The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 3, pp.25-32, Jun. 30, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.3.25
JIIBC 2019-3-4

블록체인 기반 합의 알고리즘 연구

A Study on Consensus Algorithm based on Blockchain

유순덕*

Soonduck Yoo*

요 약 블록체인 기술 핵심은 이중지불에 대한 합의 문제를 해결하는 것이며 이를 위해 이용되고 있는 알고리즘인 PoW, PoS 및 DPoS에 대하여 살펴보았다. PoW인 작업증명은 스팸 전자 메일을 보내거나 서비스 거부(Denial of service, DoS) 공격을 시작하는 등 컴퓨팅 능력의 사소하거나 악의적인 사용을 막기 위해 실현 가능한 노력을 필요로 하는 합의 시스템이다. PoS인 지분증명은 작업증명(PoW) 알고리즘의 에너지 낭비뿐만 아니라 Nothing at stake 문제를 해결하기 위해 만들어졌으며, 계산능력이 아닌 화폐 보유량에 따라 각 노드의 합의 결정권이 정해진다. DPoS는 분산 네트워크를 통해 소수의 권한을 가진 사용자들이 거래 합의를 유지하는 것으로, PoS는 모든 사용자에게 합의 권한을 가지는 것과 달리 DPos는 합의 권한을 소수의 대표자에게 제공 한다는 것이다. 즉 PoS가 직접 민주주의라면 DPoS는 간접민주주의이다. 본 내용은 블록체인 합의 알고리즘에 대한 연구를 통하여 관련 분야의 지속적인 발달에 기여하고자 한다.

Abstract The core of the block chain technology is solving the problem of agreement on double payment, and the PoW, PoS and DPoS algorithms used for this have been studied. PoW in-process proofs are consensus systems that require feasible efforts to prevent minor or malicious use of computing capabilities, such as sending spam e-mail or initiating denial of service (DoS) attacks. The proof of the PoS is made to solve the Nothing at stake problem as well as the energy waste of the proof of work (PoW) algorithm, and the decision of the sum of each node is decided according to the amount of money, not the calculation ability. DPoS is that a small number of authorized users maintain a trade consensus through a distributed network, whereas DPS provides consent authority to a small number of representatives, whereas PoS has consent authority to all users. If PoS is direct democracy, DPoS is indirect democracy. This study aims to contribute to the continuous development of the related field through the study of the algorithm of the block chain agreement.

Key Words : Blockchain, Consensus Algorithm, Double Payment, Proof of work, Proof of stake, Delagted proof os stake

I. 서론

1. 블록체인 기술

4차 산업혁명을 이끌어갈 핵심 기술로 블록체인 기술이 주목받고 있다. 다양한 영역에서 블록체인 기술을 활용하려는 노력이 진행되고 있으며 이를 기반으로 관련

*정회원, 한세대학교 국제경영학과
접수일자 2019년 5월 11일, 수정완료 2019년 6월 3일
게재확정일자 2019년 6월 7일

Received: 11 May, 2019 / Revised: 3 June, 2019 /
Accepted: 7 June, 2019
*Corresponding Author: harry-66@hanmail.net
Dept. of Business Administration, Hansei University, Korea

분야 기술 발달이 빠르게 이루어지고 있다. 블록체인 기술은 금융기관뿐만 아니라 IT 분야 기업, 정부 등이 다양한 분야에서 적용되고 있다.

블록체인 기술의 주요 핵심은 중앙에서 신뢰해야 하는 제 3자 기관(TTP: Trusted Third Party)이 없이 운영되는 분산 원장 관리기술이며, 블록체인 참여 노드들은 모두 동일한 원장을 공유하여 거래내역을 투명하게 관리할 수 있는 신뢰성이 제공된다는 것이다. 블록체인의 분산형 구조는 중앙서버 시스템과 중재 기관의 필요성을 제거할 수 있어서 기존 네트워크의 비용문제와 저가용성 문제를 해결할 수 있다.

블록체인 원장에 기록되는 정보는 참여 구성원들의 합의(Consensus)를 통해 블록이 추가될 수 있기 때문에 원장 기록에 대한 신뢰성을 가지며, 일부 구성원들의 장애 또는 악의적 방해가 존재해도 전체 합의를 유지할 수 있다.[1]

2 합의 문제

온라인 거래에서 복사본과 원본을 구별하지 못하는 문제, 즉 '이중 처리(지불) 문제'가 발생 할 수 있다. 예를 들어, 보유한 재산이 1,000원인 영희가 1,000원을 철수에게 송금 한다는 거래를 주변 노드에게 보내면서 동시에 민수에게 1,000원을 송금한다는 거래(트랜잭션)을 동시에 전송할 경우, 블록체인 시스템에서 유효한 거래를 합의를 하지 못하면 거래가 이중으로 처리 될 수 있는 문제가 발생한다. 즉 이를 피하기 위해 정상적인 거래를 위한 합의 문제가 발생한다.

