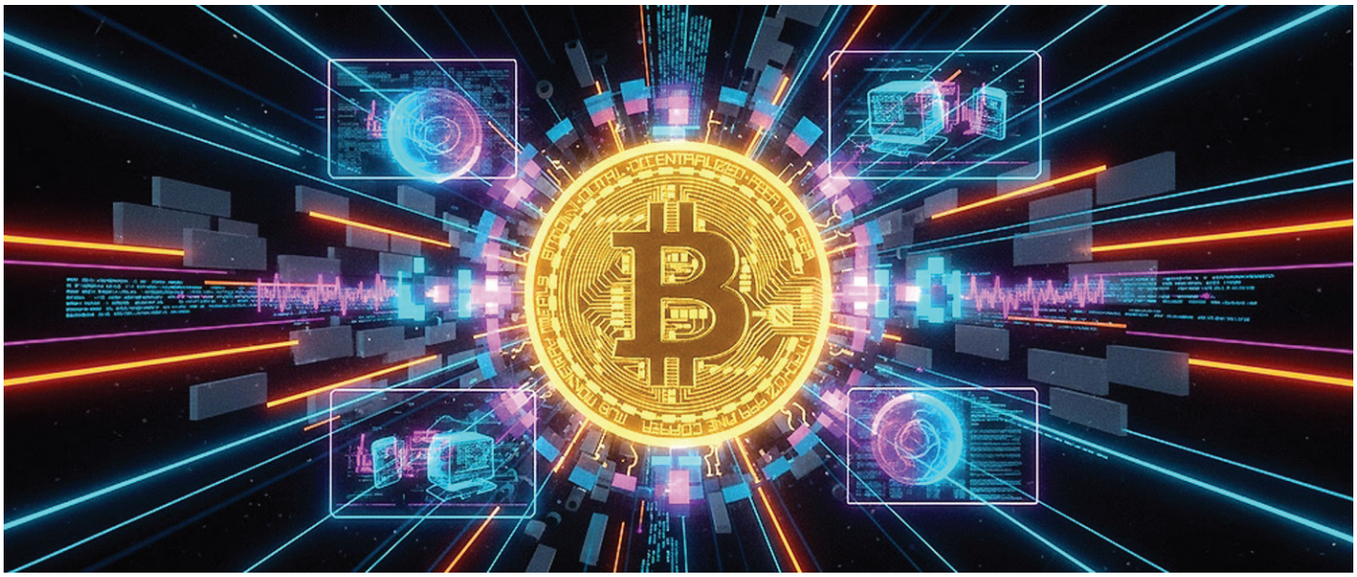
Máy tính lượng tử đang có bước phát triển nhanh chóng trong thời gian gần đây. Ảnh: ST.

Điện toán lượng tử: Nguy cơ mới đối với tài sản số

> **Điện toán lượng tử đang phát triển nhanh chóng và có thể tạo ra những thách thức chưa từng có đối với bảo mật của tài sản số. Các thuật toán lượng tử như Shor và Grover có khả năng làm suy yếu những nền tảng mật mã hiện nay. Tuy đây chưa phải là mối đe dọa tức thời, nhưng việc chuẩn bị từ sớm là cần thiết.**

Điện toán lượng tử có thể phá vỡ gì?

Hãy tưởng tượng một ngày không xa, khi những cỗ máy lượng tử siêu mạnh thức dậy, chỉ trong vài giây chúng có thể "mở khóa" hàng tỷ đô la tiền số đang ngủ yên trong ví Bitcoin hay Ethereum. Đó không phải phim khoa học viễn tưởng, mà là mối đe dọa thực tế mà cộng đồng tiền mã hóa đang phải đối mặt. Dựa trên những phân tích cốt lõi về mật mã hiện tại, bài báo này sẽ đưa bạn vào hành trình khám phá: điện toán lượng tử đang tiến gần đến mức độ nguy hiểm ra sao, và tại sao cộng đồng blockchain lại đang chạy đua với thời gian để bảo vệ tài sản số của hàng triệu người.



Tài sản số đang đối mặt với những rủi ro bảo mật mới khi điện toán lượng tử phát triển nhanh. Ảnh: ST.

