# Applications and Indian Trends in Quantum Computing and Quantum-AI

Vandna Chaturvedi

Center for Devlopment of Advance Computing(CDAC, Hyderabad)

November 10, 2025

# Outline

## This session

1. Moore's Law Saturation & Rise of Qubits
2. Problems Hard for GPUs

## Later topics

3. How Qubits Can Solve It
   - RSA Algorithm
   - Quantum Key Distribution
     - BB84 Protocol
4. Areas to Push Quantum AI Forward
   - Quantum Computing
   - Quantum Engineering and Hardware
   - Quantum Networks
   - Quantum AI and Industry 5.0
   - Education Policy and Outreach
   - Application and Domain Specialists
   - Quantum Sensing and

# Moore's Law: The Saturation Point

- **Moore's Law**: Transistor density doubles every 18-24 months
- **Current Status**: Physical limits being reached
  - Atomic-scale limitations (5nm, 3nm processes)
  - Quantum tunneling effects at nanoscale
  - Heat dissipation challenges
  - Power consumption issues
- **Classical Computing Bottlenecks**:
  - Sequential processing limitations
  - Exponential complexity problems
  - Scaling challenges for certain algorithms

# The Rise of Qubits: Timing and Evolution

**Quantum Computing Timeline**

- 1980s: Theoretical foundations
- 1990s: First algorithms (Shor, Grover)
- 2000s: Small-scale prototypes
- 2010s: Cloud quantum access
- 2020s: NISQ era
- 2030s: Fault-tolerant systems

**Qubit Evolution**

- 1998: 2 qubits
- 2016: 5-9 qubits
- 2019: 53 qubits (Google)
- 2023: 1000+ qubits
- Future: Millions of qubits

**Key Advantage**: Exponential scaling in computational space

# Problems That Challenge GPUs

- **Combinatorial Optimization**:
  - Traveling Salesman Problem (TSP)
  - Graph coloring problems
  - Boolean satisfiability (SAT)
  - Exponential search spaces
- **Cryptographic Problems**:
  - Integer factorization (RSA)
  - Discrete logarithm problems
  - Lattice-based cryptography
- **Quantum Simulation**:
  - Molecular dynamics
  - Quantum chemistry
  - Many-body quantum systems

# Why GPUs Struggle

**Architectural Limitations**

- Parallel but deterministic
- Sequential for complex dependencies
- Memory bandwidth constraints
- Limited by classical physics

**Complexity Barriers**

- Exponential time complexity
- Memory requirements scale poorly
- No quantum entanglement
- No quantum superposition advantage

**Example**: Factoring a 2048-bit RSA key

- Classical: Millions of years
- GPU: Still millions of years
- Quantum: Hours to days (with sufficient qubits)

# Quantum Advantage: Key Mechanisms

- **Superposition**: Evaluate multiple states simultaneously
- **Entanglement**: Correlated qubits enable parallel computation
- **Interference**: Amplify correct answers, cancel wrong ones
- **Quantum Parallelism**: Exponential speedup potential

**Key Applications**:

1. RSA Algorithm (Cryptography)
2. Quantum Key Distribution (Secure Communication)
    - BB84 Protocol

# RSA Algorithm: The Challenge

- **RSA Security**: Based on integer factorization
- **Classical Approach**:
  - Best known algorithm: General Number Field Sieve (GNFS)
  - Time complexity: $O(e^{c(\log N)^{1/3}(\log \log N)^{2/3}})$
  - 2048-bit RSA: Practically secure against classical computers
- **Quantum Threat**: Shor's Algorithm
  - Time complexity: $O((\log N)^3)$
  - Polynomial time factorization
  - Threatens current RSA encryption

# Shor's Algorithm: Quantum Solution

**How Shor's Algorithm Works**

1. Quantum Fourier Transform
2. Period finding subroutine
3. Factorization via period
4. Polynomial time solution

**Impact**

- Breaks RSA with sufficient qubits
- Requires ∼4000 logical qubits
- Currently: NISQ limitations
- Future: Post-quantum cryptography needed

**Status**:

- Theoretical: Proven
- Practical: Awaiting fault-tolerant quantum computers

# Quantum Key Distribution (QKD)

- **Purpose**: Secure key exchange using quantum mechanics
- **Principle**: Heisenberg Uncertainty Principle
  - Measurement disturbs quantum state
  - Eavesdropping is detectable
  - Information-theoretic security
- **Advantages over Classical**:
  - Security based on physics, not computational difficulty
  - Detects interception
  - Future-proof against quantum computers

