논문 19-44-08-20 The Journal of Korean Institute of Communications and Information Sciences '19-08 Vol.44 No.08
https://doi.org/10.7840/kics.2019.44.8.1597

전기자동차 충전 인프라에서 스마트 컨트랙트를 활용하기 위한 블록체인 네트워크 구성

장 찬 국◆, 이 옥 연°

Blockchain Network Configuration for Smart Contract in EV Charging Infrastructure

Chan-Guk Jang◆, Okyeon Yi°

요 약

최근 블록체인에 대한 관심이 증가하고 연구가 진행됨에 따라, 여러 ICT 환경에서 블록체인과의 융합에 대한 관심도 증가하고 있다. 스마트그리드 핵심 도메인 중 하나인 전기자동차 충전 인프라에서는 전기자동차 충전에 대한 거래가 존재하고 이에 따른 데이터가 생성된다. 본 논문에서는 전기자동차를 충전하는 행위 자체를 계약으로 판단하고 해당 계약을 스마트 컨트랙트에 담아 블록체인에 저장하고자 한다. 전기자동차 충전 인프라는 스마트그리드의 핵심 도메인이므로 법규에 의거하여 검증필암호모듈을 사용하여 전기자동차 충전 인프라에서 사용할 프라이빗 블록체인을 설계하고 블록체인에 담길 스마트 컨트랙트를 제안한다.

Key Words : Blockchain, smart contract, Cryptography, EV charging infrastructrue

ABSTRACT

As interest in blockchain has increased and research has progressed, interest in convergence with blockchains has also increased in many ICT environments. EV(Electric vehicle) charging infrastructure, one of the smart grid core domains, has transactions for electric vehicle charging and data is generated accordingly. In this paper, the act of charging an EV0 is judged as a contract, and the contract is to be stored in a blockchain in a smart contract. Since EV charging infrastructure is a core domain of Smart Grid, we propose the smart contract to design a private block chain for use in the EV charging infrastructure using the verified cryptographic module and to place it in a block chain.

Ⅰ. 서 론

블록체인은 2008년 사토시 나카모토의 <Bitcoin: A Peer-to-Peer Electronic Cash System>[1] 이라는 논문에서 처음 언급되었고, 그 후 가상화폐인 비트코인의 급격한 성장을 통해 대중들에게 친숙하게 다가오게 된 기술이다. 블록체인은 기존의 ICT 기술에 응용할 수 있는 범용성이 높은 기술로, 각 시스템이 개별적으로 데이터베이스에 저장하고 있던 데이터를 블록체인 기술을 통해 네트워크로 공유하는 기술이다.

여러 ICT 분야에서 블록체인에 대한 관심이 증가하는 상황에서 스마트그리드의 한 도메인인 전기자동차 충전 인프라는 전기자동차에 전력을 공급하기 위

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음" (IITP-2018-0-01396)
◆ First Author : Kookmin University Department of Financial Information Security, jangchankuk@kookmin.ac.kr, 학생회원
° Corresponding Author : Kookmin University Department of Financial Information Security, oyyi@kookmin.ac.kr, 정회원
논문번호 : 201905-069-C-RE, Received May 3, 2019; Revised May 31, 2019; Accepted June 12, 2019

한 시스템 및 기반시설을 의미하며, 다양한 ICT 기술과 유·무선 통신 기술의 융합으로 이루어져 있다. 본 논문에서는 스마트그리드의 핵심 도메인인 전기자동차의 충전을 할 때 발생하는 거래를 검증필암호모듈을 사용한 블록체인 기반의 신뢰할 수 있는 스마트 컨트랙트를 이용하여 데이터 신뢰성을 높이고 추적성을 높이고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 전기자동차 충전 인프라용 블록체인 및 스마트 컨트랙트에 대해 설명하고 3장에서는 스마트 컨트랙트에서 사용하는 암호 알고리즘의 인프라 내의 동작 시간 측정 결과를 제시한다. 마지막 4장에서는 결론 및 향후 연구를 제시하며 마무리하고자 한다.

