

허가형 블록체인을 활용한 에너지 거래 플랫폼에서의 안전한 신용기반 거래기법의 개선된 운용방법에 관한 연구

임승주, 황동엽, 김기형

아주대학교

dlaking@ajou.ac.kr, bc8c@naver.com, kkim86@ajou.ac.kr

A Study on the Improved Operation of Safe Credit-Based Transaction in Energy Trade Platform Using the Permissioned Blockchain

SeungJoo Lim, DongYeop Hwang, Ki-Hyung Kim

Ajou Univ.

요 약

사물인터넷이 점차 널리 보급되고 신재생에너지에 대한 관심이 높아지며 기존 법제도가 완화에 따라 에너지생산주체의 다원화가 이루어지고 있다. 이러한 추세에 따라 분산된 에너지생산주체 간에 안전하게 에너지를 주고받기 위한 거래 플랫폼에 대한 필요성이 크게 대두되고 있다. 본 논문은 보안성을 높인 안전한 거래를 위해 일반적인 에너지 거래 플랫폼의 시나리오에서 허가형 블록체인을 활용함과 동시에 개선된 신용등급 평가방식을 제안하였다.

I. 서론

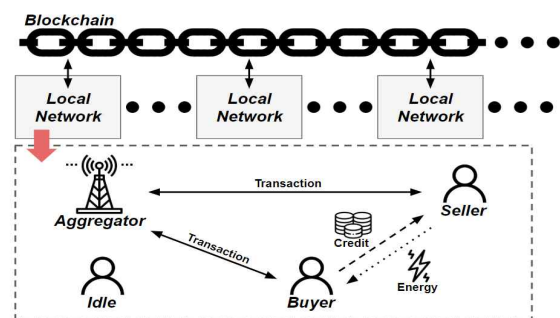
4차 산업혁명으로 인한 사물인터넷의 보편화는 기존의 중앙집중형 단방향 에너지공급방식을 분산된 양방향 에너지거래방식으로 크게 변화시키고 있다. 에너지소비자들은 각자 신재생에너지발전시설과 에너지저장장치, 스마트미터를 갖춰 소비자이자 생산자인 프로슈머로 변모하여 상호간에 에너지의 거래를 시도하며 에너지시장이란 새로운 커뮤니티의 형성을 촉발하고 있다. 이러한 움직임을 통해 기존 에너지공급자들은 일방적인 공급으로 인한 수요예측실패로부터 비교적 자유로워지고 각 소비자들은 선호에 따라 에너지공급자를 선택할 권리와 수요에 따른 에너지 구매를 통한 에너지 탄력성을 획득할 것으로 전망된다.

에너지 거래 플랫폼과 같이 분산된 노드들 간에 제3자의 개입 없이 신뢰할 수 있는 거래소를 운영하기 위해서는 2008년 Satoshi Nakamoto에 의해서 소개된 블록체인 개념을 사용하는 것이 현재 가장 효과적인 접근 방법이다.[1] 블록체인에 참여하는 노드들은 제3자의 보증 없이도 동일한 장부를 서로 공유할 수 있고, 스마트 계약을 이용하여 자동으로 사전에 정의된 계약을 체결할 수 있기 때문에 네트워크를 관장하는 기관의 개입 없이 참여하는 노드들만으로도 신뢰할 수 있는 거래소의 구현이 가능해진다.

본 논문에서는 악의적인 사용자의 거래소 참여를 제한하기 위하여 허가된 사용자만 접근이 가능한 허가형 블록체인을 사용하여 거래 플랫폼을 구현하며, 합의과정의 지연으로 인하여 발생하는 TPS(Transaction per Second)의 저하를 최소화하기 위한 기존 신용기반 거래기법[2]을 개선하여 사용한다. 본 논문에서 제안한 개선된 신용등급 평가방식은 악의적인 사용자가 입힐 수 있는 잠재적인 피해를 제한하지 않는 기존 신용기반 거래기법의 문제를 해결한다.

본 논문의 2장에서는 허가형 블록체인을 통해 구현한 에너지 거래 플랫폼의 구조에 대해 기술한다. 3장에서는 기존 신용기반 거래기법의 과정과 문제점을 기술하고, 4장에서 개선된 신용등급 평가방식을 제안한다. 마지막으로 5장에서 전체적인 내용을 결론지으며 마무리한다.

