아이리포 지식창고

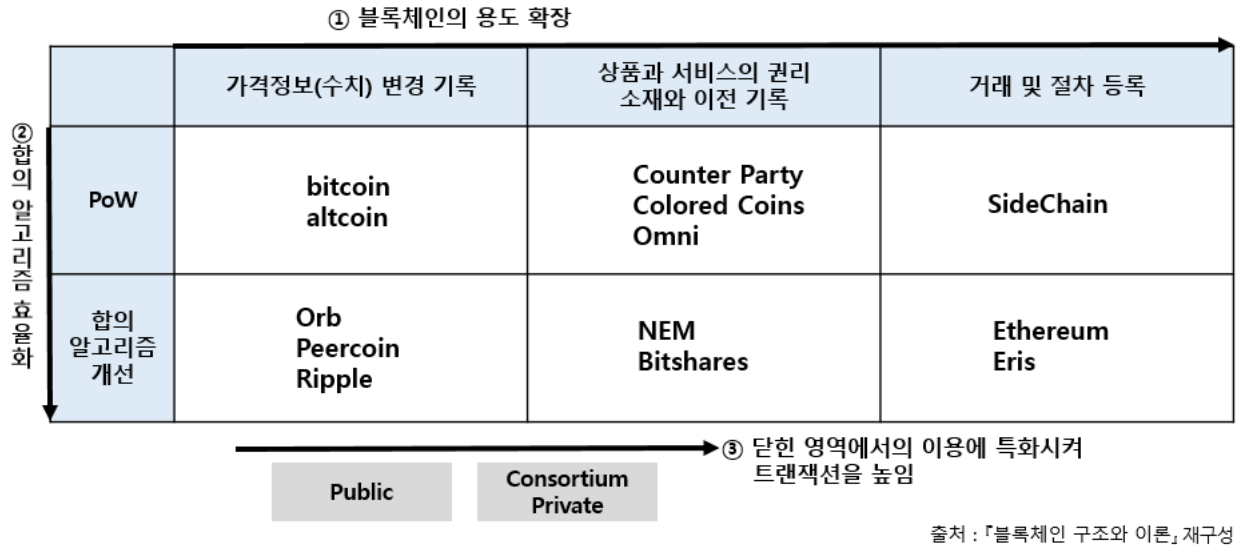
기출심화 - 01 블록체인 합의알고리즘

양경주 정보관리기술사
(kjyang75@gmail.com)

블록체인의 핵심기술, 합의 알고리즘	
Concept	**(블록체인 정의)** - 제3의 공인기관이나 중개자 개입 없이 투명하고 안전한 거래를 가능하게 하는 분산되고, 개방된 공동장부 관리 기술 **(합의 알고리즘 정의)** - P2P 네트워크와 같이 정보 도달에 시간차가 있는 네트워크에서 참가자가 하나의 결과에 대한 합의를 얻기 위한 알고리즘
KeyWord	PoW, PoS, PBFT, Sieve

변화하는 블록체인!

비트코인이라는 가상화폐를 통해 세상에 이름을 알리기 시작한 블록체인은 금융 분야뿐 만 아니라 부동산 등기, 온라인 콘텐츠, 전자투표 등 다양한 분야에서 적용가능성을 검토하며 4 차 산업혁명에서의 핵심기술로 기대되고 있다. 비트코인이나 이더리움 같이 누구나 참여 가능한 Public 형태로 시작한 블록체인은 탈 중개 등의 경제성, 위조가 불가능한 높은 보안성 등으로 **금융권 및 다양한 기업에서 관심을 보이며 R3Cev, Hyperledger Consortium 을 필두로 허가된 사람만 참여 가능한 독자적 블록체인(Consortium 혹은 Private)을 구축하고 있다**.



[그림 1] 블록체인 적용 동향

본고에서는 분산 시스템에서 신뢰성을 보장하기 위해 필요한 핵심 기술인 합의 알고리즘을 살펴보고자 한다.

I. 합의 알고리즘

가. 합의 알고리즘의 정의

- P2P 네트워크와 같이 정보 도달에 시간차가 있는 네트워크에서 참가자가 하나의 결과에 대한 합의를 얻기 위한 알고리즘

나. 대표적인 합의 알고리즘과 채택 시스템

합의 알고리즘	채택 시스템
Proof of Work	- Bitcoin Core, Ethereum 등
Proof of Stake	- Ethereum mijin
Paxos	- Google Chubby
Raft	- RAMCloud
PBFT	- Hyperledger Fabric
Sieve	- Hyperledger Fabric

II. 비트코인에서 사용한 합의 알고리즘, Proof of Work

가. Proof of Work(PoW)

- PoW 는 비트코인을 시작으로 많은 Public 블록체인에서 채택하고 있는 알고리즘이다. 확률적으로 해답이 어려운 문제를 가장 빨리 해결한 사람에게 블록을 만들 수 있도록 허가하는 방식으로 다음과 같은 절차로 이루어진다.

