Journal of Digital Convergence
Vol. 17. No. 1, pp. 195-201, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.1.195

와이코인 : 블록체인 기술을 이용한 무선랜 공유

김우성[1], 류경호[2], 박양재[1*]
[1]가천대학교 컴퓨터공학과 교수
[2]가천대학교 컴퓨터공학과 학사과정

WiCoin : Wireless LAN Sharing Using Block Chain Technology

Woo-Seong Kim[1], Kyoung-Ho Ryu[2], Yang-Jae Park[1*]
[1]Dept. of Computer engineering, Gachon University professor
[2]Dept. of Computer engineering, Gachon University undergraduate course

요 약 본 논문은 무선랜 공유를 위한 블록체인 시스템 적용 방안을 제안한다. 무선랜은 비인가 대역에서 동작하는 무료 무선 액세스 기술로 현재 폭발적으로 증가하는 무선랜 장치들로 인해 상호 간섭이 가중되고 있다. 또한 무선랜 액세스 장치가 공유되지 않아 개인이나 단체가 무분별하게 무선랜 설치를 하고 있는 것이 큰 문제이다. 최근 블록체인 기술은 이러한 상호 비협력적 시장에서 암호 화폐를 통해 효율적인 협력을 이끌어 낼 수 있음을 보여 주었다. 본 논문에서는 개별 인증 기반의 무선랜 접속 방식에서 블록체인 암호 화폐에 기반한 접속 방식을 제안한다. 제안한 시스템에서는 스마트 컨트랙트를 이용하여 웹에서의 사용자 접근이 용이하게 하였으며, 실시간 무선랜 접속을 위해 기존 작업 증명 대신 권한 증명을 구현하였다.

주제어 : 블록체인, 무선랜, 암호화폐, 스마트 컨트랙트, 권한증명

Abstract This paper proposes a blockchain system to share Wireless Local Area Network (WLAN) that recently suffers from mutual interference among increasing devices using unlicensed bands. Blockchain technology can induce cooperation from users by incentivizing them with cryptocurrency like shown in Bitcoin example. In this paper, we describe Blockchain based access mechanism in WLAN instead of conventional authentication based access. Here, users can access any WLAN access point by paying through smart contract while they also receive payment from others. In order to support real-time transaction, we apply proof-of-authority that is realized by Byzantine fault tolerant protocol instead of well-known proof-of-work that requires huge computing power and delay.

Key Words : Blockchain, WLAN, Cryptocurrency, Smart contract, Proof-of-Authority

1. 서론

최근 스마트 폰 급증에 따라 독립적인 무선 핫스팟을 원하는 개인이나 기업들이 무선 랜 설치에 앞장서고 있다. 비면허 대역의 특징으로 누구나 손쉽게 무선랜 AP를 설치 사용할 수 있어, 현재 과도하게 설치된 무선랜 액세스 포인트 (Access point, 이후 줄여 AP) 는 상호간 잦은 간섭에 유발하여 성능 저하를 발생시키고 있다. 그럼에도 불구하고 인터넷 서비스 제공자나 이동통신 사업자들이 면허대역의 셀룰러 네트워크의 부하를 줄이고자 무선

*This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (No. NRF-2017R1C1B1006607)
*Corresponding Author : Yang-Jae Park(parkyj@gachon.ac.kr)
Received October 23, 2018 Revised December 7, 2018
Accepted January 20, 2019 Published January 28, 2019

랜 AP 수를 기하급수적으로 늘리고 있다. 개인이나 기업들이 설치한 무선랜을 공유하는 데에는 분명한 한계가 있다. 보통의 경우, 개인이 무선랜을 공개하면 네트워크 자원을 공유하게 되어 상대적으로 본인의 서비스 품질이 저하되며 그렇다고 타인의 무선 랜을 사용할 수 있다는 보장도 없다. 이는 Non-cooperativie game[1]으로 간주할 수 있으며, Nash equilibrium은 각자 무선랜을 공개하지 않는 것이다.

