정 보 보 호 학 회 지
제28권 제3호, 2018. 6

블록체인 연구 동향 분석: 합의 알고리즘을 중심으로

이 대 화*, 김 형 식**

요 약

블록체인의 특징인 신뢰성, 보안성, 투명성, 탈중앙성을 지지하는 합의 알고리즘을 환경과 목표에 따라 적절하게 선택하는 것이 매우 중요하다. 본 논문에서는 합의 알고리즘에 대한 연구 동향을 파악하기 위해 블록체인을 참여 대상에 따라 퍼블릭 블록체인과 프라이빗 블록체인으로 나누어 설명하였고 체인 유지 방식에 따라 경쟁 방식 합의 알고리즘과 비경쟁 방식 합의 알고리즘으로 나누어 설명하였으며, 이를 위해 다섯가지 합의 알고리즘의 원리와 장단점 등을 분석하였다. 그리고 분석 결과를 바탕으로 참여 대상과 체인 유지 방식간의 관계와 신뢰모델과 중앙화, 속도, 보안성간의 관계를 도출해내었다. 향후에는 현재의 여러 합의 알고리즘 원리와 장단점을 발전 및 보완하여 환경과 목적에 따라 속도가 빠르고 보안적으로 안전하며 일관된 블록체인을 유지하는 합의 알고리즘을 개발할 수 있을 것이다.

Ⅰ. 서 론

2008년 나카모토 사토시는 논문 “Bitcoin: A peer-to-peer electronic cash system”[1]에서 전자 결제를 처리할 제 3자의 역할을 금융기관에 의존하는 것이 대다수 거래에서는 잘 동작하지만, 완전한 철회 불가 거래가 가능하지 않다는 점을 통해 신뢰 기반 모델이 태생적 약점을 극복하지 못하였다고 판단하였다. 그래서 그는 신뢰를 대신하기 위하여, 제 3자의 역할이 필요없는 P2P 전자 화폐 시스템을 구현하였고 이를 위해 1991년 미국 벨코어 연구소의 스튜어트 하버가 처음 구상한 블록체인을 발전시켜 도입하였다.

블록체인 시스템은 모든 거래 정보를 모든 참여자가 함께 복사하여 공유하는 분산 원장 시스템으로 자료의 분배와 공유, 암호학, 합의 알고리즘 등 다양한 기술의 집약체이다. 블록체인 시스템을 적용하기 위해서는 이중 지불 문제와 비잔틴 장군 문제를 해결해야 한다. 이중 지불 문제는 동시에 두 거래에서 통화를 재사용하는 문제이며 비잔틴 장군 문제는 분산 시스템에서 정직하지 못한 노드가 있음에도 다수의 정직한 노드에 의해 시스템이 정상적으로 작동하기 위해 어떤 규칙에 의해 의사결정을 할지 정하는 문제이다. 이 두가지 문제를 해결하여 다수의 참여자가 하나의 일관된 합의된 블록체인을 유지하기 위해 만든 것이 합의 알고리즘이다.

따라서 본 논문에서는 대표적인 다섯가지 합의 알고리즘의 원리와 장단점을 분석하고 중앙화, 속도, 보안성 등 몇가지 기준을 통해 비교하였다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 참여 대상에 따라 블록체인과 체인 유지 방식에 합의 알고리즘을 분류하여 설명하고, Ⅲ장에서는 이를 위해 PoW 합의 알고리즘, PoS 합의 알고리즘, DPoS 합의 알고리즘, PBFT 합의 알고리즘, Ripple 합의 알고리즘의 원리와 장단점에 대해 분석하며, Ⅳ장에서 합의 알고리즘을 몇가지 기준에 따라 비교하고, Ⅴ장에서 본 논문에 대한 결론을 도출할 것이다.

Ⅱ. 블록체인 및 합의 알고리즘 분류

블록체인은 참여하는 대상에 따라 퍼블릭 블록체인과 프라이빗 블록체인을 구성할 수 있고, 체인을 유지하는 방식에 따라 경쟁 방식 합의 알고리즘과 비경쟁 방식 합의 알고리즘으로 구성할 수도 있다. 합의 알고리즘 선택에 따라 다양한 결과를 만들기 때문에 블록체인의 환경과 목적에 따라 기존의 알고리즘을 그대로 혹은 발전시켜 사용하거나 기존과 다른 완전히 새로운 알고리즘을 만들어 사용하기도 한다.

