

디지털자산 거래 보안솔루션 구축 전문기업

퀀텀가드는 차세대 디지털자산 보안 및
블록체인 인프라 솔루션 서비스를 제공하는 개발전문기업 입니다.



기술성

퀀텀 내성 기암호화
기술과 다중-서명 지갑
시스템, 하이브리드
보안 아키텍처를 자체
개발하였습니다.



커스터마이징

고객의 다양한 디지털자산
비즈니스 요구사항에
최고의 보안성이 보장되는
맞춤형 솔루션을
제공합니다.



서비스 개발 문의



네트워크
보안컨설팅



업무제휴/의뢰

퀀텀가드 퀀텀월렛
Software Hardware
Hybrid-based Wallet for Emerging Digital Assets
& Custody Service



service@QuantumGuard.co.kr

암호화폐 RISKS

암호화폐의 거래는
다음과 같은 위험성이 있습니다 :

해커 위험



해커들은 공개된 암호화폐 거래 기록을 바탕으로 개인 정보를 탈취합니다.

암호화폐 거래와 관련된 IP 주소나 물리적인 컴퓨터 위치가 노출될 수 있으며, 개인 키(private key)를 저장하고 있는 웹 단말기는 해커의 우선적 공격 대상이 될 수 있습니다.

사이버 스캠



각국의 정부는 암호화폐 계정을 보험으로 보호하지 않습니다. 한국과 미국 모두 마찬가지입니다. 만약 암호화폐 거래소가 파산하더라도, 정부는 소비자의 손실을 보상하지 않습니다.

사이버 스캠



악의적 해커들은 다양한 사기 수법을 사용하고 있습니다.

가짜 코인을 만들어 막대한 피해를 입히고
가짜 지갑 주소로 자산을 가로챍니다
가짜 지갑 주소로 북한은 다중-서명

지갑에서 '25년 2월 2조원을 탈취했습니다

모바일버전
(개발중)

