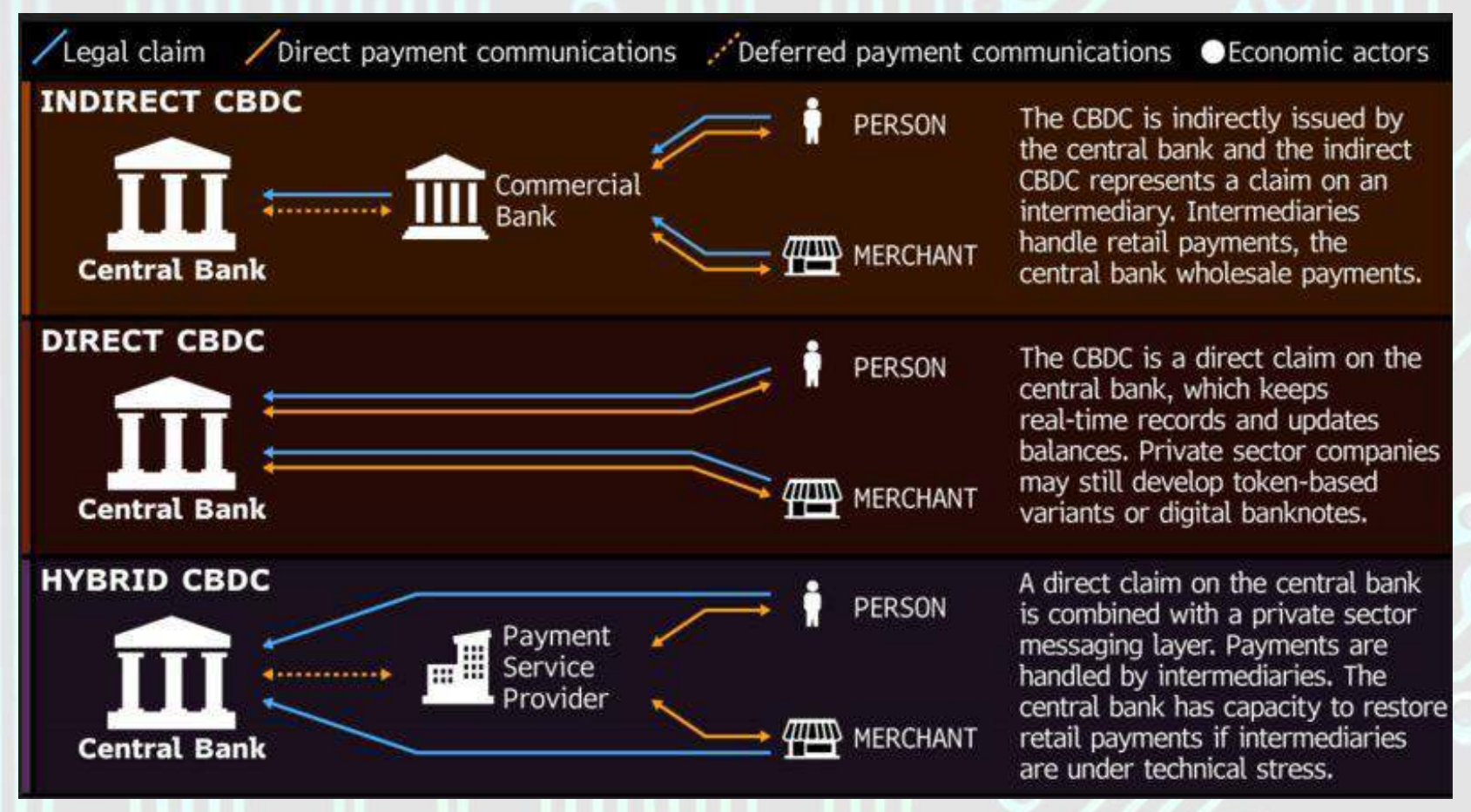
Central-Bank-Digital-Currency Blockchains; US Economic Influence Threatened – Requires Quantum Network Development & Deployment

Background

Central Bank Digital Currency (CBDC) systems use blockchain technology to secure financial transactions. CBDC bypasses the SWIFT system, which is influenced by worldwide US Dollar (USD) usage, thereby **undermining US soft-power controls**. Digitally secured Information and Communications Infrastructures (ICI) encryption, transmission and reception architectures will soon be vulnerable to quantum penetration.

