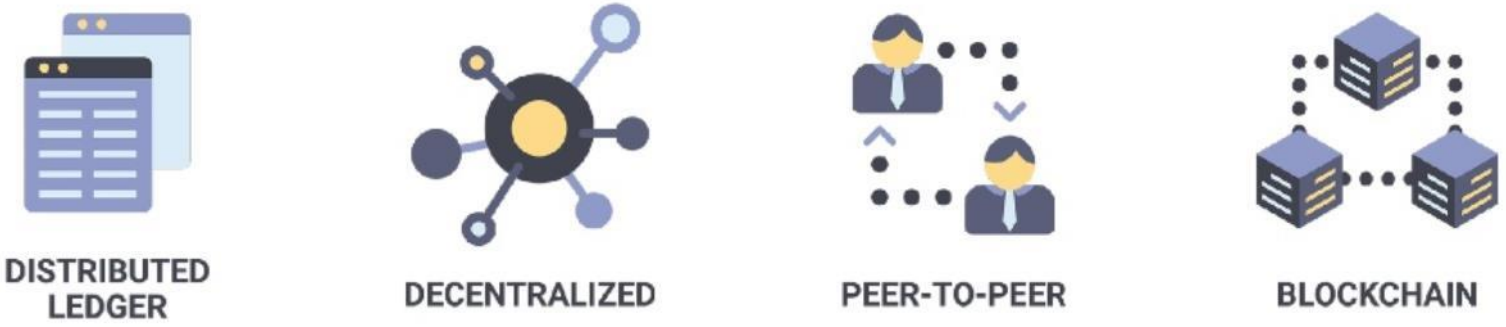
블록체인
비트코인

서강대학교
SOGANG UNIVERSITY

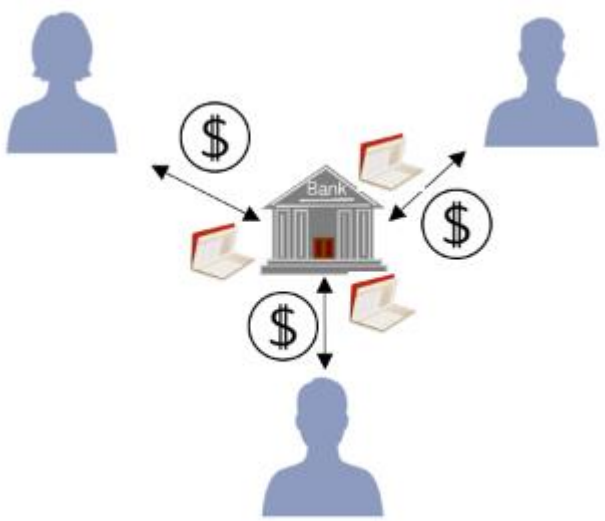
블록체인 개요

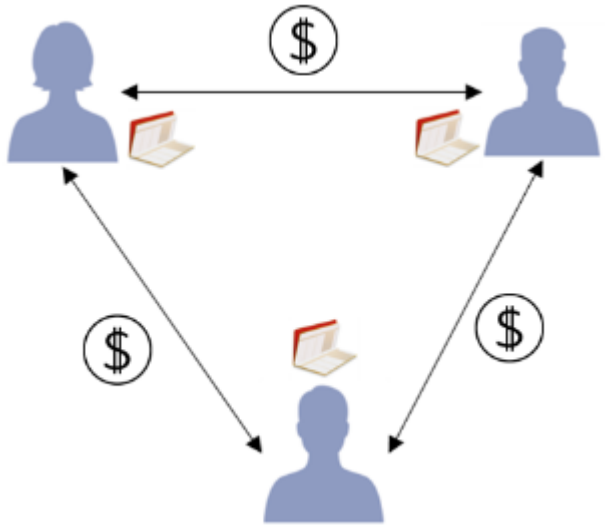
- 블록체인이란?
  - 관리 대상 데이터를 '블록'이라고 하는 자료 구조에 저장하여 체인의 형태를 이룬 것으로, 데이터를 분산 데이터 환경에 저장함으로써 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있도록 하는 분산컴퓨팅 기반의 원장 관리 기술
  - 분산 원장: 모든 거래 참여자가 거래 장부를 각각 소유하고 이를 분산하여 갖고 있는 것
  - 탈중앙화: 중앙 기관이나 중개자 없이 분산된 네트워크를 통해 거래 및 정보를 관리하는 것
  - P2P 방식: 중앙 집중화된 중간 매개자 없이 참가자 간에 직접적인 통신과 데이터 교환
  - 블록체인: 모든 거래를 블록에 담아 체인 형태로 저장



블록체인 개요

- 블록체인: 분산원장 기술

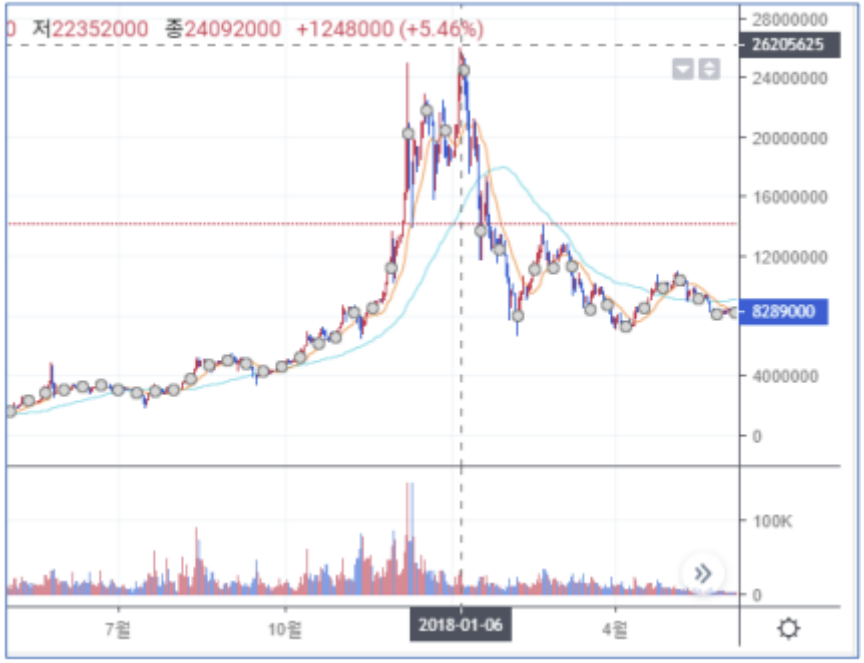




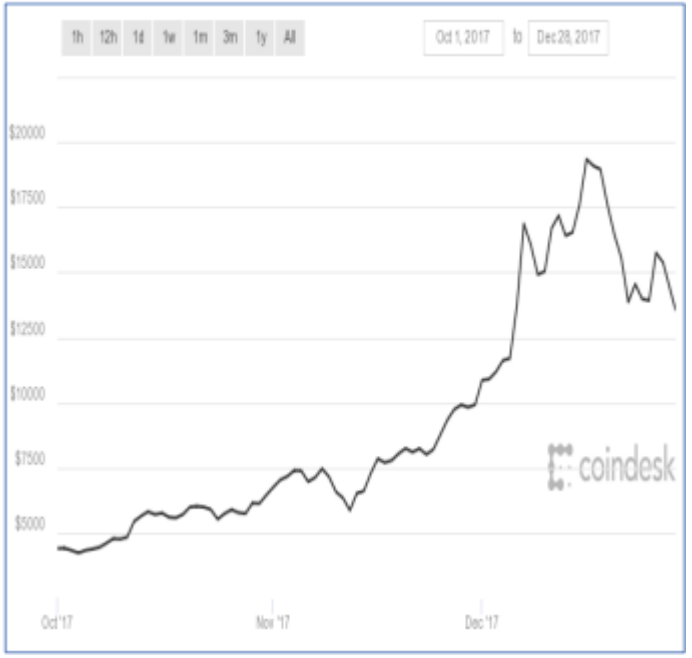
목 차

암호화폐의 출현

- 암호화폐의 출현
  - 2017년 말 암호화폐 열풍



비트코인 가격 (한국)



비트코인 가격 (미국)

* KMOOC POSTEC [블록체인 이론 및 응용]

암호화폐의 출현

- 암호화폐의 출현
  - 돈은 사람들이 재화와 서비스를 거래하는 데 사용하는 자산

물물교환

원자재 화폐

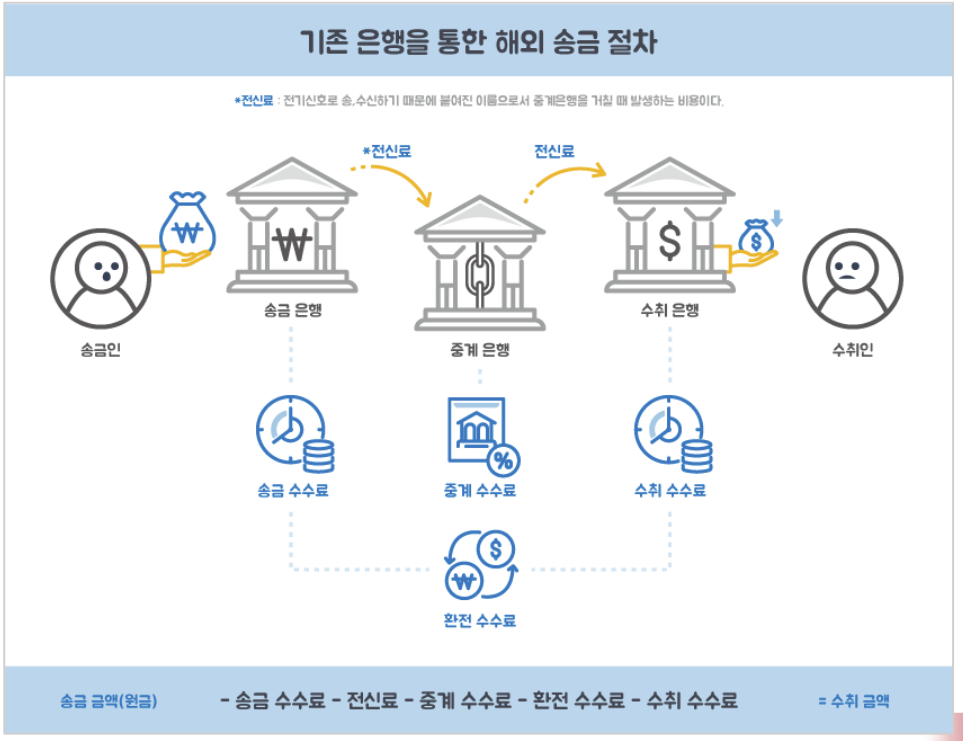
법정화폐

* KMOOC POSTEC [블록체인 이론 및 응용]

암호화폐의 출현

서강대학교 SOGANG UNIVERSITY

- 암호화폐의 출현
  - 기존 통화의 문제점
    - 생산 비용
    - 돈을 저장할 곳이 필요
    - 국가에 의해 통제: 환율 조작, 양적 완화 및 국가 이익을 위한 이자율 조정
    - 정부의 이익에 따라 조작될 위험
    - 국가마다 서로 다른 통화
    - 해외송금 문제(높은 수수료, 시간 지연 등)



암호화폐의 출현

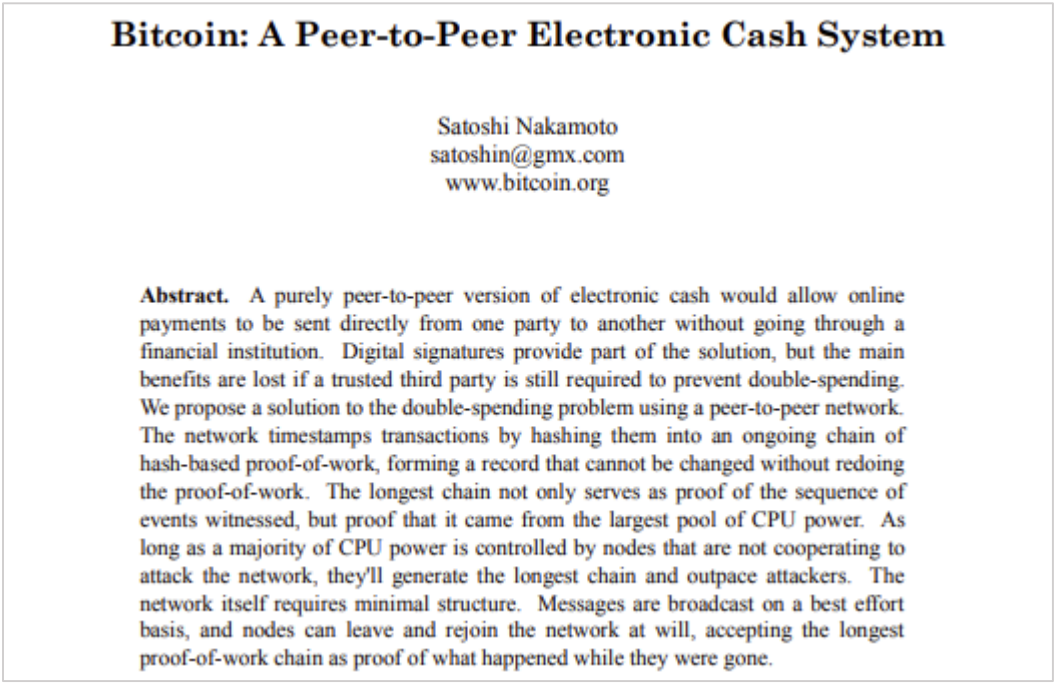
- 암호화폐의 출현
  - 암호화폐
    - 생산 비용이 거의 들지 않으며 전송 비용과 같은 거래 비용을 크게 줄일 수 있다
    - 컴퓨터의 하드디스크에 저장되므로 보관 비용이 거의 들지 않는다
    - 탈중앙화, 투명성, 국경 없는 거래
    - 문제점
      - 사기와 범죄 이용 가능성: 암호화폐의 익명성은 불법 거래, 자금 세탁, 탈세 등에 악용될 수 있는 여지
      - 가격 변동성
      - 법적 불확실성
      - 기술적 복잡성: 일반 사용자에게 암호화폐는 기술적으로 복잡할 수 있으며, 실수로 인해 자금을 잃을 위험성