기존 시스템에는 이러한 이중 처리 문제를 해결하기 위해 은행 등과 같은 신뢰 할 수 있는 제3자에게 자료 관리 권한이 위임되어 처리하고 있다. 이와 같이 제3자가 관리하는 경우, 단일 장애지점(Single Point of Failure), 중개 수수료, 거래 지연 존재 등 여러 문제가 발생한다.

이중 지불 문제를 해결하기 위해 블록체인 기술은 합의 알고리즘을 사용한다. 합의 알고리즘을 통해 P2P 네트워크 환경에서도 제3자 또는 중앙 통제시스템 없이 데이터베이스의 오류와 무결성을 보장 할 수 있다. 즉, P2P 네트워크 상의 다수의 노드들이 합의를 통해 하나의 블록체인을 유지하는 것이다. 이때 합의 알고리즘은 노드가 새 거래 데이터와 블록을 어떻게 처리할 지를 통제하는 명령어로서 역할을 수행한다. 따라서 모든 노드가 동일한 거래에 대한 처리 기록을 가지도록 함으로써 이중 처리 문제를 해결 한다. 이 합의 알고리즘은 현존하고 있는 알고리즘의 문제를 보완하기 위해 지금도 계속 연구되고 있다.

II. Background

1. 합의 알고리즘

합의 알고리즘은 분산된 프로세스 또는 시스템 간에 단일 데이터 값에 대한 합의를 달성하는 데 사용되는 컴퓨터 과학의 처리과정(프로세스)이다. 합의 알고리즘은 여러 개의 신뢰할 수 없는 노드가 포함된 네트워크에서 안정성을 확보 할 수 있도록 설계되어 있어서 합의 문제를 해결한다. 이는 분산 컴퓨팅 및 다중 에이전트 시스템에서 매우 중요하다.

이러한 현실을 수용하기 위해 합의 알고리즘은 반드시 일부 프로세스와 시스템을 사용할 수 없으며 일부 통신이 손실 될 것이라고 가정하여 합의 알고리즘은 의사결정시 내부에 결함이 있다는 것을 전제로 한다. 거래를 형성하기 위해 일반적으로 모든 노드가 같은 것에 대해 응답하지 않으므로 그 중 응답한 일부 노드가 과반수 이상인 51% 이상 존재해야 한다.

일반적으로 적용되는 합의 알고리즘에는 작업증명(PoW: Proof of Work), 지분증명(PoS: Proof of Stake), 위임된 지분증명(DPoS: delegated proof-of-stake), 실용적인 Byzantine Fault tolerance(PBFT) 알고리즘 및 DPoS (Delegated Proof of Stake 알고리즘)가 포함된다.[2]

2. 블록생성 권한 분배

허가가 필요 없는 비허가형(Permissionless) 블록체인은 특별한 자격요건 없이 각 노드는 블록을 생성 할 수 있다. 따라서 각 노드에서 블록을 쉽게 생성할 수 있기 때문에, 동시에 수많은 블록이 만들어질 수 있으며, 이는 각 노드가 하나의 블록체인에 합의하는 것을 매우 어렵게 만든다. 이에 따라 불록체인은 각 노드가 일정시간 동안 거래를 수집하여 처리하게 하고 특정 조건에 적합한 채굴자를 선정하여 블록을 생성하게 한다. 이 경우 각 연산되는 합의 알고리즘에 따라 요구하는 채굴자의 조건은 토큰 보유량, 계산능력 등인 여러 가지 합의 조건을 제시하여 합의를 한다. 이 경우 합의 알고리즘 검증에 시간으로 소요되므로 따라 즉시 거래 처리를 하지 않고 지연을 한다.

그 대표적인 합의 알고리즘인 작업증명(PoW: Proof of Work) 경우에 컴퓨터의 계산 능력에 따라 채굴 확률이 결정된다.[3] 예를 들면, 영희의 계산능력이 1이고, 철수가 3이면, 이 경우 채굴확률은 1 : 3로 결정되어, 영희가 1개 채굴할 때 철수는 3개를 채굴할 수 있다는 것으로 판단한다. 이는 블록 생성 권한 분배로 상기와 같이 채굴자의 지정된 조건 기준으로 알고리즘을 적용한다.

