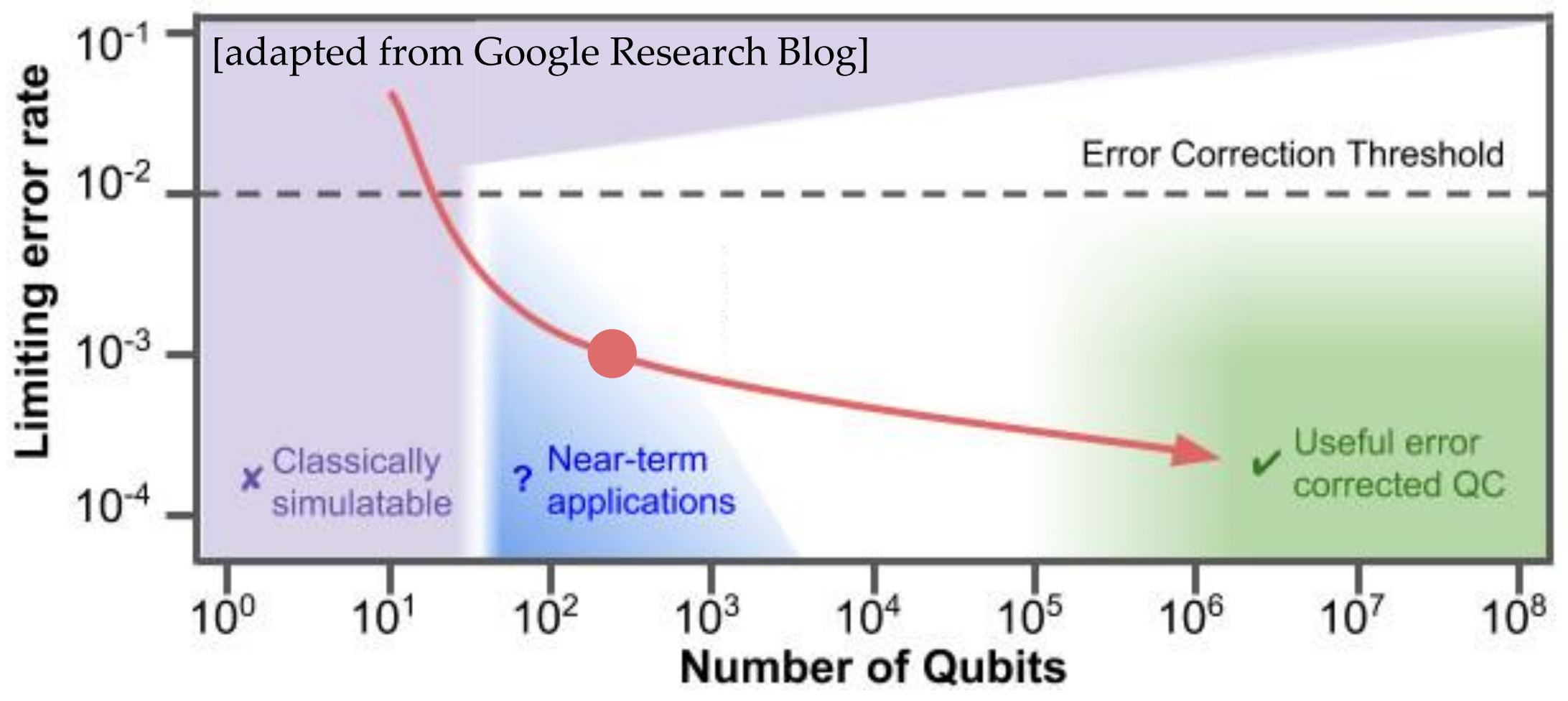
Quantum Proof of Work with Parametrized Quantum Circuits

Maximus Liu[1], Khadijeh Najafi[2], Michael Dubrovsky[3] and Mikhail Y. Shalaginov[4]

[1] Pingry School, Basking Ridge, NJ; [2] IBM Quantum, Yorktown Heights, NY; [3]PoWx, Cambridge, MA; [4]MIT, Cambridge, MA

