비트코인은 양자컴퓨팅 시대에도 살아남을 수 있는가

양자 위협과 비트코인 보안의 진화

About

Metanomia는 크립토 시장과 기술의 변화를 연구·분석하는 싱크탱크입니다.

Researchers

김연경 *Yonkyung Kim*

손혜민 *Hyemin Son*

Corresponding Author

오태민 *Taemin Oh*

Contents

들어가며

비트코인은 해킹당한 적이 있는가. 뉴스 헤드라인만 보면 그렇다고 믿기 쉽다. 2013년 CNBC는 시장 과열 이후 마운트곡스(Mt. Gox)의 보안 사고로 가격이 흔들리던 국면을 전하면서 기사 제목을 아예 '비트코인이 해킹당했다(Bitcoin Hacked)'라고 붙였다.[1] 제목만 읽으면 비트코인이라는 프로토콜 자체가 뚫린 것처럼 보인다. 그때의 사건이 단발적 보안 사고였다면, 2014년의 마운트곡스 사태는 붕괴에 가까웠다. 당시 세계 최대 비트코인 거래소였던 마운트곡스에서 고객 자산을 포함해 약 85만 개의 비트코인이 사라졌다.[2] 당시 금액으로 약 4.8억 달러, 전체 유통량의 약 7%에 해당하는 물량이었다. 많은 보도는 이를 '거래소의 파산' 혹은 '거래소 해킹'으로 전했지만, 대중에게는 '비트코인 해킹'으로 압축되어 각인됐다. 2016년에는 또 다른 대형 거래소 비트파이넥스(Bitfinex)에서도 약 12만 개의 비트코인이 탈취되며 같은 프레임이 반복됐다.[3]

그러나 이 사건들에서 뚫린 것은 비트코인 네트워크가 아니라 거래소의 서버였다. 거래소는 사용자들의 비트코인을 중앙화된 서버에 모아 보관하는 사기업이다. 비유하자면, 금고 안에 여러 사람의 금을 모아둔 보관소가 도둑을 맞은 것이지 금이라는 금속의 속성 자체가 깨진 것이 아니다. 해커가 공격한 것은 기업의 보안 체계, 즉 서버 관리와 내부 통제의 허점이었지 비트코인의 암호학적 구조가 아니었다.

비트코인 네트워크 자체는 2009년 1월 3일 출범 이래 단 한 번도 해킹당한 적이 없다.[4] 이것이 의미하는 바를 곱씹어볼 필요가 있다. 비트코인 네트워크는 16년 넘게 매 10분마다 쉬지 않고 블록을 생성해 왔다. 그 위에 쌓인 자산의 가치는 시가총액 기준 (2026년 5월) 약 1.6조 달러에 이른다. 이 네트워크의 암호를 깨뜨릴 수 있는 자에게는 엄청난 규모의 현상금이 걸린 것이나 다름없다. 전 세계의 해커, 연구 기관, 심지어 국가 수준의 행위자에 이르기까지 수많은 공격의 유인이 존재했지만, 이 시스템은 단 한 번의 침해도 허용하지 않았다.

그런데 이 견고함에 유효기간은 없는가. 이 질문이 유효한 이유는 비트코인의 방어선이 모두 하나의 전제 위에 서 있기 때문이다. 비트코인의 보안을 떠받치는 수학 자체가 깨지지 않는다는 전제다. 만약 그 수학이 깨진다면, 16년의 무결점 기록은 아무런 보증이 되지 못한다.

이 리포트는 그 전제를 양자컴퓨팅(quantum computing)이라는 새로운 기술의 등장과 함께 검토한다. 양자컴퓨터가 비트코인의 암호 체계에 어떤 위협을 가하는지, 그 위협은 얼마나 현실에 가까운지, 그리고 비트코인 커뮤니티는 어떤 방식으로 대비하고 있는지를 차례로 살핀다.

결론부터 말하면, 양자컴퓨터는 비트코인만의 문제가 아니라 현대 디지털 문명 전체의 문제이며, 비트코인은 이 도전에 대응할 수 있는 구조적 경로를 이미 갖추고 있다.

01

비트코인 보안의 두 기둥

비트코인은 중앙 기관 없이도 거래가 성립하는 분산형 전자 화폐 시스템이다. 은행이나 등기소처럼 신원을 확인하고 장부를 관리하는 단일 주체가 존재하지 않음에도, 네트워크는 특정 미사용 거래 출력(Unspent Transaction Output, UTXO)[1]이 정당한 조건을 만족할 때만 이동하도록 강제한다. 여기서 정당하다는 것은 소유자의 신원이 확인되었다는 뜻이 아니라, 해당 자산을 잠근 조건을 해제할 수 있는 개인키의 통제권이 암호학적으로 증명되었다는 뜻이다.

비트코인의 보안은 두 가지 수학적 구조에 의존한다. 첫째는 '타원곡선 암호(Elliptic Curve Cryptography, ECC)'로, 개인키로 생성한 전자서명이 공개키로 검증되는 구조를 통해 자산의 통제권, 즉 소유권에 해당하는 경제적 권한을 보호한다. 둘째는 'SHA-256 해시(hash) 함수'로, 채굴과 블록 간 연결에 사용되어 합의의 비용 구조와 기록의 무결성을 지탱한다. 이 두 기둥이 결합되어 비트코인은 은행 없는 소유 증명과 사실상 변조 불가능한 기록을 동시에 달성한다.

1)

UTXO(Unspent Transaction Output)는 아직 소비되지 않은 거래 출력값을 의미한다. 비트코인은 계좌 잔액을 기록하는 방식이 아니라, 이전 거래의 출력이 다음 거래의 입력으로 사용되는 구조를 가지며, 사용되지 않은 출력들의 집합이 사용자의 비트코인 잔액을 구성한다.

열쇠와 자물쇠

전통 금융에서 소유는 제3자의 확인과 기록에 의존한다. 예금은 은행 장부, 부동산은 등기, 주식은 예탁·계좌 기록이 최종 기준이 된다. '누가 소유자인가'에 대한 판단 권한이 특정 기관에 집중되어 있는 것이다. 반면 비트코인은 기관의 신원 확인이나 인감·서류 절차 없이도 거래가 성립한다. 비트코인이라는 자산의 통제권을 사람의 신분이 아니라 암호학적 증명으로 확립하기 때문이다. 네트워크가 확인하는 것은 '이 사람이 누구인가'가 아니라 '개인키로 유효한 서명을 만들 수 있는가'이다.

비트코인의 소유 체계는 공개키 암호학(public-key cryptography)이라는 수학적 원리에 기반한다. 사용자는 먼저 개인키(private key)를 정하고, 이로부터 공개키(public key)를 파생한다. 이 관계는 흔히 열쇠와 자물쇠에 비유된다. 개인키는 오직 소유자만 접근하는 열쇠다. 이 열쇠는 256비트(bit) 길이의 수이며, 가능한 조합의 수는 대략 2^{256}, 즉 약 1.15×10^{77}개에 이른다.[5] 이는 관측 가능한 우주에 존재하는 모든 원자의 수 추정치와 견줄 만큼 큰 수다. 경우의 수가 이처럼 거대하다는 것은 무작위 추측으로 타인의 개인키를 맞히는 시도가 현실적으로 불가능함을 의미한다. 공개키는 이 개인키로부터 수학적으로 파생된 값으로, 자물쇠에 해당한다. 누구나 이 자물쇠를 볼 수 있지만, 그것만으로는 잠금을 해제할 수 없다.

비트코인을 전송하려면 개인키로 전자서명(digital signature)을 생성해야 한다. 전자서명은 '해당 잠금 조건을 해제할 권한', 즉 '개인키를 내가 통제하고 있으며 이 거래 내용을 승인한다'는 사실을 수학적으로 증명하는 데이터다. 네트워크의 참여

자들은 공개키를 사용해 그 서명이 올바른지 확인한다. 이 구조가 작동하는 이유는 개인키와 공개키 사이에 비대칭성이 존재하기 때문이다. 개인키로부터 공개키를 계산하는 것은 쉽지만, 공개키로부터 개인키를 역산하는 것은 현재의 컴퓨터로는 사실상 불가능하다. 바로 이 비대칭성이 비트코인 전자서명의 보안을 떠받치는 핵심 전제다.

첫 번째 기둥: 타원곡선 암호

개인키에서 공개키를 계산하는 것은 쉽지만 그 역은 사실상 불가능하다는 성질은, 구체적으로 '타원곡선 암호'라는 수학적 체계 위에서 구현된다. 비트코인은 초기부터 secp256k1이라는 특정 타원곡선 위에서 작동하는 '타원곡선 디지털 서명 알고리즘(Elliptic Curve Digital Signature Algorithm, ECDSA)'을 사용해 왔다.[6] secp256k1 타원곡선에는 기준점(generator point)이라 불리는 고정된 점이 정해져 있다. 비트코인에서는 이 기준점에 개인키라는 숫자를 적용해 공개키를 만든다. 수학적으로는 기준점에 타원곡선 위의 덧셈 규칙을 개인키 값만큼 반복 적용한 결과이며, 그렇게 도달한 곡선 위의 점이 공개키가 된다. 이 계산은 매우 빠르게 수행된다. 그러나 도착점인 공개키만 보고 몇 번의 연산이 적용되었는지, 즉 개인키가 무엇인지를 역산하는 것은 현재의 고전 컴퓨터로는 사실상 불가능하다. 이 문제를 '타원곡선 이산로그 문제(Elliptic Curve Discrete Logarithm Problem, ECDLP)'라고 부른다. ECDLP의 계산적 난이도가 유지되는 한, 공개키가 드러난 경우에도 공격자가 개인키를 복원하거나 유효한 서명을 위조하는 것은 사실상 불가능하다. 이것이 비트코인의 통제권 보호를 떠받치는 첫 번째 수학적 기둥이다.

[표 1] **비트코인에서 ECC가 사용되는 방식**

적용 영역	기반 기술	기능
공개키 생성	secp256k1 타원곡선 연산	개인키로부터 공개키 생성
거래 서명	ECDSA / 슈노르(Schnorr)	통제권 증명 및 거래 승인

두 번째 기둥: SHA-256

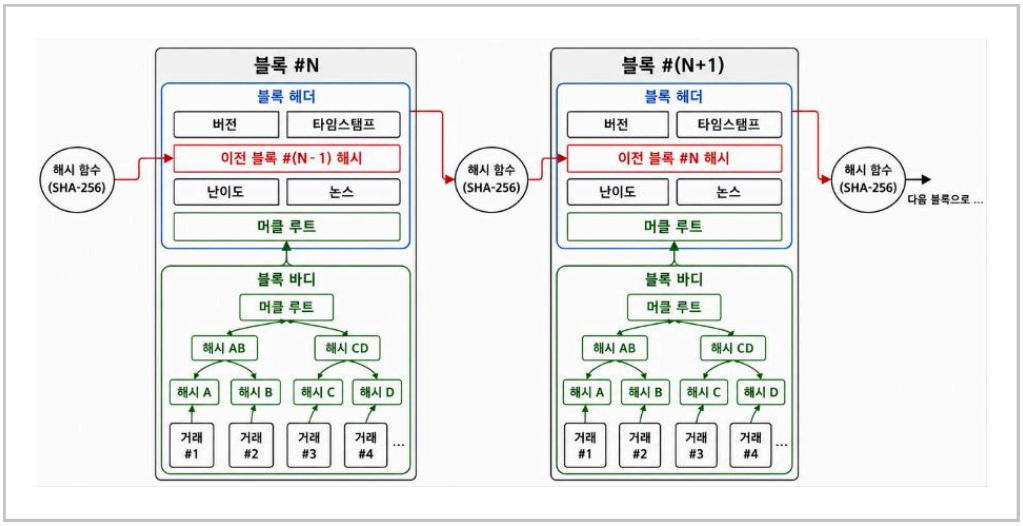
비트코인 보안의 두 번째 기둥은 'SHA-256 해시 함수'다. 해시 함수는 임의 길이의 데이터를 입력받아 고정된 길이의 해시 값을 출력하는 일방향 함수다. 같은 입력에는 항상 같은 출력이 나오지만, 입력이 아주 조금만 바뀌어도 전혀 다른 해시 값이 생성된다. 예를 들어 'Hello'와 'Hello.'는 마침표 하나 차이밖에 나지 않지만, 결과로 나오는 해시 값은 완전히 달라진다. 이런 성질 때문에 해시는 원본 데이터의 변조 여부를 검증하는 데 널리 사용된다.

비트코인에서 SHA-256은 두 가지 핵심 역할을 수행한다. 첫째, 작업증명(Proof of Work, PoW)의 기반이 된다. 비트코인에서는 특정 주체의 승인이나 권위가 아니라, 난이도 조건을 만족하는 해시 값을 찾아내는 계산 경쟁을 통해 다음 블록을

생성할 주체가 결정된다. 채굴자는 블록에 담긴 거래 내역과 여러 정보를 하나로 묶은 뒤, 그 안에서 조정 가능한 값들, 대표적으로 논스(nonce)라는 임의의 숫자를 바꾸어 가며 네트워크가 요구하는 난이도 조건을 만족하는 해시 값을 찾는다. 이 과정은 정답을 논리적으로 추론하는 계산이라기보다, 조건에 맞는 값이 나올 때까지 반복적으로 시도하는 무작위 탐색에 가깝다. 따라서 성공 확률을 높이는 사실상 유일한 방법은 더 많은 해시 계산을 수행하는 것이다. 이 구조 덕분에 블록 생성에는 현실적인 전력과 장비 비용이 수반되며, 어떤 블록이 정당한 블록으로 받아들여질지는 결국 실제로 투입된 계산 비용에 의해 좌우된다.

둘째, SHA-256은 기록의 무결성을 지탱한다. 블록체인에서 각 블록은 이전 블록의 해시를 포함함으로써 연쇄적으로 이어진다. 따라서 과거 블록의 내용이 단 1비트라도 바뀌면 그 블록의 해시가 달라지고, 그 값을 참조하는 이후 블록들과의 연결도 함께 깨진다. 과거의 한 블록을 조작한다는 것은 사실상 그 뒤에 이어지는 모든 블록들을 다시 만들어야 한다는 뜻이다. 그런데 비트코인에서 이는 단순히 데이터를 다시 정리하는 수준의 문제가 아니다. 공격자는 변경된 블록들에 대해 작업증명을 다시 수행해야 하고, 동시에 그 사이에도 계속 연장되고 있는 정직한 체인의 누적 계산량까지 따라잡아야 한다. 결국 과거 기록을 뒤집으려면 천문학적인 연산 비용과 시간의 투입이 필요하다. 비트코인의 기록이 사실상 변조 불가능한 이유가 여기에 있다.