암호화폐의 출현

서강대학교 SOGANG UNIVERSITY

- 암호화폐의 출현
  - 최초의 탈중앙화 암호화폐: 비트코인
    - 2008년 가을, 익명의 개발자 또는 개발 단체인 사토시 나카모토
    - 논문: Bitcoin: A Peer-to-Peer Electronic Cash System(https://bitcoin.org/bitcoin.pdf)
    - 중앙집중식 관리자가 없는 시스템
    - 총 코인 수 제한: 2100만 개
    - 모든 거래 내역 공개
    - 개인 정보가 필요하지 않다
    - 낮은 거래 수수료
    - 강력한 보안

    ➔ 블록체인 기술로 구현



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

블록체인 요소 기술

서강대학교 SOGANG UNIVERSITY

▪ 블록체인 특징

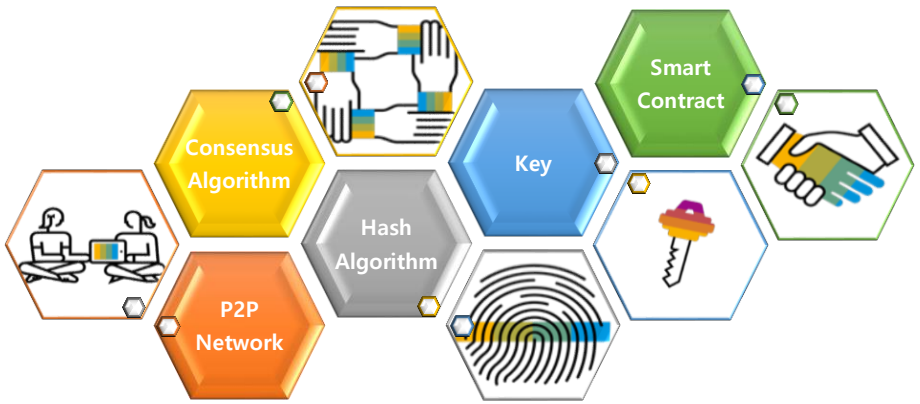
불변성

이전 데이터와 연결되어 새로운 데이터가 저장되는 형태이기 때문에 블록체인에 저장되는 데이터는 수정 및 삭제가 불가능

투명성 / 무결성

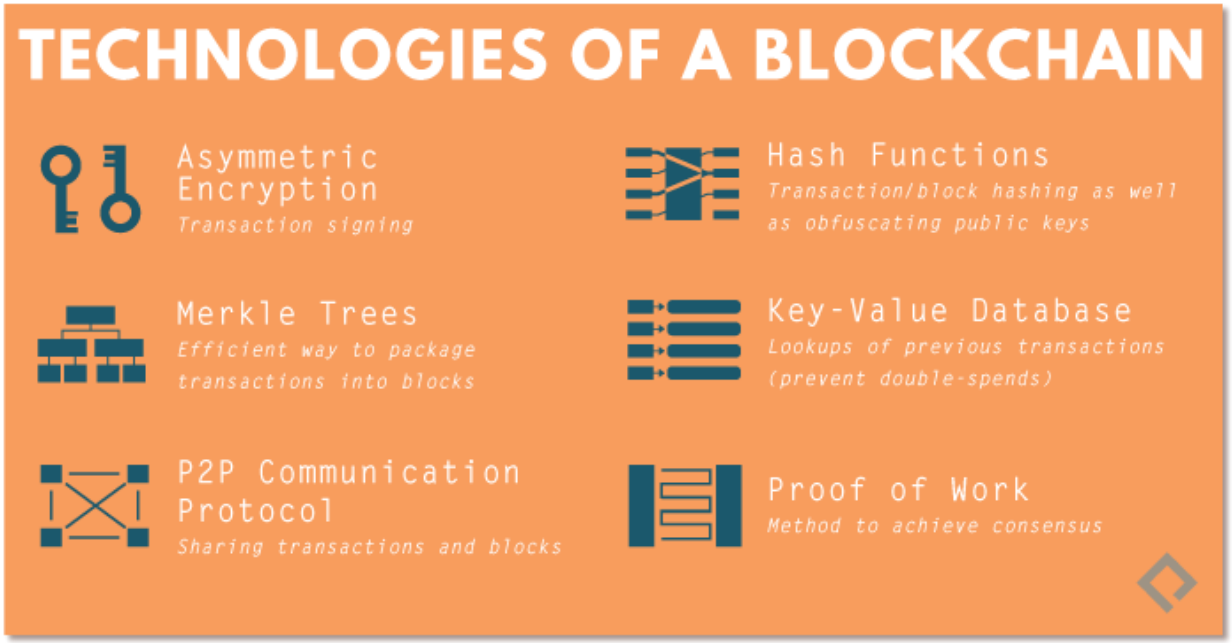
분산 네트워크를 통해서 모든 블록체인 사용자들은 동일한 데이터를 공유함

기술적 요소

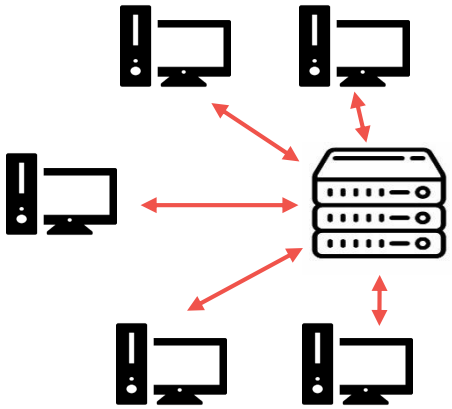


블록체인 요소 기술

- 블록체인 기반 기술
  - 암호기술
    - 해시함수
    - 비대칭키 암호화
    - 디지털서명
  - P2P Network
  - 합의 알고리즘
  - 머클트리
    - 트랜잭션의 효율적 패키징
  - Key-Value Database
    - 이전 트랜잭션 조회

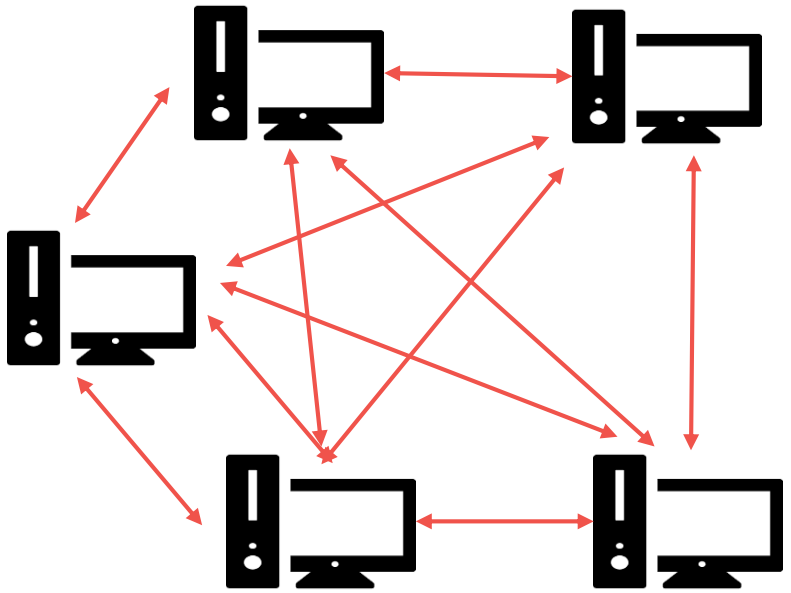


- 네트워크
  - 클라이언트 & 서버
    - 일반적으로 중앙집중 시스템의 대표적인 시스템 구현 방식
    - 클라이언트: 필요한 서비스와 데이터를 서버에 요청하고 제공받는 단말기
    - 서버: 데이터를 저장 관리하고 필요한 서비스와 데이터를 제공하는 시스템
    - 중앙집중 방식이라 관리가 효율적, 데이터 통일성
    - 단점: 서버에 과부하가 걸리면 네트워크 성능이 저하될 수 있으며, 서버 장애 시 네트워크 전체에 영향을 미침



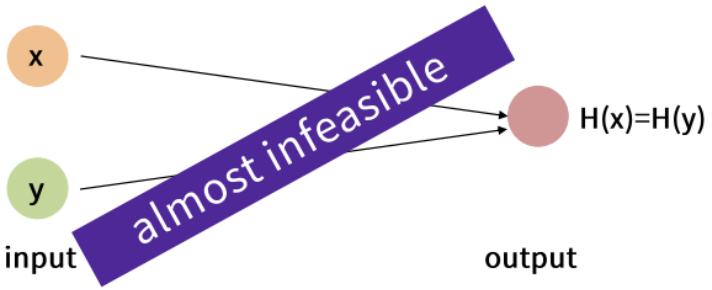
블록체인 요소 기술

- 네트워크
  - P2P(Peer to Peer Network)
    - 네트워크에 참여하는 각 노드(Node)가 중앙 서버 없이 직접 데이터를 주고 받는 방식
    - 각 노드는 서버 역할도 하면서 동시에 클라이언트 역할 수행
    - 모든 노드가 동등한 역할과 지위
    - 분산된 데이터에 대한 동기화 문제
    - 블록체인에서 사용되는 구조



블록체인 요소 기술

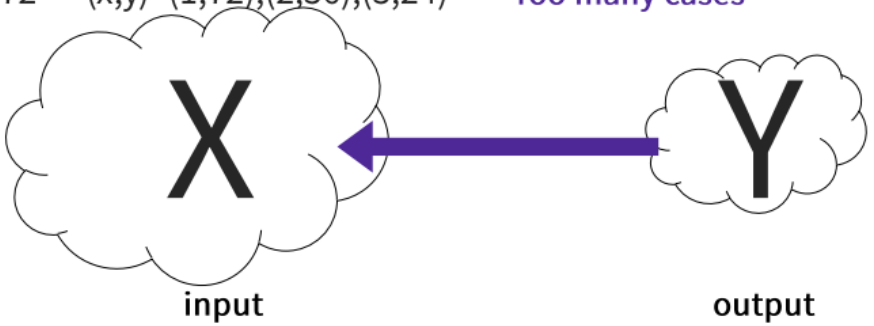
- 해시 함수: 입력 데이터를 고정된 크기의 해시값으로 변환하는 함수
  - 메시지 축약: 고정된 출력 크기
    - 임의의 길이를 갖는 데이터를 고정된 길이를 가진 해시 값으로 바꿔주는 함수
    - 용량이 큰 원본 데이터의 사이즈를 많이 줄일 수 있음
    - SHA-256 해시함수는 입력 데이터의 크기에 관계없이 256비트 길이의 해시값을 생성
  - 결정론적 특성
    - 같은 입력값에 대해서는 언제나 동일한 해시값 출력
    - 따라서, 해시값을 사용하여 데이터를 식별하거나 검증할 수 있음
  - 충돌 저항성(Collision Resistance)
    - 충돌: 서로 다른 두 입력값이 동일한 해시값을 생성
    - 좋은 해시함수는 충돌이 발생할 확률이 매우 낮아야 함



- 해시 함수: 입력 데이터를 고정된 크기의 해시값으로 변환하는 함수
  - 역상 저항성(Pre-image Resistance), 단방향성(One-way Property)
    - 주어진 해시값(Y값)으로부터 원래의 입력값(X값)을 역으로 추정하는 것이 매우 어려워야 함