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터 (2015-0-00914) 지원 및 성균관대학교 보안공학연구소 관리로 수행되었습니다.
* 성균관대학교 전자전기컴퓨터학과 보안공학연구실 (dhwa1206@skku.edu)
** 교신저자, 성균관대학교 전자전기컴퓨터학과 보안공학연구실 (hyoung@skku.edu)

2.1. 참여 대상에 따른 블록체인 분류

2.1.1. 퍼블릭 블록체인

퍼블릭 블록체인은 누구나 자유롭게 블록체인 네트워크에 참여할 수 있는 블록체인이다. 운영과 참여의 주체가 불분명하기 때문에 인센티브 제도인 코인을 발행하여 운영한다.

많은 사람들이 함께 참여하기 때문에 투명성이 강화된 모델이며, 많은 사람들이 네트워크에 참여할수록 보안이 강화된다는 장점이 있다. 하지만 많은 사람들에 의해 합의가 진행되고 전체 네트워크에 전파하여 동기화해야하기 때문에 속도가 느리다는 단점이 있다.

퍼블릭 블록체인에서는 PoW 합의 알고리즘, PoS 합의 알고리즘, DPoS 합의 알고리즘이 적합하다.

2.1.2. 프라이빗 블록체인

프라이빗 블록체인은 법적 책임을 지는 허가받은 사람만 블록체인 네트워크에 참여할 수 있는 블록체인이다. 운영과 참여의 주체가 분명하기 때문에 인센티브 제도인 코인을 발행하여 운영하지 않아도 된다.

허가받은 소수의 사람들이 참여하기 때문에 기밀성이 강화된 모델이며, 신뢰할 수 있는 사람들만 함께하여 트랜잭션 속도가 빨라진다는 장점이 있다. 하지만 적은 사람들에 의해 합의가 진행되기 때문에 일부 중앙화가 되어 보안성이 낮아질 수 있다는 단점이 있다.

프라이빗 블록체인에서는 PBFT 합의 알고리즘, Ripple 합의 알고리즘이 적합하다.

2.2. 체인 유지 방식에 따른 합의 알고리즘 분류

2.2.1. 경쟁 방식

경쟁 방식은 Finality가 보장되지 않고 동시에 여러 곳에서 서로 다른 합의를 진행하여, 특정 조건을 먼저 만족하는 단 하나의 합의만을 수용함으로써 체인의 단일성을 유지한다.

이 방식의 경우 모두가 증명에 참여하지 않아도 되기 때문에 악의적으로 참여하지 않거나 반대하는 문제를 해결했다는 장점이 있다. 하지만 포크가 발생하기 때문에 이중지불의 가능성이 있고, 발생한 포크에서 선택받지 못한 보조 체인의 경우 그동안 마이닝에서 사용했던 모든 리소스가 무효화되어 결과적으로 낭비된다는 단점이 있다.

경쟁 방식에서는 PoW 합의 알고리즘, PoS 합의 알고리즘, DPoS 합의 알고리즘이 적합하다.

2.2.2. 비경쟁 방식

비경쟁 방식은 Finality가 보장되고 한번에 하나의 합의만을 진행하며, 많은 사람들이 투표 등의 방식으로 진행함으로써 체인의 단일성을 유지한다.

하나의 체인만을 진행하기 때문에 리소스를 낭비하지 않는다는 장점이 있다. 하지만 2/3 이상이 동의해야 하는 방식에서 1/3이 투표를 진행하지 않거나 악의로 투표를 망친다면 시스템이 무너질 수 있다는 문제점이 있으며 마스터 노드 혹은 리더 노드의 컨트롤을 받아 투표를 진행하게 되기 때문에 중앙화의 단점이 있다.

비경쟁 방식에서는 PBFT 합의 알고리즘, Ripple 합의 알고리즘이 적합하다.

Ⅲ. 합의 알고리즘 분석

알고리즘 선택에 도움을 주기 위하여 현재 다수의 블록체인에서 많이 사용되고 있는 PoW 합의 알고리즘, PoS 합의 알고리즘, DPoS 합의 알고리즘, PBFT 합의 알고리즘, Ripple 합의 알고리즘까지 5종의 다양한 합의 알고리즘의 원리와 장단점에 대한 분석 및 비교를 진행하였다.

3.1. PoW 합의 알고리즘

PoW 합의 알고리즘은 새로 증명할 블록 헤더[표 1]를 SHA256 알고리즘을 통해 해시값을 구하여 nBits에서 정한 숫자보다 작은 숫자가 나올 때까지 Nonce를 1씩 증가시킨다. 이 때, nBits에서 정한 숫자보다 작은 숫자가 나올 때까지 Nonce를 1씩 증가시키는 작업을 Mining, 작업자를 Miner라고 부른다. PoW 합의 알고리즘은 CPU 혹은 GPU 의 해싱 파워를 요구하며 평균 작업은 요구되는 제로 비트 수의 지수함수로 이루어진다.

