Quantum Preparedness and Crypto Agility: Cyber Risks and Opportunities

Natalia Bakhtina, MBA, CRISC

For Canada IT & Security Leaders Forum 2024

Banff, Alberta

Agenda

- Quantum vs. Digital
- Event Scenarios
- Quantum Development Trajectory
- Y2Q: Years to Quantum
- Quantum: Risk & Opportunities
- Possible Use Cases
- Key Considerations
- Transition to Quantum Urgency
- Quantum Preparedness Action Plan
- Crypto Agility Best Practices
- Key Takeaways

Quantum Computing vs. Digital Computing

QUANTUM

- New approach in computing
- Quantum physics principles
- Quantum bits = qubits
- Qubit can store zeros AND ones
- Any combination of both zero and one SIMULTANEOUSLY = superposition
- Solving VERY complex problems
- Significant number of paths simultaneously

DIGITAL

- Classical approach to computing
- Built on bits
- Bit = unit of information that can store EITHER a zero OR a one
- Solving problems with multiple variables
- A new calculation every time a variable changes
- Each calculation is a single path to a single result

Quantum Computing: Stark Performance Difference

2019 announcement by Google re solving a complex problem

QUANTUM

200 seconds

DIGITAL

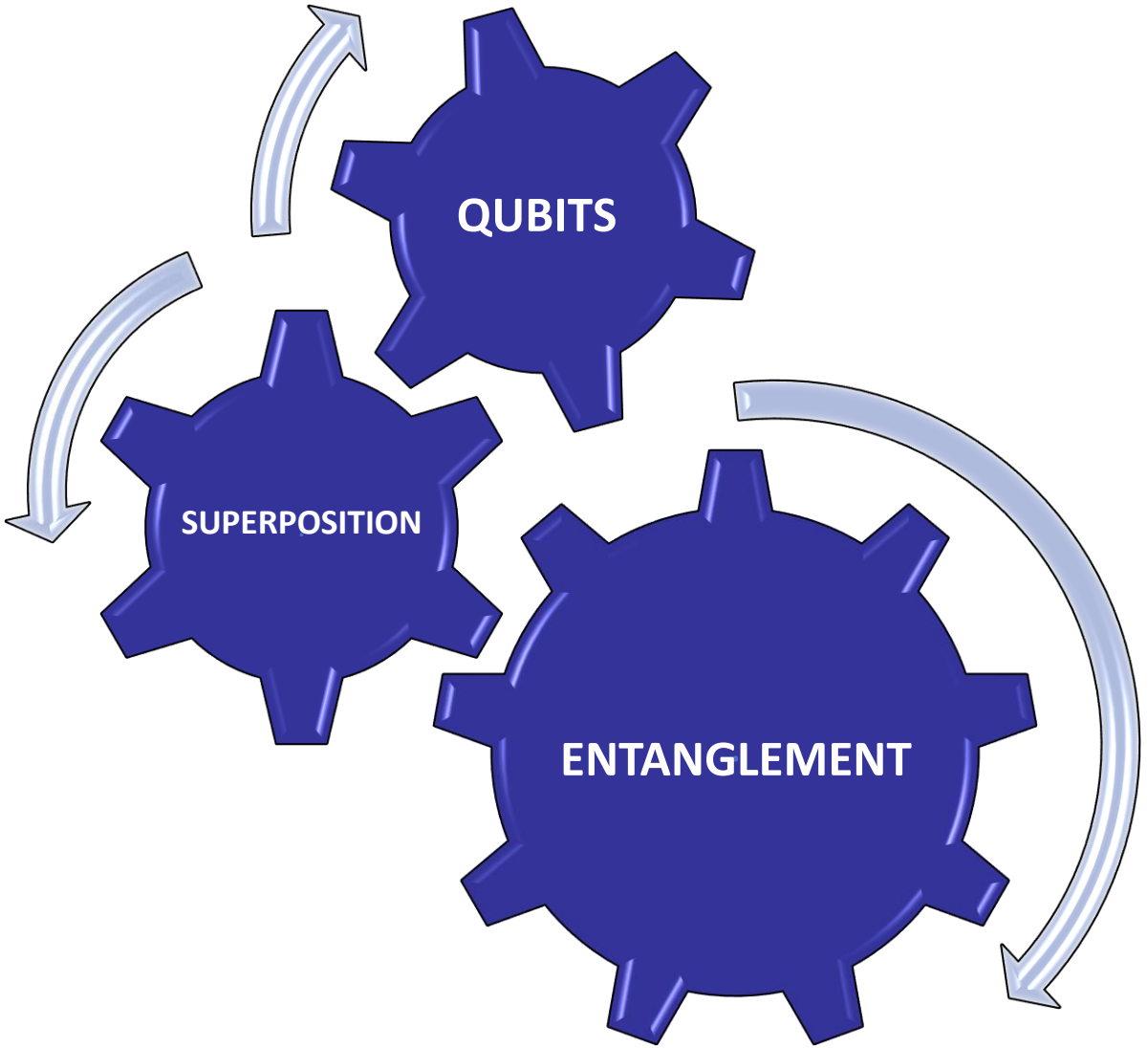
10,000 years

OR

315,569,529,000 seconds

Quantum Computing: Possible Scenarios

Quantum Computing: Key Concepts Accelerating Timeline



QUBITS

Quantum information encoded by qubits for quantum computers to process

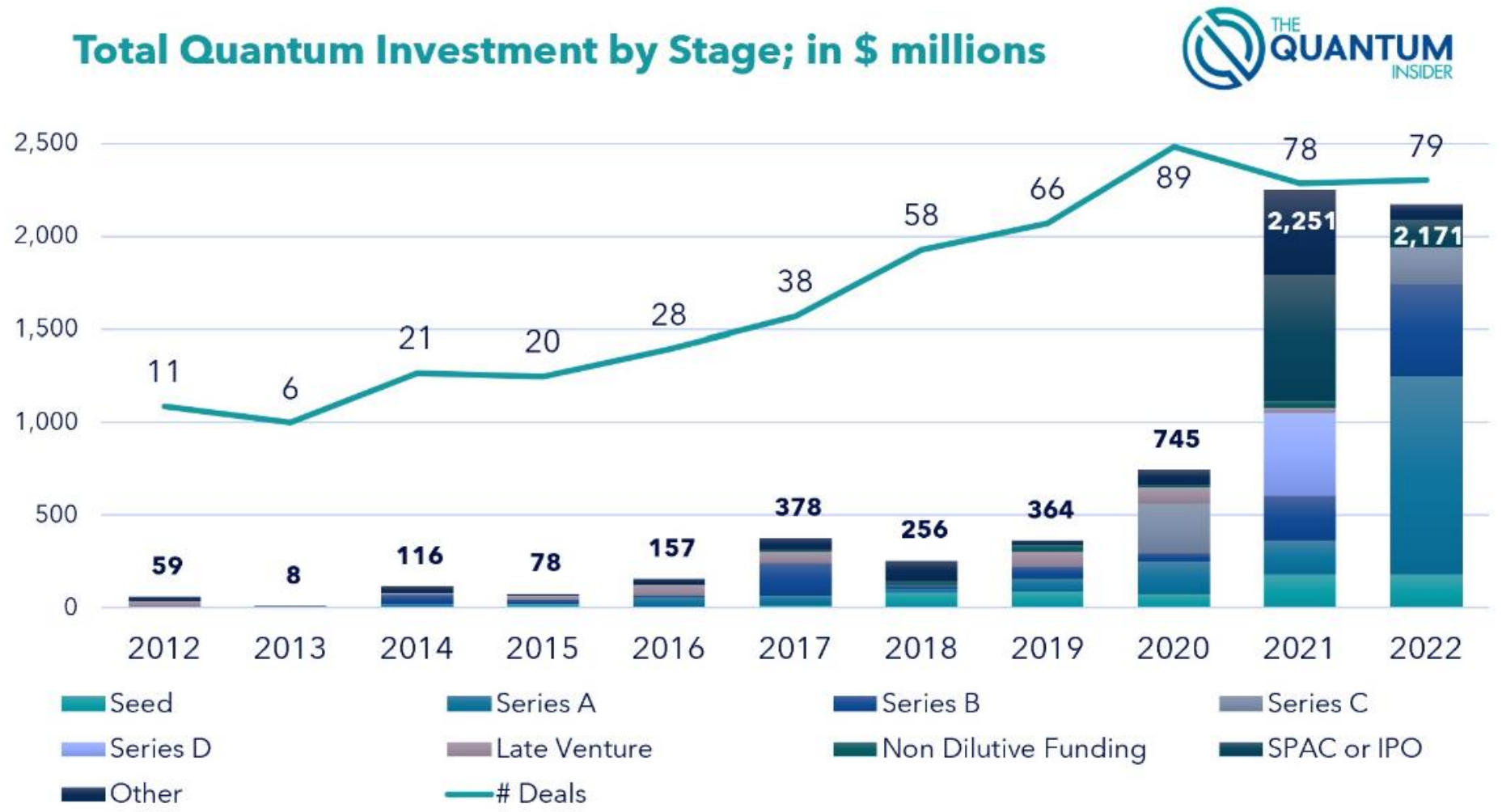
SUPERPOSITION

As qubits are combined, representation of complex problems becomes easier than classical digital computing methods