# BB84 Protocol: Quantum Key Distribution

- **Invented**: 1984 by Bennett and Brassard
- **Key Components**:
  1. **Qubit Preparation**: Alice sends qubits in random bases
     - Basis 1: $\{|0\rangle, |1\rangle\}$ (Z-basis)
     - Basis 2: $\{|+\rangle, |-\rangle\}$ (X-basis)
  2. **Qubit Measurement**: Bob measures in random bases
  3. **Key Sifting**: Public discussion of bases
  4. **Error Estimation**: Check for eavesdropping
  5. **Privacy Amplification**: Final secure key

# BB84 Protocol: Security Features

**Security Guarantees**

- Information-theoretic security
- Eavesdropping detection
- No computational assumptions
- Secure against future quantum computers

**Implementation**

- Photon polarization
- Phase encoding
- Fiber optic networks
- Satellite-based QKD
- Commercial systems available

**Current Status**:

- Commercial QKD systems deployed
- Used in banking, government
- Research in long-distance QKD
- Integration with quantum networks

# Strategic Areas for Advancement

- **4.1** Quantum Computing
- **4.2** Quantum Engineering and Hardware
- **4.3** Quantum Networks
- **4.4** Quantum AI and Industry 5.0
- **4.5** Education Policy and Outreach
- **4.6** Application and Domain Specialists
- **4.7** Quantum Sensing and Metrology
- **4.8** Quantum Cryptography

# 4.1: Quantum Computing

- **Algorithm Development**:
  - New quantum algorithms for AI/ML
  - Hybrid quantum-classical algorithms
  - Optimization for NISQ devices
- **Software Development**:
  - Quantum programming languages (Q#, Qiskit, Cirq)
  - Quantum compilers and optimizers
  - Quantum simulators
- **Error Correction**:
  - Quantum error correction codes
  - Fault-tolerant quantum computing
  - Noise mitigation techniques
- **Benchmarking**:
  - Quantum advantage demonstration
  - Performance metrics
  - Application-specific benchmarks

# 4.2: Quantum Engineering and Hardware

**Hardware Platforms**

- Superconducting qubits
- Trapped ions
- Photonic qubits
- Topological qubits
- Neutral atoms

**Engineering Challenges**

- Qubit coherence time
- Gate fidelity
- Scalability
- Cryogenic systems
- Control electronics

**Research Priorities**:

- Increasing qubit count
- Improving error rates
- Reducing form factor
- Lowering costs
- Integration with classical systems

# 4.3: Quantum Networks

- **Quantum Internet Vision**:
  - Long-distance quantum communication
  - Quantum repeaters
  - Quantum memory
  - Distributed quantum computing
- **Key Technologies**:
  - Quantum repeaters for distance
  - Quantum memory for storage
  - Entanglement distribution
  - Quantum teleportation
- **Applications**:
  - Secure quantum communication
  - Distributed quantum sensing
  - Cloud quantum computing
  - Quantum blockchain
- **Challenges**:
  - Loss in optical fibers
  - Decoherence
  - Scaling to long distances

# 4.4: Quantum AI and Industry 5.0

- **Industry 5.0 Context**:
  - Human-AI collaboration
  - Sustainable and resilient systems
  - Personalized production
  - Quantum-enhanced automation
- **Quantum AI Applications**:
  - Quantum machine learning
  - Quantum neural networks
  - Quantum optimization for logistics
  - Quantum-enhanced pattern recognition
  - Drug discovery and design
  - Financial modeling
- **Integration Challenges**:
  - Hybrid quantum-classical workflows
  - Data encoding and decoding
  - Real-time quantum processing
  - Industry-specific solutions

# 4.5: Education Policy and Outreach

**Academic Programs**

- Quantum computing courses
- Master's and PhD programs
- Online certification programs
- Industry-academia partnerships

**Outreach Activities**

- Public awareness campaigns
- Student competitions
- Workshops and seminars
- Quantum computing labs in schools

**Policy Initiatives**:

- National quantum education framework
- Curriculum development
- Teacher training programs
- Scholarship programs
- Research grants for students
- Industry internship programs

# 4.6: Application and Domain Specialists

- **Need for Specialists**:
  - Bridge quantum theory and practical applications
  - Domain-specific quantum solutions
  - Industry-specific expertise
- **Key Domains**:
  - **Healthcare**: Medical imaging, drug discovery, personalized medicine
  - **Finance**: Risk analysis, portfolio optimization, fraud detection
  - **Logistics**: Supply chain optimization, route planning
  - **Agriculture**: Crop optimization, weather prediction
  - **Energy**: Grid optimization, battery design
  - **Cybersecurity**: Threat detection, secure communications
- **Training Requirements**:
  - Quantum computing fundamentals
  - Domain expertise
  - Problem-solving skills
  - Interdisciplinary collaboration

