특집 01

사물인터넷과 블록체인 기술 적용 동향

유소망 (고려대학교), 김종완 (삼육대학교)

목차

1. 서 론

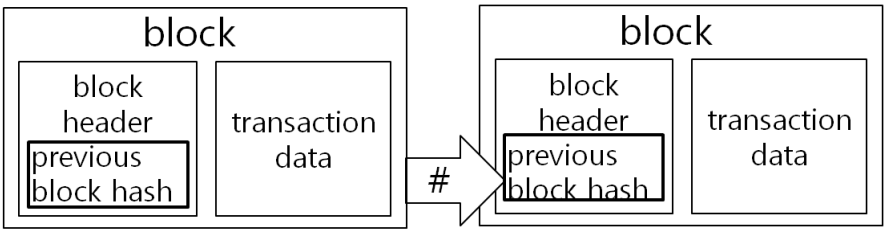
개인 간(P2P) 거래에 사용되는 암호 화폐인 비트코인(Bitcoin)은 2009년에 서비스를 시작한 이후 현재까지 거래량이 700억 달러에 이른다. 블록체인은 비트코인의 보안성에 기반이 되는 공개거래장부에 해당하며 비트코인에 적용된 블록체인은 아직까지 해킹에 노출된 적이 없는 만큼 보안에 강하다.

블록체인(Blockchain)의 보안성에 따라 최근에는 암호 화폐 뿐 아니라 공유 경제 애플리케이션, 저작권료 지급 시스템과 같이 보안성, 신뢰성이 필요한 다양한 기술에 블록체인을 적용하고 있다.

IoT는 물리적인 장비와 웹을 결합해 장비, 서비스 그리고 사용자 간의 상호작용을 활성화한다. 블록체인으로 해결할 수 있는 IoT 보안 기술에는 권한 관리, 데이터 스트림(Data Stream) 보안성 그리고 서로 다른 장비 사이의 식별 기능이 있다. 이 경우, 다음과 같은 장점이 있다. 먼저, 블록체인은 P2P 네트워크 규모에 따른 높은 데이터 신뢰성, 분산형 방식으로 많은 장비를 수용할 수 있는 확장성이 있다. 그리고 블록체인에서 공개키 인프라를 제공하기 때문에 별도의 공개키 인프라를 위한 서버 유지비용을 줄임으로써 IoT를 위한 경량의 높은 보안성을 유지할 수 있다.

하지만 블록체인이 연산을 소모하고, 네트워크 트래픽이 많이 요구되는 특성이 있어 자원이 한정된 IoT 기기에서 구동할 수 없는 한계가 있다. 또한 보안성이 작업증명이라는 채굴 조건에 따라 P2P 네트워크의 전체 연산능력에서 기인하기 때문에 규모있는 네트워크 구축의 가능성을 고려해야 한다.

이러한 맥락에서 본 논문의 구성은 다음과 같다. 2절에서 블록체인의 구조와 그에 따른 보안



(그림 1) 블록체인의 구조

성에 대해 설명한다. 3절에서는 사물인터넷에 블록체인이 적용된 연구들을 소개하며 오버레이 네트워크의 구성 방식과 그것의 최적화 방식을 소개한다. 4절에서는 P2P 네트워크 구축에 강점이 있는 스마트 컨트랙트의 응용 사례를 소개한다. 5절에서는 다양한 응용 분야를 소개하며 마지막으로 iot보안을 위한 블록체인의 추가연구를 포함한 방향을 제시하면서 6절에서 결론을 맺는다.

2. 블록체인의 구조와 보안성

이 장에서는 사물인터넷에 블록체인이 적용된 배경을 알아보기 위해 블록체인의 구조를 통해 보안성 원리를 설명한다. 미리 언급하자면, 충분한 채굴자들을 확보해 전체 블록체인 네트워크가 큰 연산 능력이 있어야 보안성을 유지할 수 있다.