ENTANGLEMENT

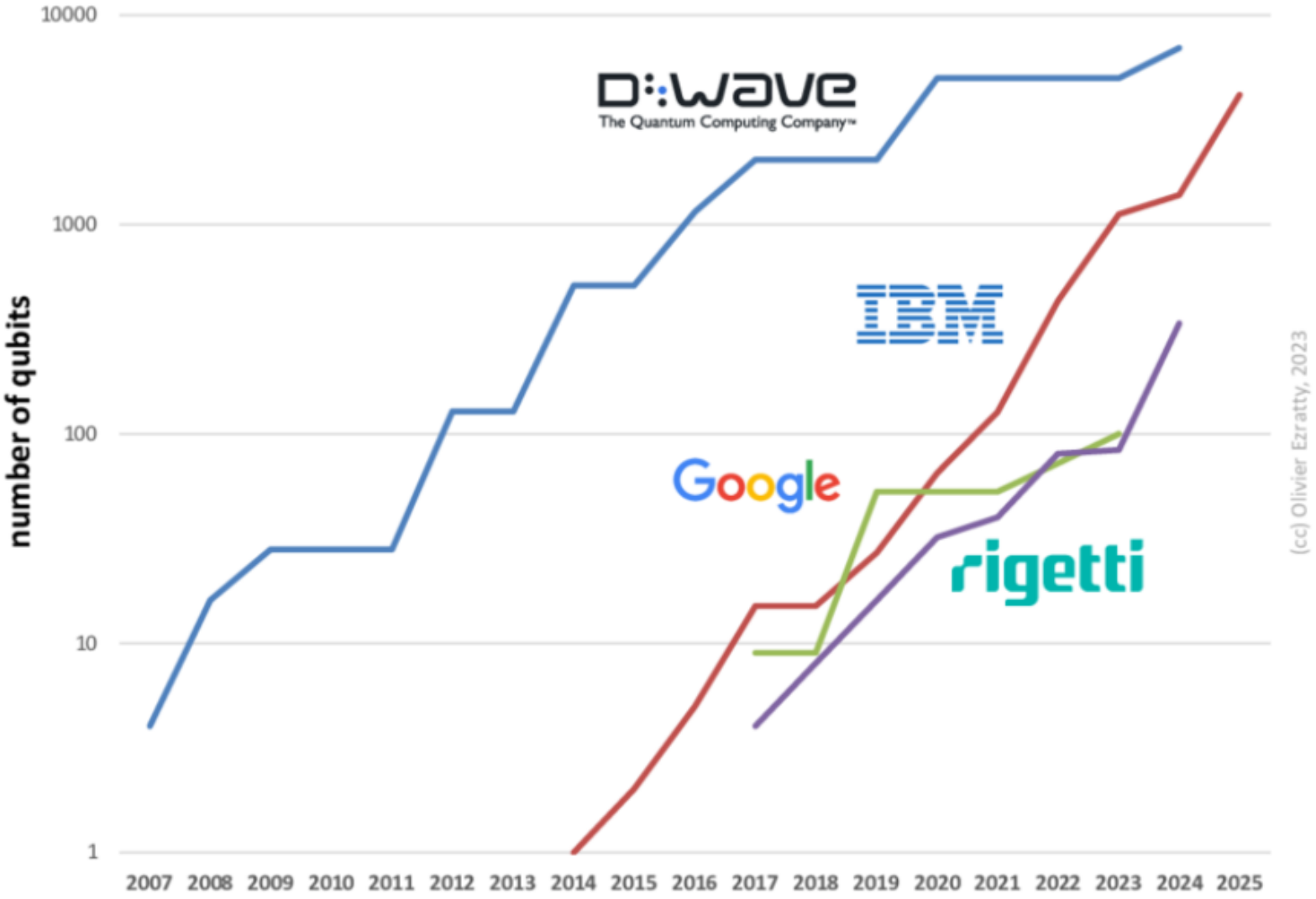
By creating correlation between two qubits, entanglement solves complex problems quicker than supercomputers

Quantum Computing: Significant Investment Growth Recently



Source: The Quantum Insider Intelligence Platform

Quantum Computing: Remarkable Growth of Achieved Qubits



Quantum Computing: Clear Trajectory

Quantum Computing: Y2Q Timeline TBD

~15 years

- 2,048 RSA bit encryption key length - 2016 NIST recommendation
- 8 hrs to factoring 2,048 bit RSA integers using only 20 million physical qubits
- Plans to build quantum computer with 1 million physical qubits by 2030
- Recently discovered topological quantum - more stable and more scalable

Quantum Computing: Risks & Opportunities

$$$

Difficult to build & require unique components, expensive tech and massive cooling

SPEED

Quantum computers are so fast that classical digital computers can never match

POTENTIAL ERRORS

Depending on the nature of qubits and quantum mechanics, errors are possible

SOLUTION POTENTIAL

No matter how complex the problem is, quantum computing allows

TARGETED TASKS

Quantum computers have the potential to find revolutionary solutions, but only in specific areas and for specific tasks