바로 이 점에서 SHA-256은 비트코인 보안의 두 번째 수학적 기둥이 된다. 타원곡선 암호가 자산을 움직일 수 있는 정당한 통제권을 가려낸다면, SHA-256은 어떤 기록이 정당한 역사로 남을지를 결정한다. 하나는 통제권을, 다른 하나는 기록의 연속성과 비용 구조를 떠받친다. 비트코인의 보안은 이 두 기둥이 함께 서 있을 때에만 성립한다.



[그림 1] **이전 블록 해시에 의한 블록 연결 구조**

각 블록의 헤더는 SHA-256 기반 해시 함수의 입력이 되며, 그 결과값은 다음 블록 헤더의 '이전 블록 해시' 항목에 저장된다. 블록 바디의 거래 내역은 머클 트리(Merkle Tree)를 통해 하나의 머클 루트(Merkle Root)로 요약되고, 이 값 역시 블록 헤더에 포함된다. 따라서 거래 내역이나 블록 헤더의 항목이 바뀌면 해당 블록의 해시가 달라지고, 이후 블록들의 연결 관계도 연쇄적으로 영향을 받는다.

02

양자컴퓨터가 겨냥하는 것

앞서 살펴본 비트코인의 두 수학적 기둥은 공개키에서 개인키를 역산하는 것이, 그리고 작업증명의 비용 구조를 무력화할 만큼 해시 탐색을 가속하는 것이 어렵다는 전제 위에 서 있다. 그러나 1980년대에 태동한 양자컴퓨팅[2] 연구는 1990년대 중반 쇼어 알고리즘(Shor's Algorithm)의 등장과 함께 이 전제를 근본적으로 흔들 수 있는 가능성을 드러냈다.[7] 양자컴퓨터가 특정 수학 문제를 기존 컴퓨터와는 비교할 수 없는 속도로 해결할 수 있다는 사실이 밝혀지면서, 비트코인을 포함한 현대 암호학 전체가 새로운 위협 환경에 놓이게 된 것이다.

기존 컴퓨터와 양자컴퓨터의 차이

우리가 일상적으로 사용하는 컴퓨터는 비트라는 단위로 정보를 처리한다. 비트는 0 또는 1이라는 두 가지 상태 중 하나만 가질 수 있으며, 모든 계산은 이러한 이진 상태(binary state)의 조합으로 이루어진다. 반면 양자컴퓨터의 기본 단위는 '큐비트(qubit)'다. 큐비트는 측정되기 전까지 0과 1 가운데 하나로 확정되지 않은 채, 두 상태의 조합으로 존재할 수 있다. 이를 '중첩(superposition)'이라 한다. 일반 비트가 동전의 앞면이나 뒷면 중 하나라면, 큐비트는 동전이 공중에서 회전하고 있는 상태에 가깝다. 다만 회전하는 동전은 결과가 이미 정해져 있으나 아직 드러나지 않은 것일 뿐인 반면, 큐비트의 중첩은 측정 전까지 두 상태의 조합으로 기술되는 양자 상태라는 점에서 다르다.

양자 시스템에는 '얽힘(entanglement)'이라는 현상도 존재한다. 얽힘이란 두 개 이상의 큐비트가 하나의 결합된 양자 상태를 이루어, 어느 한쪽의 상태를 나머지와 독립적으로 기술할 수 없게 되는 현상이다. 이 상태에서는 한쪽 큐비트를 측정했을 때 다른 쪽의 측정 결과와 강한 상관관계가 나타나며, 두 큐비트가 물리적으로 떨어져 있더라도 이 상관관계는 유지된다. 중첩이 개별 큐비트의 상태를 설명하는 개념이라면, 얽힘은 여러 큐비트가 서로 분리되지 않는 하나의 결합 상태를 이루는 현상을 설명하는 개념이다.

중첩과 얽힘이 결합될 때, 양자컴퓨터는 기존 컴퓨터, 즉 고전 컴퓨터(classical computer)와 근본적으로 다른 방식으로 계산을 수행한다. 고전 컴퓨터의 병렬 계산은 여러 개의 프로세서가 서로 다른 작업을 동시에 나누어 처리하는 방식이다. 반면 양자컴퓨터는 큐비트들이 중첩과 얽힘을 통해 여러 계산 경로의 가능성을 포함한 하나의 양자 상태를 이루도록 만든 뒤, 그 상태에 양자 연산을 적용한다. 이후 계산 과정에서 서로 다른 양자 상태들이 서로를 강화하거나 상쇄하는 '간섭(interference)'이 일어나는데, 양자 알고리즘은 이를 이용해 정답에 해당하는 결

2)

양자 컴퓨팅(quantum computing)은 양자역학의 원리를 이용해 계산을 수행하는 컴퓨터 모델이다. 1980년대 초 리처드 파인만(Richard Feynman)이 양자계를 효율적으로 모사할 계산 장치의 필요성을 제기했고, 이어 데이비드 도이치(David Deutsch)는 1985년 보편적 양자컴퓨터의 이론적 모델을 형식화했다. 이후 다양한 양자 알고리즘이 제안되면서 이 분야는 독자적인 계산 패러다임으로 발전해 왔다.

과의 확률은 높이고 원하지 않는 결과의 확률은 낮춘다. 이러한 구조 덕분에 특정 문제에서는 고전 컴퓨터보다 훨씬 적은 연산 단계로 해답에 도달할 수 있다.

물론 양자컴퓨터가 모든 문제에서 고전 컴퓨터보다 빠른 것은 아니다. 양자 계산이 압도적 우위를 보이는 영역은 특정한 수학적 문제 유형에 한정된다. 핵심은 현대 암호학의 기반이 되는 여러 문제가 바로 이 범주에 속한다는 점이다. 특히 소인수분해와 이산로그 문제는 양자 알고리즘에 의해 효율적으로 해결될 수 있는 것으로 알려져 있다.

[그림 2] **고전 컴퓨터의 병렬 처리와 양자컴퓨터의 중첩 상태 연산**
여러 개의 프로세서를 사용해 서로 다른 작업을 나누어 처리하는 고전적 병렬 계산과 달리, 양자컴퓨터는 여러 가능성을 포함한 하나의 중첩 상태에 양자 연산을 적용한다. 이후 계산 과정에서 양자 상태들 사이의 간섭을 이용해 원하는 결과가 측정될 확률을 높이고, 원하지 않는 결과의 확률을 낮춘다. 본 그림은 이러한 계산 방식의 차이를 단순화해 개념적으로 나타낸 것이다.

쇼어 알고리즘과 그로버 알고리즘

양자컴퓨터가 비트코인에 가하는 위협은 크게 두 방향으로 나뉜다. 하나는 타원곡선 암호를 겨냥하는 쇼어 알고리즘이고, 다른 하나는 해시 탐색을 가속하는 그로버 알고리즘(Grover's Algorithm)이다. 두 알고리즘 모두 비트코인의 암호학적 기반에 영향을 주지만, 그 위협의 성격은 서로 다르다. 쇼어 알고리즘이 비트코인의 통제권 구조를 직접 겨냥한다면, 그로버 알고리즘은 작업증명과 해시 탐색의 비용 구조를 약화시키는 쪽에 가깝다.

1994년 피터 쇼어(Peter Shor)가 제안한 쇼어 알고리즘은 충분히 큰 오류 정정 양자컴퓨터가 존재할 경우 이산로그 문제와 정수 소인수분해 문제를 고전 컴퓨터보다 훨씬 효율적으로 풀 수 있음을 보여주었다.[8] 비트코인의 전자서명 체계는 secp256k1 타원곡선 위의 이산로그 문제에 기반한다. 다시 말해 개인키에서 공개키를 계산하는 것은 쉽지만 공개키에서 개인키를 역산하는 것은 어렵다는 전제 위에 서 있다. 그런데 쇼어 알고리즘을 실행할 수 있는 양자컴퓨터가 등장한다면 이 전제가 흔들린다. 공개키로부터 개인키를 계산하는 일이 이론적으로 가능해지기 때

문이다.

이는 자물쇠만 보고도 그에 맞는 열쇠를 만들어내는 기술이 등장하는 것에 비유할 수 있다. 비트코인에서 자산을 움직일 수 있는 통제권은 개인키를 알고 있다는 사실에 의해 증명된다. 그런데 공개키에서 개인키를 계산할 수 있게 된다면, 공개키가 이미 노출된 주소의 자산은 공격자가 정당한 소유자처럼 이동시킬 수 있는 위험에 놓이게 된다. 이 점에서 쇼어 알고리즘은 비트코인의 첫 번째 기둥, 즉 타원곡선 암호에 기반한 통제권 보호 구조를 직접 겨냥한다.

반면, 1996년 러브 그로버(Lov Grover)가 제안한 그로버 알고리즘은 해시 함수에 대해 다른 방식의 위협을 가한다. 그로버 알고리즘은 무차별 대입 탐색에 필요한 시도 횟수를 제곱근 수준으로 줄이는 양자 알고리즘이다.[9] 어떤 조건을 만족하는 값을 찾기 위해 가능한 후보를 하나씩 시험해야 하는 경우, 고전 컴퓨터로 N번의 시도가 필요하다면 그로버 알고리즘으로는 필요한 시도 횟수가 대략 √N 수준으로 줄어든다.

이를 SHA-256에 적용하면 256비트 보안 강도가 대략 128비트 수준으로 낮아지는 효과가 발생한다. 이는 분명 상당한 약화다. 그러나 128비트 보안 역시 여전히 매우 높은 수준이다. 2의 128제곱은 약 3.4×10^{38}에 해당하는 거대한 수이며, 현존하는 계산 자원으로는 현실적으로 탐색하기 어려운 규모다. SHA-256에 대한 양자 위협은 해시 함수의 즉각적 붕괴라기보다 계산 난이도의 감소에 가깝다.

결국 양자컴퓨터가 비트코인에 가하는 위협은 두 기둥에 동일한 방식으로 작용하지 않는다. SHA-256은 그로버 알고리즘에 의해 탐색 난이도가 낮아질 뿐, 그 자체가 즉각적으로 붕괴되는 구조는 아니다. 반면 타원곡선 암호는 쇼어 알고리즘의 직접적인 공격 대상이 되며, 충분히 강력한 양자컴퓨터가 등장할 경우 공개키에서 개인키를 역산할 수 있다는, 더 직접적이고 근본적인 위협을 받는다. 따라서 양자 위협의 핵심은 공개키가 노출된 코인의 통제권이 위협받을 수 있다는 점에 있다. 다만 이것은 어디까지나 이론적 가능성이다. 실제로 이러한 공격이 가능하려면 쇼어 알고리즘을 실행할 수 있는 대규모 오류 정정 양자컴퓨터가 필요하다. 이제 살펴봐야 할 질문은, 이 위협이 실제로 얼마나 가까이 와 있는가다.

[표 2] **쇼어 알고리즘과 그로버 알고리즘 비교**

구분	쇼어 알고리즘	그로버 알고리즘
공격 대상	타원곡선 암호 (ECC)	해시 함수 (SHA-256)
공격 효과	공개키→개인키 역산 (근본적 무력화)	보안 강도 256비트→128비트 (부분적 약화)
비유	자물쇠를 보고 열쇠를 복제	금고 비밀번호 시도 속도 향상
위협 긴급도	높음	상대적으로 낮음

03

양자 위협과 이미 시작된 방어

양자컴퓨터의 진전과 아직 남은 거리

양자컴퓨터가 장기적으로 비트코인의 암호 체계에 위협이 될 수 있다는 전망은 더 이상 공상과학의 영역에만 머물러 있지 않다. 최근 몇 년 사이 주요 기술 기업들은 양자컴퓨터의 규모와 오류 정정 가능성을 보여주는 성과를 잇달아 발표했다. IBM은 2023년 1,121큐비트 규모의 양자 프로세서 콘도르(Condor)를 공개하며 1,000큐비트 장벽을 넘었다.[10] 이후 IBM은 2025년 갱신된 로드맵에서, 2029년까지 200개의 논리 큐비트와 1억 개 규모의 양자 게이트 연산을 수행할 수 있는 스타링(Starling) 시스템을 목표로 제시했다.[11] 구글은 2024년 12월, 105개 큐비트를 갖춘 양자 칩 윌로우(Willow)를 발표했다.[12] 마이크로소프트 역시 2025년 2월에 마요라나 1(Majorana 1) 칩을 발표하며, 장기적으로 단일 칩에서 100만 큐비트 규모까지 확장할 수 있는 경로를 제시했다고 밝혔다.[13]

[표 3] **주요 양자컴퓨팅 아키텍처 비교**

항목	Condor	Willow	Majorana 1
개발 기관	IBM	Google	Microsoft
공개 연도	2023	2024	2025
큐비트 규모	1,121큐비트	105큐비트	8개 큐비트 실험 칩, 100만 큐비트 확장 목표
기술 방식	초전도 큐비트 기반	초전도 큐비트 기반	위상학적 큐비트 기반
핵심 의미	1,000큐비트 장벽을 넘은 대형 프로세서	오류 정정과 논리 큐비트 안정성에서 진전	오류에 강한 새로운 큐비트 구조 제시
현재 한계	큐비트 수는 크지만 오류 허용 양자컴퓨터는 아님	뛰어난 벤치마크 성과가 곧 암호 해독 능력은 아님	현재 8큐비트 규모로, 대규모 확장은 장기 검증 과제

이 가운데 구글의 윌로우는 최근 양자컴퓨터 발전의 의미를 설명하기에 좋은 사례다. 구글에 따르면 윌로우는 기존 컴퓨터로 약 10^{25}년이 걸릴 것으로 추정되는 계산을 단 5분 만에 수행했다. 그러나 윌로우의 의미는 단순히 계산 속도에만 있지 않았다. 더 중요한 성과는 오류 정정 실험에서 큐비트 수를 늘릴수록 오류율이 낮아지는 이른바 '임계값 이하(below threshold)' 현상을 보였다는 점이다. 이는 더 많은 큐비트를 추가할수록 오류가 누적되기만 하는 것이 아니라, 적절한 오류 정정 구조 안에서는 논리 큐비트의 안정성이 오히려 개선될 수 있음을 보여준 사례였다.

