Effect of Quantum Computing on Blockchains

Quantum Blockchain

Scan this to download these slides

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130 USA
Jain@wustl.edu

A talk at Binghamton University, Binghamton, NY, October 5, 2023

These slides and audio/video recordings of this talk are at:
http://www.cse.wustl.edu/~jain/talks/qb_bu.htm

Overview

1. What is a Blockchain?
2. What is a Quantum and Quantum Bit?
3. Why can Quantum kill Blockchains?
4. How can we protect?
5. When will this all happen?

What is a Blockchain?

1. Satoshi Nakamoto invented Bitcoin
2. He used blockchains to make it decentralized
3. Since then, blockchains have found numerous other applications
4. Blockchains allow two strangers to enter
   Into a smart contract without a trusted third party.

Example of a Contract: Wedding

Example of a Contract: Wedding

- Centralized registry
- Single point of failure
- Easier to hack

- Decentralized
- No single point of failure

  ⇒ Fault Tolerant, No Monopoly
- Very difficult to hack

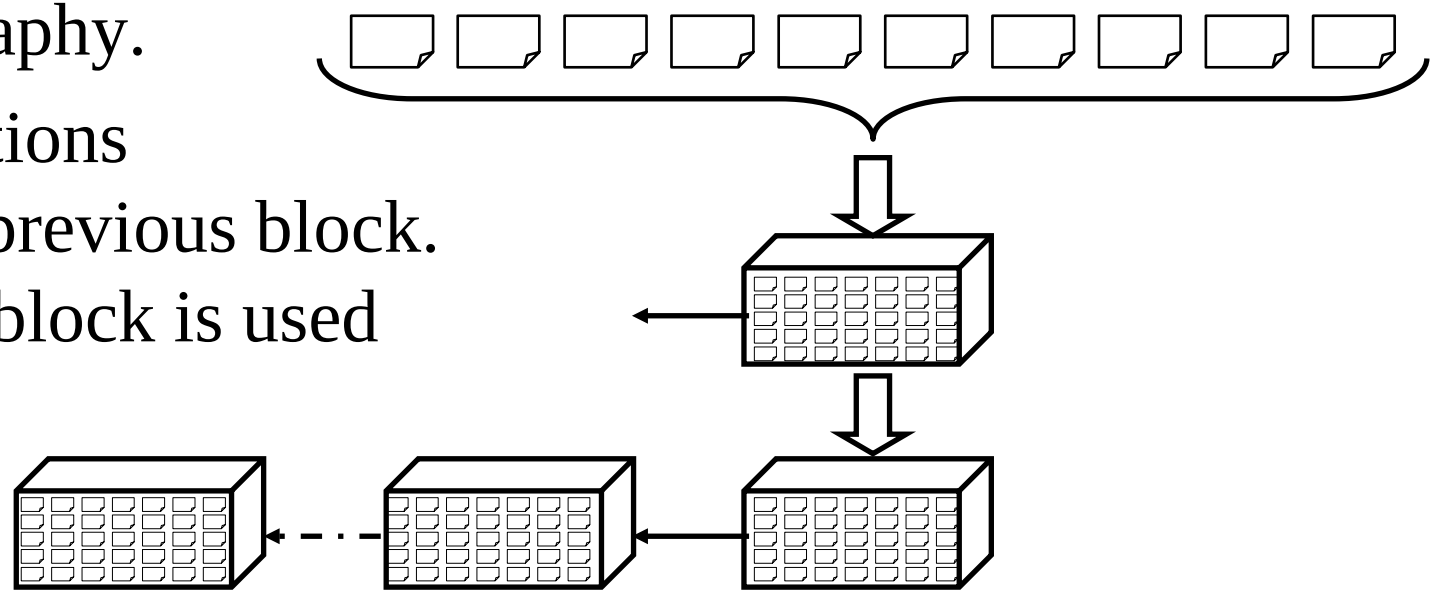
Examples of Centralized Systems

- **Banks**: Allow money transfer between two accounts
- **City Records**: Wedding registers, Property ownership
- **Networks**: Certificate Authorities, DNS

- In all cases:
  - There is a central third party to be trusted
  - The central party maintains a large database ⇒ Attracts Hackers
  - The central party may be hacked ⇒ Affects millions
  - The central party is a single point of failure.
    Can malfunction or be bribed

Blockchain Process

1. **Users** broadcast signed transactions or smart contracts.
   Sign using public key cryptography.
2. **Mining nodes** validate transactions and create blocks. Point to the previous block.
   SHA-256 hash of the previous block is used as a pointer.
3. **Blockchain nodes** validate blocks and construct a chain



- There are many users, many mining nodes, and many blockchain nodes.
  More nodes ⇒ Better. Less ⇒ Blockchain not required/useful.

