이 재 원 교수 지도
석사학위 청구논문

# 블록체인 기반의 사물인터넷 기기 관리체계의 설계에 관한 연구

2019

성신여자대학교 대학원
컴퓨터학과
이 지 윤

# 블록체인 기반의 사물인터넷 기기 관리체계의 설계에 관한 연구

이 재 원  교수 지도

이 논문을 석사학위논문으로 제출함

2018년 11월

성신여자대학교 대학원

컴퓨터학과

이 지 윤

# 인 준 서

이지윤의 석사학위 논문으로 인준함

2018년 11월

심사위원장_____(인)

심 사 위 원_____(인)

심 사 위 원_____(인)

성신여자대학교 대학원

# 논 문 개 요

사물인터넷의 기기는 소형화되어 무선에 연결된 경우가 대다수이며, 대부분 식별되지 않은 불특정 기기와 접촉한다. 기기 간 상호 통신하기 때문에 감염된 기기가 정상적인 기기와 접촉할 경우 기기를 좀비화 시킬 수도 있다. 또한 DDoS 및 스팸 공격을 일으키거나 기기를 무력화시켜 작동을 중단하고, 서비스를 유지할 수 없게 만들 위험이 상존한다. 이와 같은 문제들은 인적 및 금전적 피해와 부가적인 유지보수 비용을 발생시키기 때문에 이를 대비할 수 있는 시스템이 필요하며, 기기의 보안과 관리가 중요하다. 최근에는 다양한 IoT 기기 모니터링 서비스가 출시되고 있으며, 이는 기기의 상태와 위치, 수집되는 데이터를 관리한다. 하지만 24시간 네트워크에 접속되어야 하는 사물인터넷의 특성 상 서비스를 유지할 수 있는 지속성의 보장이 필요한데, 이와 관련된 서비스의 제공이 부족하다.

본 연구에서는 사물인터넷 환경을 위한 블록체인 기반의 IoT 기기 관리체계 방안을 제안한다. 기존 사물인터넷 환경 내에서 발생하는 IoT 기기 관리에 관한 이슈를 분석한 후, 새로운 메커니즘을 제시한다. 먼저 기기 소유자는 스마트 컨트랙트를 활용하여 자신의 기기를 등록한다. 기기에 문제가 발생하면 소유자를 식별할 수 있기 때문에 책임 추적성을 확보할 수 있고, 검증된 기기만이 접근할 수 있도록 하여 불특정한 기기와의 접촉을 방지하고, 제공되는 서비스에 대한 신뢰성을 높이고자 하였다. 또한 블록체인을 활용하여 분산화 된 체계를 구성하고, 참여자들이 다른 기기의 상태를 공유할 수 있도록 하였다. 마지막으로 기존의 IoT 기기 모니터링 플랫폼에서 지원하지 않았던 서비스의 지속성을 업무 위임을 통해 보완하고자 하였다. 제안한 관리체계 메커니즘을 검증을 통해 적용 가능성을 타진해 보았으며, 이를 적용한다면 안정적인 사물인터넷 환경 조성에 도움이 될 것으로 판단된다.

# 목 차

# 표 차 례

# 그 림 차 례

# 제 1장 서론

## 1. 연구의 배경 및 목적

사물인터넷은 사람과 사물 혹은 사물과 사물 간의 데이터를 교환하는 시스템으로, 인터넷을 기반으로 유기적인 연결을 하여 사용자에게 서비스를 제공한다[1]. 24시간 실시간으로 데이터를 수집하며, 네트워크를 통해 전달된다. 대부분의 산업에서는 사물인터넷을 활용하기 때문에 수집되는 데이터의 양이 방대해져, 이들을 가치 있게 활용하기 위해서 빅데이터와 인공지능과 같은 다른 기술과 연계하여 서비스를 제공하는 지능형 사물인터넷으로 발전하고 있다.

하지만 사물인터넷 기기는 식별되지 않은 불특정 기기와의 접촉으로 인해서 DDoS와 해킹에 취약하고, 악성코드 감염으로 인해 잘못된 기기 제어 등의 위험성이 내재되어 있어 이러한 문제에 대하여 대비할 수 있는 시스템이 필요하다. 또한 기기의 연결이 끊긴다면 상호 통신하는 기기의 작동에도 영향을 미쳐 서비스가 중단될 수 있기 때문에 지속성의 보장이 필요하다. 특히 인공지능과 빅데이터와 같은 다른 기술과 연계될 경우에는 입력 데이터에 따라 출력이 달라지기 때문에 수집되는 정보에 대한 신뢰성과 연계성이 요구된다. [그림 1]은 사물인터넷 환경 내에서 발생하는 보안 사고로 인한 피해 추산치를 나타낸다[2].

■ 사물인터넷 보안 사고로 인한 경제적 피해 추산치 (조원)


※ 자료 : 산업연구원

■ 전세계 사물인터넷 보안 지출 전망 (백만 달러)

| 2014년 | 2015년 | 2016년 | 2017년 | 2018년 |
|---|---|---|---|---|
| 231.86 | 281.54 | 348.32 | 433.95 | 547.20 |

[그림 1] IoT 보안 사고로 인한 경제 피해액 추산

블록체인은 네트워크 내 모든 참여자 간에 거래 내역을 공유하기 때문에 사실상 위조와 변조, 해킹이 불가능하며 투명성이 보장된다. 이에 본 연구에서는 블록체인 기반의 IoT 기기 관리 체계를 제안한다. 기기인증을 통해 기기에 대한 책임 추적성과 제공되는 서비스에 대한 신뢰성을 확보하며, 업무 위임을 통한 서비스의 지속성을 보장하고자 한다.

## 2. 논문의 구성

본 논문은 2장에서 사물인터넷의 이론을 정리하고, 기기 모니터링 및 기기인증 관련 연구를 통해서 동향을 분석 후 블록체인의 전반적인 개념을 정리한다. 3장에서는 사물인터넷에서 발생할 수 있는 기기 관리에 관한 이슈를 분석하고, 4장에서는 3장을 바탕으로 블록체인 기반의 기기 관리 메커니즘을 제안한다. 5장에서는 설계한 메커니즘을 프로토타이핑을 통해 적용 가능성을 확인하며, 6장 결론 및 향후 연구로 마무리 한다.

# 제 2장 관련 연구

2장에서는 사물인터넷과 블록체인에 대해서 기술한다. 먼저 사물인터넷의 정의와 주요 기술을 통해 이론을 정리하고, 기기인증에 사용되고 있는 인증 프로토콜 유형과 기기인증 관련 연구를 통해 동향을 파악한다. 또한 기존에 제공되고 있는 대표적인 IoT 기기 모니터링 플랫폼을 분석한다. 다음으로 블록체인의 개요와 구조, 동작 원리, 블록체인 2.0의 대표적인 기술인 스마트 컨트랙트에 대해 설명하여 블록체인의 전반적인 개념을 정리한다. 마지막으로 거래 검증을 위한 합의 알고리즘을 구체적으로 살펴본다.

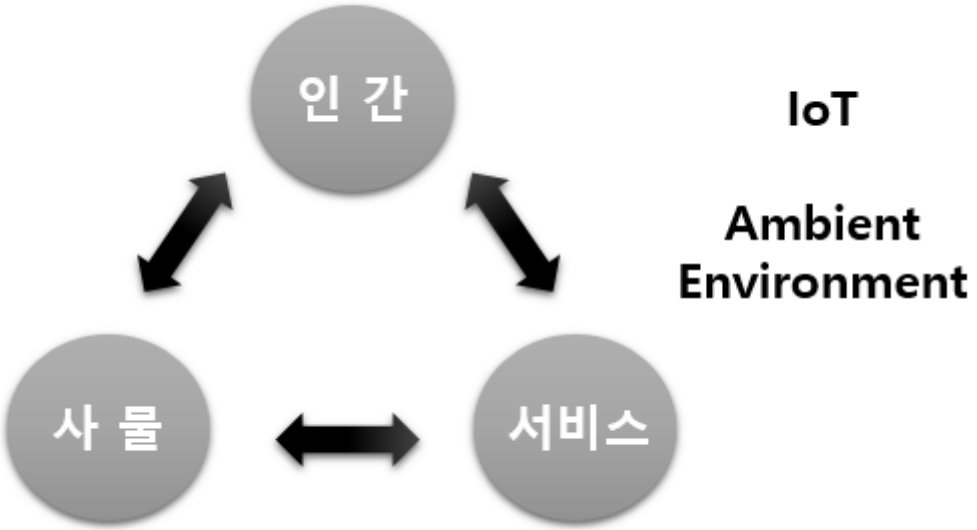
## 1. 사물인터넷

### 1) 사물인터넷 개요

사물인터넷(Internet of Things, IoT)은 1999년 Kevin Ashton이 “사물(Things)에 RFID(전자태그)와 기타 센서를 탑재하여 사물인터넷이 구축될 것”이라고 전망하면서 처음 사용되었다. 사물인터넷은 분야와 기관마다 내리는 정의가 각기 다르다. 미래창조과학부에서는 “사물인터넷은 사람·사물·공간·데이터 등 모든 것이 인터넷으로 서로 연결되어 정보가 생성·수집·공유·활용되는 초연결 인터넷”으로 정의하였다. 국제전기통신연합의 산하기관인 ITU-T에서는 “기존에 존재하는 혹은 향후에 존재할 상호 운용이 가능한 정보 기술 및 통신 기술을 활용하여 다양한 물리 및 가상 사물 간의 상호 연결을 통해 진보된 서비스를 제공할 수 있게 하는 글로벌 스케일의 인

프라"라고 정의하였다. CERP-IoT(Cluster of European Research Projects on the Internet of Things)는 "미래 인터넷의 통합 부분이며, 물리적 혹은 가상의 식별자를 가진 표준 및 상호 운용 통신 프로토콜, 물리적 형태와 지능, 자동 구성 기능과 역동적인 글로벌 네트워크 인프라"로 정의하였다.

사물인터넷은 크게 인간·사물·서비스 세 가지의 구성요소로 이루어져있으며, 이는 유기적으로 연결되어있다. 인터넷을 통해 상호 통신을 하는 사물끼리 데이터를 주고받으며, 다른 기술과 결합하여 가치 있는 정보를 생성하여 사용자에게 서비스를 제공한다[1].



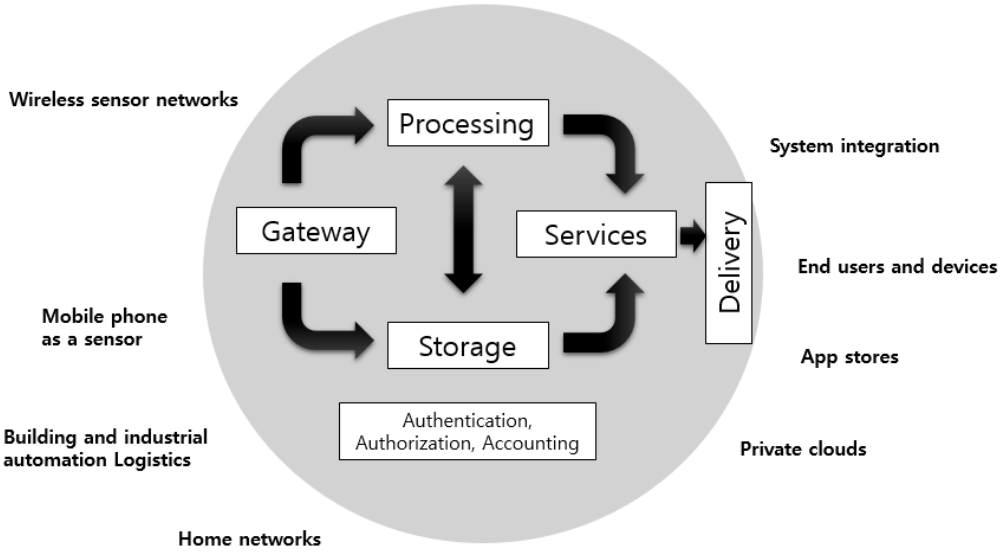

[그림 2] IoT 3대 주요 구성 요소

사물인터넷이 되기 위해 충족되어야 하는 다양한 필수 요소들이 제시되고 있다. 관점에 따라 필수 요소가 제시되는데, 맥락적으로 지능/연결과 소통/새로운 가치 제공으로 나눌 수 있다[3].


