Quantum Guard

퀀텀가드 퀀텀월렛

Software Hardware

Hybrid-based Wallet for Emerging Digital Assets & Custody Service

기술백서 인포그래프 자료

서비스 문의
service@QuantumGuard.co.kr

ChosunBiz

국제 경제 >

바이비트 해킹으로 2조원대 이더리움 도난… "北 라자루스 소행 추정"

김남희 기자

업데이트 2025.02.22. 15:34

세계 최대 가상화폐 거래소 중 한 곳인 바이비트(Bybit)가 해킹을 당해 15억달러(약 2조1500억원) 규모 가상화폐를 탈취당했다. 역대 가상화폐 탈취 중 최대 규모다.

바이비트는 22일 웹사이트에 공지를 올려 "21일 일상적인 이체 과정 중 이더리움 콜드 월렛(온라인에 연결되지 않은 오프라인 가상화폐 지갑) 중 하나에서 이상 행위를 발견했으며, 40만개의 이더리움과 에스티이더리움(stETH)을 도난당했다"고 밝혔다. 도난당한 가상화폐 가치는 15억달러 이상이라고 밝혔다.

가상화폐 거래소 바이비트(Bybit) 웹사이트에 이더리움 가격이 표시되고 있다. /AP 연합뉴스

바이비트는 "이더리움을 이더리움 멀티시그(ETH Multisig) 콜드 월렛에서 핫 월렛(온라인에 연결된 가상화폐 지갑)으로 옮기던 도중 정교한 공격으로 거래가 조작됐고, 도난된 이더리움 등이 정체불명 주소로 옮겨졌다"고 설명했다.

해킹 사고가 알려진 후 불안을 느낀 사용자들의 인출 행렬이 이어졌다. 벤 저우 바이비트 최고경영자(CEO)는 불안을 잠재우는 차원에서 회수 불가능한 손실을 충당하고 운영을 유지하기 위해 제3의 파트너들로부터 브리지론을 확보했다고 밝혔다.

핵심 키워드

- 피해규모 15억달러
- 멀티시그
- 정교한 공격
- 거래조작

퀀텀월렛의 네이티브 코드 기반 독립실행형 하이브리드 월렛 기술 소개

기술 아키텍처 및 보안 우위성 백서 인포그래프

■ 공동명의 암호화폐 보안 위협 : 사상최대 피해 규모

바이비트 해킹 사례 (2025.02)

- 피해 규모: 2조1천억원 (15억 달러)
- 공격 기법: 크롬 등 브라우저 기반 월렛의 입력 조작 및 원격 서명 변조
- 취약점 : 사회공학적 공격을 통한 멀티시그 승인 프로세스 우회

→ **기존 브라우저 기반 핫월렛 솔루션의 구조적 문제**

■ 기존 월렛 방식과 기술 비교 분석

구분	브라우저 월렛	하드웨어 월렛	퀀텀월렛
원격 공격 차단	취약	부분적	원천 차단
조작 방지	불가능	제한적	물리적 차단
양자컴퓨터 대응	미 대응	미 대응	내성 보장

