블록체인에서 '암호화'

■ 블록체인에서 '암호화

- 단순히 데이터를 숨기는 것을 넘어, **보안, 무결성, 인증 등 블록체인 시스템의 핵심 특성을** 구현하는 데 필수적인 여러 암호학적 기법을 의미

■ 블록체인에서 주로 사용되는 핵심 암호화 기법

(1) 암호학적 해시 함수(Cryptographic Hash Function)

* 역할
  - 데이터의 무결성과 불변성을 보장
* 작동 방식
  - 블록에 기록되는 거래 내역, 이전 블록의 해시값 등의 모든 데이터를 입력으로 받아 고정된 길이의 고유한 문자열(해시값)을 생성
* 특징
  - 입력 데이터가 단 1비트라도 변경되면 완전히 다른 해시값이 생성되므로, 데이터의 변조를 즉시 감지할 수 있음
  - 해시값을 통해 원래의 입력 데이터를 역으로 알아내는 것이 거의 불가능(비가역성)
  - 이전 블록의 해시를 다음 블록에 포함하여 체인처럼 연결함으로써, 한번 기록된 데이터의 수정이 거의 불가능하게 만듬

(2) 비대칭 키 암호 방식(Asymmetric Cryptography)

* 역할
  - 네트워크 참여자의 인증과 부인 방지(거래 사실을 나중에 부인할 수 없도록 함), 익명성을 제공
* 작동 방식
  - 각 사용자는 서로 다른 한 쌍의 키를 가짐
    * 개인 키(Private Key) : 사용자 본인만 소유하고 비밀로 유지하는 키
    * 공개 키(Public Key) : 네트워크에 공개되며, 다른 사람이 개인 키 소유자를 확인할 때 사용(블록체인 주소는 이 공개 키를 기반으로 생성됨)

(3) 디지털 서명

* 거래(트랜잭션)가 발생하면, 거래 내용을 해시하고,
  그 해시값에 송신자의 개인 키로 암호화하여 서명을 생성
* 수신자는 송신자의 공개 키로 이 서명을 복호화하여
  거래가 해당 개인 키 소유자에 의해 이루어졌음을 확인
* 결과
  - 개인 키 없이는 유효한 서명을 생성할 수 없어, 거래의 진위성과 부인 방지가 보장됨

(4) 데이터 암호화 (선택적 기밀성 보장)

* 블록체인의 기본 특성은 투명성이지만, 특정 블록체인(프라이빗 블록체인 등)이나
  특정 애플리케이션에서는 거래 데이터 자체의 기밀성을 위해
  대칭 키 암호 방식이나 비대칭 키 암호 방식을 사용하여 거래 내용을 암호문 형태로 기록하기도 함