Market Insight | 2026.4.2

그림: Midjourney(구글의 AI와 양자 특이점이 주는 비트코인에의 충격)

디지털자산과 양자, 그리고 AI

2029년이면 코인 다 뚫리나?

한종목

chongmok.han@miraeasset.com

김은지

eunji.kim.a@miraeasset.com

CONTENTS

Executive Summary 3
"양자 특이점 2029" 총정리 3

I. 양자 특이점 2029 4
1. CRQC(암호학적으로 유의미한 양자 컴퓨터)의 위험 4
2. 5대 핵심 관전 포인트 10
3. 이더리움의 포스트 양자 로드맵 — 준비하는 자의 청사진 20

II. 양자컴퓨터가 코인을 공격하는 경로 23
1. 다 같은 양자컴퓨터가 아니다: Fast-Clock과 Slow-Clock 23
2. 흐려지는 경계: “느린 시계”가 빨라지는 새로운 경로 26
3. CRQC 타임라인과 데드라인 28

Executive Summary

"양자 특이점 2029" 총정리

'2029'라는 숫자에 주목해야 합니다. 지난 3월 25일, 구글의 블로그에는 "Quantum frontiers may be closer than they appear"라는 글이 게시됐습니다. 그들은 "포스트 양자 암호(PQC) 전환" 시한을 공식적으로 2029년으로 못 박았습니다. 그리고 닷새 뒤인 3월 30일, 구글 퀀텀 AI는 그 선언의 수학적 근거가 되는 논문 한 편을 세상에 공개했습니다.

여기서 흥미로운 사실이 하나 있습니다. 이더리움 창시자 비탈릭 부테린(Vitalik Buterin)은 이미 2025년 8월, "2030년 이전에 Q-day가 현실이 될 확률이 대략 20% 정도"라고 수치화하여 언급한 바 있습니다. **Q-day란 양자컴퓨터가 비트코인·이더리움에 쓰이는 ECDSA 서명 체계를 현실적으로 깨기 시작하는 날을 뜻합니다. 2030년 이전이라는 비탈릭의 표현과 구글이 이번에 내놓은 2029년이라는 숫자가 묘하게 겹칩니다**. 두 사람이 독립적으로 같은 시점을 가리키고 있다면, 이것은 단순한 우연의 일치인가요? 아니면 그들은 이미 우리가 모르는 무언가를 알고 있는 것인가요? 저희의 보고서는 이 질문에서 시작합니다.

구글이 내놓은 이번 논문의 핵심 수치는 놀랍습니다. **비트코인과 이더리움을 지탱하는 256비트의 타원곡선 암호(secp256k1)를 깨는 데 필요한 물리적 큐비트가 (초전도 아키텍처 기준) 기존 추정치의 1/18 수준인 50만 개 이하로 줄어들었다는 겁니다. 게다가 해킹에 걸리는 시간은 단 9분~23분에 불과합니다**. 비트코인의 블록 생성 주기가 평균 10분임을 감안하면 이게 얼마나 파괴적인지 가늠할 수 있습니다. 같은 날 양자 스타트업인 Oratomic이 공개한 논문(qLDPC 코드에다가 중성 원자 양자컴퓨터 기술을 결합)의 의미까지 감안하면 더 충격적입니다. 실용적 '대형' 양자컴퓨터를 만들 때 필요한 큐비트 숫자를 약 2만 6천 개까지 줄일 수 있다고 했는데, 현재 세계 최고 수준의 중성 원자 양자컴퓨터는 이미 6,100개 큐비트를 다루고 있습니다. 이는 **Q-day가 생각보다 가깝다는 것을 의미합니다.**

한편, 암호학 전문가 일각에서는 '2029년 양자 파국'의 현실 가능성을 통계적으로 0에 수렴하고 아직 수십년이 걸릴 문제라고 주장하기도 합니다. 그럼에도, 그들이 느끼는 진짜 공포는 따로 있었습니다. 그들이 두려워하는 것은 양자 특이점 그 자체가 아니라, **AI가 양자 오류 수정 모델을 혁신할 경우 수십 년 격차가 순식간에 붕괴될 수 있다는 불확실성입니다**.

이 불확실성은 이미 구체적인 형태로 나타나고 있습니다. Anthropic 연구원 Nicholas Carlini의 공개 시연에서 Claude는 복잡한 툴 없이 20년 묵은 리눅스 커널 취약점을 90분 만에 찾아냈고, 스마트 컨트랙트(블록체인 위의 자동 실행 프로그램)에서 460만 달러를 자율 탈취하는 시뮬레이션을 2분 26초 만에 완수했습니다. AI 모델의 해킹 능력이 1.3개월마다 두 배씩 강력해지고 있다는 데이터는 모든 타임라인 계산을 뒤흔들 수 있는 변수입니다.

AI가 본격 투입되면 양자 발전의 타임라인 자체가 다시 써질 수 있습니다. 포스트 양자 전환 비용이 큰 블록체인은 디스카운트를 받을 가능성이 높습니다. 반대로 완벽하진 않더라도, 로드맵·실행력·암호학적 민첩성(네트워크 중단 없이 핵심 암호 모듈을 교체할 수 있는 시스템의 능력)을 이미 제도화한 생태계를 가진 블록체인은 프리미엄을 받을 가능성이 높을 것으로 사료됩니다.

I. 양자 특이점 2029

1. CRQC(암호학적으로 유의미한 양자 컴퓨터)의 위험

* CRQC: Cryptographically Relevant Quantum Computer의 줄임말로, 암호화폐를 해독할 수 있는 수준의 양자컴퓨터를 뜻함.

2025년 8월, 이더리움 창시자 비탈릭 부테린은 이런 말을 남겼다. "현대 암호를 깨는 수준의 양자컴퓨터가 2030년 이전에 등장할 확률이 약 20% 정도라고 본다(seemingly 20%)." 커뮤니티는 이 발언을 당시에도 충격적으로 받아들였다. 20%면 낮은 수치로 보이기도 하지만 생각했던 것보다는 높은 수치로 보였기 때문이다.

그로부터 7개월 뒤인 2026년 3월 30일, 구글의 퀀텀 AI 팀은 논문 한 편을 공개하며 자체 포스트 양자로의 전환 데드라인을 2029년으로 공식화해버렸다. 세상이 뒤집어지는 문제다. “2030년 이전이라는 비탈릭 부테린의 표현, 그리고 2029라는 구글의 숫자”. 한 사람은 블록체인 생태계의 내부에서, 다른 한 사람은 양자 물리학의 최전선에서 독립적으로 각 주체들이 거의 같은 시간대를 가리킨 것이다.

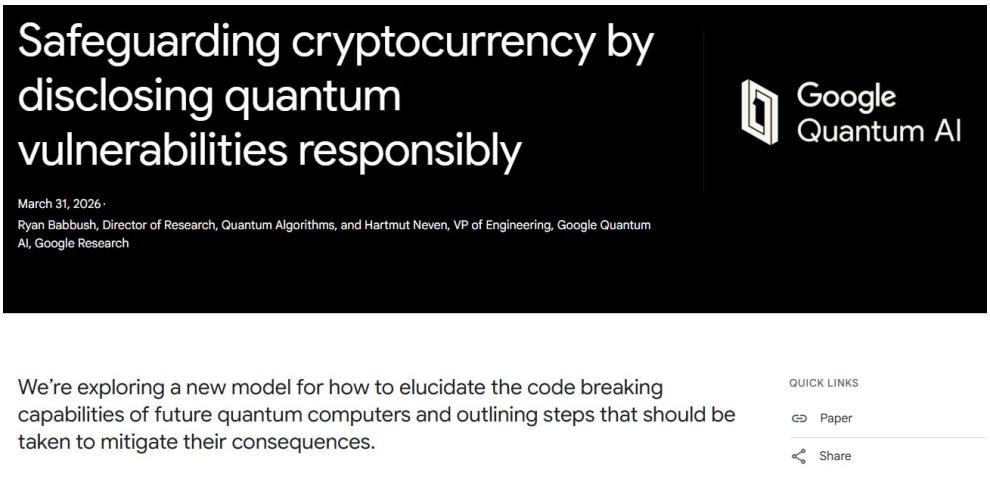
* ZKP(영지식 증명): 내용 공개 없이 그 사실이 유효함을 수학적으로 증명하는 기법. 구글은 “우리가 양자 공격 회로를 만들었다”는 사실만 증명, 회로의 설계도는 공개하지 않음. 다시 말해, “구글이 무언가를 이미 알고 있는 것 같다”고 의심하는 근거 중 하나가 바로 이런 비밀스러움.

이것은 단순 우연의 일치인가? 그게 아니면 이 두 조직은 일반에 공개되지 않은 무언가를 이미 알고 있는 것인가? 구글이 실제 공격 회로를 공개하지 않고 영지식 증명(ZKP)만 내놓은 이례적 결정, 그리고 구글의 논문 곳곳에 박힌 "최첨단 양자 알고리즘은 더 이상 공개적으로 발표되지 않을 수 있다"는 경고 문구들을 함께 읽으면, 이 가설은 단순 음모론으로 치부하기 점점 어려워진다.

** 여기서 말하는 구글의 ‘회로’라고 하는 것은 양자컴퓨터가 실제로 계산을 하는 ‘작업 순서도’. “이 양자 게이트 → 저 양자 게이트 → …” 순서로 적은 양자 명령 순서도. 즉, 쇼어 알고리즘을 양자컴퓨터의 큐비트들한테 어떤 순서로 어떤 연산(게이트)을 가하느냐 실제로 돌릴 때 쓰는 그 순서도를 뜻함.*

물론 확인할 방법은 없다. 하지만 우리가 주목하는 것은 바로 이 불확실성의 구조 자체다. 확실히 알 수 없기 때문에 더 위험하고, 확실히 알 수 없기 때문에 선제 대응만이 유일한 합리적 선택이 된다.

그림 1. 비트코인·이더리움 보안을 깨는 문제를 부상시키며, PQC 전환을 시작해야 한다는 구글 논문
Q-day가 오기 전에 2029년이 끝나기 전에 방어 체계 마이그레이션을 시작하라고 공식 통지한 것!



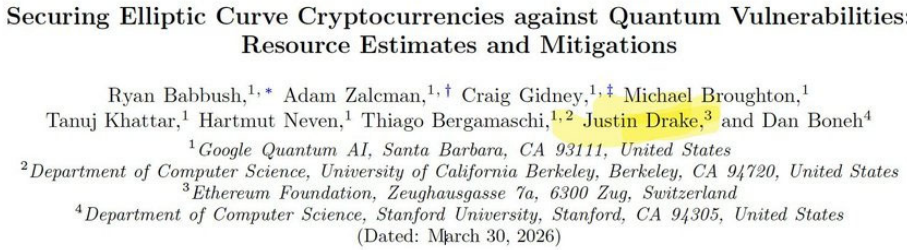
자료: 구글, 미래에셋증권 리서치센터

(1) 구글 퀀텀 AI — 쇼어 알고리즘의 극한 압축

2026년 3월 30일, 두 편의 논문이 동시에 공개됐다. 구글의 퀀텀 AI의 논문은 논리 레이어(logical layer)를, 오라토믹이라는 스타트업의 논문은 물리 레이어(physical layer)를 각각 최적화했다.

흥미로운 점은, 해당 구글 논문의 공동 저자에 이더리움 재단의 저스틴 드레이크(Justin Drake)와 스탠퍼드 대학의 댄 보네(Dan Boneh)가 이름을 올렸다는 점이다. 논문이 단순한 학술 기여를 넘어 블록체인 생태계 전반에 대한 정밀한 경고로써 설계됐음을 보여주는 구성이다.

그림 2. 비트코인·이더리움의 elliptic curve 서명 자체가 직접 표적임을 못 박는 구글의 해당 논문
논리 큐비트 1.2k~1.45k, Toffoli 70M~90M, 물리 큐비트 50만 미만이라는 공격 자원 추정을 제시



Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations

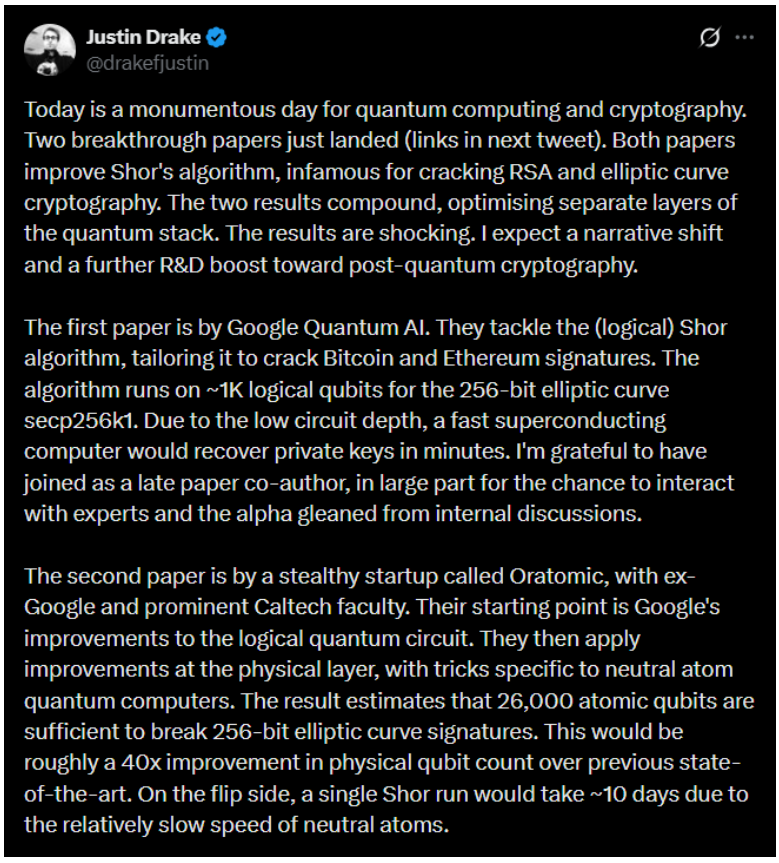
Ryan Babbush,[1,*] Adam Zalcman,[1,†] Craig Gidney,[1,‡] Michael Broughton,[1] Tanuj Khattar,[1] Hartmut Neven,[1] Thiago Bergamaschi,[1,2] Justin Drake,[3] and Dan Boneh[4]

[1]*Google Quantum AI, Santa Barbara, CA 93111, United States*
[2]*Department of Computer Science, University of California Berkeley, Berkeley, CA 94720, United States*
[3]*Ethereum Foundation, Zeughausgasse 7a, 6300 Zug, Switzerland*
[4]*Department of Computer Science, Stanford University, Stanford, CA 94305, United States*

(Dated: March 30, 2026)

자료: 구글, 미래에셋증권 리서치센터

그림 3. 양자 위협이 추상적 공포에서 실전형 경고로 넘어갔다고 고백하는 이더리움 핵심 개발자
양자 스택의 서로 다른 병목(논리+물리)이 동시에 무너지고 있다는 사실을 읽어야 한다는 뜻이다



Justin Drake
@drakefjustin

Today is a monumentous day for quantum computing and cryptography. Two breakthrough papers just landed (links in next tweet). Both papers improve Shor's algorithm, infamous for cracking RSA and elliptic curve cryptography. The two results compound, optimising separate layers of the quantum stack. The results are shocking. I expect a narrative shift and a further R&D boost toward post-quantum cryptography.

