정 보 보 호 학 회 지
제27권 제6호, 2017. 12

블록체인 기반 탈중앙화 사물인터넷 플랫폼 연구

최 종 석*, 박 종 규, 김 명 길, 김 호 원**

요 약

사물인터넷은 응용서비스, 플랫폼, 네트워크, 디바이스의 4계층으로 이루어진다. 사물인터넷의 전체적인 구조도를 보면, 다양한 디바이스가 사물인터넷 플랫폼에 센싱 빅데이터를 전송하고, 사물인터넷 플랫폼에서 수집된 데이터를 이용하여 응용서비스에 정형화된 데이터 서비스를 제공할 수 있다. 그러나 현재의 사물인터넷 플랫폼의 구조는 수백만개의 디바이스에서 생성되는 데이터를 관리하여 플랫폼에 높은 트래픽과 계산부하가 야기될 수 있는 구조이며 이로 인해 해당 플랫폼과 연동된 모든 응용서비스의 가용성이 낮아지고 단일장애지점(Single point of failure)의 원인을 제공한다. 본 논문에서는 단일장애지점에 대한 문제점을 해결하기 위해서 중앙화 된 사물인터넷 플랫폼 대신에 탈중앙화 된 사물인터넷 구조를 위한 방법을 제안하고자 한다. 특히 사물인터넷 플랫폼의 요구사항을 분석하여 탈중앙화 된 사물인터넷 플랫폼에서의 요구사항을 도출한다. 더 나아가 블록체인기반의 탈중앙화 된 사물인터넷 플랫폼을 통해서 기존의 4계층 사물인터넷 구조에서 3계층 사물인터넷 구조로 나아가는 방법을 제시한다.

Ⅰ. 서 론

정보통신기술의 발전으로 인해 스마트폰, 가전기기, 웨어러블 디바이스 등의 인터넷에 연결이 가능한 디바이스가 등장하였고, 사물인터넷(Internet of Things)은 이러한 디바이스에서 수집한 데이터를 플랫폼에서 분석하여 의미 있는 데이터로 가공하고 다양한 서비스를 만들어내기 위한 네트워크 환경이다.

사물인터넷은 응용서비스, 플랫폼, 네트워크, 디바이스의 총 4계층으로 구성이 된다. 특히 사물인터넷 플랫폼은 디바이스에서 생성 및 수집되는 데이터를 가공하고 응용서비스에 제공해주는 정형화 및 인터페이스 역할을 수행한다. 하지만 이러한 구조에서 사물인터넷 응용서비스들은 사물인터넷 플랫폼에 가용성을 의존할 수 밖에 없다. 다시 말해서, 사물인터넷 플랫폼은 단일장애지점(Single point failure)을 발생하는 요소이다. 따라서 이러한 중앙화 된 플랫폼의 이슈를 해결하기 위해 분산 사물인터넷 구조에 대한 많은 연구[1-3]가 이루어졌다. 또한 디바이스는 사용자와 연관된 민감한 데이터도 수집한다. 따라서 사물인터넷에서는 프라이버시에 대한 이슈가 발생되며, 이를 해결하기 위한 연구[4-8]도 진행되고 있다.

본 논문에서는 위에서 언급된 두가지 문제를 해결하기 위한 방안으로 블록체인을 사물인터넷에 적용하는 방법을 고려한다. 이를 위해서 분산 사물인터넷을 구성하기 위한 요구사항을 도출하고, 도출된 요구사항들을 만족하는 블록체인 기반 사물인터넷 플랫폼을 구축하기 위해 앞으로 연구되어야 할 방향을 제시한다.

본 논문에서 제안하는 블록체인 기반의 탈중앙화 사물인터넷 플랫폼의 모델은 기존의 사물인터넷 플랫폼 대신에 블록체인을 이용한 데이터허브를 구축하고 여기에서 발생할 수 있는 이슈를 앞으로의 연구과제로 제시한다.

논문 구성은 2장에서 사물인터넷 주요 표준 플랫폼에 대해서 알아보고, 3장에서는 다양한 분야에서 사용되고 있는 블록체인 관련 연구를 살펴본다. 4장에서는 분산 사물인터넷 플랫폼을 위한 요구사항을 도출하고, 블록체인기반의 사물인터넷 모델을 제시한다. 마지막으로 5장에서 결론을 맺고, 블록체인기반 사물인터넷 연구방향을 제시한다.

이 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2012-0-00265, 개방형 고성능 표준 IoT 디바이스 및 지능형 SW 개발)
* 주저자, 부산대학교 ITRC (jongseokchoi@pusan.ac.kr)
** 교신저자, 부산대학교 (howonkim@pusan.ac.kr)

Ⅱ. 사물인터넷 관련연구

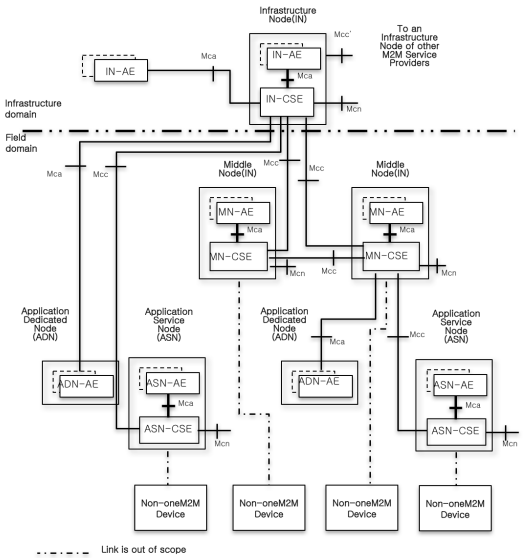
본 장에서는 사물인터넷에서 주로 사용되고 있는 플랫폼으로 oneM2M, IoTivity, AllJoyn, LWM2M의 구조에 대해서 살펴본다.