최근 비트 코인[2]을 통해 검증된 블록체인 기술이 미래 4차 산업 혁명의 주요 기술로 대두됨에 따라 다양한 분야에서 연구가 이루어지고 있다. 해당 기술은 네트워크로 연결된 분산 컴퓨터들을 이용하여 변경이 불가역적인 많은 연산량을 요구하는 체인형태의 자료구조를 생성 유지한다. 이를 이용하여 사용자간 전자화폐 거래 정보를 저장, 검색하고, 이 과정이 공공에 공개되어 투명성을 유지함으로써 임의의 정보 왜곡 및 훼손을 막을 수 있다. 상기 분산 컴퓨팅에 참여하는 컴퓨터들은 자발적으로 블록 노드의 생성과 유지, 관리 역할을 수행하는 대신, 이에 상응하는 인센티브로 대가를 받을 수 있다.

본 논문에서는 상기 블록체인 및 전자화폐 기술을 이용하여 무선랜 공유를 통해 비면허 대역 사용 효율성을 높이는 방안에 대해 제안한다.

2. 관련연구

2.1 블록체인 기술 개요

블록체인[3]은 정보를 블록에 저장하여 기존 블록에 연속적으로 연결하여 체인 형태를 구성하는 자료구조이다. 블록체인은 하나의 컴퓨터에서 동작하는 데이터베이스와 같은 자료 저장 구조가 아닌, 노드 대 노드(Peer-to-peer 혹은 P2P) 네트워크 시스템을 이용한 분산형 자료구조이다. 하지만 기존 분산형 데이터 저장 시스템의 경우, 효율성을 위해 중복 저장을 회피하는 반면 블록체인은 보안성을 위해 모든 노드들이 동일한 데이터 블록을 저장하는 것이 차이점이다.

블록체인의 보안에 있어 강점은 체인으로 연결된 블록의 일부를 임의로 변경, 훼손이 어렵다는 것이다. 가령 특정 블록의 내용을 변경하기 위해서는 해당 블록 뒤에 연결되는 블록의 내용을 바꿔야하며, 이로 인해 그 다음 블록도 연쇄적으로 변경되어야 한다. 그리고 블록체인에서는 가장 긴 체인을 항상 선택하고, 상대적으로 짧은 분화된 (forking) 체인은 버려지기 때문에 결국 긴 체인의 블록들의 내용을 바꿔야만 한다. 하지만 블록생성 주기가 짧아 블록이 생성되어 체인에 붙기 전에 이전 블록들을 모두 수정하는 것은 불가능에 가깝다.

이러한 블록체인을 관리하기 위해 비트 코인에서는 분산형 시스템을 구성하는 다 수의 컴퓨터 노드에서 작업 증명 (Proof of work)[4]을 통해 하나의 노드만이 블록을 생성하는 컨센서스를 제안하였다. 상기 작업 증명은 블록에 기록하는 정보들과 키를 통해 해쉬하는데 지정된 길이의 해쉬값을 얻는데 필요한 난수를 찾는 것이다. 이는 무작위적인 방식의 난수 발굴에 필요한 특정 컴퓨팅 노드 파워가 상기 분산 시스템을 구성하는 전체 노드의 컴퓨팅 파워의 과반을 넘기 어렵다는 가정을 통해 보안성을 유지할 수 있다.

최근 상기 블록체인 기술을 네트워크 영역에 적용하고자 하는 움직임이 있다. 블록체인을 이용하여 이동 통신 사업자간 가입자 정보를 공유하거나, 가상 망 임대 사업에 이용하고자 하는 기술에 대해 표준 단체에서 논의 중이다. 이를 위한 네트워크 슬라이싱과 제어를 위해 소프트웨어 정의 네트워크 (Software defined networking)[5] 기술에 기반한 네트워크 운영이 필요하다.

2.2 블록체인 구조 및 성능

현재 블록체인 기술을 사용한 비트코인은 블록생성 시간이 약 10분, 이더리움은 약 15초이며, 블록 당 트랜잭션 수도 제한적이다. 최근 다양한 애플리케이션을 위해 높은 초당 트랙잭션 처리 수(Transaction Per Second, TPS)를 요구하는 시스템이 늘어나고 있다[6].