What is Blockchain? Blockchain is a digital transaction ledger that stores records as blocks across computers in a P2P (peer-to-peer) network.[9]

What are Quantum Networks? Modular quantum computers linked together using qubits to transmit information via fiber-optic or free-space networks using switches and repeaters.



The CBDC is indirectly issued by the central bank and the indirect CBDC represents a claim on an intermediary. Intermediaries handle retail payments, the central bank wholesale payments.

The CBDC is a direct claim on the central bank, which keeps real-time records and updates balances. Private sector companies may still develop token-based variants or digital banknotes.

A direct claim on the central bank is combined with a private sector messaging layer. Payments are handled by intermediaries. The central bank has capacity to restore retail payments if intermediaries are under technical stress.

Fig. 2: CBDC Distribution Structures[2]

Significance

CBDC Threat: Digital currencies will diminish value of USD as "the" global currency, **reducing diplomatic bargaining power.**

Centralized CBDC security challenges

- Diminished anonymity and immutability
- Market manipulation

Decentralized CBDC security challenges

- Anonymity and nonregulatory oversight

Quantum Potential: Classical binary bits have two states: |0⟩ or |1⟩ to program information; quantum computing uses qubits which can be |0⟩, |1⟩, or *both*. This duality **increases the processing power** of a machine to perform faster, more complex operations and break classical encryption algorithms.

****Quantum Computing Disqualifies Blockchain Immutability****

QUESTION: How to secure future US power in a quantum era?

Opportunity Analysis

Leverage public-private partnerships to:

- Modernize and reinforce SWIFT capabilities
- **Develop and deploy a Quantum Internet (QI)**
  - Realize Quantum-Money[10], hybrid quantum-blockchains
  - Exploit CBDC and blockchains of corrupt entities

QI Development Challenges

Winning the near-peer state competition for "first-to-capture" Quantum Internet capabilities requires **prioritizing funding** to advance Technology Readiness Levels currently limited by:

- **Quantum teleportation and data retention optimization**
  - Topological materials for error-correction
- Rare Earth Resources -> supply chain surety

Imperfect Cloning: Post quantum (PQ) vulnerability threatening the security of quantum networks and quantum-blockchains