[그림 3] 맥락적 관점에 따른 사물인터넷 필수 요소

먼저 사물이 인간의 개입 없이도 스스로 판단하고 행동할 수 있는 '지능'이 요구된다. 사물이 스스로 정보를 수집하고, 이를 전송하는 주체적 행위가 가능해야 함을 의미한다. 또한 사물들은 서로 네트워크로 '연결'되어 서로 간 정보를 주고받고 '소통'할 수 있는 상호 통신이 가능해야 한다. 이렇게 네트워크를 통해 이루어지는 상호 통신이 주체적으로 지능적 판단을 거쳐 '새로운 가치를 제공'해야 하고, 더 높은 수준의 서비스를 제공할 수 있어야 한다.

사물인터넷은 데이터 기반의 기술로, 일반적으로 센서를 통해 데이터를 수집하여 이를 네트워크에 전달한다. 24시간 동안 네트워크에 접속되어 쉬지 않고 실시간으로 수집하고, 전송하며, 다음 그림은 이를 나타낸 것이다 [4].




출처 : Tampere University of Technology, http://www.tkt.cs.tut.fi/research/waps/

[그림 4] 사물인터넷의 데이터 수집과 전달

[그림4]의 프로세스와 같이 사물인터넷의 서비스를 구현하기 위해서는 핵심 기술이 필요하다. Gartner에서는 IoT 실현을 위한 핵심 필요 기술을 5개의 요소로 구분하였으며, 상세 내용은 아래의 표와 같다[5].

<표 1> IoT 실현을 위한 핵심 필요 기술

| 요소 기술 | 주요 내용 |
|---|---|
| 센서데이터 최적화 및 관리 기술 | IoT 서비스는 수많은 장치로 구성되고, 장치 간 데이터 전송이 빈번하게 발생하기 때문에 전력 소모가 많아진다. 이러한 이유로 네트워크의 저전력화를 위한 데이터의 경로 설정 및 흐름제어 등의 데이터 전송 효율화 기술이 중요하다. |

| 요소 기술 | 주요 내용 |
|---|---|
| 저전력 네트워킹 기술 | 통신방식에 따라 데이터 전송률, 통신반경, 단말 가격, 소모 전력이 달라지는데, 데이터 전송률은 낮지만 저전력을 사용하는 ZigBee, Bluetooth LE, Sub-GHZ 방식 및 Zwave 방식이 사용된다. |
| 저전력 임베디드 OS 기술 | 저사양의 장치에서 사용되는 HW모듈은 제한적 메모리와 성능을 가지게 되는데, 데이터 수집과 데이터 전송을 효율적으로 관리하는 경량 OS가 필요하다. TinyOS, NanoQplus 등이 사용된다. |
| 저가격·저전력 프로세서 기술 | 장치의 빠른 확산을 위해 제품의 가격이 저렴해야하며, 이는 장치 보급에 선순환을 가져올 수 있다. |
| 새로운 전력공급 및 저장 기술 | 장치 형태에 따른 플렉시블 전력 공급 장치와 장시간 사용할 수 있는 고밀도 배터리 기술이 필요하다. |

사물인터넷은 위의 기술들을 바탕으로 사용자에게 기존보다 수준 높은 서비스를 제공한다. 기기 내부에 탑재된 센서들을 통해서 상호간 통신을 하여 실시간으로 데이터를 수집하게 되며, 이들은 네트워크를 통해 전달하게 된다. 하지만 단순히 센서를 통해 데이터를 수집하는 것만으로는 어떠한 가치를 생산할 수는 없다. 대부분의 산업에서 사물인터넷을 활용하고 있는데, 그 양이 방대해져 다루기가 쉽지 않다. 데이터는 그 자체로는 가치를 제대로 살릴 수 없다. 가치 있는 정보를 생성하기 위해서 빅데이터나, 인공지능과 같은 타 기술과 연계하는 연구와 기술개발이 진행되고 있으며, 지능형 사물인터넷으로 발전하고 있다.

수집된 다량의 데이터들에서 필요한 데이터를 추출하기 위해서는 실시간으로 분석 및 저장이 가능한 비정형 데이터 분석 기법인 빅데이터 기술과 유기적으로 연결될 수 있는데, 데이터들은 저장/관리/분석의 단계를 거쳐 하나의 정보로 생성된다. 인공지능과도 연계가 되는데, 수집된 다량의 데이터 속에서 인간의 지능을 모방하기 위해 학습에 필요한 규칙, 모델 혹은 알고리즘과 같은 필요한 정보를 습득한다. 이를 통해 판단이 이루어지게 되며, 인공지능이 탑재된 사물은 이를 기반으로 행동을 하게 된다. 다음 절에서는 사물인터넷 기기 관리 관련 연구를 보다 구체적으로 설명한다.

### 2) 기기인증 관련 연구

사물인터넷 관련 초기 연구는 활용방안에 대한 연구가 대다수였다. 하지만 봇넷에 의한 기기의 감염, 비인가된 접근으로 인한 수집된 정보의 유출, 데이터의 위조 및 변조, 개인정보의 유출, 기기의 오작동 등의 문제가 발생하고 있다. 최근에는 익스플로잇을 사용한 기기 접근 권한을 탈취하는 악성코드가 증가하고 있으며, 의료 기기를 해킹하여 약물을 과다 투여할 수 있음을 시연을 통해 입증하였다[9]. 이와 같이 빈번한 보안 사고로 인해 위협분석과 기기인증을 포함한 대응 방안과 같은 보안 관련 연구가 지속되고 있다.

홍성혁 등의 연구[10]에서는 홈 IoT를 기반으로 기기에서 발생하는 보안 위협과 대응 보안 기술에 대해 분석하고, 기기인증에 관한 이슈를 제기하며 기기인증의 필요성을 언급하였다. 또한 보안기술을 크게 펌웨어 보호, 기기인증, 응용보안, 암호기술, 보안 칩 적용으로 나눠서 보안 기술의 중요성을 강조하였다. 다음은 통용되고 있는 IoT 기기인증 프로토콜 유형을 정리한 표이다[11].

<표 2> IoT 기기인증 프로토콜 유형

| 프로토콜 유형 | 상세 내용 |
|---|---|
| ID/PW | 인증 과정이 간단하지만 해킹이 쉽고, 사람의 개입 없이 사용되는 IoT 환경의 특성상 서버 관리의 문제점이 존재한다. |
| MAC Address | 인증 과정이 간편하고, 신속하나 위조가 가능해 별도의 보안 장비가 요구된다. |
| 암호 프로토콜 | 다양한 인증 방식이 존재하기 때문에 사용 환경에 맞게 인증 방식 선택이 가능하지만 암호 기술 자체에 취약점이 발견되면 인증 기술의 취약점으로 연결된다. |
| 인증서 | 인증 과정이 간단하지만, 해킹이 쉽고, 사람의 개입 없이 사용되는 IoT 환경의 특성 상 서버 관리의 문제점이 존재한다. |
| IBE | 키의 길이가 짧고, 연산 량이 적지만 ID 위장 공격에 취약하다. |

사용자 인증을 통해 기기인증을 진행하고 있는 경우도 있는데, 회원가입의 절차를 최소화하기 위해 소셜 기반의 로그인 서비스가 이에 해당한다. 또한 생체정보를 활용한 FIDO 인증 기술이 활용되고 있으며, 이 외에도 기기인증을 대체하는 기술 개발과 기기인증 관련 연구가 꾸준히 진행되어 왔다.

유기순 등의 연구[12]에서는 데이터 누출 및 위·변조 방지를 위한 경량 보안 프로토콜을 제안하였다. IoT 기기에서 BLE(Bluetooth Low Energy) 통신을 하는 어플리케이션에 적용 가능한 경량 보안 프로토콜을 설계 및 구현하였다. 이는 인증과 메시지 암호 기능을 제공하는데, SHA256- HMAC, PRESENT, LEA 알고리즘을 바탕으로 사용자 인증, 메시지 인증, 메시지 암호화 기능을 지원한다. 이 프로토콜을 통해 전송되는 개인정보를 포함한

주요 정보의 누출을 방지하여 기존 보안 기술을 개선하고자 하였다.

박병준 등의 연구[13]에서는 블록체인 기반의 IoT 기기인증 스킴을 제안하였다. 램포트 해시체인과 램포트 서명, 블록체인에 대해 분석하고, 기존 인증 프로토콜을 분석을 하여 취약점을 도출 후 이를 보완하기 위해 블록체인과 램포트 해시체인을 활용하여 경량화된 스킴을 제안하였다. 단순 해시 연산만을 요구하기 때문에 저성능 IoT 디바이스에서도 동작이 가능하도록 하여, 안전한 인증을 보장할 수 있도록 하였다.

Muhamed Turkanovic등의 연구[14]와 Parikshit N. Mahalle 등의 연구[15]에서는 사물인터넷 기기인증에 시도 응답 기반 인증기술을 활용하였다. 기기나 인증 서버가 랜덤한 값을 생성하여, 이를 상대방에게 전송한 후 상대방은 랜덤 값과 패스워드 함수 알고리즘을 적용한 결과를 반환한다. 응답을 받은 상대는 클라이언트와 같은 해시 단계를 거쳐 결과 값을 비교하여 인증을 진행한다.

마영철[16]은 기존 사물인터넷의 특징을 악용하는 위협을 방지하고, 기존 인증 기술의 한계점을 해결하기 위한 접근 방안으로 NTS(Next-TimeStamp)기술을 이용하였다. 단말기 고유의 특성과 통신의 특성을 이용한 정보를 사용하는 기술로, 주기적인 점검이 이루어질 때 단말기의 다음 응답 예측 값인 NTS를 사용한다. 매 인증마다 인증 정보가 달라져 재전송 공격이나 위장공격에 강력한 대응을 가지고 있으며, 기기 변경이 불필요하여 기존 운영환경에 즉시 적용할 수 있다는 장점이 있다.

기업에서도 기술 개발과 연구를 진행하고 있는데, 특히 시옷(CIOT)의 보안 터널 기술이 눈에 띄었다. 보안 터널은 기기 구간을 암호화하고, 기기의 인증 접근 제어가 가능하며, 안전하게 키 관리를 할 수 있다. 적용 사례로 CCTV가 무선 공유기를 통해 데이터를 타 기기나 플랫폼에 전송하는 사례가  있다. CCTV를 통해 수집되는 데이터는 녹화되는 영상으로, 개인정보가

포함될 수 있기 때문에 노출의 위협이 존재한다. 무선 공유기로 전송 중에는 데이터 공개가 불필요하므로 이 과정에서는 보안 터널을 통해 데이터를 암호화할 수 있다. 이 외에도 IoT 기기 모듈에 맞춰 H/W 보안 모듈을 경량화하여 최적화 할 수 있으며, 경량화 된 기술을 칩에 넣어 서버와 연결할 수 있다. 하지만 이는 칩 삽입을 지원하지 않은 기존 기기에 적용하기에는 힘든 아쉬움이 있다. 안전한 사물인터넷 환경을 조성하기 위해서는 기기의 다양한 사양들을 고려하는 기기인증 기술이 필요하다.

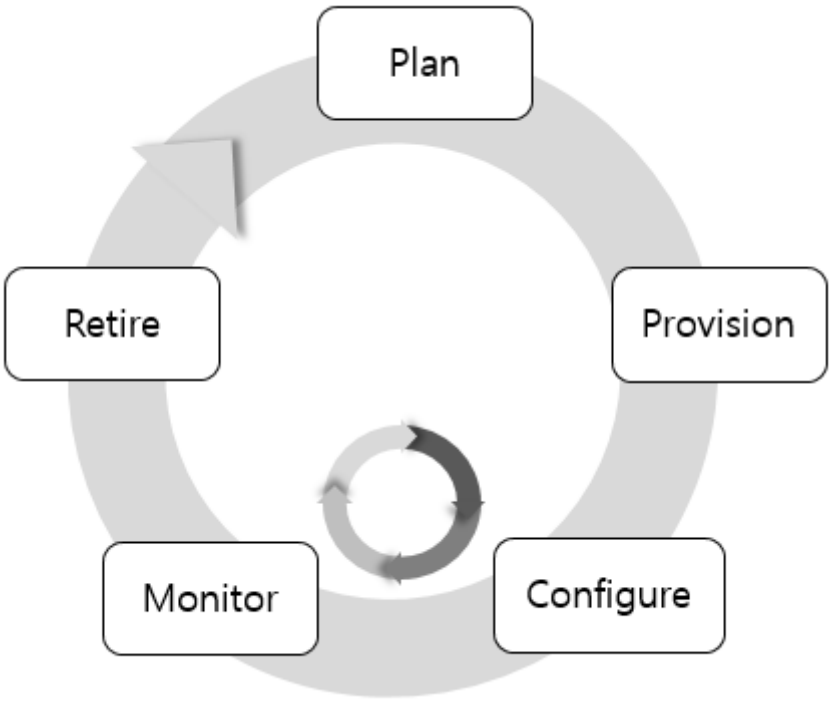
### 3) IoT 기기 모니터링 동향 분석

IoT 기기에서 발생하는 데이터 혹은 기기를 관리할 수 있는 다양한 응용 서비스들이 제공되고 있다. ‘freeboard.io’는 IoT 데이터를 가시화하기 위한 html 기반의 대쉬보드 엔진으로, 여러 IoT 데이터를 실시간으로 모니터링 할 수 있다. 이 외에도 Microsoft Azure의 IoT Hub, 더블체인의 Hdac, IBM의 Watson이 있으며, 구체적인 내용은 다음과 같다.