3. 포크(Fork: 분기) 발생을 피하기 위한 체인 선택 기준

각 노드 간 떨어져 있는 거리와 전송 속도에 따라 정해진 시점에서 노드마다 블록체인이 다르게 구성될 수 있다. 예를 들면 파란블록에 합의가 발생하여 새로운 블록인 빨간 블록이 자식으로 연결될 수 있다. 이때 자식으로 연결될 수 있는 빨간 블록은 바로 앞 블록인 파란블록에서 생성된 블록 해쉬를 포함하고 있다는 것이다. 늦게 나타난 초록색 블록이 파란블록 다음에 자식으로 연결됨으로써 포크(Fork)가 발생한다. 일반적으로 부모하나에 자식이 하나가 생성되어야 하지만 이와 같이 한 부모에 대해 여러 개의 자식 블록이 발생하는 상황을 포크(fork)라고 명칭하며, 포크는 각 노드가 소유하고 있는 분산장부 간에 일치 되지 않는 상황을 만든다. 따라서 이러한 불일치 문제를 해결하기 위해 각 블록체인은 블록체인별로 합의 규칙을 정하여 모든 노드가 파란블록에 대해 빨간 블록이 자식이 될지, 초록블록이 자식이 될지 동일하게 결정한다.

이것을 해결하기 위한 대표적인 방안이 비트코인에서 쓰이는 가장 긴 체인을 선택하여 사용하는 것이다.[4] 한 노드가 파란블록을 부모로 하여 자식으로 남색 블록을 만들고 남색 블록을 모든 노드에게 전파를 한다, 파란블록에 계속 단계별로 자식 블록이 연결됨으로서 다른 색 블록 보다 긴 체인을 형성하게 되어 파란 블록이 속한 체인이 중심 체인이 되는 방식이다.

4. 비잔틴 장군 문제

비잔틴 장군 문제를 자세히 살펴보면, 흩어져 있는 비잔틴의 장군들이 특정 성을 공격하기 위해 모든 장군들이 동일한 시간대에 공격을 한다면 전쟁에 승리 할 수 있는 상황으로 흩어져 있는 장군들은 같은 시간에 공격하기 위해 공격시간 정보를 공유 해야 한다. 그러나 비잔틴 장군들 중 첩자가 있어 중간에 정보를 제대로 전달하지 않을 수 있기 때문에 모든 장군들이 동일한 시간에 공격을 할 방법에 대한 고민이 등장한다. 이 문제에서 장군들로 표현하였지만 네트워크에 있는 악의적인 노드 또는 오작동 노드를 첩자라고 생각하면 된다.

분산 컴퓨팅의 아버지 레슬리 램포트(L. LAMPORT)가 논문을 통해 처음으로 제안한 것이 비잔틴 장군문제로, 악의적인 노드가 분산 시스템에 참여한 상황을 모델링한 것이다. 비잔틴 장군 문제를 해결하는 시스템은 악의적인 노드가 분산 시스템에 참여한 상황에서도 합의 알고리즘을 통해 전체 시스템은 신뢰가 보장된 서비스를 제공할 수 있다는 것이다. 대표적인 비잔틴 장애허용(Byzantine Fault Tolerance) 알고리즘으로 PBFT(Practical Byzantine Fault Tolerance)가 있다.

블록체인은 100% 신뢰관계가 형성되지 않은 노드들이 모여서 서로가 연결된 네트워크를 연결하여 구성한다. 따라서 악의적인 노드가 네트워크 조작을 통해 부당 이득을 취할 수 있는 가능성이 있으므로 블록체인 시스템에서 비잔틴 장군 문제(Byzantine General Problem)가 등장한다. 그러나 블록체인 기술은 네트워크에 악의적인 노드가 존재하더라도 합의 알고리즘을 통해 신뢰성 있는 환경을 제공할 수 있기 때문에 비잔틴 장군 문제를 해결 한다.

III. 합의 알고리즘 사례

1. PoW (Proof of Work, 작업증명)

PoW 개념의 등장 배경을 보면, 2004년 Hal Finney가 "재사용 할 수 있는 작업 증명"이라는 아이디어를 통해 돈에 적용 되었다. 2009년에 소개된 비트코인에 적용되어 Finney의 아이디어 중 처음으로 널리 채택된 응용프로그램이 되었다.[5] Finney는 첫 번째 비트코인 트랜잭션의 수신자이다. 작업 증명은 다른 많은 암호화폐(cryptocurrency)의 기반을 제공했다.

작업증명(PoW : Proof of Work)이란 스팸 전자 메일을 보내거나 서비스 거부(DoS: Denial of service) 공격 등 컴퓨팅 능력의 사소하거나 악의적인 이용을 막기 위해 실현 가능한 시스템이다. Proof of Work 이란 용어의 의미대로, 컴퓨터 계산 작업을 통해 블록의 유효성을 증명하고, 채굴 권리를 얻어내는 방법이다.

