정 보 보 호 학 회 지
제 32 권 제2호, 2022. 4

사물인터넷 상에서의 블록체인 기술 동향

심 민 주*, 김 원 웅*, 강 예 준*, 서 화 정**

요 약

수많은 사물들의 센서 정보를 인터넷을 통해 수집하고 분석하여 고객 맞춤형 서비스를 제공하는 사물인터넷 (Internet of Things, IoT) 서비스의 규모와 범위가 점차 확대됨에 따라 그 이점과 함께 사물인터넷이 가진 원천적인 확장성 문제와 개인정보 보안의 취약성 등에 대한 논의가 활발히 진행되고 있다. 최근에는 사물인터넷이 가진 문제점을 극복하기 위한 하나의 도구로써 블록체인을 사물인터넷에 접목하는 방안이 제시되고 있다. 본 고에서는 블록체인을 통해 사물인터넷이 가진 한계점을 극복하고 신뢰성 높은 사물인터넷 서비스를 제공하기 위해 필요한 블록체인의 합의 알고리즘들의 최신 동향에 대해 확인해 보도록 한다.

Ⅰ. 서 론

무선 스마트 센서가 탑재된 제품과 클라우드 플랫폼 사용이 증가함에 따라 전 세계의 사물인터넷의 시장 규모는 2021년 3,845억 달러에서 2027년에는 5,664억 달러로 연간 6.7%로 성장할 전망이다 [1]. 하지만 사물인터넷은 개인정보 보호에 취약할 수 있기 때문에 이를 보완하기 위한 연구가 지속해서 이뤄지고 있다. 현재 사물인터넷 보안 이슈를 해결하기 위해 탈중앙화 특징을 가진 블록체인이 주목받고 있다. 본 논문에서는 사물인터넷 접목에 용이한 블록체인의 탈중앙화 특성을 구성하는 합의 알고리즘과 사물인터넷 상의 블록체인 접목에 대한 최신 동향을 살펴본다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인의 합의 알고리즘에 대한 동향을 확인하며, 기존 합의 알고리즘을 기반으로 한 사물인터넷 상에서의 블록체인을 위한 합의 알고리즘에 대해서 알아본다. 3장에서는 사물인터넷 상에서의 블록체인에 관한 최신 연구를 알아본다. 마지막으로, 4장에서는 본 논문의 결론을 내린다.

Ⅱ. 합의 알고리즘

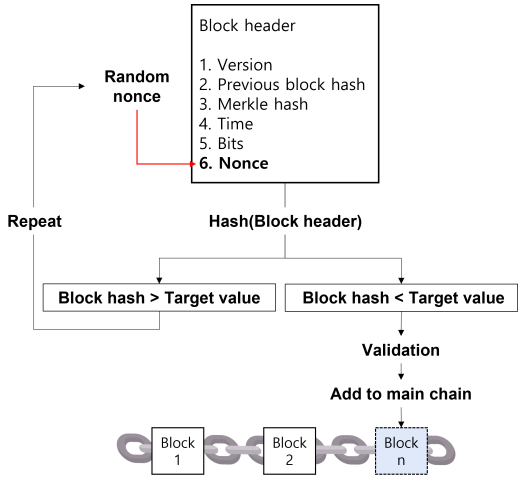
2.1. Proof of Work (PoW)

PoW는 블록체인의 보안성을 확보하기 위해 블록의 특정 해시값을 찾는 합의 알고리즘이다. 목표 값보다 작은 블록 해시값을 갖는 유효한 nonce 값을 찾는 것을 목적으로 한다 [2].

[그림 1]은 PoW 알고리즘의 세부 동작을 나타낸 것이다. 먼저, 채굴자는 임의의 nonce 값과 블록의 헤더에 저장된 정보를 결합한 것에 대한 해시값을 계산한다. 채굴자가 계산한 해시값이 목표 값 (블록 헤더의 bits 값)보다 클 경우, nonce 값을 무작위로 대입하여 해시값을 계산하는 과정을 반복한다. 이때, 목표 값보다 작은 해시값을 얻었다면, 다른 노드들은 nonce 값에 대한 검증을 진행한다. 해당 nonce 값을 블록 헤더에 넣었을 때, 목표값보다 작은 해시값이 계산되면 검증에 성공한다. 이렇게 검증된 블록은 메인체인에 추가되며, 채굴자는 보상을 받는다.

PoW는 모든 노드로부터 검증을 받아야 하므로 거래 내역을 속이기 어렵다. 하지만, 채굴 난이도가 높아짐에 따라 더 높은 컴퓨팅 파워를 필요로 한다. 이는 많은 에너지 낭비를 야기하고, 노드의 수가 늘어남에 따라 처리

본 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478, 100%).
* 한성대학교 IT융합공학부 (대학원생, minjoos9797@gmail.com, 대학원생, dnjsdndeee@gmail.com, 대학원생, etus1211@ gmail. com)
** 한성대학교 IT융합공학부 (조교수, hwajeong84@gmail.com)



〔그림 1〕 Operation process of PoW algorithm

속도가 느려지고 확장성이 저하되는 문제점이 있다.

비트코인이나 이더리움과 같이 큰 네트워크의 경우 51% 공격으로부터 안전하여 강력한 보안성을 가지고 있다. 그러나, 작은 규모의 네트워크나 신생 코인의 경우에는 높은 컴퓨팅 파워를 가진 채굴자들의 담합(mining pool)이 일어나면, 51% 이상의 네트워크 컴퓨팅 파워를 확보하는 것이 충분히 가능하므로 51% 공격에 취약해진다. 이에 따라 탈중앙화 기반의 검증 시스템이 무력화되어 기존 거래 내역에 대한 위변조가 발생할 수 있다.

PoW를 기반으로 하는 다양한 합의 알고리즘들이 존재한다. 이중 작업증명은 채굴 전용 하드웨어인 ASIC 채굴기의 사용을 허용하는 메인 알고리즘과 ASIC 채굴기의 사용을 허용하지 않는 서브 알고리즘을 통해 이중으로 작업증명을 수행한다. 이외에도 경과시간증명, 스펙터, 지연작업증명, 균형작업증명 등이 있다. 균형작업증명(ePoW)는 2.8절에서 추가적으로 설명한다.

2.2. Proof of Stake (PoS)

PoS는 블록 생성에 기여한 노드에 보상을 지급하는 합의 알고리즘이다. 이는 PoW 알고리즘의 문제점을 해결하기 위해 도입되었으며, PoW와 다르게 컴퓨팅 파워가 아닌 네트워크 참여자가 가진 지분 (stake)에 비례하여 트랜잭션을 검증하고 보상을 지급한다 [3]. 즉, stake가 많을수록 블록을 검증할 수 있는 확률이 높아지게 된다.

PoS 시스템에서는 중앙집중화를 막기 위해 무작위 블록 선택 또는 코인 나이에 따른 선택을 통해 새로운 블록을 생성할 수 있는 생성자를 결정한다. 무작위 블록 선택 방법은 가장 낮은 해시값과 가장 높은 지분의 조합을 가진 노드를 검증자로 선택한다. 이때, 지분의 크기는 모두에게 공개되어 있으므로 노드들은 일반적으로 다음 검증자를 예측할 수 있다.