NO CLOUD



강화된 보안 커널

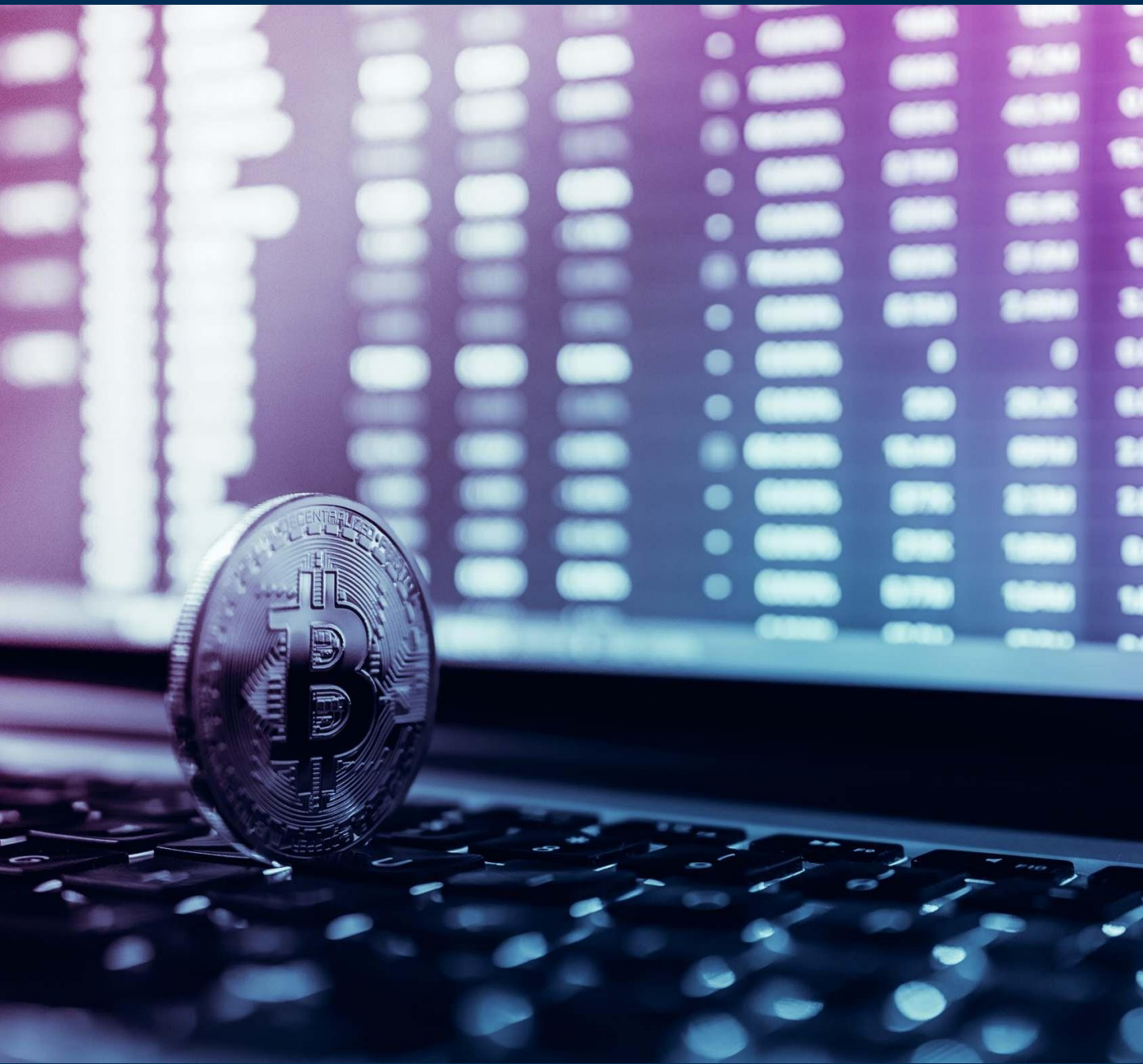
제로트러스트 아키텍처

전용 안드로이드OS

최고수준의 보안성



암호화폐/디지털자산은 보안이 생명입니다



Quantum
 Guard

KOREA'S FIRST

퀀텀가드 퀀텀월렛

Software Hardware

Hybrid-based Wallet for Emerging
Digital Assets & Custody Service

2025

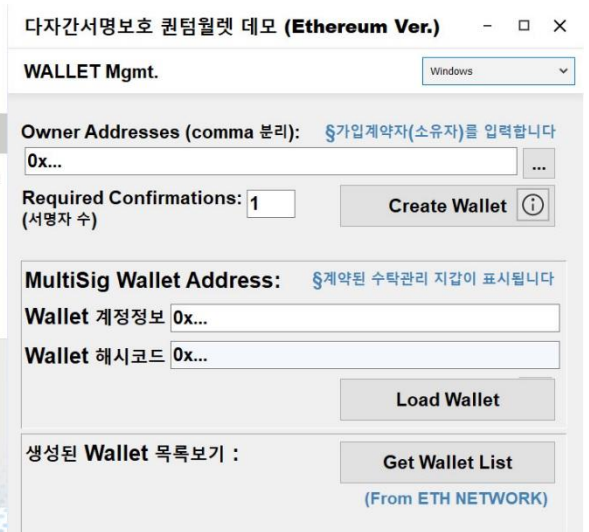
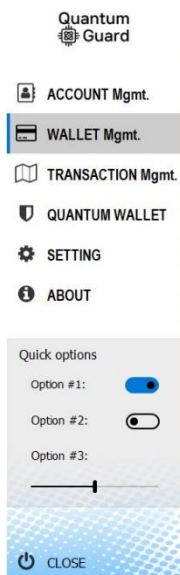
퀀텀가드 퀀텀월렛

Software Hardware

Hybrid-based Wallet for Emerging Digital Assets & Custody Service



국내 최초로 소프트웨어 핫 월렛과 하드웨어 콜드 월렛을
통합하여 美 NIST 양자내성 기암호화 기술을 적용한
“퀀텀월렛”을 소개합니다



Key Features of Quantum Wallet Architecture

이더리움 암호화폐용 퀀텀월렛 솔루션

<핵심 기능>

제품	주요 특징	고객 혜택
퀀텀가드 하드웨어 보안 지갑	물리적으로 분리된 USB 기반 저장장치	해킹으로부터 디지털 자산 완벽 보호
웹3 다중서명 관리 플랫폼	직관적인 웹 인터페이스로 다중 승인 관리	공동계약자 개별 실수나 보안 사고에 대한 자산 손실 방지
미래 양자컴퓨터 대비 솔루션	최신 양자내성 암호화 기술 적용	미래 컴퓨팅 위협 기술에도 안전한 자산 보호

