# 한 번에 끝내는
# 블록체인 개발 A to Z

---

Chapter 1

## Blockchain 1.0 - Bitcoin

Chapter 1

Blockchain 1.0 - Bitcoin

# Bitcoin의 한계점

# Bitcoin 한계점

### ❶ 느린 처리 속도

3-7 TPS의 처리속도
(VISA 24,000 TPS)

### ❷ 높은 에너지 사용량

핀란드 연간 사용량에 가까운
에너지 사용

### ❸ 제한적인 기능

BTC 전송이외의 기능이 제한

### ❹ 제한적인 익명성

Privacy 보호가 완벽하지 않음

# Bitcoin의 느린 처리 속도

### ❶ 높은 보안성

블록 생성 주기를 10분으로 하였고, 항상 10분이 유지되게 하고 있기 때문에 채굴자들은 어떤 Network Hash가 있더라도 10분 간의 Work를 진행해야 한다. (Double Spend 방지)

### ❷ Fork 가능성 낮음

전체 Blockchain Network가 하나의 Chain을 유지해야 Blockchain으로의 의미가 있는데, 이를 위해서는 Fork 발생 가능성을 줄여 최대한 하나의 Chain이 유지하도록 해야한다. Block 생성 주기를 10분으로 하게되면, 10분마다만 Fork 발생 가능성이 생기고, Re-org 하는 가능성도 줄어든다.

### ❸ Network Bandwidth 낮음

P2P Network는 노드간의 통신양이 기존 Client-Server 보다 많다. P2P의 모든 노드들간의 통신을 최대한 감소시켜야 Network Bandwidth가 낮아지고, 통신으로 인한 노드의 부하가 낮아질 수 있다.

# 대안 블록체인

### ❶ Ripple

2013년 출시한 은행들간의 Swift 망을 대체하기 위해 제시된 블록체인 프로토콜
1500 TPS 정도의 성능 제공

### ❷ Fabric

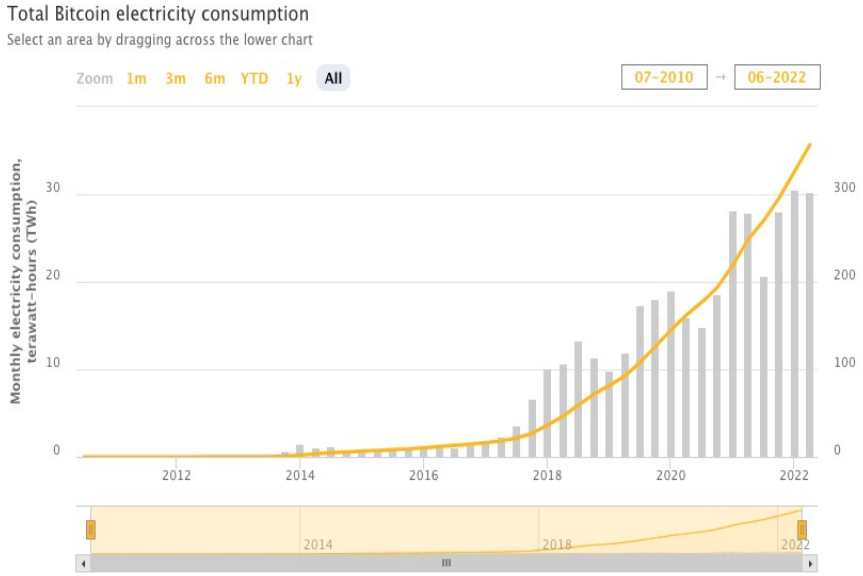
2016년 출시한 기업용 블록체인으로 Hyperledger 재단에서 운영 출시하였다.
Permissioned Blockchain의 대표적인 사례로 삼성SDS에서 특정 기술을 적용하여 20,000 TPS까지 지원한다고 밝혔다.

### ❸ Solana

2020년 출시한 MainNet으로 빠른 성능과 저렴한 수수료를 기반으로 출시한 블록체인 플랫폼이다. 최대 65,000 TPS를 지원한다고 하지만 현재 실제 사용량에 따라 약 1,000 TPS의 성능을 보여주고 있다.