II. 허가형 블록체인기반 에너지 거래 플랫폼



[그림 1] 에너지 거래 플랫폼 구조도

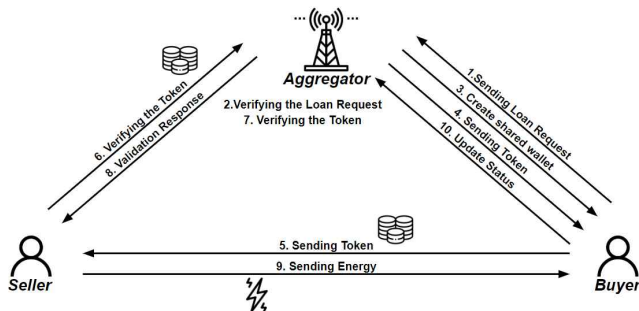
블록체인은 크게 공개형과 허가형으로 구분된다. 공개형 블록체인은 Satoshi Nakamoto가 제시한 Bitcoin이나 Vitalik Buterin이 제시한 Ethereum[3]처럼 참여하고자 하는 노드는 별도의 인증절차 없이 자유롭게 참여할 수 있기 때문에 확장성이 뛰어난 반면 악의적인 사용자의 유입을 막지 못한다는 단점이 있다. 허가형 블록체인은 IBM의 Hyperledger Fabric[4]처럼 네트워크를 관리하는 주체의 허가를 통해서만 참여할 수 있으므로 신뢰할 수 없는 노드의 유입을 제한할 수 있으나 이를 인가할 주체의 선정이 모호하고 블록체인의 탈중앙화 특성을 저해한다는 단점이 있다.

기존 신용기반 거래기법[2]에 사용된 에너지 거래 플랫폼의 구조는 [그림 1]과 같다. 에너지 거래 플랫폼에는 거래를 발생시키는 User노드와 에너지 거래를 수집하고 블록을 생성하는 Energy Aggregator(EAG)노드 두 종류의 노드가 존재한다. User노드는 에너지를 구매하고자하는 Buyer와 판매하고자하는 Seller, 거래를 발생시키지 않는 Idle의 세 가지 상태를 가질 수 있으며, 에너지를 거래하고자 하는 Buyer 또는 Seller 상태의 User노드들은 스마트 계약을 통해 EAG노드를 거쳐 거래를 수행하게 된다. EAG노드는 이때 기록한 거래를 네트워크에 전파하며 새로운 블록을 생성하는 합의과정에 참여한다. 새로운 블록의 합의과정에는 사전에 검증되어 선정된 EAG노드들만이 참여할 수 있으며, 합의 알고리즘으로

PBFT를 사용함으로써 전체 EAG노드 중 $\frac{1}{3}$ 이상의 노드에 장애가 발생하지 않는 이상 정상적으로 합의를 도출하는 것이 가능하다.[5]

따라서 허가형 블록체인을 이용해 인가된 사용자만의 접근을 허용하고 적절하게 구현된 스마트 컨트랙트를 이용해 거래를 발생시키고 검증된 합의 알고리즘을 사용함으로써 안전한 에너지 거래 플랫폼의 구현이 가능하다.

III. 신용기반 거래기법의 구조와 문제점



[그림 2] 신용기반 거래기법 구조도

블록체인은 분산된 노드들 간에 중개자 없이 신뢰성 있는 거래가 수행가능하다는 장점이 있지만, 실제로 거래가 이뤄지고 자산이 오가기까지 합의과정이 끝나길 기다려야만 한다는 단점이 존재한다. 때문에 다음 거래를 수행하기 위한 잔고가 이체되기까지는 이전 합의과정이 이뤄지는 만큼의 지연이 발생하게 되어 거래 플랫폼의 TPS가 크게 저하된다.

Zhetao Li는 위 문제를 해결하기 위해 충분한 자산 없이도 신용등급에 기반한 대출을 통해 거래를 발생시킬 수 있는 신용기반 거래기법[2]을 [그림 2]와 같이 제안하고 있다. 모든 User노드는 각자 부여된 신용등급을 갖고 EAG노드에게 대출을 신청할 수 있으며 신용등급의 높낮이에 따라 각기 다른 한도와 금리가 결정되어 대출받은 금액으로 합의과정동안 새로운 거래를 수행하는 것이 가능해져 TPS가 저하되는 문제를 해결한다.