<하드웨어 보안 지갑 기능>

기능	설명	사용자 이점
원클릭 디바이스 감지	하드웨어 USB키 연결 시 자동 인식 및 상태 표시	간편한 연결과 즉각적인 사용 가능
자동 백업 & 복원	지갑 정보 자동 백업 및 간편 복구	데이터 손실 걱정 없는 안심 사용
암호화된 자산 정보 저장	모든 정보는 강력한 암호화 저장	디바이스 분실해도 자산 안전 보장
QR코드 키 추출	필요시 보안 키를 QR코드로 저장(페이퍼월렛기능)	네트워크 없이도 정보 이전 가능
하이브리드 모듈 연동	다른 보안 모듈과 원활한 정보 교환	다양한 시스템과 확장 가능한 호환성

<다중서명 관리 플랫폼 기능>

기능	설명	사용자 이점
스마트 계약 자동 배포	원클릭으로 다중서명 계약 생성	복잡한 기술 지식 없이도 고급 보안 구현
참여자 관리 시스템	다중서명 참여자 쉽게 추가/관리	조직 변화에 유연하게 대응
트랜잭션 상태 모니터링	모든 거래 제안 및 승인 현황 실시간 확인	투명한 자산 관리와 감사 용이성
스마트 서명 확인	승인 조건 자동 검증 및 처리	인적 오류 방지 및 프로세스 자동화
직관적 사용자 인터페이스	복잡한 블록체인 기술을 쉽게 사용	전문가가 아니어도 쉬운 자산 관리

* 전체 기능은 커스터마이징 가능합니다

Key Features of Quantum Wallet Architecture

이더리움 암호화폐용 퀀텀월렛 솔루션

<주요 기술 사양>

구성요소	설명
하드웨어 콜드월렛	USB 기반 오프라인 키 저장 시스템
W3C Web3.0 멀티시그 핫월렛	W3C Web3.0 기반 다중 서명 트랜잭션 처리 시스템
양자내성 암호화 모듈	ML-KEM과 AES-256을 결합한 하이브리드 암호화 시스템

<W3C Web3.0 멀티시그 퀀텀월렛 기술 사양>

기능	기술 상세
UX 프레임워크	Google Chrome / Microsoft Edge
블록체인 연동	JavaScript 웹3 상호운용 표준
네트워크 지원	Ethereum Net(현재)
스마트 컨트랙트	Solidity 기반 멀티시그 월렛 컨트랙트
키 저장	하드웨어 물리 키 저장(Customizable)
서명 메커니즘	M-of-N 다중 서명 방식

<양자내성 암호화 모듈 기술 사양>

기능	기술 상세
양자내성 알고리즘	ML-KEM 768 (Kyber) 알고리즘
키 교환 프로토콜	캡슐화/디캡슐화 방식
융합 대칭 암호화 모듈	AES-256
키 길이	공개키: 1568바이트, 비밀키: 3168바이트, 공유비밀: 32바이트

퀀텀가드 퀀텀월렛의 의미

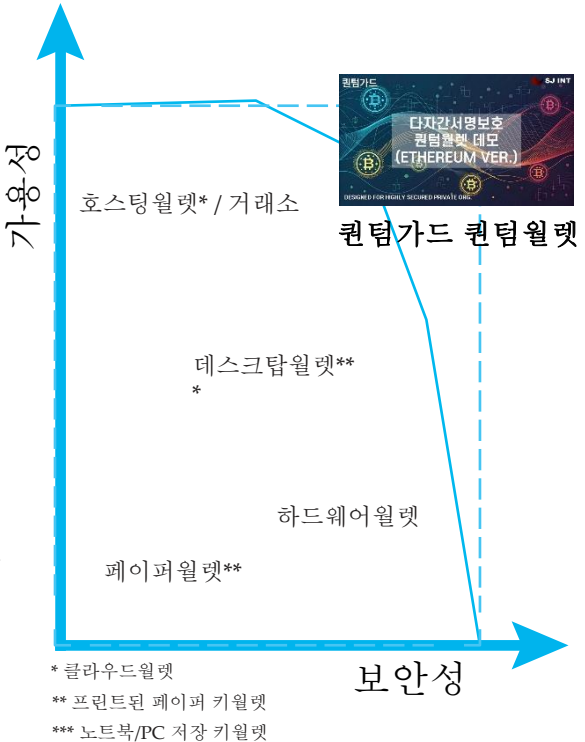
2020년 미국에서, 2023년 한국에서 그리고 동남아시아 등 세계에서 디지털 수탁시장이 법적으로 오픈 되었습니다. 세계가 불경기 속에서 가상화폐/암호화폐 및 디지털화폐 시장은 고속 성장하고 있는 시장입니다.