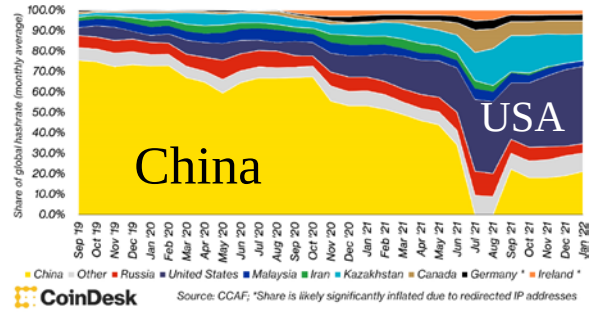
Key Strengths of Blockchains

1. **Distributed**: No single point of failure
2. **Decentralized Consensus**: Transactions are valid only if agreed by a majority
3. **Trustless**: Transacting or processing parties do not need to trust each other
4. **Cryptographic Security**: Elliptic Curve Cryptography
5. **Non-Repudiation Guarantee**: All transactions are signed

Key Weaknesses of Blockchains

1. **Distributed**: Everyone sees every transaction from a given address
   ⇒ reduced privacy.
2. **Decentralized Consensus**: If several mining pools allow a fraudulent block, the block becomes valid ⇒ 51% attack.
3. **Trustless**: No one is responsible ⇒ No one to complain to.
4. **Cryptographic Security**: Based on public-key cryptography.
   a. Stealing private key ⇒ ID theft.
      Over $2B have been stolen from crypto exchanges in 2022 [CNBC]
   b. SHA-256 hash is used in the Merkle Tree inside the blocks
   c. SHA-256 hash is used as pointers between blocks
   d. Uses inverting SHA-256 hash in the Proof-of-Work puzzle to determine the winner of the new coins and transaction fees.
5. **Non-Repudiation Guarantee**: Signatures based on public-key cryptography.

Bitcoin Mining Share



How Quantum Threatens Blockchains?

1. Easy to factorize large numbers

- Easy to find the private key given the public key
- Anyone with your private key can sign your contracts ⇒ ID theft
- They can empty your wallet by giving away your cryptocurrencies

2. Easy to invert one-way hash functions

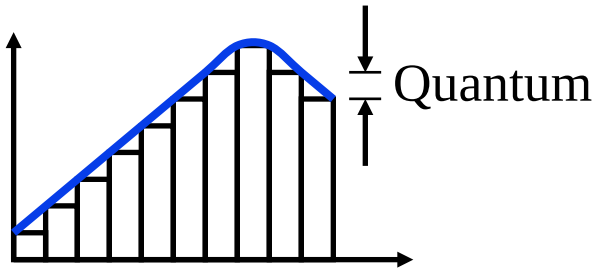
Proof-of-Work uses a puzzle to find the number that hashes below a threshold ⇒ Trivial to win Proof-of-Work puzzles

3. Easily find hash collisions: Two numbers with the same hash

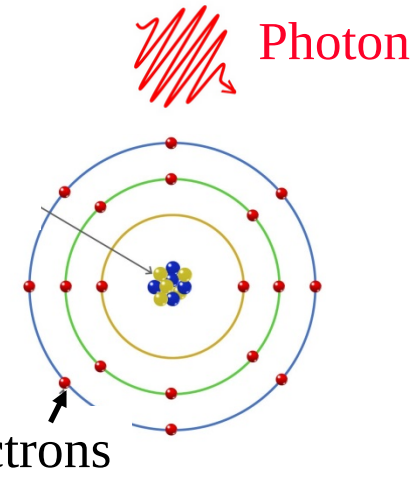
- Hash is used in Merkle tree ⇒ Can change a transaction with no change in hash
- Hash of a block is used as a pointer by the next block
  ⇒ Can change a block such that the hash does not change.

