허가형 블록체인을 이용한 마이크로 그리드 에너지 공유 프레임워크

전정민 ˚, 강선무, 홍충선*

경희대학교

jmjeon0212@khu.ac.kr ˚, etxkang@khu.ac.kr, *cshong@khu.ac.kr

MicroGrid Energy Sharing Framework using Permissioned Blockchain

Jeongmin Jeon ˚, Sunmoo Kang, Choong Seon Hong*

*Kyung Hee University

요 약

미래사회는 에너지인터넷을 구축하여 에너지를 공유하고 더 나아가 에너지 사용과 온실가스 사용을 최소화하는 제로 에너지 지향사회로 나아갈 것이다. 이에 따라 에너지 시스템은 중앙 집중형 에너지 공급 시스템에서 ICT기반 분산형 에너지 공급 시스템으로 패러다임이 변화하고 있다. 이러한 변화 트렌드에 적용될 수 있는 ICT융합 기법으로써, 본 논문에서는 Permissioned Blockchain 기반 스마트 컨트렉트를 활용한 에너지 공유 프레임워크를 제안한다. 이는 에너지 공유 시 중앙화된 회사나 데이터베이스가 거래 데이터를 참조하는 경우 발생하는 데이터 위·변조에 대한 위험성, 다시 말해 데이터 무결성이 보장되지 않는 문제를 해쉬 기반 Winternitz One-Time Signature(W-OTS) 기법을 적용하여 해결함으로써 중개자 개입 없이 가까운 거리에 있는 프로슈머와 소비자 사이에서 에너지를 안전하게 공유할 수 있는 환경을 제공한다.

1. 서 론

최근 SmartGrid(SG)에서 개인 간의 전력거래를 위한 블록체인 적용하려는 움직임이 활발하다. 전력망과 통신기술의 융합으로 탄생한 전력 데이터 거래 시스템은 기존 전력망과 비교하면 안정성, 효율성을 가진다. 신재생 에너지, 전기자동차, 프로슈머 등 새로운 서비스가 등장하여도 전력망과의 유연하게 연동할 수 있는 확장성을 향상한다. SG와 블록체인 기술의 결합은 프로슈머와 소비자의 전력거래를 할 수 있는 전력망으로 진화해오고 있다[1].

현재 우리나라는 프로슈머와 소비자 간의 전력을 거래할 수 있는 서비스가 필요하지만, 현재 이와 관련된 안전한 전력거래 인프라가 국내에 존재하지 않은 실정이다[2]. 일반적으로 에너지 요금부과 수익은 데이터 또는 서비스에 따라 달라지기 때문에 데이터 무결성은 에너지 거래 사기 문제를 예방하는데 핵심적인 역할을 한다[3].

4차 산업혁명과 함께 스마트 미터를 이용해 전력 사용정보를 공급자에게 제공하는 SG 시스템과 한 단계 발전하여 에너지의 소비와 생산 및 판매를 같이하는 프로슈머(Prosumer)의 개념이 확대된 MicroGrid(MG) 시스템이 등장하였다[4]. MG와 블록체인이 제공하는 장점은 데이터의 무결성,신뢰성이 보장되며 중앙으로 모여있지 않고 데이터의 분산된 분권화 및 보안, 투명성을 지킬 수 있다.

따라서 본 논문에서는 Permissioned Blockchain(PB)을 기반으로 스마트 컨트렉트를 활용한 보안성이 높고 투명한 전력을 거래가 가능한 MG 에너지 공유 프레임워크를 제안한다. 이때 중앙화된 회사나 Database(DB)에 의해 위변조를 방지하기 위해 IOTA에서는 W-OTS를 사용한다. 이를 블록체인과 분산된 복잡한 에너지 거래 및 데이터 교환의 무결성과 신뢰성 확보와 관련된 복잡한 문제를 해결하고자 한다. 스마트 컨트랙트는 에너지 공급자와 소비자 간의 미리 정의된 규칙을 기반으로 감시 가능한 다중 상대 트랜잭션을 지원하는 자동화된 스마트 컨트렉트을 가능하게 한다[3].

