블록체인 네트워크의 대표노드 선출 및 해임에 관한 연구

정필수*, 전우직**, 오형석**, 윤대일**, 강성원*
*한국과학기술원 전산학부
**(주)유미테크
e-mail : psjung@kaist.ac.kr

A Study on electing and dismissing delegate node of blockchain network

Pilsu Jung*, Hyeongseok Oh**, Woojik Chun**, Daeil Yune**, Sungwon Kang*
*School of Computing, KAIST
** Ubiquitous Media Technology

요 약

블록체인은 탈중앙화된 신뢰 기반 분산 데이터베이스로 높은 신뢰성과 보안성을 제공하지만 기존의 블록체인들은 확장성이 떨어진다는 문제를 지닌다. 이 문제를 해결하기 위해 기존의 방법들은 소수의 대표노드들을 선출하여 합의 과정을 간소화 하려 하였다. 그러나 이러한 시도는 대표노드를 선출하기 위해 지분 기반 투표 방식을 사용하기 때문에 많은 지분을 가진 노드들에게 권한이 집중될 수 있다는 한계를 갖는다. 본 연구는 이러한 한계점을 해결한 대표노드 선출/해임 모델을 소개한다. 제안 방법은 Raft 의 투표 알고리즘을 확장하여 대표노드의 공정한 선출과 대표노드의 부적절한 행위를 예방한다. 제안 방법은 모델 검증을 통해 도달 가능성, 안전성, 활동성이 확인되었다.

1. 서론

블록체인은 peer-to-peer 네트워크에서 전자 서명을 통해 일련의 트랜잭션을 기록하는 분산 공개 데이터베이스이다[1]. 이 기술은 기존의 리더/팔로워 아키텍처 스타일 분산데이터베이스의 중앙집권화된 관리권한을 다수의 노드에 분산시킴으로써, 관리기관에 대한 신뢰(trust) 가정 없이도 신뢰할 수 있는 데이터베이스가 유지되도록 한다. 그러나 블록체인 기술은 일련의 합의 절차로 인한 성능 저하와 전파 지연 문제로 인해, 트랜잭션의 처리속도가 느리다는 한계를 가진다. 이 문제를 개선하기 위해, Cosmos[2], EOS[3], bitshares[4] 등과 같은 여러가지 방법들이 제시되었다. 이들의 공통적으로 소수의 대표노드들을 선출하고 이들에게만 블록을 검증 및 생성할 수 있는 권한을 부여함으로써 블록 생성 및 전파 시간을 줄이려 하였다. 그러나 이들의 투표 방법은 노드의 보유 지분에 비례하여 투표 권한을 할당하기 때문에 많은 지분을 가진 노드들에게 권한이 집중될 수 있고, 오직 합의 절차를 위한 목적으로만 설계되었다는 한계를 가진다.

본 연구는 블록체인 네트워크에서 특정 노드에 권한을 집중시키지 않고 대표노드를 선출 하는 방법을 소개한다. 제안 방법은 Raft[5]를 확장하여 참여 노드에게 동등한 투표 권한을 부여함으로써 권한의 집중을 완화시킨다. 뿐만 아니라, 제안 방법은 참여 노드가 대표노드의 부적절한 행위를 감시하여 해임시킬 수 있는 기능을 통해, 대표노드의 권한 집중을 막는다. 제안 방법을 검증하기 위해, Uppaal 도구를 사용하여 모델 검증을 수행하였다. 그 결과, 도달 가능성(reachability), 안전성(safety)과 활동성(liveness) 검사에서 모든 검사 항목을 통과하였다.