Ⅱ. 스마트 컨트랙트를 이용한 전기자동차 충전 인프라

본 장에서는 전기자동차 충전 인프라에서의 프라이빗 블록체인을 제안한다. 전기자동차 충전 인프라의 블록체인 네트워크를 설명하고 각각의 요구사항을 설명하고 또한 기존에 다양한 곳에서 사용하고 있는 프라이빗 블록체인을 그대로 사용하기 보다는 전기자동차 충전 인프라에 맞는 프라이빗 블록체인을 설계하고자 한다. 마지막으로, 스마트 컨트랙트를 이용하여 전기자동차 충전 인프라를 구성하는 방안을 서술한다.

2.1 전기자동차 충전 인프라

전기자동차 충전 인프라는 전기자동차에 전력을 공급하기 위한 기반시설과 서비스로 다양한 시스템 및 통신기술들이 조합되어 구성된다. 전기자동차 충전 인프라는 크게 전력공급시스템, 인프라운영시스템, 고객정보시스템, 충전스테이션으로 구성된다.[2] 이러한 전기자동차 충전 인프라는 전기자동차, 전기자동차 충전기, 전기자동차 충전 사업자, 전력회사 등 크게 네 가지의 개체로 구성되어 있다. 이 개체간의 통신시에 전송되는 정보들은 전기자동차 충전 정보, 과금 정보, 기기 정보, 사용자 정보 등 노출되고 변경되면 전체 시스템에 영향을 줄 수 있는 정보들이다. 하지만 전기자동차 충전 인프라는 기존 ICT 기술을 그대로 사용하고 있기 때문에, 기존 서비스나 시스템이 가지고 있는 보안 위협을 가지고 있다.

이러한 보안 위협을 가지는 전기자동차 충전 인프라는 거래의 신뢰성과 데이터의 무결성을 제공하기 위해서는 별도의 보안 조치가 필요하다. 따라서 본 논문에서는 거래의 신뢰성을 높이고, 데이터의 무결성을 제공하기 위해 블록체인을 도입하고자 한다.

전기자동차 충전 인프라에서의 블록체인은 퍼블릭 블록체인이나 프라이빗 블록체인을 기반으로 제공할 수 있다. 퍼블릭 블록체인은 누구나 네트워크에 참여하여 블록체인 내에 있는 정보를 읽고, 쓰고, 검증할 수 있지만 높은 가치 변동성과 검열 저항성, 제한된 확장성, 익명성 등 전기자동차 충전 인프라가 사용하기에는 무리가 있다.[4] 특히, 개인정보보호법[5]에 따라 퍼블릭 블록체인을 사용하기엔 어려움이 있다. 하지만 프라이빗 블록체인의 경우, 하나의 중앙기관이 네트워크에 참여하는 것에 대한 권한을 가지고, 신뢰할 수 있는 사용자들만 네트워크에 참여해서 데이터를 공유하고 검증할 수 있다. 그리고 소수의 노드만으로도 거래를 확정할 수 있기 때문에 전기자동차 충전 인프라에서 사용하기 용이하다. 현재 국내의 전기자동차 충전 인프라는 한국전력공사가 관리하고 여러 충전 서비스 사업자가 사용자에게 요금을 청구하는 형식이 대다수이다. 따라서 전기자동차 충전 인프라용 프라이빗 블록체인은 한국전력공사가 중앙기관으로 운영하기 용이하다. 따라서, 본 논문에서는 전기자동차 충전 인프라에서의 블록체인으로 프라이빗 블록체인을 제안한다.

2.2 제안하는 전기자동차 충전 인프라용 블록체인 네트워크

제안하는 전기자동차 충전 인프라용 블록체인 네트워크는 Fig. 1과 같다.

Fig. 1에서 설명하는 전기자동차 충전 인프라용 블록체인에 참여하는 노드는 충전을 원하는 전기자동차 소유주 노드, 전기자동차 충전기 노드, 전력회사 노드, 마이닝 노드이다. 아래 Table 1은 각 노드의 기능을 설명한 것이다.