What is a Quantum?

- Quantization: Analog to digital conversion
  - **Quantum** = Smallest discrete unit



- **Wave Theory**: Light is a continuous wave. It has a frequency, phase, amplitude
- **Quantum Mechanics**: Light behaves like discrete packets of energy that can be absorbed and released
- **Photon** = One quantum of light energy
- Photons can move an electron from one energy level to the next higher level
- Photons are released when an electron moves from one level to a lower energy level



Quantum Bits

1. Computing bit is a binary scalar: 0 or 1
2. Quantum bit (Qubit) is a 2×1 vector of complex numbers,

$$\begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} = \frac{3}{5}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{4}{5}\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Dirac Notation $\quad |0> \quad |1>$

3. When a qubit is measured, the result is discrete (0 or 1) and probabilistic
   The probability of each vector element is proportional to its modulus square

$$\begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} \quad \begin{matrix} 9/25 \\ 16/25 \end{matrix} \quad \begin{matrix} 36\% \longleftarrow \text{Probability of being measured as 0} \\ 64\% \longleftarrow \text{Probability of being measured as 1} \end{matrix}$$

4. Qubit measurement can result in any of its two values. This is called superposition.
5. *n*-qubit are vectors of 2^n elements and can be written as expressions with 2^n coefficients

$$\begin{bmatrix} 4/5 \\ 1/5 \\ 2/5 \\ 2/5 \end{bmatrix} = \frac{4}{5}|00> + \frac{1}{5}|01> + \frac{2}{5}|10> + \frac{2}{5}|11>$$

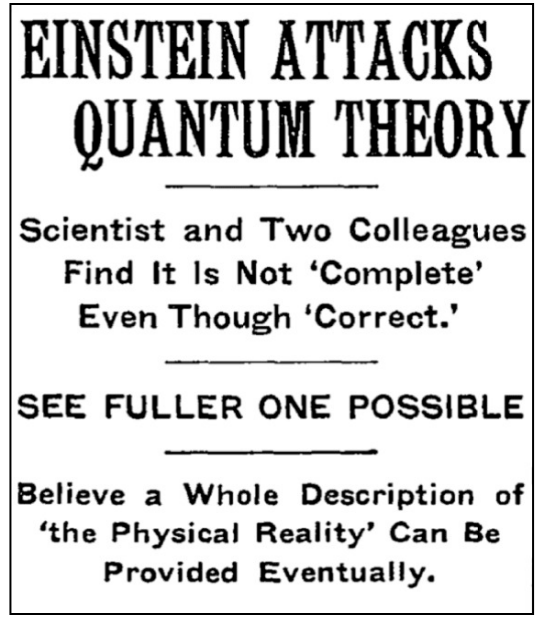
Special Case:

$$\begin{bmatrix} 4/5 \\ 0 \\ 0 \\ 3/5 \end{bmatrix} = \frac{4}{5}|00> + \frac{0}{5}|01> + \frac{0}{5}|10> + \frac{3}{5}|11>$$

Entanglement

- Two qubits can be entangled ⇒ Their states are correlated
  - Momentum, spin, polarization, or position are correlated
  - Even when they are far apart
  - Any change of one qubit affects the other
    ⇒ Teleportation of state ⇒ Quantum Key Distribution
- 1935: Einstein called it a paradox since change happens at a speed faster than light
- 1967: Kocher developed an apparatus to produce entangled photons
- 1984: Quantum Key Distribution (QKD) protocols using entanglement
- 2022: Physics Nobel Prize for experiments with entangled photons

Both think the same



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

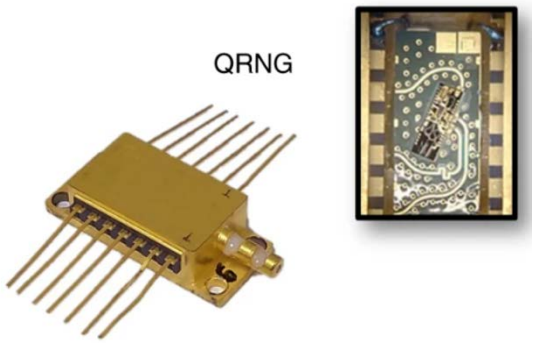
SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