① A 가 B 에게 송금을 의뢰(트랜잭션)한다.

② 발행된 트랜잭션은 P2P 네트워크를 통해 참가자 전원에게 브로드캐스트 된다.

③ 트랜잭션을 받은 승인자는 블록을 생성하기 위한 요건을 만족시키는 해답을 찾기 시작한다.

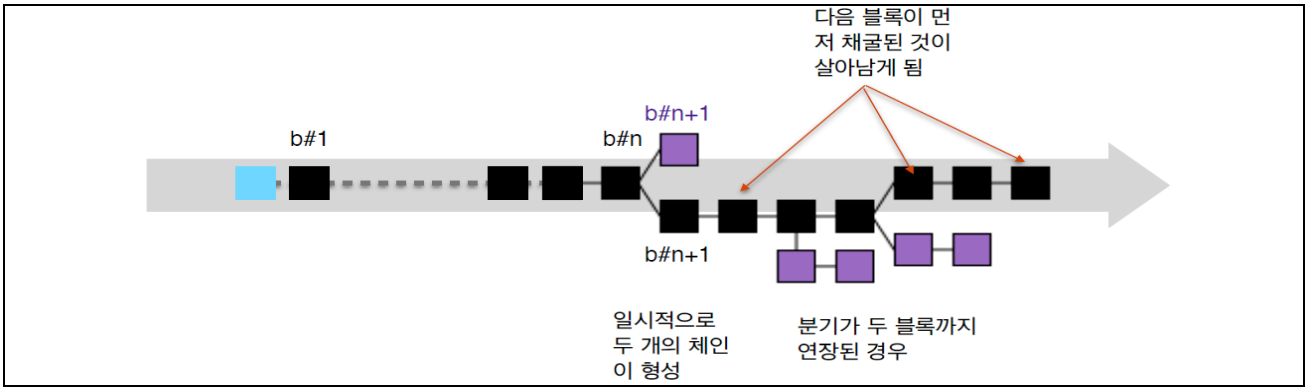
- 블록의 해시 값 ≤ 난이도를 만족하는 난수(nonce)값 찾기 (컴퓨팅 파워 필요)

④ 처음 조건을 만족하는 해답을 발견한 승인자가 참가자 전원에게 브로드캐스트 한다.

⑤ 블록을 받은 각 노드는 정당한 블록인지 검증한다. 50%이상이 동의하면 블록은 체인에 추가된다.

⑥ 송금이 완료된다.

- ③ 번 과정에서 동시에 두 사람이 해답을 찾을 경우 두 개의 블록이 생성될 수 있다. 이 경우를 분기(fork)라고 하며 분기가 발생하면 승인자(마이닝 노드)들은 둘 중 하나의 블록체인을 선택하여 다음 블록을 생성하게 된다. 이후, 먼저 블록이 생성되는 블록체인이 유효한 블록체인이 된다. 즉, 더 긴 블록을 선호하는 정책으로 분기를 해결한다.



나. Proof of Work 의 문제점

문제점	설명
51%문제	- ⑤번의 과정에서 특정 마이너가 전체 네트워크의 과반수 이상을 차지하는 경우, 다른 마이너가 생성한 블록을 승인하지 않는 등 결과를 자유롭게 조작할 수 있음
파이널리티 (결제완전성) 불확실성	- ③번의 과정에서 분기가 발생할 경우, 블록체인은 긴 체인을 올바른 것으로 판단한다. 이 때 짧은 체인을 사용하고 있던 노드는 해당 블록이 선택되지 않음으로 거래 잔액이 변경되거나 거래 자체가 없던 것으로 될 수 있다. - 비트코인은 이런 현상을 방지하기 위해 거래 확정 후 6 블록 가량 기다려야 다음 거래를 할 수 있게 한다. - 이런 불확실성은 금융 시스템에서의 도입을 어렵게 한다.
성능한계	- P2P 상의 정보 공유 시간, 여러 노드가 합의를 통해 검증하는 시간 등이 필요하다. - 이로 인해 실시간 처리에는 부적합하다.
블록체인 용량	- 모든 블록 정보를 각각의 노드에 보유해야 한다.

