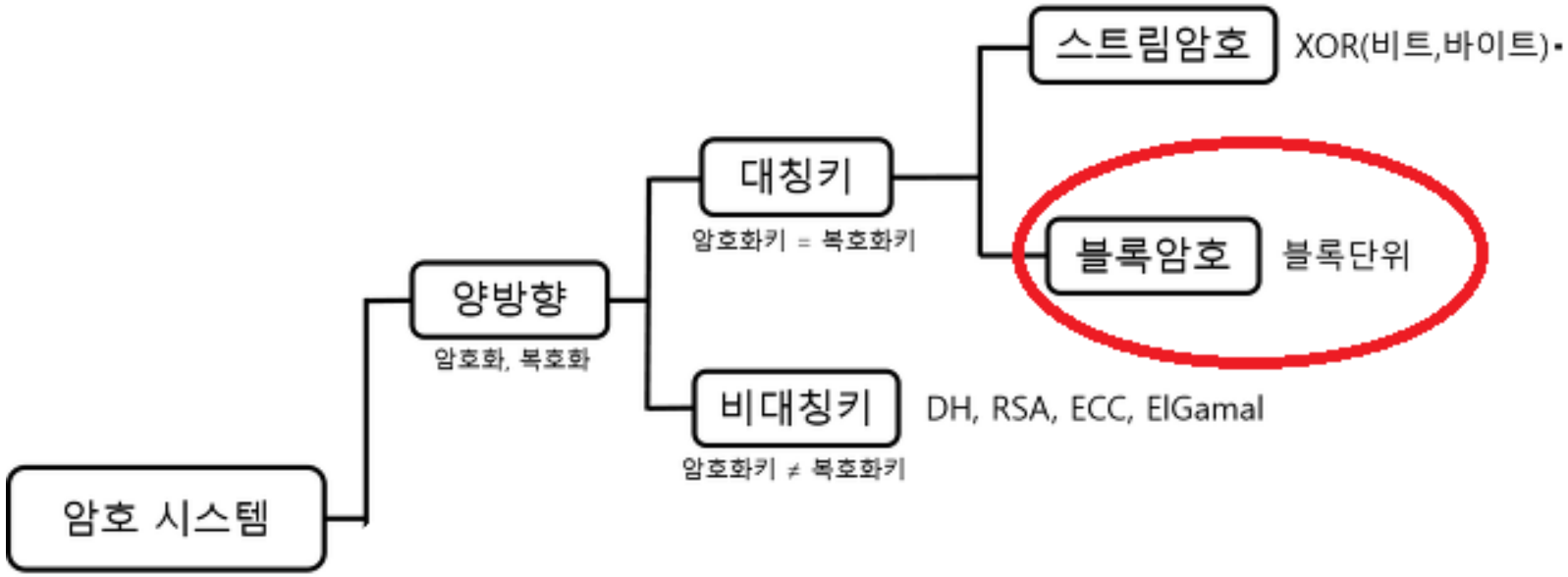
블록 암호

001/ 블록 암호, 블록 체인



001/ 블록 암호, 블록 체인

블록암호(block cipher) : 정보를 정해진 블록 단위로 암호화하는 대칭키 암호 시스템

블록(block) : 데이터를 저장하는 단위

헤더(header)

- 암호코드

ex) 머클해시(머클루트)나 넌스(nounce)

바디(body)

- 내용

크기에 따라 블록 하나에 들어가는 내역의 수도 달라진다.

001/ 블록 암호, 블록 체인

머클루트, 정보들이 변경 되었는지에 대한 유효성을 검사하는 역할을 수행하고 머클루트의 결과 값을 통해 블록 해시의 정보가 구성됨으로 그 블록의 유효성 또한 검사 가능