# 4.7: Quantum Sensing and Metrology

- **Quantum Sensors**:
  - Atomic clocks (GPS, navigation)
  - Magnetometers (medical imaging, geology)
  - Gravimeters (geology, navigation)
  - Gyroscopes (navigation systems)
- **Applications**:
  - Precision measurements
  - Medical diagnostics (MRI, brain imaging)
  - Geological surveys
  - Defense and security
  - Fundamental physics research
- **Advantages**:
  - Higher sensitivity than classical sensors
  - Better resolution
  - Lower power consumption
  - Compact form factors
- **Market Potential**: Multi-billion dollar market

# 4.8: Quantum Cryptography

**Quantum Cryptographic Techniques**

- Quantum Key Distribution (QKD)
- Quantum Digital Signatures
- Quantum Random Number Generation
- Post-Quantum Cryptography
- Quantum Secure Direct Communication

**Research Areas**

- Long-distance QKD
- Device-independent QKD
- Continuous variable QKD
- Quantum-resistant algorithms
- Integration with existing systems

**Commercial Status**:

- Commercial QKD systems available
- Deployed in banking and government
- Standardization efforts (ETSI, ITU-T)
- Growing market for quantum-safe security

# National Quantum Mission (NQM)

- **Launched**: Government of India initiative
- **Budget**: Significant investment in quantum technologies
- **Duration**: Multi-year mission
- **Objectives**:
  - Develop quantum computers
  - Establish quantum communication networks
  - Build quantum sensing capabilities
  - Foster quantum research and development
  - Create quantum ecosystem in India

# 5.1: Vision of National Quantum Mission

- **Strategic Vision**:
  - Make India a global leader in quantum technologies
  - Develop indigenous quantum capabilities
  - Create quantum-ready workforce
  - Establish quantum infrastructure
- **Key Pillars**:
  1. Quantum Computing and Algorithms
  2. Quantum Communication and Security
  3. Quantum Sensing and Metrology
  4. Quantum Materials and Devices
- **Expected Outcomes**:
  - Quantum computers with 50-1000 qubits
  - Quantum communication networks
  - Quantum sensors for various applications
  - Quantum-ready workforce
  - Thriving quantum startup ecosystem

**Institutional Leaders**

- **IISc Bangalore**: Quantum algorithms, quantum-AI
- **IITs**: Multiple IITs with quantum research
- **TIFR**: Quantum information theory
- **RRI**: Quantum optics and computing
- **PRL**: Quantum technologies

**Industry Leaders**

- **TCS**: Quantum computing research
- **Infosys**: Quantum services
- **Wipro**: Quantum labs
- **Tech Mahindra**: Quantum communication
- **Startups**: Multiple quantum startups

**Key Researchers**: Leading Indian scientists in quantum computing and quantum-AI research

# 5.3: What's There for Society and Startups

- **For Society**:
  - Secure communication networks
  - Better healthcare through quantum sensors
  - Improved weather prediction
  - Enhanced cybersecurity
  - Job opportunities in quantum sector
  - Quantum literacy and awareness
- **For Startups**:
  - Funding opportunities through NQM
  - Access to quantum infrastructure
  - Collaboration with research institutions
  - Market opportunities in quantum applications
  - Support for quantum hardware development
  - Quantum software and services market
  - Incubation and acceleration programs

# Amaravati Quantum Valley Mission

- **Location**: Amaravati, Andhra Pradesh
- **Vision**: Create a world-class quantum technology hub
- **Objectives**:
  - Establish quantum research and development center
  - Build quantum computing infrastructure
  - Foster quantum startup ecosystem
  - Create quantum technology cluster
  - Attract global quantum companies
- **Components**:
  - Quantum research labs
  - Quantum computing facilities
  - Startup incubators
  - Training and education centers
  - Industry collaboration spaces

# Amaravati Quantum Valley: Vision

- **Global Hub**: Become a leading quantum technology center
- **Innovation Ecosystem**:
  - Research institutions
  - Industry partners
  - Startups and entrepreneurs
  - Investors and funding agencies
- **Key Focus Areas**:
  - Quantum computing and algorithms
  - Quantum communication and security
  - Quantum sensing and metrology
  - Quantum-AI applications
  - Quantum materials and devices
- **Expected Impact**:
  - Thousands of jobs in quantum sector
  - Multiple quantum startups
  - Breakthrough research and innovations
  - Global recognition as quantum hub

# Amaravati Quantum Valley: Timeline

- **Phase 1 (Years 1-2)**:
  - Infrastructure development
  - Research facility establishment
  - Initial partnerships
  - Talent acquisition
- **Phase 2 (Years 3-5)**:
  - Quantum computing systems operational
  - Startup ecosystem development
  - Research outputs and publications
  - Industry collaborations
- **Phase 3 (Years 6-10)**:
  - Full-scale operations
  - Commercial quantum applications
  - Global partnerships
  - Self-sustaining ecosystem
- **Milestones**:
  - Quantum research labs: Year 2
  - First quantum computer: Year 3-4
  - Startup incubator: Year 2

