블록체인으로 사물 인터넷의 무결성을 보장하는 시스템

A system to ensure the integrity of Internet of things by using Blockchain

김영석
Young-Seok Kim

(22012) 인천광역시 연수구 아카데미로 119 인천대학교 컴퓨터공학부
youngseokaaa@gmail.com

Abstract

사물 인터넷 기기의 개수가 늘어나는 만큼 보안위협 또한 같이 늘어나고 있다. IBM의 'The Dangers of Smart City Hacking'[5]에 따르면 사물 인터넷 기기의 데이터를 조작하는 행위가 일어난다면 심각한 문제를 일으킬 수 있다고 경고한다. 이에 본 논문에서는 사물 인터넷 시스템의 무결성을 보장하기 위해 비트코인과 라이트닝 네트워크를 사용한다. 블록체인 기술은 각각의 사용자가 데이터를 저장할 때 특정 합의 알고리즘을 통해 블록을 생성하는 방식으로 데이터를 사용자들과 공유하고 저장한다. 이는 탈 중앙적인 구조로 누구나 참여하여 데이터를 저장할 수 있지만 악의적인 사용자 또한 참여하여 시스템을 무력화시킬 수 있다. 블록체인에서는 이를 흔히 '51% 공격' 이라고 부른다. 본 논문에서는 정상적인 사용자들에게 51% 공격을 했을 때 무결성이 지켜지는지 확인 하기 위한 실험을 진행하였다. 그 결과 악의적인 사용자가 시스템의 절반 이상의 해시 연산력을 보유할 경우 데이터를 수정해 무결성을 위협할 수 있다는 점을 확인했다. 하지만 국내에서 진행하는 '스마트홈 10만 가구 구축' 프로젝트에 적용했을때 10만 가구 이상의 해시 연산력을 보유하여야 무결성을 위협할 수 있기에 현실적으로 불가능 하다. 그래서 본 논문에서는 사물 인터넷의 무결성을 보장하기 위해 비트코인을 사용한 시스템을 제안한다.

Keywords: 블록체인, 사물 인터넷, 비트코인, 무결성, 51% 공격, 라이트닝 네트워크

1. 서론

2020년에는 2019년보다 21% 늘어난 58억개의 사물 인터넷 기기가 존재하게 될 것이다. 그중 대부분의 사물 인터넷은 가정용으로 제작되며 관련 시장규모가 매년 성장하고 있다.[1] 2022년 까지 국내에서도 스마트홈 10만 가구 구축을 목표로 세부 추진과제를 수행하고 있다.[2]

하지만 사용자가 늘어남에 따라 그만큼 해킹 위협 또한 같이 늘어나고 있다. 예를 들어 2016년 10월 보안이 허술한 사물 인터넷 기기에 악성 코드를 설치하여 서버를 공격한 미라이 봇넷(Mirai botnet) 사건이 있었다. 이를 통해 트위터, 넷플릭스, CNN 을 포함한 다수 웹사이트들의 접속이 차단되는 일이 발생했다.[3] 국내에서는 아파트 공용 서버가 해킹을 당해 현관문 비밀번호가 초기화 되고 전등이 꺼졌다 켜졌다 반복하는 등의 피해가 일어났다.[4] IBM의 'The Dangers of Smart City Hacking'에 따르면 사물 인터넷의 데이터를 조작하는 행위가 일어나게 된다면 심각한 문제를 일으킬 수 있다고 경고한다.[5] 예를 들어 가정에서 날씨가 더운데도 온도가 낮다고 데이터를 조작하여 히터를 계속 작동시키거나 사용하지 않는 가전제품들을 모두 작동시키는 행위 등이 될 수 있다.

많은 기업들은 블록체인이 사물 인터넷의 보안

과 신뢰성을 향상 시킬 수 있는 기술 중 하나로 생각 하고 관련 연구가 계속되고 있다.[6] 이는 블록체인이 가진 특징인 탈 중앙화에 기반 한다. 블록체인의 경우 누구나 참여가 가능하며 다수결을 기반으로 시스템을 유지한다.