The first paper is by Google Quantum AI. They tackle the (logical) Shor algorithm, tailoring it to crack Bitcoin and Ethereum signatures. The algorithm runs on ~1K logical qubits for the 256-bit elliptic curve secp256k1. Due to the low circuit depth, a fast superconducting computer would recover private keys in minutes. I'm grateful to have joined as a late paper co-author, in large part for the chance to interact with experts and the alpha gleaned from internal discussions.

The second paper is by a stealthy startup called Oratomic, with ex-Google and prominent Caltech faculty. Their starting point is Google's improvements to the logical quantum circuit. They then apply improvements at the physical layer, with tricks specific to neutral atom quantum computers. The result estimates that 26,000 atomic qubits are sufficient to break 256-bit elliptic curve signatures. This would be roughly a 40x improvement in physical qubit count over previous state-of-the-art. On the flip side, a single Shor run would take ~10 days due to the relatively slow speed of neutral atoms.

자료: Justin Drake, 미래에셋증권 리서치센터

*** 쇼어 알고리즘: 1994년 개발된 양자컴퓨팅 알고리즘. 타원 곡선 암호(ECC)와 RSA(일반 은행들이 쓰는) 암호를 전부 다 해독 가능. 비트코인·이더리움 서명 체계의 핵심 위협이 되는 알고리즘.**
개인키에서 공개키를 계산하는 것은 쉽지만, 공개키에서 개인키를 역산하는 것은 고전 컴퓨터로는 사실상 불가능. 하지만, 쇼어 알고리즘을 사용하면 계산 가능.

이 논문의 핵심 성과는 쇼어 알고리즘(Shor's Algorithm)이라는 양자 프로그램이 필요로 하는 '논리 큐비트' 숫자다. 예전에는 2,000개 정도 필요했는데, 이제 1,200개~1,450개로 줄였다. 구글은 실용적으로 쓸 수 있는 두 가지 방법을 제시했다. 그러니까 새로운 알고리즘을 발명한 것은 아니라, 기존 쇼어 알고리즘의 논리적 구조를 재설계해 필요한 큐비트 수와 게이트 수를 동시에 극단적으로 압축한 것이다.

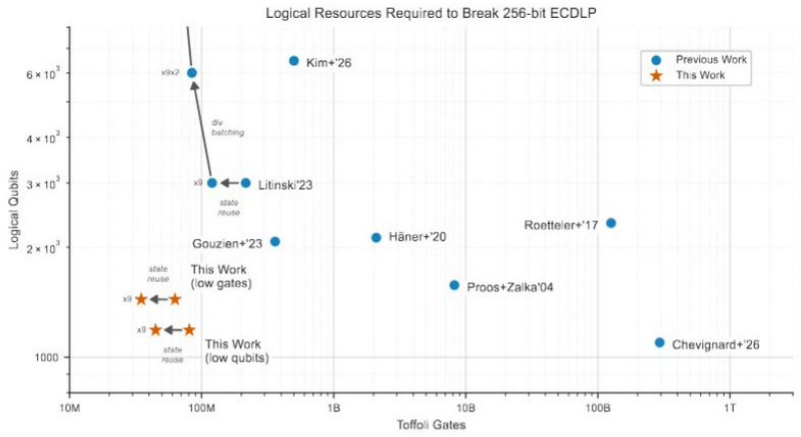
** 논리적 큐비트: 수십~수백 개의 물리 큐비트를 묶어 오류 자동정정한 '깨끗한' 단위. 실제 알고리즘이 쓰는 것.*
** 물리적 큐비트: 실제 하드웨어의 기본 단위. 노이즈가 많아 오류 교정 없이는 복잡한 연산이 불가능.*

표 1. 구글이 내놓은 두 가지 회로, 암호화폐 해독에 걸리는 시간은 줄어드는 중

변형	논리 큐비트	토폴로지 게이트	물리 큐비트	실행 시간
Low-Qubit (저큐비트형)	**1,200개**	9,000만 개	**50만 개 이하**	~23분
Low-Gate (저게이트형)	**1,450개**	7,000만 개	**50만 개 이하**	~18분
기존 최고 효율 (Litinski'23)	~3,000개+	~2억 개	~900만 개	—

자료: Google Quantum AI, 미래에셋증권 리서치센터

그림 4. 구글 논문의 승부처는 하드웨어가 아니라, 논리 레이어의 쇼어 알고리즘 최적화였음
별표로 표시된 "This Work"가 기존 연구보다 더 적은 논리 큐비트와 Toffoli gates 구간으로 이동
하드웨어가 그대로여도 알고리즘 설계를 혁신함으로써 Q-day는 당겨진다는 것을 의미



자료: 구글, 미래에셋증권 리서치센터

*** 마법 상태 증류: Toffoli 게이트(양자 연산의 핵심 단위)를 구동하기 위해 'T state'라는 특수 양자 상태를 지속 공급해야 하는데, 이 생산 과정이 전체 양자 컴퓨팅 자원의 대부분을 소모해왔음. 구글은 이 부하를 획기적으로 줄인 것.**

그런데 진짜 중요한 혁신은 큐비트 숫자만이 아니다. '마법 상태 증류(Magic State Distillation)'라는 부분을 크게 줄인 것이다. 양자컴퓨터가 중요한 계산을 하려면 'T state'라는 특별한 '양자 상태'를 계속 만들어야 하는데, 이걸 만드는 과정이 컴퓨터 자원의 대부분을 잡아먹었다. 구글은 이 과정을 획기적으로 가볍게 만든 것이다.

그래서 실제 초전도 양자컴퓨터에서 구글의 방식을 사용하면 개인키(사용자들의 암호화폐 지갑 비밀번호)를 뽑아내는 데 이론적으로 9~23분밖에 안 걸리게 된다고 한다. 여기서 '프라이밍'이라는 개념이 나오는데, 이를 쉽게 말하면 "미리 준비 작업을 끝내놓는 것"이다. 쇼어 알고리즘은 두 단계로 나뉜다.

① 공개키(public key)와 상관없는 공통 준비 작업 (미리 끝내 놓을 수 있음)
② 실제 공개키를 넣고 개인키(private key)를 뽑는 작업

* 멤풀(Mempool): 암호화폐의 트랜잭션(거래들)이 블록에 기록되기 전에, "공개 대기"하는 장소. 이곳에서 바로 공개키가 노출되는 10분가량의 시간이 양자 공격의 기회가 됨.

공격자가 ①번을 미리 끝내놓고 기다리면, mempool에서 공개키가 나타나는 순간 바로 ②번만 돌리면 된다. 이렇게 하면 공격 시간이 반으로 줄어서, 비트코인 블록이 만들어지는 평균 10분 안에 개인키를 뽑을 수 있는 것이다. 이걸 온스펜드(On-Spend) 공격이라고 부른다.

(2) 오라토믹(Oratomic) — 중성 원자의 역습

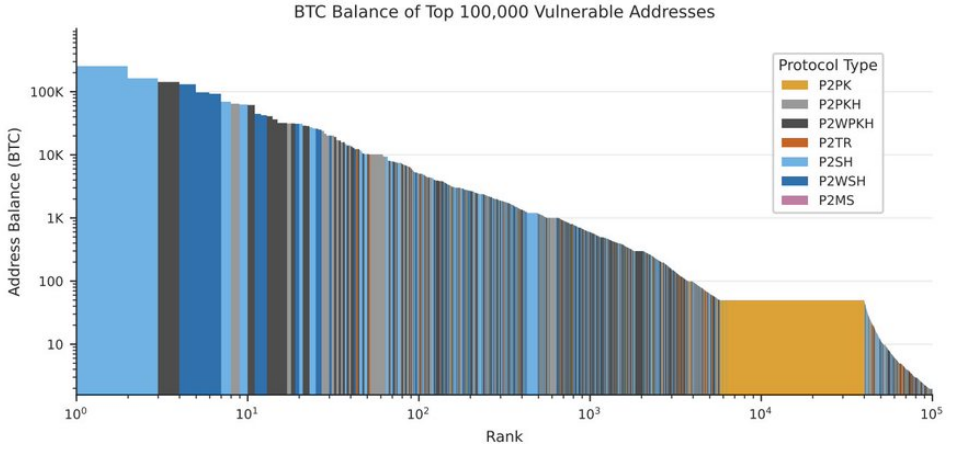
같은 날, 스텔스 스타트업 오라토믹(Oratomic)이 발표한 논문은 또 다른 충격이었다. 전 구글 연구원들과 칼텍(Caltech) 교수들이 만든 회사다. 구글이 논리 레이어에서 달성한 최적화를 그대로 받아들이고, 거기에 중성 원자(Neutral Atom) 기반의 물리 레이어 최적화를 추가하는 방식을 택했다. 그들의 핵심 기술은 qLDPC(Quantum Low-Density Parity-Check) 코드라는 새로운 오류 정정 방식이다.

지금까지 양자컴퓨터가 오류를 잘 고치기 위해 가장 많이 쓰던 방식인 '표면 코드'라는 것은 문제가 있었다. 구글도 이번에 사용한 이 방식은 물리 큐비트의 97%를 그냥 오류 교정에만 써버리기 때문이다.

즉, 실제 계산에 쓸 수 있는 큐비트가 3%밖에 안 남는 엄청난 낭비였다. 오라토믹이 쓴 새로운 오류 정정 방식인 qLDPC는 다르다. 기존 방식은 "바로 옆 큐비트끼리만 연결"할 수 있었는데, qLDPC는 멀리 떨어진 큐비트끼리도 자유롭게 연결할 수 있게 만들어졌다. 그 결과 낭비가 거의 사라지고, 같은 성능을 내면서도 훨씬 적은 큐비트로 충분해졌다.

결과는 충격적이다. ECC-256(비트코인·이더리움이 쓰는 암호)을 깨는 데 단 26,000개의 중성 원자 큐비트만 있으면 된다고 그들은 밝혔다. 이에 걸리는 시간은 고작 10일 정도에 불과하다. 10일이 길게 느껴질 수도 있지만, 오래된 공개키(예를 들어, P2PK같이 2009~2010년에 주로 사용된 방식)를 노리는 '휴지기(At-Rest) 공격'에는 충분히 실용적인 시간이라는 게 업계의 평가다.

그림 5. 양자 리스크가 순수 이론이 아니라, 이미 공개키가 노출된 거대한 자산 풀의 문제임을 시사
오라토믹의 논문에서는 양자 공격에 취약한 비트코인의 숫자가 무려 약 670만 개로 말하고 있음…



자료: Oratomic, 미래에셋증권 리서치센터

그리고 현재 세계에서 가장 큰 중성 원자 양자컴퓨터는 이미 6,100개의 큐비트를 보유하고 있다. 목표까지 남은 거리가 갑자기 가깝게 느껴지기 시작한다. 예전에는 수백만 개가 필요하다고 했는데, 이제는 수만 개 수준으로 확 줄었으니 기술적으로 현실감이 확 살아났다.

또한, 여기서 주목할 사실이 하나 더 있다. 오라토믹 논문의 기술 분석에 따르면, LLM(대규모 언어 모델)이 QEC(양자 오류 정정) 코드에 활용됐으나, 해당 코드의 세부 내용은 논문에서 생략된 것이다. 왜 생략됐는지는 명시되지 않았다. 그러나 분명한 것은, **AI가 양자 오류 정정 코드의 발견에 이미 투입되고 있다는 사실이다.** 이는 뒤에서 다룰 "AI 특이점" 논의의 직접적인 근거가 된다.

