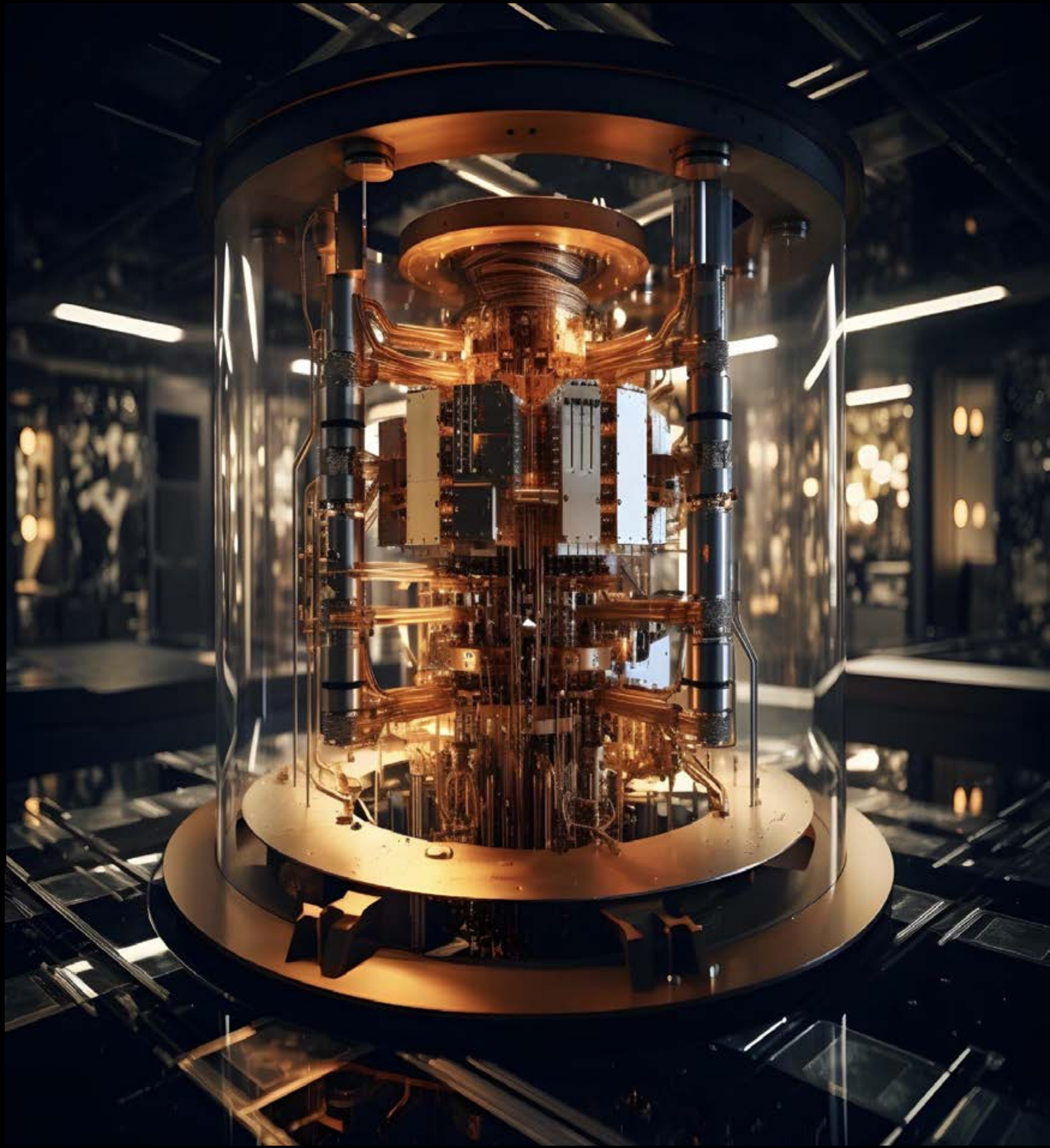