2.1. oneM2M

본 절에서는 oneM2M의 전체 아키텍쳐를 살펴본다. oneM2M은 다양한 서비스의 요구사항을 만족시킬 수 있는 사물인터넷에서의 공통 플랫폼을 정의하고, 타 플랫폼과의 상호동작(Internetworking)을 표준화하였다. 다양한 응용 간의 호환을 위한 인터페이스를 정의하여 종래의 수직적인 형태의 사물인터넷 플랫폼에서 벗어나 수평적인 플랫폼을 구성하여 사물인터넷 플랫폼의 파편화 방지, 개발 및 운용 비용을 감소할 수 있다. 스마트 홈, 스마트 카, 에너지, 헬스케어, 엔터프라이즈, 공공서비스와 같은 7개 산업 분야의 Use Case를 반영하여 요구사항을 도출하고, 핵심 기능(데이터수집 및 보고 기능, 기기의 원격 제어, 연결성 유지,보안 및 프라이버시 기능 등)과 인터페이스를 정의하였다.

oneM2M의 개체는 User/End-User, application service provider, M2M service provider, network operator로 구성된다. User/End-User는 M2M 솔루션을 사용하는 개인 또는 기업을 의미하며, Application service providers는 M2M 서비스를 제공하는 제공 주체를 의미한다. M2M service provider는 application service provider에게 M2M 공통 서비스를 제공하는 주체이며, network operator는 M2M service provider에게 네트워크를 제공하는 주체이다.

oneM2M은 여러개의 노드(Node) 연결되어 하나의 인프라를 형성하며, 하나의 노드는 AE(Application Entity)와 CSE(Common Service Entity), NSE(Network Service Entity)로 구성된다. 기능적인 관점에서 AE는 M2M 서비스를 제공하기 위한 애플리케이션 기능 로직을 담당하며, CSE는 AE를 위한 12개의 공통 서비스기능 제공한다. NSE는 CSE에게 네트워크 장치 관리 및 서비스 등을 제공하고, 각각의 개체(Entity)는 참조점(Reference Point)을 통해서 상호 동작한다. 이 때, 참조점은 CSE와 AE, CSE간의 연결을 의미하며, 실제 통신을 위한 바인딩 프로토콜(Binding



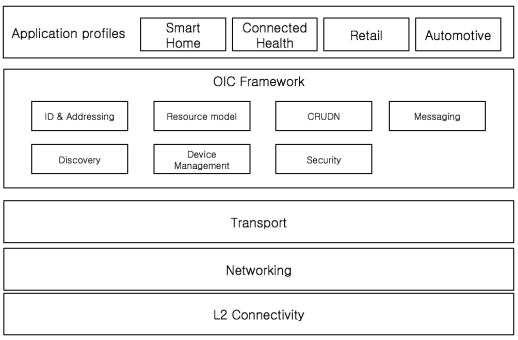
〔그림 1〕 oneM2M 전체 구조도

Protocol)에 매핑되어 통신을 수행한다. [그림 1]은 oneM2M의 전체 구조를 보여준다. [그림 1]에서 Mca는 CSE-AE간의 통신, Mcc는 CSE-CSE간의 통신, Mcn은CSE와 NSE간의 통신, Mcc`는 다른 Infrastructure Domain CSE와의 통신을 나타낸다.

CSE는 Lookup/Discovery/Resolution을 포함한 다양한 같은 공통 서비스 기능(Common Service Function)을 제공하며, ROA(Resource-Oriented Architecture)에 기반하여 CRUDN(Create, Retrieve, Update, Delete, Notify) 연산을 12개의 공통 서비스 기능에게 제공한다.

2.2. IoTivity

[그림 2]는 IoTivity 전체 구조도를 보여준다. IoTivity는 Application profiles, OCF Framework, Transport, Networking, L2 Connectivity 계층으로 구성된다. Application profiles 계층은 Smart Home, Connected Health, Retail, Automotive 등의 다양한 응용 어플리케이션이 수행된다. OCF Framework는 Application profiles 계층에서 수행되는 어플리케이션이 요구하는 기능을 제공해주는 계층으로 ID& Addressing, Resource model, CRUDN, Messaging, Discovery, Device Management, Security 기능을 제공



〔그림 2〕 IoTivity 전체 구조도

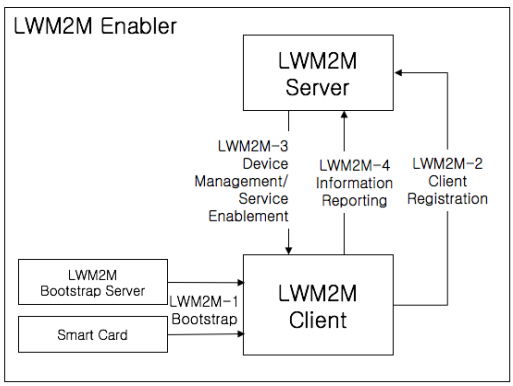
한다. Transport 계층은 특정 QoS(Quality of Service) constraints를 가지는 단대단(End-To-End) 전송기능을 제공한다. Networking 계층은 인터넷과 같은 네트워크 상에서 디바이스 간의 데이터 교환 기능을 제공하며, L2 Connectivity 계층은 물리 계층과 데이터 링크 계층 간의 연결을 제공한다.

2.3. LWM2M

[그림 3]은 LWM2M의 전체 구조도를 보여준다. LWM2M은 LWM2M Bootstrap 서버, 스마트카드, LWM2M 서버/클라이언트로 구성된다. LWM2M Enabler 는 LWM2M 서버와 LWM2M 클라이언트 요소를 기술한다.