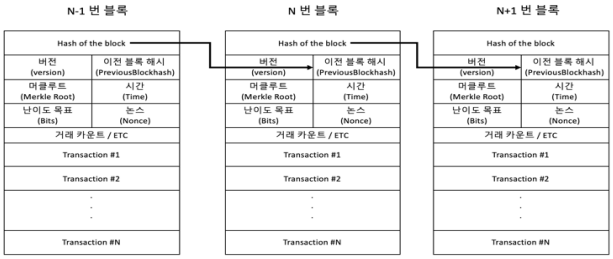
하지만 누구나 참여가 가능 하다는 건 악의적인 사용자도 참여가 가능하다는 걸 의미한다. 만약 악의적인 사용자가 전체 네트워크의 50%를 넘는 해시 연산력을 보유한다면, 정상적인 사용을 원하는 유저들보다 빠르게 위변조된 블록을 만들 수 있다. 그러나 이는 블록체인에 참여하는 사용자가 많아질수록 더욱 어려워진다. 가령 국내에서 진행하는 스마트 홈 10만 가구 구축 프로젝트에 블록체인을 사용하게 된다면 10만 가구 이상의 해시 연산력을 보유하여야 공격이 가능하기에 현실적으로 불가능에 가깝다.

본 논문에서는 사물 인터넷 시스템의 무결성을 보장하기 위해 블록체인 기술을 사용한 비트코인을 사용하였다. 비트코인의 경우 개발단계부터 탈 중앙화에 초점을 맞춰서 개발된 시스템이다.[7] 또한 사물 인터넷의 특성상 실시간으로 통신하여 데이터를 주고 받아야 하기 때문에 비트코인의 '라이트닝 네트워크' 를 사용하였다.

2. 관련 연구

2.1. 블록체인(Blockchain)

블록체인[7]은 2009년 사토시 나가모토가 발표한 'Bitcoin: A Peer-to-Peer Electronic Cash System' 논문을 통해 비트코인 이라는 가상 화폐를 만들면서 사람들에게 알려졌다. 비트코인의 핵심기술인 블록체인은 신뢰받는 제3자 개입없이 거래 기록의 무결성을 보장해주며, 이를 통해 개인과 개인의 거래를 가능하게 해준다.



(그림 1) 블록체인 아키텍처

블록체인의 구조는 (그림 1)과 같다. 먼저 서버에 블록의 해시값을 저장한다. 이때 해시값은 블록에 들어있는 값들과 이전 해시값을 합쳐서 만든다. 이를 통해 이전 값들을 수정하게 될 경우 그 블록의 해시값 부터 이후의 해시값들 까지 모두 바뀌게 된다. 따라서 내가 가지고 있는 블록이 수정이 된 경우 다른 사람들이 가지고 있는 블록과 해시값이 다르기에 어디부터 수정이 됐는지 확인이 가능하다.

2.2. 라이트닝 네트워크(Lightning Network)

라이트닝 네트워크[8]란 비트코인의 느린 속도를 해결하기 위해 개발한 프로토콜이다. 이는 기존의 비트코인이 평균 10분에 한번씩 블록을 생성하여 거래를 저장했던 방식과는 다르게 사용자 간의 개별 채널을 구성 후 채널 안에서 거래를 진행한다. 그 후 결과만 블록체인에 기록하는 방식이다. 이 기술을 통해 기존의 비트코인에서 거래 마다 수수료를 지불하던 방식에서 모든 거래가 종료된 후 라이트닝 네트워크로 채널을 닫을 때 거래의 최종 결과만 블록체인에 기록하게 되어 수수료의 절감 효과도 생기게 되었다.

2.3. 사물 인터넷(Internet of Things)