- Microsoft Azure ‘IoT Hub’

IoT Hub는 클라우드에서 호스팅되는 관리 서비스로, 응용 프로그램과 기기 간의 양방향 통신을 하는 중앙 메시지 허브 역할을 한다. 이를 통해 기기와 클라우드 호스팅 솔루션 백 엔드 간에 안정적이고 안전한 통신을 구축할 수 있으며, 기기-클라우드 원격 분석과 기기에서 파일 업로드 및 클라우드에서 기기를 제어하는 요청-회신과 같은 메시징 패턴을 지원한다. 또한 모니터링을 사용하여 기기 오류와 기기 연결과 같은 이벤트를 추적하여 상태를 유지 관리 할 수 있으며, [그림 5]는 IoT Hub의 기기 수명 주기를 나

타낸 그림이다.




출처 : Microsoft, https://docs.microsoft.com/ko-kr/azure/iot-fundamentals/

[그림 5] IoT Hub 기기 수명 주기

운영자가 기기 그룹을 간편하고 정확하게 대상화하고, 쿼리를 위한 기기 메타 데이터 구성표를 만들 수 있으며, 이 기기 메타 데이터를 태그 및 속성 형식으로 저장할 수 있다.

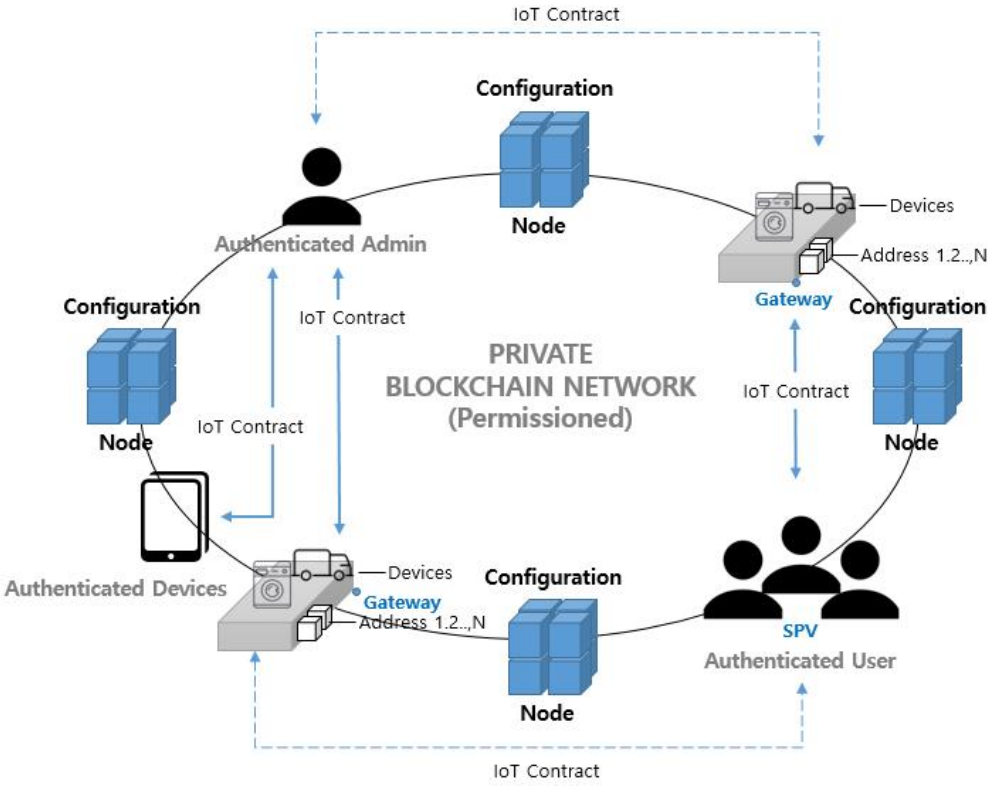
새 기기를 IoT Hub에 안전하게 공급하고, 운영자가 기기의 기능을 즉시 검색할 수 있도록 하며, ID 레지스트리를 사용하여 기기 ID 및 자격 증명을 만들고, 사용할 수 있다. 또한 정상적인 상태와 보안을 유지하며 기기에 대한 구성 변경과 펌웨어 업데이트를 가능하게 한다. 기기 상태와 현재 작업

상태를 모니터링하고 문제 발생 시 운영자에게 알린다. 기기 업데이트 작업 상태를 실시간 보고할 수 있으며, 대시보드 보고서를 작성할 수 있다. 마지막으로 오류가 발생하거나, 서비스 수명 주기가 끝나면 기기를 교체하거나 서비스를 해제할 수 있으며, 물리적 기기를 바꾸는 경우에는 기기 정보를 유지하거나 사용이 중지될 경우에는 보관한다[6].

IoT Hub는 기기 관리에 용이한 서비스로, 기기의 상태를 모니터링 할 수 있는 점이 본 연구와 비슷하지만, 클라우드 기반이 아닌 블록체인 기반의 기기 관리 체계를 구축하여 기기의 상태를 운영자 뿐만 아니라 참여하는 참가자들이 공유할 수 있도록 보완하여 차별점을 두고자 하였다.

- **더블체인 'Hdac'**

빅데이터를 통해 Blockchain IoT를 기반으로 구현된 플랫폼으로, 용도에 따라서 사용을 제한할 수 있고 연결된 모든 디바이스를 제어한다. 안전한 인증, 높은 신뢰성, 다양한 가용성에 기초하여 IoT 기기 간 상호 인증 체계를 조성하고자 하며, 인증된 블록체인 노드, 사용자, 디바이스, 게이트웨이들을 private 블록체인에서 운용한다. 사용자는 권한이 부여된 게이트웨이 혹은 디바이스를 제어한다. 접근 권한과 상황에 따라 기기 제어가 가능하고, 사용자와 기기의 권한을 블록체인에 보관하여 조회할 수 있도록 한다. 또한 DDoS, 스니핑 등과 같은 보안 위협에 대응할 수 있도록 IoT 위협 탐지를 통해서 블록체인 상에서 이루어지는 사용자 기기 간의 변경 사항을 상시 모니터링 하여 이상 상황을 관리자에게 통보하도록 한다[7].




출처 : 더블체인, http://doublechain.co.kr/03service/service_business_01.php#nolink

[그림 6] IoT 블록체인 네트워크 구성

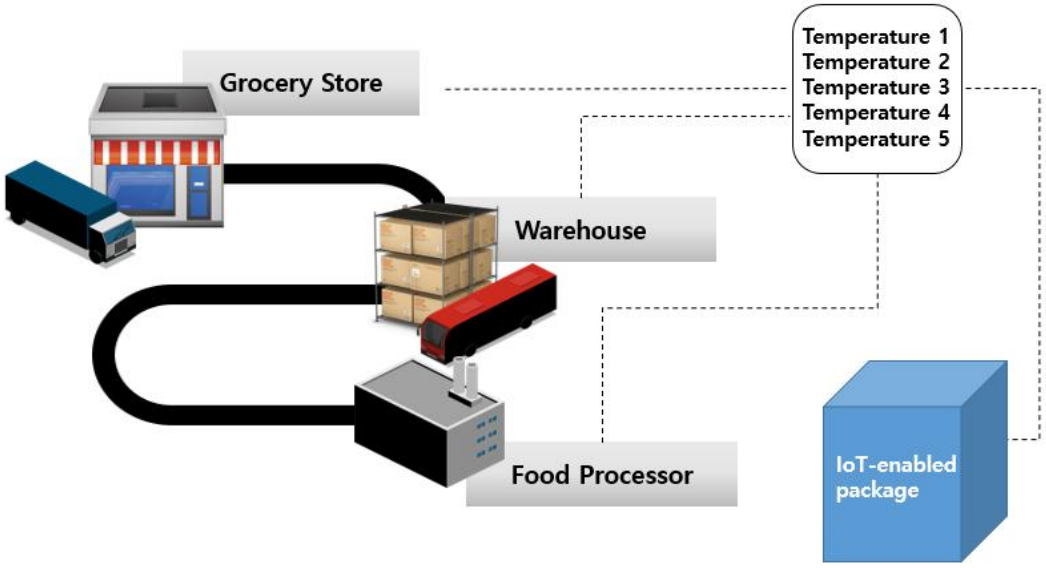
Hdac은 블록체인 기반의 관리 체계라는 점이 본 연구에서 제안하고자 하는 체계 방안과 유사하다. 하지만 안면 인식을 통한 사용자 인증과 기기 간 상호 인증 체계를 조성하는 것과 달리 본 연구에서는 스마트 컨트랙트를 통한 기기인증을 하여 이를 차별점으로 두었다.

- IBM 'Watson IoT Platform Blockchain Service'

IBM Watson IoT Platform Blockchain Service는 Watson IoT Platform에서 추가적으로 제공하는 프로그램으로, 블록체인을 활용하여 신뢰성과 투명성을 높이고, 기기의 활용을 극대화할 수 있다. 또한 프로세스를 자동화하고 간소화하여 공급망 내에 발생하는 지연 문제와 낭비, 분쟁을 최소화 할 수 있다.

기기가 데이터를 전송하면, 이는 private 블록체인에 기록되며 모든 참여자들과 데이터를 공유한다. 중앙 통제와 관리 없이 데이터에 접근하고 공급할 수 있으며, 기기의 위치와 유지보수 상태를 추적하고 모니터링을 할 수 있으며, 블록체인에 참여한 모든 노드가 이를 확인할 수 있다.

크게 화물 운송, 구성 요소 추적 및 준수, 운영 유지 관리 데이터 기록으로 나누어서 활용 방안을 설명할 수 있다.




출처 : IBM, https://www.ibm.com/us-en/marketplace/iot-blockchain

[그림 7] Blockchain and the Internet of Things explained

화물 운송 시에는 선박 컨테이너의 온도와 위치, 상태 및 도착 시간을 시스템을 통해 기록하고, 확인할 수 있다. 이를 통해 당사자 간에 발생하는 데이터를 신뢰할 수 있고, 제품을 신속하고 효율적으로 운반할 수 있다. 항공기나 차량 같은 경우에는 이들을 구성하는 구성 기기들을 추적하여 규정을 준수하고, 안전을 확보한다. 블록체인에 저장된 데이터를 통해서 당사자들은 수명 전반에 걸쳐서 구성 요소를 확인할 수 있으며, 이를 규제 기관과 운송업체, 제조업체와 공유하여 안전을 확보하고, 효율적으로 비용을 절약할 수 있다. 운영 유지 관리 데이터 기록을 통해서 IoT 기기는 중요한 시스템의 안전 상태와 조직의 유지 관리 상태를 추적하는데, 유지보수를 위해서 블록체인을 모니터링하고, 작업을 기록할 수 있는 서비스를 제공한다[8].

Watson IoT Platform Blockchain Service는 블록체인 기반의 기기의 활용을 극대화할 수 있는 서비스로, 구성 기기들을 추적할 수 있으며, 수집되는 데이터에 대한 모니터링이 가능하며, 이는 유통에 용이하게 사용될 수 있다. 하지만 공급 중 구성된 기기에 문제가 발생할 경우 책임을 추적할 수 있으나, 기기의 조치가 신속하게 처리되지 않는다면 공급되는 상품에 문제가 발생할 수 있다. 본 연구에서는 업무 위임을 통해 위의 상황에서 요구하는 서비스 지속성 부분을 보완하여 안정적인 환경을 제공하고자 한다.