2. 관련 연구

블록체인의 확장성을 개선하기 위해, Cosmos[2], EOS[3], bitshares[4]는 공통적으로 Delegated Proof-of-Stake (DPoS)를 사용한다. DPoS 는 참여 노드들 가운데 대표노드단을 구성하여 이들에게 블록을 검증하고 생성하는 권한을 위임한다. Cosmos 은 100 개, EOS 와 Steemit 은 21 개, bitshares 은 101 개의 대표노드를 선출한다. Proof-of-Stake (PoS)와 달리, 소수의 대표노드들만 합의에 참여하기 때문에 블록 검증 및 생성 비용을 상당히 절감시킬 수 있다. 그러나, 이 방법들은 노드가 가진 지분(토큰, 코인 등) 양에 비례하여 투표 권한을 부여하기 때문에 소수 노드들의 투표로 대표노드가 결정될 수 있다는 한계가 있다. 참여 노드가 대표노드를 감시하여 부적절한 행위를 막을 수 있지만, 이 기능 또한 많은 지분을 가진 노드에 권한이 집중된다. 또한, DPoS 는 블록체인의 합의 알고리즘을 위한 목적에 국한된 메커니즘이다.

이러한 한계점을 개선하기 위해, 우리는 Raft[5]의 투표 알고리즘을 확장하여 일반화된 투표 알고리즘을 제안한다. Raft 의 상세한 설명은 다음 장에서 자세히 설명한다.

3. Raft

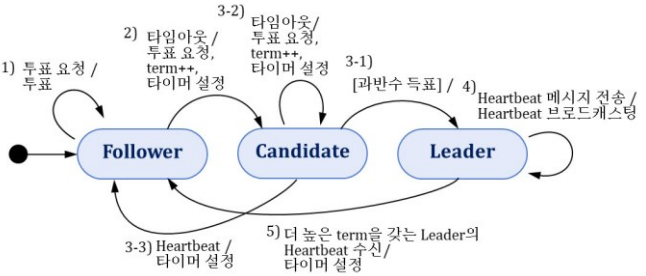
Raft 는 클라이언트의 명령을 한 클러스터의 여러 노드에서 동일하게 수행함으로써 노드들의 상태를 동일하게 관리하는 분산 합의 알고리즘이다[5]. 이 알고리즘은 노드의 결함으로 인해 발생되는 문제를 차단함으로써 안전성을 보장하기 위해 사용된다. 예를 들어, 한 노드가 결함으로 인해 잘못된 결과를 생성할 경우, 알고리즘에 의해 그 노드는 다른 노드들과 합의를 이루지 못하여 기각되고 결함이 없는 다수의 노드가 생성하는 결과로 수렴되어 최종적으로 올바른 결과를 얻게 된다.

한 클러스터의 노드들을 동일한 상태로 만들기 위해, Raft 는 클러스터의 리더 노드를 선출한다. 그림 1 은 Raft 의 리더 선출 절차를 보여주는 노드의 상태 천이 다이어그램이다. Follower 상태의 노드가 Leader 상태의 노드로 전환되는 과정은 다음과 같다:

1) 노드의 초기 상태는 Follower 이다. Follower 노드는 다른 노드들에게 투표를 요청받을 시, 즉각 투표한다.
2) Follower 노드는 Leader 노드로부터 heartbeat 메시지를 주기적으로 받는다. 그러나 Leader 노드의 문제로 인해, 타이 아웃 시간 동안 heartbeat 메시지를 받지 못하면 다른 노드들에게 투표를 요청 한 후, Candidate 상태로 전환된다. 동률 득표 확률을 줄이기 위해, 타임 아웃 시간은 임의의 값으로 설정된다[2]. 이때, 전역 변수 term 의 값을 증가시킨다.

3-1) 과반수 득표 시 Leader 상태로 전환 한다.
3-2) 투표 결과, 동률이 되거나 과반수를 득표하지 못하면 Candidate 노드는 다른 노드들에게 투표를 재요청한다.
3-3) 투표 중, 다른 노드로부터 heartbeat 메시지 수신 시, Follower 상태로 전환된다.

4) Leader 노드는 다른 노드들에게 heartbeat 메시지를 브로드캐스트한다.
5) 자신보다 더 높은 term 을 가진 노드로부터 heartbeat 메시지 수신 시, Follower 상태로 전환된다.