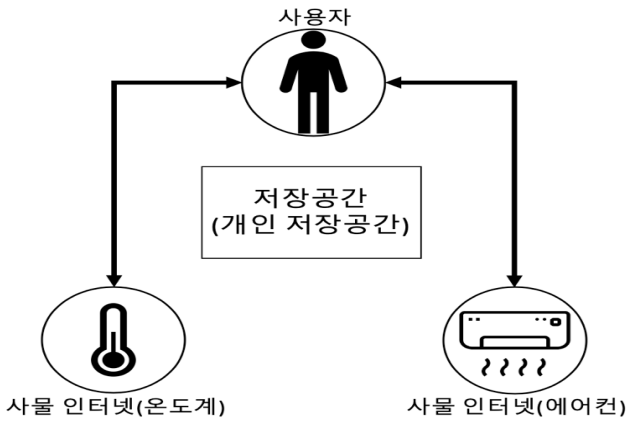
사물 인터넷의 개념은 정의를 내리는 사람에 따라 다양하게 표현된다.[9] 그래서 이러한 정의들을 종합 했을때 사물 인터넷은 모든 사물과 사람들이 인터넷으로 연결되어 서로 정보를 주고받는 것을 의미한다. 최근 사물인터넷은 스마트 홈, 스마트 빌딩, 스마트 시티, 스마트 팩토리등 다양한 분야에 접목되어 분야를 넓혀가고 있다.[10] 하지만 서론에서 제시했듯이 사용자가 많아지고 생활에 더 가까워 지면서 해킹 위험 또한 같이 늘어나고 있다.

이에 따라 국내외의 사물 인터넷 보안 관련 기관들은 다양한 사물 인터넷 보안 표준을 개발하고 있다.[11]

2.4. 무결성(Integrity)

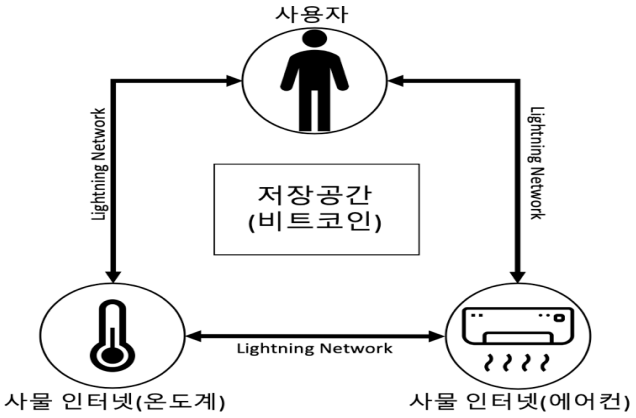
무결성 이란 정보보안의 세 가지 원칙 중 하나이며, 정보를 원치 않는 변경으로 부터 보호하는 것을 의미한다. 사물 인터넷 환경에서도 보안 위협과 취약점을 개선하기 위해 정보 보안의 세 가지 원칙을 기준으로 관련 연구가 진행되고 있다.[12] 본 논문에서는 사물 인터넷의 무결성을 보장하기 위해 비트코인을 사용한 시스템을 제안한다.

3. 제안 시스템



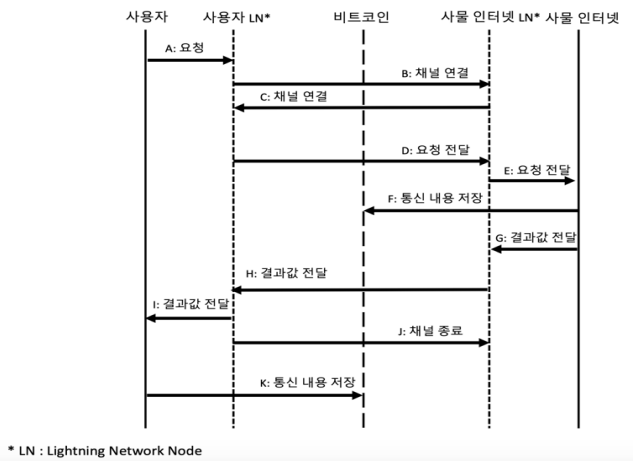
(그림 3) 기존의 사물 인터넷 시스템

(그림 3)은 기존의 사물 인터넷 시스템을 보여준다. 이는 서론에서 제시 했듯이 사물 인터넷 내의 저장된 데이터를 조작하게 되면 치명적인 문제가 발생한다. 본 논문에서는 비트코인과 라이트닝 네트워크를 사용하여 무결성을 보장하는 사물 인터넷 시스템을 제안한다. 비트코인은 한번 기록된 데이터는 수정이 어려운 특징이 있어 사물 인터넷의 무결성을 보장할 수 있다. 라이트닝 네트워크를 사용하면 비트코인의 단점 이 느린 속도와 비싼 수수료를 해결할 수 있다. 이를 통해 실시간으로 사물 인터넷과 통신이 가능하다. 하지만 비트코인도 완벽히 해킹의 위험에서 벗어나지는 못했다. 이를 '51% 공격'이라 부르는데 이는 4장의 실험에서 서술한다.