2.1 블록체인의 구조

블록체인의 기본 구조는 다음과 같다. 먼저, 블록(Block)에는 (그림 1)과 같이 트랜잭션(Transaction)이라고 불리는 거래 내역이 저장된다. 블록들의 헤더(Header)는 이전 블록 데이터를 암호화하는 해시(Hash)값을 연결고리로 하는 체인 형태로 이어져있다. 또한 전체 네트워크의 모든 노드(Node)에 데이터가 중복 저장되어 있으므로 위변조가 불가능하다. 더욱이 블록은 일정 난이도를 갖고 생성되어 체인이 길어질수록 블록의 신뢰도가 증가한다.[2]

2.2 블록의 채굴 과정

거래를 위조할 수 없도록 채굴자(Miner)[1]들은 트랜잭션 내역을 수집해 검증하고 작업증명(PoW, Proof of Work)이라는 연산 능력 경쟁을 통해 블록을 생성한다. 해시 함수는 역산으로 각 출력 값에 대응하는 입력 값을 찾기 어려운 일방향(One Way) 연산을 수행한다. 이러한 특성을 이용하여 채굴자들이 서로 연산 능력을 경쟁할 수 있는 조건이 주어진다. 작업증명은 해시연산을 반복하면서 특정 난이도[2](Difficulty)가 출력 값으로 나오는 입력 값(넌스, Nonce)을 찾는 것이다. 작업 증명을 성공해 생성한 블록을 후보블록이라고 한다.

2.3 장부 내역에 대한 합의 과정

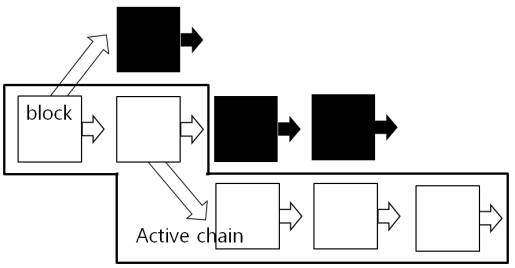
블록의 생성에 성공한 채굴자는 해당 후보 블록을 브로드캐스팅(Broadcasting)하며 이웃 채굴자는 수신한 블록을 검증한다. 검증 과정에서는 수신한 후보 블록에 포함된 트랜잭션들을 개별

1) 채굴자들은 P2P 노드로서 작업증명을 수행하여 블록을 생성한다. 비트코인에서 블록생성에 성공하는 채굴자는 새로 발행된 비트코인을 보상으로 받는다. 채굴자가 새 코인을 보상으로 받는 거래 내역도 새 블록에 포함된다.

2) 난이도는 블록 채굴의 어려운 정도를 조절하며 모든 노드가 알고 있는 전체 네트워크의 설정 값이다.

적으로 확인하고 작업증명 연산을 다시 수행한다. 후보 블록에 문제가 없으면 검증되었다는 의미로 자신의 블록체인에 포함시키고 이후에 블록체인에 저장된 데이터를 기반으로 새 블록을 채굴한다. 비트코인에서는 이 과정이 6번 반복되면 해당 블록에 포함된 거래가 승인된다.

앞서 설명한 연산 능력의 경쟁 조건을 이용해 안전하게 블록체인에 합의하기 위한 최장체인 알고리즘이 있다. 이 알고리즘에서 블록체인은 (그림 2) 와 같이 나뭇가지 모양으로 분기하며 비트코인에서는 분기된 가지 중 (그림 2)의 하얀 블록들로 표시된 부분과 같이 가장 긴 체인을 선택한다. 이때, 선택된 체인을 액티브 체인(Active Chain)이라고 부른다[1].



(그림 2) 최장체인 알고리즘

2.4 이중지불 공격과 블록체인의 보안성

블록체인을 공격하는 방법에는 대표적으로 이중지불 공격이 있다. 공격자가 가진 잔고를 한 번 사용한 뒤 해당 거래 데이터를 무력화 시키는 가짜 체인을 발표해 다시 지불에 사용하는 것이다. 공격자가 가짜 블록체인을 배포해 거래 내역을 조작하려면 네트워크가 변조된 블록을 받아들이게 해야 한다. 이를 위해서는 가장 긴 체인을 만들기 위해 빨리 블록을 만들어 전파해야 한다. 또한 가짜 체인보다 긴 체인이 생성되는 것을 막기 위해 공격자의 트랜잭션에 반하는 트랜잭션과 그것을 저장한 다른 채굴자의 블록이 승인되는 것을 막아야 한다. 따라서 이중지불 공격을 막기 위해서는 공격자가 전체 네트워크 연산 능력 중 50% 이상을 소유하고 있어야 한다.

