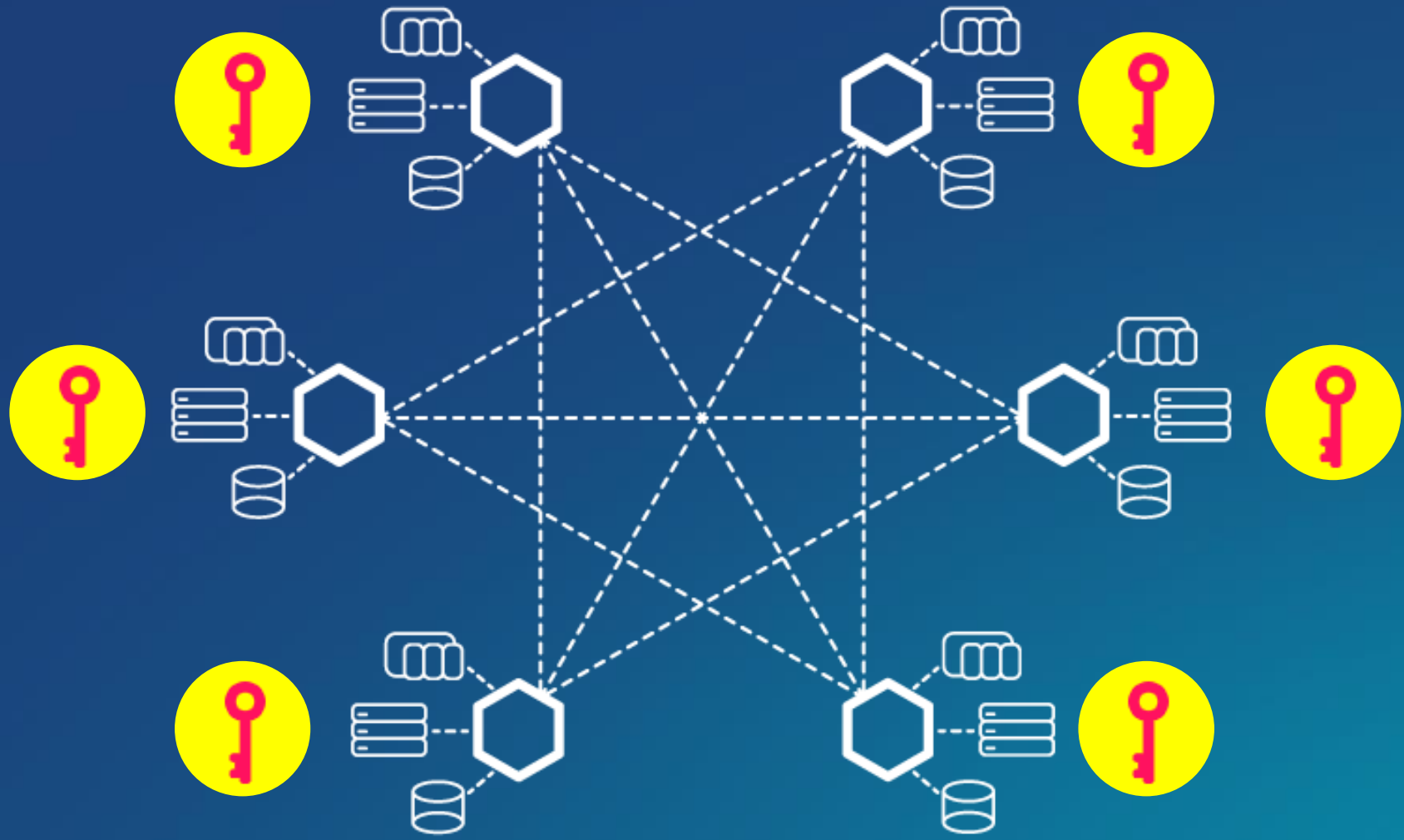
TEEvault –암호화폐 키 관리 솔루션

TEEvault - Blockchain Key Management Solution

TEEware

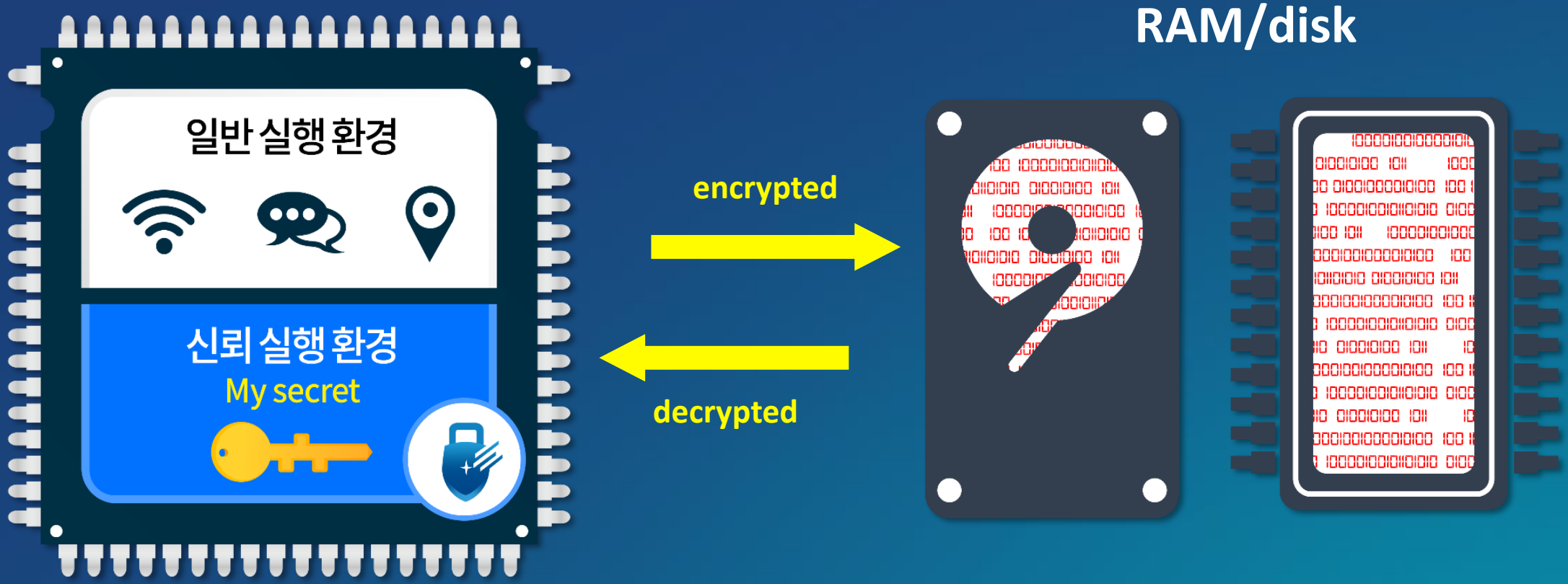

“A chain is only as strong as its weakest link”

The weakest link is key management.