비단 디지털수탁 즉 커스터디 시장 뿐만 아니라, 암호화폐 시장에서 블록체인과 함께 핵심 기술은 월렛기술 입니다.

자산을 저장하고 관리하는 블록체인 그리고 자산의 키를 관리하는 월렛이 그것입니다.

오른쪽 그림은 시장의 월렛기술을 보안성과 가용성으로 도식화한 것입니다. 현재 시장에서 다양한 기술이 존재하지만 모두 사양과 기능이 다릅니다. 그런데 주목할 점은 다양한 월렛기술이 공존한다는 것입니다. 그래서 저희 개발진의 생각은 생각했습니다. “모든 월렛기술이 가치사슬에 모두 중요하고 모든 월렛기술의 필요하다는 점”에 주목했습니다.

저희 기술 개발진의 시작은 국방 분야입니다. 국방정보,통신,보안 기술과 프로젝트를 오랜 기간 수행했습니다. 저희는 현재 암호/디지털화폐 시장에서 가장 앞선 기술인 커스터디/디지털수탁 월렛 기술을 기업용으로 독자적으로 개발했습니다. 이에 한 발 더 나아가 2024년 미국 국립기술표준원에서 양자내성암호화 체계로 공식발표한 항양자 암호화 모듈을 융합,개발하여 “퀀텀월렛”으로 발표하게 되었습니다.



I. Supported Cryptocurrencies / 지원 암호화폐 및 지원 예정 암호화폐

ERC20/
Ethereum
(current)

Bitcoin
(~25.06)

Litecoin
(~25.12)

Bitcoin cash
(~26.03)

II. PlatformSupported / 지원 플랫폼

Hybrid Wallet
(current)

Secured Wallet For
Payment (TBA)

Personal
Wallet For
Gaming(TBA)_

Secured Wallet
For NFT(TBA)

기업용

기업용

개인용

기업용
개인용

| 3

Key Features of Quantum Wallet Architecture

퀀텀가드 vs 경쟁 솔루션 비교표

<퀀텀가드 vs MetaMask 비교>

기능/특성	퀀텀월렛 지갑 Mgmt.	MetaMask
구현 플랫폼	독립실행형 + 클라우드 연동(예정)	브라우저 확장 프로그램 및 모바일 앱
대상 시장	기업용 및 개인용	주로 개인 사용자
다중 서명 지원	통합 다중 서명 관리 시스템	⚠ 제한적(외부 다중 서명 컨트랙트 필요)
오프라인 보안	하드웨어 콜드월렛 통합	× 핫월렛 기반(별도 하드웨어 지갑 필요)
양자내성 암호화	ML-KEM 기반 미래 대비 보안	× 미지원
사용자 정의 기능	기업 요구에 맞춤 커스터마이징 가능	× 제한된 사용자 설정
대규모 자산 관리	대규모 자산 안전 관리에 최적화	⚠ 소액 거래 중심 설계
확장성	모듈식 설계로 다양한 확장 가능	⚠ 제한된 플러그인 지원
감사 및 규정 준수	기업 감사 추적 및 규정 준수 기능	× 제한적인 거래 이력만 제공
개발자 API	개발 중(제한적 API 제공)	광범위한 개발자 API 제공