Ex) multiplication
mul(8*9) =72
Find x,y =72 → (x,y)=(1,72),(2,36),(3,24)…

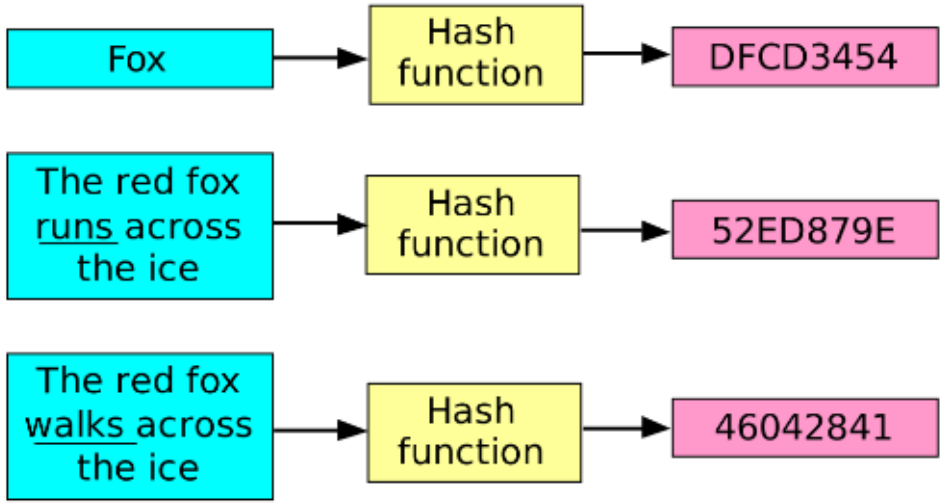
Easy to calculate
Too many cases



  - 제2 역상 저항성(Second Pre-image Resistance)
    - 주어진 입력값과 동일한 해시값을 갖는 또 다른 입력값을 찾는 것이 매우 어려워야 함

블록체인 요소 기술

- 해시 함수: 입력 데이터를 고정된 크기의 해시값으로 변환하는 함수
  - 빠른 계산 속도
    - 해시함수가 실시간 검증 또는 데이터 무결성 확인과 같은 작업에서 자주 사용되기 때문
  - 균등 분포: 가능한 모든 해시값이 균등하게 분포되도록 설계되어야 함
  - 미세한 변화에 대한 민감성
    - 입력값에 아주 작은 변화가 생기더라도, 출력되는 해시값은 완전히 달라야 함



블록체인 요소 기술

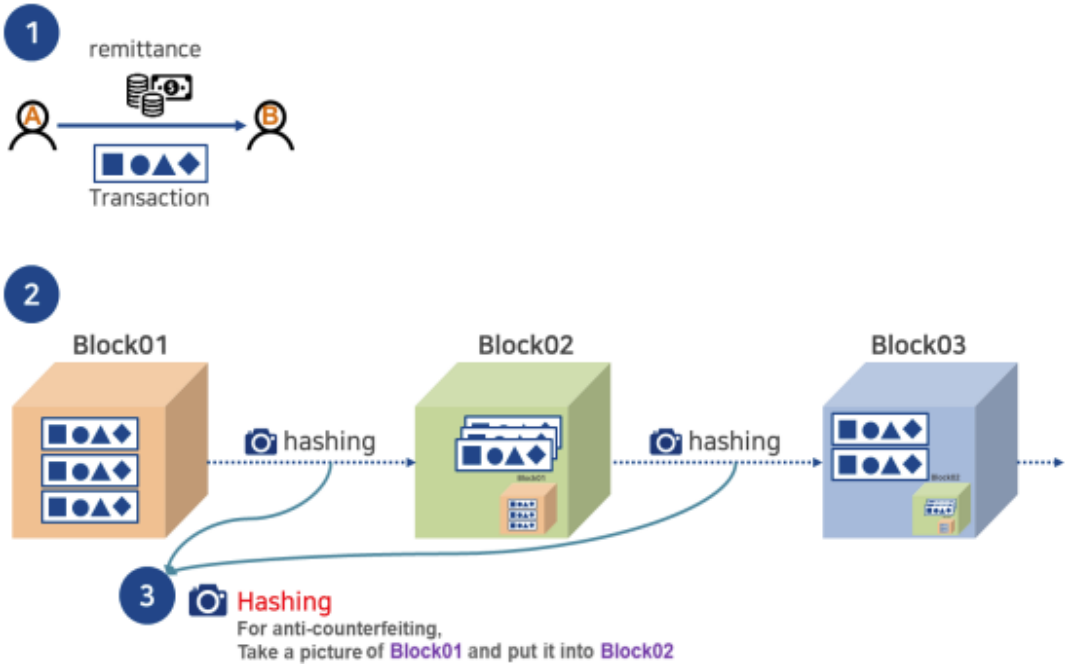
- 해시 함수
  - 해시함수의 안전성은 충돌 저항성 (Collision Resistance)와 역상 저항성 (Preimage Resistance)에 있음
    - 충돌 저항성: 생성된 해시 값이 겹치지 않을 확률
    - 역상 저항성: 어떤 무작위 해시 값이 주어졌을 때 그 해시 값의 입력을 찾아낼 수 없는 것

  ➔

  - 자료를 해시화해서 저장 또는 전송함으로써, 그 자료를 다른 누군가가 알아내지 못하게 하는 것이 목적 (기밀성 보호)
  - 해시함수는 중간에 누군가 자료를 수정했다면 해시값이 달라지므로 그 사실을 알 수 있게 함으로써 자료의 무결성을 지키는 것이 목적
  - SHA-256(비트코인), Keccak256(이더리움)과 같이 다양한 해시 함수가 존재함

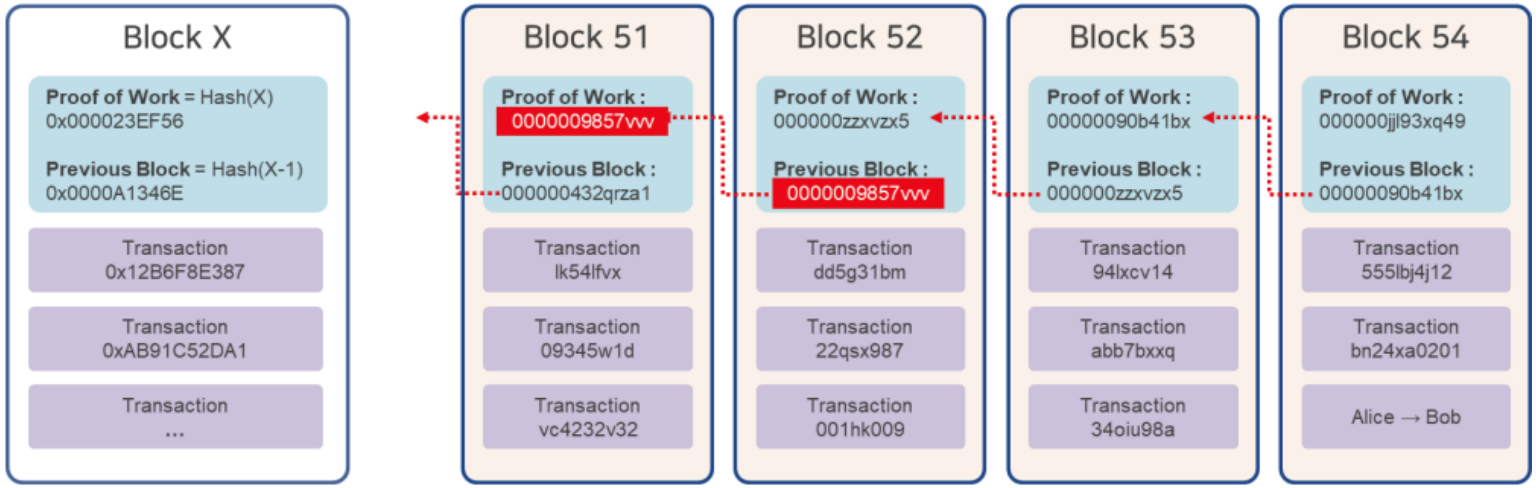
블록체인 요소 기술

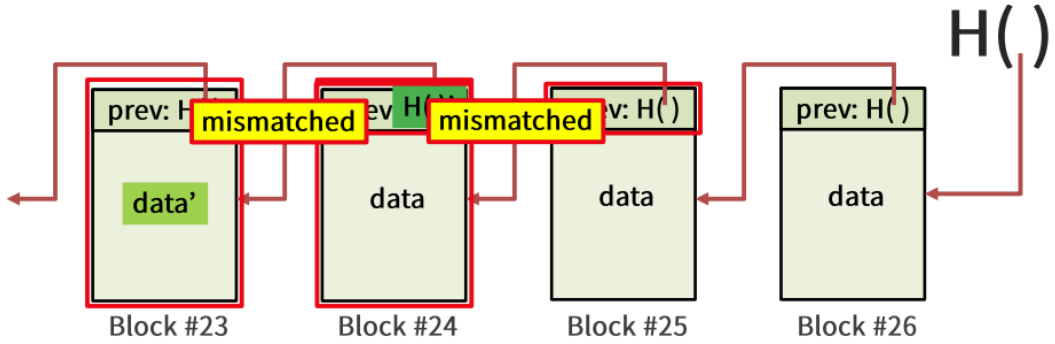
- 해시 함수의 활용
  - 해시값
    - 정보가 저장된 곳을 가리키는 일종의 포인터로 사용
    - 해시가 가리키고 있는 데이터가 변경되었는지 검증하는 데 사용
  - 블록 생성시 해시함수를 이용해 블록 연결



블록체인 요소 기술

- 해시 함수의 활용
  - 블록체인에서 해시 함수는 데이터의 무결성을 검증하는데 사용



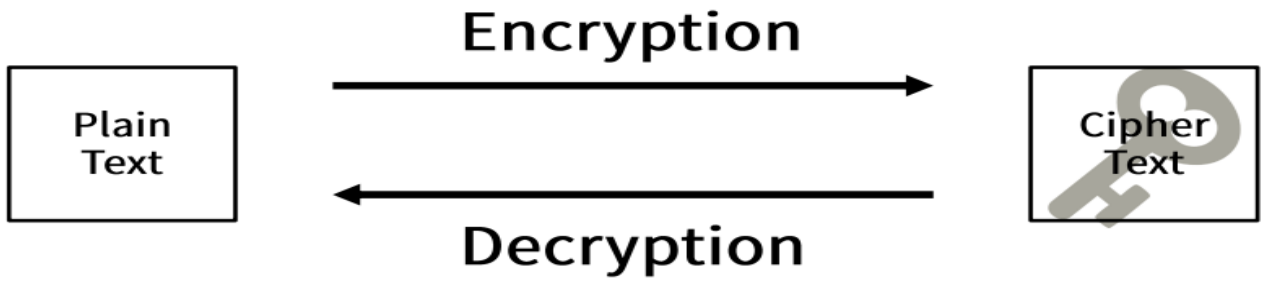


블록체인 요소 기술

서강대학교 SOGANG UNIVERSITY

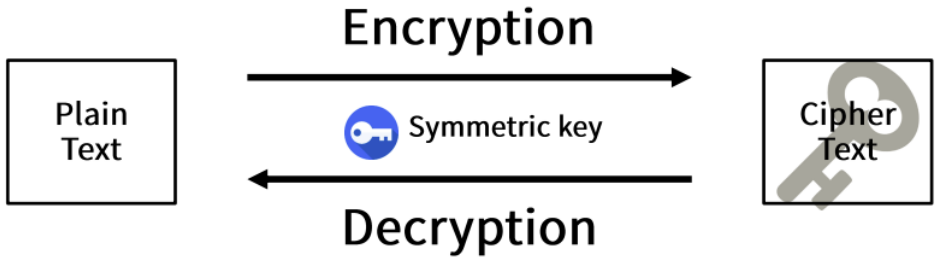
- 해시 함수의 활용
  - 거래 내역의 간략화
    - 아무리 긴 거래 내용이라도 256비트로 만들 수 있다
  - 거래의 시간적 순서화
    - 다음 거래에서 지금 단계 거래 내용의 해시값이 다시 입력값이 되므로 과거 거래 내용의 진실성을 이 해시값으로 보장

- 암호화
  - 암호화 (Encryption)
    - 어떠한 자료를 이해할 수 없는 형태로 만들어서 자료의 기밀성(Confidentiality)을 보장
    - 암호화에 쓰이는 비밀 값을 “키“ 라고 표현함
  - 원래의 데이터를 이해할 수 없는 형태로 변환하고, 복호화를 통해 다시 원래의 형태로 되돌리는 과정을 포함
    - 하나의 메시지를 암호화할 때 암호화되지 않은 메시지를 “평문(plain text)” 라고 표현
    - 암호화된 메시지를 “암호문(cipher text)” 라고 표현