## 2. 블록체인

### 1) 블록체인 개요

블록체인은 “거래정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 P2P 네트워크에 분산하여 참여자가 공동으로 기록하고 관리하는 기술”이라고 정의할 수 있으며, 탈중앙화의 분산화된 구조를 가지며, 데이터를 저장할 수 있는 구조를 가졌다[17]. 가명의 개발자 Satoshi Nakamoto가 발표한 논문 <Bitcoin : Peer-to-Peer Electronic Cash System>에서 제안한 비트코인으로부터 시작되었는데, 중개인과 같은 금융 기관이 없는 금융거래 플랫폼을 만들고자 하였으며, 전자화폐인 비트코인의 이중 지불 문제를 해결하고자 하였다.

블록체인은 분산원장 시스템으로 노드 간 통신이 이루어지는데, 네트워크에 참여한 모든 노드가 동일한 장부를 소유하고, 데이터를 공유하며, 발생된 거래를 검증하기 때문에 데이터의 위·변조가 어려워 신뢰성과 무결성을 보장한다. 또한 오픈소스에 의해 쉽게 구축할 수 있어 확장할 수 있는 장점이 있으며, 모든 거래 기록에 공개적으로 접근할 수 있어 투명하다[18,19].

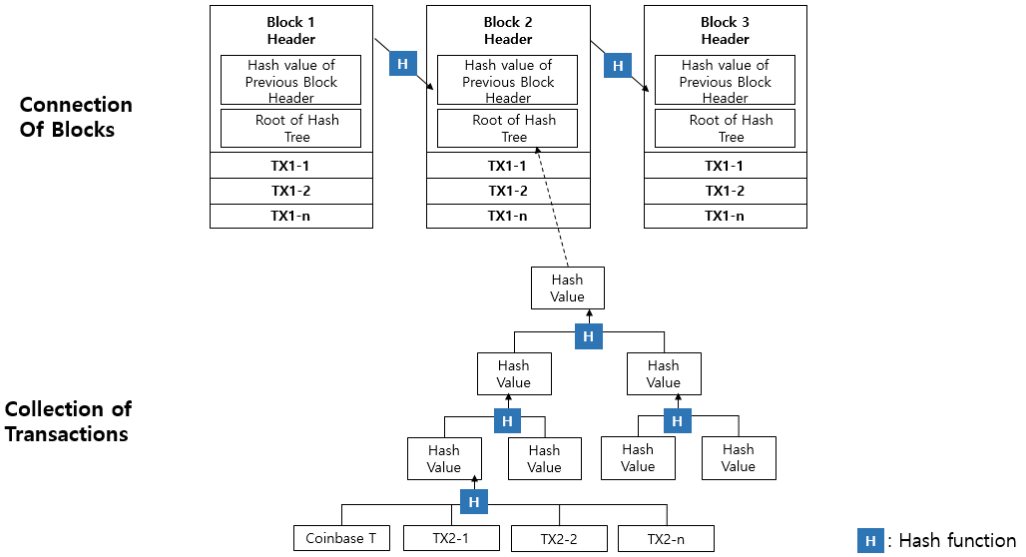
블록체인 네트워크는 참여자의 성격과 범위, 작업증명 참가권한에 따라서 크게 퍼블릭 블록체인, 프라이빗 블록체인, 컨소시엄 블록체인 세 유형으로 분류할 수 있다[20,21].

<표 3> 블록체인 네트워크 유형

| | 퍼블릭 블록체인 | 프라이빗 블록체인 | 컨소시엄 블록체인 |
|---|---|---|---|
| **권한** | 모든 참여자 | 허가된 참여자 | 컨소시엄 참여자 |
| **주요 내용** | - 보편적으로 사용<br>- 네트워크에 접근하는 모든 참여자들은 거래 내역을 포함한 모든 장부 열람 가능<br>- 작업증명 및 지분증명 시 내부 화폐 필요<br>- 위험관리와 안정적인 생태계 조성 필요 | - 독자적으로 사용 가능하며, 하나의 개체가 내부 관리 | - 반 중앙형 블록체인으로, 기관들이 컨소시엄을 이뤄 구성함<br>- 노드 간 합의된 규칙을 통해 공증된 참여 가능<br>- 참여자 간 비즈니스 계약과 시스템의 안전 보장 요구 |
| **특징** | - 네트워크 확장이 어려움<br>- 트랜잭션 속도가 느림 | - 비교적으로 트랜잭션 속도가 빠름 | - 네트워크 확장이 비교적 쉽고,<br>트랜잭션 속도가 빠름 |

## 2) 동작 원리

블록에는 거래 내역이 기록되는데, 다음 그림과 같이 전자서명을 통해 서로 연결되어있다. 각 블록들은 모두 연결되어 있으며, 서로의 유효성을 증명한다.




출처 : Soichiro Takagi, Blockchain Economices: Why it is important for social sciences

[그림 8] 블록체인 구조

블록체인의 첫 번째 블록은 genesis블록이며, 이 후 10분 주기로 블록이 생성되어 사슬처럼 연결된다. 현재의 블록이 유효하기 위해서는 genesis블록부터 모든 블록이 유효해야하는데, 이를 검증하는 과정을 작업증명이라 한다. 작업증명은 적절한 nonce를 찾는 연산 과정이며, 여기서 컴퓨팅 파워가 요구된다. nonce를 구하면 블록이 고정되며, 이는 네트워크에 참여하는

참여자들에게 전파되어 체인을 형성한다[22].

블록들은 해시 알고리즘에 의해 암호화되기 때문에, 입력 값이 바뀌면 결과 값도 변경되므로 이 점을 이용하여 이전 블록과 다음 블록 간의 연결을 검증할 수 있다. 검증된 블록들은 과반의 합의를 통해 확정이 된다.

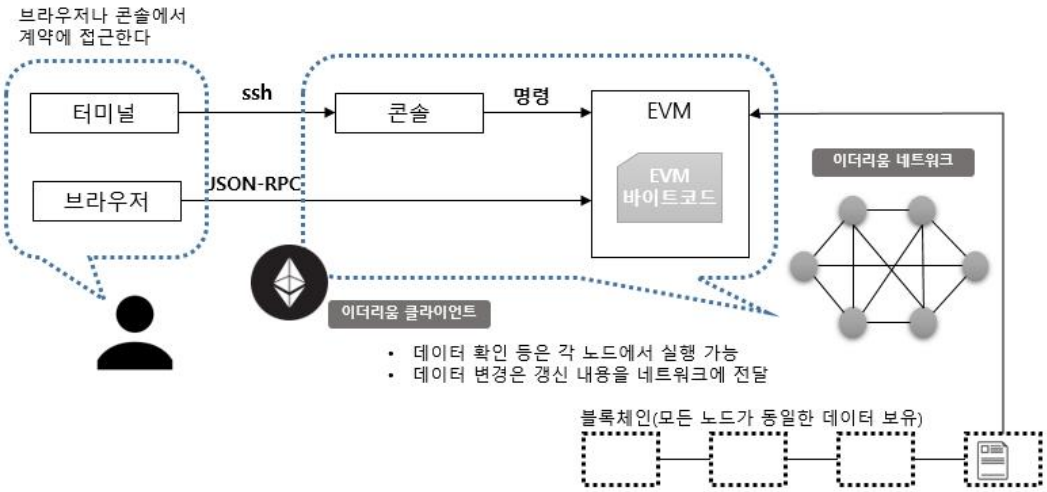
블록체인의 원리를 정리하면 다음과 같다[23].

① 거래 발생 시 네트워크 참여자에게 전파
② 새로운 거래 내역을 블록에 취합
③ 해당 블록에 대한 작업증명 시도
④ 작업증명 성공 시 해당 블록을 네트워크 참여자에게 전파
⑤ 모든 참여자는 해당 블록이 유효하면 승인
⑥ 모든 참여자는 블록 승인 의사 표출

### 3) 스마트 컨트랙트

스마트 컨트랙트(Smart Contract)는 1994년 Nick Szabo에 의해 처음 제안되었으며, 블록체인 2.0의 대표적인 기술로, Christopher D. Clack은 스마트 컨트랙트를 “자동화 된, 집행 가능한 계약이며, 법적 권리 및 의무의 이행을 통해 시행 가능한 계약”이라고 정의하였다[24]. 계약 시 설정된 조건 및 수행 내용을 프로그램 코드로 작성하고, 계약 체결과 동시에 자동으로 실행되며, 이를 통해 신뢰할 수 있는 제 3자의 필요성을 최소화 할 수 있는 기술이다[25,26]. 스마트 컨트랙트는 블록체인의 거래 데이터와 동일하게 처리되어, 데이터를 임의로 조작하기 어렵기 때문에, 거래 내역뿐만 아니라 프로그램 코드에 대해서도 수준 높은 안전성을 제공한다[27].

스마트 컨트랙트를 지원하는 블록체인 플랫폼으로는 대표적으로 Ethereum이 있다. 기존의 비트코인 스크립팅 시스템의 취약점인 상태 저장의 한계와 반복문의 제한을 보완하고, 각 라인을 실행할 때 마다 수수료를 발생시켜 네트워크 상 수수료의 한계를 설정하여 무한루프를 방지하였다.

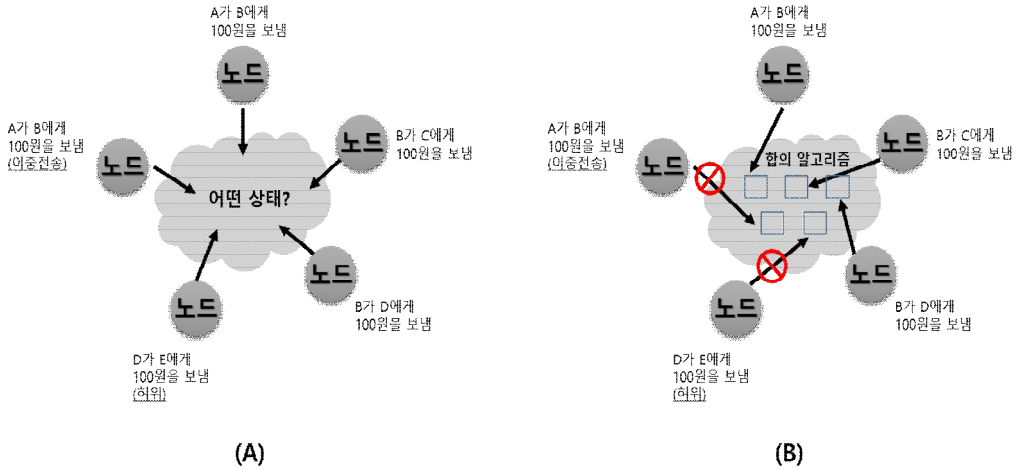



[그림 9] 스마트 컨트랙트 실행 개념도

스마트 컨트랙트 템플릿을 활용하면 비용 및 위험요소절감, 효율성 개선이 가능하며, 강제성·독립성·자율성의 특징을 가지고 있다. 이러한 특징으로 주식거래 서비스, 부동산 거래 서비스, 실물 자산거래 서비스, 전자투표 등 다양한 분야에서 활용되고 있다[28,29].

### 4) 합의 알고리즘

합의 알고리즘은 P2P 네트워크와 같이 정보의 지연과 미도달의 문제점을 해결하기 위한 목적으로 사용되며, 이를 통해 하나의 블록체인을 유지시킨다. 데이터를 변조할 의도가 없어도 이중 송신에 따른 중복의 처리나 잘못된 정보에 의한 오작동 등의 위험이 존재하는데, 합의 알고리즘을 통해 이러한 문제를 해결하며, 아래의 그림은 합의 알고리즘의 역할을 나타낸다[29,30].




[그림 10] 합의 알고리즘의 역할

(A)는 합의 알고리즘이 존재하지 않으면 어느 것이 허위 사실이고, 어느 것이 이중 전송이 되는지 알 수 없음을 나타내며, (B)는 합의 알고리즘을 통해 진위 판단을 할 수 있음을 나타낸다.

대표적으로 사용되고 있는 합의 알고리즘에는 PoW(Proof of Work), PoW(Proof of Stake), DPoS(Delegated Proof of Stake), PoI(Proof of Importance), PBFT(Practical Byzantine Fault Tolerance)가 있다[31].