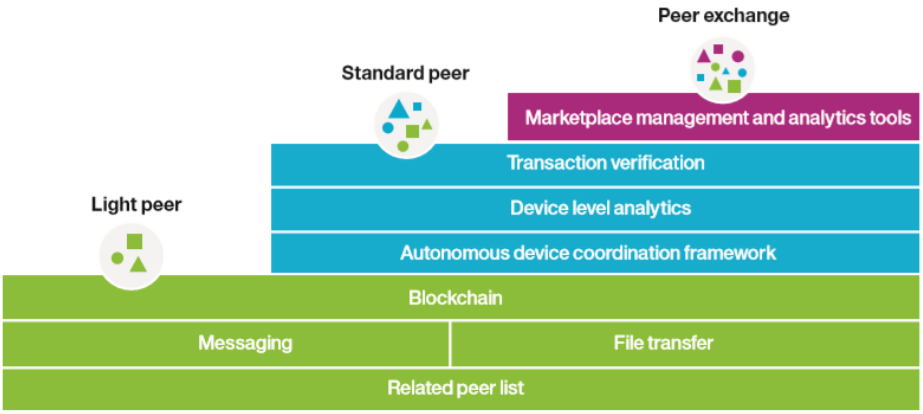
그런데 비트코인의 경우 컴퓨팅 파워(Computing Power)가 약 2800만 펩타플롭스(PetaFLOPS)가 넘는다[3]. 이는 세계에서 연산 능력이 가장 높은 슈퍼컴퓨터인 중국의 선웨이 타이후라이트(Sunway TaihuLight)가 93펩타플롭스인 것을 고려할 때 비트코인 메인 네트워크의 공격이 사실상 불가능한 것을 알 수 있다.

이와 같은 블록체인의 보안성을 적용하는 분야가 다양하다. 최근에는 암호 화폐 뿐 아니라 에어비앤비(Airbnb)와 같은 공유 경제 앱(App), 은행이나 저작권료 지급 시스템과 같이 보안성 및 신뢰성이 필요한 다양한 분야에 적용하고 있다.

3. 연산 오버헤드 문제의 해결 방안

IoT 환경에 블록체인을 적용하면 단일 서버로 IoT 기기들을 관리하는 것보다 많은 기기를 수용할 수 있고 서버가 다운될 우려가 없어 안정적이다. 하지만 블록체인이 작업증명을 수행하기 위해 해시 연산을 반복적으로 수행해 컴퓨팅 오버헤드가 크기 때문에 사물인터넷에 블록체인을 적용하려면 필연적으로 연산 오버헤드 문제를 해결해야 한다. 따라서 이 장에서 채굴의 기능을 담당하는 노드와 트랜잭션 생성을 담당하는 노드를 구분하는 해결 방법이 대표적인 해결방법을 소개한다.

블록체인을 IoT에 적용한 대표적인 사례로 어뎁트(Adept)가 있다. 블록체인을 응용해 사물인터넷 기기가 서로 직접 소통하는 P2P 네트워크를 구축하는 목적이다. 스마트 홈과 같은 환경에



(그림 3) Adept의 3가지 피어 타입[4]

서 프라이버시가 침해되거나 안전상의 위험이 없기 위해 블록체인을 사용해 IoT 기기의 설정 파일을 암호화한다.

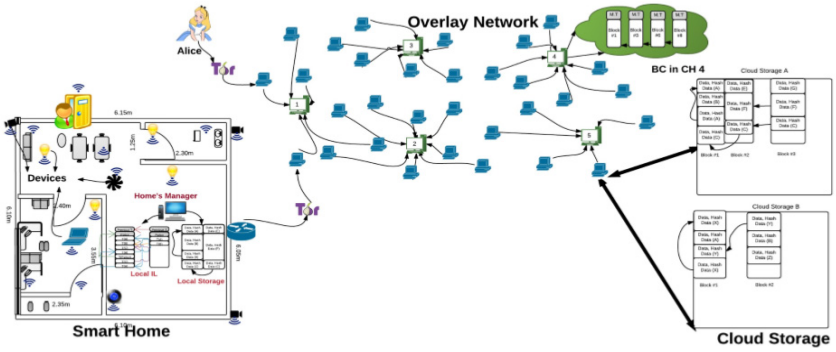
어뎁트는 (그림 3)과 같이 IoT기기의 한정된 자원으로 블록체인 기능을 사용하기 위해 채굴 기능을 하는 피어를 따로 두는 3가지의 피어 타입(Peer Type)을 제공하고 있다. 그 중 라이트 피어(Light Peer)와 스탠다드 피어(Standard Peer)는 메모리와 저장 공간이 제한적인 IoT 기기에서 블록체인을 구동해야 하는 문제를 해결하기 위한 것이다.

