# Chapter 1. 블록체인의 이해

블록체인은 거래의 묶음으로 만들어진 블록들을 서로 연결해서 (chaining) 구성한다. 분산시스템에서는 합의를 통해서 블록을 인증하고 블록체인으로 이렇게 연결해 나간다. 많이 쓰이고 있는 합의방식은 작업증명 PoW이고, 지분증명 PoS을 적용해 나가고 있다. 블록체인은 금융, NFT, 물류 등에 적용되고 있다. 처리속도가 느리고, 저장용량이 증가한다는 문제를 풀기 위해 샤딩, 라이트닝 네트워크와 같은 방식을 활용할 수 있다.

# 1. 블록체인에 대한 관심

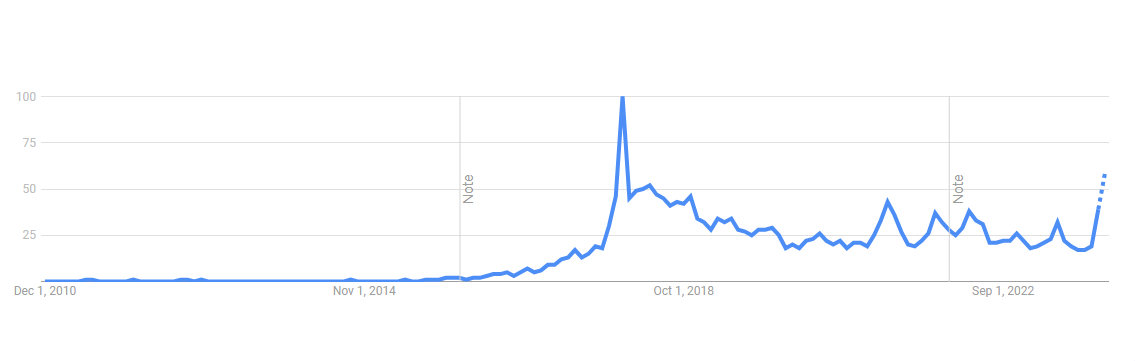
골드러시! 때 아닌 골드러시라고 심드렁하게 말하겠지만, 현재 새로운 디지털골드가 나타났다고 한다. 디지털 시대에 금 역할을 할 것이라는 거창한 약속과 함께 말이다.

암호화폐에 대한 보도가 늘어나면서, 아무리 관심이 없다고 하더라도 "비트코인"이라는 단어를 들어봤을 것이다. 처음에는 일부 극소수만 알고 있다가, 이제는 누가 말해도 이상하지 않을 정도로 알려지고 있다.

뉴스 보도량만 봐도 그렇다. 비트코인 가격이 올랐다는 등 암호화폐와 관련하여 보도가 늘어나고 있고, 이를 반증하듯이 구글 트랜드를 보면 비트코인이나 블록체인에 대한 검색이 2017년 이후 급격하게 증가했다는 것을 볼 수 있다. 그 후 비트코인이나 암호화폐의 가격이 오르고 내리는 정도에 따라 검색량이 등락을 하고 있다.

여러 통계를 보면, 블록체인 시장은 급격히 늘어가는 것으로 보인다. 가트너는 2025년 1760억달러, 2030년에는 폭발적으로 증가해 3조 1천억달러에 이를것이라고 전망하고 있다. 미국이 전체의 40%를 지출, 서유럽, 중국, 아시아태평양 (일본 제외) 순서로 뒤따를 것으로 예상했다.

블록체인은 내재한 암호화폐를 통해 지급결제 플랫폼으로 유용성이 있지만, 확산되는 단계로 진입할지 아직은 두고 볼 일이다.



alt text

# 2. 블록체인

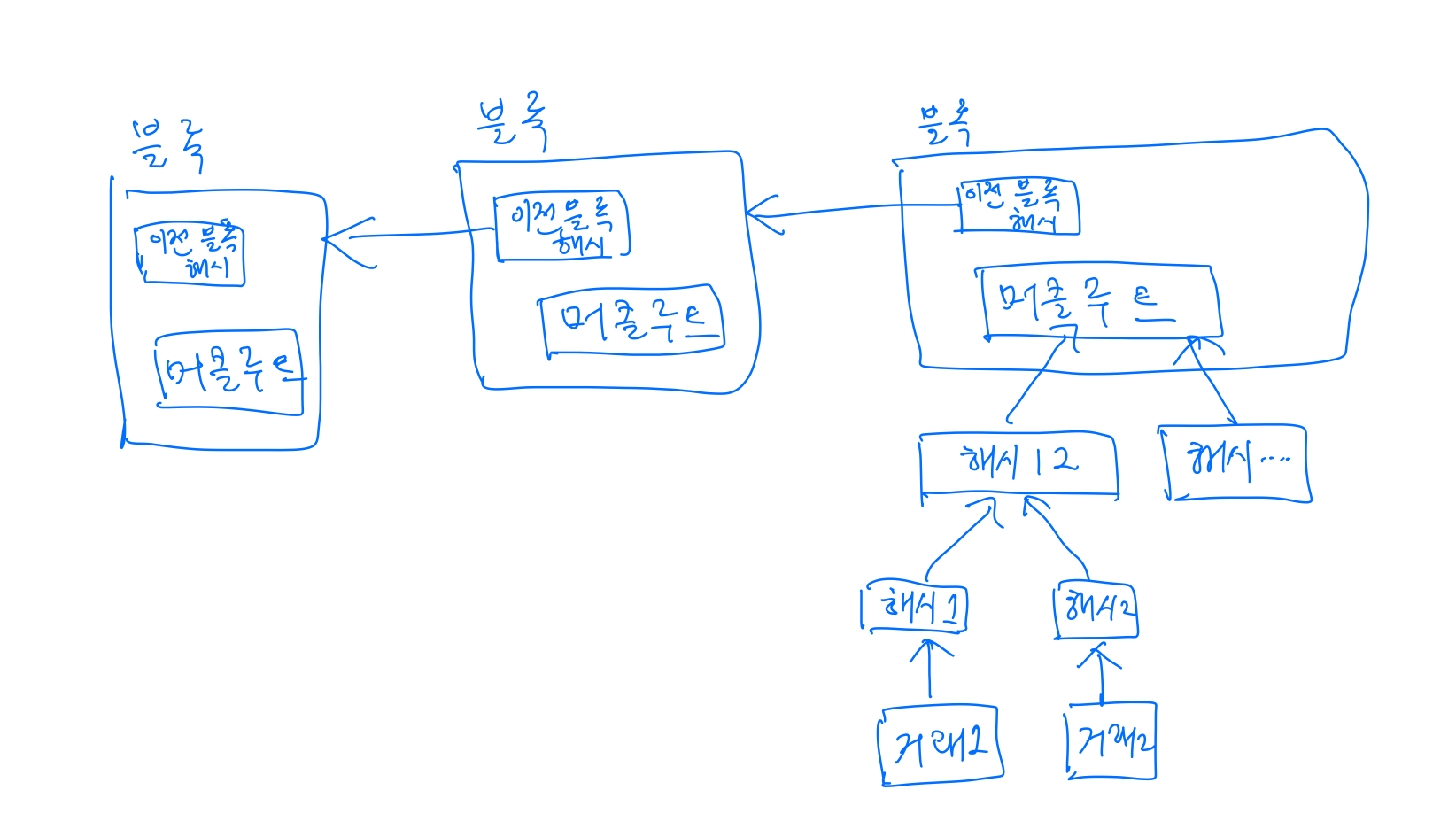
## 2.1 블록체인이란?