PoW는 블록 생성을 하려 하는 노드들이 특정 해쉬 값을 찾는 연산을 수행하여 특정한 난이도 작업을 수행함을 증명하는 것인데, 해쉬 값을 찾기 위해 채굴자들은 경쟁을 하고, 특정 채굴자가 목표 값에 해당하는 해쉬 값을 찾게 되면 블록이 생성되는 경쟁 방식이다[32].

PoS는 PoW의 과도한 컴퓨팅 파워 소비 문제를 해결하기 위한 대안으로 제시되었는데, 참여자의 소유 지분이 블록 생성권의 지분율이 되는 합의 알고리즘이다. 컴퓨팅 파워의 낭비를 감소하고, 블록 생성 주기를 단축시킬 수 있어 리소스 관점에서 효율적이나, Nothing at Stake와 초기 코인 분배 문제(Initial Distribution Problem)가 발생할 수 있다[30].

DPoS는 PoS와 달리 지분에 비례한 투표로 대표자를 선출하고, 이들에게 블록 생성과 검증에 대한 권한을 부여하는 합의에 대한 권리를 위임한다. 이 방식을 사용하면 블록 생성 시 소요되는 합의 시간과 비용을 감소할 수 있고, 상대적으로 생성되는 블록의 개수도 많아 속도 면에서 유리하고, 확장성을 향상한다. Slasher, Tendermint 등에 이 방식을 적용하고 있다.

PoI는 NEM에서 사용되는 합의 알고리즘으로 거래량, 거래금액 등 네트워크에 기여도가 많은 참여자에게 기여도 점수를 부여하고, 이를 기준으로 수수료를 분배하기 때문에 거래량과 신용이 중요하다. 단순히 지분율로 수수료를 분배하지 않기 때문에 PoS보다 동등한 기회를 제공한다.

PBFT는 비잔틴 장군 문제 발생 시에도 네트워크 합의를 보장하는 알고리즘이다. 네트워크 참여자 중 1명이 프라이머리가 되며, 클라이언트의 요청 순서를 정렬하고, 결과를 기입하여 다른 노드들에게 전파하는 역할의 노드가 된다. 프라이머리는 자신을 포함한 모든 참여자에게 요청을 보내고, 이후 결과를 집계하여 다수의 값을 사용해 블록을 확정한다[31]. 일정 비율 이상의 노드가 합의하면 블록이 검증된다는 점이 DPoS와의 차별점이다.

프라이빗 블록체인은 참여한 노드들이 이미 검증되었기 때문에, 악의적인

의도를 가진 참가자를 가려내는 것보다는 파이널리티 불확실성(Finality Uncertainty)과 성능이 중요하다. PBFT는 다수의 의사를 반영하여 결정하기 때문에, 다음 블록 생성 시 체인의 분기가 발생하지 않아 결제 완료성이 보장되고, 반복적 연산을 하지 않아 전력과 컴퓨팅 자원의 소모가 적어 성능과 속도면에서 유리하다. 이와 같은 이유로 블록체인 오픈 소스 플랫폼 중 Eris와 Hyperledger와 같은 프라이빗 블록체인에서 주로 채택된다.

# 제 3장 사물인터넷에서의 기기 관리에 관한 이슈 분석

사물인터넷은 데이터 기반의 기술로 수집되는 데이터에 있어 무결성과 연계성, 신뢰성이 요구된다. 또한 기기를 통하여 데이터를 수집하고, 다른 기기와의 상호 통신으로 수집된 데이터를 전송하기 때문에 최근에는 기기의 보안과 관리의 중요성이 대두되고 있다. 사물인터넷은 기기의 탈취와 도난, 해킹 및 비인가된 접근 등으로 인한 데이터의 위조 및 변조와 같은 보안 위협에 치명적이다. 또한 감염된 기기가 정상적인 기기와 접촉하여 이를 좀비화 시키고 DDoS 및 스팸 공격을 일으키거나 기기를 무력화 시켜 작동을 중단하여 서비스를 유지할 수 없게 만든다. 이와 같은 문제들은 인적 피해 및 금전적 피해로 연결되기 때문에 식별되지 않은 기기와의 접촉을 방지하여 신뢰성을 확보하여야하고, 안정적인 환경이 조성되어야한다.

먼저, 기기가 참여하고 있는 네트워크 혹은 플랫폼의 신뢰성을 높이기 위한 방안의 하나로 기기인증을 통해 식별된 기기만이 참여할 수 있도록 해야한다. 사물인터넷은 기기를 활용하여 데이터를 수집하고, 상호통신을 하기 때문에 다른 기기와의 접촉이 많다. 특히 사물인터넷은 소형화로 무선 인터넷에 연결된 경우가 많은데, 이 같은 경우는 어디서 해킹 공격이 시도되고, 악성코드가 감염이 되는지 파악하기 어렵기 때문에 비인가된 접근을 방지하여야 한다. 기기인증에 사용되는 인증서나 암호 프로토콜 등은 높은 연산과 처리량을 요구하기 때문에 저사양 기기에서는 이를 수용할 수 없다. 또한 새로운 보안 기술을 탑재하기 위해서는 새로운 기기를 생성하거나 별도의 칩을 기기에 삽입하기도 하는데, 이와 같은 경우는 기존 기기에 적용하기에 한계가 있기 때문에 기기의 다양한 사양들을 고려하는 기기인증 기술이 필요하다.

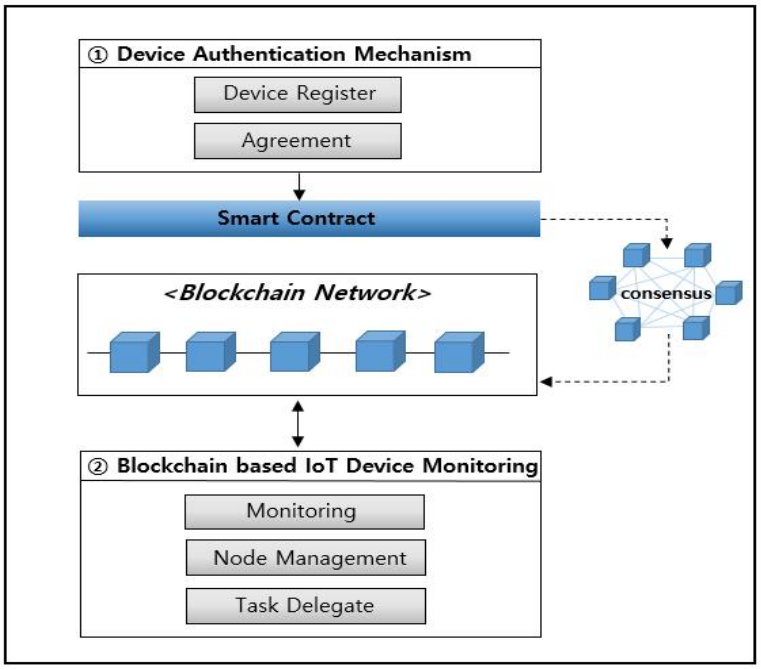
사물인터넷에서의 서비스를 안정적으로 이용하기 위해서는 지속성도 고려되어야 한다. 기기는 24시간 네트워크에 연결되어 중단 없이 계속 유지되어 한다. 다른 기기와 상호 통신하기 때문에 하나의 기기가 연결이 끊긴다면, 타 기기의 작동에도 영향을 미칠 수 있으며, 서비스가 중단될 수 있기 때문에 지속성의 보장이 필요하지만 이와 관련된 연구는 미흡하였다.

안정적인 서비스를 제공하기 위해서 사물인터넷 모니터링 및 기기 제어 서비스를 제공하는 응용 프로그램이 있지만, 대다수 데이터 관리 관련 시스템이었으며, 기기 관리 서비스를 제공하는 솔루션은 부족하였다. 또한 다수가 중앙 집중 형 관리 체계로 유지되고 있기 때문에 시스템과 서비스에 대한 데이터 위조 및 변조, 잘못된 기기 제어 등의 위험성이 내재되어 있고, DDoS와 해킹에 취약하기 때문에 이러한 문제에 대하여 대비할 수 있는 시스템이 필요하다.

# 제 4장 블록체인 기반의 IoT 기기 관리체계의 설계

본 연구에서는 블록체인을 이용하여 안전한 IoT 기기 관리체계를 설계하는 것을 목표로 하며, 기기인증을 통해 기기와 사용자의 신뢰성을 확보하고, 서비스 지속성, 식별을 통한 책임 추적성의 문제를 해결하고자 한다. 4장에서는 사물인터넷에서의 기기 관리에 관한 이슈를 바탕으로 블록체인 기반의 IoT 기기 관리 메커니즘을 제안한다.

## 1. 설계 개요




[그림 11] 블록체인 기반의 IoT 기기 관리체계 메커니즘

사물인터넷은 기기를 활용하여 데이터를 수집하고, 다른 기기와 상호통신을 한다. 이러한 이유로 기기에 대한 보안과 관리가 필요한데, 불특정 다수의 기기와 접촉하기 때문에 악성코드의 감염과 기기의 제어 및 오작동으로 인해서 데이터 보안 관련 문제가 발생하고 있다.

이러한 문제를 해결하기 위한 블록체인 기반의 IoT 기기 관리 메커니즘을 제안한다. 적용하는 대상으로는 프로젝트 혹은 유통 과정에 참여하는 기기 소유자 그룹 및 플랫폼에서 서비스를 이용하고 있는 다수의 기기를 관리하는 사업자로 볼 수 있다. 메커니즘은 크게 ① DAM(Device Authentication Mechanism)과 ② BIM(Blockchain based IoT Device Monitoring)으로 구성된다.

①에서는 기기인증을 진행하는데, 기기 소유자와 기기의 데이터를 등록하고, 업무 위임 동의 여부 조건을 설정하기 위해 스마트 컨트랙트를 활용한다. 이는 검증이 된 기기만 플랫폼에 접근할 수 있도록 하여 신뢰성을 확보하고, 비인가된 접근을 방지할 수 있다. 기기 소유자가 식별되기 때문에 불특정한 기기에 의해 소유자의 기기가 감염될 가능성을 낮추고, 범죄에 악용될 시 책임을 추적할 수 있어 안전한 서비스 환경을 안정적으로 조성할 수 있을 것으로 생각된다.

다수의 기기를 관리하는 사용자나 사업자는 ②를 통해서 기기의 상태를 한 번에 모니터링 할 수 있어 관리가 용이하다. 노드에 문제가 발생 했을 시 소유자를 알 수 있기 때문에 결함의 발생을 보고하여 이에 대한 조치를 취할 수 있으며, 같은 기능을 수행하는 주변 기기에 업무를 위임할 수 있어 서비스를 지속할 수 있다. 기존 IoT 관련 플랫폼은 중앙 집중의 형식이 대다수이기 때문에 해킹에 취약하지만, 블록체인의 분산 원장 원리를 활용하면 취약점을 보완할 수 있고, 참여자 모두가 노드의 상태를 공유할 수 있는 장점이 있다. 다음 절에서는 세부 기능을 상세하게 설명한다.

## 2. 세부 기능

### 1) DAM(Device Authentication Mechanism)

블록체인 네트워크에 참여하기 위해서는 기기 소유자가 자신의 기기를 사전에 등록하는 기기인증 절차가 필요하다. 기기 소유자는 스마트 컨트랙트를 통해 사용자 지갑 주소, 기기 고유 식별 번호, 영역, 동의 여부를 작성하며, 세부 내용은 다음 표와 같다.