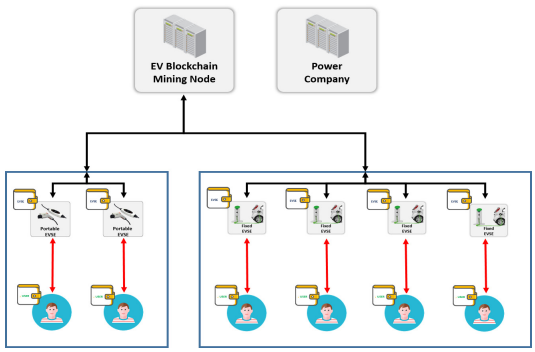

그림 1. 전기자동차 충전인프라용 블록체인 네트워크 구성도
Fig. 1. Blockchain Network Diagram for Electric Vehicle Charging Infrastructure

표 1. 전기자동차 충전 인프라 보안 위협 및 필요 보안 기능[3]
Table 1. Electric Vehicle Charging Infrastructure Security Threats and Required Security Services.[3]

Security Threat	Security Service
Forgery	Confidentiality
Alteration	Confidentiality
Leakage	Confidentiality
Man in the middle attack	Confidentiality / Integrity
Malware	integrity
Brute force attack	Authentication
Hijacking	Authentication
Elevation of privilege	Authentication
Replay attack	Authentication

Table 2와 같이 전기자동차 소유주 노드는 가상 지갑 형태로 해당 가상 지갑은 전기자동차 충전기 노드에서 동작하게 한다. 또한, 전기자동차 충전기 노드는 소유주 가상 지갑과 생성한 스마트 컨트랙트를 마이닝 노드에게 전달하여야 한다. 또한, 발행한 스마트 컨트랙트가 담겨져 있는 블록만을 저장하는 기능을 갖는다. 전력회사 노드는 전기자동차 충전 인프라용 블록체인의 관리하는 노드로, 주로 생성된 모든 블록의 저장을 한다. 마이닝 노드는 아래 절에서 자세히 설명한다.

Table 2. Blockchain Nodes for Electric Vehicle Charging Infrastructure

Blockchain node	Explanation	Requirement Features
EV Owner node	The owner of the EV joins the blockchain and proceeds to charge through the smart contract.	- Wallet
EV Supply Equipment node	It is implemented inside an EV charger and includes nodes that charge EV owner node and charge in smart contract	- Wallet - Communication Blockchain database
Power Company node	Nodes that manage blockchains for EV charging infrastructure and have all blockchain.	- Communication Blockchain database
Mining node	Nodes that block all smart contracts generated in blockchains for EV charging infrastructure into blocks.	- Communication mining

아래 절에서는 전기자동차 충전 인프라용 블록체인에서의 기능 및 요구사항을 설명한다.

2.2.1 전기자동차 충전 인프라용 블록체인 사용자 가입 및 코인 충전

전기자동차 충전 인프라는 아직까지는 전력회사의 주도로 이루어지기 보다는 전기자동차 충전 사업자의 주도로 발전해 나가고 있다. 하지만 스마트그리드의 한 도메인인 전기자동차 충전 인프라가 여러 전기자동차 충전 사업자별로 개발로 진행될 때에는 미래에 완전한 스마트그리드로의 운영이 어렵기 때문에 본 논문에서 제안하는 전기자동차 충전 인프라용 블록체인의 관리 및 운영 주체는 전력회사이다.

전기자동차 충전 인프라용 블록체인에 가입을 하고자 하는 사용자는 전력회사를 통해 가입하고 계정, 즉 지갑(공개키)과 개인키를 발급받는다. 본 충전 시스템은 일종의 가상 화폐인 충전 코인으로 충전 요금을 납부한다. 해당 코인은 마이닝을 통해 얻어지는 것이 아니라, 사용자가 일정 코인을 실제 화폐를 통해 교환하여, 충전이 완료되면 충전 요금을 코인을 통해 납부하고 해당 기록이 스마트 컨트랙트에 작성된다.

2.2.2 공개키 및 개인키 발급

전기자동차 충전 인프라용 블록체인에서는 스마트 컨트랙트 발생시 서명 방법을 일반적인 블록체인에서 서명 생성, 검증을 위해 사용되는 ECDSA P-256을 사용할 것이다. 따라서 사용되는 공개키와 개인키 쌍은 블록체인 운영 주체인 전력회사에서 제공하는 타원곡선암호 기반 인증서를 사용하는 것을 제안한다. 우리나라의 경우, 한국전력공사에서 제공하는 PKI 시스템을 이용하는 것을 제안한다.