PoW는 작업증명으로, 컴퓨터 연산을 통해 특정 Nonce 값(블록 헤더의 해시 값이 난이도에 제시된 값보다 작은 값이 나오게 하는 Nonce값)을 먼저 찾는 사람이 블록을 채굴(검증)할 권리를 제공하는 구조이다[1][2]. 또한 연결

되는 블록이 증가할수록 해당 난이도는 점점 올라가게 된다. 이러한 값을 찾기 위해서는 랜덤 숫자를 입력하여 문제를 해답을 구하는 방법 밖에는 없기 때문에, 전력을 많이 소비하는 고 성능 컴퓨터 일수록 연산 능력이 높아 결국 채굴 확률이 커진다.

사용자가 실제로 변조를 감지하는 방법은 해시를 통해 작업증명의 역할을 하는 긴 문자열을 사용하는 것이다. 주어진 데이터 집합을 해쉬함수(비트코인은 SHA-256을 사용한다)에 넣으면 해시를 하나만 생성한다. 그러나 원본 데이터의 일부분을 조금만 변경해도 완전히 인식 할 수 없는 해시가 된다. 원래 데이터 세트의 크기에 상관없이 주어진 함수에 의해 생성된 해시는 동일한 길이이다. 해시는 단방향 함수이므로 해시를 생성한 데이터가 원본 데이터와 일치하는지 확인하기 위해 원본 데이터를 가져오는 방법을 사용할 수 없다.

비트코인 트랜잭션 집합에 대한 해시를 생성하는 것은 현대 컴퓨터에서는 어렵다. 따라서 프로세스를 운영으로 바꾸기 위해 비트코인 네트워크는 일정 수준의 난이도를 설정한다. 이 설정은 새 블록이 "마이닝" 되도록 조정되어 약 10분마다 유효한 해시를 생성하여 블록체인에 추가된다. 난이도 설정은 해시에 대한 '대상'을 설정하여 수행된다. 대상이 낮을수록 유효 해시집합이 작아지고 해시 집합을 생성하는 것이 어려워진다.

실제로 이것은 긴 0의 문자열로 시작하는 해시를 의미한다. 예를 들어 블록 # 429818의 해시는 0000000000000000004dd3426129639082239efd583b5273b1bd75e8d78ff2e8d이다. 이 블록에는 1,000개가 넘는 비트코인이 포함된 2,012건의 트랜잭션과 이전 블록의 헤더가 들어 있다. 사용자가 하나의 거래금액을 0.0001 비트 동전만큼 변경한 경우 결과 해시는 인식 할 수 없으며 네트워크는 더 이상 거래가 되지 않는다.

주어진 데이터 집합은 오직 하나의 해시를 생성 할 수 있기 때문에 어떻게 채굴자가 목표 아래에 해시를 생성하는지 확인하는 방법으로 채굴자는 nonce ("number used")라는 정수를 추가하여 입력을 변경한다. 유효한 해시가 발견되면 네트워크로 브로드 캐스팅되고 블록이 블록체인에 추가된다.

마이닝은 경쟁적인 과정이지만 경주보다는 복권에 가깝다. 평균적으로, 누군가는 10분마다 허용되는 작업증명을 생성할 것이지만 그것이 누구인지는 누구나 추측할 수 있다. 채굴자가 함께 모여 채굴 블록 기회를 늘리면 거래 수수료가 발생하고 제한된 시간 동안 새로 생성된 비트 동전에 대한 보상이 발생한다.

작업증명에 따르면, 블록체인의 모든 측면을 변경하는 것이 매우 어렵다. 이러한 변경에는 이후의 모든 블록을 다시 마이닝 해야 하기 때문이다. 또한 해시기능을 완료하는 데 필요한 기계 및 전원이 비싸기 때문에 사용자 또는 사용자 풀이 네트워크의 컴퓨팅 성능을 독점하기가 어렵다. PoW는 확률적으로 마지막엔 하나의 블록체인을 합의하게 되는 알고리즘으로 일시적으로 합의가 깨질 수 있다.

일반적인 합의 알고리즘이 적은 수의 공격 노드와 다수는 정상적인 행동을 한다는 가정(보통 3g+1 이상이 정상 운영이 되고, g는 오류 노드의 수)을 통해 작동하는 알고리즘이다. 작업증명 알고리즘은 글로벌한 규모의 완전히 오픈된 네트워크에서 운영할 수 있는 알고리즘이다.

작업증명 알고리즘의 단점은 느린 속도와 낭비되는 에너지가 많다는 것이다. 블록을 생성하기 위해서 무의미한 해시 값을 찾아 내야 하고, 그 작업을 위해 불 필요한 리소스들이 투입되어 무의미한 에너지 소비가 증가하는 한 계점을 보유하고 있다.

