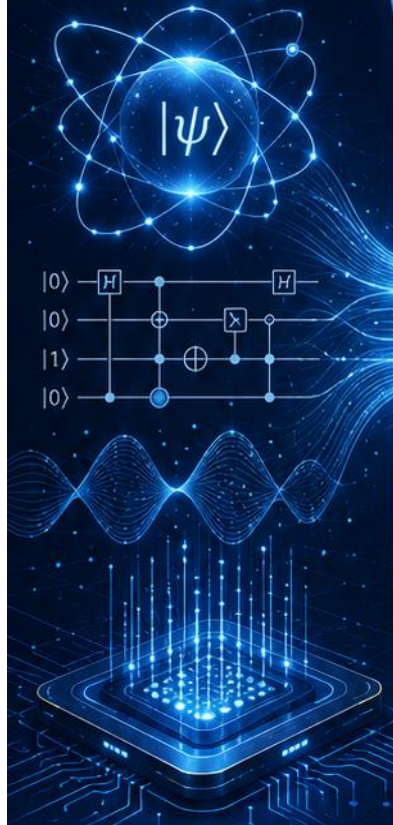


MASA DEPAN DATA SCIENCE

• Dampak Quantum Computing dan Blockchain •

QUANTUM
COMPUTING



DATA SCIENCE



BLOCKCHAIN



AI &
Machine
Learning



Big Data &
Analytics



Quantum
Optimization



Data
Provenance



Smart
Contract



Post-Quantum
Security



Trust, Privacy,
Governance

Oleh: Rudy C Tarumingkeng

Rudy C Tarumingkeng: **MASA DEPAN DATA SCIENCE: DAMPAK
QUANTUM COMPUTING DAN BLOCKCHAIN**

Oleh:

[Prof Ir Rudy C Tarumingkeng, PhD](#)

Professor of Management NUP: 9903252922

Professor Emeritus, IPB-University

Anggota MPR-RI, 1982-1987

Dekan Fak. Kehutanan IPB University. 1967-1968, 1968-1971, 1977-1978

Rektor, Universitas Cenderawasih, Papua (1978-1988, dan

Rektor, Kampus AGRO Manokwari sekarang Universitas Papua Manokwari

Coordinator, CIDA/DIKTI SFU Burnaby BC Canada 1988-1991

Rektor, Universitas Kristen Krida Wacana, Jakarta (1991-2000)

Ketua, Dewan Guru Besar, IPB-University, Bogor (2005-2006)

AI - Data Analyst, dan Ketua, Senat Akademik, IBM-ASMI, Jakarta 2024-

© RudyCT Academic Series

rudyc75@gmail.com

14 Juli 2026

Berikut artikel akademik yang membahas perkembangan Data Science dalam konteks komputasi kuantum, blockchain, keamanan pascakuantum, tata kelola data, serta implikasinya bagi organisasi dan Indonesia. DOI dicantumkan untuk sumber yang memilikinya.

MASA DEPAN DATA SCIENCE: DAMPAK QUANTUM COMPUTING DAN BLOCKCHAIN

Abstrak

Data Science berkembang dari disiplin yang berfokus pada pengolahan data, statistika, dan pemodelan prediktif menjadi infrastruktur epistemik bagi organisasi, pemerintahan, sains, dan masyarakat digital.

Perkembangan kecerdasan buatan, machine learning, komputasi awan, Internet of Things, serta model bahasa berskala besar telah memperluas kemampuan manusia dalam mengumpulkan, mengintegrasikan, menganalisis, dan menggunakan data. Meskipun demikian, ekosistem Data Science menghadapi keterbatasan mendasar. Keterbatasan tersebut mencakup tingginya kebutuhan komputasi, semakin besarnya volume dan dimensionalitas data, kesulitan optimasi, ketidakpastian mengenai asal-usul data, kurangnya interoperabilitas, konsentrasi penguasaan data, masalah privasi, manipulasi informasi, serta rendahnya kepercayaan terhadap model yang tidak transparan.

Dua teknologi yang berpotensi memengaruhi arah perkembangan Data Science adalah quantum computing dan blockchain. Quantum computing memperkenalkan paradigma komputasi yang menggunakan prinsip

superposisi, interferensi, dan keterikatan kuantum. Secara teoretis, algoritma kuantum dapat memberikan percepatan bagi kelas masalah tertentu, termasuk pencarian, faktorisasi, simulasi sistem kuantum, penyelesaian sistem persamaan linear, optimasi, sampling, dan machine learning. Dalam Data Science, kemampuan tersebut membuka kemungkinan pengembangan quantum machine learning, quantum-enhanced optimization, quantum generative modelling, quantum sampling, dan analisis sistem kompleks. Namun, realisasi manfaat praktisnya masih menghadapi keterbatasan perangkat keras, noise, koreksi kesalahan, kebutuhan pengkodean data, kesulitan pelatihan, dan belum konsistennya bukti bahwa algoritma kuantum mengungguli metode klasik pada data dunia nyata.

Blockchain menawarkan kontribusi yang berbeda. Teknologi ini tidak terutama mempercepat analisis, melainkan membangun kepercayaan, ketertelusuran, integritas, dan koordinasi di antara pihak-pihak yang tidak sepenuhnya saling mempercayai. Blockchain dapat digunakan untuk merekam data provenance, mengelola identitas dan hak akses, mengaudit perubahan dataset, mencatat riwayat model, mengatur pasar data, mendukung federated learning, memberikan insentif kepada penyedia data, dan mengotomatisasi aturan melalui smart contract. Akan tetapi, blockchain juga menghadapi kendala berupa skalabilitas, latensi, kompleksitas tata kelola, perlindungan privasi, interoperabilitas, ketidakpastian hukum, serta risiko memasukkan data yang salah ke dalam catatan yang sulit diubah.

Hubungan quantum computing dan blockchain bersifat paradoksal sekaligus komplementer. Quantum computing berpotensi meningkatkan kemampuan analitik dan optimasi, tetapi juga mengancam skema kriptografi kunci publik yang digunakan untuk mengamankan banyak sistem blockchain. Algoritma Shor secara teoretis dapat memecahkan masalah faktorisasi dan logaritma diskret yang menjadi dasar RSA dan kriptografi kurva eliptik, sedangkan algoritma Grover mengurangi tingkat

keamanan efektif sejumlah skema kriptografi simetris. Kondisi ini mendorong transisi menuju post-quantum cryptography, crypto-agility, tanda tangan digital tahan kuantum, serta desain quantum-safe blockchain. Pada Agustus 2024, National Institute of Standards and Technology menyelesaikan tiga standar utama kriptografi pascakuantum, yaitu FIPS 203, FIPS 204, dan FIPS 205. Organisasi didorong untuk mulai memetakan aset kriptografi dan merencanakan migrasi karena perubahan sistem keamanan berskala besar memerlukan waktu panjang. ([NIST](#))

Artikel ini menjelaskan kemungkinan masa depan Data Science melalui konvergensi komputasi klasik, kecerdasan buatan, quantum computing, blockchain, federated learning, dan privacy-enhancing technologies. Pembahasan mencakup landasan konseptual, potensi aplikasi, arsitektur data masa depan, risiko etika, keamanan, tata kelola, dampak manajerial, skenario perkembangan hingga 2050, serta agenda strategis bagi Indonesia. Kesimpulan utama artikel ini adalah bahwa quantum computing dan blockchain tidak akan menggantikan Data Science klasik secara langsung. Keduanya akan menjadi lapisan pelengkap dalam arsitektur hibrida. Komputasi kuantum akan digunakan secara selektif untuk bagian masalah yang memiliki struktur sesuai, sedangkan blockchain akan digunakan ketika integritas, koordinasi, auditabilitas, kepemilikan, dan kepercayaan lebih penting daripada kecepatan pemrosesan semata. Masa depan Data Science dengan demikian bukan hanya mengenai model yang semakin akurat, tetapi juga sistem pengetahuan yang dapat diverifikasi, aman, adil, tahan terhadap ancaman baru, dan dapat dipertanggungjawabkan.

Kata Kunci: *Data Science, quantum computing, quantum machine learning, blockchain, data provenance, federated learning, post-quantum cryptography, smart contract, kecerdasan buatan, tata kelola data.*

1. Pendahuluan

Data telah menjadi salah satu sumber daya utama dalam ekonomi digital. Organisasi menggunakan data untuk memahami pelanggan, memprediksi permintaan, mengoptimalkan operasi, mengembangkan produk, mengelola risiko, mendukung penelitian, dan merancang kebijakan publik. Perusahaan teknologi membangun model bisnis berdasarkan kemampuan mengumpulkan serta menganalisis jejak digital. Rumah sakit mengintegrasikan data klinis, citra, laboratorium, dan genomik. Pemerintah menggunakan data kependudukan, ekonomi, kesehatan, pendidikan, dan lingkungan untuk mendukung perencanaan.

Perkembangan tersebut melahirkan Data Science sebagai bidang interdisipliner yang menggabungkan statistika, matematika, ilmu komputer, machine learning, rekayasa data, pengetahuan domain, visualisasi, dan komunikasi. Data Science tidak hanya menghasilkan laporan mengenai masa lalu. Bidang ini memungkinkan prediksi mengenai masa depan, rekomendasi tindakan, eksperimen, simulasi, dan otomatisasi keputusan.

Namun, keberhasilan Data Science menimbulkan tantangan baru. Dataset semakin besar, model semakin kompleks, dan kebutuhan komputasi semakin tinggi. Pelatihan model berskala besar dapat membutuhkan infrastruktur mahal dan energi yang besar. Banyak masalah optimasi tidak dapat diselesaikan secara efisien ketika jumlah kemungkinan meningkat secara eksponensial. Model dapat kehilangan kinerja ketika distribusi data berubah. Penggunaan data lintas organisasi menghadapi hambatan privasi, regulasi, kepemilikan, dan kurangnya kepercayaan.

Masalah lain berkaitan dengan kebenaran dan integritas data. Model yang canggih tetap dapat menghasilkan keputusan buruk apabila data telah dimanipulasi, salah dicatat, tidak lengkap, atau tidak representatif. Dalam ekosistem data yang melibatkan banyak organisasi, sulit menentukan siapa

yang menghasilkan data, kapan data diubah, metode apa yang digunakan, dan apakah pihak tertentu memiliki kewenangan mengaksesnya.

Pada saat yang sama, konsentrasi data pada sejumlah platform besar menimbulkan ketimpangan kekuasaan. Pihak yang menguasai data, infrastruktur komputasi, dan model memiliki kemampuan besar untuk menentukan bentuk pengetahuan digital. Data Science dengan demikian bukan sekadar persoalan teknis. Ia berkaitan dengan politik data, distribusi manfaat, keadilan, privasi, kedaulatan digital, dan kepercayaan sosial.

Dalam konteks ini, quantum computing dan blockchain sering dipandang sebagai teknologi yang dapat mengubah masa depan Data Science. Keduanya memiliki logika yang berbeda.

Quantum computing berusaha mengubah cara komputasi dilakukan. Teknologi ini memanfaatkan fenomena mekanika kuantum untuk menjalankan kelas perhitungan tertentu dengan cara yang tidak dapat ditiru secara efisien oleh komputer klasik. Potensinya terdapat pada simulasi sistem kuantum, optimasi, pencarian, analisis struktur berdimensi tinggi, dan machine learning.

Blockchain berusaha mengubah cara kepercayaan digital dibentuk. Blockchain memungkinkan sejumlah pihak memelihara catatan bersama yang sulit diubah tanpa bergantung sepenuhnya pada satu otoritas pusat. Potensinya terdapat pada integritas data, auditabilitas, koordinasi, smart contract, identitas, kepemilikan aset digital, dan tata kelola lintas organisasi.

Apabila Data Science menjawab pertanyaan mengenai bagaimana memperoleh pengetahuan dari data, quantum computing berhubungan dengan bagaimana sebagian perhitungan dapat dilakukan secara lebih efisien. Blockchain berhubungan dengan bagaimana data, model, transaksi, dan hak dapat dikelola secara dapat dipercaya.