TEEvault 요구사항 – 1. TEE Protection

TEE (Trusted Execution Environment; 신뢰 실행 환경) 기술로 블록체인 키를 보관하여 해커의 공격에도 매우 안전해야 함



TEEvault 요구사항 – 2. Insider Proof

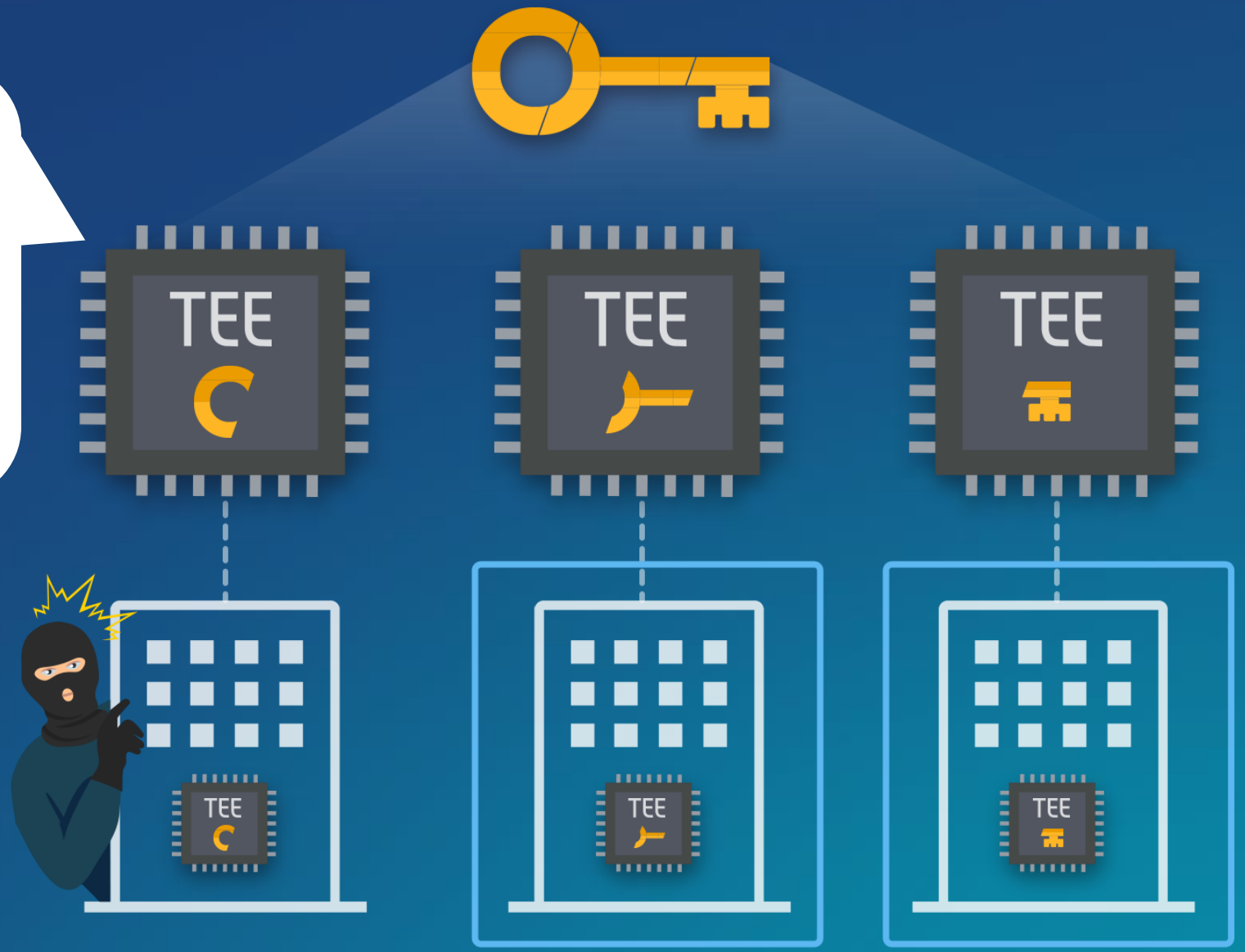
신뢰 실행 환경은 **내부자의 위협까지 가정하여 안전하게 설계**되어
내부 관리자라도 승인되지 않은 절차로는 주요 정보에 접근할 수 없어야 함

TEEvault 요구사항 – 3. Fail Safe

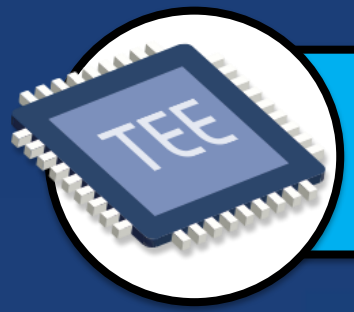
주요 정보를 **여러 서버에 분산**시켜 보관함으로 일부 장치에서 고장이 발생하더라도 안전하게 데이터를 유지해야 함

TEEvault 요구사항 – 4. Threshold Signature

주요 정보를 **암호학적 기법으로 분산**시켜 저장하고 사용하여 암호학적으로도 안전하게 키를 보호해야 함



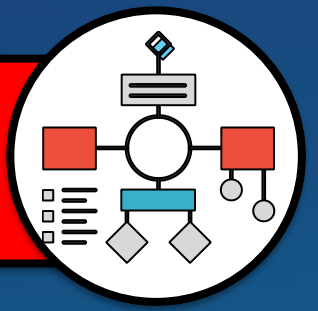
Two Key Protection Mechanisms



Trusted Execution Environment

- ✔ **Secure execution environment** (Protected memory and storage)
- ✔ **Protection from physical adversary**
- ✔ **Protection from infected host** (malicious process, OS, hypervisor)
- ✔ **Hardware-enforced security**