(3) 큐비트 추정치의 궤적

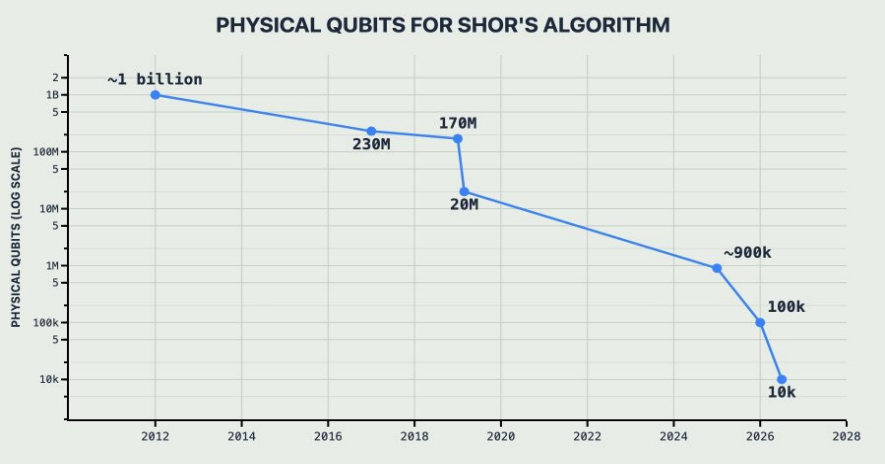
물리 큐비트 요구치가 줄어드는 궤적을 보면 상황의 심각성을 실감할 수 있다. 10년 만에 필요한 큐비트 숫자가 3만 배 이상 줄었다. 특히 지난 1년 동안 떨어진 속도가 정말 무섭게도 가장 가파르다.

표 2. ECC-256 공격에 필요한 물리 큐비트 숫자: 계단식으로 "10년 만에 3만 배" 압축

연도	필요 물리 큐비트 (ECC-256)	연구 기관
2012	~10억 개	Jones et al.
2019	~2,000만 개	Gidney & Ekerå
2025	~90만 개	Babbush et al.
2026	~50만 개	구글 Quantum AI
2026	~26,000개	오라토믹

자료: Google Quantum AI, Oratomic, 미래에셋증권 리서치센터

그림 6. 공격에 필요한 물리 큐비트 요구치가 계단식으로 붕괴하고 있다
단순 HW 제조 진보가 아니라, 쇼어 알고리즘 최적화와 qLDPC 같은 오류정정 혁신이 겹쳤기 때문



자료: Oratomic, 미래에셋증권 리서치센터

앞에서 설명했지만, 이러한 필요 큐비트의 극단적 감소는 하드웨어가 비약적으로 발전해서가 아니다. 표면 코드(Surface Code)에서 qLDPC로 넘어가는 양자 오류 수정 알고리즘의 효율화와, 쇼어 알고리즘의 논리 게이트 최적화가 만들어낸 결과다. 이로써, 목표 지점(비트코인 파훼) 자체가 인류의 현재 기술력 방향으로 맹렬하게 돌진해오고 있는 상황이다.

비트코인이나 이더리움이 의존하고 있는 256비트 타원곡선 암호(ECC-256)는 같은 보안 수준의 RSA-2048보다 양자 공격에 100배나 더 취약한 것으로 밝혀졌다. 블록체인 업계가 ECC를 선택했던 이유(보안/서명이 가볍다는 효율성)가 오히려 양자 시대에는 가장 큰 약점이 되어버린 아이러니한 상황이다.

논문이 또 하나 강조하는 불편한 사실이 있다. 양자컴퓨터 기술은 천천히 조금씩 발전하는 게 아니라, 어느 순간 임계값(Threshold)을 넘으면 갑자기 폭발적으로 발전할 수 있다는 점이다. 구글의 논문에는 직접 이렇게 써 있다. "32비트 암호를 깨는 데 성공한 순간과 256비트 암호를 실제로 깨는 순간 사이에 거의 시간이 없을 수도 있다." 즉, 경고 신호 없이 갑자기 올 수 있다는 뜻이다.

2. 5대 핵심 관전 포인트

(1) 관전 포인트 1: "2029 카운트다운"과 AI 변수

양자 위협은 더 이상 수십 년 뒤의 공상과학이 아니며, qLDPC의 최적화와 AI의 개입으로 물리적 큐비트 장벽이 무너지고 있고, 2029년이라는 '실존적 카운트다운'이 시작되었다.

왜 구글은 2029년을 콕 집었나

구글이 찍은 2029년 데드라인은 철저히 계산된 기업 규제 대응이자 시장 선점 선일 수도 있다. 미국 국립표준기술연구소(NIST)는 기존 암호 체계의 단계적 폐기를 2030년부터, 완전 금지를 2035년으로 설정한 바 있다. 구글 같은 빅테크는 정부 기관과 계약을 유지하려면 그 전에 PQC 전환을 마쳐야 한다. 이러한 암호학 전환에는 수년의 리드타임이 필요하다. 2029년이라는 것은 본인들의 규제 데드라인을 맞추기 위해 역산된 숫자일 수 있다.

다만 이러한 정치적 계산으로만 치부할 수는 없다. 훨씬 중요한 것은, 알고리즘의 개선이 선형이 아니라 복리로 일어나고 있다는 점이다. 구글 논문 자체가 명시하고 있는 것을 좀 더 쉬운 말로 의역을 하자면 다음과 같다. "양자컴퓨터는 물리 큐비트 숫자를 천천히 늘려가는 게 아니라, '한 번 문턱(threshold)을 넘으면 갑자기 커지는' 방식으로 발전한다. 그래서 32비트의 작은 퍼즐을 깨는 정도의 공개 시연을 하는 시점과 비트코인·이더리움의 보안을 깨버리는 '256비트 해독'하는 시점의 차이는 거의 없을 수 있다." 물론 현재는 6비트 정도에 불과하지만, 진보의 속도가 기하급수적이라는 것을 감안해야 한다.

세계적 양자 컴퓨팅 이론가 스콧 아론슨은 이 두 논문(구글과 오라토믹)의 결합 효과에 대해 이렇게 평가했다: "두 결과를 합치면, 비트코인 서명은 이전에 알려졌던 것보다 확실히 더 일찍 양자 공격에 취약해 보인다. 특히 칼텍 그룹은 단 25,000개의 물리 큐비트만으로 충분할 수 있다고 추정하는데, 1년 전 최선의 추정치는 수백만개의 큐비트였다." 그리고는, 이번 논문이 복리로 효과를 내면서 Q-day라고 하는 것이 적어도 본인의 예상 대비 1년은 더 앞당겨졌다고 표현했다. 물론, 오라토믹의 창업자 블루스타인도 같은 맥락에서 말했다. 그는 유틸리티 규모의 내결함성 양자컴퓨터가 2029년 말까지 나올 수 있다고 보고 있다.

진짜 변수 — AI가 개입하면 타임라인은 소용없다

디지털자산 프로젝트들의 암호학 전문가들 중 일부는, 양자 특이점에 대한 코인 충격에 대해 걱정 너무 하지 말라면서도 그들의 진짜 공포를 말하기도 했다. 그들의 말을 종합하면 다음과 비슷하다.

"두세 해 전만 해도 2050년 이전에는 불가능하다고 봤다. 지금도 그렇게 생각한다.
하지만 AI가 앞으로 10년 안에 무엇을 할 수 있는지 나는 예측조차 할 수 없다.
AI가 내일 무엇을 할지도 모른다."

이더리움 재단의 핵심 유명 엔지니어인 저스틴 드레이크(Justin Drake)는 구글 논문에 공동 저자다. 그리고 구글의 논문도 "AI가 아직 양자 회로 최적화에 본격 투입되지 않았다(not yet!)"고 언급하며 비슷한 포인트를 짚고 있다. 현재까지의 모든 알고리즘 개선은 순수한 인간 수학자들의 결과물인 것이다. AI가 본격 투입되면 어떤 속도로 큐비트 요구치가 내려갈지, 아무도 모른다.

* qLDPC 코드: 차세대 오류 정정 방식. 멀리 떨어진 큐비트끼리도 오류 체크를 할 수 있어 훨씬 적은 물리 큐비트로 동일한 논리 큐비트를 구현.

* PQC: 포스트 양자 암호(Post-Quantum Cryptography)의 줄임말. 양자컴퓨터로도 해독 어려운 차세대 암호.

그런데 앞서 살펴봤듯, 오라토믹의 논문에서는 이미 LLM이 QEC 코드 발견에 투입되었다. AI가 양자 오류 정정의 최전선에 이미 투입되었으나, 그 성과가 너무 혁신적이어서(또는 다른 이유로) 아직 세상에 공개되지 않고 있다고 사료된다. 이는 드레이크의 의중을 오히려 더 강화한다. AI의 개입은 이미 시작됐고, 우리가 볼 수 있는 것은 빙산의 일각일 수 있다.

구글의 TPU가 양자 알고리즘 연구에 활용될 것

구글의 소위 "AI 프론티어" 전략은 AI의 적극 개입에 관한 우리의 생각을 구체화한다. 구글에는 AlphaQubit 프로젝트가 있다. 이는 직접적으로 양자 컴퓨팅의 오류 정정을 AI로 개선하는 과학적인 프로젝트다. 그런데, 이러한 프로젝트를 직접적으로 지원하는 구글이 가진 병기가 바로 그들의 ASIC인 TPU다. TPU를 막대한 규모로 병렬 연결하는 그들의 데이터센터 구조(Torus 토폴로지)가 힘을 발휘하는 것이다.

구글의 토폴로지는 OpenAI나 Anthropic이 GPU 중심인 것과 다르다. 그 두 회사는 상대적으로 크기가 작은 모델을 만든 다음, 반복적이고 빠른 제품 배포를 하면서 계속해서 피드백을 받아 강화학습을 수행한다. 하지만 구글은 Torus 토폴로지 구조가 가진 제약사항 때문에, 작은 모델을 초고속으로 분산 학습시키며 강화학습 이터레이션(반복 학습)을 수행하는데는 불리하다. 그 결과 "작은 모델 → 빠른 RL 사이클 → 연구원에게 즉시 배포"라는 전략을 포기하고, 초대형 모델 위주로 어떻게 보면 반강제로 가게 되는 셈이다.

따라서 구글은 AI 제품 경쟁에서는 민첩성이 떨어지는 것처럼 보이지만, 그들의 포커스가 과학(양자 컴퓨팅 포함)이라고 생각하면 얘기가 다르다. 구글은 엔터프라이즈 코딩 어시스턴트 회사라기 보다는, 과학·공학 난제를 푸는 상위 추론 시스템을 지향하는 방향으로 가닥을 잡는 듯하다. 작은 모델 배포에 집중하기보다 초대형 모델을 내부적으로 깊이 있게 돌려 AI for Science라는 별도의 승리 조건을 만든 것이다. 이런 관점에서 보면, 이번에 나온 '양자 회로 최적화'처럼 깊은 추론과 긴 호라이즌이 필요한 문제에 가장 잘 맞는 하드웨어로서 TPU가 사용되는 듯하다.

(2) 관전 포인트 2: 공격 회로 비공개 + ZKP = 비밀 군비 경쟁

구글이 이번에 양자 공격 회로를 숨기고 영지식 증명(ZKP)만 공개한 것은, 최첨단 양자 암호 해독 기술이 투명한 학술의 영역을 떠나 국가 안보와 빅테크 주도의 '비밀 군비 경쟁' 단계로 진입했음을 뜻한다.

설계도 없는 증명 — 이 선택이 의미하는 것

이번 논문에서 가장 이례적인 결정은 공격 회로(Attack Circuit) 자체를 공개하지 않았다는 것이다. 구글은 대신 ZKP(영지식 증명, Zero-Knowledge Proof)를 활용했다. SP1이라는 zkVM을 통해, "우리는 실제로 이 공격 회로를 보유하고 있으며, 9,024개의 무작위 테스트 케이스에서 올바르게 작동함을 확인했다"는 사실 그 자체만 외부에 전달했다. 회로의 세부 내용은 완전히 블랙박스인 것이다.

구글은 그 회로를 숨긴 이유도 논문에 명시했다. "미국 정부와 협의하여 악의적 행위자에게 공격 설계도를 제공하지 않기 위함." 이 문장은 두 가지를 동시에 말한다. 첫째, 구글이 이미 실용적 수준에 근접한 공격 회로를 보유하고 있을 가능성이다. 둘째는 이 기술이 국가 안보의 영역에서 관리되기 시작했다는 사실이다.

* zkVM (Zero-Knowledge Virtual Machine): 어떠한 프로그램이 실행됐다는 사실을 ZK 방식으로 증명하는 시스템. 이번에 구글이 사용한 것은 Succinct Labs의 SP1.

최첨단 양자 알고리즘은 더 이상 대중과 학계에 투명하게 공유되지 않으며, 은밀하고 치명적인 군비 경쟁 체제로 돌입했다는 선언이다. 물론, 이렇게 정보를 비공개로 유지하면 악의적 행위자의 접근을 늦출 수 있지만, 동시에 방어자의 준비도 늦춘다. 구글은 충분한 경고를 주되 설계도는 넘기지 않는 중간 경로를 택한 것이다.

지금 수집, 나중에 해독 — 이미 시작된 전쟁

구글 논문의 공동 저술자 저스틴 드레이크는 상황을 이렇게 요약했다. "앞으로는 최첨단 알고리즘이 검열될 것이라고 가정해야 한다. 학술 발표의 공백은 곧 진보의 신호가 될 것이다." 이는 "CRQC(암호학적으로 유의미한 양자컴퓨터)가 아직 없는데 왜 지금부터 대비해야 할까?"라는 질문의 답변이 된다. 전쟁이 이미 시작됐기 때문이다.

미국 NSA, 중국 국가안전부 등 주요 국가 정보기관들은 현재 전 세계의 암호화된 데이터를 수집·저장하고 있다는 것은 공공연한 사실이다. 지금 당장 해독할 수 없어도, CRQC가 완성되는 순간 과거에 쌓인 데이터를 일괄 해독하기 위해서다. 이것을 "지금 수집, 나중에 해독(Harvest Now, Decrypt Later, HNDL)" 전략이라 한다.

비트코인 블록체인에 영원히 새겨진 모든 공개키는 이미 어딘가의 서버에 수집되어 쌓이고 있을 수 있다. CRQC 완성의 최초 신호는 이번과 같은 논문이나 기업의 공개된 보도자료가 아닐 것 같다. 오랜 기간 휴면에 있던 암호화폐 지갑에 있던 대규모 코인들이 조용히 mixer(자금 세탁 서비스)로 이동하는 트랜잭션으로 목격될 가능성이 더 높다.