본 논문의 2장에서는 블록체인에 개념, 해쉬 기반 서명 기법 W-OTS 를 살펴보고, 3장에서는 본 논문의 프레임워크 시스템 모델과 work flow 다이어그램에 관한 내용을 설명한다. 4장에서는 기존에 비트코인에 서명검증인 ECDSA(Elliptic Curve Digital Signature Algorithm)과 무결성 검증을 위해 제안하는 W-OTS 내용과의 서명 알고리즘 서명 비교 내용을 다루며, 마지막 5장은 본 논문의 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 블록체인(Blockchain)의 개념

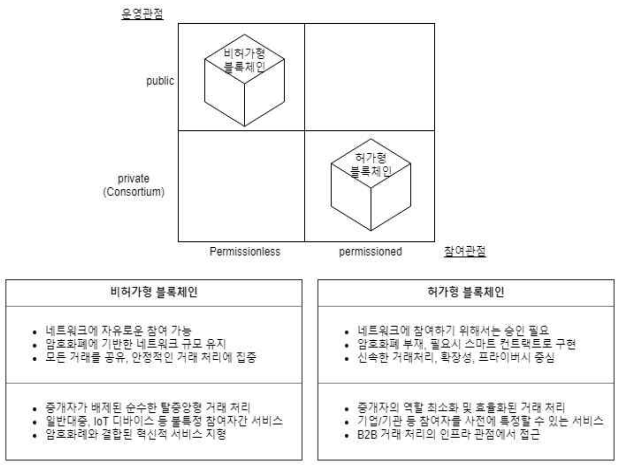

그림 1. 블록체인 유형별 특징

블록체인 기술은 변조 및 수정으로부터 보호된 블록이라고 불리는 지속적으로 증가하는 레코드 목록을 유지 관리하는 분산 데이터베이스이다. 각 블록은 타임 스탬프와 이전 블록에 대한 링크를 포함한다[5]. 스마트 컨트렉트은 가치를 교환하는 기술이나 응용프로그램으로 정의된다. 허가형(permissioned) 블록체인은 합의과정에 참여하려면 사전 승인이 필요하며, 참여자 개개인을 지정하는 프라이빗(private)블록체인과 특정 그룹 내에 사전 합의에 따라 쓰기 권한을 가지는 컨소시엄(consortium)블록체인으로 분류된다[6]. 본 논문에서는 기존 중앙화된 전력시스템에 문제점을 MG에서 허가형 블록체인으로 해결하면서 프로슈머와 소비자 간에 안전하고 데이터의 무결성이 보장되는 에너지 계량 및 청구 시스템을 단순화할 수 있는 프레임워크를 제안한다. 또한 허가형 블록체인에 트랜잭션 검증방법과 PB에 최적화된 W-OTS 기법을 비교하고 성능 측면에서의 PB 기반 에너지 공유 프레임워크의 이점을 보이고자 한다.

2.2 해쉬 기반 서명 기법 W-OTS

기존에 서명기법에 효과적인 서명 생성뿐만 아니라, 서명의 크기가 서명키, 검증키와 같이 매우크다는 단점을 보완을 위해 메시지 다이제스트값의 일부분의 비트에 대해 동시에 서명하는 방식을 사용하여, 서명키,검증키, 서명의 종합적으로 압축시켰다[7]. 분산원장에서 사용되는 Merkle의 트리 인증과 같이 사용하는게 적합하다.

이는 Merkle Signature scheme(MSS)의 크기를 확연하게 줄인다. 따라서 W-OTS는 효과적인 MSS를 가능하게 하며 센서 네트워크 및 분산원장 프로토콜에서 인증에 사용된다.

본 논문에서는 중앙화된 회사나 DB에서 참조하게 될 때 데이터 무결성을 보장하기 위해 W-OTS 방법을 통해 위변조 방지를 제안한다.