Tất cả bắt nguồn từ nền tảng bảo mật cốt lõi của tiền số: mật mã khóa công khai. Bitcoin, Ethereum và hầu hết các blockchain khác đều dựa vào hai "lá chắn" chính - thuật toán chữ ký ECDSA trên đường cong elliptic secp256k1 và các hàm băm SHA-256 hay Keccak-256. Chúng hoạt động hoàn hảo với máy tính cổ điển, giúp xác thực giao dịch và bảo vệ quyền sở hữu. Nhưng khi điện toán lượng tử bước vào cuộc chơi, mọi thứ thay đổi hoàn toàn.

Hai "vũ khí" lượng tử chính là thuật toán Shor (phát minh năm 1994 bởi nhà toán học Peter Shor) và thuật toán Grover (1996 bởi Lov Grover). Chúng khai thác những nguyên lý kỳ diệu của thế giới lượng tử - chồng chập và vướng víu - để làm những việc mà máy tính cổ điển phải mất hàng tỷ năm mới làm nổi.

Thuật toán Shor - kẻ phá hoại huyền thoại - hoạt động dựa trên nguyên lý chồng chập lượng tử và biến đổi Fourier lượng tử nhanh chóng. Thay vì phải thử mò mẫm từng khả năng một cách chậm chạp như máy tính truyền thống, Shor tìm ra "chu kỳ ẩn" trong các số lớn chỉ trong thời gian đa thức (polynomial time). Kết quả là nó giải quyết triệt để bài toán logarit rời rạc trên đường cong elliptic (ECDLP) - nền tảng của ECDSA. Với chỉ khoảng 2.330 đến 2.619 qubit logic (đã được sửa lỗi hoàn chỉnh), một máy tính lượng tử chạy Shor có thể biến khóa công khai thành khóa riêng tư, mở toang bất kỳ ví nào đã từng lộ thông tin. Khi đó, kẻ tấn công có thể chiếm quyền truy cập và chuyển tài sản chỉ trong thời gian rất ngắn.

Còn thuật toán Grover thì "hiền lành" hơn nhiều: nó sử dụng kỹ thuật khuếch đại biên độ để tìm kiếm không cấu trúc trong không gian khổng lồ. Thay vì kiểm tra từng khả năng một cách tuyến tính, Grover chỉ cần khoảng căn bậc hai số lượng thử nghiệm - tức là mang lại tốc độ tăng gấp đôi (quadratic speedup). Đối với hàm băm SHA-256, điều này làm giảm mức bảo mật từ 2^{256} xuống còn khoảng 2^{128} - hiện vẫn được đánh giá là nằm ngoài khả năng tấn công thực tế của bất kỳ máy tính lượng tử nào trong nhiều thập kỷ tới [1]. Do đó, tính toàn vẹn của blockchain (mining và lịch sử khối) vẫn được bảo vệ vững chắc.

Rủi ro lớn nhất không nằm ở việc phá vỡ toàn bộ chuỗi khối, mà ở chính những ví đã từng gửi giao dịch - nơi khóa công khai đã bị "phơi bày" công khai. Hiện nay, khoảng 25% nguồn cung Bitcoin (tương đương 4,5-6,7 triệu BTC, trị giá nửa nghìn tỷ USD) đang rơi vào tình trạng dễ tổn thương này.

Mức độ đe dọa thực tế

Những người nắm giữ tài sản số đừng hoảng loạn quá sớm vì vào thời điểm hiện tại, điện toán lượng tử đang ở giai đoạn "bùng nổ nhưng chưa đủ nguy hiểm" [1]. Các ông lớn công nghệ đang chạy đua khốc liệt,

với những bước tiến đáng kinh ngạc về phần cứng, sửa lỗi và kiến trúc siêu máy tính. IBM vừa công bố bản thiết kế mới mang tính đột phá cho "Quantum-Centric Supercomputing" ngày 12/3/2026 [2], kết hợp processor lượng tử với GPU/CPU cổ điển để giải quyết vấn đề thực tế. Bộ xử lý Nighthawk của họ hiện đạt 120 qubit mỗi module, có thể ghép ba module thành 360 qubit và chạy đến 7.500 cổng logic - đủ để hướng tới "quantum advantage" (lợi thế lượng tử) vào cuối năm 2026. Heron thế hệ trước vẫn đang hoạt động với 133-156 qubit có độ chính xác cao, trong khi Kookaburra sắp ra mắt sẽ tích hợp bộ nhớ lượng tử và đơn vị xử lý logic đầu tiên.