라이트 피어(Light Peer)는 메모리(Memory)와 저장 공간에 한계가 있는 IoT 장비에 사용되며 지갑 보유, 메세징, 트랜잭션 수행 기능을 할 수 있다. 스탠다드 피어(Standard Peer)는 라이트 피어의 기능을 포함해 트랜잭션 검증 기능을 추가적으로 수행한다[4].

[5]도 같은 방식을 사용하는데, 이것은 비트코인에서 단순지불검증[3] 방식과 같다. IoT 기기에서는 트랜잭션만 수행하고 나머지 블록 채굴을 하는 기능은 일반 서버로 구성된 P2P 네트워크에서 수행한다. 논문에서는 스마트 홈(Smart Home) 사용자의 프라이버시(Privacy) 보안성과 확장성을 위해 블록체인을 적용하고 블록체인의 보안성에 대해 설명한다. DDOS 공격의 경우 모든 장비들의 트랜잭션이 채굴자에게 검사되므로 공격자로 의심되는 IoT 노드들을 차단할 수 있다. 또한 링킹 어택(Linking Attack)은 같은 공공키를 사용하는 거래들을 연결해 실제 ID를 유추하는 공격이다. 프라이버시 문제가 발생할 수 있어 채굴자가 트랜잭션 마다 다른 개인키를 사용해 해결한다.

하지만, 트랜잭션이 발생하거나 후보 블록이 생성되었을 때 브로드캐스팅(Broadcasting)하는 특성이 있어 네트워크 트래픽이 많이 발생한다. 그에 따라 [6]은 (그림 4)와 같이 네트워크 오버헤드와 지연 시간을 줄이기 위해 오버레이 노드를 클러스터로 그룹 짓는다. 각 클러스터에서는 클러스터 헤드(CH, Cluster Head) 노드를 선출한다. 클러스터 헤드는 공공키 리스트를 가지고

3) 풀 노드는 블록체인 전체를 저장하며 트랜잭션 기능과 채굴 기능을 모두 수행하지만 단순지불검증 노드는 트랜잭션 기능만 수행한다. 단순 지불검증 노드는 주로 스마트폰과 같은 자원이 한계적인 기기를 의미한다. 단순지불검증 노드는 트랜잭션 정보와 블록 헤더의 머클 루트(Root)를 가지고 풀 노드에게 머클 경로의 증명을 요청하여 해당 트랜잭션이 블록에 포함되었는지 유무를 확인할 수 있다.



(그림 4) 클러스터가 있는 오버레이 네트워크 구조[6]

블록을 생성하는 권한을 부여하고 IoT 기기의 접근을 허용한다. 또한 블록체인 데이터의 크기 문제를 해결하기 위해 블록체인 데이터를 블록 번호에 맵핑(Mapping)되도록 구성해 클라우드 스토리지(Cloud Storage)에 저장한다.

이 장에서 설명한 방식을 사용하면 블록을 채굴자들이 감소하여 전체 네트워크의 연산 능력 감소와 그에 따른 보안성의 약화의 우려가 있다. 실제로 비트코인의 경우에도 단순지불검증 노드가 가장 많다. 채굴자와 블록체인 사용자의 역할을 따로 설정하지 않고 병합하면 채굴자 네트워크를 유지하기가 수월할 것이다.

또한 블록체인의 채굴 네트워크를 구축해 단일 서버 구축 비용을 줄일 수 없다. 블록체인 기반의 암호화폐들은 채굴자들이 보상으로 발행한 화폐를 지급받는다. 하지만 외부 채굴자가 없는 프라이빗 네트워크에서 블록체인은 오히려 모든 노드가 같은 데이터를 중복 저장하며, 연산 능력 경쟁을 위해 소모적으로 작업 증명을 수행하기 때문에 단일 서버에 비해 비용이 적다고 볼 수 없다.

