한화투자증권

2026년 4월 1일
디지털자산

RWA Weekly

양자 리스크, 시장은 '합의 능력'을 평가한다

▶ Analyst 최윤영 yy.choy@hanwha.com 3772-7402

구글이 최근 연구를 통해 양자컴퓨터가 기존 예상보다 훨씬 적은 자원으로 ECC 를 해독할 수 있음을 보여주며, 양자 리스크가 '이론'에서 '준비 단계'로 이동했음을 시사했습니다. 다만 CRQC 는 여전히 기술적 장벽이 높아 단기적인 시스템 붕괴 가능성은 낮고, 암호체계에 대한 영향도 점진적으로 확대되는 구조로 보는 것이 타당합니다. 비트코인은 퍼블릭 키 노출 여부에 따라 일부 자산이 직접적인 취약 영역에 해당될 수 있는 반면, 이더리움은 스마트컨트랙트와 생태계 구조로 인해 보다 광범위한 시스템 리스크를 내포합니다. 결국 핵심 변수는 각 네트워크의 PQC 전환 속도와 합의 형성 능력이며, 이에 따라 향후 리스크 프리미엄이 차별화될 가능성이 높습니다.

양자컴퓨팅, 이론적 위협에서 현실 준비 단계로

구글은 최근 연구를 통해 양자컴퓨터가 암호화폐 보안의 핵심인 ECC(Elliptic Curve Cryptography)를 기존 예상보다 훨씬 적은 자원으로 해독할 수 있음을 제시했다. 특히 ECDLP-256 문제를 해결하는 데 필요한 자원이 크게 감소하며, 과거 대비 약 20배 수준의 효율 개선이 이루어진 것으로 나타났다. 이는 양자컴퓨팅 기반 암호 해독이 상용화까지는 여전히 시간이 필요하지만, 기술적 진입 장벽이 빠르게 낮아지고 있음을 시사한다.

이와 함께 구글은 PQC(Post-Quantum Cryptography) 전환 목표 시점을 기존 대비 앞당겨 2029년까지 완료할 것을 권고하였고, 양자 리스크 대응이 '장기 과제'에서 '준비 단계'로 이동하고 있음을 명확히 했다. 이는 기존 NIST 기준(2030년 취약 알고리즘 폐기, 2035년 완전 전환) 대비 상당히 앞선 일정으로, 산업 전반의 대응 속도를 끌어올리는 신호로 해석된다.

다만 비트코인의 암호를 실질적으로 위협할 수준의 CRQC(Cryptographically Relevant Quantum Computer)는 여전히 오류 보정과 시스템 안정성 측면에서 기술적 장벽이 존재한다. 이에 따라 CRQC는 여전히 훨씬 더 이후 단계에서 현실화될 가능성이 높으며, 현재 시점에서 즉각적인 시스템 붕괴를 우려할 단계는 아니다. 양자컴퓨팅 발전은 비선형적이지만 단계적으로 이루어지며, 이에 따라 암호체계에 대한 영향도 점진적으로 확대될 가능성이 높다. 즉, 단일 임계점에서의 급격한 붕괴보다는 대응 가능한 시간적 여유가 존재하는 구조로 보는 것이 타당하다.

비트코인 보안 구조의 취약 지점과 현실적 리스크 범위

비트코인의 보안은 해시 함수(Hash Function)와 ECC 두 축으로 구성되며, 이 중 ECC는 양자컴퓨터에 상대적으로 취약한 영역이다. 특히 퍼블릭키가 노출되는 구조에서는 양자 알고리즘(Shor's algorithm)을 통해 프라이빗키 역산 가능성이 존재한다. 이러한 리스크는 구글 연구에서 보다 구체적으로 세분화되는데, 거래 전송 과정에서 퍼블릭키가 노출되는 순간을 노리는 'on-spend 공격', 이미 퍼블릭키가 온체인에 노출된 지갑을 대상으로 하는 'at-rest 공격', 그리고 프로토콜 초기 설정값을 복구하는 'on-setup 공격'으로 구분된다. 이 중 특히 at-rest 공격은 퍼블릭키가 이미 노출된 자산을 시간 제약 없이 공격할 수 있다는 점에서 현실적 위험도가 높고, 초기 P2PK(Pay-to-Public-Key) 주소 등 퍼블릭키가 노출된 구조를 기준으로 약 230만 BTC 규모의 자산이 직접적인 양자 취약 영역에 해당하는 것으로 분석된다.