Horizon Threat

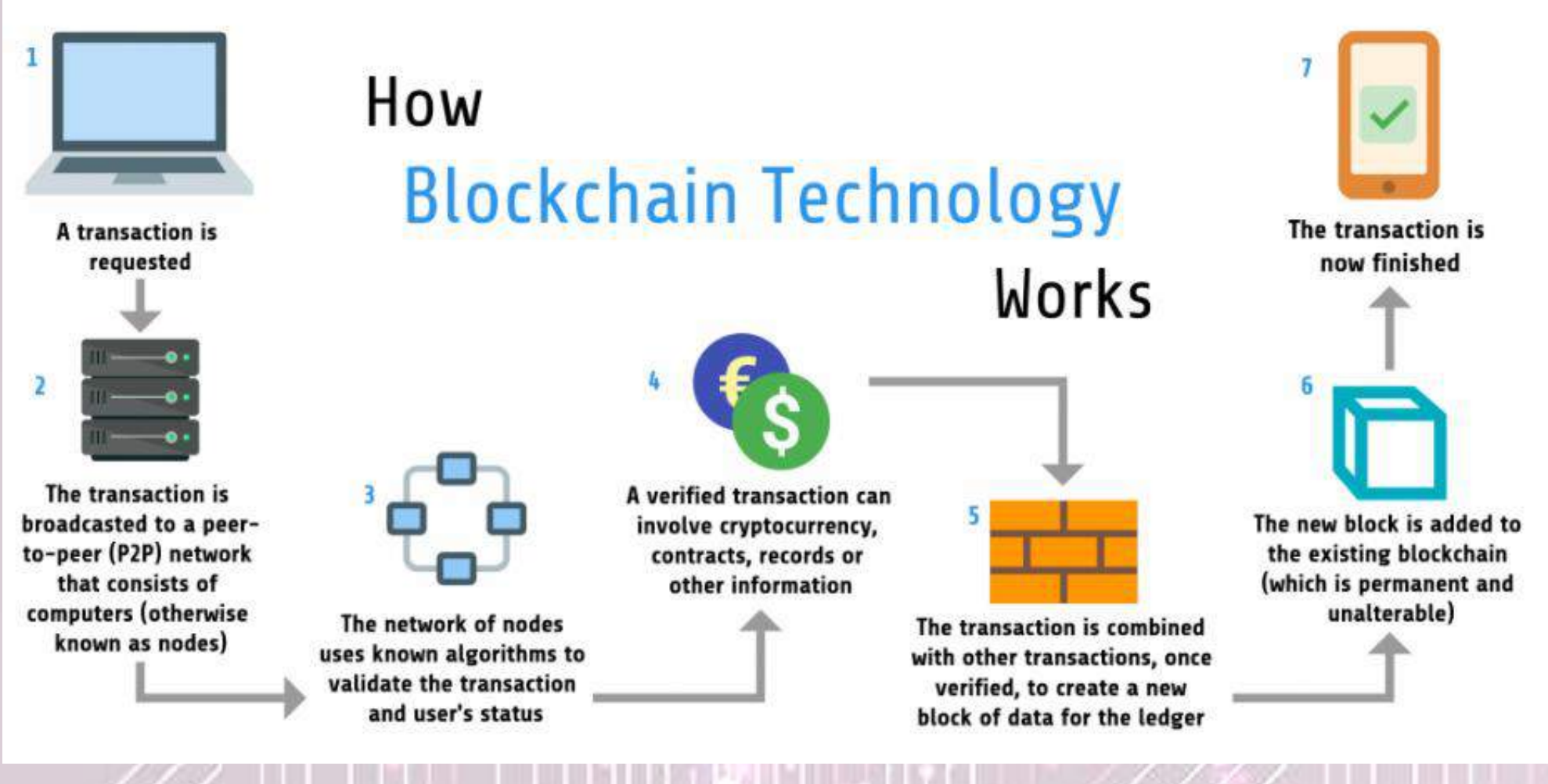
Quantum Supremacy will **Control** future data and financial **Security Strategies.**

Figure 1: Quantum qubit breaking blockchain encryption[1]

Research Methodology

Investigated quantum technology (QT) priorities, development status, and technology readiness levels using CBDC as a case-analysis for practical application implications. Considered post quantum (PQ) environments. Identified key QT actors for joint-resilience strategies. Utilized the following resources:

- Academic journal publications
- Subject Matter Expert (SME) interviews
- Open-source tools and news articles



1 A transaction is requested