- 불특정 다수의 사용자가 참가하는 인터넷과 같은 환경에서 PoW 는 유효한 알고리즘이다. 하지만 신뢰된 참가자들이 컨소시엄을 만들어 운용하는 비즈니스 모델에서는 의미 없는 기능이다.

Ⅲ. PoW 외 다양한 합의 알고리즘

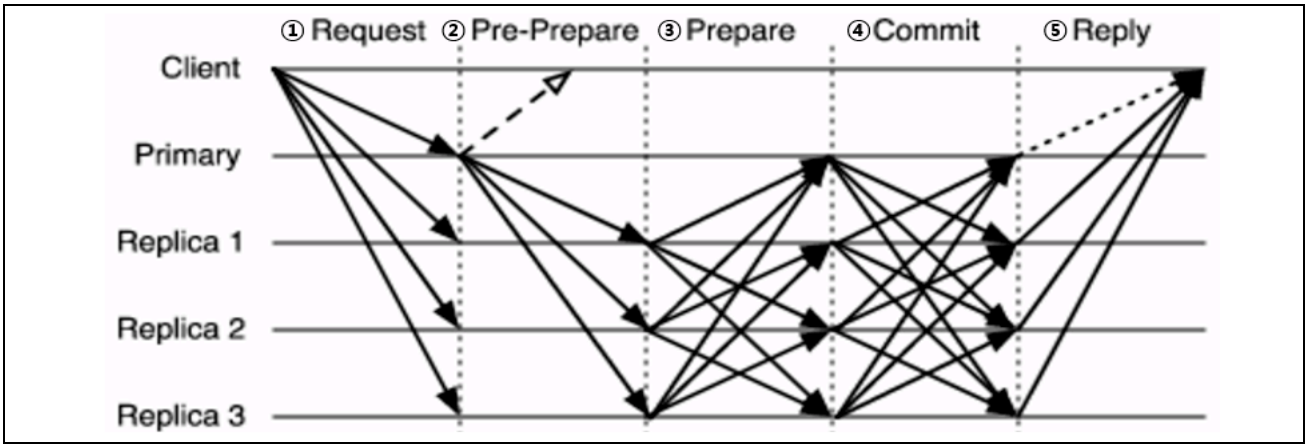
가. Proof of Stake(PoS)

- 이더리움이 채택할 예정인 알고리즘으로 PoW 와 기본 방식은 동일하나 **화폐량을 더 많이 소유하고 있는 승인자가 우선하여 블록을 생성할 수 있는 방식이다**. 화폐량에 따라 해시 계산의 난이도가 낮아지기 때문에 PoW 와 비교하여 자원 소비가 작다.

나. PBFT(Practical Byzantine Fault Tolerance)

- PoW 와 PoS 의 단점인 파이널리티 불확실성과 성능 문제를 해결한 알고리즘으로 Hyperledger Fabric 과 Eris 등 컨소시엄 형에서 이용하고 있다.(분기가 발생하지 않음)
- 네트워크의 모든 참가자를 미리 알고 있어야 하며, 참가자 중 1 명이 Primary(리더)가 되어 자신을 포함한 모든 참가자에게 요청을 보낸다. 그 요청에 대한 결과를 집계한 뒤 **다수의 값을 사용해 블록을 확정한다**.

