블록체인을 이용한 스마트 그리드 시스템의 기기 인증 방안

이성훈*, 김광조**

*카이스트 소프트웨어 대학원/ **카이스트 전산학부

Device authentication in Smart Grid System using Blockchain

Sung-Hoon Lee*, Kwangjo Kim*

*Software Graduate Program, KAIST/ **School of Computing, KAIST

요 약

최근 전력사용의 불균형 심화와 요금 과다로 인해 전력회사와 소비자 간의 분쟁이 빈번하게 발생하고 있어 이를 해결하는 스마트 그리드 시스템의 도입을 적극적으로 시도하고 있다. 스마트 그리드 시스템과 연계하여 사용하는 ICT 기술은 다양한 보안 위협을 가지고 있으므로 결국 스마트 그리드 시스템의 심각한 보안 위협이 된다. 본 논문에서는 다양한 보안위협에 대응하기 위해 스마트 그리드 시스템의 구성 기기들을 인증하는 데 비트코인의 핵심기술인 블록체인을 사용하여 저렴하고 안전한 스마트 그리드 시스템의 인증 방법을 제안하고 그 실용성을 검증한다.

I. 서론

스마트 그리드의 구축 규모가 점차 확대됨에 따라 다양한 ICT 기술들이 기존 전력망에 설치되고 있다. 스마트 그리드를 구성하는 다양한 기기들은 이제 인터넷에 연결되어 사물인터넷을 구성하고 서로 통신하며 최적의 전력소비와 효율적 전력생산을 하게 될 것이다. 그러나, 사용하는 기기들이 인터넷에 연결됨으로써 현재 인터넷 환경에서 발생하는 보안 문제들이 스마트 그리드 시스템에도 똑같이 발생할 수 있다.

또한, 이미 구축된 스마트 그리드 시스템에서는 보안 위협에 대한 방비가 없어 다양한 보안 위협에 노출된 상태이다. 그중 우리나라에서 구축 진도가 가장 빠른 AMI(Advanced Metering Infrastructure) 부분은 250만 가구 이상의 일반 소비자의 전력사용정보가 연계되어 있어[1] 보안 적용이 필수적으로 요구되는 상황이다.

그리고, AMI 보안에 대한 연구는 진행되고 있으나 구축비용 증가와 관련 표준 부재로 즉시 도입에 어려움을 겪고 있다. 본 논문에서는 블록체인을 이용하여 스마트 그리드 시스템을 구성하는 기기들을 적은 비용으로 효과적으로 인증하여 스마트 그리드 시스템을 보다 안전하고 빠르게 구축하는 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 배경지식을 알아보고, 3장에서는 선행연구, 4장에서는 핵심내용인 기기인증에 관해 설명하고 5장에서는 제안한 시스템을 구현 및 검증하고, 끝으로 6장에서는 결론을 맺는다.

II. 배경지식

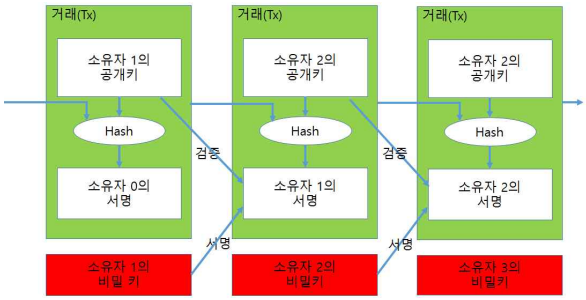
2.1 스마트 그리드

스마트 그리드는 효율적인 전력생산과 소비를 위해 기존 전력망에 다양한 ICT 기술을 접목, 실시간으로 정보를 교환하여 최적의 전력생산과 소비의 사이클을 제공하는 차세대 전력망이다. 스마트 그리드를 이루는 대표적인 기술에는 전력을 효율적으로 생산하는 지능형 전력망 기술, 소비자와 실시간 통신이 가능한 양방향 통신 인프라, 생산된 전력을 저장하고 운송하는 기술, 다양한 신재생 에너지 생산 및 구축 기술, 마지막으로 생산된 에너지를 합리적인 소비로 유도하는 정보 제공 기술 등이 있다.