(그림 1) Raft 의 상태 천이 다이어그램

선출된 리더 노드는 클라이언트로부터 받은 명령들을 복제하여 다른 노드들에게 전달하고 전달받은 노드는 복제된 명령들을 동일한 순서로 수행하여 리더 노드와 동일한 상태를 유지한다. 그러나, Raft 의 투표 알고리즘은 노드간의 큰 성능 차이와 노드의 부적절한 행동 가능성을 고려하지 않기 때문에 블록체인을 위한 신뢰할 수 있는 대표노드를 선출하는데 한계가 있다. 따라서 두 기능이 추가 및 확장될 필요가 있다. 첫째, 블록체인의 대표노드는 블록체인의 기능을 대표로 수행할 수 있어야 하므로, 노드의 능력에 따라 대표노드로 선출 가능한 노드와 불가능한 노드로 구분되어야 한다. 둘째, 대포노드의 권한 집중을 완화하기 위해, 참여 노드는 대표노드를 해임할 수 있는 권한을 가져야 한다. 이들을 고려하여, 우리는 블록체인 네트워크의 대표노드 선출 및 해임 방법을 제안한다.

4. 제안 방법

이 절에서는 Raft 의 투표 알고리즘을 확장하여 블록체인을 위한 대표노드 선출 및 해임 방법을 소개한다. 그림 2 는 제안 방법의 상태 천이 다이어그램이다. Raft 와 유사하지만 다음 다섯 가지 차이점을 갖는다.

노드의 타입 및 역할. 블록체인의 참여 노드는 투표노드 또는 후보노드 중 하나를 선택할 수 있다. 투표노드는 투표 활동만 가능하지만 후보노드는 투표 활동뿐만 아니라 대표노드가 되기 위한 선거를 개시할 수 있다. 따라서 사용자는 목적에 맞게 노드의 타입 설정이 가능하다. 모든 노드는 투표를 통해 대표노드를 해임할 수 있는 권한을 갖는다. 이를 통해, 대표노드로의 권한 집중을 막는다.

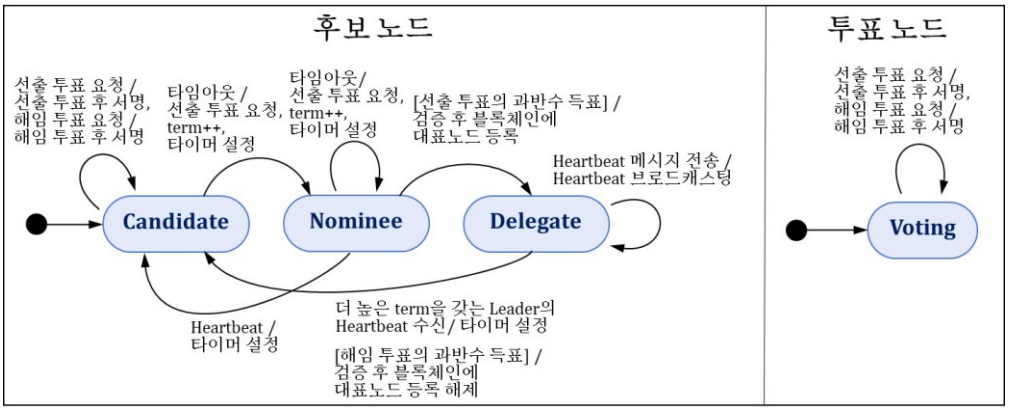
노드의 상태. Raft 는 다중 노드의 상태 동일하게 관리하기 위해 사용되는 반면, 제안 방법은 블록체인의 대표노드를 선출하기 위해 사용된다. 이러한 목적의 차이로 인해, 제안 방법은 Raft 와 다른 용어를 사용한다. Raft 는 노드의 상태를 Follower, Candidate, Leader 로 정의한다. 제안 방법은 투표 노드의 상태를 Voting 으로 정의하고, 후보 노드의 상태를 Candidate, Nominee, Delegate 로 정의한다.