그러나 이러한 성과가 곧바로 암호 해독 능력을 의미하는 것은 아니다. 윌로우가 풀었던 문제는 양자컴퓨터의 성능을 측정하기 위해 설계된 벤치마크 문제였다. 구글 역시 발표 이후 인터뷰에서 이 점을 분명히 했다. 구글 대변인은 "현재 추정으로는 RSA[3]를 깨뜨리기까지 적어도 10년은 더 걸릴 것이며, 이를 위해서는 약 400만 개의 물리 큐비트(physical qubit)[4]가 필요할 것으로 보인다"고 말했다.[14] 따라서 윌로우의 성과는 양자컴퓨터의 가능성을 보여주는 중요한 진전이지만, 그것은 아직 암호 체계를 해독할 수 있는 실용적 능력과는 거리가 있다.

비트코인의 경우, 암호 해독에 필요한 양자컴퓨터의 규모는 매우 크다. 연구자들은 비트코인이 사용하는 타원곡선 서명 체계를 공격하기 위해서는 수백만에서 수천만 개 수준의 물리 큐비트가 필요할 것으로 추정한다. 서섹스대학교 연구팀은 특정 오류 정정 방식과 하드웨어 가정을 바탕으로 한 자원 추정에서, 비트코인의 secp256k1 기반 타원곡선 서명 체계를 하루 안에 공격하기 위해서는 약 1,300만 개 규모의 물리 큐비트가 필요할 수 있다고 분석했다.[15] 구글의 윌로우 칩이 105개의 물리 큐비트 규모라는 점을 고려하면, 필요한 수준과의 차이는 약 12만 배에 이른다. 이 격차는 현재 양자컴퓨터 기술 수준과 실용적 암호 공격 사이에 아직 상당한 거리가 있음을 보여준다.

암호 해독에 필요한 큐비트 수가 이렇게 커지는 이유를 이해하려면 양자컴퓨터의 오류율(error rate) 문제를 함께 보아야 한다. 큐비트는 매우 민감한 양자 상태에 의존하기 때문에 외부 환경의 작은 간섭에도 쉽게 오류가 발생한다. 따라서 실제 계산을 수행하려면 오류 정정을 위한 많은 추가 물리 큐비트가 필요하다. 이 때문에 양자컴퓨터 연구에서는 하드웨어에 실제로 구현된 물리 큐비트와 오류 정정을 통해 안정적인 계산 단위로 구성되는 논리 큐비트(logical qubit)를 구분한다. 하나의 안정적인 논리 큐비트를 구현하려면 오류 정정 방식과 오류율에 따라 수백 개에서 수천 개의 물리 큐비트가 필요할 수 있다. 서섹스대학교 연구팀이 제시한 '1,300만 큐비트'라는 추정치 역시 논리 큐비트가 아니라 오류 정정을 포함한 물리 큐비트 규모를 가리킨다. 나아가 이를 실제 장치로 구현하려면 큐비트 자체뿐 아니라 제어, 측정, 냉각, 배선 등 막대한 하드웨어 인프라가 함께 필요하다.

이러한 기술적 한계 때문에 현재의 양자컴퓨터는 흔히 'NISQ(Noisy Intermediate-Scale Quantum)' 단계에 있는 것으로 설명된다. 이 용어는 물리학자 존 프레스킬(John Preskill)이 제안한 개념으로, 50개에서 수백 개 수준의 큐비트를 가진 잡음 많은 초기 단계의 양자컴퓨터를 의미한다.[16] NISQ 장치는 양자 중첩과 얽힘 같은 현상을 실제로 구현할 수 있지만, 동시에 노이즈와 오류가 많아 장기간 안정적인 계산을 수행하기 어렵다. 따라서 현재의 양자컴퓨터는 특정 실험적 문제나 제한된 최적화 계산에서는 의미 있는 성과를 보여주지만, 비트코인의 암호 체계를 깨는 것과 같은 대규모 계산을 수행하기에는 아직 기술적으로 부족한 단계에 있다.

그러나 이것이 양자 위협을 무시해도 된다는 뜻은 아니다. 중요한 것은 양자컴퓨터가 당장 비트코인을 깨뜨릴 수 있느냐가 아니라, 그 위협이 현실화되는 시점을 정확히 예측하기 어렵다는 데 있다. 양자컴퓨터 연구는 빠르게 진행되고 있고, 오류 정정과 하드웨어 확장성의 문제도 점진적으로 개선되고 있다. 결국 양자 위협은 당장의 붕괴가 아니라 시간표의 문제다.

3)

RSA는 1977년 로널드 리베스트(Ronald Rivest), 아디 샤미르(Adi Shamir), 레너드 애들먼(Leonard Adleman)이 제안한 대표적인 공개키 암호 방식이다. 이 방식은 두 개의 큰 소수 p와 q를 곱해 만든 큰 합성수 n에서 다시 원래의 소수 p와 q를 찾아내는 소인수분해가 매우 어렵다는 점에 보안의 기초를 둔다. 그러나 충분히 큰 오류 정정 양자컴퓨터가 등장하면 쇼어 알고리즘을 통해 이 문제를 효율적으로 풀 수 있다. 이 때문에 RSA는 비트코인이 직접 사용하는 서명 체계는 아니지만, 양자컴퓨터의 암호 위협을 설명할 때 대표적인 사례로 자주 언급된다.

4)

물리 큐비트(physical qubit)는 실제 하드웨어에 구현된 개별 큐비트를 의미한다. 이에 비해 논리 큐비트(logical qubit)는 여러 물리 큐비트를 오류 정정 방식으로 결합해, 계산 과정에서 발생하는 오류를 감지하고 보정할 수 있도록 만든 안정적인 계산 단위다.

비트코인이 장기적으로 글로벌 금융 인프라로 남으려면 양자 내성 전환을 사전에 준비해야 한다. 이 전환은 단순히 암호 알고리즘 하나를 교체하는 문제가 아니라, 지갑, 노드, 거래소, 사용자, 프로토콜 합의가 함께 움직여야 하는 장기적 이행 과정이다. 준비가 빠르면 전환은 질서 있는 업그레이드가 되지만, 준비가 늦으면 양자컴퓨터를 가진 공격자보다 먼저 움직여야 하는 시간 경쟁이 된다.

양자 위협은 비트코인만의 문제가 아니다

여기서 한 가지 중요한 사실을 짚어야 한다. 양자컴퓨터가 제기하는 암호학적 위협은 암호화폐에만 한정되지 않는다. 비트코인은 secp256k1 기반 타원곡선 서명 체계와 SHA-256 해시 함수를 사용하지만, 이 기술들은 비트코인을 위해 특별히 만들어진 고립된 기술이 아니다. 더 정확히 말하면, 비트코인은 공개키 암호, 전자서명, 암호학적 해시 함수라는 현대 디지털 보안 인프라의 핵심 기술 계열 위에 서 있다.

SHA-256은 SHA-2 계열에 속하는 대표적인 암호학적 해시 함수로, 미국 국가안보국(National Security Agency, NSA)이 설계하고 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)가 표준으로 발표한 알고리즘이다. 오늘날 SHA-2 계열 해시 함수는 전자서명, 인증서, 소프트웨어 무결성 검증, 보안 통신 등 다양한 영역에서 사용되며, 온라인 결제와 클라우드 서비스의 데이터 보호를 구성하는 암호학적 기반 중 하나로도 활용된다.

현대 인터넷 보안의 핵심 프로토콜인 전송 계층 보안(Transport Layer Security, TLS)도 이러한 암호 기술 위에서 작동한다. TLS는 인터넷 통신을 암호화하기 위한 표준 프로토콜로, HTTPS 통신의 기반이 되는 보안 기술이다. 사용자가 브라우저 주소창에서 HTTPS로 시작하는 웹사이트에 접속할 때, TLS는 서버 인증서를 검증해 서버의 신원을 확인하고, 안전한 통신을 위한 세션 키를 합의한다. 이 과정에는 공개키 암호, 디지털 서명, 인증서, 해시 함수가 함께 사용된다. TLS는 단순히 웹사이트 접속에만 쓰이는 기술이 아니다. 이메일 보안, 클라우드 서비스, 응용 프로그래밍 인터페이스(Application Programming Interface, API) 통신, 기업 네트워크 등 인터넷 인프라 전반이 TLS와 그 주변의 인증 체계에 의존한다.

이 과정의 중심에는 공개키 기반 구조(Public Key Infrastructure, PKI)가 있다. PKI는 디지털 인증서를 통해 특정 공개키가 실제로 특정 서버나 조직에 속한다는 사실을 보증하는 시스템이다. 웹 브라우저는 신뢰할 수 있는 인증기관의 루트 인증서를 기반으로 서버 인증서를 검증하고, 이를 통해 인터넷 통신의 신뢰 체인을 형성한다. 이러한 구조는 오랫동안 RSA나 타원곡선 기반 공개키 암호와 전자서명에 의존해 왔다. 다시 말해 우리가 웹사이트에 접속하고, 앱을 설치하고, 소프트웨어 업데이트를 받고, 클라우드에 데이터를 저장하는 일상적 행위의 배후에는 공개키 암호와 해시 함수가 구성한 보이지 않는 신뢰 구조가 작동하고 있다.

전통 금융 시스템 역시 이 구조에서 벗어나 있지 않다. 온라인 뱅킹 인증, 금융 거래 메시지 보호, 카드 결제 네트워크, 국제 결제 시스템, 전자문서 인증, 소프트웨어 코드 서명 등은 모두 공개키 인증, 전자서명, 암호화 통신 기술에 깊이 의존한다. 현대

금융 시스템은 서버, 인증서, 키, 서명, 해시, 보안 프로토콜이 결합된 암호학적 신뢰 구조 위에서 작동한다.

따라서 충분히 강력한 양자컴퓨터가 등장할 경우 영향을 받는 것은 비트코인만이 아니다. 인터넷 보안 통신, 전자서명, 인증서, 금융 거래, 소프트웨어 배포, 정부와 공공 부문의 보안 시스템 등 디지털 신뢰를 구성하는 광범위한 영역이 동시에 영향을 받는다. 양자컴퓨터 앞에서 취약한 것은 현대 문명의 디지털 보안 체계 전반이다. 그리고 역설적으로 바로 이 사실이 비트코인에게 일정한 완충 효과를 제공한다. 비트코인 커뮤니티만 이 문제를 해결해야 하는 것이 아니라, 전 세계의 정부와 기업, 연구기관이 같은 문제를 동시에 풀고 있기 때문이다.

이미 시작된 양자 내성 암호 전환

이 공동의 대응은 이미 시작되었다. 2024년 8월 NIST는 8년간 진행된 국제 표준화 과정을 거쳐 최초의 최종 양자 내성 암호(Post-Quantum Cryptography, PQC) 표준 3종을 확정 발표했다.[17] 첫 번째는 ML-KEM(Module-Lattice-Based Key-Encapsulation Mechanism)이다. 이는 통신 당사자가 안전하게 비밀키를 공유할 수 있도록 설계된 키 캡슐화 방식으로, 기존 인터넷 보안 프로토콜에서 사용되던 키 교환 구조를 양자컴퓨터 이후의 환경에 맞게 대체하거나 보완하기 위해 설계되었다. 두 번째는 ML-DSA(Module-Lattice-Based Digital Signature Algorithm)이다. 이는 기존의 RSA나 ECDSA 서명을 대체하기 위한 격자 기반 전자서명 방식이다. 세 번째는 SLH-DSA(Stateless Hash-Based Digital Signature Algorithm)이다. 이는 해시 함수 기반 전자서명 방식으로, ML-DSA와는 다른 수학적 접근에 기반하며, ML-DSA가 취약해질 경우를 대비한 보완적 표준으로 제시되었다.

[표 4] **NIST가 발표한 양자 내성 암호 표준 3종**

표준명	정식 명칭	용도	기반 수학	내용
FIPS 203	ML-KEM	키 공유	격자 문제	비밀 열쇠를 안전하게 공유
FIPS 204	ML-DSA	전자서명	격자 문제	내가 작성했음을 증명
FIPS 205	SLH-DSA	전자서명	해시 기반	장기 보안 안전장치

양자 내성 암호는 하나의 알고리즘을 가리키는 말이 아니다. 그것은 양자컴퓨터가 효율적으로 풀기 어려운 여러 수학적 문제를 기반으로 한 암호 기술들의 집합이다. 현재 가장 유력한 접근 방식 중 하나는 격자 기반 암호다. 격자 기반 암호는 고차원 격자 문제의 계산 난이도에 보안의 기초를 두며, 키 공유와 전자서명 모두에서 강력한 후보로 평가된다. 그러나 키와 서명 크기가 커지고, 시스템 적용 과정에서 저장 공간과 통신 비용이 증가할 수 있다는 부담도 있다. 해시 기반 서명은 보안 가정이 비교적 단순하고 오랜 연구를 통해 안정성이 검토되어 왔다는 장점이 있지만, 서명 크기와 계산 효율 면에서 불리할 수 있다. 이 때문에 미래의 보안 인프라는 하나의

기술에만 의존하기보다 서로 다른 수학적 기반을 가진 여러 암호 기술들을 조합하는 방향으로 발전할 가능성이 크다.

중요한 점은 이러한 변화가 연구 단계에만 머물러 있지 않다는 사실이다. NIST는 새 표준들이 즉시 사용할 준비가 되어 있다고 밝히며, 컴퓨터 시스템 관리자들에게 가능한 한 빨리 새로운 표준으로 전환을 시작할 것을 권고했다. 주요 기술 기업들도 양자 내성 암호를 실험적 또는 부분적으로 도입하기 시작했다. 구글과 클라우드플레어는 TLS 등 인터넷 통신 프로토콜에서 양자 내성 키 교환 방식을 시험하고 일부 배포해 왔으며,[18] 애플은 아이메시지(iMessage)에 양자 내성 암호를 반영한 PQ3 프로토콜을 도입했다.[19] IBM 역시 IBM 클라우드(IBM Cloud)의 양자 안전 TLS 모드와 IBM 퀀텀 플랫폼(IBM Quantum Platform)의 PQC 전환 계획 등 양자 내성 보안 인프라 개발을 진행하고 있다.[20] 또한 줌(Zoom)은 줌 워크플레이스(Zoom Workplace)와 줌 미팅(Zoom Meetings)에 양자 내성 종단 간 암호화(post-quantum end-to-end encryption, E2EE) 기능을 제공한다고 발표했다.[21]

이 흐름은 중요한 사실을 보여준다. 적어도 현재까지는, 양자컴퓨터를 실용적 암호 공격 수준까지 끌어올리는 일보다 양자컴퓨터에 저항하는 암호 체계를 확산시키는 일이 더 빠르게 진행되고 있다. 방패가 창보다 먼저 제도화되고 있는 셈이다. 양자컴퓨터가 실제 위협이 되기 훨씬 전부터, 글로벌 인터넷 인프라와 금융 시스템은 이미 새로운 암호 체계로 이동하기 시작했다.