* Metamask : 미국 블록체인 소프트웨어 지갑 솔루션.최다가입 플랫폼

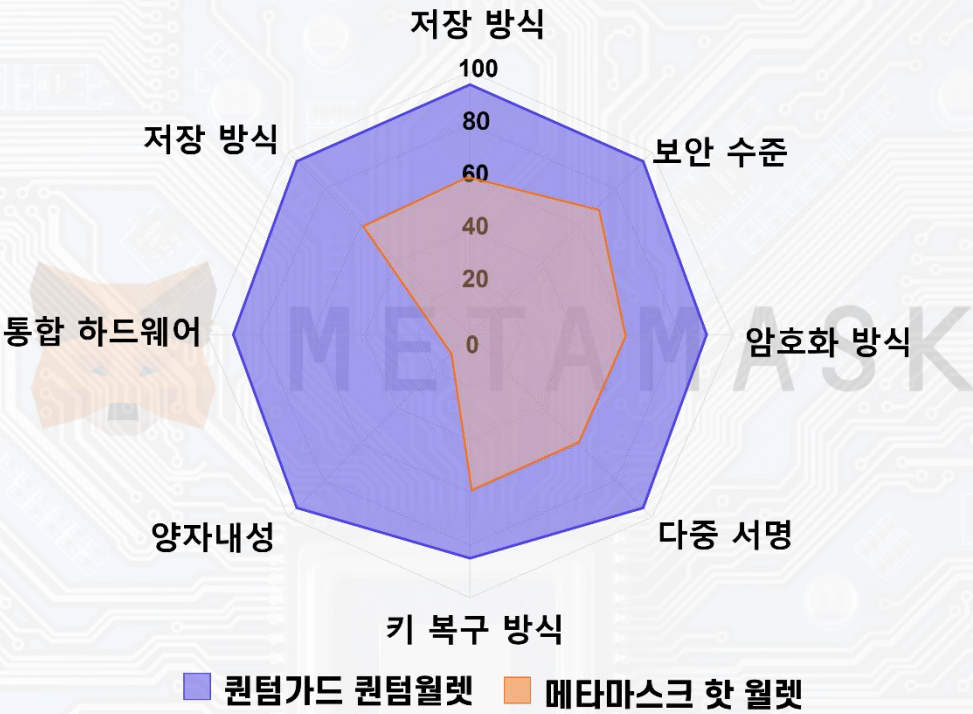
<퀀텀가드 vs Trezor 콜드월렛 비교>

기능/특성	퀀텀월렛 하드웨어키 Mgmt.	Trezor 콜드월렛
구동 방식	표준 USB 저장장치 기반 소프트웨어	전용 하드웨어 칩 기반
전용 매체	표준 USB 사용으로 물리매체 제한 없음	× 유료의 전용 하드웨어 USB 구매 필요
다중 서명 관리	통합 다중 서명 인터페이스 제공	⚠ 제3자 소프트웨어 필요
기업 맞춤화	기업 요구사항 맞춤 구성 가능	× 제한된 맞춤화
양자내성 보안	ML-KEM 기반 양자내성 암호화 제공	× 기존 암호화만 지원
소프트웨어 업데이트	소프트웨어 업데이트	⚠ 펌웨어 업데이트 필요
통합 백업 솔루션	자동화된 백업 및 복구 시스템	⚠ 수동 백업 (복구 문구 기록)
스마트 계약 상호작용	직관적인 스마트 계약 인터페이스	× 제한적 지원
물리적 보안	강력한 소프트웨어 암호화 후 물리저장	물리적 변조 방지 설계
대용량 트랜잭션 관리	기업 수준 트랜잭션 처리	× 개인용 거래 중심

