블록체인의 개념과 원리

블록체인은 데이터를 블록 단위로 저장하고, 각 블록을 암호학적으로 연결하여 체인 구조를 형성하는 분산 원장 기술(DLT) 입니다. 각 블록은 이전 블록의 해시 값을 포함해 데이터의 무결성과 보안성을 유지하며, 네트워크 참여자 간의 합의를 통해 새로운 블록이 추가됩니다. 이를 통해 중앙 기관 없이도 투명하고 신뢰할 수 있는 거래 및 기록 관리가 가능하며, 금융, 공급망, 헬스케어 등 다양한 분야에서 활용됩니다.

블록체인의 주요 특징

탈중앙화

단일 기관이 통제하지 않고, 네트워크 참여자가 공동으로 운영

불변성

블록체인에 기록된 데이터는 수정·삭제가 불가능

투명성

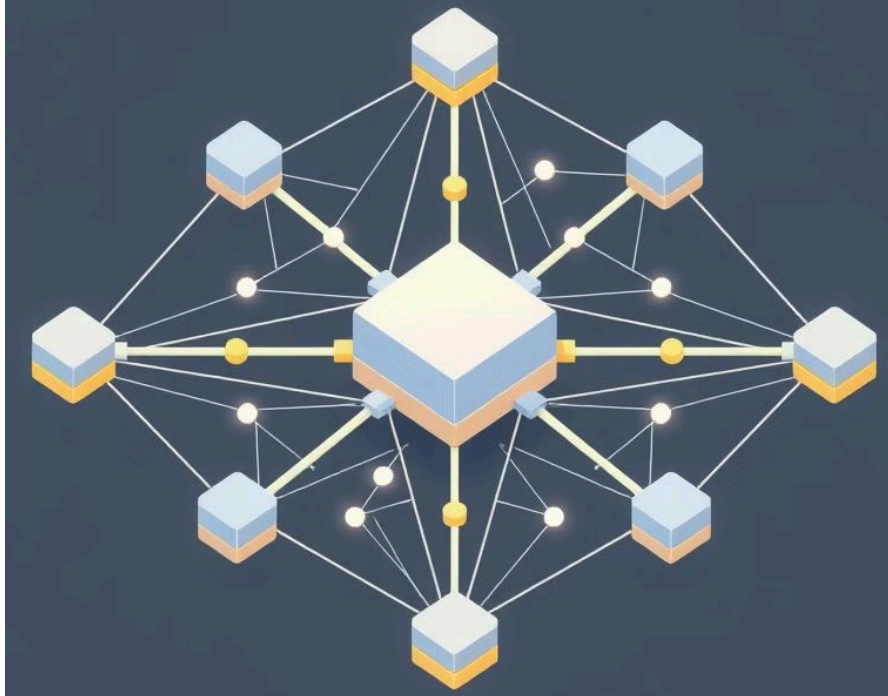
누구나 거래 내역을 조회할 수 있지만, 익명성은 유지 가능

보안성

해싱, 디지털 서명, 암호화 기술로 높은 보안성 확보

합의 메커니즘

- PoW(작업 증명), PoS(지분 증명) 등 다양한 검증 방식



기존 중앙 집중형 시스템과 차이점

중앙 집중형 시스템의 한계

- 단일 서버가 데이터를 관리 → 해킹, 조작 위험
- 중앙 기관의 검열 가능성
- 중개자 개입으로 거래 비용 증가

블록체인의 차별점

- 데이터를 여러 노드에 분산 저장 → 단일 장애점 없음
- 신뢰할 수 있는 중개자 없이 직접 거래 가능
- 모든 거래 내역이 네트워크 참여자에게 공유됨

블록의 구조

블록 헤더

이전 블록 해시, 머클 루트, 타임스탬프 등

블록 바디

실제 거래 기록 저장

구성 요소	설명
이전 블록 해시	이전 블록을 가리키는 해시 값
머클 루트	블록 내 모든 암호화의 요약 값
타임 스탬프	블록 생성 시간
난이도 목표	블록 해시가 만족해야하는 조건
넌스(Nonce)	Pow에서 올바른 해시를 찾기 위한 숫자

