블록체인

**개념**: 블록체인이란 일종의 데이터 분산 저장 프로토콜이다.

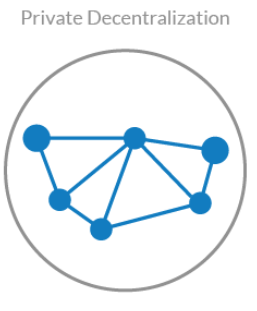
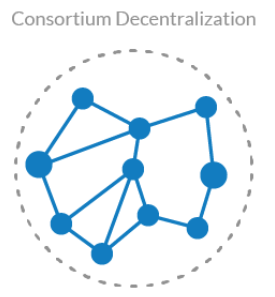
암호화된 데이터를 블록이라고 하며 블록들은 해싱(SHA-2 해시함수 사용, 256비트의 해싱결과)을 통해 서로를 매핑한다. 블록들의 집합를 하나의 블록체인이라고 하며 퍼블릭 블록체인의 경우 집단의 모든 노드(컴퓨터)가 각각 블록체인을 자신의 소유한다. 새로운 블록을 생성할 때는 시스템 내의 모든 노드의 과반수 이상의 동의를 얻어야 함.

탈중앙화, 작업 증명으로 인한 보안성이 특징.

등장 배경: 개인용 컴퓨터의 가격하락, 인터넷 속도의 향상

**블록체인의 종류**

|  |  |  |  |
| --- | --- | --- | --- |
|  | 퍼블릭 블록체인 | 프라이빗 블록체인 | 컨소시엄 블록체인 |
| 장점 | 보안성 보장 | 비교적 빠른 속도 |  |
| 특징 | 네트워크 참여조건만 갖추면 블록생성가능 | 관리자에게 허가된 주체만 블록 생성 가능 | 퍼블릭+프라이빗의 중간 |
| 속도 | 7~20 tps | 1000tps 이상 | 중간 정도 |
| 활용사례 | 비트코인, 이더리움 | 나스닥(링크,미진) | 코다, 하이퍼렛져 패브릭 |

퍼블릭 블록체인: 공개형 블록체인이라고도 하며, 블록 공유로 데이터 보안성을 보장할 수 있다.

이더리움의 경우 1초에 평균 13개 정도의 트랜잭션으로 트랜잭션 처리속도가 매우 느림

(페이스북은 1초에 17만 5천개의 트랜잭션 처리)

프라이빗 블록체인: 사전에 허가받은 노드만 사용가능. 트랜잭션 처리속도가 비교적 빠름.

서비스 구축자와 사용자가 일치하는 경우 적합(기업 내부 자체시스템 구축 등)

공유되지않아 노드가 아니면 추적이 불가, 블록체인의 기본적인 운영하는 주체가 없음을 위배

컨소시엄 블록체인: 프라이빗 블록체인이 여러 개 결합된 형태. 프라이빗 블록체인에 비해 비교적 개인의 독점을 막을 수 있다.

**이더리움**: 분산화 컴퓨팅 플랫폼에 기반한 블록체인. 비트코인으로부터 하드포크됨.

스마트 컨트랙트(스크립팅 기능)-특정 조건을 만족하면 자동으로 트랜잭션 발생하는 프로그램

\*solidity- 이더리움에서 스마트 컨트랙트 코딩을 위해 사용하는 언어

\*가스- EVM 상에서 스마트 컨트랙트의 코드를 실행시키기 위한 수수료

1트랜잭션=21000가스 소모(10원 정도), 1가스(1gwei)=10^-9 ETH

DApp(Decentralized Application)-블록체인을 기반으로 P2P 방식으로 실행되는 어플

ex)도박어플, 금융거래소

화폐(ether, ETH)-스마트 컨트렉트를 실행할 떄 사용되는 연산능력에 대한 수수료

이더리움의 한계: 속도가 13tps 정도로 매우 느리고 작업증명 방식을 사용하기 때문에 뛰어난 연산능력을 갖고있는 소수에게 권력이 집중될 수 있다. 이에 대한 해법으로 지분증명 방식이 있다.

**퍼블릭 블록체인의 활용 사례:**

1. 가상화폐: 비트코인,이더리움,리플 등 가상화폐나 금융거래 분야로는 이미 활용이 많이 되고 있다. 특히 이더리움의 스마트 계약 기능을 활용해서 공급자와 소비자 간의 거래가 신용카드사, 은행 등을 거치지 않고 바로 가능해진다.
2. 음식의 유통경로 추적: 영국 SW회사 프로비넌스, 소매업자와 소비자가 재료를 생산에서부터 유통까지 전 과정을 명확하게 추적할 수 있도록 함.
3. SW 개발에 보안성 강화: 방산업체 록히드마틴&블록체인 전문업체 Guardtime Federal, SW 개발 프로세스 추적,저장에 사용.
4. 디지털 콘텐츠 관리: Ascribe, 아티스트와 콘텐츠 소비자를 직접 이어주고 저작권, 결제등을 관리할 수 있도록 함.
5. 의료기록 추적: DokChain, 개인의 의료내역을 안전하고 정확학 저장할 수 있도록 함.

의료데이터의 익명화(암호화)로 인해 연구원들에게 연구자료 제공 가능

1. 대출 승인: 급여명세서, 소득,은행잔고 증명서 등을 블록체인화 함으로써 대출 승인의 속도 향상가능.
2. 보험금 청구: 보험 사기와 관련해서 동일 사건의 이중결제 가능성을 낮출 수 있다.
3. 감사 추적: 변호사-클라이언트 간의 대화,데이터,문건 등을 변경없이 기록하기 쉽게 돼 재판에서 유용한 증거로 사용될 수 있음.
4. 전자투표: 기존의 전자투표 시스템에 보안을 강화해 신뢰성을 강화시켜줌.