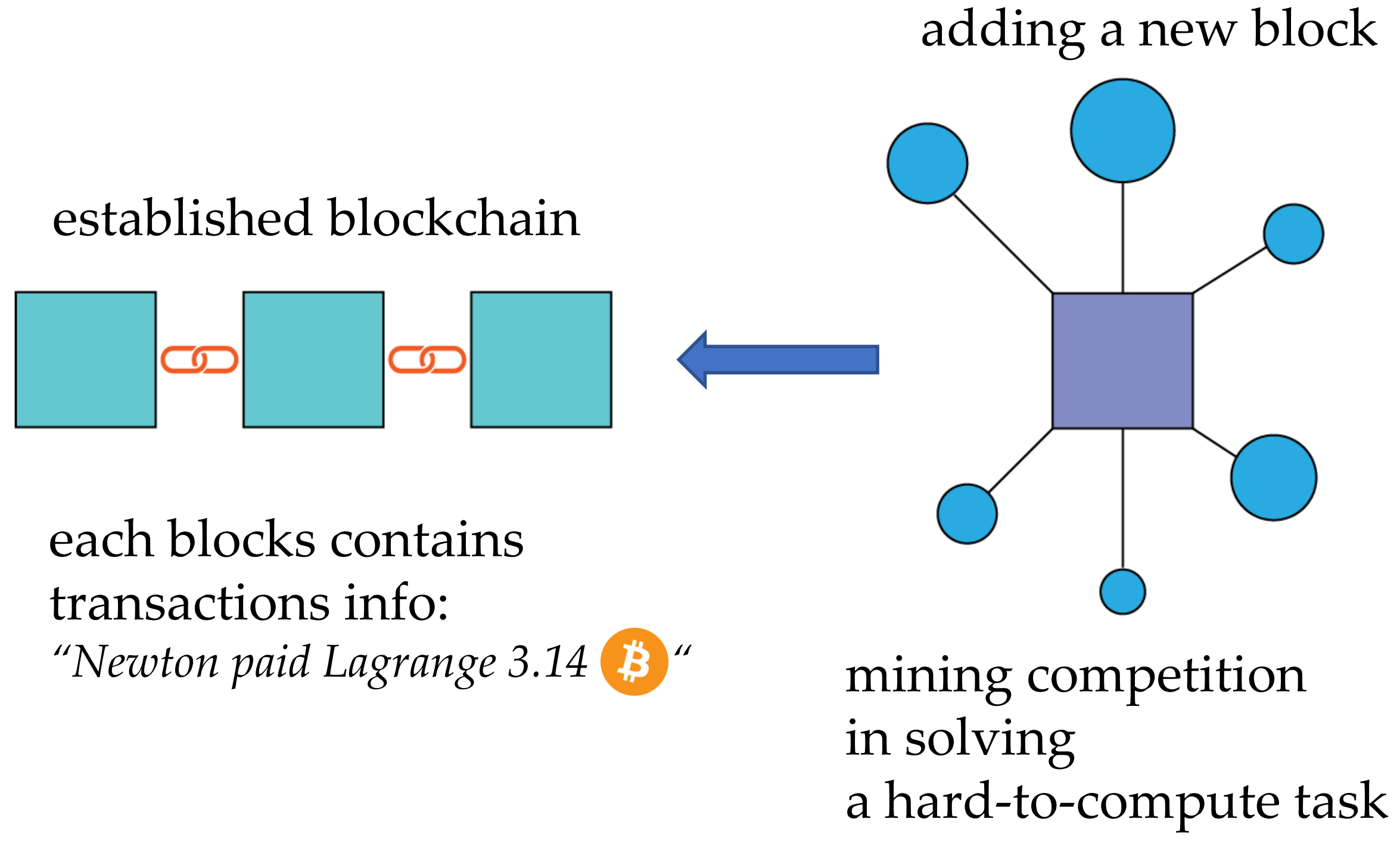
QuARC 2023
QSEC Annual Research Conference

Dozens of quantum computers are publicly available via cloud providers on Amazon Braket, Azure Quantum, IBM Q, etc.



How can we use available quantum computers?