4. 스마트 컨트랙트와 응용

스마트 컨트랙트(Smart Contract)[7]는 블록체인에 거래 내역 뿐 아니라 변수와 함수를 저장할 수 있도록 해 블록체인을 응용할 수 있는 다양한 가능성을 열어 주목받고 있다. 이 장에서는 보안성을 제공할 수 있는 큰 규모의 프라이빗 네트워크(Private Network)[4]를 구축하지 않고 스마트 컨트랙트를 사용해 이미 구축된 퍼블릭 네트워크(Public Network)를 IoT환경에 적용하는 연구를 소개한다. 하지만 아직 매 트랜잭션이 인증되는데 소요되는 지연 시간이 있는 단점이 있다.

이더리움(Ethereum)은 블록체인을 프로그래밍할 수 있는 플랫폼(Platform)이다. 즉, 프로그래머들이 블록체인 위에서 코인(Coin)의 거래 방식을 규정할 수 있도록 스마트 컨트랙트라는 스크립트(Script)를 구동할 수 있다. 예를 들어, 스마트 컨트랙트를 가지고 클라우드 펀딩(Cloud Funding)과 같은 제3자 간의 거래를 구현할 수 있다. 그러므로 스마트 컨트랙트를 통해 블록체인의 다양한 적용 가능성이 제공된다. 또한 이더리움의 메인 네트워크(Main Network)를 사용할 수 있다는 장점이 있다.

비트코인과 이더리움에서 블록체인의 상태

4) 비트코인, 이더리움과 같은 누구나 네트워크에 참여할 수 있는 블록체인 환경을 퍼블릭 네트워크라고 한다. 반대로 하나의 기관에서 독자적으로 사용하는 블록체인 환경을 프라이빗 네트워크라고 한다. 여러 기관들이 협력해서 구성하는 블록체인 환경은 컨소시움 네트워크(Consortium Network)라고 하며, 허가된 기관만 네트워크에 참여할 수 있다.

(State)는 블록체인에 저장된 모든 변수와 그 값이다. 변수 중에는 모든 계정들이 소유한 이더리움 잔고와 컨트랙트의 내부 변수가 있다. 새 트랜잭션의 입력 값은 이전 상태이며 출력 값은 새로운 상태이다. 이더리움은 이 상태 개념을 기반으로 튜링완전성을 제공해 블록체인의 무한한 응용 가능성을 제공한다.

앨런 튜링은 튜링완전언어를 사용하며 무한한 저장공간이 있다면 이 세상의 모든 문제를 풀 수 있는 기계를 만드는 것이 가능하다고 주장했다. 이더리움에서 블록체인이 무한에 근접한 저장공간의 역할이다. 튜링완전언어는 프로세스를 분할해 아주 작은 단위로 사용할 수 있으며, 조건 설정과 반복문이 있다. 이더리움에서는 솔리디티(Solidity)라는 프로그래밍 언어를 지원한다.

비트코인에서 스크립트를 제한했던 이유는 블록체인이 무한루프에 빠지지 않게 하기 위해서이다. 이 문제를 해결하기 위해 이더리움에서는 스마트컨트랙트의 등록과 트랜잭션마다 수수료[5]가 요구된다. 하지만 이 소비를 계산하는 것도 네트워크에서 합의 과정을 거쳐야 하므로 오버헤드가 된다.

[8]은 다수의 IoT 장비에 대해 장비의 설정과 사용자 인증을 지원하며 동기화 문제없이 수용하기 위해 블록체인을 적용했으며 장비 설정 방법을 쉽게 구현하기 위해 이더리움의 스마트 컨트랙트를 적용했다. [7]에서 세터(Setter), 게터(Getter)함수를 만들어 LED, 에어컨의 설정 값을 블록체인에 저장하도록 구현했는데 이 연구는 스마트 컨트랙트를 사용한 구현이 상당히 단순하다는 것을 설명하고 있다. 하지만 이러한 방식은 12초의 트랜잭션 시간을 기다려야 한다. 또한 자원이 한정적인 IoT 장비에 블록체인을 구동할 수 없어 블록체인을 구동하는 프록시(Proxy) 역할을 하는 별도의 서버가 필요하다.