전기자동차 소유주의 경우는 위에서 언급한 프라이빗 블록체인 참여를 위해 가입할 때 각각의 계정에 대한 인증서가 발급되어야 한다. 전기자동차 충전기 노드의 경우는 전기자동차 충전기가 설치되거나 배포될 때에 미리 기기 인증서와 개인키를 주입하고 인증서에 포함된 공개키 정보가 지갑의 주소를 대신한다.

2.2.3 마이닝 노드

전기자동차 충전 인프라용 블록체인은 프라이빗 블록체인으로, 모든 노드가 마이닝을 할 필요가 없다. 퍼블릭 블록체인의 경우, 마이닝을 통한 보상을 통해 실제 코인이 전달되고 블록 생성을 원활하게 한다. 하

지만 전기자동차 충전 인프라용 프라이빗 블록체인의 경우 신뢰된 참여자간의 네트워크이고 전기자동차 충전 스마트 컨트랙트의 블록화라는 특정 목표를 가진 블록체인이다,

따라서 전기자동차 충전 인프라용 프라이빗 블록체인 마이닝 기능만 하는 마이닝 노드를 따로 신설하는 것을 제안한다. 해당 마이닝 노드는 프라이빗 블록체인을 운영하는 전력회사에 두며, 블록체인 네트워크의 모든 블록을 생성할 때 관여한다. 따라서 다른 일반 노드는 마이닝에 참여할 수 없고, 마이닝 노드 또한 마이닝 보상은 주어지지 않으며 마이닝 난이도 또한 블록 생성 주기에 맞게 선택하여야 한다.

2.2.4 전기자동차 충전 인프라용 블록체인 어플리케이션 사용

전기자동차 소유주가 자신의 전기자동차 충전기에 가상 지갑을 활성화하기 위해서는 일종의 블록체인 어플리케이션이 있어야 한다. 해당 블록체인 어플리케이션은 충전을 진행할 전기자동차 소유주가 자신의 계정 정보와 개인키를 전기자동차 충전기에 입력하여, 가상 지갑을 활성화하는 기능을 갖는다. 또한, 해당 어플리케이션 UI를 통해 코인 충전 및 전기자동차 충전 내역, 사용 내역 등을 조회할 수 있는 기능을 갖는다.

전기자동차 소유주가 전기자동차 충전을 원하여 충전소를 방문하여 충전할 경우, 일반 주유소를 사용하는 것처럼 충전량을 결정하고 충전금액을 납부하게 된다. 전기자동차 소유주는 발급된 계정을 통해 충전량을 전기자동차 충전기에 입력하면 사용자의 가상 지갑이 전기자동차 충전기 노드와의 스마트 컨트랙트를 생성하여 충전을 진행한다. 충전량을 어플리케이션을 통해 입력할 경우 해당 정보는 스마트 컨트랙트의 입력값이 된다. 만약 해당 충전 전력양이 충전된다면 조건을 만족하였기 때문에 충전 요금을 소유주의 코인을 통해 지불하게 된다.

이동형 전기자동차 충전기를 통하여 충전할 경우는 일정 기간 동안의 충전량을 충전사업자에게 납부하게 된다. 이동형 전기자동차 충전기는 전기자동차 소유주의 소유이기 때문에 처음 사용시 발급된 계정을 입력하면 그 충전기 노드는 블록체인 가입자만을 위한 노드로 사용되게 된다. 이때에는 매 충전 시 충전된 전력량 및 거래 정보가 블록체인 네트워크에 저장되고 일정 기간이 지나면 전기자동차 소유주의 코인을 통해 충전 금액을 납부해야 한다.

2.2.5 암호모듈 사용

전기자동차 충전 인프라용 블록체인에서 사용하는 암호기술은 스마트 컨트랙트에 사용되는 전자서명과 블록 생성시 사용되는 해시함수 두 가지이다. 두 암호기능 모두 다양한 알고리즘을 사용해서 제공할 수 있지만, 전기자동차 충전 인프라용 블록체인에서 사용되는 모든 암호기술은 지능형전력망의 구축 및 이용촉진에 관한 법률[6]과 지능형전력망 정보의 보호조치에 관한 지침[7]의 제 10조에 의거하여 검증필암호모듈을 사용하여야 한다. 따라서 두 가지 기능은 반드시 검증필암호모듈 보호함수 목록에 있는 알고리즘을 통해 제공되어야 한다. 아래 표는 전자서명과 해시함수 알고리즘이다.