현재 비트코인 한 블록을 생성하기 위해서는 위해선 5,000,000 TH/s(1 TH/s = 초당1,000,000,000,000번의 해시연산) 이상의 해시 파워가 필요로 한다.[6] 특정 연산 능력만이 강요되다 보니, 연산 능력이 집약된 별도 칩들이 등장하게 되고 블록 생성의 보상을 다 같이 나눠서 가지기 위한 연맹인 마이닝 풀(Mining Pool)이 생성되고 이세력의 공유는 더욱 강화 되었다. 이러한 문제점 때문에 다른 가상 화폐들에서는 새로운 형태의 PoW 알고리즘을 만들기 위한 시도가 진행되고 있다.

컴퓨팅 능력에 의존하는 PoW의 구조 덕분에 PoW는 보안성을 가장 큰 장점으로 보유하고 있다. 따라서 블록체인 노드의 '51% 공격' 을 손쉽게 방어할 수 있는 구조이기 때문이다. 악의적인 공격자가 51% 공격하기 위해서는 51% 이상의 컴퓨팅 연산 능력을 확보해야 하지만 이는 현실적으로 천문학적인 소요 비용을 요구하기 때문에 이를 통해 악의적인 노드(공격자)가 얻을 수 있는 이익은 소요 비용 보다 낮다.

비트코인은 "블록체인"으로 알려진 일종의 분산원장에 의해 뒷받침되는 디지털 통화이다. 이 원장에는 순차적인 블록으로 정렬된 모든 비트코인 트랜잭션의 기록이 포함되어 있어 사용자가 자신의 소유물을 두 번 이상 쓸 수 없는 구조이다. 훼손을 방지하기 위해 원장은 공개되거나 배포 되고 있기 때문이다. 임으로 변경된 버전은 다른 사용자들에 의해 신속하게 거부된다.

비트코인은 블록체인의 합의 알고리즘을 사용하여 노

드 간의 합의를 도출한다. 블록체인은 P2P(Peer to Peer) 네트워크에서 분산 컴퓨터에 의해 관리되는 분산 데이터베이스로 생각할 수 있다. 각 피어는 SPOF(Single Point of Failure)를 방지하기 위해 원장 사본을 유지 관리 하고 업데이트 및 유효성 검사는 모든 사본에 동시에 반영된다.[7]

비트코인은 광부가 제출한 블록 내에서 채굴이 이루어지도록 보장하는 메커니즘을 포함시킴으로써 신뢰성이 부족한 네트워크의 보안을 보장하기 위해 PoW(proof of work) 알고리즘을 사용한다. 채굴자의 컴퓨터에 있는 소프트웨어는 트랜잭션 관련 알고리즘을 해결하기 위해 처리 용량에 접근한다. 이 블록은 계산 집약적인 프로세스에서 생성된 암호화된 해시에 대한 작업증명이다. 모든 당사자가 원장에게 일련의 블록을 제출할 수 있지만 합의를 가짜로 만드는데 필요한 컴퓨팅 리소스의 양이 너무 많아 노력 대비 효과가 거의 없다.

2. PoS (Proof of Stake, 지분증명)

지분증명(PoS : Proof of Stake) 시스템은 2011년에 처음 소개되었으며, 2012년 Peercoin을 구현한 최초의 암호 해독 기술이며 블록체인 기술에서 일반적으로 사용되는 합의 프로토콜 중 하나이다. 지분증명은 암호화폐(cryptocurrencies)가 블록을 검증하는데 사용하는 합의 알고리즘 중의 하나이다.[8] 기존 작업증명 알고리즘의 에너지 낭비문제와 Nothing at stake 문제에 대한 대안으로 제작되었으며, 컴퓨터 계산능력이 아닌 화폐 보유 정도에 따라 각 노드의 합의가 결정된다.

지분증명 시스템에서, 다음 블록의 생성자는 부분적으로 사용자가 보유하고 있는 암호화폐(cryptocurrency)의 정도 또는 어떤 경우에는 그 특성을 보유하고 있는 기간에 의해 결정되는 무작위 시스템에 의해 결정된다. 화폐에 대한 연산 능력 대신에, 블록을 생성하고 관련 보상을 받을 확률은 사용자가 네트워크에서 토큰 또는 암호 해독성을 유지하는 것에 비례한다. 즉 잠재적인 유효성 검사시 집합이 40개의 토큰을 보유하고 있는 영희, 30개를 가지고 있는 철수, 20개 가진 민수 및 10개 가진 현수로 구성된 경우, 영희는 40%, 철수 30%, 민수 20%, 현수 10% 중에서 지분을 더 많이 보유한 사람이 유리해지는 구조를 가지고 있다.

지분증명 시스템에 대한 무작위 추출은 중앙 집중화를 방해한다. 그렇지 않으면 시스템의 가장 부유한 개인이 항상 다음 블록을 만들고 지속적으로 부를 늘려 결과적으로 시스템을 통제하게 된다.