# Startup Opportunities in Quantum Technologies

**Quantum Software**

- Quantum algorithms
- Quantum simulators
- Quantum compilers
- Quantum-AI frameworks
- Quantum optimization tools

**Quantum Applications**:

- Drug discovery platforms
- Financial modeling tools
- Logistics optimization
- Cybersecurity solutions
- Quantum cloud services

**Quantum Hardware**

- Qubit controllers
- Cryogenic systems
- Quantum sensors
- Photonic devices
- Control electronics

# Specific Problem Areas for Startups

- **Quantum-AI Applications**:
  - Quantum machine learning platforms
  - Quantum-enhanced data analytics
  - Quantum neural network frameworks
  - Industry-specific quantum solutions
- **Quantum Communication**:
  - QKD systems and services
  - Quantum network infrastructure
  - Quantum secure communication apps
  - Quantum random number generators
- **Quantum Sensing**:
  - Medical imaging devices
  - Navigation systems
  - Geological survey tools
  - Precision measurement instruments
- **Quantum Education**:
  - Online quantum courses
  - Quantum simulation platforms
  - Quantum programming tools

# Market Opportunities for Startups

- **Emerging Markets**:
  - Quantum cloud computing: $850M by 2025
  - Quantum cryptography: $500M by 2025
  - Quantum sensing: $1.5B by 2025
  - Quantum-AI: Rapidly growing market
- **Support Mechanisms**:
  - Government funding through NQM
  - Incubation programs
  - Industry partnerships
  - Research collaborations
  - Access to quantum infrastructure
- **Success Factors**:
  - Clear value proposition
  - Domain expertise
  - Technical team
  - Market understanding
  - Strategic partnerships

# 8: Differentiation from CDAC QC_Toolkit.in and quinverse.in

**CDAC QC_Toolkit.in**

- Government initiative (CDAC)
- Focus: Quantum computing toolkit
- Target: Research and education
- Features:
  - Quantum simulators
  - Algorithm libraries
  - Educational resources

**quinverse.in**

- Private/platform
- Focus: Quantum computing services
- Target: Industry and research
- Features:
  - Quantum cloud access
  - Quantum algorithms
  - Consulting services

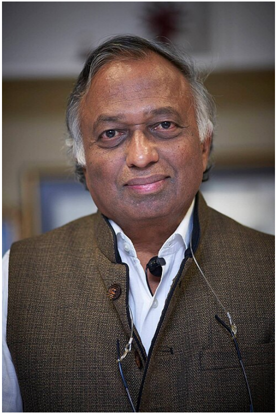
# Key Differentiators and Opportunities

- **Unique Value Propositions**:
  - **Domain-Specific Solutions**: Industry-focused quantum applications
  - **Quantum-AI Integration**: Specialized quantum-AI platforms
  - **Startup-Focused**: Tools and services for quantum startups
  - **Indian Market Focus**: Solutions for Indian use cases
  - **Hardware Access**: Direct access to quantum hardware
- **Competitive Advantages**:
  - Specialized algorithms for specific industries
  - Better user experience and interface
  - Lower cost solutions
  - Local support and services
  - Integration with Indian quantum infrastructure
- **Market Gaps**:
  - Industry-specific quantum solutions
  - Quantum-AI platforms
  - Startup-friendly tools
  - Educational platforms with hands-on access
  - Quantum consulting for Indian companies

# Strategic Positioning

- **Complementary Approach**:
  - Work alongside CDAC and quinverse
  - Fill specific market gaps
  - Provide specialized services
  - Target different customer segments
- **Key Differentiators**:
  1. **Industry Focus**: Solutions for specific industries (healthcare, finance, logistics)
  2. **Quantum-AI**: Specialized quantum-AI platforms and tools
  3. **Startup Ecosystem**: Tools and services for quantum startups
  4. **Indian Applications**: Solutions tailored for Indian market needs
  5. **Accessibility**: User-friendly interfaces and lower barriers to entry
  6. **Integration**: Seamless integration with existing systems
- **Success Strategy**:
  - Identify niche markets
  - Build domain expertise
  - Partner with industry leaders
  - Focus on user experience
  - Provide comprehensive support

# Thank You



"The 21st century belongs to India" - Vijay Bhatkar

# Conclusion

- Quantum computing represents a paradigm shift beyond Moore's Law limitations
- Qubits offer solutions to problems that challenge classical GPUs
- Multiple areas need advancement to push quantum-AI forward
- India's National Quantum Mission and Amaravati Quantum Valley provide strong foundation
- Significant opportunities exist for startups in quantum technologies
- Differentiation through specialization and domain expertise is key
- India is well-positioned to be a global leader in quantum technologies

# Thank You

Questions?

Contact: your.email@example.com