### 블록체인은 거래 데이터와 해시값으로 구성된 블록들의 연결

우선 '블록체인'이라는 단어부터 이해해 보자. '블록체인'이라는 단어의 뜻 그대로 보자면, 이는 블록이 체인(chain)처럼 연결된 것을 의미한다. 즉 블록체인은 블록의 묶음인 것이다.

그렇다면 블록은 무엇일까? 블록은 거래의 묶음이다. 그냥 물건을 연결하듯이 한 것이 아니라, **해시 기법이라는 암호화 방법을 이용해서 묶어 놓은 것**이다. 거래(transaction)는 또 무엇이란 말인가? 주문, 송금 또는 예금, 모두 거래에 해당한다. 이러한 거래들은 은행에서 컴퓨터 서버를 이용해서 기록되는 것이 일반적이다. 그러나 블록체인에서는 이러한 거래 내역을 블록에 저장한다.

뿐만 아니라 그러한 거래 내역들을 해시 기법을 이용해서 암호화 한다. 이렇게 암호화된 거래 내역들은 그림에서 보듯이 요약본 형태로 해시화한다. 이들을 또 해시화시키는 작업을 계속해서 최상단 해시만 남을 때까지 반복한다. 마지막으로 남은 해시를 머클 루트(Merkle Root)라고 부르고, 이는 블록에 있는 모든 거래 내역의 요약본에 해당된다. 비유를 하면, **굴비 꾸러미를 하나씩 엮어서 생긴 맨 윗 매듭이 '머클루트'**이다.



블록체인

좀 더 기술적으로 정리하면, 트리의 리프 노드(leaf node)에 해당되는 거래1을 해싱(해시화)해서 해시1을 만든다. Hash1은 다른 거래 내역인 거래2를 해싱해서 만들어진 해시2와 묶여서 다시 해시화되고, 새로운 값인 Hash12를 만들어낸다. 이런 방식으로 거래를 하나씩 계층적으로 서로 묶어서 모든 거래의 해싱이 완성되고 최상단 노드의 해시 값이 '머클루트'가 된다.

이렇게 암호화 해놓으면 어떤 장점이 있는 것일까? 누군가 블록에 포함된 거래 정보를 수정하는 시도가 있다면, 해시값이 달라지고, 결국 꾸러미가 틀어지게 된다. 그런데 참여자 노드들은 동일한 데이터 블록들을 공유하고 있기 때문에 특정 노드의 블록이 잘못되었다면, 다른 노드들에 있는 해시값을 비교해서 잘못된 것을 쉽게 찾아낼 수 있다. 이러한 특징때문에 블록체인은 일단 기록이 되면 수정이 아예 불가능하게 된다.

이와 같이 거래 데이터가 쌓이면 블록이 되는 것이고, 또 블록을 해시로 연결해서 블록체인으로 만들게 된다. 블록이 모여서 완성이 되면, 블록은 자신을 유일하게 식별해 주는 해시 값을 가지게 된다. 이와 같이 블록들은 서로 앞 블록의 식별자 '해시 포인터 hash pointer'를 가지고 있는 방식으로 연결되며, 이를 암호화해서 누구나 쉽게 알지 못하도록 하고 있다. 자료구조 중 한가지인 리스트에서 앞 또는 뒤에 있는 노드(node)의 주소를 이용해서 연결하는 것처럼, 블록체인은 블록의 해시값을 이용해서 연결된다.

더 알아보기: 해시

블록체인에서는 sha256이라고 알려진 방법으로 어떤 데이터로부터 크기에 관계없이 항상 64바이트의 해시를 생성한다. 예를 들어 "나는 모모은행에 200원을 입금했다"라는 데이터로부터 해시를 생성하면 "63add0f99dfdf453b20658ebf8fd33702d3c01f32bc51e8ee978dc8374ab6355"이 된다. 그런데 거래 정보를 "나는 모모은행에 201원을 입금했다"로 변경하면 해시값은 "6818a4380113396112fd8740cbf2d51dd463cab03950c5d1b7e5d3ecb9d80796"가 된다. 이렇게 숫자 한 개만 바뀌었을 뿐인데도 해시값은 완전히 다르게 생성된다. 블록체인의 자주 활용되는 중요한 기법이므로 뒤에 자세히 설명하게 된다.

#### 블록체인은 수정불가능한 분산원장

블록체인은 데이터들이 들어있는 블록들을 인터넷상에서 서로 연결(chain)하여, 중앙 집중 서버 없이 데이터를 기록, 인증, 보존, 관리하는 디지털 장부로서 **분산원장기술** (DLT, Distributed Legder Technology)을 의미한다. 하지만 이렇게 서버 없이 데이터를 기록하고 관리한다고 많은 사람들이 관심을 기울이지는 않을 것이다. 블록체인 기술은 다수의 참여자들이 정보를 변조하기 어렵도록 공유함으로써 데이터를 기록하고 보존하며, 관리하는 기술이다. 여기서 중요한 부분은 데이터를 변조하기 어렵다는 점이다.

블록은 거래 데이터들이 기록되어 있는 거래 원장이다. 쉽게 생각하면, 거래 원장은 모든 거래 내용들을 기록해놓은 장부라고 생각할 수 있다. 그런데 이러한 데이터들이 아무렇게나 저장되어 있다면, 남들이 쉽게 수정할 수 있다는 문제가 있다. 그래서 블록의 데이터들은 **해시 기법이라는 암호화 방법을 이용해서 처리**되어 있다. 그리고 이렇게 생성된 해시 값은 블록에 데이터와 함께 저장된다. 해시 기법은 데이터의 내용을 이용해서 처리하기 때문에, 블록에 포함된 거래 정보를 단 한글자라도 수정한다면, 해시값이 달라지고, 결국 수정되었음을 알 수 있다. 즉 거래를 암호화하며, 수정이 불가능하도록 하고 발생한 거래를 누구나 볼 수 있도록 적어놓은 원장, 그래서 공개된 분산원장(Distributed Ledger)이라고 한다.

이렇게 연결되어 있는 블록들은 기존 클라이언트/서버 구조의 중앙 집중형 서버 없이 블록체인에 참여하는 노드(참여자)간에 P2P 형태(서버에 의존하지 않고 서로 연결된 컴퓨터간 통신 방법)들에 복제되어 저장되기 때문에, 중앙 서버가 해킹되면 데이터가 조작될 수 있는 보안 문제가 발생하지 않는다. 또한 분산시스템에서는 **합의 알고리즘을 통해 거래를 인증**하고, 블록체인에 기록한다. 이 기록은 중앙에서 통제되는 것이 아니라, 참여하는 모든 컴퓨터에 **분산되어 동기화**된다. 따라서 거래가 인증되고 쓰여지고 나면 **수정될 수 없는**, 영원히 지워지지 않는 특성을 가진다. 즉 블록체인의 데이터는 네트워크 환경에 연결되어 있는 분산된 컴퓨터들에 데이터가 저장되어 있어, 아무나 임의대로 수정할 수 없고, 반대로 누구라도 조회할 수 있다는 장점이 있다. 이러한 점 때문에 기록에 대한 '신뢰'가 매우 높고, 이러한 신뢰를 필요로 하는 여러 산업군에서 관심을 가지고 있다.