작업증명과 같은 시스템에 대한 지분증명의 주된 이점은 훨씬 적은 에너지를 사용하므로 비용이 더 효율적이라는 것이다. 작업증명 시스템을 사용하는 비트코인 거래가 2주만에 네덜란드 가정의 평균 전기 요금을 엄청나게 증가 시킨 것을 보면, 이것은 비효과적이고 지속 불가능하다는 것을 보여 주었다.

이런 측면에서 지분증명은 훨씬 적은 전기 사용량을 소요되기 때문에 우수한 합의 프로토콜로 간주 될 수 있다. 또한, 지분증명 시스템은 저비용 고효율적이기 때문에 네트워크를 유지하기 위해 채굴자에게 인센티브를 부여하는 수단으로 많은 새로운 동전을 발급해야 할 필요가 없다. 이로 인해 특정 동전의 가격을 보다 안정하게 유지하는 데 도움이 된다.

지분증명 프로토콜의 증명은 개인이 시스템에 참여하도록 격려하는 것뿐만 아니라 어떤 개인이 네트워크를 전체를 제어하지 못하게 하는데 효과적이다. 즉 51%의 공격을 수행하기 위해서는 개인이나 그룹이 네트워크상의 대부분의 동전을 소유해야 한다.

한 사람이 모든 것을 사들이는 경우 많은 개인이 통화 거래를 종료하고 다른 사람들이 절대적 인수를 저지하기 위해 가격을 올릴 것이기 때문에 모든 동전을 충분히 구입하는 것이 극도로 비싸다. 또한 공격자가 보유하고 있는 동전의 가치를 크게 하락시키기 때문에 네트워크를 공격하는 것은 완전히 비 생산적이다.

근본적으로, 암호화폐에서 가장 높은 지분을 가진 사용자는 어떤 공격이라도 보유하고 있는 암호화폐의 명성과 가격을 하락시키기 때문에 네트워크를 유지하고 보호하는 데 가장 많은 관심을 가지고 있다. 그러나 지분증명에는 단점이 있으며, 그 중 하나는 "아무런 문제가 없다(Nothing at stake)"는 문제로 다양한 블록체인 생성을 지원하여 블록은 생성되지만 합의가 해결되지 못하는 경우에 발생하여 생성한 블록이 가치가 없는 경우가 발생한다.

지분증명 합의는 비잔틴 결함 허용문제를 해결하는데 특히 적합하다. 이는 모든 유효성 검사기가 네트워크에 의해 추적되고 ID(예 : Lisk 지갑 주소)의 신원을 알고 있기 때문이다. 비잔틴 결함 허용문제(BFT : Byzantine Fault Tolerance)은 검증자의 2/3가 정직해야 하므로 이러한 개별신원을 추적하면 기능적 상태를 유지하는 데 도움이 된다. 따라서 전반적으로 지분증명 합의 프로토콜은 의도된 목적을 효율적으로 수행하는 견고한 시스템이다.

3. PoW와 PoS의 비교

PoW의 지지자는 암호가 통화로 더 효과적으로 기능할 수 있다고 주장하고 있으며, PoS 모델은 사용자가 장시간 동안 동전을 버려서 비활성화 상태로 만드는 것에 대한 인센티브를 제공한다[3].

PoS의 경우 시스템의 전반적인 우수성으로 비트코인이 만든 에너지 소비 문제를 해결 한다. 비트코인의 네트워크에 더 많은 거래와 사용자가 추가됨에 따라 성장을 수용하기 위해서는 더 많은 컴퓨팅 성능이 필요하고 네트워크에 추가되는 컴퓨팅 성능이 높을수록 해시 비율이 높아진다. 블록을 생성하기 위해 컴퓨터가 생성해야 하는 작업량이 증가하게 되면 더 많은 어려움이 따르게 되며, 이러한 증가 된 출력은 더 많은 에너지 소비로 이어진다. 비트코인의 성장과 채굴 난이도는 기하 급수적으로 에너지 소비와 관련되어 있으며 비평가들은 이것을 PoW 모델에서 해결할 수 없는 문제로 보고 있다.[9]

