TPM 기반 IoT 블록체인

https://youtu.be/-h8jawE6oZo

IoT 블록체인에 TPM 활용

1. 아이디어
   - IoT에는 intel sgx와 같은 TEE를 활용할 수 없음
   - 이를 대신해서 TPM 활용

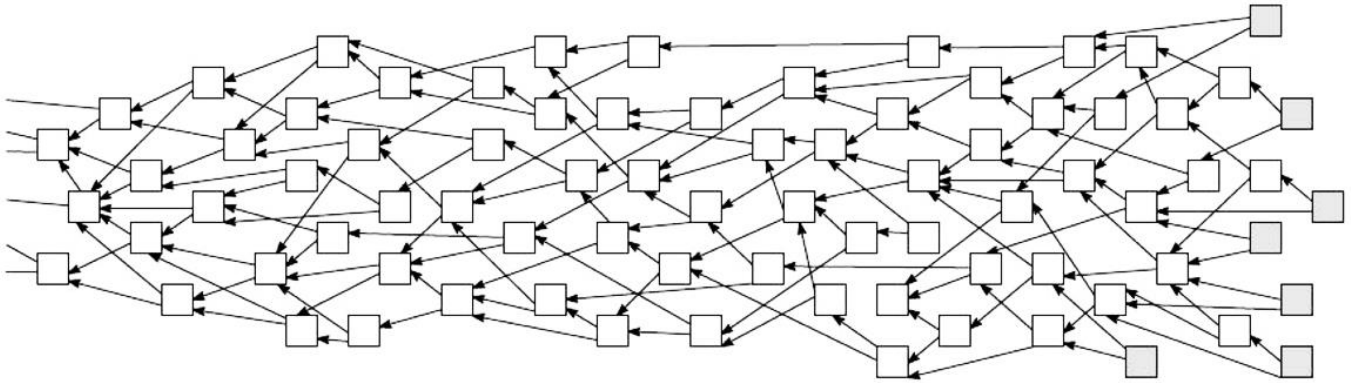
- TEE기반 합의 알고리즘
  - 경과 시간 증명(PoET: Proof of Elapsed Time)
  - 행운 증명 (PoL: Proof of Luck)

  → TEE의 어플리케이션 레벨의 보호 기능을 활용

  → TPM은 TEE를 대체할 수 없음

IoT 블록체인

- DAG
  - 블록체인과 유사하지만, 선형 구조 대신 비순환 그래프로 데이터를 기록하는 방식
  - 각 트랜잭션은 독립적으로 발생하며, 방향성을 가진 그래프 형태로 연결



- Ex) Tangle: IOTA는 IoT 환경에서의 마이크로 트랜잭션을 효율적으로 처리하기 위해 설계된 DAG 기반 분산원장 기술 사용

→ DAG 기반의 분산원장 + TPM

→ TPM를 활용 보안 기능 향상

TPM의 무결성 기능

- 네트워크에 연결되는 모든 기기의 무결성을 확인하는 기능 제공
  - 무결성 측정: TPM은 시스템 부팅 과정에서 실행되는 소프트웨어 및 하드웨어 구성 요소의 상태를 측정하고, 이 값을 PCR(Platform Configuration Registers)에 저장.
  - 원격 인증(Remote Attestation): 저장된 무결성 측정값을 기반으로, TPM은 외부 엔티티에게 현재 플랫폼의 상태를 증명. 이를 통해 원격에서 시스템의 무결성을 검증 가능.
  - 신뢰 기반 부팅(Trusted Boot): TPM은 부팅 과정에서 신뢰할 수 없는 구성 요소가 로드되지 않도록 보장하며, 이를 통해 시스템의 전체적인 보안성을 향상.

→ 산업, 정부와 같이 보안적 요소가 필요한 경우 노드의 무결성에 활용

원격 인증(Remote Attestation)의 중앙화

- 원격 인증(Remote Attestation)
  - 시스템 측정 및 PCR 저장:
    - 클라이언트 시스템이 부팅 시 각 구성 요소의 해시 값을 계산하고 TPM의 PCR에 저장
  - Attestation 요청 및 Quote 생성:
    - 중앙 서버가 클라이언트에게 시스템 상태 증명을 요청
    - 클라이언트의 TPM은 요청된 PCR 값을 포함한 Quote를 생성하고 서명
  - Quote 전달 및 검증:
    - 클라이언트는 서명된 Quote를 중앙 서버로 전송.
    - 중앙 서버는 서명을 검증하고 PCR 값들을 신뢰할 수 있는 값과 비교.
  - 결과 판단 및 조치:
    - 검증 결과에 따라 클라이언트의 신뢰성을 판단

- 신뢰할 수 있는 제3자 필요

DAA (Direct Anonymous Attestation)

- 익명성을 보장하면서도 사용자의 신뢰성을 검증할 수 있는 보안 인증 프로토콜
- ECC, 영지식 증명

- **가입(Join Phase)**: 사용자는 그룹에 가입할 때 TPM이나 신뢰할 수 있는 플랫폼을 통해 익명성을 갖춘 서명을 생성
- **증명(Sign/Attestation Phase)**: 사용자가 인증을 요청할 때, TPM은 익명 서명을 생성하여 해당 플랫폼이 신뢰할 수 있는 환경이라는 것을 증명.
- **검증(Verification Phase)**: 인증을 받는 서버나 플랫폼은 사용자의 익명 서명을 검증.

관련 구현물

- SimpleIOTA
  - https://github.com/leewaygroups/simpleIOTA/tree/master

- IBM TSS 소프트웨어를 기반으로 DAA 프로토콜 구현
  : 라즈베리파이 가능
  - https://github.com/UoS-SCCS/ecc-daa

- 간단한 구현을 기반으로 프로토타입 작성 예정

TPM 기반 IoT 블록체인의 장점

- **블록체인**
  - 공유 및 투명한 데이터 액세스
  - 변경 불가능/변경 방지 원장
  - 검증된/거부할 수 없는 트랜잭션
  - 기밀 기록 및 거래

- **TPM**
  - **다수의 장치 관리:**
    수많은 장치가 연결되어있는 IoT 네트워크에서, 각 장치의 무결성과 신뢰성을 검증 가능.
  - **프라이버시 보호:**
    IoT 환경에서 장치의 신원을 노출하지 않고도 보안을 유지

주의점

- DAA와 DAG 분산원장의 실시간환경의 IoT에서 충분히 동작 가능한지 여부
- 장점과 단점의 정확한 분석 필요 : 방어가 가능해지는 기존공격, 추가 취약점 등
- 구현 가능성 : 기존 구현물을 최대한 사용해서 간단한 단계부터 수행
- 실험 환경의 한계 : 대상 IoT환경을 구축하는 것이 어려움, 실행, 구현 가능한 범위 내에서 환경을 고려해야함.

Q & A