다만 모든 비트코인이 동일한 수준의 리스크에 노출된 것은 아니다. 최신 주소 체계(P2PKH, SegWit 등)는 퍼블릭키가

즉시 노출되지 않는 구조를 갖고 있어 상대적으로 안전성이 높으며, 사용자가 자산을 새로운 주소로 이동시키는 방식으로 일정 수준 대응이 가능하다. 구글 역시 단기 대응 방안으로 주소 재사용 최소화 등 보안 관행 개선을 제시하고 있다.

이더리움: 스마트컨트랙트가 결합된 시스템 리스크

이더리움의 양자 리스크는 네트워크 전반으로 확장될 수 있다. 우선 이더리움은 한 번 거래가 발생하면 퍼블릭키가 바로 공개되는 구조를 갖고 있어, 주요 지갑이 지속적으로 공격 대상이 될 수 있다. 여기에 더해 스마트컨트랙트의 관리자 계정은 자금 이동이나 시스템 변경까지 가능한 '핵심 통제 권한'을 갖고 있어 리스크의 범위가 훨씬 넓다. 또한 레이어2, 브리지, 디파이(DeFi) 등 현재 이더리움 생태계의 주요 서비스들은 기존 암호 방식에 의존하고 있어, 양자 공격이 현실화될 경우 일부 영역이 아니라 여러 영역이 동시에 영향을 받을 가능성이 있다. 특히 데이터 검증 구조 중 일부는 한 번 취약점이 노출될 경우 이후에도 반복적으로 악용될 수 있는 성격의 리스크가 존재한다는 점에서 리스크가 더 크다.

이러한 구조적 리스크에 대응하기 위해 이더리움 재단은 양자내성 서명 체계 도입을 포함한 단계적 대응 방향을 제시하고 있으며, 특히 계정 추상화(Account Abstraction)를 기반으로 다양한 서명 알고리즘으로의 전환이 가능하도록 설계 유연성을 확보하는 접근을 취하고 있다. 다만 이미 배포된 스마트컨트랙트, 브리지, 레이어2 네트워크는 개별적으로 업그레이드가 필요하다는 점에서, 단일 프로토콜 변경만으로 해결되기 어렵고 생태계 전반의 점진적 마이그레이션이 요구된다는 한계가 존재한다.

PQC 전환: 기술 문제가 아니라 '합의의 문제'

양자컴퓨팅 리스크에 대한 근본적 대응은 PQC(Post-Quantum Cryptography)로의 전환이다. 이는 이미 글로벌 인터넷 인프라 전반에서 개발 및 적용이 진행 중이며, 블록체인 역시 동일한 방향으로 전환이 가능하다. 비트코인의 경우 소프트포크 등을 통해 PQC 기반 서명 체계 도입이 기술적으로 가능하다는 점에서 해결 불가능한 문제는 아니다.

다만 핵심 제약은 기술이 아니라 네트워크 구조에 있다. 비트코인은 탈중앙화된 합의 기반 네트워크라는 특성상 업그레이드가 느리고, PQC 도입 과정에서 서명 크기 증가, 검증 비용 상승 등 성능 저하와 보안 강화 간 트레이드오프가 존재한다. 특히 기존 취약 주소에 남아 있는 비트코인을 어떻게 처리할 것인지(이동 유도, 동결 등)는 향후 중요한 논쟁 포인트로 남아 있다.