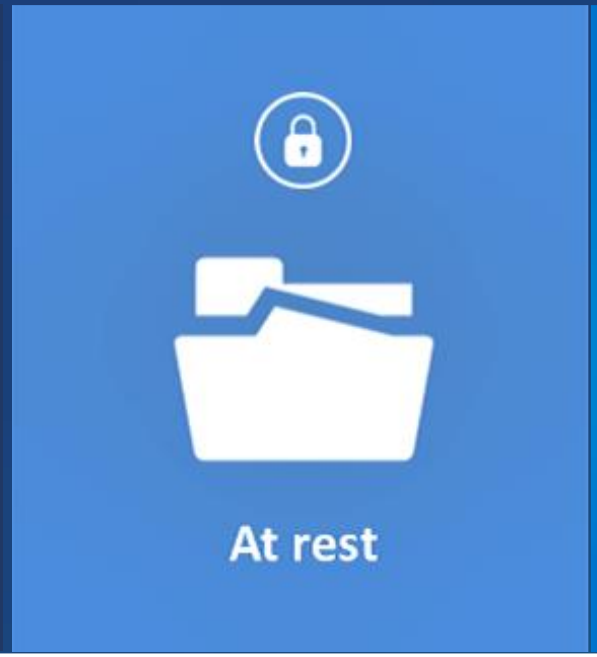
Crypto Technology



- ✔ **Multi-party computation technique** (in particular, threshold signature)
- ✔ **Safety net from device failure or loss**
- ✔ **Distributed risk across multiple locations**
- ✔ **Threshold characteristic - robust and tolerant**

Two orthogonal mechanisms are combined to deliver maximum security

Three Phases of Data

	 At rest	 In transit	 In use
Location	Disk (HDD, SSD)	Network (LAN, WAN)	Memory (RAM)
Primary applications	File server, DBMS	Web server, server applications	Any application
Protected by	Volume encryption, File encryption, DB encryption	TLS/SSL, IPsec, VPN protocols	?

TEE Usage Example

Runtime memory (RAM)

```
002c 0103 0b52 6f6e 2057 6561 736c 6579  .,...Ron Weasley
1332 3135 312d 3335 3232 2d34 3430 322d  .2151-3522-4402-
3736 3838 0333 3032 2c01 0310 4865 726d  7688.302,...Herm
696f 6e65 2047 7261 6e67 6572 1333 3835  ione Granger.385
392d 3636 3937 2d37 3637 392d 3836 3539  9-6697-7679-8659
0336 3434 2c01 030c 4861 7272 7920 506f  .644,...Harry Po
7474 6572 1331 3233 342d 3233 3435 2d33  tter.1234-2345-3
```

Credit card number exposed!

```
6a10 8bfe 52e0 3891 b3ed a8bf 6590 14bc  j...R.8.....e...
9993 ed70 2c72 5616 d965 ebdd e8a4 c5fb  ...p,rV..e......
d61f 034c a1c0 2ef1 eb14 0851 a73c 0740  ...L.......Q.<.@
eac8 caf2 9d11 7d89 5cd3 1d41 2df4 6911  ......}.\..A-.i.
d1b7 59ac 54a6 687b 1f67 02f9 e4ad 8e9d  ..Y.T.h{.g......
8faa c83d 3d9f 48a5 4325 5a0f 5e98 efe3  ...==.H.C%Z.^...
ee2c df9c 413a 79cd b42a f061 bd95 e0a4  .,..A:y..*.a....
```

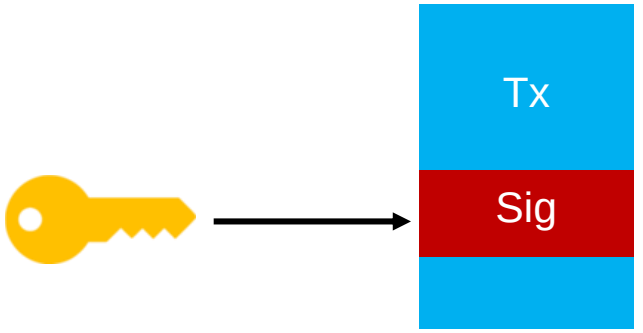
Runtime memory encrypted

TEE encrypts runtime memory of existing applications,
protecting sensitive information (PII, finance, private key) from advanced threats.