메시지 유형. Raft 와 달리, 제안 방법은 두 가지 유형의 메시지를 사용한다. 첫째는 peer-to-peer (P2P) 메시지로, 두 노드 간의 통신을 위해 사용된다. 제안 방법에서 이 메시지 유형은 투표 요청/응답, 해임 요청/응답과 같이 블록체인에 등록되지 않는 활동을 위해 사용된다. 두 번째는 블록체인 메시지로, 주어진 데이터를 검증하거나 블록체인에 등록시키기 위해 사용된다. 제안 방법에서 이 메시지 유형은 투표자들의 투표 내역을 검증하고 트랜잭션을 통해 투표 내역과 결과를 블록체인에 등록하여 모든 참여 노드에게 공개하기 위해 사용된다.

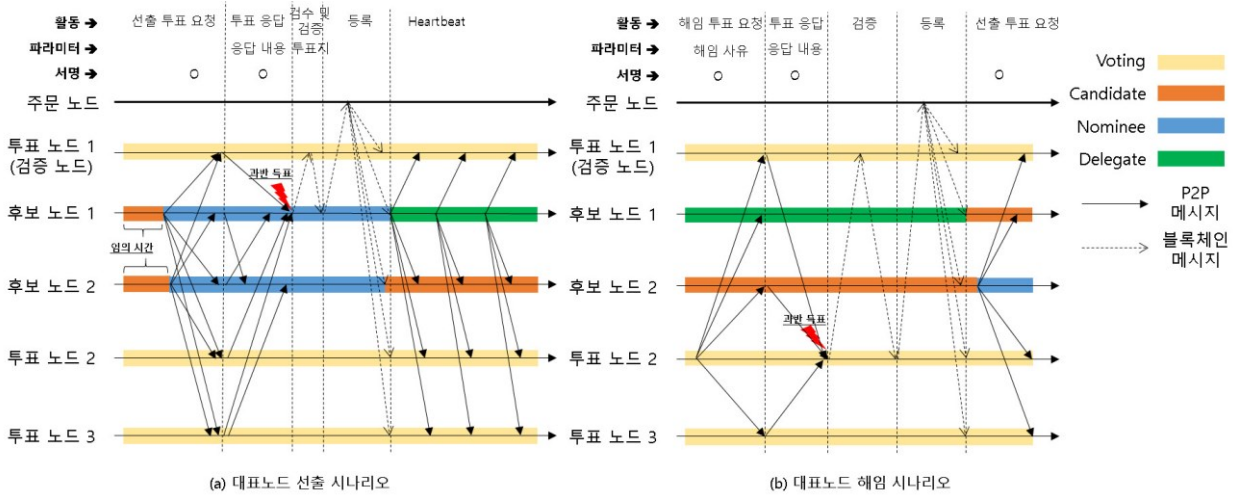
대표노드 선출 및 등록. Raft 와 같이, 대표노드는 참여 노드들의 투표를 통해 선출된다. 그러나 제안 방법은 투표자들의 신원 확인과 투표 내역을 검증하기 위해, 전자 서명을 사용한다. 서명된 투표지는 투표 권한을 소유한 투표자가 올바르게 투표했음을 증명한다. 또한 제안 방법은 대표노드가 투표를 통해

공정히 선출되었다는 사실을 공개하기 위해, 투표 내역과 결과를 블록체인에 등록(commit)한다. 이를 통해, 부정행위가 발생되지 않도록 예방할 수 있다. 선출된 대표노드는 heartbeat 메시지를 브로드캐스팅하여 대표노드가 정상적으로 동작하고 있음을 알린다.

대표노드의 해임. 모든 참여 노드는 대표노드의 부적절한 행위 또는 자격 미달 등의 사유에 대한 해임 투표를 진행할 수 있다. 해임 투표 시, 전자 서명을 통해, 투표자들의 신원과 투표 내역을 확인한다. 과반 득표 시, 대표노드는 해임되고 투표 내역과 해임 사실을 블록체인에 등록한다. 대표노드가 해임되면, 후보 노드들은 대표노드가 되기 위한 투표를 시작한다.



