

암호화폐 비트코인의
핵심기술, 블록체인

인터넷 상에서 Safety, Liveness,
Fault tolerance를 모두 만족하는 합의 메커니즘을
만드는 일은 이론적으로 불가능함

- 우리는 이중 몇가지(최대 2가지)를 선택할 수 밖에
없으며, 이로 인해 블록체인상의 합의
- 메커니즘은 매우 다양한 형태를 띠게 됨

Bitcoin의 경우

- Liveness와 Fault Tolerance를
선택한 대신 Safety를 희생시킴
- 이로 인해 판정이 번복될 가능성이 항상 존재함

채굴(Mining)이란?

비트코인의 중복사용을
막기 위해 사용자들

장부(블록)를 만들고,
회람하고, 투표를 통해
초부를 선정하는 일들을
끊임없이 반복해서
수행해야 함

자발적으로 장비를
구입하고, 돌리고,
전기요금까지 내기란
쉽지 않음
→ 문제를 해결하고자
인센티브 개념을 도입
→ 채굴(Mining)

co.n.sensus
Mechanisms

- Heaviest/Longest chain Selection Rule
- PBFT
- Ben-Or
- Tendermint/cosmos
- Avalanche
- etc

Sybil co.n.trol
Mechanisms

- PoW(Proof of work)
- PoS(Proof of Stake)
- ...

블록체인이 당면
기술적 한계들

블록체인이 만능은 아니며,
한계점도 분명히 존재함

탈중앙화 및 확장성,
개인정보보호 문제

블록체인 생태계 전반에 영향을
미칠 수 있는 매우 중요한 문제이며,
해결하기 또한 쉽지 않은 매우
어려운 문제임