ThresholdSig

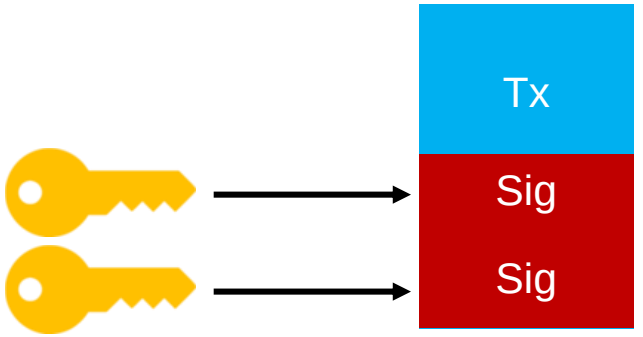
SingleSig

- An account depends on single private key



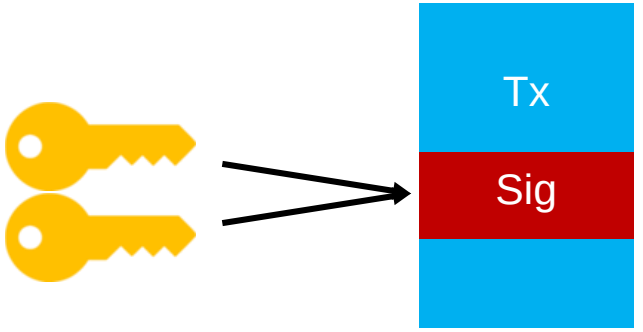
MultiSig

- t-of-n approval security
- Requires platform support
- Higher transaction fee



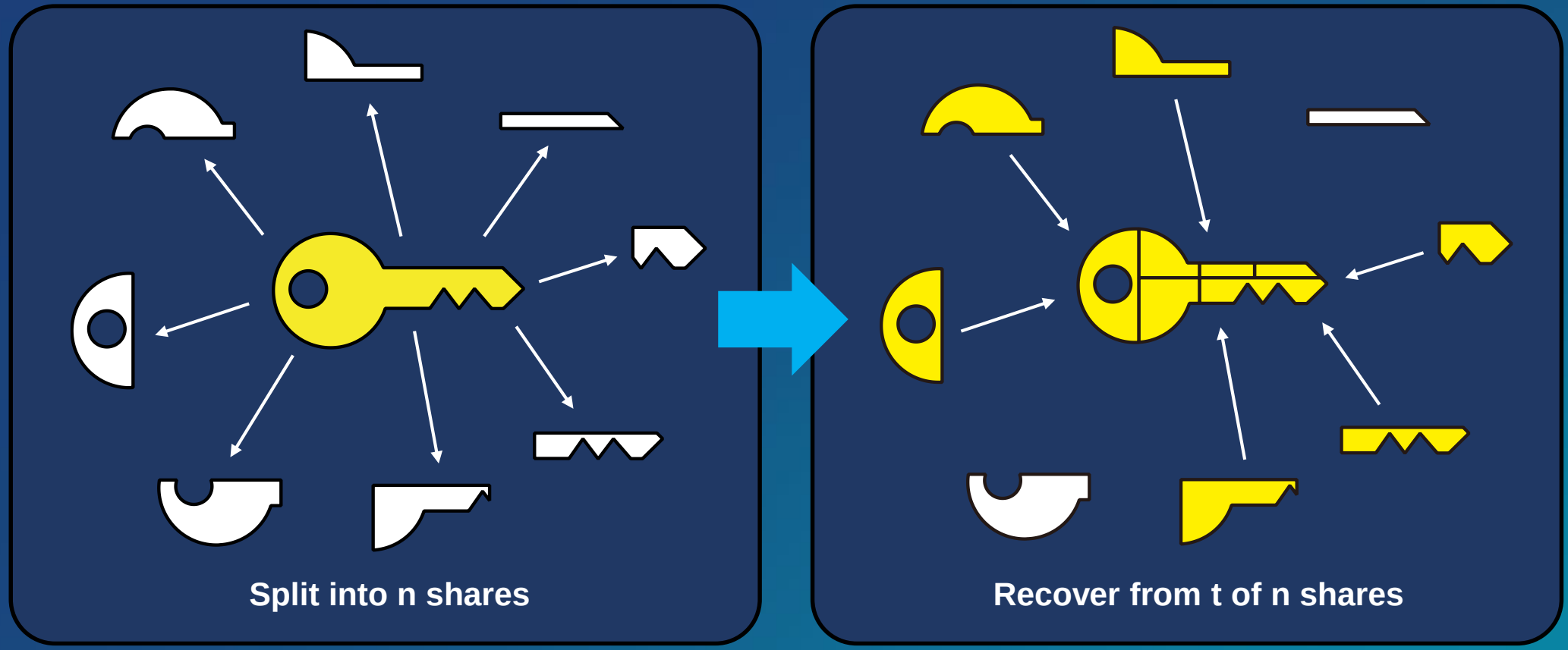
ThresholdSig

- t-of-n approval security
- Platform-independent
- Configuration is invisible to the blockchain



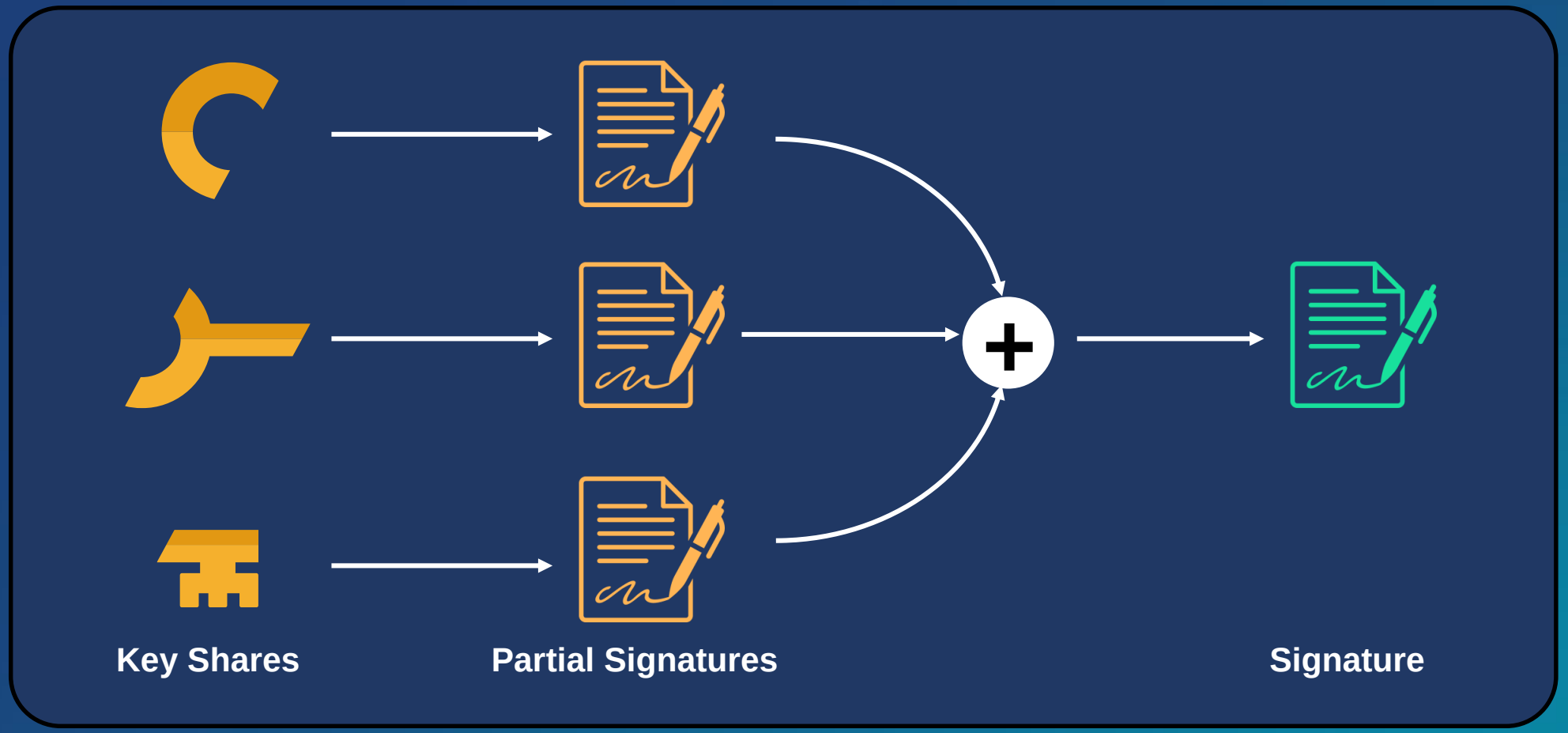
Recap: Secret Sharing

- ✔ Ex) Shamir's Secret Sharing (SSS)
- ✔ Split a private key into multiple shares
- ✔ Recover the original private key to sign a message



