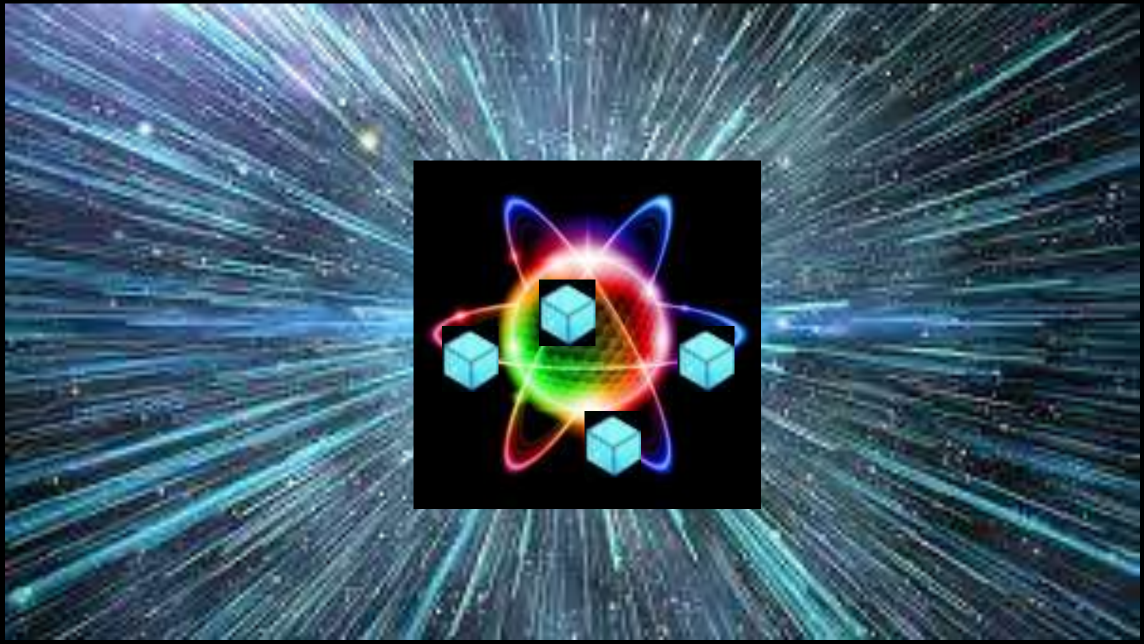


Quantum Blockchains

Cryptography, entanglement, and quantum blocktime

"[T]he technology for the control of complex quantum many-body systems is advancing rapidly, and we appear to be at the dawn of a new era in physics"
– physicist Leonard Susskind, 2019

Melanie Swan, MBA, PhD
Quantum Technologies
UCL Centre for Blockchain Technologies

San Jose CA, November 20, 2021

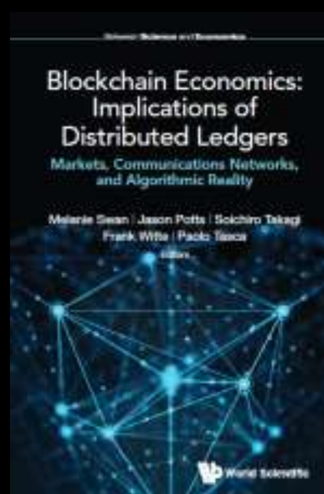
Slides: http://slideshare.net/LaBlogga

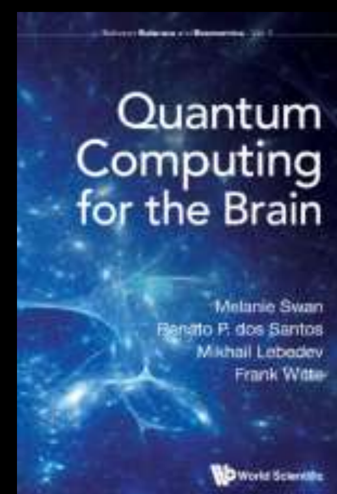
Research program

Smart Network Theory

- Aim: progression towards a Kardashev-plus society marshalling all tangible and intangible resources

Blockchain	Blockchain Economics	Quantum Computing	Quantum Computing for the Brain
2015	2019	2020	2022



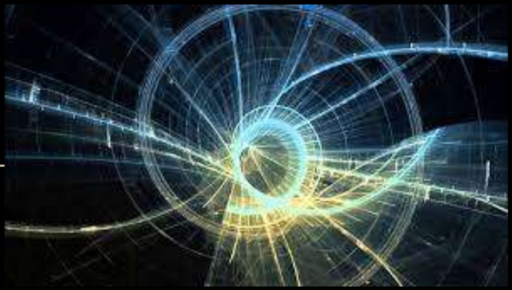


Thesis

Quantum blockchains are practically, a smart network automation technology, and theoretically, a tool for considering the problem of time

Smart networks: intelligent large-scale self-operating computation networks constituted as simple rules to support complex behavior (e.g. quantum and classical blockchains and deep learning neural nets; and BCI cloudminds and molecular manufacturing networks)

Definitions



- Quantum
  - The scale of atoms (nanometers 10^{-9}), ions and photons (picometers 10^{-12}), & subatomic particles (femtometers 10^{-15})
- Quantum computing
  - Computation performed with engineered quantum systems
    - Physical systems comprised of quantum objects (atoms, ions, photons) manipulated through logic gates
- Blockchain (distributed ledger technology)
  - Distributed database of asset ownership, peer network-maintained
  - Ex: global decentralized provisionless cryptocurrency (Bitcoin)
- Quantum blockchains
  - Blockchains using quantum methods for quantum-secure cryptography, consensus (mining), and other protocols

Source: Swan, M., dos Santos, R.P., Lebedev, M.A. & Witte, F. (2022). *Quantum Computing for the Brain.* London: World Scientific.

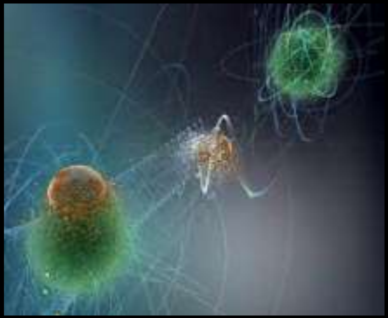
Agenda

- Quantum computing
- Blockchains (cryptoeconomics)
- Quantum blockchains
- Advanced: quantum blocktime

Why quantum computing?

- Quantum computing provides a more capacious architecture with greater scalability and energy efficiency than current methods of classical computing and supercomputing, and more naturally corresponds to the three-dimensional structure of atomic reality

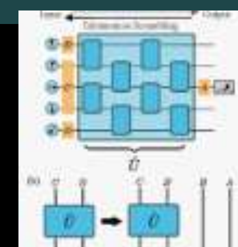
  - Scalability
    - Test more permutations (2^n) than classically
  - Find hidden correlations in systems
    - Entanglement modeling
  - Model 3D phenomena natively
    - Feynman: universal quantum simulation
  - Math: we have more math than we can solve
    - And need new math for new problem classes



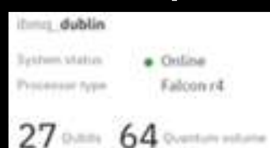
Source: Feynman, R.P. (1982) Simulating physics with computers. *Int J Theor Phys*. 21(6):467-88.

What is quantum computing?

- Quantum computing is the use of engineered quantum systems to perform computation: physical systems comprised of quantum objects (atoms, ions, photons) manipulated through configurations of logic gates



- Quantum platforms available via cloud services
  - IBM Q 27-qubit, IonQ 32-qubit, Rigetti 19Q Acorn



IBM: systems online
https://quantum-computing.ibm.com/services?services=systems

Available quantum computing platforms

Annealing (directed not programmed)	General logic circuit	Photonic (high-dimensionality (3+))
D-Wave Systems Quantum annealing machine	IBM/Rigetti Quantum processor (superconducting circuits)	IonQ ion trap Rydberg arrays Cold atom arrays Neutral atoms GBS Optical platforms

GBS: Gaussian Boson Sampling: method for sampling bosons using squeezed light states (classically hard-to-solve)

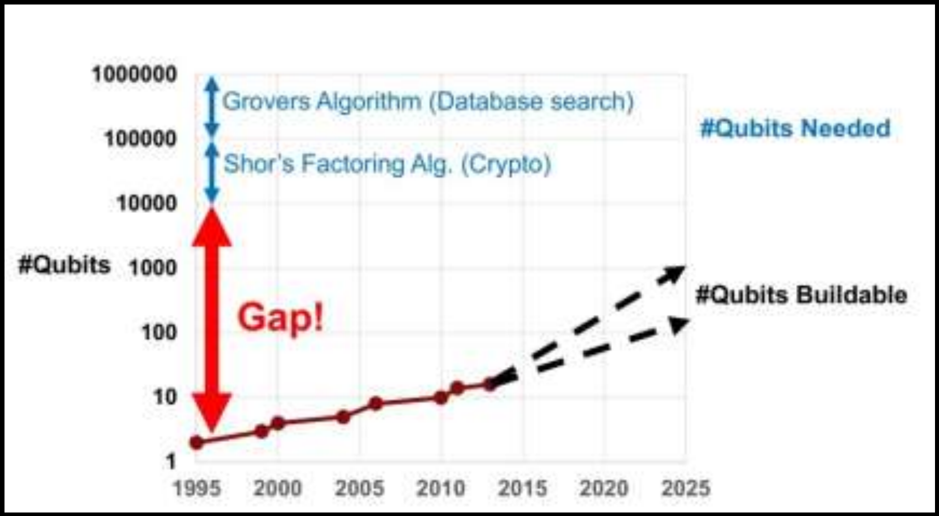
Source: Swan, M., dos Santos, R.P., Lebedev, M.A. & Witte, F. (2022). *Quantum Computing for the Brain*. London: World Scientific.

Status

Quantum computing

"Substantial technical breakthroughs are needed in quantum error correction to progress from NISQ (noisy intermediate-scale quantum) devices to fully FTQC (fault-tolerant quantum computing)" – quantum information scientist, John Preskill, 2021

- Need technical breakthrough for quantum error correction
- Currently available
  - NISQ (noisy intermediate-scale quantum) devices
    - 25-100 qubit machines that do not require error correction to solve a certain range of problems (primarily related to optimization)
- Long-term
  - FTQC (fault-tolerant quantum computing) devices
    - Quantum error correction needed to scale to hundreds of thousands and millions of qubit-sized machines

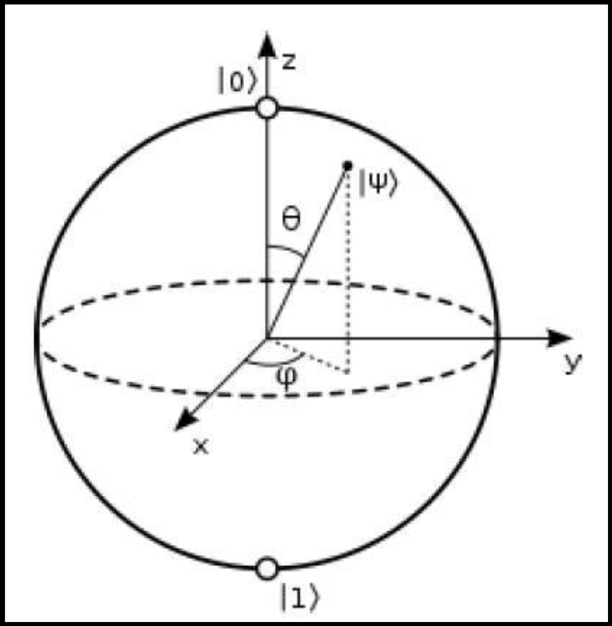


Sources: Preskill, J. (2021). Quantum computing 40 years later. arXiv: 2106.10522.
https://amitray.com/roadmap-for-1000-qubits-fault-tolerant-quantum-computers/

Quantum scalability

Bloch sphere: the qubit's Hilbert space
Hilbert space: generalization of Euclidean space to infinite-dimensional space (the vector space of all possible wavefunctions)

- Quantum computers
  - Hold all combinations of a problem in superposition simultaneously
    - 10 quantum bits hold 1,024 (2^{10}) different numbers simultaneously
  - Process all possible solutions simultaneously
- Classical computers
  - Hold one permutation at a time
  - Process sequentially



Bloch sphere: particle movement in X, Y, Z directions

Source: Hensinger, W.K. (2018). Quantum Computing. In Al-Khalili, J. Ed. *What the Future Looks Like*. New York: The Experiment. Pp. 133-43. (p 138)

Wavefunction

Wavefunction: description of the quantum state of a system

- The **wavefunction** (Ψ) (psi "sigh")
  - The fundamental object in quantum physics
    - Complex-valued probability amplitude (with real and imaginary wave-shaped components) [intractable]
  - Contains all the information of a quantum state
    - For single particle, complex molecule, or many-body system (multiple entities)
  - Schrödinger equation
    - Measures positions or speeds (momenta) of complete system configurations

Schrödinger wave equation

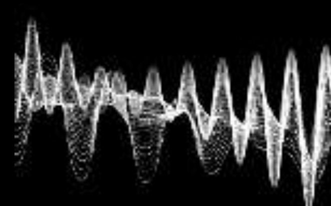
$E\Psi(r) = -\hbar^2/2m\ \nabla^2\ \Psi(r) + V(r)\Psi(r)$

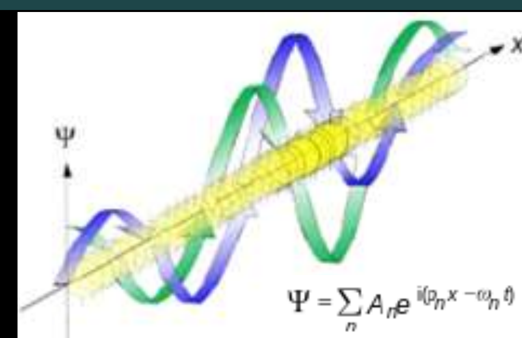
Total Energy = Kinetic Energy (motion) + Potential Energy (resting)

$$E\Psi(\mathbf{r}) = \frac{-\hbar^2}{2m}\nabla^2\Psi(\mathbf{r}) + V(r)\Psi(\mathbf{r})$$

Total Energy = Kinetic Energy + Potential Energy

Ψ = the wavefunction that describes a specific wave (represented by the Greek letter Ψ)





Source: Carleo, G. & Troyer, M. (2017). Solving the Quantum Many-Body Problem with Artificial Neural Networks. *Science*. 355(6325):602-26.

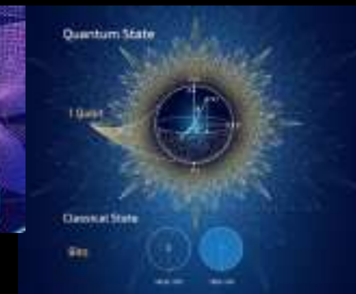
Quantum scale: 10^{-9} to 10^{-15} m

- "Quantum" = anything at the scale of
  - Atoms (Nano 10^{-9})
  - Ions and photons (Pico 10^{-12})
  - Subatomic particles (Femto 10^{-15})
- Nanotechnology is already "quantum"

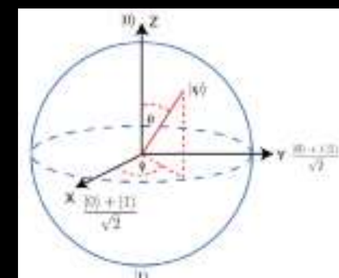
	Scale		Entities	Special Properties
1	1×10^{1} m	Meter	Humans	
2	1×10^{-9} m	Nanometer	Atoms	Van Der Wals force, surface area tension, melting point, magnetism, fluorescence, conductivity
3	1×10^{-12} m	Picometer	Ions, photons	Superposition, entanglement, interference, entropy (UV-IR correlations), renormalization, thermality, symmetry, scrambling, chaos, quantum probability
4	1×10^{-15} m	Femtometer	Subatomic particles	Strong force (QCD), plasma, gauge theory
5	1×10^{-35} m	Planck scale	Planck length	

Primary

Quantum properties



- Superposition
  - An unobserved particle exists in all possible states simultaneously, but collapses to only one state when measured



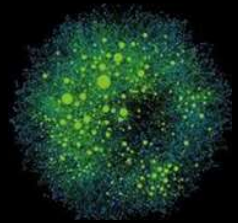
- Entanglement (used in quantum teleportation)
  - Physical attributes are correlated between a pair or group of particles (position, momentum, polarization, spin), even when separated by large distance
    - “Heads-tails” relationship: if one particle is in a spin-up state, the other is in a spin-down state

- Interference
  - Wavefunction amplitudes reinforce or cancel each other out (cohering or decohering)

Image Credit: Sandia National Laboratories

Full slate of

Quantum properties obtained "for free"



- Superposition, entanglement, and interference
  - Wavefunctions computed with density matrices & the Born rule
  - Quantum probability: find distribution & generate data
  - Heisenberg uncertainty: position-momentum, energy-time
- Entropy (# subsystem microstates & interrelatedness)
  - UV-IR correlations, topological entanglement entropy
- Scale renormalization (renormalization group flow)
  - Symmetry: gauge-invariant ordering properties
- Information scrambling: chaotic vs diffusive spread
- Thermality: temperature-based phase transition
  - Energy levels (ground state, excited state)
- Lattices: 3+ dimensional spacetimes

Source: Swan, M., dos Santos, R.P., Lebedev, M.A. & Witte, F. (2022). *Quantum Computing for the Brain.* London: World Scientific.

Uncertainty Tech

Quantum uncertainty relations

- Heisenberg uncertainty principle
  - Trade-off between conjugate variables: the more that is known about position, the less that can be known about momentum
    - Position-momentum
    - Energy-time (frequency)
    - Electric field-polarization density
    - Gravitational potential-mass density

Photon qubit encoding early-late arrival bins ←

- Entropic uncertainty (entropy = measure of uncertainty in a system)
  - Stronger & easier-to-compute form of Heisenberg uncertainty
    - Lower bound of Heisenberg uncertainty (Holevo is upper bound)
      - Min-entropy measures the uniformity in the distribution of a random variable (as a lower bound of the sum of entropies comprised by the temporal and spectral Shannon entropies or (equivalently) as the quantum generalization of conditional Rényi entropies)
  - The lower the min-entropy, the higher the certainty of the system producing a certain outcome
    - Apps: unbreakable cryptography, faster search, certified deletion

Calculate uncertainty using entropy instead of standard deviation

Sources: Halpern, N.Y., Bartolotta, B. & Pollack, J. (2019). Entropic uncertainty relations for quantum information scrambling. *Nat Comm Phys*. 2(92). Broadbent, A. and Islam, R. (2020). Quantum encryption with certified deletion. arXiv:1910.03551v3.

Entropy and entanglement (correlations)

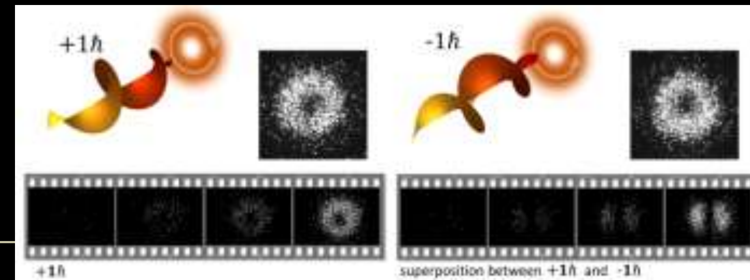
- Entropy: # microstates of a system

  - 2nd law of thermodynamics: total entropy of an isolated system cannot decrease over time
  - # of microscopic arrangements of a system
    - # air particle configurations all leading to room temperature of 72°F
  - Minimum # of bits (qubits) to send a message (information-noise)
- Entanglement: correlated properties of quantum particles
- Entanglement entropy: system interrelatedness
  - Measure as short-range long-range correlations
    - The degree of interconnectedness of subsystems in a system
  - Structure emerges from the correlations between quantum subsystems: time, space, gravity
    - Entanglement and other types of correlations

Source: Horodecki, M., Oppenheim, J. & Winter, A. (2007). Quantum state merging and negative information. *Commun Math Phys*. 269(1):107-36.