블록체인은 접근성에 따라 크게 퍼블릭 블록체인(Public Blockchain)[7]과 프라이빗 블록체인(Private Blockchain)[8]으로 구분된다. 상기 비토코인과 이더리움이 퍼블릭 블록체인을 사용하며, 퍼블릭 블록체인은 네트워크에 별다른 제한 없이 노드로 들어올 수 있고 내부 트랜잭션을 모든 노드가 공유하고 공증한다. 최근 비트코인은 약 11000개,이더리움은 약 23000개의 노드가 생성되어 상기 절차로 인한 블록생성 시간은 늘어나고 있다. 성능 개선을 위해 블록 생성률을 늘리는 경우, 엉클블록이 늘어난다. 엉클블록이란 동시에 블록이 생성되었을 때 유효성은 검증되었더라도 메인 체인에 연결되지 못한 블록을 의미한다. 이러한 엉클 블록이 많이 생성하

게 되면 네트워크의 보안이 낮아진다. 폐쇄형 블록체인으로도 불리는 프라이빗 블록체인은 네트워크 상에서 만든 인증방식을 통하여 검증된 계정만이 참가할 수 있다. 그리고 본 논문은 프라이빗 블록체인노드들의 합의 알고리즘을 상기 작업증명이 아닌 권한증명(Proof of Authority)[9]으로 한다. 난수를 찾아 합의하는 작업증명과 달리 권한 증명은 신분을 기반으로 한(identity as a stake)합의 매커니즘이다. 블록을 생성하는 노드를 풀 노드(full node)라고 하는데, 풀 노드 중에서 블록생성 권한을 가진 리더는 차례대로 위임받는다. 하지만 만일 악의적이라고 판단되면 다른 풀 노드들이 투표를 진행하고 추방한다. 이렇게 제한된 풀 노드 수로 인해 권한증명을 기반으로 한 프라이빗 블록체인은 퍼블릭 블록체인에 비해 트랜잭션처리 속도가 빠르다. 이는 본 논문이 제안하는 무선랜 공유가 실시간으로 처리되어야하는 문제점을 해결할 수 있다.

3. 블록체인을 이용한 무선랜 인증

3.1 블록체인 기반 무선랜 구조

본 논문이 제안하는 블록체인을 이용한 무선랜 인증에 대해, Fig. 1은 블록체인과 무선랜 네트워크 구조를 보여준다. 무선랜 AP 혹은 NAS (Network Access Server)는 단말의 인터넷 접속을 제어하기 위해 블록체인 시스템과 연동을 통해 단말 인증을 수행한다. 그림에서 BAS (Block-chain based authentication server) 는 블록체인 기반 인증 서버이다. BAS는 블록체인을 유지 관리하는 컴퓨팅 노드로 블록체인의 블록은 마이닝 하는 기능을 포함할 수도 있고 그렇지 않을 수도 있다. 마이닝을 하지 않는 경우, 라이트 노드(light node)로 블록 내용인 트랜잭션을 탐색하거나 계정 정보를 열람하는 기능만 가질 수 있다. 또한 BAS은 AP/NAS 사이에 무선랜 인증을 위한 인터페이스를 가지고 있으며 인증 절차에 필요한 메시지를 처리하고 가입자 정보를 관리하는 기능을 한다. 또한 블록체인 플랫폼 관리를 위한 기능, 관리자 인터페이스 등을 포함하고 있다. 상기 시스템에서 단말(MS)는 라이트 노드로 블록체인의 내용을 열람하거나 본인의 계정에서 특정 계정으로 코인을 전송하는 트랜잭션 요청을 수행할 수 있고 사용자 편의를 위해 상기 기능에 대한 웹 기반의 인터페이스를 가지고 있다.