Pertemuan ketiga teknologi tersebut menghasilkan beberapa pertanyaan mendasar:

1. Apakah quantum computing benar-benar dapat mempercepat machine learning dan analitik data?
2. Jenis masalah Data Science apa yang sesuai untuk algoritma kuantum?
3. Bagaimana blockchain meningkatkan data provenance dan reproduktibilitas model?
4. Apakah blockchain dapat mengurangi konsentrasi penguasaan data?
5. Bagaimana federated learning dan blockchain dapat bekerja bersama?
6. Bagaimana ancaman kuantum memengaruhi keamanan blockchain?
7. Bagaimana organisasi harus mempersiapkan transisi pascakuantum?
8. Apa implikasi konvergensi tersebut bagi manajemen, pendidikan, dan kebijakan publik?

Pertanyaan-pertanyaan ini tidak dapat dijawab dengan optimisme teknologi semata. Banyak klaim mengenai quantum computing dan blockchain bersifat spekulatif. Beberapa manfaat hanya berlaku pada asumsi matematis tertentu. Implementasi dunia nyata menghadapi kendala biaya, integrasi, regulasi, dan organisasi.

Karena itu, masa depan Data Science perlu dipahami melalui pendekatan kritis. Teknologi baru seharusnya dinilai berdasarkan masalah yang dapat diselesaikannya, bukan berdasarkan popularitas istilahnya.

2. Evolusi Data Science

2.1 Dari Statistika menuju Data Science

Akar Data Science terdapat dalam statistika, ilmu pengukuran, pengambilan sampel, dan metode ilmiah. Statistika menyediakan kerangka untuk memahami variasi, ketidakpastian, hubungan antarvariabel, dan inferensi dari sampel menuju populasi.

Perkembangan komputer memungkinkan pengolahan data dalam skala lebih besar. Basis data relasional, data warehouse, dan business intelligence kemudian membantu organisasi menyimpan serta menyajikan informasi secara terstruktur.

Pada tahap berikutnya, data mining berkembang untuk menemukan pola yang sebelumnya tidak diketahui. Machine learning memperluas kemampuan tersebut dengan membangun sistem yang mempelajari fungsi dari data. Internet, telepon pintar, sensor, dan media sosial menghasilkan data dalam volume, kecepatan, dan keragaman yang belum pernah terjadi sebelumnya.

Data Science muncul sebagai integrasi berbagai tradisi tersebut. Donoho menjelaskan bahwa Data Science tidak dapat direduksi menjadi statistika atau pemrograman saja. Bidang ini mencakup keseluruhan aktivitas yang berhubungan dengan pengumpulan, pemrosesan, analisis, representasi, dan penggunaan data.

2.2 Data Science pada Era Kecerdasan Buatan

Perkembangan deep learning meningkatkan kemampuan analisis gambar, suara, bahasa, dan video. Model foundation dan model bahasa besar memungkinkan satu model digunakan untuk berbagai tugas. Interaksi dengan data tidak lagi selalu dilakukan melalui kode atau dashboard. Pengguna dapat mengajukan pertanyaan menggunakan bahasa alami.

Namun, kemajuan tersebut disertai biaya. Model modern membutuhkan data, komputasi, memori, dan energi dalam jumlah besar. Model juga dapat menghasilkan informasi yang tidak benar, mengandung bias, atau sulit dijelaskan.

Data Science masa kini karena itu menghadapi dua tujuan yang terkadang bertentangan. Tujuan pertama adalah meningkatkan kemampuan prediksi dan otomatisasi. Tujuan kedua adalah memastikan bahwa proses tersebut aman, dapat dipercaya, dan bertanggung jawab.

Quantum computing berpotensi membantu tujuan pertama dengan memperluas kemampuan komputasi untuk masalah tertentu. Blockchain berpotensi membantu tujuan kedua melalui integritas, provenance, dan koordinasi terdesentralisasi.

2.3 Data Science sebagai Infrastruktur Pengetahuan

Data Science bukan sekadar kumpulan algoritma. Ia merupakan infrastruktur untuk membentuk pengetahuan.

Infrastruktur tersebut mencakup:

- Sumber data.
- Prosedur pengumpulan.
- Standar metadata.
- Sistem penyimpanan.
- Pipeline transformasi.
- Model analitik.
- Mekanisme validasi.
- Sistem keputusan.
- Tata kelola.
- Manusia yang merancang dan menggunakan sistem.

Kesalahan pada salah satu bagian dapat memengaruhi keseluruhan hasil. Oleh sebab itu, masa depan Data Science tidak dapat hanya dibahas dari perspektif algoritma. Arsitektur, keamanan, organisasi, dan institusi juga harus diperhatikan.

3. Hakikat Quantum Computing

3.1 Bit dan Qubit

Komputer klasik menggunakan bit yang berada dalam keadaan 0 atau 1. Komputer kuantum menggunakan quantum bit atau qubit.

Keadaan qubit dapat dituliskan sebagai:

$$\begin{bmatrix} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \end{bmatrix}$$

dengan:

$$\begin{bmatrix} |\alpha|^2 + |\beta|^2 = 1 \end{bmatrix}$$

Koefisien (α) dan (β) merupakan amplitudo probabilitas. Ketika diukur, qubit menghasilkan 0 atau 1 dengan probabilitas yang ditentukan oleh kuadrat amplitudo.

Superposisi tidak berarti bahwa komputer kuantum secara sederhana membaca seluruh jawaban sekaligus. Algoritma kuantum harus mengatur amplitudo dan interferensi agar hasil yang benar memiliki probabilitas pengukuran lebih tinggi.

3.2 Superposisi

Superposisi memungkinkan keadaan kuantum direpresentasikan sebagai kombinasi beberapa basis keadaan. Untuk (n) qubit, sistem dapat direpresentasikan dalam ruang keadaan berdimensi (2^n).

Kemampuan representasi tersebut menjadi salah satu sumber potensi komputasi kuantum. Namun, tidak semua informasi dalam keadaan itu

dapat dibaca secara langsung. Pengukuran menghasilkan informasi terbatas.

3.3 Entanglement

Entanglement atau keterikatan kuantum merupakan korelasi antara qubit yang tidak dapat dijelaskan sebagai kombinasi keadaan independen.

Entanglement memungkinkan algoritma memproses korelasi tertentu dengan cara yang berbeda dari komputer klasik. Meskipun demikian, keberadaan entanglement saja tidak menjamin keunggulan komputasi. Struktur algoritma dan masalah tetap menentukan.

3.4 Interferensi

Algoritma kuantum menggunakan interferensi untuk memperkuat amplitudo jawaban yang diinginkan dan mengurangi amplitudo jawaban yang salah.

Prinsip ini sangat penting. Keunggulan kuantum tidak muncul hanya karena terdapat banyak keadaan, tetapi karena algoritma mengatur evolusi keadaan sehingga pengukuran memberikan hasil bermakna.

3.5 Quantum Gate dan Circuit

Quantum gate mengubah keadaan qubit. Rangkaian quantum gate membentuk quantum circuit.

Beberapa gate dasar meliputi:

- Hadamard gate.
- Pauli-X, Y, dan Z.
- Rotation gates.
- Controlled-NOT.
- Controlled-phase.

Quantum circuit kemudian diukur untuk memperoleh hasil klasik.

3.6 Quantum Annealing dan Gate-Based Computing

Quantum annealing dirancang terutama untuk optimasi. Masalah diubah menjadi fungsi energi, kemudian sistem mencari keadaan energi rendah.

Gate-based quantum computing bersifat lebih umum. Pendekatan ini menggunakan quantum circuit yang dapat diprogram.

Keduanya tidak boleh disamakan. Sebuah metode yang berhasil pada quantum annealer belum tentu langsung diterapkan pada komputer kuantum universal.

4. Algoritma Kuantum yang Relevan bagi Data Science

4.1 Algoritma Shor

Algoritma Shor menunjukkan bahwa komputer kuantum yang cukup besar dan terkoreksi kesalahan dapat memfaktorkan bilangan bulat serta menyelesaikan masalah logaritma diskret dalam waktu polinomial. Temuan ini penting karena keamanan RSA dan beberapa sistem kriptografi kunci publik bergantung pada sulitnya masalah tersebut bagi komputer klasik. ([IEEE Xplore](#))

Dampak algoritma Shor terhadap Data Science tidak terutama berupa percepatan analisis. Dampak utamanya terdapat pada keamanan data, identitas, tanda tangan digital, komunikasi, dan blockchain.

4.2 Algoritma Grover

Algoritma Grover memberikan percepatan kuadratik untuk pencarian tidak terstruktur. Pencarian klasik terhadap (N) kemungkinan membutuhkan orde ($O(N)$), sedangkan pencarian kuantum ideal membutuhkan sekitar ($O(\sqrt{N})$) evaluasi. ([ACM Digital Library](#))

Dalam Data Science, ide Grover dapat relevan bagi pencarian kombinatorial, optimasi, deteksi pola, dan analisis ruang solusi. Namun, percepatan kuadratik tidak otomatis membuat semua pencarian data

menjadi lebih cepat. Biaya menyiapkan oracle, memasukkan data, mengoreksi kesalahan, dan membaca hasil harus diperhitungkan.

4.3 Quantum Linear Systems Algorithm

Harrow, Hassidim, dan Lloyd memperkenalkan algoritma kuantum untuk sistem persamaan linear. Dalam kondisi tertentu—misalnya matriks sparse, condition number terkendali, dan keluaran yang dibutuhkan berupa properti tertentu dari solusi—algoritma tersebut secara teoretis dapat memberikan percepatan besar. ([APS Link](#))

Sistem persamaan linear merupakan inti banyak metode Data Science:

- Regresi.
- Optimasi.
- Principal component analysis.
- Simulasi.
- Sistem rekomendasi.
- Analisis jaringan.

Namun, algoritma ini tidak memberikan seluruh vektor solusi secara gratis. Membaca semua elemen dapat menghilangkan keuntungan. Karena itu, manfaatnya lebih mungkin muncul ketika pengguna membutuhkan statistik atau ekspektasi tertentu.

4.4 Quantum Sampling

Banyak masalah machine learning berkaitan dengan sampling dari distribusi kompleks. Komputer kuantum secara alamiah menghasilkan hasil probabilistik.

Quantum sampling berpotensi digunakan dalam:

- Bayesian inference.
- Generative modelling.

- Monte Carlo.
- Estimasi risiko.
- Optimasi stokastik.

Percepatan potensial tergantung struktur distribusi dan kemampuan menyiapkan keadaan kuantum.

4.5 Quantum Simulation

Simulasi sistem kuantum merupakan aplikasi yang paling alami. Molekul, material, dan reaksi kimia pada dasarnya merupakan sistem kuantum.

Quantum simulation dapat membantu menghasilkan data ilmiah yang kemudian dianalisis oleh Data Science. Dampaknya dapat muncul dalam:

- Penemuan obat.
- Material baru.
- Baterai.
- Katalis.
- Energi.
- Pertanian.
- Teknologi iklim.

Dalam kasus ini, quantum computing tidak hanya mempercepat machine learning. Ia dapat menghasilkan jenis data baru yang sulit diperoleh melalui simulasi klasik.

4.6 Variational Quantum Algorithms

Perangkat kuantum saat ini masih memiliki noise dan jumlah qubit terbatas. Variational quantum algorithms menggunakan kombinasi komputer klasik dan quantum circuit.

Prosesnya adalah:

1. Komputer klasik memilih parameter.
2. Quantum circuit menjalankan perhitungan.
3. Hasil pengukuran digunakan untuk menghitung fungsi tujuan.
4. Optimizer klasik memperbarui parameter.
5. Proses diulang.

Variational quantum algorithms telah dikembangkan untuk simulasi, optimasi, machine learning, dan persamaan linear. Akan tetapi, metode ini menghadapi masalah noise, biaya pengukuran, dan trainability. ([Nature](#))

5. Quantum Machine Learning

5.1 Pengertian

Quantum machine learning atau QML merupakan bidang yang menggabungkan algoritma kuantum dengan machine learning.

QML dapat dibagi menjadi beberapa kategori:

1. Algoritma kuantum untuk data klasik.
2. Algoritma kuantum untuk data kuantum.
3. Machine learning klasik untuk mengendalikan sistem kuantum.
4. Metode quantum-inspired yang berjalan pada komputer klasik.

