

1. Introduction to Blockchain

Contents

1. 블록체인의 정의: 신뢰 기반의 분산 기술
2. 블록체인의 구성 요소:
 - 블록(Block)
 - 트랜잭션(Transaction)
 - 체인(Chain)
3. 블록체인의 네트워크 구조:
 - 노드(Node): 블록체인을 구성하는 참여자
 - 피어(Peer): 탈중앙화 네트워크에서의 노드 간 연결
4. 중앙화 vs. 탈중앙화: 블록체인의 차별점
5. 블록체인 아키텍처

1. 블록체인의 정의: 신뢰 기반의 분산 기술

Blockchain 의 정의 :

- 블록체인은 디지털 데이터를 투명하고 안전하게 저장하고 관리하기 위한 **분산 장부 기술(Distributed Ledger Technology)**

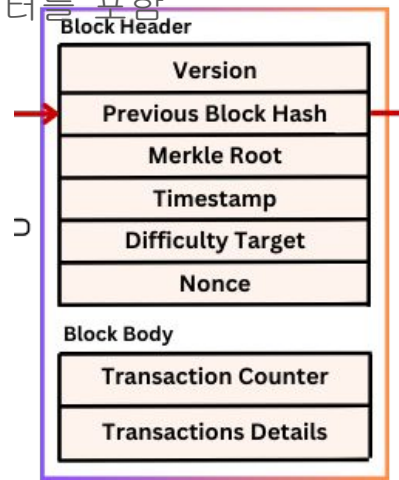
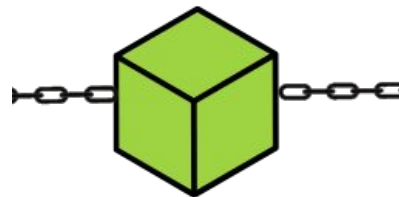
Blockchain의 특징 :

- 블록체인은 신뢰할 수 없는 환경에서도 중앙 기관 없이 신뢰를 구축할 수 있는 기술
- 데이터를 시간 순서대로 기록하며 변경이 불가능한 구조로, 투명성과 보안성을 보장
- 주로 가상화폐(비트코인 등), 스마트 컨트랙트, 탈중앙화 금융(DeFi) 등에서 활용

2. 블록체인의 구성 요소 (블록)

블록 (Block) :

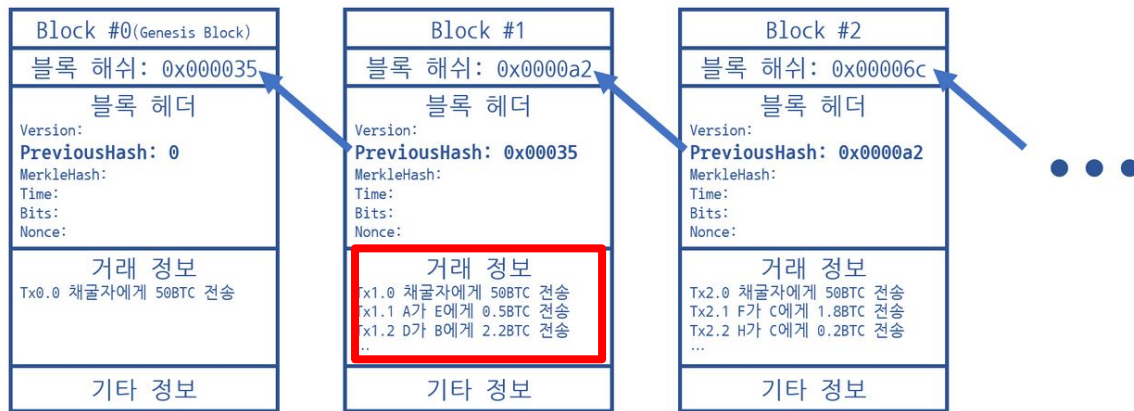
- 블록은 데이터가 저장되는 기본 단위
- 각 블록은 **헤더(Header)**와 **바디(Body)**로 구성
 - **헤더**: 이전 블록의 해시값, 생성 시간, 난이도 값, nonce(nonce) 등 메타데이터를 포함
 - **바디**: 트랜잭션 데이터를 저장
- 블록은 암호화된 방식으로 연결되어 체인을 형성



2. 블록체인의 구성 요소 (트랜잭션)

트랜잭션 (Transaction) :

- 블록체인에서 기록되는 데이터의 최소 단위
- 일반적으로 트랜잭션은 사용자 간 자산 이동(예: 비트코인 전송) 또는 스마트 컨트랙트 실행을 의미
- 트랜잭션은 블록 생성 전, 네트워크 노드에서 검증되어야 함