#### 블록체인은 프로그램이 가능한 컴퓨터

그런데 왜 이처럼 단순한 데이터의 연결에 불과한 블록체인이 관심을 받는 것일까? 그 이유는 분산 컴퓨팅이다. 블록체인은 암호화폐인 비트코인에 내장되어 있는 기술이다. 최초의 암호화폐로 알려진 비트코인의 블록체인은 프로그래밍이 가능한 매체가 아니었기 때문에, 뭔가 비지니스 서비스를 제공하려 해도 불가능한 수준이었다. 이는 해당 블록체인 기술이 비트코인을 위해서만 만들어졌기 때문이었다. 하지만 암호화폐 기술 중에는 프로그래머가 직접 코드를 작성해서 배포하고 실행할 수 있는 것들도 있다. 이러한 블록체인에서 동작하는 프로그램을 스마트 컨트랙(smart contract)이라고 한다.

블록체인에는 우리가 프로그램을 하듯 스마트컨트랙을 만들어 배포해 놓을 수 있을 뿐만 아니라 발생하는 트랙잭션이 기록되기도 한다. 따라서 프로그밍이 가능한 분산 데이터베이스라고 볼 수 있다.

블록체인 기술이 암호화폐를 내장한 플랫폼에서 발전하여 금융거래만 기록할 수 있다고 오해할 수 있지만, 블록체인 기술은 사실 가치있는 모든 **경제적 거래를 프로그래밍하여 기록**할 수 있다. 블록체인을 그냥 단순하게 줄여서 하나의 컴퓨터라고 생각해도 무리가 없다. 단 우리가 쓰고 있는 개인용 컴퓨터와는 다른 분산컴퓨터라고 생각해야 한다. 따라서 프로그래밍하는 방법도 기존 방식과는 다를 수밖에 없다.

## 2.2 마이닝

암호화폐에서 '마이닝(mining)한다'는 말이 쓰인다. 설마 채굴하는 장면을 연상하지는 말자. 마이닝이란 다름 아닌 **거래를 인증하는 과정**을 말한다.

비트코인은 금전거래가 발생하면 거래기록을 블록으로 만든다. 네트워크 노드(node 또는 상하 계층이 아닌 동등하다는 의미로 peer라고 한다)는 그 블록을 인증하기 위해 마이닝을 수행한다. 비트코인은 약 10분쯤 걸린다. 인증된 거래는 블록체인에 붙여지고 실시간으로 공유된다. 특정 기관이 거래를 인증하는 것이 아니라, 누구나 인증에 참여할 수 있다. 여러 참여자 가운데 실제 인증을 하게 되는 참여자는 그 노력에 대해 보상을 받게 된다. 이 과정을 마이닝이라고 한다.

참여자는 컴퓨터이고, 금액과 거래는 디지털화 되어 있다. 기존 종이 화폐가 사용되지 않는다. 또한 그 처리비용도 기존 신용거래 또는 금전거래의 수수료보다 저렴하다. 그러니까 **마이닝이 끝났다는 말은 그 트랜잭션이 인증되었고, 블록체인에 기록**된다는 말이다.

마이닝을 하는 과정은 해시 값을 생성하는 계산능력(hashrate)에 의해 결정되는데 더 강력한 컴퓨팅 파워를 가지면 마이닝을 보다 빠르게 할 수 있다. 마이닝에 특화된 컴퓨터를 만들어서 활용하기도 한다.

마이닝은 많은 전력이 필요해서 환경 친화적이 아니라는 비판이 있어, 국가 별로 정책의 차이가 있지만 채굴업을 단속하기도 한다. 그러나 국가의 통화나 증권시장의 토큰 증권으로 도입하려는 등 블록체인을 산업의 발전적 기술로 활용하려는 추세는 지속되고 있다.

## 2.3 플랫폼으로서의 블록체인

잘 알려진 투자자 워런 버핏 Warren Buffett은 비트코인은 비트코인은 망상(delusion)이라고 했다. 심지어는 "Rat Poison Squared" 정말로 쥐약이라며 부정적인 입장이었지만 블록체인은 유망한 기술이라고 말했다.

새삼 우리가 주목하는 것도 비트코인에 내재하는 블록체인 기술이다. 화폐라는 매우 중요한, 실수가 허용되지 않는 금융기록을 블록체인에 전송하고, 기록하는 기술이 중요하다. 기존에 존재하는 암호, 머클트리, P2P 기술을 영리하게 조합하여 창의적인 화폐로 만들었고 현재는 블록체인이 한 개의 개발 플랫폼으로 받아들여지고 있다. HTTP가 문자정보의 인터넷 프로토콜이라면, 암화화폐(Cryptocurrency)는 금융프로토콜으로서 지급 결제 플랫폼이다. 플랫폼으로서 합의, 보안, 통신 기술을 내포하고 있다.

* **합의** 계층: 블록을 생성한 후 체인으로 연결해 가기 위해 합의가 필요하다. 앞서 살펴본 바와 같이 합의가 되어야 비로서 정당한 블록으로 인정된다. 암호화폐 별로 적용되는 합의 알고리즘은 서로 다르게 고안되어 적용될 수 있다.
* **보안** 계층: 블록체인에서의 데이터는 위변조를 막기 위해 암호기술을 적용한다. 트랜잭션은 발생하면 디지털 서명을 하고, 수신 측에서 진본인지 인증할 수 있다. 또한 블록은 해시로 암호화하고 이를 통해 서로 연결해 놓고, 데이터가 변경되면 해시들이 연쇄적으로 변경되어야 하는 구조라서 안전할 수 밖에 없다.
* **통신** 계층: 트랜잭션이 발생하면 P2P 상에 전파가 되고, 블록체인의 동기화가 이루어 진다.

# 3. 암호화폐

블록체인은 어느 날 한 순간에 생겨난 것이 결코 아니다. 비트코인에 내재되어 있는 기술로서, 비트코인과 더불어 이미 사용되어 오고 있는 것이다. 비트코인에서는 발생하는 거래를 기록하고, 쌓아서 블록으로, 그리고 블록들을 체인으로 연결해 놓고 있다.

그렇다면 비트코인은 또 어디서 갑자기 튀어나온 기술일까?

## 3.1 비트코인 이전의 암호화폐들

암호화폐는 최근에 관심을 끌어서 그렇지 사실은 이미 꽤 오래 전부터 만들어진 기술이다.

* 1982년 David Chaum이 당시 30세도 되지 않은 젊은 나이에 **디지털 화폐(Digital Cash)**를 처음으로 고안하였다. 여기에서 **블라인드 사인(blind signature)**이라는 현재의 디지털 서명과 유사한 기법을 적용한다. 원본은 노출하지 않고 (blinded), 서명을 한 후에 나중에 공개된 방식으로 원본과 비교하여 인증할 수 있게 된다. 봉투에 서명하면, 먹지를 통해 원본 문서에 서명이 새겨지고 나중에 원본과 일치하는지 인증하는 방식에 비유할 수 있다. RSA와 같은 디지털서명도 원본을 해싱해서 보지 못하게 하고, 키를 사용해서 서명한다는 점에서 거의 다르지 않다.
* 1997년 Adam Back이 자신의 논문 "Hashcash - A Denial of Service Counter-Measure"에서 해시캐시(Hashcash)를 제안하고 있다. 해시캐시는 일종의 암호문자로 일정 CPU 시간을 투입해야 획득할 수 있고, 이를 이메일 헤더에 첨부해야 송부할 수 있게 한다 (우표가 없으면 발송이 되지 않듯이). 비록 적은 노력(비용)이라 해도, DDoS와 같은 대량 발송은 지불이 과도해져 실행될 수 없게 된다. 이러한 방식으로 이메일 스팸이나 DDoS 공격, 거래 거부 공격(distributed denial-of-service attack)을 막을 수 있다는 제안이다.
* 1998년 Wei Dai가 b-money 익명 분산 전자 화폐를 제안했다. 화폐 발행은 작업 증명 PoW (Proof-of-Work)에 투입된 비용 hashcash만큼 이루어진다. 작동 방식이 비트코인과 유사했다. 이더리움의 제일 적은 단위 wei는 이 기술의 제안자 이름에서 유래가 되었다고 한다.
* 2004년 Hal Finney는 비트코인에 앞서 작업 증명 PoW를 고안했고, 2009년 1월 비트코인의 첫 거래를 받았다고 한다. 역시 Finney라는 이더리움의 화폐단위도 여기서 그 유래를 짐작할 수 있다.
* 2008년 비트코인이 태어난다. 비트코인은 Satoshi Nakamoto가 제안한 디지털화폐, 2009년 1월 3일 block 0을 마이닝하면서 처음 발행, 2009년 2월 11일 Bitcoin Core v0.1 프로그램이 공개된다. 비트코인은 기존에 있는 기술을 창의적으로 조합해 고안되었다. 암호 서명, PoW 등도 이미 나와 있는 기술이었다. Satoshi도 b-money를 참조했다고 밝힌 적이 있다.