블록체인 생태계가 "양자컴퓨터가 눈앞에 보일 때 대응하면 된다"는 관망 전략에 의존하고 있다면, 그 전략 자체가 적의 가장 강력한 무기가 된다. **실질적 진보가 비밀 뒤에서 일어나는 세계에서는, 공개된 학술 데이터만으로 위협 타임라인을 추정하는 것 자체가 구조적 오류다. 전쟁은 이미 시작됐다.**

(3) 관전 포인트 3: 비트코인의 화석화 vs 이더리움의 암호학적 민첩성

기술 부채와 이념적 경직성으로 인해, 구조 재편(하드포크)을 미루는 비트코인의 '화석화'는 치명적일 수 있고, '암호학적 민첩성'을 갖춘 이더리움(L2/ZK)으로 스마트 머니의 거대한 헷징(혹은 Rotation)이 촉발될 가능성도 엿보인다.

* 하드포크(Hard Fork): 블록체인의 핵심 규칙을 바꾸는 업그레이드. 이전 버전과 호환 불가. 커뮤니티 합의 필수. 합의가 안되면 코인의 분기(branch)가 발생. 대표적인 것이 이더리움과 이더리움 클래식.

ECC가 먹잇감 1순위인 이유

블록체인 생태계에 가장 서늘한 수치는 따로 있다. ECC-256(비트코인·이더리움이 사용하는 타원곡선 암호 기술)은 동일 보안 수준의 RSA-2048보다 양자 공격에 약 100배 취약하다. 오라토믹의 논문에 따르면, RSA-2048을 며칠 만에 깨려면 약 10만 개의 큐비트가 필요하지만, ECC-256은 불과 2만 6천 개면 충분하다.

일반적인 고전 컴퓨팅 환경에서는 ECC가 최고의 선택이었다. 서명의 크기 자체가 작아 블록체인의 '블록 공간'을 아끼고 검증 속도가 빨랐기 때문이다. 그러나 양자 컴퓨팅의 쇼어 알고리즘 앞에서는 완전히 반대가 된다. Web 2.0의 보안 체계(RSA)가 무너지기 훨씬 이전에, Web 3.0인 블록체인(ECC)이 가장 먼저, 가장 적은 비용으로 양자 해커의 최우선 먹잇감이 된다. 과거의 스마트한 선택이 양자 시대에는 치명적 약점으로 돌아온 셈이다.

비트코인의 편향?

비트코인 코어 진영은 양자 위협의 속도를 일정 부분 경시하는 단계에 머물며 일종의 편향에 빠져 있다고 사료된다. 영향력 있는 세 명의 개발자 입장이 이를 단적으로 보여준다.

- Luke Dashjr (작년 12월): "양자는 실제 위협이 아니다. 비트코인은 더 큰 문제들을 다뤄야 한다."

- Adam Back (작년 11월): "20~40년은 걸릴 것이다. 그 전에 준비할 시간이 충분하다."

- Peter Todd (작년 8월): "암호학적으로 유의미한 양자컴퓨터는 존재하지 않는다. 장난감 문제를 푸는 데모는 의미가 없다."

크립토 업계의 유명한 인플루언서인 Nic Carter가 설명한 도식을 보면 상황 변화가 매우 흥미롭다는 것을 알 수 있다. **CRQC에 대해 회의적이었던 개발자 진영의 태도가 "양자는 가짜 기술 → "양자는 실제이지만 30년 후" → "양자 위험은 있지만 투자자들의 과도한 우려가 더 문제" → "가까워지면 그때 대응하면 된다"(현재 비트코인 코어 개발진의 위치) → "지금 당장 전환해야 한다"로 바뀌는 중이라는 것이다.**

Carter의 말처럼 우리 또한, 비트코인 개발자들이 암묵적으로 의존하는 전제, 즉, CRQC 개발이 느리고 공개적이며 선형적으로 일어날 것이라는 전제가 잘못됐다고 생각한다. 양자 특이점을 향한 진보는 비밀리에 일어날 것이며, 위협이 명확해지기 전에 행동해야 한다. 그 시점이 늦어질수록 남은 시간은 이미 없다!

리더가 없는 비트코인이 전환하려 해도 일단 딜레마에 빠진다

비트코인은 현재 양자 위협에 대한 프로토콜 수준의 대응을 진행하고 있지 않다. 설령 암호화폐 커뮤니티가 PQC 전환에 합의하더라도, 기술적 장벽이 기다린다. 포스트 양자 암호(PQC)는 기존 서명보다 수십 배 거대하기 때문에 비트코인에 도입 시 하드포크와 격렬한 블록 크기 전쟁을 불가피하게 만든다.

NIST(미국 표준기술연구소)가 2024년에 공식 표준으로 정한 양자컴퓨터 시대에 안전한 새 서명 방식인 ML-DSA의 서명 크기는 약 2,400바이트다. 기존 메이저 코인들에 쓰이고 있는 ECDSA 서명(64바이트) 대비 37배나 크다. 그런데 비트코인의 블록 크기는 1MB(세그윗 포함 4MB)로 극도로 제한돼 있다. 그대로 적용하면 블록당 처리 가능한 트랜잭션 수가 현재의 1/10 이하로 줄고, 초당 처리 가능한 거래는 0.3건 수준으로 떨어진다. 수수료는 수백~수천 달러로 치솟는다. 쉽게 말해 PQC를 도입하면 도저히 못쓰는 수준이다.

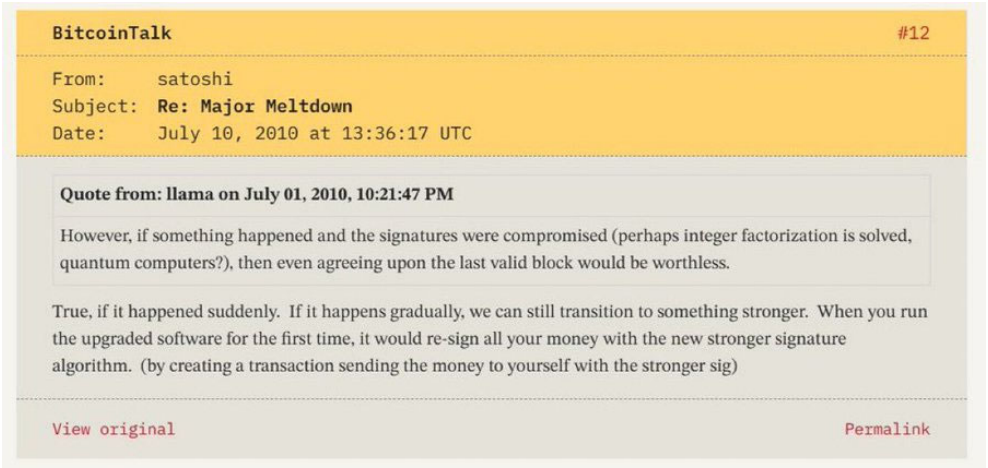
* **ECDSA:** 비트코인·이더리움의 서명 알고리즘. 그 기반 기술이 되는 게 ECC. "내가 이 돈을 보낸 사람이다"라는 걸 증명하는 디지털 서명인데, 크기가 아주 작아서 블록체인에 효율적. 그러나, 양자컴퓨터에게는 최우선 표적.

이를 해결할 유일한 기술적 경로는 새로운 서명 방식을 도입하는 것이지만, 이를 위해서는 심층적인 하드포크가 필요하다. 그런데 비트코인에는 이더리움 재단 같은 공식적 리더십이 없다. 비트코인의 무지배(Leaderless) 구조는 평시에는 강력한 해자이나, 프로토콜의 뼈대를 갈아엎어야 하는 이러한 전시 상황에서는 치명적인 의사결정 마비를 초래할 수도 있다.

과거 2017년 "블록 크기 1MB"를 둘러싼 대한 뜨거운 논쟁으로 비트코인 캐시(BCH)가 분리됐던 하드포크의 역사적 전례가 있다. 물론 이번에는 그것과는 비교할 수 없는 수준의 갈등이 예상된다. PQC 전환은 그보다 훨씬 더 큰 규모의 구조적 변경을 요구하기 때문이다.

** 사토시 나카모토는 2010년 이 문제를 이미 예견했다. "점진적으로 일어난다면 더 강한 것으로 전환할 수 있다"는 기록이 BitcoinTalk에 남아 있다. 그러나 現 커뮤니티가 이 탈출구를 쓸 의지와 능력을 갖고 있는지가 문제다.*

그림 7. 2010년 7월 사토시가 직접 쓴 비트코인톡 글을 캡처
사토시가 2010년에 이미 양자 위협의 방향 자체는 이해하고 있었다는 증거
문제는 오늘의 비트코인이 그 변화를 받아들일 합의 능력을 갖고 있느냐는 별개의 문제라는 것
즉 사토시의 통찰은 있었지만, 그 탈출구를 실행할 현재의 시스템 역량은 좀 불안한 게 사실



자료: BitcoinTalk 포럼, 미래에셋증권 리서치센터

그림 8. GitHub 커밋: "BIP360" Pay to Merkle Root
비트코인 진영도 완전히 손 놓고 있는 것은 아니라는 정황 신호, 향후 마이그레이션 여지를 만듦.
하지만, 진짜 병목은 이런 코드가 아니라 하드포크, 커뮤니티 합의, 대규모 자산 이주…

자료: Bitcoin Core GitHub 저장소, 미래에셋증권 리서치센터

이더리움의 차별화 — 포스트 양자 5단계 로드맵

한편, 이더리움 재단은 양자컴퓨터의 위협을 단순한 방어 과제가 아니라, 네트워크 전체를 한 단계 업그레이드할 수 있는 구조 개편의 기회로 보고 있다.

다시 말하지만, 여기서 말하는 양자 위협이란, 미래의 강력한 양자컴퓨터가 지금의 암호체계를 무너뜨려 지갑 서명이나 자산 보안을 위협할 수 있다는 뜻이다. 이런 위협이 현실화되기 전에 미리 새로운 보안 체계(PQC)로 갈아탈 수 있느냐가 중요하다.

이더리움은 이런 종류의 대규모 구조 전환을 실제로 해낸 전례가 있다. 2016년 DAO 해킹 당시에는 커뮤니티 합의를 통해, 블록체인 기록을 되돌리는 매우 예외적인 결정을 내렸고, 2022년에는 작업증명(PoW)에서 지분증명(PoS)으로 전환하는 'The Merge'를 네트워크 중단 없이 성공시켰다. 쉽게 말해, 이더리움은 "한 번 만들어진 규칙은 영원히 못 바꾼다"는 문화보다, 필요하다면 사회적 합의와 기술적 실행을 통해 시스템을 업그레이드할 수 있다는 문화를 가졌고 또 증명했던 체인이다.

그래서 포스트 양자 보안에서도 이더리움은 비교적 빠르게 움직이고 있다. 이더리움 재단은 2026년 1월, 포스트 양자 보안을 최우선 전략 과제로 공식화했다. 전담 조직과 연구 인센티브를 마련하며 로드맵도 선제적으로 정리하고 있다. 이는 R&D 수준이 아니라, 미래 금융 인프라의 핵심 보안 규칙을 미리 갈아끼우겠다는 것이다. 다시 말해, 이더리움은 양자 시대가 왔을 때 뒤늦게 대응하는 것이 아니라, 그 시대에 맞는 금융 레일이 되겠다는 방향성을 이미 세웠다.

이더리움 핵심 개발자 저스틴 드레이크가 이 위기를 "장애물이 아니라 기회"라고 말하는 이유도 여기에 있다. 만약 이더리움이 포스트 양자 전환을 성공적으로 해낸다면, 전 세계 누구나 접근 가능한 글로벌 금융 네트워크가 가장 앞선 보안 체계를 먼저 탑재하는 사례가 될 수 있다.

사실 코인만 위험한 게 아니에요

그런데, 여기서 CRQC의 위험이라는 것이 암호화폐에만 직격탄이 아님을 명심하자. 블록체인(ECC 암호 기반)이 가장 먼저, 가장 적은 비용으로 양자 해커의 최우선 먹잇감이 되기는 하지만, **SWIFT도 양자 특이점의 공격 대상이 된다. CRQC가 깨뜨리는 대상은 '코인'만이 아니라 현재 널리 쓰이는 공개키 암호와 디지털 서명 체계이고, 이는 암호화폐 지갑뿐 아니라 인터넷 트래픽, 전자상거래, 금융 메시징, 계정 인증 전반에 깔려 있다. 따라서, 이더리움이 포스트 양자 보안을 갖추면, 비트코인뿐 아니라 변화 속도가 느린 전통 금융 시스템과 비교해도 "미래형 보안을 갖춘 결제·자산 인프라"라는 강력한 차별점을 얻게 될 수 있다.**

표 3. CRQC는 코인만이 아니라 전통 금융·인터넷 전체 공개키 암호 체계도 충분히 위협한다

	ECC 256비트 (비트코인·이더리움)	RSA 2048비트 (일반 웹 / 정부 / 금융기관)
논리적 큐비트 (Shor 알고리즘 최적화)	1,098~1,450개	~1,730~2,043개
물리적 큐비트 (초전도+표면코드)	〈500,000개	〈1,000,000개
물리적 큐비트 (중성원자+qLDPC)	10,000~26,000개	~102,000개
깨지는 데 소요 시간	• 초전도: 9분 이내 (primed attack) • 중성원자: 10일 이내 (26k 큐비트)	• 초전도: 수주~수개월 • 중성원자: 97일 (102k 큐비트)

자료: 구글, 오라토믹, 미래에셋증권 리서치센터

반대로 말하면, 구조를 쉽게 바꾸기 어려운 디지털자산 네트워크는 양자 위협 앞에서 보안 기술 부채가 쌓일 수 있다. 이 지점에서 시장은 단순히 “어느 코인이 더 유명한가”가 아니라, “어느 네트워크가 실제로 미래 위협에 맞춰 스스로를 업그레이드할 수 있는가”를 보기 시작할 가능성이 높다. 결국 스마트 머니는 가격 차트만 보는 것이 아니라, 장기적으로 자산을 안전하게 실어 나를 수 있는 시스템이 무엇인지 따져보게 되기 때문이다.