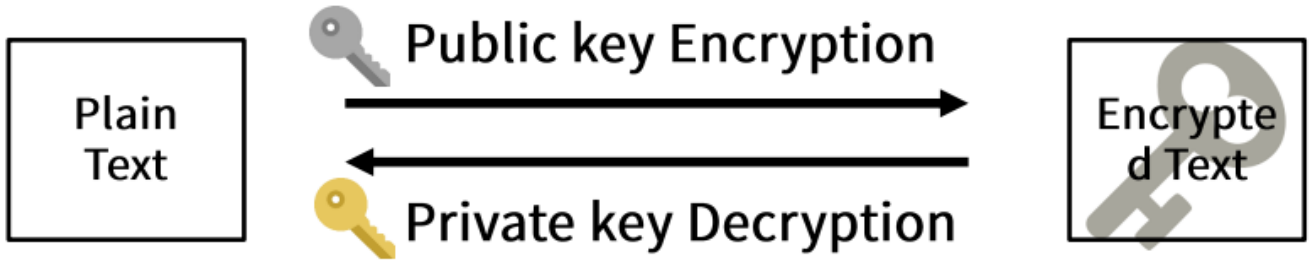


블록체인 요소 기술

- 암호화 키와 복호화 키가 일치하는지 여부에 따라 대칭형 키 암호화 기법과 비대칭형 암호화 기법으로 분류
  - 대칭키(Symmetric key)
    - 하나의 키로 암호화/복호화를 진행
    - 속도가 빠름
    - 3DES, AES가 대표적
  - 비 대칭키(Asymmetric key)
    - 개인키와 공개키가 존재
    - RSA가 대표적인 알고리즘
    - 공개키 암호화
    - 디지털 서명(전자서명)



- 비대칭키 알고리즘
  - 공개키 암호화
    - 개인 키를 가진 사용자만 공개키로 암호화된 데이터를 확인할 수 있기 때문에 문서를 특정 사용자를 위해 암호화하는 데 사용

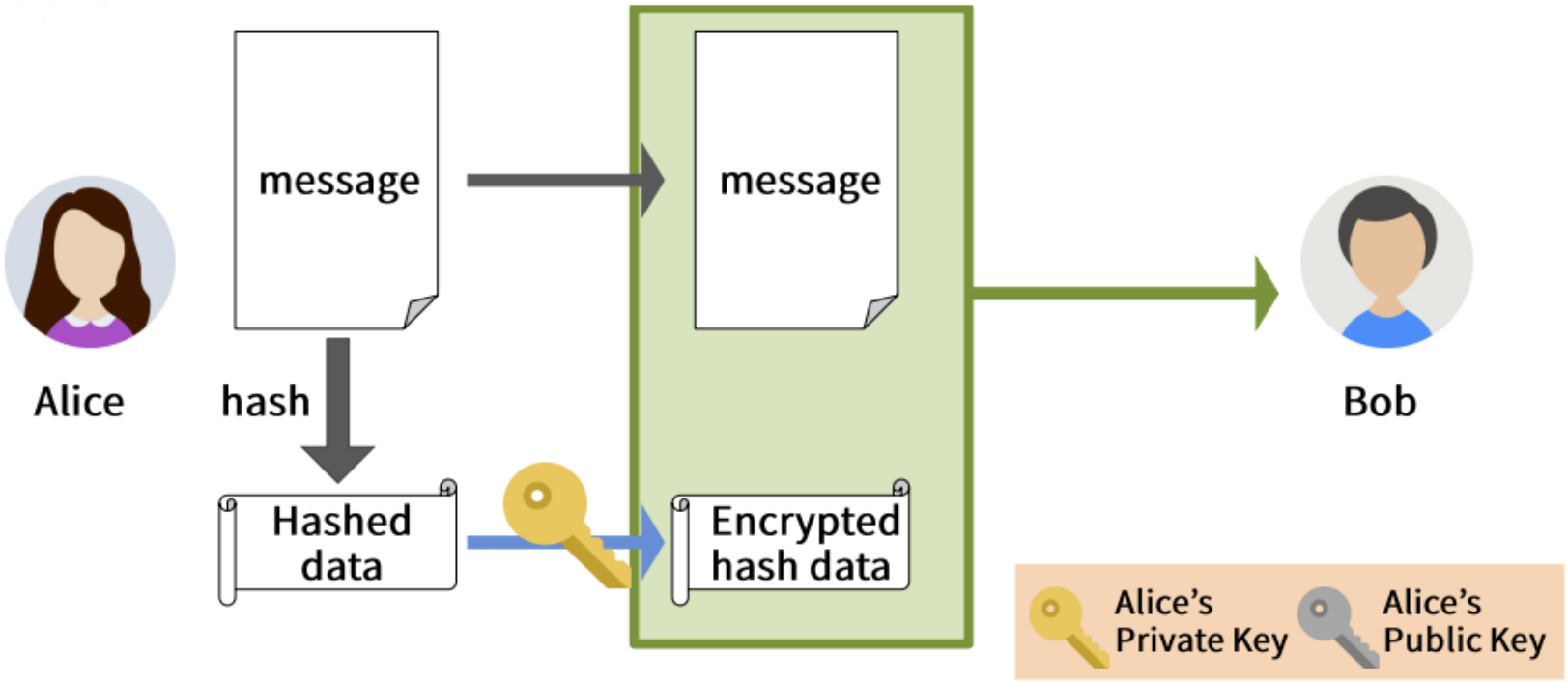


블록체인 요소 기술

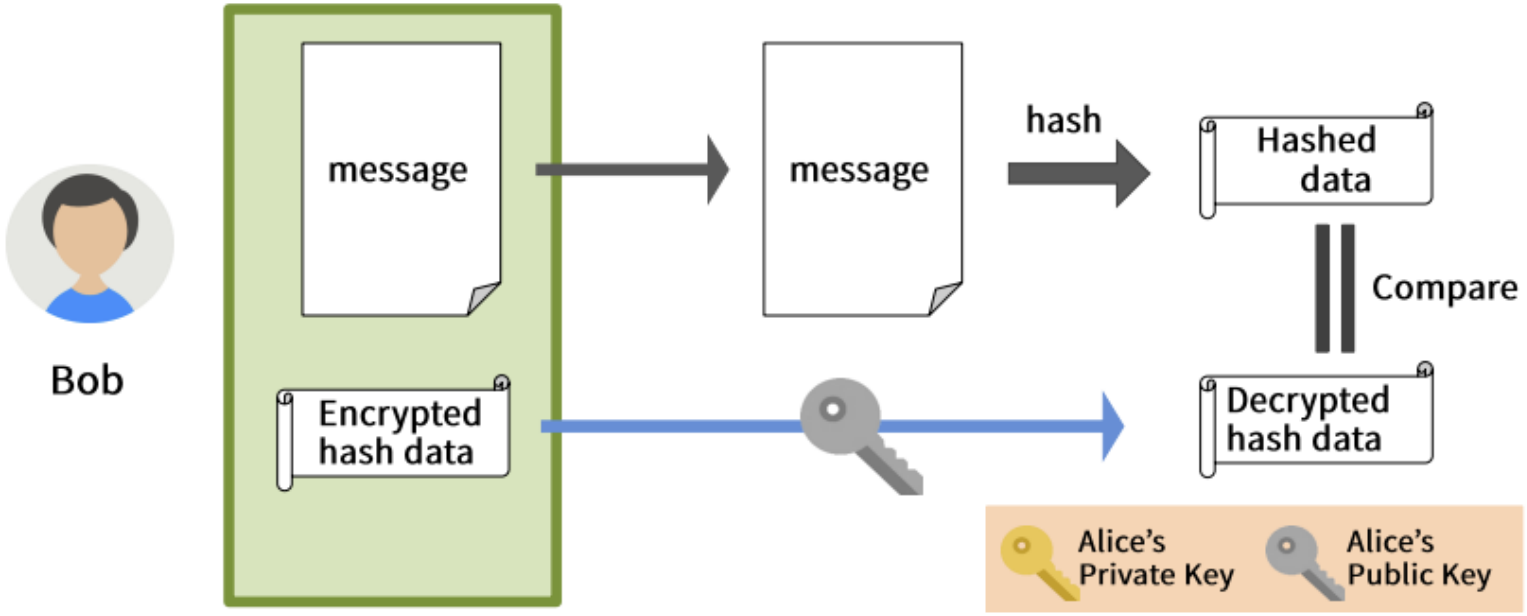
- 비대칭키 알고리즘
  - 디지털 서명 (Digital Signature)
    - 특정 사용자가 문서를 보냈다는 것을 증명, 또는 검증하기 위한 시스템
      - 송신자가 개인키로 서명하고, 수신자가 공개키로 서명을 검증
    - 전자서명을 위해 개인 키로 암호화된 문서를 제공하고 공개키로 이 문서를 복호화해서 풀리면, 전달받은 데이터가 해당 사용자가 보낸 문서임을 증명할 수 있음
    - 내가 온라인상에서 어떤 메시지를 타인에게 보내는데 그 타인의 입장에서 자기가 받은 메시지가 내가 보낸 메시지라고 확신을 갖도록 그 메시지에 내가 어떤 조작을 하는 것(문서에 사인)

블록체인 요소 기술

- 블록체인의 전자서명
  - 서명(Signing)
    - 원본 데이터가 아닌, 메시지를 해시한 해시 값을 서명자의 개인 키를 이용해서 서명
    - 해시값 이용: 메시지 축약으로 시간 절약, 메시지 무결성 보장



- 블록체인의 전자서명
  - 검증(Verification)
    - 서명 부분을 떼내어 앨리스의 공개키(Public key)로 복호화(Decryption)
    - 원본 데이터를 앨리스가 사용한 것과 동일한 해시 함수를 이용하여 해싱
    - 원본 데이터의 해시값과 앨리스의 서명을 앨리스의 공개키를 이용해 복호화한 값이 일치하는지 확인: 메시지가 변조되지 않았으며 송신자의 서명이 유효함을 확인할 수 있음