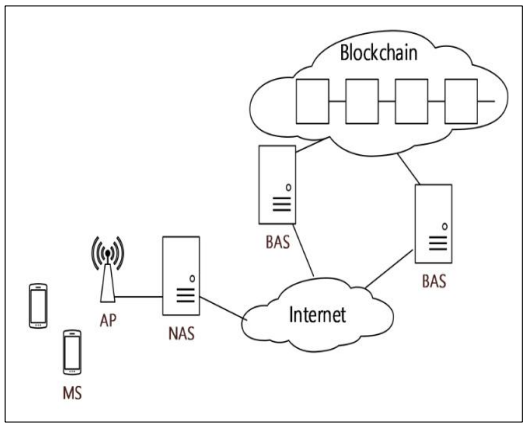

Fig. 1. WLAN authentication with block-chain

블록체인을 이용한 무선랜 접근 제어를 위해 상기 단말들은 각 각 고유의 계정을 가지고 있으며, 해당 계정은 사용자가 블록체인 시스템 가입을 통해 발급 받을 수 있다. 상기 블록체인 시스템은 본 서비스를 제공하는 업체 혹은 기관에 의해 유지 관리 될 수 있다. 동일하게 무선랜 접속을 허용하고자 하는 AP의 경우도 블록체인 계정을 생성 지정해야 한다. 이는 무선랜 AP를 공개하고자하는 사용자가 본인의 AP를 BAS에 등록할 때, AP/NAS는 BAS에 계정 생성 요청을 하게 되고, BAS는 해당 AP의 ID (AP의 MAC 주소 혹은 이에 상응하는 ID) 에 대한 계정을 생성하고 결과를 NAS에 통보한다. 이 때, AP에 대한 개인키 (private key)는 사용자의 공개키 (public key)를 이용하여 암호화해서 보낸다. 이러한 절차 이후에 BAS는 하위 등록된 AP에 대한 블록체인 계정 정보를 아래의 Table 1과 같이 생성 관리한다. 각 계정 정보는 임의 생성된 개인키와 이에 상응하는 공개키 쌍으로 관리 되며, 공개키는 블록체인의 계정 정보로 사용된다.

Table 1. AP account information at BAS

AP ID (MAC address)	Account Number	Private Key
9A:37:98:7B:8F:01	1F1tAaz5x1HUXrCNLbtMDqcw6o5G	EIH736llbgu2
B7:DC:87:3E:88:AC	KLJAL82938HFG97AHNJVhkh688fhg	87yahhh2hg6
2D:76:0A:17:B3:25	l87af26H8u7jglagG765lsBAaf6Oi26Zh	LFyt39l3rnkar