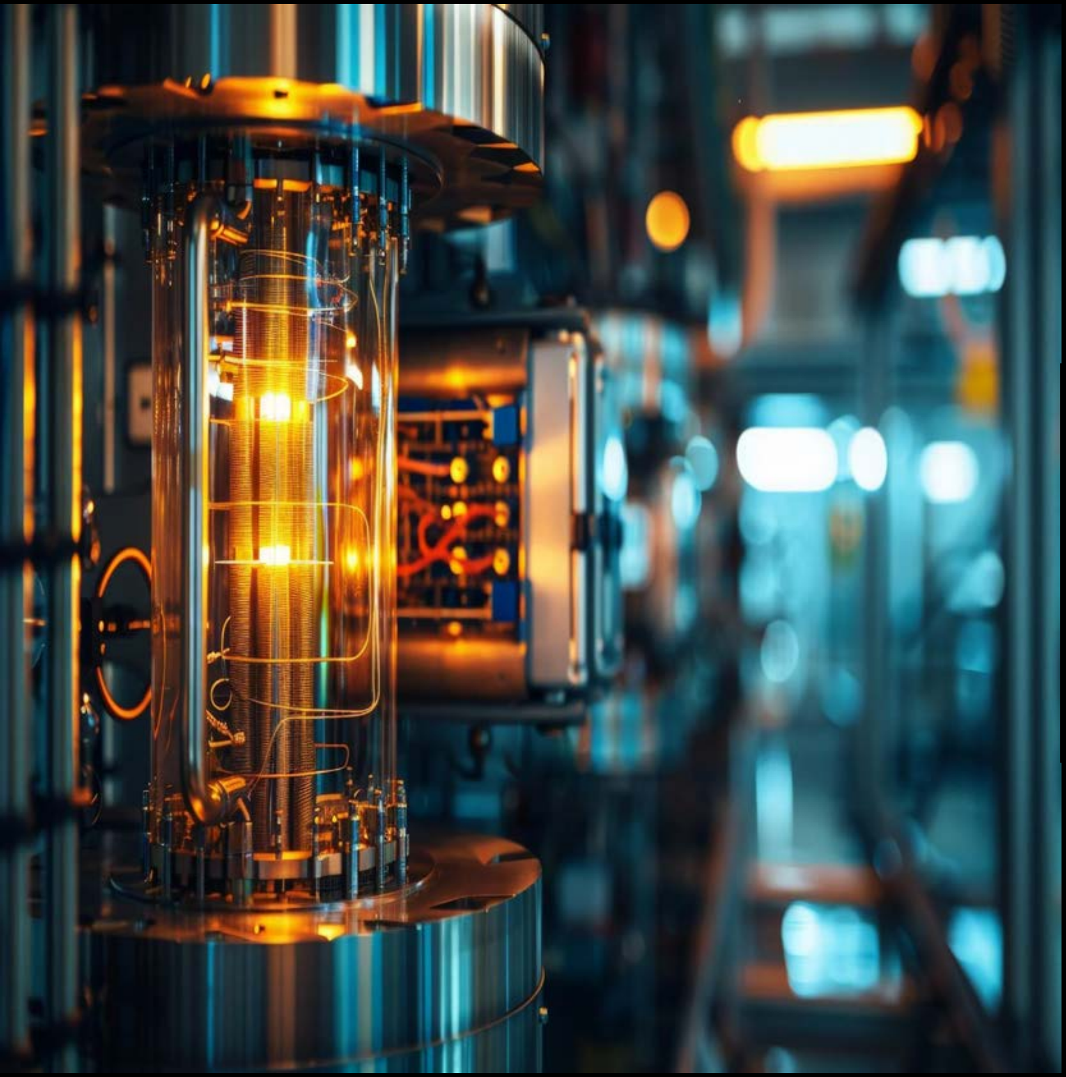
The Quantum Leap