LWM2M을 사용하기 위해서 최초에는 선택적으로 Bootstrap단계를 수행할 수 있다. LWM2M의 부트스트랩 단계는 LWM2M 서버의 일부 정보 또는 상호 인증 등을 간소화하기 위한 파라미터를 사전에 LWM2M 클라이언트에 기술하는 과정이다. LWM2M Bootstrap 서버와 스마트카드를 이용해 LWM2M 부트스트랩을 수행한다. LWM2M 클라이언트는 LWM2M 서버에 클라이언트 등록을 수행하고, LWM2M 서버는 LWM2M 클라이언트를 관리하기 위해서 Device Management, Service Enablement 기능을 제공한다. 또한 LWM2M 클라이언트는 LWM2M 서버의 리소스 관리를 돕기 위해서 Information Reporting 기능을 제공한다.

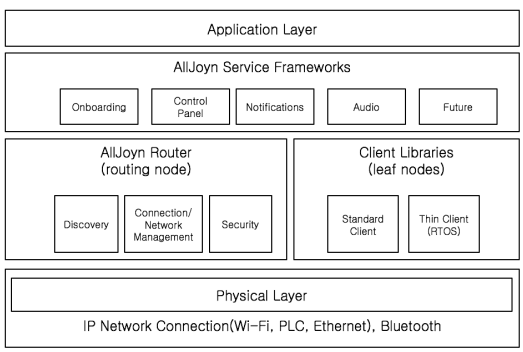
LWM2M에서 M2M User가 M2M 서비스 제공자에게 서비스를 제공받고, M2M 서비스 제공자가 LWM2M 서버와 M2M응용서비스를 제공한다. LWM2M 서버는 네트워크를 통해서 LWM2M클라이언트에 접근 할 수 있다. 또한 LWM2M서버를 M2M 서비스 제공자가 아닌 네트워크 서비스 제공자가 LWM2M 서버를 운영하고, LWM2M 서버의 인터페이스를 M2M 응용서비스에 제공하고, LWM2M 서버/클라이언트 간의 통신을 수행한다.



〔그림 3〕 LWM2M 전체 구조도

2.4. AllJoyn

[그림 4]는 AllJoyn의 전체 구조도를 보여준다. AllJoyn은 Application Layer, AllJoyn Service Frameworks, AllJoyn Router, Client Libraries, Physical Layer로 구성된다. Physical Layer는 Wi-Fi, PLC, Ethernet 등의 IP기반 통신과 Bluetooth 통신 모듈 물리적인 인터페이스를 가지는 계층이다. 하나의 AllJoyn 노드는 다수의 AllJoyn 앱과 하나의 AllJoyn 라우터로 구성되는데, AllJoyn 앱을 개발하기 위한 기능을 제공하는 것이 Client Libraries 계층이며, AllJoyn



〔그림 4〕 AllJoyn 전체 구조도

라우터가 다른 AllJoyn Router와 통신을 하기 위해 필요한 기능을 제공하는 것인 AllJoyn Router 계층이다. AllJoyn Service Frameworks는 실제 AllJoyn 앱이 사용하기 위한 Onboarding, Control Panel, Notifications, Audio 등의 기능을 제공해준다. Application Layer는 AllJoyn Service Frameworks 계층에서 제공되는 기능들을 이용하여, 생성된 AllJoyn 앱들이 구동하는 계층이다.

AllJoyn은 근거리 기반의 기기간 P2P(Peer-To-Peer) 통신이며, 중계서버를 사용하지 않고 디바이스 간의 통신을 사용한다. Bluetooth나 Wi-Fi 등의 물리적인 통신 방식 위에 소프트웨어 프레임워크로 개발된 통신을 이용하기 때문에 하드웨어에 의존적이지 않다. AllJoyn은 디바이스 간의 세션 연결을 위해서 RMI(Remote Method Invocation)방식의 D-Bus를 이용한다.

Ⅲ. 블록체인 관련연구

본 장에서는 블록체인의 기술 응용분야로 금융, 자동차, 항만물류 분야에서 블록체인이 응용되고 있는 방법과 사물인터넷 분야에서 블록체인이 어떤 역할을 할 수 있는지 살펴본다.

3.1. 금융분야

블록체인 기술의 발전에 가장 크게 기여한 분야로, 시장에 블록체인 기술을 적용해 처음으로 사회의 관심을 받은 분야이다. 주로 화폐에 많이 응용되고 있으며, 전자 화폐 네트워크에서 일어나는 거래들을 기록하고 관리하는 기술로, 분산 데이터베이스의 한 형태로 사용되고 있다.

암호화폐에서 블록체인 기술은 개방적이고, 투명하며 검증 가능한 시스템으로 활용되었다. 국가나 인증된 기관의 통제 없이, 화폐 네트워크 참여자들이 정해진 프로토콜을 통하여 상대에 대한 신뢰가 없더라도 거래를 보장받는 점은 화폐에 있어서 혁신적인 개념이다. 인증기관이 없는 탈중앙화라는 점 또한 기존의 금융계에 많은 변화를 요구했다.

2009년 처음으로 블록체인이 적용된 암호화폐인 비트코인이 개발되었다. 이후 여러 화폐로서의 기술적인 한계를 극복하는 블록체인 기술들이 발전해 나가면서, 많은 알트코인(Alternative Coin)이 개발되었다. 이러한 암호화폐 시장은 지속해서 성장해왔으며, 최근 폭발적으로 규모가 커지면서 현재 2017년 12월에는 5조 달러 정도의 시장이 형성되어있다.