Google cũng không kém cạnh: chip Willow 105 qubit [3] đã chứng minh khả năng sửa lỗi lượng tử có thể mở rộng (error correction dưới ngưỡng bề mặt), hoàn thành số lượng phép tính khổng lồ chỉ trong chưa đầy 5 phút, trong khi siêu máy tính cổ điển cần tới 10 septillion năm (một con số với 25 chữ số 0). Độ trung thực cổng đơn đạt 99,97% và hệ thống đã chạy gần 10 tỷ chu kỳ sửa lỗi mà không sai sót.

Không dừng lại ở đó, Quantinuum vừa công bố một kết quả đáng chú ý: Họ thực hiện tính toán với tới 94 qubit logic được bảo vệ (48 qubit được sửa lỗi hoàn chỉnh) chỉ từ 98 qubit vật lý - lần đầu tiên qubit logic vượt trội hơn hẳn qubit vật lý thô [4]. IonQ và các hệ thống trapped-ion khác cũng đang đẩy nhanh lộ trình lên hàng trăm qubit logic. Tuy nhiên, tất cả vẫn còn rất xa so với yêu cầu thực sự để chạy Shor ổn định: cần hàng triệu đến hàng chục triệu qubit vật lý fault-tolerant (có khả năng sửa lỗi).

Hiện tại, chưa có hệ thống nào đạt được quy mô đó - lỗi vẫn còn quá cao và việc sửa lỗi đòi hỏi overhead khổng lồ. IBM dự kiến đạt fault-tolerant quy mô lớn vào năm 2029, còn các chuyên gia từ Global Risk Institute (báo cáo 2025-2026) [5] và Citi Institute [6] đánh giá xác suất xuất hiện "cryptographically relevant quantum computer" (CRQC) chỉ rơi vào khoảng 28-49% trong thập kỷ tới (đến năm 2036), và tăng vọt lên 51-70% trong 15 năm, thậm chí 60-82% trước năm 2044. Hiện tại, mối lo lớn nhất không phải tấn công ngay lập tức, mà là chiến lược "harvest now, decrypt later" - các cơ quan tình báo đang lặng lẽ thu thập dữ liệu mã hóa để chờ ngày lượng tử "thức tỉnh".

Vendor	Cloud	Device	Qubits	BSEQ	EPLG	Mirror Circuits	CLOPS‡	QML Kernel	LR-QAOA	WIT	QFT	Metriq score
Example benchmark weights (scale-based)				0.2069	0.1494	0.1703	0.2069	0.0733	0.1494	0.0145	0.0293	
IBM	IBMQ	ibm_boston	156	135.51	338.40	625.62	104.31	190.94	173.61	116.07	145.98	252.61
Quantinuum	NEXUS	quantinuum_h2_2	56	58.08	181.53	539.88	_ ‡	361.42	89.12	126.89	523.15	188.05
IBM	IBMQ	ibm_pittsburgh	156	132.03	258.53	267.71	103.74	149.32	168.27	118.11	126.69	174.51
IBM	IBMQ	ibm_kingston	156	125.09	149.27	371.68	104.83	171.57	161.68	110.49	93.17	174.23
IBM	IBMQ	ibm_marrakesh	156	129.43	201.11	249.28	102.30	130.57	152.69	113.20	80.23	156.82
IBM	IBMQ	ibm_fez	156	134.64	37.30	173.07	106.72	119.37	131.88	111.90	58.28	116.77
IBM	IBMQ	ibm_torino	133	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
IQM	AWS Braket	iqm_emerald	54	56.53	12.75	15.94†	_ ‡	25.87†	22.65	85.97	31.43	23.76
IQM	AWS Braket	iqm_garnet	20	30.20	9.84	2.99†	_ ‡	23.88†	11.62	92.24	44.13	14.34
Rigetti	AWS Braket	rigetti_ankaa_3	82	5.72	8.65	0.28†	_ ‡	12.84†	0.48	59.90	4.50	4.54
OriginQ	OriginQ	wukong_72	72	6.34	0.00*	0.04	_ ‡	11.20	2.47	56.91	1.53	3.38

Dữ liệu đánh giá hiệu năng được thu thập bằng metriq-gym v0.4-v0.6 trên nhiều thiết bị lượng tử và nền tảng đám mây khác nhau. Bảng bao gồm kết quả được chuẩn hóa cho các tác vụ đánh giá hiệu năng từ bộ Metriq. Nguồn: https://arxiv.org.