코인 나이에 따른 선택 방법은 블록 생성 과정에 참여하고자 하는 노드들이 네트워크상에 일정량의 코인을 자신의 지분으로 staking 해야 한다. Staking은 보상받기 위해 암호화폐의 일정량을 자신의 지분으로 고정하는 것을 의미한다. 코인의 나이는 코인이 stake된 기간과 코인 수의 곱으로 계산되며, 노드가 새로운 블록을 생성하면 코인의 나이는 0으로 초기화된다. 따라서 코인의 나이가 많아질 때까지 일정 시간이 소요되기 때문에 가장 많은 지분을 차지한 노드가 네트워크를 지배하여 다시 블록을 생성하는 것을 방지한다.

PoS는 블록 생성을 위해 컴퓨팅 파워를 소모할 필요가 없어 에너지 효율이 높고 모든 노드에 검증받지 않아도 된다. 따라서, PoS는 PoW보다 거래 처리 속도가 빠르며 에너지 소비도 적다.

또한, 자본이 많을수록 높은 컴퓨팅 파워를 가질 수 있는 PoW보다 PoS가 탈중앙화에 유리하다. 그 이유는 다음과 같다. PoS는 중앙집중화를 방지하기 위해 무작위 블록 선택이나 코인 나이에 따른 선택을 하므로, 자본이 100배이더라도 100배 이상의 지분을 가질 수 없기 때문이다.

하지만, PoS는 전체 토큰의 51%를 한 명의 참여자가 소유할 경우 중앙화된다. 그리고 다수의 코인을 보유하여 staking 할수록 검증 권한은 커지고 검증 보상으로 코인을 받는 것이 반복된다. 또한 체인에 포크가 발생할 때, 자신의 지분 증명을 위한 한계 비용이 없어 지분을 가진 참여자들이 양쪽 체인에 투표하여 블록체인의 정당성을 해칠 수 있다. 이를 해결하기 위해 PoS 알고리즘을 수행할 때 보증금을 내고, 잘못될 경우 보증금의 일부를 잃도록 하는 등의 방법들이 고안되고 있다.

PoS 기반으로 만들어진 다양한 합의 알고리즘이 존재한다. 리스지분증명은 본인 소유의 암호화폐를 다른 노드에 리스 (lease)로 임대해준 후 보상을 받는 합의 알고리즘이다. 하이퍼 위임증명은 일정 시간 안에 빠른 응답이 가능한 노드들만이 합의에 참여하는 합의 알고

리즘이다. 이러한 방식을 통해 기존 블록체인의 속도 문제를 개선할 수 있다. 이외에도 위임지분증명, 마스터노드 지분증명, 포크능력증명 등과 같은 PoS 기반의 합의 알고리즘들이 있다. 위임지분증명(DPoS)은 2.3절에서 설명한다.

2.3. Delegated Proof of Stake (DPoS)

DPoS는 참여자들이 가진 코인의 지분율에 따른 투표권을 행사하여 대표자들을 선출하며, 선출된 대표자들만이 새로운 블록의 유효성을 검증하는 과정에 참여하게 되는 합의 알고리즘이다 [4, 5, 6]. 또한 기존 합의 알고리즘에서의 컴퓨팅 자원을 통한 경쟁을 줄이기 위하여 PoS 기반의 투표 과정을 도입하였으며, PoS에서 64초가 걸리던 블록 생성 시간을 3초로 낮추었다.

DPoS는 투표를 통해 PoS에 비해 민주적으로 대표자를 선출하게 되며, 선출된 대표자들만이 거래내역 검증에 참여하므로 처리 속도 향상에서의 이점이 존재하게 된다. 대표자들은 20~100명의 인원으로 구성되며, 교대로 블록에 대한 검증을 수행한다. 블록은 3초마다 하나씩 차례대로 검증되며, 지정된 시간 안에 검증을 완료하지 못한 경우, 해당 블록을 건너뛰고 다음 블록으로 대체하게 된다.

검증 과정을 통해 새로운 블록을 블록체인에 추가하며, 검증을 진행한 대표자는 해당 블록에 존재하는 트랜잭션들의 수수료를 그에 따른 보상으로써 얻게 된다. 대표자가 보상을 얻게 되면, 투표에 참여한 사람의 지분에 비례하여 보상을 분배하게 된다. 예를 들어, 해당 대표자에게 투표를 한 사람이 전체 코인의 5%의 지분을 가지고 있다면, 보상의 5%를 분배받게 된다. 그러나 대표자가 악의적인 행동을 보이거나 반복적으로 블록을 검증하는 것에 실패하게 되면, 대표자는 검증에 대한 권한을 잃게 되며, 해당 블록을 검증하기 위한 새로운 대표자가 선출된다. 이러한 결격사유가 없다면, 대표자는 장기간 블록을 생성할 수 있는 권리를 보유하게 된다.

대다수의 DPoS 환경에서 유권자들의 투표율이 높지 않아 소수의 유권자가 선출한 대표자가 고정되는 현상이 발생한다. 이는 중앙 집중화 정도를 높여 보안 위험으로 이어지게 되는 문제점을 가지고 있다.

2.4. Proof of Importance (PoI)

PoI는 경제에 대한 중요도에 관계되는 점수를 할당하여 더 높은 중요도 점수를 가지고 있는 계정이 블록을 검증할 가능성이 높아지는 합의 알고리즘이다 [7, 8]. PoI는 PoS와 유사하지만, 코인 지분에 전적으로 의존하지 않고 중요도 점수를 측정하기 위한 다양한 요소가 존재한다는 점에서 차이가 있다. 즉, 노드의 지분만을 고려하는 것이 아닌 네트워크에서의 생산적인 활동을 포함한 사용자의 토큰 사용 및 이동을 모니터링하여 신뢰도와 중요도를 설정한다.

PoI에서는 다음 블록에 대한 검증자로 선택되기 위한 척도로써 지난 30일 동안 사용한 총 통화량, 보유 통화 금액, 다른 노드 간의 상호 연결 정도와 같은 요소가 사용된다. 이는 지난 30일 동안의 거래 내역에서 최근 거래에 대하여 더 많은 가중치를 부여하게 된다. 그리고 블록 생성을 위한 보유 통화 금액이 많거나 상호 연결된 노드의 일부일 경우 더 높은 가중치를 갖게 된다. 이러한 요소에 의하여 비활성 사용자에 대한 패널티를 부과하면서, 활성화된 사용자에게는 보상에 대한 더 많은 기회를 주게 된다.