Threshold Signature

- ✔ Split a private key into multiple shares
- ✔ Collaboratively calculate signature
- ✔ Private key shares are never exposed to other participants



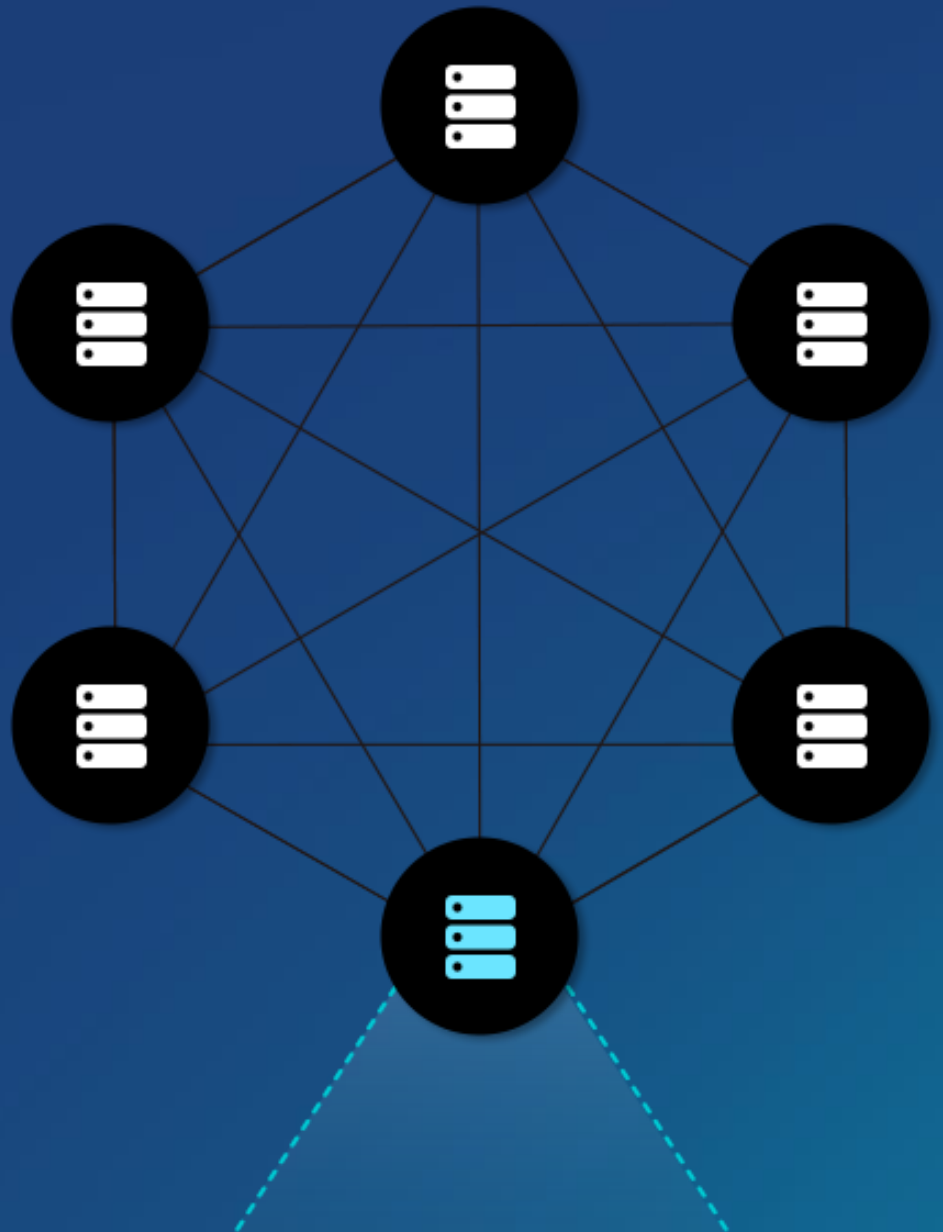
Trustworthy security solution for digital assets

TEEvault

Blockchain Key Mangement Solution

TEEvault는 엔터프라이즈 환경에서 암호화폐를 안전하게 보관하고 관리할 수 있는 키관리 솔루션입니다. 암호화폐 개인키의 생성, 백업, 서명의 전 과정은 격리된 신뢰실행환경(Trusted Execution Environment, TEE) 에서 일어나기 때문에 해킹과 물리적인 공격이 있어도 키가 유출되지 않습니다. TEEvault의 임계 암호 (threshold cryptography) 기술을 활용하면 암호화폐 키를 나누어 각기 다른 장소에 저장할 수 있으므로 리스크가 분산되고 재해로부터 즉시 복구할 수 있습니다.