(그림 2) 제안 방법의 성태 천이 다이어그램



(그림 3) 제안 방법의 대표노드 선출 및 해임 시나리오

그림 3(a)는 두개의 후보노드와 세개의 투표노드가 대표노드를 선출하는 시나리오이다. 본 시나리오는 하이퍼레저 패브릭 프레임워크[6]를 기반으로 한다. 먼저, 후보노드는 임의의 시간 동안 대표노드의 heartbeat 메시지를 수신 받지 못하면 모든 노드에게 투표 요청 메시지를 서명과 함께 전송한 후, candidate 상태에서 nominee 상태로 전환한다. 그 후, 과반수를 먼저 득표한 노드는 검증 노드(endorser)에게 투표 내역을 전달하여 검증받는다. 검증 노드는 투표자의 서명과 투표지를 대조하여 투표가 올바르게 이뤄졌음을 검증한다. 검증이 완료되면 주문 노드(orderer)는 대표노드를 블록체인에 등록하기 위해 트랜잭션을 생성하고 전파하여 모든 참여 노드에게 알린다. 선출된 대표노드는 정상적으로 동작하고 있음을 알리기 위해 heartbeat 메시지를 브로드캐스트한다.

그림 3(b)는 동일한 구성에서 대표노드를 해임하는 시나리오이다. 한 참여 노드가 대표노드의 부적절한 해위를 적발한 경우, 해임 사유와 함께 해임 투표를 요청한다. 해임 투표를 요청 받은 노드들은 사유를 확인하고 서명과 **함께** 응답한다. 과반수의 노드가 동의하면 검증 노드에게 검증 받은 후, 투표가 유효하면 주문 노드를 통해 대표노드가 해임되었음을 블록체인에 등록한다. 블록체인을 통해 대표노드의 해임 사실을 알게 된 후보노드는 대표노드가 되기 위해 그림 3(a)의 대표노드 선출 시나리오를 따른다.

5. 모델 검증

제안하는 대표노드 선출 및 해임 모델을 검증하기 위해, 타임드 오토마타(timed-automata) 기반 모델 검증 자동화 도구인 Uppaal[7]을 사용하였다. 타임드 오토마타는 클럭(clock)을 사용하여 실시간 시스템의 특성을 잘 나타낼 수 있고, 잘 정의된 의미론(semantics)을 기반으로 정형검증이 가능하다[8].

Uppaal 은 계산 트리 논리(computational tree logic)을 사용하여 세 가지 속성을 검증한다. 첫째는 도달 가능성(reachability)으로, 최초 상태(initial state)로부터 특

정 상태에 도달 가능한지 검증한다. 둘째는 안전성으로, 주어진 문제가 절대로 일어나지 않는지 검증한다. 셋째는 활동성(liveness)으로, 어떤 일이 결국 발생되는지 검증한다. 계산 트리 논리는 총 5 가지 연산을 제공한다. A[]는 “모든 경로에서 항상”, A<>는 “모든 경로에서 결국”, E[]는 “어떤 경로에서 항상”, E<>는 “어떤 경로에서 결국”, □→ψ 는 “식 □ 가 만족하면 결국 식 ψ를 만족한다는 것을 의미한다.

표 1 은 3 개의 후보노드와 2 개의 투표노드를 통해 제안 방법의 모델을 검증하는 9 개의 핵심 질의문을 보여준다. N 은 노드 수, CNode1, CNode2, CNode3 은 후보노드, VNode1, VNode2 는 투표노드, EVotes 는 각 노드가 대표노드가 되기 위한 득표 수, DVotes 는 대표노드에 대한 해임 득표 수이다. 제안 방법은 대표노드 선출 및 해임에 관해 지켜져야 할 핵심 질의문을 모두 통과하였다. 이는 제안 방법의 대표노드 선출 및 해임에 관한 주요 원칙들이 문제 없이 지켜진다는 것을 의미한다. 제안 방법의 모델 및 검증 결과는 https://github.com/psjung/BCVotingSystem 링크의 ModelChecking.xml 파일에서 상세히 확인할 수 있다.