시간이 지나면서 더 큰 네트워크를 구성할수록 안정성과 안전성이 증가하며, 간단한 구조로 누구나 구성하기 쉽다는 장점이 있다. 하지만 해싱 파워를 이용하기 때문에 51%의 해싱 파워를 보유하면 네트워크 전체 합의를 좌우할 수 있는 51% 공격이 가능[9]하며, 불필요하게 많은 양의 컴퓨터 자원을 사용한다는 단점이 있다.

현재 비트코인, 라이트코인, 제트캐시, 모네로 등의 합의 알고리즘으로 사용되고 있다.

〔표 1〕 비트코인 블록 헤더

이름	설명
Version	소프트웨어 및 프로토콜 정보
Merkle root hash	개별 트랜잭션 해시로 구성한 2진 트리의 루트 트리
Time	블록 생성 시간
Previous block header hash	이전 블록의 해시값
nBits	작업의 난이도를 조절
Nonce	0부터 시작하여 1 씩 증가하는 숫자

3.2. PoS 합의 알고리즘

PoS 합의 알고리즘은 자신이 보유한 지분만큼 증명에 참여하여 신규 블록을 생성한다. 다시 말해 여러 블록 후보 중 합당하고 생각하는 블록에 대해 자신이 보유한 지분만큼 투표를 하고 그 블록이 최종적으로 많은 투표를 받아 정식 블록으로 등록된다면 자신이 투표한 만큼 새 블록의 보상을 받는 방식이다. 따라서 제안자들은 블록 생성자와 지분 보유자의 이해 관계를 일치함을 통해 나쁜 의도로 블록을 생성할 동기를 없애고자 하였으며, PoS 합의 알고리즘에서는 PoW 합의 알고리즘의 Miner 대신 Validator, Mining 대신 Minting 이라는 표현을 사용한다.

해시값을 구하지 않고 투표를 함으로써 불필요하게 많은 양의 컴퓨터 자원을 낭비하는 문제를 해결하였으며, 해싱 파워가 아닌 지분을 사용하기 때문에 51% 공격을 훨씬 힘들게 했다는 장점이 있다. 하지만 지분이 많을수록 더 많은 증명을 할 수 있기 때문에, 은행의 이자와 비슷하여 시장에 유통되지 않을 수 있으며, 여러 곳에 동시에 투표하여 투표의 공정성을 해치는 Nothing at Stake 문제가 발생한다는 단점이 있다.

현재 퀀텀[2], 스트라티스[3] 등의 합의 알고리즘으로 사용되고 있다.

3.3. DPoS 합의 알고리즘

DPoS 합의 알고리즘은 투표를 통해 증인 혹은 대표자를 선출하여 그들로 하여금 PoS 합의 알고리즘을 진행하도록 한다. 대표자가 되고 싶은 후보자는 자신의 공개키를 네트워크에 공약과 함께 등록하고, 투표자는 지갑에 포함된 투표 권한을 통해 자신의 지분만큼 표를 받아 대표자에게 투표한다. 만약 임명받은 대표자들이 Nothing at Stake 와 같은 행위를 통해 부당 이익을 챙기고자 한다면 그 즉시 투표자들은 투표를 진행하여 새로운 대표자를 선출할 수 있다.

일반적인 PoS 합의 알고리즘을 지분 가진 사람들에 의해 이루어지는 직접 민주주의라고 본다면 DPoS 는 지분 가진 사람들 중 일부 대표자를 선출하여 이루어지는 간접 민주주의라 할 수 있다. 스팀[4]의 경우 현재 20명, 이오스[5]의 경우 동률을 막기위해 홀수인 21명 선출하여 진행하기 때문에 빠르며, Nothing at Stake 문제를 해결했다는 장점이 있다. 하지만 거래소와 같이 많은 지분을 보유한 곳이 투표권을 남용하여 자신들에게 유리한 대표자를 선출할 수도 있으며, 일부 중앙화로 보안성 및 투명성이 위협받을 수 있다는 단점이 있다.

현재 이오스, 스팀, 비트쉐어 등의 합의 알고리즘으로 사용되고 있다.