[9]는 스마트 시티(Smart City)의 주민들이 센서 모니터링을 할 때 환경 데이터에 누구나 접근 가능하지만 수정은 불가능하도록 권한을 제한하기 위해 블록체인을 적용한 CitySense시스템을 제안했다. 이 시스템은 날씨, 습도, 온도와 같은 환경 데이터를 주민들이 받아볼 때 정확한 정보를 전달하기 위해 주민들이 데이터를 수정할 수 없고 접근만 할 수 있도록 설계했다. 특히, 트랜잭션을 통해 노드 간에 통신하도록 구현하고 있으며 컨트랙트를 포함한 트랜잭션을 통해 계정 간에 메시지를 주고받을 수 있게 했다. 이 메시지는 수신자의 주소, 호출할 컨트랙트 함수, 파라미터(Parameter)의 리스트(List)를 포함한다. 스마트 컨트랙트를 이용해 센서(Sensor)로부터 메시지(Message)를 받는 함수, 정보를 다시 받아 블록체인에 저장하고 사용자의 질의를 받아 정보를 제공하는 함수를 구현했다.

5. 다양한 적용 가능성

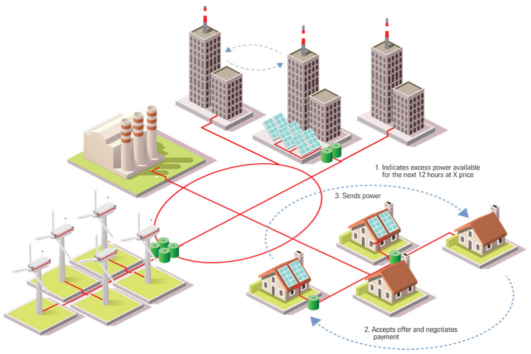
이 장에서는 사물인터넷과 블록체인 기술이 응용된 연구들을 소개한다. 블록체인 기술은 사물인터넷 분야에서 스마트 그리드와 SD-IoT와 같이 다양한 적용가능성이 있다.

5.1 스마트 그리드

스마트 그리드(smart Grid)는 전기 및 정보통신 기술을 활용하여 전력망을 지능화·고도화한 것인데, 신재생에너지의 사용을 확대하여 소비자의 참여로 설비가 운영되면서 에너지 이용효율

5) 거래수수료는 송금자가 지불하며 해당 거래가 포함된 블록을 생성한 채굴자에게 주어진다. 이더리움에서는 가스(Gas)를 거래수수료로 사용하며 가스는 이더리움을 가지고 사고 팔 수 있다.

을 극대화하는 전력망이다 [10]. 스마트그리드에 블록체인을 적용하면 비용을 줄이면서 안정성 있는 관리 시스템을 구축 수 있다.



(그림 5) 비중앙집중형 스마트그리드[10]

골드만 삭스(Goldman Sachs)의 보고서에서 블록체인을 스마트 그리드(Smart Grid)에 적용할 것을 제안했다. (그림 5)와 같이 에너지(Energy) 생산자가 소비자인 양방향식 환경을 구성한다. 비중앙집중적인 시스템을 통해 전력 중개자의 비용을 줄이며 안정성 있는 에너지 마켓을 만들 수 있다는 장점이 있다 [11].

DeviceChain[12]은 이러한 접근 방법의 프로토타입 구현을 위해 블록체인을 이용해 스마트그리드 기기를 인증하는 방식을 제안했다. DeviceChain은 AMI 6)기기 인증 내용을 블록체인에 저장하고 검침 서버들이 블록을 검증한다. 기존의 PKI(Publick Key Infrastructure, 공개 키 인프라)는 최소 4단계를 거쳐 인증처리를 하고 서버도 용도에 맞게 독립적으로 4개 이상이 필요하다. 이에 반해 DeviceChain은 서버와 기기 간에만 일어나는 절차로 비교적 간단하다.