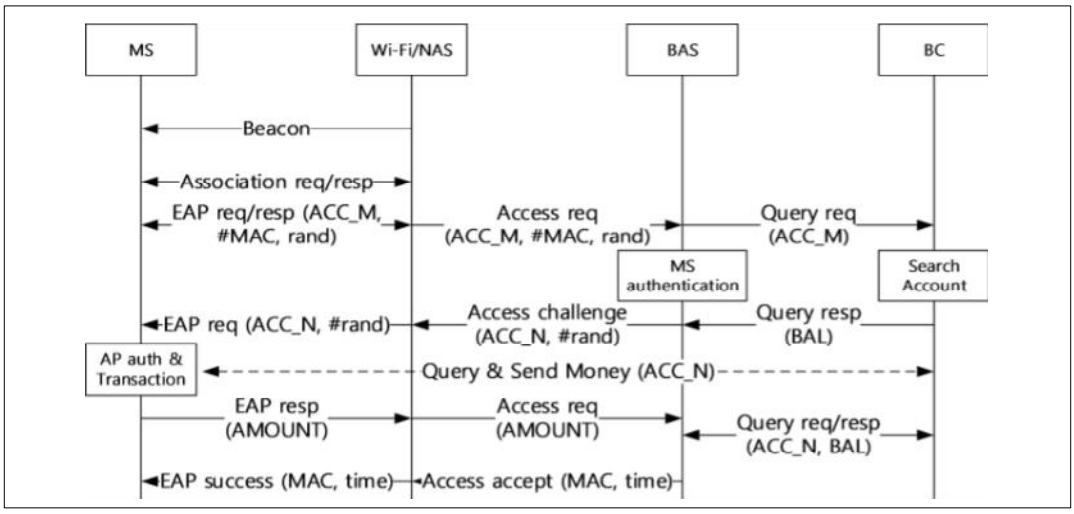

Fig. 2. WLAN authentication procedure with block-chain

3.2 블록체인 기반 무선랜 인증 절차

Fig. 2는 블록체인 기반 무선랜 네트워크에서의 인증 및 네트워크 접속 절차를 나타낸 메시지 흐름도 이다. 우선 단말 인증 방식에 대해 AP로부터 beacon 메시지를 주기적으로 전달 받는다. 가령, IEEE 802.11 메시지[10]에서 authentication request/response를 통해 authentication algorithm = BC (Fig. 1 참고) 과 같은 새로운 인증 방식을 정의할 수 있다. 단말이 무선랜 AP에 association 된 이후에, NAS는 AP를 통해 단말에 ID를 요청할 수 있다. 이에 단말은 본인의 계정 정보 (ACC_M)와 본인의 MAC 주소를 개인키로 암호화한 값과 상호 인증에 사용할 random 값을 nounce로 EAP 메시지[11]에 포함 시켜 AP/NAS에 응답한다. 해당 메시지는 NAS에서 등록된 BAS로 전송한다. Fig. 2에서는 기존 AAA에서 사용하는 RADIUS 프로토콜[12]을 사용하거나 또는 일반적인 HTTP와 범용적인 프로토콜을 이용할 수 있다. BAS에서 Access request 를 수신하였을 경우, 암호화된 #MAC을 ACC_M을 사용해 복호화하여 단말의 MAC 주소를 확인하고, 계좌 정보인 ACC_M을 BC(Block Chain)에서 탐색하여 현재 잔고를 확인한다. 상기 MAC 주소가 주소 형태를 가지지 않거나 계좌 정보가 조회 되지 않는 경우, Access reject을 보내어 단말 접근을 제한하고 그렇지 않은 경우 단말로부터 수신한 random 값을 이를 개인키로 암호화한 #rand 값을 가지고 Access challenge 절차를 수행한다. 이때 AP에 해당하는 계정정보인 ACC_N 값을 포함하여 무선랜 AP을 통해 단말에 전송한다. 이 때, AP의 MAC 주소 (즉 SSID)가 EAP를 포함하는 프레임에 포함되어 있는지 확인하여, ACC_N이 현재 연결 중인 AP에 해당하는지 확인한다. 단말은 상기 ACC_N 를 가지고 #rand를 복호화하여 이전에 송신한 rand 값과 동일 여부를 확인하여 AP의 계정을 인증한다. 단말이 상기 계정 인증 절차가 완료되면 특정 금액을 송금하기 위한 트랜잭션을 BC에 요구한다. 상기 트랜잭션 처리 후, EAP 응답으로 송금한 내역을 BAS에 전달한다. BAS는 해당 트랜잭션이 잘 처리되었는지 BC에 확인한 후, access accept 메시지에 단말 MAC 주소와 유효 시간을 포함하여 보낸다. 이후 AP는 해당 시간동안 단말 MAC에 대한 트래픽을 인터넷으로 통과시키고, 이후에는 해당 트래픽을 차단한다.

4. 구현

4.1 iptables을 통한 AP 접근 관리

구현을 위해 컴퓨터를 AP로 만들고 BAS에 등록하였다. AP를 만들기 위해 운영체제는 리눅스14.0.4 이상을 요구한다. 그리고 AP접근 및 제어를 위해 iptables[13]를 쉘 프로그래밍 하였다. iptables는 시스템 관리자가 리눅스 커널 방화벽이 제공하는 테이블들과 그것을 저장하는 체인, 규칙들을 구성할 수 있게 해주는 사용자 공간 응용 프로그램이다. 체인에 규칙을 생성하고 테이블에 저장한 후 패킷을 필터링하면 해당 테이블을 통해 네트워크 자

