2020년도 한국통신학회 하계종합학술발표회

신뢰수준 기반의 분산원장 네트워크 구성방법

최환석, 이우섭
한밭대학교

hkrock7904@gmail.com, wsrhee@hanbat.ac.kr

Trust level based distributed ledger network configuration method

Choi Hoan Suk, Rhee Woo Seop
Hanbat National University

요 약

블록체인 기술은 동일한 정보를 모든 구성원에게 분산 저장하여, 정보의 투명성 및 신뢰성을 확보할 수 있다. 하지만 블록을 추가하기 위해 모든 구성원이 합의 알고리즘을 수행해야 하기 때문에, 사물인터넷과 같은 대량, 실시간 요청을 처리하기 어렵다. 따라서 본 논문은 블록체인 네트워크에 참여하는 노드의 신뢰수준을 기반으로 기능 및 권한을 제한하여 소수의 합의 구성원으로 신뢰적 동작을 할 수 있는 신뢰수준 기반 분산원장 네트워크의 구성방법을 제안한다.

Ⅰ. 서 론

블록체인으로 대표되는 분산원장 기술은 구성원이 모두 동일한 데이터를 보유하도록 하여 데이터의 안정성 및 접근성을 향상시킨다. 하지만 네트워크의 모든 노드가 블록생성을 위한 합의 알고리즘을 수행하고, 동일한 블록을 소유해야 하기 때문에 처리속도 및 용량의 한계를 가지고 있다[1]. 따라서 최근 다양한 합의 알고리즘의 연구[2]와 노드 별로 차등적 역할을 수행하는 체인 네트워크[3]의 개발이 진행되고 있다.

선행연구인 [4]는 신뢰 관리기술을 기반으로 체인 네트워크의 구성원을 식별, 허가하여, 신뢰성 있는 구성원만 참여하는 사설 네트워크를 제안하였다. 하지만 이 또한 합의에 참여하는 노드가 증가할수록 비용 및 지연이 증가할 것이다. 따라서 본 논문은 노드의 신뢰수준을 기반으로 차등적 권한 및 기능을 수행하게 하는 신뢰수준 기반 분산원장 네트워크를 제안한다.

Ⅱ. 제안하는 신뢰수준 기반 분산원장 네트워크

제안하는 분산 네트워크는 네트워크를 구성하는 노드의 신뢰정도에 따라 역할 및 권한을 차등적으로 적용하며 그림 1과 같이 신뢰노드, 후보노드, 접근노드로 구분한다.

o **신뢰노드** (Trust Node): 충분한 신뢰를 가진 노드를 의미하며, 초기에는 네트워크의 생성을 위한 제네시스 블록을 소유하고 있는 부트노드가 신뢰노드의 구성원이 된다. 정기적 혹은 정책적으로 구성원 선출 메커니즘에 의해 후보노드 중 하나의 노드를 신뢰노드로 선출한다. 신뢰노드 그룹은 그림 1 과 같이 매시네트워크 형태로 완전히 연결되어 있으며, 새로운 블록을 추가하기 위한 합의 알고리즘을 수행한다. 또한 추가된 블록을 분산 저장하고 새로운 신뢰노드 선출을 위해 지속적으로 이웃노드로 연결된 후보노드의 신뢰관련정보를 수집한다.

o **후보노드** (Candidate Node): 접근노드중 지속적인 트랜잭션 처리를 통해 신뢰수준이 증가하여 선출된 노드이며 추후 신뢰노드 승급의 후보 자격을 가진다. 새로운 후보노드 선출을 위해 현재 후보노드는 자신과 연결된 인접 접근노드의 신뢰정보를 지속적으로 수집한다. 또한 신뢰노드 선출과 마찬가지로 구성원 선출 메커니즘에 의해 접근노드 중 하나의 노드를 후보노드로 선출한다. 선출된 후보노드는 신뢰노드로부터 전달받은 블록을 전파하여 분산 저장 및 유지한다. 또한 접근노드의 요청을 처리하기 위해 분산 저장하고 있는 블록의 읽기, 쓰기 트랜잭션을 수행한다.

o **접근노드** (Access Node): 해당 네트워크에 최초로 접속한 노드로써 블록을 직접적으로 저장할 권리를 가지지 못한다. 또한 구성원 선출의 권한이 없고, 후보노드를 통해서만 네트워크에 접근할 수 있다. 접근노드의 가장 큰 역할은 서비스에 참여하는 다양한 장치 및 사용자의 DApp(Decentralized Application)을 인증하고, 인증된 대상으로부터 생성된 데이터를 후보노드에 전달하여 간접적으로 블록 생성 및 트랜잭션 수행을 요청하는 것이다. 또한 장치나 DApp 의 요청을 처리하기 위해 후보노드에게 블록의 접근을 요청한다. 장치 및 DApp 사용자간 요청의 처리, 후보 노드와의 트랜잭션 정보를 기반으로 접근 노드의 신뢰가 측정된다.