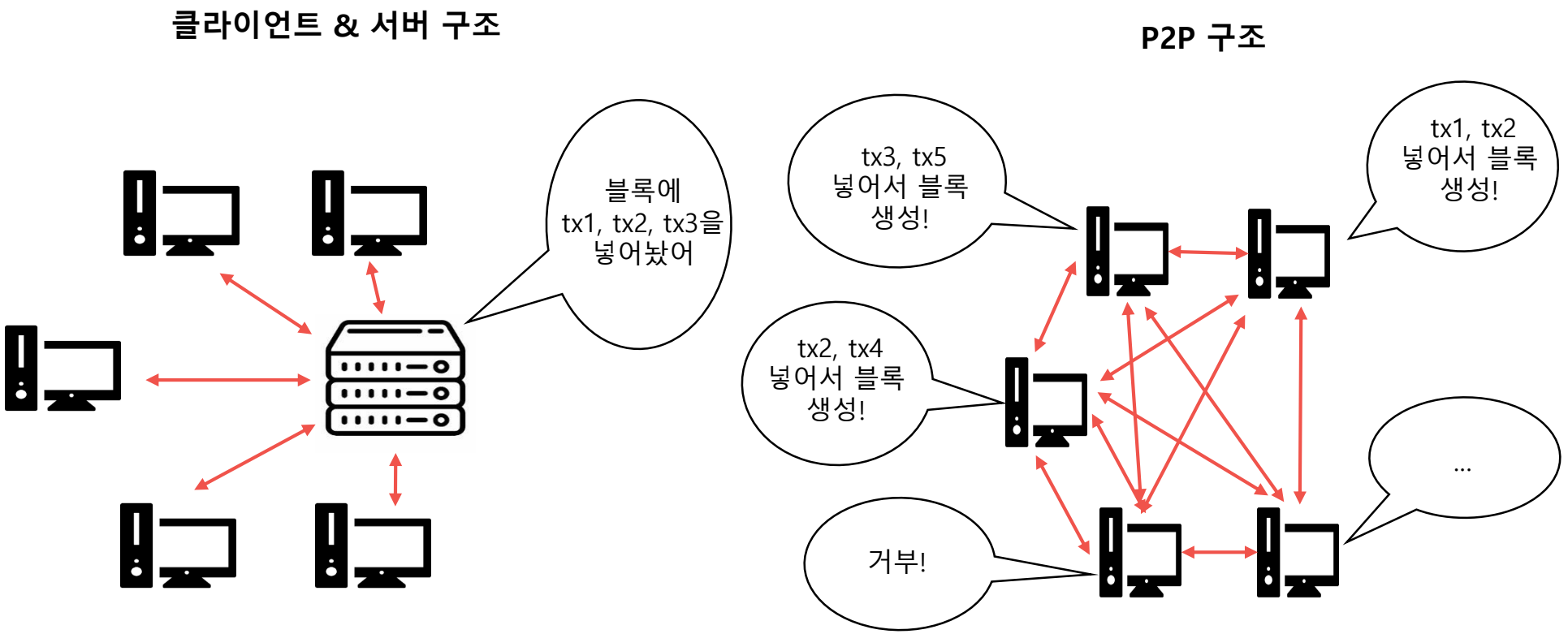


블록체인 요소 기술

서강대학교 SOGANG UNIVERSITY

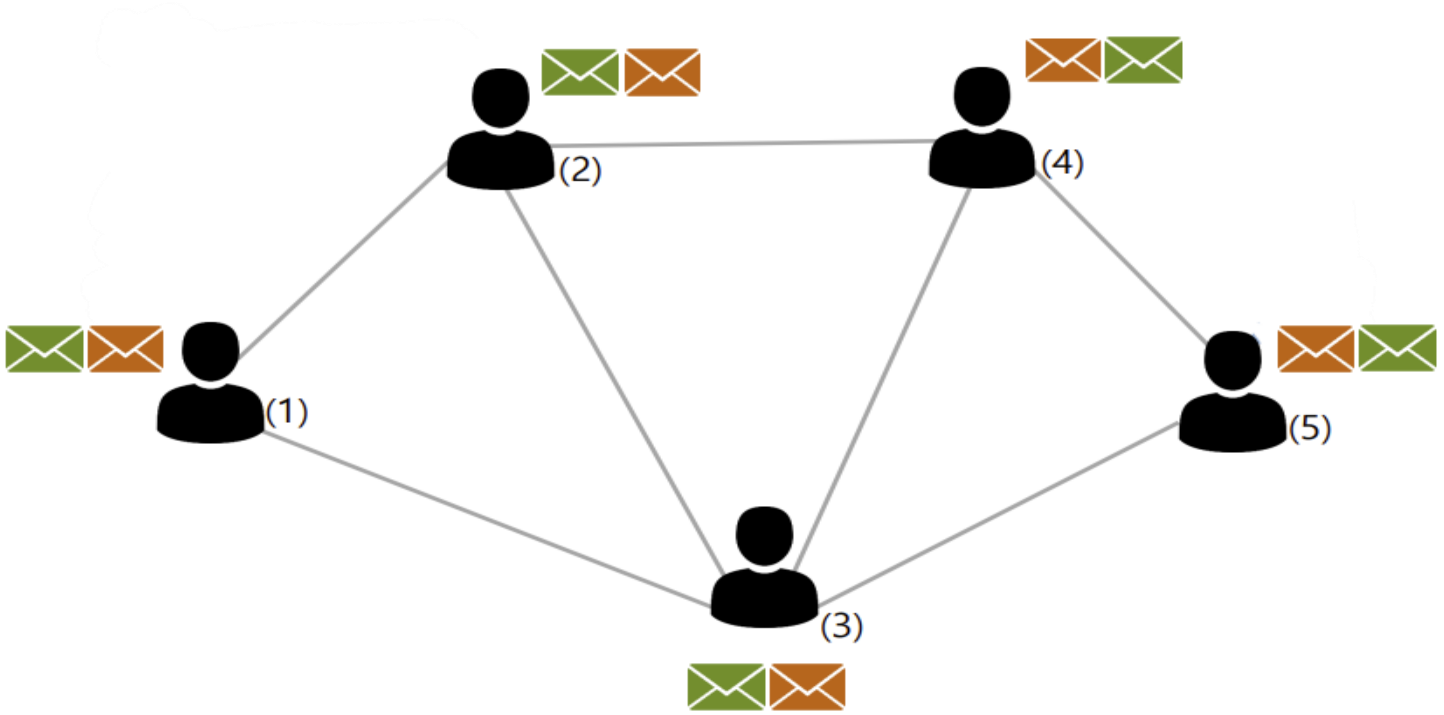
- 비트코인의 비대칭키 활용한 전자서명 방식
  - 보내는 내용
    - 원문
    - 원문의 해시값을 개인키로 암호화
    - 공개키
  - 검증 방법
    - 암호화된 해시값을 공개키로 복원
    - 원문을 해시
    - 위 두 값이 같은지 확인

- 분산 합의(Distributed Consensus) 필요성



블록체인 요소 기술

- 분산 합의 필요성
  - (1)번과 (5)번 참여자가 동시에 메시지를 생성
  - 네트워크 연결 상황에 따라 다른 결과가 있을 수 있음



블록체인 요소 기술

서강대학교 SOGANG UNIVERSITY

- 분산 합의(Distributed Consensus)
  - 신뢰할 수 없는 통신 네트워크에 의해서 연결된 프로세스들 간의 합의 즉 다수의 노드들이 참여해 있는 P2P 네트워크에서 합의
  - 분산 합의 알고리즘: 분산 시스템에서 모두가 동일한 상태를 가지고 있을 수 있도록 하는 것
  - 블록체인에서는 참여자 중 누구에게 다음 블록을 생성할 권한을 주느냐를 결정하는 것

블록체인 요소 기술

서강대학교 SOGANG UNIVERSITY

- 분산 합의(Distributed Consensus)의 잠재적인 문제
  - 일부 노드 가 고장 나거나 잘못 동작할 수 있음
  - 일부 노드가 의도적으로 악의적일 수 있음
  - 네트워크가 P2P 시스템으로 모든 노드가 서로 연결되어 있지 않다면 불완전
  - 모든 노드 쌍이 서로 연결되어 있는 것은 아니고, 인터넷 연결 상태가 좋지 않아서 네트워크에 결함이 있을 수 있음
  - 인터넷을 통한 연결로 인한 지연 문제

블록체인 요소 기술

서강대학교 SOGANG UNIVERSITY

- 합의 알고리즘 종류
  - 작업증명(PoW: Proof of Work)
    - 해당 작업에 참여했음을 증명하는 방식의 알고리즘

    - 네트워크 참여자들이 복잡한 수학 문제를 푸는 작업을 수행하며, 이 작업의 결과로 얻어진 값이 블록의 유효성을 증명
    - 작업은 일반적으로 컴퓨터의 연산력을 사용하며, 누가 먼저 문제를 푸는지에 따라 새로운 블록을 생성하고 블록체인에 추가할 권한이 부여됨
    - 참여자는 많은 양의 연산 작업을 수행해야 하므로 시간과 에너지를 소비하게 됨 -> 네트워크는 악의적인 공격자가 너무 쉽게 블록을 생성하거나 조작하는 것을 어렵게 함
    - 블록 생성 과정에서 많은 컴퓨팅 파워가 소비되고 높은 에너지를 사용하게 되는 단점
    - 컴퓨팅 파워가 큰 마이너의 영향력이 커진다는 문제

* KMOOC POSTEC [블록체인 입문]

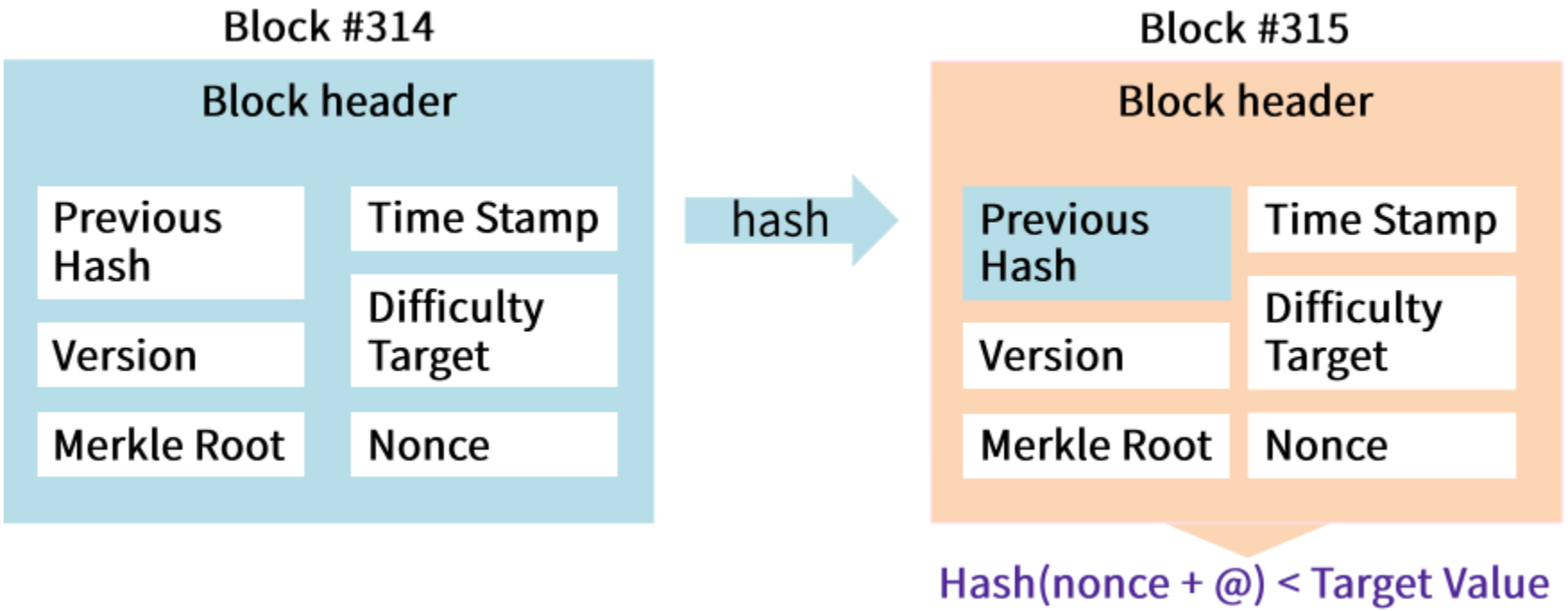
블록체인 요소 기술

- 합의 알고리즘 종류
  - 지분증명(PoS: Proof of Stake)
    - 암호화폐를 보유하고 있는 지분율에 비례하여 의사결정 권한을 주는 방식
    - 보증금(스테이킹)을 예치함으로써 사용자는 네트워크의 안정성과 보안을 유지하면서 새로운 블록을 생성하거나 기존 블록을 검증
    - 환경 친화적
  - 위임증명(DPoS: Delegated Proof of Stake)
    - 암호화폐 소유자들이 각자의 지분율에 비례하여 투표권을 행사하여 자신의 대표자를 선정하고, 이 대표자들끼리 합의하여 의사결정을 내리는 방식
    - 네트워크 상의 검증자 수를 제한하여 높은 수준의 확장성을 제공하는 PoS의 변형

* KMOOC POSTEC [블록체인 입문]

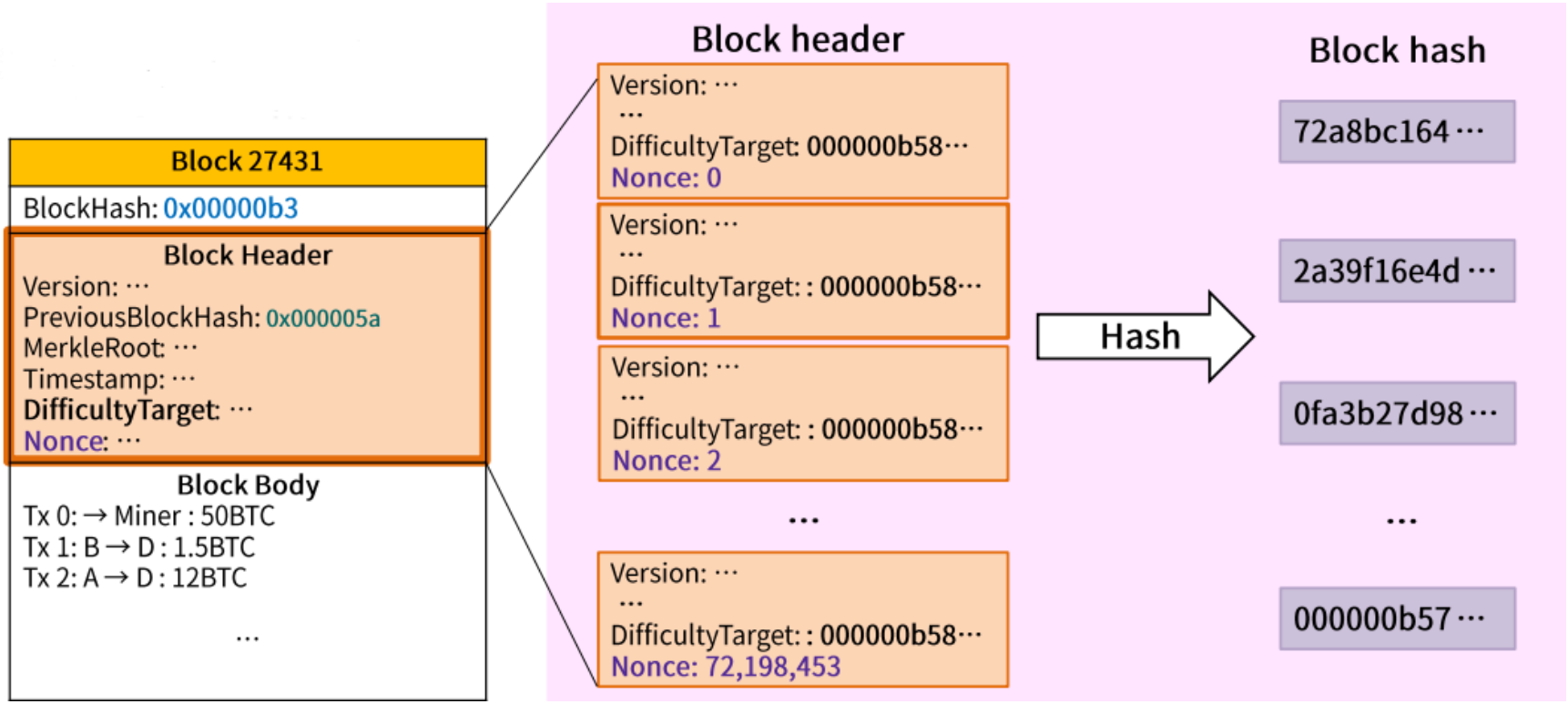
블록체인 요소 기술

- 작업증명(PoW: Proof of Work)
  - 블록 헤더의 해시값이 특정 숫자보다 작아지게 하는 값(nonce) 구하기
    - 블록 헤더의 나머지 값은 고정값이므로 nonce를 변경하며 해시값 계산