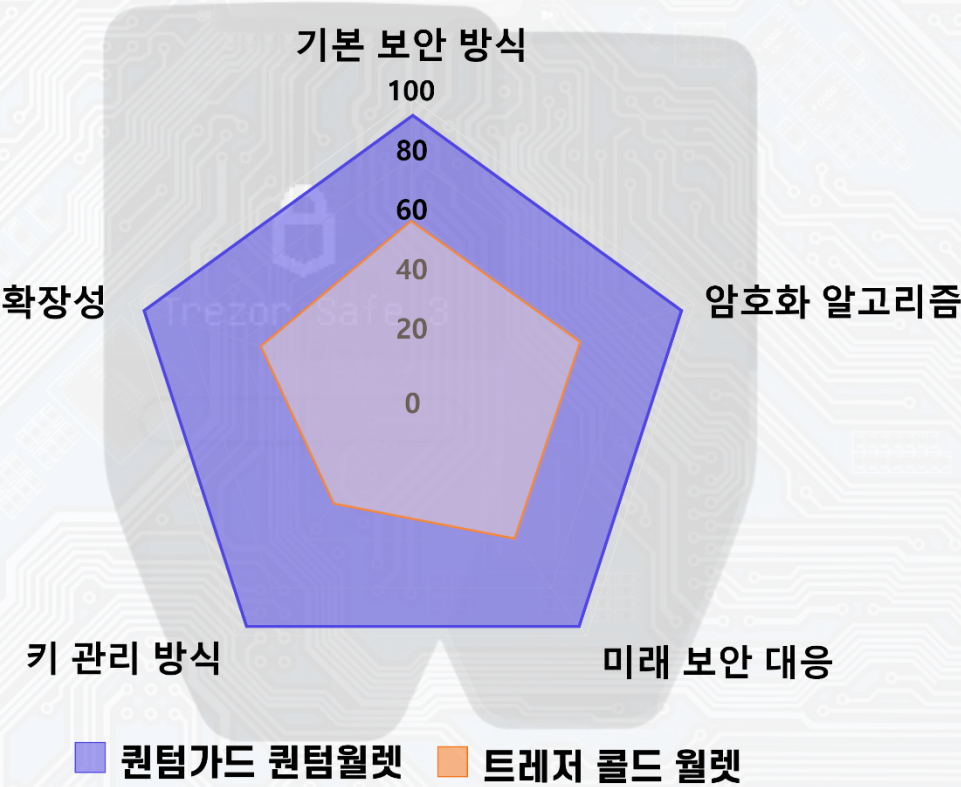
* Trezor : 체코 콜드월렛 외장 저장 장치 솔루션.최다판매 장치

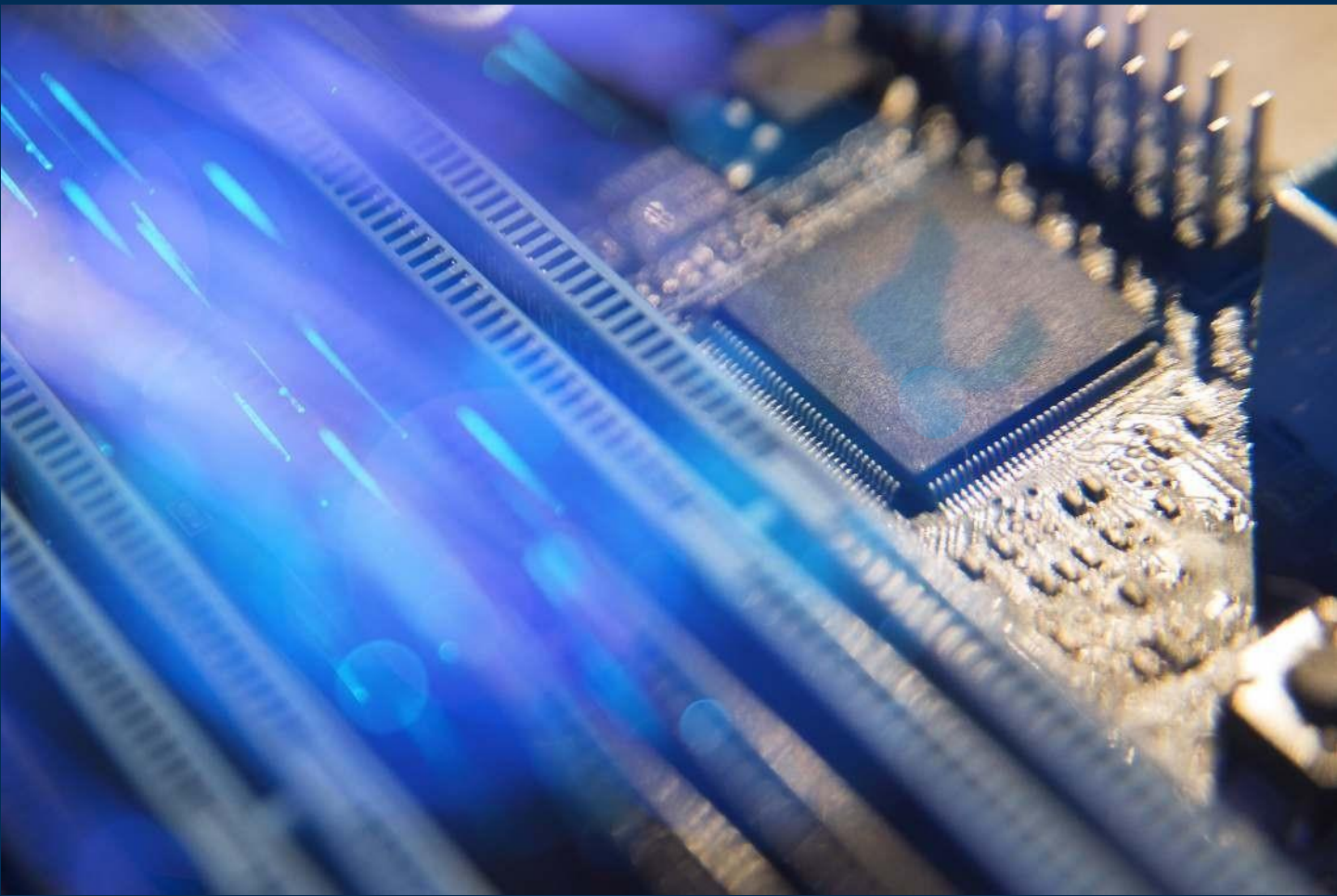
Key Features of
Quantum Wallet Architecture
퀀텀가드 vs 경쟁 솔루션 비교표