PoI는 PoS에서의 문제점을 보완하기 위하여 설계되었다. PoS에서는 사용자가 지분을 갖기 위하여 가능한 한 많은 코인을 비축하고, 블록 검증에서 더 많은 보상을 얻기 위하여 거래를 억제함으로써 지분을 차지하는 것에 집중하게 한다. 하지만 PoI의 경우 거래를 활발히 할수록 중요도 점수가 높아지게 되며 보상에 대한 더 많은 기회를 얻을 수 있게 된다. 이는 해당 네트워크의 경제가 활성화된다는 것을 의미하며, 부의 집중을 완화시키거나 부의 재분배를 실현시킬 수 있게 된다. 그리고 PoS에서는 블록 생성에 리소스 비용이 들지 않기 때문에 포크가 이루어질 때마다 양쪽 체인에서 자유롭게 블록을 생성할 수 있게 된다. 그러나 PoI에서의 중요도 점수는 네트워크 상에서의 활동을 기반으로 하기 때문에, 두 개의 포크에서 활동을 자유롭게 하기 위해서는 두 가지 거래 활동 패턴을 지원해야 하므로 두 네트워크에서의 블록을 즉각적으로 생성하기가 어렵다.

2.5. Proof of Elapsed Time (PoET)

PoET는 모든 노드에 동일한 기회를 제공하는 추첨

시스템을 따름으로써 프로세스를 보다 효율적으로 유지하는 합의 알고리즘이다 [9]. PoET는 각 노드에 대하여 무작위로 생성된 대기 시간을 적용하여 해당 시간 동안 휴면 상태를 유지하도록 하며, 대기 시간이 끝난 노드부터 블록에 대한 검증 권한을 갖게 된다. 검증 권한을 가진 노드는 블록을 획득하며, 새 블록을 블록체인에 commit 할 수 있게 된다. 해당 노드는 필요한 정보를 전체 피어 네트워크에 브로드캐스트 하게 되고, 다음 블록을 탐색하기 위하여 동일한 프로세스를 다시 반복하게 된다.

PoET는 잠재적인 충돌을 줄이기 위하여 노드가 많을수록 대기 시간이 길어지며, 정직한 노드보다 빠른 속도로 블록을 생성하는 악의적인 노드를 탐지하기 위하여 통계적 테스트를 사용한다. 그리고 생성 및 검증 비용을 줄이기 위하여 무작위 대기 시간을 여러 번 사용한다.

PoET는 PoW와 유사하지만 PoW는 경쟁 작업 메커니즘으로 수행되고, PoET는 무작위 선택 메커니즘을 갖는다는 차이가 있다. 즉, 네트워크 내의 노드가 검증자로 채택되기 위하여 계속해서 컴퓨팅 파워를 사용할 필요가 없으므로 훨씬 적은 에너지가 사용된다. 그리고 노드가 지정된 시간 동안 절전 모드로 전환되고 그 동안 다른 작업을 수행할 수 있어 네트워크 에너지 효율성이 높아진다.

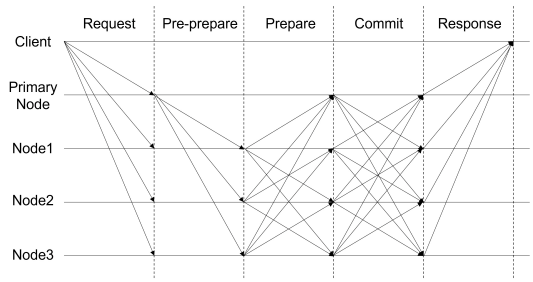
PoET는 보안 환경 (Intel SGX 그리고 ARM TrustZone) 내에서 신뢰할 수 있는 코드를 실행하여 참가자 또는 기타 허가된 기관이 결과를 검증할 수 있게 되어 네트워크 합의의 투명성을 향상시킨다. PoET는 참여 노드가 실제로 무작위이며 참가자가 선택되기 위해 의도적으로 더 짧은 시간을 선택할 수 있는 것이 아닌 특정 분포 내에서 무작위로 시간이 선택되도록 해야 한다. 이때, 최대한 많은 수의 네트워크 참가자에게 당첨 확률을 분산시켜야 한다. 그리고 선택된 노드가 대기 시간을 완료하였는지 확인하는 과정이 존재하여야 한다.

2.6. Practical Byzantine Fault Tolerance (PBFT)

PBFT는 비잔틴 장군 문제를 해결하기 위해 제시되었다. 악의적인 노드가 네트워크 내에 존재하여도 합의를 도출할 수 있는 알고리즘이다. PBFT는 네트워크 내에 악의적인 노드가 f개일 경우 총 노드의 개수 (n)가 $n = 3f + 1$개 이상일 경우 성공적인 합의가 이루어질 수 있다는 이론에 근거한다 [10].

[그림 2]는 PBFT 알고리즘의 동작 방식을 보여준다. PBFT의 동작 방식은 크게 Pre-prepare, Prepare, Commit 단계로 구성된다. 먼저 클라이언트가 Primary 노드에게 상태 변환을 요청하는 메시지를 전송한다. Primary 노드는 클라이언트의 요청을 정렬하고, 요청에 대한 결과를 기입하여 다른 노드들에게 브로드캐스트한다. Primary 노드를 제외한 백업 노드들은 Primary 노드로부터 수신한 pre-prepare 메시지를 다른 노드들에게 브로드캐스트하며, 동시에 다른 노드들로부터 $2f$개의 메시지를 수집한다. 이때, $2f$개의 메시지를 수집한 경우를 prepared certificate라고 하며, 다른 노드들로부터 가장 많이 받은 같은 메시지를 확인한 후에 해당 메시지를 다른 노드들에게 브로드캐스트한다. 동시에 다른 노드들로부터 $2f + 1$개의 메시지를 수집한 경우를 committed certificate라고 한다. 그리고 마지막으로 클라이언트에게 Reply 메시지를 보냄으로써 합의가 이루어진다.

이 같은 과정을 통해, 두 번의 브로트캐스트가 발생하며, 최종적으로 모든 노드가 합의를 이룬 같은 메시지를 가질 수 있다. 이때, 다른 노드들이 Primary 노드의 행동을 보고 악의적인 행동을 한다고 판단된다면, 다수결을 통해 Primary 노드를 교체할 수 있기 때문에 신뢰도가 높은 알고리즘이다. 하지만, 악의적인 노드가 $f = \frac{n-1}{3}$보다 많을 경우에는 정상적인 합의가 되지 않는다. 그리고 모든 노드에 대해 2번씩 브로드캐스트가 발생하므로 통신비용이 증가하고, 확장성이 떨어진다는 단점이 있다.



〔그림 2〕 Operation process of PBFT algorithm

2.7. Proof of Double Committee (PoDC)

PoW, PoS, DPoS, 그리고 PBFT 등은 합의 속도 지연, 에너지 소모 기반 하드웨어 구조, 다수의 노드에 의한 중앙화, 그리고 51% 공격에 취약한 구조를 가지고 있다. PoDC는 DPoS 방식과 PBFT 방식을 개선한 신규 합의 알고리즘인 양원제 합의 알고리즘으로써 기존 문제를 해결한다. PoDC는 ReapChain에서의 내부 노드와 외부 노드 간의 균형을 위해 상임 위원회 노드와 운영 위원회 노드를 운영하고, 해당 노드들로 이중 위원회를 구성하여 합의 과정을 수행한다[11,12].

ReapChain은 블록 생성을 위해 라운드 테이블을 생성한다. 이때 PoDC는 하나의 라운드에서 상시 운영되는 14개의 상임 위원회 노드와 예측 불가능한 양자 난수 (QRN, Quantum Random Number)를 통해 선발된 15개의 운영 위원회 노드가 합의에 참여하게 된다. 이때 ReapChain의 QSN (Quantum Safety Net) 네트워크 내에서 합의가 이루어지므로 신뢰성 및 보안성을 보장할 수 있다.