블록체인 요소 기술

- 작업증명(PoW: Proof of Work)
  - 예) 블록난이도(000000b58…)보다 작게 하는 nonce 구하기

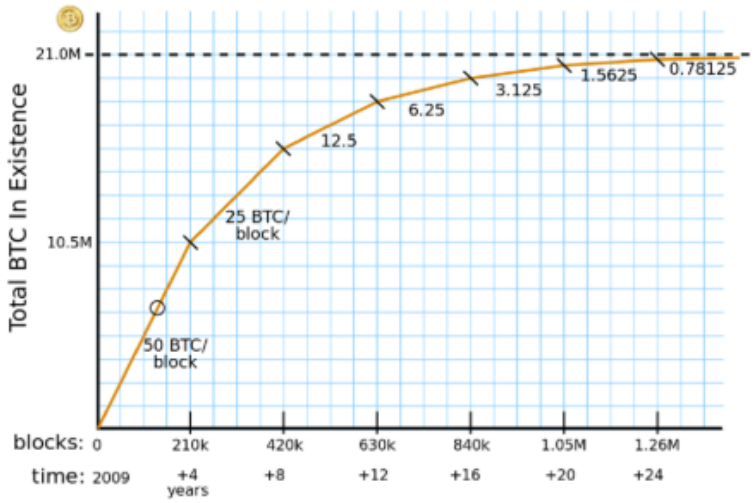


블록체인 요소 기술

- 채굴(Mining)
  - 블록체인에 추가할 새로운 블록을 생성
  - 비트코인이라는 암호화폐를 발행
  - 새로운 블록을 생성하기 위해서 채굴자들은 네트워크에 컴퓨팅 파워를 제공하고, 그에 대한 보상으로 비트코인을 지급받는 것
  - 비트코인을 채굴하는 과정은 일종의 퍼즐 풀기
    - 시간과 컴퓨팅 파워를 소모해서 퍼즐을 풀 수 있는 값(nonce)을 찾기
    - 퍼즐의 난이도: 퍼즐을 완성하는 시간이 10분 정도 소요되도록 주기적으로 조절
    - 해답을 찾는 과정을 작업증명 (Proof of Work)이라 하고, 이것은 채굴자가 새 블록을 생성하기 위해 어려운 계산을 하려고 했다는 사실을 증명하는 역할

블록체인 요소 기술

- 채굴에 의한 보상
  - 새로운 블록 생성시 새로운 코인을 발행해서 얻는 보상
    - 총 비트코인 총발행량은 21,000,000 BTC로 제한
    - 평균적으로 약 4년의 주기(210,000 블록)를 가지고 통화 발행량이 감소
    - Coinbase transaction(Generation Tx)



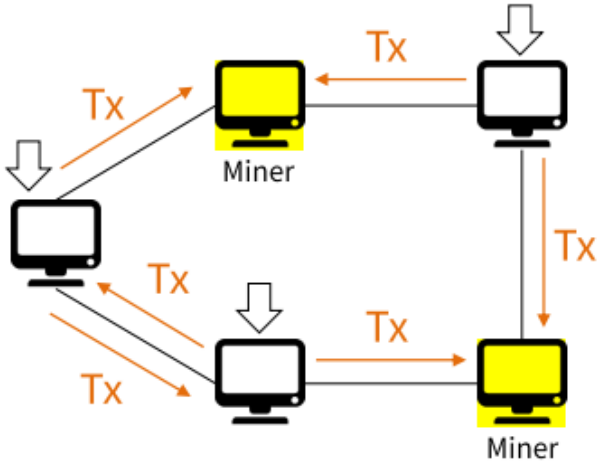
  - 이체 수수료
    - 해당 블록 내에 들어있는 거래들에 대한 수수료
    - 송신자가 보낸 비트코인의 총량에서 수신자가 받은 비트코인의 총량의 차이

블록체인 요소 기술

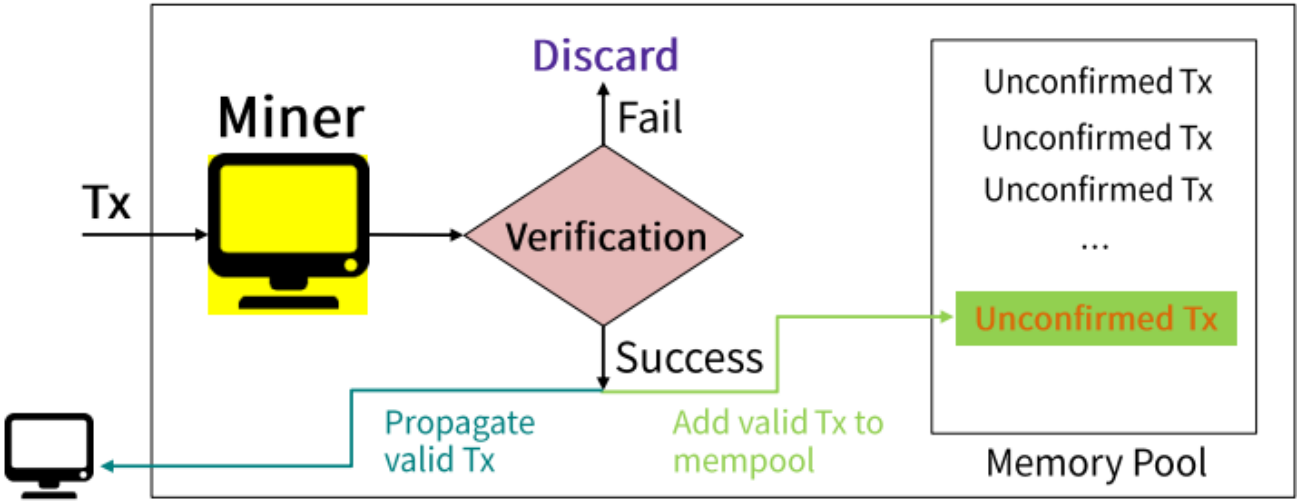
- 채굴(Mining) 방식의 변화
  - CPU 채굴: 비트코인이 처음 등장했을 때는 개인 컴퓨터의 중앙 처리 장치(CPU)를 사용
    - 비트코인 네트워크의 난이도가 점차 상승하면서 효율성이 낮아짐
  - GPU 채굴: 그래픽 처리 장치(GPU)를 이용한 채굴, GPU는 병렬 처리 능력이 뛰어나기 때문에 CPU에 비해 더 빠른 채굴이 가능
  - ASIC 채굴: ASIC(Application-Specific Integrated Circuit, 응용 특수집적 회로) 칩 이용
    - ASIC은 특정 알고리즘에 특화된 칩으로, 일반적인 컴퓨터보다 훨씬 효율적인 채굴 가능
    - 이에 따라 채굴 난이도가 크게 상승
  - 채굴 풀(Mining pool)
    - 개인 채굴자들이 다른 사람들과 함께 마이닝 하여 채굴 확률을 높이도록 한 것
    - 개개인의 컴퓨팅 파워를 모아 채굴 확률을 높이고, 투자된 지분만큼 수익을 배분
  - 에너지 효율적이거나 친환경적인 채굴 방법에 대한 연구와 노력이 진행중

블록체인 요소 기술

- 채굴 프로세스
  - 거래 생성과 브로드캐스팅

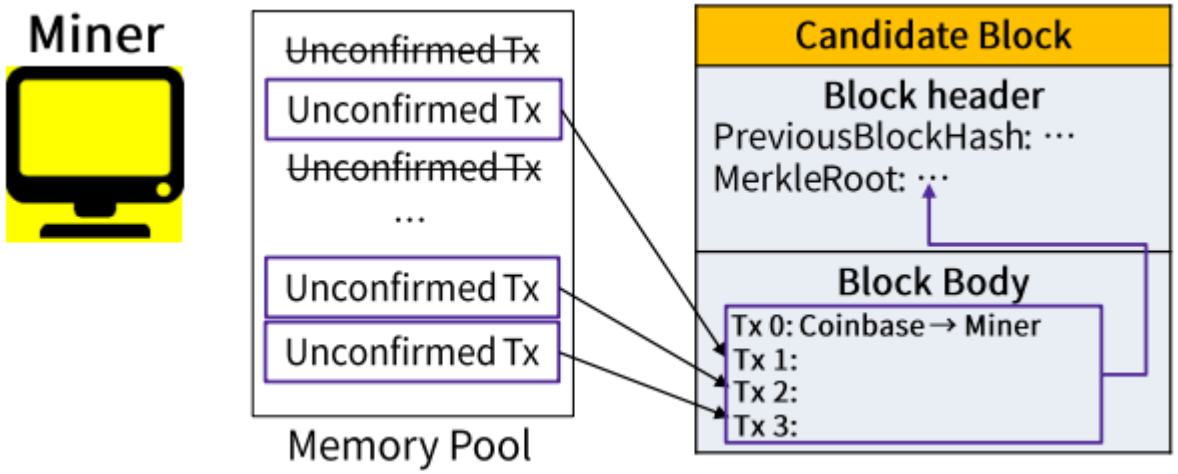


  - 트랜잭션이 유효한지 검증
    - 유효한 트랜잭션으로 판단되면, 이 트랜잭션을 memory pool(transaction pool)에 추가하고 이 트랜잭션을 자신과 연결된 peer 노드들에게 전파
    - 만약 트랜잭션이 유효하지 않다고 판단되면, 이 트랜잭션을 버려서 무시



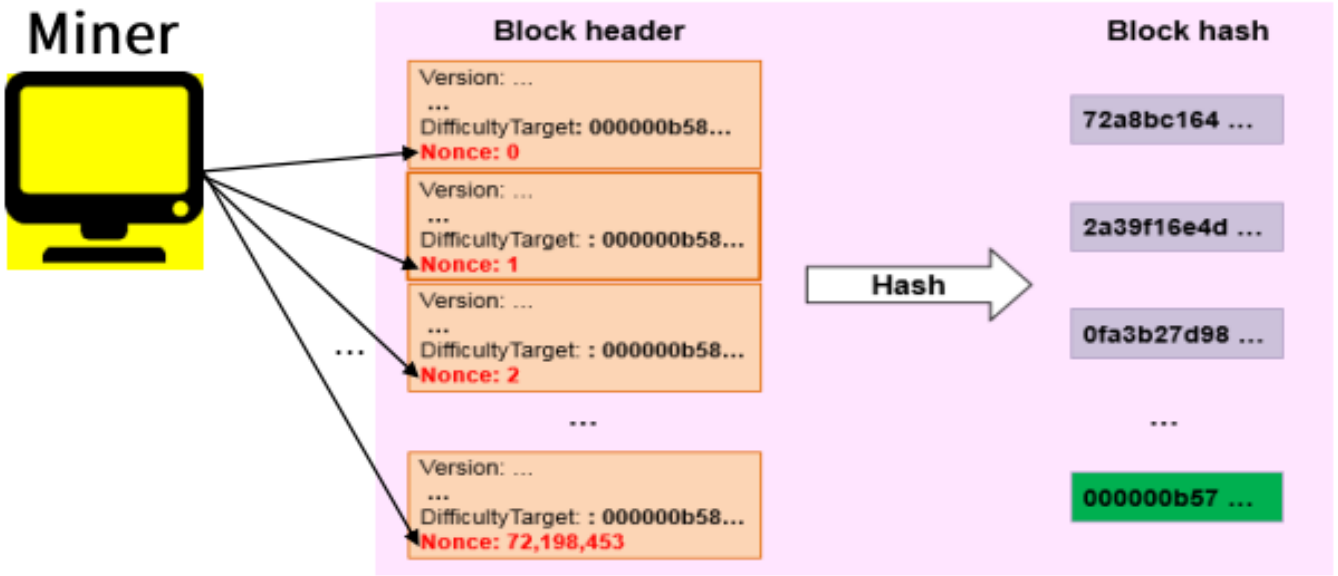
블록체인 요소 기술

- 채굴 프로세스
  - PoW: 새로운 블록 생성을 준비
    - 이전 블록에 포함된 트랜잭션을 메모리풀에서 제거
    - 후보 블록 생성: 메모리풀에서 우선 순위가 높은 트랜잭션 선택