Revolutionizing Secure Software Development with Quantum Computing



Quantum computing, with its ability to process information in fundamentally new ways, is poised to revolutionize secure software development paradigms. This presentation explores the core principles of quantum computing, including qubits, superposition, and entanglement, which enable exponential computational speedups. Quantum algorithms like Shor's algorithm for factoring large numbers and Grover's algorithm for database searches illustrate the potential to outperform classical algorithms, achieving efficiency gains of up to 1000x in certain applications.

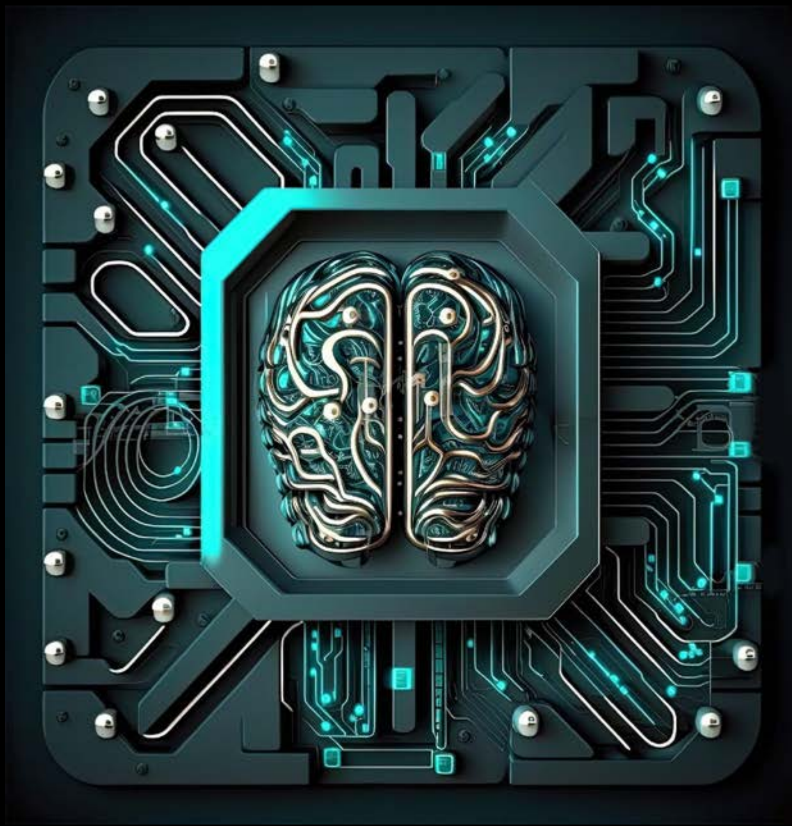


Classical Computer VS Quantum Computer

Task	Classical Computer	Quantum Computer
Number of states represented (50 qubits)	1	1.13 x 10^15
Time to factor 2048-bit RSA key	300 trillion years	10 seconds
Average number of operations to search 1 million entries	500,000	1,000
Time for specific calculation (Google's Sycamore)	10,000 years	200 seconds

Estimated Qubit Count

Year	Quantum Computing Market Size (Billion $)	Estimated Qubit Count in Leading Systems
2020	0.5	50
2021	1.2	100
2022	2.8	200
2023	6.5	400
2024	15.0	800
2025	25.0	1600
2026	35.0	3200
2027	45.0	6400
2028	52.0	12800
2029	58.0	25600
2030	65.0	51200



Quantum Principles

- Qubits: Basic unit of quantum information.
- Superposition: Ability to be in multiple states simultaneously.
- Entanglement: Strong correlations between qubits, even over large distances.