2 The transaction is broadcasted to a peer-to-peer (P2P) network that consists of computers (otherwise known as nodes)

3 The network of nodes uses known algorithms to validate the transaction and user's status

4 A verified transaction can involve cryptocurrency, contracts, records or other information

5 The transaction is combined with other transactions, once verified, to create a new block of data for the ledger

6 The new block is added to the existing blockchain (which is permanent and unalterable)

7 The transaction is now finished

Fig. 3: Blockchain Architecture[3]

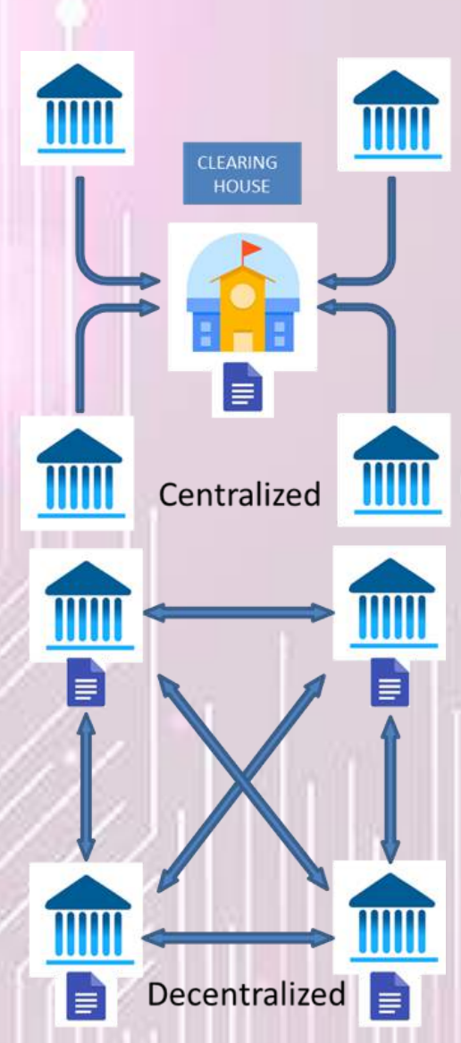


Fig. 4: Blockchain Ledger Distribution[4]