■ 핵심 보안 기술

멀티레이어 보안

- 네이티브 실행환경
  브라우저 종속성 제거
- 하드웨어 연동 인증
  물리적 보안장치 필수
- 암호학적 무결성
  차세대 암호화 적용

지능형 위협 대응

- 사회공학적 공격 → 차단
- UI/UX 조작 → 차단
- 원격 서명 변조 → 차단
- 키 탈취 시도 → 차단

99% 원천차단

하이브리드 스토리지

- 콜드 스토리지
  오프라인 키 보관
- 핫 액세스
  실시간 거래 처리
- 심리스 연동 : 취약구간 제거
  투명한 보안 처리

■ 기술 혁신 포인트

양자컴퓨터 보안 시대 대비

- Post-Quantum Cryptography 준수
- 하이브리드 보안 모델
- 선제적 대응 체계

→ **미래 위협 완전 대응**

<최고의 공격 차단율 지향>

Zero-Trust 보안 모델

- 모든 거래 물리적 인증 요구
- 네트워크 신뢰 가정 제거
- 다층 검증 시스템

→ **원격 조작 원천 차단**

■ 보안 프로세스 플로우

1 거래 요청 → 2 물리적 인증 → 3 암호화 처리 → 4 서명 완료

조작 차단 보안환경 內
심리스 일괄 처리

□ 원천적 위해 차단

- 원격 조작
- 악성코드 삽입
- 사회공학적 공격
- 서명 변조 시도

■ 경쟁 우위 요약

악성 해킹 기법 원천적 차단 기능 및 구동 환경

- 하이브리드 보안 체계 + 양자내성 암호화 + 네이티브 독립형 실행환경
- 바이비트 해킹에서 핵심이었던 원격 조작 공격 무력화

→ **차세대 가상화폐 솔루션에 높은 보안성으로 새로운 기술적 지향점 제시 및 수익 창출**

퀀텀월렛의 네이티브 코드 기반 독립실행형 하이브리드 월렛 기술 소개
비즈니스 가치 및 시장 기회 인포그래프

■ 시장 기회 및 규모

Grand View Research, CoinGecko, Research & Markets, Future Market Insights 등 다수 시장조사 기관 데이터

글로벌 암호화폐 시장
$3.5T
2024년 기준 시가총액
연 30% 성장률 지속

지갑 보안 시장
$33B
예상 TAM (2025년)
고성장 세그먼트

해킹 피해 규모
$15B
2025년 단일 피해규모
급증하는 위협

■ 비즈니스 가치 제안

□ 비용 절감 효과
보안 침해 리스크 획기적 감소
- 연간 보안 사고 손실 최소화
- 컴플라이언스 비용 획기적 절감

운영 효율성 극대화
- 보안 관리 인력 절약
- 시스템 침해 유지비용 최대 감소

→ **연간 수십억원 비용 절감**

□ 수익 증대 효과
신뢰도 향상을 통한 고객 유치
- 보안 우위 마케팅 효과
- 기관 투자자 신뢰 확보

프리미엄 보안 서비스 제공
- 고수익 고객층 타겟
- 새로운 수익 모델 창출

→ **매출 증익에 효과적 기여**

□ 경쟁 우위 확보
기술 특허 및 IP 확보
- 핵심 원천기술 보유
- 시장 진입 장벽 구축

시장 선점 리더십
- 글로벌 스탠다드 제시
- 업계 표준화 주도

→ **시장 지배력 향상에 기여**

■ 타겟 시장 분석

Primary Target Market
암호화폐 거래소
- 대형 자산 보관 및 멀티시그 운영 • 해킹 위험 최소화

기관 투자자
- 법인 공동 디지털 자산 관리 • 실제적 고수준 보안 충족

DeFi 프로토콜
- 스마트컨트랙트 기반 자금 운용

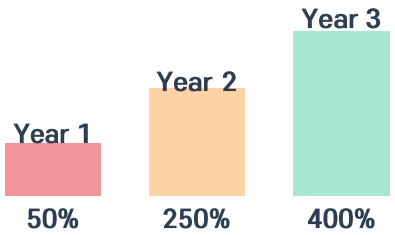
Secondary Market
개인 투자자 (고액 자산)
- 프리미엄 보안 서비스 선호층

기업 디지털 자산관리
- 디지털 자산 포트폴리오 관리

정부 기관
- 공인 디지털 화폐 인프라

■ 투자 수익률 분석

(자사 임의 상계)



투자 수익률 예측
- 초기 개발 및 IP 역량 확보: 1년차 50% ROI
- 시장 확장 및 파트너십: 2년차 250% ROI
- 글로벌 스케일링: 3년차 400% ROI

핵심 성공 요인
- 해킹에 강인한 디지털 자산 지킴이로 시장 신뢰도 확보
- 양자내성 기술로 미래적 보안 가치 실현

■ 파트너십 전략

기술 제휴
- 블록체인 인프라 제공업체 통합
- 보안 솔루션 업체 상호 연동
- 학술기관 연구개발 협력
- 디지털자산 보안 기구 참여

사업 협력
- 거래소 및 핀-테크 기업 JV
- 시스템 통합업체 채널 파트너십
- 글로벌 진출 현지 파트너 발굴
- 정부기관 보안 솔루션 포괄적 수주

투자 유치
- 블록체인 특화 VC 투자
- 정부 매칭 R&D 프로젝트
- 전략적 투자자 참여
- SERIES 포지션을 위한 준비

■ 핵심 성과 지표

□ 3년 내 달성 목표
- 시장점유율 15% 달성 • 연매출 최소 200억원 돌파 • TOP 글로벌 거래소와 전략적 파트너-쉽 추진
- 세계 시장 고객의 디지털 자산 방어율 목표 달성 • 양자내성 암호화 인증 획득 • 글로벌 시장 진출

→ **지속적 기술우위를 제공하는 차별화된 블록체인 보안 솔루션의 리더로 도약**