## 3.2 비트코인은 화폐로서 기능하는가?

비트코인을 비롯한 블록체인 기반의 암호화폐는 **중앙은행이 개입하지 않아도 개인들이 자유롭게 입출금, 송금 등의 금융거래**를 할 수 있다. 금융거래는 **디지털서명**을 적용하여 보안을 철저히 하고, 은행이 그 거래를 독점하지 않고 사용자들이 **분산하여 저장**하기 때문에 위변조 또는 해킹이 사실상 불가능하다.

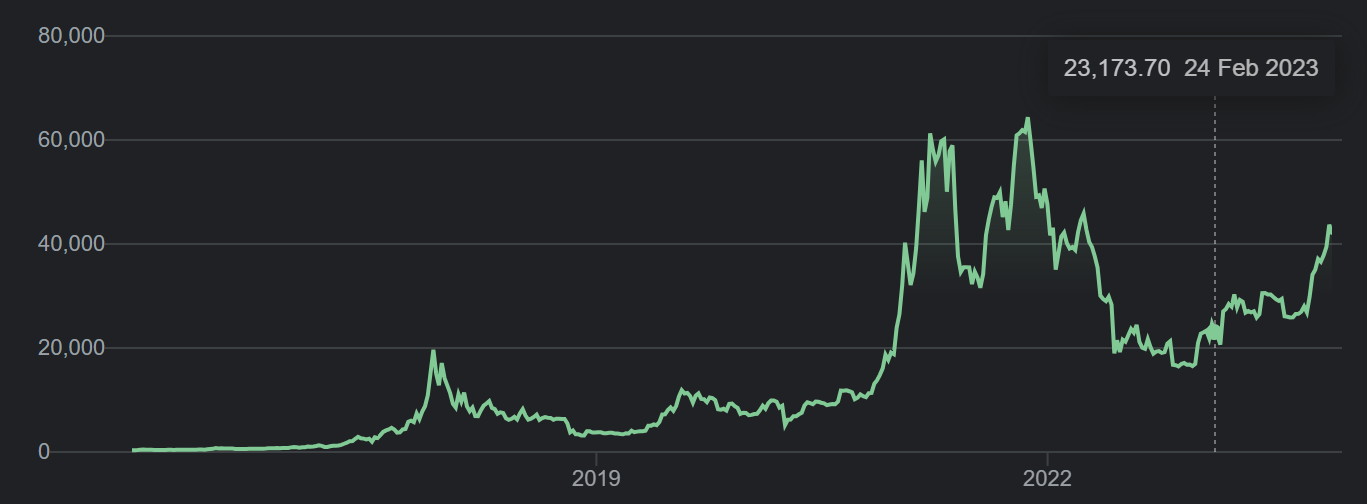
우리가 사용하는 화폐는 정부에서 발행하고 실물로 존재하지만 비트코인은 알고리즘에 따라 발행이 되고, 유통이 된다. 실물 화폐는 필요에 따라 정부가 더 발행할 수 있지만, 비트코인은 발행량이 한정되어 있다. 2009년 1월 처음 발행된 후, 최대 2100만 비트코인이 발행되도록 설계되어 있다.

화폐는 가치의 척도, 가치의 저장, 교환의 수단이다. 비트코인이 화폐로서 기능하는지, 그 적격성에 대해서는 아직 의문이 남아있다.

블룸버그가 보도한 미국 블록체인 연구기관 Chainalysis에 따르면 2019년 첫 4개월간 비트코인 거래 중 1.3%만이 실제 상거래에 활용되고 있고, 98% 이상이 거래소에서만 회전되고 있다는 뜻이다. 이런 추세는 지금도 크게 달라지지 않아서 실제 화폐로서 활발하게 쓰이지 못하고 있다.

비트코인은 투자대상으로서 인식되고 있는 편이다. 2018년 갑자기 비트코인에 대한 관심이 증가하면서 그에 따라 가격도 급등락하고 있다. 그 관심은 투자대상으로서 비트코인 가격에 고스란히 반영되고 있다. 2018년 가격이 급등하면서 논란 끝에 실물 가치에 대한 의심이 높아져 급락하였다. 이전에는 13달러에 머물렀지만 2017년 2만달러까지 치솟았고, 2018년에 들어서 수백달러로 폭락을 경험하였다.

비트코인이 '디지털 골드'라고 불리우더니 실제 가격도 금 값과 차이가 없었던 적도 있었다. 2017년 12월 기준으로 2천만원을 상회하다가 2019년 4백만원으로 수직낙하하고, 그러다가 2021년에서 2022년 그 가격이 전고점을 넘어서 8천만원까지 천정부지로 솟은 바 있다. 2021년 1월 테슬라의 일론 머스크가 무려 15억 달러 (약 1조6500억원), 하나에 대략 3만 달러(약 3300만원)의 가격으로 투자하여 화제가 된 바 있다. 다른 자산이 하락하면서 디지털 금의 역할을 할 것이라는 기대에 미치지 못하고 있다.



alt text

## 3.3 대안 코인들

비트코인에 대한 관심이 높아지면서 많은 암호화폐가 등장하고 있다. 비트코인을 제외한 이들 암호화폐를 대안 코인 또는 알트코인 (Alternative Coins)이라고 한다. 대개는 비트코인에서의 프레임워크를 본 따서 P2P 상에서 마이닝되는 방식으로 코인이 발행되고 있다.

2019년 초 2500여개, 2021년 초 4500여개, 2022년 초 10,000개 규모로 코인의 발행은 늘어가면서 변동하고 있다. 그 총액은 천문학적인 숫자인 1조 달러를 돌파하고 있다 (참조 https://www.investing.com/crypto/currencies).

대부분의 암호화폐는 시세의 변동성이 크지만, 1위는 비트코인이 여러 대안 코인들 사이에서 일종의 기축통화 역할을 하면서 전체의 대부분을, 그리고 이더리움(ethereum)이 다음 자리를 차지하고 있다. 이 둘을 합치면 50%가 넘는 시장을 형성하고 있다. 순위의 변동이 있지만 Cardano, Solana, 도지코인 등 다양한 대안코인들이 생겨나기도 하고 또는 금융사고가 나기도 하여 불안정안 상황을 보이고 있다.

최근 CBDC Central Bank Digital Currency, 중앙은행이 발행한 디지털화폐에 대해 여러 나라가 관심을 보이고 있다. 중국이 적극적으로 2022년 동계올림픽에 맞추어 디지털 위안화, 일명 e-CNY를 도입하고 있다. 미국은 연방준비위원회 FED가 CBDC를 검토하고 있다. 유럽, 일본, 러시아, 터키, 싱가포르 등 세계의 80%가 CBDC 연구를 진행하고 있다 (2020년 1월 국제결제은행 BIS 보고서).