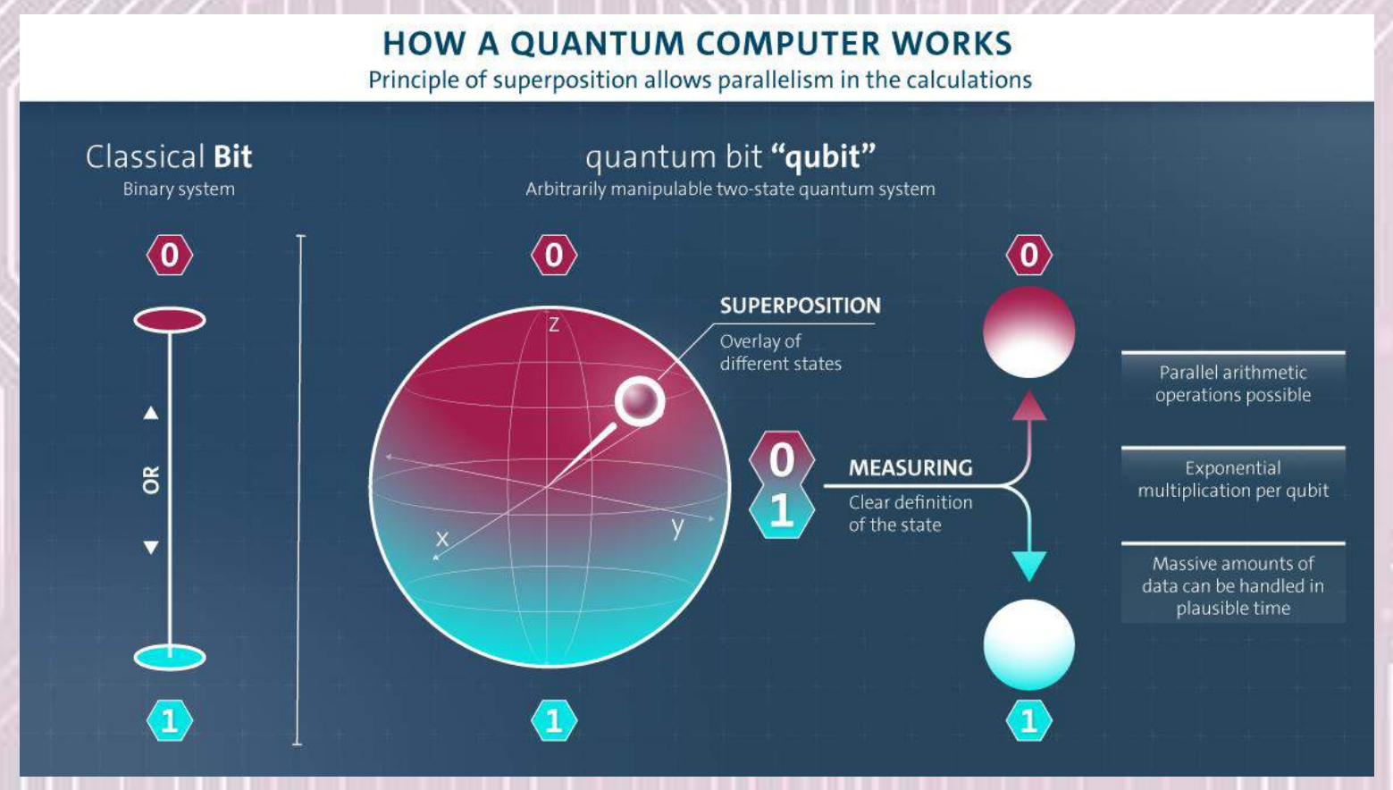
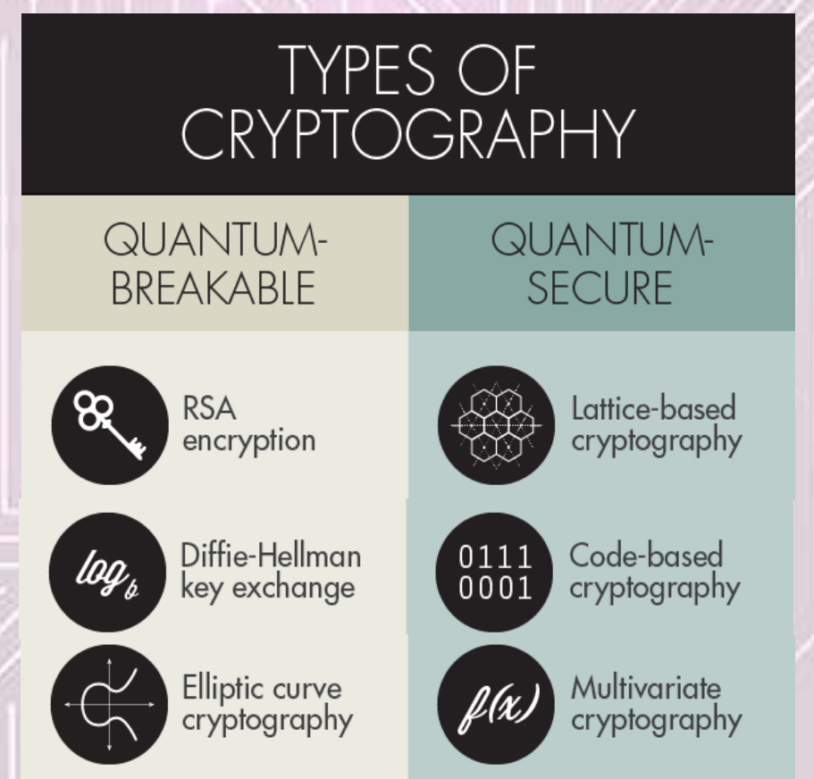

