# 블록체인

1871005 강예준

한성대학교 HANSUNG UNIVERSITY

유튜브 주소 : https://youtu.be/r_Oq-WytXbY

CryptoCraft LAB
https://crypto.modoo.at

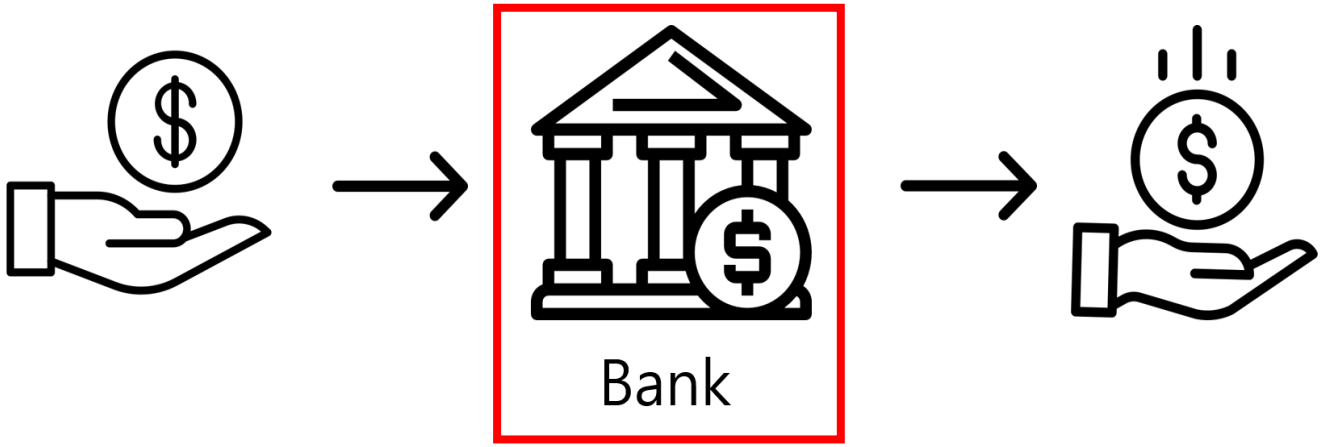
# Contents



CryptoCraft LAB

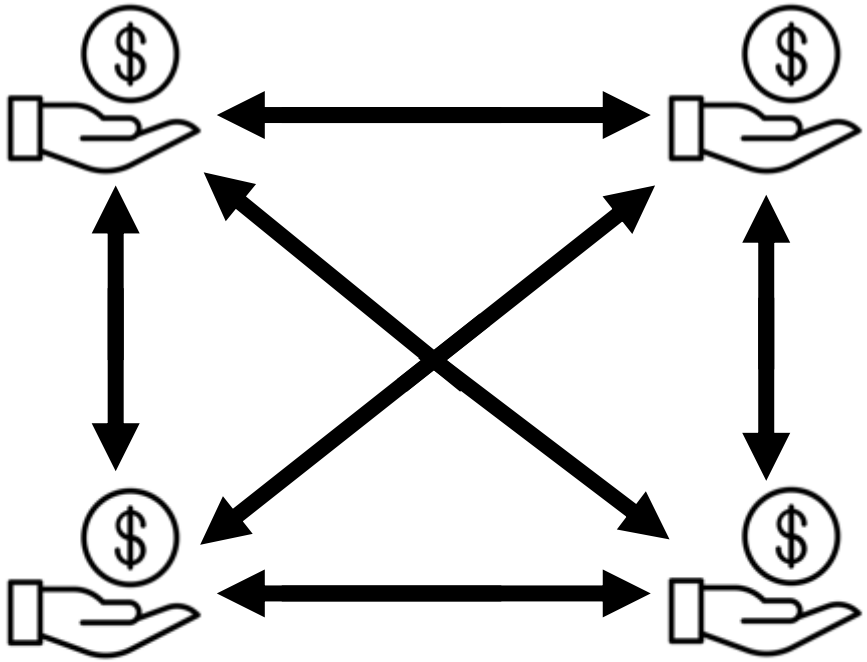
# 01. 블록체인의 정의와 배경

# 1. 블록체인의 정의와 배경



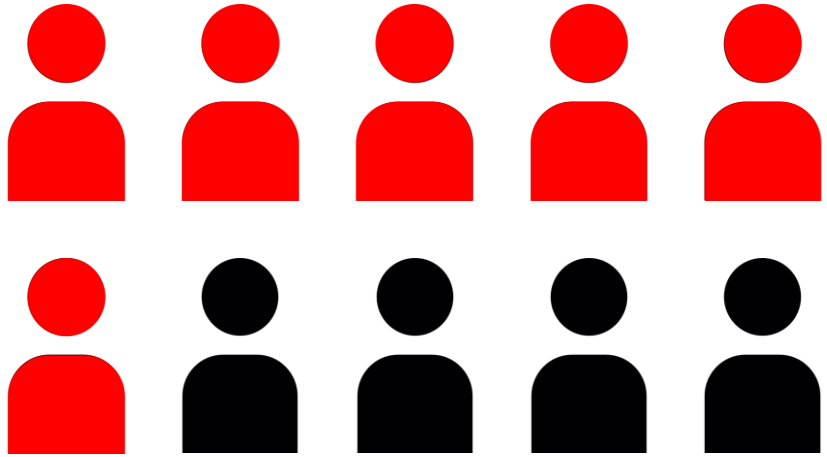

**기존 거래 시스템 방식**

# 1. 블록체인의 정의와 배경



**블록체인 거래 시스템 방식**

# 1. 블록체인의 정의와 배경



**51% Attack**

# 02. 블록체인의 분류

# 02. 블록체인의 분류

| | 퍼블릭 블록체인 | 컨소시엄 블록체인 | 프라이빗 블록체인 |
|---|---|---|---|
| **관리 주체** | 모든 거래 참여자 (탈중앙화) | 컨소시엄에 소속된 참여자 | 중앙기관이 모든 권한 보유 |
| **거버넌스** | 한 번 정해진 법칙을 바꾸기 매우 어려움 | 컨소시엄 참여자들의 합의에 따라 상대적으로 용이하게 법칙을 바꿀 수 있음 | 중앙기관의 의사결정에 따라 용이하게 법칙을 바꿀 수 있음 |
| **거래속도** | 느림 | 빠름 | 빠름 |
| **데이터 접근** | 누구나 접근 가능 | 허가받은 사용자만 접근가능 | 허가받은 사용자만 접근 가능 |
| **거래증명** | PoW, PoS와 같은 알고리즘에 따라 거래증명자가 결정되며, 거래증명자가 누구인지 사전에 알 수 없음 | 거래증명자가 인증을 거쳐 알려진 상태이며, 사전에 합의된 규칙에 따라 거래검증 및 블록 생성이 이루어짐 | 중앙기관에 의하여 거래증명이 이루어짐 |
| **활용사례** | 비트코인, 이더리움 | R3 CEV | 나스닥의 비상장 주식거래소 플랫폼인 링크(Linq) |