암호화폐의 시장이 커짐에 따라 일어나는 사회적으로 부정적인 여파 또한 커지고 있다. 암거래, 불법 자금세탁, 사기 및 해킹 등에 암호화폐가 활용되고 있다. 2013년 마약, 무기, 인신매매, 장기 등 불법 암거래 사이트인 실크로드가 FBI에 의해 폐쇄되기 전까지 비트코인이 암거래의 거래 통화로 사용되었으며, 아직도 알려지지 않은 딥웹의 암거래 사이트에서 암호화폐가 사용되고 있다. 그뿐만 아니라 인터넷 네트워크를 통해 랜섬웨어와 같은 악성코드를 여러 보안에 취약한 PC에 감염시키고 이를 풀어주는 대가로 비트코인을 요구하는 불법 행위, 2014년 Mt. Gox 거래소 비트코인 loss 사건 등 많은 문제와 피해가 발생하고 있다. 하지만 블록체인 기술의 보안성을 제공하는 핵심인 분산된 원장에 대한 공격은 아니었으며 실제 피해 규모의 99% 이상이 블록체인 기술 자체의 보안성이 아닌, 네트워크를 통한 계정, 지갑 등의 해킹으로 기존의 중앙화 서버 데이터베이스, 분산된 수정 가능한 서버 데이터베이스보다 더 높은 보안성을 가진 기술이라는 것이 증명되었다.

암호화폐 뿐만 아니라, 블록체인 기술은 본인인증 기술에도 도입되고 있다. 국내에서는 공인인증서가 대표적이다. 공인인증서는 인증된 제3기관의 중앙 서버에서 관리되어, 금융 소비자들이 개별 금융기관에서 거래를 시작할 때마다 인증서를 재발급 받거나 가져오는 기능과 인증서 생성, 폐기와 같은 관리에서도 많은 불편함이 있었다. 특히 공인인증서 정보 유출은 중앙서버에서 인증서를 가져오고, 내보내는 것에서 비롯되는데, 블록체인 기술에서는 이러한 기능 자체가 필요 없어 유출 위험이 현저히 낮아지는 효과가 있다. 이러한 인증서 기술은 국내 제1, 2금융권 은행 및 투자회사와 여러 IT 기술업체들이 협력하여 개발되었고 시험 서비스를 진행중이다.

복잡한 금융 절차 없이 아주 빠르고 쉽게 적용할 수 있으면서 금융 업계의 전반적인 대부분 시스템에 적용 가능하다는 점에서 많은 관심과 기대감을 바탕으로 대규모 프로젝트들이 계획되고 있다. 오스트레일리아 증권거래소에서 블록체인 시스템 도입을 검토하고 있으며, 독일 거래소는 시스템개혁프로젝트 ‘Exchange 4.0’

을 발표, 국가적인 차원에서 거래에 관련된 블록체인 기술 개발에 박차를 가하고 있다. 싱가포르에서는 중앙은행의 주도하에 블록체인 기술을 적용한 채권거래, 해외송금 등을 실험 운용하고 있다. 이외에도 러시아 중앙은행을 중심으로 한 러시아 컨소시엄, 미국 신용협동조합협회를 중심으로 한 CU Ledger, 중국 31개 금융기관 및 IT기업의 FBSC, 11개의 금융기관 및 Wanxian 블록체인 연구소를 중심으로 한 China Ledger 등 세계 여러 국가의 금융기관들은 자국 시스템에 발 빠르게 블록체인 기술을 적용, 개발 및 연구하고 있다. 각 국가 내에서의 협력뿐 아니라, 국제은행 간 송금, 환전, 국제 무역 등에도 블록체인 기술의 실증 시험이 이루어지고 있다. 외환거래결제 서비스 기업인 CLS 그룹은 블록체인을 이용한 환전 서비스 개시 시행할 것으로 발표했고, 바클레이즈 은행은 국제무역 거래에 블록체인 기술을 적용해 이미 성공시켰다. 또한, 독일에서는 HSBC 등의 7개 은행이 공동 국제 무역금융 플랫폼 'DTC(Digital Trade Chain)'을 개발해 거래 프로세스를 간결화하고 사무처리의 대폭적인 효율 향상을 계획 중이다.

이러한 블록체인 기술이 발달함에 따라 국가의 경계를 넘어 글로벌 기업들 간의 블록체인 기술을 위한 세계적인 컨소시엄들 또한 생겨나고 있다. 그중에서도 특히 R3와 Ripple Group은 금융업계에 특화된 글로벌 컨소시엄이다. R3는 2015년 9월 바클레이즈, UBS 등 세계적인 메이저 금융기관 9곳이 설립한 컨소시엄으로, 2017년 4월 시점에는 80개사 이상이 참여하고 있다. 특히 금융기관에 특화된 블록체인 플랫폼인 Corda를 개발하고, 2016년 11월부터 소스를 공개해 보급하는 등 활발히 활동 중이다. Ripple Group의 경우 2016년 9월 뱅크 오브 아메리카, 산탄데르 은행, 도쿄 은행 등 세계적인 은행 6곳이 국제 은행 간 송금 시스템 개발을 목적으로 한 컨소시엄이다. 2018년 초부터 블록체인 기반의 새로운 국제송금 서비스 시작이 예정되어 있다.

3.2. 자동차분야

블록체인 기술이 발전되고, 플랫폼 개발이 진행되면서, 블록체인 기술은 신뢰성, 보안이 필요한 영역에 많은 접근이 있었다. 자동차 분야는 보안에 아주 민감한 영역으로, 블록체인 기술을 통해 혁신적으로 발전할 수 있는 한 분야이다. 연구가 진행되고 있는 블록체인 기술 영역은 크게 두 가지 정도로 분류할 수 있는데, 첫 번째로 지능형 차량 간(V2V, Vehicle-to-Vehicle)에 적용하는 것, 두 번째로 지능형 차량과 네트워크 간(V2X, Vehicle-to-everything)에 적용하는 것이다.