(그림 4) 비트코인과 라이트닝 네트워크를 사용한 사물 인터넷

(그림 4)는 본 논문에서 제시하는 비트코인과 라이트닝 네트워크를 사용한 사물 인터넷 시스템이다. 사용자와 사물 인터넷 간의 통신에는 라이트닝 네트워크가 사용되고 통신 내용은 저장 공간인 비트코인에 저장되어 다른 사용자와 공유된다. 이에 대한 과정은 (그림 5)를 통해 볼 수 있다.



(그림 5) 비트코인을 적용한 사물 인터넷 통신 시퀀스 다이어 그램

(그림 5)는 비트코인을 적용한 사물 인터넷의 통신 시퀀스 다이어 그램이다.

단계 A: 사용자가 사물 인터넷을 조작하기 위해 라이트닝 네트워크를 통해 명령을 요청한다.

단계 B, C: 사용자의 라이트닝 네트워크와 사물 인터넷의 라이트닝 네트워크가 통신을 위해 서로

채널을 연결한다.

단계 D, E: 사용자와 사물 인터넷 간의 채널이 연결되어 사용자의 명령을 전송하고 실행한다.

단계 F: 사물 인터넷은 사용자에게 요청 받은 통신 내용을 비트코인에 저장한다.

단계 G, H, I: 사물 인터넷이 사용자에게 결과값을 전달한다.

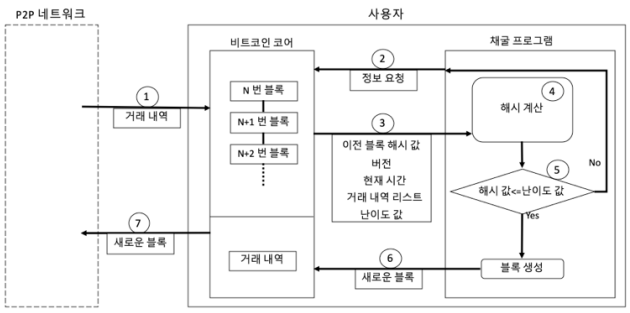
단계 J: 사용자가 결과값을 받고 채널을 종료한다.

단계 K: 사용자는 사물 인터넷 에게 받은 통신 내용을 비트코인에 저장한다.

4. 실험 및 결과

블록체인 기술의 핵심적인 가치는 탈 중앙화 시스템이다. 이는 누구나 참여가 가능하며 의사결정 또한 과반수 이상의 합의가 필요하다. 하지만 어느 집단이나 개인이 시스템 안에서 과반수 이상의 힘을 가지게 된다면 어떻게 될까? 비트코인에서는 이를 '51% 공격'이라 한다. 본 실험에서는 51% 공격을 구현하여 정상적인 사용자들의 거래를 공격했을 때 변화를 확인한다.

4.1. 51% 공격(>50% 공격, 과반수 공격) 실험



(그림 6) 비트코인 블록 생성 과정

(그림 6)은 비트코인의 블록 생성 과정을 순서대로 보여준다.

①: 사용자들간의 거래가 발생하면 거래 내역은 P2P네트워크를 통해 전체 사용자에게 전달된다. 사용자는 전달 받은 거래 내역을 비트코인 코어에 저장한다.

②: 채굴 프로그램은 블록 생성에 필요한 정보(이전 블록 해시값, 버전, 현재 시간, 거래 내역 리스트, 난이도 값)를 비트코인 코어에 요청한다.

③: 비트코인 코어는 채굴 프로그램에 요청 받은 정보를 전달한다.

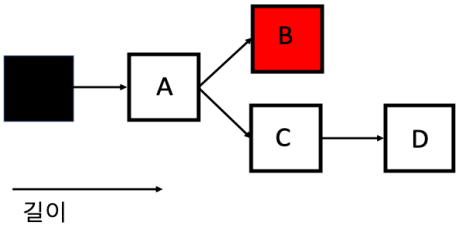
④: 받은 정보와 임의의 값을 더하고 해시 함수를 이용해 해시값을 구한다.

⑤: 난이도 값과 해시값을 비교하여 해시값이 난이도 값보다 크다면 과정 ②부터 다시 실행한다. 해시값이 난이도 값보다 작을 경우 블록을 생성한다.