블록체인의 작동 원리

1

거래 발생

사용자가 블록체인 네트워크에서 거래 요청

2

거래 검증

네트워크 노드가 거래의 유효성을 검증

3

블록 생성

유효한 거래가 블록으로 묶여 새로운 블록 형성

4

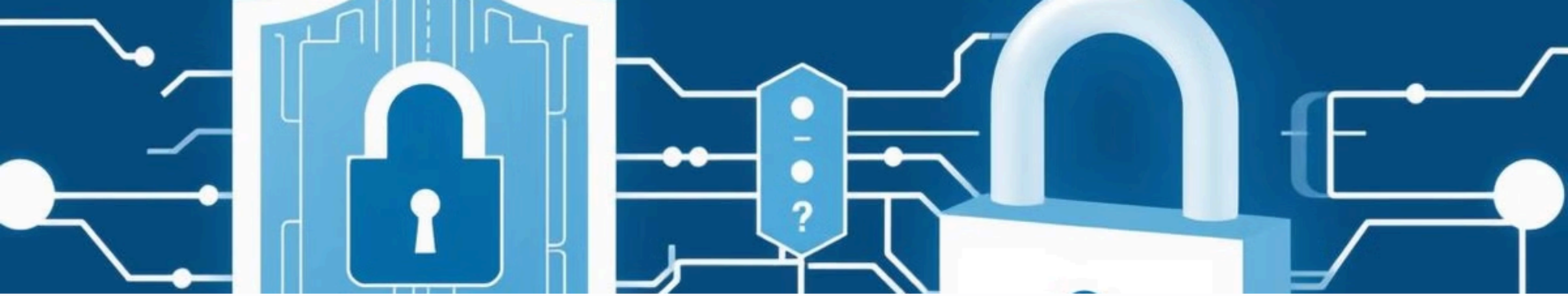
합의 과정

PoW, PoS 등의 방식으로 블록 유효성 검증

5

블록 추가

새로운 블록이 기존 체인에 연결



블록체인의 암호화 기술

해싱

- 데이터를 일정한 길이의 암호화된 값으로 변환
- SHA-256 등의 해시 알고리즘 사용

공개키 암호화

- 공개키(Public Key)와 개인키(Private Key)로 암호화
- 개인키는 거래 승인에 사용, 공개키는 신원 확인에 사용

1

2

3

디지털 서명

- 거래의 신뢰성을 보장하기 위해 개인키를 사용하여 서명
- 누구나 공개키로 서명을 검증 가능

기존 중앙 집중형 시스템과 차이점

금융

암호화폐, 국경 간 결제, 탈중앙화 금융(DeFi)

공급망 관리

물류 추적, 위조 방지

헬스케어

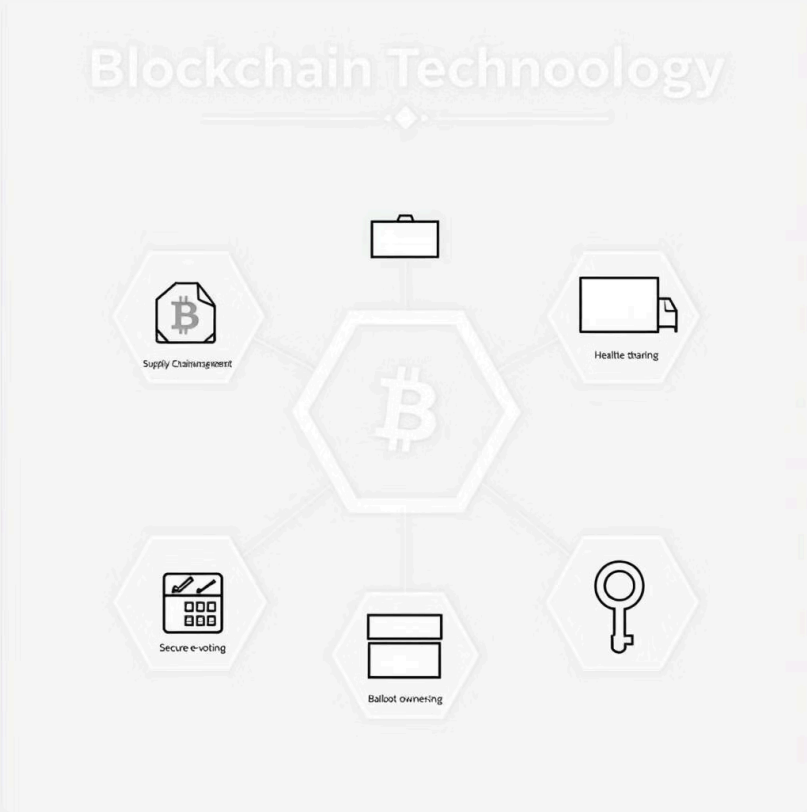
환자 기록 관리 및 데이터 공유

전자 투표

보안성이 높은 투표 시스템 구축

디지털 자산

NFT(대체 불가능한 토큰), 저작권 보호



블록체인의 미래 전망 및 과제

기술적 발전

- 확장성 향상을 위한 샤딩(Sharding), Layer 2 솔루션
- 에너지 효율성을 고려한 친환경 합의 알고리즘 개발 (PoS 전환)

법적·규제 문제

- 정부 규제 및 법적 프레임워크 마련 필요
- 개인정보 보호 문제와 KYC(고객 신원 확인) 요구

보안 문제 해결

- 스마트 컨트랙트 보안 취약점 해결
- 양자 컴퓨팅 시대 대비한 블록체인 암호화 기술 개발