Qubit
s

$\alpha|0a+\beta|1\rangle$

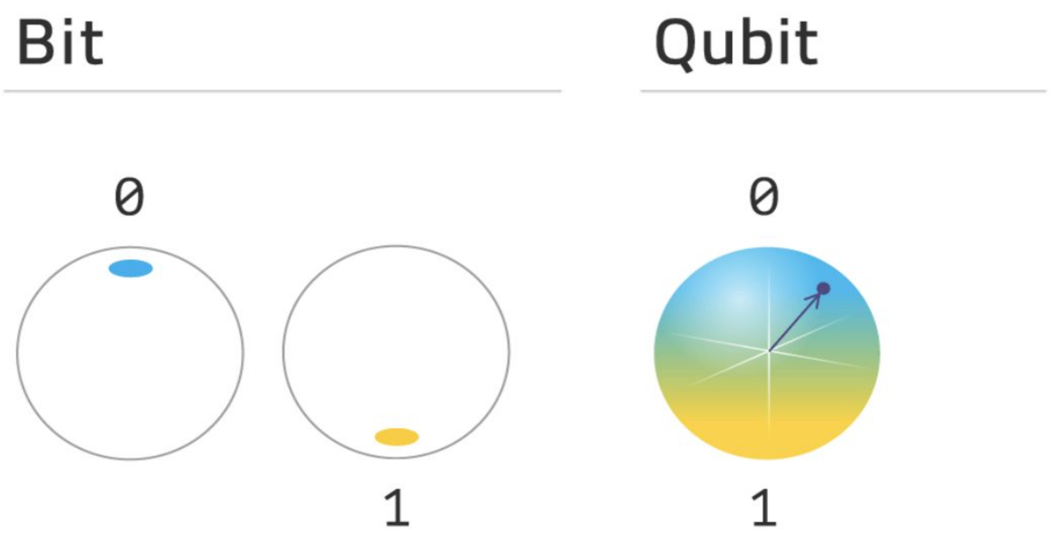
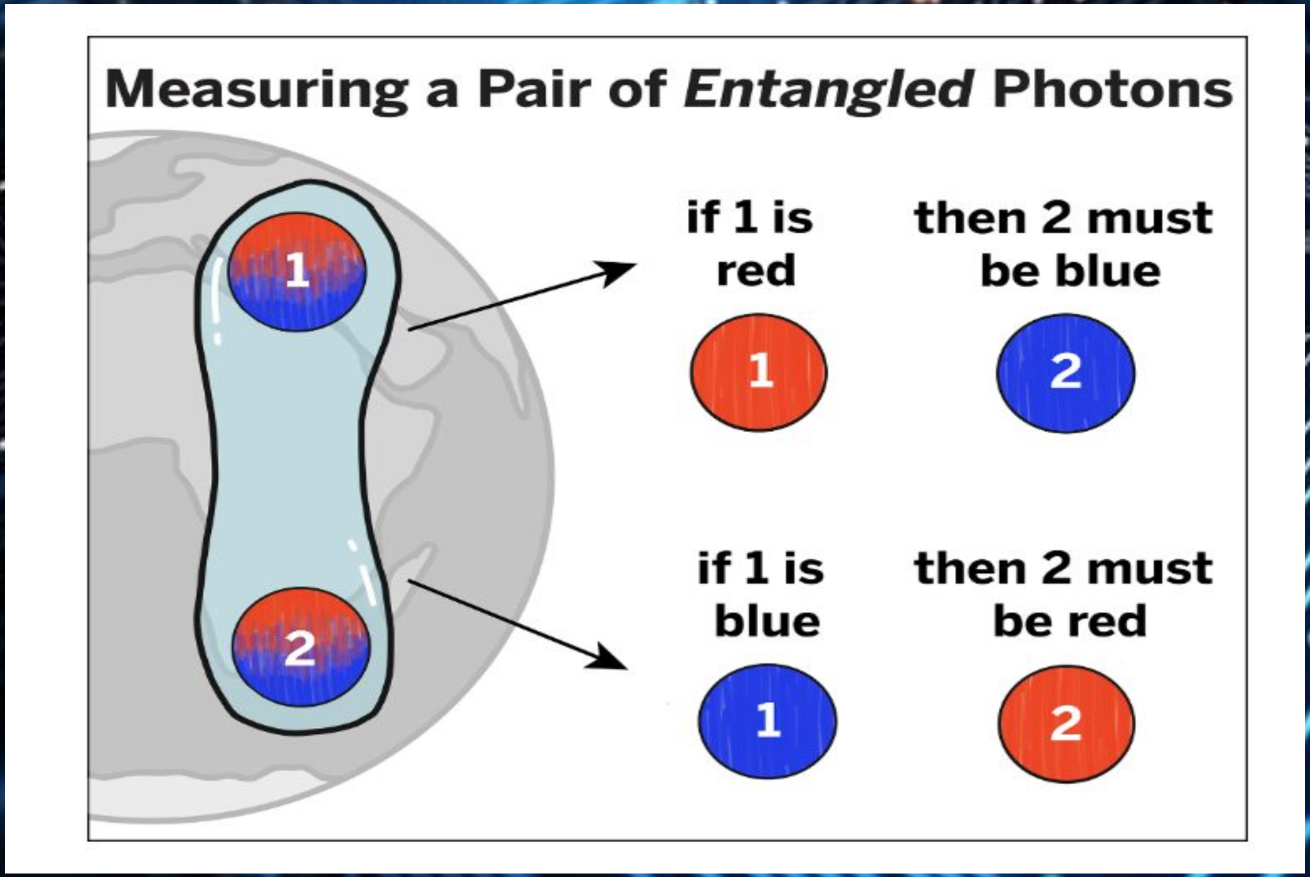