V2V에 블록체인 기술을 적용하는 방법 연구는 차량 간의 소규모 통신 채널에 많은 초점을 맞춰서 이루어지고 있다. 지능형 차량 간의 데이터 공유에 블록체인을 기반으로 신뢰 환경을 설계하는 프레임워크 기술[9], 가시적인 빛 초음파를 공유하는 차량 간의 사이드 채널에 대한 블록체인 기반의 세션 프로토콜 기술[10] 등이 있으며 이들은 모두 지능형 차량을 하나의 peer로 생각하여, 인증된 제3기관이나, 서로에 대한 신뢰가 없어도 된다는 블록체인의 가장 큰 장점이자 기본 개념을 적용한 연구이다.

V2X의 경우는 더욱더 폭넓고 활발한 연구가 진행되고 있다. V2X 통신에 블록체인 기술을 적용해 리소스를 제한하고, 확장성을 가진 새로운 모델 제안[11], 개인 정보 보호 및 거래에 대한 신뢰성과 투명성을 제공하는 블록체인 기반의 전기 자동차 충전[12] 및 V2X의 엔터티 하나하나를 모두 peer로 고려하고, 이를 블록체인 네트워크에 참여시켜 자동차 보안 및 개인 정보 보호를 보장하는 분산 솔루션[13] 등이 있다.

위 기술들은 모두 2017년에 제시된 기법들이며, 기존의 자동차 통신에서 원격 조정, 대규모 네트워크 해킹 등 사회적으로 가장 민감하고 큰 걸림돌인 보안성 문제를 블록체인 기법을 적용해 해결 방법 제시한 것이다. 아직 위 기법에 대한 실질적인 실증시험이 있지 않았지만, 자동차 분야에 블록체인 기술이 보안성 문제를 해결할 수 있다는 큰 장점과 실질적으로 적용 가능하다는 점에서 앞으로 활발히 연구가 진행될 것으로 보인다.

3.3. 항만물류분야

비트코인으로 금융 분야에서 먼저 발전하기 시작한 블록체인은 그 다음으로 물류 분야에서 주목받기 시작했다. 이는 블록체인의 특징인 거래 원장이 분산되고, 신뢰할 수 없는 사용자에게 안전하며, 거래 내역이 투명하고, 데이터의 위변조가 어려운 것이 물류 사업에 적합하기 때문이다.

블록체인을 물류 공급망에 적용하면 데이터 위변조가 어려운 블록체인의 특성에 따라 제품의 생산부터 최

종 소비까지 공급 이력이 투명하게 공개된다. 이로써 유통 과정에서 원산지 조작, 제조 및 유통기간 변경, 제품 바꿔치기 등이 불가능해진다. 이에 소비자들은 식자재에 대한 신뢰도를 높일 수 있고, 제품의 정품 유무와 제품의 가격에 대한 정당한 가치를 측정할 수 있다. 특히 식자재의 경우, 운송망이 선진화된 국가에선 운송 과정에서 농식품이 상하는 경우가 3%도 되지 않지만, 중국과 같이 농식품 소비를 많이 하면서 운송망이 아직 선진화 되지 않은 경우는 운송 과정에서 25~30%의 농식품이 상한다[14]. 이 경우 식자재 유통망에 블록체인을 적용한다면 소비자들이 보다 안전한 먹거리를 선택하는데 도움이 될 것이다.

물류업계는 블록체인으로 화물들의 위치를 실시간으로 추적하면서 자신들의 화물을 관리할 수 있다. 이는 화물의 선적부터 인도까지 보다 합리적으로 운송 경로를 지정할 수 있게 해주며 이로 인해 운송 시간을 단축하고 운송 경비를 절감할 수 있다. 예를 들면 선적할 화물들의 위치가 바로 파악이 된다면 선박은 환적항에서의 정박 시간을 단축시킬 수 있다. 또 다른 예로 수출을 하기 위해서는 선박을 수배하고 선적을 예약한 후 배가 항에 도착하면 선적을 한다. 이러한 일련의 신고 절차나 선박의 적재 정보, 화물의 위치가 수출입 업체, 운송 업체, 항만, 세관과 은행 등에 공유된다면 제도적 절차가 뒷받침 된다는 가정 하에 많은 경비와 시간을 절약할 수 있다.

거래사간의 장부 공유로 인한 거래 시간 단축도 고려해 볼 수 있다. 이는 금융 분야와 더 맞물리지만, 실제로 수많은 물량이 국제적으로 오가는 항만물류 분야에서는 은행을 거치지 않고 적은 수수료로 빠르게 거래를 진행할 수 있다. 이렇듯 블록체인이 물류업계에 미칠 수 있는 기대효과가 매우 크기 때문에 해운·항만·물류업계에서는 블록체인의 도입을 적극 추진 중이다.

세계 최대의 컨테이너선 운용회사인 Maersk 그룹은 2017년 3월 5일, IBM과 함께 IBM의 Hyper ledger Fabric 솔루션을 운송 및 물류에 적용할 것이라고 밝혔다. 이는 공급망 프로세스를 디지털화하고 거래 파트너 간의 정보를 투명하게 하여 수천만개의 컨테이너들을 관리하고 추적할 수 있게 한다. Maersk는 케냐의 몸바사로부터 네덜란드의 로테르담 항까지 가는 컨네이너에 POC(Proof Of Concept)를 수행하여 추적하고 있다.