Bitcoin blockchain

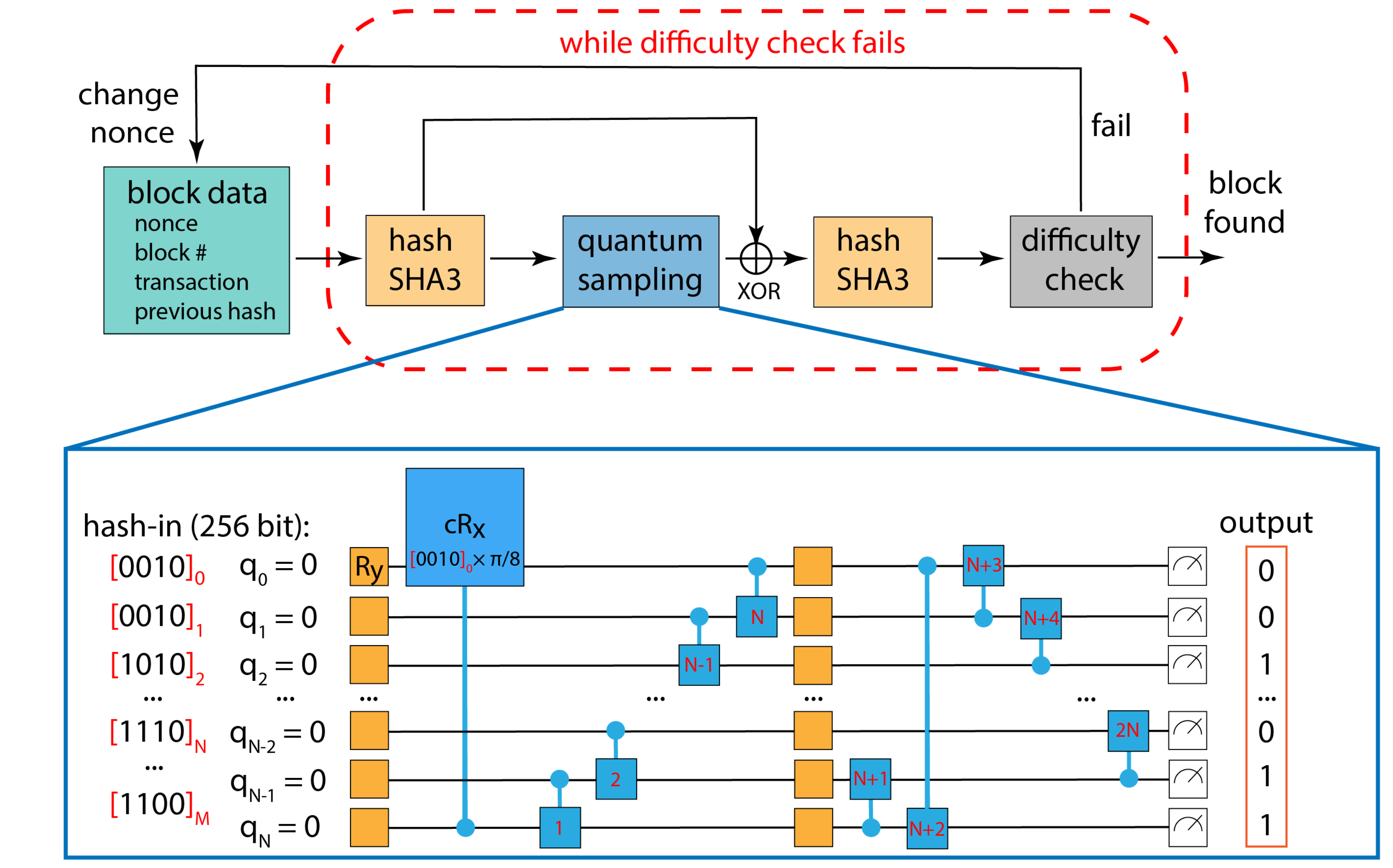


each blocks contains transactions info:
"Newton paid Lagrange 3.14 ₿"

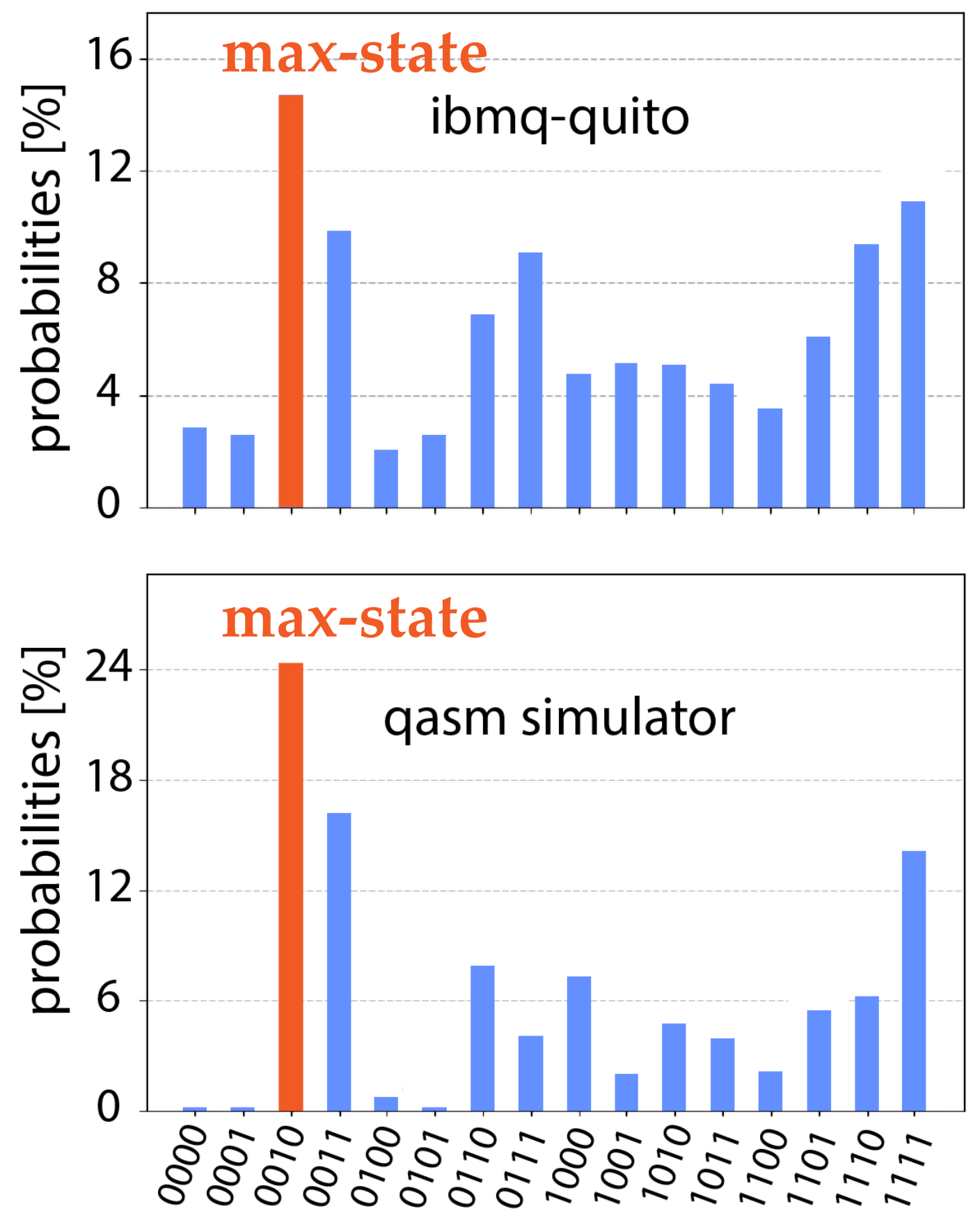
mining competition in solving a hard-to-compute task