이러한 국제적 전환은 비트코인에게도 중요한 시사점을 제공한다. 비트코인이 미래에 양자 내성 암호로 전환해야 한다면, 그것은 미지의 영역을 홀로 개척하는 일이 아니라 이미 세계가 움직이고 있는 방향을 따라가는 과정이 될 가능성이 크다. 그러나 비트코인의 전환은 정부나 기업이 중앙에서 명령할 수 있는 시스템 업데이트가 아니다. 지갑, 노드, 거래소, 채굴자, 사용자, 개발자 커뮤니티가 함께 움직여야 하는 합의의 문제다. 따라서 비트코인에게 남은 과제는 양자 내성 전환을 어떤 방식으로, 어떤 시점에, 어떤 사회적 합의를 통해 이루어낼 것인가에 있다.

04

비트코인의 전환 경로

양자컴퓨터가 실제 위협이 된다면 비트코인의 장기적 대응은 타원곡선 기반 서명 체계에서 양자 내성 서명 체계로 이동하는 것이다. 그러나 문제는 전환 가능성 자체가 아니라, 그것을 비트코인의 합의 구조 안에서 어떤 방식으로 구현할 것인가에 있다. 이는 단순한 소프트웨어 업데이트가 아니라, 프로토콜 규칙, 지갑과 거래소 인프라, 사용자 행동, 커뮤니티 합의가 함께 움직여야 하는 장기적 이행 과정이다.

업그레이드되어 온 비트코인

비트코인은 흔히 변하지 않는 규칙 위에 세워진 시스템으로 이해된다. 이 말은 어느 정도 맞다. 비트코인의 통화량, 작업증명, 난이도 조정, 거래 검증 규칙처럼 네트워크의 핵심 질서를 구성하는 요소들은 쉽게 바뀌지 않는다. 그러나 비트코인이 전혀 변화하지 않는다는 뜻은 아니다. 정확히 말하면, 비트코인은 '임의로 바뀌지 않는 시스템'이다. 변화가 가능하되, 그 변화는 공개적인 제안, 오랜 검토, 코드 구현, 네트워크 참여자의 채택, 그리고 사회적 합의를 거쳐야 한다.

이러한 변화는 보통 비트코인 개선 제안(Bitcoin Improvement Proposal, BIP)이라는 형식을 통해 논의된다. BIP는 비트코인 프로토콜이나 관련 표준의 변경 사항을 문서화하고, 그 기술적 내용과 도입 이유, 예상되는 영향을 공개적으로 검토하기 위한 제안 형식이다. 제안자는 먼저 비트코인 개발 메일링리스트(bitcoindev mailing list)[22] 등 공개 논의 공간에서 아이디어의 필요성과 실현 가능성을 설명하고 커뮤니티의 피드백을 받는다. 이후 초안이 충분히 정리되면 깃허브(GitHub)의 BIP 저장소에 풀 리퀘스트(pull request) 형태로 제출된다. BIP 편집자는 형식과 범위 등 편집 기준을 검토한 뒤 번호를 부여하고 저장소에 병합한다. 그러나 BIP로 등록되었다는 사실이 곧 그 제안이 채택되었거나 네트워크의 합의를 얻었다는 뜻은 아니다. 최종적인 채택 여부는 개발자, 노드 운영자, 채굴자, 지갑·거래소 사업자, 사용자들이 실제로 그 규칙을 구현하고 실행할 것인지에 달려 있다.

이때 프로토콜 규칙을 바꾸는 방식은 크게 소프트포크와 하드포크로 나뉜다. 소프트포크는 기존 규칙보다 더 엄격한 조건을 추가하는 방식이다. 업그레이드하지 않은 노드도 새 규칙에 따라 만들어진 블록을 대체로 유효한 블록으로 받아들일 수 있기 때문에, 기존 네트워크와의 호환성을 유지하기 쉽다. 반면 하드포크는 기존 규칙과 호환되지 않는 새로운 규칙을 도입하는 방식이다. 이 경우 참여자들이 같은 방향으로 업그레이드하지 않으면 네트워크가 서로 다른 규칙을 따르는 두 체인으로 갈라질 수 있다. 비트코인에서는 대체로 소프트포크 방식의 점진적 변화가 선호되어 왔다.

이러한 절차를 거쳐 실제 네트워크에 반영된 대표적인 사례가 2017년에 활성화된 세그윗(Segregated Witness, SegWit)이다. 소프트포크로 도입된 세그윗은 거래를 검증하는 데 필요한 서명 데이터를 거래의 기본 정보와 분리해 별도로 처리하도록 한 업그레이드였다. 이 변화는 BIP-141에 정리되어 있다.[23] 쉽게 말해, 거래의 핵심 내용과 그 거래를 승인했다는 증명 데이터를 구분해 저장하고 검증하는 방식으로 구조를 바꾼 것이다. 세그윗은 블록 용량을 단순한 바이트 수가 아니라 '블록 무게(block weight)'라는 기준으로 계산하도록 바꾸었고, 이 과정에서 서명 데이터는 일반 거래 데이터보다 낮은 가중치로 계산되었다. 이 변화는 거래 구조의 유연성을 높이고, 블록 공간을 더 효율적으로 사용할 수 있게 했다.[24] 그 결과 기존 네트워크와의 호환성을 유지하면서도 블록의 실질적인 처리 용량을 늘리는 효과가 발생했다.

2021년에 활성화된 탭루트(Taproot)도 중요한 사례다. 탭루트는 비트코인에 새로운 서명 방식과 더 유연한 지출 구조를 도입한 업그레이드였다.[25] 기존의 모든 ECDSA 서명을 폐기한 것이 아니라, 탭루트 출력과 지출 경로에서 슈노르(Schnorr) 서명을 사용할 수 있도록 새로운 규칙을 추가한 것이다. 슈노르 서명은 여러 사람이 함께 승인해야 하는 거래를 더 간결하게 처리할 수 있는 기반을 제공한다. 또한 탭루트는 복잡한 지출 조건이 있더라도, 실제로 사용된 조건만 블록체인에 드러나도록 만들었다. 예를 들어 여러 개의 잠금 해제 조건이 미리 설정되어 있더라도, 그중 사용되지 않은 조건들은 공개하지 않고 실제 사용된 경로만 보여줄 수 있다. 이로써 탭루트는 거래의 효율성을 높이는 동시에, 불필요한 정보와 사용되지 않은 조건을 블록체인에 노출하지 않는 방식으로 프라이버시도 개선했다.

중요한 점은 탭루트 역시 비트코인의 기존 규칙을 한꺼번에 갈아엎은 변화가 아니었다는 사실이다. 탭루트는 기존 주소와 서명 방식을 모두 폐기하지 않고, 새로운 출력 유형과 지출 방식을 추가하는 형태로 도입되었다. 이 업그레이드는 하드포크가 아니라 소프트포크로 이루어졌고, 비트코인 메인넷의 블록 높이 709,632에서 활성화되었다. 따라서 탭루트는 비트코인이 보수적인 합의 구조 안에서도 새로운 서명 방식과 더 복잡한 지출 조건을 수용할 수 있음을 보여주는 사례다.

세그윗과 탭루트는 비트코인이 고정된 기술 덩어리가 아니라, 매우 신중하지만 실제로 진화할 수 있는 시스템임을 보여준다. 세그윗은 거래 구조와 블록 공간 사용 방식을 바꾸었고, 탭루트는 새로운 서명 방식과 스크립트 표현 방식을 도입했다. 두 업그레이드 모두 비트코인의 보수적 개발 문화 안에서 장기간 검토와 합의를 거쳐 이루어졌다. 이 사실은 양자 내성 전환을 이해하는 데 중요하다. 비트코인은 아무렇게나 바뀌지 않지만, 절대로 바뀔 수 없는 시스템도 아니다.

점진적 전환을 위한 기술적 경로

양자 내성 전환의 첫 단계는 기존 서명 체계를 하루아침에 폐기하는 것이 아니라, 새로운 지출 조건을 비트코인 안에 추가할 수 있는 통로를 마련하는 것이다. 앞서 살핀 세그윗과 탭루트의 사례와 유사하게, 양자 내성 전환 역시 기존 주소와 거래 방식을 당장 폐기하기보다 새로운 출력 구조를 먼저 도입하고 사용자가 시간을 두고 이동할 수 있도록 하는 방향에서 논의될 가능성이 크다.

현재 논의되는 대표적 경로 중 하나가 BIP-360에 제시되어 있다. BIP-360은 새로운 출력 유형인 '머클 루트로 지불(Pay-to-Merkle-Root, P2MR)'을 제안한다.[26] 탭루트 출력은 내부 공개키를 그대로 기록하는 것이 아니라, 내부 공개키와 스크립트 트리 정보를 결합해 계산한 출력 키를 기록한다. 반면 P2MR은 탭루트의 키 경로 지출(key path spend)을 제거하고, 여러 지출 조건을 담은 스크립트 트리의 머클 루트만을 출력에 기록한다. 쉽게 말해, 자산을 잠그는 데 필요한 공개키나 세부 조건을 미리 드러내는 대신, 그 조건들이 존재한다는 암호학적 요약값만 블록체인에 남기는 것이다. 이처럼 P2MR은 스크립트 트리를 256비트 해시값으로 요약해 기록하기 때문에, 향후 양자내성 서명 방식이나 관련 스크립트 조건이 비트코인에 도입될 경우 이를 담아낼 수 있는 출력 구조가 될 수 있다.

BIP-360은 양자 공격을 장기 노출 공격(long exposure attack)과 단기 노출 공격(short exposure attack)으로 구분한다. 장기 노출 공격은 공개키가 블록체인에 오랫동안 드러나 있을 때, 공격자가 미래의 양자컴퓨터를 이용해 개인키 복구를 시도하는 상황을 가리킨다. 공개키로 지불(Pay-to-Public-Key, P2PK) 방식이나 탭루트처럼 공개키가 출력 단계에서 드러나는 구조는 이런 공격에 상대적으로 취약할 수 있다. 반면 단기 노출 공격은 거래가 멤풀에 머무는 동안 공개된 공개키를 이용해 개인키를 복구하고, 이에 기반한 새로운 거래를 더 높은 수수료와 함께 네트워크에 전파하는 방식이다. P2MR 역시 자산을 실제로 지출하는 순간에는 사용 중인 서명 체계의 공개키가 공개될 수 있다. 따라서 기존 ECDSA나 슈노르 서명처럼 공개키가 지출 시점에 노출되는 구조에서는, 거래가 멤풀에 머무는 동안 발생하는 단기 노출 공격까지 막을 수는 없다.

BIP-360 자체는 ML-DSA나 SLH-DSA 같은 양자내성 서명 알고리즘을 비트코인에 도입하는 제안이 아니다. 그것은 미래에 양자내성 서명 체계가 도입될 수 있도록, 공개키의 장기 노출을 줄인 출력 구조를 먼저 마련하는 제안에 가깝다. BIP-360 문서 역시 P2MR만으로는 거래가 확정되기 전 멤풀에서 잠시 공개되는 공개키를 공격하는 단기 노출 공격까지 막을 수 없으며, 더 정교한 양자 공격에 대응하려면 향후 양자내성 서명의 도입이 필요할 수 있다고 설명한다.

이러한 점에서 P2MR은 완성된 방어막이라기보다 전환을 위한 발판에 가깝다. 탭루트가 제공하던 유연한 스크립트 구조는 최대한 유지하면서도, 코인이 사용되기 전부터 공개키가 오래 노출되는 문제를 줄이려는 방식이기 때문이다. 또한 기존 탭루트 구조를 최대한 활용함으로써 지갑, 거래소, 라이브러리 등 기존 인프라가 적응해야 할 변화의 폭을 줄이려는 보수적 접근이기도 하다.

물론 이러한 경로에도 비용은 있다. P2MR은 탭루트의 키 경로 지출을 제거하기 때문에, 가장 단순한 탭루트 키 경로 지출보다 거래 데이터가 커질 수 있다. 일반적인 탭루트 키 경로 지출은 서명 하나만 제시하면 되지만, P2MR에서는 사용된 스크립트와 그 스크립트가 머클 트리에 포함되어 있음을 보여주는 증명 정보가 함께 필요하기 때문이다. 따라서 P2MR은 공개키 장기 노출 위험을 줄이는 대신, 블록 공간과 수수료 측면에서 일정한 부담을 가져올 수 있다. 이 문제는 향후 양자내성 서명 알고리즘이 실제 비트코인에 도입될 경우 더욱 중요해진다. 대체로 양자내성 서명은 기존 ECDSA나 슈노르 서명보다 크기가 크기 때문에, 새로운 보안성을 얻는 대가로 거래 크기와 검증 비용이 증가할 수 있다.[27] 따라서 P2MR은 공개키 장기 노

출 위험을 줄이는 대신, 블록 공간과 수수료 측면에서 일정한 부담을 가져올 수 있다. 이 문제는 앞으로 양자 내성 서명 알고리즘을 실제 비트코인에 적용할 때 더 중요해진다. 대체로 양자 내성 서명은 기존 ECDSA나 슈노르 서명보다 크기가 크기 때문에, 새로운 보안성을 얻는 대가로 거래 크기와 검증 비용이 증가할 수 있기 때문이다.