네트워크에 참여하는 노드의 수가 늘어나 네트워크의 규모가 커지더라도 합의 과정에는 총 29개의 노드만 참여하기 때문에 데이터 처리 속도를 유지할 수 있다. 그리고 상임 위원회가 여전히 정상적으로 운영되고 있는지 확인하기 위하여 운영위 노드의 비율은 항상 52% 이상으로 유지함으로써 합의의 공정성을 확보하여 탈중앙화 문제를 해결한다.

상임 위원회 노드는 처음에 거버넌스 커뮤니티에서 작동한다. 기존 상임 위원회 노드 중 동작을 멈추거나 기준을 충족하지 못한 노드는 별도의 거버넌스 투표 절차를 거쳐야 한다. 운영 위원회 노드 중 상임 위원회의 특정 기준을 만족하는 후보자는 상임 위원회로 선택될 수 있다. 운영 위원회는 양자 난수를 이용한 무작위 선출 방식으로 선택되며, 다시 양자 난수와 공개키를 이용하여 암호화 기능이 포함된 난수 티켓 부여 방식을 사용한다.

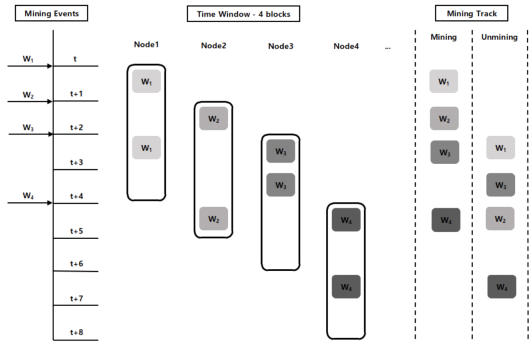
상임위 노드가 전체 합의 노드 중에서 48%를 차지하고 있고, 운영위 노드는 양자 난수를 통하여 선발되기 때문에 악의적인 사용자 노드의 비율이 지속적으로 52%를 점유하는 경우는 불가능하다고 볼 수 있다.

2.8. equilibrium Proof of Work (ePoW)

ePoW는 기존 PoW의 문제점을 보완한 합의 알고리즘으로, Hdac 블록체인을 위해 고안되었다. ePoW는 기존 PoW 방식 기반이지만, 한 번 채굴에 성공한 노드는 일정 기간 강제로 휴식을 취하도록 만들어 다른 노드에 채굴 기회를 공평하게 나누어 주는 합의 알고리즘이다[13]. 이러한 방식으로 합의에 참여하는 노드의 개체 수 감소를 방지하고, 다수의 마이닝 노드가 참여할 수 있는 동기를 부여할 수 있다. 결과적으로, 채굴 경쟁을 위한 과도한 컴퓨팅 파워 투입에 따른 에너지 낭비 방지와 채굴 기회에 대한 공정한 기회 분배를 할 수 있다. [그림 3]은 ePoW 합의 알고리즘을 도식화한 것이다.

ePoW는 작업 증명 주기 안에 채굴을 달성한 마이닝 노드에 대해 연속적 채굴 시도에 제약을 부여한다. 즉 채굴 독과점을 방지하기 위하여 블록 윈도우 개념을 적용하였다. 노드가 채굴에 성공하면, 블록 윈도우 적용 동안은 새로운 블록을 채굴할 수 없다. 만약 블록 윈도우 적용 기간에 블록 채굴에 성공하여도 Hdac 블록체인 전체 네트워크에 유효한 블록으로써 인정받을 수 없으므로 채굴을 시도할 필요성이 사라진다. 따라서 자발적으로 채굴 시도를 하지 않도록 하여 해시 계산에 낭비되는 컴퓨팅 자원을 줄이도록 한다.

블록 윈도우 사이즈 Ws는 시간 함수 $f(t)$로 표현할 수 있으며, $Ws = f(t)$와 같이 나타낼 수 있다. $f(t) = (N \times 0.7) \times t \times tm$ 으로 정의 되며, t는 현재까지의 누적 블록 수를 의미하며, tm은 10년간 누적 블록 수를 의미한다. 노드 인자 N 은 최근 채굴 성공 노드 목록에서 산정된다. 이때, 최대 블록 윈도우 사이즈Ws 도달 시점이 10년인 것은 총 발행량의 80%



〔그림 3〕 ePoW Consensus algorithm

이상에 도달하는 시점으로 지정되었기 때문이다. 이처럼, $f(t)$는 시간에 비례하여 증가하는 함수이다. 이에 따라, 윈도우 사이즈는 시간이 흐름에 따라 점진적으로 증가하게 된다. 이는 곧 초기 참여자에게는 큰 기회가 있으며, 시간이 지남에 따라 특정 채굴 노드가 채굴을 독점하기가 점점 더 어려워지고, 더 공평한 분배가 이루어질 수 있다는 것을 의미한다.

2.9. RAFT

RAFT는 연산 과정이 복잡한 PAXOS의 단점을 보완한 합의 알고리즘이다. RAFT 상에 노드들은 Follower, Candidate, Leader 총 세 가지 종류의 상태가 있다[14].

[그림 4]은 RAFT 내의 서버 노드 상태를 도식화 한 것이다. 모든 노드는 Follower 상태에서 시작하며, Follower 상태 노드는 Leader 노드로부터 AppendEntry 메시지를 받아 처리한다. 만약 Leader 노드의 부재로 일정 시간 동안 AppendEntry를 받지 못할 경우에 Follower가 Candidate 상태로 전환되어 새로운 Leader 노드를 선정한다. Candidate 상태 노드는 Leader 노드로 선출될 가능성이 있는 노드이다. 투표 요청 메시지를 다른 노드에 보낸 시점으로부터 timeout이 시작되며, timeout이 끝나기 전까지 과반의 투표를 받게 되면, Leader 노드로 선정된다. Leader 상태 노드는 Candidate 노드가 Leader 노드로 선정된 상태를 말한다. Leader 노드의 역할은 클라이언트로부터 받은 변경 사항을 Leader 노드의 LogEntry에 저장한 후에, AppendEntry 메시지를 Follower 노드에 전송한다. LogEntry는 Term과 Index 그리고 Data를 포함하고 있다. Term은 Leader 노드를 선출할 때마다 1씩 증가하는 번호로써 Leader 노드의 ID 역할을 한다. Index는 새로운 Log가 저장될 때마다 1씩 증가하는 번호이다. Leader 노드로부터 AppendEntry 메시지를 받은 Follower 노드는 새로운 Log Entry를 저장한 후, Leader 노드에 AppendEntryResponse 메시지를 보낸다. Leader 노드는 Follower 노드 중에서 과반수로부터 AppendEntryResponse 메시지를 받았다면, entry를 commit한 후에 client에게 응답 메시지를 보내고, Follower 노드에는 entry가 commit되었음을 알린다. commit되었음을 알게 된 Follower 노드들은 각자 자신의 entry를 commit한다. 이로써 모든 노드가 동일한 데이터를 갖게 된다.

