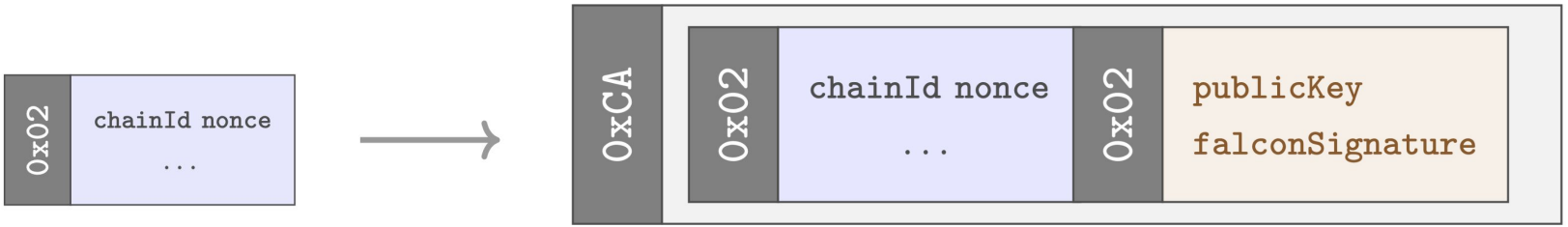
CATX design: $\texttt{Tx} = \texttt{0xCA} \,\|\, \texttt{bodyType} \,\|\, \text{RLP}(\texttt{bodyData}) \,\|\, \texttt{sigType} \,\|\, \text{RLP}(\texttt{sigData})$

Cryptographically agile transactions (CATX)

Legacy typed-transaction:

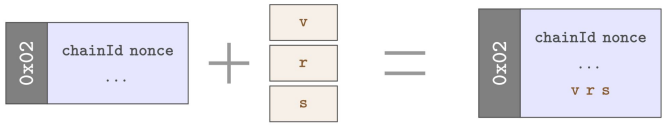


CATX design: $\texttt{Tx} = \texttt{0xCA} \,\|\, \texttt{bodyType} \,\|\, \text{RLP}(\texttt{bodyData}) \,\|\, \texttt{sigType} \,\|\, \text{RLP}(\texttt{sigData})$

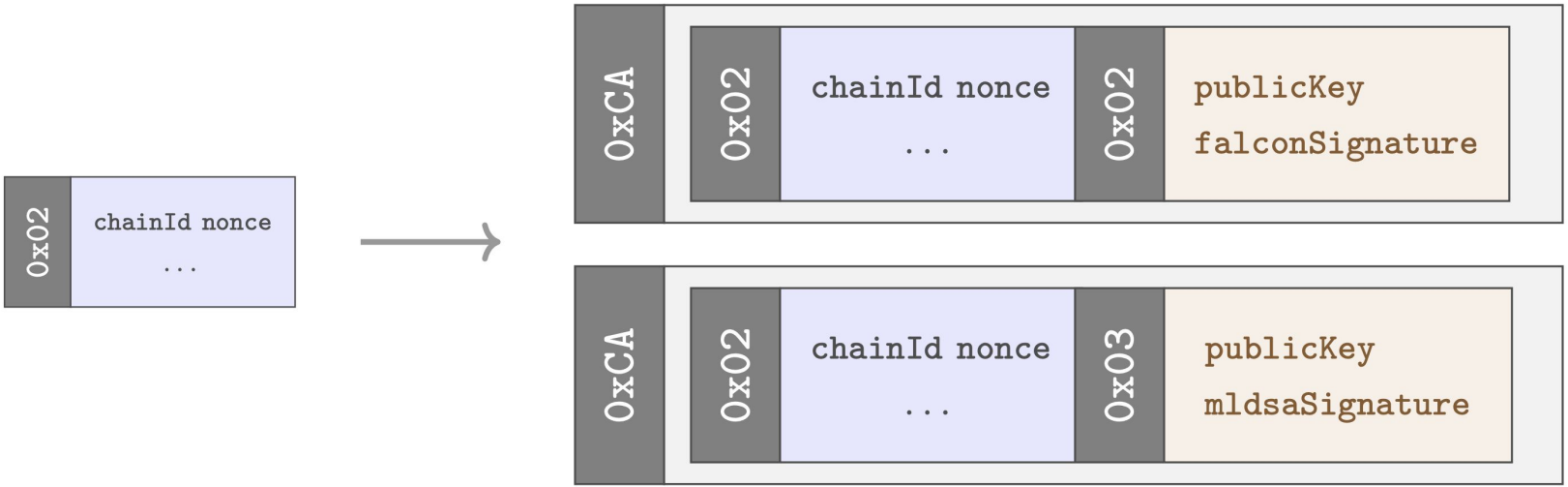


Cryptographically agile transactions (CATX)