- **decentralized** ledger of transactions
- successful **secure** record since its inception [secured by computational hardness]
- driving force for **developing superior hardware** [primarily GPUs and ASICs]

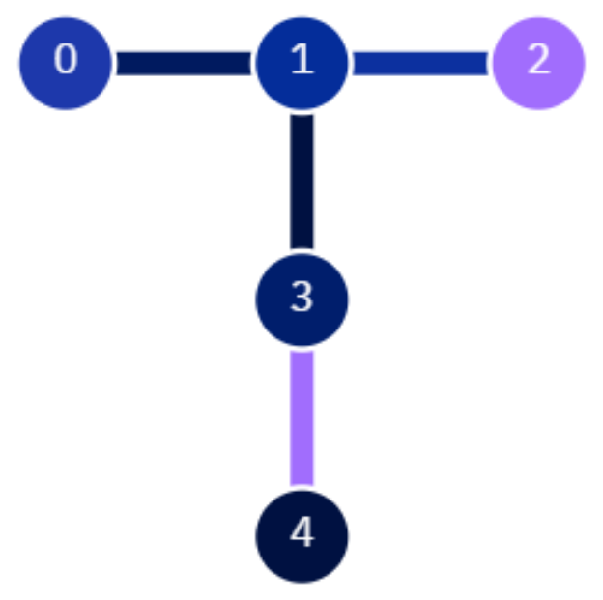
Bitcoin mining cycle with a quantum add-on



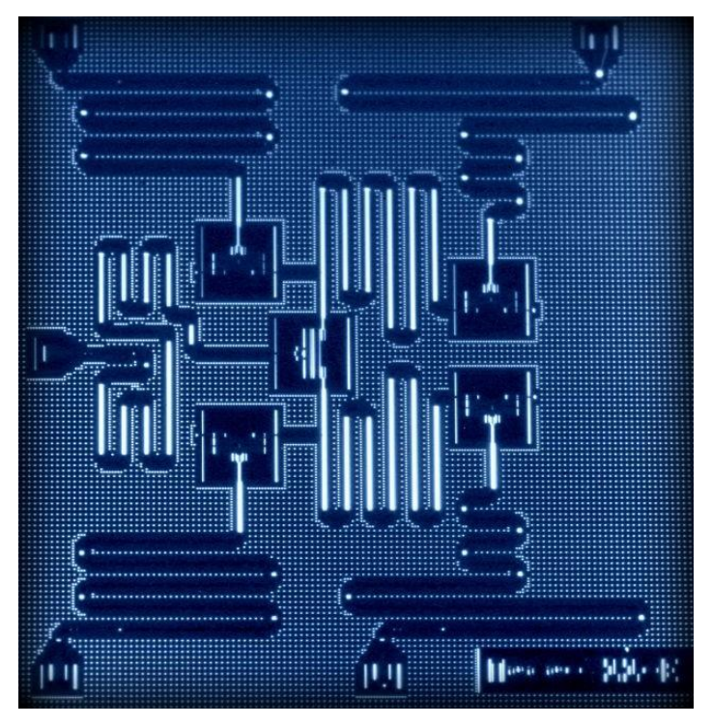
output histograms of the measurd quantum states after 20, 000 shots