RAFT는 블록이 블록체인에 추가되는 즉시 블록의 Finality가 보장되기 때문에 fork가 발생하지 않으며, 여러 노드 중 일부에 장애가 발생하더라도 합의가 진행된다는 장점을 가지고 있다. 또한 기존의 연산 과정이 복잡하여 이해하기 어려운 PAXOS 알고리즘과 달리 RAFT는 프로토콜이 복잡하지 않으며 구현하기 용이하도록 설계되어있다.

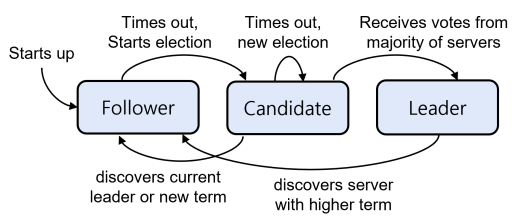
Ⅲ. 블록체인 기반 IoT 프로젝트

본 장에서는 블록체인 기반 IoT 프로젝트들의 최신 동향에 대해 살펴본다.

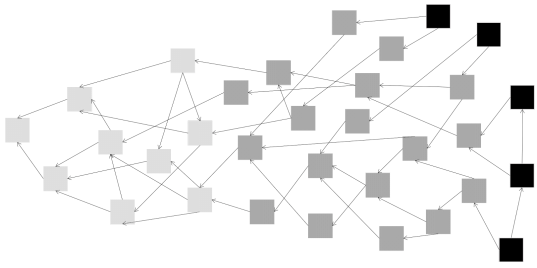
3.1. IOTA

IOTA (Internet of Things Application)는 독일의 스타트업으로, 블록체인이 아닌 Tangle 알고리즘을 기반으로 개발된 암호화폐이다 [15, 16, 17]. Tangle은 방향성 비순환 그래프 (Directed Acyclic Graph, DAG)를 기반으로 하는 알고리즘이다. [그림 5]은 Tangle의 구조를 나타낸 것이다.

비트코인과 이더리움은 다수의 트랜잭션을 하나로 관리하기 위해 블록이라는 개념을 사용하였다. 이와 달리 Tangle은 트랜잭션을 관리하기 위해 블록을 사용하



〔그림 4〕 Server states in RAFT.



〔그림 5〕 Structure of IOTA Tangle.

지 않는다. 블록 대신 새로운 트랜잭션을 발행하기 위해서 검증되지 않은 2개의 트랜잭션을 승인해 주는 방식으로 동작한다. IOTA는 아직 검증되지 않은 트랜잭션을 Tip이라고 칭한다. IOTA는 채굴자가 없으므로 새로운 트랜잭션을 발행할 때는 TSA (Tip Selection Algorithm)을 사용한다. 예를 들어, 참여자 A가 새로운 트랜잭션 T를 생성하기 위해서는 임의로 선택된 Tip 2개의 트랜잭션을 A가 검증해야 한다. 이 과정은 다음과 같다.

A의 개인키로 트랜잭션 T에 서명한 후, 기존 네트워크에 포함된 2개의 Tip을 TSA를 사용하여 선택한다. 그리고 2개의 Tip에 대해 A는 충돌하는지 검사를 한다. 검사 결과 2개의 Tip이 충돌하지 않는다는 결과가 나오면, 2개의 Tip에 대해 검증을 진행한다. 이처럼, 트랜잭션을 생성한 거래자 (참여자)는 동시에 트랜잭션 검증도 해야 하므로 IOTA Tangle은 거래 수수료가 없고, 거래자가 많을수록 트랜잭션의 처리 속도도 빨라진다.

3.2. IoT Chain

IoT Chain (ITC)은 중국의 IOTA라고도 불리며, 사물인터넷에 블록체인 기술을 적용하기 위해 PBFT, SPV (Simple Payment Verification), DAG (Directed Acyclic Graph), 그리고 CPS (Cyber Physical System) 등을 채택하였다 [15, 18, 19].

ITC는 메인체인에서 PBFT 합의 알고리즘을 사용하고 사이드체인에서 DAG를 사용하기 때문에 효율적으로 트랜잭션을 처리할 수 있다. 그리고 SPV를 사용하여 DAG의 데이터 확장문제도 해결하였다. SPV는 블록의 헤더만으로 지불 확인을 수행하는 것을 의미하며, 블록체인 결제 확인 비용을 감소시키는 이점을 갖고 있다. ITC는 SPV를 사용하여 결제 확인의 효율성을 높여 전체 네트워크의 성능 향상을 보장하였다. 그리고 대량의 계산과 빅데이터를 기반으로 하는 다차원 스마트 기술 시스템인 CPS를 참고하여 ITC의 시스템 구조를 구축하였다.

2020년 4월 기준으로 ITC의 메인체인 네트워크 노드 동기화에 대한 최적화가 완료되었고, ITC를 적용한 탈 중앙화된 암호화 자산 관리 도구 제품을 개발하는 중이다. 그리고 중국 국내 자동차 플랫폼과 협력하여 자동차 지능형 하드웨어에 대한 블록체인을 구축하는 자동차 네트워킹 솔루션이 진행 중이다.

3.3. IBM-ADEPT

IBM-ADEPT는 IBM과 삼성이 공동으로 개발한 Autonomous Decentralized to Peer-to-Peer Telemetry (ADEPT) 프로젝트로, ADEPT는 사물인터넷 환경에서 확장성과 보안이 강화된 P2P (Peer-to-Peer) 블록체인 시스템이라고도 불린다[20]. ADEPT는 이더리움 (Ethereum), BitTorrent, 그리고 TeleHash 기술을 기반으로 한다. 이더리움은 블록체인을 기반으로 한 스마트 컨트랙트를 구현하기 위한 분산 컴퓨팅 플랫폼이다. BitTorrent는 P2P 파일 전송 프로토콜이며, BitTorrent를 이용하면 효율적으로 대용량 파일을 전송하는 것이 가능하다. TeleHash는 암호화된 개인 메시 (mesh) 네트워킹 프로토콜로, 중앙 서버 권한 없이 데이터를 안전하게 공유할 수 있는 특징을 갖고 있다.

또한, 이더리움을 통해 ADEPT에 연결된 사물인터넷 장치가 서로 안전하고 효율적으로 통신하는 것이 가능하다. 이러한 특징을 활용해 IBM은 ADEPT 기술이 적용된 스마트 삼성 세탁기에서 발생할 수 있는 여러 사례를 보여주었다. ADEPT 기술이 적용된 삼성 세탁기는 세제 공급 부족을 감지하고, 기존 계약이 체결되어 업체에 세제 주문을 요청하는 등의 작업을 수행할 수 있다. 그리고 해당 세탁기가 고장 났을 경우, 자체 점검이 가능한 스마트 기능이 탑재되었기 때문에 시스템은 어느 위치가 고장 났는지 판단한다. 예를 들어, 시스템이 모터가 고장 났다고 판단하면, 모터의 보증기간에 대해 확인을 한다. 보증기간이 아직 남아있다면, 시스템은 주변 수리점을 확인하여 출장 수리에 대해 요청을 한다. 보증기간이 끝났다면, 소유주에게 수리점과 따로 계약을 맺어야 한다고 알리고, 수리점에서 제시한 견적에 대한 정보를 전달하는 등의 작업을 수행한다.