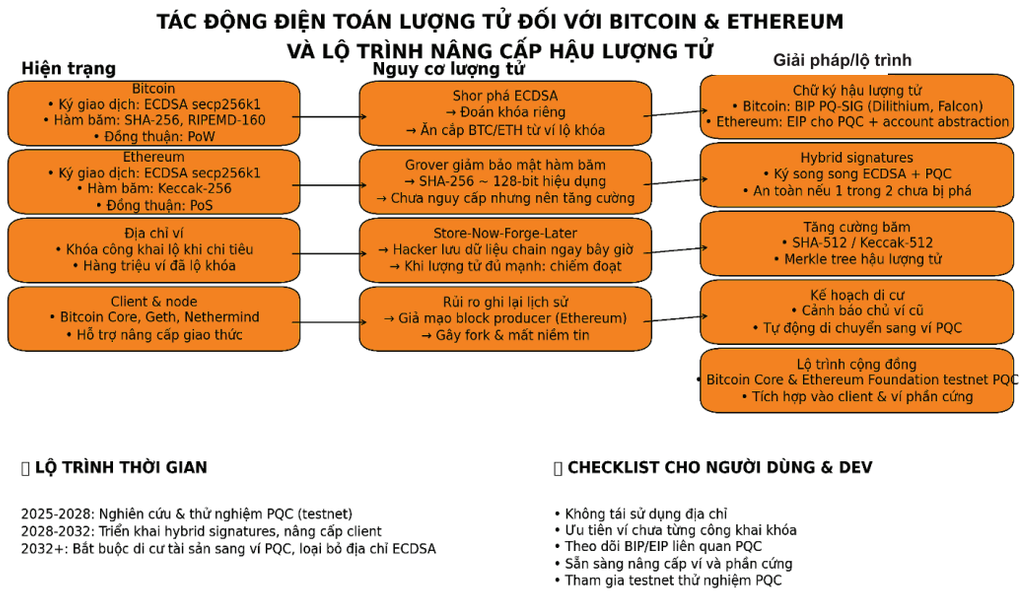
Giải pháp phòng ngừa: Chuyển sang mật mã hậu lượng tử

Dù vậy, cộng đồng blockchain đã chủ động triển khai các hướng chuyển đổi hậu lượng tử (Post-Quantum Cryptography - PQC) với tốc độ chóng mặt.

NIST - cơ quan tiêu chuẩn Mỹ - đã chính thức ban hành các thuật toán mới : FIPS 203: ML-KEM (từ CRYSTALS-Kyber) - mã hóa khóa; FIPS 204: ML-DSA (từ CRYSTALS-Dilithium) - chữ ký; FIPS 205: SLH-DSA (từ SPHINCS+) - chữ ký hash-based; FIPS 206 (đang hoàn thiện): FN-DSA (từ FALCON); Thêm HQC (Hamming Quasi-Cyclic) được chọn năm 2025 làm backup [7]. Những "lá chắn" này chịu được cả Shor lẫn Grover, dù chữ ký lớn hơn một chút.

Bitcoin đang có những bước đi đáng chú ý: BIP-360 (Pay-to-Merkle-Root) [8] đã được chính thức tích hợp vào kho mã nguồn tháng 2/2026. Cơ chế này khéo léo ẩn khóa công khai, biến Taproot thành "lá chắn lượng tử" đầu tiên, mở đường cho chữ ký PQC đầy đủ sau này.

Ethereum cũng không kém cạnh: Vitalik Buterin vừa công bố "quantum roadmap" [9] đầy tham vọng hồi tháng 2/2026, tập trung thay thế chữ ký validator BLS bằng phiên bản hash-based, nâng cấp KZG commitments và chuẩn bị EIP-8141 để ví người dùng dễ dàng chuyển sang chế độ lượng tử an toàn. Solana, Cardano và hàng loạt dự án khác đang chạy đua theo. Người dùng thông minh có thể bắt đầu di chuyển coin từ địa chỉ cũ sang địa chỉ mới ngay trong thời điểm hiện tại - một bước nhỏ nhưng cứu cả tài sản tương lai.