# 4. 분산 처리

블록체인이 관심을 끄는 이유는 분산환경에서 작동이 되기 때문이다.

보통 트랜잭션은 발생하면, 특정 서버가 맡아서 처리하게 된다. 블록체인은 분산이라 이와는 다르다. 어느 특정 서버가 아니라 네트워크 상에 **서로 연결된 컴퓨팅 플랫폼에 분산해서 처리**된다. 그러나 논리적으로는 하나의 플랫폼에서 처리되는 것처럼 보인다.

분산시스템은 컴퓨팅 노드(피어)들이 서로 Peer to Peer Network **P2P**를 통해 연결되고, 서버-클라이언트 역할이 고정되어 있지 않다. 서버가 중앙에 위치해서 처리하는 것이 아니라, **네트워크에 접속된 그 어떤 컴퓨터도 서버**가 될 수 있다.

중앙집중식에서는 이러한 처리가 특정 서버에 의존하는데 반해, P2P에서는 서로 자발적으로 참여한다는 점이 다르다. 어떤 노드이건 서로 동동하게 참여한다. 자신들이 **자발적으로 디스크 저장공간, 처리능력, 네트워크 능력을 제공하고 참여**한다.

P2P 기술은 마이크로소프트의 윈도우 업데이트에서도 적용하고 있다. 이전에는 마이크로소프트사의 서버에서 다운로드해서 설치하는 형식이었다면, 지금은 네트워크에 연결되어 있는 많은 사용자들의 컴퓨터에 다운로드되어 있던 업데이트 내용을 공유하는 식으로 사용하고 있다 (사용자가 참여하지 않겠다고 설정하지 않으면 자동으로 공유하게 된다).

금융에서는 **은행이 없어지고, 블록체인이 대신**할 수 있게 될 수도 있다. 부분적으로라도 이렇게 된다면 매우 혁신적이다. 송금을 할 때에도 디지털사인을 하고 지급자에게 송금하고 블록체인에 기록하면 된다. 은행을 매개로 송금할 필요가 없게 된다.

그럼에도 불구하고 거래의 위변조가 불가능하여 블록체인에 대한 기술적 신뢰가 높다. 기술적 신뢰라고 말한 것은 '심리적 신뢰'와는 조금 다르기 때문이다.

다만 정부로서는 통화에 대한 통제력이 약화되고, 과세에 대한 어려움이 예상되기 때문에 문제가 될 수 밖에 없다.

|  |  |  |
| --- | --- | --- |
| 구분 | 중앙집중형 | 분산형 |
| 서버에 의존? | 어느 한 곳에 서버가 있다 | 중앙서버가 없고, P2P 네트워크의 어느 노드도 서버가 될 수 있다 |
| 거래의 보관? | 데이터베이스 서버에 거래가 기록된다 | 블록체인에 거래가 기록된다 |

# 5. 비잔틴 장군 문제

비잔틴 장군 문제는 분산시스템에서 합의를 이루기 어려운 상황을 명확히 보여주고 있다.

전쟁에서 아군 부대는 부대들 끼리 서로 **연합**해야만 승리하는 상황에 처해있다. 부대를 지휘하는 장군들이 서로 **약속**한대로 공격만 하면 되는데, 이런 간단한 일조차도 실제로는 까다로운 문제이다.

부대는 서로 다른 지역에 위치하고 있어 **전령**을 통한 메시지 전달이 필요하다. 그러나 전령이 포획된다면 **메시지는 전달이 되지 않고** 공격은 당연히 실패하게 된다. 메시지를 전달 받은 장군이 수신응답을 다른 장군에게 보낼 경우에도 또한 포획될 수 있다.

더 나아가, 일부 장군이 **배신자**라고 하면 문제는 더욱 복잡해 진다. 메시지가 전달되었다 하더라도 믿을 수 있느냐는 문제가 있다. 배신한 장군이 있다면 그 메시지는 **위조**될 수도 있기 때문이다.

이러한 문제를 해결하려면 배신자를 적발하거나, 배신자가 알 수 없는 방식으로 메시지를 암호화해서 위조를 막거나, 메시지를 원본과 대조하여 확인하는 등 여러 방법을 강구해야만 한다.

# 6. 합의

비잔틴의 문제에서 보듯이, 여러 노드가 참여하는 분산시스템은 메시지를 전달하면서 유실되거나 **위변조**될 위험이 있다. 뿐만 아니라 발신된 **정보가 유실되거나 지연**될 가능성이 있기 때문에 정확한 정보를 공유하는 것이 어렵다. 그럼에도 불구하고 분산 시스템에서는 참여하는 **노드들 간에 서로 다를 수 있는 정보를 합의를 통해 신뢰를 보장**하게 된다.

새로운 거래가 네트워크에 전파되면, 노드들은 그 거래를 원장에 포함할지를 결정해야 한다. 이 경우 다수의 노드가 합의하면 거래를 포함하여 원장의 상태를 변경하고 합의에 이르렀다고 한다.

블록체인은 다수가 참여하지만, 그 중에는 악의적인 노드가 포함될 수 있다. 이런 경우 블록체인은 어떻게 합의를 하고 신뢰할 수 있는 상태로 만들어 나갈 것인가?

몇 가지 대표적인 합의 방식으로는 비잔틴장애허용, 지분 증명(Proof of Stake), 위임 지분 증명(Delegated Proof of Stake), 권위 증명(Proof of Authority), 경과 시간 증명(Proof of Elapsed Time)이 있다.

## 6.1 비잔틴장애허용

비잔틴 장군문제는 정보 전달이 누락되거나 배신자에 의해 정보가 위조되면 합의에 이를 수 없고 **비잔틴 장애**가 발생한다. 이런 경우 전체가 혼란에 빠져서 실패하지 않도록 합의하는 알고리즘이 필요하다.

1999년 Castro와 Liskov에 의해 제안된 Practical Byzantine Fault Tolerance (pBFT)를 살펴보자.

전체 구성원의 1/3이 배신자라고 하더라도 나머지 2/3가 동의하면 합의라고 가정하는 것이다. 여기서 배신자란 잘못된 정보를 전달하는 노드를 나타낸다. 노드 간에 서로 정보 전달을 해서, 대다수 즉 2/3가 응답하기를 기다리고, 받은 모든 메시지 중 가장 많이 일치하는 데이터로 합의에 이르게 된다. 여기서 노드란 참여자를 나타내고, 블록체인에서는 블록 체인을 가지고 있는 컴퓨터를 일컫는다. Hyperledger, Stellar, Ripple 등 블록체인에서 활용되고 있다. 이 알고리즘은 효율적이어서 블록체인이 아니더라도 활용되고 있다.

참여자들끼리 매우 빈번하게 소통하여 메시지가 위조되었거나 출처를 분명히 할 수 있다. 그러나 **노드가 늘어날수록 정보 교환량이 급격히 늘어**난다는 단점이 있다.