또한 Maersk는 마이크로소프트와 운송 보험에 대한 블록체인을 20주에 걸쳐 테스트 했다. 화주는 화물이 손상되거나, 폭풍으로 인해 운송이 지연되거나, 복잡한 항구에서 출항이 지연되거나, 해적으로 인해 습격을 받는 등 여러 가지 상황에 대해 중개인을 통해 보험을 구입한다. 이에 보험 거래에 블록체인을 적용하여 해운 공급망의 감사 측면을 보다 쉽게 만들고 데이터 변조 방지 및 공유를 통해 다양한 당사자가 보험료 조건을 정하도록 하였다.

유럽 최대의 무역항인 로테르담 항은 2016년 11월부터 물류 사업에 중심을 둔 블록체인 컨소시엄에 참가하고 있다. 그리고 영국국제화물협회(BIFA)도 블록체인이 공급망에 혁신을 일으킬 것으로 보고 있다.

우리나라는 2017년 5월 31일, 해운물류 블록체인 컨소시엄이 창립되어 블록체인 기술을 물류사업에 시범 운용하기로 하였다. 컨소시엄은 2017년 말까지 실제 수출입 물품을 대상으로 물류 프로세스 전반에 블록체인을 적용하고 아울러 법적·제도적 이슈도 협의한다.

3.4. 사물인터넷분야

사물인터넷은 소형 하드웨어와 무선 네트워크 기술의 발전으로 미래를 바꿀 기술로 각광 받았으나 제한된 플랫폼으로 인해 확장성이 부족하고 보안에 취약한 점이 그동안 단점으로 지적되었다. 그러나 여전히 4차 산업혁명의 근간에는 사물인터넷이 있다고 해도 과언이 아닐 만큼 사물인터넷은 각종 ICT 기술 융합의 중심에 위치하고 있다. 이러한 사물인터넷의 중요성을 부각하고 단점을 보완할 수 있는 기술로 블록체인이 지목되고 있다. 블록체인이 사물인터넷에 적용되면 가장 먼저 중앙 집중식이던 구조가 분산 구조가 되면서 여러 가지 변화가 생기게 된다.

먼저 사물인터넷 디바이스 간의 연결이 P2P 구조가 되면서 구성원 모두가 동등한 지위가 되어 계층 구조가 완화되게 된다. 이에 시스템 구축 및 유지비용이 절감하게 된다. 또한 게이트웨이와 같은 별도의 추가 장비 없이도 새로운 사물인터넷 디바이스가 시스템에 참여할 수 있게 된다.

개별 사물인터넷 디바이스들은 보안에 취약하며 그간 디바이스를 공격하여 시스템까지 공격하는 사례가 있어왔다. 2016년 데프콘에서 Nest의 온도 조절기를 해킹하여 비트코인을 요구하는 랜섬웨어를 시연한 것은

유명한 예다. 그러나 블록체인으로 인해 분산된 데이터를 가지는 환경에서는 사물인터넷 디바이스 하나만 공격하는 것은 의미가 없다. 즉, 시스템 일부에 문제가 생기더라도 전체 시스템은 대체로 안전하며 영향이 적다. 그렇기에 사물인터넷과 블록체인을 융합하여 응용하려는 시도도 다양하다.

Horizon은 사물인터넷을 블록체인으로 연결하여 모든 데이터를 수집하고 분석하려는 오픈소스 프로젝트다. Horizon에 참가한 노드들은 Horizon을 사용하여 서로를 발견하고 스마트 컨트랙트에 따라 자신의 거래 정보를 공유하고 원장에 기록한다. 따라서 모든 Horizon 참가자들은 서로의 거래 내용을 알 수 있고 합의를 통해 업데이트 되는 내용은 위변조가 불가능하다. Horizon의 참가자는 기본적으로 생산자와 소비자로 나뉘며 생산자의 데이터를 소비자가 받는 형태가 된다. 예를 들어 소비자가 특정 형태의 데이터를 원할 때 해당 정보를 Horizon에 올리면 생산자와 매칭이 되고 서로 간의 거래는 블록체인에 등록하여 계약을 완료하게 된다. 현재는 라디오 내용 분석이나 항공기 위치 추적, 디바이스의 현재 GPS 위치 추적 등 8가지 기능이 제공되고 있다.

아이오타(IOTA)는 암호화폐의 한 종류이지만, 사물인터넷의 리소스 공유를 지원한다. 아이오타는 블록이 없는 블록체인을 구현하며 다만 사물인터넷 디바이스들이 Tangle이라 불리는 분산된 공유 원장만을 통해 서로 리소스를 주고받는 것을 목표로 한다.

Ⅳ. 사물인터넷과 블록체인 융합 방안

본 장에서는 블록체인기반의 사물인터넷 환경을 구축하기 위해서 만족되어야 하는 요구사항을 도출하고, 블록체인 기술을 사물인터넷 환경에 적용하는 방안을 제시한다.

4.1. 사물인터넷에서 요구사항

블록체인 기반의 탈중앙화 사물인터넷 시스템을 구축할 때 요구되는 사항은 아래 [표 1]과 같다.