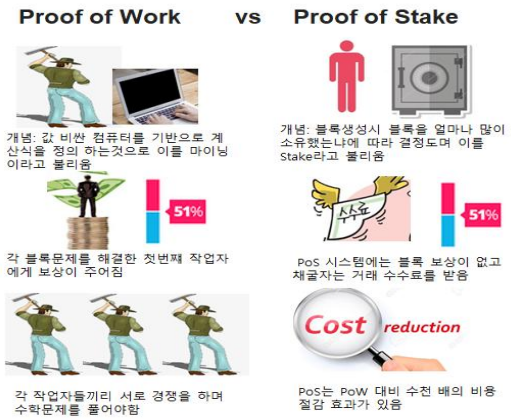

그림 1. PoW와 PoS의 비교
Fig. 1. Comparison of PoW and PoS

PoS의 경우 블록체인에 대한 51%의 공격을 방어한다. 최근의 비트코인 Cash와 비트코인 내전에서 볼 수 있듯이, 불균형적인 채굴로 인해 블록체인 네트워크가 사실상 중앙 집중화 될 수 있다. PoS 블록체인의 대다수를 제어하기 위해 유효성 검사기는 해당 암호의 전체 공급량의 51% 이상을 소유해야 한다. 그래서 누군가 Cardano의 블록체인을 공격하기 위해서는 Cardano의 가치가 609,286,157.643 달러가 되어야 하며 이런 일은 거의 불가능하다.

PoW의 경우 통화의 동전이 발행되고 유통되면 모든 블록 보상이 중단된다는 것이다. 이것은 PoW 동전을 인센티브로 삼아 PoS 모델로 업데이트 할 수 있다.

표 1. PoW와 PoS의 특징 비교
Table.1 Feature comparison between PoW and PoS

구분	PoW	PoS
채굴방식	o 블록 채굴시 채굴자가 얼마나 노력을 했는지에 따라 달라짐	o 블록 채굴시 얼마나 많은 코인을 보유하느냐에 따라 정해짐
보상	o 보상은 채굴자에게 점점 줄어듬 o 51% 공격하여 확보하는 경우 보상이 거의 없음	o 51%에 대한 공격 시 비용이 많이 들게 설계됨
현상	o 이 시스템은 채굴팀이 확보됨 o 시간이 지남에 따라 중앙집중화 현상 발생	o 분산 시스템을 유지 o 코인 중심으로 협력체계를 구축하기 위해 노력을 해야 함

4. DPoS(Delegated Proof of Stake, 위임된 지분증명)

위임된 지분증명(이하 DPoS라고 함)은 네트워크 전체에서 진실에 대한 반박 할 수 있는 합의를 유지하고 거래를 확인하며, 디지털 민주주의의 한 형태로 행동하는 합의 알고리즘이다.

DPoS는 PoW 방식의 대안으로 등장한 PoS 방식의 불완전 점이 등장하여, 이를 해결할 수 있는 방안으로서 EOS의 창시자 '댄 라리머'에 의해 제안된 합의 방식이다. 이는 위임된 지분 증명 방식으로 PoS와의 차이점은 합의 권한을 소수 대표자에게 투표권을 제공한다는 것이다. 따라서 PoS가 직접 민주주의라면 DPoS는 간접민주주의이다.

지분 보유자들은 지분에 비례한 투표권을 행사하여 자신들을 대신하여 블록 생성과 검증, 네트워크 유지, 합의에 대한 권한을 소수에게 위임한다. 성공 사례인 'Steemit'은 DPoS방식을 채택하여 21명의 증인(대표자)를 사용하여 DPoS 방식과 퍼블릭 블록체인의 적용 가능성을 확인했다.

위임 된 지분증명의 증거는 합의를 달성하기 위한 사회시스템과 결합된 실시간 투표를 사용한다. 이 방법은 가장 일반적인 것으로서 등장한 다른 방식대비 가장 적은 참여자가 참여하는 중앙화된 일치 프로토콜이라고 볼 수 있다. 그럼에도 불구하고 모든 토큰 소유자는 네트워크에서 일어나는 일에 대해 일부 영향력을 행사 할 수 있다.

DPoS의 가장 주요 장점은 투표에 의해 선출된 일부 대표자들이 전체를 대신하여 블록을 생성할 수 있다는 점이다. 때문에 상대적으로 빠른 합의속도와 저비용으로 운영된다는 장점이 존재한다. 이와 동시에 전체 네트워크 관리와 프로젝트에 대해 무관심한 일반 이용자들은 편의성이 증가한다.

일부 대표자들은 토큰 소지자에 의해 각각의 역할에 배정된다. 토큰 소유자가 가지고 있는 투표권(투표 가중치라고도 함)은 계정에 보유하고 있는 기본 토큰의 수에 따라 결정된다. 대의원은 네트워크를 원활하고 안전하게 운영 할 수 있도록 최대한의 관심을 가지고 선택하는 것이 중요한다. 일부 DPoS 버전에서는 대의원이 시간제한 보안 계정(악의적인 행동으로 몰수 된 경우)에 자금을 입금하여 약정을 표시해야 한다. 이 버전의 DPoS는 보증금을 기반으로 한 지분 증명 이라고도 한다.

주요 역할을 보면 다음과 같다.