Qubit encoding

Photon orbital angular momentum (OAM)

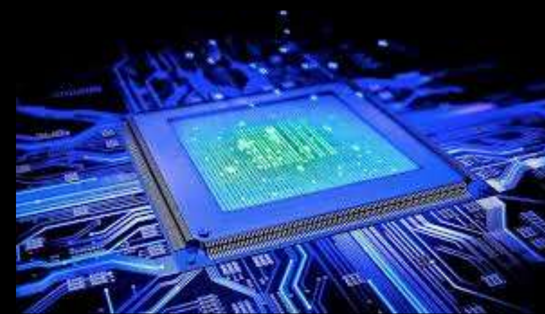


- Information is encoded onto a qubit using degrees of freedom which correspond to physical parameters
  - Spin, angular momentum, polarization, spatial mode

	System	Quantity	Qubit (One-Zero)
1	Electrons	Spin	Up/Down
		Charge	0/1 Electrons
2	Josephson junction	Charge	0/1 Cooper pair
		Current	Clockwise/Counter-clockwise
		Energy	Ground/Excited state
3	Single photon	Spin angular momentum (polarization)	H/V, L/R, Diagonals
		Orbital angular momentum (spatial modes)	Left/Right
		Waveguide propagation path	0/1 Photons
		Time-bin, Frequency-bin	Early/Late arrival bins
4	Optical lattice, quantum dot	Spin	Up/Down
5	Majorana fermions	Topology	Braiding

Sources: Flamini, F., Spagnolo, N. & Sciarrino, F. (2018). Photonic quantum information processing: a review. *Rep Prog Phys*. 82(016001). Erhard, M., Fickler, R., Krenn, M. & Zeilinger, A. (2018). Twisted photons: new quantum perspectives in high dimensions. *Light Sci. Appl*. 7(17146).

Chip progression: CPU-GPU-TPU-QPU



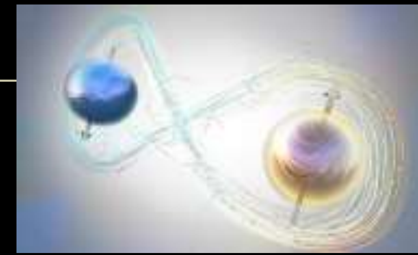
- Graphics processing units (GPUs)
  - Train machine learning networks 10-20x faster than CPUs
- Tensor processing units (TPUs)
  - Direct flow-through of matrix multiplications without having to store interim values in memory
- Quantum processing units (QPUs)
  - Solve problems quadratically (polynomially) faster than CPUs via quantum properties of superposition and entanglement

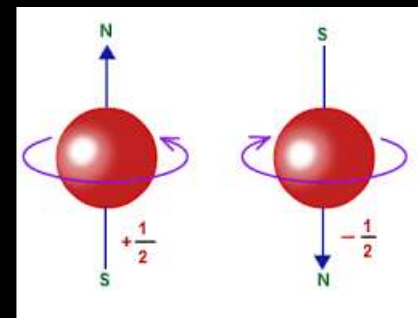
CPU	GPU	TPU	QPU
2	125	420	

Peak teraFLOPs in 2019 benchmarking analysis

Sources: Vescovi et al . (2017) Radiography registration for mosaic tomography. *J Synchrotron Radiat*. 24:686-94. LeCun, Y., Bengio, Y. & Hinton, G. (2015) Deep Learning. *Nature*. 521(7553):436-44. P. 439. Wang, Y.E., Wei, G.-Y. & Brooks, D. (2019) Benchmarking TPU, GPU, and CPU Platforms for Deep Learning. arXiv:1907.10701.

Computing architectures

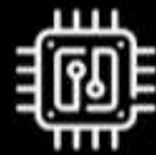




Classical:Quantum
as
Abacus:Logarithm

2500 BC
Abacus

→



20th Century
Classical

→

21st Century
Quantum

- Classical-supercomputer supplanted by quantum and neuromorphic computing (spiking neural network)

Traditional Von Neumann architectures

- Classical Computing
- Supercomputing

Beyond Moore's Law architectures

- Quantum Computing
- Neuromorphic Spiking Neural Networks

Source: Neurommorphic SNNs: Boahen, K. (2014). Neurogrid: A Mixed-Analog-Digital Multichip System for Large-Scale Neural Simulations. *Proc IEEE.* 102(5):699-716.

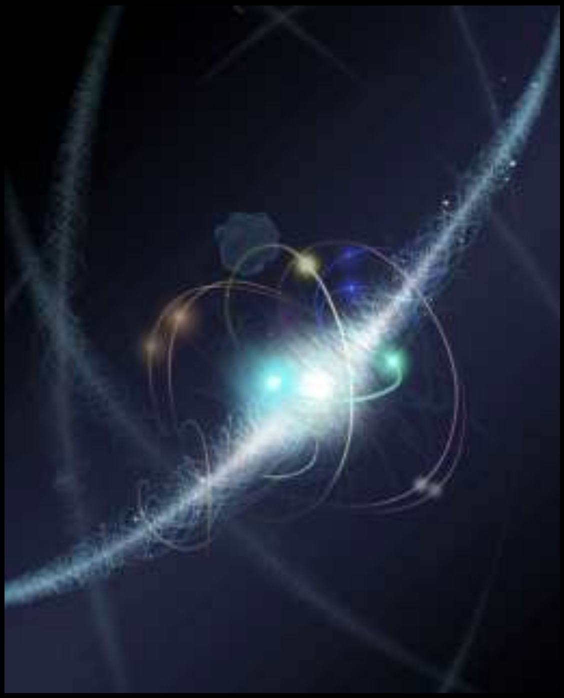
Interpretations of Quantum Mechanics

- Copenhagen interpretation: widely-accepted idea of the probabilistic nature of reality (Bohr-Heisenberg, 1925-27)
  - Particles exist in a superposition of all possible states, only the probability distribution can be predicted ahead of time, before the particle wavefunction is collapsed in a measurement
- Einstein interpretation (EPR) (1935):
  - (“God does not play dice”) rejects probability in favor of causality
  - No “spooky action at a distance” since faster-than-light travel is impossible, but entanglement (Bell pairs) now proven as the explanation for how remote particles influence each other
- Everett many-worlds interpretation (1956)
  - All possibilities described by quantum theory occur simultaneously in a multiverse composed of independent parallel universes

Practical advance: treat quantum mechanics as an engineering problem, not as a philosophical problem
EPR: Einstein-Podolsky-Rosen paradox

Post-quantum cryptography

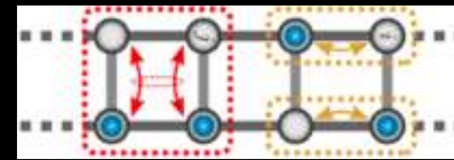
- "Y2K of crypto" problem
  - Quantum computing threatens existing global cryptographic infrastructure
    - Online banking, email, blockchains
- Solution
  - Migrate to quantum-secure algorithms
  - Estimated roll-out 2022-23 (US NIST)
- Mathematical shift
  - From factoring (number theory)
  - To methods based on lattices (group theory)
- Application: quantum key distribution
  - Satellite-based QKD: over 1200 km
  - Terrestrial QKD: over 300 km fiber & 144 km free space



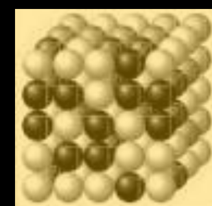
Quantum Key Distribution

Sources: Alagic *et al*. (2020). Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309; Barker, W. *et al.* (2021). Migration to Post-Quantum Cryptography. NIST; Simon, C. (2017). Towards a global quantum network. *Nat Photonics*. 11:678.

NIST algorithm selection



- NIST: 26 of 69 algorithms advance to post-quantum crypto semifinal (Jan 2019)
  - Public-key encryption (17)
  - Digital signature schemes (9)
- Approaches: lattice-based, code-based, multivariate
  - Lattice-based: target the Learning with Errors (LWE) problem with module or ring formulation (MLWE or RLWE)
  - Code-based: error-correcting codes (Low Density Parity Check (LDPC) codes)
  - Multivariate: field equations (hidden fields and small fields) and algebraic equations



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Second Round Candidates

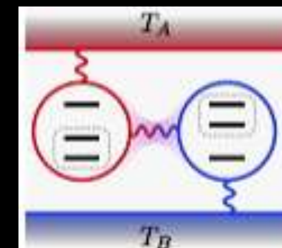
BIKE	
Classic McEliece	
CRYSTALS-DILITHIUM	
CRYSTALS-KYBER	
FALCON	
FrodoKEM	
GeMSS	
HQC	
LAC	
LEDAcrypt	
LUOV	Rainbow
MQDSS	ROLLO
NewHope	Round5
NTRU	RQC
NTRU Prime	SABER
NTS-KEM	SIKE
Picnic	SPHINCS+
qTESLA	Three Bears

Source: NISTIR 8240: Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, January 2019, https://doi.org/10.6028/NIST.IR.8240.

Status: rewrite computational algorithms to take advantage of known quantum speedups (in processing linear algebra routines, Fourier transforms, and other optimization tasks)

Quantum Math Tech

Quantum algorithms overview



- Shor's Algorithm (factoring)
  - Period-finding function with a quantum Fourier transform
    - A classical discrete Fourier transform applied to the vector amplitudes of a quantum state (vs general number field sieve)
- Grover's Algorithm (search)
  - Find a register in an unordered database (only √N queries vs all N entries or at least half classically)
- VQE: variational quantum eigensolvers (quantum chemistry)
  - Finds the eigenvalues of a matrix (Peruzzo, 2014)
- QAOA: quantum approximate optimization algorithm
  - Combinatorial optimization (Farhi, 2014)
- QAOA: quantum alternating operator ansatz (guess)
  - Alternating Hamiltonians (cost and mixing) model (Hadfield, 2021)

Quantum algorithms

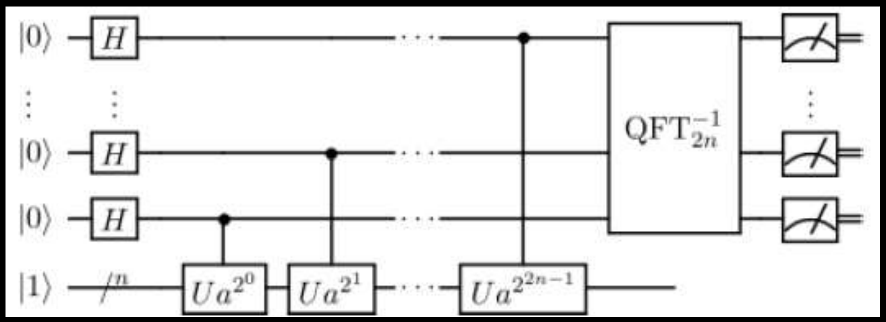
- General expectation: quantum vs classical algorithm
  - Quadratic, exponential, polynomial speedup
- Shor's factoring algorithm (subgroup-finding)
  - <u>Exponential advantage</u> for problems including factoring and discrete logarithm
  - Addresses only a small set of problems, but covers a large amount of the cryptographic landscape
- Grover's search algorithm
  - <u>Quadratic advantage</u> (more modest) vs. classical, but broad applicability indicates versatility
  - Quantum search algorithm allows searching any (including unsorted and unstructured) dataset for items that fulfill a condition, or are elements of a subset

Sources: Shor, P.W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal of Computing. 26(5):1484-1509; Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. Proceedings 28th Annual ACM Symposium on the Theory of Computing, STOC '96, pp. 212-19. ACM, New York, NY, USA, 1996.

Shor's factoring algorithm

- Period-finding function with a quantum Fourier transform
  - Quantum Fourier transform: a classical discrete Fourier transform applied to the vector amplitudes of a quantum state
  - Exponentially faster than classical algorithms (the general number field sieve)
- Two part function:
  - A reduction of the factoring problem to the problem of order-finding (which can be executed classically)
  - A quantum algorithm to solve the order-finding problem

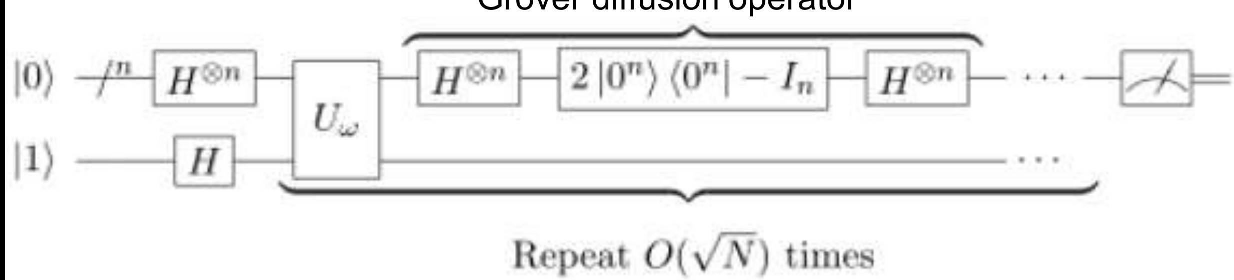
Quantum subroutine: period-finding function



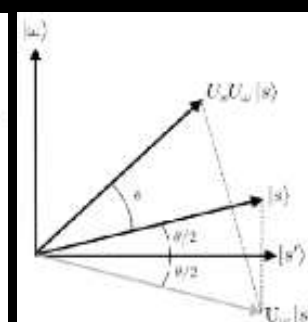
Source: Shor, P.W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal of Computing. 26(5):1484-1509.

Grover’s search algorithm

- Find a particular register in an unordered database
  - Search an unsorted database with quadratic speedup
  - A classical search of an unsorted database may need to check all N entries, and on average has to check at least half
  - A quantum search only needs to make √N queries
  - Uses function inversion and mean-median estimation
- Grover diffusion operator
  - Desired state amplitude is higher than that of others



Quantum circuit representation of Grover’s algorithm



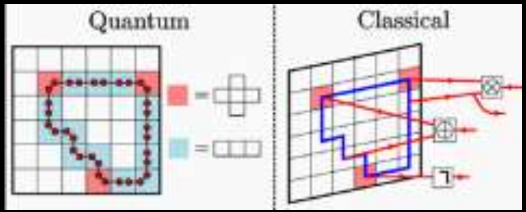
The operator is a reflection in the hyperplane, rotating the state vector in each iteration

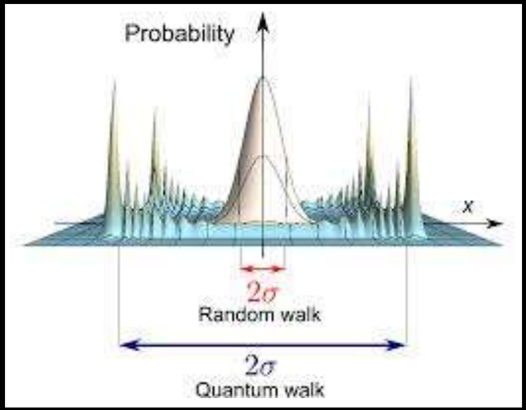
Source: Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. Proceedings 28th Annual ACM Symposium on the Theory of Computing, STOC ‘96, pp. 212-19. ACM, New York, NY, USA, 1996.

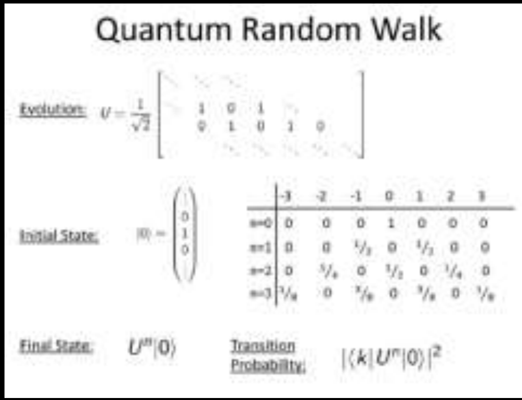
Quantum information science primitive (building block)

Quantum walks

- Quantum version of random walk to model complex behavior as Brownian motion (particles, neurons, traders)
  - Quadratically faster per ballistic propagation through lattice walk environment vs classical diffusive spread
    - Walk travels through all paths in superposition
    - Application: faster cryptography and search
  - Random walk
    - Coin flip and Markov (stochastic) processes
  - Quantum walk
    - Coin flip via quantum coin-flip operator (Hadamard coin)
    - Multi-dimensional lattice graph walk environment
    - Quantum walk algorithm
    - Time regime (discrete-continuous)



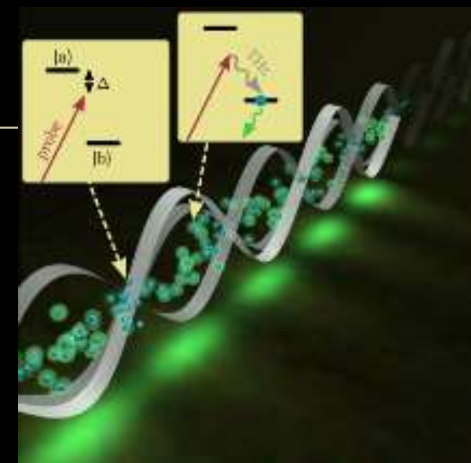




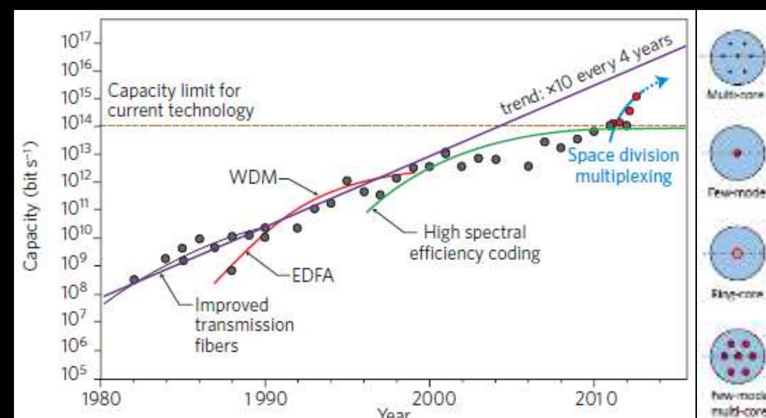
Hadamard coin (operator): flips a qubit into a one or zero

Source: Kendon. V. (2020). How to Compute Using Quantum Walks. *EPTCS*. 315:1-17.

Quantum networks



- Ultra-fast secure quantum photonic networks for communication, computation, and sensing
- Fiberoptic multiplexing
  - Write (modulate) data onto light
    - Time (TDM)
    - Wave (WDM) – forward-space
    - Space (SDM) – transverse-space (sideways and length-ways)



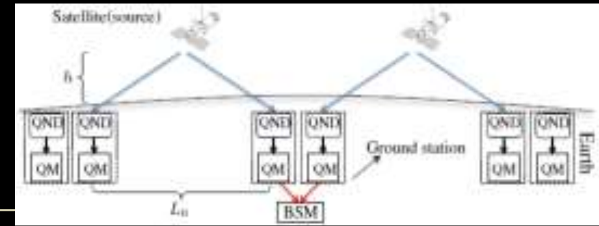
Moore's Law for Multiplexing Information

	Domain	Multiplexing Method	Modulation Mode	Year
1	Time	TDM: Time-division multiplexing	Time synchronization between sender and receiver	1880s
2	Wave	WDM: Wave-division multiplexing	Multiplex onto forward direction of wave movement	1990
3	Space	SDM: Space-division multiplexing	Multiplex onto transverse forward direction of wave movement	2013

Source: Richardson, D.J., Fini, J.M. & Nelson, L.E. (2013). Space-division multiplexing in optical fibers. *Nat Photon*. 7:354-62.

Quantum networks

Entanglement distribution



- Full-stack roadmap for end-to-end qubit delivery
  - Entanglement generation needed for quantum key distribution, quantum teleportation, quantum sensing
    - Teleportation: transmit a quantum state to another location
  - Many proposals for distilled, swapped, heralded (confirmed), high-dimensional entanglement

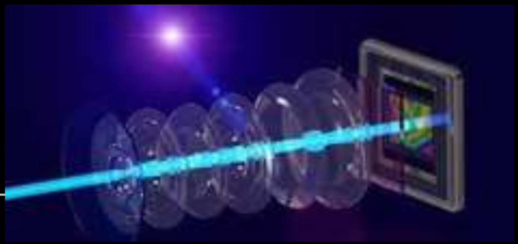
Quantum

Quantum Network Stack: OSI Layers with Entanglement Services

	OSI Stack	Unit	Description	Quantum entanglement service
1	Application	Data	End-user	End-user data presentation layer
2	Presentation	Data	Syntax	
3	Session	Data	Synchronization	
4	Transport	Segments	End-to-end-connection	Qubit transmission
5	Network	Packets	Packets	Long distance entanglement
6	Link	Frames	Frames	Robust entanglement generation
7	Physical	Bits	Physical Infrastructure	Initial entanglement generation

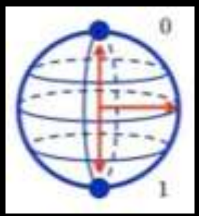
Sources: OSI (Open Systems International) Classical Network Stack and Dahlberg *et al.* (2019). A Link Layer Protocol for Quantum Networks. *Proc ACM SIGCOMM 2019*. Pp. 1159-73.