결과적으로 하나의 서비스는 다수의 장치, DApp 과 1 개 이상의 접근노드, 후보노드, 신뢰노드를 통해 구성된 서비스 네트워크를 통해 제공된다.

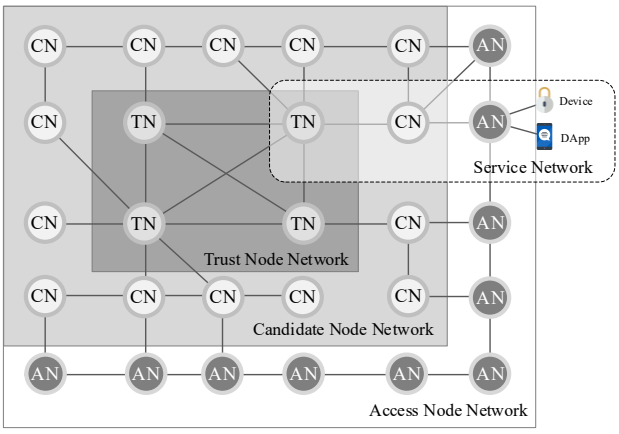

그림 1. 신뢰수준 기반 분산원장 네트워크

2.1 신뢰 계산 및 신뢰 값 전파 방법

노드 A 가 평가한 노드 B 의 신뢰 값(T_{AB})은 요청성공 여부에 따라 아래와 같이 계산한다. 노드 A 가 B 에게 전달한 요청이 성공했을 때, n 의 값을 증가시키며, T_{AB} 를 2^n 으로 계산한다. 이때 T_{AB} 의 최대값을 100 으로 한다. 만약 요청이 실패했을 경우 n 을 감소하여 T_{AB} 값을 반으로 조절한다.

IF (Req_{AtoB} = Success)	n++;
ELSE	n--;
IF (2^n >= 100)	T_{AB} = 100;
ELSE	T_{AB} = 2^n;

위와 같이 계산된 신뢰값은 노드마다 상대적이며, 네트워크의 토폴로지에 따라 다양한 노드간 신뢰값이 계산된다. 이러한 값은 그림 2 와 같은 방법으로 전파되어 최종적으로 특정 노드의 신뢰 값이 된다.

(1) 인접 노드의 신뢰를 지속적으로 계산한다.

(2) 자신이 계산한 신뢰 값을 인접 노드에게 전달한다.

(3) 다른 노드가 계산한 자신의 신뢰 값을 삭제하고, 전달받은 값 중 다른 노드가 계산한 이웃노드 신뢰값을 삭제한다. (중복될 경우 자신이 계산한 값을 선택함.)

(4) 인접하지 않은 노드의 신뢰는 타 노드(이웃노드)가 전달한 대상의 신뢰값과 그 값을 전달한 이웃노드에 대한 신뢰값의 곱으로 계산하고 브로드캐스팅 하여 전파한다. 결과적으로 모든 노드의 신뢰값을 가진다.