(1) 노드가 항상 가동되고 있는지 확인한다.
(2) 네트워크를 통해 트랜잭션을 블록으로 수집한다.
(3) 블록을 서명하고 브로드 캐스팅하여 트랜잭션의 유효성을 검사한다.
(4) 합의와 관련하여 문제가 있는 경우 DPoS는 이를 공정하고 민주적인 방법으로 해결할 수 있다.

DPoS는 소수에 의한 효율성을 증명해냈지만, DPoS를 비판하는 많은 사람들은 공통된 질문을 던진다. 소수 대표단에 의해 운영되는 네트워크가 탈중앙화의 기본 원리에 위배된다는 것이다. 기술적으로 검토하면, 노드의 소수 집중적 방식은 블록체인 기술이 가지고 있는 강점인 '탈중앙화 기반 보안성'을 상실하는 단점이 있다. 모든 네트워크가 소수 집단에 운영되면 공격에 취약해 지는 것은 당연하다.

IV. 결론 및 시사점

블록체인 기술이 제 3자 기관을 필요하지 않으며 신뢰성을 확보하는 시스템으로 핵심기술로 거래에 대한 합의 알고리즘이 존재한다.[10, 11] 참여자들이 블록을 생성하거나 거래 시 정상적인 거래임을 검증하기 위해 합의 알고리즘을 사용한다.

블록체인 기술의 핵심은 이중지불에 대한 합의 문제를 해결하는 것이다. 이를 위해 이용되고 있는 합의문제 알고리즘인 PoW, PoS, DPoS에 대하여 살펴보았다.

PoW인 작업증명은 스팸 전자 메일을 보내거나 서비스 거부(DoS: Denial of service) 공격을 시작하는 등 컴퓨팅 능력의 사소하거나 악의적인 사용을 막기 위해 실현 가능한 노력을 필요로 하는 합의 시스템이며, PoS인 지분증명은 기존 작업증명 알고리즘의 에너지 소비문제와 Nothing at stake 문제를 해결하기 위해 제작 되었으며, 컴퓨터 계산능력이 아닌 화폐 보유량에 따라 각 노드의 합의 결정권이 정해진다.

DPoS는 PoS처럼 분산 네트워크에서 합의를 통해 거래를 인증하며 거래를 확인하며, PoS와의 차이점은 권한을 소수의 대표자에게 제공한다는 것이다. 즉 PoS가 직접 민주주의라면 DPoS는 간접민주주의로 볼 수 있다.

본 내용은 블록체인의 핵심 기술인 합의 알고리즘에 대한 원리 이해를 도모하여 관련 분야의 지속적인 연구 발전에 기여하고자 한다.

References

[1] Heeyoul Kim, Analysis of Security Threats and Countermeasures on Blockchain Platforms, Journal of KIIT. Vol. 16, No. 5, pp. 103-112, May 31, 2018.

[2] Shin Eun-seop, Results of preliminary feasibility study for long-term technology development project of block chain, 2019.

[3] Park Yeon-a, Kim Jong-hyun, Kim In-kyu, A Case Study on the Application of Ethereum-Blockchain Technology for Electronic Voting System,. Journal of inforamtion technology and architecture, vol.15 no.2 pp.201-218, 2018.

[4] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2018.

[5] Sun Jong-cheol, A Reference M odel for Korea Real Estate Administration Intelligence System using Blockchain, Korea Broadcasting University Graduate School, 2018.

[6] Cho Seok-yoon, A Study on the Application of National Electronic Procurement System Using Block Chain, 2017.

[7] An Yong Bae, Public institution evaluation s ystem based on cloud, Korea University, 2014.

[8] Jang Seung-il, On establishment of an alternative e-business escrow platform u sing block chain based smart contract, Dongguk University, 2018.

[9] Yoon Kyung Kim, Future Leadership of Conductor in Public Orchestra : Public Management Perspectives, Korean association for organization studies, vol.15, no.4, pp. 25-56, 2019.

[10] Yoo Soonduck, Kim kiheung, A Study on Improvement for Service Proliferation Based on Blockchain, The journal of institude of internet broadcasting communication, vol 18 no 1 pp.185-194, 2018.

[11] Kim Sam-Taek, Analysis on Consensus Algorithms of Blockchain and Attacks, Korean Convergence Society, Vol(9) No 9, pp.83-88, 2018

저 자 소 개

유 순 덕(정회원)

•1991년 2월 : 국민대학교 수학과(학사)
•1994년 2월 : 연세대학원 수학과 (이학석사)
•1995년 12월 : 영국뉴카슬 대학 응용수학 (석사)
•2010년 3월 ~ 2013년 2월 : 한세대학교 IT융합박사
•2013년 9월 ~ 현재 : 한세대학교 조교수
•관심분야 : 전자금융, 창업 및 벤처, 빅데이터, 정부정책, 개인정보 및 보안