2.2 블록체인[2,7]

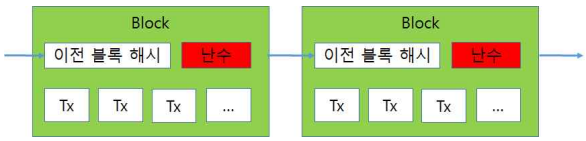
블록체인은 가상화폐 중 가장 많이 사용되고 활성화되어 있는 '비트코인'을 유지하는 기반 보안 기술이다. 비트코인에서 블록체인은 주기적으로 발행하는 화폐인 비트코인의 가치가 이동한 이력을 저장하는 일종의 분산된 디지털 장부라고 할 수 있다. 이 장부는 위변조할 수 없는 암호학적 기술로 만들어지며 비트코인의 소

유권 이동을 위하여 [그림 1]과 같은 비트코인의 거래(Transaction) 과정과, 발생한 거래를 모아 시간이 매우 오래 걸리는 특정 조건의 해시값을 갖게 하는 난수(Nonce) 찾기 문제로 거래내용의 위변조를 방지할 수 있는 작업증명(Proof of Work) 단계 등으로 만들어진다.



[그림 1] 비트코인의 거래 과정

위변조 여부를 판단하기 위해 비트코인 거래들이 모인 블록의 해시를 만드는데, 이때 이전 블록의 해시값도 입력되어 현재 블록의 해시를 만들 때 영향을 주게 된다. 이 블록들은 [그림 2]처럼 논리적으로 연결되는데 이를 블록체인이라 부른다. 이때 조건에 맞는 블록 해시값을 찾은 사용자(Node)는 새로운 비트코인의 가치를 받게 되는데 작업증명 과정과 비트코인 가치를 받는 것을 채굴(Mining)이라 표현한다.



[그림 2] 블록체인 개념도

III. 선행연구

3.1 기기 인증 시스템

기기 인증에는 다양한 기술들이 사용되는데 그중 보안 수준이 가장 강력한 기술은 공개키 기반 구조(PKI)하에 기기별 인증서를 이용한 인증 시스템으로, 가장 높은 안정성과 확실한 기기 식별 기능을 가지고 있다. 한국전력에서도 2015년 6월에 가진 AMI 보안 공청회에서 공개키 기반 기기 인증서를 이용한 AMI 보안 기술과 정책을 발표하였다.[3,4]

PKI 기반 인증시스템은 일반적으로 응용별로 계층적으로 구성되며 인증요구자를 대면 신원확인하여 등록하는 등록서버(RA), 공인 인증서를 발급하는 인증서버(CA), 인증서를 온라인 검증하는 OCSP서버 등으로 구성된다.[5]

3.2 블록체인의 응용

블록체인은 그 편의성 때문에 비트코인 이외에 새로운 시스템과 서비스에 적용하는 사례가 지속적으로 발굴되고 있다. 대표적으로 금융 거래내용을 분산 저장하여 은행 고객의 인증 정보와 자산을 디지털화하여 소유권을 증명하는 시스템, 등기 또는 증명서 등 데이터를 검증하여 그 존재를 증명하는 시스템 등이 있다. 최근에는 사물인터넷과 연계를 위한 개념증명으로 삼성전자와 IBM에서 ADEPT라는 시스템을 발표한 바가 있다.[6]

IV. 기기 인증

4.1 인증 시스템의 구성 방법

본 논문에서는 블록체인을 이용한 스마트 그리드 시스템의 기기 인증방식을 'DeviceChain'이라 한다. DeviceChain을 스마트 그리드에 적용하는 방법은 다음과 같다. DeviceChain에서 이용하는 블록체인은 스마트 그리드에 접속 가능한 기기의 인증상태를 저장하는 역할로 스마트 그리드의 다양한 서버에서 동작한다. 서버에서 DeviceChain은 기기의 정보를 확인하는 단계와 확인된 기기의 인증 상태를 블록체인에 저장하는 단계, 저장된 기기의 인증 상태를 체크하는 단계를 수행한다. 서버에 접속하는 다양한 기기들은 DeviceChain을 통해 블록체인에 등록되고 인증 단계를 거쳐 통신이 이루어진다. [표 1]은 스마트 그리드에서 DeviceChain의 수행 기능이다.