Pembagian ini penting. Tidak semua metode berlabel "quantum machine learning" membutuhkan komputer kuantum.

5.2 Quantum Feature Map

Quantum feature map mengodekan data klasik ke dalam keadaan kuantum. Quantum circuit kemudian membentuk ruang fitur yang mungkin sulit direpresentasikan secara klasik.

Model kernel kuantum berusaha menghitung kemiripan antar data melalui overlap keadaan kuantum. Penelitian menunjukkan bahwa quantum feature space tertentu memiliki potensi memberikan pemisahan pola yang kuat. Namun, manfaatnya bergantung pada struktur data dan kemampuan komputer klasik meniru kernel tersebut.

5.3 Variational Quantum Classifier

Variational quantum classifier menggunakan quantum circuit berparameter untuk klasifikasi.

Prosedurnya:

- Data dikodekan.
- Circuit berparameter diterapkan.
- Qubit diukur.
- Fungsi kerugian dihitung.
- Parameter diperbarui.

Model ini menyerupai neural network, tetapi transformasinya dilakukan melalui quantum gate.

5.4 Quantum Neural Network

Istilah quantum neural network digunakan untuk berbagai arsitektur quantum circuit yang dapat dilatih. Potensinya meliputi representasi fungsi kompleks dan pemanfaatan ruang Hilbert berdimensi tinggi.

Namun, istilah "neural" tidak berarti bahwa arsitekturnya identik dengan jaringan saraf klasik. Struktur optimasi, pengukuran, dan gradien memiliki karakteristik berbeda.

5.5 Quantum Support Vector Machine

Quantum support vector machine memanfaatkan quantum subroutine untuk feature mapping atau penyelesaian bagian tertentu dari optimasi.

Keunggulan teoretis dapat muncul ketika kernel kuantum sulit dihitung secara klasik. Namun, evaluasi harus membandingkan dengan metode klasik terbaik, bukan baseline yang lemah.

5.6 Quantum Generative Models

Quantum generative models berusaha mempelajari distribusi data. Model tersebut dapat berupa:

- Quantum Boltzmann machine.
- Quantum circuit Born machine.
- Quantum generative adversarial network.
- Quantum autoencoder.

Potensi aplikasinya antara lain menghasilkan data sintetis, simulasi, dan anomaly detection.

5.7 Quantum Reinforcement Learning

Quantum reinforcement learning menggabungkan quantum circuit dengan agen yang belajar dari reward.

Aplikasinya secara teoretis mencakup:

- Robotika.
- Penjadwalan.
- Logistik.
- Pengelolaan energi.
- Keuangan.
- Strategi adaptif.

Bukti keunggulan praktisnya masih berkembang.

6. Apakah Quantum Computing Akan Merevolusi Data Science?

Jawabannya perlu dibedakan antara potensi teoretis dan bukti empiris.

6.1 Potensi Teoretis

Komputasi kuantum memiliki potensi pada masalah yang melibatkan:

- Ruang solusi sangat besar.
- Struktur aljabar tertentu.
- Sampling kompleks.
- Optimasi kombinatorial.
- Simulasi sistem kuantum.
- Data yang secara alamiah bersifat kuantum.

Beberapa algoritma memberikan percepatan polinomial atau eksponensial dalam model teoretis.

6.2 Keterbatasan Empiris

Bukti keunggulan QML pada dataset klasik dunia nyata belum konsisten. Sebuah kajian sistematis tahun 2025 terhadap aplikasi QML dalam kesehatan digital menemukan bahwa sebagian besar penelitian menggunakan simulasi ideal atau dataset kecil. Hanya sebagian kecil yang menguji kondisi perangkat keras realistis, dan tidak terdapat kecenderungan konsisten yang menunjukkan keunggulan empiris QML dibandingkan metode klasik. ([Nature](#))

Temuan tersebut tidak berarti QML tidak memiliki masa depan. Temuan itu menunjukkan bahwa klaim harus dibuat secara hati-hati.

6.3 Kekuatan Data bagi Model Klasik

Huang dan rekan menunjukkan bahwa beberapa masalah yang sulit dihitung secara langsung dapat diprediksi oleh model klasik apabila tersedia data pelatihan yang memadai. Dengan kata lain, keuntungan komputasi kuantum tidak otomatis berubah menjadi keuntungan

pembelajaran. Model klasik dapat mempelajari pola masukan-keluaran tanpa melakukan seluruh perhitungan yang mendasarinya. ([Nature](#))

Implikasinya sangat penting. Penilaian quantum advantage dalam machine learning harus menjawab:

- Apakah masalah tersebut benar-benar sulit bagi metode klasik?
- Apakah data tersedia bagi model klasik?
- Apakah quantum data loading efisien?
- Apakah keluaran dapat dibaca tanpa biaya besar?
- Apakah perbandingan dilakukan dengan baseline terbaik?
- Apakah keuntungan tetap ada setelah noise dan koreksi kesalahan?

6.4 Data Loading Bottleneck

Sebagian algoritma QML mengasumsikan data dapat dimasukkan ke quantum state secara efisien. Dalam praktiknya, data klasik mungkin berjumlah sangat besar.

Apabila waktu mengodekan data sebanding dengan membaca seluruh dataset, keuntungan komputasi dapat hilang. Quantum random access memory sering diasumsikan dalam teori, tetapi implementasinya dalam skala besar tetap menjadi tantangan.

6.5 Output Bottleneck

Quantum state dapat menyimpan representasi berdimensi tinggi, tetapi pengukuran menghasilkan keluaran terbatas. Untuk memperoleh estimasi akurat, circuit perlu dijalankan berulang.

Apabila pengguna membutuhkan seluruh vektor hasil, jumlah pengukuran dapat menjadi besar.

6.6 Noise dan Error Correction

Qubit sangat sensitif terhadap lingkungan. Noise menyebabkan decoherence dan kesalahan gate.

Perangkat saat ini sering disebut berada dalam era noisy intermediate-scale quantum atau NISQ. Preskill menggunakan istilah tersebut untuk menggambarkan komputer kuantum yang belum memiliki koreksi kesalahan penuh tetapi cukup besar untuk mengeksplorasi tugas tertentu.

Sistem fault-tolerant membutuhkan logical qubits yang dibangun dari banyak physical qubits. Koreksi kesalahan menambah overhead yang besar.

6.7 Barren Plateau

Variational quantum circuit dapat mengalami barren plateau, yaitu wilayah fungsi kerugian dengan gradien sangat kecil. Kondisi ini membuat pelatihan sulit.

Masalah tersebut dapat dipengaruhi oleh kedalaman circuit, ansatz, noise, dan metode inisialisasi.

6.8 Dequantization

Beberapa algoritma kuantum menginspirasi algoritma klasik yang lebih baik. Proses ini disebut dequantization.

Fenomena tersebut menunjukkan bahwa riset kuantum tetap bermanfaat meskipun komputer kuantum belum memberikan keunggulan langsung. Konsep kuantum dapat memperbaiki algoritma klasik.

7. Masa Depan Komputasi Hibrida

Masa depan Data Science kemungkinan tidak berbentuk penggantian komputer klasik oleh komputer kuantum. Bentuk yang lebih realistis adalah quantum-centric atau hybrid computing.

Arsitektur tersebut mencakup:

- CPU untuk logika umum.

- GPU atau accelerator untuk deep learning.
- HPC untuk simulasi dan komputasi numerik.
- QPU untuk submasalah tertentu.
- Cloud untuk orkestrasi.
- Blockchain untuk trust dan provenance.

IBM, misalnya, mengembangkan visi quantum-centric supercomputing yang mengintegrasikan CPU, GPU, dan QPU. Roadmap vendor perlu dipahami sebagai target pengembangan, bukan jaminan pencapaian. Akan tetapi, arahnya menunjukkan bahwa quantum processor diposisikan sebagai accelerator, bukan komputer mandiri yang menggantikan seluruh infrastruktur klasik. ([IBM Research](#))

Dalam alur Data Science masa depan:

1. Data dikumpulkan melalui sistem klasik.
2. Data dibersihkan dan direduksi secara klasik.
3. Submasalah diidentifikasi.
4. Submasalah tertentu dikirim ke QPU.
5. Hasil dikembalikan ke workflow klasik.
6. Model dievaluasi, dijelaskan, dan dioperasikan secara klasik.

Pendekatan ini mirip penggunaan GPU. Pengguna tidak memindahkan seluruh sistem ke GPU. Mereka menggunakan GPU untuk operasi yang sesuai.

8. Potensi Quantum Computing dalam Bidang Data Science

8.1 Optimasi Portofolio

Optimasi portofolio melibatkan pemilihan kombinasi aset di bawah berbagai batasan. Ketika jumlah aset, skenario, dan constraint meningkat, ruang solusi menjadi besar.

Quantum annealing dan QAOA dapat digunakan untuk formulasi quadratic unconstrained binary optimization. Namun, manfaat praktis harus dibandingkan dengan solver klasik modern.

8.2 Manajemen Rantai Pasok

Penjadwalan, routing, alokasi kapasitas, dan pemilihan pemasok merupakan masalah kombinatorial.

Quantum optimization dapat membantu submasalah tertentu, terutama ketika organisasi membutuhkan solusi berkualitas tinggi dalam waktu terbatas.

8.3 Penemuan Obat

Quantum simulation dapat memodelkan molekul. Machine learning kemudian digunakan untuk memprediksi properti dan menyaring kandidat.

Konvergensi ini dapat membentuk pipeline:

- Simulasi kuantum menghasilkan data.
- Data Science mengidentifikasi pola.
- Model generatif mengusulkan kandidat.
- Eksperimen memvalidasi.
- Hasil digunakan untuk memperbaiki model.

8.4 Material dan Energi

Material baru untuk baterai, katalis, pupuk, hidrogen, dan penangkapan karbon membutuhkan pemahaman sistem elektron.

Quantum computing dapat menghasilkan simulasi, sedangkan Data Science mempercepat pencarian dalam ruang material.

8.5 Risiko dan Monte Carlo

Quantum amplitude estimation secara teoretis dapat mempercepat estimasi ekspektasi dibandingkan Monte Carlo klasik.

Potensi aplikasinya meliputi:

- Value-at-Risk.
- Pricing derivatif.
- Reliability.
- Risiko iklim.
- Simulasi proyek.

Realisasi penuh membutuhkan perangkat fault-tolerant dan state preparation yang efisien.

8.6 Cybersecurity Analytics

Quantum computing dapat membantu optimasi dan deteksi pola, tetapi juga meningkatkan kemampuan penyerang.

Data Science keamanan pada era kuantum harus memantau:

- Aset kriptografi rentan.
- Penggunaan kunci publik.
- Perubahan protokol.
- Anomali migrasi.
- Serangan terhadap implementasi pascakuantum.

9. Pengertian Blockchain

Blockchain adalah bentuk distributed ledger yang mempertahankan catatan transaksi di antara sejumlah node. Catatan dikelompokkan dalam blok dan dihubungkan secara kriptografis.

Karakteristiknya meliputi:

- Distribusi.
- Konsensus.
- Hash kriptografis.
- Tanda tangan digital.
- Ketertelusuran.
- Sulitnya perubahan sepihak.
- Kemampuan menjalankan smart contract pada platform tertentu.

Blockchain tidak identik dengan Bitcoin atau cryptocurrency.
Cryptocurrency merupakan salah satu aplikasi.

9.1 Public Blockchain

Public blockchain memungkinkan partisipasi terbuka.

Keunggulannya:

- Transparansi.
- Censorship resistance.
- Partisipasi luas.
- Tidak bergantung pada satu organisasi.

Keterbatasannya:

- Skalabilitas.
- Privasi.
- Biaya.
- Tata kelola.
- Kepastian hukum.

9.2 Permissioned Blockchain

Permissioned blockchain membatasi partisipasi pada pihak yang memiliki izin.

Pendekatan ini lebih sesuai bagi:

- Konsorsium industri.
- Pemerintahan.
- Rumah sakit.
- Rantai pasok.
- Perbankan.
- Penelitian.

Kelebihannya adalah kontrol akses dan performa. Namun, tingkat desentralisasinya lebih rendah.