Lộ trình nâng cấp hậu lượng tử cho các nhà đầu tư tài sản số tham khảo. Nguồn: MT.

Ý nghĩa thực tiễn với người dùng và khuyến nghị hành động

Vậy ý nghĩa thực sự với những tổ chức, cá nhân đang nắm giữ tài sản số là gì, và bạn nên làm gì ngay lúc này để không trở thành nạn nhân của "cơn bão lượng tử" đang lặng lẽ hình thành?

Trước hết, hãy nhìn rõ bức tranh thời gian một cách thực tế và không màu hồng:

Giai đoạn ngắn hạn (2026-2030): Đây là giai đoạn tương đối an toàn. Với công nghệ lượng tử hiện tại chỉ mới đạt vài trăm qubit vật lý và lỗi sửa chữa vẫn còn rất cao, không có bất kỳ rủi ro thực tế nào đối với tài sản số của bạn. Bạn có thể yên tâm nắm giữ, giao dịch và thậm chí mở rộng danh mục mà không cần lo lắng. Đây chính là khoảng thời gian phù hợp để chuẩn bị từ sớm mà không phải chịu áp lực.

Giai đoạn trung hạn (2031-2035): Đây là lúc "cửa sổ cảnh báo" bắt đầu mở. Khả năng CRQC xuất hiện tăng lên đáng kể (theo Global Risk Institute 2025). Các địa chỉ cũ đã lộ khóa công khai sẽ trở thành mục tiêu số một. Nếu bạn vẫn giữ coin trong ví legacy (P2PKH hoặc thậm chí Taproot chưa nâng cấp), rủi ro "harvest now, decrypt later" sẽ bắt đầu hiện hữu rõ ràng. Đây là thời điểm bạn **phải** hành động.

Giai đoạn dài hạn (2036 trở đi): Nếu blockchain chưa hoàn tất nâng cấp PQC, đây có thể là giai đoạn rủi ro tăng mạnh nếu quá trình nâng cấp hậu lượng tử không hoàn tất. Một cuộc tấn công quy mô lớn có thể xảy ra chỉ trong vài giờ, và hàng trăm tỷ đô la có thể biến mất mà không để lại dấu vết. Nhưng nếu cộng đồng hoàn thành BIP-360, EIP-8141 và các hard fork tương ứng trước đó, thì toàn bộ hệ sinh thái sẽ chuyển sang "quantum-resistant" - giống như việc chúng ta đã nâng cấp từ HTTP sang HTTPS cách đây hai thập kỷ.

Đối với cá nhân sở hữu thông thường (dưới 1 BTC hoặc tương đương):

Bước 1: Kiểm tra ngay địa chỉ ví của bạn trên công cụ như "Quantum Vulnerability Checker" (đã có trên các explorer như Blockchair hoặc dịch vụ miễn phí của Kudelski Security). Xem địa chỉ đã từng gửi giao dịch chưa - nếu có, nó đang ở trạng thái "lộ khóa công khai".

Bước 2: Tạo ví mới hỗ trợ BIP-360/P2MR (hiện tại Ledger, Trezor và một số ví software như Electrum đã cập nhật). Chuyển toàn bộ coin sang địa chỉ mới này. Chi phí gas trên Ethereum hiện rất thấp, trên Bitcoin chỉ khoảng vài đô la.

Bước 3: Bật tính năng "address reuse prevention" và kích hoạt multi-signature nếu có thể. Đồng thời theo dõi hai nguồn tin cậy mỗi quý: blog Bitcoin Core và Ethereum Foundation blog.

Đối với nhà đầu tư nắm giữ tài sản số lớn (trên 10 BTC hoặc tương đương): Đừng chờ hard fork chính

thức. Hãy bắt đầu "quantum migration plan" ngay trong năm 2026: chia nhỏ tài sản thành nhiều đợt chuyển (drip-feeding) để tránh tạo dấu vết lớn. Sử dụng dịch vụ chuyên nghiệp như Fireblocks hoặc Copper với module PQC-ready. Đồng thời, nhà đầu tư cân nhắc mua bảo hiểm crypto chuyên biệt chống rủi ro lượng tử (đã xuất hiện trên một số sàn lớn).