ibmq-quito coupling map



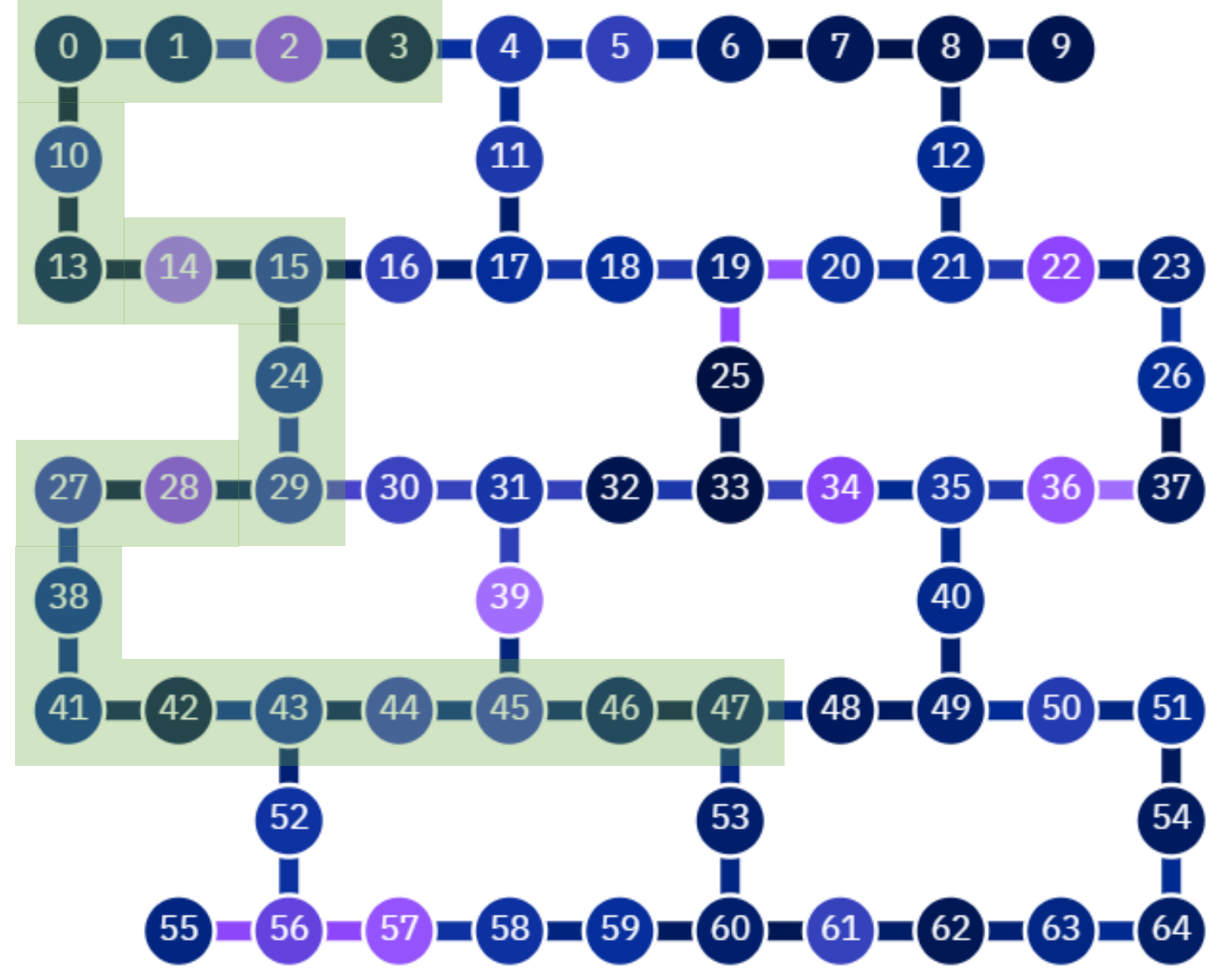
5 qubit computer by IBM



Found max-state(s) is further **multiplexed** with the input hash-string, **hashed** again, and **released** as an output for difficulty check.

Block is claimed **found** if the input **nonce** leads to the output with a specified **number of zeroes**