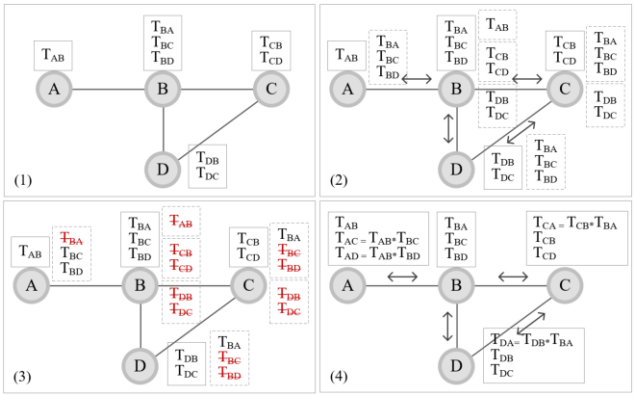

그림 2. 근접 노드의 신뢰값 전파 방법

2.2 신뢰값 기반 승급노드 선출 메커니즘

앞서 설명한대로 특정 등급으로 승급할 노드를 선출하는 것은 해당 등급의 모든 멤버가 결정한다. 예를 들어 신뢰노드로 승급할 후보노드를 선출하는 경우, 모든 신뢰노드는 그림 2 의 신뢰값 전파방법을 통해 "신뢰네트워크 + 후보네트워크" 범위의 모든 노드에 대한 신뢰값을 가진다. 승급할 새로운 노드가 필요한 경우, 그림 3 과 같은 선출 메커니즘이 동작한다. 이는 대표적 합의 알고리즘인 PBFT (Practical Byzantine Fault Tolerance)의 방식을 기반으로 한다. 먼저, 노드 승급을 요청하는 노드는 자신이 선택한 승급노드 및 수집한 모든 노드의 신뢰정보를 K-1 개의 나머지 신뢰노드에게 전달한다. 이를 전달받은 노드들은 자신의 신뢰테이블과 비교하여 가장 높은 신뢰를 갖는 노드를 각자 선택하여, 나머지 노드에게 전달한다. 각각의 노드가 승급 제안에 관한 선택을 회신하면, 모든 노드는 K-1 개의 동일한 선출결과를 수신하게 된다. 결과적으로 모든 노드는 가장 많이 득표한 노드를 동일하게 선출할 수 있다. 결과적으로 K 개의 노드로 이루어진 네트워크에서 승급노드를 선출할 때, K*(K-1) 개의 메시지가 발생하게 된다. 만약 선출결과 동일 점수를 가지고 있는 노드가 2 개 이상일 경우, 또는 전체 노드 수의 2/3 이상 추천된 노드가 존재하지 않을 경우 선출 실패로 간주하여 아무 노드도 승급하지 않는다.

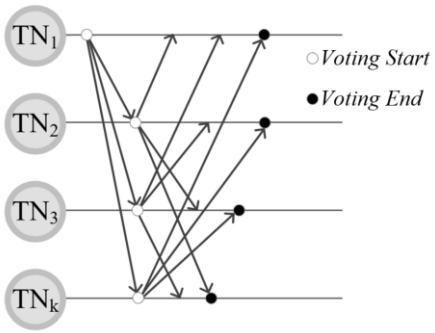

그림 3. 신뢰값 기반 승급노드 선출 메커니즘

Ⅲ. 결론

본 논문은 블록체인 기술의 필수적 요소인 합의 알고리즘의 오버헤드를 줄이기 위해 신뢰수준 기반의 분산원장 네트워크 구성방법을 제안하였다. 제안한 방법은 신뢰를 기반으로 네트워크를 구성하는 노드를 3 가지로 구분하고, 신뢰 수준에 따라 차등적인 역할 및 권한을 부여하였다. 제안하는 네트워크는 소수의 인증된 신뢰 노드간에 합의알고리즘을 수행하기 때문에 최소한의 합의시간을 소모할 것으로 생각된다. 또한 네트워크의 신뢰성 보장을 위해 모든 노드들은 인접 노드의 신뢰를 측정하여 전달하며, 측정된 신뢰를 기반으로 승급노드를 선출하는 메커니즘을 제안하였다. 새로 참여한 노드는 제안하는 메커니즘을 통해 신뢰가 증가하여 상위 수준의 네트워크 구성원으로 승급될 때까지 지속적으로 네트워크에 기여하며 전반적인 분산원장 네트워크의 신뢰를 향상시킬 것으로 기대된다. 추후 제안하는 방법의 우수성 입증을 위해 네트워크 시뮬레이터 기반의 성능분석을 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2020 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획 평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00833, 5G 기반 지능형 IoT 트러스트 인에이블러 핵심기술 연구)

참 고 문 헌

[1] Ali Dorri, Salil S. Kanhere, Raja Jurdaky and Praveen Gauravaram, "Blockchain for IoT security and privacy: The Case Study of a Smart Home," IEEE PerCom2017, March 2017.

[2] 임종철, 고남석, "세대별 블록체인 합의 알고리즘," 한국통신학회지 정보와통신, vol. 37, no. 3, pp. 3-12, Feb. 2020.

[3] Ground1, "Klaytn," https://www.klhttps://www.klaytn.com/aytn.com/

[4] H.S. Choi, G.M. Lee, W.S. Rhee, "Hierarchical Trust Chain Framework for IoT Services," IEEE ICUFN 2019, Jul. 2019.