Bits vs. Qubits (Qudits)



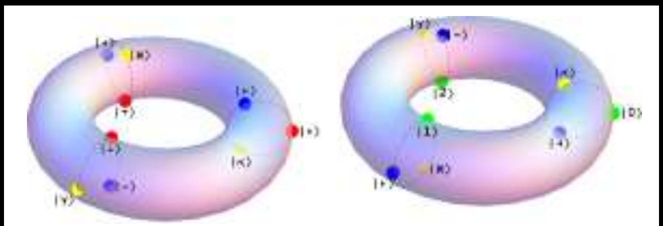
- Quantum networks imply multi-dimensionality
  - Photonics, qudits, GHZ states (3+ entangled parties)
- Qudits: quantum information digits
  - A qubit exists in a superposition of 0 and 1 before being collapsed to a measurement at the end of the computation
  - A qutrit exists in the 0, 1, and 2 states until collapsed for measurement (9-unit structure conducive to error correction)
  - 7 and 10 qudit systems tested, 4 optical qudits achieved the processing power of 20 qubits

Classical System
(0/1 bits)



Quantum System
(complex-valued qubits
on a Bloch sphere)

Error correction:
Qutrit stabilizer code on a torus



GHZ (Greenberger-Horne-Zeilinger) state: entangled quantum state involving at least three subsystems (particle states or qubits)

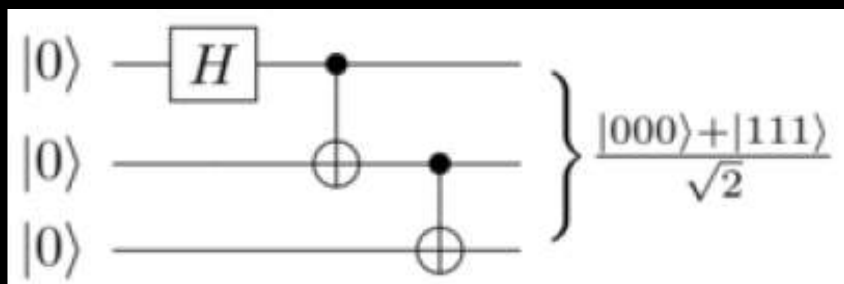
Source: Imany, P. *et al*. (2019). High-dimensional optical quantum logic in large operational spaces. npj *Quant Inf*. 5(59):1-10.

Quantum information science primitive

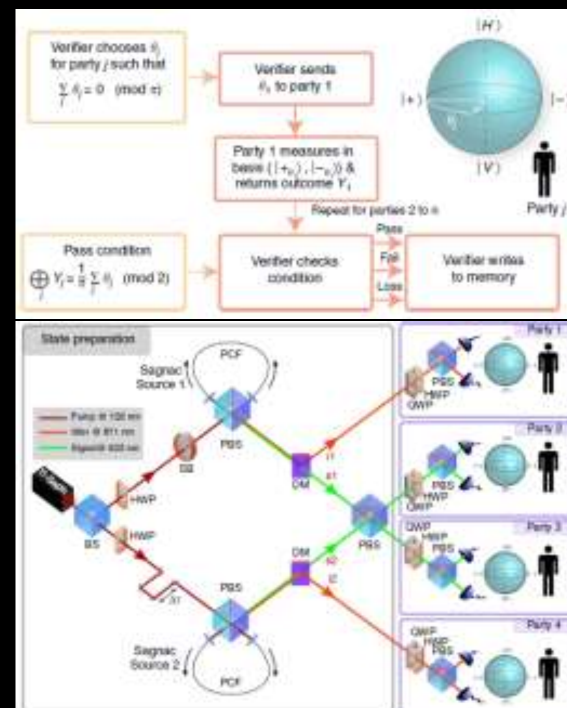
GHZ state: multiple entangled parties

- Greenberger-Horne-Zeilinger (GHZ) state: entangled quantum state involving at least three subsystems (particles, states, qubits) to encode quantum information

Generate 3-qubit GHZ state using quantum logic gates



Four-party GHZ state



- Use GHZ states for secure updating in quantum networks
    - Byzantine fault tolerance (BFT): verified multipartite entanglement in an open network of untrusted parties

Sources: Greenberger, D.M., Horne, M.A. & Zeilinger, A. (1989). Going beyond Bell's theorem. *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*. Ed. M. Kafatos. Dordrecht: Kluwer. Pp. 69-72. McCutcheon, W. *et al.* (2016). Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* 7:13251.

GHZ multiparty entangled states enable

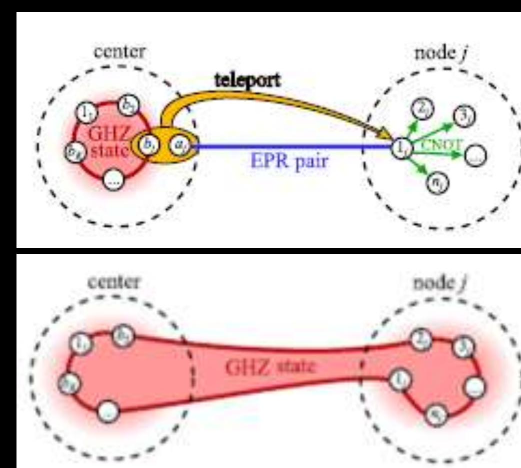
Global quantum clock network

Implication: secure quantum network node updating for quantum blockchains

- Satellite-based atomic clock network
  - Nodes use network-wide entangled states to interrogate local oscillators
  - Randomly-selected node leads round
- Prepare entangled network state
  - Initiating node prepares and teleports a GHZ state, nodes use teleported qubits to grow the GHZ state to all local qubits
  - Result: network-wide GHZ state
- Measure and update
  - Nodes measure oscillator phase to show center-of-mass detuning amount (error) to stabilize network reference frequency

Secure ultra-precise clock signal

Network-wide entangled GHZ state



Source: Lukin laboratory: Komar, P. *et al*. (2014). A quantum network of clocks. *Nature Physics*. 10(8):582.

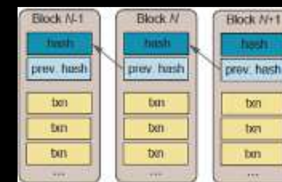
Agenda

- Quantum computing
- Blockchains (cryptoeconomics)
- Quantum blockchains
- Advanced: quantum blocktime

What is a blockchain?

Blockchain: smart network automation technology with tracking, remuneration, voting, automated execution, and multiscalar fleet-many item coordination

- Blockchain (distributed ledger technology): distributed database of asset ownership, peer-network maintained
  - Transaction blocks linked together with cryptography



    - Each block has a hash of the previous block, forms a chain
    - Cannot change any block without rewriting the whole chain
    - Nodes use an automated software protocol to validate new blocks
    - "Secure by design" distributed system with Byzantine fault tolerance
      - Safe communication in open networks with constantly cheating parties
    - Traditional intermediaries (banks) not required
    - *Example*: Bitcoin: global decentralized provisionless cryptocurrency
- Cryptoeconomics: blockchain-based digital economic infrastructure for immediate payments (cryptocurrency) and ongoing financial transactions (smart contracts)

Source: Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol CA: O'Reilly Media.

Crypto modernity mentality

Traditional Modernity	Digital Modernity	Crypto Modernity
	Planetary-scale technology development Internet	Blockchains
	2015 There's an app for that~! It's the economy, stupid~!	2021 There's a protocol for that~! It's the cryptography-based economy, my friend~!
1990 I've got a broker	1995 I've got a browser (1995: Netscape IPO)	2021 I've got a wallet I can be my own bank~!

Information revolution waves

- Internet I - (1990-2020+)
  - Digitization of information: News, media, entertainment, stock trading, mortgage finance, credit, open-source software
- Internet II - (2010-2050+)
  - Digitization of money: cryptographic assets: blockchain-based cryptocurrencies and smart contracts: money, payments, economics, finance, legal agreements (RegTech)
- Internet III - (2020-2050+)
  - Digitization of biology and matter: remaining industries: health, pharmaceuticals, agriculture, building materials, construction, automotive, transportation, energy, neural files
    - 3D printing, atomically-precise molecular manufacturing, nanofab

Source: Swan, M., dos Santos, R.P. & Witte, F. (2020). *Quantum Computing: Physics, Blockchains, and Deep Learning Smart Networks*. London: World Scientific.

information.

email.

voice.

video.

money.

neural files.

challenge: secure internet transfer of increasingly valuable and unique files

Low Sensitivity	information. email. voice. video.
Medium Sensitivity	money.
High Sensitivity	neural files.

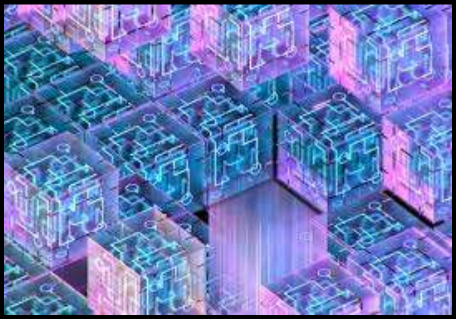
internet transfer.

file header indicates traffic type, software version, routing, etc.

Digital money: special requirements

- Information: send a PDF file or image many times
- Money: requires unique instances (no double-spending)

- Enabled by the internet as an always on 24/7 global network technology to check transactions in real-time
  - Network time-stamps every transaction
    - Can submit duplicate transactions (try to double-spend) but the network only counts the first one
  - Blockchain network checks every transaction
    - Computational confirmation by each node



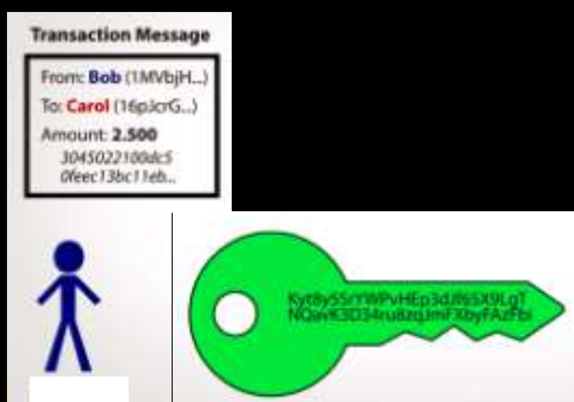
EMR: Electronic Medical Record

How does Bitcoin (any cryptocurrency) work?

Use Wallet app to submit transaction

Scan recipient address and submit transaction
Address: 32-character alphanumeric string

Coin appears in recipient wallet
(receive immediately, confirm later)



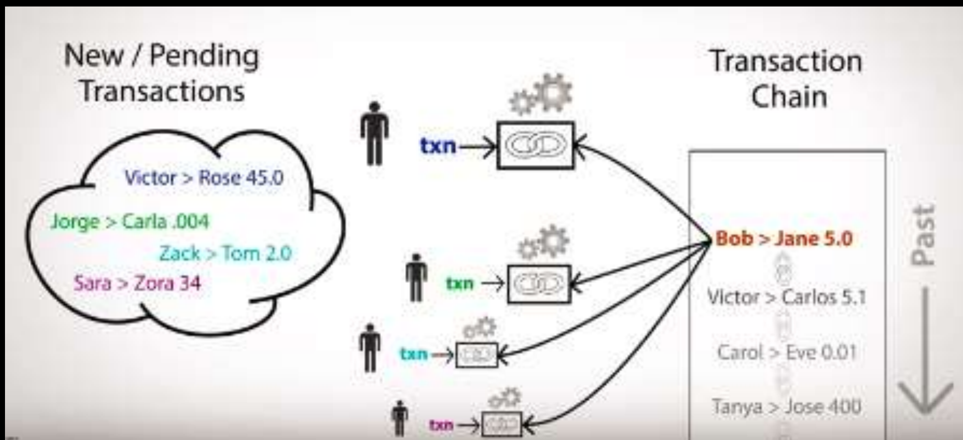
Wallet has keys not money
Creates PKI signature address pairs

A unique PKI signature for each transaction

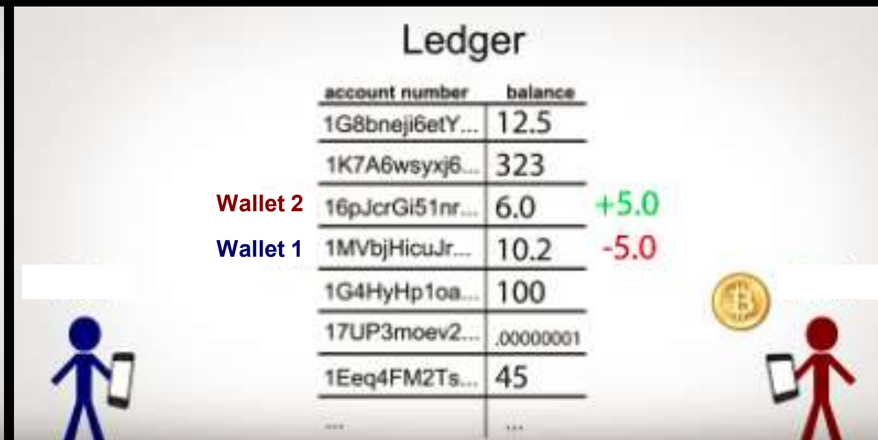
PKI: public-private key pair (cryptography standard)
Source: https://www.youtube.com/watch?v=t5JGQXCTe3c

What happens in the background?

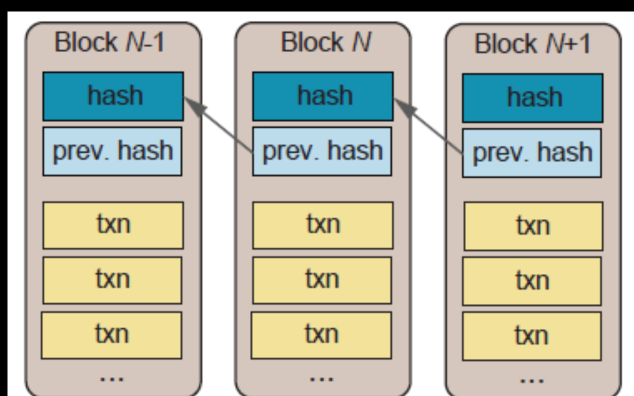
P2P network confirms & records transaction



Transactions submitted to a pool and miners assemble new batch (block) of transactions each 10 min (btc)



Transaction computationally confirmed and ledger account balances updated



Each block: transactions and a cryptographic hash of the last block, chaining the blocks, hence "blockchain"

Citizen Infrastructure

Github

bitcoin / **bitcoin**

Peer network maintains the blockchain: ledger nodes and mining nodes

Source: https://www.youtube.com/watch?v=t5JGQXCTe3c

How robust is the network?

- 12,817 global nodes hosting Bitcoin ledger (Nov 2021)
  - Historical context: 5,404 global nodes (Dec 2016)

GLOBAL BITCOIN NODES DISTRIBUTION

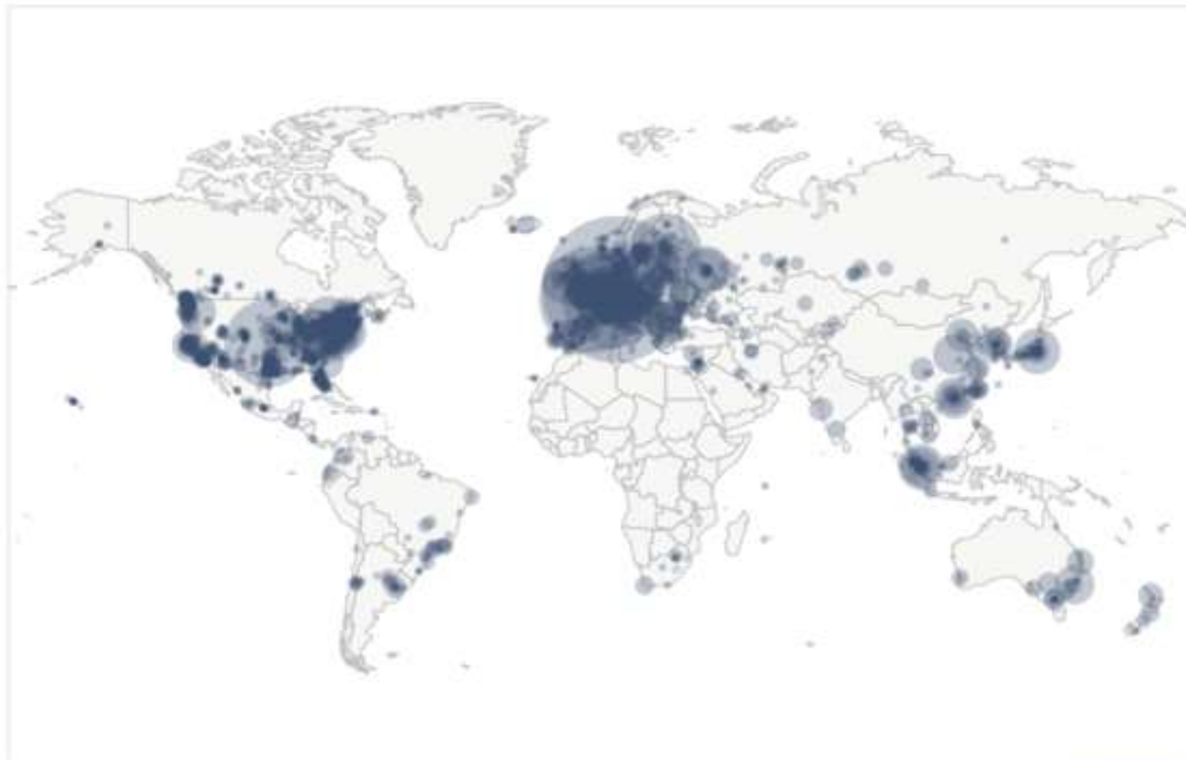
Reachable nodes as of Wed Nov 3 13:37:45 2021 MST.

12817 NODES | 24h | 90d | 1y

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	5400 (42.13%)
2	United States	1831 (14.29%)
3	Germany	1804 (14.08%)
4	France	547 (4.27%)
5	Netherlands	385 (3.00%)
6	Canada	331 (2.58%)
7	United Kingdom	255 (1.99%)
8	Russian Federation	197 (1.54%)
9	Finland	189 (1.47%)
10	Switzerland	135 (1.05%)

More (89) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Source: https://getaddr.bitnodes.io/

I can be my own bank~!

Some well-known wallets: Mycelium, Blue, Zap, Trezor (cold storage)

Practical considerations

Wallet apps: decision parameters

- Custodial or non-custodial (self-custody)
  - Custodial: wallet provider backs up your keys (Basic)
  - Non-custodial: only you have access to your keys (Advanced)
- Smart contract functionality
  - Monetary transfer only (Basic)
  - Join and write smart contracts (Advanced)
- Hot-warm-cold storage; desktop or mobile wallet
- Advanced features
  - Lightning network (Level Two overlays): immediate transactions
  - Tied to Visa/Mastercard debit card at point of sale (cash back)
- Consumer or enterprise wallet (Hyperledger, Symbiont)

technical deep-dive.

Mining shifting to US as China bans cryptocurrency production (June 2021)

Source: https://www.illumina.com/science/technology/next-generation-sequencing.html

Source: https://www.seattletimes.com/business/bitcoin-miners-exit-china-beat-a-path-to-the-u-s-as-crypto-climate-shifts/

USD $45 million/day business:
block reward 6.25 btc/block ($312,500) x 6 blocks/hour x 24 hours/day ~= $45,000,000
(at Bitcoin = $50,000)

mining.

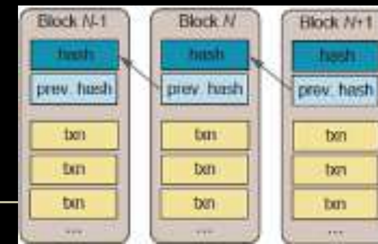
Blockchain primitive (building block)

Hash functions

- Hash function: function converting any length input (image, movie, legal document) to a fixed length encrypted output
  - Example: output (digest) of the SHA-256 hash function for
    - "My last will and testament on this day"
      - 13789917A50601C55D396B83FD98F1A0BED628948AD5F84890C63210E0897D76
    - "My last will and testament, on this day"
      - C6E9D7F4C9F7D0C8CD24E4D674BED1146331DB61555F9D68EBAAA3A0E827BBAB
    - Adding one comma results in a completely different hash digest
  - NP-complete problem: hard to compute, easy to verify
    - Cannot guess the output ahead of time without putting the inputs into the algorithm and performing the calculation
      - Must do the actual "work" to compute the output

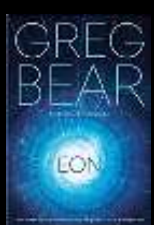
Source: SHA-256 hash algorithm: https://passwordsgenerator.net/sha256-hash-generator/

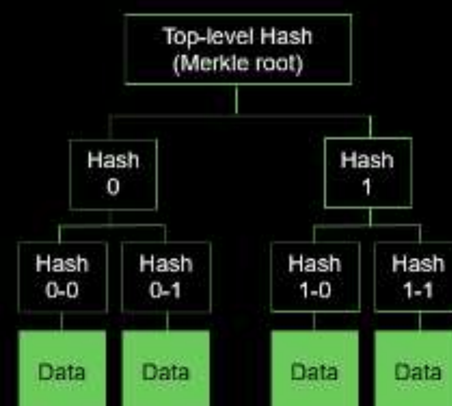
Hash-linked data structure



Blockchain: transaction blocks hashed together

- Merkle tree: hierarchical structure of hash codes corresponding to a large data structure
  - A hash is made for each data element, then a hash of these hashes, and so on, hierarchically until there is just one top-level hash that calls the entire data structure, the Merkle root
- One top-level Merkle root calls an entire data corpus
  - Bitcoin blockchain: 700,000+ transaction blocks since inception (Jan 2009) as of Sep 2021
  - All Github code, all Pubmed publications
  - An entire brain or cloudmind (brain of brains)
  - All human knowledge (digitally encoded)
    - Data pillar (crypto science fiction, Bear, *Eon*, 1985)
  - Whole human genome or brain file





Source: Swan, M., dos Santos, R.P. & Witte, F. (2020). *Quantum Computing: Physics, Blockchains, and Deep Learning Smart Networks*. London: World Scientific.