Quantum Proof-of-Work at minimal viable quantum advantage

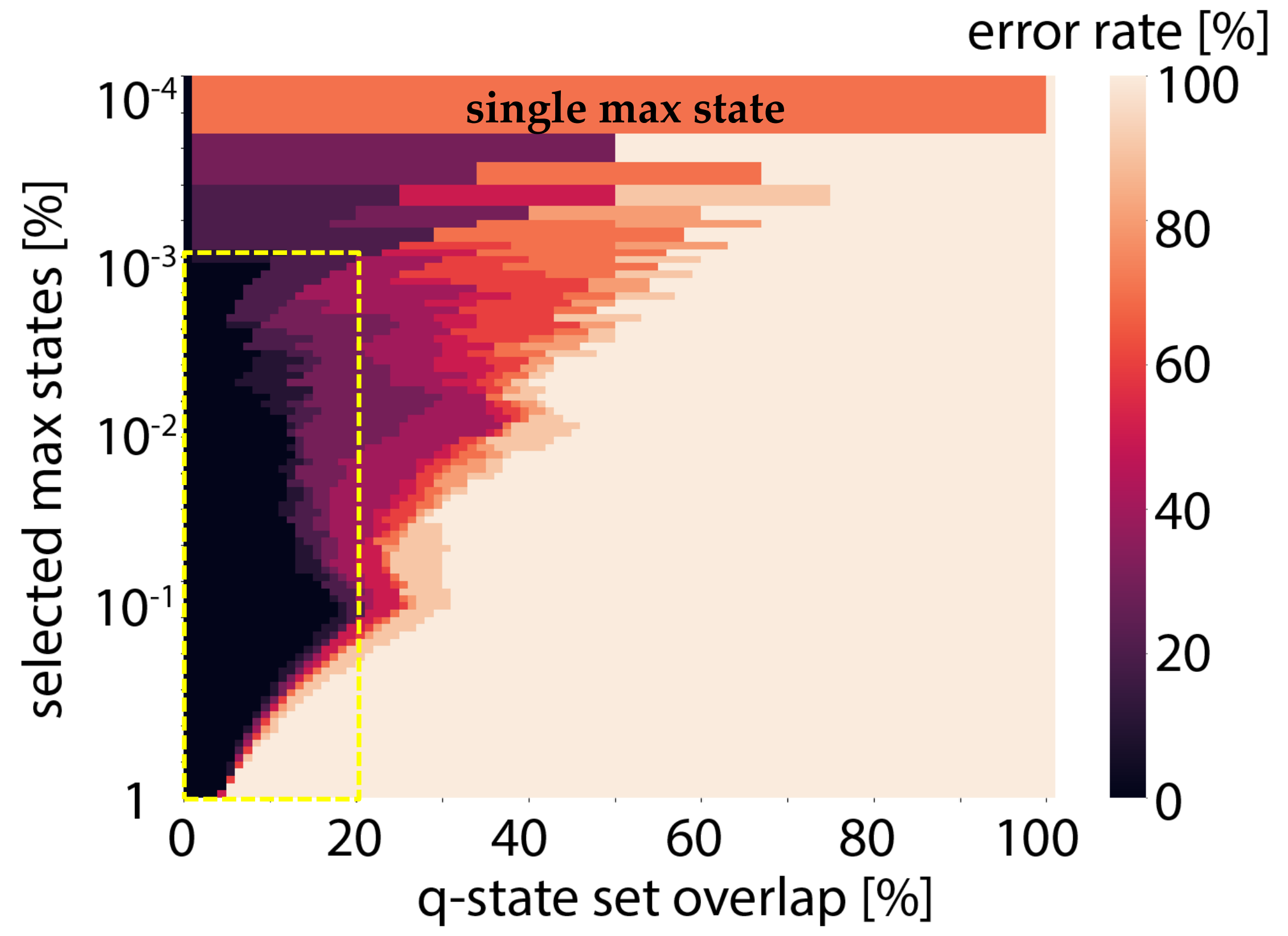


65-qubit ibm-ithaca quantum processor

nominal accuracy metrics:
- CNOT error – 1.1 %
- Readout error – 2.1%

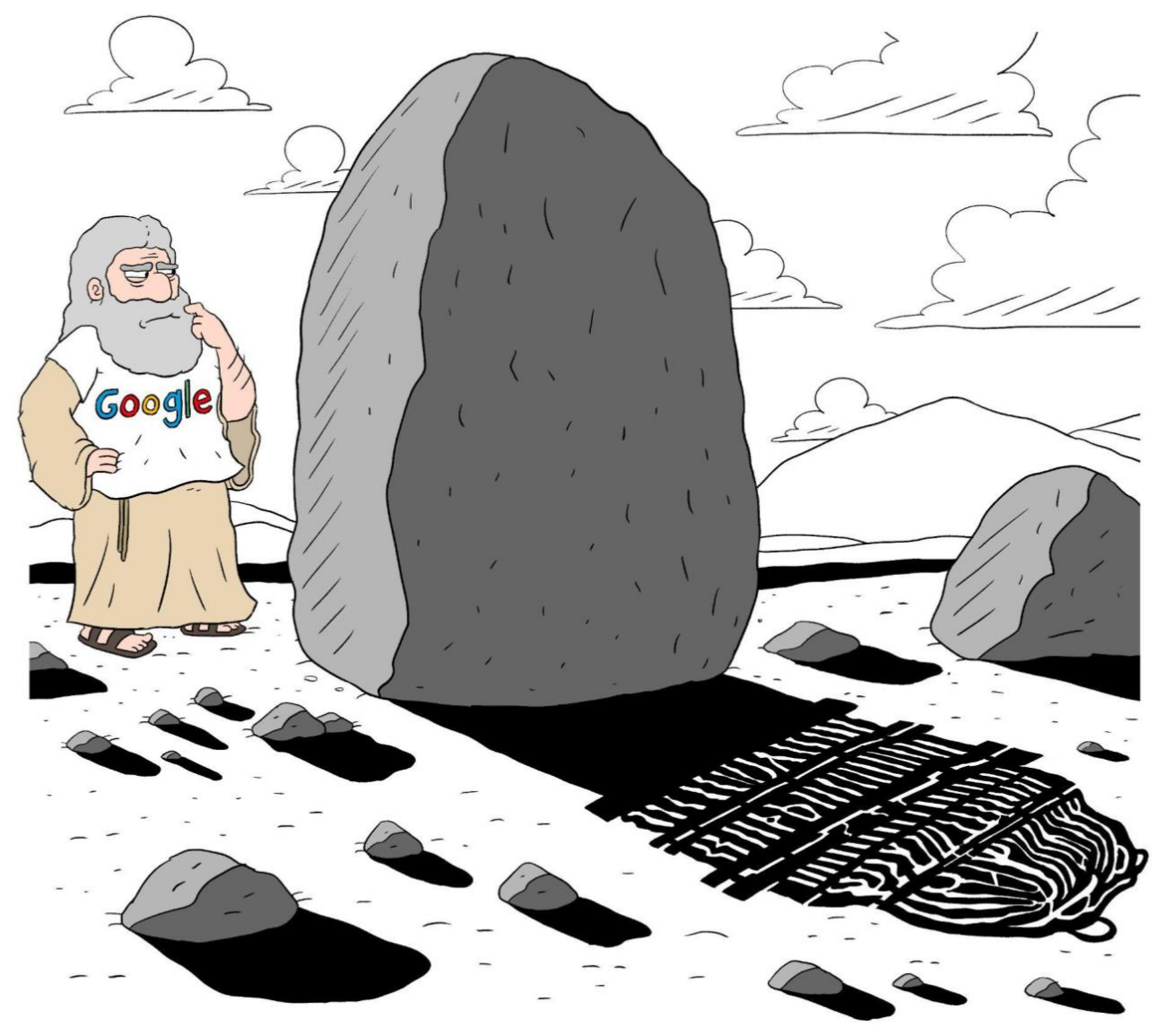
qasm simulations on a sequence of continuously connected **20 noisy qubits**

