서론

현재 네트워크로는 계속해서 늘어나는 IoT 장비들을 제어하기 힘들 것이라 판단

블록체인에 대해 정의

블록체인의 핵심인 합의 알고리즘에 대해 설명

블록체인

블록체인은 비트코인을 위해 고안된 기술

P2P네트워크 상에서 안전한 거래가 가능하도록 고안: 이를 위해 해시 함수, 디지털 서명 사용

블록체인 구성 - 블록 헤더, 블록 바디

블록 헤더 – 이전 블록 헤더의 해시 값이 들어있어 linked-list 방식처럼 모든 블록이 연결되어 있다. 합의 알고리즘에 이용하는 임의의 nonce값 등이 포함되어 있다.

블록 바디 – 지원하는 서비스(ex 비트코인, 이더리움 등)에 따라 다른 값이 들어간다.

합의 알고리즘

블록체인은 공개되어 있기 때문에 함의 알고리즘을 통해 데이터를 저장해야 한다

합의 알고리즘을 통해 블록체인 내의 데이터 무결성이 보장

PoW(Proof of Work, 작업 증명)

가장 보편적으로 알려진 합의 알고리즘

공식: h(h(n-1 th block header) || nonce) < x, h(x)는 해시 연산

Nonce: 0부터 시작해서 1씩 증가하는 32bits의 수

X: 몇 개의 0으로 시작되는 256bits의 수

해시 연산은 역 연산이 어렵기 때문에 해당 x를 찾기 위해서는 순차적으로 대입해야 함

-> 즉 컴퓨팅 파워가 큰 node일수록 블록생성에 걸리는 시간이 줄어든다.

6개 이상의 node들이 이 연산을 통해 증명 작업을 완료하면 블록체인에 포함

PoS(Proof of Stake, 지분 증명)

계산 능력이 아닌 화폐의 보유량에 따라 각 node의 합의 결정권이 달라짐

PoS를 이용하면 PoW를 사용할 때 보다 보안성이 증가

DPos(Delegated Proof of Stake, 위임된 지분 증명)

투표 결과에 의한 상위 101개의 node에게만 블록 생성 권한을 부여

합의에 걸리는 시간과 비용 감소

단위 시간 동안 생성되는 블록의 개수도 PoW와 PoS에 비해 상대적으로 많음