Hash-linked data structure applications

Brain DAC and quantum brain DAC

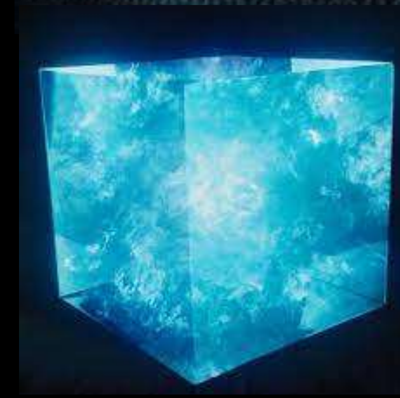
Blockchain Thinking

The Brain as a Decentralized Autonomous Corporation

- A brain is a Merkle forest of ideas
  - A group of Merkle trees, each calling an arbitrarily-large thought trajectory
- Brain DAC I: Basic Brain DAC
  - Instantiate thinking in a blockchain
- Brain DAC II: Quantum Brain DAC
  - Quantum brain DAC: brain DAC instantiated on a quantum platform
    - Quantum blocktime and superpositioned states (Egan’s solipsist nation)
  - Personal connectome scan
    - NFT-controlled blockchain hash structure
  - Cloudmind realization
    - Between-mind thought interoperability

DAC: distributed autonomous corporation = package of blockchain-based smart contracts for automated execution
Source: Swan, M. (2015). Blockchain thinking: The brain as a DAC (decentralized autonomous corporation). *IEEE Technology and Society Magazine* 34(4):41-52

Proof-of-work hash functions secure the blockchain



- PoW hash functions designed to reduce email spam
  - Force email senders to find a hash value for the email with an arbitrary number of leading zeros
    - Includes a timestamp to prevent pre-computation of useful hashes
    - Must hash the same input with a large number of trial-and-error nonce values until a hash meeting the requirements is obtained
- Nonce (number used once)
  - Used in PoW systems to vary the input to a hash function to obtain a hash for an input that fulfills certain arbitrary conditions

PoW: proof-of-work, systems that require participants to perform a resource-consuming proof of work to prove their good player behavior

Bitcoin proof-of-work mining

Custom mining ASICs represent the hashing algorithm in hardware

- Miners calculate a hash value using the block header (constant for a specific block) and a nonce (random string changed repeatedly) to create a hash digest that hopefully meets the block requirements

- Called "mining" because find/mint new coin
  - Custom ASICs: rate of 4 billion guesses/second
  - Software adjusts difficulty level per number of miners
  - Winning hash has a certain number of leading zeros
    - Impossible to know ahead of time because depends on the data in the current block, must trial-and-error guess
  - First miner to get a winning hash announces victory
    - Other miners confirm the result and append the block
    - If multiple winning blocks, takes a few rounds for the network to adopt the longest chain

ASIC: Application Specific Integrated Circuit https://blockexplorer.com/block/0000000000000000002274a2b1f93c85a489c5d75895e9250ac40f06268fafc0

Block Explorer News Market Bitcoin cash Zcash

Step 1: Find the nonce (NP-complete problem). A miner guesses a nonce (random string), appends it to the hash of the current header, rehashes the value, and compares to the target hash value (which has a certain number of leading zeros). If the resulting hash value is equal to or lower than the target, the miner has a solution and is awarded the block

Step 2: Record the block. The block hash is the digest of SHA-256 run on six data elements: 1. Bitcoin version number 2. previous block hash 3. Merkle Root of all the transactions in the block 4. timestamp 5. difficulty target 6. nonce

Target value: an integer in the range of [0, (2^{256} - difficulty)]

Difficulty: a measure of how hard it is to create a hash that is less than the target (system-set computational number involving floating point operations, exponents, integrals); re-tuned every 2016 blocks (~2 weeks) to keep PoW as a meaningful deterrent against rogue miners as the overall network computation power increases or decreases

Block #544795

BlockHash 0000000000000000002274a2b1f93c85a489c5d75895e9250ac40f06268fafc0

18 leading zeros (can vary)

Summary

Number Of Transactions	3055	**Difficulty**	7454968648263.241
Height	544795 (Mainchain)	**Bits**	1725c191
Block Reward	12.5 BTC	**Size (bytes)**	804055
Timestamp	Oct 7, 2018 1:23:31 PM	**Version**	536870912
Mined by		**Nonce**	869666145
Merkle Root	2c29aa31fcd7dc9ed1c21361b6fec8...		
Previous Block	544794		

The winning nonce (number used once) for this block, a number appended to the current header, that when re-hashed, meets the difficulty level (for any block, the Bitcoin nonce is an integer between 0 and 4,294,967,296)

Transactions

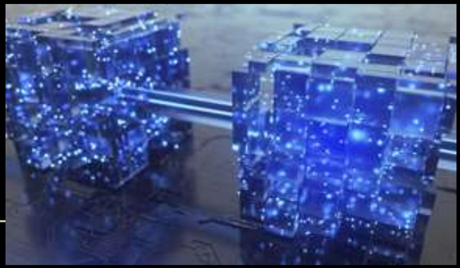
deaa0b42c9ec00ce38717f30937c85d72940bbb60cc9b9fcfd4dec0220235067

12.58442651 BTC (U)

Summary: the hash is calculated using the block header, which is constant for a specific block, and a nonce, which is changed repeatedly by the miner, to create different hash digests in the hope of finding a digest that fits the block requirements

HERE: Oct 7, 2018 (18 leading zeros)
https://blockexplorer.com/block/0000000000000000002274a2b1f93c85a489c5d75895e9250ac40f06268fafc0
RECENT: Nov 6, 2021 (19 leading zeros)
https://www.blockchain.com/btc/block/0000000000000000000633b91a8cd72235104935c9d3af0b0edae9ad6f89f4ef

Bitcoin difficulty



- Bitcoin software automatically tunes to adjust some variables and keep others relatively fixed
  - To continue producing a block every ~10 minutes, if more miners come onto the network, the difficulty is increased
    - More people trying to solve an arbitrary puzzle will find the answer more quickly than fewer people, so the puzzle is made more difficult to keep the same rate of puzzle solving
  - The bitcoin blockchain hashing algorithm is tuned to an arbitrary difficulty by changing the required min-max value of the hash as miners come onto or exit the network

Bitcoin difficulty comparison: increase from 2018 to 2021
(automatically adjusts every 2016 blocks (~2 weeks) per compute power on the network)

	Block	Date	Difficulty	Nonce	# Transactions
1	544795	Oct 7, 2018	7,454,968,648,262.24	869,666,145	3055
2	708081	Nov 3, 2021	21,659,344,833,264.85	802,610,441	2978

Source: Bard, D.A. *et al*. (2021). Quantum Advantage on Proof of Work. arXiv:2105.01821v1.

Longest chain rule

- Longest chain rule: nodes adopt the longest PoW chain
  - Blockchains are based on the longest chain: the chain that a majority of the network holds as the state of the blockchain
  - A miner can create a malicious block and add it to the network but it will not be accepted by a majority of the nodes, as other peers on the network will reject the block and choose an alternate proposed block, therefore, excluding the malicious block from the longest chain
  - Truth system based on what majority of peers take to be true
- Transaction confirmation vs settlement finality
  - If multiple winning blocks, takes a few rounds for the network to adopt the longest chain (chain recorded by most miners)
  - A block is committed (settlement finality) when buried sufficiently deep in the chain (6+ confirms)

Source: Rajan, D. & Visser, M. (2019). Quantum Blockchain using entanglement in time. *Quantum Rep*. 1(2):1-9.

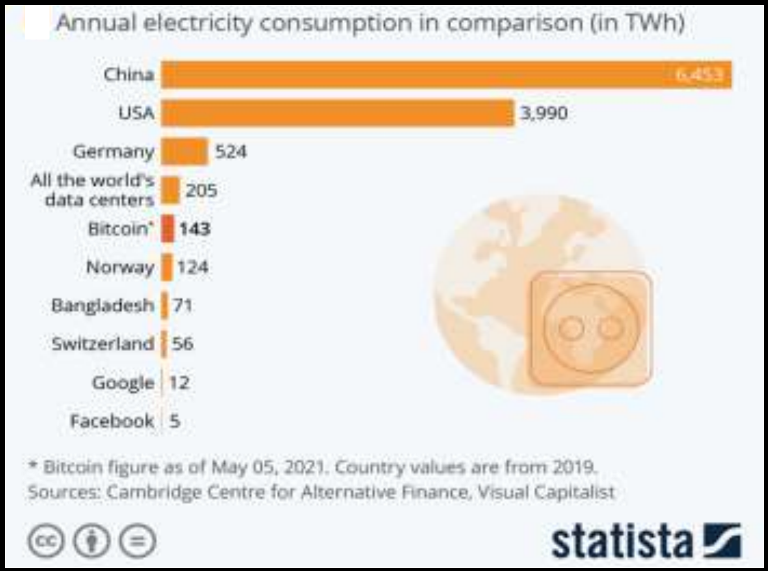
51% attack

- Cryptocurrencies are peer network based
- 51% attack: controlling the majority (51%) of the network's computational power
  - Malicious controlling a majority (51%) of the network's computational power
  - Can potentially overwhelm the consensus mechanism by adding blocks to the chain faster than the rest of the network can compete
  - Result: control of what is included in new blocks but cannot rewrite past history

Source: Rajan, D. & Visser, M. (2019). Quantum Blockchain using entanglement in time. *Quantum Rep*. 1(2):1-9.

PoW mining energy consumption

- Proof-of-work competition among miners ensures security of blockchain ledger
  - Critics argue “wasteful” use of resources but provides secure computational system (700,000 btc blocks as of Sep 2021)
  - 39 per cent of proof-of-work mining is powered by renewable energy, primarily hydroelectric energy (Cambridge study, 2021)
  - Alternatives: proof-of-stake, entropy
- Energy consumption
  - Less than all the world’s data centers
  - Less than China, USA, Germany
  - Less overhead than worldwide bank branch infrastructure
    - Resource substitution from physical to digital domain



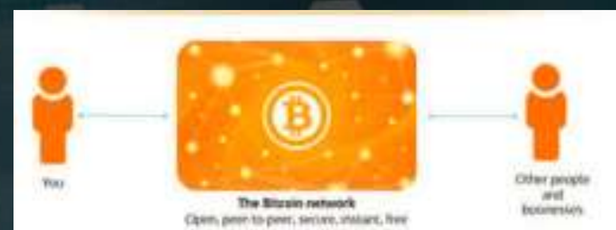
Sources: Statista. (2021). https://www.statista.com/chart/18632/estimated-annual-electricity-consumption-of-bitcoin/
Blandin, A. *et al*. (2021). 3rd Global Cryptographic Benchmarking Study. University of Cambridge.

old model.

new model.

banks.

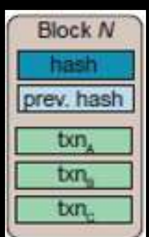
networks.



money.

What is Bitcoin?

- First, largest, best-known cryptocurrency
  - 700,000+ blocks (Sep 2021)
  - Each with a few thousand tx
- Satoshi white paper (2008)
  - Digital monetary system
    - PoW hash-linked blocks
    - Automated tx validation
    - Network time-stamping
    - Game-theoretic incentives
- First transaction 12 January 2009
    - Nakamoto 10 btc to Hal Finney (reusable proof of work creator)



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Source: Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https:// bitcoin.org/bitcoin.pdf

Money supply

	Date	Money supply	Status
1	Aug 2021	18,700,000	89% issued and outstanding
2	2140e	21,000,000	Fully issued and outstanding

- Total Bitcoin money supply: 21,000,000
  - Estimated to be fully issued and outstanding in May 2140
  - Issued and outstanding as of Aug 2021: 18,700,000 (89%)
- Miners: accountants that record the transaction
  - Wallet default suggests 1% transaction fee
- Miner incentive = block rewards + transaction fees
  - Shift in proportion over time
    - Block reward share decreases
    - Transaction fee share increases (greater transaction volume)
  - Block rewards halved every 210,000 blocks (~4 years)

	Block reward	Date	Block height
1	50 btc	Jan 2009	0
2	25	Nov 2012	210,000
3	12.5	Jul 2016	420,000
4	6.25	May 2020	630,000
5	3.125	2024e	840,000

Sources: Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https:// bitcoin.org/bitcoin.pdf; Controlled Supply en.bitcoin.it/wiki/

Bitcoin denominations

- Satoshis: common unit of transfer (wallet default)
  - 500 satoshis = USD $0.25 (at Btc = $50,000)
    - $5 coffee = 10,000 satoshis
  - 1 satoshi = USD $0.0005 (at Btc = $50,000)

	Unit	Abbreviation	Description	BTC
1	Satoshi	SAT	Satoshi	0.00000001 BTC
2	Microbit	uBTC	Microbit or bit	0.000001 BTC
3	Millibit	mBTC	Millibitcoin	0.001 BTC
4	Centibit	cBTC	Centibitcoin	0.01 BTC
5	Decibit	dBTC	Decibitcoin	0.1 BTC
6	Bitcoin	BTC	Bitcoin	1 BTC
7	Decabit	daBTC	Decabitcoin	10 BTC
8	Hectobit	hBTC	Hectobitcoin	100 BTC
9	Kilobit	kBTC	Kilobitcoin	1000 BTC
10	Megabit	MBTC	Metabitcoin	1,000,000 BTC

100 millionth of a BTC

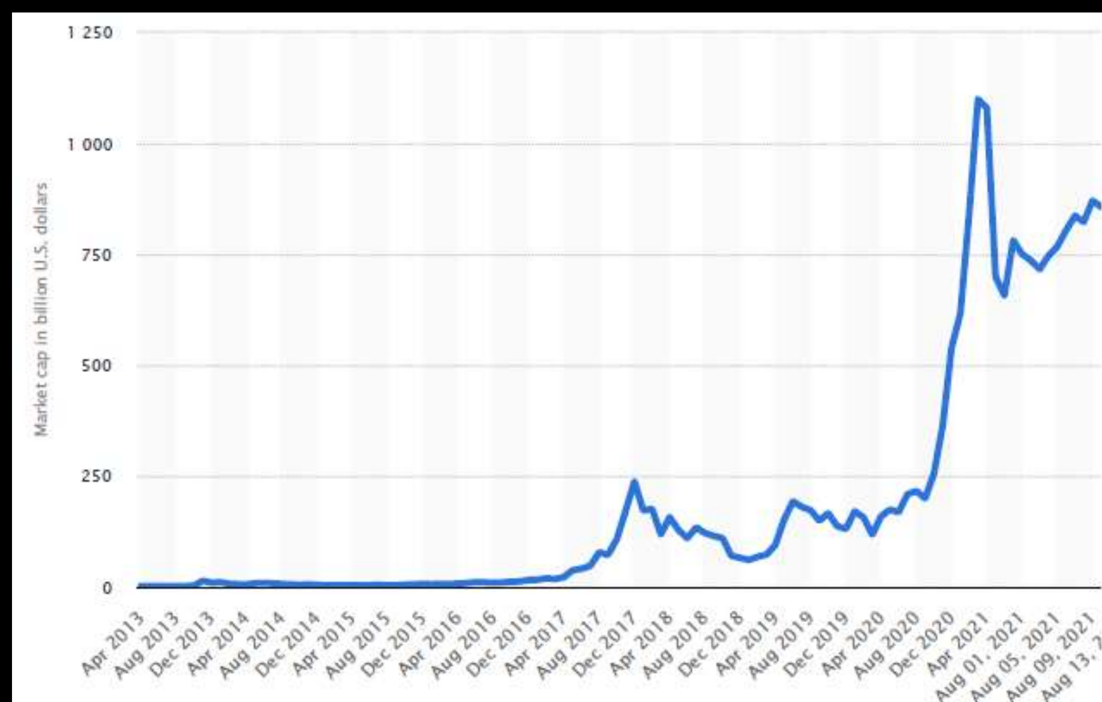
1 millionth of a BTC

Source: Bitcoin Foundation, https:// bitcoin.org/

$2 tn crypto market capitalization (Aug 2021)

- ~$1 tn Bitcoin ($800 mn)
- ~$1 tn other cryptocurrencies
- Heuristic is ½ is bitcoin

Market capitalization of Bitcoin
April 2013 to August 15, 2021 (USD billion)
Source: Statista 2021



Market capitalization is calculated by multiplying the total number of Bitcoins in circulation by the Bitcoin price

Source: https://www.statista.com/statistics/377382/bitcoin-market-capitalization/

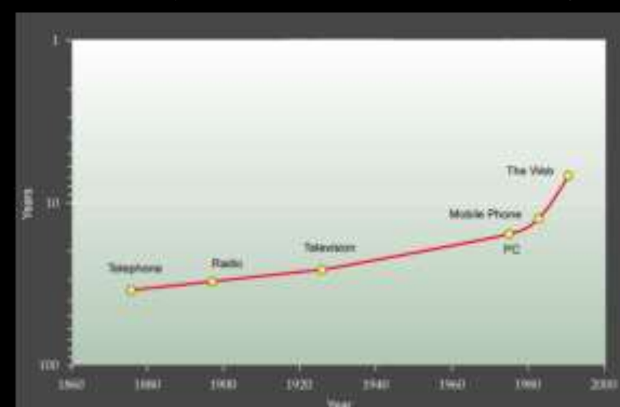
Crypto market research (2018-2020)

- 101 million unique users (Sep 2020)
  - In 191 million accounts opened at NAM-EUR registered service providers
  - 30% business and institutional clients
  - Fiat-cryptoasset transactions dominate
- Stablecoins (pegged cryptocurrencies)
  - Tether 4 to 32%; non-Tether 11 to 55%
- Cryptoasset companies doing KYC
  - 87% versus 52% (registered providers)
  - Helped by Financial Action Task Force (FATF) harmonization of KYC/AML standards across jurisdictions

	Year	Unique users (registered wallets)
1	2017	2.9-5.8 million
2	2018	35 million
3	2020	101 million

~1.3% of world population

Mass use of inventions (years until used by 25 percent of population)



KYC: Know Your Customer: identity checks required for customers of registered financial institutions

Sources: Blandin, A. *et al*. (2020). 3rd Global Cryptographic Benchmarking Study. Cambridge Centre for Alternative Finance. University of Cambridge. September 2020. Mass use of inventions: http://www.kurzweilai.net/the-law-of-accelerating-returns

Cryptoeconomics

- Cryptoeconomics: blockchain-based digital economic infrastructure for immediate payments (cryptocurrency) and ongoing financial transactions (smart contracts)
- Cryptoeconomic applications
  - Stablecoins (pegged cryptocurrencies)
  - Central bank digital currencies
  - DeFi: decentralized finance
    - Smart contract-based financial systems
  - Non-fungible tokens (NFTs)
  - Proof-as-a-feature (computational verification)
    - Zero-knowledge proofs (ZKP)
    - Verified random functions (VRF)

Blockchain 1.0: Currency
Blockchain 2.0: Contracts
Blockchain 3.0: Beyond financial market applications: space, genomics, supply chain