[표 1] 스마트 그리드에서 DeviceChain의 수행 기능

스마트 그리드	DeviceChain 기능	비고
서버	-기기정보 확인 -인증상태 저장 -인증상태 체크	
기기	-등록 및 인증 요청	

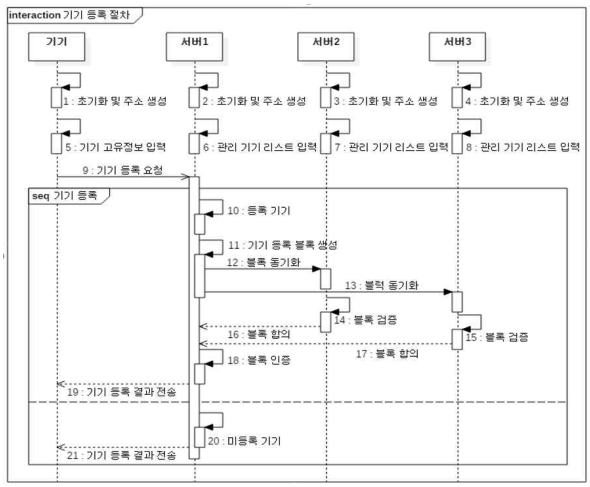
4.2 기기 등록

스마트 그리드에서 통신은 서버와 기기 간에 이루어진다. 보안 통신을 위해서 서버는 통신하기 전에 해당 기기가 신뢰할 수 있는 기기임을 확인이 필요하다. 다음과 같은 절차로 기기 인증상태를 DeviceChain에 등록하여 기기 인증처리를 한다.

[그림 3]은 DeviceChain의 기기 등록절차로 서버와 기기는 블록체인 거래를 위하여 DeviceChain을 통해 ECDSA와 같은 서명 방식의 공개키와 개인키를 생성한다. 그리고 기기는 고유정보와 공개키를 전자서명 후 서버에 전송하여 DeviceChain에 기기 등록을 요청한다.

서버는 수신 정보를 통해 스마트 그리드 인증 기기 정보와 비교하여 인증 기기임을 확인한다. 그리고 DeviceChain에서 발행한 서버 소

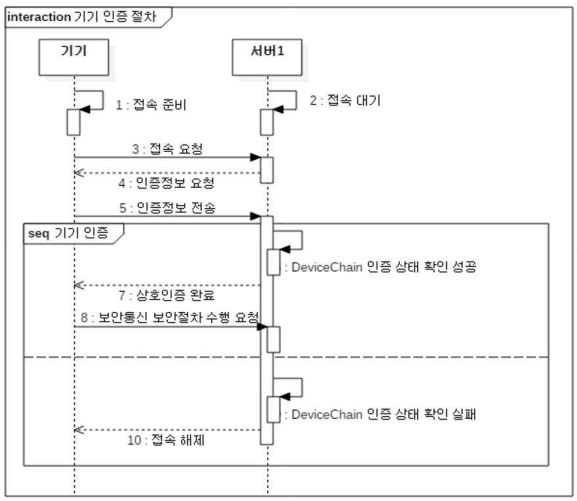
유의 인증토큰을 기기로 소유권을 이전한 내용을 블록체인에 저장한다. 저장된 블록은 DeviceChain 서버들 간에 동기화되고 동기화된 서버에서는 블록의 내용을 각각의 인증 기기 정보와 블록 검증 알고리즘을 통해 검증한다. 모든 서버는 검증이 끝나면 블록에 대한 검증 결과를 동기화한다. 모든 서버에서 합의하게 되면 해당 블록의 기기들은 인증된 기기로 인정받게 된다.



[그림 3] DeviceChain의 기기 등록절차

4.3 기기 인증

기기는 DeviceChain의 서버에서 이전된 인증토큰을 통하여 스마트 그리드에서 통신하게 된다. [그림 4]는 DeviceChain의 기기 인증절차로 기기는 서버와 통신하기 위해 서버에 전자서명한 인증정보를 전송한다. 서버에서는 수신 정보를 통해 DeviceChain에 인증상태를 확인하고 인증 기기임을 확인하면 보안 통신을 위한 보안절차를 수행한다.