Figure 1: Visualizing a bit and a qubit.

Entanglement

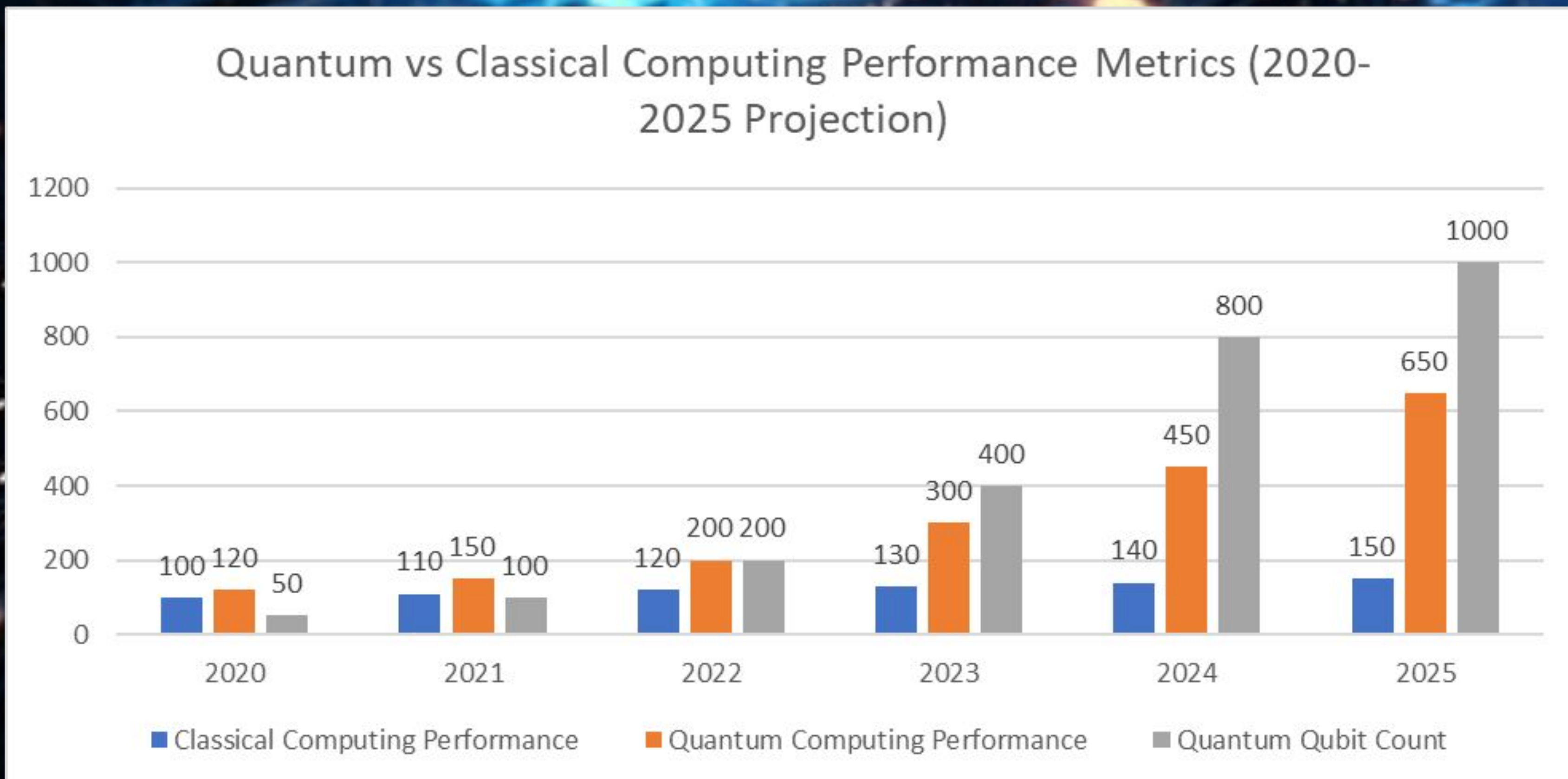


Quantum Algorithms

- Shor's Algorithm: Efficient factoring of large numbers.
- Grover's Algorithm: Quadratic speedup for database searches.

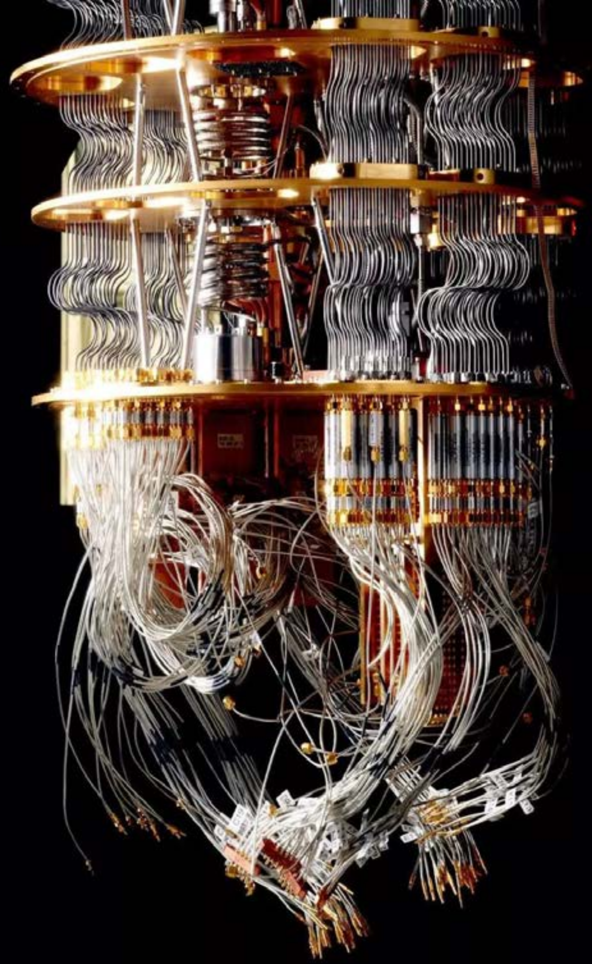
Shift in Software Development

- Evolution of programming languages and techniques.
- New languages: Qiskit, Q#, Cirq.
- Hybrid computing models: Collaboration between quantum and classical systems.
- Optimization of performance for cryptography and machine learning tasks.



Quantum vs Classical Computing Performance Metrics (2020-2025 Projection)
1200
1000
800
600
400
200
0
100
120
50
110
150
100
120
200
200
130
300
400
140
450
800
150
650
1000
2020
2021
2022
2023
2024
2025
Classical Computing Performance
Quantum Computing Performance
Quantum Qubit Count