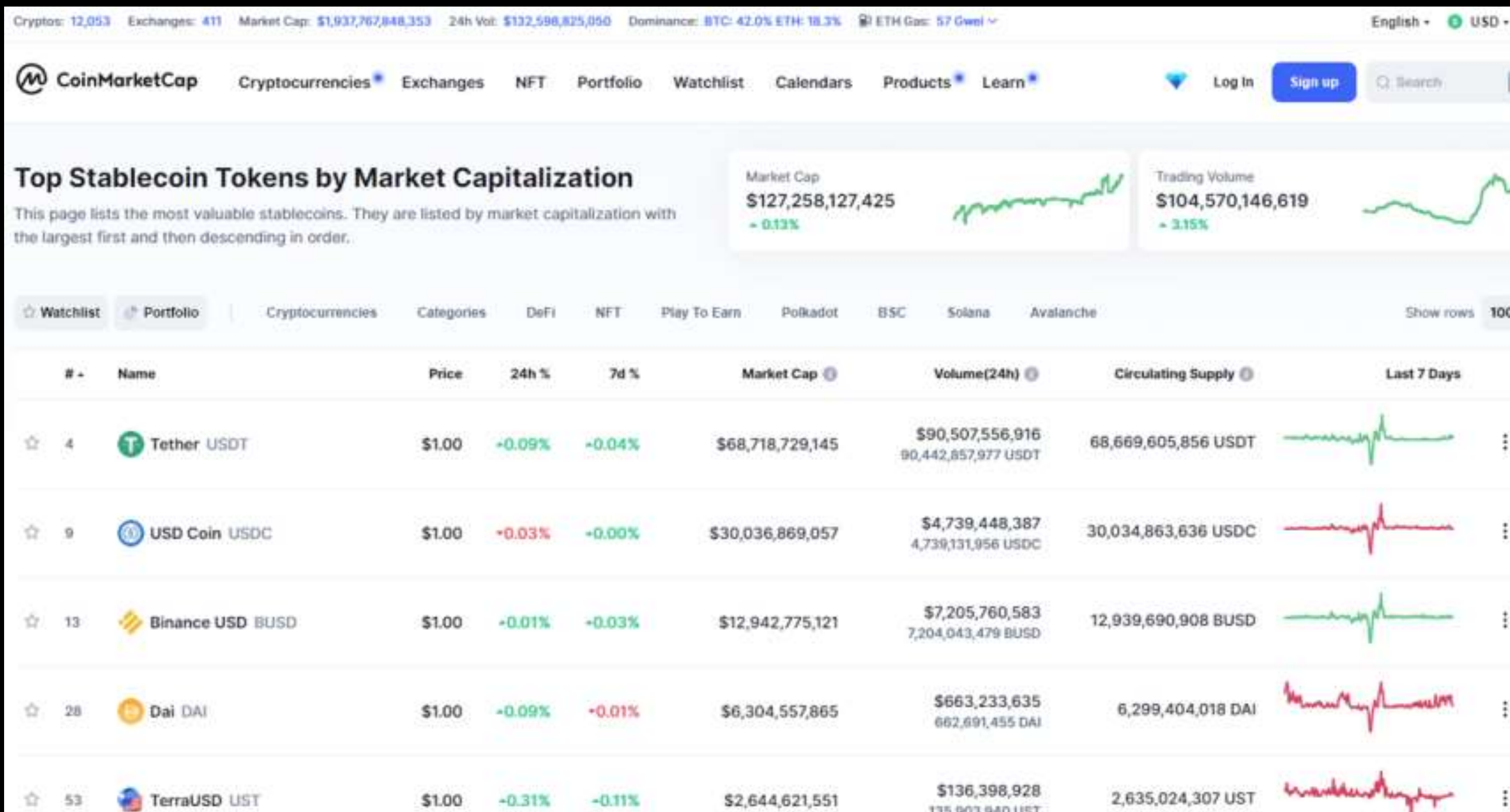
Stage: digitize existing financial infrastructure with blockchains

Vision: create digital institutions that better serve the public good

Sources: Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* Sebastopol CA: O'Reilly Media. Swan, M., dos Santos, R.P. & Witte, F. (2020). *Quantum Computing: Physics, Blockchains, and Deep Learning Smart Networks*. London: World Scientific.

Stablecoins (asset-pegged cryptocurrencies)

- Pegged to fiat currencies (Yen, Euro, USD) or other cryptocurrencies



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
4	Tether USDT	$1.00	0.09%	0.04%	$68,718,729,145	$90,507,556,916 90,442,857,977 USDT	68,669,605,856 USDT	
9	USD Coin USDC	$1.00	0.03%	0.00%	$30,036,869,057	$4,739,448,387 4,739,131,956 USDC	30,034,863,636 USDC	
13	Binance USD BUSD	$1.00	0.01%	0.03%	$12,942,775,121	$7,205,760,583 7,204,043,479 BUSD	12,939,690,908 BUSD	
28	Dai DAI	$1.00	0.09%	0.01%	$6,304,557,865	$663,233,635 662,691,455 DAI	6,299,404,018 DAI	
53	TerraUSD UST	$1.00	0.31%	0.11%	$2,644,621,551	$136,398,928 135,903,940 UST	2,635,024,307 UST	

Source: USD Coin (Circle) https://coinmarketcap.com/view/stablecoin/

Central bank digital currency (CBDC)

- Digital central back currencies might decrease or complement the demand for cryptocurrencies
- US: Digital Dollar program
  - Faster, cheaper, safer payments
  - “You wouldn’t need stablecoins or cryptocurrencies if you had a digital U.S. currency” - Fed Chief Jerome Powell
  - Jul 2021 Powell told the House Financial Services Committee that the digital dollar project is moving forward
- China: e-CNY (announced Jul 2021)
  - Feb 2021 pilot program
    - Digital yuan pilot program distributed 10 million yuan (~1.5 million) as part of a major test for the project

Smart contract (automated execution)

- Economic activity: 2/3 future obligations

	Instrument	Activity	Volume	Blockchain instrument
1	Currency	Money: immediate transfer	One third	Cryptocurrency payments
2	Contract	Finance: ongoing obligation	Two thirds	Smart contracts

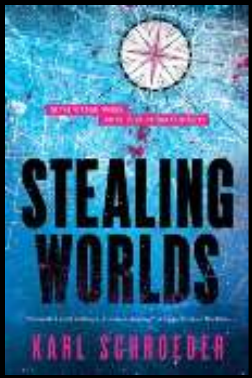
- Smart contract: blockchain-registered code that automatically executes per specified conditions
  - Automated compliance: FinTech (FINRA) and RegTech
    - Outsourced-to-technology legal & financial industry impact

- Legal contracts (4 elements)
  - Agreement (terms)
  - Parties (at least two parties)
  - Timeframe
  - Economic consideration

Crypto science fiction: corporations replaced by AI DACs (Schroeder, *Stealing Worlds*, 2019)

DAC (distributed autonomous corporation): package of smart contracts for automated execution

2019



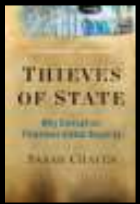
Source: Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* Sebastopol CA: O'Reilly Media.

DeFi (decentralized finance)

Crypto Modernity
There's a protocol for that~!

- DeFi blockchain-based financial infrastructure
  - Open, permissionless financial systems platforms
  - Replicates existing financial services in a more open and transparent way
    - Does not rely on intermediaries and centralized institutions, but open protocols and decentralized applications (DApps)
    - Smart contracts assume the role of custodians, central clearing houses, and escrow services
  - Digitalization of the finance industry
    - Execute financial transactions with blockchains
  - Phase: early-stage, high-risk, criminals & charlatans
    - Could become regulated (like ICOs and exchanges)
      - Boom and bust cycles
        - Tulips, roaring 1920s (bootlegging), internet boom and day trading (1990s), crypto booms and crashes

"It is naïve to think that those who can take resources will not" - corruption expert, Sarah Chayes, T*hieves of State*, 2014



DApp: distributed applications *Source:* Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*. Second Quarter 2021. 103(2):153-74.

ICO: initial coin offering (the analog of an IPO for a cryptocurrency project)

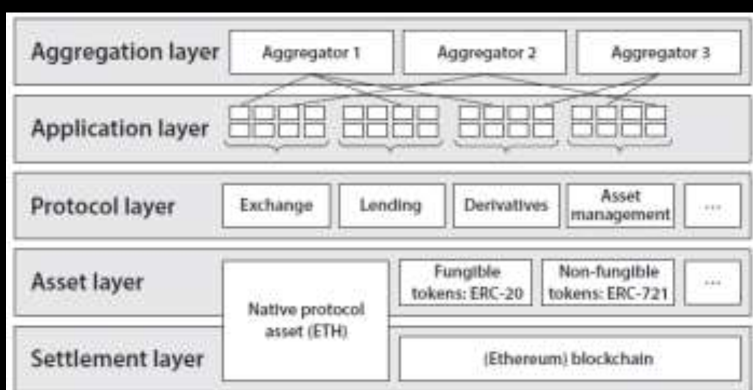
DeFi applications

- DeFi applications
  - Decentralized lending (crypto loans)
    - Users deposit digital assets into liquidity pools that the protocol lends out
  - Crypto derivatives: futures, options, hedging
  - Decentralized insurance
  - Staking (earn return on staked position)
- User empowerment: contribute decentralized capital
  - Earn return on contributed capital and infrastructure
    - Not previously built into blockchain architectures
  - Maintain self-custody of cryptoassets (self-sovereignty)
  - Participate in protocol governance (voting)

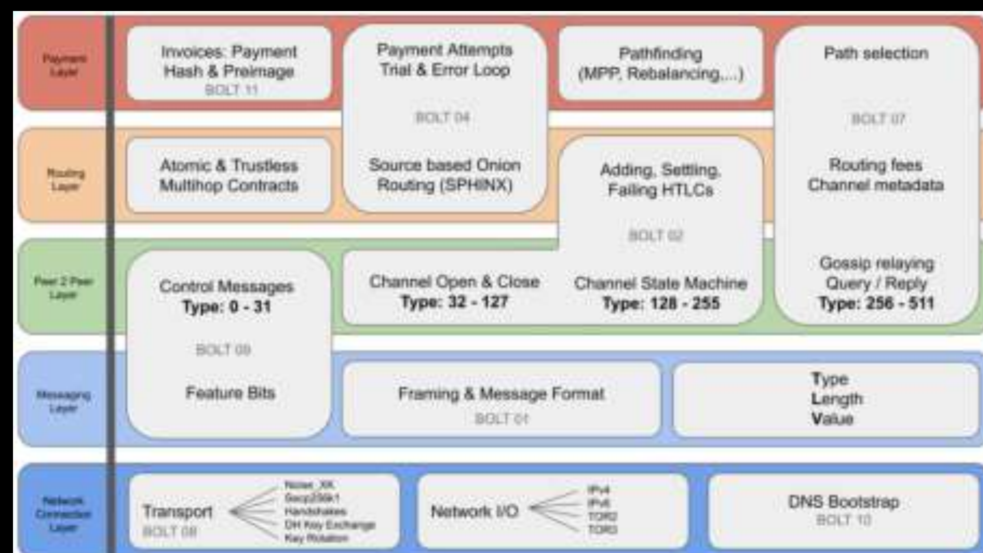
Source: Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*. Second Quarter 2021. 103(2):153-74.

The DeFi protocol stack

- Open-source interoperable protocol stack built on public smart contract platforms (e.g. Ethereum)
- Transactions automatically executed
  - Agreements enforced by code
  - Legitimate state changes persist on a public blockchain



Source: Schär, F. (2021). Decentralized Finance



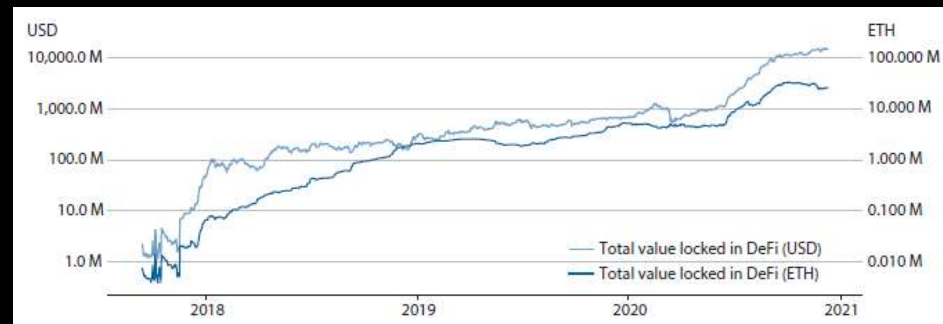
Source: https://github.com/lnbook/lnbook/blob/develop/06_lightning_architecture.asciidoc

Source: Antonopoulos, A.M., Osuntokun, O. & Pickhardt, R. (2021). *Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments.* Sebastopol CA: O'Reilly Media. https://github.com/lnbook/lnbook

DeFi market volume

- Financial instruments as a decentralized protocol, but DeFi protocols are an unregulated business (as of Nov 2021)
- USD $10 billion committed in Ethereum blockchain smart contracts (2Q2021) (Schär)

USD $10 billion committed in DeFi contracts (USD ETH)



Examplar categories of DeFi activity (defipulse.com)

LENDING | DEXES | DERIVATIVES | PAYMENTS | ASSETS

DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
1.	Aave	Multichain	Lending	$13.83B	7.95%
2.	Maker	Ethereum	Lending	$11.91B	4.54%
3.	Curve Finance	Multichain	DEXes	$11.62B	-6.49%
4.	InstaDApp	Ethereum	Lending	$10.53B	-13.20%
5.	Compound	Ethereum	Lending	$10.18B	3.49%
6.	Uniswap	Ethereum	DEXes	$6.18B	2.79%
7.	Convex Finance	Ethereum	Assets	$5.93B	-0.35%
8.	yearn.finance	Ethereum	Assets	$4.05B	6.34%
9.	SushiSwap	Ethereum	DEXes	$3.51B	-6.76%
10.	Liquity	Ethereum	Lending	$2.03B	-6.79%

ETH: ether, the cryptoasset of the Ethereum smart contract platform *Source:* Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*. Second Quarter 2021. 103(2):153-74.

Non-fungible tokens (NFTs)

- Blockchains: fungible (money) and non-fungible tokens (crypto art, patent, genome, EMR, gaming)
- NFT: unique token registered to a blockchain representing other data (image, genome, digital asset)
  - Verify authenticity and track ownership
- CryptoKitties (early NFT)
  - Ethereum smart contracts for breeding digital cats (NFTs)
    - 500,000 sold for a total of USD $40 million (Feb 2018)
  - Blockchain smart contract interoperability example
    - CryptoDragons game: own dragon NFT and feed it CryptoKitties (send the dragon contract tokens defined by the kitties contract)

“Catribute” DNA

Sources: https://www.algorand.com/resources/blog/the-importance-of-low-transaction-costs--lower-carbon; NFT valuation: https://www.linkedin.com/pulse/valuation-considerations-non-fungible-tokens-nfts-nataliya?trk=public_profile_article_view

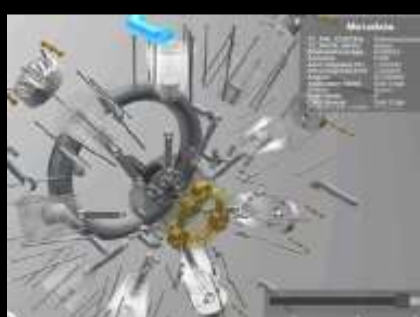
Financial infrastructure

Gaming and 3d prototyping NFTs

- Unity and Unreal engine 3d prototyping
  - Substantial source of digital asset creation
    - Virtual reality CAD-CAM prototyping, product design and test
  - Game Asset Store merchandizing (analog to the App Store)
    - Blockchain-register game engine-developed assets as NFTs
    - Plug-ins (e.g. Arkane-Unity) enable NFT contract creation
  - Model for molecular printing design exchange (Etsy + Unity + NFTs)

GAME ASSET STORE

Lightweight CAD viewer



Robotic simulation

Digital Twin software

Prototyping in VR

Sources: https://unity.com/products; Corke, G. (2019). Unity for manufacturing. *Develop 3D*. https://develop3d.com/features/unity-visualisation-vr-manufacturing-industrial-design-game-on-simulation/

Intellectual property NFTs

Etsy NFTs

- Cryptoart
  - NFT marketplaces for minting cryptoart
    - OpenSea, Rarible, Foundation
- Author rights protection
  - SIAE (Società Italiana degli Autori ed Editori), the largest copyright agency in Italy issued NFTs representing author rights, tokenizing 4.5 million rights of 95,000 member authors (Algorand) (Apr 2021)
- Genomics and pharmaceutical supply chain
  - George Church NFT genome (Oasis Network)
  - MediLedger blockchain: reduce pharmaceutical fraud
- Blockchain gaming assets
  - Characters, equipment, currency

Sources: https://www.algorand.com/resources/blog/the-importance-of-low-transaction-costs--lower-carbon; NFT valuation: https://www.linkedin.com/pulse/valuation-considerations-non-fungible-tokens-nfts-nataliya?trk=public_profile_article_view

Christie's $69 million NFT sale (2021)

- Collage created over 5,000 days by US-based digital artist Beeple
  - Political cartoons of current events
    - Themes: fear and obsession with technology, resentment and desire for wealth, political turbulence
- First purely digital artwork (NFT) offered at Christie's
    - Sold online for $69,346,250 (2021)
    - NFT as a guarantee of authenticity
    - Christie's accepting Ether payments

Everydays: The First 5,000 Days
Beeple, 2007-2020

Artworld acceptance: "Beeple is looking at his whole body of work as it is presented on Instagram as a kind of Duchampian readymade" – specialist Noah Davis

Source: https://www.christies.com/features/Monumental-collage-by-Beeple-is-first-purely-digital-artwork-NFT-to-come-to-auction-11510-7.aspx

Cryptographic primitive

Proof-as-a-feature

- Proof of result automatically built in as a feature
  - Zero-knowledge proofs (zkSNARKs, zkSTARKs)
  - Verifiable random functions (VRF) (randomness generation)
- Verifiable Random Function: function that provides publicly verifiable proof of output correctness
  - Private key holder computes the hash
  - Anyone with the public key can verify the hash
- Use cases: generate (provable) randomness
  - Used to mint NFTs (non-fungible tokens)
  - Cryptographic lottery (random selection for mining round)
  - Prevent dictionary attacks with restricted query access
  - On-chain randomness: VRF result published to blockchain for ongoing verification (Chainlink)

Cryptographic primitive

Zero-knowledge proof technologies

- Zero-knowledge proof: process in which one party (prover) proves to another (verifier) knowledge of a value (personal data) without revealing the value
  - Data verification is separate from data, private because conveys “zero knowledge” of the underlying information
  - Example: swap colored balls between hands, attester says “switched” or “not switched” without saying the color

Zero-knowledge proof systems

	Zero-knowledge proof system	Proof size	Trusted setup?	Proof time	Verification time	Quantum secure?
1	SNARKs	1.3 kB	Yes	Fast	Fast	No
2	Bulletproofs	1-2 kB	No	Fast	Not very fast	No
3	STARKs	20-30 kB	No	Not very fast	Very fast	Yes

Sources: Swan, M., dos Santos, R.P. & Witte, F. (2020). *Quantum Computing: Physics, Blockchains, and Deep Learning Smart Networks*. London: World Scientific. SNARKs (2014), bulletproofs (2018), STARKs (2018) (Ben-Sasson, 2014, 2018; Bunz, 2018)

Computational verification

- Proof system with verification built into the process
  - Elaborate computational proof structure of hash functions, Merkle paths, time-stamping; costly to create, easy to verify
- SNARK: succinct non-interactive arguments of knowledge
  - Multi-party computation: non-trusting parties conduct a computation on their own unique fragments of a larger dataset to produce an outcome, nodes have zero knowledge of the fragments held by others (requires trusted setup)
- STARK: scalable transparent argument of knowledge

Quantum secure

  - Sophisticated proof architecture based on error correction codes, random queries, and inconsistency checks
    - Fast verification time: Reed-Solomon interactive oracle proof of proximity protocol for exponential speedup in verification time, using an error-correction code based method (Ben-Sasson, 2018, p. 6)

Source: Swan, M., dos Santos, R.P. & Witte, F. (2020). *Quantum Computing: Physics, Blockchains, and Deep Learning Smart Networks*. London: World Scientific.

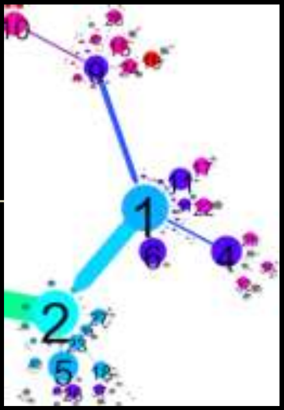
IPFS: proof of time and space

- Proof system with verification built into the process

  - Example: a worker punches a time clock every hour and submits the time-stamped records at the end of the day for verification. The supervisor does not need to check the worker's activity every hour, only confirm the oracular (third-party) output of the time punches
- PoRep (proof of replicating storage)
  - Proof of using space to store real (not random) bits over time
  - Prover performs a proof every 15 min, and sends a daily Merkle root corresponding to the proofs (100 proofs/day)
- Slow-time hash functions
  - Bona fide storage providers provide persistent file storage
  - Do not care if hashing functions operate in slow-time
    - Similar structure to 10 min bitcoin block time so enough miners can examine and confirm the block

Source: Fisch, B. (2018). PoReps: Proofs of space on useful data. ia.cr/2018/678..