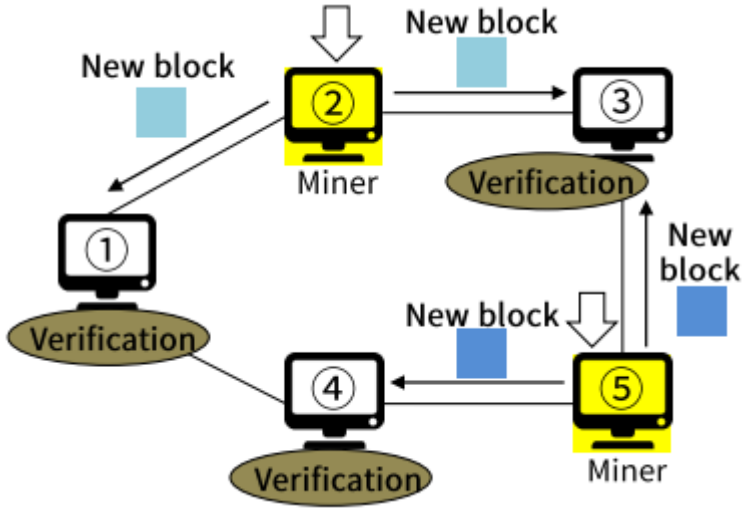
블록체인 요소 기술

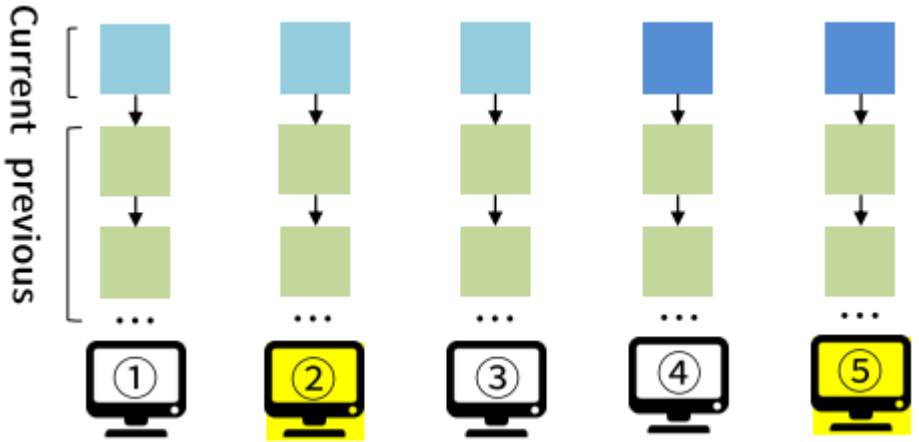
- 채굴 프로세스
  - PoW: 새로운 블록 생성
    - 알맞은 nonce 값 찾기
      - Nonce를 변화시키면서 후보블록 헤더의 캐시값 계산하여 DifficultyTarget과 비교



블록체인 요소 기술

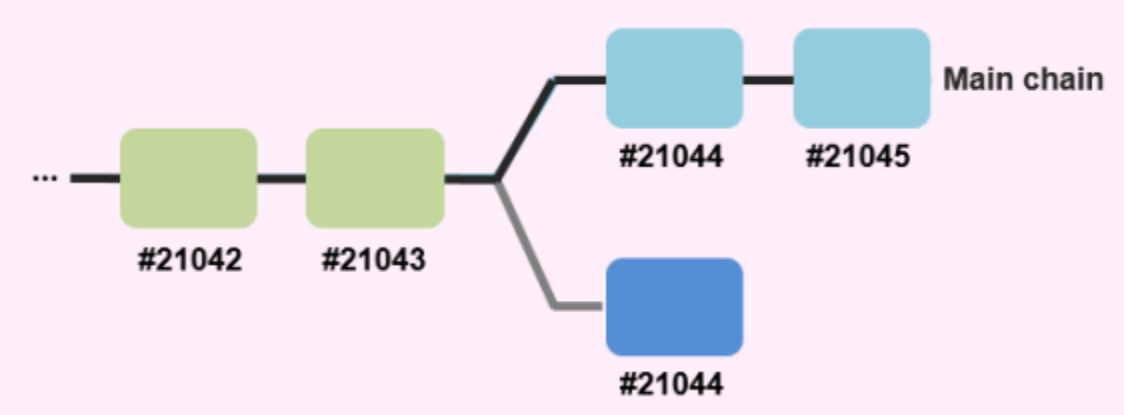
- 채굴 프로세스
  - 마이닝에 성공한 블록 전파
  - 각 노드에서 새 블록의 유효성을 검증
  - local blockchain에 해당 블록을 연결
    - 블록의 분기 가능
  - DifficultyTarget 조정





블록체인 요소 기술

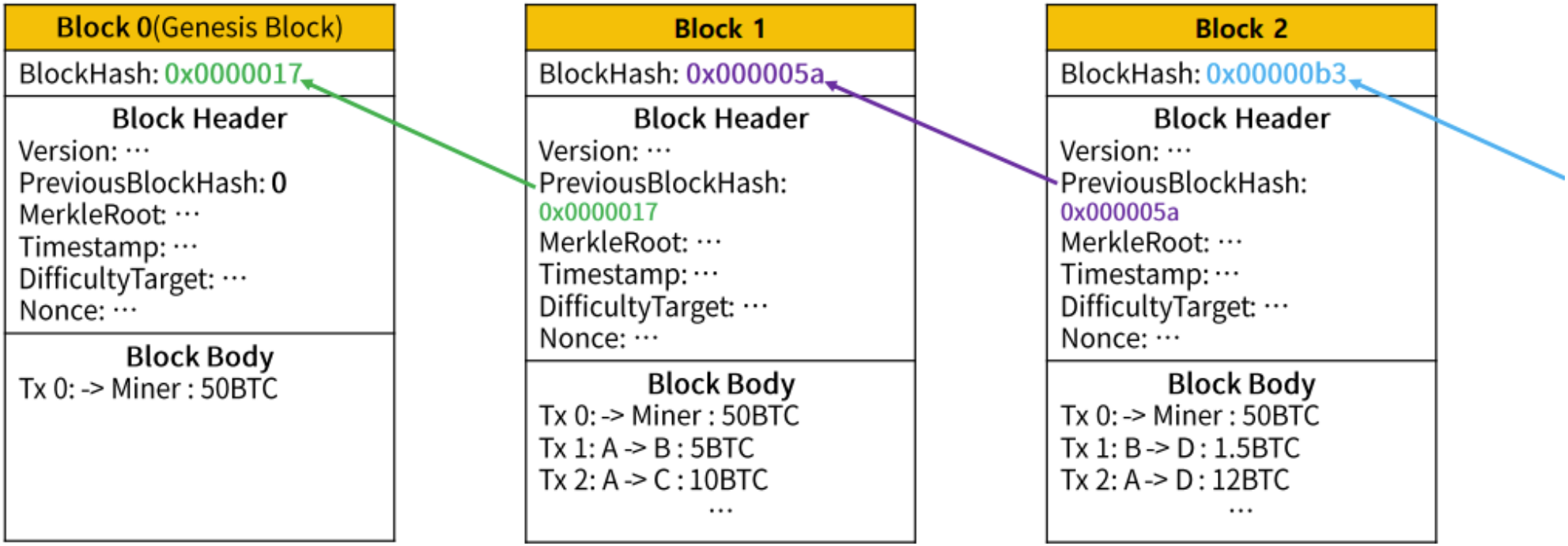
- 블록의 분기(fork)
  - 가장 긴 체인을 메인 체인으로 정함



- 비트코인의 분산 합의 프로세스
  - 첫 번째, 모든 풀 노드가 각 거래에 대해 독립적으로 검증을 실시
  - 두 번째, 작업 증명 알고리즘을 이용하여, 마이너들은 검증된 거래들을 새로운 블록에 추가
  - 세 번째, 모든 노드들이 새 블록을 검증한 후 블록체인에 연결
  - 네 번째, 모든 노드가 작업증명을 통해 연결한 체인들 중 가장 긴 체인을 선택

블록체인 요소 기술

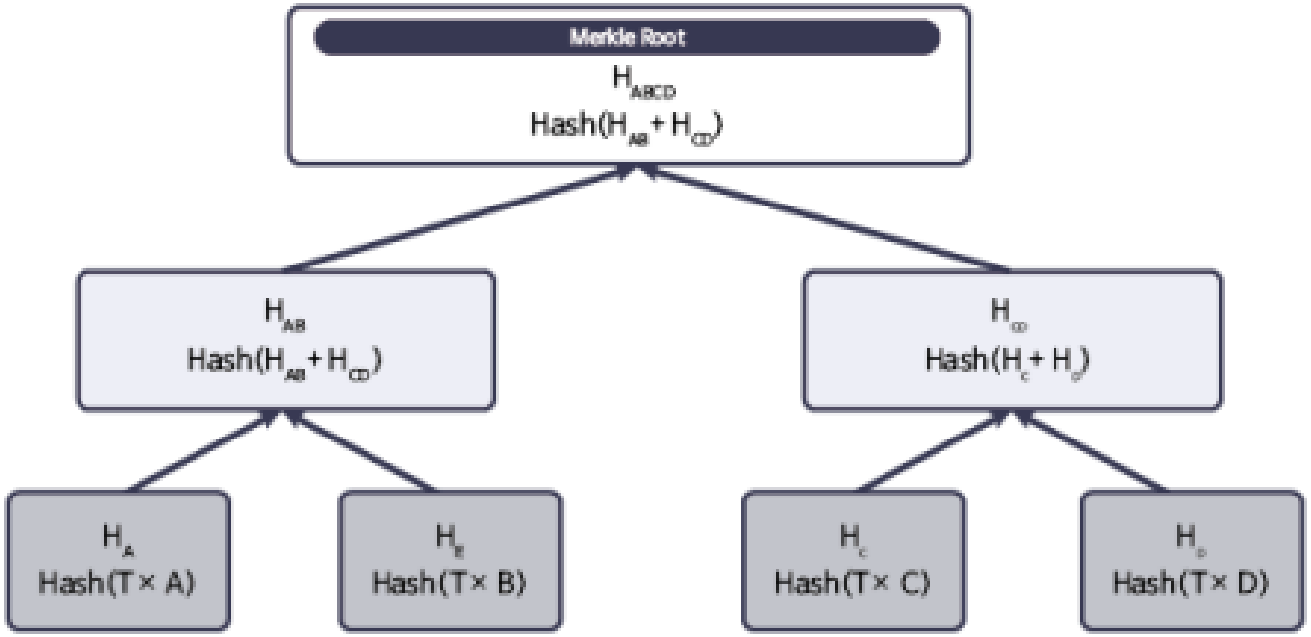
- 블록체인: 모든 참여자가 공유하는 '하나의 거대한 분산 공개 장부'
  - Transaction들 → Block들 → Blockchain
  - 블록: 블록체인에서 데이터가 갱신되는 한 주기 또는 최소 단위
  - 블록 해시(Block Hash): 블록 식별자



블록체인 요소 기술

- 블록
  - 블록 헤더(Block Header):
    - Version: 프로토콜 버전
    - 이전 블록 해시 (Previous Block Hash): 이전 블록의 고유 식별자인 해시 값, 이전 블록과의 연결을 만들어 체인을 형성
    - 타임스탬프 (Timestamp): 블록이 생성된 시간
    - 난이도 목표 (Difficulty Target): 채굴 과정에서 새로운 블록을 생성하기 위해 필요한 작업 증명의 난이도, 난이도는 블록 생성 속도에 따라 2주마다 조정
    - Nonce: 블록의 채굴 과정에서 사용되는 난수 값, 채굴자는 Nonce 값을 조정하여 해시 결과 값의 패턴을 찾아냅니다.
    - 머클루트 해시(merkle root hash): 블록에 포함된 모든 트랜잭션의 해시
  - 블록 바디: 마이너에게 비트코인을 발행하는 Coinbase 거래와 다수의 거래내역을 포함