3. 제안사항

3.1 구조

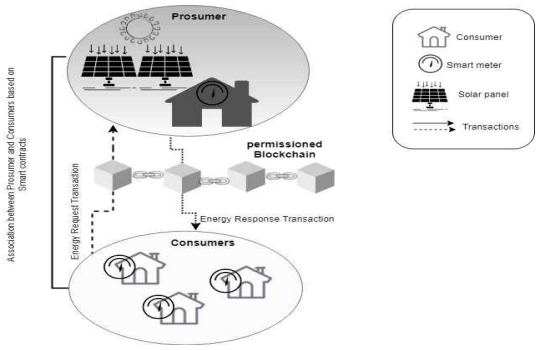

그림 2. System Model

본 논문은 그림 2과 같이 MG에서 허가형 블록체인을 활용한다. 스마트 미터 장치는 전기 에너지를 판매하고 구매할 수 있는 자동화된 에이전트 역할을 할 수 있다.

본 논문에서 제안하는 시스템 모델을 활용하여 에너지가 필요로 하는 소비자가 프로슈머에게 에너지를 요청을 하면 중개자 없이 허가형 블록체인 스마트 컨트렉트를 통하여 거래 내역이 저장이 된다. 블록이 체인에 저장되고 소비 전력을 추가 또는 제거하려면 스마트 컨트렉트을 제거하여 스마트 컨트렉트을 업데이트 해야하다[8]. 블록체인 네트워크 내의 참가자가 특정 제작자가 두 번 판매하지 않고 전기 에너지를 실제로 그리드에 주입 했는지 여부를 서로 독립적으로 확인할 수 있다.

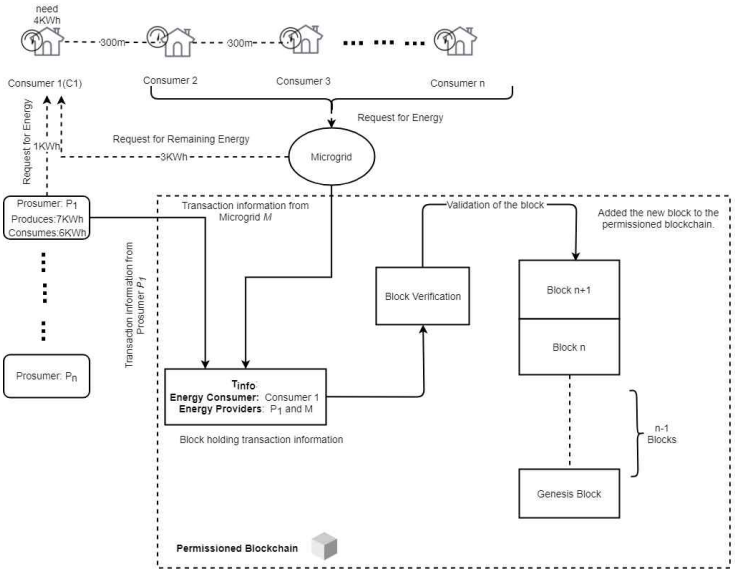

그림 3 Work-Flow Diagram

그림 3는 [8]에서 허가형 코인 기반에 스마트컨트랙트 에너지 거래를 활용하여 MG에서 PB 기반에 스마트 컨트렉트를 이용한 거래를 통해 기밀성, 무결성, 유효성을 개선한 프레임워크를 제안한다. 그림3은 Work-Flow Diagram이며, 스마트 미터는 중개자 대신에 전기 에너지를 거래할 수 있는 자동화된 Agent 역할을 한다. N개에 Smart meter 인프라가 구축된 소비자는 필요한 KWh를 독립된 분산전원으로 국소적인 전력공급 시스템인 MG[1]를 통해서 여분에 신재생 에너지 또는 태양열 에너지가 있는 프로슈머에게 요청하고 거래할 수 있다.

Micro grid Level:

① “C1” 은 “P1” 스마트 컨트랙트에 따라 4KWh를 요청한다.

② MG는 전기 라우팅 및 전력선 지원을 기반으로 트랜잭션을 수행 할 수 있는지 여부를 확인한다.

③라우팅이 유효화되면 MG는 “P1” 이 거래를 지원하는 회선 용량과 관련하여 “C1” 에게 전송할수 있게 한다.

④ MG는 거래조건을 충족 시키기 위해 MG에게 잔여 전

력을 요청한다.

⑤ 네트워크는 P1에 잔여전력 1KWh를 MG를 통해 C1에게 제공한다.