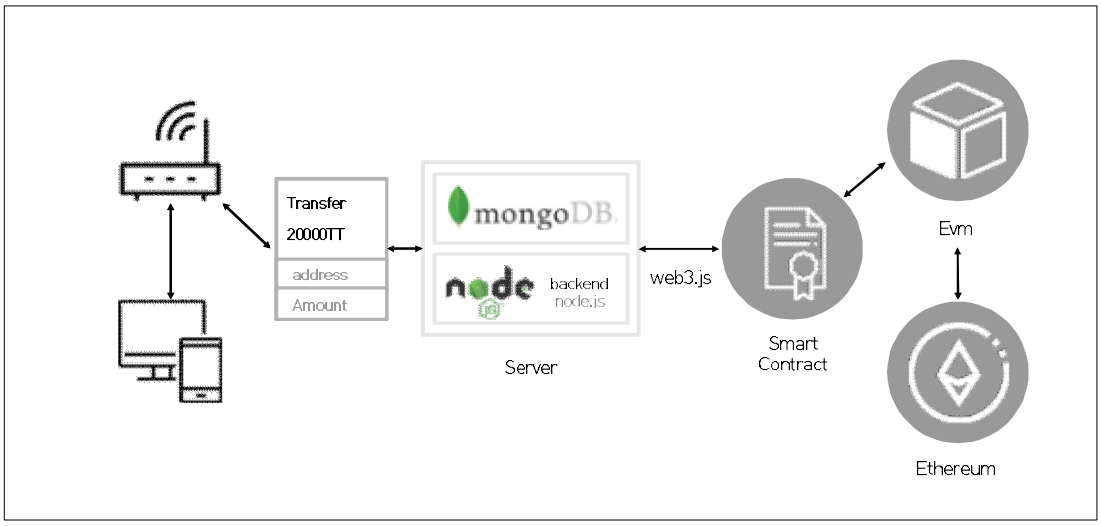

Fig. 3. System Configuration

원이 악용되는 것을 방지할 수 있는 라우팅 및 전송 정책을 만들 수 있다. iptables의 체인은 크게 INPUT체인, OUTPUT체인 그리고 FORWARD체인으로 나뉜다. 라우터로 사용되는 호스트 컴퓨터를 통과하는 패킷의 필터를 FORWARD체인에서 작업하였다. 먼저 “iptables -A FORWARD -s 192.168.10.12 -p tcp -dport 80 -j DROP” 와 같은 규칙을 추가하여, 해당 IP(192.168.10.12)에서 들어오는 패킷 중 tcp프로토콜의 80(www:웹서버 포트)번 포트를 목적지로 하는 패킷을 버린다. 상기 규칙은 모든 IP address에 적용한다. 그리고 사용자가 AP를 구매 할 수 위해 특정 포트(3030)는 열어 BAS에 접근가능하게 한다. 구매가 완료되면 해당 사용자 IP address만 상기 규칙을 ACCEPT으로 변경한다.

4.2 시스템 구성도

본 논문의 시스템 구성도는 Fig. 3와 같다. 사용자가 BAS에 등록된 AP 연결 요청 시 서버에 접속하여 거래하는 웹페이지를 보여준다. 여기서 웹서버는 node.js로 개발하고 서버 자체 데이터베이스는 NoSQL인 몽고DB(MongoDB)를 이용한다. 블록체인뿐만 아니라 서버 내에도 데이터베이스를 두는 이유는 블록체인에 데이터를 저장하기 위해서는 일종의 수수료인 Gas가 소요되기 때문이다. 그래서 회원정보, 게시판 목록 등 무선랜 인증에 필요하지 않은 기본적인 데이터는 서버 데이터베이스에 저장한다. 그리고 Web3.js는 Blockchain server - Client 간의 소통을 위해 고안된 모듈이며, 서버 언어 node.js에 최적화 되어있다. 웹과 유사하게 JSON 형식으로 통신을 하고, 고유의 RPC 통신을 이용하여 Client의 Request와 Respond를 관리한다. 블록체인 어플리케이션에서 사용되는 주요 모듈이며, 보안성 또한 뛰어나 web3.js를 이용하였다.

그리고 스마트 컨트랙트(Smart Contract)[14]란 블록체인을 기반으로 금융거래, 공증 등 다양한 계약을 체결하고 이행하는 것을 말한다. 따라서 무선랜 거래에 대하여 공증하기 위해 BAS의 스마트 컨트랙트는 무선랜 인증에 필요한 정보를 저장한다. 스마트 컨트랙트는 솔리디티(Solidity)로 개발하였고 솔리디티는 EVM(Ethereum Virtual Machine)에서 작동 가능한 바이트 코드로 컴파일 된다. 그리고 FrontEnd는 node.js의 뷰 템플릿엔진인 ejs를 이용하여 반응형 웹으로 개발하였다.