구현에는 비트코인 테스트넷(Testnet)을 사용했다. 테스트넷은 개발자들이 실제 비트코인을 소유하지 않으며 메인 블록체인을 망가뜨릴 위험 없이 비트코인을 테스트할 수 있는 별도의 블록체인이다. 이러한 구현 방식은 블록에 트랜잭션들이 저장되고 남는 여유 데이터 공간이 한계적이기 때문에 비트코인을 커스터마이징(Customizing)하는 데 한계가 있다. 또한 비트코인이 메인 네트워크를 사용하는 것이 아니므로 전체 네트워크의 연산 능력을 유지하는 비용이 많이 소요되며 네트워크 규모가 작을수록 보안성이 약화된다. 따라서 적절한 네트워크 구성 방식이 연구될 필요성이 있다.

5.2 네트워크 관리 보안성

소프트웨어 정의 네트워크(SDN, Software Defined Networking)는 트래픽(Traffic) 목적지를 결정하는 컨트롤 플래인(Control plain)과 포워딩(Forwarding)을 담당하는 데이터 플래인(Data Plain)을 분리함으로써 네트워크 관리를 추상화한다. 그에 따라 SDN의 네트워크 관리 가능성에 보안성을 결합하는 장점이 있다.

(그림 6) SD-IoT에서 가상 자원[13]

SDN을 IoT에 적용한 것을 SD-IoT라고 하며 이는 가상 자원을 노출 시켜 장비의 권한 관리와

6) AMI(Advanced Metering Infrastructure, 원격검침인프라)는 스마트 미터(smart meter)에서 측정한 전력 사용량 데이터를 전송해 원격에서 전력 사용을 분석하는 기술이다.

IoT 컴포넌트의 커스터마이징을 쉽게 한다. [13]는 (그림 6)과 같이 클라우드 상에서 Bluemix 플랫폼을 사용해 블록체인으로 가상 자원을 허가받을 수 있는 시스템을 제안했다.

5.3 사물인터넷 기기 관리의 보안성

[14]는 사물인터넷 기기의 소유자가 프라이버시를 침해 받지 않고 센서 데이터를 판매해 수수료를 받을 수 있는 ChainAnchor 시스템을 제안한다. 블록체인에서 각 사용자에게 해쉬 값 기반의 공공키가 아이디로 부여되며 트랜잭션에 사용된다. 익명성을 사용해 기기 소유자의 프라이버시를 보호한다는 장점이 있다.

[15]는 펌웨어 기기를 블록체인을 통해 안전하게 업데이트 할 수 있는 시스템을 제안한다. 펌웨어 기기가 블록체인 노드에 업데이트를 요청하면, 블록체인 노드는 해당 기기의 업데이트 여부를 확인한다. 기기가 최신 버전으로 업데이트 되지 않은 경우 블록체인 노드가 최신 펌웨어의 피어 리스트를 제공한다. 그 다음 업데이트를 요청한 노드는 최신 펌웨어를 가진 노드에게 다운로드를 받는다. 반대로 최신 버전의 펌웨어가 업데이트 요청을 한 경우에는 펌웨어가 검증되고 해당 노드가 최신 피어 리스트에 추가된다. 펌웨어의 완전성(integrity)과 최신 버전의 업데이트 여부를 검증하는 보안적인 장점이 있지만 취약성과 버그의 진단은 포함하지 않는다.

사물인터넷 기기 관리의 보안성에 블록체인을 적용한 방식들은 각 사물인터넷 기기가 주기적으로 블록체인에 트랜잭션을 생성한다는 공통점이 있다. 하지만 블록체인은 한 블록에 저장될 수 있는 트랜잭션 데이터의 양의 제한이 있다. 트랜잭션 처리량을 늘이기 위해 블록을 크게 만들면 블록을 브로드캐스팅하기 때문에 네트워크 트래픽이 증가하며, 스토리지의 블록체인 크기가 증가하는 트레이드 오프(trade off)가 있다. 따라서 사물인터넷 기기가 생성하는 트랜잭션을 효율적으로 수용할 수 있는 연구가 필요하다.