큐비트 요구량이 기하급수적으로 폭감하는 수학적 궤적과 탈중앙화 네트워크를 업그레이드하는 데 걸리는 수년의 딜레이를 생각하면 답은 하나뿐이다. 블록체인 생태계의 마이그레이션 타임머신은 '지금 당장' 가동되어야만 생존할 수 있다.

(4) 관전 포인트 4: PQC 전환이 만드는 ‘불변성 도그마’의 해체

블록체인에서의 절대 도그마(의심이나 비판 없이 절대적인 진리처럼 받아들이는 믿음)였던 '불변성(Immutability)'이라는 철학이라는 게 이제 양자 물리 법칙 앞에서 폐기될 수도 있을 것 같다. 공격이 가시화되기 전에 선제적으로 스스로 암호를 해체하고 재조립(PQC 전환)하는 코인 생태계만이 미래 금융의 패권을 가질 수 있기 때문이다.

공격은 시작된 후엔 막을 수 없다

공격이 시작된 후 패치를 하는 사후 대응 방식은 “단 9분 만에” 시스템 권한이 통째로 넘어가는 포스트 양자 시대에는 절대 통용되지 않는 안일한 행위다. 전통적인 소프트웨어 보안에서는 취약점 발견 → 패치 배포 → 업데이트 적용이라는 주기가 유효했다. 그러나 양자 컴퓨팅과 AI의 결합이 만드는 공격 환경은 이 주기 자체를 무의미하게 만든다.

구글의 논문도 직접 경고하듯, 양자 하드웨어의 발전은 “선형적이지 않으며” 은밀하게 임계점을 돌파한다. 따라서 생태계의 마이그레이션은 물리적 위협이 입증되기 수년 전에 완료되어야 한다. Q-Day 이후에는 이미 늦다.

불변성의 역설 — 강점이 족쇄가 되는 순간

"한 번 기록된 것은 영원히 변하지 않는다"는 것은 비트코인의 가장 강력한 서사였다. 그러나 동시에 가장 위험한 족쇄가 될 수도 있다. 블록체인의 불변성은 두 가지 전제 위에 서 있다. 타원 곡선 암호 체계가 깨지지 않는다는 것, 그리고 네트워크가 인간 수준의 공격자만을 상정한다는 것이다. 양자 컴퓨팅은 이 두 전제를 동시에 공격한다.

CRQC가 현실화되면 비트코인 커뮤니티는 선택의 기로에 선다. 불변성을 지키다가 자산이 털리게 두겠는가? 아니면 불변성의 서사를 버리고 하드포크를 하겠는가? 두 선택지 모두 고통스럽다. 불변성이라는 철학적 낭만을 버리고, 파괴적인 양자 공격 앞에서 스스로를 해체하고 재조립하는 생태계만이 미래에 살아남을 수 있을 것이다. 향후 모든 Web 3.0 및 금융 인프라의 가치 평가는 시스템 중단 없이 암호 모듈을 빠르게 교체할 수 있는 민첩성(Cryptographic Agility)에 의해 결정될 가능성이 높아보인다.

(5) 관전 포인트 5: "진짜 위험은 따로 있다… 바로 AGI"

디지털 자산의 진정한 위협은 멀리 있는 양자컴퓨터가 아니라, 지금 이 순간 빠르게 자라고 있는 AI 지능이라고 생각한다. AGI(범용 인공지능)가 양자 컴퓨팅 제어권을 확보할 경우, 가장 먼저 탈취를 시도할 절대적 목표물은 방어자가 없는 암호화폐 휴면 지갑이 될 것이다.

Anthropic의 Black-hat LLMs — 이미 일어나고 있는 현실

* **제로데이(0-day):** 아직 패치가 없는, 개발사도 모르는 취약점.

Anthropic 연구원 Nicholas Carlini가 밝힌 공개 시연은 AI 업계에 적잖은 파장을 주었다. 그의 메시지는 두 문장으로 압축된다. 첫째는 LLM이라는 것이 이제 자율적으로, 그리고 복잡한 툴 없이도 핵심 소프트웨어의 제로데이 취약점을 찾아내고 익스플로잇할 수 있다는 것이다. 둘째는 그 인공지능이 섬뜩할 정도로 빠르게 발전하고 있다는 내용이다.

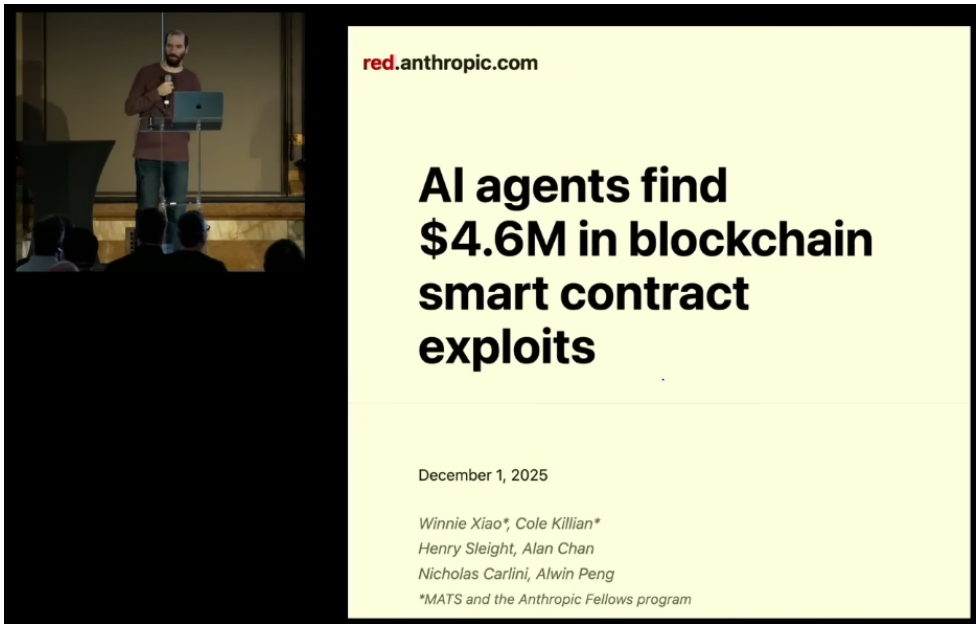
그가 시연한 사항들을 보면 소름이 돋을 정도다. 가장 충격적인 내용은 Ghost CMS를 보여준 사례다. Ghost CMS는 GitHub 별 5만 개 이상의 유명 콘텐츠 관리 시스템이고, 역사상 단 한 번도 치명적 취약점이 발견된 적 없는 소프트웨어였다. 하지만 Claude는 단순한 프롬프트 지시만으로 90분 만에 Blind SQL Injection(프로그램이 데이터베이스에 질의할 때 악의적 코드를 삽입해 인증 없이 데이터 탈취) 취약점을 찾아냈고, 관리자 API 키와 비밀번호 해시를 아무 인증 없이 추출하는 스크립트까지 작성했다.

스마트 컨트랙트 — AI에게 가장 적합한 사냥터

* **스마트 컨트랙트(Smart Contract):** 블록체인에 배포되는 자동 실행 프로그램. 조건이 충족되면 코드가 자동으로 자금을 이동시킨다. 코드 = 자본이라는 특성상 취약점 발견 즉시 수익화 가능.

그런데 Nicholas Carlini의 시연 중 크립토 업계가 집중해서 봐야 할 것은 따로 있었다. Anthropic의 MATS 연구진은 AI 에이전트가 블록체인 스마트 컨트랙트(블록체인에 배포되는 자동 실행 프로그램)에서 460만 달러를 자율 탈취하는 시뮬레이션을 2분 26초 만에 완수한 것이다.

그림 9. AI 해커가 현실 세계의 자본을 직접적으로 탈취하는 스마트 컨트랙트로 올 수 있다는 경고
에이전트가 인간 개입 없이 460만 달러 규모의 DeFi 공격 경로를 자율적으로 생성해 냈음을 증명. 이 연구 결과는 향후 기관 투자자들의 RWA 토큰화 인프라가 직면할 가장 큰 리스크의 선행지표.



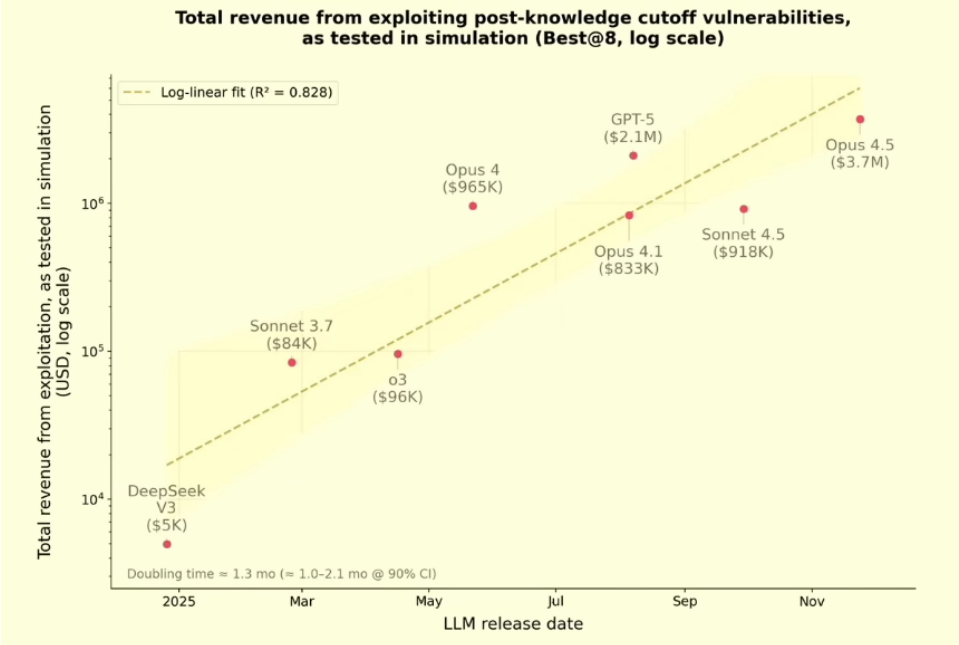
자료: Anrhtopic, Nicholas Carlini, 미래에셋증권 리서치센터

이 시뮬레이션의 통제 변수를 알고 보면 더 무섭다. 모델의 학습 데이터에 포함될 수 없는 '지식 차단일(Knowledge Cutoff) 이후'에 배포된 스마트 컨트랙트만을 대상으로 했다. 과거 해킹 사례를 암기해 재현한 게 아니라, 진짜 제로데이 상태의 코드를 실시간 분석해서 실제 코인을 탈취한 것이다.

블록체인의 스마트 컨트랙트가 AI에 완벽한 해킹 사냥터가 되는 이유는 세 가지다. 첫째, 스마트 컨트랙트 코드는 오픈소스로 공개돼 있어 AI가 즉시 분석 가능하다. 둘째, 취약점 트리거 순간 암호화폐가 자동으로 이체되어 성공하면 즉시 경제적 보상을 받는다. 셋째, 블록체인 네트워크에 한 번 배포된 스마트 컨트랙트는 수정이 극도로 어렵다.

Anthropic의 연구진이 밝힌 데이터 포인트들은 더욱 냉혹하다. AI 모델의 해킹 능력이 무려 1.3개월마다 두 배씩 강력해지고 있다는 것이다. 무어의 법칙(18~24개월마다 집적도 2배)보다 15배 이상 빠른 속도다. Claude 3.5 Sonnet이 수천 달러 수준의 버그를 찾았다면, 불과 몇 달 뒤의 모델은 수백만 달러짜리 복잡한 금융 로직을 자율적으로 파괴한다.

그림 10. 대형언어모델별 스마트 컨트랙트 해킹을 통한 탈취 수익은 점점 얼마나 높아졌을까?
Y축이 로그 스케일: 모델의 세대가 교체될 때마다 해킹 가능한 자본 규모가 기하급수임을 표현
DeepSeek V3는 몇 백만원 짜리 버그에 그쳤다면 현재의 최신모델은 수십억 원 규모 해킹이 가능.
모델의 해킹 능력이 1.3개월마다 두 배씩 강력해진다는 게 포인트!