또한, 한국전력공사는 취약한 키 생성 알고리즘 및 서명 알고리즘을 사용하지 않고 검증필암호모듈의 사용을 통한 PKI 구축을 통해, 전기자동차 소유주 및 모든 노드의 개인키, 공개키를 발급해야 한다.

표 3. 전기자동차 충전 인프라용 블록체인에서 사용해야할 암호 알고리즘[8]
Table 3. Cryptographic Algorithm to Use in Blockchain for Electric Vehicle Charging Infrastructure[8]

Function	algorithm	Using
Hash	SHA-2 Series	For computation of muckle root and public key operations
Digital Signature	ECDSA P-256	For smart contract double signing

2.3 제안하는 전기자동차 충전 인프라용 스마트 컨트랙트

전기자동차 충전 인프라용 블록체인에서의 스마트 컨트랙트[9]는 전기자동차 소유자 노드인 가상 지갑과 전기자동차 충전기 노드 사이에서 발생한다.

스마트 컨트랙트의 정의는 앞서 2장에서도 언급하

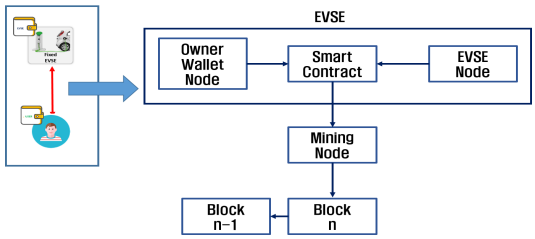

그림 2. 전기자동차 충전 인프라에서 발생하는 스마트 컨트랙트
Fig. 2. Smart Contracts from Electric Vehicle Charging Infrastructure

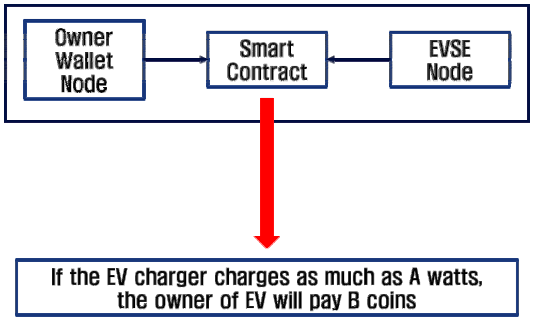

그림 3. 전기자동차 충전 인프라 스마트 컨트랙트 예시
Fig. 3. Example of Smart Contracts from Electric Vehicle Charging Infrastructure

였지만, 특정 계약 조건이 달성되면 계약 내용이 진행되는 것이다. 따라서 전기자동차 충전 인프라에서의 스마트 컨트랙트는 전기자동차 소유자가 충전하고자 하는 전력량이 계약 조건이 되고, 전기자동차 충전기가 해당 전력량을 충전하게 된다면 계약 조건이 달성되는 것이다. 이때의 보상은 충전 요금이 된다. 다음 그림은 스마트 컨트랙트의 간략한 예시이다.

해당 스마트 컨트랙트는 전기자동차 소유주의 개인키와 전기자동차 충전기 노드의 개인키로 이중 서명된다. 스마트 컨트랙트에 참여하는 당사자인 소유주와 전기자동차 충전기의 개인키로 서명하기 때문에 데이터 무결성과 부인방지 기능을 모두 제공할 수 있다. 또한, 이중 서명이 되어 있기 때문에 계약이 완료된 후에는 둘 중 한 당사자가 계약의 내용을 변경할 수 없다. 따라서 이중 서명된 스마트 컨트랙트는 ”Read-Only“ 기능만 제공한다.

Ⅲ. 성능 측정 및 결과

스마트 컨트랙트 발생 시 예상되는 가장 큰 부하는 전자서명 생성시간이다. 본 절에서는 제안하는 전기자동차 충전 인프라에서의 스마트 컨트랙트 사용시 사용해야 하는 암호 알고리즘인 ECDSA P-256을 이용한 전자서명의 생성 및 검증과 HASH SHA-256의 동작 시간 측정에 대한 결과를 제시한다.