<퀀텀가드 vs MetaMask 비교>



<퀀텀가드 vs Trezor 콜드월렛 비교>





전용 워크스테이션 운용 환경

저희 퀀텀윌렛 하이브리드 시스템은 다음의 운용 환경에서 제공됩니다 :



Enterprise

Professional

Powerful Small Workstation

보안과 신뢰성 높은 전용 워크스테이션을 공급합니다



Normal mode

Windows

Applications

Kernel

Secure mode

virtualization-based security

Credential

Other isolated services

Secured kernel + Code Integrity

Hypervisor

Hardware

Strongly Secured OS Machine

삼성NOX는 가장 뛰어난 보안 운용 환경입니다. 그와 동일한 수준의 독립실행 보안 운용환경을 고객에서 제공합니다



Virtualization-based security

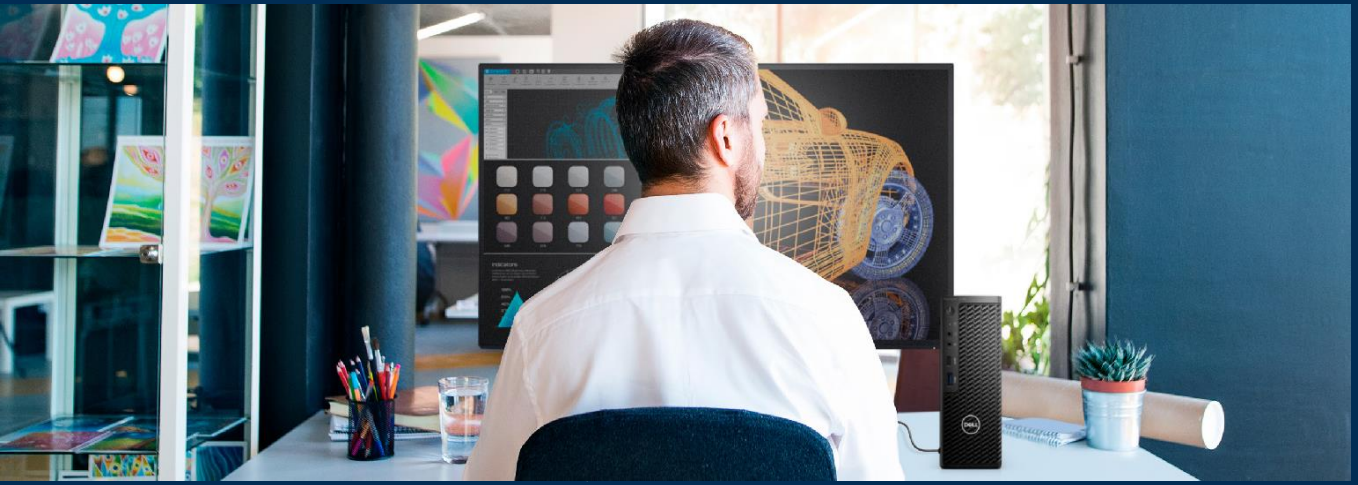


Military Grade Secured Network

Full Duplex 크로스 도메인 기능을 제공하는 군사용 보안 네트워크 솔루션을 제공합니다.



Defense Network



<기술비교 : 트레저의 콜드월렛 보안취약점>


* 가장 유명한 USB 콜드월렛

기능 사항	보안 취약점	기술적 위험 요소 및 설명
전자서명 기능	펌웨어 종속성 증가	- 펌웨어 취약점(제로데이 취약점) - 공격 벡터(Attack Vector) : 해커가 시스템을 공격할 수 있는 경로가 확대됨
하드웨어 사양	공급망 공격 취약성	- Supply Chain Attack - 제품 생산/유통 과정에서 악성 요소 삽입 - 후조작(Tampering) - 장치가 사용자에게 전달되기 전 물리적 조작 가능성
신뢰 구조 확장	신뢰 의존도 증가	- Trust Minimization : 신뢰해야 할 요소를 최소화하는 보안 원칙 - 공격자 목표가치(Target Value) - 해커가 얻을 수 있는 가치가 집중되어 공격 동기 강화
자동화된 서명 검증	검증 로직 복잡화	- 위조된 서명 요청 : 악성 트랜잭션을 정상처럼 보이게 하는 속임수 - 검증 우회(Validation Bypass) : 보안 검증 절차를 건너뛰게 만드는 공격
브라우저/앱 연동 방식	의존성 프레임워크 취약성	- 중간자 공격(MITM) : 통신 중간에서 정보를 가로채는 공격 기법 - 메타데이터 조작 : 거래 정보의 부가 데이터를 변조하는 공격

<핵심 보안 원칙>

 단순성 원칙

 인지적 편의성 함정

 권한의 최소화 원칙

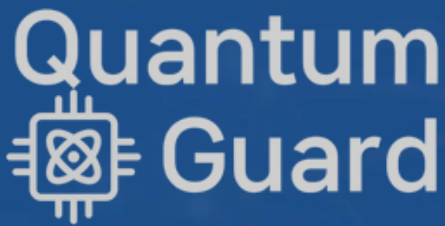
 기능 만능의 보안 환상

<장비사양 : 전용 워크스테이션 소프트웨어 인증>

보안 기능	Precision Compact(3260)	Dell Precision SFF(3460)
TPM 2.0	✓	✓
새시 침입 스위치	✓	✓
케이블 잠금 슬롯	✓	✓
Dell Trusted Device (SafeBIOS)	✓	✓
Digital Device Identity	✓	✓
Secured Component Verification	✓	✓
Secure BIOS Baseline	✓	✓
Secured-core PC	✓	✓
Self-encrypting Storage Drive	✓ (옵션)	✓ (옵션)
FIPS 인증 스토리지	✓ (옵션)	✓ (옵션)
지문 인식기	외부기기 제공	✓ (옵션)
Intel Secure Boot	✓	✓
Intel Authenticate	✓	✓
Contact card reader	외부기기 제공	✓ (옵션)

<기술사양 : 전용워크스테이션 보안 인증 및 기능>

인증 유형	Precision Compact(3260)	Dell Precision SFF(3460)
ISV 인증	✓	✓
MIL-STD 테스트	✓	✓
Dell Optimizer for Precision	✓	✓
Dell Client Command Suite (DCCS)	✓	✓
Dell PremierColor	✓	✓



퀀텀가드 퀀텀월렛
Software Hardware
Hybrid-based Wallet for Emerging
Digital Assets & Custody Service

감사합니다

서비스 문의
service@QuantumGuard.co.kr