〔표 1〕 블록체인 기반 탈중앙화 사물인터넷 요구사항

No.	요구사항
1	플랫폼으로부터 인가받지 않은 노드도 쉽게 플랫폼에 참여 및 탈퇴가 가능해야한다
2	플랫폼에 참여한 노드는 자신 외에 플랫폼에 참여한 모든 노드를 발견할 수 있어야 한다
3	플랫폼에 참여한 모든 노드들은 평등한 권한을 가진다
4	플랫폼에 참여한 모든 노드들의 리소스는 공유된다
5	공유된 리소스를 통해 데이터의 기밀성과 무결성을 보장할 수 있어야 한다
6	데이터의 가용성과 접근성을 보장해야 한다
7	신뢰할 수 없는 노드로부터의 데이터는 합의 과정에서 폐기되어야 한다
8	플랫폼에 참여한 악의적인 노드로부터의 공격에 전체 플랫폼은 안전해야 한다
9	플랫폼에 참여한 일부 노드의 장애가 전체 플랫폼의 장애로 확산되지 않아야 한다
10	DoS 공격으로부터 전체 플랫폼이 마비되지 않아야 한다

4.1.1 플랫폼 참여 및 탈퇴

기존의 중앙화 사물인터넷 플랫폼 구조에서는 사물인터넷 디바이스를 플랫폼에 등록 시키고 인가를 한 수 사용을 했으나, 탈중앙화 사물인터넷 플랫폼에서는 사물인터넷 디바이스가 자유롭게 플랫폼에 참여하고 탈퇴가 가능하다.

4.1.2 플랫폼 내 노드의 발견

플랫폼에 참여한 노드는 플랫폼에 참여한 모든 노드를 발견하고 거래(리소스 교환)를 할 수 있다.

4.1.3 평등한 권한

기존 사물인터넷 플랫폼처럼 서버 역할을 하는 노드가 없으므로 플랫폼 내 모든 노드는 동등한 권한을 지니며 상태 변화를 할 때는 전체 노드들의 합의 과정을 가진다.

4.1.4 리소스 공유

플랫폼에 참여한 모든 노드들의 리소스는 서로에게 투명하게 공개되고 공유된다.

4.1.5 기밀성 및 무결성 보장

리소스는 암호화 되어 공개되어 허가 받지 않은(거래 당사자가 아닌) 노드에게는 기밀성이 유지된다. 또한 모든 노드가 데이터를 공유하므로 무결성이 보장된다.

4.1.6 데이터 가용성과 접근성 보장

모든 노드들은 플랫폼 내의 다른 노드의 리소스에 접근이 가능하며 정해진 프로토콜에 따라 노드 간 계약을 맺고 데이터를 사용할 수 있다.

4.1.7 신뢰할 수 없는 데이터 폐기

신뢰할 수 없는 노드(계약 내용과 다른 데이터를 보내거나, 네트워크가 불안정하거나, 다른 노드와 상이한 상태를 지닌)의 데이터는 합의 과정을 통해 폐기하고 공유하지 않는다.

4.1.8 단일지점에서의 공격 방지

악의적인 노드, 또는 외부에서 공격을 받아 플랫폼 내에서 변질한 단일 노드는 합의 과정에서 극히 일부의 능력 밖에 내지 못하므로 플랫폼 내 노드들에 공유된 전체 데이터를 위변조 할 수 없다.

4.1.9 단일장애지점으로부터의 장애 확산 방지

플랫폼 내 모든 노드는 동일한 권한을 가지므로 단일 장애지점이 발생하더라도 해당 노드를 배제해도 데이터 공유에 큰 영향이 발생하지 않는다.

4.1.10 DoS 공격 방지

DoS 공격은 단일장애지점을 만드는 데 효과적인 공격이나 탈중앙화 된 사물인터넷 플랫폼에서는 일정 비율 이상의 참여 노드를 공격해야하므로 DoS 공격에 강인하다.

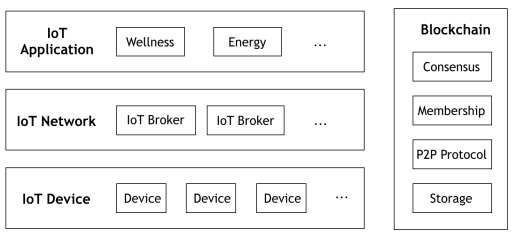
4.2. 블록체인기반 사물인터넷 플랫폼

본 절에서는 사물인터넷에서 단일장애지점(Single point of failure) 문제를 해결할 수 없는 기존의 사물인터넷 환경을 블록체인 기술을 통해서 해결하기 위한 방안을 제시한다. 사물인터넷 환경은 응용서비스, 플랫폼, 네트워크, 디바이스의 4개의 계층으로 나누어진다. 이러한 전형적인 사물인터넷 플랫폼에서는 디바이스에서 수집되는 사물인터넷 빅데이터를 사물인터넷 게이트웨이 또는 브로커(Broker)를 통해서 사물인터넷 플랫폼으로 전달된다. 사물인터넷 플랫폼에서는 주로 데이터를 분석 후 정형화하는 역할과 응용서비스를 위해 가공하는 역할을 수행한다. 하지만, 사물인터넷기반 응용서비스들은 하나의 플랫폼에서 데이터를 제공받는다. 다시 말해서, 모든 응용서비스는 하나의 플랫폼에 가용성을 의존할 수밖에 없으며, 이것은 단일장애지점의 원인을 제공할 수 있다.

사물인터넷 플랫폼은 근본적으로 데이터허브의 역할을 제공하는데, 본 논문에서는 위에서 언급된 문제를 해결하기 위해서 블록체인기반 데이터허브 사물인터넷 플랫폼을 제시한다. 블록체인기반의 데이터허브는 사물인터넷 브로커와 응용서비스가 주체가 되어 데이터를 블록으로 하는 블록체인을 구성한다.

기존의 사물인터넷 환경은 수직적인 4계층 구조를 가지고 있었지만, 블록체인기반 사물인터넷 환경에서는 사물인터넷 플랫폼을 대신할 수 있는 블록체인 계층을 수평적으로 구성한다.