일반적으로 전기자동차 충전 인프라에서 전기자동차 충전기는 유선망이나 이동통신을 사용하여 충전 서비스 서버와 데이터 통신을 진행한다. 전기자동차 충전기에서 발생하는 데이터 주기는 평균 1분이며 수초 이내로 전송되는 것을 요구한다.

제안하는 전기자동차 충전 인프라 스마트 컨트랙트는 전기자동차 충전기에서 생성된다. 따라서 본 실험은 기존 이동형 전기자동차 충전기에서 실제로 사용하고 있는 두 개의 LTE 모듈을 사용하였다. 또한, 고정형 전기자동차 충전기를 대신하여 여러 IoT 환경에서 사용되는 라즈베리파이 3와 임베디드 리눅스 장비를 통하여 진행하였다. 또한, 이러한 장비들과의 비교를 위해 일반 데스크탑에서도 동일한 실험을 진행하였다.

각 운영환경에서의 실험은 모두 검증필암호모듈 KMULiB V2.0을 사용하여 진행하였으며, 전자서명 생성 및 검증은 1회 기능 수행 시간을 측정하였고, 20회 실험하였고, 정확한 측정을 위해 해시함수는 10,000회 기능 수행 시간을 측정하였고, 마찬가지로 20회 실험하였다. 아래 [Table 5], [Table 6], [Table 7]은 실험 결과이다.

표 4. 암호 알고리즘 동작 실험 환경
Table 4. Cryptographic Algorithm Experimental Environment

Devices		Spec
AMTelecom LTE Module	Processor	ARMv7 rev5 1.2GHz
	OS	Embedded Linux Kernel 3.0
	RAM	128MB
	Compiler	arm-oe-linux-gnueabi-gcc
Teladin LTE Module	Processor	Qualcomm MDM9215
	OS	Embedded Linux Kernel 3.0
	RAM	128MB
	Compiler	arm-oe-linux-gnueabi-gcc
Raspberri Pi 3	Processor	ARM Cortex A53
	OS	RASPBIAN STRETCH LITE 1.2GHz
	RAM	1GB
	Compiler	gcc 6.3
Embedeed Linux Device	Processor	TI AM3359(based ARM Cortex-A8) 700MHz
	OS	Embedded Linux Kernel 3.0
	RAM	DDR3 256MB
	Compiler	gcc 3.14
Desktop	Processor	Intel core i7-4790 CPU 3.6GHz
	OS	Ubuntu 14.04 Kernel 3.19
	RAM	4GB
	Compiler	gcc 4.8.4

표 5. 전자서명 1회 생성 기능 수행시간(초)
Table 5. Excution time of Digital Signature Generation Function(Sec)

	AMTelecom LTE Module	Teladin LTE Module	Raspberri Pi 3	Embedded Linux Device	Desktop
1	0.377	0.831	0.277	0.577	0.032
2	0.376	0.832	0.277	0.576	0.032
3	0.377	0.831	0.278	0.577	0.032
4	0.376	0.831	0.278	0.576	0.032
5	0.376	0.832	0.277	0.577	0.033
6	0.377	0.831	0.277	0.576	0.033
7	0.377	0.832	0.278	0.577	0.033
8	0.376	0.831	0.277	0.576	0.032
9	0.377	0.831	0.278	0.577	0.032
10	0.377	0.832	0.277	0.577	0.032
11	0.377	0.831	0.278	0.576	0.032
12	0.377	0.831	0.278	0.576	0.033
13	0.377	0.831	0.278	0.577	0.032
14	0.376	0.831	0.278	0.576	0.032
15	0.376	0.832	0.277	0.577	0.032
16	0.377	0.831	0.278	0.577	0.033
17	0.377	0.831	0.278	0.576	0.032
18	0.377	0.831	0.277	0.577	0.032
19	0.376	0.832	0.277	0.576	0.032
20	0.377	0.831	0.277	0.577	0.032
AVG	0.377	0.831	0.278	0.577	0.032

표 6. 전자서명 1회 검증 기능 수행시간(초)
Table 6. Excution time of Digital Signature Verification Function(Sec)