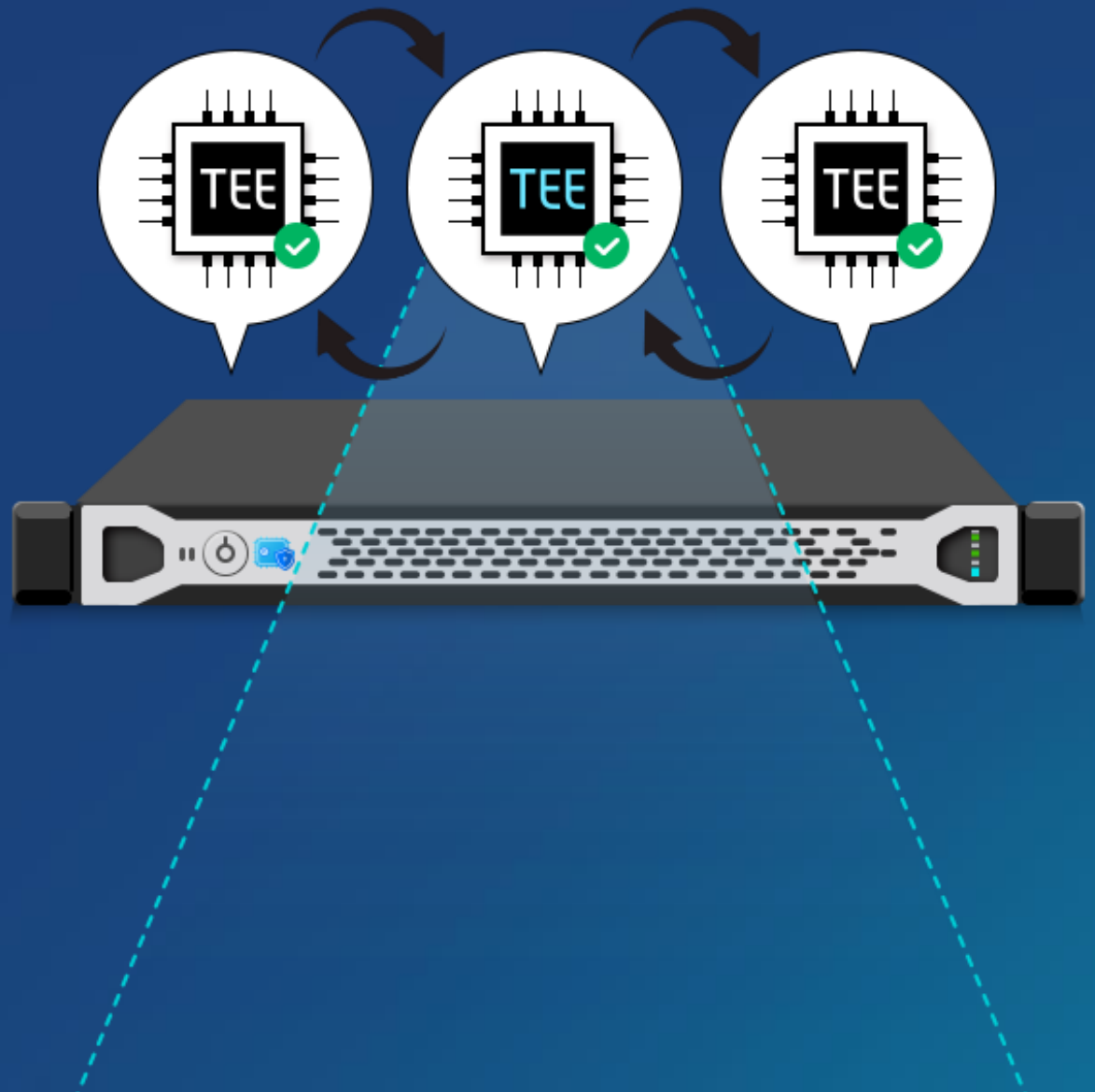
System Architecture



Safe as much as you connect

- ✓ 키의 분산으로 인한 리스크 분산
- ✓ 자연 재해 등으로부터 고가용성 유지
- ✓ 임계 암호 기술을 통한 암호학적 멀티시그 지원 (이더리움 등)