9.3 Smart Contract

Smart contract merupakan program yang dijalankan oleh jaringan blockchain.

Smart contract dapat:

- Memeriksa kondisi.
- Mengatur hak akses.
- Memindahkan aset.
- Memberikan insentif.
- Merekam persetujuan.
- Mengotomatisasi aturan.

Christidis dan Devetsikiotis menunjukkan bahwa kombinasi blockchain serta smart contract dapat mengatur interaksi perangkat dan pihak yang tidak saling mempercayai tanpa perantara pusat tunggal. ([ResearchGate](#))

10. Dampak Blockchain terhadap Data Science

Blockchain tidak dirancang untuk menggantikan data warehouse, data lake, atau database berperforma tinggi. Nilai utamanya terletak pada trust layer.

10.1 Data Provenance

Data provenance adalah catatan mengenai:

- Asal data.
- Waktu penciptaan.
- Pihak yang menghasilkan.
- Transformasi yang dilakukan.
- Akses.
- Versi.
- Hubungan dengan data lain.

Dalam Data Science, provenance diperlukan untuk menjawab:

- Apakah data asli?
- Apakah data telah diubah?
- Model dilatih menggunakan versi apa?
- Siapa yang memberikan label?
- Apakah penggunaan data memiliki izin?
- Bagaimana hasil dapat direproduksi?

Blockchain dapat mencatat hash, timestamp, identitas, dan peristiwa transformasi. Ramachandran dan Kantarcioglu mengembangkan SmartProvenance untuk mengumpulkan serta memverifikasi provenance secara terdistribusi. ([ACM Digital Library](#))

10.2 Off-Chain Storage

Menyimpan seluruh dataset besar di blockchain umumnya tidak efisien. Desain yang lebih realistis adalah:

- Data berada di penyimpanan off-chain.
- Blockchain menyimpan hash.
- Blockchain menyimpan pointer.
- Blockchain mencatat hak akses.
- Smart contract mengatur penggunaan.

Pajoo dan rekan menunjukkan arsitektur yang menyimpan metadata aktual dalam sistem big data, sedangkan verification tags serta pointer dicatat pada permissioned blockchain. Pendekatan ini mengurangi overhead dan tetap memberikan integritas serta traceability. ([Springer Link](#))

10.3 Reproducible Data Science

Reproduksi model membutuhkan:

- Dataset yang tepat.
- Kode.
- Parameter.
- Library.
- Lingkungan.
- Seed.
- Riwayat perubahan.

Blockchain dapat menjadi registry yang mencatat fingerprint artefak tersebut. Ia tidak harus menyimpan file besar, tetapi memastikan bahwa artefak yang digunakan sesuai dengan versi tercatat.

10.4 Model Provenance

Model provenance mencakup:

- Pengembang.
- Data pelatihan.
- Tujuan.
- Versi.
- Validasi.
- Approval.
- Deployment.
- Monitoring.
- Retirement.

Catatan yang tidak mudah dimanipulasi dapat memperkuat audit AI.

10.5 Data Marketplace

Data memiliki nilai, tetapi pasar data menghadapi ketidakpercayaan.

Penyedia data khawatir data disalin tanpa kompensasi. Pembeli khawatir kualitas buruk. Individu tidak mengetahui bagaimana data digunakan.

Blockchain dan smart contract dapat mendukung:

- Lisensi penggunaan.
- Pembayaran otomatis.
- Pelacakan penggunaan.
- Royalti.
- Reputasi penyedia.
- Hak pencabutan tertentu.
- Provenance.

Namun, blockchain tidak menjamin kualitas data. Ia hanya mencatat transaksi dan pernyataan. Data palsu yang dimasukkan dapat tetap menjadi catatan palsu yang permanen.

11. Blockchain dan Federated Learning

11.1 Federated Learning

Federated learning memungkinkan model dilatih di beberapa lokasi tanpa memindahkan seluruh data mentah ke pusat.

Proses dasarnya:

1. Model global dikirim kepada peserta.
2. Peserta melatih model menggunakan data lokal.
3. Update dikirim.
4. Update diagregasi.
5. Model global diperbarui.

Pendekatan ini berguna ketika data tidak boleh atau tidak dapat dipusatkan.

Contohnya:

- Rumah sakit.
- Bank.
- Perangkat bergerak.
- Pabrik.
- Pemerintah daerah.
- Perguruan tinggi.

11.2 Kelemahan Federated Learning Terpusat

Federated learning tradisional masih bergantung pada aggregator.

Risikonya:

- Single point of failure.
- Manipulasi agregasi.
- Kurangnya audit.
- Peserta tidak mendapat insentif.
- Sulit menilai kontribusi.
- Model poisoning.

11.3 Blockchain-Enabled Federated Learning

Blockchain dapat digunakan untuk:

- Mencatat model update.
- Mengatur agregasi.
- Memberikan insentif.
- Mencatat reputasi.
- Menegakkan aturan.
- Mengurangi ketergantungan pada satu aggregator.
- Mendukung audit.

Ma dan rekan mengusulkan paradigma pembelajaran terdistribusi yang menggabungkan federated learning serta blockchain untuk mengurangi single point of failure dan membangun lingkungan partisipasi yang lebih dapat dipercaya. ([arXiv](#))

Kajian mengenai blockchain-based federated learning menunjukkan potensi dalam auditabilitas dan koordinasi, tetapi juga menyoroti overhead komunikasi, komputasi, penyimpanan, konsensus, serta perlindungan terhadap update berbahaya. ([ACM Digital Library](#))

11.4 Kasus Konsorsium Rumah Sakit

Bayangkan lima rumah sakit ingin membangun model prediksi penyakit langka.

Mereka tidak dapat menggabungkan rekam medis karena regulasi dan privasi.

Federated learning memungkinkan setiap rumah sakit melatih model secara lokal. Blockchain konsorsium mencatat:

- Identitas institusi.
- Versi model.
- Waktu update.
- Persetujuan.
- Nilai kontribusi.
- Hasil validasi.
- Audit.

Zero-knowledge proof dapat digunakan untuk membuktikan kepatuhan tertentu tanpa membuka data pasien.

Namun, sistem tetap memerlukan:

- Standar data.
- Harmonisasi definisi.
- Pengamanan endpoint.
- Validasi klinis.
- Tata kelola.
- Mekanisme menangani poisoning.

12. Blockchain, Zero-Knowledge Proof, dan Privasi

Blockchain menciptakan transparansi, tetapi transparansi dapat bertentangan dengan privasi.

Zero-knowledge proof memungkinkan satu pihak membuktikan bahwa suatu pernyataan benar tanpa membuka informasi dasarnya.

Contoh:

- Membuktikan usia di atas batas tanpa membuka tanggal lahir.
- Membuktikan saldo memadai tanpa membuka jumlah saldo.
- Membuktikan model memenuhi threshold fairness tanpa membuka data sensitif.
- Membuktikan komputasi dilakukan sesuai aturan tanpa membuka input.

Dokumentasi Ethereum menjelaskan bahwa zero-knowledge proof dapat memverifikasi kebenaran pernyataan tanpa mengungkapkan isi pernyataan atau cara memperolehnya. (ethereum.org)

Zhou dan rekan menilai bahwa integrasi blockchain dan ZKP dapat memperkuat identity sharing dengan mengurangi kebutuhan membuka data pribadi, meskipun terdapat tantangan implementasi, standarisasi, dan performa. ([ScienceDirect](https://www.sciencedirect.com))

12.1 ZK-Proof untuk Data Science

ZKP dapat mendukung verifiable machine learning.

Sebuah organisasi dapat membuktikan bahwa:

- Model menggunakan versi yang disetujui.
- Prediksi dihitung sesuai algoritma.
- Dataset memenuhi syarat tertentu.
- Jumlah observasi melampaui minimum.

- Data tidak mengandung kategori terlarang tertentu.
- Hasil agregat berada dalam rentang.

Konsep ini penting bagi audit AI lintas organisasi.

12.2 Batas ZKP

ZKP tidak menyelesaikan semua masalah.

Ia dapat membuktikan bahwa komputasi mengikuti program tertentu. Namun, apabila programnya salah atau inputnya palsu, proof tetap dapat valid.

ZKP juga tidak menjamin data selalu tersedia. Dokumentasi Ethereum menekankan bahwa validitas komputasi dan data availability merupakan masalah berbeda. (ethereum.org)

13. Smart Contract sebagai Tata Kelola Data

Smart contract dapat mengotomatisasi kebijakan data.

Contohnya:

- Akses hanya diberikan kepada peneliti terverifikasi.
- Dataset hanya boleh digunakan selama periode tertentu.
- Pembayaran dilakukan setelah hasil validasi.
- Model update ditolak apabila tidak memenuhi standar.
- Kompensasi dibagikan berdasarkan kontribusi.
- Penggunaan data dicatat.

Namun, hukum dan organisasi tidak dapat sepenuhnya direduksi menjadi kode.

Kode menghadapi:

- Bug.

- Ambiguitas.
- Keadaan yang tidak diperkirakan.
- Perubahan regulasi.
- Konflik interpretasi.
- Kebutuhan diskresi.

Prinsip "code is law" tidak cukup untuk lingkungan organisasi. Desain yang lebih baik adalah "code under governance", yaitu smart contract beroperasi dalam kerangka kelembagaan yang memiliki mekanisme koreksi, banding, dan akuntabilitas.

14. Hubungan Paradoks Quantum Computing dan Blockchain

Quantum computing dan blockchain memiliki hubungan ganda.

Pertama, quantum computing dapat mendukung optimasi, sampling, dan machine learning yang digunakan dalam ekosistem blockchain.

Kedua, quantum computing mengancam fondasi kriptografi blockchain.

14.1 Ancaman terhadap Digital Signature

Blockchain menggunakan digital signature untuk membuktikan kepemilikan private key.

Banyak blockchain menggunakan elliptic-curve cryptography. Algoritma Shor secara teoretis dapat menyelesaikan discrete logarithm pada komputer kuantum fault-tolerant yang cukup kuat.

Penyerang dapat:

- Menghitung private key dari public key.
- Membuat tanda tangan palsu.
- Mengambil alih aset.

- Menyamar sebagai validator.
- Memalsukan transaksi.

Ancaman belum berarti komputer kuantum saat ini mampu melakukan serangan tersebut. Akan tetapi, migrasi harus dimulai sebelum serangan menjadi praktis karena perubahan protokol membutuhkan waktu.

14.2 Ancaman terhadap Hash

Grover memberikan percepatan kuadratik terhadap brute-force search. Dampaknya terhadap hash dan kriptografi simetris dapat dimitigasi dengan panjang kunci atau output yang lebih besar.

Secara kasar, keamanan (n) -bit terhadap pencarian klasik dapat berkurang menjadi sekitar $(n/2)$ -bit terhadap Grover dalam asumsi ideal. Namun, biaya implementasi serangan kuantum nyata tetap kompleks.

14.3 Harvest Now, Decrypt Later

Data terenkripsi yang dicuri hari ini dapat disimpan dan didekripsi pada masa depan ketika komputer kuantum relevan tersedia.

Risiko ini penting bagi data yang memiliki umur kerahasiaan panjang:

- Data kesehatan.
- Rahasia negara.
- Kekayaan intelektual.
- Identitas biometrik.
- Kontrak jangka panjang.
- Data pertahanan.

15. Post-Quantum Cryptography

Post-quantum cryptography adalah kriptografi yang dirancang untuk berjalan pada komputer klasik tetapi tahan terhadap serangan komputer kuantum yang diketahui.

Pendekatan tersebut meliputi:

- Lattice-based cryptography.
- Hash-based signatures.
- Code-based cryptography.
- Multivariate cryptography.
- Isogeny-based cryptography, meskipun beberapa kandidat mengalami serangan.

Pada 13 Agustus 2024, NIST menyelesaikan:

- FIPS 203: ML-KEM.
- FIPS 204: ML-DSA.
- FIPS 205: SLH-DSA.