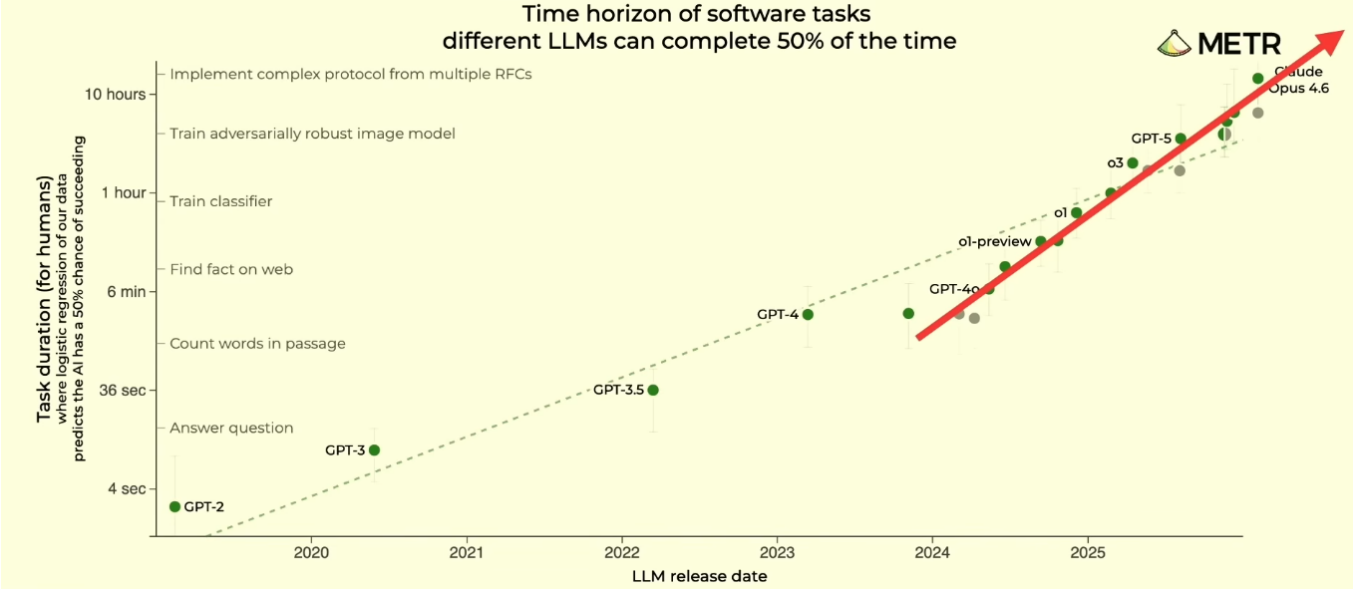
자료: Anrhtopic, Nicholas Carlini, 미래에셋증권 리서치센터

Anthropic 내부로부터 유출된 문서에 따르면, 곧 출시될 Claude Mythos(내부 코드명 Capybara) 모델에 대해 이렇게 적혀져 있다. "현재 다른 어떤 AI 모델보다 사이버 역량에서 훨씬 앞서 있으며, 방어자들의 노력을 훨씬 능가하는 방식으로 취약점을 악용할 수 있는 모델들의 다가오는 물결을 예고한다." 이 모델이 공개된 날 사이버보안 주식은 폭락했다.

AI가 CRQC를 당길 가능성이 어느 때보다 크다

문제는 CRQC(암호학적으로 유의미한 양자컴퓨터)를 '먼 미래의 사건'으로 취급하는 순간, 이미 방어는 늦을 수 있다는 점이다. "두세 해 전만 해도 2050년 이전에 이런 일이 벌어지리라 상상도 못 했다."고 양자 전문가들이 말하고 있는데, 그 상상할 수 없었던 것을 현실로 앞당기고 있는 것이 바로 AI의 개입이다.

그림 11. METR의 소프트웨어 태스크 수행 시간 지수 함수 그래프
가파르게 상승하는 붉은색 추세선은 고난도 인간 엔지니어링 태스크를 자율 수행하는 AI 역량이 통제 불가능한 궤도에 올랐음을 증명
특히 올해 들어 기울기가 더 가파르게 바뀌고 있다는 것을 의역해서 표현하자면, AI의 지능 창출력이 2025년의 기대보다 더 높아졌다는 것
과거의 경험칙에 의존하여 내년의 해킹 위협 수준을 올해와 비슷할 것이라 오판하면 안됨…



자료: Anrhtopic, Nicholas Carlini, 미래에셋증권 리서치센터

AI는 소프트웨어 취약점을 찾는 해킹 도구에 그치지 않는다. 반도체 설계, 양자 오류 보정, 실험 자동화, 재료 탐색, 제어 알고리즘 최적화 같은 양자컴퓨팅의 병목 전반에 침투해 연구 생산성을 끌어올릴 수 있는 범용 가속화 도구다. 다시 말해, 양자 특이점은 인간 연구자들의 속도로 오는 것이 아니라, AI가 증폭한 과학 엔진의 속도로 다가올 수 있다. 블록체인 생태계의 진짜 위협은 양자컴퓨터의 등장이 아니라, 그것이 AI와 결합하는 순간이다.

그리고 그 순간이 도래했을 때 공격자가 가장 먼저 노릴 표적은 이미 공개된 지 오래됐고, 방어 주체가 부재하며, 일단 탈취가 시작되면 되돌릴 방법도 거의 없는 암호화폐 주소들일 가능성이 높다. 그래서 CRQC 문제의 본질은 "양자가 언제 오느냐"가 아니라, "그 시점이 생각보다 훨씬 빨라질 수 있다"는 전제하에 하루빨리 보안 체계 마이그레이션을 준비하느냐에 있다.

3. 이더리움의 포스트 양자 로드맵 — 준비하는 자의 청사진

(1) 이더리움의 5차원 취약성 구조

사실 이더리움의 양자 취약성은 비트코인보다 넓고 복잡하다. 구글 논문은 이를 5개로 분류했다. 아래 표를 보면 이더리움의 양자 리스크가 "계정·관리키·코드·합의·데이터 가용성"으로 퍼져 있는 다층 시스템 리스크라는 점을 알 수 있다. 즉 생태계 전체의 신뢰 구조가 흔들린다는 게 정확한 표현이다.

표 4. 구글에서 밝힌 이더리움의 취약성 유형 및 노출 규모

취약성 유형	핵심 내용	추정 노출 규모
계정 취약성	최초 트랜잭션 발생 시 공개키 영구 노출. 상위 1,000개 ETH 계정 데이터 해킹	**~2,050만 ETH**
관리 키 취약성	USDT·USDC 등 스테이블코인 관리 키 노출. 탈취 시 무한 발행·DeFi 공격 가능	**~2,000억 달러**
코드 취약성	EVM 프리컴파일에 PQC 지원 없음. zkSTARK 기반 Starknet 상대로만 안전	—
합의 취약성	BLS 서명 기반 타원 곡선 기반. 검증자 2/3 장악 시 체인 이력 재작성 가능	**~3,700만 ETH(스테이킹)**
데이터 가용성 취약성	KZG 약정 설정값 누출 시 L2 데이터 가용성 증명 영구 위조 가능. Dencun 이후 전체 L2에 해당	—

자료: Google Quantum AI 논문, 미래에셋증권 리서치센터

*** EVM 프리컴파일:** EVM 안에 미리 박아둔 고성능 '특수 함수'. 스마트컨트랙트가 무거운 암호 연산을 코드로 직접 짜지 않고, 정해진 주소를 호출해서 더 싸고 빠르게 씀. 즉 PQ 서명 Precompiles는 포스트양자 서명 검증 기능을 그런 형태로 EVM 레이어에 기본 탑재하겠단 뜻.

계정 취약성은 애초에 이더리움 계정 모델의 구조적 문제에서 비롯된다. 그리고 관리키 취약성의 ~2,000억 달러는 USDT·USDC 같은 스테이블코인 관리자 키가 뚫릴 경우의 파급력을 뜻한다. CRQC로 이 관리자 키를 탈취하면 토큰 무한 발행, DeFi(탈중앙화 금융) 프로토콜 장악이 가능해진다. 2026년 2월 기준 스테이블코인 및 RWA 관련 노출 규모만 약 2,000억 달러로 추정된다.

그리고 코드 취약성은 현재의 EVM 프리컴파일은 PQC를 기본 지원하지 않는다는 뜻이다. 그래서 일반 EVM 생태계는 구조적으로 뒤처져 있다. 4번째인 합의 취약성의 본질은, 이더리움의 합의 메커니즘에서 사용되는 BLS 서명 집계(수십만 개의 검증자 서명을 하나로 압축하는 기술)도 결국 타원 곡선 기반이라 양자 공격에 취약한 문제다. 검증자 2/3를 장악하면 체인 이력을 재작성까지 할 수 있으므로, 2026년 2월 기준 약 3,700만 이더리움 코인이 잠겨 있는 스테이킹의 보안도 곧 양자 특이점 문제와 직결된다.

마지막으로 데이터 가용성 취약점은 파급력 측면에서 제일 위험하다. CRQC로 비밀키를 단 한 번 추출하면, 이후에는 양자컴퓨터 없이 그냥 고전 컴퓨터로도 L2 데이터 가용성 증명을 무한히 위조할 수 있다. 없었던 데이터를 원하는대로 계속 만들 수 있다는 말이다. Dencun 업그레이드 이후, L2 데이터가 이 구조에 의존하고 있기 때문에 이더리움 생태계 전체가 오염될 수 있다.

(2) 방어적 가속주의와 5단계 마일스톤

이더리움의 창시자 비탈릭 부테린이 제시한 "방어적 가속주의(Defensive Accelerationism, d/acc)"는 기술 위협에 두려워하기보다 방어 기술 발전을 극한으로 끌어올려 선제 대응한다는 입장을 가진 철학이다. 단순한 슬로건만은 아니다. 지난 2월 '올해는 이더리움이다'라는 보고서에서 우리가 말했듯, **이더리움 재단은 이미 PQC 전환을 위한 전담 리소스를 배치해서 팀을 만들었다. 또한 EIP-7932(PQC 서명 방식을 위한 프리컴파일 도입 제안)를 공식 논의 중**이기도 하다.

게다가, 2016년 DAO 해킹 당시 커뮤니티 합의를 통해 블록체인 이력을 되돌린(롤백한) 전례도 있다. 필요할 때 결단을 내릴 수 있는 거버넌스 구조와 의지가 어느정도 검증됐다는 말이다.

이와 관련해 이더리움 재단이 공식적으로 가동 중인 '포스트 양자 보안'에 관한 로드맵은 "pq.ethereum.org" 사이트에 공개되어 있다. 이 로드맵은 계정·합의·코드·데이터 가용성의 전 레이어에 걸쳐 5단계 마일스톤을 설정하고 있다. 각 마일스톤은 알파벳 순서대로 명명되는데, 아래 표의 ★ 표시는 포스트 양자 관련 핵심 업그레이드임을 뜻한다.

표 5. 이더리움 포스트-퀀텀(PQ) 마일스톤 로드맵

프로젝트 명	마일스톤	레이어	의미 및 내용
I★	PQ Key Registry (이주 대상자 명부를 만드는 단계)	합의 (Consensus)	PQ 공개키 등록 시스템 구축. 양자 공격이 시작되면 기존 ECDSA 키를 폐기하고 사전 등록된 PQ 키로 전환할 수 있게 하는 "탈출구(Escape Hatch)" 확보가 목적. L1에 PQ 키를 사전 등록하는 EVM 프리컴파일(EVM에 내장된 특수 함수) 또는 시스템 컨트랙트를 배포하는 것이 핵심.
J★	PQ 서명 Precompiles (사용 가능한 애플리케이션으로 만듦)	실행 (Execution)	PQC 서명 검증 함수 내장. PQ 서명 검증을 EVM 레벨에서 효율적으로 처리할 수 있도록 프리컴파일을 도입하는 단계. 서명 크기가 수십 배 커지는 PQC의 부담을 가스비(이더리움 네트워크의 수수료) 최적화로 상쇄.
L★	PQ Attestations + LeanVM (BLS를 STARK 기반 PQ 구조로 옮김)	합의+데이터	합의 레이어의 핵심 수술. 기존 BLS 서명 대신 STARK 기반 PQ 서명으로 전환. 동시에 LeanVM 도입으로 암호학적 최적화와 초경량 ZK 가상머신으로 무거운 PQ 서명 처리를 효율화. ** LeanVM은 해시 기반 PQ 암호학 처리만을 위해 설계된 초경량 ZK 가상머신. 불필요한 기능을 모두 제거해 연산 효율을 극대화한 이더리움 자체 개발 도구.*
M★	PQ Sig Aggregation + PQ Blobs (L2 전체 데이터 레이어까지 양자 내성화)	실행+데이터	서명 집계 기술과 동시에 양자 내성 블롭(Blob) 업그레이드. BLS 대체와 KZG 다항식 약정을 STARK 기반 양자 내성(PQC)으로 교체. L2 전체 생태계의 데이터 안전성 확보.
장기	Full PQ Consensus (완전한 합의)	전 레이어	모든 레이어에서 타원 곡선 의존성이 제거된 완전한 포스트 양자 이더리움. 실행·합의·데이터의 모든 암호학 기반 요소를 타원 곡선에서 해시 기반으로 전환. PQ 트랜잭션·PQ 슬롯·이더리움의 완전한 양자 내성 확보.

자료: 이더리움 재단, 미래에셋증권 리서치센터

이더리움의 포스트 양자 대응이 한 번의 패치가 아니라, 등록 → 검증 → 합의 수술 → 집계/데이터 교체 → 전면 전환으로 이어지는 단계적 마이그레이션이라는 점을 보여준다. 즉 기술 문제가 아니라 시스템 재건축이라고 봐야 겠다. 위의 로드맵 표가 말하는 메시지는 명확하다. **이더리움의 경쟁력은 지금 양자 위협에 안전해서가 아니라, 위험을 이미 잘 알고 전체 스택을 순서대로 뜯어고칠 설계도를 이미 갖고 있고 대비/착수를 했다는 점이다.**

* **STARK:** 거대한 계산이 제대로 수행됐다는 사실을, 내용을 전부 다시 계산하지 않고 짧은 증명으로 확인하는 방식. "해시 함수 기반의 영지식 증명" 방식이라서, 타원 곡선 의존성이 없음. 즉, 양자 시대에도 근본적인 방어가 가능.

(3) STARKs — 포스트 양자 시대의 궁극적 방패

이더리움이 포스트 양자 전환의 핵심 무기로 선택한 것은 STARKs다. NIST 표준인 격자 기반 암호(ML-DSA 등)가 아닌 해시 기반 접근을 택한 이유가 있다.

격자 기반 암호는 양자 내성이 있다고 여겨지지만, 수학적 구조의 복잡성으로 인해 예기치 못한 알고리즘에 뚫릴 가능성을 완전히 배제할 수 없다. 반면 **해시 함수는 양자 컴퓨터의 구조상 역연산이 물리적으로 불가능에 가깝다.** 그로버 알고리즘(Grover's Algorithm)이 해시 함수를 약화시킬 수 있지만 그 효과는 키 길이를 두 배로 늘리는 정도에 불과하다.