May 4, 1935 Issue of the New York Times, Source: Wikipedia

Quantum Random Number Generator

- Cryptographic keys generated using pseudo-random number generators (PRNG) can be broken using the known information about the PRNG.
- Need true random numbers to generate cryptographic keys that have no bias
- Thermal noise is sometimes used, but it has a bias
- It is easy to get true random numbers using quantum mechanics
- ID Quantique supplies quantum random number generator (QRNG) chips
  - Samsung uses it in Galaxy Quantum 2 smartphones



Ref: E. Gent, "Quantum Randomness Now Boosts Everyday Security," IEEE Spectrum, Aug 2021, https://spectrum.ieee.org/quantum-randomness-boosts-everyday-security

Factorization on Classical Computer

- Brute-Force using primes: 1, 2, 3, 5, 7, …, $\sqrt{N}$
- There is no general-purpose factorization algorithm
- In 2019, scientists factored a 240-digit (795-bit) number (RSA-240) using 900 core years. RSA 1024 will take 500 times longer.
- Most difficult to factor are products of two primes of similar size ⇒ used for cryptography
- In 2020, RSA-250 was broken using 2700 core years (using an optimized algorithm).
- No published algorithm can factor a b-bit number in $O(b^k)$ time.
  ⇒ No polynomial time algorithm using classical computing
- In 1994, Shor published an algorithm to factorize in polynomial time on a quantum computer ⇒ Polynomial in log N

Shor's Factoring Algorithm

- Peter Shor, a graduate of and a professor at MIT, developed an algorithm to find prime factors of numbers exponentially faster than conventional computers
- Select an arbitrary number a, such that a is co-prime to N
  $\Rightarrow a$ is a prime such that GCD(a, N) = 1
  GCD = greatest common divisor $\Rightarrow$ a and N have no common factors.
- **Step 1:** Find the period of the a^i mod N sequence, i.e., find p such that Mod(a^p, N)=1
- **Step 2:** Prime factors of N might be GCD$(N, a^{p/2}+1)$ *and* GCD$(N, a^{p/2}-1)$
  If p is odd, you need to select another a and go back to step 1
- Example: N=15, a=2;
  2^i mod 15 for i=0, 1, 2, …
  = 1, 2, 4, 8, 1, … $\Rightarrow$ p=4
- The factors are GCD(2^2+1, 15) and GCD(2^2-1, 15), i.e., 3 and 5.

Ref: P. W. Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring," Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, IEEE, 1994, p. 124

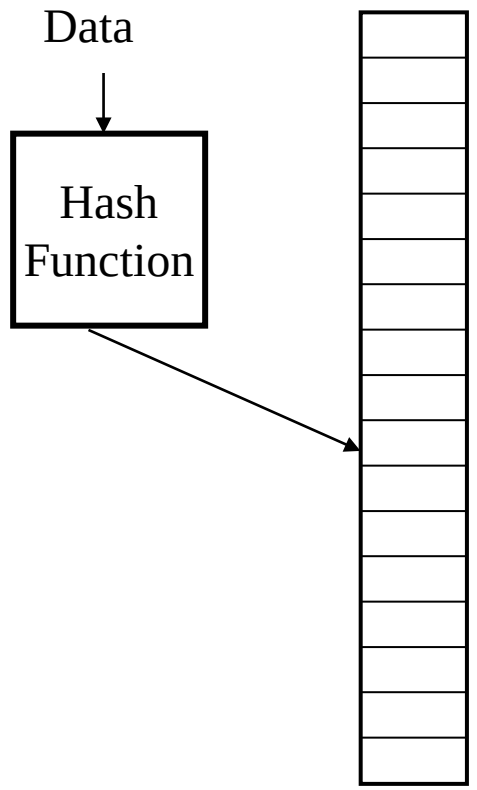
Hash Function

- **Database Search hash functions**

1. Take variable size input
2. Produce fixed output size (Size of table N)
3. Be easy to compute
4. Be pseudorandom so that it distributes uniformly over the table
   ⇒ Minimizes collisions