3.4. SLOCK IT

SLOCK.IT은 독일 스타트업으로, 이더리움 기반의 USN (Universal Sharing Network)인 공유 경제를 위한 플랫폼을 만드는 것을 목표로 한다 [21, 22]. SLOCK.IT은 이더리움의 스마트 계약을 통해 Smart Lock의 기능이 포함된 제품을 직접 공유할 수 있으며,

대여하거나 판매를 하는 것도 가능하다.

거래단위는 이더리움의 화폐인 이더 (Ether)로, 이더를 지불하여 스마트 계약이 실행되면 스마트 잠금장치가 장착된 제품에 대해 잠금이 해제되어 해당 제품에 대한 거래가 가능하다. 이용자들이 사용하고 있지 않은 제품에 대해 직접적인 키 교환 없이 온라인으로도 키 교환이 가능하다. 현재 SLOCK.IT은 캐나다 회사인 Blockchain Development Labs (BC Development Labs)의 자회사이며, BC Development Labs GmbH로 명칭이 변경되었다. IoT 상에서의 공유 경제를 위한 플랫폼을 만드는 목표를 넘어서 개인의 디지털 자산을 보호하기 위한 플랫폼을 목표로 개발하고 있다.

3.5. Hyperledger Fabric

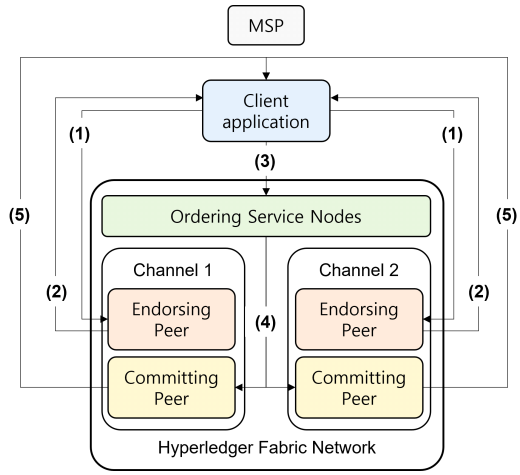
하이퍼레저 패브릭은 리눅스 재단에서 기업용 블록체인 개발을 위해 만든 오픈 소스 형태의 프로젝트이다. 누구나 참여할 수 있어 참여자 간의 신뢰가 없는 퍼블릭 블록체인과 달리, 신원 확인이 된 경우에만 참여할 수 있는 허가형 프라이빗 블록체인이다 [23]. 따라서 신원 확인이 된 사용자만이 하이퍼레저 패브릭 블록체인에 참여할 수 있어 악의적인 행동을 하는 참여자가 생길 위험이 타 블록체인보다 적다.

하이퍼레저 패브릭을 구성하는 요소는 채널, MSP (Membership Service Provider)와 5가지 종류의 노드 (Endorsing, Committing, Anchor, Leader Peer, Ordering Service node)가 있다. 이를 통해 트랜잭션에 대한 접근 권한을 제어하고, 참여자들에 대한 인증을 수행한다. 그리고 블록체인 네트워크 유지, 트랜잭션 처리, 그리고 원장 및 체인코드 관리 등의 작업을 한다.

하이퍼레저 패브릭은 블록체인 네트워크의 논리적 분할이 가능하며, 각 분할된 네트워크를 채널이라고 한다. 분리된 채널 간에는 체인코드 및 분산 원장 공유가 불가능하며, 채널에 대한 권한이 있는 참여자만 접근할 수 있다. 이때, 체인 코드를 통해 스마트 컨트랙트와 같이 애플리케이션의 로직을 만들고 실행할 수 있으며, 이는 Go, Java, 그리고 Javascript 언어를 통해 구현할 수 있다.

하이퍼레저 패브릭의 구성요소 중 하나인 MSP는 인증 및 인가를 관리하는 중앙 인증 기관이며, MSP를 통해 인증서를 발급받아 블록체인 네트워크에 접근할 수 있다. 그리고 해당 인증서가 폐기되거나 변조되면, 접근 권한을 폐기한다. MSP가 있음으로써 참여자가 새로운 블록을 추가하면, 해당 참여자의 전자서명이 블록에 기록된다. 이에 따라 어떤 참여자가 어떤 블록을 추가했는지 추적할 수 있고 채널 및 정책 등을 설정하여 참여자들 간의 프라이버시가 강화된다.

하이퍼레저 패브릭의 세부 동작 과정은 [그림 6]과 같다. 먼저 클라이언트 애플리케이션에서 블록체인 네트워크에 Endorsing peer들에게 트랜잭션을 요청한다. 해당 트랜잭션 proposal에는 사용자의 정보가 서명 형태로 삽입되어있다([그림 6]의 (1)). Endorsing peer들은 해당 서명과 트랜잭션을 확인한 후 체인 코드를 실행하여 클라이언트 애플리케이션에게 proposal response를 전송한다. 해당 과정에서는 실제 분산원장에 결과가 반영되지 않는다 ([그림 6]의 (2)). 클라이언트 SDK가 Endorsing peer들의 서명을 확인하고, 각 peer들로부터 수신한 proposal response를 비교한다. 위와 같은 과정을 통해 비교 검증을 수행한 후, 클라이언트는 proposal과 proposal message가 담긴 트랜잭션을 ordering service에 보낸다. 그 후, ordering service node에서는 해당 트랜잭션을 수신하여 시간순으로 정렬하여 블록을 생성한다 ([그림 6]의 (3)). 트랜잭션 블록이 각 채널의 committing peer에게 전달되고, 해당 peer는 트랜잭션을 확인한 후, valid 또는 invalid 값을 태그한다([그림 6]의 (4)). 각 피어들은 위와 같은 과정을 통해 검증을 마친 블록을 채널 내의 원장에 추가하



〔그림 6〕 Transaction flow in Hyperledger Fabric.

고, 클라이언트에게 결과를 전송한다 ([그림 6]의 (5)).

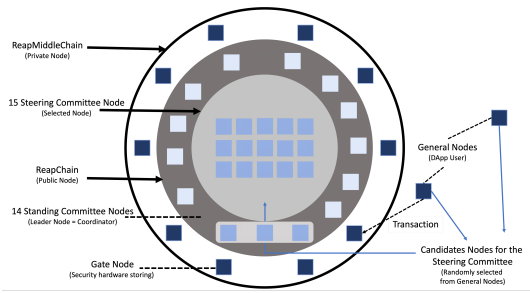
하이퍼레저 패브릭은 응용 프로그램을 개발하기 용이하도록 모듈형 구조로 되어 있어 유연성이 보장되고 최적화에 용이하다. 1.x 버전에서는 Kafka, 2.x 버전에서는 RAFT 합의 알고리즘을 사용한다. 허가형 블록체인은 모든 노드가 검증된 노드이므로 신뢰를 기반으로 하기 때문에 이보다 더 복잡한 합의 알고리즘이 요구되지는 않는다. Kafka, RAFT 모두 CFT (Crash fault tolerance) 방식이다. 해당 방식은 BFT에 비해 보안성이 떨어지지만 간단하고 빠르다는 이점이 있다.