⑥: 생성한 블록은 비트코인 코어에 전달한다.

⑦: 비트코인 코어에서 전달 받은 새로운 블록을 P2P 네트워크를 통해 다른 사용자들에게 전달한다. 사용자들은 전달 받은 블록을 자신의 블록에 추가하게 된다.

본 논문에서 악의적인 사용자는 (그림 6)의 비트코인 블록 생성 과정 중 ②의 과정을 조작한다. 이를 통해 악의적인 사용자는 거래 내역을 포함하지 않는 블록을 만들어 정상적인 사용자들에게 정상적인 블록이라 판단하게 하고 동기화 하는 것을 목표로 한다. 이는 비트코인에서 가장 긴 블록을 정상적인 블록이라 판단하기 때문이다.



(그림 7) 블록 구조도

악의적인 사용자는 (그림 7)의 블록 A가 생성된 후 진행된 거래를 조작하기로 한다. 그래서 블록A가 생성된 후 악의적인 사용자는 정상적인 사용자들과 연결을 끊는다. 정상적인 사용자들과 연결을 끊었기에 정상적인 사용자들이 'A-C-D'

순서로 블록을 만들어 전파할 때 악의적인 사용자는 동기화를 하지 않는다. 악의적인 사용자는 조작된 블록을 만들어 정상적인 사용자들보다 블록의 길이가 길어지면 정상적인 사용자들과 연결을 한다. 정상적인 사용자들은 악의적인 사용자의 블록이 더 길기에 정상적인 블록이라 판단하고 동기화를 진행한다.

공격의 진행 순서는 다음과 같다.

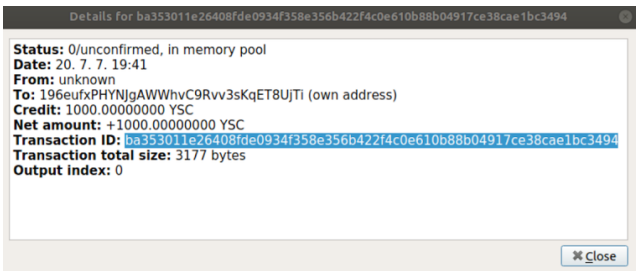
ㄱ. 정상적인 사용자들은 [사용자A가 사용자B에게 1000코인을 준다] 라는 거래를 진행하고 해당 거래가 포함된 블록을 만든다.

ㄴ. 악의적인 사용자는 정상적인 사용자들이 블록을 만들고 있을 때 연결을 끊고 거래 내역을 포함하지 않는 블록을 만든다.

ㄷ. 악의적인 사용자의 블록이 정상적인 사용자들의 블록보다 많아지게 되면 정상적인 사용자들과 연결한다.

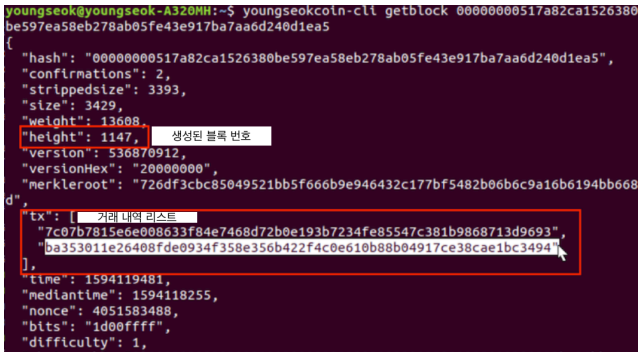
4.2. 실험 결과

정상적인 사용자와 악의적인 사용자는 1146번 블록부터 연결을 끊었다. [사용자A가 사용자B에게 1000 코인을 준다] 라는 거래는 1147번 블록에 들어가 생성 되었다. (그림 8)은 해당 거래가 기록된 트랜잭션이다. 여기서 'Transaction ID'는 해당 트랜잭션이 다른 트랜잭션과 구별될 수 있도록 부여된 아이디를 말한다.

