컴퓨터 알고리즘 1주차 과제

2019040164 정지오

과제: 4차산업혁명의 기술들 중 컴퓨터 알고리즘의 발달을 가장 잘 설명할 수 있는 기술을 제시하고 그 기술에 대해 응용되어 사용된 컴퓨터 알고리즘에 대해 조사하여 제출하세요.

저는 4차산업혁명의 기술들 중 컴퓨터 알고리즘의 발달을 가장 잘 설명할 수 있는 기술은 블록체인 기술인 것 같습니다. 먼저 블록체인 기술과 블록체인 기술을 가능케하는 알고리즘에 대해 간단하게 설명하겠습니다. 블록체인 기술이란 온라인 거래 정보를 수정할 수 없도록 데이터를 블록(block)으로 만들고 암호기술을 사용한 고리 모양의 체인(chain)으로 연결하여 분산 컴퓨팅 기술로 저장 · 관리하는 방식을 말합니다. 이러한 블록체인은 일정 시간 동안 네트워크 참여자가 거래 정보를 서로 교환해 확인하고 검증하는 과정을 거쳐, 서로 동의한 거래 정보들만 하나의 블록으로 만드는 방식으로 진행됩니다. 그리고 새로 만들어진 블록을 전 블록체인에 연결하고 그 복사본을 만들어서 각 네트워크의 참여자에게 전송해 분산해서 저장합니다. 이때 정보를 안전하게 저장하게 위해 블록체인은 중앙화 된 서버 대신 합의 알고리즘을 사용합니다. 합의 알고리즘이란 분산원장 시스템 내의 모든 노드(node)가 일관성 있는 분산원장을 보유할 수 있도록 네트워크 연결을 통해 새로운 기록의 공유, 검증 및 추가에 대한 전체의 동의를 이끌어 내는 알고리즘을 말합니다. 개념이 좀 어려운 것 같아 쉽게 설명해보겠습니다. 블록체인은 앞서 말씀드렸듯이 기본적으로 분산 시스템입니다. 데이터를 안전하게 저장하기 위해 각 참여자들에게 정보를 분산시켜 저장하는 것이죠. 즉, 참여자 모두가 볼 수 있는 장부인 것입니다. 이렇게 모든 거래자가 거래 장부를 소유하기 때문에 중앙화된 서버보다 신뢰성과 보안성이 높습니다. 이러한 합의 알고리즘에는 PoW(Proof of Work), PoS(Proof of Stake), DPoS입니다. DPoS(Delegated Proof of Stake)등이 존재합니다.

이제 본론으로 들어가서 블록체인이 사용하는 기본 알고리즘에 대해 설명하겠습니다. 블록체인이 사용하는 컴퓨터의 기본 알고리즘은 바로 Brute force Algorithm입니다. Brute force Algorithm이란 무차별 대입 알고리즘으로, 카운터를 늘리고 새로운 해시를 계산하고 검증하는 과정을 반복하는 알고리즘입니다. 이를 이해하기 위해서 해시에 대해 먼저 알아야 하므로 해싱, 해시, 해시 함수에 대해 설명하겠습니다. 해싱이란 어떤 특정한 데이터에 대한 해시를 얻는 과정입니다. 해시란 계산된 데이터의 고유한 표현값입니다. 해시 함수는 임의의 길이를 가진 데이터를 입력으로 받아 고정된 길이의 해시값을 생성하는 함수입니다. 블록체인에서 해싱은 블록의 일관성을 보장하는데 사용됩니다. 해싱 알고리즘의 입력 데이터에는 이전 블록의 해시값도 포함되어 있기 때문에 체인상의 어떤 한 블록을 변경하는건 거의 불가능합니다. 하나의 블록을 변경하면 해당 블록에 대한 해시와 그 이후의 모든 블록들에 대한 해시를 다시 계산해야 하기 때문입니다. 이러한 알고리즘은 가상화폐에서 사용됩니다. 비트코인을 예로 들어보겠습니다. 비트코인은 초기에 이메일 스팸을 방지하기 위해 개발된 작업 증명 알고리즘인 해시캐시를 사용했습니다. 알고리즘은 다음 스텝들로 나눌 수 있습니다. 먼저, 공개적으로 알려진 데이터를 가져옵니다. 여기에 카운터를 더합니다(카운터는 0부터 시작합니다). 그 후에 data + counter의 해시를 구하고 해시가 특정 요구사항을 충족하는지 확인합니다. 이를 충족한다면 알고리즘을 끝내고 그렇지 않다면 카운터를 증가시켜 3번과 4번 스텝을 반복합니다. 즉, 이는 무차별 대입 (Brute-force) 알고리즘으로 카운터를 늘리고 새로운 해시를 계산하고 검증하는 과정을 반복하는 것입니다.