전체 장군 중 f 배신자가 있는 경우, 합의를 하려면:

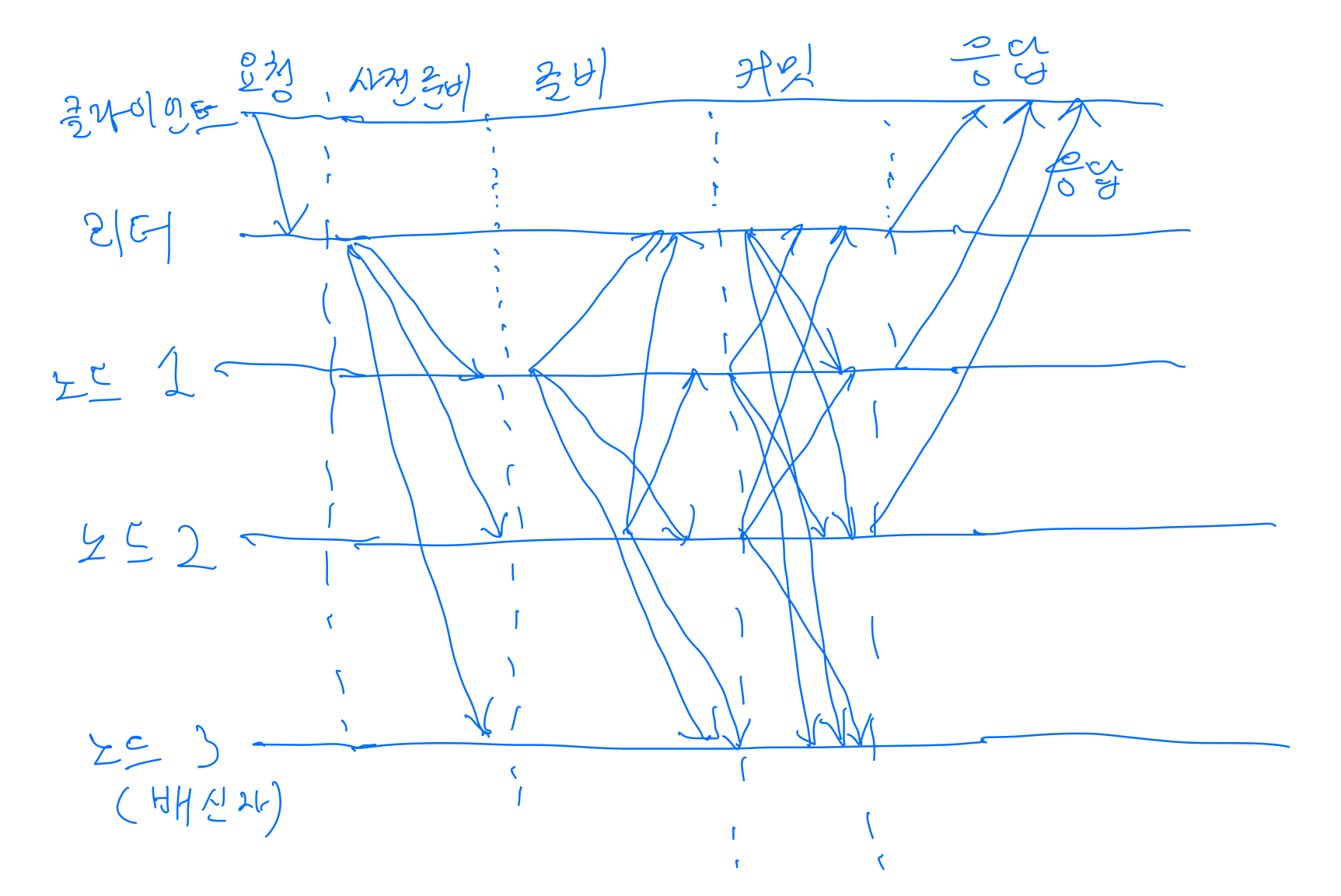
* 3f + 1 만큼의 노드가 필요하고,
* 각 노드는 서로 최소 2f + 1 통신 경로가 확보되어 있어야 하고
* f + 1 회 이상의 정보 교환이 있어야 한다.

합의하는 절차는 순서대로 진행된다. 리더 노드가 클라이언트로부터 메시지를 전달해달라는 요청을 받으면 다음에 설명하는 프로토콜을 실행시켜서 요청하는 메시지가 괜찮은지 확인한다.

* 사전 준비 단계: 리더 노드가 연결되어 있는 모든 노드들에게 데이터를 보내면서 합의가 필요하다고 "pre-prepare" 메시지 전송
* 준비 단계: 각 노드들은 "pre-prepare" 메시지를 받고, "prepare" 메시지를 합의에 참여하는 모든 다른 노드에 각각 전송.
* 커밋 단계: 각 노드들은 "prepare" messages 받으면 합의에 참여하는 모든 노드에 "commit" 메시지를 각각 전파.

마지막 응답 단계에서는 커밋 단계에서 메시지를 전달 받은 모든 노드들이 클라이언트로 응답한다. 클라이언트는 대다수 즉 2/3가 모두 응답하기를 기다리고, 받은 모든 메시지 중 가장 많이 일치하는 데이터로 합의.

그림에서 보인 것처럼 노드 3는 메시지를 전달하지 않거나 혹은 전혀 다른 메시지를 전달할 수 있다. 하지만 클라이언트는 노드 3로부터 다른 메시지를 전달 받더라도, 나머지 노드들에서 동일한 메시지를 전달받으므로, 제대로 된 합의가 도출될 수 있다.



alt text

## 6.2 작업 증명

PoW(Proof of Work)는 **작업을 증명**한다는 의미이다. 2008년 사토시 나카모토의 논문, "비트코인: P2P 전자화폐 시스템 Bitcoin: A Peer-to-Peer Electronic Cash System"에서 소개된 합의 방식이다.

**비트코인**에서 도입된 PoW를, 비트코인을 발명한 이름을 따서 **나카모토 합의**라고 한다. 이렇게 작업 증명하는 과정을 '마이닝'이라고 한다.

"작업 증명"은 수학적 문제, 기준 해시보다 작은 값을 찾는 과정이라서 상당한 노력이 필요해서 블록체인에 적용하려면 '과연 가능할까?'라는 근본적인 한계가 지적되고 있다 (Gervais et al., 2016, On the security and performance of proof of work blockchains, In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 3-16). 현재 이 문제에 대해 제시되고 있는 솔루션들은 대개 지분 증명(Proof of Stake, PoS), 위임 지분 증명(DPoS, Delegated Proof of Stake) 등의 대안적 알고리즘이 제시되고 있다.

## 6.3 지분 증명

PoW는 경쟁적으로 마이닝이 이루어지기 때문에 이런 컴퓨팅 파워가 낭비된다는 문제가 있다. 또한 작업증명에 걸리는 시간으로 인해 지연되는 문제를 해결하기 위해 지분 증명(PoS, Proof of Stake)이 제안되고 있는데, **노드가 보유한 잔고를 기준**으로 권한을 분배하는 합의 방식이다. 예를 들면, 10%의 잔고를 가지면 10%의 블록을 생성하는(forge) 권한을 부여하는 것이다. PoW에서와 같이 마이닝을 통해 블록이 생성되지 않기 때문에 채굴 보상이 주어지지는 않는다.

**PoW에서는 블록이 마이닝을 통해 생성되지만, PoS에서는 마이닝이 없다**. 단 **PoS에서는 forger가 블록을 생성하고 채굴보상 대신에 처리비용을 받게 된다**. **Peercoin**이 2013년 PoS를 처음으로 구현했고 이더리움도 버전 Casper에 채택하고 있다.

그러나 이 방식이 앞선 PoW의 단점을 모두 극복하고 분산, 성능, 보안의 목적을 모두 달성할 수 있는 가에 대한 논란이 있다. 이 방식에서 극단적이지만 어느 **특정 노드가 매우 잔고가 많은 부자라면 오히려 중앙화** 되는 단점이 있다. **"Nothing At Stake"**, 즉 노드가 불량하게 행동해도 불리할 게 없다는 비판이다.