# 높은 에너지 사용량

비트코인은 PoW를 위해 매년 90테라와트시의 전력을 사용하고, 이는 핀란드의 평균 연간 전력 소비량보다 많고 미국 평균 가정의 2개월치 사용량이다.

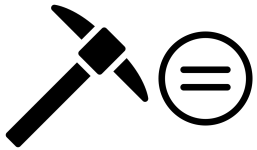



(출처 : https://ccaf.io/cbeci/index)

# 에너지
# 사용량 감소

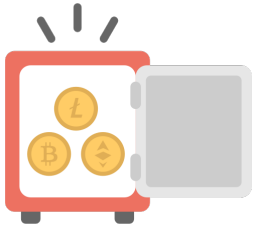
- 높은 에너지 사용량과 빠른 성능을 위해서 많은 블록체인이 최근 합의 알고리즘으로 PoS(Proof of Stake)를 사용하고 있다.
- Proot Of Stake는 지분 방식 증명으로 소유하고 있는 토큰의 수량에 따라 일정량의 투표권을 제공하는 방식이다.

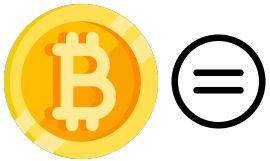
Proof Of Work



1 Block For Share

Proof Of Stake

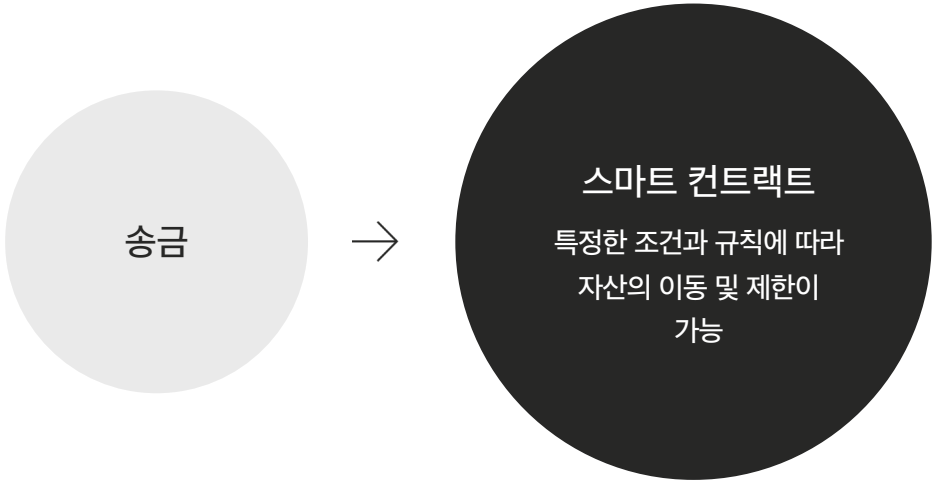




1 Block For Share

# 제한적인 기능

1세대 Bitcoin은 자산의 저장, 송금 기능 이외의 기능을 제공하고 있지 않고 있기 때문에, Digital Gold라고 불린다. 하지만 2세대 Blockchain인 Ethereum은 Smart Contract를 통해 Defi와 같은 금융서비스를 제공할 수 있다.



# 제한적인 익명성

### ❶ PKI를 이용한 익명성

Bitcoin의 익명성은 신원인증 없이 PKI를 이용해서만 거래를 하여, 사용자의 실제 신원을 숨기는 익명성을 제공한다.

### ❷ Key 재사용 제한

Bitcoin 공식 문서에서는 사용자의 익명성을 제한하기 위해서 Key(주소) 사용을 한번만으로 제한할 것을 권장하고 있다.

### ❸ Mixer

CoinJoin과 같은 코인 Mixer 기능을 통해 다른 사용자와의 거래에 나의 거래를 숨길 수 있는 기능을 제공하고 있다.