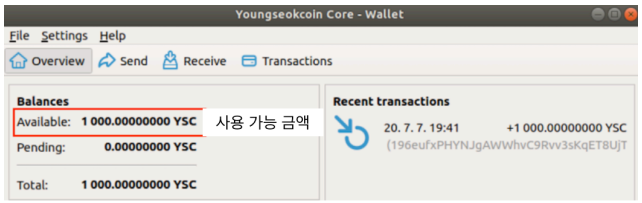


(그림 8) 거래 트랜잭션

(그림 9)는 생성된 블록 번호와 저장된 트랜잭션을 빨간색 테두리로 표시하였다. (그림 10)은 블록이 생성된 후 사용가능 금액에 1000 코인이 표시된 사진이다.



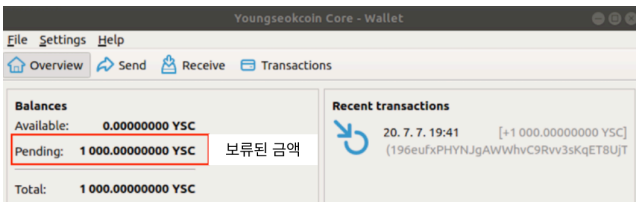
(그림 9) 정상적인 사용자들이 만든 1147 번 블록



(그림 10) 정상적인 사용자의 잔액

악의적인 사용자는 정상적인 사용자들보다 블록을 많이 만든 뒤 정상적인 사용자들과 연결하였다. 그러자 정상적인 사용자들의 블록이 악의적인 사용자의 블록으로 대체 되었고 거래 내역이 블록에서 사라지게 되었다. (그림 11)에서 1147번 블록으로 대체되어 기존의 거래가 사라진 모습을 확인할 수 있다. (그림 12)는 기존의 사용가능에 있던 1000코인이 보류된 금액으로 전환된 것을 확인할 수 있다.

(그림 11) 악의적인 사용자의 1147번 블록으로 변경



(그림 12) 변경된 잔액

5. 결론

본 논문에서는 사물 인터넷의 무결성을 보장하기 위해 비트코인을 사용하였다. 기존의 사물 인터넷 시스템은 저장된 데이터를 악의적으로 조작 할 수 있었다. 하지만 블록체인 기반의 비트코인을 사용한다면 저장된 데이터의 악의적인 조작이 어려워 지기에 시스템의 무결성을 지킬 수 있다. 물론 실험에서 확인했듯이 전체 시스템의 과반수 이상의 해시 연산력을 보유한다면 데이터를 악의적으로 수정할 수 있다. 그러나 국내에서 진행하는 '스마트홈 10만 가구 구축' 프로젝트에 블록체인 기술을 적용한다면 적어도 10만 가구에 해당하는 해시 연산력을 보유하여야 하기에 현실적으로 어렵다. 따라서 본 논문에서는 비트코인을 사용해 사물 인터넷의 무결성을 보장하는 시스템을 제안한다.

Github 주소 : https://github.com/teamnova-ailab/A_system_to_ensure_the_integrity_of_Internet_of_things_by_using_Blockchain

References

[1] Laurence Goasduff "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020" Gartner, 2019

[2] 김경훈, "스마트홈 서비스 플랫폼", NICE 평가정보, 2019.9

[3] Maria Korolov "What is a botnet? When armies of infected IoT devices attack" csoonline, 2019

[4] 이동인, 오대석, "구멍 뚫린 스마트홈.. 현관문이 저절로 열려", 매일경제, 2019.7

[5] "The Dangers of Smart City Hacking", IBM, 2018.8

[6] Katie Costello "Gartner Survey Reveals Blockchain Adoption Combined With IoT Adoption Is Booming in the U.S." Gartner, 2019

[7] Satoshi Nakamoto, "Bitcoin:A Peer-to-Peer Electronic Cash System", 2008, pp.1-9

[8] Joseph Poon, Thaddeus Dryja "The Bitcoin Lightning Network", 2016

[9] 이학준, "사물인터넷 기반의 스마트홈", 한국통신학회지, 2015.3, pp.44-49

[10] 권영환, "사물인터넷 (IoT, Internet of Things)의 특징과 고려사항", 소프트웨어정책연구소, 2018.2

[11] 김영갑, 황인태, "사물인터넷 보안 표준화 동향", 한국통신학회지, 2017.2, pp.90-100

[12] 정용식, 차재상, "IoT 디바이스 보안 점검 기준", 한국통신학회지, 2017.1, pp.27-33