예를 들어, 여러 fork가 존재하더라도 마이닝에 따른 보상만 받으면 되기 때문에 맞는 fork인지 아닌지 마이닝하면 된다고 행동한다는 것이다. 그 결과 모든 fork를 인증하여 여러 갈래가 발생하게 되는 것이다. PoW에서는 이런 문제가 발생하지 않는다. 마이너들이 맞는 chain에 블록을 추가하면 그에 따라 보상을 받기 때문이다. PoS는 단점을 보완하기 위해 코인별로 수정하여 쓰이고 있다. Delegated PoS (Bitshares) 이더리움도 차기 버전에서 수정된 PoS를 테스트하고 있다.

# 7. 블록체인의 적용분야

처음에는 주로 비트코인과 같은 암호화폐의 거래내역을 기록하는 저장소로서 알려졌다. 거래를 안전하게 기록하고 중복을 방지하기 위한 독특한 설계때문에 주목을 끌었고 이를 블록체인 1.0이라고 하자.

이후 이더리움이 등장하면서 이른바 블록체인 2.0이 시작한다. 단순히 암호화폐의 거래를 기록하는 기능에 국한되지 않고, 블록체인은 프로그래밍이 가능한 오픈 플랫폼으로 진화하고 있다. 스마트 컨트랙을 개발하고, API를 사용하여 다양한 분야에서 응용이 가능해지는 단계로 나아가고 있다.

이제 웹 3.0은 중앙 집중형 시스템에서 벗어나 분산 탈중앙화된 경험을 제공하는 블록체인 기반의 웹을 지향하고 있다.

블록체인 기술이 발전함에 따라 다양한 분야에서 그 활용이 확대되고 있다.

* **블록체인 기반 스마트폰**: 국내에서는 삼성에서 블록체인 지갑이 내장된 **갤럭시S10**을 출시하였다. 2021년 자체 두 번째 블록체인 핸드폰으로, 삼성전자가 위메이드트리와 함께 갤럭시S21 시리즈로 블록체인 휴대폰인 위믹스 폰을 출시하였다. 그 때 제공하였던 위믹스 토큰이 한때 급등하기도 해서 화제가 되기도 하였다. 2022년 미국 블록체인 개발사 솔라나가 스마트폰 사가(Saga)을 공개하고 있다. 이스라엘 스타트업인 시린랩스(Sirin Labs)의 자체 시린OS에서 작동하는 블록체인 핸드폰 **Finney**, 대만의 스마트폰 제조사인 HTC의 **엑소더스 1**, 중국 기업인 레노버와 슈가(Sugar), 창홍(Changhong), 펀디엑스 사의 **BOB, Blok on Blok** (이통사가 필요없고 휴대폰번호가 없이, 블록체인에서 전화, 문자 가능, 2020년 1월 CES에서 발표) 등이 이미 블록체인 스마트폰을 공개하고 있다.
* **분산 네트워크 기반 SNS**: 블록체인을 기반으로 한 소셜 네트워크 서비스는 사용자의 개인 정보 보호와 데이터 무결성을 보장하며, 중앙 집중식 서비스의 단점을 보완할 수 있다. 스팀 (https://steem.com/), 채팅, 집단지성의 akasha (https://akasha.org/) 등 SNS에도 블록체인이 활용되고 있다.
* **디지털 신원확인 및 보안**: 분산 신원 확인 시스템을 통해 사용자의 신원을 안전하게 관리하고 보안을 강화할 수 있다. 한국에서도 공인인증서를 대체하는 블록체인기반 **뱅크사인**이 2018년 8월 개발되었지만, 경쟁에 밀려 2021년 신규발급을 중단하고 금융결제원이 분산신원증명(Distributed ID)인 '뱅크아이디'를 출시하였다.
* **디지털 자산**: 보안 토큰 발행 (STO), 대체 불가능 토큰 (NFT), 디지털 자산의 발행과 거래, 토큰화된 자산의 유통, 스마트 계약을 활용한 자동화된 거래 등 다양한 방식으로 블록체인 기술이 활용되고 있다.
* 금융 서비스 분야: 스마트 계약을 활용한 자동화된 금융 상품, 블록체인을 기반으로 인터넷 오락 서비스의 이용료, 디지털 콘텐츠의 소액 판매 등의 마이크로결제, 해외 결제 및 정산 서비스, 크라우드펀딩 등의 금융 관련 분야에서 도입되고 있다. 게임하면서 버는 "play to earn"도 새로이 등장하고 있다.
* IoT 및 스마트 시티: 블록체인을 기반으로 장치의 디지털 신원, 전기차 충전을 위한 에너지의 거래, 도시 인프라 및 서비스의 자동화, 블록체인 투표를 통한 시민들이 도시 운영 및 개발에 참여하는 등 IoT(Internet of Things, 사물인터넷) 기기 간의 통신 및 데이터 교환을 안전하게 처리하는 데에도 활용될 수 있다.

# 8. 블록체인의 문제 및 개선방안

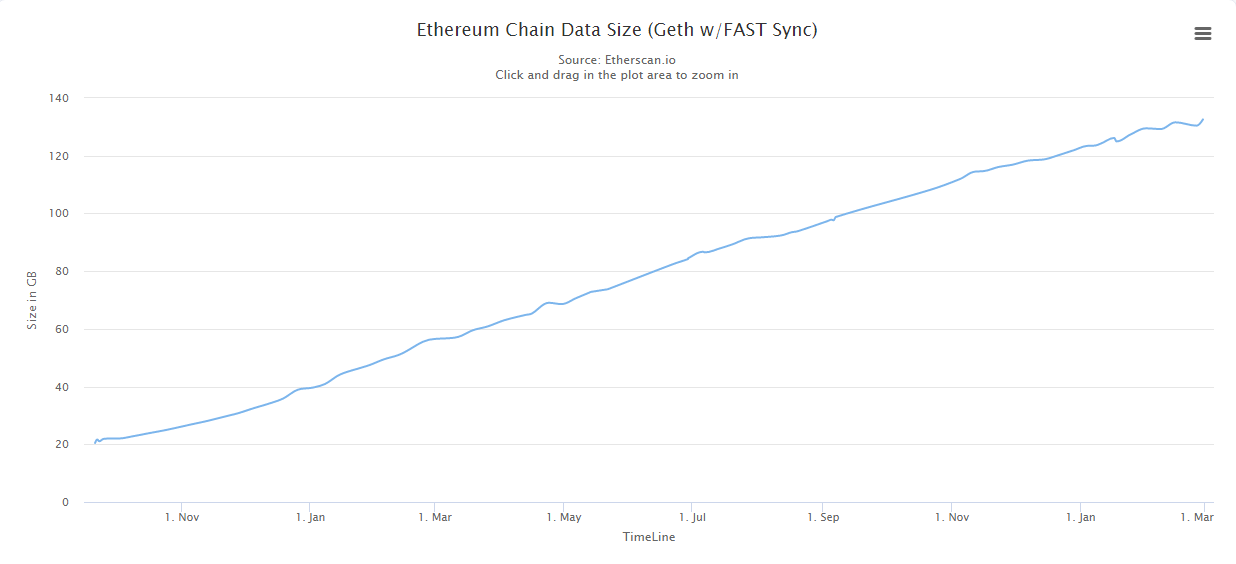
블록체인 기술은 분산원장, 불변성, 분산 프로그램이 가능한 플랫폼이라는 특징으로 많은 관심을 받고 있지만, 여전히 몇 가지 한계점이 존재한다.