STARKs (scalable transparent argument of knowledge)



- Elaborate scheme to evaluate inconsistency
  - Prover conducts a proof, and hashes the proof
    - Instantiates proof in a chain (hash-linked data structure) with the data hashed up to the Merkle root
  - Prover executes a "proof-of-work" by creating a huge temporary apparatus attesting to the internal consistency of the hash-linked data structure
    - Conducts random sampling of the proof structure via queries to an external oracle (such as a SHA-256 hash function)
    - Demonstrates that many various random Merkle paths through the data structure are internally consistent
    - Analogy to witness cross-examining: detailed questioning is designed to reveal any internal inconsistency in the story
  - Prover compresses activity to a small proof, sent to verifier

New

Source: Ben-Sasson, E. *et al*. (2018). Scalable, transparent, and post-quantum secure computational integrity. ia.cr/2018/046.

bitcoin

Bitcoin summary

Traditional functions of money
- Medium of exchange
- Store of value
- Unit of account

$

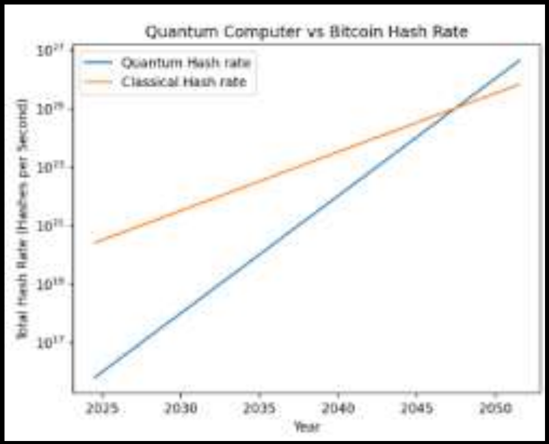
- Important planetary-scale economic technology
- Long view: currently strong, as is, persist for years, not decades unless resolve early-stage tech issues
  - Scalability, quantum upgrade path, adoption ease, trust
  - Fallacy: 13 years of transaction history = permanency
  - Money supply 89% issued and outstanding
- Price appreciation means incentive is to *hold* (store of value), not *use* cryptocurrency (medium of exchange)
- Growth in transaction size but not transaction volume
  - But sidechain, off-chain (Lightning, level 2) tx volume growth
  - Ecosystem becoming more sophisticated (stablecoins, DeFi)

Agenda

- Quantum computing
- Blockchains (cryptoeconomics)
- Quantum blockchains
- Advanced: quantum blocktime

Quantum blockchains

- Quantum blockchains
  - Blockchains using quantum methods for quantum-secure cryptography, consensus (mining), and other protocols
- Quantum threat to blockchains
  - Blockchains especially vulnerable to quantum attacks because classical cryptography (SHA-256) centrally integrated
    - Cannot simply update the crypto (QKD), protocol redesign implied
  - But, quantum blockchains are not immediately immanent (~2045e)
    - Developer facility with cryptographic models
      - Zero-knowledge proofs
      - Elliptical curve cryptography
      - Crypto-signature technologies



Sources: Swan, M., dos Santos, R.P., Lebedev, M.A. & Witte, F. (2022). *Quantum Computing for the Brain.* London: World Scientific.
Bard, D.A. *et al.* (2021). Quantum Advantage on Proof of Work. arXiv:2105.01821v1.

Quantum blockchain proposals

- Quantum money (per no-cloning rule)
- Cryptography (quantum key distribution (QKD))
  - Quantum walks, entropic uncertainty, spacetime-based (quantum secret sharing localized to spacetime)

Shor's algorithm (factoring)

	Quantum Platform
Proof of Work (PoW) (mining, consensus)	
GHZ states (Rajan) using quantum BFT (McCutcheon)	Optical
Entanglement-based PoW (Bennet)	Optical
Nonce-finding via Grover search (Bard)	General
Universal spin models (Kalinin) via Ising lattices (Cuevas)	Annealing

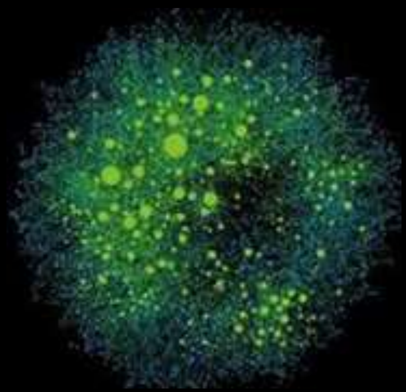
Grover's algorithm (search)

- Time-stamping: based on time entanglement
- Mining, consensus: consortium subset selection
  - Entropy (Dfinity), verifiable random functions (Algorand)

Source: Swan, M. dos Santos, R.P. and Witte, F. (2020). *Quantum Computing: Physics, Blockchains, and Deep Learning Smart Networks.* London: World Scientific.

Quantum PoW with Grover's search

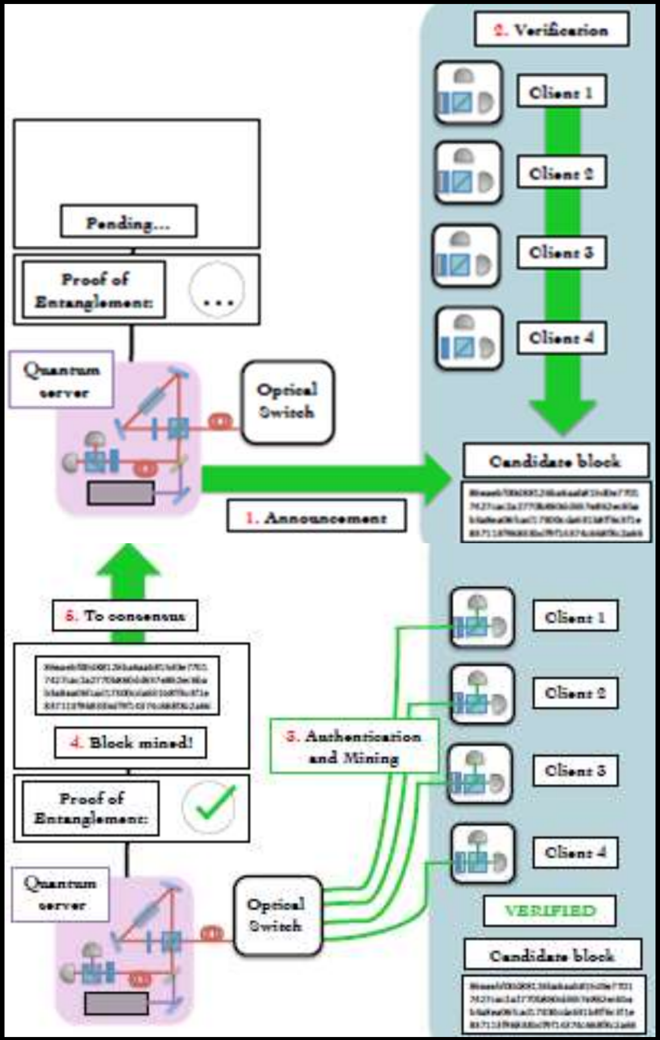
- Proof of Work: NP-complete problem (difficult to calculate, easy to verify), hence conducive to Grover's search
  - PoW miner finds a SHA-256 hash for a pre-determined string that is under a certain value
    - The hash is calculated using the block header, which is constant for a specific block, and a nonce, which is changed repeatedly by the miner, to create different hash digests in the hope of finding a digest (hash algorithm output) that meets the block requirements
  - Implication: a quantum computer with a memory register large enough to run Grover's algorithm on the necessary hash size would have a quadratic advantage over any classical device, including custom mining ASICs



Source: Bard, D.A. *et al*. (2021). Quantum Advantage on Proof of Work. arXiv:2105.01821v1.

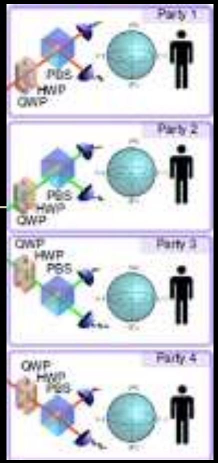
Entanglement-based PoW (greener mining)

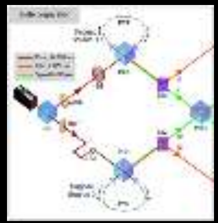
- Proof-of-entanglement mining
  - Nodes participate in an energy efficient quantum mining protocol to generate and commit entanglement towards securing a blockchain
  - Servers announce candidate blocks to a pool of clients who verify blocks against verification criteria
  - Authenticated clients participate block mining through an interactive protocol
  - Upon successful mining, the block is admitted into a consensus round for inclusion into the blockchain



Source: Bennet, A.J. & Daryanoosh, S. (2019). Energy efficient mining on a quantum-enabled blockchain using light. *Ledger*. 4(2019). arXiv:1902.09520.

GHZ state-based quantum blockchains

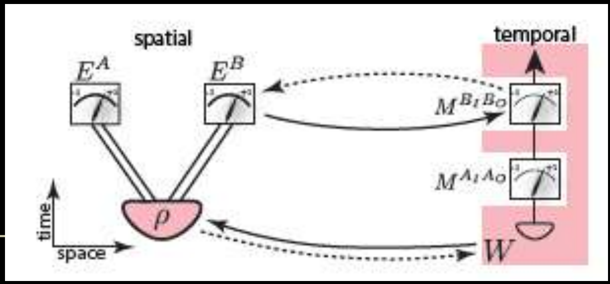




- Problem: run a blockchain on a quantum network
  - How do nodes append a valid block (BFT secure updating)
- Phase I: hash-linked data structure functionality is provided by entangled states in quantum networks
  - Classical blockchains: nodes appending a block rerun the hashing algorithms to confirm the new block is valid
  - Quantum blockchains: nodes join a GHZ state with other nodes to recieve valid block transfer (afterwhich can rerun hashing)
- Phase II: time entangled GHZ states for time-stamping
  - Crypto: QKD for cryptographic transfer
  - BFT: entangled GHZ states for node updating
  - Time-stamping: time entangled GHZ states

BFT Byzantine Fault Tolerance; *Sources:* Rajan, D. & Visser, M. (2019). Quantum Blockchain using entanglement in time. *Quantum Rep.* 1(2):1-9 using BFT updating McCutcheon, W. *et al*. (2016). Experimental verification of multipartite entanglement in quantum networks. *Nat Commun.* 7:13251.

Time entanglement



- Space and time correlations have a different structure

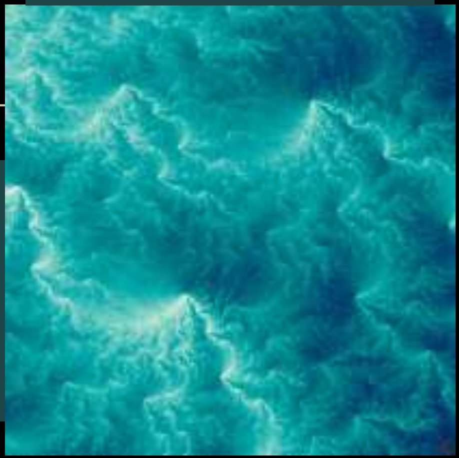
	Spatial Quantum Correlations	Temporal Quantum Correlations
1	Observed through local measurements on spatially separated quantum systems	Observed between subsequent measurements on the same system
2	Monogamy of entanglement (one entangled pair at a time); used in Quantum Key Distribution	Manipulate monogamy and polyrelational entanglement & other correlational interactions
3	Represented by operators	Represented by a number to parameterize a sequence of events

- Differences can vary based on measurement method
  - Projection vs POVM (positive-operator valued measure) of how global system measurement impacts local subsystem
- Temporal quantum correlation use cases
  - Bell (pair) states based on temporal not spatial correlation, temporal quantum computing (cluster states for one-way quantum computing), multipartite (GHZ) correlations

Sources: Ringbauer, M. *et al*. (2018). Multi-time quantum correlations with no spatial analog. *NPJ Quantum Inf*. 4:37; Costa, F. *et al*. (2018). A unifying framework for spatial and temporal quantum correlations. *Phys Rev A*. 98:012328.

Chaos, scrambling, and OTOCs

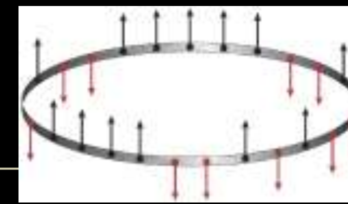
Complex Systems Tech

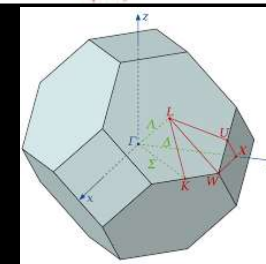


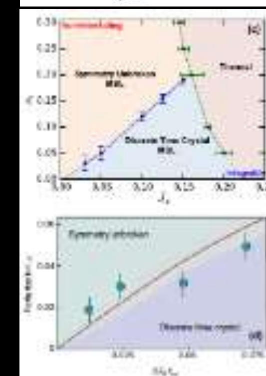
- Chaos: seemingly random states are governed by deterministic laws and sensitivity to initial conditions
- Quantum chaotic systems
  - Initial ballistic growth slows and saturates (described by the Lyapunov exponent, a quantification of the butterfly effect)
- Complex systems: often chaotic and fast-scrambling
  - E.g. brain, black hole (fast-scrambling: rapid information spread)
- Out-of-time-order correlation functions (OTOCs)
  - Evolve a quantum system backward or forward in time to apply actions and measure the system (scrambling time and chaoticity)
    - Calculate the rate of system divergence by comparing how fast two initially-commuting operators decay to become non-commuting

Source: Swingle, B., Bentsen, G., Schleier-Smith, M. & Hayden, P. (2016). Measuring the scrambling of quantum information," *Phys Rev A*. 94:040302.

Discrete time crystals







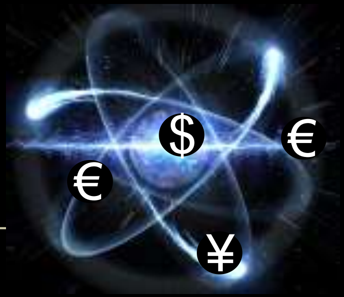
Spacetime crystals and superfluids

- Crystal: repeating structure (lowest-energy configurations are periodic)
  - Space crystal: repeating structure in space
  - Time crystal: repeating structure in time
    - Floquet time crystal: time translation symmetry breaking model with phase winding (event times through a common interval)
    - Floquet periodicity: orbit-bifurcation temporal structure
  - Spacetime crystal: repeating structure in space & time
- Discrete time crystals: novel material phases that do not reach thermal equilibrium (quantum memory)
  - Low-energy physics explains emergent behavior of superconducting strange metals (non-Fermi liquids)
    - Superfluid: fluid with zero viscosity which flows without loss of kinetic energy (quantum computing and quantum gravity)

Sources: Lin, H.W., Maldacena, J. & Zhao, Y. (2019). Symmetries Near the Horizon. J High Energ Phys. 08:049. Else, D.V. *et al*. (2021). Non-Fermi liquids as ersatz Fermi liquids: general constraints on compressible metals. arXiv:2007.07896v4. Monroe laboratory: Zhang, J. *et al*. (2016) Observation of a Discrete Time Crystal. *Nature*. 543:217-20.

Quantum blockchains application

Quantum finance and econophysics



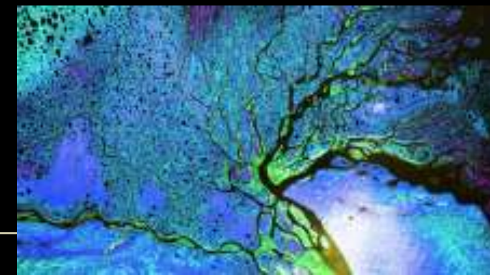
Chern-Simons topological invariants

- Quantum finance: quantum algorithms for portfolio optimization, risk management, option pricing, and trade identification
- Model markets with physics: wavefunctions, gas, Brownian motion

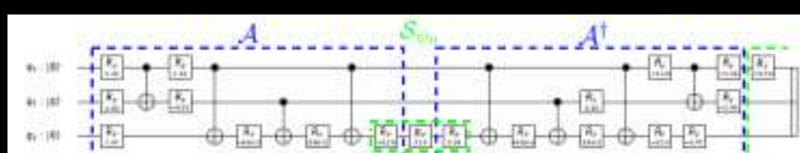
Ref	Application Area	Project	Quantum Method	Classical Method	Platform
1	Portfolio optimization	S&P 500 subset time-series pricing data	Born machine (represent probability distributions using the Born amplitudes of the wavefunction)	RBM (shallow two-layer neural networks)	Simulation of quantum circuit Born machine (QCBM) on ion-trap
2	Risk analysis	Vanilla, multi-asset, barrier options	Quantum amplitude estimation	Monte Carlo methods	IBM Q Tokyo 20-qubit device
3	Risk analysis (VaR and cVaR)	T-bill risk per interest rate increase	Quantum amplitude estimation	Monte Carlo methods	IBM Q 5 and IBM Q 20 (5 & 20-qubits)
4	Risk management and derivatives pricing	Convex & combinatorial optimization	Quantum Monte Carlo methods	Monte Carlo methods	D-Wave (quantum annealing machine)
5	Asset pricing and market dynamics	Price-energy relationship in Schrödinger wavefunctions	Anharmonic oscillators	Simple harmonic oscillators	Simulation, open platform
6	Large dataset classification (trade identification)	Non-linear kernels: fast evaluation of radial kernels via POVM	Quantum kernel learning (via RKHS property of SVMs arising from coherent states)	Classical SVMs (support vector machines)	Quantum optical coherent states

VaR: Value at Risk a quantile of the loss distribution (a widely used risk metric); conditional VaR
POVM: positive operator valued measure; RKHS: reproducing kernel Hilbert space

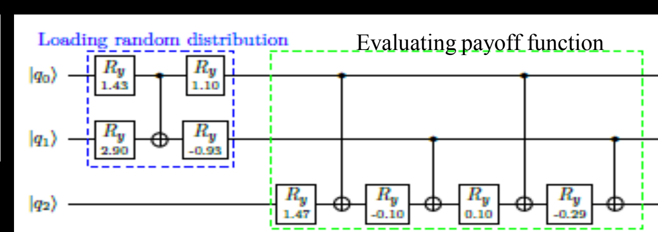
Quantum finance (references)



1. Alcazar, J., Leyton-Ortega, V. & Perdomo-Ortiz, A. (2020). Classical versus Quantum Models in Machine Learning: Insights from a Finance Application. *Mach Learn: Sci Technol*. 1(035003). arXiv:1908.10778v2.
2. Stamatopoulos, N., Egger, D.J., Sun, Y. *et al*. (2020). Option pricing using quantum computers. *Quantum*. 4(291). arXiv:1905.02666v5.
3. Woerner, S. & Egger, D.J. (2019). Quantum risk analysis. *npj Quantum Information*. 5(15). arXiv:1806.06893v1.
4. Bouland A., van Dam, W., Joorati, H. *et al*. (2020). Prospects and challenges of quantum finance. arXiv:2011.06492v1.
5. Lee, R.S.T. (2020). *Quantum Finance: Intelligent Forecast and Trading Systems*. Singapore: Springer.
6. Chatterjee, R. & Yu, T. (2017). Generalized Coherent States, Reproducing Kernels, and Quantum Support Vector Machines. *Quantum Information and Communication*. 17(1292). arXiv:1612.03713v2.



Quantum amplitude estimation circuit for option pricing
Source: Stamatopoulos (2020).



Quantum blockchains application

Quantum BCI (brain computer interface)

- Technological advance suggests whole-brain modeling
  - Connectome mapping, molecular-scale imaging
  - Quantum neuroscience needed for
    - Multiscalar data processing (brain network-neuron-synapse tiers)
    - Wave function modeling, neural signaling, synaptic integration

Neural entities and quantum computation: 86 billion neurons and 242 trillion synapses are within reach in the big data era of available cloud services quantum computing

	Level	Estimated Size	
1	Neurons	86×10^9	86,000,000,000
2	Glia	85×10^9	85,000,000,000
3	Synapses	2×10^{14}	242,000,000,000,000
4	Avogadro's number	6×10^{23}	602,214,076,000,000,000,000,000
5	19 Qubits (Rigetti-available)	2^{19}	524,288
6	27 Qubits (IBM-available)	2^{27}	134,217,728
7	53 Qubits (Google-research)	2^{53}	9,007,199,254,740,990
8	79 Qubits (needed at CERN LHC)	2^{79}	604,462,909,807,315,000,000,000

Source: Swan, M., dos Santos, R.P., Lebedev, M.A. & Witte, F. (2022). *Quantum Computing for the Brain.* London: World Scientific.