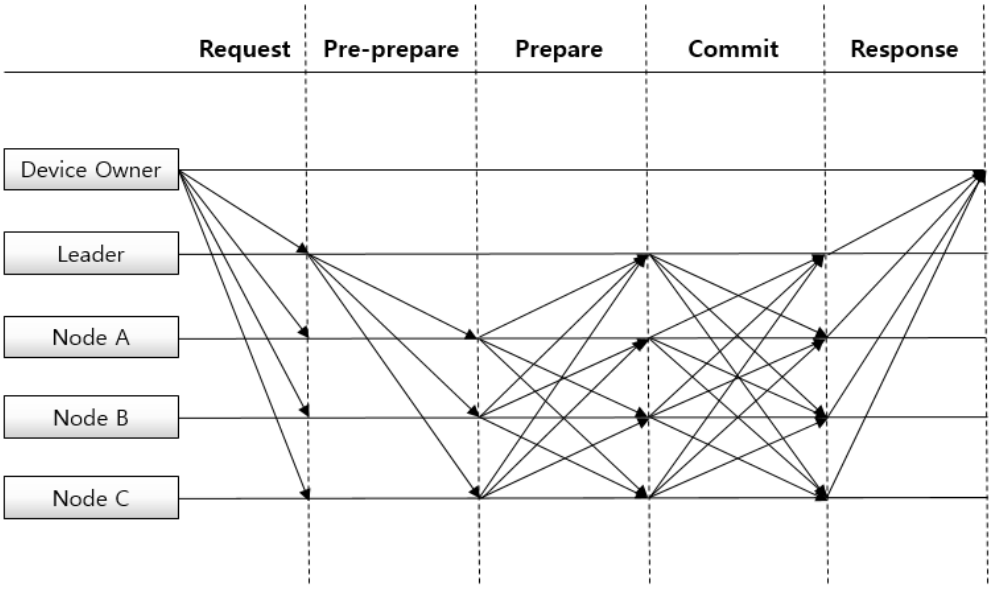
<표 4> DAM 등록 세부 사항

| 구분 | 세부 내용 |
|---|---|
| Device ID | 임의로 부여된다. |
| 사용자 지갑 주소 | 사용자를 식별할 수 있도록 지갑 주소가 수집되어 등록된다. |
| 기기 고유 식별 번호 | 기기 고유 식별 번호를 수집한다. |
| 영역 | 현재 기기가 설치 혹은 작동되어 있는 영역을 등록한다. |
| 동의 여부 | 같은 영역 내 비슷한 기능을 수행하는 기기에 문제 발생 시, 해당 기기의 업무를 넘겨받아 수행한다는 동의를 받는다. |
| 검증 여부 | 최초 검증 여부에는 검증되지 않음으로 작성되었다가 확인 후 검증됨으로 변경된다. |

기기 소유자는 위의 내용을 바탕으로 자신의 기기를 등록하는 것에 대해 합의를 요청한다. 합의 방식에는 Hyperledger나 Eris 등 프라이빗 블록체인에서 채택하고 있는 PBFT 알고리즘을 활용할 것을 제안한다.

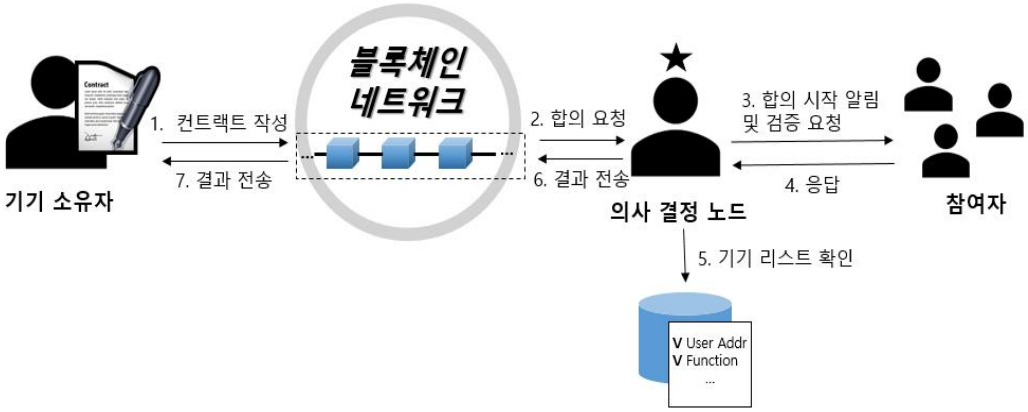
네트워크 내에는 유일한 Leader노드가 존재하는데, 이 노드는 요청에 대

한 결과를 기입하며, 다른 노드들에게 이를 전파하는 역할을 한다. 기기 소유자는 Leader 노드를 포함한 모든 노드들에게 합의 요청을 보낸다. Leader 노드는 모든 구성원들에게 합의의 시작을 알리는 Pre-prepare 메시지를 전달하고, 이를 전달받은 노드들은 검증을 수행한다. 그 결과를 자신을 제외한 모든 노드에게 Prepare 메시지로 전달한다. 전체 구성원들 중 정족수 이상의 노드에게 받은 Prepare 메시지를 Commit 메시지라고 하며, 각 노드는 Commit 메시지를 자신을 제외한 모든 노드들에게 전달한다. 이 과정이 끝나면 모든 노드들은 정족수 이상이 합의한 결과를 가지게 된다.




[그림 12] PBFT 알고리즘 기반의 동작 방식

[그림 12]를 기반으로 한 기기인증 프로세스는 다음과 같다.




[그림 13] 기기인증 프로세스

사전에 의사 결정 노드를 선출하며, 의사 결정 노드는 기기 리스트를 가지고 있다고 가정한다. 이 기기 리스트에는 기기 소유자와 기기를 식별할 수 있는 고유 정보와 그에 따른 기기의 기능 등의 내용을 내포하고 있어, 같은 기능을 하는 기기에 업무를 위임할 때 판단할 수 있는 지표로 활용된다.

기기 소유자는 기기 등록 컨트랙트 작성 후 블록체인 네트워크 참여자들에게 합의를 요청한다. 의사 결정 노드는 참여자들에게 합의를 시작하는 메시지를 전달하면, 참여자들은 검증을 시작하고, 결과를 의사 결정 노드에게 반환한다. 참여자들의 의견과 기기 리스트에 정당한 기기 소유자인지 비교한 결과를 바탕으로 합의 결과를 전송한다.

### 2) BIM(Blockchain based IoT Device Monitoring)

#### - Monitoring

모니터링은 참여하고 있는 기기들 간 유기적으로 연결되어있는 유통과 같은 경우에 적용하면 프로세스 전반에 걸쳐 기기를 용이하게 관리할 수 있고, 구성된 기기들을 확인할 수 있다. 분산환경에서 같은 원장을 공유하는 블록체인 특성을 활용하여 서로의 상태를 실시간으로 공유할 수 있고, timestamp를 통해 언제 어디서 문제가 발생하였는지 책임을 추적할 수 있다.

사용자는 다수의 기기를 영역 별로 모니터링 할 수 있어 기기를 용이하게 관리할 수 있다. 기기의 상태를 모니터링 할 때 기기의 결함이 발생하면 기기 소유자에게 이를 보고하여 조치를 취할 수 있으며, 결함에는 피어나 신호가 끊기는 문제가 해당될 수 있다. 또한 등록된 기기의 컨트랙트에 검증 여부가 검증되지 않음으로 되어있다면, 노드의 연결을 끊어 더 이상 네트워크에 참여할 수 없게 하고, 플랫폼에 접근할 수 없게 한다.

블록체인 기반이기 때문에 참여자 간의 기기 상태를 공유할 수 있어, 유통과 같이 유기적으로 연결되어있고, 참여하고 있는 기기를 전반에 걸쳐 관리하기에 용이하다.

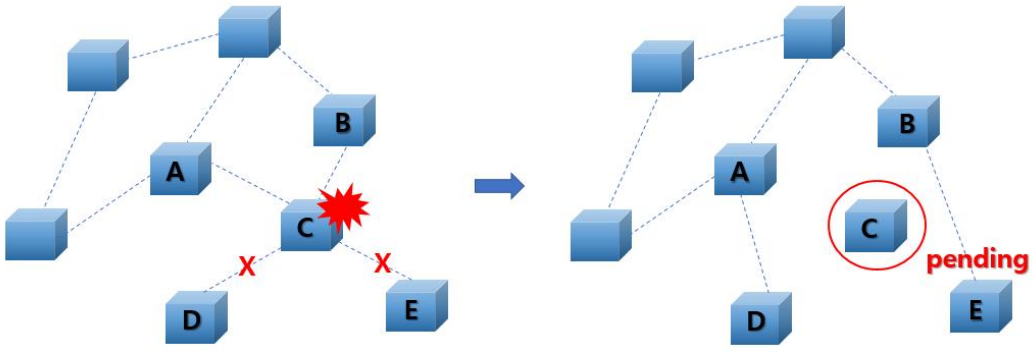
#### - Node Management & Task Delegate

서비스가 유지되기 위해선 기기가 끊임없이 작동되어야하기 때문에 기기의 상태를 고려해야한다. 기기 동작 중지의 경우에는 ① 생성 및 폐기, ② 기기 자체 결함으로 인해 정상적인 동작이 불가할 경우, ③ 서비스 지연으

로 나눌 수 있다.

①, ②, ③과 같이 노드에 변수가 발생하면 주위 노드에게 이를 알려 문제가 되는 노드의 업무를 넘겨받아 서비스가 지속되도록 해야 하며, 전체 네트워크와 구성요소의 기능 자체는 중단 없이 유지할 수 있도록 해야 한다.

[그림8]에서는 노드들이 서로 유기적으로 연결되고 있으며, 하나의 노드에 결함 발생 시 주변 노드에게 이를 알리고, 역할을 대체함을 보여준다. 서비스 관리자는 플랫폼을 통해 보고를 받으면 이를 주변 노드에게 알리고, 문제가 발생한 해당 노드에 조치를 취한다.




[그림 14] Task Delegate 예시

예를 들어 (a)는 C노드에 변수가 발생하여 기능을 유지하지 못하는 경우이다. C노드는 수집된 데이터를 D노드에게 전송하고, E노드로부터 데이터를 전달받아 다른 노드에게 전송하는 역할을 하고 있었지만, 결함 발생으로 인해 이러한 업무를 지속할 수 없다. (b)는 BIM을 적용하여, 결함이 발생한 C노드를 pending하고, 이를 주변 노드인 A노드와 B노드에게 알리고, 역할

을 넘긴다. A노드는 가까운 D노드와 연결되고, B노드는 가까운 E노드와 연결되어 C노드의 기능을 대신하게 된다. pending된 C노드는 서비스 관리자에 의해 조치가 취해지고, 복구가 가능하면 다른 노드와 다시 연결할 수 있어야 한다.

# 제 5장 설계에 대한 프로토타입

## 1. 프로토타입 환경 구성

테스트 환경을 구축하기 위해서 사용자의 지갑은 ubuntu 16.04 LTS, 기기 소유자의 지갑은 Raspbian-jessie 운영체제를 탑재한 라즈베리 파이를 활용하였다. 스마트 컨트랙트를 지원하는 Go-Ethereum 1.7.0 버전을 통해 프로토타입을 진행하였으며, 라즈베리 파이를 프라이빗 블록체인의 Geth 클라이언트 노드로 활용하기 위해서 저전력 ARM CPU용 Geth 프로그램을 설치하였으며, 이는 저사양의 기기에서도 원활하게 작동할 수 있도록 한다.

스마트 컨트랙트는 Solidity 언어로 작성하였는데, 이는 EVM을 통해 실행할 수 있다. 브라우저인 Remix와 IntelliJ, Visual Studio 등에 플러그인을 설치하면 사용할 수 있어 다양한 개발 환경을 지원한다.

기기 소유자가 기기를 쉽게 등록할 수 있도록 등록 화면은 Javascript와 HTML을 사용하였으며, 원활한 진행을 위해 이더리움 테스트 네트워크에서 프로토타입을 수행하였다.

노드는 크게 플랫폼에 접근하려는 기기를 검증하기 위해 기기인증을 하고, 플랫폼에 참여하고 있는 기기들을 관리하기 위한 사용자 노드, 자신의 기기를 플랫폼에 참여시키는 기기 소유자 노드, 이미 기기를 검증받아 플랫폼에서 서비스를 이용하고 있는 참여자 노드로 볼 수 있다.

<표 5> 참여 노드 분류

| 분류 | 상세 내용 |
|---|---|
| user | - 의사 결정 노드인 leader 노드로, 네트워크 내 유일한 노드<br>- 컨트랙트를 열람할 수 있으며, 검증 여부 Update 가능 |
| owner | - 기기를 소유한 노드로, 네트워크 내에 다수 존재<br>- 기기 등록 컨트랙트 작성<br>- 참여자 노드도 이에 해당 |

## 2. 프로토타입

### 1) 알고리즘

4장에서 제시하였던 설계의 활용 가능성에 대한 검증을 위해서 프로토타입 개발을 진행하기 위해서 알고리즘을 제시한다. 설계에 대한 동작 절차는 아래 알고리즘과 같다.

