구글, 암호화폐 암호 공격에 필요한 QC 자원 감소 가능성 제시

(2026.04.20., 양자정보연구지원센터)

□ 구글, 양자컴퓨터 기반 암호화폐 공격 자원 감소 가능성 제시

○ 기존 대비 훨씬 적은 자원으로 암호 해독 가능성 제기, 보안 전환 필요성 부각

- 타원곡선암호(ECC) 해독에 필요한 큐비트·연산량 대폭 감소
- 실질적 위협 수준의 양자컴퓨터 도달 시점이 앞당겨질 가능성

○ 양자 알고리듬 및 기술적 진전

- 최적화된 쇼어 알고리즘 적용으로 자원 요구량 약 10배 감소
- 약 1,200개 논리 큐비트 및 수천만 회 연산으로 문제 해결 가능
- 약 50만 개 이하 물리 큐비트로 수 분 내 공격 수행 가능성 제시

○ 암호화폐 및 블록체인 보안 영향

- 대부분 블록체인이 ECC 기반으로 구조적 취약성 내포
- 거래 중 공격(on-spend) 및 지갑 대상 공격(at-rest) 시나리오 존재
- 스마트컨트랙트·지분증명 등으로 공격 표면 확대

○ 양자컴퓨터 아키텍처별 위협 차이

- **초전도·광자 기반은 빠른 실시간 공격 가능성**
- 이온트랩·중성원자 방식은 장기 노출 지갑 공격에 유리

○ 대응 방안 및 보안 전략

- 양자내성암호(PQC)로의 전환이 근본적 해결책
- 공개키 노출 최소화, 주소 재사용 금지 등 단기 대응 필요

- 블록체인 전체 전환은 기술·거버넌스 측면에서 복잡

ㅇ 장기적 리스크 요인

- 장기간 미사용 지갑(휴면 자산) 보호 어려움
- 이미 공개키가 노출된 자산은 업그레이드 불가
- 상당량의 암호화폐가 잠재적 공격 대상

ㅇ 연구 공개 방식 및 특징

- 제로지식증명 활용한 책임 있는 공개 방식 채택
- 공격 방법은 공개하지 않고 결과 검증 가능하도록 설계
- 과장·과소평가 모두 위험하다는 점 강조

ㅇ 향후 전망

- 양자컴퓨팅 발전과 알고리즘 개선으로 위협 격차 지속 축소
- 즉각적 위험은 아니나 대응 준비 기간 단축
- 기술·산업·정책 간 협력 통한 선제 대응 필요

ㅇ 결론

- 암호화폐 생태계 신뢰 유지를 위해 조기 대응 필수
- 양자시대 대비 보안 전환이 디지털 경제 핵심 과제로 부상

(원문)

1. https://thequantuminsider.com/2026/03/31/google-suggests-quantum-attacks-on-cryptocurrency-encryption-may-require-fewer-resources/