- **Cryptographic Hash Functions**

5. One-way. It is very difficult to find x, given h(x).
6. Given x, It is not possible to find y, such that h(y)=h(x)
7. Strong Collision Resistant: It is not possible to find any two x and y, such that h(y)=h(x)

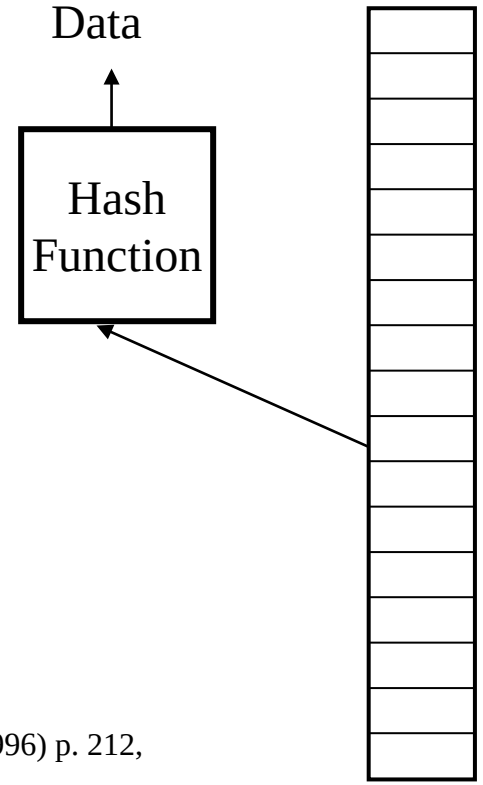


Inverting Hashes

- Hashes are one-way functions
- Given x, it is easy to find h(x),
  but given h(x), very difficult to find x
- Hash inversion is used as the puzzle in the Bitcoin blockchain
- Bitcoin miners try to find x that will hash to a number h(x)<N
- The difficulty increases as N is decreased
- As the computing power increases, Bitcoin difficulty is also increases, requiring more and more computing energy
- This applies to all other blockchains that use "Proof-of-Work" as the consensus algorithm

Grover's Algorithm

- Lov Kumar Grover, a graduate of IIT Delhi and Ph.D. from Stanford invented a "quantum mechanical database search algorithm."
- Unstructured search using $O(\sqrt{N})$ operations, where N is the size of the search table.
- Can invert any hash in $O(\sqrt{N})$ operations
  Classical computing takes O(N) operations
- Miners can solve an SHA-256 puzzle in 2^{128} iterations rather than 2^{256}
  $\Rightarrow$ 10 *quadrillion* times faster $\Rightarrow$ Big money saver for Bitcoin miners
- A hacker can find hash collisions a ten quadrillion times faster
  - Makes changing transactions/blocks a ten quadrillion times faster without affecting hash values



Ref: L. K. Grover, "*A fast quantum mechanical algorithm for database search*," 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212, https://arxiv.org/abs/quant-ph/9605043

How to Protect Blockchains?

A. Quantum-Resistant Blockchains

1. **Post-Quantum Cryptography**: Does not use factoring. NIST recommends:
   - ✓ CRYSTALS-KYBER for public-key encryption and key-establishment
   - ✓ CRYSTALS-DILITHIUM, FALCON, and SPHINCS+ for Digital signature
2. **Secret-Key Cryptography**: With sufficiently large keys
3. **Larger Hashes**: SHA-512

B. Quantum Native Blockchains: Hybrid of classical computing and quantum computing.

Most quantum circuits require classical communication lines after measurement.

Ref: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

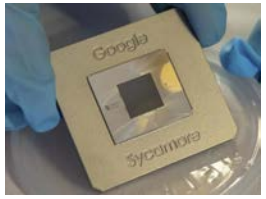
Challenges for Quantum

- **Decoherence**: Qubits lose their state over time.
  In nanoseconds to seconds, depending upon the temperature.
  - Need near zero-kelvin (10 milli Kelvin) temperature ⇒ Large cooling equipment.
  - Need extra qubits for quantum error correction to overcome decoherence
- Errors in quantum computers accumulate fast and require a thousand times more qubits to take care of errors
- Most of the research is theoretical.
  Practical experiments are limited to a tiny number of qubits.

