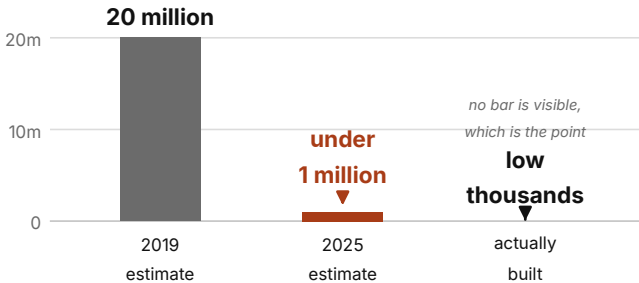


From 20 million qubits to under 1 million, and machines are still in the low thousands

Noisy qubits estimated as necessary to break RSA-2048, in 2 peer-reviewed analyses, against the machines that exist. Same unit throughout. The 2025 figure is a stated upper bound, and machine sizes move constantly, so neither is pinned to an exact value.



Source: Gidney and Ekerå, Quantum 5, 433 (2021); Gidney (2025). LaMarr Labs, lamarrlabs.com/resources