Brain computer interface (BCI)

- Brain computer interface (BCI): connection between a brain and an external device

BCI technology	Equipment mode	Functionality
Core BCI (brain-computer inferface)	Non-invasive (external) or invasive (implanted) electrode array	Basic use case: prosthetic limb and cursor control
Cloudmind B/CI (brain/cloud interface)	On-board ecosystem of medical neuronanorobots	Advanced used case: health monitoring, information access, collaboration, fun

- BCI aim: productivity, well-being, and enjoyment
  - Short-term: map, monitor, and enhance health (prevent condition onset)
    - Example: neuronanorobots provide directed electrical stimulus to the brain to dissolve blood clots using ultrasound
  - Long-term: enable new physical and mental capabilities (Euclidean+ spacetime)

	B/CI function	B/CI metric	Maslow tier	Objective
1	Map personal connectome	Energy, glucose, oxygen, ATP	Maslow 1	Physiological survival
2	Monitor homeostasis	Neurotransmitter balances	Maslow 2	Psychological well-being
3	Cure pathologies	Ideas, neurotransmitters, energy	Maslow 3	Self-actualization
4	Enhance neural activity	Ideas, new cloudmind design	Beyond-Maslow	New levels of achievement

Sources: Martins *et al*. (2019). Human Brain/Cloud Interface. *Front. Neurosci*, 13(112):1-24. Marosfoi *et al*. (2015). Shear-Activated Nanoparticle Aggregates Combined with Temporary Endovascular Bypass to Treat Large Vessel Occlusion. *Stroke* 46(12), 3507-13.

Neuronanorobots and nanorobots

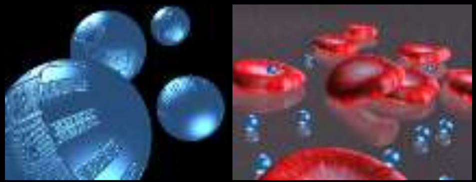
- Coordinate nanorobot fleets blockchain (quantum BCI)
- Neuronanorobots (1:1 correspondence)
  - Axonal endoneurobot (axons)
  - Synaptobot (synapses)
  - Gliabot (glial cells)
- Standard proposed medical nanorobots
  - Respirocytes (artificial red blood cells (RBC))
  - Clottocytes (artificial platelets)
  - Microbivores (artificial phagocytes)
  - Chromallocytes (chromosome replacement)
  - Toothbot (plaque and stain removal)
- Nanorobot size: ~1,000 nm

Axonal endoneurobot

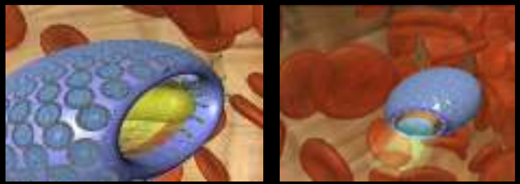
Synaptobot

Gliabot

Respirocytes (artificial RBC)



Microbivore (artificial immune cell)

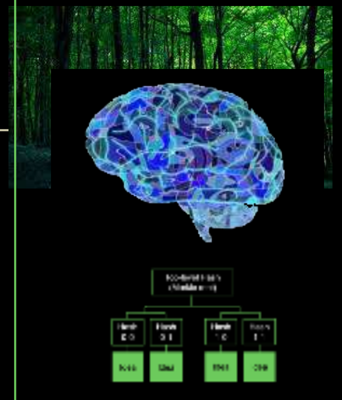


Sources: Martins *et al*. (2019). Human Brain/Cloud Interface. *Front Neurosci.* 13(112):1-24.
Freitas Jr., Robert A. (2000, 2005, 2012). http://www.imm.org.

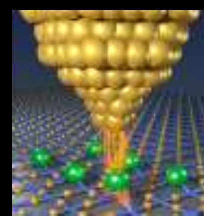
Quantum BCI

- Quantum BCI: quantum-instantiated BCI
  - Quantum BCI partner for memory backup, restore, revive, monitor and neuronanorobot coordination
- Software: quantum blockchain brain DAC
  - Security, automation, multiscalar coordination
  - PDE mathematics to model neural signaling (waves)
  - Quantum blocktime as the native compute-time regime
    - Enhancement opportunities per non-Euclidean spacetime
- Hardware: print quantum BCIs with molecular manufacturing (atomically-precise nanofab)
- Cryogenic temperatures: superconducting and suspension
  - Instantiate copy of suspended brain as quantum brain DAC with superconducting phase transitions as neural signals

Quantum BCI DAC



Atomically-precise molecular manufacturing



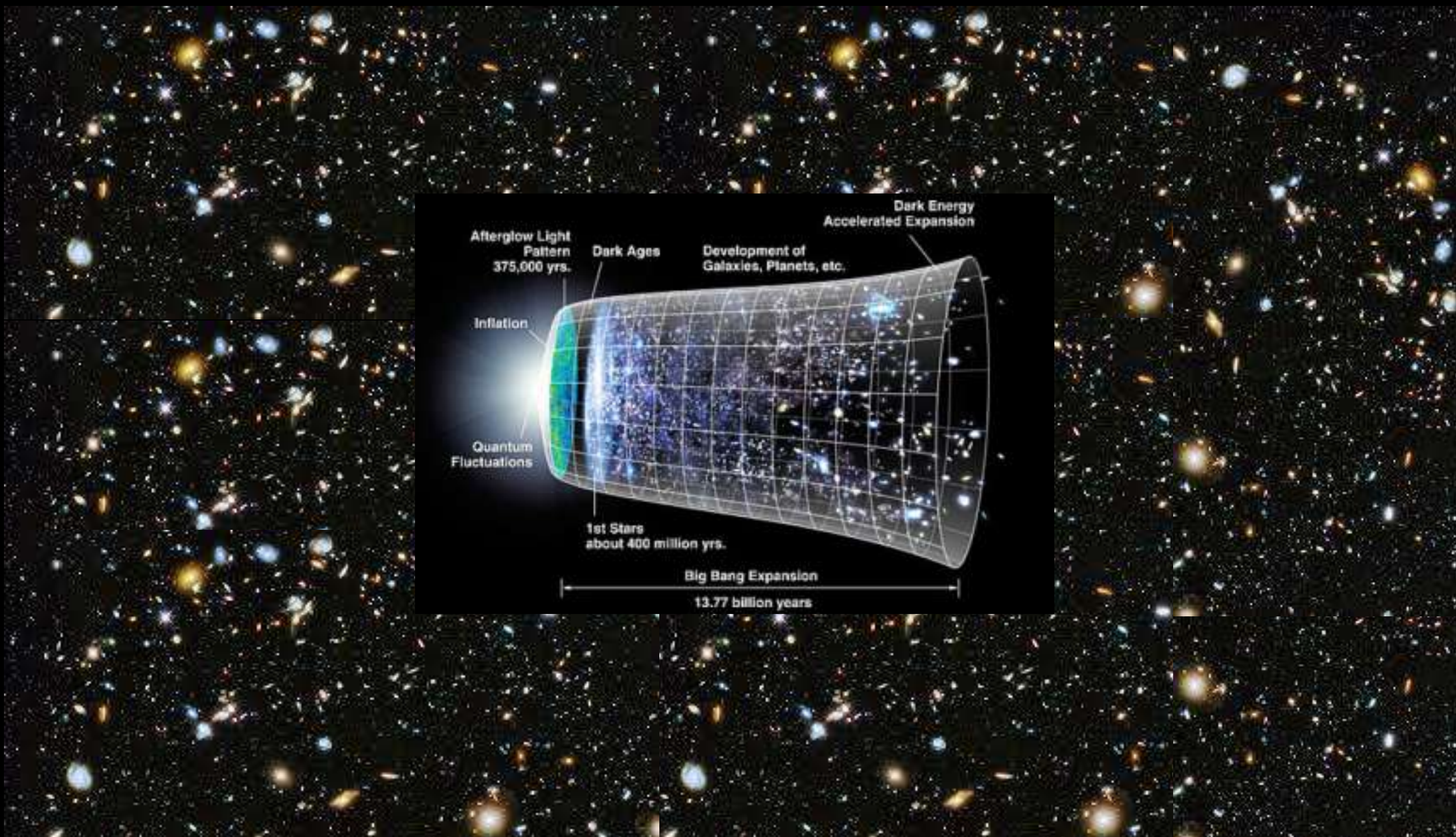
PDE: partial differential equation (multiple unknown variables)

Source: Swan, M. dos Santos, R.P., Lebedev, M.A. and Witte, F. (2022). *Quantum Computing for the Brain.* London: World Scientific.

Agenda

- Quantum computing
- Blockchains (cryptoeconomics)
- Quantum blockchains
- Advanced: quantum blocktime

Space



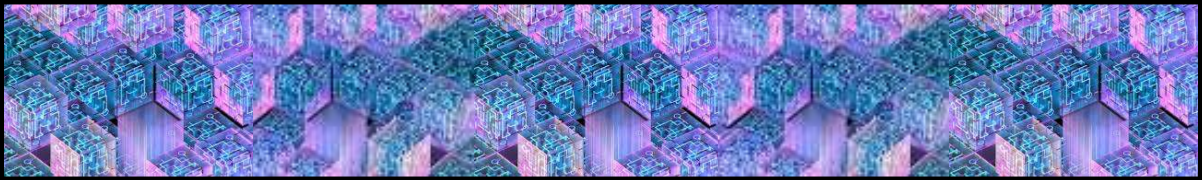
Dark Energy
Accelerated Expansion
Afterglow Light
Pattern
375,000 yrs.
Dark Ages
Development of
Galaxies, Planets, etc.
Inflation
Quantum
Fluctuations
1st Stars
about 400 million yrs.
Big Bang Expansion
13.77 billion years

- # Our futures

Inspiration of the Sea	Inspiration of the Road	Inspiration of Space
Melville, Conrad 1851	Kerouac 1957	Musk-Bezos-Branson 2000-2050e
		
Baleinier au Mouillage (Whaler at anchor), Henri Durand-Brager, 1814-79	Whole Earth Catalog, sign off issue, Stewart Brand, 1971	100th Mission Launch, SpaceX, Florida SpaceCoast, April 2021

Quantum blockchains in space

- Beyond planetary expansion
- Space has diverse time and space regimes
- The technology we use in space must likewise accommodate diverse time and space regimes
  - Secure communications technology
    - Extra-planetary quantum photonic networks
  - Smart network automation and economic technology
    - Quantum blockchains
      - With its own formal time regime, blocktime
      - In the quantum instantiation, quantum blocktime



Time

The whole idea of "time" is just an approximation anyway
– physicist Sean Carroll, *The Big Picture*, 2016, p. 198

- Most frequently used noun in the English language
  - Does not pick out a real feature of the universe and cannot be perceived directly
  - Universal illusion in constant everyday use
- Scientists generally think time is "real" but differ regarding its emergence and progression
  - Problem: unscientific opinion-based domain
- Native temporal regimes
  - Physical theories
  - Neural faculties
  - Technologies

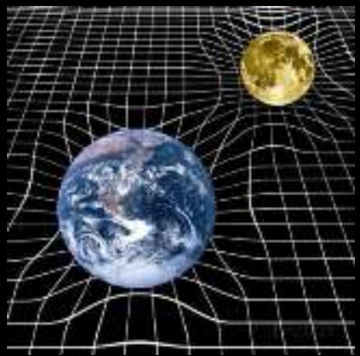
Source: Carroll, S. (2015). The Reality of Time. The Preposterous Universe blog, 2015 (April 3, 2015). https://www.preposterousuniverse.com/blog/2015/04/03/the-reality-of-time/

General relativity and quantum mechanics

- The "Problem of Time"
  - Incompatibility: the two marquis theories describing the physical world operate with different time and space regimes
  - Quantum mechanics (the Schrödinger wavefunction)
    - Formulated in the background of the Newtonian framework of absolute time and space
  - General relativity
    - Based on Riemannian curved geometry in a time and space that can twist and fluctuate in a more dynamical and sophisticated way

Quantum Mechanics

Particles (small light objects)



General Relativity

Planets (large heavy objects)

Source: Barbour, J. (2009). The Nature of Time. arXiv: 0903.3489.

Euclidean and non-Euclidean spacetime

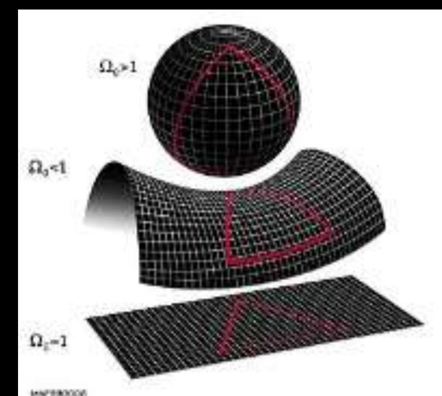
- Euclidean geometry (everyday)
  - Triangle angles sum to 180°
- Non-Euclidean geometry (space)
  - Positively-curved space: sphere (e.g. the Earth)
    - Triangle angles sum to greater than 180°
  - Negatively-curved surface: saddle or mountain pass
    - Triangle angles sum to less than 180°
  - Example: general relativity
    - How mass and energy bend the curvature of spacetime

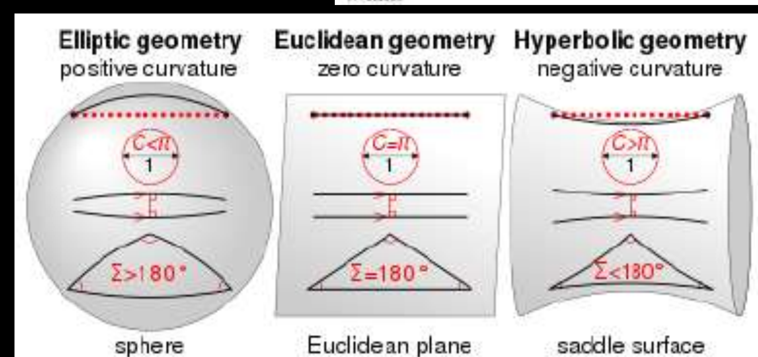
Great Barrier Reef (hyperbolic plane)

Elliptic geometry (positively-curved)

Hyperbolic geometry (negatively-curved)

Flat geometry (no curvature)





Towards physical law compatibility

- Problem
  - GR and QM are not interoperable (re: time and space regimes)
  - Euclidean and non-Euclidean spacetimes
- Requirement: relate GR-human-QM time regimes
  - Operate in domains with relativistic and quantum effects
    - Further expansion into space, study of black holes, dark energy & dark matter, early universe inflation

<u>Problem of Time (Philosophy)</u>
Kant's *Critique of Pure Reason* 1781
Time and space: ideal and real nature
Same problem: integrate diverse temporal regimes, via faculty-specific time domains

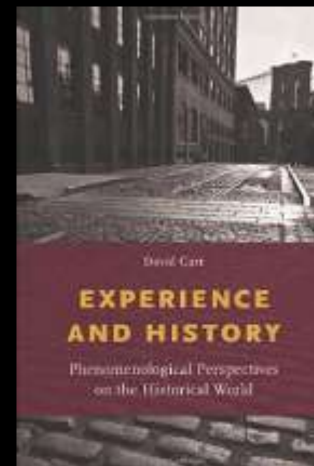
General Relativity: infinite magnitude Non-Euclidean spacetimes	Sensibility: infinite magnitude (GR)
Human Scale: everyday reality Euclidean spacetime	Understanding: line-drawing (human)
Quantum Mechanics: multiplicity and simultaneity	Reason: multiplicity (QM)

GR: general relativity; QM: quantum mechanics
Source: Swan, M. (submitted). Kant's Transcendental Dialectic: The Time of Reason.

Human time regimes

Problem: How can we make more time?

- Human time
  - One-way arrow, continuous, regular, periodic, inexorable advance
    - Fixed endpoints: birth and death
- "Make more time" by accessing events in other temporal trajectories
  - History as a form of time parallelism
    - A series of past events that we share but did not live directly
  - Literature: alternative event series
  - Photos of someone's travel voyage
    - Social media lifestreams: Facebook, Twitter, Instagram, YouTube, TikTok



Khafre's Pyramid and Great Sphinx of Giza (2500 BCE)

Source: Carr, D. (2014). *Experience and History: Phenomenological Perspectives on the Historical World.*

Compute time regimes

- Compute-time of technology
  - Clocktime eras stop, reverse, manipulate time: malleable, interruptible, multi-regime
    - Variable clocktime speeds, start and stop, wait for an event, repeat (while loop), reverse and go backwards, run faster or slower, operate in a “no time” regime (unmarked by events)
  - Explosion in classes of compute technology
    - Each could have a unique temporal and spatial regime specific to its activities
      - BCIs (brain-computer interfaces), personal robotics, drones, IoT (Internet of Things), quantified self wearables, smart city sensors, self-driving vehicles, factory automation, big data analytics, deep-learning neural nets

Source: Swan, M. Rethinking Authority With The Blockchain Crypto Enlightenment. Response to The Edge Question 2016: What do you consider the most interesting recent news? What makes it important? John Brockman, Ed., 2016.

Blocktime

- Blocktime: the compute-time of blockchains
  - Technology operates on the basis of its own native time regime
- Forms of blocktime
  - Block time unit: average time to add a new block to the chain
    - Bitcoin ~10 min so enough miners have time to confirm
  - Blockheight: total number of blockchain blocks (Btc 700,000 Sep 2021)
    - New software updates go into effect at certain a blockheight
- Blocktime examples (self-contained technology program operates per its own time regime)
  - Miner rewards paid 100 blocks after block is added (~17 hours)
  - Mining difficulty changed every 2016 blocks (~2 weeks)
  - Block reward halving every 210,000 blocks (~4 years)
  - Time lock: restricted time period: escrow, check-dating
  - Time arbitrage opportunities between FiatFi and DeFi

Bitcoin: ~10 min
Ethereum: ~10 sec

FiatFi and DeFi: fiat finance and decentralized finance

Temporality regimes

- Human-time: continuous biological time
- Compute-time: manipulatable time
  - Blocktime: compute-time of blockchains
- Time is indexical: every technology has a de facto compute-time conducive to the event cycles and schedule of its activities
  - Blocktime is an early example of formalizing and incorporating the native compute-time of the technology into its operations
  - Implication: time multiplicity
    - Native compute-time domains made explicit in other smart network technologies (e.g. deep learning nets with predictive future modeling)

Quantum blocktime

- Quantum blocktime: the compute-time of quantum blockchains, which is quantum computational
- Quantum computational time formulations
  - Based on quantum mechanics
    - Traditional construction of Schrödinger wavefunction in the background of absolute time and space (Newton)
    - More recent discoveries of time entanglement, information scrambling, chaotic ballistic spread and saturation cycles, discrete time crystals, Floquet periodicity, spacetime superfluids, OTOCs (out of time order correlation functions)

Source: Swingle, B., Bentsen, G., Schleier-Smith, M. & Hayden, P. (2016). Measuring the scrambling of quantum information. *Phys Rev A*. 94:040302.

Quantum blocktime

- Quantum computing time formulations include
  - Quantum mechanics: via operation
  - Human-scale: human interpretable results (upon measurement)
  - General relativity: via the information perspective
- Information perspective (classical and quantum)
  - Entropy measure of system state
    - Information qu(bits) required to send a system state
  - Unified picture of problem domains that have aspects of both general relativity and quantum mechanics
    - Black hole information paradox (AdS/CFT, complexity)
      - Entanglement status of outward-evaporating Hawking radiation
    - Quantum relativistic information (gravitational waves, inflation)

Sources: Harlow, D. & Hayden, P. (2013). Quantum computation vs. firewalls. *J High Energ Phys*. 1306:85. Maldacena, J. (1999). The large N limit of superconformal field theories and supergravity. *Intl J Theor Phys*. 38(4):1113-33.

Quantum blocktime

Multi-time interface

- Result: quantum computing, as an information domain, integrates GR-human-QM time regimes
- Quantum blockchains as the technology platform
  - Implements diverse time regimes
  - Has its own native time formalizations via quantum blocktime
    - Blockchain events: rewards, difficulty adjustment, updates
    - Quantum blockchain events: energy-time (frequency) Heisenberg uncertainty principle trade-off variables, entanglement, superposition, quantum walks, teleportation, quantum contracts
- Alternative time paradigm (multi-time interface)
    - Alternative Euclidean time regimes (history, literature, social media) make “more time” by accessing unlived trajectories
    - Alternative non-Euclidean time regimes make “more time” by accessing different time regimes

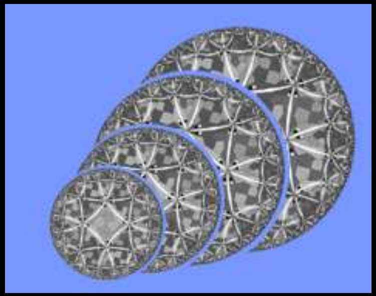
Sources: Harlow, D. & Hayden, P. (2013). Quantum computation vs. firewalls. *J High Energ Phys*. 1306:85. Maldacena, J. (1999). The large N limit of superconformal field theories and supergravity. *Intl J Theor Phys*. 38(4):1113-33.