그럼에도 BIP-360이 중요한 이유는, 비트코인의 양자 내성 전환이 반드시 전면적이고 급격한 하드포크로만 가능한 것은 아니라는 점을 보여주기 때문이다. P2MR은 기존 주소와 거래 방식을 즉시 폐기하지 않고, 새로운 출력 유형을 추가해 사용자가 자산을 점진적으로 이동할 수 있는 선택적 경로를 제시한다. 이 방식에서 전환은 단번의 명령이 아니라, 먼저 통로를 열고 그 통로로 자산이 서서히 이동하는 과정에 가깝다.

요약하자면, 비트코인의 양자 내성 전환은 기술적으로 불가능한 일이 아니다. 이미 전 세계 보안 인프라는 양자 내성 암호로 이동하기 시작했고, 비트코인 내부에서도 공개키 노출을 줄이고 미래의 양자 내성 서명 체계를 수용하기 위한 구조적 실험이 논의되고 있다. 또한 양자 내성 전환은 발행 상한 변경처럼 보유자의 이해관계와 정면으로 충돌하는 사안도 아니다. 양자컴퓨터가 실제로 비트코인의 서명 체계를 위협할 정도로 발전한다면, 채굴자, 개발자, 거래소, 지갑 사업자, 일반 보유자 모두가 같은 위험에 놓이기 때문이다. 따라서 전환의 방향 자체에 대해서는 비교적 폭넓은 합의가 형성될 가능성이 높다.

결국 문제는 전환의 필요성보다 그 구현 방식에 있다. 어떤 출력 구조와 서명 알고리즘을 채택할 것인지, 이를 소프트포크로 도입할 수 있는지, 지갑과 거래소가 얼마나 빨리 지원할 수 있는지, 사용자가 실제로 자산을 새 주소로 이동할 것인지가 모두 맞물려 있기 때문이다. 기술적 경로는 열릴 수 있지만, 그것이 실제 보안으로 이어지려면 사용자, 지갑, 거래소, 노드, 채굴자의 자발적 채택과 분산된 합의가 뒤따라야 한다. 그리고 바로 이 지점에서 전환의 시간표와 잔여 코인의 문제가 등장한다. 전환이 언제 시작되느냐에 따라 이 과정은 질서 있는 이행이 될 수도, 공격자와의 경쟁이 될 수도 있다. 또한 끝내 이동하지 않거나 이동할 수 없는 코인은 별도의 판단 대상으로 남는다.

전환의 시간표와 잔여 코인의 문제

양자 내성 전환을 이해하려면 먼저 시간표의 문제를 살펴봐야 한다. 양자컴퓨터가 비트코인에 위협이 되는 방식은 하나의 순간으로 오지 않는다. 더 정확히 말하면, 그 위협은 전환이 언제 시작되느냐에 따라 전혀 다른 성격을 갖는다. 양자 공격이 실용화되기 이전에 비트코인이 미리 대응 체계를 도입하는 경우와, 양자 공격이 이미 실용화된 이후에야 대응이 시작되는 경우는 같은 문제가 아니다. 전자는 비교적 질서 있는 이행의 문제이고, 후자는 공격자와의 경쟁 문제다.

첫 번째 경우, 전환은 비교적 안정적인 과정이 될 수 있다. 네트워크가 먼저 새로운 양자 내성 주소 체계나 새로운 지출 조건을 도입하고, 사용자들이 충분한 시간을 두고 기존 자산을 새로운 주소로 이동하도록 설계할 수 있기 때문이다. 이 경우 전환

의 핵심은 사용자가 자신의 지출 권한을 이용해 자산을 새로운 양자 내성 주소로 옮길 수 있도록 절차를 마련하는 데 있다. 사용자는 지갑이나 거래소가 제공하는 전환 기능을 통해 기존 주소에 있던 자산을 새로운 주소로 이동시키고, 네트워크는 그 거래가 새 규칙에 맞는지 검증한다. 이런 방식이라면 전환은 단번의 충격이 아니라 긴 시간에 걸친 이동 과정이 된다.

반면 두 번째 경우, 전환은 훨씬 위험한 양상을 띤다. 양자컴퓨터가 이미 공개키를 보고 개인키를 찾아낼 수 있는 수준에 도달한 뒤에야 대응이 시작된다면, 기존 자산을 새로운 양자 내성 주소로 옮기는 과정 자체가 공격의 기회가 될 수 있기 때문이다. 평상시라면 사용자는 지갑이나 거래소를 통해 기존 자산을 새 주소로 보내면 된다. 그러나 빠른 양자 공격자가 이미 존재하는 상황에서는, 기존 주소를 지출하는 순간 공개키가 네트워크에 드러나고 공격자가 그 공개키를 바탕으로 개인키를 계산해 경쟁 거래를 만들 수 있다. 원래 소유자는 자신의 코인을 양자 내성 주소로 옮기려 하지만, 공격자는 그 찰나의 공개키 노출을 이용해 같은 코인을 먼저 가져가려 할 수 있는 것이다. 이때 문제는 더 이상 단순한 업그레이드가 아니다. 그것은 누가 먼저 거래를 만들어 네트워크에 기록시키는가의 시간 경쟁이 된다. 결국 언제 전환을 시작하느냐가 양자 내성 전환을 질서 있는 이행으로 만들지, 공격자와의 경쟁으로 만들지를 결정한다.

이러한 문제의식은 학계의 전환 프로토콜 연구에서도 확인된다. 임페리얼칼리지 런던(Imperial College London) 암호화폐 연구·공학센터(Centre for Cryptocurrency Research and Engineering)의 스튜어트(I. Stewart) 등은 2018년 논문에서 '커밋-지연-공개(commit–delay–reveal)' 방식의 전환 프로토콜을 제안했다.[28] 이 방식은 양자 내성 서명 체계가 이미 비트코인에 도입되었지만, 일부 자산이 여전히 기존 비양자내성 출력에 남아 있는 상황을 전제로 한다. 이름 그대로 이 프로토콜은 세 단계로 이루어진다. 먼저 '커밋' 단계에서 사용자는 기존 공개키와 새 양자 내성 공개키를 그대로 공개하지 않고, 두 값을 함께 해시한 값만 블록체인에 남긴다. 이 해시값은 나중에 공개될 두 공개키의 내용을 미리 봉인해둔 약속과 같다. 해시값만으로는 두 공개키의 내용을 알 수 없지만, 나중에 두 공개키가 공개되었을 때 그것들이 과거에 남겨둔 해시값과 일치하는지는 검증할 수 있다.

다음은 '지연' 단계다. 사용자는 해시값을 남긴 뒤 곧바로 자산을 옮기지 않고, 충분한 기간 동안 기다린다. 저자들은 예시적으로 6개월의 지연 기간을 제안한다. 이 기간이 필요한 이유는 커밋 기록을 충분히 깊은 과거의 일부로 만들기 위해서다. 커밋이 몇 블록 전의 기록에 불과하다면 공격자가 체인 재조직을 통해 그 기록을 되돌리고 자신에게 유리한 기록을 새로 끼워 넣으려 할 수 있다. 그러나 커밋 기록이 6개월 전의 기록이 되면, 그것을 되돌리려면 장기간의 블록 역사를 다시 써야 한다. 이는 기술적·경제적으로 매우 어렵고, 설령 시도되더라도 네트워크 전체가 명백한 공격으로 인식할 가능성이 크다.

마지막은 '공개(Reveal)' 단계다. 충분한 지연 기간이 지난 뒤 사용자는 기존 공개키와 새 양자내성 공개키, 그리고 과거에 두 키의 연결을 커밋해두었음을 증명하는 검증 정보를 공개한다. 동시에 새 양자내성 개인키로 만든 서명을 제출해 자신이 새 양자내성 키도 통제하고 있음을 증명한다. 이때 공격자가 공개된 기존 공개키를 보고 뒤늦게 기존 개인키를 계산하더라도, 새 양자내성 개인키를 알지 못하며 정당한

소유자만이 지연 기간 이전에 남길 수 있었던 커밋 기록도 사후에 만들어낼 수 없다. 따라서 새 규칙 아래에서는 뒤늦게 기존 개인키를 알아낸 것만으로는 자산을 탈취하기 어렵다. 저자들은 이 방식이 ECDSA가 이미 손상된 상황에서도 작동할 수 있으며, 비트코인 프로토콜 수정이 필요하지만 소프트포크를 통해 구현할 수 있다고 설명한다.

다만 이 방식은 보편적 해법은 아니다. 특히 아직 공개키가 드러나지 않은 기존 출력의 안전한 이전을 주된 대상으로 한다. 이미 공개키가 장기간 노출된 코인이나, 짧은 시간 안에 대량으로 이전해야 하는 상황까지 해결하기는 어렵다. 그럼에도 이 사례는 양자 내성 전환의 핵심이 단순한 새 주소 도입에 있지 않음을 보여준다. 더 어려운 문제는 과거의 규칙 아래 생성된 자산을 어떤 절차를 거쳐 새로운 보안 체계 안으로 편입할 것인가에 있다. 공개키가 언제 드러나는지, 커밋 기록을 얼마나 오래 기다려야 하는지, 어떤 거래를 정당한 이전으로 인정할 것인지가 모두 합의 규칙의 문제가 된다. 결국 양자 내성 전환은 암호 알고리즘의 교체인 동시에, 기존 자산을 새로운 보안 질서로 이주시킬 절차의 설계다.

그러나 어떤 절차가 마련되더라도 모든 코인이 그 이주 과정에 참여할 수 있는 것은 아니다. 지갑이 오래되어 새 형식을 지원하지 않을 수도 있고, 사용자가 전환 필요성을 인지하지 못할 수도 있으며, 장기 보유자가 의도적으로 아무 행동도 하지 않을 수도 있다. 더 심각한 경우도 있다. 개인키가 분실되었거나, 소유자가 사망했거나, 접근 권한이 영구히 사라진 코인은 어떤 전환 경로가 열리더라도 스스로 이동할 수 없다. 결국 전환 절차는 이동할 수 있는 자산을 위한 길을 열어줄 수는 있지만, 이동하지 않거나 이동할 수 없는 자산의 문제까지 자동으로 해결하지는 못한다.

하드포크가 이루어진다고 해서 이 문제가 곧바로 사라지는 것도 아니다. 물론 하드포크는 기존 UTXO의 처리 방식을 새롭게 정할 수 있다. 특정 코인을 동결하거나, 별도의 조건을 부과하거나, 새 체인에서 다르게 계산하도록 설계할 수도 있다. 그러나 단순히 새로운 합의 규칙을 도입한다고 해서 과거의 모든 코인이 자동으로 양자 안전한 주소에 다시 놓이는 것은 아니다. 소유자의 자발적 이동 없이 기존 코인을 양자 내성 체계 안으로 편입하려면, 그 자체가 별도의 개입 규칙이 되어야 한다. 다시 말해 하드포크는 문제를 없애는 장치라기보다, 어떤 코인을 어떻게 인정하고 제한할 것인지에 대한 더 강한 판단을 요구하는 방식이다.

이 지점에서 양자 내성 전환은 이동 가능한 코인과 이동하지 않거나 이동할 수 없는 코인을 갈라놓는다. 이동 가능한 코인은 비교적 분명하다. 소유자가 개인키를 보유하고 있고, 지갑과 거래소가 새로운 주소 형식을 지원하며, 충분한 시간이 주어진다면 이 코인들은 새로운 체계로 이전될 수 있다. 문제는 그 반대편에 있는 코인들이다. 공개키가 이미 노출된 오래된 코인, 장기간 움직이지 않은 코인, 개인키가 사라진 로스트 코인, 그리고 사토시 나카모토의 초기 코인처럼 소유자의 의사를 확인할 수 없는 자산은 전환 과정에서 별도의 쟁점으로 남는다.

따라서 비트코인의 양자 내성 전환에서 새로운 서명 체계나 주소 형식을 마련하는 것은 첫 번째 과제일 뿐이다. 더 어려운 문제는 그 체계로 이동하지 않는 코인을 어떻게 해석할 것인가에 있다. 그것들은 정당한 장기 보유자의 자산인가, 접근 불가능한 로스트 코인인가, 공개키 노출로 인해 양자 공격자가 노릴 수 있는 취약 자산인가, 아니면 네트워크가 별도의 방식으로 다루어야 할 위험 자산인가. 다음 장의 쟁

점은 바로 여기에 있다. 비트코인이 양자 내성 체계로 전환할 수 있는가가 아니라, 그 전환에 참여하지 않거나 참여할 수 없는 코인을 어떻게 다룰 것인가의 문제다.

05

사토시 코인과 로스트 코인의 문제

앞 장에서 본 것처럼, 양자 내성 전환의 가장 어려운 문제는 새로운 주소 체계를 마련하는 데서 끝나지 않는다. 이 장에서는 그 전환에 참여하지 않거나 참여할 수 없는 코인들, 특히 공개키가 이미 노출된 오래된 코인과 사토시 코인, 로스트 코인이 어떤 쟁점을 만드는지 살펴본다.

공개키가 이미 노출된 코인들

양자 위협의 관점에서 모든 비트코인 UTXO가 같은 위험에 놓여 있는 것은 아니다. 핵심은 공개키가 블록체인에 이미 드러나 있는지, 그리고 그 상태가 얼마나 오래 지속되었는지에 있다. 초기 비트코인에는 P2PK 방식이 사용되었는데, 이 방식에서는 공개키가 잠금 스크립트에 직접 포함된다. 다시 말해 코인이 생성되는 순간부터 공개키가 블록체인에 노출된다. 따라서 이러한 UTXO는 미래의 양자컴퓨터가 충분히 강력해질 경우 장기 노출 공격의 직접적인 표적이 될 수 있다. 공격자가 이미 공개되어 있는 공개키를 바탕으로 개인키 역산을 시도할 수 있기 때문이다.

반면 오늘날 널리 사용되어 온 공개키 해시로 지불(Pay-to-Public-Key-Hash, P2PKH) 방식에서는 공개키 자체가 아니라 공개키의 해시값이 먼저 블록체인에 기록된다. 이 구조에서는 실제로 코인을 지출하기 전까지 공개키가 드러나지 않는다. 공개키 해시는 공개키를 한 번 더 암호학적으로 요약한 값이기 때문에, 공격자가 해시값만 보고 바로 공개키를 알아내기는 어렵다. 이런 점에서 P2PKH는 P2PK보다 공개키 장기 노출 위험이 낮다.