이에 대해서, **이더리움 생태계 안에는 이미 STARK 계열의 L2인 Starknet이 있어 실증 사례가 있다는 점이 중요하다. 해시 기반 STARK 방식으로 가는 기술적 경로가 이미 이더리움권 안에서 자라고 있다는 것이기 때문이다.** 물론, 최종 목표는 그 논리를 이더리움 생태계 전반으로 확장하는 것이다.

STARKs가 전면 적용되면 이더리움은 수백만 개의 PQ 서명을 매우 가벼운 형태로 압축해 블록체인에 올릴 수 있다. 비트코인이 덩치 큰 PQC 서명 때문에 교통체증에 시달릴 때, 이더리움은 처리량을 유지하면서도 양자 내성을 확보하는 우위를 가질 수 있다. 이것이 이더리움의 암호학적 민첩성이다.

다만 여기서 단서를 붙여야 한다. 암호학적 민첩성은 방향성의 우위이지, 자동 면죄부가 아니다. PQC는 소프트웨어 알고리즘 교체로 구현 가능하지만 블록체인에서의 전환은 일반적인 소프트웨어 업데이트와 달리 고통스러운 작업을 수반한다. "커뮤니티의 합의, 자산 마이그레이션, 서명 크기 증가에 따른 비용 구조 변화, 암호화폐 지갑 재설계, 그리고 무엇보다도 L1뿐 아니라 L2 및 브릿지 레이어까지 포함한 연쇄적 마이그레이션"까지 싹 필요하다.

따라서 이더리움이 비트코인보다는 현재 낫다는 말이지 안전하다는 뜻은 아니다. 더 정확하게는, 이더리움 재단의 리더십 아래 상대적으로 빠른 방향 설정은 가능하겠지만, L2 생태계 전체의 마이그레이션은 별도의 전쟁이라 할수 있다. 결국 시장이 주목해야 할 것은 이러한 선언이 아니라 실행의 속도다. **양자 시대를 맞아 최종 승자가 되는 블록체인은 가장 완벽한 체인이 아니라, 가장 빠르게 스스로를 뜯어고칠 수 있는 체인일 가능성이 높다.**

(4) 종합하면…

양자 위협은 더 이상 수십 년 뒤의 공상과학이 아니며, '2029년'이라는 실체적 생존 카운트다운이 시작되었다. 구글 퀀텀 AI와 오라토믹의 동시 논문 발표, 스콧 아론슨이라는 양자 권위자와 수많은 양자컴퓨팅 전문가들의 독립적 검증 등이 이를 뒷받침한다.

구글이 공격 회로를 숨기고 ZKP만 공개한 것은 비밀 군비 경쟁의 시작이다. 1940년대의 "핵 기밀(Frisch-Peierls)"의 역사가 운율을 따르는 세계가 지금 다시 도래하고 있다.

* 오토 프리쉬와 루돌프 파이어를스는 1940년 연쇄 반응에 필요한 우라늄(U-235)의 양을 계산했지만, 직전까지 핵분열 연구가 공개적으로 출판되고 있었음에도 그 결과를 공개하지 않았다. 이것이 핵 기밀의 시작이었다.

비트코인의 리더 없는 거버넌스와 이념적 경직성은, PQC 전환이라는 생존 과제 앞에서 구조적 약점이 된다. 반면 이더리움은 재단의 리더십, d/acc 철학, ZK 인프라의 이중 활용, 그리고 가동 중인 5단계 로드맵으로 양자 시대의 차별화된 생존 경로를 확보하고 있다.

또한, 오라토믹 논문이 LLM의 성능이 개입된 QEC(양자 오류 정정) 코드로 이미 증명했듯, **진짜 와일드카드는 양자 특이점 자체가 아니라 그것을 가속시키는 AI의 특이점이다.** Anthropic의 스마트 컨트랙트 460만 달러 탈취 시뮬레이션이 보여주듯, AI는 이미 블록체인의 가장 약한 고리를 이미 공략하고 있다. 매 1.3개월마다 두 배로 성장하는 AI 공격 역량 앞에서, 관망의 스탠스는 전략이 아니라 항복에 가까운 선택이다.

불변성이라는 낭만의 시대 도그마를 버리고, 양자 법칙 앞에서 스스로를 해체하고 빠르게 변화하는 생태계만이 Web 3.0 이후의 금융 패권을 가질 수 있다. **암호학적 민첩성을 내재화한 생태계와 그렇지 못한 생태계 사이에 역사적인 자본 이동이 시작될 것으로 보인다**.

II. 양자컴퓨터가 코인을 공격하는 경로

* CRQC: Cryptographically Relevant Quantum Computer의 줄임말로, 암호화폐를 해독할 수 있는 수준의 양자컴퓨터를 뜻함.

1. 다 같은 양자컴퓨터가 아니다: Fast-Clock과 Slow-Clock

구글 논문은 "양자컴퓨터가 언제 등장하는가"라는 질문에서 한 걸음 더 나아가, "어떤 플랫폼의 양자컴퓨터가 먼저 CRQC에 도달하는가"가 위협의 성격 자체를 결정한다는 점을 명시했다.

(1) 두 가지 계열: 속도가 공격 유형을 결정한다

Fast-Clock 계열은 초전도(superconducting), 광자(photonic), 실리콘 스핀(silicon spin) 방식이다. Google, IBM, Amazon, Rigetti, Intel, PsiQuantum, Xanadu 등이 이 범주에 속한다. 게이트 속도(큐비트에 연산을 수행하는 속도)가 마이크로초(100만분의 1초) 수준이며, 오류 정정 사이클도 그에 준한다. 빠른 연산 속도가 핵심 장점이다.

Slow-Clock 계열은 이온 트랩(ion trap)과 중성 원자(neutral atom) 방식이다. IonQ, Quantinuum, QuEra, Infleqtion, Atom Computing, Pasqal 등이 여기에 해당한다. 기본 연산 속도는 Fast-Clock 대비 약 100~1,000배 느리다.

이 속도 차이가 공격의 물리학을 좌우한다.

(2) 공격 유형: At-Rest vs On-Spend

- At-Rest Attack(정적 공격): 오랫동안 블록체인에 공개된 공개키를 노리는 공격이다. 공격자에게 며칠에서 수십 일의 시간이 주어진다. P2PK 방식으로 잠긴 사토시 시대 코인, Taproot 주소, 주소를 재사용한 지갑이 모두 이 공격의 대상이다. Slow-Clock CRQC로도 충분히 실행 가능하다.

- On-Spend Attack(동적 공격): 사용자가 트랜잭션을 브로드캐스트(네트워크에 전파)하는 순간, 해당 트랜잭션이 블록에 기록되기 전까지의 짧은 시간 창(window) 안에 공개키를 탈취해 위조 트랜잭션을 삽입하는 공격이다. 비트코인의 경우 평균 블록 생성 시간이 10분이므로, 공격자는 그 안에 개인키 도출을 완료해야 한다. Fast-Clock CRQC가 전제되어야 한다.

(3) On-Spend 성공 확률의 산술

초전도 아키텍처를 기준으로 On-Spend 공격을 가정하면, 양자 회로의 실행 속도는 큐비트 자체의 물리적 속도만으로 결정되지 않는다. 실제 시스템에서는 양자 연산의 다음 단계를 결정하는 고전 제어 시스템의 반응 시간(reaction time)이 병목이 된다. 논문은 초전도 큐비트의 표준 반응 시간인 10마이크로초를 적용했다. Toffoli 게이트(양자 연산의 기본 단위이자 비용 지표)당 50% 오버헤드를 더하면, 7,000만 게이트는 약 18분, 9,000만 게이트는 약 23분에 실행된다.

여기서 "primed(사전 준비)" 상태라는 개념이 등장한다. 쇼어 알고리즘은 크게 두 단계로 구성된다.

첫 번째 단계는 어떤 공개키를 공격하든 상관없이 프로토콜 공통 파라미터만으로 실행되는 준비 단계다. 두 번째 단계는 실제 공개키를 입력받아 개인키를 도출하는 단계다. 공격자는 첫 번째 단계를 공격 이전에 미리 실행해 양자컴퓨터를 대기 상태로 유지할 수 있다. 이렇게 하면 공개키가 포착되는 순간 두 번째 단계만 실행하면 되므로, 실질적인 공격 소요 시간은 절반인 약 9~12분으로 줄어든다.

비트코인 트랜잭션이 브로드캐스트되면 즉시 블록에 기록되는 것이 아니라, 멤풀(mempool, 공개 메모리풀)이라는 대기열에 먼저 올라간다. 채굴자가 다음 블록을 생성할 때까지 이 대기열에 머무르는 시간이 공격자에게 주어지는 창이다. 비트코인의 평균 블록 생성 시간은 10분이지만, 블록 생성은 확률적 포아송 과정(이전 블록과 무관하게 매 순간 같은 확률로 독립적으로 발생하는 확률 과정)이라 실제로는 1분 만에 생성되기도 하고 30분이 넘기도 한다.

논문이 제시한 성공 확률 모델에 따르면, 초전도 CRQC가 9분 안에 키를 도출할 경우 비트코인 On-Spend 공격의 성공 확률은 약 41%다. 동전 던지기보다 약간 낮은 확률이지만, 공격자 입장에서는 여러 번 시도하면 성공이 사실상 보장되는 수준이다.

이더리움의 경우 블록 생성 시간이 약 12초에 불과해 초전도 CRQC로도 On-Spend 공격이 사실상 불가능하다. 하지만 이더리움의 주요 위협은 On-Spend가 아닌 At-Rest 상태에 있다. 앞서 살펴본 계정 취약성, 관리키 취약성, 합의 취약성 모두 시간 제약 없이 공격할 수 있는 At-Rest 유형이다.

양자컴퓨터가 쇼어 알고리즘을 실행하면서 Toffoli 게이트를 구동하려면 "T state"라는 특수한 양자 상태를 외부에서 지속적으로 주입해야 한다. 엔진이 돌아가려면 연료를 계속 공급해야 하는 것과 같은 구조다. 이 T state를 만들어내는 큐비트는 알고리즘 실행에 쓰이는 큐비트와 별개로 따로 할당해야 한다. T state 공급 속도가 양자 공격의 현실성을 결정하는 1차 거름망이다.

(4) Fast-Clock: 연료 공급에 여유가 있다

7,000만 개의 Toffoli 게이트를 9분 안에 실행하려면 초당 약 50만 개의 T state가 필요하다. T state 하나를 만드는 데는 약 50,000 큐비트-라운드(큐비트 수 × 오류 정정 사이클 수)가 필요하다.

오류 정정 사이클이 1마이크로초인 Fast-Clock에서는 25,000개의 큐비트를 T state 생산에 할당하면 초당 약 50만 개를 공급할 수 있다. 25,000 큐비트는 알고리즘 전체 실행에 필요한 50만 큐비트의 5%에 불과하다. 부담이 작으니 On-Spend에 필요한 속도를 맞출 수 있다.

(5) Slow-Clock: 연료 공급이 불가능하다

오류 정정 사이클이 100마이크로초 이상인 Slow-Clock에서는 같은 속도로 T state를 공급하려면 큐비트를 100배 더 투입해야 한다. 계산하면 약 250만 큐비트가 T state 생산에만 필요해지는데, 이는 알고리즘 자체 실행에 필요한 50만 큐비트의 5배다. 현실적으로 감당할 수 없는 수준이다.

결국 **Slow-Clock은 9분짜리 On-Spend를 위한 T state 공급 자체가 물리적으로 불가능하다. 반면 며칠의 시간이 주어지는 At-Rest 공격은 T state를 천천히 생산해도 되므로 가능하다**. 이것이 두 플랫폼의 위협 유형이 갈리는 물리적 근거다.

표 6. T state 공급 속도가 1차 거름망

	Fast-Clock (초전도)	Slow-Clock (이온 트랩/중성 원자)
오류 정정 사이클	~1 마이크로초	~100 마이크로초 이상
T state 생산용 큐비트	~25,000개 (전체의 5%)	~250만개 (전체의 500%)
T state 생산 부담	가벼움	현실적으로 불가능
At-Rest 공격	가능	가능
On-Spend 공격	가능	불가능
위협 시점	At-Rest와 On-Spend 동시	At-Rest가 먼저, On-Spend는 훨씬 후

자료: Google, 미래에셋증권 리서치센터

2. 흐려지는 경계: “느린 시계”가 빨라지는 새로운 경로

Slow-Clock 계열이 At-Rest 공격만 가능하다는 분석은 현재 기술 수준을 기준으로 한 스냅샷이다. 그러나 이온 트랩 기술의 발전 방향을 살펴보면, Fast-Clock과 Slow-Clock의 경계 자체가 재정의될 가능성이 있다.

(1) 이온 트랩의 근본 한계: 물리법칙이 속도를 결정한다

이온 트랩은 전기장으로 원자를 공중에 띄워 레이저로 조작하는 방식이다. 큐비트 두 개를 얽히게 만드는 2큐비트 게이트를 실행하려면 이온의 집단 진동 모드를 매개로 사용해야 하는데, 이 진동 모드를 제어하는 데 수십~수백 마이크로초가 걸린다. 이것은 레이저의 성능이나 제어 장비의 문제가 아니라, 이온이라는 물질 자체의 물리적 진동 주파수에 의해 결정되는 한계다. 칩 위에 올리거나 제어 방식을 바꾼다 하더라도 본질적으로 안고 가야 하는 물리적 제약이다.