Ref: M. Dyaknov, "The case against Quantum Computing," IEEE Spectrum, Nov 15, 2018, https://spectrum.ieee.org/the-case-against-quantum-computing#toggle-gdpr
D. Monroe, "Quantum Computers and the Universe," Communications of the ACM, December 2022, p10-11, https://dl.acm.org/doi/pdf/10.1145/3565977

Challenges for Quantum (Cont.)

- The most promising method of quantum computing consists of Interconnected Josephson junctions cooled to 10 milli-Kelvins.

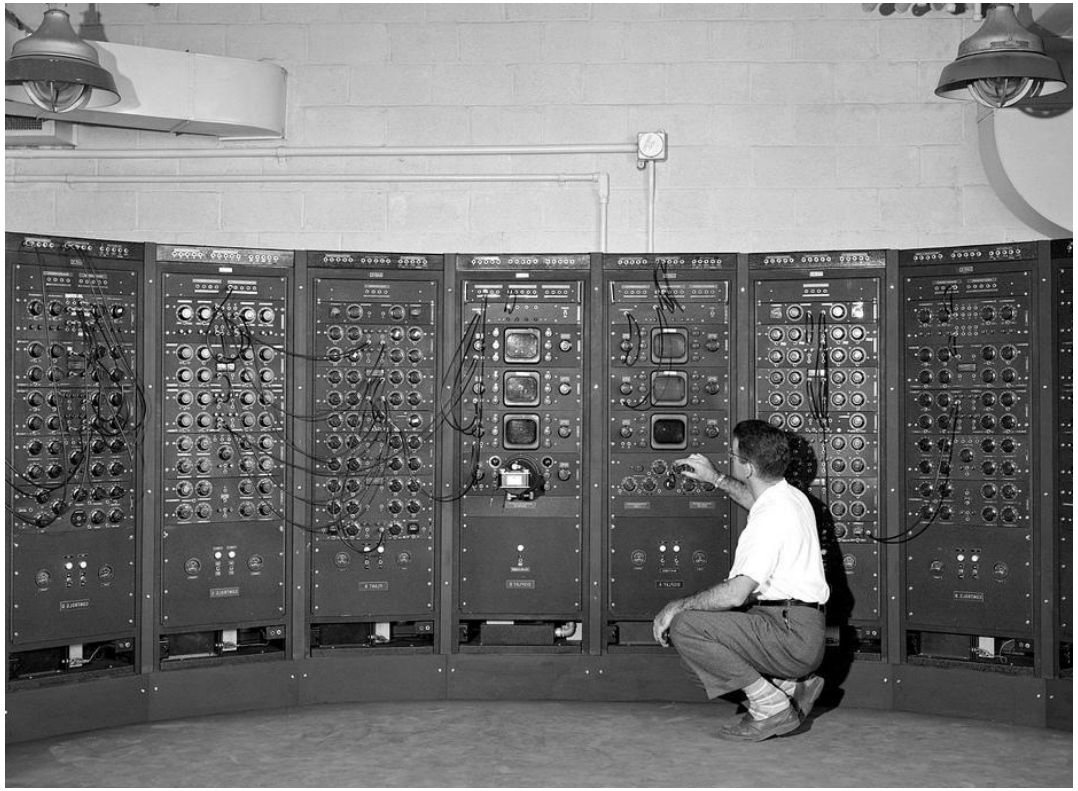


  - Developed initially by D-Wave systems. Now used widely.
  - November 9, 2022: IBM announced the world's largest quantum computer, Osprey, with 433 qubits
  - 12-qubit (Intel's Tunnel Falls), 256-qubit (QuEra's Aquila), and 53-qubit (Google's Sycamore) chips announced but few details
  - D-Wave Systems claims to have a 5000+ qubits computer using quantum annealing.
- Need 1000-100,000 qubit quantum computers to do exciting problems
  - 1000 qubits require $2^{1000} \sim 10^{300}$ parameters to describe its state
  - This number is larger than the *number of subatomic particles* in the observable universe.
  - One potential way is to reduce connectivity between qubits

Ref: https://www.newscientist.com/article/2346074-ibm-unveils-worlds-largest-quantum-computer-at-433-qubits/

Quantum Hardware

IBM's Quantum System One (2019) 20-qubit in a 9 ft cube



ENIAC (1943) 20 accumulators (10 decimal digits each)