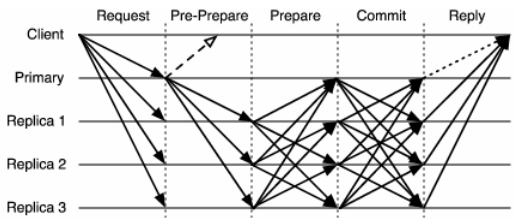
3.4. PBFT 합의 알고리즘

PBFT 합의 알고리즘은 선출된 하나의 리더 노드가 검증 노드를 이용하여 타당하다고 검증된 거래를 수신하여, 합의 요청을 모두에게 전파하고 2/3 표를 획득하여 블록을 생성한다. PBFT 합의 알고리즘은 일부 비정상 노드가 존재하더라도 정상 작동하도록 하는 분산 시스템의 BFT 알고리즘을 발전시켜서, 비동기식 네트워크에서도 사용가능하도록 하였다. 또한 PBFT 에서는 전체 네트워크로 전파하여 투표하는 두번의 브로드 캐스팅 과정을 통해 더 높은 확률로 리더나 검증 노드가 이상한 노드를 보다 정확하게 제거하였다[그림 1].

이미 검증된 거래를 수신하여 진행하기 때문에 보다

〔표 2〕 합의 알고리즘 비교

	PoW	PoS	DPoS	PBFT	Ripple
블록체인 타입	퍼블릭 블록체인	퍼블릭 블록체인	퍼블릭 블록체인	프라이빗 블록체인	프라이빗 블록체인
토큰 필요성	필요	필요	필요	불필요	불필요(사용)
체인 유지 방식	경쟁 방식	경쟁 방식	경쟁 방식	비경쟁 방식	비경쟁 방식
신뢰 모델	비신뢰	비신뢰	신뢰	신뢰	신뢰
중앙화	탈중앙화	탈중앙화	중앙화	중앙화	중앙화
트랜잭션 속도	10분 x 6컨펌	12초 x 100컨펌	1,5초 x 30컨펌	5초	2~10초
보안성	높음	높음	낮음	낮음	낮음
사용처	비트코인, 라이트코인, 모네로	퀀텀, 스트라티스	이오스, 스팀, 비트쉐어	하이퍼 레져 페브릭	리플



〔그림 1〕 PBFT 합의 알고리즘의 동작 방식[8].

신뢰할 수 있으며, 동시에 비동기적으로 여러 투표를 진행하기 때문에 빠르다는 장점이 있다. 하지만 확장이 어려운 구성이며, 33%의 노드가 투표를 진행하지 않거나 의도하여 반대만한다면 시스템이 정지될 수 있다는 단점이 있다[6].

현재 IBM의 하이퍼 레져 페브릭의 합의 알고리즘으로 사용되고 있다.

3.5. Ripple 합의 알고리즘

Ripple 합의 알고리즘은 네트워크 검증 서버에 의해 실행되는 비동기 라운드 기반 프로토콜로 수집 단계, 합의 단계, 마감 단계로 구성되어 진행된다. 수집 단계에서는 검증서버가 네트워크로부터 트랜잭션을 수신하여 서명의 유효성과 관련 정보의 정확성을 검사하고 제안서를 다시 네트워크에 후보 집합으로 브로드 캐스팅한다. 합의 단계에서는 서버들이 전달 받은 제안서에 대해 투표를 진행하여 합의한다. 마감 단계에서는 제안서가 80% 이상의 동의를 얻으면 제안서를 후보 집합에서 제거하여 원장에 정식으로 등록되며 한 라운드가 마감된다.

Ripple 합의 알고리즘은 실시간 결제 시스템을 목표로 대량의 결제를 빠르게 처리하는 것을 목표로 하며, 주로 은행간 이체 서비스를 중점으로 서비스하는 목적으로 만들어졌기 때문에 속도의 중심을 두어 개발하여 빠른 속도가 장점이다. 그러나 아주 큰 중앙화를 통해 빠른 속도를 구축했으며, 20% 의 노드가 투표를 진행하지 않거나 의도하여 반대만한다면 시스템이 정지될 수 있다는 단점이 있다[7].

현재 리플의 합의 알고리즘으로 사용되고 있다.

Ⅳ. 합의 알고리즘 비교

여러 합의 알고리즘의 장단점을 비교한 만든 합의 알고리즘 비교 표[표 2][10][11]는 다음과 같은 의미를 가지고 있다.