	AMTelecom LTE Module	Teladin LTE Module	Raspberri Pi 3	Embedded Linux Device	Desktop
1	0.726	1.600	0.537	1.111	0.064
2	0.727	1.600	0.537	1.112	0.063
3	0.726	1.600	0.537	1.111	0.064
4	0.727	1.600	0.538	1.111	0.062
5	0.726	1.600	0.537	1.111	0.061
6	0.727	1.600	0.537	1.111	0.062
7	0.726	1.601	0.538	1.111	0.062
8	0.727	1.600	0.537	1.111	0.063
9	0.726	1.600	0.537	1.111	0.062
10	0.727	1.600	0.537	1.111	0.064
11	0.726	1.600	0.537	1.112	0.062
12	0.726	1.601	0.536	1.111	0.063
13	0.726	1.600	0.538	1.111	0.062
14	0.726	1.600	0.537	1.111	0.064
15	0.727	1.601	0.537	1.112	0.062
16	0.726	1.600	0.538	1.111	0.063
17	0.727	1.600	0.537	1.111	0.062
18	0.726	1.601	0.537	1.111	0.063
19	0.727	1.600	0.538	1.112	0.062
20	0.726	1.600	0.537	1.112	0.060
AVG	0.726	1.600	0.54	1.111	0.063

검증필암호모듈 KMULiB V2.0을 사용하여 전자서명 생성 및 검증, 해시함수 기능에 대해 실험을 해본 결과, 전기자동차 충전 인프라 스마트 컨트랙트를 생성할 때 필수적으로 사용되는 전자서명 생성 기능의 경우, 전자서명 1회 생성시 라즈베리파이 3에서 200ms로 가장 작게 소모되었고, LTE 이동통신 모듈에서 최대 800ms가 소모되었다.

이때 일반 PC에서는 약 30ms가 소모되었다. 전기자동차 충전 인프라용 블록체인의 노드 간 인증 시 사용될 전자서명 1회 검증은 최소 수행 시간은 라즈베리파이 3에서 500ms, 최대 수행 시간은 LTE 이동통신 모듈에서 1.6s가 소모되었다.

또한, 일반 PC에서는 약 60ms가 소모되었다. 일반적으로 전기자동차 충전 인프라에서 이동통신을 사용하여 데이터가 전송될 때 이동통신의 특성상 일반적 연결 지연 시간은 약 50ms 정도가 소모되고, 이 또한 네트워크 환경의 영향을 많이 받는다.

그리고, 전기자동차 충전기에서 발생하는 데이터는 수 초 이내에 전송되는 것이 요구된다. 따라서 본 실험의 결과는 전기자동차 충전 인프라 스마트 컨트랙트에서 가장 핵심적인 기능인 ECDSA P-256을 이용한 이중 서명을 수행하는 시간이, 최적화 소스가 아님에도 불구하고 모든 실험 장비가 800ms 이내에 생성하는 것을 통해 전기자동차 충전 인프라에서 전자서명을 사용하여 스마트 컨트랙트를 생성하는 것이, 전기자동차 충전 인프라의 가용성을 해치지 않고 블록체인을 사용하여 데이터의 무결성 및 위·변조를 막는 것이 가능하다는 것을 보였다.

또한, 해시함수의 경우 10,000회 측정값이 최소 20ms에서 최대 70ms이므로 전기자동차 충전 인프라용 블록체인 및 스마트 컨트랙트에서 해시함수에 의한 지연이 되지 발생하지 않는다는 것을 보였다.

표 7. 해시함수 10,000회 기능 수행시간(초)
Table 7. Excution time of Hash value generation 10,000 times(sec)