Ref: https://www.datacenterdynamics.com/en/news/ces-ibm-announces-q-system-one-quantum-computer-9ft-cube/

Quantum Simulators

- QCEngine: https://oreilly-qc.github.io/
- Qiskit, https://qiskit.org/
  - Qiskit OpenQASM (Quantum Assembly Language), https://github.com/QISKit/openqasm/blob/master/examples/generic/adder.qasm
- Q# (Qsharp), https://docs.microsoft.com/en-gb/quantum/?view=qsharp-preview
- Cirq, https://arxiv.org/abs/1812.09167
- Forest, https://www.rigetti.com/forest
- List of QC Simulators, https://quantiki.org/wiki/list-qc-simulators
- See the complete list at: https://en.wikipedia.org/wiki/Quantum_programming

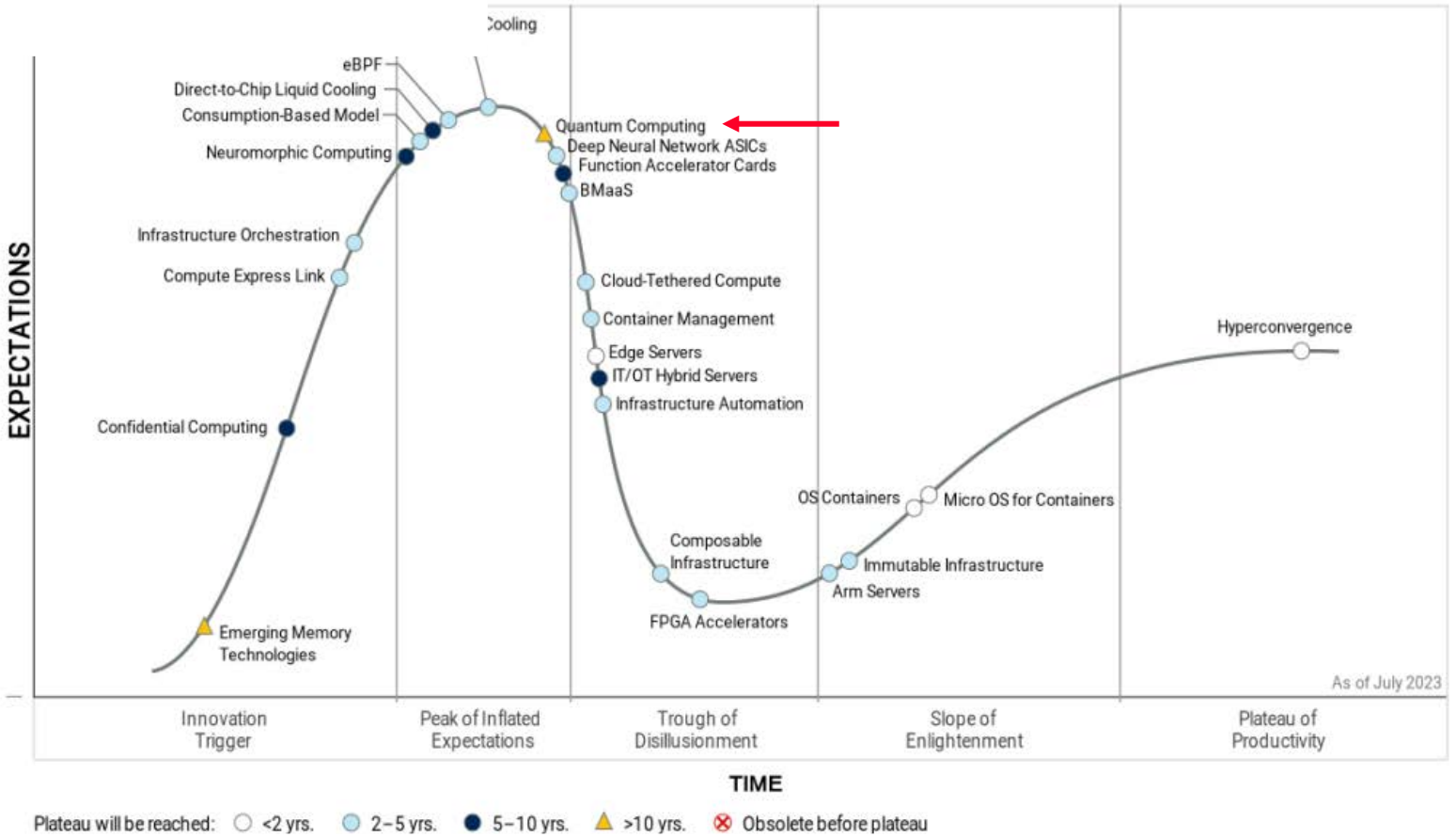
Ref: James Dargan, "**Top 63 Quantum Computer Simulators For 2022," The Quantum Insider,** Top 63 Quantum Computer Simulators For 2022 (thequantuminsider.com)