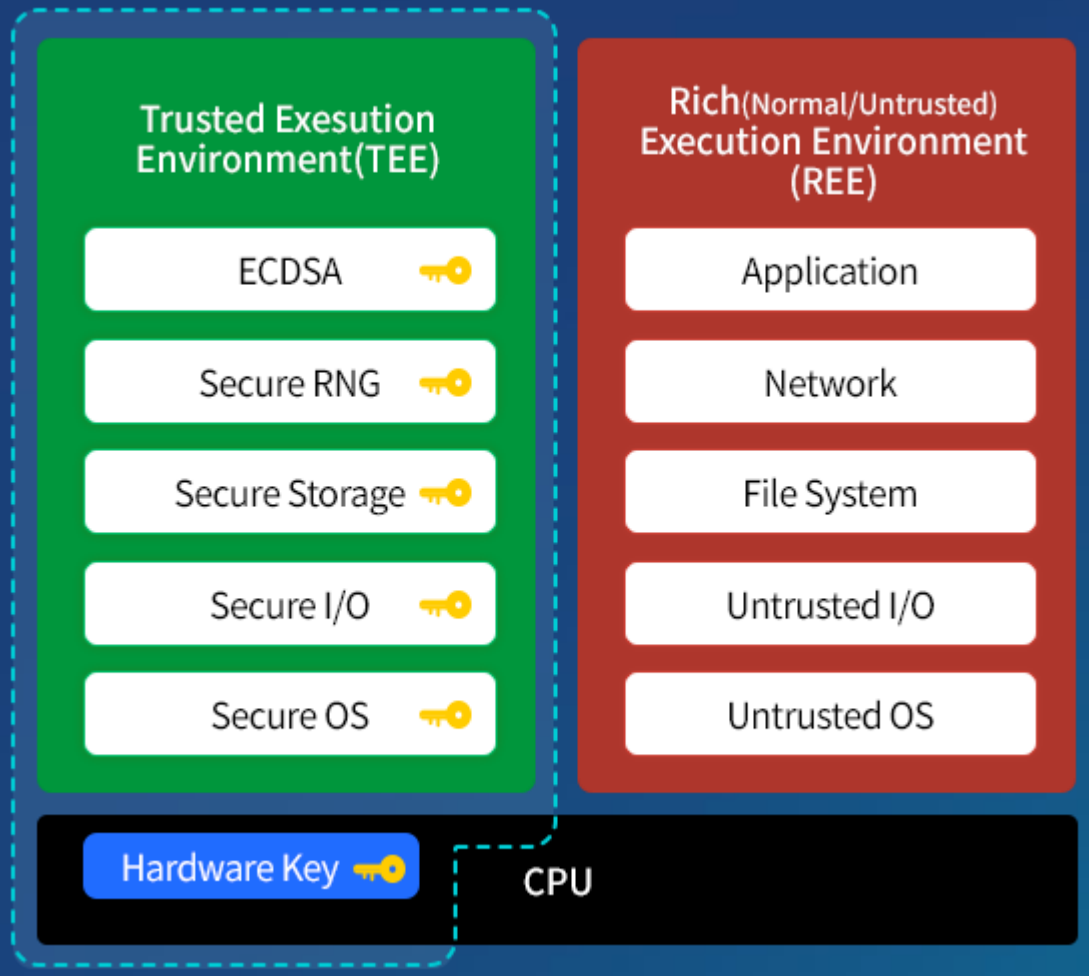
System Architecture



Robustness tripled

- ✓ 삼중 백업을 통한 데이터 유실 방지
- ✓ 인증된 TEE간 저장된 키 동기화
- ✓ TEE간 로드밸런스로 성능 향상

System Architecture



Hardware-enforced security boundary

- ✓ REE로부터 완벽히 격리된 TEE
- ✓ Hardware Key를 통한 데이터 보호
- ✓ 전자현미경으로도 찾기 힘든 Hardware Key

Components

TEEvault Core

- 2u rack mount
- TEE-based key storage

TEEvault Bridge

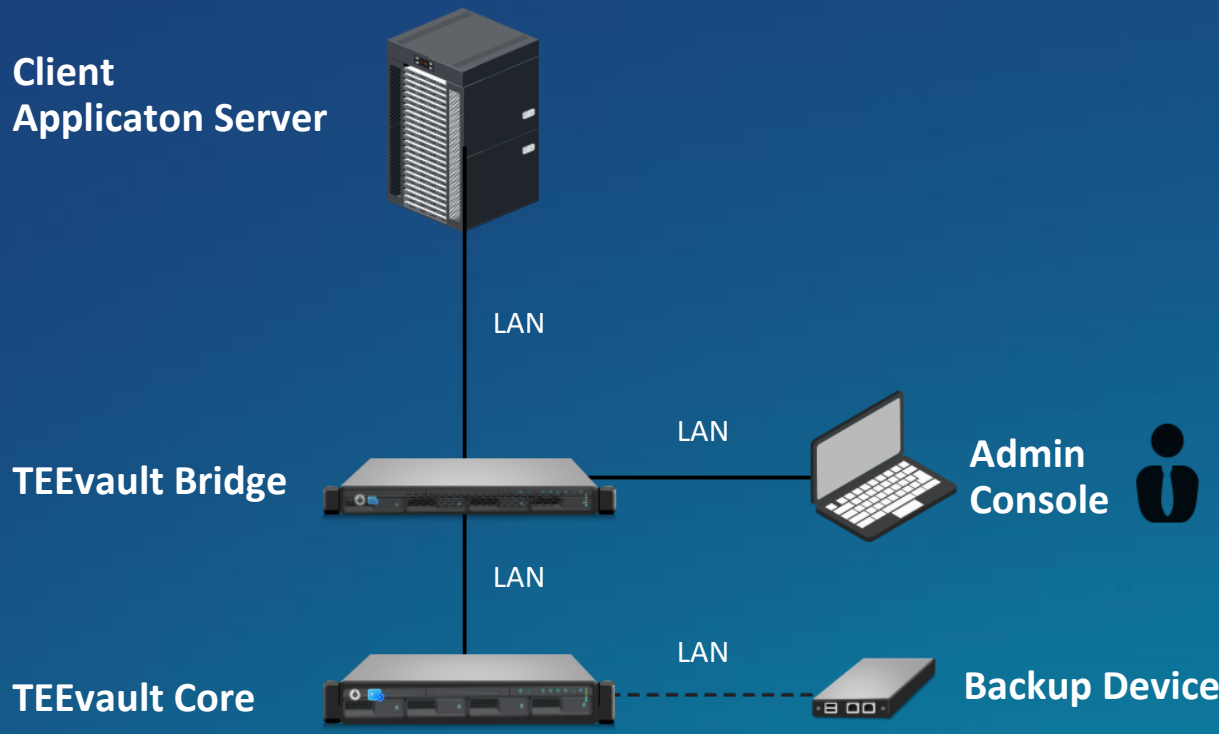
- 1u rack mount
- Manager & Monitor

Backup Device

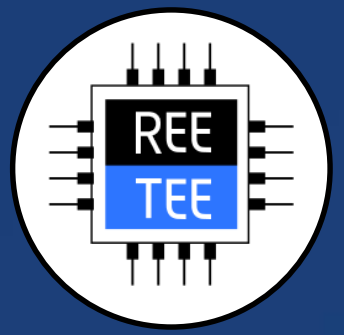
- Portable backup device
- TEE-based key storage

Docs & Manual

- API documentation
- Installation Manual

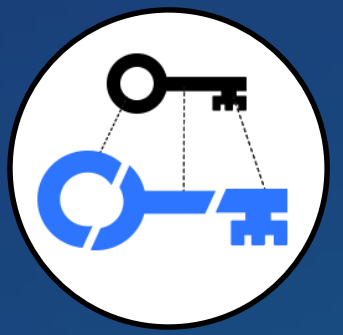


Features



TEE를 이용한 키의 안전한 사용

한 디바이스에서 일반실행환경(REE)과 신뢰실행환경(TEE)이라 불리는 두 개의 OS를 실행할 수 있습니다. 키를 다루는 모든 연산은 신뢰실행환경에서 일어나 해커가 침투할 수 없습니다.

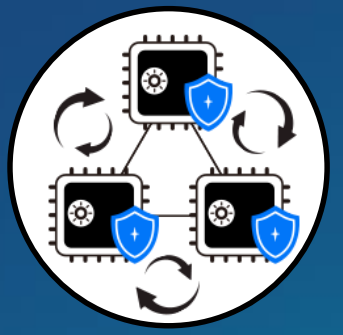


임계 암호를 이용한 분산 저장

암호키를 여러 조각으로 나누는 임계 암호(threshold signature) 기술을 활용하였습니다. 어느 디바이스도 온전한 키를 가지지 못하기 때문에 분실과 도난의 리스크를 분산시킬 수 있습니다.