Legacy typed-transaction:



CATX design: $\texttt{Tx} = \texttt{0xCA} \,\|\, \texttt{bodyType} \,\|\, \text{RLP}(\texttt{bodyData}) \,\|\, \texttt{sigType} \,\|\, \text{RLP}(\texttt{sigData})$



Experiments

Experiments

Main question:

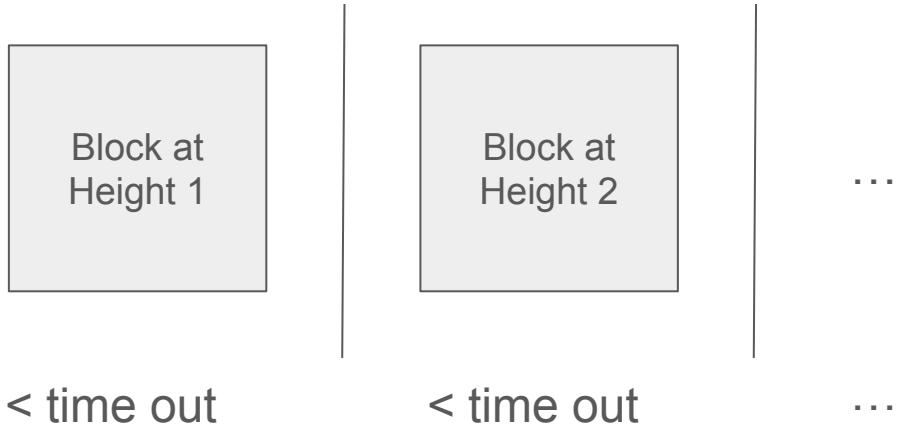
TPS: Tx/s

Experiments

Main question:

TPS: Tx/s

Tendermint consensus:

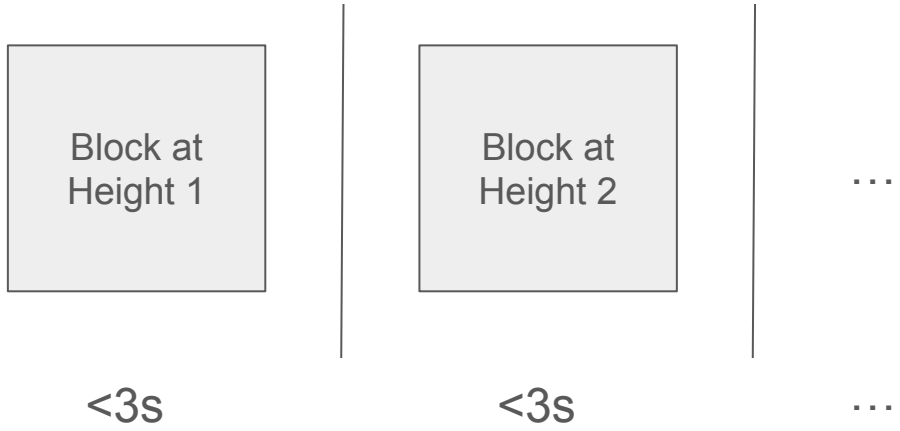


Experiments

Main question:

TPS: Tx/s

Tendermint consensus:

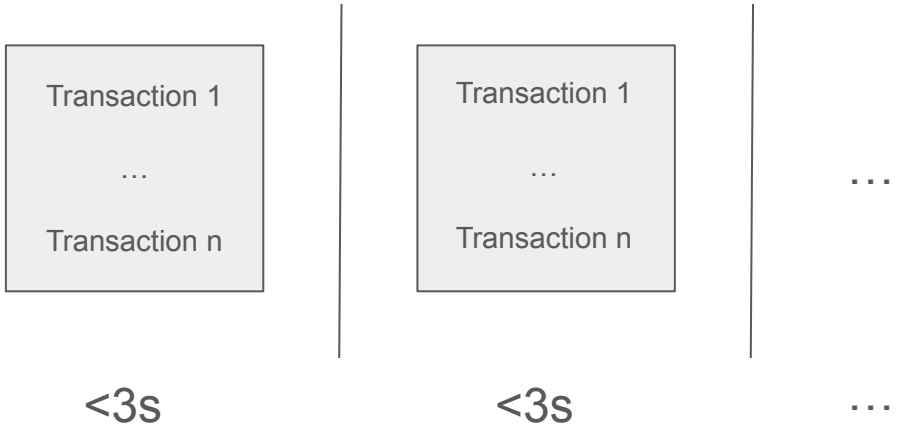


Experiments

Main question:

TPS: Tx/s

Tendermint consensus:



Experiments

Main question:

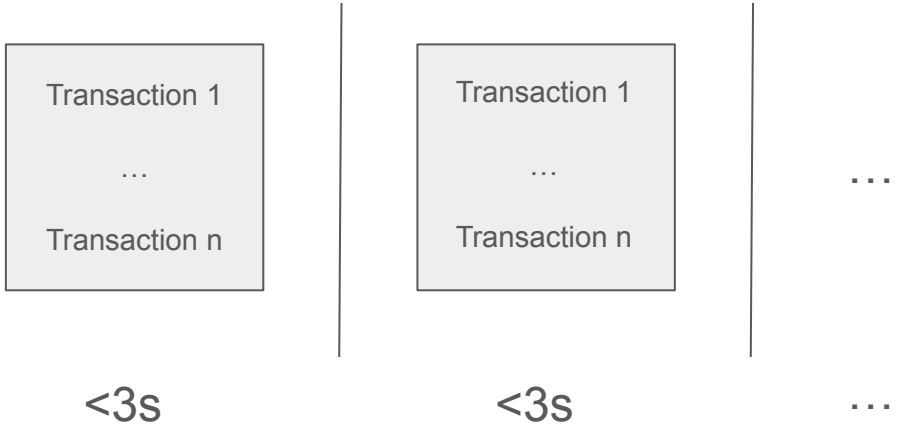
TPS: Tx/s

Tendermint consensus:

1 block proposer:

- Gather Tx
- Verifies Tx
- Proposes block

Attestors check



Experiments

Main question:

TPS: Tx/s

Tendermint consensus:

1 block proposer:

- Gather Tx
- Verifies Tx
- Proposes block

Attestors check

<3s

<3s

Constraints:

- CPU & disk i/o

Experiments

Main question:

TPS: Tx/s

Tendermint consensus:

1 block proposer:

- Gather Tx
- Verifies Tx
- Proposes block

Attestors check

<3s

<3s

Constraints:

- CPU & disk i/o
- Gas

Experiments

Main question:

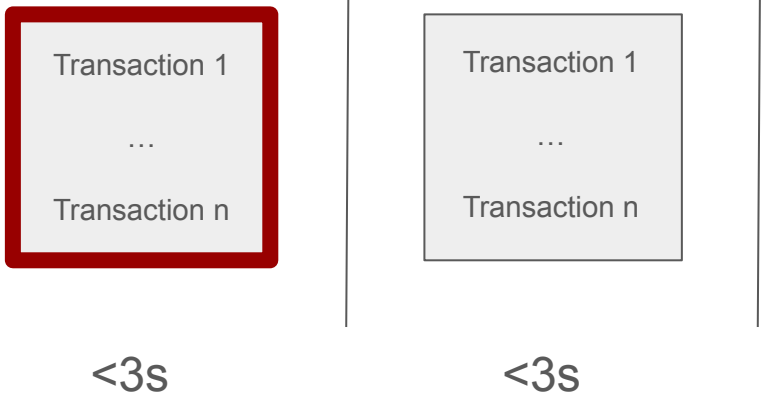
TPS: Tx/s

Tendermint consensus:

1 block proposer:

- Gather Tx
- Verifies Tx
- Proposes block

Attestors check



Constraints:

- CPU & disk i/o
- Gas
- Block size

Experiments

Type	Peak TPS	Sustained TPS	Gas%	Size%	Bottleneck
Legacy	4,021	3,963	19%	1%	CPU
ECDSA	4,032	3,964	22%	2%	CPU
Falcon-512	3,730	1,625	78%	72%	Mixed
ML-DSA-44	2,210	3,794	46%	**100%**	**Block size**

Experiments

Type	Peak TPS	Sustained TPS	Gas%	Size%	Bottleneck
Legacy	4,021	3,963	19%	1%	CPU
ECDSA	4,032	3,964	22%	2%	CPU
Falcon-512	3,730	1,625	78%	72%	Mixed
ML-DSA-44	2,210	3,794	46%	**100%**	**Block size**

ECDSA: limited by round timeout

Falcon + ML-DSA: limited by block size

MAgiCS '26 Workshop (affiliated with Eurocrypt 2026)

10 May 2026, Rome

Thank you

Manuel B. Santos

manuel.batalha.santos@gmail.com