Status of Shor's Algorithm

- 2001: IBM was able to factor 15 with a 7-qubit computer.
- 2012: the factorization of 15 was performed with solid-state qubits
- 2012: the factorization of 21 was achieved
- 2019: an attempt to factor 35 on an IBM Q System One failed because of accumulating errors.
- Quantum circuit for Shor's algorithm needs to be custom-designed for each choice of N and each choice of a
- Needs two q-qubit registers, where $q \approx \log_2 N$

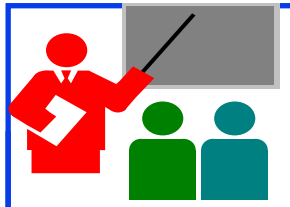
Ref: https://en.wikipedia.org/wiki/Shor%27s_algorithm

Gartner's Hype Cycle for Compute, 2023



Research & Startup → Sell Startup → Technology Profit → Manufacturing Profit →

Ref: T. Harvey, J. Donham, "Hype Cycle for Compute, 2023," Gartner G00790907, July 10, 2023, 87 pp.



Summary

1. Quantum computing is based on the discrete nature of photons (Quantum)
2. Qubits indicate the state of a photon.
   n qubits are represented by a vector of 2^n complex numbers
3. Quantum has several interesting phenomena, such as entanglement that can be used to teleport information or to link blocks
4. Shor's factorization algorithm allows the factorization of integers in less time than in classical computing
5. Grover's algorithm can help invert hashes in less time than in classical computing.
6. These algorithms can break blockchains
7. Quantum-Safe Crypto is in standardization
8. Fortunately, it isn't easy to make sufficient large quantum computers now.
   $\Rightarrow$ Not possible for Shor's algorithm or Grover's algorithm to have any impact on this generation of blockchains (2008-2128)

Our Papers

- Tara Salman, Ali Ghubaish, Roberto Di Pietro, Mohammed Baza, Raj Jain and Kim-Kwang Raymond Choo **CrowdFAB: Intelligent Crowd-Forecasting using Blockchains and its use in Security**, Transactions on Dependable and Secure Computing, October 2023.
- Zebo Yang, Maede Zolanvari, Raj Jain, "**A Survey of Important Issues in Quantum Computing and Communications**," IEEE Communications Surveys and Tutorials, March 2023, http://www.cse.wustl.edu/~jain/papers/qsurvey.htm
- Zebo Yang, Tara Salman, Raj Jain, and Roberto Di Pietro, "Decentralization using Quantum Blockchain: A Theoretical Analysis," IEEE Transactions on Quantum Engineering, September 2022, 16 pp., http://www.cse.wustl.edu/~jain/papers/qbif.htm
- Tara Renduchintala, Haneen Alfauri, Zebo Yang, Roberto Di Pietro, and Raj Jain, "A Survey of Blockchain Applications in the FinTech Sector," Journal of Open Innovation: Technology Market, and Complexity 2022, Vol. 8, Issue 4, 185, http://www.cse.wustl.edu/~jain/papers/fintech.htm

Our Papers (Cont)

- Tara Salman, Raj Jain, Lav Gupta, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains," IEEE 1st International Workshop on Advances in Artificial Intelligence for Blockchain (AIChain 2019), held in conjunction with the 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019, http://www.cse.wustl.edu/~jain/papers/rpmcewa.htm
- Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka, "Security Services Using Blockchains: A State of the Art Survey" IEEE Communications Surveys and Tutorials, First Quarter 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm
- Tara Salman, Raj Jain, and Lav Gupta, "Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/talks/qb_bu.htm