그러나 P2PKH라고 해서 위험이 완전히 사라지는 것은 아니다. 해당 UTXO를 지출하는 순간 공개키가 거래 안에 포함되어 네트워크에 공개되기 때문이다. 다만 일반적인 경우라면 이 노출은 제한적인 위험에 그친다. 거래가 확정되면서 해당 UTXO는 이미 소비되고, 같은 주소에 더 이상 잔액이 남아 있지 않다면 공격자가 뒤늦게 개인키를 계산하더라도 가져갈 코인이 없기 때문이다. 하지만 같은 주소를 반복해서 사용하는 경우에는 이야기가 달라진다. 한 번의 지출로 공개키가 공개된 이후에도 같은 주소에 잔액이 남아 있거나, 이후 다시 그 주소로 자금을 받는다면 공격자는 이미 공개된 공개키를 대상으로 개인키 역산을 시도할 시간을 갖게 된다. 이 때문에 비트코인에서는 주소 재사용을 피하는 것이 중요한 보안 관행으로 권장되어 왔다. 양자 위협의 관점에서 보면 이 원칙은 더 중요해진다. 기존에는 주소 재사용이 주로 프라이버시와 일반 보안의 문제였다면, 양자컴퓨터 시대에는 공개키 노출 시간을 줄이는 방어 전략이 된다. 공개키가 한 번도 드러나지 않은 코인과 이미 공개키가 노출된 코인은 같은 위험 상태에 있지 않으며, 양자 내성 전환 역시 이 차이를 전제로 논의되어야 한다.

[표 5] 비트코인 주소 유형별 양자 취약도

주소·출력 유형	공개키 노출 방식	양자 위협 관점
P2PK	출력 생성 시 공개키가 직접 노출	장기 노출 위험이 가장 큼
P2PKH	지출 전에는 공개키 해시만 노출, 지출 시 공개키 공개	주소 재사용 시 위험 증가
P2TR	탭루트 출력키가 온체인에 노출	장기 노출 문제를 가질 수 있음
P2MR	출력에는 머클 루트만 기록	공개키 장기 노출을 줄이지만, 지출 시점의 단기 노출 문제는 별도 대응 필요

사토시 코인과 로스트 코인

이 구분은 비트코인의 오래된 코인들을 볼 때 더 중요한 의미를 갖는다. 초기 비트코인에는 공개키가 직접 노출되는 P2PK 출력이 사용된 경우가 있었고, 그중 일부는 지금까지 한 번도 이동되지 않았다. 특히 사토시 나카모토가 채굴한 것으로 추정되는 약 100만~110만 개[29]의 비트코인은 양자 보안 논의에서 반복적으로 언급되는 사례다.

사토시 코인 문제가 중요한 이유는 분명하다. 사토시 코인으로 추정되는 대규모 비트코인이 양자 공격에 의해 이동한다면, 시장은 그것을 단순한 해킹 사건으로만 받아들이지 않을 가능성이 크다. 그것은 비트코인의 가장 오래된 잠금 상태가 깨졌다는 신호가 되고, 동시에 대규모 잠재 공급이 시장에 등장할 수 있다는 신호가 된다. 이 규모는 전체 발행량 2,100만 개의 약 5%에 해당한다. 이 물량이 갑자기 이동하거나 시장에 매도될 수 있다고 인식되는 것만으로도 가격과 신뢰에 큰 충격을 줄 수 있다.

문제는 사토시 코인에만 그치지 않는다. 개인키가 분실되어 더 이상 이동할 수 없는, 이른바 '로스트 코인'도 양자 내성 전환에서 별도의 쟁점을 만든다. 현재까지 움직이지 않았다는 사실만으로 어떤 코인이 정말 분실되었는지, 아니면 단순히 장기 보유되고 있는지 확정할 수는 없다. 문제는 실제로 개인키가 사라졌거나 소유자의 의사를 확인할 수 없는 코인이다. 이러한 코인은 새로운 양자 내성 주소로 이동할 수 없기 때문에, 전환 과정에서 처리 원칙의 문제를 남긴다.

따라서 양자 내성 전환은 두 가지 문제를 동시에 드러낸다. 하나는 공개키가 이미 노출된 코인의 보안 문제다. 이러한 코인은 충분히 강력한 양자컴퓨터가 등장할 경우 직접적인 공격 대상이 될 수 있다. 다른 하나는 이동하지 않거나 이동할 수 없는 코인의 처리 문제다. 소유자가 키를 통제하고 있으면 새로운 주소로 이동할 수 있지만, 개인키가 사라졌거나 소유자의 의사를 확인할 수 없는 코인은 전환 과정에 참여할 수 없다. 이 두 문제는 서로 겹칠 수 있지만, 성격은 다르다. 전자는 암호학적 취약성의 문제이고, 후자는 소유권과 불변성, 네트워크 개입의 한계를 둘러싼 판단의 문제다.

이처럼 양자 내성 전환은 이동하지 않거나 이동할 수 없는 코인을 네트워크가 어떻

게 해석할 것인가의 문제를 남긴다. 바로 이 지점에서 논의는 이른바 '양자 도난'과 '양자 복구'라는 상반된 해석의 문제로 넘어간다. 공개키가 이미 드러난 오래된 코인을 누군가 양자컴퓨터를 이용해 이동시킬 수 있게 된다면, 네트워크는 그것을 유효한 지출로 받아들여야 하는가. 아니면 공격자가 양자컴퓨터를 이용해 공개키가 노출된 코인을 먼저 이동시키지 못하도록, 양자 내성 주소로 옮길 수 있는 유예 기간이 지난 뒤 그 지출을 제한해야 하는가. 이 질문은 단순한 보안 정책의 문제가 아니다. 그것은 비트코인에서 소유권을 무엇으로 볼 것인지, 그리고 네트워크가 보안을 이유로 기존 규칙에 어디까지 개입할 수 있는지의 문제와 직결된다.

움직이지 않는 코인을 둘러싼 네 가지 선택

이 문제를 둘러싼 선택지는 크게 네 가지로 정리할 수 있다. 첫째는 기존 규칙을 그대로 유지하는 것이다. 이 관점에서 비트코인의 소유권은 신원, 의도, 장기 보유 여부가 아니라 유효한 서명을 만들 수 있는 능력에 의해 판정된다. 공개키가 블록체인에 드러나 있고, 누군가가 양자컴퓨터를 이용해 그 공개키에 대응하는 개인키를 계산한 뒤 유효한 서명을 만들어낸다고 하더라도 네트워크는 그 지출을 막지 않는다. 이 해석에 따르면 양자컴퓨터를 이용한 지출은 프로토콜 외부의 침입이라기보다, 비트코인이 전제해 온 암호학적 난제가 더 이상 충분히 어렵지 않게 된 결과에 가깝다. 이 접근의 장점은 명확하다. 네트워크는 사후적으로 소유자를 판단하지 않고, 특정 코인을 임의로 차단하지 않으며, '유효한 서명은 유효한 지출'이라는 규칙을 끝까지 유지한다. 그러나 그 대가도 크다. 원래 소유자의 관점에서 보면 양자컴퓨터를 이용한 지출은 사실상 탈취에 가깝고, 특히 사토시 코인이나 대규모 장기 미사용 코인이 갑자기 이동할 경우 시장은 이를 대규모 잠재 공급이 깨어난 신호로 받아들일 수 있다. 규칙은 보존되지만, 그 규칙이 보호하려던 경제적 신뢰가 흔들릴 수 있는 것이다.

둘째는 동결이다. 동결은 일정한 전환 유예 기간이 지난 뒤에도 양자 내성 주소로 이동하지 않은 공개키 노출 코인의 지출을 제한하거나, 특정 유형의 오래된 UTXO를 더 이상 사용할 수 없도록 만드는 방식이다. 이 접근은 양자컴퓨터를 가진 공격자가 공개키가 노출된 코인의 개인키를 계산해 대량의 자산을 이동시키는 사태를 막기 위한 안전장치로 제안될 수 있다. 특히 사토시 코인이나 오래된 미사용 코인이 공격자에 의해 이동한다면, 실제 매도가 이루어지지 않더라도 그 가능성만으로 가격과 신뢰에 큰 충격이 발생할 수 있다. 이런 점에서 동결은 가장 직접적인 방어책처럼 보인다. 그러나 동결은 비트코인의 기본 원칙과 정면으로 충돌한다. 비트코인에서 자산의 통제권은 법적 신원이나 중앙기관의 승인보다 개인키의 통제에 의해 정의된다. 그런데 네트워크가 특정 코인을 '오래 움직이지 않았다'거나 '양자 공격에 취약하다'는 이유로 지출하지 못하게 만든다면, 이는 유효한 서명을 만들 수 있는 자가 코인을 지출할 수 있다는 원칙에 예외를 두는 일이다. 더구나 실제 소유자가 장기 보유 중이었거나, 뒤늦게 키를 회복했거나, 기술적 이유로 전환 시기를 놓친 경우에도 그 권한이 차단될 수 있다. 동결은 공격자를 막을 수 있지만, 동시에 정당한 소유자의 권리까지 함께 묶어버릴 위험을 안고 있다.

셋째는 조건부 복구다. 이는 기존 규칙 유지와 전면 동결 사이의 절충안이다. 예를

들어 전환 유예 기간이 지난 뒤 기존 타원곡선 서명만으로는 공개키 노출 코인을 곧바로 지출할 수 없도록 제한하되, 정당한 소유자가 자신이 해당 자산을 통제해 왔다는 사실을 별도의 방식으로 증명할 수 있다면 양자 내성 주소로 이전할 수 있도록 하는 방식이다. 이론적으로는 영지식 증명(Zero-Knowledge Proof, ZKP)을 활용해 일부 유형의 소유자에게 제한적 복구 경로를 제공하는 방안도 생각해볼 수 있다.[30] 영지식 증명은 어떤 비밀을 직접 공개하지 않고도 그 비밀을 알고 있다는 사실을 증명할 수 있게 하는 암호학적 기술이다. 따라서 복구 과정에서 소유자가 보유한 별도의 비밀을 공개하지 않으면서도, 일정한 조건 아래 정당한 통제권을 증명하는 구조를 설계할 수 있을 가능성이 있다.

그러나 이 접근은 매우 조심스럽게 다루어져야 한다. 단순히 기존 개인키를 알고 있음을 증명하는 방식이라면 양자 공격자도 같은 개인키를 계산할 수 있으므로 정당한 소유자와 공격자를 구분하기 어렵다. 조건부 복구가 의미를 가지려면 블록체인에 공개되지 않은 별도의 비밀이 필요하다. 예컨대 일부 지갑에서 사용하는 BIP-39 방식의 시드 구문(seed phrase),[31] 즉 지갑을 복구할 때 쓰는 일련의 단어 조합처럼 공격자가 공개키로부터 역산할 수 없고 정당한 소유자만 알고 있는 정보가 있어야 한다. 하지만 초기 비트코인 지갑에는 이런 방식의 시드 구문이 없었고, 사토시 코인이나 초기 채굴 코인에 어떤 별도의 비밀이 남아 있는지 확인할 방법도 없다. 개인키가 실제로 사라진 로스트 코인에도 이 방식은 적용될 수 없다. 따라서 영지식 증명을 활용한 복구 경로는 일부 지갑과 일부 사용자에게는 가능성을 제공할 수 있지만, 사토시 코인과 로스트 코인 문제 전체를 해결하는 보편적 해법으로 보기는 어렵다.

넷째는 소각이다. 소각은 동결보다 더 극단적인 선택이다. 일정한 유예 기간이 지나도 양자 내성 주소로 이동하지 않은 공개키 노출 코인을 영구적으로 사용할 수 없게 만들거나, 경제적으로 유통 가능 공급에서 제외하는 방식이다. 이 접근은 양자 공격자가 로스트 코인이나 오래된 코인을 탈취해 시장에 유입시키는 위험을 원천적으로 차단할 수 있다. 또한 장기적으로는 양자 취약 코인이 언제든 시장에 등장할 수 있다는 불확실성을 제거하는 효과도 기대할 수 있다. 그러나 그 대가는 가장 크다. 소각은 누군가의 정당한 장기 보유 자산을 네트워크가 임의로 무효화할 수 있다는 선례를 만든다. 비트코인이 신뢰받는 이유 중 하나가 임의적 몰수와 검열에 저항하는 데 있다면, 소각은 그 원칙과 가장 강하게 충돌하는 선택이다. 보안을 위해 공급의 일부를 제거할 수 있다는 선례가 만들어지는 순간, 비트코인의 절차적 불변성은 이전과 같은 의미를 유지하기 어려워진다.

결국 이 네 가지 선택은 모두 서로 다른 위험을 안고 있다. 규칙 유지는 비트코인의 절차적 중립성을 보존하지만 양자 공격자가 오래된 코인을 이동시키는 위험을 감수한다. 동결은 공격 가능성을 차단하려 하지만 정당한 장기 보유자의 지출 권한까지 제한할 수 있다. 조건부 복구는 절충을 시도하지만, 정당한 소유자와 양자 공격자를 구별할 수 있는 별도의 증명 조건이 있을 때에만 제한적으로 작동한다. 소각은 가장 강력한 방어책이지만, 비트코인의 반검열성과 소유권 불가침 원칙을 가장 크게 훼손한다.

따라서 사토시 코인과 로스트 코인의 문제는 양자컴퓨터가 등장할 경우 어떤 암호 알고리즘을 쓸 것인가의 문제가 아니다. 그것은 움직이지 않는 코인을 비트코인 생

태계가 어떻게 해석할 것인가의 문제다. 움직이지 않는 코인은 정당한 장기 보유자의 자산인가, 접근 불가능한 로스트 코인인가, 양자 공격자가 가져갈 수 있는 무주물(無主物)인가, 아니면 네트워크가 보호하거나 격리해야 할 위험 자산인가. 이 질문에 대한 답은 기술만으로 정해지지 않는다. 그것은 비트코인 공동체가 소유권, 불변성, 보안, 경제적 안정성 가운데 무엇을 더 우선할 것인지에 대한 판단을 요구한다.

다음 장의 문제는 여기서 시작된다. 만약 이 선택을 둘러싸고 합의가 이루어지지 않는다면, 비트코인은 하나의 기술적 업그레이드가 아니라 체인의 정통성과 절차적 불변성을 둘러싼 더 깊은 갈등에 직면할 수 있다.