⑥ 마지막으로 , MG는 3KWh를 “C1”로 보낸다.

4. 성능 및 속성 비교

그림 4 트랜잭션 서명검증 결과 그래프

표 1 트랜잭션 서명 검증 (단위:ms)

알고리즘		구분
ECDSA		2.048
W-OTS	w=2	0.435
	w=3	0.537
	w=4	0.603

본 검증에서는 트랜잭션에 대해 검토할 때 임의의 트랜잭션에 대해 ECDSA 서명을 만들고 그 서명을 검토하는데 걸리는 시간과 Merkle 서명에 대한 서명 검증에 걸리는 시간을 서로 비교하는 실험을 하였다. 기존 시스템과 비교했을 때, 기존 블록체인 트랜잭션에 대해 검증으로는 한번만 검증하지만, W-OTS를 활용하게 되면 첫 번째 단계로 트랜잭션 서명에 대한 검증을 수행하고 2단계로 검증키와 인증 경로의 값들을 이용해 머클 트리 값을 구하여 한번 더 검증하는 방식이다. 단계적인 측면에서는 기존 블록체인이 속도 면에서 우위일것으로 예상되었으나, W-OTS기법이 4-5배 빠르게 서명에 대해서 검증한다는 사실을 확인할 수 있다. 뿐만 아니라 서명 검증 시 MSS를 이용함으로써, 기존의 ECDSA 서명 검증과는 다르게 추가로 머클 루트의 값에 대한 무결성을 검증할 수 있었다[9]. 본 논문에서는 중앙화된 기관이나 데이터베이스가 참조할 때 W-OTS 기법을 사용하여 에너지 거래 시 생기는 트랜잭션에 보다 신속하고 안전하게 무결성을 보장할 수 있음을 보였다.

5. 결론 및 향후 연구

본 논문에서는 W-OTS를 통해 PB에서 거래내역을 재참조를 할 때 발생할 수 있는 데이터의 위·변조를 막고 데이터의 무결성을 지켰다.

스마트 컨트렉트를 통해 가까운 거리 내에 있는 소비자는 MG를 통하여 프로슈머에게 원하는 에너지를 요청을 하면 안전하게 지역 내 에너지를 공유할 수 있음을 확인했다. PB 블록체인을 기반으로 하였기 때문에 소비자,프로슈머, MG 및 정부기관(KEPCO)가 데이터 공유 및 처리를 안전하게 할 수 있는 이점을 보였다.

향후 연구로는 Hybrid Blockchain(BC)를 사용하여 에너지 이중 지불과 같은 문제점을 해결하는 것을 연구할 계획이다.

ACKNOWLEDGMENT

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구입니다. (No. 70300038) *Dr. CS Hong is the corresponding author

6. 참고문헌

[1] 홍원표,(2018).최근 마이크로그리드 기술개발 동향 분석.조명・전기설비,32(6),40-52.

[2] Winter, Thomas. “The Advantages and Challenges of the Blockchain for Smart Grids.“ (2018).

[3] Sabah Suhail, Choong Seon Hong, M Ali Lodhi, Faheem Zafar, Abid Khan, and Faisal Bashir. Data trustworthiness in IoT. In Information Networking (ICOIN), 2018 International Conference on, pages 414-419. IEEE, 2018.

[4] 박찬국, 김양수,(2016).우리나라 P2P 전력거래 가능성 연구. 에너지경제연구원 수시연구보고서,1-85,2016

[5] L. Trottier, “original-bitcoin”, 2013, [Online]. Available on Github

[6] P. Franco, “Understanding Bitcoin: Cryptography, Engineering and Economics”, John Wiley & Sons. p. 9, 2014

[7] Billet, O., Robshaw, M. J., Peyrin, T. (2007, July). ” On building hash functions from multivariate quadratic equations” In Australasian Conference on Information Security and Privacy pp. 82-95.

[8] Nehai, Zeinab & Guérard, Guillaume. (2017). INTEGRATION OF THE BLOCKCHAIN IN A SMART GRID MODEL. CYSENI. 2017.

[9] 배봉진, “블록체인에 대한 해시 기반 서명 기법 적용방안”.부산대학교 대학원 석사학위논문, 2017.