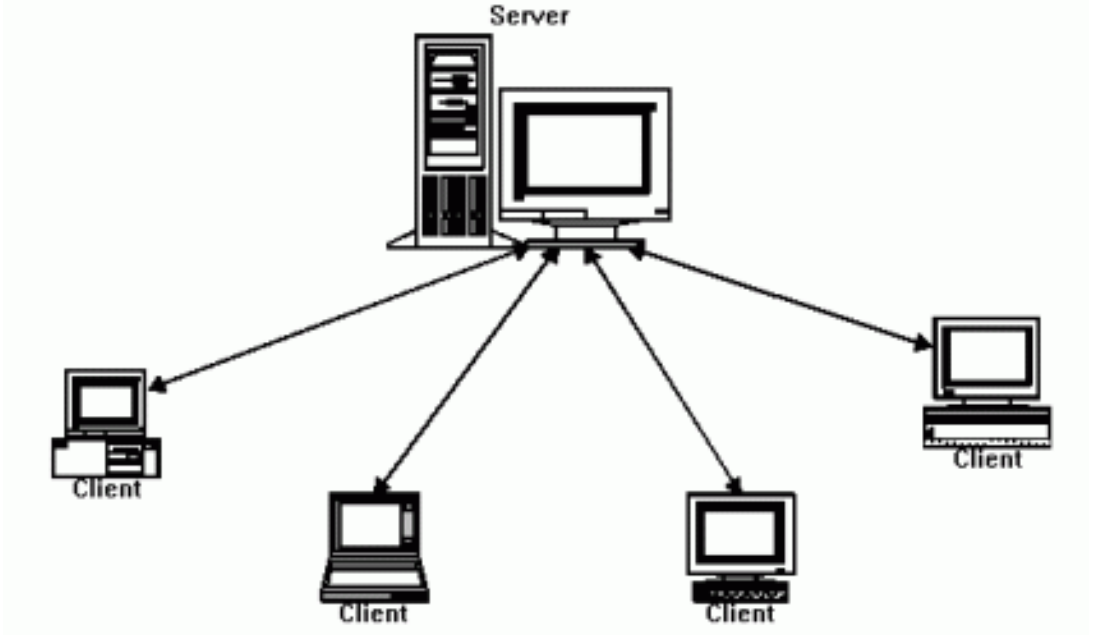
블록체인 합의과정

https://youtu.be/vQTiEcV5XtU

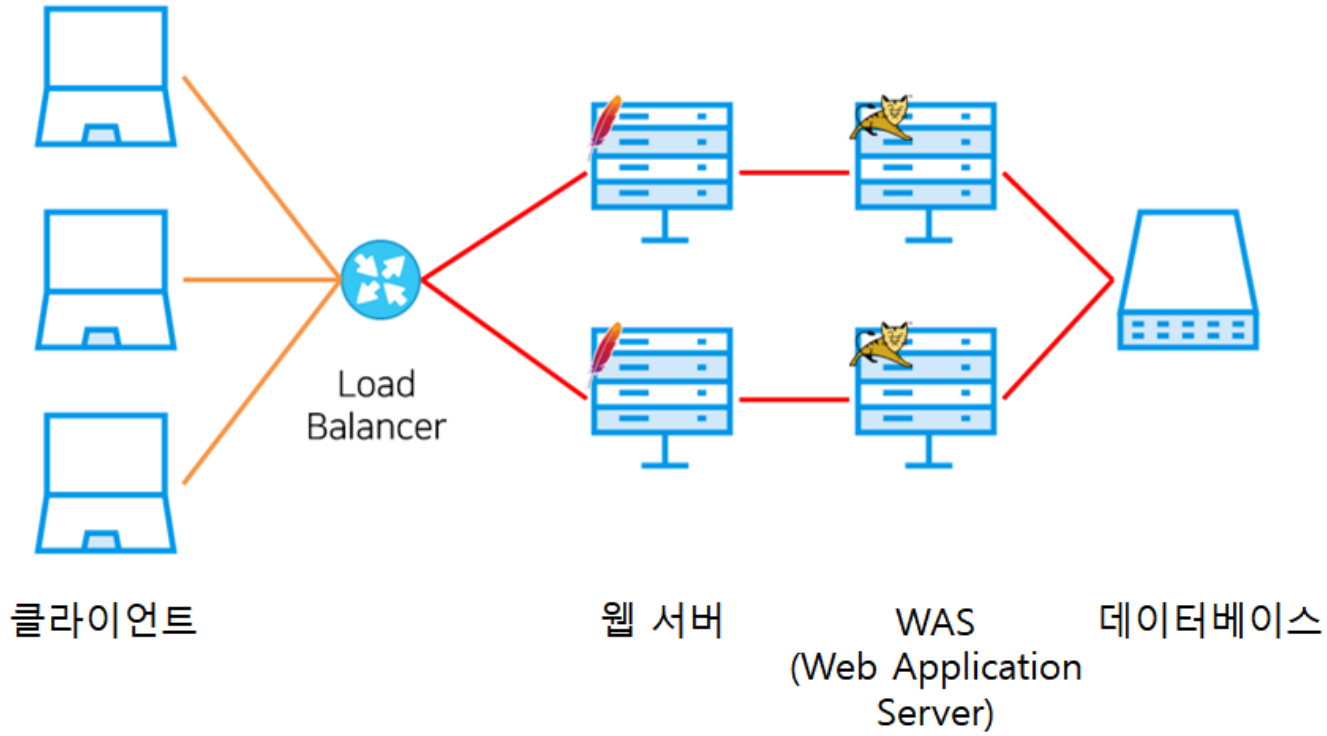
서버-클라이언트 데이터 전달

- 중앙 서버를 통한 데이터 전달
- 서버 과부하 발생 가능



분산 처리 시스템

- 과부하를 줄임
- 추가적인 확장 가능