NIST mendorong organisasi mulai beralih karena inventarisasi, penggantian protokol, interoperabilitas, pengujian, dan migrasi sistem memerlukan waktu. ([NIST](#))

15.1 Quantum-Safe Blockchain

Blockchain quantum-safe dapat menggunakan:

- Post-quantum signatures.
- Hybrid signatures.
- Hash-based addresses.
- Crypto-agility.
- Key rotation.
- Protocol upgrade.

- Migration contract.

15.2 Hybrid Cryptography

Pada masa transisi, sistem dapat menggunakan tanda tangan klasik dan pascakuantum secara bersamaan.

Tujuannya adalah:

- Menjaga kompatibilitas.
- Mengurangi risiko algoritma baru.
- Memungkinkan migrasi bertahap.

15.3 Crypto-Agility

Crypto-agility adalah kemampuan mengganti algoritma tanpa membangun ulang seluruh sistem.

Sistem Data Science masa depan harus mencatat:

- Algoritma.
- Versi.
- Key length.
- Certificate.
- Dependency.
- Lokasi penggunaan.
- Masa berlaku.

Crypto-agility merupakan kemampuan organisasi, bukan hanya fitur software.

16. Blockchain Pascakuantum

Migrasi blockchain lebih sulit dibandingkan sistem terpusat.

Dalam sistem terpusat, organisasi dapat menetapkan pembaruan. Dalam public blockchain, perubahan membutuhkan konsensus komunitas, pengembang, validator, pengguna, dan penyedia layanan.

Masalah migrasi meliputi:

- Alamat lama.
- Aset tidak aktif.
- Public key yang telah terbuka.
- Smart contract lama.
- Hardware wallet.
- Cross-chain bridge.
- Validator.
- Governance.

Roadmap Ethereum saat ini memasukkan future-proofing terhadap quantum computing sebagai agenda jangka panjang. Dokumentasi resminya mengakui bahwa tanda tangan akun berbasis ECDSA dan sebagian proof system dapat terpengaruh oleh komputer kuantum yang cukup kuat. (ethereum.org)

Transisi dapat menimbulkan pertanyaan sulit:

- Apakah aset pada alamat rentan harus dipindahkan?
- Apa yang terjadi pada pemilik yang kehilangan akses?
- Apakah jaringan boleh membekukan aset?
- Apakah perubahan tersebut melanggar prinsip immutability?
- Siapa yang menentukan deadline migrasi?

Masalah tersebut menunjukkan bahwa keamanan teknologi selalu berkaitan dengan governance.

17. Konvergensi Quantum Computing, Blockchain, dan Data Science

Konvergensi ketiganya dapat membentuk ekosistem baru.

17.1 Quantum-Enhanced Analytics dengan Provenance Blockchain

Data dikumpulkan dari banyak organisasi. Blockchain mencatat asal, izin, dan transformasi. Submasalah optimasi dikirim ke quantum processor. Hasil, parameter, dan versi circuit dicatat pada ledger.

Manfaatnya:

- Analisis berkemampuan tinggi.
- Auditabilitas.
- Reproduksi.
- Pembagian hak.
- Kepercayaan lintas organisasi.

17.2 Blockchain untuk Akses Quantum Cloud

Quantum processor kemungkinan tetap menjadi sumber daya langka dan mahal.

Blockchain dapat digunakan untuk:

- Mengatur reservasi.
- Mencatat penggunaan.
- Membayar resource.
- Mengaudit job.
- Memverifikasi service-level agreement.
- Mengelola konsorsium.

Namun, database biasa mungkin lebih efisien apabila semua pihak mempercayai satu penyedia. Blockchain hanya diperlukan ketika terdapat masalah kepercayaan atau koordinasi lintas institusi.

17.3 Quantum Randomness

Perangkat kuantum dapat menghasilkan random number yang bersumber dari proses fisik kuantum.

Randomness penting bagi:

- Kriptografi.
- Sampling.
- Simulasi.
- Konsensus.
- Eksperimen.

Blockchain dapat mencatat bukti sumber dan distribusi randomness.

17.4 Verifiable Quantum Computation

Pada masa depan, organisasi mungkin menggunakan quantum cloud tanpa memiliki perangkat.

Pertanyaan penting:

Bagaimana pengguna mengetahui bahwa penyedia benar-benar menjalankan komputasi kuantum sesuai permintaan?

Riset verifiable quantum computation dan cryptographic proof dapat membantu. Blockchain dapat merekam proof dan audit trail, tetapi verifikasi kuantum memerlukan protokol khusus.

17.5 Decentralized Science

Decentralized science dapat menggunakan blockchain untuk:

- Pendanaan penelitian.

- Kepemilikan dataset.
- Provenance eksperimen.
- Replikasi.
- Pembagian royalti.
- Kolaborasi global.

Quantum computing dapat menghasilkan data simulasi ilmiah, sedangkan Data Science menganalisis hasilnya.

18. Arsitektur Data Science Masa Depan

Arsitektur masa depan kemungkinan bersifat berlapis.

18.1 Lapisan Akuisisi

Sumber:

- Sensor.
- Satelit.
- Perangkat kesehatan.
- Sistem transaksi.
- Laboratorium.
- Quantum experiments.
- Media digital.

18.2 Lapisan Edge

Edge computing melakukan:

- Penyaringan.
- Anonimisasi.

- Deteksi awal.
- Federated training.
- Pengurangan data.

18.3 Lapisan Data Fabric

Data fabric menghubungkan:

- Data warehouse.
- Data lake.
- Lakehouse.
- Knowledge graph.
- Metadata catalog.
- Feature store.

18.4 Lapisan Trust

Blockchain atau distributed ledger digunakan untuk:

- Identitas.
- Provenance.
- Persetujuan.
- Hak akses.
- Audit.
- Lisensi.
- Model registry.

18.5 Lapisan Privacy

Teknologi yang digunakan:

- Differential privacy.

- Federated learning.
- Secure multiparty computation.
- Homomorphic encryption.
- Zero-knowledge proof.
- Trusted execution environment.

18.6 Lapisan Komputasi

- CPU.
- GPU.
- TPU.
- HPC.
- Quantum processor.
- Quantum annealer.

18.7 Lapisan Intelligence

- Machine learning.
- Deep learning.
- Causal inference.
- Generative AI.
- Quantum machine learning.
- Optimization.
- Simulation.

18.8 Lapisan Governance

- Kebijakan.
- Risk management.

- Ethics.
- Compliance.
- Human oversight.
- Audit.
- Incident response.

Arsitektur ini menunjukkan bahwa blockchain dan quantum computing merupakan bagian dari ekosistem, bukan pengganti seluruh sistem.

19. Data Provenance sebagai Fondasi Kepercayaan AI

Model AI hanya dapat dipercaya apabila data dan prosesnya dapat ditelusuri.

Data provenance dapat menjawab empat pertanyaan:

1. **Origin:** dari mana data berasal?
2. **Transformation:** apa yang dilakukan terhadap data?
3. **Authority:** siapa yang memiliki kewenangan?
4. **Purpose:** untuk tujuan apa data digunakan?

Blockchain dapat memperkuat provenance karena catatan perubahan disalin di beberapa node dan dihubungkan melalui hash.

Namun, istilah “immutable” perlu dipahami secara hati-hati. Blockchain tidak membuat kenyataan menjadi benar. Blockchain membuat perubahan catatan menjadi sulit dilakukan tanpa terdeteksi.

Prinsip yang tepat adalah:

Blockchain dapat menjamin integritas catatan setelah pencatatan, tetapi tidak menjamin kebenaran fakta sebelum pencatatan.

Masalah hubungan dunia fisik dan digital disebut oracle problem.

Apabila sensor rusak, blockchain akan menyimpan hash dari data yang salah. Oleh sebab itu, Data Science masa depan membutuhkan:

- Sensor terkalibrasi.
 - Identitas sumber.
 - Validasi silang.
 - Anomaly detection.
 - Audit lapangan.
 - Governance.
-

20. Blockchain untuk Model AI yang Dapat Diaudit

Model AI mengalami perubahan sepanjang siklus hidup.

Tahapnya meliputi:

- Pengembangan.
- Pelatihan.
- Validasi.
- Approval.
- Deployment.
- Monitoring.
- Retraining.
- Retirement.

Ledger dapat mencatat:

- Model hash.
- Dataset hash.

- Kode.
- Hyperparameter.
- Metrik.
- Approval.
- Tanggal.
- Pengembang.
- Validator.

Dalam sektor berisiko tinggi, catatan tersebut membantu menunjukkan bahwa organisasi telah menjalankan proses yang wajar.

Contohnya, bank menggunakan model credit scoring. Ketika nasabah menggugat keputusan, organisasi dapat menunjukkan:

- Versi model.
- Variabel.
- Waktu prediksi.
- Kebijakan yang berlaku.
- Approval.
- Penjelasan.
- Override.

Blockchain bukan satu-satunya teknologi untuk audit trail. Database append-only juga dapat digunakan. Blockchain bernilai ketika catatan perlu dipercaya oleh banyak pihak dengan kepentingan berbeda.

21. Implikasi bagi Kesehatan

21.1 Quantum Computing

Quantum simulation dapat mendukung penemuan molekul. QML dapat dieksplorasi untuk klasifikasi dan prediksi.

Namun, bukti keunggulan QML dalam kesehatan digital belum konsisten. Kajian tahun 2025 menemukan keterbatasan rigour, data encoding, noise, dan skalabilitas. ([Nature](#))

21.2 Blockchain

Blockchain dapat mendukung:

- Consent management.
- Rekam provenance.
- Sharing lintas rumah sakit.
- Uji klinis.
- Rantai pasok obat.
- Credential tenaga kesehatan.

21.3 Arsitektur yang Realistis

Data pasien disimpan off-chain dan terenkripsi. Blockchain mencatat consent, hash, dan hak akses. Federated learning memungkinkan rumah sakit membangun model bersama. ZKP membuktikan kepatuhan tanpa membuka data.

Risiko:

- Kebocoran metadata.
- Identitas ulang.
- Ketidaksetaraan akses.
- Model bias.
- Smart contract bug.
- Kesalahan klinis.

22. Implikasi bagi Keuangan

Quantum computing berpotensi digunakan untuk:

- Optimasi portofolio.
- Pricing.
- Monte Carlo.
- Credit risk.
- Fraud.
- Scenario analysis.

Blockchain digunakan untuk:

- Settlement.
- Tokenisasi.
- Identitas.
- Trade finance.
- Audit.
- Data sharing.
- Smart contract.

Ancaman kuantum sangat relevan karena sistem keuangan bergantung pada tanda tangan digital, sertifikat, dan komunikasi terenkripsi.

Lembaga keuangan perlu mengembangkan cryptographic inventory.

Inventaris tersebut memetakan:

- Algoritma.
- Kunci.
- Sertifikat.

- Aplikasi.
- Vendor.
- Data yang dilindungi.
- Umur kerahasiaan.
- Ketergantungan.

Migrasi pascakuantum perlu dipandang sebagai program transformasi risiko, bukan proyek IT kecil.

23. Implikasi bagi Rantai Pasok

Blockchain dapat merekam:

- Asal bahan.
- Sertifikasi.
- Pergerakan.
- Kepemilikan.
- Temperatur.
- Kondisi.
- Pembayaran.

Data Science dapat memprediksi:

- Permintaan.
- Keterlambatan.
- Risiko pemasok.
- Kerusakan.
- Emisi.

- Fraud.

Quantum optimization dapat membantu:

- Routing.
- Penjadwalan.
- Network design.
- Inventory allocation.

Arsitektur ini relevan bagi pangan, farmasi, kehutanan, pertambangan, energi, dan maritim.

Dalam kehutanan, misalnya:

1. Data satelit memantau tutupan.
2. Sensor dan drone mengumpulkan data.
3. Blockchain mencatat provenance dan izin.
4. Data Science mendeteksi perubahan.
5. Quantum optimization mengatur rute pengawasan.
6. Smart contract mengelola insentif konservasi.

Namun, teknologi tidak menggantikan verifikasi lapangan dan hak masyarakat lokal.

24. Implikasi bagi Lingkungan dan Perubahan Iklim

Data Science iklim menghadapi sistem berdimensi tinggi dan ketidakpastian besar.

Quantum computing dapat membantu simulasi tertentu, optimasi energi, dan material hijau.

