**Abstract 정리**

많은 분야에서 블록체인 기술을 사용 중이다. 우리는 IoT에 적용하기로 했다.

왜냐하면 현재의 server-client 기술로는 수천 수만 개의 IoT장비를 동기화하는데 한계가 있기 때문이다. 그래서 블록체인을 이용해서 IoT 시스템을 만들 것이다.

RSA 공용키 암호화 방식을 사용. 공용키는 이더리움에, 개인키는 개별 장치에 저장되게 한다. 이더리움을 선택한 이유는 스마트 계약을 사용하기 때문이다. IoT 장치 구성을 쉽게 관리하고 키 관리 시스템을 구축할 수 있게 해준다. 즉 이더리움이 시스템을 제일 세밀하게 관리해줄 수 있다고 생각했다.

**INTRODUCTION 정리**

비트코인 이후 많은 암호화폐가 나타났다. 또한 암호화폐뿐만 아니라 다른 여러 분야에서도 블록체인 기술을 적용하기 시작했다. 하지만 비트코인은 한계점이 존재

1. 블록을 만드는데 10분이 걸림
2. UTXO로 거래 추적 가능, 스크립팅을 지원하지만 루프를 사용할 수 없다. 즉 튜링 완전하지 않다.

즉, 비트코인은 화폐 거래만을 생각해서 만들어진 블록체인 기반의 기술이다.

* UTXO란? Unspent Transaction Output의 약자로 아직 쓰지 않은 잔액이라는 뜻.
* 비트코인에서는 트랜잭션에 의한 결과물들의 합을 잔액이라고 한다.
* 한마디로 거래 단위이며, 거래, 채굴할 때 마다 해제, 생성된다.
* <https://brownbears.tistory.com/382>, <https://steemit.com/blockchain/@niipoong/utxo-bitcoin-trading-and-utxo>
* 튜링 완전이라는 의미: 튜링 머신과 같은 계산 능력을 가진다는 것. 어떠한 문제도 풀어낼 수 있다.

이더리움은 이러한 한계를 고려해서 만든 블록체인이다. 이더리움은 블록 만드는데 약 12초만에 블록을 생성한다. 그리고 스마트 계약이 가능하다 개발자들은 이더리움 위에 프로그램을 작성할 수 있는데 이더리움은 루프를 지원, 즉 튜링 완전하다. 그리고 허가가 있어야 수정이 가능하다.

IoT의 시대가 열리면서 많은 곳에서 IoT를 사용하고 있다. 하지만 기존의 기술로는 수백 수천 개의 IoT 장치들을 동기화 하는데 어려움이 있고, 서버-클라이언트 모델에서 서버가 취약하면 모든 기기에 문제가 생기게 된다.

그러나 블록체인을 사용하면 분산 원장으로 인해 쉽게 동기화가 가능하다. 또한 합의 알고리즘을 사용함으로써 블록체인 안의 데이터를 위조하는 것이 어렵고, 거나 DOS 공격으로부터도 안전하다.

그래서 우리는 IoT 기기 관리에 이더리움을 사용할 것을 제안한다. 스마트 계약을 이용해 IoT 장치를 정의하는 코드를 작성하고, 악성 공격자들을 막기 위해 스마트키 계약에 공공 키 인프라를 구축할 수 있다.