블록체인 타입은 참여하는 대상에 따라 퍼블릭 블록체인과 프라이빗 블록체인으로 나뉜다. 토큰 필요성은 블록체인 타입에 따라 퍼블릭 블록체인은 인센티브로 토큰이 필요하고 프라이빗 블록체인은 필요하지 않다. 그러나 코인 이코노미를 목적으로 사용할 수도 있다. 체인 유지 방식은 Finality가 보장되지 않는 비경쟁 방식과 보장되는 경쟁 방식으로 나뉜다. 신뢰 모델은 합의에 참여하는 노드가 알려지거나 신뢰되는지에 따라 신뢰 모델과 비신뢰 모델로 나뉜다. DPoS 합의 알고리즘은 투표를 통해 선출된 투표자를 알고 있으며 신뢰할 수 있

기 때문에 PoS 합의 알고리즘에서 시작했더라도 신뢰 모델로 분류하였다. 중앙화는 신뢰 모델에 따라 결정된다. 트랜잭션 속도는 각 합의 알고리즘이 트랜잭션을 검증하여 새로운 블록을 생성하는데 걸리는 시간을 의미한다. 그러나 일반적으로 중앙화 정도와 비례하여 속도는 향상된다. 보안성은 해킹에 안전한 정도를 의미한다. 공격의 목표가 되는 장애점이 적어질수록 보안이 취약하다고 할 수 있다. 일반적으로 중앙화 정도와 반비례하여 보안성은 저하된다.

비교 결과 퍼블릭 블록체인은 토큰을 필요로 하며, 경쟁 방식을 통해 체인을 유지하고, 프라이빗 블록체인은 토큰을 필요로 하지 않지만 코인 이코노미를 목적으로 사용할 수 있으며, 비경쟁 방식을 통해 체인을 유지한다는 것을 알 수 있었다. 또한 신뢰모델은 중앙화를 이루어 속도가 향상된다는 장점이 있지만 장애점을 적게 가짐으로써 보안성은 저하된다는 단점이 있고, 비신뢰모델은 탈중앙화를 이루어 장애점을 많이 가짐으로써 보안성이 향상된다는 장점이 있지만 속도가 저하된다는 단점이 있다는 것을 알 수 있었다.

Ⅴ. 결 론

본 논문에서는 이중 지불 문제와 비잔틴 장군 문제를 해결하고 다수의 참여자가 하나의 일관된 블록체인을 유지하기 위해 만든 여러 합의 알고리즘의 원리와 장단점을 분석 및 비교하였다. 향후에는 현재 여러 합의 알고리즘의 원리와 장단점을 고려하여 환경과 목적에 따라 보다 속도가 빠르고 보안적으로 안전하게 일관된 블록체인을 유지하는 합의 알고리즘의 개발이 요구된다.

참 고 문 헌

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf Accessed: 2018-05-01.

[2] Qtum Foundation, "Qtum Technical WhitePaper", https://qtum.org/wp-content/uploads/2017/01/Qtum-technical-white-paper-draft-version.pdf, Accessed: 2018-05-01.

[3] Chris Trew, Guy Brandon and Nicolas Dorier, "Stratis White Paper", https://stratisplatform.com/files/Stratis_Whitepaper.pdf Accessed: 2018-05-01.

[4] "Steem White Paper", https://steem.io/steem-whitepaper.pdf Accessed: 2018-05-01.

[5] "EOS Technical White Paper", https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md Accessed: 2018-05-01.

[6] "Hyperledger Consensus", https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf Accessed: 2018-05-01.

[7] "Ripple Consensus White Paper", https://ripple.com/files/ripple_consensus_ whitepaper.pdf Accessed: 2018-05-01.

[8] Miguel Castro and Barbara Liskov, "Practical Byzantine Fault Tolerance", Third Symposium on Operating Systems Design and Implementation, pp. 173-186, 1999.02.

[9] Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, Srdjan Capkun, "On the Security and Performance of Proof of Work Blockchains", 2016, ACM SIGSAC Conference on Computer and Communications Security, pp. 3-16, 2016.10.

[10] C. Dwork, N. Lynch, L. Stockmeyer, “Consensus in the presence of partial synchrony,” Journal of the ACM, vol. 35, no. 2, pp. 288-323, 1988.

[11] M. J. Fischer, N. A. Lynch, M. S. Paterson, “Impossibility of distributed consensus with one faulty process,” Journal of the ACM, vol. 32, no. 2, pp. 374-382, 1985.

〈저 자 소 개〉

이 대 화 (Daehwa Rayer Lee)
학생회원

2017년 8월 : 용인대학교 컴퓨터과학과 학사
2018년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : Blockchain, Security Engineering, Usable Security

김 형 식 (Hyoungshick Kim)
종신회원

1999년 2월 : 성균관대학교 정보공학부 학사
2001년 2월 : KAIST 컴퓨터 과학과 석사
2012년 2월 : University of Cambridge 컴퓨터공학과 박사
2013년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 조교수
관심분야 : Security Engineering, Usable Security. Social Computing