**블록체인의 유형 (출처:정보통신산업진흥원)**

# 02. 합의 알고리즘

# 02. 합의 알고리즘

- 블록체인 네트워크 상에서 데이터(블록)의 무결성 검증 및 생성을 위한 노드 간 미리 정의된 절차 기반 의사결정 알고리즘

- 대표적인 합의 알고리즘

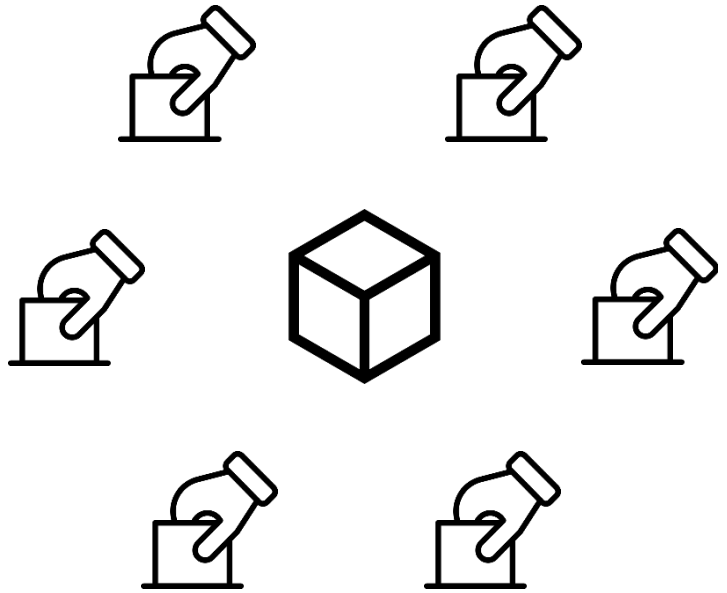
1) PoW(Proof of Work)
2) PoS(Proof of Stake)
3) DPoS(Delegated Proof-of-Stake)

# 1) PoW(Proof of Work) 합의 알고리즘

- 작업증명
- 사토시 나카모토가 제안한  가장 보편적인 합의 알고리즘
- 새로운 블록을 생성하여 제안할 수 있는 권한을 받기 위해서는 퍼즐을 풀어야함
- 퍼즐을 푸는 과정을 ' 채굴 ' 한다고 표현
- 채굴에 성공하면 암호화폐를 지급 받음
- 문제를 풀기 위한 CPU 혹은 GPU의 높은 해싱 파워를 요구
- PoW 합의 알고리즘을 사용하는 대표적인 사례로는 비트코인, 라이트코인, 제트캐시 등이 있음

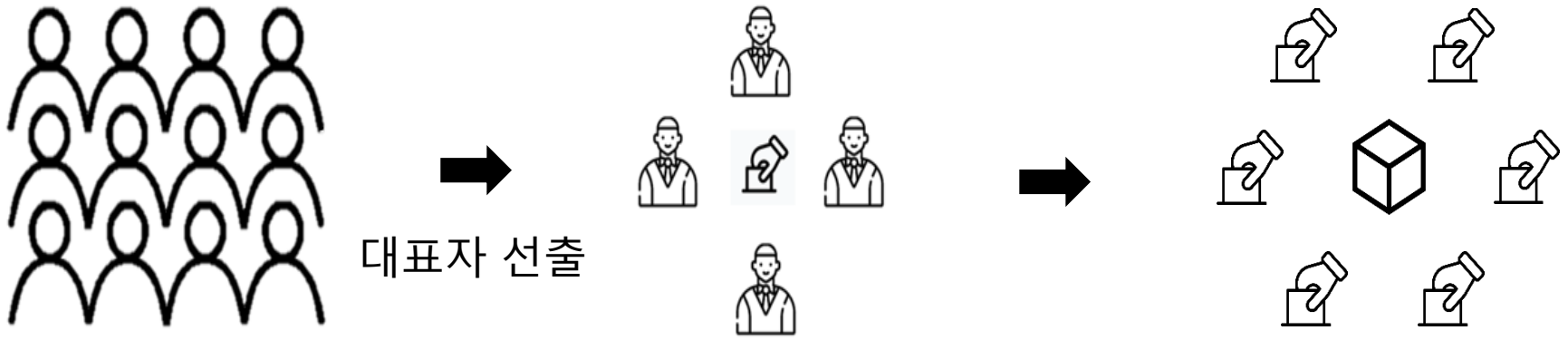
# 2) PoS(Proof of Stake) 합의 알고리즘

- 지분증명
- 투표를 통해 토큰 보유량만큼 증명에 참여하여 다음 블록을 생성하는 알고리즘
- 참여자는 다음 블록으로 제안된 블록 후보들 중에서 합당하다고 생각하는 블록에 투표
- PoW 합의 알고리즘의 단점인 많은 양의 컴퓨터 자원을 소모하여 문제를 푸는 방식을 개선



# 3) DPoS(Delegated Proof-of-Stake) 합의 알고리즘

- 위임을 한 지분방식
- 투표를 통해 선출된 대표들은 PoS 합의 알고리즘을 진행
- 합의 시간과 비용⬇
- 속도⬆



# 감사합니다!