[그림 4] DeviceChain의 기기 인증절차

V. 시스템 구현 및 검증

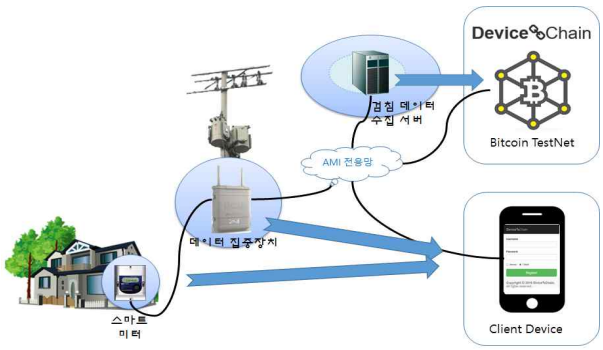
5.1 시스템 개발환경

DeviceChain 구현 및 테스트는 스마트 그리드의 AMI 시스템을 모델로 하여 시스템을 구현하였다. AMI 시스템은 [표 2]에서처럼 크게 세 부분으로 구성되어 있다. 첫째로 사용자의 전력사용량을 기록하는 스마트 미터, 두 번째는 전력사용량을 스마트 미터에서 읽어 저장하고 검침 서버에 전송하는 데이터집중장치, 마지막으로 데이터집중장치에서 검침 데이터를 수신받아 정보서비스를 해주는 검침 서버이다.

[표 2] AMI 시스템 구성

구분	기능	비고
스마트 미터	-사용자 전력사용량 기록	기기
데이터집중장치	-스마트 미터 검침 -검침 데이터 서버 전송	기기
검침 서버	-정보서비스	서버

DeviceChain에서 블록체인 기술을 이용하여 AMI 기기 인증 내용을 블록으로 저장하고, 블록을 합의하는 기능은 검침 서버들이 수행하며, 기기 등록요청과 인증 요청은 인증의 대상인 데이터집중장치 및 스마트 미터에서 수행한다. 그리고 DeviceChain을 실제 AMI 환경에서 구축할 수 없어 가상의 환경을 시뮬레이션하여 테스트한다. 검침 서버의 블록체인 기술 적용은 Bitcoin TestNet을 이용하고 AMI 기기의 등록요청과 인증 요청기능을 스마트폰 앱으로 대신하였다. [그림 5]은 AMI 시스템에 DeviceChain을 적용한 시뮬레이션 환경이다.



[그림 5] DeviceChain을 적용한 시뮬레이션 환경

5.2 시스템 구현

DeviceChain의 공통기능으로 검침 서버와 AMI 기기 간의 Bitcoin TestNet에서 거래에 사용되는 공개키 관리 기능이 있다. 검침 서버와 AMI 기기에 각각 유일한 공개키 쌍이 생성되면 검침 서버에는 AMI 기기를 인증할 인증토큰을 발행하여 기기 인증에 사용한다.

검침 서버는 DeviceChain에 AMI 기기 인증

정보를 관리하고 AMI 기기에서 등록 요청 시, 관리하는 기기 인증 정보와 비교하여 확인된 기기만 DeviceChain에 인증토큰을 이전하여 Bitcoin TestNet에 동기화하여 등록한다.

AMI 기기는 기기 자신의 고유정보로 DeviceChain에 등록 요청하고, AMI 기기와 검침 서버 간 접속 테스트 시뮬레이션을 통해 DeviceChain의 인증기능을 테스트한다.

구현된 DeviceChain의 수행 절차는 다음과 같다. 먼저 검침 서버와 AMI 기기에서 DeviceChain을 통해서 Bitcoin TestNet 공개키 쌍을 각각 만든다. 검침 서버에서는 등록 대상 AMI 기기의 정보를 입력하고, AMI 기기에서는 자신의 기기 정보를 생성하고 해당 정보로 검침 서버에 기기 등록을 요청하면 검침 서버에서는 기기 정보를 확인하고 DeviceChain에 기기를 등록한다. 마지막으로 AMI기기에서 검침 서버에 접속 테스트를 요청하면 검침 서버에서 DeviceChain을 통해 해당 기기의 인증 상태에 따라 인증 결과를 보여준다.