Blockchain dapat mendukung:

- Carbon accounting.
- Renewable energy certificate.
- Traceability.
- Climate finance.
- Pembayaran jasa ekosistem.

Tetapi blockchain sendiri dapat memiliki jejak energi.

Proof-of-work membutuhkan konsumsi energi tinggi karena keamanan dibangun melalui kompetisi komputasi. Proof-of-stake menggunakan mekanisme berbeda dan secara umum membutuhkan energi lebih rendah. Peralihan Ethereum menuju proof-of-stake menunjukkan bahwa desain consensus memiliki dampak besar terhadap energi. ([Frontiers](#))

Keberlanjutan tidak boleh dinilai hanya berdasarkan konsumsi listrik. Perlu dipertimbangkan:

- Perangkat keras.
- Pendinginan.
- Lokasi energi.
- E-waste.
- Replikasi.
- Social value.
- Sistem yang digantikan.

Komputer kuantum juga membutuhkan infrastruktur khusus, termasuk pendinginan kriogenik untuk sejumlah platform. Karena itu, klaim bahwa komputasi kuantum selalu lebih hijau belum dapat dibuat secara umum.

25. Risiko Etika

25.1 Konsentrasi Kekuasaan Quantum Computing

Quantum processor membutuhkan modal, laboratorium, dan keahlian tinggi. Infrastruktur dapat terkonsentrasi pada sejumlah negara dan perusahaan.

Risikonya:

- Ketergantungan.
- Ketimpangan akses.
- Monopoli pengetahuan.
- Kedaulatan data.
- Ketimpangan riset.

25.2 Ilusi Desentralisasi Blockchain

Sistem dapat disebut terdesentralisasi tetapi tetap dikuasai oleh:

- Validator besar.
- Exchange.
- Cloud provider.
- Core developer.
- Pemilik token.
- Penyedia oracle.

Desentralisasi perlu diukur, bukan diasumsikan.

25.3 Permanensi dan Hak Menghapus

Blockchain sulit diubah, sedangkan regulasi dapat memberikan hak koreksi dan penghapusan.

Solusi dapat berupa:

- Menyimpan data off-chain.

- Menyimpan hash saja.
- Encryption key deletion.
- Chameleon hash.
- Permissioned governance.

Tidak ada solusi yang sempurna untuk semua kasus.

25.4 Automated Governance

Smart contract dapat mengeksekusi aturan secara otomatis.

Risikonya:

- Aturan tidak adil.
- Bug.
- Tidak ada ruang banding.
- Tidak mempertimbangkan konteks.
- Memindahkan kekuasaan kepada pembuat kode.

25.5 Quantum Divide

Masyarakat dapat mengalami kesenjangan baru antara pihak yang memiliki quantum capability dan yang tidak.

Kesenjangan tersebut dapat memengaruhi:

- Riset.
- Farmasi.
- Keamanan.
- Keuangan.
- Pertahanan.
- Industri.

26. Keamanan dan Tata Kelola

26.1 Security by Design

Sistem harus dirancang aman sejak awal.

Prinsipnya:

- Least privilege.
- Zero trust.
- Encryption.
- Segmentation.
- Key management.
- Logging.
- Incident response.
- Post-quantum readiness.

26.2 Privacy by Design

Data yang dikumpulkan harus minimum.

Organisasi perlu menentukan:

- Dasar pemrosesan.
- Tujuan.
- Retensi.
- Hak akses.
- Transfer.
- Penghapusan.

26.3 Quantum Readiness Assessment

Assessment meliputi:

1. Inventarisasi kriptografi.
2. Klasifikasi data.
3. Penilaian umur kerahasiaan.
4. Identifikasi vendor.
5. Prioritas migrasi.
6. Uji algoritma pascakuantum.
7. Crypto-agility.
8. Business continuity.

26.4 Blockchain Governance

Governance harus menjelaskan:

- Siapa node operator?
- Siapa mengubah protokol?
- Bagaimana sengketa diselesaikan?
- Siapa bertanggung jawab?
- Bagaimana data salah diperbaiki?
- Bagaimana peserta keluar?
- Bagaimana biaya dibagi?

26.5 Model Governance

Model kuantum atau klasik tetap memerlukan:

- Dokumentasi.
- Validasi.
- Benchmark.

- Monitoring.
- Explainability.
- Stress testing.
- Human oversight.

27. Explainability pada Quantum Machine Learning

Model kuantum berpotensi semakin sulit dijelaskan karena melibatkan quantum state dan pengukuran probabilistik.

Pertanyaan explainability meliputi:

- Fitur apa yang memengaruhi prediksi?
- Apakah model stabil?
- Apakah circuit mempelajari pola substantif?
- Apakah hasil dapat direproduksi?
- Apa pengaruh noise?
- Apakah quantum component memberikan nilai?

Pendekatan yang mungkin:

- Feature importance klasik.
- Analisis circuit.
- Sensitivity.
- Counterfactual.
- Surrogate model.
- Ablation.
- Measurement attribution.

Explainability QML belum sematang explainable AI klasik. Dalam keputusan berisiko tinggi, organisasi mungkin memilih model hibrida dengan quantum component terbatas dan decision layer yang lebih transparan.

28. Blockchain dan Kualitas Data

Blockchain sering dikaitkan dengan integritas, tetapi kualitas data mencakup lebih banyak dimensi:

- Accuracy.
- Completeness.
- Consistency.
- Timeliness.
- Validity.
- Relevance.

Blockchain terutama membantu:

- Traceability.
- Non-repudiation.
- Tamper evidence.
- Versioning.

Ia tidak otomatis memperbaiki:

- Nilai hilang.
- Kesalahan sensor.
- Bias sampling.
- Definisi tidak konsisten.
- Data tidak relevan.

Karena itu, data quality management tetap diperlukan.

Smart contract dapat menegakkan aturan format, tetapi tidak selalu memahami realitas substantif.

29. Dampak terhadap Profesi Data Scientist

Data scientist masa depan memerlukan kompetensi baru.

29.1 Quantum Literacy

Tidak semua data scientist harus menjadi fisikawan kuantum. Namun, mereka perlu memahami:

- Qubit.
- Circuit.
- Noise.
- Quantum advantage.
- Data encoding.
- Keterbatasan.
- Hybrid workflow.

29.2 Cryptographic Literacy

Data scientist perlu memahami:

- Hash.
- Digital signature.
- Encryption.
- Key management.
- Post-quantum migration.
- Zero-knowledge proof.

29.3 Distributed Systems

Kompetensi mencakup:

- Consensus.
- Smart contract.
- Off-chain storage.
- Federated learning.
- Distributed identity.

29.4 Governance

Data scientist harus memahami:

- Privacy.
- Fairness.
- Accountability.
- Audit.
- Regulasi.
- Hak masyarakat.

29.5 Domain Expertise

Teknologi semakin kompleks, sehingga pengetahuan domain semakin penting.

Model quantum atau blockchain tidak dapat menentukan sendiri:

- Tujuan.
- Nilai.
- Risiko.
- Materialitas.

- Konsekuensi.
-

30. Dampak terhadap Manajemen

30.1 Strategi Teknologi

Manajemen perlu membedakan:

- Teknologi yang siap diterapkan.
- Teknologi yang perlu diuji.
- Teknologi yang perlu dipantau.
- Teknologi yang belum relevan.

Blockchain untuk provenance mungkin siap dalam kasus konsorsium tertentu. Quantum machine learning mungkin masih bersifat eksperimen dalam banyak aplikasi data klasik.

30.2 Portfolio Approach

Organisasi dapat membagi investasi:

- 70 persen pada penguatan data klasik.
- 20 persen pada eksperimen teknologi baru.
- 10 persen pada riset jangka panjang.

Proporsi tersebut bersifat ilustratif. Intinya adalah jangan mengorbankan kualitas data dasar demi mengejar teknologi futuristik.

30.3 Build, Buy, atau Partner

Quantum computing kemungkinan diakses melalui cloud. Blockchain dapat dibangun secara internal atau konsorsium.

Keputusan mempertimbangkan:

- Kompetensi.

- Data sensitivity.
- Vendor lock-in.
- Biaya.
- Interoperabilitas.
- Regulasi.
- Kedaulatan.

30.4 New Risk Categories

Manajemen perlu memasukkan:

- Quantum risk.
- Cryptographic obsolescence.
- Smart contract risk.
- Consensus risk.
- Oracle risk.
- Token incentive risk.
- Model provenance risk.

31. Skenario Masa Depan Data Science

Skenario bukan prediksi pasti. Skenario membantu organisasi mempersiapkan beberapa kemungkinan.

31.1 Skenario Pertama: Classical AI Dominance

Komputer klasik, GPU, dan accelerator terus berkembang. Quantum computing tidak memberikan keunggulan praktis yang luas.

Blockchain digunakan secara terbatas untuk audit dan settlement.

Implikasi:

- Investasi utama tetap pada data engineering.
- QML menjadi niche.
- Quantum-inspired algorithms lebih penting.
- Post-quantum security tetap dibutuhkan.

31.2 Skenario Kedua: Hybrid Quantum Acceleration

Komputer kuantum fault-tolerant berkembang untuk submasalah tertentu.

Organisasi menggunakan QPU melalui cloud untuk:

- Simulasi.
- Optimasi.
- Sampling.
- Risk analytics.

Data Science tetap klasik pada sebagian besar pipeline.

31.3 Skenario Ketiga: Decentralized Data Economy

Regulasi privasi dan ketidakpercayaan terhadap platform terpusat mendorong:

- Federated learning.
- Personal data wallet.
- Blockchain identity.
- Data marketplace.
- ZKP.

Individu memiliki kontrol lebih besar atas data.

31.4 Skenario Keempat: Quantum Security Crisis

Perkembangan quantum computing lebih cepat daripada migrasi.

Sebagian sistem mengalami krisis keamanan. Organisasi yang tidak memiliki crypto-agility menghadapi biaya tinggi.

31.5 Skenario Kelima: Trusted Intelligence Infrastructure

Quantum computing, blockchain, privacy technology, dan AI terintegrasi.

Model dapat:

- Menggunakan data tanpa membuka data mentah.
- Membuktikan proses.
- Mencatat provenance.
- Menyediakan audit.
- Menggunakan accelerator kuantum.

Ini merupakan skenario paling transformatif, tetapi membutuhkan standardisasi dan tata kelola global.

32. Tahapan Waktu Perkembangan

32.1 Jangka Pendek: 2026–2030

Fokus utama:

- Penguatan data governance.
- Eksperimen QML.
- Hybrid quantum-classical prototype.
- Blockchain provenance.
- Federated learning.
- Inventarisasi kriptografi.
- Migrasi awal PQC.
- Pendidikan quantum literacy.

Pada periode ini, sebagian besar QML masih berada pada pilot atau riset. Blockchain enterprise akan dipilih berdasarkan use case, bukan hype.

32.2 Jangka Menengah: 2030–2040

Kemungkinan:

- Logical qubit lebih matang.
- Quantum cloud lebih stabil.
- Penggunaan pada kimia dan material.
- Optimasi industri khusus.
- Post-quantum cryptography menjadi standar.
- Blockchain lama harus bermigrasi.
- Verifiable AI berkembang.
- Data marketplace terdesentralisasi tumbuh.

32.3 Jangka Panjang: 2040–2050

Kemungkinan:

- Quantum accelerator menjadi bagian HPC.
- Data kuantum menjadi sumber data penting.
- Quantum-native machine learning berkembang.
- Kriptografi klasik rentan ditinggalkan.
- AI governance menggunakan proof.
- Digital identity lebih terdesentralisasi.

Ketidakpastian semakin besar ketika horizon waktu semakin panjang.

33. Agenda Strategis bagi Indonesia

Indonesia memiliki kebutuhan besar terhadap Data Science dalam:

- Pangan.
- Energi.
- Kesehatan.
- Kehutanan.
- Kelautan.
- Transportasi.
- Keuangan.
- Pemerintahan.
- Pendidikan.
- Mitigasi bencana.