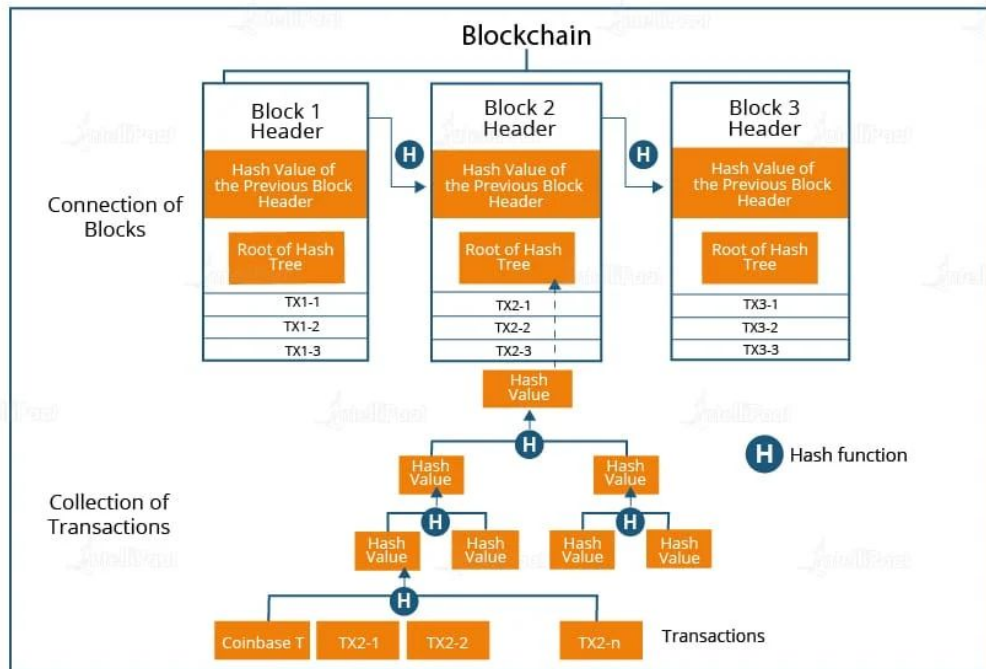


2. 블록체인의 구성 요소 (체인)

체인(Chain) :

- 블록들이 연결되어 형성된 데이터의 연속체
- 각 블록은 이전 블록의 해시값을 포함하여 변조가 불가능
- 데이터의 무결성을 보장하고, 신뢰할 수 없는 환경에서도 신뢰를 제공

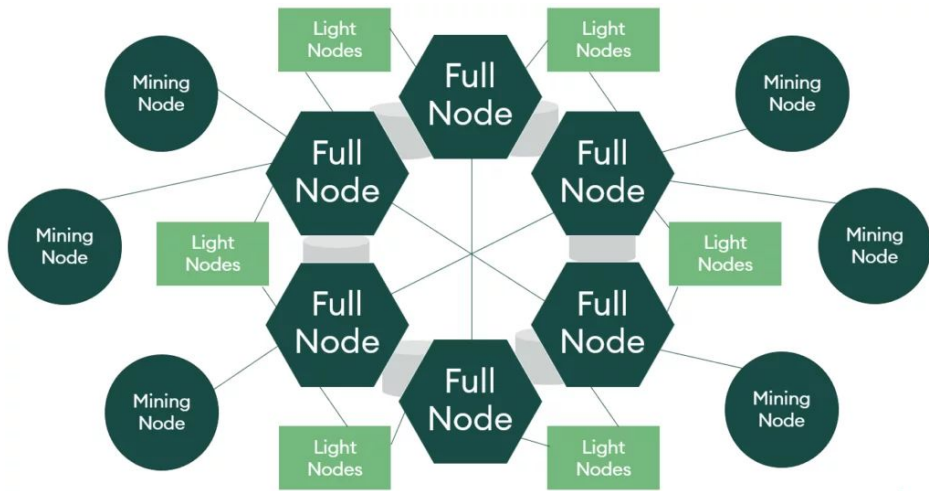
Structure of Blockchain



3. 블록체인의 네트워크 구조

노드(Node) :

- 블록체인을 구성하는 참여자(컴퓨터 또는 서버)
- 각 노드는 블록체인의 복사본을 저장 & 새로운 트랜잭션과 블록을 검증하고 동기화



3. 블록체인의 네트워크 구조

노드의 유형:

- **풀 노드(Full Node):** 전체 블록체인을 저장하며 트랜잭션 및 블록 검증에 참여
- **라이트 노드(Light Node):** 주요 데이터만 저장하며 간단한 작업 수행
- **마이닝 노드(Mining Node):** 새로운 블록을 생성하는 역할 수행

노드 유형	저장 데이터	장점	단점
풀 노드	전체 블록체인	네트워크 완전 검증 가능	저장 공간과 리소스 요구
라이트 노드	블록 헤더만	저장 공간과 리소스 절약	완전 검증 불가

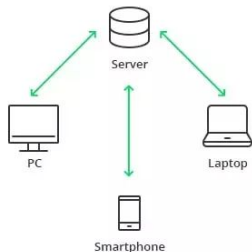
3. 블록체인의 네트워크 구조

피어(Peer) :

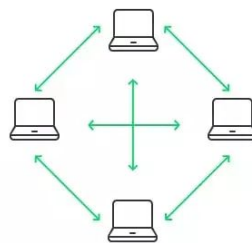
- 탈중앙화 네트워크에서 노드 간의 연결을 의미
- 블록체인은 P2P(Peer-to-Peer) 네트워크로 구성되며, 모든 노드가 동등한 권한을 가짐
- 피어 간 데이터는 실시간으로 전파 및 동기화

4. 중앙화 vs. 탈중앙화: 블록체인의 차별점

	중앙화 시스템	탈중앙화 시스템
특징	중앙 서버 또는 기관이 데이터를 관리	데이터가 네트워크의 모든 노드에 분산 저장
예시	은행, 클라우드 서버	비트코인, 토렌트
장점		단일 장애점 제거, 데이터 위조 및 해킹 사실상 불가능 투명성 및 신뢰성
단점	단일 장애점, 데이터 위조 및 해킹 가능성	확장성 문제, 데이터 처리 속도가 느릴 수 있음



Client-server



P2P network

5. 블록체인 아키텍처

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Low	High	High
Centralization	No	Partial	Yes
Consensus process	Permissionless	Needs permission	Needs permission

5. 블록체인 아키텍처

Public Blockchain

- **특징**
 - 완전한 탈중앙화, 투명성, 보안(높은 수준의 보안을 위해 작업증명 PoW 또는 지분증명 PoS와 같은 합의 알고리즘 사용), 익명성
- **장점**
 - 개방형 네트워크로 누구나 접근 가능
 - 탈중앙화로 인해 신뢰의 중개자(은행, 정부 등)가 필요 없음
- **단점**
 - 느린 처리 속도
 - 높은 에너지 소비 (특히 PoW 기반 시스템)
- **사용 사례**
 - 비트코인, 이더리움과 같은 암호화폐
 - 완전한 투명성과 개방성이 필요한 응용 (ex 글로벌 결제 시스템, 분산 금융DeFi)

5. 블록체인 아키텍처

Consortium Blockchain

- **특징**
 - 부분적 탈중앙화(멤버가 제한), 접근 제한, 효율성(제한된 참여자로 인해), 보안 강화
- **장점**
 - 처리 속도와 효율성이 높음
 - 데이터 접근과 관리가 제한적이므로 기업 간 협력에 적합
- **단점**
 - 완전한 탈중앙화가 아니므로 신뢰의 중개자가 여전히 필요
 - 투명성이 **Public Blockchain** 보다 낮음
- **사용 사례**
 - 금융기관 간 결제 시스템 : 여러 은행 간 빠르고 안전한 결제를 처리 (ex. R3의 Corda)
 - 공급망 관리 : 다양한 이해관계자가 공유하면서도 기밀성 유지 (ex. Hyperledger Fabric)
 - 헬스케어 데이터 관리 : 병원과 연구소간 민감한 데이터 교환

5. 블록체인 아키텍처

Private Blockchain

- 특징
 - 중앙 집중화, 접근 완전 제한, 효율성 극대화, 보안 강화
- 장점
 - 빠르고 효율적이며 맞춤형 설계 가능
 - 기업 내부의 데이터 관리와 Workflow에 최적화
- 단점
 - 탈중앙화가 거의 없고, 소유자의 신뢰에 의존
 - Public Blockchain에 비해 투명성이 매우 낮음
- 사용 사례
 - 기업 내부 데이터 관리 : ex. 직원 기록 관리, 내부 자산 추적
 - 정부 관리 시스템 : ex. ID발급, 세금 기록 등 민감 데이터 처리
 - 은행 내부 시스템 : 거래 기록과 같은 민감한 데이터를 효율적으로 관리

End