HOW A QUANTUM COMPUTER WORKS
Principle of superposition allows parallelism in the calculations
Classical Bit
Binary system
quantum bit "qubit"
Arbitrarily manipulable two-state quantum system
0
OR
1
Z
x
y
SUPERPOSITION
Overlay of different states
MEASURING
Clear definition of the state
Parallel arithmetic operations possible
Exponential multiplication per qubit
Massive amounts of data can be handled in plausible time

Fig. 5: Quantum Computing Qubits[5]


TYPES OF CRYPTOGRAPHY

QUANTUM-BREAKABLE	QUANTUM-SECURE
RSA encryption	Lattice-based cryptography
Diffie-Hellman key exchange	Code-based cryptography
Elliptic curve cryptography	Multivariate cryptography

Fig. 6: Cryptography Comparison[6]

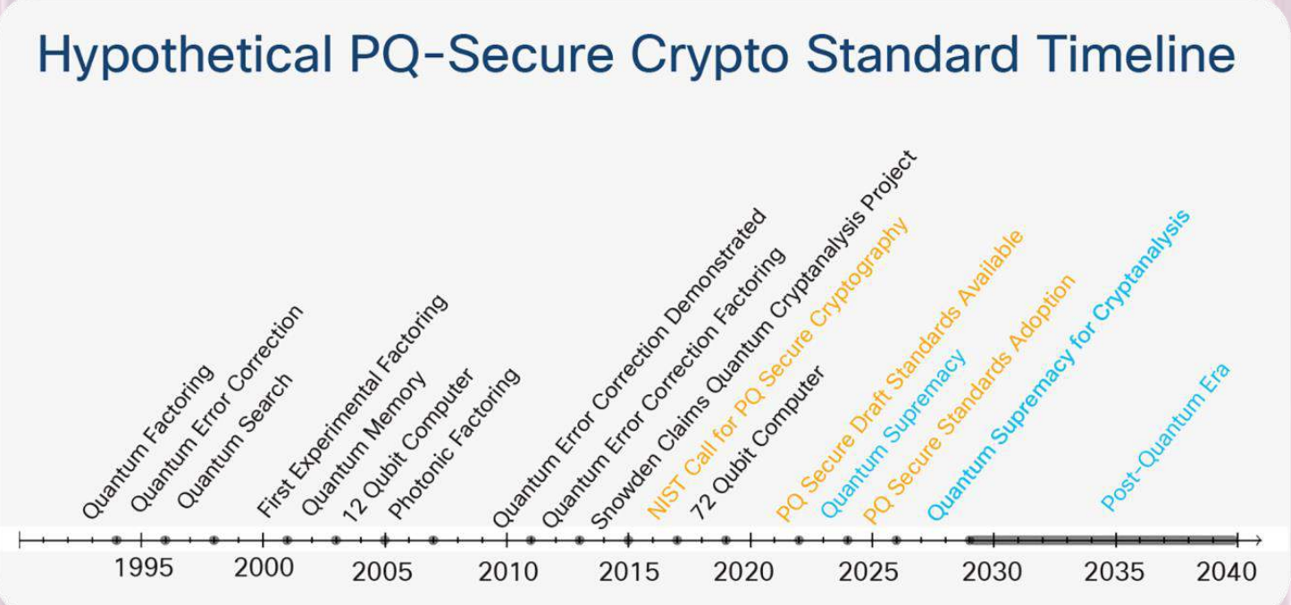


Fig. 7: Development Timeline for Post Quantum Era[7]

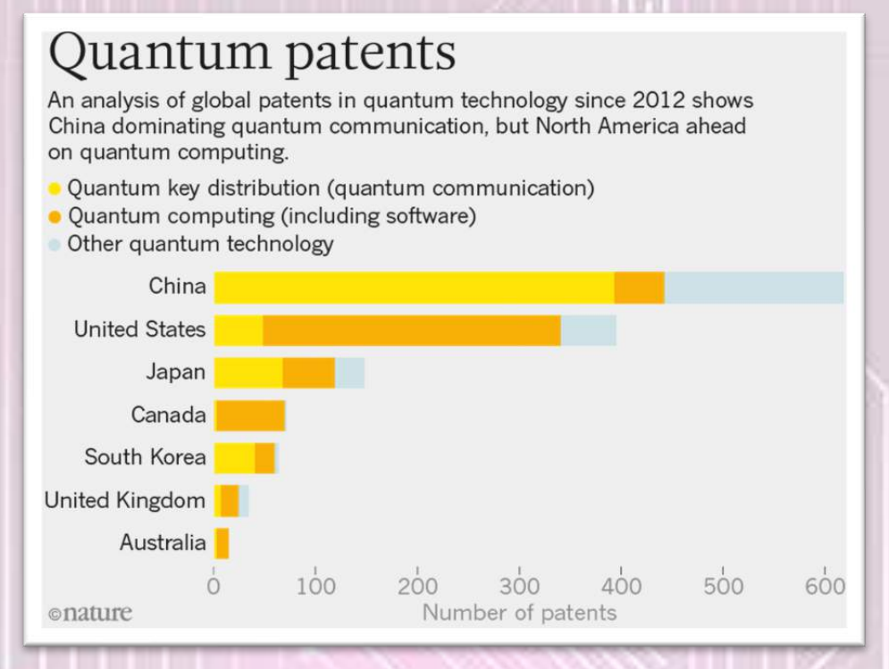


Fig. 8: Quantum Computing & Communication Patent Trends[8]

Resilience Strategies

1) Mobilize public-private consortiums and allied coalitions to:
   - Advance quantum technologies
   - **Standardize advanced encryption algorithms**
     - Research PQ hard problems
2) **Develop hybrid classical-quantum systems**
3) Establish international CBDC norms and requirements

Future Research

Investigate how Quantum Game Theory affects the intersection of quantum-driven Artificial Intelligence and state security strategies.

Acknowledgements

Research conducted under the advisement of Dr. Jeannie Johnson and Professor Briana Bowen.

Sources Link

Erika Mueller
Electrical Engineering
Utah State University
Center for Anticipatory Intelligence
erika.mueller@aggiemail.usu.edu