5.3 결과

DeviceChain을 통해 AMI 시스템에서 AMI 기기 등록과 통신을 위한 기기 인증을 시뮬레이션하여 보안 통신의 첫걸음인 기기 인증 기능을 구현하고 테스트하였다.

[표 3]은 PKI 기반 인증시스템과 Device Chain을 간략히 비교한 것으로 PKI 기반 인증시스템은 RA, CA, OCSP 등의 서버를 이용하여 등록, 주입, 인증, 검증 등을 보조 인증 수단을 이용하여 최소 4단계를 거쳐 인증처리를 하고, 서버도 용도에 맞게 독립적으로 4개 이상이 필요하다. 이에 반해 DeviceChain은 서버와 기기 간에만 일어나는 절차로 비교적 간단히 AMI 기기 인증 시스템을 운영할 수 있다. 이는 운영시간을 단축할 수 있고 분산 저장된 정보로 검침 서버가 모두 인증이 가능하여 백업과 동시에 서버 장애가 전체 시스템에 영향 없이 운영할 수 있다.

[표 3] 인증시스템의 비교

구분	PKI 기반 인증시스템	DeviceChain	효과
수행 단계	등록, 발급, 인증, 주입 등 복잡	등록, 인증 등 간단	시간 단축
서버 소요	RA, CA, OCSP 등 추가	기존 서버	비용 절감

또한, 현재 비트코인 블록체인 기준으로 1개 블록이 최대 1M byte의 크기로 10분당 한 개씩 생성되는데 1년 동안 운영했을 때 최대 51G bytes가 생성된다. 이는 기존 검침 서버에 블록체인과 함께 운영이 가능한 수준으로 구축 비용도 절감할 수 있을 것으로 기대된다.

VI. 결론

최근에 골드만 삭스에서 블록체인을 통해 비용절감 사례를 발표하였는데 스마트 그리드에서도 다양한 분야에 블록체인의 응용 가능성과 효과가 있음을 예측하였다.[8]

본 논문에서도 스마트 그리드 확대의 장애요인 중 하나인 보안 위협을 해결하는 방안으로, 기존 시스템보다 저렴한 비용과 효율적인 방법으로 운영할 수 있는 블록체인을 이용한 스마트 그리드 기기 인증 방안을 제시하였다. 그리고 AMI 시스템을 모델링 하여 기기 인증 기능을 테스트함으로써 블록체인의 스마트 그리드 적용 가능성을 확인하였다.

블록체인은 지금도 계속 연구되고 있고, 다양한 분야에서 응용사례가 나오고 있다. 관련 법규의 부재 및 처리속도, 저장용량 등의 해결해야 할 기술적인 문제로 블록체인 기술의 확대에도 시간이 좀 더 필요하지만, 스마트 그리드와 같은 대규모 시스템에서 그 효용의 가치는 비용과 운영효율 면에서 크기 때문에 블록체인의 기술적 발전이 스마트 그리드에서 효과를 얻을 수 있을 것으로 기대된다.

그리고 블록체인 기술을 스마트 그리드에 다양한 분야에 적용하기 위한 블록체인 프로토콜 및 합의 알고리즘에 관한 연구가 추가로 필요하다.

[참고문헌]

[1] KEPCO 보도자료, 올해 AMI 구축사업 200만호 2천억원 투자한다, 2016.

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, pp,3-4, bitcoin.org, 2009.

[3] KISA, Device authentication service application for information and communication devices, pp,8-22, 2011

[4] KEPCO 보도자료, 전력연구원 AMI 보안기술 사외 공청회, 2016.

[5] 현무용, 김태훈, 김재희, 김종화, 스마트그리드 기기 인증시스템의 설계 및 구현, pp,1-2, 한국통신학회, 2014.

[6] IBM, ADEPT: An IoT Practitioner Persppective, 2015.

[7] Andreas M, 비트코인, 블록체인과 금융의 혁신 Masteing Bitcoin: Unlocking Digital Cryptocurrencies, pp,49-68, O'REILLY, 2015.

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