4.3 스마트 컨트랙트를 통한 무선랜 관리

서버에서 발생한 트랜잭션을 블록체인에 저장하기 위해 블록체인 네트워크 IP address와 포트를 연동시켰다. 여기서 트랜잭션이란 무선랜 관리를 위해 데이터를 스마트 컨트랙트에 저장시키는 것을 말한다. 그래서 스마트 컨트랙트에 접근하기 위해 스마트 컨트랙트를 블록체인 네트워크에 배포하고 해당 address 값을 받아 서버에 저장했다. 결국 트랜잭션은 스마트 컨트랙트 address값으로 접근하여 블록체인에 저장된다.

```
    // AP Struct
struct AP{
    address account; // Account Information
    bool state;      // AP State

    // User list using AP
    uint user_num;
    mapping(uint=>address) users;
}

// mapping AP to MAC
mapping(string=>AP) public list_AP;

// User Struct
struct User{
    string Mac;

    //AP Information purchased by User
    mapping(string=>bool) state;
    mapping(string=>uint) start_time;
    mapping(string=>uint) time;
    mapping(string=>uint) number;
}

   // Mapping to address, not MAC
mapping(address=>User) public list_User;
```

Fig. 4. smart contract content

스마트 컨트랙트는 무선랜을 관리하기 위해 AP정보와 사용자 정보를 스마트 컨트랙트에 Fig. 4와 같이 저장한다. 먼저 AP구조체는 AP 계좌 정보와 AP가 사용 가능한지 상태를 저장하는 변수를 가진다. 이러한 상태변수를 가지는 이유는 존재여부를 확인할 수 있는 containKey와 같은 함수가 없기 때문이다. 그리고 해당 AP를 사용하고 있는 유저목록을 매핑하여 저장한다. 매핑은 키값으로 해당 값을 가지는 해시와 같다. 이러한 AP구조체는 다시 한 번 MAC값을 키값으로 매핑된다. 다음으로 사용자를 등록할 때 User구조체에 사용자 device의 MAC값을 저장한다. 그리고 AP를 사용할 때는 해당 AP의 MAC값을 키값으로 상태, 현재 시간, 사용할 시간 그리고 AP구조체에 유저목록을 저장하는 users의 키값인 user_num을 저장한다. user_num을 저장하는 이유는 사용자가 AP를 모두 사용하면 AP 구조체의 users에서 해당 유저를 삭제하기 위함이다. 그리고 User구조체는 MAC값이 아닌 address로 매핑한다. 이유는 사용자가 AP를 구매하면 여러 디바이스에서 사용하기 위해서이다. AP, User구조체 뿐만 아니라 AP를 등록하고 사용자가 AP를 사용하기 위해 상기 구조체에 데이터를 저장할 수 있는 함수 또한 스마트컨트렉트에 선언했다.

4.4 권한증명 기반의 프라이빗 블록체인 구조

이더리움을 권한증명 기반의 프라이빗 네트워크로 구축하기 위해 Puppeth툴을 사용하였다. Puppeth는 이더리움을 프라이빗 네트워크로 구축할 뿐만 아니라 합의 알고리즘을 권한증명으로 지정할 수 있다. 그리고 실시간 거래가 이뤄지도록 블록생성시간을 1초로 설정하였다.

초기 블록체인의 풀 노드를 구성하기 위해서 Amazon EC2(Amazon Elastic Compute Cloud)를 이용하였다. 풀 노드는 3개의 가상서버로 구축했고 이를 제어하기 위한 컨트롤러 가상서버도 구축하였다[15]. 컨트롤러에서 풀 노드을 접근하고 제어하기 위해 모든 가상서버를 같은 keypair로 생성하고 컨트롤러에는 keypair를 저장한다. 그리고 컨트롤러 가상서버에서 puppety를 실행시키고 풀 노드 3개를 연결하여 권한증명 기반의 프라이빗 블록체인을 구축했다.

풀 노드에게 부여한 서비스로는 sealnode, bootnode 그리고 ethstats가 있다. 풀 노드1에게는 위 3개의 서비스를 모두 부여하고 나머지 풀 노드2와 풀 노드3에게는 sealnode만 부여했다. 먼저 ethstats는 이더리움 네트워크를 모니터링하기 위한 설정이다. 노드1에게 ethstats 서비스를 부여했기 때문에 노드1의 IP address로 접근하여 현재 네트워크의 노드, 블록, 블록 타임등 상태를 확인할 수 있다. 다음으로 노드 1에게 부여한 bootnode는 본 네트워크(이더리움 권한 증명 네트워크)에 모든 풀 노드가 참여할 수 있도록 부트스트랩 해주는 서비스이다. 마지막으로 sealnode는 네트워크에 발생하는 트랙잭션을 검증하기 위한 권한을 노드에 부여하기 때문에 모든 풀 노드에게 부여한 것이다.