- PBFT 처리과정



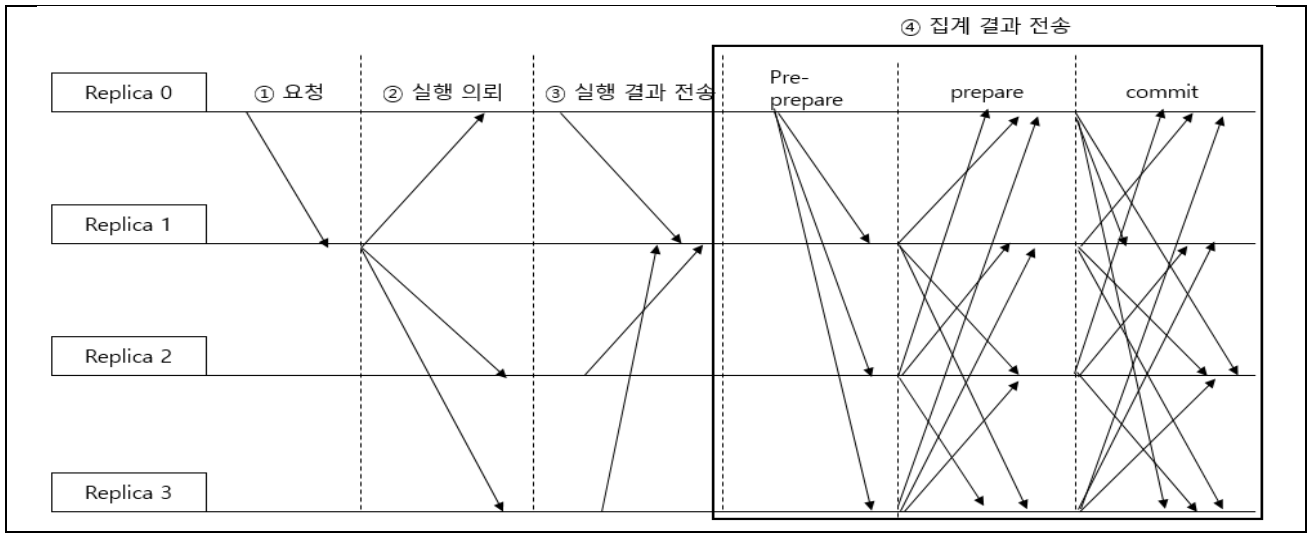
① 클라이언트가 모든 노드에 요청을 브로드캐스트 한다
② Replica0 가 primary(리더)가 되고 순차적으로 명령을 다른 노드에 전달한다.
③ 각 노드는 ②의 명령을 받으면 Primary(Replica0)를 포함한 모든 노드에 회신한다.
④ 각 노드는 ③에서 전달된 명령을 일정 수 이상 수신하면 Primary(Replica0)를 포함한 모든 노드에 수신한 신호를 전송한다.
⑤ 각 노드는 ④에서 보낸 명령을 일정 수 이상 수신하면 명령을 실행하고 블록을 등록해 client 에 reply 를 반환한다.

- 매우 고속으로 동작하지만 참가자 전원과 의사소통하기 때문에 참가자가 증가하면 처리속도가 저하된다.

다. Sieve

- IBM 에서 고안한 PBFT 를 확장한 알고리즘으로 실행 결과 전송과 집계전송으로 흐름이 나뉘어져 있으며, 합의 형성 전 단계에서 실행 결과를 검토해 결과가 다른 경우 중지시킨다. 각 노드의 실행결과가 다를 가능성을 조기에 탐지하고 싶을 때 유용하다.
- Hyperledger Fabric 에 채택되어 있지만 2016 년 7 월 기준으로 제외되었다.

- Sieve 처리 과정



① 각 노드 중 하나가 Client 가 되고, 리더의 명령을 송신한다.
② 리더(Replica1)가 각 노드에 실행의뢰를 전송한다.
③ 각 노드는 의뢰를 실행하고 결과를 리더에게 전달, 결과가 일정 수에 도달하지 못하면 중단되며 요청은 무시된다.
④ 수신한 결과가 중지가 아니라면 그 증거로 결과를 집계한다.(이 때 PBFT 가 사용되는 경우가 많음)

Ⅳ. 합의 알고리즘간 비교표

구분	PBFT/Sieve	PoW	PoS
통신 비용	각 서버간 통신으로 높음	로컬 통신만으로 비용 낮음	로컬 통신만으로 비용 낮음

결함허용대수	1/3 미만까지 문제없음	1 대	1 대
원리	다수결	CPU 계산량	보유한 자산 크기
CPU 연산비용	낮음	높음	중간 정도, PoW 보다 낮음
권한의 분산	참가 서버 모두가 평등	전기세가 낮은 지역에 집중될 수 있음	일반적으로 화폐 보유는 집중될 가능성 높음
참가 조건	신뢰 서버만 참가 가능	어떤 서버도 참가 가능	어떤 서버도 참가 가능
비밀보호를 위한 인증	사전에 서로 신뢰한 공개 암호화 키 사용	참가 시 준비한 공개 암호화 키 사용	참가 시 준비한 공개 암호화 키 사용

- 2015 년 경부터 컨소시엄형에서의 이용을 전제로 한 블록체인 기반이 등장하고 있으며, PoW 가 아닌 다른 합의 알고리즘을 채택하는 경우가 많아졌다. PBFT 등의 알고리즘은 분산 데이터베이스나 분산 파일 시스템 등에 이용되고 있지만 아직 블록체인에서 활용 사례는 많지 않다. 상황에 맞는 최적의 합의 알고리즘을 선택할 수 있기 위해서는 더 많은 실증 실험이 필요하다.

"끝"

[참고문헌]

1) 블록체인 구조와 이론(2017.06), 위키북스
2) 비트코인의 기술, 블록체인의 원리(2016.01),SPRI