Challenges in Quantum Software Engineering

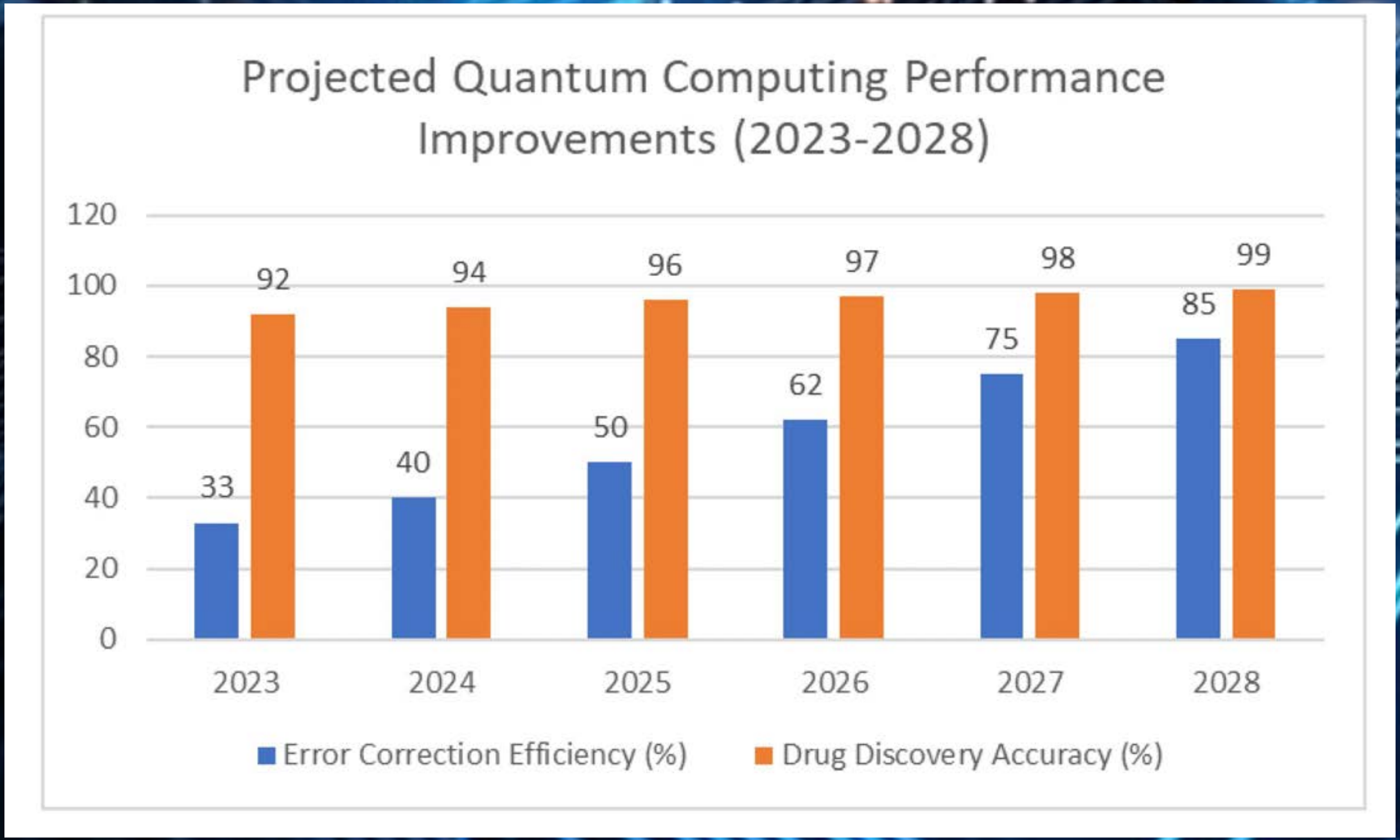


- Debugging complexity: Quantum state collapse upon measurement.
- Error susceptibility: Decoherence and noise.
- Scalability: Qubit scalability
- Algorithm Development

Opportunities in Quantum Computing

- Enhancing software security: Breaking traditional encryption methods.
- Development of unbreakable quantum cryptographic techniques.
- Revolutionizing optimization problems in logistics and finance.
- Quantum simulations for breakthroughs in materials science.
- Quantum machine learning: Up to 500x speed improvements in AI tasks.

Projected Quantum Computing Performance Improvements (2023-2028)



Conclusion

- Transformative impact on secure software development.
- Addressing challenges and leveraging opportunities.
- Insights into the future of quantum software engineering and its implications for cybersecurity.
- Exciting potential for solving complex problems.

References

1. Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.
2. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search.
3. Nielsen, M. A., & Chuang, I. L. (2011). Quantum Computation and Quantum Information.
4. Boston Consulting Group (2021). The Next Decade in Quantum Computing—and How to Play.
5. IBM Quantum. Qiskit Documentation.
6. Microsoft. Q# Documentation.
7. Google. Cirq Documentation.

Thank you