qubit-noise data was adopted from the actual ibm-ithaca backend

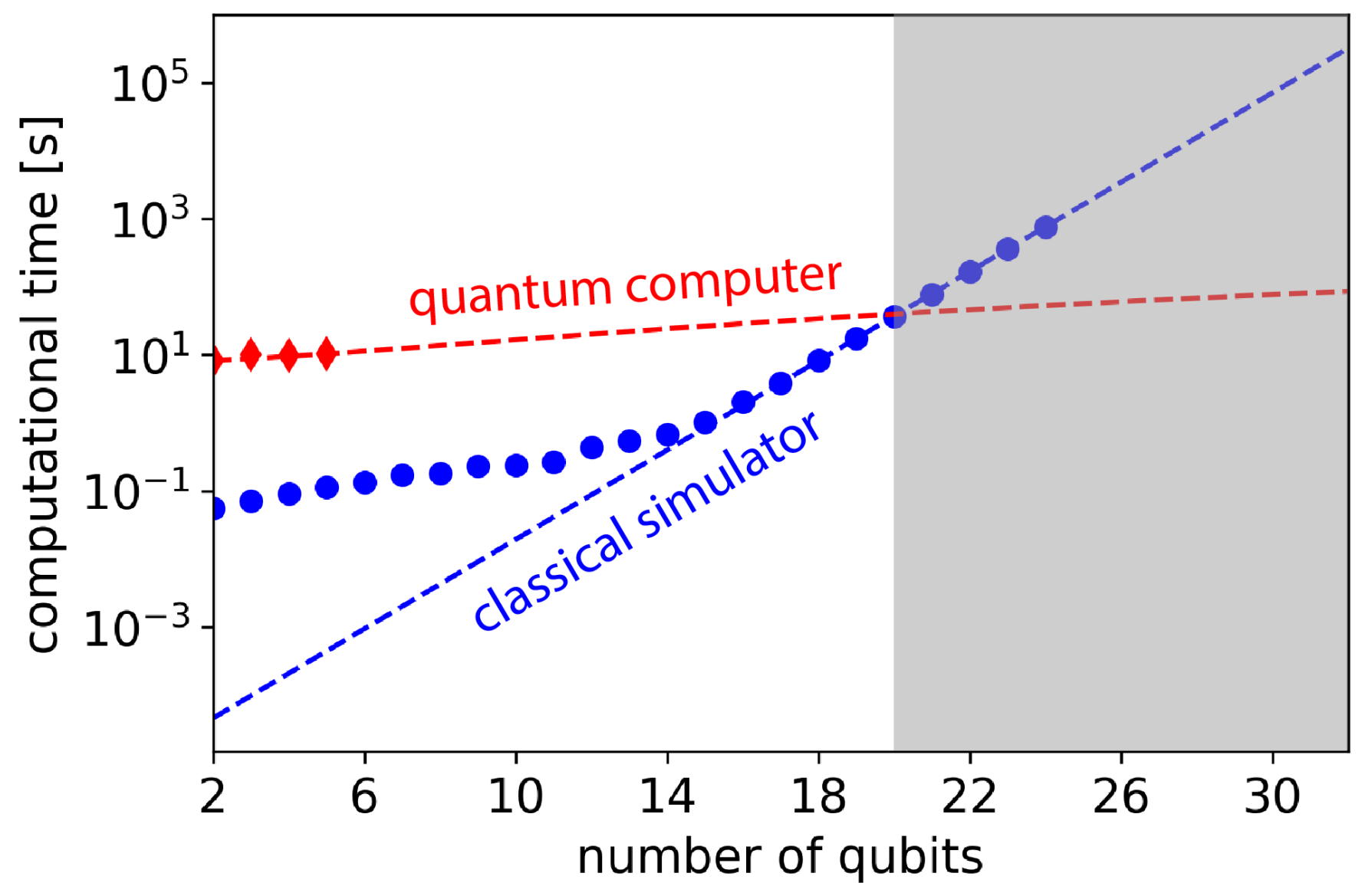


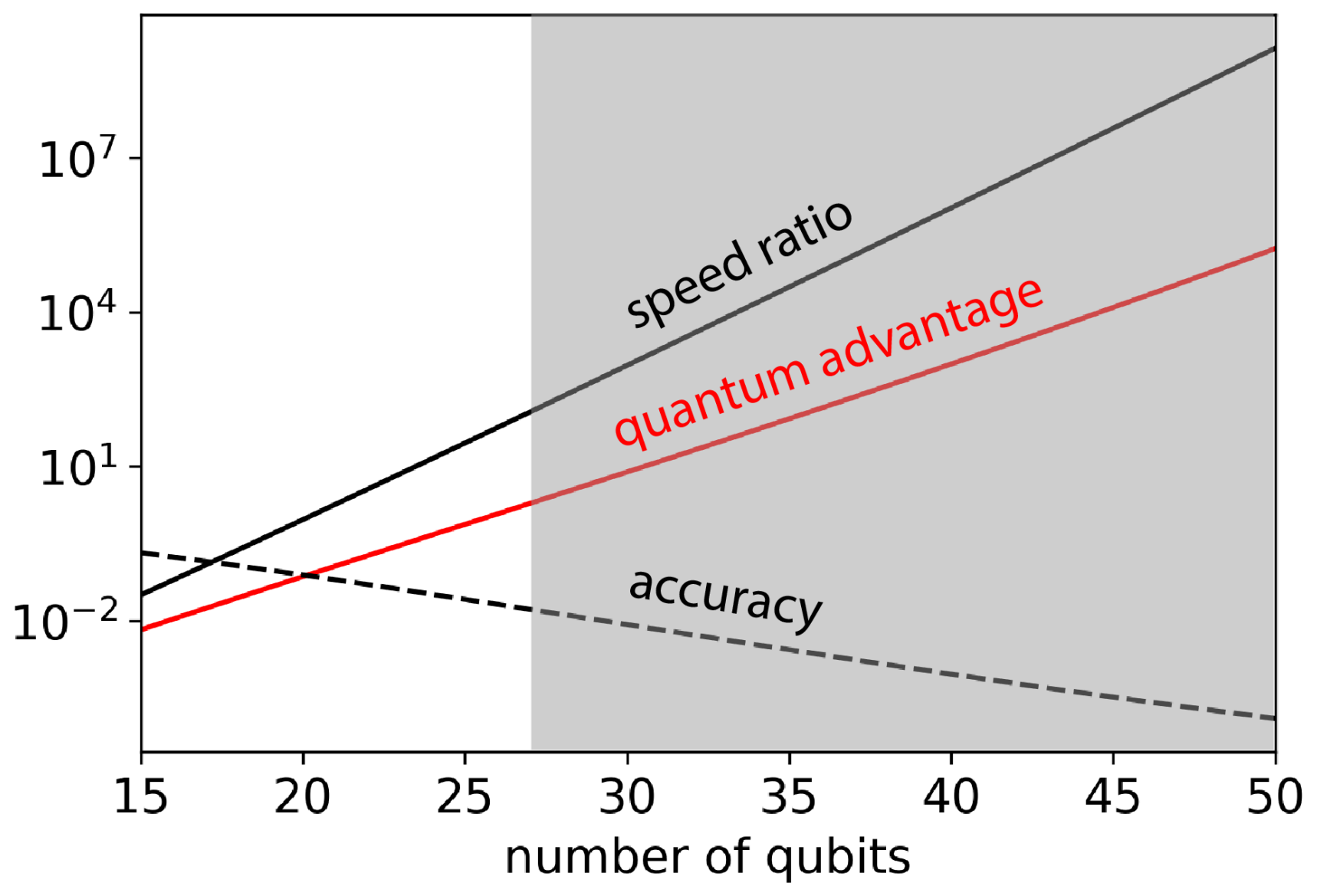
- With a large number of qubits, it is necessary to select a few max-states (not only a single one)
- At verification stage, the block is accepted by the qBTC network if there is at least a partial agreement between the lists of the max-states
- For the 20-qubit qPoW protocol, the best agreement happens when there is 20% overlap in the top 0.1% of the max-states, i.e. 200 out of 1000 max-states are the same

Can Google contrive a computation so complex, Google itself cannot verify it?



Quantum advantage reached with 20+ qubits





Take-home Outputs

- proposed a protocol for quantum-computer compatible proof of work (cryptographic mechanism used in Bitcoin mining)
- verified it on a realistic model of a 20-qubit superconducting IBM quantum processor

References:

[1] M. Shalaginov, M. Dubrovsky, "Quantum Proof of Work with Parameterized Quantum Circuits," arXiv:2204.10643v2, 2022.
[2] M. Dubrovsky, B. Penkovsky, et al., "Towards Optical Proof of Work," 2020.
[3] IBM Quantum. https://quantum-computing.ibm.com/, 2023

Acknowledgements: we are thankful to IBM Quantum for providing access to quantum computing resources. M. L. is supported by the Scholarship of Future Scholars at AARD.