06

하드포크와 정통성의 분기

하드포크가 가를 수 있는 두 개의 비트코인

앞 장에서 살펴본 네 가지 선택지가 하나의 합의로 수렴하지 못한다면, 쟁점은 결국 어느 규칙을 따를 것인가로 이동한다. 이때 하드포크는 단순한 업그레이드 방식이 아니라, 같은 과거를 공유한 네트워크가 서로 다른 규칙 아래에서 갈라지는 사건이 된다. 동일한 UTXO 집합을 두고도 한 체인은 기존 서명 규칙을 그대로 인정할 수 있고, 다른 체인은 양자 공격에 취약한 코인의 지출에 제한을 둘 수 있다. 이 경우 비트코인은 하나의 기술적 전환이 아니라, 서로 다른 소유권 해석을 가진 두 체인 사이의 선택 문제에 직면한다.

한쪽은 기존 규칙을 유지하는 길을 선택할 수 있다. 이 체인에서는 유효한 서명이 제시되는 한, 그 서명이 기존 소유자가 만든 것인지 양자컴퓨터로 역산한 개인키로 만들어진 것인지 구분하지 않는다. 비트코인의 소유권은 신원이나 의도가 아니라 유효한 서명으로 판정된다는 원칙을 끝까지 유지하는 것이다. 이 관점에서 네트워크가 할 일은 소유자를 해석하는 것이 아니라 규칙에 맞는 서명을 검증하는 데 있다.

반대로 다른 체인은 공개키가 노출된 오래된 코인이나 장기간 이동하지 않은 코인에 별도의 제한을 둘 수 있다. 일정한 유예 기간 안에 양자 내성 주소로 이동하지 않은 코인의 지출을 제한하거나, 공개키 노출 코인에 대해 추가 조건을 요구하거나, 특정 범주의 UTXO를 동결 또는 소각하는 방식이 가능하다. 이 체인은 기존의 서명 규칙만으로는 충분하지 않다고 판단한다. 양자컴퓨터가 암호학적 전제를 무너뜨리는 상황에서는, 유효한 서명이라는 형식만으로 정당한 소유권을 판정할 수 없다는 것이다.

이때 두 체인은 같은 과거를 공유하지만 서로 다른 철학을 구현하게 된다. 전자는 '유효한 서명은 유효한 지출'이라는 원칙을 유지하고, 후자는 '양자 공격이 가능한 조건에서는 기존 서명 규칙만으로 소유권을 판단할 수 없다'고 본다. 전자는 절차적 중립성을 강조하고, 후자는 시스템 보호와 경제적 안정성을 강조한다. 어느 쪽도 단순히 기술적으로만 옳거나 그르다고 말하기 어렵다. 양쪽 모두 비트코인의 중요한 가치 중 하나를 붙잡고 있기 때문이다.

이와 유사한 사례는 이미 암호화폐 역사에 존재한다. 2016년 이더리움 생태계에서는 탈중앙화 투자 펀드처럼 설계된 스마트 컨트랙트 프로젝트 '더 DAO(The DAO)'가 공격을 받았다. 공격자는 이더리움 프로토콜 자체가 아니라 더 DAO의 스마트 컨트랙트 취약점을 이용해 대규모 이더를 빼냈다. 이 사건은 '코드대로 실행된 결과를 그대로 인정해야 하는가, 아니면 공동체가 개입해 피해를 되돌려야 하는

가'라는 논쟁을 불러왔다. 결국 이더리움 커뮤니티는 하드포크를 통해 해킹 피해를 복구하는 체인을 선택했다.[32] 이 하드포크는 블록 1,920,000에서 실행되었고, 이더리움 재단은 당시 약 1,200만 ETH가 회수 계약으로 이동했다고 설명했다. 반면 이에 반대한 일부 참여자들은 기존 체인을 유지했고, 그 결과 '이더리움 클래식(Ethereum Classic, ETC)'이 형성되었다. 이 사건은 하드포크가 단순한 기술 수정이 아니라 '무엇을 정당한 역사로 볼 것인가'의 문제임을 보여준다.

양자컴퓨터 문제도 이와 유사하게, 어떤 거래를 정당한 역사로 인정할 것인가의 질문을 던진다. 공개키가 노출된 오래된 코인의 이동을 유효한 지출로 볼 것인지, 아니면 양자 도난으로 보고 제한할 것인지에 대한 합의가 이루어지지 않는다면, 비트코인은 서로 다른 소유권 철학을 가진 체인들로 갈라지게 될 것이다. 이 경우 어느 체인이 '정통 비트코인'인지는 코드만으로 결정되지 않는다. 정통성은 노드 운영자, 채굴자, 거래소, 지갑 사업자, 커스터디 기관, 기관투자자, 자가 보관(self-custody) 사용자, 일반 사용자의 선택 속에서 형성된다. 어떤 체인을 채굴할 것인지, 어떤 체인을 BTC로 표시할 것인지, 어떤 체인을 수탁 자산으로 인정할 것인지, 어떤 체인을 장기 보유할 것인지가 모두 정통성의 일부가 된다. 하드포크는 코드를 나누는 사건이지만, 정통성은 그 코드를 실행하고 가치를 부여하는 사회적 선택을 통해 만들어진다.

제도권 하드포크와 공공재화의 유혹

여기서 더 급진적인 가능성도 생각해볼 수 있다. 그것은 기존 비트코인 체인 안에서 오래된 코인을 동결하거나 소각하는 방식이 아니라, 아예 새로운 규칙을 가진 체인을 만들고, 그 체인을 제도권 인프라가 비트코인의 새로운 기준 체인으로 인정하도록 유도하는 방식이다. 이 시나리오에서는 특정 블록 높이를 기준으로 스냅샷을 찍고, 일정한 유예 기간 안에 양자 내성 주소로 이동하지 않은 코인을 '미이동 자산'으로 분류한다. 이후 새 체인은 이 코인들을 네트워크 보안 기금, 개발 기금, 공공재 기금 등으로 배정하도록 설계될 수 있다.

기술적으로 이런 포크가 불가능한 것은 아니다. 하드포크는 기존 규칙과 호환되지 않는 새로운 합의 규칙을 도입하는 방식이므로, 새 체인에서는 특정 조건을 충족하지 않은 UTXO를 기존 체인과 다르게 처리하도록 설계할 수 있다. 예를 들어 일정 시점까지 양자 내성 주소로 이동하지 않은 공개키 노출 코인을 더 이상 개인이 지출할 수 있는 자산으로 인정하지 않고, 이를 새 체인의 공공재 기금으로 귀속시키는 규칙을 만들 수 있다. 이 경우 포크 지지자들은 오래된 취약 코인을 양자 공격자의 전리품으로 남겨두기보다, 새 체인에서 격리하고 네트워크 전체의 보안과 개발을 위한 재원으로 전환하는 편이 더 합리적이라고 주장할 수 있다. 앞 장에서 살펴본 것처럼, 사토시 코인이나 장기 미사용 코인의 이동 가능성은 시장에 잠재적 공급 충격으로 받아들여질 수 있기 때문이다. 이 점에서 재분배형 하드포크는 단순한 기술적 방어책이 아니라, 양자 위협을 계기로 오래된 코인의 소유권과 사용처를 다시 정의하려는 정치경제적 제안이 된다.

그러나 이 시나리오의 핵심은 기술이 아니라 정통성이다. 누구나 새로운 규칙을 가진 포크 체인을 만들 수는 있지만, 어떤 포크든 곧바로 비트코인의 정통성을 획득하

는 것은 아니다. 새 체인이 비트코인의 이름과 유동성을 획득하려면 주요 거래소, 커스터디 사업자, 상장지수펀드(Exchange-Traded Fund, ETF) 발행사, 기관투자자, 채굴자, 노드 운영자, 자가 보관 사용자들이 그 체인을 받아들여야 한다. 특히 비트코인이 제도권 금융 안으로 깊이 들어온 이후에는 어느 체인이 ETF의 기초자산으로 인정되는가, 어느 체인이 커스터디 시스템에서 보관 가능한 자산으로 취급되는가, 어느 체인이 주요 거래소에서 BTC 티커를 유지하는가가 시장 선택에 큰 영향을 줄 수 있다.

현물 비트코인 ETF와 같은 제도권 상품은 하드포크 상황에서 어느 네트워크를 신탁 목적상 적절한 네트워크로 볼 것인지에 대한 판단을 스폰서의 재량에 맡기는 조항을 둘 수 있다. 예컨대 블랙록(BlackRock)의 아이셰어즈 비트코인 트러스트(iShares Bitcoin Trust) ETF의 투자설명서는 비트코인 네트워크의 하드포크가 발생할 경우, 신탁 계약이 허용하는 범위에서 스폰서가 신탁 목적상 어떤 네트워크를 적절한 네트워크로 볼지 재량으로 판단할 수 있다고 설명한다.[33] 이는 ETF 스폰서가 비트코인 네트워크의 합의 규칙을 바꿀 수 있다는 뜻은 아니다. 다만 하드포크로 복수의 체인이 병존할 경우, 자신이 운용하는 금융상품 안에서 어느 체인을 신탁 목적상 비트코인으로 취급할지를 결정할 수 있다는 뜻이다. 다시 말해 제도권 상품은 포크 상황에서 단순한 관찰자가 아니라, 특정 체인에 이름과 유동성을 부여하는 선택자가 될 수 있다.

바로 이 지점에서 제도권 하드포크의 정치경제적 의미가 드러난다. 만약 블랙록 같은 대형 금융회사, 주요 거래소, 커스터디 기관, 더 나아가 규제기관과 국가가 세법, 회계 기준, 수탁 규칙, 거래소 규제 등을 통해 특정 포크 체인을 사실상 우대한다면, 상당수 기관투자자와 금융상품은 그 체인을 따라갈 유인을 가질 수 있다. 이 경우 하드포크는 단순한 커뮤니티 내부의 기술 분기가 아니라, 제도권 인프라가 어느 체인에 이름과 유동성을 부여하는가의 문제가 된다. 비트코인의 정통성은 코드 저장소와 개발자 메일링리스트만이 아니라, ETF, 수탁, 회계, 세법, 거래소 상장, 기관 포트폴리오의 언어 속에서도 다투어지게 된다.

하지만 바로 그 지점에서 재분배형 하드포크는 비트코인의 정체성을 가장 날카롭게 흔든다. 제도권 기관들이 특정 포크를 지지한다고 해서 그것이 곧 비트코인 공동체 전체의 합의를 의미하지는 않는다. 자가 보관 사용자, 풀노드 운영자, 채굴자, 기존 개발자 커뮤니티 등이 그 규칙을 받아들이지 않는다면, 새 체인은 기존 비트코인의 연속체가 아니라 제도권이 승인한 별도의 포크 코인으로 남을 수 있다. 제도권은 이름과 유동성의 상당 부분을 움직일 수 있지만, 그것만으로 비트코인의 정통성을 완전히 결정할 수는 없다.

더 근본적인 쟁점은 공공재화라는 명분이 비트코인의 소유권 원칙과 충돌할 수 있다는 데 있다. 이동하지 않은 코인을 공공재로 확보한다는 발상은 로스트 코인과 장기 보유 코인을 외부에서 구별하기 어렵다는 문제를 남긴다. 어떤 코인이 수년 또는 수십 년 동안 움직이지 않았다고 해서 그것이 반드시 분실된 코인이라고 단정할 수는 없다. 그것은 장기 보유자의 자산일 수 있고, 상속을 기다리는 자산일 수 있으며, 정치적·법적·개인적 이유로 이동하지 않은 자산일 수도 있다. 따라서 비트코인 본체의 합의 규칙 안에서 특정 시점까지 이동하지 않았다는 이유만으로 그 코인을 공공재 기금에 편입하려면, 단순한 보안 조치를 넘어 소유권을 다시 판정한다는 정통성

부담을 감수해야 한다.

공공재 기금을 누가 관리할 것인지도 문제다. 그것이 개발자 기금이라면 어떤 개발자가 그 자금을 배분할 것인가. 보안 기금이라면 어떤 채굴자나 검증 인프라에 보상이 돌아갈 것인가. 국가가 관리한다면 비트코인은 다시 주권 권력의 재정 논리 안으로 편입되는 것이 아닌가. 민간 금융기관이 관리한다면 그것은 공공재인가, 아니면 제도권 수탁 인프라가 통제하는 새로운 준비금인가. 이러한 질문이 열리는 순간, 비트코인은 다시 신뢰해야 할 관리자를 필요로 하는 체계로 이동한다.

따라서 재분배형 하드포크는 양자 공격의 위험을 제도적으로 통제하려는 강력한 시나리오인 동시에, 비트코인의 검열 저항성, 소유권 불가침, 공급 규칙, 그리고 정통성의 원천을 가장 날카롭게 시험하는 선택지다. 그것은 로스트 코인을 공공재로 바꾸자는 제안처럼 보이지만, 실제로는 '누가 로스트 코인을 판정할 수 있는가', '누가 비트코인의 이름을 결정할 수 있는가', '누가 움직이지 않는 자산을 다시 배분할 권한을 갖는가'라는 질문을 불러온다. 이 질문은 기술만으로 답할 수 없다. 그것은 비트코인이 제도권 금융과 국가 권력의 언어 속에서 재정의될 것인지, 아니면 자가 보관 사용자와 풀노드 운영자를 포함한 분산된 참여자들의 선택 속에서 자신의 정통성을 유지할 것인지의 문제와 연결된다.

맺음말

양자컴퓨터 문제는 비트코인의 약점을 드러내는 질문이면서, 동시에 비트코인의 본질을 다시 확인하게 만드는 질문이다.

비트코인의 발행량 상한은 2,100만 개로 고정되어 있고, 반감기 일정은 예측 가능하며, 중앙은행이나 정부처럼 통화 규칙을 재량적으로 조정하는 기관도 없다. 이 예측 가능성은 비트코인이 장기적 신뢰를 획득한 중요한 이유다. 화폐의 규칙이 쉽게 바뀐다면, 누구도 그것을 장기적인 가치 저장 수단으로 신뢰하기 어렵다.

그러나 비트코인의 불변성은 코드의 모든 내용이 영원히 고정되어 있다는 뜻이 아니다. 비트코인은 이미 여러 차례 업그레이드되어 왔고, 앞으로도 새로운 위협에 대응하기 위해 변화해야 할 수 있다. 중요한 것은 변화의 여부가 아니라 변화의 방식이다. 코드의 일부는 시대의 위협에 따라 바뀔 수 있지만, 그 변화가 정당성을 얻으려면 공개적 검증, 자발적 채택, 분산된 합의라는 절차를 통과해야 한다. 비트코인의 불변성은 아무것도 바뀌지 않는다는 뜻이 아니라, 합의 없이는 아무도 규칙을 바꿀 수 없다는 뜻이다.