**Algorithm**

**input:** A blockchain address addr, a device number deviceNum, a zone, and a agreement
**Output:** A deviceID id, a isVerified and a isAccept

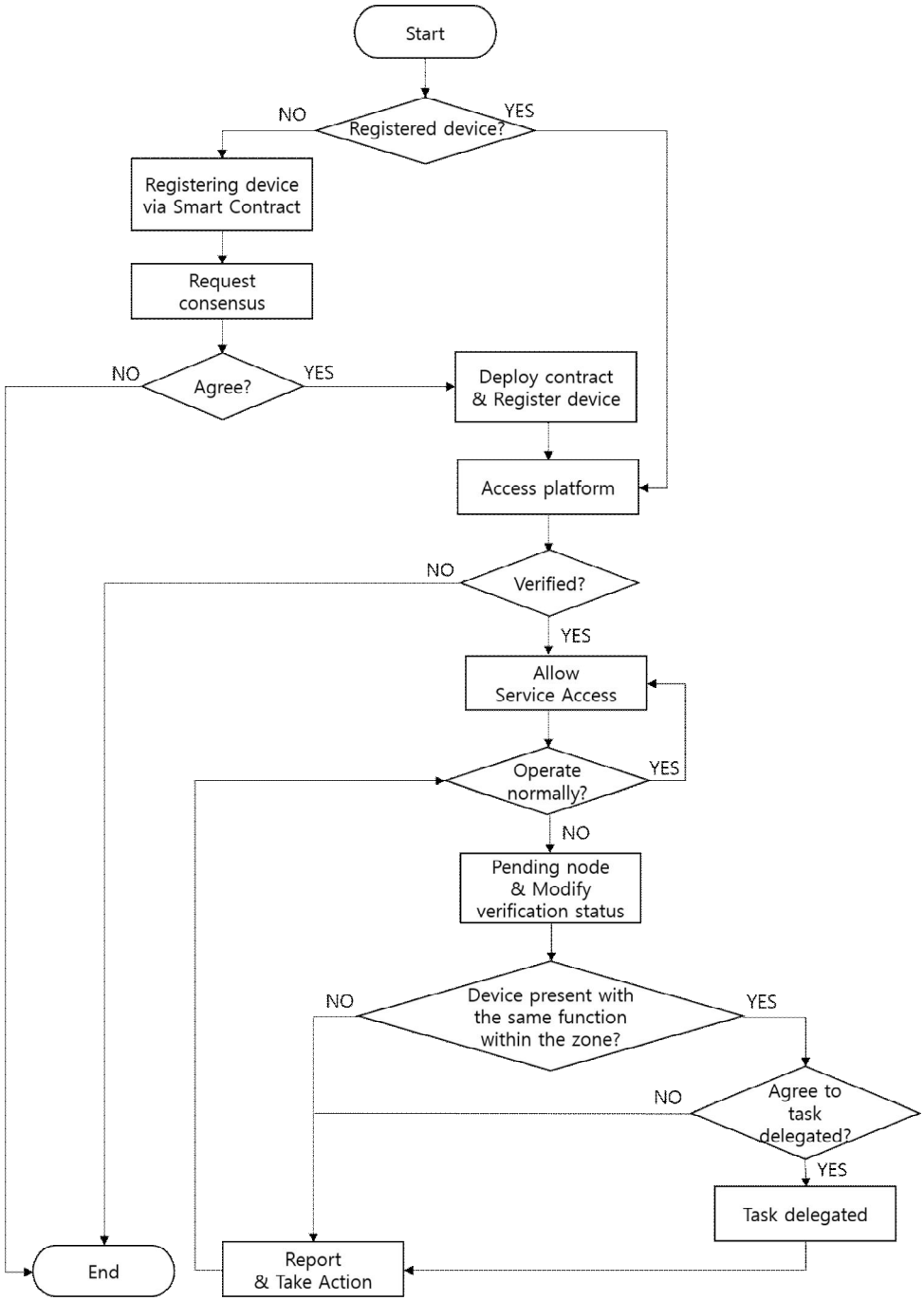
```
node ← node
node_u ← user node
node_d ← device owner node
node_p ← participant node

if (Registered(node_d)) = false then
    node_d.createContract ← setCondition(node_d.addr, node_d.deviceNum, node_d.zone,
    node_d.agreement)
    while(Accept(node_u))= true
    {
      leader ← node_u
        if node_d.requestConsensus then
          if leader.broadcastRequest then
              reply Result
    }
   contractDeploy
   return id, isVerified ← true
else
   if Registered(node_d.id) then
       try to access the platform
   end if
end if

if Access(node_d) then
  node_d ← pending
  if (isVerified) = true then
     return isAccept ← true
     node_d ← allow to access the platform
  else
     send FailMessage
  end if
end if
```

```
33
34 if (deviceOperate(node_d)) = false then
35    node_d ← pending
36    isVerified.node_d ← false
37    isAccept.node_d ← false
38    zone.node_p ← zone.node_d
39    if (agreement.node_p) = true then
40       task delegate
41    end if
42 end if
```

먼저 사용자는 사전에 기기 소유자가 기기를 등록할 수 있도록 조건을 설정한 스마트 컨트랙트를 블록체인 네트워크에 배포한다. 기기 소유자는 플랫폼에 접근하기 위해서 먼저 사전에 배포되었던 컨트랙트를 통해 기기를 등록하여야한다. 조건에 맞게 작성한 후 의사결정자에게 합의를 요청하는데, 사전에 사용자를 의사결정자로 선정한다. 다른 참여자들의 의견을 반영하여 등록이 결정되면 해당 스마트 컨트랙트는 네트워크에 전파되며, 사용자는 컨트랙트의 검증 여부를 검증됨으로 변경한다. 이렇게 검증된 기기는 플랫폼에 접근하여 서비스를 이용할 수 있다.

사용자는 플랫폼에 참여하고 있는 기기를 모니터링한다. 노드의 피어 혹은 신호가 끊기는 문제가 발생하는지 확인하며, 기기의 결함이 발생하면 같은 영역 내에 비슷한 기능을 하는 기기를 확인한다. 이 때 사용자는 기기의 기능을 사전에 파악하고 있다고 가정한다. 비슷한 기능을 하는 기기의 컨트랙트 중 다른 기기의 결함 발생 시 업무 위임 동의 여부가 동의로 되어있다면 업무를 위임하여 서비스가 중단되지 않도록 지속한다. 만약 같은 영역 내에 비슷한 기능을 하는 기기가 존재하지 않거나 동의 여부가 동의하지 않음이라면 문제가 발생한 기기의 소유주에게 기기의 결함을 보고하고, 조취를 취하게 한다.

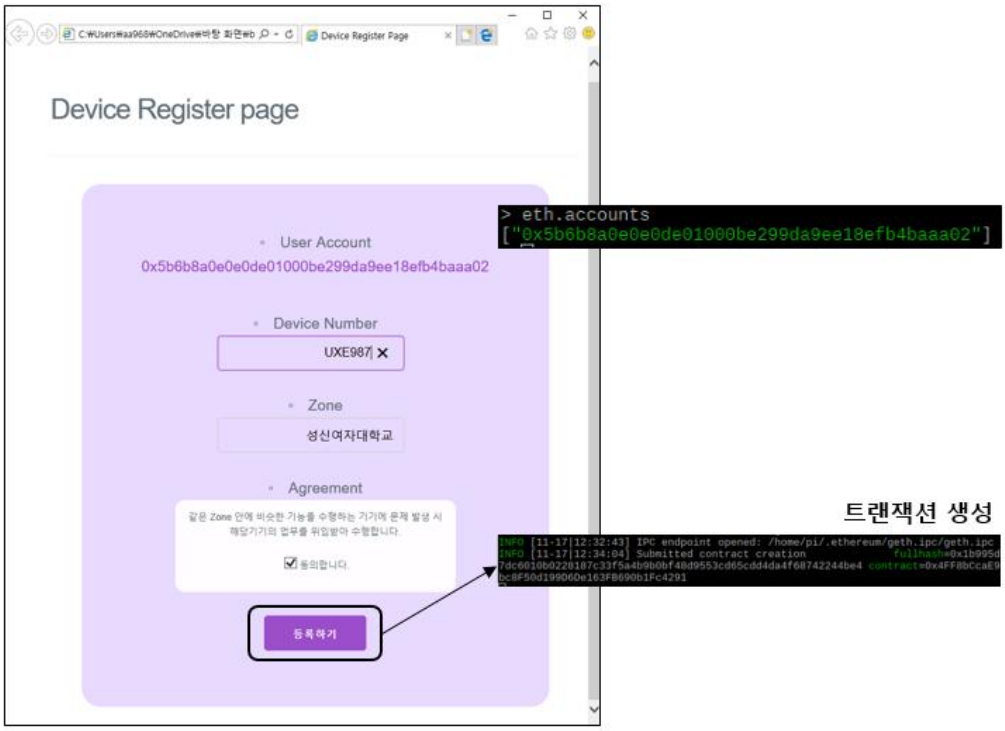
다음은 프로세스를 플로우차트로 나타낸 것이다.




[그림 15] 기기 관리 체계 프로세스

### 2) 프로토타입 동작 화면

기기 소유자가 자신의 기기를 등록하기 위한 컨트랙트 작성 화면은 다음과 같다.

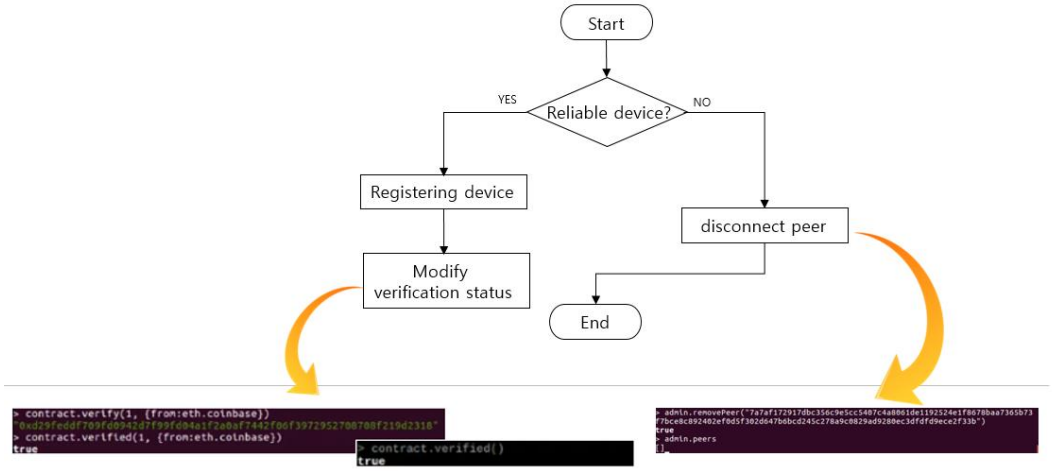



[그림 16] Device Register page 작성 화면

기기 소유자는 기기 등록을 위한 Device Register page를 통해 스마트 컨트랙트의 조건에 맞게 직접 입력을 한다. 같은 기기 소유자가 다수의 기기를 등록할 때 용량을 줄이기 위해 구조체 형식으로 저장을 하게 되는데, 이때 기기를 구분하기 위해서 기기 고유 식별번호를 입력하게 하였으며, 이는 hash값으로 저장된다. 스마트 컨트랙트를 통해 기기의 고유 식별번호나

MAC Address를 자동으로 수집하기에는 아직까지 기술의 한계가 존재하고, 서비스 안정성을 위한 업무 위임에 대한 동의를 받기 위해서 직접 등록하도록 하였다.

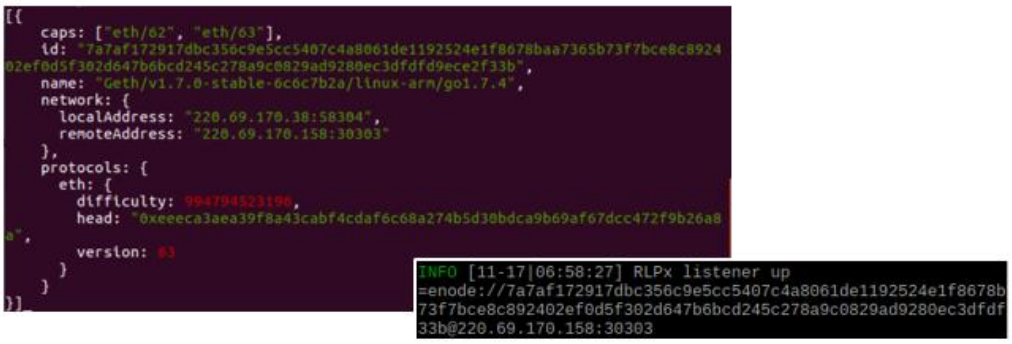
먼저 User Account에는 기기 소유자의 지갑 주소를 불러와 임의로 작성할 수 없게 하였다. Device Number에는 기기 고유 식별 번호를, Zone에는 기기가 설치 및 작동하는 영역을 입력한다. Agreement에는 업무 위임에 대한 동의 여부를 체크할 수 있으며, 작성 후 등록하기를 누르면 트랜잭션이 생성된다.