확장성도 문제다. 기존 방식은 개별 이온을 조작할 때마다 정밀하게 정렬된 레이저 빔을 사용한다. 큐비트 수가 수십 개를 넘어가면 수십 개의 레이저를 동시에 정밀하게 제어해야 하는데, 이 복잡도가 큐비트 수에 비례해 폭발적으로 증가한다. 이른바 "레이저 스파게티" 문제다. 수백만 큐비트로의 확장은 이 구조로는 사실상 불가능하다.

(2) EQC: 레이저를 버린 이온 트랩

Oxford Ionics는 이 문제를 다른 경로로 접근했다. EQC(Electronic Qubit Control)라 불리는 이 기술은 레이저 대신 실리콘 칩에 내장된 안테나에 전류를 흘려 마이크로파 자기장을 생성하고, 이것으로 양자 게이트를 구동한다. 레이저가 필요 없으니 "레이저 스파게티" 문제가 사라진다. 모든 제어 회로가 반도체 칩 위에 집적되므로 일반 반도체 팹(fabrication facility, 반도체 제조 공장)에서 제조할 수 있고, 큐비트 밀도를 기존 1차원 선형 배열 대비 최대 300배까지 높일 수 있다.

아이온큐(IonQ)는 2025년 6월 Oxford Ionics를 10억 달러 규모에 인수하며 자사 로드맵의 핵심으로 흡수했다.

다만 EQC는 이온 트랩의 확장성 문제를 해결하는 기술이지, 게이트 속도를 빠르게 하는 기술이 아니다. 마이크로파로 제어한다는 점이 초전도 큐비트와 표면적으로 유사해 보이지만, 이온의 집단 진동 모드를 이용해 큐비트를 얽히게 만드는 물리적 메커니즘은 그대로다. 2큐비트 게이트 속도는 여전히 수십~수백 마이크로초 수준에 머문다.

(3) 속도가 아니라 오류율이 경계를 무너뜨린다

그렇다면 게이트 속도가 빨라지지 않는데, EQC가 Fast/Slow-Clock 경계를 어떻게 흔들 수 있을까? 답은 속도가 아닌 오류율에 있다.

Oxford Ionics는 현재 단일 큐비트 오류율 세계 기록을 보유하고 있다. 이온 트랩은 구조적으로 초전도 큐비트보다 오류율이 낮은데, EQC는 레이저 노이즈를 제거함으로써 이 장점을 더욱 극대화했다. 그 결과 물리 큐비트 대 논리 큐비트의 변환 비율이 극적으로 달라진다.

초전도 방식에서는 논리 큐비트(오류 정정이 완료된, 실제 연산에 사용 가능한 큐비트) 하나를 만들기 위해 물리 큐비트 500~1,000개가 필요하다. 하지만 아이온큐가 제시하는 EQC 기반 시스템에서는 이 비율이 약 13:1 수준까지 낮아질 수 있다. 오류율이 낮으면 오류 정정에 쏟아붓는 물리 큐비트 수가 줄어들고, 같은 논리 큐비트를 구현하는 데 필요한 전체 시스템 규모가 작아지기 때문이다.

이것이 T state 생산 문제와 연결된다. Slow-Clock의 T state 병목은 "같은 속도로 T state를 공급하려면 큐비트를 100배 더 투입해야 한다"는 것이었다. 그런데 물리:논리 큐비트 비율이 13:1이라면, 같은 논리 큐비트 수를 구현하는 데 필요한 전체 물리 큐비트 수 자체가 줄어들고, 상대적으로 T state 생산에 할당할 수 있는 여유가 생긴다. 게이트 하나하나는 느리지만, 알고리즘 전체를 완주하는 데 필요한 게이트 수 자체가 줄어드는 효과도 있다.

구글 논문도 이 가능성을 열어두고 있다. "새로운 magic state 생산 기법이 등장하면 Slow-Clock도 On-Spend 공격이 가능해질 수 있다"는 조건부 경고를 남겼는데, EQC 기반 시스템이 정확히 그 예외 케이스를 만들어가는 경로에 있다.

결론적으로 EQC를 탑재한 이온 트랩은 논문의 Fast/Slow-Clock 이분법으로 깔끔하게 분류되지 않는다. 게이트 속도는 여전히 느리지만, 오류율 우위가 시스템 전체의 효율을 높여 그 간극을 좁혀가는 경로다. **양자 위협 타임라인을 논할 때 Fast-Clock 계열만 주시하는 것으로는 충분하지 않다.**

표 7. Slow-Clock이 1차 거름망을 통과한다면?

	Fast-Clock	Slow-Clock 기존	개선된 Slow-Clock(EQC 가정)
오류 정정 사이클	~1 마이크로초	~100 마이크로초 이상	~100 마이크로초 이상
물리:논리 큐비트 비율	~500~1,000:1	~500:1 (추정)	**~13:1**
T state 생산용 큐비트	~25,000개 (전체의 5%)	~250만 개 (전체의 500%)	대폭 감소 (비율 개선 효과)
T state 생산 부담	가벼움	현실적으로 불가능	**가능성 ↑**
At-Rest 공격	가능	가능	가능
On-Spend 공격	**가능**	**불가능**	**조건부 가능성**
위협 시점	At-Rest와 On-Spend 동시	At-Rest가 먼저	At-Rest 우선, On-Spend 가능성 열림
Fast/Slow 분류	Fast-Clock	Slow-Clock	**경계 재정의 가능성**

자료: Google, 미래에셋증권 리서치센터

3. CRQC 타임라인과 데드라인

앞선 분석을 종합하면 하나의 질문으로 귀결된다. 그래서 데드라인은 언제일까?

(1) 아이온큐의 로드맵이 말하는 것

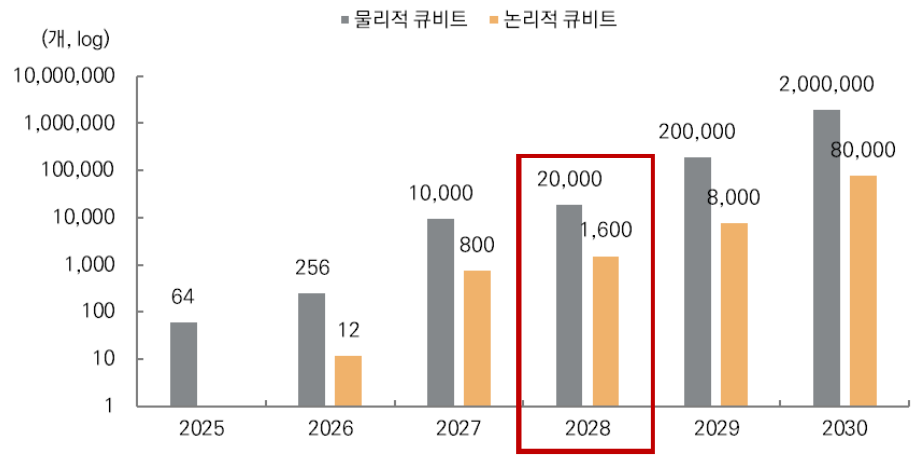
아이온큐는 2025년 6월 Oxford Ionics 인수를 반영해 로드맵을 대폭 업데이트했다.

표 8. 아이온큐의 양자컴퓨팅 로드맵

시점	물리 큐비트	논리 큐비트	주요 마일스톤
2025	~100	—	Tempo 개발자 시스템
2027	10,000+	~800	단일 칩, break-even 달성 목표
2028	20만 (2칩 연결)	~1,600	광자 네트워킹 개시
2030	200만+	4만~8만	멀티모듈 시스템

자료: IonQ, 미래에셋증권 리서치센터

그림 12. 아이온큐의 큐비트 로드맵



자료: IonQ, 미래에셋증권 리서치센터

2028년 수치에 주목해야 한다. 이번 논문이 제시한 ECDLP 해독 임계치는 논리 큐비트 1,200~1,450개다. **IonQ의 2028년 목표인 약 1,600개 논리 큐비트는 이 임계치를 넘어선다. 숫자만 놓고 보면 2028년에 CRQC 임계치를 통과한다는 계산이 나온다.**

물론 숫자가 충분해진다고 해서 곧바로 CRQC가 되는 것은 아니다. 두 가지 전제가 추가로 충족되어야 한다.

첫째, 오류율이다. IonQ는 2027년까지 논리 큐비트의 오류율이 물리 큐비트보다 낮아지는 "break-even(손익분기점)" 지점을 목표로 하고 있다. 이것이 달성되어야 오류 정정이 실질적으로 작동하는 fault-tolerant(내결함성) 연산이 가능해진다. 2030년까지 논리 오류율을 10^(-12)까지 줄이는 것이 최종 목표다.

둘째, 지속 가능한 연산 시간이다. ECDLP 해독은 수십 분에서 수 시간의 연속 연산이 필요하다. 현재 양자컴퓨터는 결맞음 시간(coherence time, 큐비트가 양자 상태를 유지하는 시간)이 연산 지속을 제한하는 요소로 작용한다. 이온 트랩은 초전도 대비 결맞음 시간이 길다는 장점이 있으나, 게이트 속도가 느려 서로 상쇄되는 부분이 있다.

한편 Fast-Clock 계열도 CRQC를 향해 독자적으로 진행 중이다. Google은 2024년 Willow 프로세서에서 오류 정정 임계값 이하의 오류율을 처음으로 달성했다. IBM은 2029년까지 100만 큐비트 시스템을 목표로 로드맵을 운영 중이다. Fast-Clock 계열이 충분한 규모에 도달하면 On-Spend와 At-Rest 위협이 동시에 현실화된다.

(2) 임계값 모델의 함의

양자컴퓨팅의 발전이 임계값(threshold) 모델의 형태를 따른다는 점도 주의해야 한다. 큐비트 수가 선형적으로 증가하면서 능력이 점진적으로 향상되는 구조가 아니라, 특정 기술적 장벽을 돌파하는 순간 불연속적으로 도약하는 구조다.

이는 "32비트 ECDLP 공개 데모 성공"과 "256비트 ECDLP 실제 해독" 사이의 시간이 거의 없을 수 있다는 점을 의미한다. 업계가 스케일링 장벽을 돌파하기 전까지 경고 신호가 없다가, 돌파하는 순간 곧바로 CRQC 수준에 도달할 수 있다.

논문은 여기서 한 걸음 더 나아간다. 상업화에 가까워질수록 연구 투명성이 낮아질 것을 경고한다. CRQC가 달성된 경우 학술적 공개가 아니라 기밀 프로그램의 형태로 먼저 구축될 가능성을 배제할 수 없으며, 그 경우 최초 CRQC의 존재는 학술 발표가 아닌 온체인 이상 거래로 처음 감지될 수 있다는 것이다. 따라서, 현재 공개된 로드맵과 기술 발전 방향을 종합하면 주요 분기점은 약 2~3년 뒤로 다가온다.

표 9. 분기점 도래까지 약 2~3년

시점	시나리오	위협 유형	비고
2027	Slow-Clock break-even 달성	At-Rest 위협 가시화	IonQ 로드맵 기준
2028	Slow-Clock ECDLP 임계치 도달 가능	At-Rest 공격 현실화	논리 큐비트 수 충족
2028~2030	Fast-Clock At-Rest 임계치 도달 가능	At-Rest + On-Spend 동시 위협	초전도 계열
2030~	EQC 기반 Slow-Clock On-Spend 가능성	전방위 위협	오류율 개선 속도에 의존

자료: 미래에셋증권 리서치센터

(3) 커뮤니티의 딜레마 — 합의 없는 시계

사토시 코인을 포함한 약 230만 BTC의 휴면 자산은 CRQC 등장 시 사실상 선착순으로 탈취 가능한 자산이 된다. 이에 대해 비트코인 커뮤니티는 세 가지 대응을 논의 중이다.

- Do Nothing(아무것도 하지 않기): 프로토콜을 그대로 유지한다. "양자컴퓨터가 공개키에서 개인키를 추출하는 것은 정당한 소유권 행사"라는 극단적 자유주의 해석에 기반한다.

- Burn(소각): 특정 시점 이후 P2PK 등 취약 주소의 자산을 사용 불가로 처리한다. 사토시의 코인을 포함해 수십억 달러의 자산이 영구적으로 소각된다는 윤리적 쟁점이 있다.

- Hourglass(모래시계): 취약 주소에서의 지출 속도를 제한한다. 한 번에 전액을 인출할 수 없게 만들어 탈취의 경제적 인센티브를 낮추는 방식이다.

2025년 Presidio Bitcoin Quantum Summit에서 세 방안에 대한 지지는 거의 동등하게 "분산"되었다. 커뮤니티 합의 전망이 불투명하다는 의미다. 비트코인의 leaderless 거버넌스 구조에서 이 수준의 프로토콜 변경을 합의하는 것은 구조적으로 어려워 보인다. **시간은 흐르고, 합의는 멀다.**

Compliance Notice

- 당사는 자료 작성일 현재 조사분석 대상법인과 관련하여 특별한 이해관계가 없음을 확인합니다.
- 당사는 본 자료를 제3자에게 사전 제공한 사실이 없습니다.
- 본 자료를 작성한 애널리스트 김은지은(는) 자료작성일 현재 알파벳 40주 보유하고 있습니다.
- 본 자료는 외부의 부당한 압력이나 간섭없이 애널리스트의 의견이 정확하게 반영되었음을 확인합니다.

본 조사분석자료는 당사의 리서치센터가 신뢰할 수 있는 자료 및 정보로부터 얻은 것이나, 당사가 그 정확성이나 완전성을 보장할 수 없으므로 투자자 자신의 판단과 책임하에 종목 선택이나 투자시기에 대한 최종 결정을 하시기 바랍니다. 따라서 본 조사분석자료는 어떠한 경우에도 고객의 증권투자 결과에 대한 법적 책임소재의 증빙자료로 사용될 수 없습니다. 본 조사분석자료의 지적재산권은 당사에 있으므로 당사의 허락 없이 무단 복제 및 배포할 수 없습니다.