이더리움은 더 복잡하다. 기본 프로토콜이 PQC로 전환되더라도 이미 배포된 스마트컨트랙트, 브리지, 레이어2 네트워크는 각각 개별적으로 업그레이드를 수행해야 한다. 즉, 단일 체인 업그레이드로 해결되지 않는 문제가 있으며, 이는 실제 전환 난이도를 높이는 요인이다.

핵심은 '언제 깨질 것인가'가 아니라 '전환이 가능한가'

양자컴퓨팅은 디지털자산 시장에서 처음으로 등장한 '순수 기술 리스크'지만, 그 성격은 단기 충격보다는 중장기 변수에 가깝다. 양자컴퓨팅의 상용화 시점과 암호 해독 능력 확보까지의 경로는 기술 발전의 비선형적 특성으로 인해 예측 불확실성이 높다. 다만, 글로벌 인터넷 인프라 전반이 동일한 위협에 노출돼 있는 만큼 대응 역시 병행적으로 진행될 가능성이 높다.

특히 이번 구글의 연구와 타임라인 조정은 양자 리스크가 개념적 논의를 넘어 실제 대응을 요구하는 단계로 이동하고 있음을 시사한다. 이러한 구조에서는 특정 시점의 기술 돌파보다, 그 이전에 이루어지는 대응 속도와 준비 수준이 더욱 중요한 변수로 작용한다. 향후 시장은 "양자컴퓨터가 언제 등장하는가"보다, 각 네트워크가 PQC 전환 로드맵을 얼마나 명확히 제시하고 실행하는가에 따라 리스크 프리미엄이 차별화될 가능성이 높다.

[Compliance Notice] (공표일: 2026 년 4 월 1 일)

이 자료는 조사분석 담당자가 객관적 사실에 근거해 작성하였으며, 타인의 부당한 압력이나 간섭없이 본인의 의견을 정확하게 반영했습니다. 본인은 이 자료에서 다룬 종목과 관련해 공표일 현재 관련 법규상 알려야 할 재산적 이해관계가 없습니다. 본인은 이 자료를 기관투자자 또는 제 3 자에게 사전에 제공한 사실이 없습니다. (최윤영)
저희 회사는 공표일 현재 이 자료에서 다룬 종목의 발행주식을 1% 이상 보유하고 있지 않습니다.

[종목 투자등급]

당사는 개별 종목에 대해 향후 1 년간 +15% 이상의 절대수익률이 기대되는 종목에 대해 Buy(매수) 의견을 제시합니다. 또한 절대수익률 -15~+15%가 예상되는 종목에 대해 Hold(보유) 의견을, -15% 이하가 예상되는 종목에 대해 Sell(매도) 의견을 제시합니다. 밸류에이션 방법 등 절대수익률 산정은 개별 종목을 커버하는 애널리스트의 추정에 따르며, 목표주가 산정이나 투자의견 변경 주기는 종목별로 다릅니다.

[산업 투자의견]

당사는 산업에 대해 향후 1 년간 해당 업종의 수익률이 과거 수익률에 비해 양호한 흐름을 보일 것으로 예상되는 경우에 Positive(긍정적) 의견을 제시하고 있습니다. 또한 향후 1 년간 수익률이 과거 수익률과 유사한 흐름을 보일 것으로 예상되는 경우에 Neutral(중립적) 의견을, 과거 수익률보다 부진한 흐름을 보일 것으로 예상되는 경우에 Negative(부정적) 의견을 제시하고 있습니다. 산업별 수익률 전망은 해당 산업 내 분석대상 종목들에 대한 담당 애널리스트의 분석과 판단에 따릅니다.

[당사 조사분석자료의 투자등급 부여 비중] (기준일: 2026 년 3 월 31 일)

투자등급	매수	중립	매도	합계
금융투자상품의 비중	90.7%	9.3%	0.0%	100.0%