암호 체계가 실제로 무력화되는 상황이 온다면, 기존 규칙을 그대로 유지하는 것이 오히려 시스템 전체를 위험에 빠뜨릴 수 있다. 소유권을 보호하기 위해 만들어진 서명 규칙이 더 이상 소유권을 안전하게 보호하지 못한다면, 그 규칙을 조정하는 일은 원칙의 포기가 아니라 원칙을 지키기 위한 변화가 될 수 있다. 이 점에서 양자 내성 전환은 비트코인의 불변성과 충돌하는 것이 아니라, 불변성을 지속시키기 위해 필요한 진화다.

다만 모든 변화가 같은 정당성을 갖는 것은 아니다. 새로운 서명 체계와 주소 형식의 도입은 보안을 강화하는 업그레이드로 받아들여질 수 있다. 하지만 움직이지 않는 코인의 처리, 하드포크, 제도권의 체인 선택, 공공재화의 시도는 더 깊은 질문을 불러온다. 그것은 단순히 어떤 기술을 채택할 것인가의 문제가 아니라, 누가 소유권을 판정할 수 있는가, 누가 비트코인의 이름을 결정할 수 있는가, 어떤 절차를 거친 변화가 정당한 변화인가의 문제다.

따라서 양자컴퓨터가 제기하는 근본적인 질문은 비트코인이 자신의 원칙을 훼손하지 않으면서도 필요한 변화를 감당할 수 있는가다. 바꿔야 할 것은 바꿀 수 있어야 한다. 그러나 아무도 임의로 바꿀 수 없어야 한다. 그 긴장, 곧 변화 가능성과 임의 변경 불가능성 사이의 균형 위에서 비트코인의 다음 시간이 결정될 것이다.

주

1. Matt Clinch, “Bitcoin Hacked: Price Stumbles After Buying Frenzy,” CNBC, April 4, 2013, accessed February 28, 2026, https://www.cnbc.com/2013/04/04/bitcoin-hacked-price-stumbles-after-buying-frenzy.html

2. Yoshifumi Takemoto and Sophie Knight, “Mt. Gox Files for Bankruptcy, Blames Hackers for Losses,” Reuters, February 28, 2014, accessed March 13, 2026, https://www.voanews.com/a/reu-mt-gox-files-for-bankruptcy-blames-hackers-for-losses/1861341.html

3. Stan Higgins, “The Bitfinex Bitcoin Hack: What We Know (and Don’t Know),” CoinDesk, August 4, 2016, accessed February 28, 2026, https://www.coindesk.com/markets/2016/08/03/the-bitfinex-bitcoin-hack-what-we-know-and-dont-know

4. 비트코인 프로토콜의 핵심 암호학이나 합의 체계가 외부 공격으로 붕괴하여 네트워크 차원에서 자산 탈취가 확정된 사례는 없다. 다만 코드 수준의 치명적 취약점이 발견된 적은 있다. 2010년 8월, 정수 오버플로우 버그를 이용한 거래가 블록 74,638에 포함되면서 약 1,844억 개의 비트코인이 생성되었으나, 개발자들은 신속히 수정 버전을 배포했고 네트워크는 해당 블록이 포함된 분기를 버리고 정상 체인으로 재조정했다. 2018년에는 CVE-2018-17144가 공개되었는데, 이는 중복 입력 처리를 악용해 노드를 중단시키는 서비스 거부(DoS) 공격과, 더 심각하게는 인플레이션을 유발할 수 있는 취약점을 포함했다. 다행히 수정 릴리스가 공개되며 문제가 발생하기 전에 대응이 이루어졌다. 이 두 사건은 비트코인이 완전무결한 시스템은 아니라는 사실과 함께, 오픈소스 합의 프로토콜이 취약점을 발견하고 봉합하며 스스로를 갱신해 온 방식 자체를 보여준다.
“Bitcoin Block 74,638,” Blockchain.com Explorer, mined August 15, 2010, https://www.blockchain.com/explorer/blocks/btc/74638.
Bitcoin Core, “Disclosure of CVE-2018-17144,” September 20, 2018, https://bitcoincore.org/en/2018/09/20/notice.

5. 엄밀히 말하자면, 비트코인에서 유효한 개인키는 secp256k1이 허용하는 일정한 범위 안의 숫자들이며, 그 개수는 2^{256}보다 약간 작다. 다만 그 차이는 전체 규모에 비하면 무시할 수 있을 만큼 작으므로, 2^{256}로 근사해도 큰 무리는 없다.

6. 2021년 탭루트(Taproot) 업그레이드 이후 비트코인은 탭루트 출력에서 슈노르(Schnorr) 서명을 사용할 수 있게 되었다. 이 서명 역시 기존 ECDSA와 마찬가지로 secp256k1 타원곡선 위에서 작동하는 ECC 기반 서명 방식이므로, 양자 위협에 대해서도 같은 계열의 취약성을 공유한다.

7. Peter W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” in Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS, 1994), 124–34, https://doi.org/10.1109/SFCS.1994.365700.

8. Shor, “Algorithms for Quantum Computation,” 124–34.

9. Lov K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” in Proceedings of the 28th Annual ACM Symposium on Theory of Computing (1996), 212–19, https://doi.org/10.1145/237814.237866.

10. Jay Gambetta, “The Hardware and Software for the Era of Quantum Utility Is Here,” IBM Quantum Research Blog, December 4, 2023, accessed May 21, 2026,

https://www.ibm.com/quantum/blog/quantum-roadmap-2033.

11. Ryan Mandelbaum et al., “How IBM Will Build the World’s First Large-Scale, Fault-Tolerant Quantum Computer,” IBM Quantum Research Blog, June 10, 2025, accessed May 21, 2026, https://www.ibm.com/quantum/blog/large-scale-ftqc.

12. Hartmut Neven, “Meet Willow, Our State-of-the-Art Quantum Chip,” Google Blog, December 9, 2024, accessed February 28, 2026, https://blog.google/technology/research/google-willow-quantum-chip.

13. Catherine Bolgar, “Microsoft’s Majorana 1 Chip Carves New Path for Quantum Computing,” Microsoft Source, February 19, 2025, accessed May 21, 2026, https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing.

14. Kevin Williams, “What Google's Quantum Computing Breakthrough Willow Means for the Future of Bitcoin and Other Cryptos,” CNBC, December 22, 2024, accessed February 28, 2026, https://www.cnbc.com/2024/12/22/what-google-quantum-chip-breakthrough-means-for-bitcoins-future.html.

15. Mark Webber, Vincent Elfving, Sebastian Weidt, and Winfried K. Hensinger, “The Impact of Hardware Specifications on Reaching Quantum Advantage in the Fault Tolerant Regime,” AVS Quantum Science 4, no. 1 (2022): 013801, https://doi.org/10.1116/5.0073075.

16. John Preskill, “Quantum Computing in the NISQ Era and Beyond,” Quantum 2 (2018): 79, https://doi.org/10.22331/q-2018-08-06-79.

17. National Institute of Standards and Technology, “NIST Releases First 3 Finalized Post-Quantum Encryption Standards,” August 13, 2024, accessed May 21, 2026, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

18. Kris Kwiatkowski and Luke Valenta, “The TLS Post-Quantum Experiment,” Cloudflare Blog, October 30, 2019, accessed May 21, 2026, https://blog.cloudflare.com/the-tls-post-quantum-experiment.

19. Apple Security Engineering and Architecture, “iMessage with PQ3: The New State of the Art in Quantum-Secure Messaging at Scale,” Apple Security Research Blog, February 21, 2024, accessed May 21, 2026, https://security.apple.com/blog/imessage-pq3.

20. Michael Osborne, Katia Moskvitch, and Jennifer Janechek, “NIST’s Post-Quantum Cryptography Standards Are Here,” IBM Research Blog, August 13, 2024, accessed May 21, 2026, https://research.ibm.com/blog/nist-pqc-standards.

21. Zoom, “Zoom Bolsters Security Offering with the Inclusion of Post-Quantum End-to-End Encryption in Zoom Workplace,” Zoom News, May 21, 2024, accessed May 21, 2026, https://news.zoom.com/post-quantum-e2ee.

22. “Bitcoin Development Mailing List,” Google Groups, accessed May 22, 2026, https://groups.google.com/g/bitcoindev.

23. BIP-141은 증인(witness) 데이터를 거래 유효성 검증에 필요한 별도 데이터 구조로 정의하고, 서명과 스크립트 데이터를 이 구조로 이동시킨다. 증인 데이터는 별도의 증인 머클 트리로 묶여 코인베이스 거래 안의 증인 커밋먼트(witness commitment)를 통해 블록에 커밋된다. 세그윗 이후 블록 용량은 ‘블록 무게(block weight)’로 계산되며, 비증인 데이터는 1바이트당 4무게 단위(weight units, WU), 증인 데이터는 1바이트당 1WU로 계산된다. 블록 무게 한도는 4,000,000WU다.
Eric Lombrozo, Johnson Lau, and Pieter Wuille, “BIP 141: Segregated Witness

(Consensus Layer),” Bitcoin Improvement Proposals, GitHub, assigned December 21, 2015, accessed May 22, 2026, https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki.

24. 세그윗은 또한 서명 데이터가 거래 식별자에 영향을 미치던 구조를 바꾸어 거래 가변성(transaction malleability) 문제를 완화하는 효과도 가져왔다. 거래 가변성이란 거래의 실질적 내용은 바꾸지 않으면서도 서명 데이터 등을 조작해 거래 식별자(transaction ID, txid)를 달라지게 만들 수 있는 문제를 말한다. 거래 식별자가 바뀌면 아직 확정되지 않은 거래를 기준으로 이어지는 후속 거래나 결제 확인 과정에 혼란이 생길 수 있기 때문에, 이를 완화한 것은 이후 확장성 기술의 기반을 마련했다는 의미를 가진다.

25. 탭루트 업그레이드는 BIP-340, BIP-341, BIP-342에 나뉘어 정리되어 있다. BIP-340은 secp256k1 위에서 작동하는 64바이트 슈노르 서명을 표준화했고, BIP-341은 탭루트를 세그윗 버전 1 출력으로 정의했으며, BIP-342는 탭루트 지출 경로에서 사용되는 탭스크립트(Tapscript)의 검증 규칙을 정리했다.
Pieter Wuille, Jonas Nick, and Tim Ruffing, “BIP 340: Schnorr Signatures for secp256k1,” Bitcoin Improvement Proposals, GitHub, assigned January 19, 2020, accessed May 22, 2026, https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki.
Pieter Wuille, Jonas Nick, and Anthony Towns, “BIP 341: Taproot: SegWit Version 1 Spending Rules,” Bitcoin Improvement Proposals, GitHub, assigned January 19, 2020, accessed May 22, 2026, https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki.
Pieter Wuille, Jonas Nick, and Anthony Towns, “BIP 342: Validation of Taproot Scripts,” Bitcoin Improvement Proposals, GitHub, assigned January 19, 2020, accessed May 22, 2026, https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki.

26. Hunter Beast, Ethan Heilman, and Isabel Foxen Duke, “BIP 360: Pay-to-Merkle-Root (P2MR),” Bitcoin Improvement Proposals, GitHub, assigned December 18, 2024, accessed May 22, 2026, https://github.com/bitcoin/bips/blob/master/bip-0360.mediawiki.

27. P2MR의 데이터 크기 증가는 주로 탭루트의 가장 단순한 키 경로 지출과 비교할 때 발생한다. 반대로 같은 스크립트 경로 지출끼리 비교하면, P2MR은 내부 공개키를 포함하지 않으므로 동등한 탭루트 스크립트 경로 지출보다 작아질 수 있다. 즉 P2MR의 비용 증가는 비교 기준에 따라 달라진다. 핵심은 공개키 장기 노출 위험을 줄이는 대신 일부 지출 방식에서 블록 공간 부담이 커질 수 있다는 데 있다.

28. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt, “Committing to Quantum Resistance: A Slow Defence for Bitcoin against a Fast Quantum Computing Attack,” Cryptology ePrint Archive, Paper 2018/213, 2018, accessed May 22, 2026, https://eprint.iacr.org/2018/213.

29. 이 수치는 확정된 사실이라기보다 블록 패턴 분석에 근거한 추정이다. 사토시의 정확한 보유량과 해당 코인의 실제 소유 상태를 확정할 방법은 없다.

30. BitMEX Research, “Mitigating The Impact of The Quantum Freeze,” BitMEX Blog, February 9, 2026, accessed May 22, 2026, https://www.bitmex.com/blog/Mitigating-The-Impact-Of-The-Quantum-Freeze.

31. Marek Palatinus, Pavol Rusnak, Aaron Voisine, and Sean Bowe, “BIP 39: Mnemonic Code for Generating Deterministic Keys,” Bitcoin Improvement Proposals, GitHub, assigned September 10, 2013, accessed May 22, 2026, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki.
BIP-39는 결정론적 지갑(deterministic wallet)을 생성하기 위한 니모닉 코드(mnemonic code) 또는 니모닉 문장(mnemonic sentence)의 구현 방식을 설명한다. 이 방식에서 사람이 기억하거나 기록하기 쉬운 단어들의 조합은 이후 지갑의 시드(seed)를 생성하는 데 사용된

다.

32. Ethereum Foundation, “Hard Fork Completed,” Ethereum Foundation Blog, July 20, 2016, accessed May 23, 2026, https://blog.ethereum.org/2016/07/20/hard-fork-completed.

33. iShares Bitcoin Trust ETF, Prospectus, July 31, 2025, as supplemented November 21, 2025, accessed May 23, 2026, https://www.ishares.com/us/literature/prospectus/p-ishares-bitcoin-trust-12-31.pdf.

비트코인은 양자컴퓨팅 시대에도 살아남을 수 있는가

양자 위협과 비트코인 보안의 진화

Researchers

김연경 *Yonkyung Kim*

손혜민 *Hyemin Son*

Corresponding Author

오태민 *Taemin Oh*

Editorial Designer

윤성아 *Seongah Youn*

Contact

손혜민 hyeomin0109@gmail.com