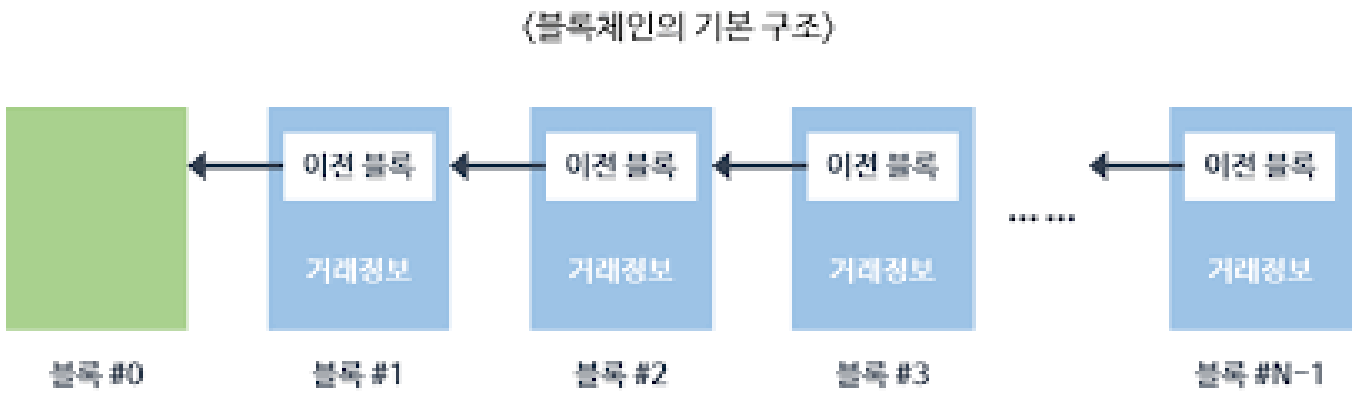
논스(Nonce) : 블록을 연결하기 위한 작업 증명

머클 루트 생성 과정

1. 최초 데이터를 SHA256 형태의 해시값으로 변환한다.
2. 가장 가까운 노드 두 개를 한 쌍으로 묶어 합친 후 해시값으로 변환한다.
3. 계속해서 해시값으로 변환하여 마지막 하나가 남을 때까지 이 과정을 반복한다.

001/ 블록 암호, 블록 체인

제네시스블록(genesis block) : 블록체인에서 생성된 첫 번째 블록



002/ 암호화, 패딩

패딩 : 블록 크기의 배수로 만드는 것

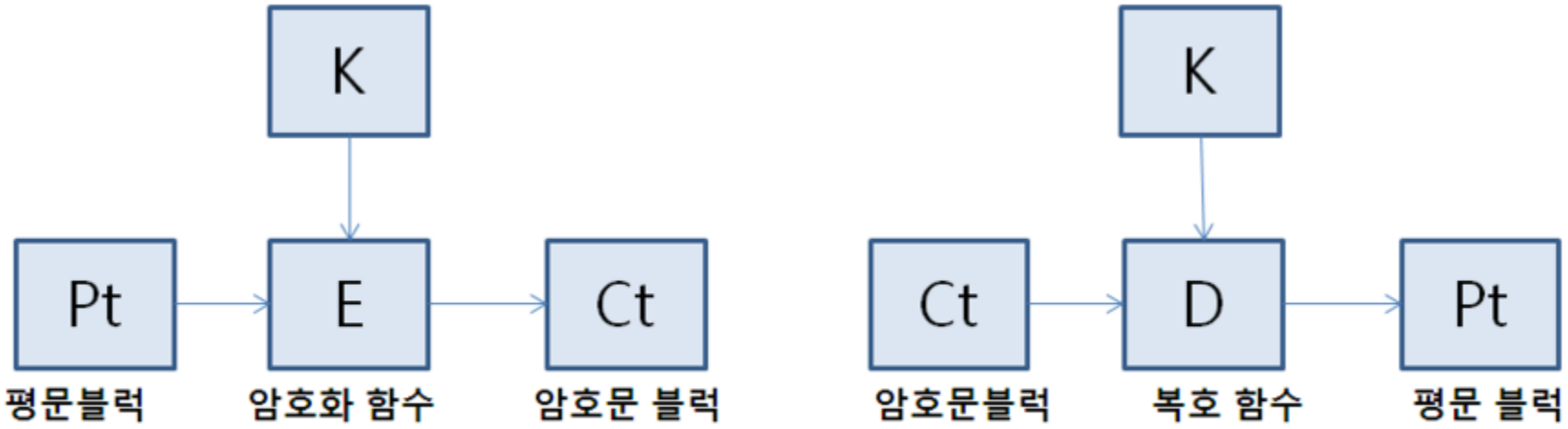
- PKCS 패딩
- Zero 패딩
- ISO10126 패딩
- X923 패딩
- …

데이터 암호화 표준(Data Encryption Standard; DES)

64비트 단위 블록으로 구성된 평문 메시지에 16라운드의 반복적인 황호화 과정을 실행

평문 : 64 * n비트

002/ 암호화



[그림] 대칭 블록암호 암복호화

Ct =E(Pt, K)
Pt=D(Ct, K)

003/ 장,단점

장점

블록 단위 암호화로 인해 기호를 삽입하거나 제거가 불가능하고 다양한 운영 방법에 의해 혼돈과 확산의 이론을 기반으로 설계될 수 있는 것이 장점이다.

단점

블록 단위로 암호화가 이루어지기 때문에 평문 비트들이 완전한 하나의 블록으로 구성한 다음에 암호화 되므로 암호화 과정이 블록의 크기에 따라 지연된다. 즉, 암호화 시간이 느리다.

THANK YOU