3.6. ReapChain

ReapChain은 국내 스타트업으로, 새로운 하이브리드 블록체인을 구현하였다 [24, 25, 26]. 또한, 새로운 합의 알고리즘인 PoDC (Proof of Double Committee)를 제안하였으며, 블록체인의 Trilemma를 해결하였다. PoDC에 대한 자세한 사항은 2.7절에서 설명되었다. ReapChain의 하이브리드 블록체인은 Shell-core 구조로 되어 있다. Shell-Core 구조는 ReapMiddleChain이라는 프라이빗 블록체인과 ReapChain이라는 퍼블릭 블록체인이 합쳐진 이중 체인 구조이다. [그림 7]은 Shell-Core 구조를 나타낸 것이다.

[그림 7]에서 확인할 수 있듯이 속도가 빠른 프라이빗 블록체인인 ReapMiddleChain이 외부에 배치되어 트랜잭션을 먼저 처리한다. 처리한 트랜잭션의 응답 값을 DApp들에 즉시 제공한다. 그리고 탈중앙화와 보안성이 높은 퍼블릭 블록체인인 ReapChain을 내부에 배치하여 미리 프라이빗 블록체인에서 처리한 트랜잭션에 PoDC 합의 알고리즘을 적용하여 최종 블록으로 만든다.

현재 사용되는 블록체인은 네트워크 참여자들 간의 모든 합의를 완료하는 것으로 거래 투명성과 신뢰성을 확보한다. 그러므로 데이터의 실시간 처리가 불가능하다는 단점이 있다. ReapChain은 거래 처리 속도 문제를 해결하기 위해 임시 원장 (Temporary Ledger)과 영구 원장 (Permanent Ledger)의 개념을 도입하였다. 프라이빗 블록체인인 REAP Middle Chain에 데이터를 저장하여 임시 원장으로 사용한다. 그 후, 퍼블릭 블록체인인 ReapChain에 블록 데이터를 기록하고 영구 원장으로 관리한다.



〔그림 7〕 Sell-Core Structure of Reapchain.

ReapChain은 준비 단계에서 Proposal Block을 전파하는 것을 제외하고, 일정한 형태로 구성되어 있다. 그러므로 블록체인의 네트워크를 확장하여 네트워크의 노드의 수가 증가하더라도 PoDC 합의 과정에서는 항상 고정된 숫자의 노드만 참여하여 진행된다. 따라서, 네트워크가 확장되더라도 처리 속도는 일정하게 유지되며 이에 따라 확장성을 확보할 수 있다.

ReapChain의 탈중앙화는 다음을 만족한다. 모든 블록이 생성되고 확정되는 과정이 자발적으로 진행된다. 이때 각 블록이 생성될 때마다 합의 과정에 참여하는 주체도 달라진다. 그리고 블록 확정을 위한 노드를 후보군으로 확정하는 것도 지정된 알고리즘에 의해서 이뤄진다.

ReapChain은 보안성을 만족하기 위해서는 기밀성, 가용성, 그리고 무결성을 유지해야 한다. ReapChain의 블록이 생성될 때, 권한이 있는 사용자만 접근할 수 있도록 공개키 방식을 사용한다. 이때, 양자 난수를 사용하여 선택된 노드만 열람할 수 있도록 각 노드별로 공개키를 별도로 제공하여 블록을 확정하는 단계에서 허가된 노드만 투표에 접근하도록 한다. 이와 같은 이유로 ReapChain은 기밀성을 유지하며, 모든 사용자가 보안키를 이용하여 생성한 블록만 접근할 수 있으므로 가용성도 유지한다. 그리고 ReapChain은 양자 난수를 사용하여 블록을 확정하기 때문에 무결성을 유지한다. 이에 따라 ReapChain은 보안성이 만족된다.

ReapChain에서 제공하는 로드맵에 따르면, 2021년 4가지 분야에 대해 오픈베타를 거쳐 정식 서비스를 운영하였다. 그 분야는 PID 기반 IoT 물류시스템, ReapChain 기반 간편결제, ReapChain 기반 매출 누락 방지, 그리고 디지털 전통시장 및 배달 솔루션이다. 2022년은 메인넷 정식 오픈을 목표로 하고 있다.

3.7. IoTex

IoTeX는 미국의 스타트업으로, 다수의 블록체인이 계층적으로 구성된 네트워크이다[27]. 계층적으로 구성된 다수의 블록체인은 동시에 동작한다. 루트 체인은 퍼블릭 블록체인이며, 독립적인 서브 체인을 관리하는 구조로 되어 있다. 서브 체인은 루트 체인에 의존적이며, 사물인터넷 기기와 연결되어 상호작용한다. 서브 체인과 루트 체인은 분리되어 있어 서브 체인이 제대로 동작하지 않아도 루트 체인은 영향을 받지 않는다. IoTeX 토큰은 루트 체인의 토큰으로, 서브체인은 IoTeX 토큰을 사용하거나 서브 체인 자체 토큰을 발행하여 사용한다. 서브 체인에서 발행한 토큰은 판매하거나 공개적으로 거래되는 거래소에서 교환이 가능하다.

IoTeX는 DPoS, PBFT, 그리고 VRFs (Verifiable Random Functions)의 개념을 결합한 Roll-DPoS 합의 알고리즘을 제안하였다. DPoS와 PBFT에 대한 설명은 2장에서 제시되어 있다. VRFs는 입력에 대해 검증 가능한 의사 난수 값을 출력하는 함수이다.

Roll-DPoS는 총 4단계로 구성되어 있다. 모든 노드가 참여 가능한 투표를 통해 위원회를 구성하고, 선정된 모든 위원회 노드는 블록을 제안한다. 그리고 블록을 제안하지 않은 모든 다른 노드들은 PBFT를 통해 후보자 블록에 대한 투표를 진행하여 블록을 확정한다.

IoTeX는 스마트홈, 자율주행 자동차, 공유 경제 등의 다양한 분야에 활용된다. 2021년 IoTeX가 발표한 로드맵에 따르면, 탈중앙화된 자율 기계 (DAMs, Decentralized Autonomous Machines)를 도입한다. DAMs를 등록하고 관리하기 위한 개방형 프레임워크를 개발을 계획하고 있다.

3.8. Hdac

Hdac은 현대BS&C에서 설립한 회사인 에이치닥 테크놀로지에서 사물인터넷 산업의 효율성과 보안을 보장하기 위해 인증, M2M (Machine to Machine) 거래, 그리고 매핑 등을 지원하기 위한 목적으로 개발되었다[28, 29]. 인증은 다수의 디바이스나 사용자가 서로를 정확하게 확인할 수 있는 것을 의미하고, M2M 거래는 다수의 디바이스에서 특정 금액에 대해 청구하거나 지불하는 것이 가능한 것을 의미한다. 매핑은 사용자나 디바이스에 대한 인증이 완료된 후, 서로 연결되는 것을 의미한다.