BRIN memiliki Pusat Riset Fisika Kuantum dan mengembangkan kegiatan penelitian serta edukasi kuantum. BRIN juga mengelola infrastruktur high-performance computing yang dapat menjadi fondasi menuju eksperimen hybrid computing. ([BRIN - Badan Riset dan Inovasi Nasional](#))

Bappenas telah menempatkan transformasi digital, kedaulatan data, Satu Data Indonesia, serta pengembangan industri digital dalam agenda pembangunan jangka panjang. Hal tersebut memberikan dasar institusional bagi pengembangan ekosistem data yang lebih terintegrasi. ([Bappenas Library](#))

33.1 Membangun Fondasi Data

Sebelum mengejar quantum computing, Indonesia perlu memperkuat:

- Kualitas data.
- Interoperabilitas.
- Metadata.

- Talenta.
- Cloud nasional.
- HPC.
- Cybersecurity.
- Tata kelola.

33.2 Pusat Riset Quantum-Data Science

Perguruan tinggi dan BRIN dapat membentuk program lintas disiplin:

- Fisika.
- Matematika.
- Ilmu komputer.
- Statistika.
- Kimia.
- Manajemen.
- Hukum.
- Etika.

33.3 Quantum-Safe Government

Pemerintah perlu memetakan:

- Certificate.
- Infrastruktur identitas.
- Arsip jangka panjang.
- Pertahanan.
- Kesehatan.
- Keuangan.

- Data kependudukan.

33.4 Blockchain Konsorsium

Use case potensial:

- Sertifikasi komoditas.
- Traceability pangan.
- Legalitas kayu.
- Rantai pasok obat.
- Credential pendidikan.
- Penelitian.
- Carbon market.

33.5 Pengembangan Talenta

Kurikulum perlu mencakup:

- Linear algebra.
- Probability.
- Quantum information.
- Machine learning.
- Distributed systems.
- Cryptography.
- Governance.
- Ethics.

34. Roadmap Organisasi

Tahap 1: Data Fundamentals

Organisasi memastikan:

- Data tersedia.
- Definisi konsisten.
- Metadata.
- Security.
- Governance.
- MLOps.

Tanpa fondasi ini, quantum atau blockchain tidak memberikan nilai.

Tahap 2: Use-Case Mapping

Identifikasi masalah:

- Apakah masalah komputasi?
- Apakah masalah kepercayaan?
- Apakah masalah privasi?
- Apakah masalah koordinasi?

Quantum computing cocok apabila hambatan utama adalah komputasi tertentu.

Blockchain cocok apabila hambatan utama adalah trust lintas pihak.

Tahap 3: Readiness Assessment

Quantum readiness:

- Kompetensi.
- Problem formulation.
- Classical benchmark.
- Cloud access.

- Security.

Blockchain readiness:

- Participants.
- Governance.
- Incentives.
- Data model.
- Legal basis.

Tahap 4: Prototype

Prototipe harus memiliki:

- Baseline klasik.
- Metrik.
- Cost.
- Risk.
- Exit criteria.

Tahap 5: Independent Evaluation

Evaluasi:

- Apakah performa meningkat?
- Apakah biaya masuk akal?
- Apakah sistem lebih aman?
- Apakah pengguna mempercayai?
- Apakah dapat diintegrasikan?

Tahap 6: Scale

Skalabilitas mencakup:

- Teknologi.
- Organisasi.
- Regulasi.
- Kompetensi.
- Vendor.

Tahap 7: Continuous Monitoring

Pantau:

- Performa.
- Security.
- Drift.
- Quantum developments.
- Cryptographic standards.
- Protocol governance.

35. Kerangka Pengambilan Keputusan Teknologi

Sebelum memilih quantum computing, tanyakan:

1. Apakah masalah memiliki struktur yang sesuai?
2. Apakah terdapat algoritma kuantum?
3. Apakah data encoding efisien?
4. Apakah output yang dibutuhkan terbatas?
5. Apakah baseline klasik sudah dioptimalkan?
6. Apakah keuntungan bertahan setelah overhead?
7. Apakah perangkat tersedia?

8. Apakah manfaat ekonomi jelas?

Sebelum memilih blockchain, tanyakan:

1. Apakah terdapat banyak pihak?
2. Apakah pihak tidak sepenuhnya saling percaya?
3. Apakah shared ledger dibutuhkan?
4. Apakah satu database pusat cukup?
5. Apakah aturan dapat dikodekan?
6. Siapa mengelola governance?
7. Bagaimana data salah diperbaiki?
8. Apakah privasi terlindungi?
9. Apakah biaya konsensus sebanding?

Apabila satu database terpercaya dapat menyelesaikan masalah dengan lebih sederhana, blockchain mungkin tidak diperlukan.

36. Agenda Penelitian Masa Depan

36.1 Benchmark QML yang Realistis

Penelitian perlu menggunakan:

- Dataset dunia nyata.
- Baseline kuat.
- Hardware nyata.
- Noise.
- Total runtime.
- Energy.

- Data loading.
- Measurement cost.

36.2 Quantum Advantage untuk Data Klasik

Perlu diidentifikasi struktur data yang benar-benar memberikan keuntungan.

36.3 Explainable QML

Diperlukan metode interpretasi yang stabil.

36.4 Blockchain Provenance Standard

Diperlukan standar untuk:

- Dataset.
- Model.
- Transformasi.
- Consent.
- Audit.

36.5 Verifiable Machine Learning

Riset perlu menggabungkan:

- ZKP.
- Federated learning.
- Secure computation.
- Model governance.

36.6 Quantum-Safe Blockchain Migration

Masalah:

- Legacy address.

- Hybrid signature.
- Key recovery.
- Governance.
- Cross-chain.
- Performance.

36.7 Sustainability

Penelitian harus membandingkan total lifecycle cost.

36.8 Human and Institutional Factors

Teknologi tidak berhasil hanya karena protokolnya benar.

Penelitian perlu menilai:

- Trust.
- Adoption.
- Power.
- Incentives.
- Regulation.
- Culture.
- Inequality.

37. Refleksi Kritis

Quantum computing dan blockchain sering ditempatkan dalam narasi revolusi. Narasi semacam itu dapat mendorong investasi, tetapi juga menciptakan ekspektasi berlebihan.

Komputasi kuantum bukan komputer yang selalu lebih cepat. Keuntungannya bergantung pada algoritma, data, input, output, hardware, dan error correction.

Blockchain bukan database yang selalu lebih aman. Keuntungannya bergantung pada governance, consensus, node, cryptography, dan kualitas input.

Data Science bukan proses yang otomatis objektif. Hasilnya bergantung pada tujuan, definisi, data, model, dan nilai manusia.

Konvergensi teknologi tidak menghilangkan persoalan lama. Ia dapat memperbesar persoalan tersebut.

Model yang bias dapat menjadi lebih cepat dengan quantum computing.

Data yang salah dapat menjadi lebih sulit diperbaiki setelah dicatat pada blockchain.

Smart contract yang tidak adil dapat mengeksekusi diskriminasi secara konsisten.

Oleh sebab itu, pertanyaan yang tepat bukan:

Seberapa canggih teknologi ini?

Pertanyaan yang lebih penting adalah:

Masalah apa yang diselesaikan, siapa yang memperoleh manfaat, siapa yang menanggung risiko, bagaimana kesalahan diperbaiki, dan siapa yang bertanggung jawab?

38. Data Science Berorientasi Kemanusiaan

Masa depan Data Science tidak boleh hanya diukur melalui:

- Akurasi.
- Kecepatan.

- Throughput.
- Jumlah qubit.
- Jumlah transaksi.

Ukuran lain diperlukan:

- Fairness.
- Privacy.
- Accessibility.
- Sustainability.
- Accountability.
- Social value.
- Human dignity.

Quantum computing dan blockchain seharusnya digunakan untuk memperluas kemampuan manusia, bukan mengurangi manusia menjadi objek data.

Dalam kesehatan, tujuan akhirnya adalah kesejahteraan pasien.

Dalam pendidikan, tujuan akhirnya adalah perkembangan manusia.

Dalam pemerintahan, tujuan akhirnya adalah pelayanan dan keadilan.

Dalam bisnis, tujuan akhirnya bukan hanya efisiensi, tetapi penciptaan nilai yang berkelanjutan.

39. Prinsip-Prinsip Masa Depan Data Science

39.1 Problem First

Teknologi dipilih setelah masalah dipahami.

39.2 Classical Benchmark First

Solusi kuantum harus dibandingkan dengan metode klasik terbaik.

39.3 Trust but Verify

Blockchain tidak menghilangkan kebutuhan verifikasi.

39.4 Privacy by Design

Privasi dirancang sejak awal.

39.5 Crypto-Agility

Sistem harus dapat mengganti kriptografi.

39.6 Human Accountability

Tanggung jawab tetap berada pada manusia dan institusi.

39.7 Hybrid Architecture

Gunakan teknologi sesuai keunggulannya.

39.8 Proportionality

Kompleksitas harus sebanding dengan manfaat.

39.9 Sustainability

Hitung dampak energi dan lingkungan.

39.10 Continuous Learning

Model, ancaman, dan teknologi terus berubah.

40. Kesimpulan

Masa depan Data Science akan dibentuk oleh peningkatan volume data, kompleksitas model, kebutuhan komputasi, tuntutan privasi, serta kebutuhan akan kepercayaan dan auditabilitas. Quantum computing dan blockchain menawarkan jawaban terhadap bagian berbeda dari tantangan tersebut.

Quantum computing berpotensi memperluas kemampuan komputasi bagi kelas masalah tertentu. Potensinya paling kuat pada simulasi kuantum, optimasi, sampling, persamaan linear, dan analisis data kuantum. Quantum machine learning membuka ruang bagi feature mapping, generative modelling, dan hybrid learning.

Namun, keunggulan teoretis tidak otomatis menjadi keuntungan praktis. Data loading, output measurement, noise, error correction, barren plateau, dan metode klasik yang terus berkembang merupakan hambatan penting. Bukti empiris saat ini belum menunjukkan bahwa QML secara konsisten mengungguli machine learning klasik pada data dunia nyata. Karena itu, pendekatan yang tepat adalah eksperimen disiplin dengan benchmark yang kuat.

Blockchain memberikan kontribusi melalui trust, provenance, traceability, audit, smart contract, dan pembelajaran terdistribusi. Teknologi ini dapat membantu memastikan bahwa dataset, transformasi, model, consent, dan keputusan dapat ditelusuri. Blockchain juga dapat mendukung data marketplace, federated learning, dan verifiable AI.

Namun, blockchain bukan obat bagi semua masalah data. Ia tidak menjamin kebenaran input, tidak otomatis menjaga privasi, dan tidak selalu lebih efisien daripada database pusat. Implementasinya menghadapi scalability, governance, interoperability, dan legal uncertainty.

Pertemuan quantum computing dan blockchain menghasilkan ancaman besar terhadap kriptografi. Algoritma Shor mengancam RSA dan elliptic-curve cryptography. Algoritma Grover memengaruhi tingkat keamanan efektif pencarian kunci dan hash. Karena itu, migrasi menuju post-quantum cryptography harus dimulai sebelum komputer kuantum kriptografis tersedia.

Masa depan yang paling realistis adalah arsitektur hibrida:

- Komputer klasik mengelola sebagian besar data.

- GPU menangani deep learning.
- HPC menjalankan simulasi.
- Quantum processor menangani submasalah tertentu.
- Blockchain menyediakan trust layer.
- Privacy technologies melindungi data.
- Manusia menetapkan tujuan dan bertanggung jawab.

Bagi Indonesia, prioritas utama adalah memperkuat kualitas data, interoperabilitas, keamanan siber, HPC, talenta, riset kuantum, tata kelola blockchain, dan kesiapan pascakuantum. Teknologi futuristik tidak boleh menjadi alasan mengabaikan fondasi.

Masa depan Data Science bukan hanya masa depan mesin yang lebih cepat. Ia adalah masa depan sistem pengetahuan yang lebih kompleks. Tantangannya adalah memastikan bahwa sistem tersebut tidak hanya kuat secara komputasi, tetapi juga benar secara metodologis, aman secara teknis, sah secara hukum, adil secara sosial, dan bertanggung jawab secara moral.

Glosarium

Amplitude

Besaran kompleks dalam keadaan kuantum yang menentukan probabilitas hasil pengukuran.