[그림 17] 검증 결과 적용

컨트랙트가 배포되고, 사용자는 등록된 컨트랙트를 확인 후 검증되지 않은 기기라고 판단이 되면 모니터링 대상이 아니므로 더 이상 네트워크에 참여할 수 없도록 연결을 끊는다. 사용자는 등록하고자 하는 기기가 신뢰할 수 있으면 modifier을 통해 검증 여부를 verified로 변경한다. deviceID는 등록하고자 하는 기기에 순차적으로 부여하는데, 첫 번째로 등록하여 deviceID를 1로 부여한 것을 화면을 통해 볼 수 있다. 이 ID를 통해 검증

여부를 변경하며, 기기에서도 검증 여부를 확인할 수 있다. 변경사항이 있으면 컨트랙트의 등록 내용을 수정할 수 있으며, 변경 시에는 트랜잭션이 발생하기 때문에 확인이 가능하다.




[그림 18] 연결 노드 확인


[그림 19] 연결 상태 공유

연결된 기기를 확인할 수 있는데, 이는 참여자들 간에도 공유가 되어 확인할 수 있다. 기기가 정상적으로 작동할 경우 노드의 연결을 확인할 수 있지만, 작동이 중지되거나 전원이 꺼진 경우에는 노드의 연결을 확인할 수 없다. 이런 경우 주소를 통해서 등록된 기기의 소유자를 식별 후 기기의 결함을 보고한다. 또한 기기의 영역을 확인하여 영역 내 같은 기능을 수행하는 기기의 소유주에게 업무 위임에 대한 보고를 한다.

### 3) 주요 IoT 기기 모니터링 체계와의 비교 평가

본 논문에서는 블록체인 기반의 사물인터넷 기기 관리체계를 제안하였다. 최근에는 신뢰성을 확보하고, 비용을 절감할 수 있는 블록체인 기반의 서비스들이 제공되고 있으나, 본 연구에서는 구성에 참여하는 요소인 사물인터넷 기기 자체에 블록체인을 직접 적용한 방안을 제안함으로써 다른 체계와의 차별성을 두었다. 기존에 제공되고 있는 서비스는 대다수 기기를 식별할 수 있었지만, 본 연구 방안에서는 사용자 식별을 추가하여, 악용되는 기기에 대한 책임 추적성을 보완하고자 하였다. 또한 기기의 이상 탐지 여부를 확인할 수 있고, 이를 운영자에게 보고하는 기능은 제공하고 있지만, 유기적으로 연결되어있는 기기에 대한 지속성 보완 서비스의 제공은 미흡하여, 업무 위임을 통해 이를 보완하여 타 서비스와 차별화된 기능을 제공한다. 아래는 기존에 제공되고 있는 IoT 모니터링 체계와의 비교한 표이다.

<표 6> 기존 모니터링 체계와의 비교 평가

| 구분 / 비교항목 | IoT Hub | Hdac | Watson IoT Platform Blockchain Service | 본 연구 방안 |
|---|---|---|---|---|
| 운용 환경 | 클라우드 컴퓨팅 | 블록체인 | 블록체인 | 블록체인 |
| 기기 모니터링 서비스 제공 | √ | √ | √ | √ |
| 사용자 식별 | - | √ | - | √ |
| 이상 탐지 | √ | √ | √ | √ |
| 지속성 보완 서비스 제공 | - | - | - | √ |

# 제 6장 결론 및 향후 연구

사물인터넷은 사람과 사물 혹은 사물과 사물 간의 데이터 교환을 근간으로 하는 시스템이다. 다른 서비스와의 상호 운영을 통해서 융·복합 서비스에 요구되는 다양한 정보를 유기적으로 수집하여 복합 정보를 생성하고, 공유할 수 있으며 점차 지능적으로 발전하고 있다. 사물인터넷은 기기를 통해서 데이터를 수집하고, 상호통신하기 때문에 기기의 관리와 보안의 중요성이 대두되고 있다. 이러한 문제점을 보완하기 위한 IoT 기기 관리 플랫폼이 출시되고 있으며, 기기의 위치와 상태, 수집되는 데이터를 관리하는 서비스를 제공한다. 하지만 대부분의 기존 서비스는 중앙 집중 형이며, 지속성과 관련된 서비스의 제공이 부족하다.

이에 본 논문에서는 블록체인을 기반으로 하여 기존 IoT 기기 관리 시스템을 보완하는 체계를 제안하였다. 본 연구에서는 저사양의 사물인터넷 기기에 블록체인을 직접 적용한 체계 방안을 제안하였다는 것이 다른 연구와의 차별점이라 볼 수 있다. 스마트 컨트랙트를 활용하여 기기를 등록하여 기기의 책임 추적성을 확보하고, 제공되는 서비스에 대한 신뢰성을 높이고자 하였다. 또한 블록체인 네트워크를 활용하여 분산화 된 체계를 구성하고, 기기의 상태를 참여자들과 공유할 수 있도록 하였으며, 업무 위임 기능을 통해 지속성을 보완하고자 하였다.

하지만 사람의 개입이 최소화되어야 하는 IoT의 특성을 반영하기에는 미흡하다. 먼저 사용자와 기기 소유자는 사전에 블록체인 관련 지식이 있어야 하며, IoT 기기를 관리하기 위해서 별도의 네트워크를 구성해야하는 번거로움이 존재한다. 또한 기기 소유자가 직접 스마트 컨트랙트를 작성하여 기기를 등록하여야 하며, 사용자는 기기에 결함이 발생하여 업무 위임 시 직접

기기 소유자에게 보고하고, 위임을 해야 한다.

향후에는 본 연구의 미흡한 점을 보완하여 사람의 개입을 최소화하는 자동화된 IoT 기기 관리 체계를 구축하고자 한다. 또한 기기의 생명주기에 맞는 세분화된 스마트 컨트랙트에 대한 연구를 지속적으로 하고자 하며, 아울러 기기에서 수집되는 데이터의 무결성 보장을 위한 데이터 관리 방안에 대해서도 추가적인 연구를 진행할 계획이다.

# 참 고 문 헌


[1] 민경식, “사물 인터넷(Internet of Things)”, 인터넷 & 시큐리티 이슈, 2012.

[2] “타겟형 랜섬웨어 확산...IoT 보안 새로운 숙제”, KINEWS, 2017년 1월 11일, http://www.kinews.net/news/articleView.html?idxno=75039.

[3] 엄주희, 박정기, “사물인터넷 환경 변화에 따른 상호작용성에 관한 사례 연구 -스마트 디바이스를 중심으로-”, 한국과학예술포럼, Vol. 19, pp. 471-486, 2015.

[4] www.tkt.cs.tut.fi/research/waps/

[5] 박영희, “사물인터넷의 빅데이터 개론”, 광문각, 2017.

[6] https://docs.microsoft.com/ko-kr/azure/iot-fundamentals/

[7] http://doublechain.co.kr/03service/service_business_01.php#nolink

[8] https://www.ibm.com/us-en/marketplace/iot-blockchain

[9] 이동혁, 박남제, “IoT 기기의 보안성 확보를 위한 제도적 개선 방안”, 정보보호학회논문지, Vol. 27, No. 3, 2017.

[10] 홍성혁, 신현준, “시나리오 분석을 통한 사물인터넷(IoT)의 취약성 분석”, 한국융합학회논문지, Vol. 8, No. 9, 2017.

[11] 한국정보보호학회, “사물통신(Machine-to-Machine)에서의 정보보호를 위한 효율적 인증시스템 연구”, 2010.

[12] 유기순, 김성준, 박원규, 장민호, 임대운, “경량 보안 프로토콜 구현”, 통신학회논문지, Vol. 43, No. 4, pp. 723-729, 2018.

[13] 박병주, 이태진, 곽진, “블록체인 기반 IoT 디바이스 인증 스킴”, 정보보호학회논문지, Vol. 27, No. 2, pp. 343-351, 2017.

[14] Muhamed Turkanovic, Bostjan Brumen and Marko Holbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion”, AD Hoc Networks, Vol. 20, pp.96-112, 2014.

[15] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, “Identity Authentication and Capability Based Access Control(IACAC) for the Internet of Things”, Journal of Cyber Security and Mobility, Vol. 1, No. 4, pp. 309-348, 2013.

[16] 마영철, “IoT환경에서 단말기 인증을 위한 NTS기반 보안기술 연구”, 숭실대학교 대학원 IT정책경영학과 박사학위논문, 2017.

[17] 정현준, 이홍노, “블록체인개발 현황과 보안이슈 변화 동향”, 정보보호학회지, Vol. 28, No. 3, 2018.

[18] 이지윤, 박수민, 홍승필, “블록체인 환경 내 노드 인증 및 식별 방안 제언”, 한국통신학회 학술대회논문집, pp. 476-477, 2018.

[19] 홍승필, “금융권 블록체인 활용 방안에 대한 정책연구”, 전자금융과 금융보안, Vol. 06, 2016.

[20] 김태우, “블록체인이 자본시장에 미치는 영향”, 예탁결제, Vol. 97, 2016.

[21] 한승우, “블록체인 활용사례로 알아보는 금융권 적용 고려사항”, 전자금융과 금융보안, Vol. 3, 2016.

[22] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.

[23] 조수현, 이정빈, 박재용, 이대건, 인호, “이더리움 베이직”, BOOKSTAR, 2018.

[24] Christopher D. Clack, Vikram A. Bakshi and Lee Braione, “Smart

Contract Templates: foundations, design landscape and research directions", 2016.

[25] Nick Szabo, "Smart Contracts", 1994.

[26] Melanie Swan, "Blockchain: Blueprint for a new economy", O'Reilly Media, 2015.

[27] 남진석, 양해술, "블록체인을 활용한 국민주택채권 정보 중계시스템 개선방안 연구", 디지털융복합연구, Vol. 15, No. 8, pp. 203-212, 2017.

[28] 와타나베 아츠시, 마츠모토 유타, 니시무라 요시카즈, 시미즈 토시야, "블록체인 애플리케이션 개발 실전 입문", 위키북스, 2017.

[29] 이루다, "블록체인을 활용한 전자투표 시스템 구축", 상명대학교 대학원 컴퓨터과학과 석사학위논문, 2017.

[30] 아카하네 요시하루 외, "블록체인 구조와 이론", 위키북스, 2017.

[31] 김혜리, "블록체인 기반의 신뢰할 수 있는 스마트 컨트랙트 모델 연구", 성신여자대학교 대학원 컴퓨터학과 박사학위논문, 2018.

[32] 임종철, 유현경, 곽지영, 김선미, "블록체인과 합의 알고리즘", ETRI, 2018.

# ABSTRACT

## A Study on the Design of IoT Device Management System based on Blockchain

Lee, Ji Yun
Department of Computer Science
Graduate School of
Sungshin University

Devices in the Internet of Things are miniaturized and connected to wireless, and most contact with an unspecific unidentified device. If the infected device comes into contact with a normal device, the device may become a zombie. There is also a risk of causing DDoS and spam attacks or disabling devices that can disrupt operations and prevent services from being maintained. Because these problems incur personal and financial damage and additional maintenance costs, systems are needed to prepare for them, and the security and management of the devices are important. Recently, various IoT device monitoring services are have been released, which manages the status and location of the devices and the collected data. However, it is necessary to guarantee the continuity of maintaining the service due to the characteristics of the Internet, which is connected to the 24-hour network, but there is a lack of services related to this.

This paper propose IoT device management system based on Blockchain. After analyzing issues related to the management of IoT devices in the existing IoT environment, present a new mechanism. First, device owners register their devices using smart contacts. If a problem occurs in a device, the owner can be identified, thereby ensuring accountability and ensuring that only the verified device can be accessed to prevent contact with unspecified devices, increase the reliability of the service provided. In addition, the decentralized system was constructed using the lockchain, allowing participants to share the status of other devices. Finally, it was intended to supplement continuity of services that were not supported by existing IoT device monitoring platforms by task delegation. The management system mechanism proposed in this study has been validated to examine its applicability, and it is considered that applying it will help create a stable Internet of Things environment.