SOLUTION COMPLEXITY

Given the complexity and speed that quantum computing can achieve, quantum computers can run complex simulations

Quantum Computing: Potential Use Cases

ENCRYPTION

DATA ANALYTICS

PATTERN MATCHING

DECISION OPTIMIZATION

FORECASTING & PREDICTIONS

CYBERSECURITY

RESEARCH & DEVELOPMENT

AVIATION & AEROSPACE

AUTOMOTIVE

CYBER THREATS

Quantum Computing: Key Considerations to Crypto Agility

- Encrypted data stolen
- May still be unencrypted for now
- Quantum computing decryption is a matter of time

LOOMING THREAT

- Quantum-secure takes time: multi-step journey
- Data
- Tooling
- Infrastructure
- Policies
- Training

PREPARATION JOURNEY

- Canada: Guidance on becoming cryptographically agile - ITSAP.40.018 (05'22), Preparing your organization for the quantum threat to cryptography - ITSAP.00.017 (02'21)
- US: the Quantum Computing Cybersecurity Preparedness Act is Law H.R. 7535 (12.22.2022)
- Encouragement to adopt technology protecting against quantum computing attacks

QUANTUM LAW

Transition to Quantum: Urgency Drivers

2032 - fundamental cryptography disruption

- **10-15 year-life span data at risk**: 'harvest now, decrypt later' exfiltration / breaches on the rise
- Healthcare, financial services, government - most targeted sectors & at highest risk
- **Fraudulent** updates, authentication, decryption, alteration, extortion, counterfeiting **attacks**
- NIST-selected **CRYSTALS-Kyber vulnerabilities**

Transition to Quantum - holistic approach and significant investment required

- Quantum-vulnerable encryption risk & threat assessment, strategy, C-BoM, data / systems management, algorithms interoperability
- Greater **regulatory scrutiny** and standardization requirements in development
- **Solution to complexity** requires significant time & efforts

High risk and anticipation, yet … low activity

- **2030 Quantum to become mainstream**: 62% organization in Canada and 78% in the US
- **Quantum disruption** and decryption of today's data only a **matter of time**: 60% in Canada and 73% in the US
- **Need better quantum preparedness** and data resilience: 62% in Canada and 81% in the US
- 95% - Quantum relevance to and **impact to data security is assessed as 'High'**
- 65% - own **data at risk** 'High' or 'Very High'
- 25% - quantum resilience currently addressed in the risk management strategy

Quantum Computing: Crypto Agility Journey Components

Central 'Organization': governance, tools, guidance

Crypto Policies: enterprise-wide awareness & requirements

Shared Responsibility: collaboration & delegation

Procurement Policy: crypto agility go forward

New IT Change Management Policies:

- Ongoing inventory maintenance,
- Configuration change management

New Frameworks:

- Incident response
- Software layer for APIs
- Application development
- Secure update mechanisms

Inventory: products that use cryptography and C-BoM

Transition Plan: non-agile products / legacy cryptography to upgrade to crypto agile products

Recommended Standardized Crypto Algorithms: ITSP.40.111 and ITSP.40.062

Crypto Algorithms Validation under Cryptographic Module Validation Program

Crypto Products **Vendor / 3rd Party Review**:

- Support for crypto agility
- Software / firmware upgrade policies
- Required crypto agility updates

Quantum Computing: Crypto Agility Best Practices

CENTRALIZED VISIBILITY
Cryptography products, algorithms, roles: where, what, how and who. 'Shadow' cryptography in scope

OWNERSHIP
Appropriate teams / groups and suitable duties

ACTIVE RESPONSIBILITY
Awareness. Agreement. Operationalization.

COMPLIANCE
Defined accountability. Industry practices. Legislative guidance. Corporate standards.

DATA GOVERNANCE
Comprehensive current meta data. Clear scope: sensitive, confidential, business, personal, etc.

SUPPLIERS
Contracts. Provisions. Disclosures. Roadmaps. SLA's. Standards. Audits.

RESOURCING
Sufficient & knowledgeable. Crypto experience. Training.
IT risk management leverage, cyber governance & assurance

VULNERABILITIES
Full lifecycle management and proper SLA's

THE LATEST
Crypto techniques, algorithms, technology. High bits sizes.

HARDWARE
Updates, upgrades and patches
OR switch

MONITORING & REPORTING
Products and roles. Crypto libraries, keys, key mgmt. systems.
Ongoing ownership tracking. Maintenance. Reporting.

AUTOMATION
Where suitable: management and replacement tracking

Quantum Computing: Key Takeaways for Quantum-Proof

- **QUANTUM: WHEN, NOT IF**
- **PREPARATION IS KEY**
- **NEED TIME**
- **PARTNERSHIP IS SUCCESS**

Questions?

Natalia Bakhtina, MBA, CRISC

LinkedIn