<표 1> 제안 모델의 검증 항목 리스트

검증 속성	질의문(query)	검증 내용
도달 가능성	E<> CNode1.Delegate or CNode2.Delegate or CNode3.Delegate	후보노드는 Delegate 상태가 될 수 있다.
	E<> CNode1.Delegate or CNode2.Delegate or CNode3.Delegate and DVotes>=N/2+1	Delegate 상태의 노드는 해임 투표 결과 과반수를 득표할 수 있다.
	E<> (CNode1.Nominee and EVotes[0]>=N/2+1) or (CNode2.Nominee and EVotes[1]>=N/2+1) or (CNode3.Nominee and EVotes[2]>=N/2+1)	Nominee 상태의 노드는 대표노드 선출 투표 결과 과반수의 득표할 수 있다.
	E<> CNode1.Nominee and CNode2.Nominee and CNode3.Nominee	모든 후보노드는 함께 Nominee 상태가 될 수 있다.
활동성	A<> (CNode1.Delegate + CNode2.Delegate + CNode3.Delegate >= 2) imply (CNode1.Delegate + CNode2.Delegate + CNode3.Delegate == 1)	2 개 이상의 대표노드가 존재할 시, 결국 1 개의 대표노드로 줄어든다.
	A<> numFail<N/2 and CNode1.Nominee imply CNode1.Delegate	반 이상의 노드가 failure 되지 않는 이상 대표노드는 뽑힌다.
안전성	A[] forall(i:int[0,N-1]) (EVotes[i]>=0 and EVotes[i]<=N)	대표노드 선출 시, 모든 노드는 노드 수 이상 득표할 수 없다.
	A[] forall(i:int[0,N-1]) (DVotes[i]>=0 and DVotes[i]<=N)	대표노드 해임 시, 모든 노드는 노드 수 이상 득표할 수 없다.
	A[] not deadlock	데드락이 발생되지 않는다.

6. 결론

본 연구는 블록체인 네트워크의 대표노드를 선출하고 해임하는 방법을 소개하였다. 제안 방법은 Raft 의 투표 알고리즘을 확장하여 블록체인의 각 참여 노드에게 동등한 투표 권한을 부여하고 해임 절차를 통해 대표노드의 권한을 분산시킴으로써 기존 연구에서 사용하는 투표 절차의 한계를 완화하였다.

향후 연구에는 본 대표노드 선출 및 해임 모델을 이용하여 블록체인의 확장성 문제를 월등히 개선할 수 있는 계층적 블록체인 아키텍처를 설계할 계획이다. 그 후, 계층적 블록체인 아키텍처의 확장성을 기존 방법들과 비교하여 우수성을 보일 계획이다.

Acknowledgement

본 논문은 2019 년도 과학기술정보통신부의 재원으로 정보통신기획평가원 블록체인 융합기술 개발사업의 지원을 받아 수행된 연구 결과입니다. [과제번호: 2019-0-00132 / 과제명:재귀적 구조화를 통한 블록체인 저지연 네트워킹 기술]

참고문헌

[1] Tapscott, D., Tapscott, A., 2016. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.

[2] Kwon, J., Buchman, E., Cosmos: A network of distributed ledgers. White Paper. 2017. https://cosmos.network/whitepaper

[3] Cox, T. EOS.IO Technical White Paper. 2017. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[4] Schuh, F., Larimer, D., 2017. Bitshares 2.0: General overview. https://bitshares.org.

[5] Ongaro, D., Ousterhout, J., 2014. In search of an understandable consensus algorithm. In 2014 {USENIX} Annual Technical Conference, pp. 305-319.

[6] Cachin, C., 2016. Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers, 310, p. 4.

[7] Larsen, K. G., Pettersson, P., Yi, W., 1997. UPPAAL in a nutshell. International Journal on Software Tools for Technology Transfer (STTT), 1(1), pp. 134-152.

[8] Alur, R. and Dill, D. L., 1994. A theory of timed automata. Theoretical Computer Science, Vol. 126, pp.183-235.