Quantum blocktime applications

Quantum BCI

Quantum BCI

- Quantum blocktime as the native compute-time of the quantum BCI
  - Port the brain to another time dimension, literally
  - Instantiate thinking in non-Euclidean spacetime
    - Positive-curvature elliptic geometry (sphere)
    - Negative-curvature hyperbolic geometry (AdS/CFT correspondence)
  - Implications
    - Test AdS/Brain quantum neuroscience multiscalar model of neural signaling (network-neuron-synapse-molecule)
    - Potential novel enhancement opportunities
    - Explore superpositioned consciousness
      - Test quantum cognition hypotheses (Penrose)



AdS/Brain: quantum neuroscience multiscalar neural field theory

Source: Swan, M. dos Santos, R.P., Lebedev, M.A. and Witte, F. (2022). *Quantum Computing for the Brain.* London: World Scientific.

Thought tokening

- Thinking functionality as an overlay
  - AI deep learning nets
    - Pattern recognition (sound, image, object, face)
    - Concept identification (tennis game)
    - Generative learning (make new samples)
  - Quantum AI deep learning nets
    - Born machines replace Boltzmann machines
      - Output interpretation of loss function based on Born rule
  - Thought-tokening overlay for computational “thinking”
    - Thinking as a rule-based activity
      - Word-types: universals, particulars, indexicals
      - Encoded into a formal system as thought-tokens, registered to blockchains

Existing

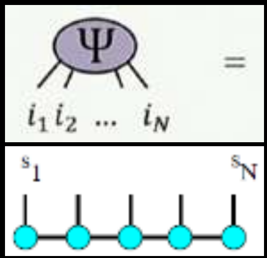
New

Source: Cheng, S., Chen, J. & Wang, L. (2018). Information perspective to probabilistic modeling: Boltzmann machines versus Born machines. *Entropy*. 20:583.

Quantum blockchains in space

Index Tech

Tensors are indexical



- Smart network technologies needed for next steps in beyond planetary expansion into space
  - Indexicality tools: persistent form, fillable content
    - Tensor networks: canonical quantum index technology
      - Treat dimensions as indices (expand and contract)
- Quantum blockchain (blocktime) applications
  - Multi-time interface
    - Quantum blockchains in space application
      - Integrate GM-human-QM time, and Euclidean and non-Euclidean time regimes for interoperability
  - Tokenized thinking
    - Quantum blockchains in space application
      - Tokenized thinking automation technology for asteroid mining and space settlement; thought-tokening adds an intelligence layer

Time is indexical

Thinking is indexical

Status

Blockchains in space

- Secure comms and extra-planetary economic system
- European Space Agency Space 4.0 vision:
  - A sustainable space sector connected with the global economy using DLT (distributed ledger technology) applications for payments, procurement, supplier agreements, and automated smart contracts
- Applications (ESA Space 4.0, NASA SensorWeb)
  - Financing and smart contract trustless execution
  - Supply chain management (provenance blockchains)
  - Networking and communications, traffic management
  - Identity and intellectual property rights management
- Space-as-a-service (SpaceChain) SPACECHAIN
  - 2019 Bitcoin demo in space, Jun 2021 Ethereum launch

NASA SensorWeb: interoperable satellite sensors

Sources: Torben, D. (2017). Distributed Ledger Technology Leveraging Blockchain for ESA's Success. ESA HQ: Strategy Department; Jones, K.L. (2020). Blockchain in the Space Sector. The Aerospace Corporation space consultancy. https://www.aero.org

Agenda

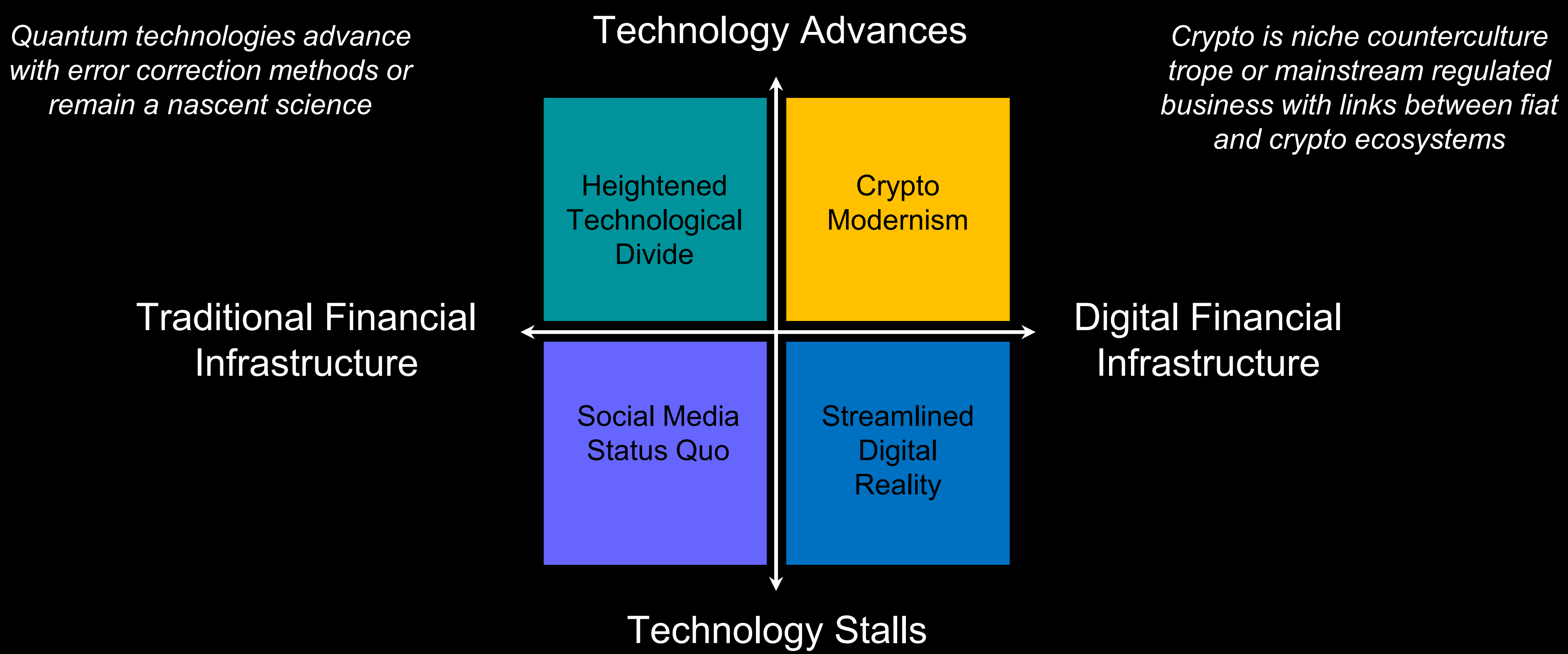
- Quantum computing
- Blockchains (cryptoeconomics)
- Quantum blockchains
- Advanced: quantum blocktime

Thesis

Quantum blockchains are practically, a smart network automation technology, and theoretically, a tool for considering the problem of time

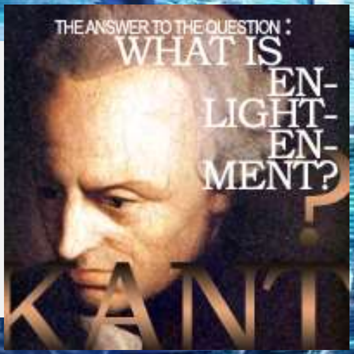
Quantum blockchains future scenarios

- Two biggest drivers: technological advance and implementation of digital financial infrastructure

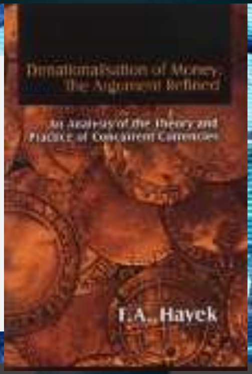


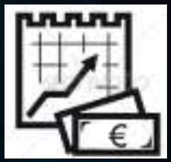
Source: GBN (Global Business Newtork) Scenario Planning technique

“One ought to think autonomously, free of the dictates of external authority” - *Immanuel Kant*



“Multiple private currencies should compete for customer business”
- Friedrich Hayek





cryptocitizen.

Crypto modernism sensibility

- Societal rights and responsibilities

Ancient Greece

Vote, participate in public discourse

Crypto Modernism

Vote, participate in public discourse, provide citizen-contributed infrastructure, maintain self-sovereignty in use of capital and other activities

Source: Becoming Self-Sovereign: How to Set Up a Bitcoin Node, With Lightning
https://www.coindesk.com/tech/2020/12/15/becoming-self-sovereign-how-to-set-up-a-bitcoin-node-with-lightning/

The Crypto Enlightenment

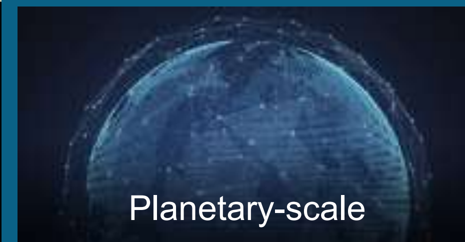
- The emergence from self-imposed tutelage in the context of money and economic life (Kant)
- "Wealth of planets" (Adam Smith)
  - Network-based digital economies
  - Worldwide and eventually extra-planetary trading systems
    - Ships
    - Trains
    - Airplanes
    - Internet (e-commerce)
    - Blockchains

The Quantum Enlightenment

- Kardashev-plus society marshalling all tangible and intangible resources
  - News, information, entertainment (internet)
  - Money, economics, and finance (blockchain cryptoeconomics)
  - Neuroscience, genomics, peak health maintenance (CRISPR, BCI, DNA sequencing, anti-aging prevention)
  - Molecular manufacturing (3d nanofabrication of matter)
- Aim: improved quality of life and greater capacity realization in intelligence, well-being, and enjoyment

<u>Citizen Sensibility</u>

The Quantum Citizen (quantum networks) 2020s+



The Global Information Citizen (internet) 1990s

The Global Economic Crypto Citizen (blockchains) 2000s

The Global Genomic Citizen (CRISPR, genomics, anti-aging) 2010-2020s

The Global Molecular Citizen (3d atomic nanofab printing) 2020-2050s

Conclusion

Digital news	Green dot	Low sensitivity
Digital money	Yellow dot	Medium sensitivity
Digital brains	Red dot	High sensitivity

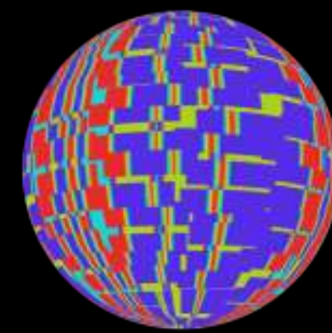
- Blockchains
  - Large-scale economic technology
  - Cryptography-rich software (proof technology built-in)
  - Blockchain 1.0: Currency
  - Blockchain 2.0: Contracts
    - Digitize existing financial infrastructure with blockchains
    - Economic system incentives (digital institutions as a public good)
  - Blockchain 3.0: Beyond financial market applications
    - Space, genomics, supply chain
- Quantum computing
  - High-profile worldwide scientific endeavor (security, policy)
    - Multiple platforms available via cloud services
    - Core infrastructure development: algorithms, hardware, apps

Conclusion

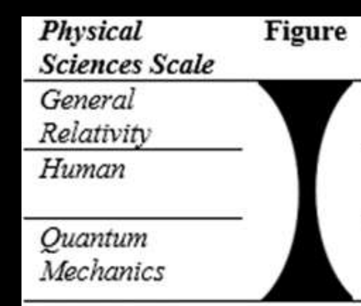
- Quantum blockchains
  - Smart network automation technology for advanced projects
    - Tracking, automated execution (smart contracts), remuneration, voting, multilevel system coordination
    - Other smart network technologies: CRISPR, BCIs, deep learning nets, molecular manufacturing, IoT
  - Emblematic direction of smart network technologies
    - Quantum computing instantiation
    - Quantum photonic network instantiation
      - Global photonic networks: internet revolution
      - Global quantum photonic networks: quantum revolution
    - Native compute-time regimes for event denomination
    - Tokenized thinking as intelligence overlay
    - Cryptographic self-verification proof mechanisms

Conclusion

- Foundational physics discoveries re: time are being deployed in compute technologies
  - Quantum information time formulations
    - Time entanglement, discrete time crystals, Floquet periodicity, OTOCs (out of time order correlation functions), quantum teleportation, information scrambling, spacetime superfluids
- Time regimes become interoperable via compute-time formalizations
  - Physical theories: GR-human-QM
- Quantum photonic networks
  - Optical domain, qudits, GHZ multipartite entanglement, indexicality



Possible Planck-scale lego-like assembly of time and space



Risks and limitations

- Error correction stalls
  - Unable to progress from ~100-qubit to million-qubit machines
- Quantum technology cycle too early
  - QPUs do not roll-out through worldwide semiconductor supply chains
- Materials discovery stalls
  - Cannot find/make room-temperature superconductors
- Limitations of underlying physical theories
  - Slow pace of quantum algorithm discovery
- Social adoption and alienation
  - Lack of interest in implementing intensive technologies

QPU: Quantum Processing Unit. *Sources:* Swan, M., dos Santos, R.P., Lebedev, M.A. & Witte, F. (2022). *Quantum Computing for the Brain.* London: World Scientific. Preskill, J. (2021). Quantum computing 40 years later. arXiv: 2106.10522.

Crypto science fiction

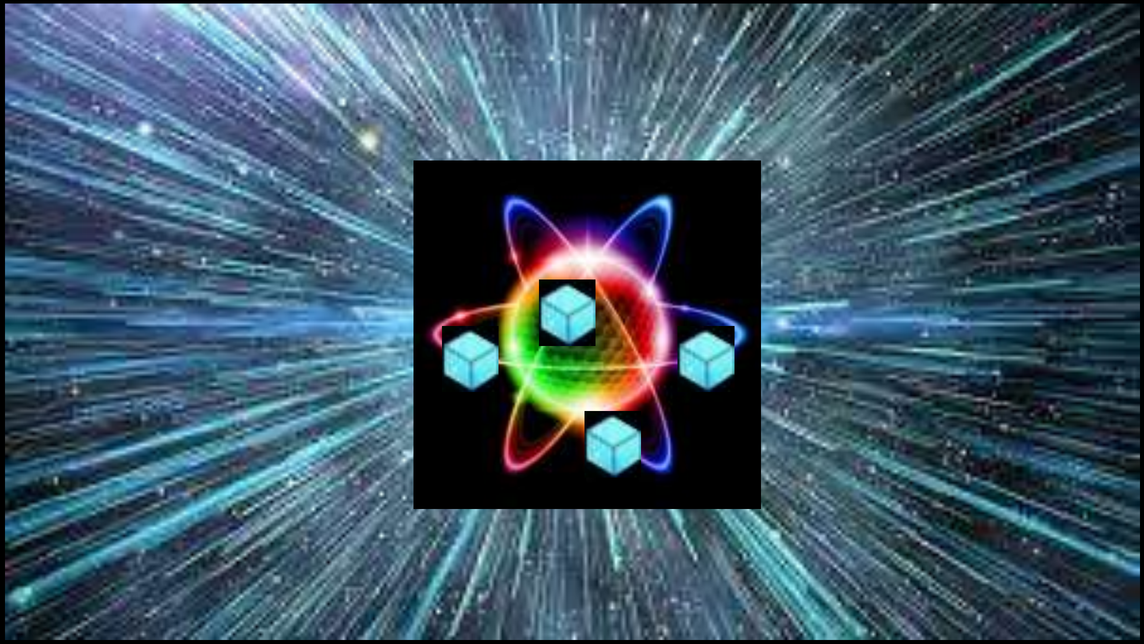
- Schroeder: corporations replaced by AI DACs
- Robinson: crypto climate policy fiction
    - Carbon coin: one coin per ton of carbon-dioxide-equivalent sequestered from the atmosphere, but centrally administered by a world central bank
- Stross: interstellar economic expansion
    - Graeber's *Debt*, for the next 5,000 years
    - Slow-medium-fast money, time, information
        - 3 kinds of money in China (2200-771 BC): superior (pearls & jade), middle (gold), lower form of payment (knives & spades)
    - Neural blockchains
        - Crypto identity verification signed with the hash of a mind state vector at a certain time
        - Memory palace (on a detachable brain drive)
        - Self-defined "truffle pig" augmentation capabilities

2019

2020

Source: Stross, C. (2013). *Neptune's Brood*. New York: Penguin. in some sense, a science fiction implementation of Graeber, D. (2011). *Debt: The First 5,000 Years*. Brooklyn NY: Melville House Publishing.

Thank you! Questions?



Quantum Blockchains

Cryptography, entanglement, and quantum blocktime

"[T]he technology for the control of complex quantum many-body systems is advancing rapidly, and we appear to be at the dawn of a new era in physics"
– physicist Leonard Susskind, 2019

San Jose CA, November 20, 2021

Slides: http://slideshare.net/LaBlogga

Melanie Swan, MBA, PhD
Quantum Technologies
UCL Centre for Blockchain Technologies

UCL CBT Singularity UNIVERSITY

Quantum blockchain jokes

That's the t|ket>

- Heisenberg to policeman
  - No, I don't know how fast I was going, but I know where I am (I am certain of that)
- A neutron walks into a bar
  - For you, no charge
- A quantum particle walks into two bars
- One particle to another
  - "I lost an electron" "How can you tell?" "I feel positive"
- What did the Valley Girl physicist say?
  - "Like, gauge me with a stick"
- Kondo problem (condensed matter) or
  - Condo problem: apartment or condo living?
- Hello sports fans~!
  - "MBL" not MLB – many-body localization
  - "NFL" the other "NFL" – non-Fermi liquid

Quantum Mechanics

- How many miners does it take to change a lightbulb?
  - 1, but 99+ to compete for it and check the work
- Blockchain-registered digital images of Gandalf?
  - Non-fungible Tolkiens
- Where do Eskimos keep their Bitcoin?
  - In a cold wallet
- Why is the Bitcoin difficulty so high?
  - Too much hash (power)
- What did the Valley Girl quantum crypto-trader say?
  - "Uh, I'm so Shor" (Shor's algorithm)

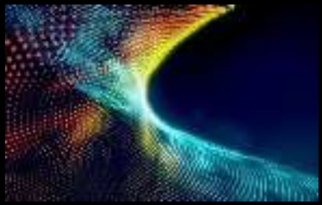
Blockchain

How many Horodeckis does it take to….

- Formalize an entanglement witnessing protocol?
  - 4: Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. (2009). Quantum entanglement. *Rev Mod Phys*. 81(2):865
- Define a teleportation protocol with Bell's inequalities?
  - 3: Horodecki, R., Horodecki, M. & Horodecki, P. (1996). Teleportation, Bell's inequalities and inseparability. arXiv: 9606027
- Propose a quantum entanglement distillation protocol?
  - 2: Horodecki, M. & Horodecki, P. (1998). Reduction criterion of separability and limits for a class of protocols of entanglement distillation. arXiv: 9708015
- Define quantum mixed state separability criterion?
  - 1: Horodecki, P. (1997). Separability criterion and inseparable mixed states with positive partial transposition. *Phys Lett A*. 232:333

Entropic uncertainty use case

Certified deletion



Appendix

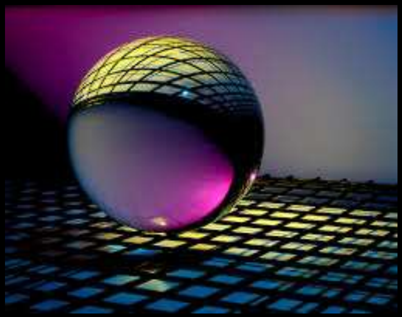
- Certified deletion: prove information has been deleted
- Enabling feature
  - Classical information is measured in the 0/1 basis whereas quantum information can be measured in an orthogonal basis (plus-minus spins, +1/-1, vertical-horizonal polarizations)
- Example: two parties have classical information that one party would like deleted (e.g. an old copy of a will)
  - Step 1: Deleting party (lawyer) creates an amalgam of the classical information with random quantum information (by interspersing qubits into the classical bitstring)
    - Result: classical content and quantum content become entangled, such that measuring information about the qubit side provides information about the classical side, namely whether the classical bits are random or coherent (the will)

Source: Broadbent, A. & Islam, R. (2020). Quantum encryption with certified deletion. arXiv:1910.03551v3.

Entropic uncertainty use case

Certified deletion

- Step 2: Lawyer encodes the amalgamation and sends to client, indicating the basis in which to measure the qubits
- Step 3: Client decodes the message to find out the qubit content that accompanies the classical content
- Step 4: Lawyer deletes the classical content and re-encodes the message
- Step 5: Since the contents are linked, the client can confirm that the lawyer's classical side is now random bits, and the information is provably deleted



Source: Broadbent, A. & Islam, R. (2020). Quantum encryption with certified deletion. arXiv:1910.03551v3.