블록체인 업계의 표준 준수

다양한 블록체인 프로토콜을 지원할 수 있도록 BIP-32, 39, 44 표준 및 ECDSA, Keccak 등의 암호 알고리즘을 지원합니다

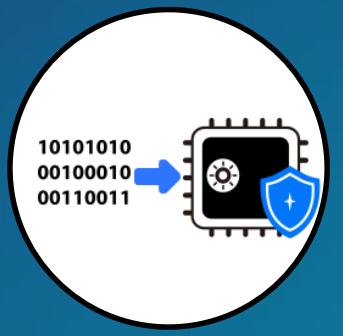


실시간 백업

TEEvault 내부의 키 저장소는 삼중으로 hot-backup됩니다. 일부 저장소의 장애에도 서비스의 중단없이 고가용성을 유지할 수 있습니다.

키의 생성 및 사용 이력에 대한 통합 관리

키는 TEEvault 밖으로 나가지 않는 대신 키에 대한 모든 이력은 TEEvault에 남게 됩니다. 이 로그를 보고 키가 언제 어디에서 누가 사용했는지 알 수 있습니다.



기존에 보유한 블록체인 키의 이전

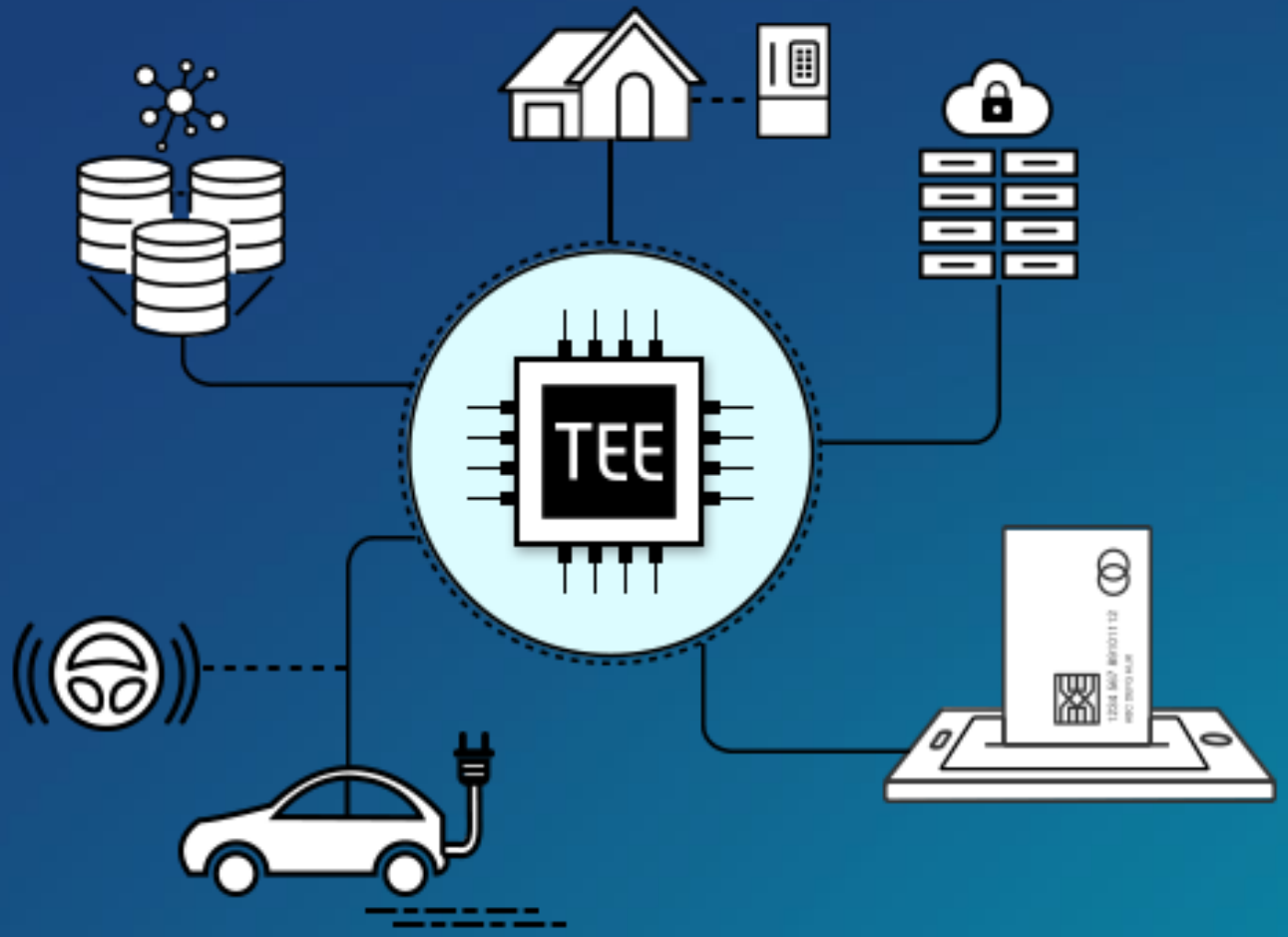
다른 방식으로 관리하던 키를 TEEvault로 쉽게 옮길 수 있습니다. 전송 과정에서의 노출을 최소화하기 위하여 인증된 TEEvault만 열어볼 수 있도록 암호화하여 옮길 수도 있습니다.

TEEvault vs. Traditional HSM

	TEEvault	Traditional HSM
BIP-32 key deriviation	Securly computed inside the trusted execution environment (TEE)	Not implemented in HSM. Must be done manually outside HSM.
Crypto algorithms	Supports secp256k1, secp256r1, ed25519. Covers significant amount of blockchain protocols.	Mostly supports secp256r1 and secp256k1. Some blockchains like Ripple and Stellar are not supported.
Threshold signature	Implemented for secp256k1. Supports arbitrary k-of-n setup.	Not supported
HA/DR	▪ Built-in redundancy in every TEEvault Core ▪ Threshold signature provides cryptography-level redundancy and security ▪ Dedicated backup device securely stores keys.Admin cannot see its content inside TEE	▪ Backed up using multiple HSM devices with client's manual effort. ▪ Backup files should be transferred through public Internet
Storage capacity	More than 100k ECDSA keys	Usually limited to 1k ~ 100k keys

Vision

TEEware는 첨단 보안 기술을 활용하여 블록체인, 핀테크, IoT 등 첨단 기술 분야에 새롭게 발생하는 보안 문제를 해결하여 안전한 세상을 만들고자 합니다.



https://www.teeware.kr

contact@teeware.kr