직면한 주요 과제 중 하나는 **확장성(scalability)**이다. 암호화폐는 그 특성상 발행속도를 제한하고 있다. 그림에서 보듯이 (source: https://etherscan.io/chart/tx), 하루에 많은 경우 170만 건 내외를 기록하고 있고, 이는 약 20 TPS이다. TPS(Transactions Per Second)란 초당 처리 건수를 나타내는 말로, 하루의 처리 건수를 86400으로 나누어서 계산한다. 마이닝 방법이 PoS로 개선되겠지만, 비자 또는 마스터카드의 처리 속도가 24,000 TPS에 이르는 것과 비교하면 아직 갈 길이 멀다고 하겠다.



alt text

또한 블록체인이 2019년 130GB를 넘어서 점점 커지고 있다 (https://etherscan.io/chart2/chaindatasizefast). 사진, 동영상 같은 콘텐츠는 용량이 커서 블록체인에 저장하게 되면 비용이 적지않게 발생하거나, 비효율적일 수 있다. 분산형 파일시스템 IPFS(Inter Planetary File System)는 파일을 저장할 때 잘게 쪼개어 네트워크에 분산하고 블록체인에는 인덱스 해시만 저장한다. 분산된 파일에는 인덱스 해시가 있어, 원본은 그 해시를 찾아서 조립하게 된다. 이러한 탈중앙화 블록체인 스토리지로는 IPFS를 포함해 sia, storj, maidsafe 등이 있다.



alt text

**시빌 공격(Sybil attack)**이란 악의적인 사용자가 혼자지만 다수의 IP 또는 컴퓨터를 활용하거나 여러 가짜 계정을 발급하여 악의적으로 시스템을 공격하는 위협을 말한다. 이런 공격은 사용자를 인증하고 식별하는 체계를 도입하여 막을 수 있다.

PoW, PoS와 같은 합의체제에서는 대규모의 컴퓨팅 파워 또는 토큰을 소유해야만 공격에 성공할 수 있다. 예를 들면 노드의 **51%**가 동시에 악의적으로 공격을 하게 되면 블록을 자신들이 원하는 대로 변조할 수 있지만, 이런 대규모의 소유는 참여자가 많아질 수록 거의 불가능하다.

특정 노드가 거래가 완성되는 것을 악의적으로 방해할 수 있지만, 참여 노드들은 지속적으로 마이닝하면서 블록을 생성해 나가기 때문에 그런 일부 노드의 악의적인 공격은 무산될 수 밖에 없다. 네트워크를 교란하기 위해 대규모 거래를 발생하게 되는 것도 비용이 비례해서 발생하기 때문에 별 의미가 없다.

현재 블록체인 확장성의 한계를 극복하기 위해서 몇 가지 방안이 제시되고 있다.

1. 대안적 합의 알고리즘 적용: PoW를 대신하여 앞서 설명한 PoS와 같은 대안적 합의 알고리듬을 적용하여 블록체인 네트워크의 처리 속도를 높이고 있다.
2. **샤딩(Sharding)** 기술 도입: 블록체인에서 발생하는 모든 거래를 단일 체인에 기록하는 대신, 여러 개의 샤드로 나누어서 처리하는 방식이다. 각 샤드는 담당하는 노드가 있어 독립적으로 거래를 처리하도록 구성하여 속도를 빠르게 하고, 확장성을 해결하고 있다. 이더리움은 노드에 샤드를 할당하면 해킹의 공격에 노출될 수 있으므로, 무작위로 노드를 선정하고 샤드를 할당하고 있다. 샤딩을 하게 되면 초당 최대 1,000 TPS를 처리할 수 있다. Vitalik은 샤딩과 레이어2 방식을 결합하면 최대 1,000,000 TPS를 처리할 수 있다고 전망한다. 샤딩은 레이어1에서 구현하는 기술로 다음에 설명하는 레이어2 기술과 대비된다.
3. 레이어2 방식 적용: 블록체인 네트워크 외부에서 추가적인 처리를 수행하여 블록체인의 부하를 줄이는 기술로서 상태채널, 사이드체인, 그리고 라이트닝 네트워크가 해당된다.

* 상태 채널(State Channels)은 블록체인 네트워크 상에서 발생하는 거래를 오프 체인(off-chain)으로 이동시켜 블록체인 상의 부하를 줄이는 기술이다.
* 사이드 체인(Sidechains)은 블록체인 네트워크의 기본 체인(메인 체인)과는 별도의 독립적인 블록체인으로 운영된다.
* **라이트닝 네트워크**: 블록체인 위에서 처리하지 않고, 결제 채널을 별도로 만들어 오프체인방식으로 레이어2에서 처리하는 것을 말한다. 사용자 간에 공동지갑을 열어, 거래를 블록체인을 경유하지 않고 실행한다. 거래가 많아도 공동 지갑 내에서 일어지는 일이므로 비용이나 마이닝이 필요하지 않다. 거래가 더 이상 필요하지 않으면 잔고를 정산하고, 단일 거래로 블록체인에 기록하면 된다.

## 연습문제

1. 지난 5년의 비트코인, 이더리움 가격의 변화를 알아보시오.
2. 블록체인은 블록의 연결이다. 블록의 해시 값을 트리로 연결하여 머클 트리를 만들고, 이 연결을 체인이라고 한다. OX로 답하시오.
3. 블록체인에 기록되어도 오래된 거래는 수정할 수 있지만, 직전의 거래는 수정할 수 있다. OX로 답하시오.
4. 마이닝이란 채굴한다는 의미이고, 거래를 암호화하는 과정을 말한다. OX로 답하시오.
5. 블록체인은 플랫폼으로서 합의를 통해 블록을 인증하면, 암호화는 필요하지 않다. OX로 답하시오.
6. 암호화폐는 DDoS 공격을 막기 위해 고안이 된 적이 있다. OX로 답하시오.
7. 이더리움의 최소단위 Wei는 어디서 비롯되었는지 답하시오.
8. 작업 증명은 비트코인에서 처음 적용이 된 기술이다. OX로 답하시오.
9. 화폐는 가치의 척도, 가치의 저장수단, 교환 수단으로서 기능한다고 한다. 암호화폐가 화폐로서 기능하는지 설명하시오.
10. 대안 코인들은 어떤 것들이 있는지 찾아서 시가 총액 순서대로 5개를 적어보시오.
11. CDBC는 중앙은행이 발행한 디지털화폐이다. OX로 답하시오.
12. 분산 시스템은 클라이언트-서버 방식과 달리 서버가 없다. OX로 답하시오.
13. 작업 증명은 어떤 작업을 했다고 확인하는 것을 의미한다. 어떤 작업을 해야 하는지 설명하시오.
14. 지분 증명은 작업 증명에서 지적되는 컴퓨팅 자원이 소모되는 것을 막고, 처리 속도를 빠르게 하기 위해 노드가 보유한 잔고를 기준으로 권한을 분배하는 합의 방식이다. OX로 답하시오.
15. 비트코인과 이더리움에 어떤 합의방식이 사용되고 있는지 적으시오.
16. 블록체인을 1.0과 2.0이라고 구분하기도 하는데, 무엇이 발전한 것인지 설명하시오.
17. 블록체인을 적용하면 공인인증서를 대신할 수 있다. OX로 답하시오.
18. 블록체인을 적용하면 은행의 개입 없이 송금이 가능하다고 한다. OX로 답하시오.
19. 블록체인 핸드폰이 출시되고 있는데, 어떤 점에서 유망한지 설명하시오.
20. 블록체인은 시간이 가면서 크기가 증가할 수 밖에 없다. 어떤 해결방이 있는지 설명하시오.
21. 블록체인은 처리시간이 오래 걸리는 문제가 있다. 어떤 해결방안이 있는지 설명하시오.