6. 결론 및 향후 전망

본 논문에서는 사물인터넷의 보안을 위해 사용된 블로체인의 응용과 연구를 조사했다. 블록체인은 IoT 기기의 인증, 설정, 센서 데이터 교환의 보안 등을 위해 사용되고 있다. 이는 블록체인이 제공하는 장부의 신뢰성에 의한 보안성, 분산형 방식으로 많은 장비를 수용할 수 있는 확장성, 공개키 인프라로 인한 낮은 서버 유지비용 그리고 생산자와 소비자가 소통하는 양방향 시스템 구성의 장점을 이용한 것이다.

사물인터넷과 관련된 보안 기능을 신속하게 지원하기 위해 트랜잭션 검증 시간의 지연 문제를 해결하는 연구가 필요하다. 또한 IoT 보안 기능을 위해 공격자가 데이터를 위조할 수 없게 하기 위해서는 공격자가 연산 능력의 과반을 소유하는 것을 막아야 한다. 그러므로 블록체인 네트워크의 규모를 유지할 수 있는 연구가 지속적으로 필요하다. 예를 들어, 큰 규모의 채굴 네트워크를 유지하기 위해서는 자원이 한정적인 기기에서 블록체인을 구동할 수 있도록 CPU 자원을 많이 소모하는 작업 증명은 지분 증명(PoS, Proof of Stake)[7]과 같이 낮은 CPU 자원을 소모하는 증명 방법의 적용에 대한 연구도 추가되어야 한다. 마지막으로 블록체인의 트랜잭션 처리량을 늘려서 사물인터넷이 생성하는 데이터를 수용할 수 있는 연구도 필요하다.

7) 계산능력이 아닌 각 노드의 지분 보유량에 따라 합의 결정권이 달라져 작업 증명의 과도한 CPU 소모를 피할 수 있다.

참 고 문 헌

[1] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system”, 2008년.

[2] 이혁준, 이수미. “비트코인의 신뢰구조와 이중지불의 위협” 정보보호학회지. 2016년.

[3] 비트코인 차트, http://www.vnbitcoin.org/bitcoincharts.php

[4] IBM, https://www-935.ibm.com/services /multimedia/GBE03662USEN.pdf

[5] Dorri, Ali, et al. “Blockchain for IoT security and privacy: The case study of a smart home.” Pervasive Computing and Communications Workshops (PerCom Workshops), 2017년.

[6] Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. “Towards an Optimized BlockChain for IoT.” Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. ACM, 2017년.

[7] Wood, Gavin. “Ethereum: A secure decentralised generalised transaction ledger.” Ethereum Project Yellow Paper , 2014년.

[8] Huh, Seyoung, Sangrae Cho, and Soohyung Kim. “Managing IoT devices using blockchain platform.” Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017년.

[9] Ibba, Simona, et al. “CitySense: blockchain-oriented smart cities.” Proceedings of the XP2017 Scientific Workshops. ACM, 2017년.

[10] 한국전력공사, http://home.kepco.co.kr/kepco/KO/C/htmlView/KOCDHP001.do?menuCd=FN05030501

[11] Goldman Sachs, Blockchain Putting Theory into Practice, pp.25-32, the-blockchain.com, 2016년.

[12] 이성훈, 김광조. “블록체인을 이용한 스마트 그리드 시스템의 기기 인증 방안”, 한국통신학회 하계종합학술발표회. 한국통신학회, 2016년.

[13] Samaniego, Mayra, and Ralph Deters. “Using Blockchain to push Software-Defined IoT Components onto Edge Hosts.” Proceedings of the International Conference on Big Data and Advanced Wireless Technologies. ACM, 2016년.

[14] Thomas Hardjono, Ned Smith. ”Cloud-based commissioning of constrained devices using permissioned blockchains.“ IoTPTS '16 Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. ACM, 2016년.

[15] Boohyung Lee, Jong-Hyouk Lee. “Blockchain-based secure firmware update for embedded devices in an Internet of Things environment.” The Journal of Supercomputing. Springer, 2017년.

저 자 약 력

유 소 망

이메일 : somang4819@gmail.com

- 2011년~2015년 동덕여자대학교 문헌정보학과 (학사)
- 2015년~2017년 고려대학교 컴퓨터학과 (석사)
- 관심분야 : 블록체인, 핀테크

김 종 완

이메일 : kimj@syu.ac.kr

- 현재 삼육대학교 교양대학 조교수 (컴퓨터과학전공)
- 관심분야 : 빅데이터, Skyline, IoT응용