**Abstract**

현재 블록체인은 IoT 장비에 적용하기에는 계산 오버헤드가 너무 큼

블록체인의 장점을 유지한 채 오버헤드를 없앤 경량 블록체인 제안

**1. Introduction**

블록체인이 여러 분야에서 사용되는 이유 -> POW에 의한 분산된 privacy와 보안 제공

그러나 IoT 장치에 그대로 적용하기에는 문제가 있다. 대표적으로 POW 사용으로 인한 높은 자원을 요구하게 된다.

스마트 홈 시나리오를 예시로 들어 경량 블록체인에 대해 설명

제안한 경량 블록체인은 높은 자원 요구 등의 단점을 없애고, 원래의 이점을 유지

계층 구조 선택: 자원 소비를 최적화, 네트워크 확장성 증가

계층: smart home, overlay network, cloud storage

Smart home의 IoT 장치는 중앙에서 관리되는 private Immutable Ledger와 대칭 암호를 사용 -> 처리 오버헤드를 줄이기 위해

블록은 POW를 해결하지 않고 BC에 추가되므로 추가 오버헤드가 상당히 감소

**2. Literature Review**

**2.1 Privacy and Security in IoT**

IoT 장비들의 보안은 낮은 자원 능력, 표준화 미비 등으로 어려움을 겪고 있다

여러 가지 방법이 나왔지만 여전히 세 가지 과제를 해결해야 한다.

1. Resource optimization: IoT 장치의 제한된 자원은 높은 수준, 복잡한 보안 방법에 적합하지 않다.
2. Privacy: 여러 타입의 데이터를 드러내면서 사용자의 privacy는 지켜져야 한다.
3. Centralization: 중앙집중방식은 IoT에 적합하지 않은 경향이 있다.

**2.2 Bitcoin BC**

비트코인 mining은 POW로 알려진 자원을 소비하는 암호 퍼즐을 푸는 것을 포함.

이를 이용해 조직 및 사람과 IoT 사용자의 데이터를 공유할 수 있는 블록체인 기반 다중 계층 방식을 제안한 논문이 있으나 여기서는 IoT 기기들이 항상 PoW를 해결하기 위한 충분한 자원을 가지고 있다고 가정

PoW를 해결하기 위해서는 현재 컴퓨터를 사용해도 어려운데, IoT 장치가 이를 해결하는 것은 어렵다.

**3. BC-Based Smart Home Architecture**

트랜잭션을 통해 다른 계층과 통신

**3.1 Smart Home**

스마트홈은 IoT기기, local immutable ledger(IL), local storage로 구성

Local private IL은 BC와 비슷하지만 중앙, 즉 smart home manager(SHM)이 관리

SHM은 IoT 장치와 local storage 통신을 위해 공유 키를 사용

IoT 장치들은 데이터를 공유, 요청, 또는 저장하기 위해 트랜잭션 생성 가능

**3.2 Overlay**

Peer-to-peer network 형식

네트워크 오버헤드와 delay를 줄이기 위해 node들을 클러스터로 묶고, 각 클러스터에서 Cluster Head(CH)를 선택

각각의 CH는 unique Public Key(PK)로 새로운 블록 생성, 이 PK는 다른 CH에 의해 알려진다.

CH는 다음 목록을 유지

PK of Requesters

이 클러스터에 연결된 SHM의 데이터에 접근할 수 있는 PK 목록(내가 요청한 PK)

PK of Requestees

나에게 접근이 허용된 이 클러스터에 연결되어 있는 SHM의 PK 목록(요청 받은 PK)

CH들끼리 거래 내역에 대한 ledger를 가지고 있는 public 블록체인을 유지

트랜잭션에 Multisig 적용, requester와 requestee가 모두 서명해야 유효한 거래

각 트랜잭션은 두 개의 출력: 승인된 거래의 개수, 거절된 거래의 개수

Distributed Trust and POW Elimination

분산된 신뢰를 사용 – 받은 블록을 확인하고, 그 확인 과정의 오버헤드를 줄이기 위해서

다음과 같은 과정을 따른다.

1. 처음으로 거래하는 유저의 모든 트랜잭션은 악의가 있다고 가정하고 확인되어야 한다.

2. 이번 트랜잭션의 PK와 이전 트랜잭션의 출력 PK와 비교하여 요청자가 특정 원장에 트랜잭션을 추가할 권리를 가지고 있는지 확인한다.

3. 요청자의 서명은 그 거래에서 그의 PK를 사용하여 확인한다.

4. 검증자는 현재 트랜잭션이 성공인지 실패인지 판단해서 둘 중 하나만 증가시킨다.

위 단계가 성공적으로 통과되면 트랜잭션은 확인이 된 것이다.

각각의 CH는 직간접적인 증거를 기초로 신뢰 등급을 유지한다.

Direct evidence