Blockchain

Distributed ledger yang menggunakan kriptografi dan consensus untuk memelihara catatan bersama.

Blockchain Trilemma

Trade-off antara decentralization, security, dan scalability dalam desain blockchain.

Barren Plateau

Kondisi fungsi kerugian quantum circuit memiliki gradien sangat kecil sehingga sulit dilatih.

Classical Computing

Komputasi menggunakan bit klasik.

Consensus Mechanism

Metode bagi node blockchain untuk menyepakati status ledger.

Crypto-Agility

Kemampuan sistem mengganti algoritma dan protokol kriptografi.

Data Availability

Ketersediaan data yang diperlukan untuk memverifikasi atau melanjutkan operasi sistem.

Data Lineage

Riwayat aliran dan transformasi data.

Data Provenance

Informasi mengenai asal-usul, kepemilikan, perubahan, dan penggunaan data.

Data Science

Bidang interdisipliner untuk memperoleh pengetahuan dan keputusan dari data.

Decentralized Science

Ekosistem penelitian yang memanfaatkan teknologi terdesentralisasi untuk koordinasi, pendanaan, dan provenance.

Differential Privacy

Metode perlindungan privasi dengan menambahkan noise terkontrol pada hasil analisis.

Distributed Ledger

Catatan digital yang direplikasi dan diselaraskan di beberapa node.

Entanglement

Korelasi kuantum yang tidak dapat dijelaskan sebagai keadaan independen.

Error Correction

Teknik mendeteksi dan memperbaiki kesalahan komputasi.

Federated Learning

Pembelajaran machine learning lintas lokasi tanpa memusatkan seluruh data mentah.

Fault-Tolerant Quantum Computing

Komputasi kuantum yang menggunakan koreksi kesalahan sehingga dapat menjalankan circuit panjang secara andal.

Feature Map

Transformasi data menuju ruang representasi baru.

Grover Algorithm

Algoritma kuantum untuk pencarian tidak terstruktur dengan percepatan kuadratik.

Hash

Fungsi yang mengubah input menjadi fingerprint digital.

Homomorphic Encryption

Kriptografi yang memungkinkan komputasi dilakukan terhadap data terenkripsi.

Hybrid Computing

Integrasi CPU, GPU, HPC, dan quantum processor.

Interference

Penguatan atau pengurangan amplitudo kuantum.

Interoperability

Kemampuan berbagai sistem untuk bertukar dan menggunakan informasi.

Logical Qubit

Qubit yang dilindungi koreksi kesalahan dan dibentuk dari sejumlah physical qubits.

Machine Learning

Metode komputasi yang mempelajari pola dari data.

NISQ

Noisy Intermediate-Scale Quantum, era perangkat kuantum dengan jumlah qubit terbatas dan noise tinggi.

Off-Chain Storage

Penyimpanan data di luar blockchain.

Oracle

Mekanisme yang memasukkan informasi eksternal ke dalam blockchain atau quantum algorithm.

Physical Qubit

Komponen fisik yang merepresentasikan qubit.

Post-Quantum Cryptography

Kriptografi klasik yang dirancang tahan terhadap serangan komputer kuantum.

Proof-of-Stake

Mekanisme consensus berdasarkan aset yang dipertaruhkan validator.

Proof-of-Work

Mekanisme consensus yang menggunakan kompetisi komputasi.

Qubit

Unit dasar informasi kuantum.

Quantum Advantage

Kondisi ketika komputer kuantum menjalankan tugas dengan sumber daya lebih baik daripada pendekatan klasik relevan.

Quantum Annealing

Pendekatan kuantum untuk mencari keadaan energi rendah dalam masalah optimasi.

Quantum Circuit

Rangkaian quantum gate yang menjalankan algoritma kuantum.

Quantum Computing

Paradigma komputasi berdasarkan prinsip mekanika kuantum.

Quantum Feature Map

Pengkodean data ke keadaan kuantum untuk membentuk ruang fitur.

Quantum Machine Learning

Integrasi quantum computing dan machine learning.

Quantum Processor Unit

Perangkat keras yang menjalankan quantum circuit.

Quantum Random Access Memory

Konsep memori untuk mengakses data dalam superposisi kuantum.

Quantum-Safe Blockchain

Blockchain yang menggunakan mekanisme kriptografi tahan kuantum.

Shor Algorithm

Algoritma kuantum untuk faktorisasi dan logaritma diskret.

Smart Contract

Program yang dieksekusi oleh jaringan blockchain.

Superposition

Keadaan kuantum sebagai kombinasi beberapa basis keadaan.

Tamper-Evident

Karakteristik sistem yang membuat perubahan tidak sah dapat diketahui.

Tokenization

Representasi hak atau aset dalam bentuk token digital.

Variational Quantum Algorithm

Algoritma hibrida yang menggabungkan quantum circuit dan optimizer klasik.

Zero-Knowledge Proof

Metode membuktikan kebenaran pernyataan tanpa membuka informasi dasar.

Daftar Pustaka

Abbas, A., Sutter, D., Zoufal, C., Lucchi, A., Figalli, A., & Woerner, S. (2021). The power of quantum neural networks. *Nature Computational Science*, 1, 403–409. <https://doi.org/10.1038/s43588-021-00084-1>

Asif, R. A. R., & Hassan, S. R. (2023). Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Frontiers in Blockchain*, 6, 1151724. <https://doi.org/10.3389/fbloc.2023.1151724>

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, 549, 195–202. <https://doi.org/10.1038/nature23474>

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>

Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Endo, S., Fujii, K., McClean, J. R., Mitarai, K., Yuan, X., Cincio, L., & Coles, P. J. (2021). Variational quantum algorithms. *Nature Reviews Physics*, 3, 625–644.
<https://doi.org/10.1038/s42254-021-00348-9>

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.
<https://doi.org/10.1109/ACCESS.2016.2566339>

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7), 1366–1385.
<https://doi.org/10.1109/TKDE.2017.2781227>

Donoho, D. (2017). 50 years of data science. *Journal of Computational and Graphical Statistics*, 26(4), 745–766.
<https://doi.org/10.1080/10618600.2017.1384734>

Dwork, C. (2006). Differential privacy. In *Automata, Languages and Programming* (pp. 1–12). Springer. https://doi.org/10.1007/11787006_1

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing* (pp. 169–178). ACM. <https://doi.org/10.1145/1536414.1536440>

Gokhale, S. S., Dhote, R. R., & Delhibabu, R. (2026). A review of quantum machine learning algorithms, applications, and emerging advantages. *Discover Computing*, 29, 226. <https://doi.org/10.1007/s10791-026-10085-1>

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1), 186–208.
<https://doi.org/10.1137/0218012>

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (pp. 212–219). ACM. <https://doi.org/10.1145/237814.237866>

Gupta, R. S., Wood, C. E., Engstrom, T., Pole, J. D., & Shrapnel, S. (2025). A systematic review of quantum machine learning for digital health. *npj Digital Medicine*, 8, 237. <https://doi.org/10.1038/s41746-025-01597-z>

Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103(15), 150502. <https://doi.org/10.1103/PhysRevLett.103.150502>

Havlíček, V., Córcoles, A. D., Temme, K., Harrow, A. W., Kandala, A., Chow, J. M., & Gambetta, J. M. (2019). Supervised learning with quantum-enhanced feature spaces. *Nature*, 567, 209–212. <https://doi.org/10.1038/s41586-019-0980-2>

Huang, H.-Y., Broughton, M., Mohseni, M., Babbush, R., Boixo, S., Neven, H., & McClean, J. R. (2021). Power of data in quantum machine learning. *Nature Communications*, 12, 2631. <https://doi.org/10.1038/s41467-021-22539-9>

Huang, H.-Y., Kueng, R., & Preskill, J. (2022). Quantum advantage in learning from experiments. *Science*, 376(6598), 1182–1186. <https://doi.org/10.1126/science.abn7293>

Huang, J., Kong, L., Chen, G., Xiang, Q., Chen, X., & Liu, X. (2023). Blockchain-based federated learning: A systematic survey. *IEEE Network*, 37(6), 150–157. <https://doi.org/10.1109/MNET.129.2200346>

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210. <https://doi.org/10.1561/22000000083>

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of*

the American Medical Informatics Association, 24(6), 1211–1220.

<https://doi.org/10.1093/jamia/ocx068>

Lloyd, S., Mohseni, M., & Rebentrost, P. (2014). Quantum principal component analysis. *Nature Physics*, 10, 631–633.

<https://doi.org/10.1038/nphys3029>

Ma, C., Li, J., Shi, L., Ding, M., Wang, T., Han, Z., & Poor, H. V. (2022). When federated learning meets blockchain: A new distributed learning paradigm. *IEEE Computational Intelligence Magazine*, 17(3), 26–33.

<https://doi.org/10.1109/MCI.2022.3180932>

McClean, J. R., Boixo, S., Smelyanskiy, V. N., Babbush, R., & Neven, H. (2018). Barren plateaus in quantum neural network training landscapes. *Nature Communications*, 9, 4812. <https://doi.org/10.1038/s41467-018-07090-4>

Montanaro, A. (2016). Quantum algorithms: An overview. *npj Quantum Information*, 2, 15023. <https://doi.org/10.1038/npjqi.2015.23>

National Institute of Standards and Technology. (2024a). *Module-lattice-based key-encapsulation mechanism standard* (FIPS 203).

<https://doi.org/10.6028/NIST.FIPS.203>

National Institute of Standards and Technology. (2024b). *Module-lattice-based digital signature standard* (FIPS 204).

<https://doi.org/10.6028/NIST.FIPS.204>

National Institute of Standards and Technology. (2024c). *Stateless hash-based digital signature standard* (FIPS 205).

<https://doi.org/10.6028/NIST.FIPS.205>

Ning, W., Zhu, Y., Song, C., Li, J., & Huang, H. (2024). Blockchain-based federated learning: A survey and new perspectives. *Applied Sciences*, 14(20), 9459. <https://doi.org/10.3390/app14209459>

- PajooH, H. H., Rashid, M., Alam, F., & Demidenko, S. (2021). IoT big data provenance scheme using blockchain on Hadoop ecosystem. *Journal of Big Data*, 8, 114. <https://doi.org/10.1186/s40537-021-00505-y>
- Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P. J., Aspuru-Guzik, A., & O'Brien, J. L. (2014). A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5, 4213. <https://doi.org/10.1038/ncomms5213>
- Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2, 79. <https://doi.org/10.22331/q-2018-08-06-79>
- Ramachandran, A., & Kantarcioglu, M. (2018). SmartProvenance: A distributed, blockchain-based data provenance system. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy* (pp. 35–42). ACM. <https://doi.org/10.1145/3176258.3176333>
- Rebentrost, P., Mohseni, M., & Lloyd, S. (2014). Quantum support vector machine for big data classification. *Physical Review Letters*, 113(13), 130503. <https://doi.org/10.1103/PhysRevLett.113.130503>
- Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117–2135. <https://doi.org/10.1080/00207543.2018.1533261>
- Schuld, M., Bocharov, A., Svore, K. M., & Wiebe, N. (2020). Circuit-centric quantum classifiers. *Physical Review A*, 101(3), 032308. <https://doi.org/10.1103/PhysRevA.101.032308>
- Schuld, M., & Killoran, N. (2019). Quantum machine learning in feature Hilbert spaces. *Physical Review Letters*, 122(4), 040504. <https://doi.org/10.1103/PhysRevLett.122.040504>
- Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on*

Foundations of Computer Science (pp. 124–134). IEEE.

<https://doi.org/10.1109/SFCS.1994.365700>

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. <https://doi.org/10.1137/S0097539795293172>

Wiebe, N., Braun, D., & Lloyd, S. (2012). Quantum algorithm for data fitting. *Physical Review Letters*, 109(5), 050505.

<https://doi.org/10.1103/PhysRevLett.109.050505>

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLOS ONE*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>

Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, 80, 103678.

<https://doi.org/10.1016/j.jisa.2023.103678>

Copilot for this article: ChatGPT, Access date: 14 July 2026. Author's account (Rudy C Tarumingkeng). <https://chatgpt.com/c/6a55aedb-5ee0-83ec-8a3c-cf2be8efd52e>