[그림 5]와 같은 블록체인기반 사물인터넷 아키텍처에서는 사물인터넷 디바이스에서 수집되는 데이터는 직접적으로 또는 사물인터넷 네트워크계층을 거쳐서 블록



〔그림 5〕 블록체인기반 사물인터넷 구조도

체인 네트워크에 추가된다. 사물인터넷 응용서비스에서는 사물인터넷 플랫폼 대신에 블록체인 네트워크로부터 데이터를 가져올 수 있다. 이러한 구조에서는 단일장애지점에 대한 문제가 사라지며, 블록체인 기술을 이용하여 데이터에 대한 신뢰성 및 일관성을 보장받을 수 있다.

Ⅴ. 결론 및 향후연구

고전적인 사물인터넷의 4계층 구조에서는 사물인터넷 플랫폼이 데이터허브 및 데이터가공을 위한 주요역할을 수행함에 따라 응용서비스에 서비스 친화적 데이터를 제공해주는 반면, 사물인터넷 플랫폼에 모든 서비스가 가용성을 의존하게 되는 단일장애지점에 대한 이슈를 야기한다.

본 논문에서는 이를 해결하기 위해서 기존의 수직적인 4계층 사물인터넷 구조에서, 플랫폼을 제외하고 블록체인계층을 수평적으로 배치하여 사물인터넷 디바이스, 네트워크, 서비스가 블록체인 네트워크를 통해서 상호간의 데이터 및 서비스를 제공해주는 역할을 수행할 수 있는 구조를 제시하였다. 이러한 구조에서는 다양한 응용서비스가 상호간에 데이터를 공유할 수 있는 선순환 구조를 가질 수 있다. 하지만 블록체인에서 프라이버시 이슈와 권한제어 등의 이슈가 있다.

따라서, 실질적으로 블록체인기반 사물인터넷 구조를 구축하기 위해서는, 데이터 유형정의, 탈중앙화 데이터 저장소 관리에 대한 이슈와 블록체인 기술의 근본적인 이슈로써 고속검색, 실시간성, 데이터 접근권한제어에 대한 연구가 필요하다.

참 고 문 헌

[1] R. Roman, J. Zhou, J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” *Computer Networks*, 57, pp. 2266-2279, 2013

[2] D. Christin, A. Reinhardt, P. S. Mogre, R. Steinmetz, “Wireless sensor networks and the internet of things: selected challenges,” *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose sensornetze*, pp. 31-34. 2009

[3] M. J. Covington, R. Carskadden, “Threat implications of the internet of things,” *In Cyber Conflict (CyCon)*, pp. 1-12, June, 2013

[4] A. Alcaide, P. Esther, M. José, R. Arturo, “Anonymous authentication for privacy-preserving IoT target-driven applications,” *Computers & Security*, 37, pp. 111-123, 2013

[5] X. Lin, S. Lin, Q. Haipeng. “Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications.” *Computers & Security*, 48, pp. 142-149, 2015

[6] J. B. Bernabe, L. H. Jose , V. M. Moreno, A. F. S. Gomez, “Privacy-preserving security framework for a social-aware internet of things.” *In International conference on ubiquitous computing and ambient intelligence*, pp. 408-415, December, 2014

[7] A. Ukil, S. Bandyopadhyay, A. Pal, “Iot-privacy: To be private or not to be private. In Computer Communications Workshops (INFOCOM WKSHPS),” pp. 123-124, April, 2014

[8] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, 76, pp. 146-164, 2015

[9] Singh, Madhusudan, and Shiho Kim. “Blockchain Based Intelligent Vehicle Data sharing Framework.” *arXiv preprint arXiv: 1708.09721*, July, 2017

[10] S. Rowan, M. Clear, M. Gerla, M. Huggard, , C. M. Goldrick,“Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels,” *arXiv preprint arXiv:1704.02553*, April, 2017

[11] R. W. van der Heijden, F. Engelmann, D. Mödinger, F. Schönig, F. Kargl, “Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication,” *Scalable and Resilient Infrastructures for Distributed Ledgers*, October, 2017

[12] F. Knirsch, A. Unterweger, D. Engel,

"Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science-Research and Development*, pp.1-9, September, 2017

[13] A. Dorri, M. Steger, S. S. Kanhere, R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, pp.119-125, December, 2017

[14] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," *Service Systems and Service Management (ICSSSM)*, 2016 13th International Conference on. IEEE, pp. 1-6. June. 2016.

〈저 자 소 개〉

최 종 석 (Jongseok Choi)
정회원

2011년 2월 : 동명대학교 공학사
2013년 2월 : 부산대학교 공학석사
2017년 2월 : 부산대학교 공학박사
관심분야 : 정보보호 및 보안, 사물인터넷, 블록체인, 취약점 분석

박 종 규 (Jong-gyu Park)
정회원

2014년 2월 : 부산대학교 정보컴퓨터공학과 졸업
2014년 9월~현재 : 부산대학교 컴퓨터공학과 석박사 통합과정
관심분야 : 정보보호 및 보안, 사물인터넷, 블록체인, FPGA 구현

김 명 길 (Myeong-kil Kim)

2017년 2월 : 부산대학교 정보컴r퓨터공학과 졸업
2017년 3월~현재 : 부산대학교 컴퓨터공학과 석사과정
관심분야 : 정보보호 및 보안, 사물인터넷, 블록체인

김 호 원 (Howon Kim)
정회원

1993년 2월 : 경북대학교 공학사
1995년 2월 : 포항공과대학교 공학석사
1999년 8월 : 포항공과대학교 공학박사
2004년 8월 : Ruhr University Bochum, Post Doctorial
1998년 12월~2008년 2월 : 한국전자통신연구원 정보보호센터 선임연구원/팀장
2008년 3월~현재 : 부산대학교 전기컴퓨터공학부 정교수
관심분야 : 사물인터넷, 정보보호 및 보안, 머신러닝/딥러닝, FPGA/ASIC 칩 설계