퍼블릭 블록체인인 Hdac에 다수의 프라이빗 블록체인이 사이드체인 형태로 연결되는 구조로 되어있다. 프라이빗 블록체인은 최초로 생성된 블록체인 노드를 구축한 관리자가 다른 노드에 권한을 부여할 수 있고, ePoW와 라운드로빈 방식으로 블록을 생성할 수 있다. 프라이빗 블록체인은 암호화된 채널을 만들어서 통신할 수 있는 기능도 제공하는데 이 채널을 생성한 두 명의 특정한 사용자만 이용할 수 있다.

Hdac은 프라이빗 블록체인에서 동작하는 사물인터넷 기기 간의 상호 인증과 트랜잭션을 위한 Hdac*T라는 토큰을 사용하는 플랫폼이다. 그리고 기존 PoW의 문제점인 컴퓨팅 파워에 따라 채굴 환경이 집중되는 현상을 해결하기 위해 새로운 합의 알고리즘인 ePoW를 개발하였다. ePoW는 2.8절에서 상세히 설명되어 있다.

2022년 1월 기준으로 Hdac은 스테이블 코인을 출시하고 발행할 것이라고 하였다. 스테이블 코인은 기존의 화폐 (실물 자산)와 일대일로 연동시켜 가격의 안전성을 보장하도록 설계된 암호화폐이다. 그리고 NFT (Non-Fungible Token)와 스마트 계약 등의 핵심 기술을 개발하는 것 등의 로드맵을 공개하였다. 2021년에 Hdac의 새로운 메인넷인 RIZON이 출범되는 등의 목표를 달성하였다.

Ⅳ. 결 론

본 논문에서는 블록체인의 다양한 합의 알고리즘과 사물인터넷 상에서의 블록체인에 대한 동향을 살펴보았다. 기존 합의 알고리즘을 기반으로 하는 사물인터넷 상에서의 블록체인과 함께 보다 사물인터넷에 최적화된 새로운 합의 알고리즘도 활발히 연구되고 있음을 확인할 수 있다. 이에 따라, 향후 사물인터넷의 발전과 상용화에 따라 사물인터넷 상에서의 블록체인과 이에 따른 합의 알고리즘에 관한 지속적인 연구가 필요할 것으로 판단된다.

참 고 문 헌

[1] Markets and Markets, IoT Technology Market with COVID-19 Impact Analysis, by Node

Component (Sensor, Memory Device, Connectivity IC), Solution (Remote Monitoring, Data Management), Platform, Service, End-Use Application, Geography－Global Forecast to 2027. 2021. Available online: https://www.marketsandmarkets.com/Market-Reports/iot-application-technologymarket-258239167.html (accessed on 12 January 2022).

[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[3] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." self-published paper, August 19.1 (2012).

[4] Hu, Qian, et al. "An improved delegated proof of stake consensus algorithm." Procedia Computer Science 187 341-346 (2021).

[5] Saad, Sheikh Munir Skh, and Raja Zahilah Raja Mohd Radzi. "Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos)." International Journal of Innovative Computing 10.2 (2020).

[6] Yang, Fan, et al. "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism." IEEE Access 7, 118541-118555, (2019).

[7] Alyaseen, Imad Fakhri Taha. "Consensus algorithms blockchain: A comparative study." International Journal on Perceptive and Cognitive Computing 5.2, 66-71(2019).

[8] Gamage, H. T. M., H. D. Weerasinghe, and N. G. J. Dias. "A survey on blockchain technology concepts, applications, and issues." SN Computer Science 1.2, 1-15 (2020)

[9] Chen, Lin, et al. "On security analysis of proof-of-elapsed-time (poet)." International Symposium on Stabilization, Safety, and Security of Distributed Systems. Springer, Cham, 2017.

[10] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery." ACM Transactions on Computer Systems (TOCS) 20.4 (2002): 398-461.

[11] REAPCHAIN, “Introduction of PoDC (Proof of Double Committee) Consensus Algorithm”, https://medium.com/reapchain/introduction-of-podc-proof-of-double-committee-consensus-algorithm-87793054d624

[12] REAPCHAIN, “PoDC (Proof of Double Committee) consensus algorithm”, https://medium.com/reapchain/podc-proof-of-double-committee-consensus-algorithm-4c8680cc293b

[13] Hdac, https://hos-forward.s3-accelerate.amazonaws.com/hos/download/Hdac_WhitePaper(KOR)_v1.0.2.pdf

[14] Ongaro, Diego, and John Ousterhout. "In search of an understandable consensus algorithm." 2014 USENIX Annual Technical Conference (Usenix ATC 14). 2014.

[15] Hong, Eungi, Soojin Lee, and Seung-Hyun Seo. "사물 인터넷을 위한 블록체인 기술 동향." Review of KIISC 28.3 (2018): 38-46.

[16] Popov, Serguei. "The tangle." White paper 1.3 (2018).

[17] IOTA, https://blog.iota.org/

[18] IoT Chain, https://iotchain.io/

[19] IoT Chain, “IoT Chain A high-security lite OS”, 2018

[20] IBM, "ADEPT: An IoT Practitioner PerspectiveD", 2015.

[21] SLOCK.IT, https://slock.it/usn.html

[22] SLCOK.IT, https://goodrobot.com/papers/Slock.it_Blockchain-Research-Institute.pdf

[23] Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." Proceedings of the thirteenth EuroSys conference. 2018.

[24] REAPCHAIN, https://reapchain.com/index.php

[25] REAPCHAIN, “WHITE Paper ver 0.9” https://reapchain.com/file/kr/WhitePaper.pdf

[26] REAPCHAIN, “Yellow Paper ver 0.7” https://reapchain.com/file/kr/YellowPaper.pdf

[27] IoTex, https://iotex.io/research

[28] Hdac, https://hdactech.com/

[29] Hdac, https://github.com/Hdactech/doc/wiki/Whitepaper

〈저자소개〉

심 민 주 (MinJoo Sim)
정회원
2021년 2월 : 한성대학교 IT융합공학부 학사 졸업
2021년 3월~현재 : 한성대학교 IT융합공학부 석사과정
<관심분야> 암호구현, 정보보호

김 원 웅 (WonWoong Kim)
정회원
2022년 2월 : 한성대학교 IT융합공학부 학사 졸업
2022년 3월~현재 : 한성대학교 IT융합공학부 석사과정
<관심분야> 인공지능, 블록체인

강 예 준 (YeaJun Kang)
정회원
2022년 2월 : 한성대학교 IT융합공학부 학사 졸업
2022년 3월~현재 : 한성대학교 IT융합공학부 석사과정
<관심분야> 블록체인, 인공지능 보안

서 화 정 (HwaJeong Seo)
종신회원
2010년 2월 : 부산대학교 컴퓨터공학과 졸업
2012년 2월 : 부산대학교 컴퓨터공학과 석사
2015년 4월~5월 : 싱가포르 난양공대 인턴쉽
2016년 2월 : 부산대학교 컴퓨터공학과 박사
2017년 3월 : 싱가포르 과학기술청 연구원
2017년 4월~현재 : 한성대학교 조교수
<관심분야> 블록체인, 인공지능 보안