그러나 기존 신용기반 거래기법에서는 의도적으로 대출을 상환하지 않는 User노드를 차단 목록에 추가하여 네트워크에서 완전히 배제하고 있을 뿐, 이러한 악의적인 사용자가 얼마나 큰 피해를 줄 수 있는지에 대한 제한을 걸어두지 않고 있다. 기존 신용기반 거래기법에서는 User노드가 신청한 대출이 인정받기 위한 조건을 다음과 같이 정의하고 있다 :

- 1) 계좌에 일정량 이상의 잔고가 있어야한다
- 2) 에너지 거래를 통한 일정한 수입이 있어야한다
- 3) 신용등급이 음수가 아니어야한다

그러나 악의적인 사용자가 계속해서 대출을 신청하더라도 현재 잔고와 이전 수입증명에는 영향이 없으며 신용등급은 다음의 세 가지 경우에만 변경된다 :

- 1) 대출기간 내에 상환할 경우 신용등급이 오른다
- 2) 대출기간을 초과하여 상환할 경우 신용등급이 낮아진다
- 3) 대출기간을 초과하였음에도 상환하지 아니하면 차단한다

따라서 대출기한을 넘기기 전까지 신용등급이 변하지 않기 때문에 악의적인 사용자는 일정기간 동안 대출을 무한정 받는 것이 가능하다.

IV. 개선된 신용등급 평가방식

따라서 본 논문에서는 위 문제를 해결하기 위해 개선된 신용등급 평가방식을 다음과 같이 제시한다[6] :

$$Credit\ Value = \frac{\sum_{t=0}^T (cr_t \cdot \gamma_t)}{T+1} \cdot \ln(1 + e^{-L/loanlimit})$$

위 수식을 통해 User노드의 최종 신용등급은 직전 신용등급 cr 과 감쇠

상수 γ 와의 연산의 합을 합의횟수 T 로 나눈 것에 대출받은 횟수 L 과 연산한 값으로 계산된다. 서서히 감소하게끔 사전에 정의된 감쇠상수 γ 의 곱으로 인해 합의가 진행될수록 신용등급이 낮아져 아무런 거래도 대출도 발생시키지 않는 경우에도 합의가 진행되는 동안 신용등급은 천천히 낮아지게 된다. 또한 대출을 신청하면 신청할수록 로그연산자에 의해서 신용등급이 큰 폭으로 낮아지게 되어 사전에 정의한 최대대출횟수인 $loanlimit$ 번을 초과하여 대출을 신청할 경우 반드시 신용등급이 음수가 되어 대출 신청기준을 충족시킬 수 없게 된다. 그리고 매 합의가 이뤄질 때마다 당시의 신용등급을 기록하여 과거의 신용등급이 현재 신용등급에 영향을 주기 때문에 급격한 신용등급의 변화는 불가능하다.

따라서 대출을 많이 신청할수록 신용등급이 더욱 큰 폭으로 떨어져 최대대출횟수를 초과하여 대출을 신청할 수 없게 되므로 악의적인 사용자로 인한 피해의 한계를 규정할 수 있으며, 네트워크에 성실히 참여하지 않아 기여도가 낮은 노드의 신용등급은 자연스레 낮아지게 함으로써 네트워크의 활성화 또한 유도할 수 있다.

V. 결론

본 논문에서는 허가형 블록체인을 활용하여 안전한 에너지 거래 플랫폼을 구축할 수 있음을 보이고 합의과정으로 인한 거래지연을 최소화하기 위한 신용기반 거래기법에서의 신용등급 평가방법에 대한 개선안을 제시하였다. 4차 산업혁명에 힘입어 실현가능성이 점차 커지고 있는 에너지 거래 플랫폼을 안전하고 효과적으로 구현하는 데 있어서 허가형 블록체인이 유용하게 사용될 전망이며, 신용기반 거래기법은 블록의 합의가 이뤄지기 전에도 거래를 발생시킬 수 있게 함으로써 에너지 거래 플랫폼뿐만 아니라 다른 블록체인 응용 기술에도 기여할 것으로 예상된다. 따라서 이를 검증하기 위해 IBM의 Hyperledger Fabric을 기반으로 에너지 거래 플랫폼을 구현하여 성능을 평가하고 개선할 계획이다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터 지원사업과 2018년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업의 지원과 2020년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (IITP-2020-2018-0-01396, NRF-2018R1D1A1B07048697, P0008703, 2020년 산업전문인력역량 강화사업)

참 고 문 헌

- [1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, (www.bitcoin.org)
- [2] Zhetao Li et al, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things", IEEE Transactions on Industrial Informatics, 2017
- [3] Vitalic Buterin, "Ethereum Whitepaper", 2013, (ethereum.org/en/whitepaper/)
- [4] IBM, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", EuroSys conference, 2018
- [5] Miguel Castro, Barbara Liskov, "Practical Byzantine Fault Tolerance", Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999
- [6] Zhou Su et al, "A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain", IEEE Internet of Things, 2019