5. 결론

본 논문에서는 최근 블록체인 기반의 분산원장을 이용한 인센티브 시스템에 대한 관심이 증가하는 가운데, 기존 무선랜 접속 인증 방식을 대체할 수 있는 암호화폐 기반의 인가 제어 기법에 대해 제안하였다 . 기존 무선랜이 지정된 사용자에 대해서만 접근 제어가 가능한 반면 , 제안한 방식은 암호 화폐 시장 참여자 모두에게 접근권한을 부여할 수 있어 비인가 대역에서의 공유를 통해 무분별한 무선랜 설치를 방지하고 보다 효율적인 자원 사

용을 가능하게 한다 . 무선랜 인증 지연을 줄이고자 실시간 트랜잭션 처리가 가능한 권한기반 증명 절차를 적용 구현하였다 . 구현 시스템 성능 분석에 관한 내용은 지면 관계 상 , 후속 논문 발표를 통해 보여 질 예정이다.

REFERENCES

[1] K. Ritzberger. (2002). *Foundations of non-cooperative game theory*. OUP Catalogue.

[2] S. Nakamoto. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

[3] M. Swan. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

[4] M. Vukolić. (2015, October). *The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International Workshop on Open Problems in Network Security* (pp. 112-125). Springer, Cham.

[5] N. McKeown. (2009). Software-defined networking. I*NFOCOM keynote talk , 17(2),* 30-32.

[6] S. Kieran. (2018). *Vitalik – Ethereum en route to a million transactions per second.* (Online). https://bravenewcoin.com/insights/vitalik-ethereum-en-route-to-a-million-transactions-per-second

[7] I. C. Lin & T. C. Liao. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security, 19(5),* 653-659.

[8] P. Jayachandran. (2017). *The difference between public and private blockchain.* (Online). https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain

[9] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri & V. Sassone. (2018). *PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain.*

[10] A. Raniwala & T. C. Chiueh. (2005, March). *Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network.* In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE (Vol. 3, pp. 2223-2234). IEEE.

[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson & H. Levkowetz. (2004). *Extensible authentication protocol* (EAP) (No. RFC 3748).

[12] J. Hill. (2001). *An analysis of the RADIUS authentication protocol*. InfoGard Laboratories.

[13] G. N. Purdy. (2004). *Linux iptables Pocket Reference: Firewalls, NAT &Accounting* . " O'Reilly Media, Inc.".

[14] V. Buterin. (2014). *A next-generation smart contract and decentralized application platform.* white paper.

[15] C. Collin. (2016). *Using puppeth To Manually Create An Ethereum Proof Of Authority* (Clique) Network On AWS. (Online). https://medium.com/@collin.cusce/using-puppeth-to-manually-create-an-ethereum-proof-of-authority-clique-network-on-aws-ae0d7c906cce

김 우 성(Kim, Woo Seong) [정회원]

- 2000년 2월 : 서울시립대학교 전자전기공학부 (학사)
- 2004년 2월 : 한국과학기술원 네트워크 (공학석사)
- 2012년 3월 : Univ. of California, Los Angeles 네트워크 (공학박사)
- 2015년 2월 ~ 현재 : 가천대학교 컴퓨터공학과 교수
- 관심분야 : 차량 네트워크, 5G 네트워크, 블록체인, 정보보호
- E-Mail : wooseong@gachon.ac.kr

류 경 호(Ryu, Kyoung Ho) [학생회원]

- 2014년 3월 ~ 현재 : 가천대학교 컴퓨터공학과 학사과정
- 관심분야 : 블록체인, 네트워크, 정보보호
- E-Mail : rudgh1368@naver.com

박 양 재(Park, Yang Jae) [정회원]

- 1985년 2월 : 인하대학교 전자공학과 (공학사)
- 1990년 8월 : 인하대학교 정보공학과 (공학석사)
- 2003년 8월 : 인하대학교 전자계산공학과 (공학박사)
- 2001년 1월 ~ 2002년 12월 : 주식회사 이메디피아 원격의료연구소 연구소장
- 1993년 2월 ~ 현재 : 가천대학교 IT대학 컴퓨터공학과 교수
- 관심분야 : HCI, 모바일 네트워크, 감성공학, 블록체인
- E-Mail : parkyj@gachon.ac.kr