Đối với doanh nghiệp, quỹ đầu tư và tổ chức: Thực hiện ngay "Cryptographic Agility Audit" - một đánh giá toàn diện hệ thống (công cụ miễn phí từ NIST có sẵn). Lập kế hoạch migrate PQC trong vòng 18-24 tháng tới, tương tự cách các ngân hàng đã chuẩn bị cho NIST PQC. Đừng quên đào tạo đội ngũ developer về Dilithium và Kyber - đây sẽ là nhóm kỹ năng rất quan trọng trong năm 5 tới. Các quỹ lớn như BlackRock hay Fidelity đã bắt đầu làm việc này từ cuối 2025; nếu bạn chưa, bạn đang tụt hậu nghiêm trọng.

Khi các tổ chức, cá nhân di chuyển sớm sang địa chỉ quantum-safe, tài sản số của họ không chỉ an toàn hơn mà còn có thể tăng giá trị khi thị trường công nhận "quantum premium" - tức là coin ở địa chỉ mới sẽ được ưu tiên và định giá cao hơn trong mắt nhà đầu tư tổ chức. Hơn nữa, hành động sớm giúp người sở hữu tài sản số tránh được tâm lý hoảng loạn khi tin tức về CRQC thực sự bùng nổ trên truyền thông.

Điện toán lượng tử không phải ngày tận thế của tài sản số, mà là lời nhắc nhở mạnh mẽ: công nghệ luôn tiến hóa, bảo mật phải tiến hóa nhanh hơn. Với những bước chuẩn bị chủ động như BIP-360 và roadmap của Vitalik, cộng đồng blockchain đang biến mối đe dọa thành cơ hội để trở nên mạnh mẽ hơn bao giờ hết. Tài sản số của bạn vẫn còn tương lai rực rỡ - miễn là bạn hành động ngay hôm nay, thay vì chờ đợi cơn bão lượng tử ập đến ✍

Minh Thiện

TÀI LIỆU THAM KHẢO:

[1] R. Murphy (2025), "Why quantum computing won't crack bitcoin's security in our lifetime", https://medium.com/@DrRoyMurphy/why-quantum-computing-wont-crack-bitcoin-s-security-in-our-lifetime-39091815f0d0, truy cập ngày 15/03/2026.

[2] IBM (2026), "IBM releases a new blueprint for quantum-centric supercomputing" (03/2026), https://newsroom.ibm.com/2026-03-12-ibm-releases-a-new-blueprint-for-quantum-centric-supercomputing, truy cập ngày 15/03/2026.

[3] H. Neven (2024), "Meet Willow, our state-of-the-art quantum chip", https://blog.google/innovation-and-ai/technology/research/google-willow-quantum-chip/, truy cập ngày 15/03/2026.

[4] M. Swayne (2026), "Quantinuum researchers demonstrate quantum computations with dozens of protected logical qubits" (03/2026), https://thequantuminsider.com/2026/03/10/quantinuum-researchers-demonstrates-quantum-computations-with-dozens-of-protected-logical-qubits/, truy cập ngày 15/03/2026.

[5] M. Mosca, M. Piani (2026), "Quantum threat timeline report 2025" (09/03/2026), https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/, truy cập ngày 15/03/2026.

[6] Cici Institute (2026), "Citi institute quantum threat report", https://www.citigroup.com/rcs/citigpa/storage/public/Citi_Institute_Quantum_Threat.pdf, truy cập ngày 15/03/2026.

[7] Trung tâm tài nguyên an ninh máy tính (CSRC) (2026), "Post-quantum cryptography", https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization, truy cập ngày 15/03/2026.

[8] "Bitcoin's quantum upgrade path: What BIP-360 changes and what it does not" https://www.tradingview.com/news/cointelegraph:01f09357a094b:0-bitcoin-s-quantum-upgrade-path-what-bip-360-changes-and-what-it-does-not/, truy cập ngày 15/03/2026.

[9] M. Nijkerk (2026), "Vitalik Buterin unveils Ethereum roadmap to counter quantum computing threat", https://www.coindesk.com/tech/2026/02/26/vitalik-buterin-unveils-ethereum-roadmap-to-counter-quantum-computing-threat, truy cập ngày 15/03/2026.