- 투명성 보장



분산 처리 시스템 - 투명성

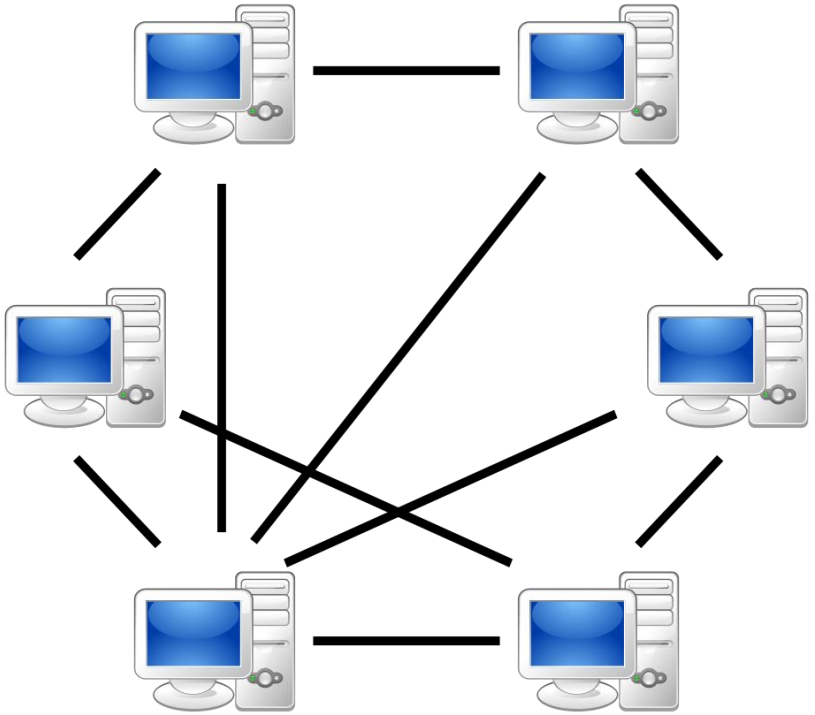
- 위치 (Location)
- 이주 (Migration)
- 복제 (Replication)
- 병행 (Concurrency)
- 접근 (Access)
- 성능 (Performance)
- 규모 (Scaling)
- 고장 (Failure)