	AMTelecom LTE Module	Teladin LTE Module	Raspberri Pi 3	Embedded Linux Device	Desktop
1	0.030	0.070	0.020	0.030	0.003
2	0.030	0.070	0.020	0.030	0.003
3	0.030	0.070	0.020	0.030	0.003
4	0.030	0.070	0.020	0.030	0.003
5	0.030	0.070	0.020	0.030	0.003
6	0.030	0.070	0.020	0.030	0.003
7	0.030	0.070	0.020	0.030	0.003
8	0.030	0.070	0.020	0.030	0.003
9	0.030	0.070	0.020	0.030	0.004
10	0.030	0.070	0.020	0.030	0.003
11	0.030	0.070	0.020	0.030	0.003
12	0.030	0.070	0.020	0.030	0.003
13	0.030	0.070	0.020	0.030	0.003
14	0.030	0.070	0.020	0.030	0.003
15	0.030	0.070	0.020	0.030	0.003
16	0.030	0.070	0.020	0.030	0.003
17	0.030	0.070	0.020	0.030	0.004
18	0.030	0.070	0.020	0.030	0.003
19	0.030	0.070	0.020	0.030	0.003
20	0.030	0.070	0.020	0.030	0.004
평균	0.030	0.070	0.020	0.030	0.003

Ⅳ. 결 론

프라이빗 블록체인은 신뢰된 노드만 참여하여 원장을 공유하는 방식으로, 데이터 변조가 어렵고 높은 신뢰성을 갖는데 의미가 있다. 본 논문에서는 프라이빗 블록체인을 스마트그리드의 한 도메인인 전기자동차 충전 인프라에 도입시켜 충전 및 결제 데이터 등을 공유하여 데이터 위·변조를 어렵게 하여 신뢰성을 높이자 한다. 또한, 지능형전력망의 제도적 요구사항인 검증필암호모듈을 사용하여야 한다고 제안하였다. 마지막으로 전기자동차 충전 인프라에서 스마트 컨트랙트를 사용하는데 큰 영향이 없다는 실험까지 진행하였다.

향후 연구로는 제안하는 전기자동차 충전 인프라용 블록체인 및 블록체인 애플리케이션의 안전한 개발과 프라이빗 블록체인의 안전한 관리 정책에 관해 연구하고자 한다.

또한, 스마트 컨트랙트의 고도화 및 취약성 검증을 통해 실제 전기자동차 충전 인프라에 실증 및 적용을 목표로 한다.

References

[1] S. Nakamoto, "*Bitcoin : A peer-to-peer electronic cash system*(2008)," URL: http://www.bitcoin.org/pdf(2012)

[2] H.-G. Lee, "Development status and prospect of electric vehicle charging infrastructure" *KIPE Mag*., vol. 15, no. 6, pp. 73-76, Dec. 2010.

[3] S. Kang and J. Seo, "An analysis of the security threat and security requirements for electric vehicle charging infrastructure," *J. KIISC*, vol. 22, no. 5, pp. 1027-1037, Oct. 2012.

[4] Finector Report, *Development process and understanding of blockchain technology*, pp. 22-44, Aug. 2016.

[5] Personal Information Protection Commission, *Study on the Effect of Blockchain Technology on Personal information Protection*, Oct. 2018.

[6] "*Smart Grid Construction and Utilization Promotion Act*," Ordiance of the Ministry of Knowledge Economy, no. 211, Nov. 2011.

[7] "*Guidelines for Protection of Smart Grid Information,*" Ordiance of the Ministry of Knowledge Economy, http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000172731

[8] *Korea Cryptographic Module Validation Program*, NIS, http://service1.nis.go.kr

[9] N. Szabo, "*The idea of smart contract*," 1994.

장 찬 국 (Chan-Guk Jang)

2016년 2월 : 국민대학교 수학과 학사

2018년 2월 : 국민대학교 금융정보보안학과 석사

2018년 3월~현재 : 국민대학교 금융정보보안학과 박사과정

<관심분야> 네트워크 보안, 정보보안 프로토콜, 검증필암호모듈 구현/적용

[ORCID:0000-0002-3791-1006]

이 옥 연 (Okyeon Yi)

1988년 2월 : 고려대학교 수학과 학사

1990년 2월 : 고려대학교 일반대학원 수학과 석사

1996년 8월 : University of Kentucky 대수학 박사

1997년~1999년 : 고려대학교 Post Doc.

1999년~2001년 : 한국전자통신연구원 선임연구원/팀장

2001년 9월~현재 : 국민대학교 정보보안암호수학과, 금융정보보안학과 교수

2013년~현재 : 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 사업단장

<관심분야> 검증필암호모듈 구현/적용, 네트워크 보안

[ORCID:0000-0001-8156-2360]