분산 처리 시스템 - 단점

- 소프트웨어 개발 난이도
- 데이터 처리 서비스의 질이 떨어짐
- 보안 문제

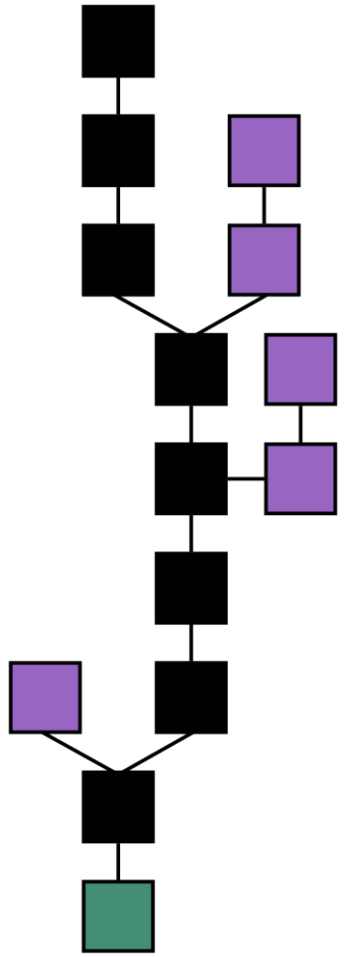
P2P

- Peer-to-Peer
- Peer 간 상호작용을 통해 구동

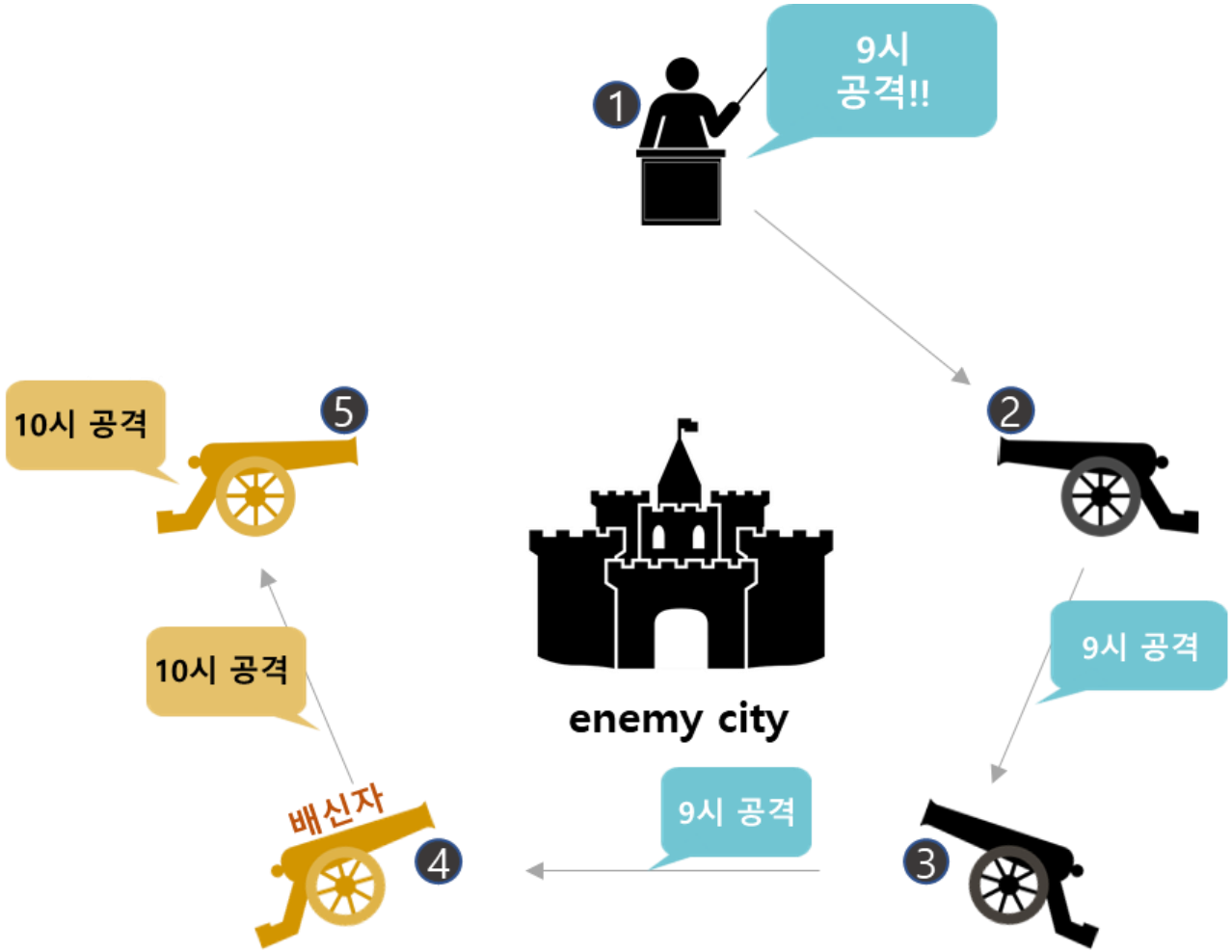


블록체인

- P2P 방식을 이용한 블록 생성
- 중앙 저장소 없이 데이터 전송/열람



비잔틴 장군 문제



합의 알고리즘

- 생성된 블록의 정당성을 확인

- 퍼블릭 / 프라이빗 블록체인에 따라 구분

퍼블릭 블록체인

- 특정 조직의 승인이 필요 없이 네트워크 참여자의 의사에 따라 참여/탈퇴 결정
- 투명성 및 보안성 강화
- 속도가 느림

퍼블릭 블록체인

- 작업 증명 (Proof of Work, PoW)
- 가장 보편적인 방법
- 컴퓨터의 연산을 이용하여 특정 난이도의 문제를 해결

퍼블릭 블록체인

- 지분 증명 (Proof of Stake, PoS)
- 작업 증명의 컴퓨팅 파워 낭비 문제 해결
- 보유한 자산을 기준으로 권한 분배

퍼블릭 블록체인

- 위임 지분 증명 (Delegated Proof of Stake, DPoS)
- 코인 보유자들이 대표 몇 명한테 투표
- 대표는 새로운 블록의 생성과 검증 과정에 합의를 도출할 책임을 가짐

프라이빗 블록체인

- 허가 받은 사람들만이 참여하는 네트워크
- 속도가 빠름
- 중앙화 되어 보안성이 낮아질 가능성

프라이빗 블록체인

- Paxos
- 리더를 선정한 뒤 과반수의 동의를 통해 합의
- 악의를 가진 참가자가 있으면 적절하지 않음

프라이빗 블록체인

- PBFT (Practical Byzantine Fault Tolerance)
- 대표자 한 명을 선출하고 그 대표자가 참여자들에게 요청을 보냄
- 답변을 집계하여 확정

Q & A