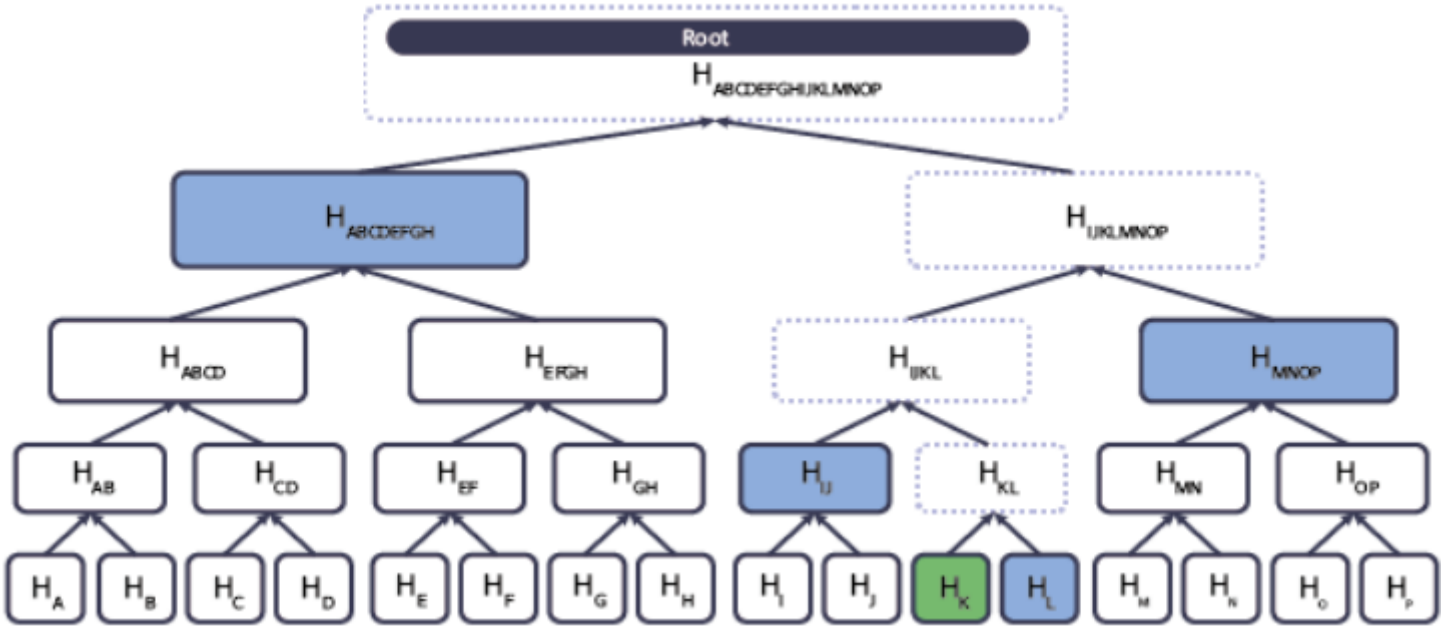
- 머클트리(Merkle tree)
  - 이진 해시 트리
  - 상위 노드는 각각 자식 노드들의 해시 값이 된다
  - 암호 해시 알고리즘으로: SHA-256 두 번 적용
  - 블록 내에 있는 모든 거래를 요약



블록체인 요소 기술

서강대학교 SOGANG UNIVERSITY

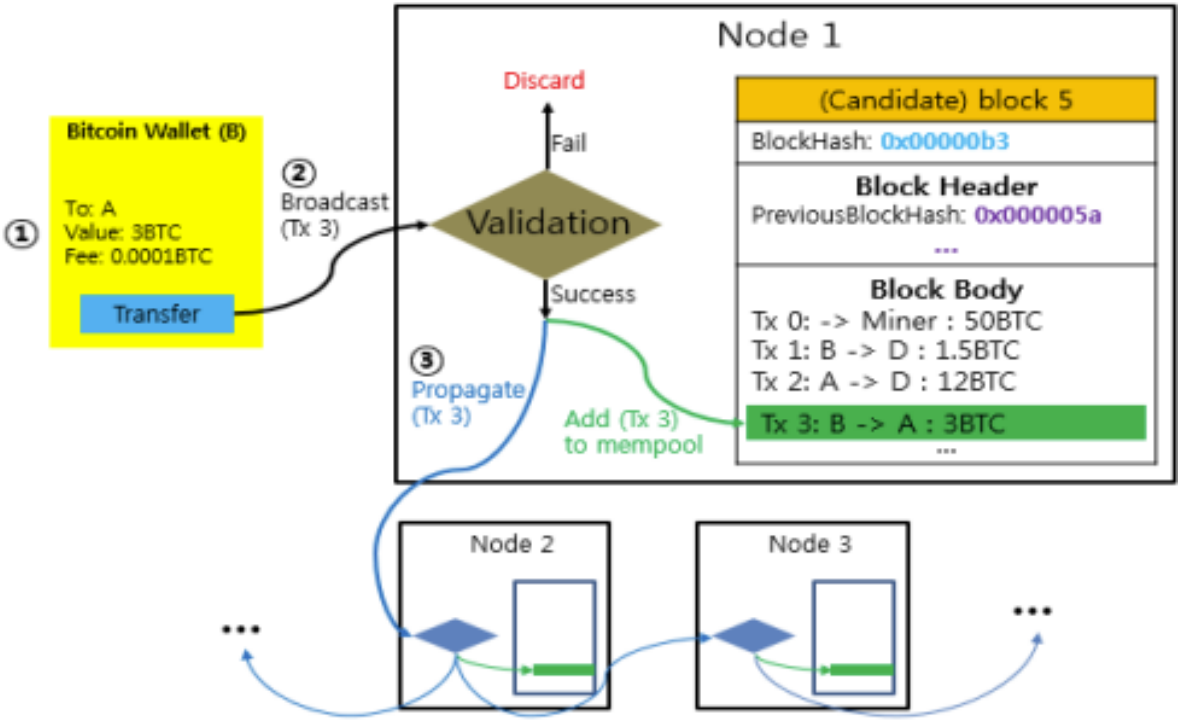
- 머클트리(Merkle tree)
  - 거래들이 블록 내부에 포함되는지 여부를 검증하는데 아주 효율적인 프로세스를 제공
  - 머클경로: 특정 거래와 트리의 루트를 연결
  - log2(N)의 머클경로의 데이터만 필요



비트코인 구성 요소

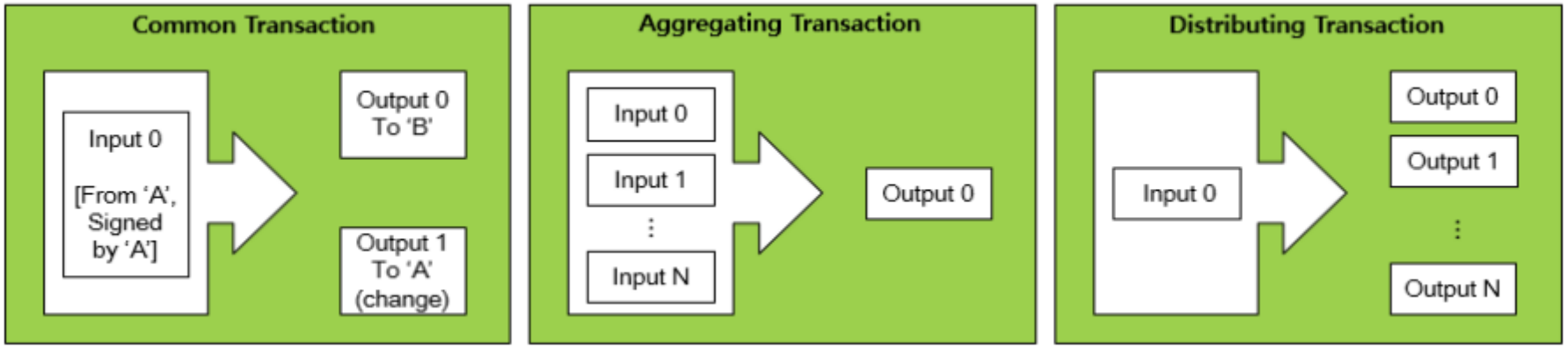
- 거래(transaction)
  - 비트코인 시스템 내에 있는 참가자들 간 가치를 전송하는 행위를 인코딩한 데이터 구조
  - 각 거래는 전 세계적 장부에 들어있는 공개된 항목

  - 거래의 생성과 전파 과정
    1. 거래의 생성
    2. 거래의 전송과 유효성 검증
    3. 검증된 거래의 전파와 메모리 풀 추가



비트코인 구성 요소

- 거래(transaction)
  - 비트코인 네트워크에서 자산의 이동과 관련된 모든 작업 포함
  - 트랜잭션은 다수의 입력(input)과 다수의 출력(output)으로 구성
  - 거래수수료 (transaction fee) = 입력의 합계 – 출력의 합계
  - 거래의 유형
    - 하나의 입력에서 대상 출력과 자기자신에게 잔돈(change)를 보내는 출력을 갖는 거래
    - 다수의 입력을 하나의 출력으로
    - 하나의 입력을 쪼개서 여러 개의 출력 값으로 분배할 수 있는 거래

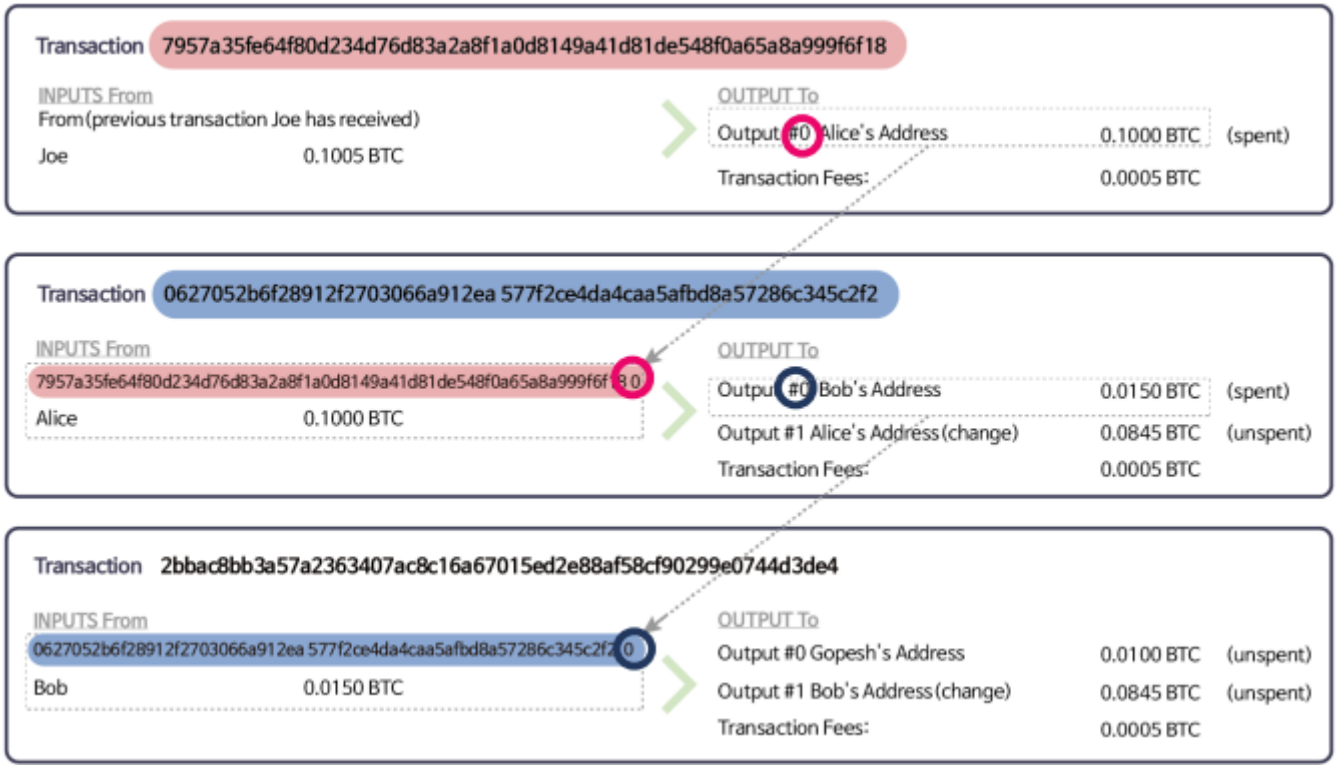


비트코인 구성 요소

- 비트코인의 UTXO(Unspent Transaction Output, 소비되지 않은 거래 출력)
  - 미사용 트랜잭션 출력값
  - 비트코인은 잔고가 없고, 블록체인에 기록된 "소비되지 않은 출력값"을 통해 코인의 존재 여부 확인
    - 예) A와 B로부터 각각 1비트코인과 3비트코인을 받아 총 4비트코인을 갖게 되었으면, 지갑에는 4비트코인이 한꺼번에 묶여 있지 않고 1비트코인, 3비트코인을 각각 UTXO로 저장
    - 비트코인 잔액의 개념은 지갑 애플리케이션이 해당하는 모든 UTXO를 다 더해서 보여주는 값
  - UTXO가 거래의 입력으로 사용될 때는 부분만 사용하는 것이 아니라 전부를 사용, 보낼 금액이 입력값의 UTXO보다 더 적다면 자신의 주소로 잔액을 보내야 함
  - 거래 입력 값(Transaction input): 하나의 거래에 의해서 소비되는 UTXO를 의미, 거래에서 UTXO가 소비될 때 현재 소유자의 서명을 가지고 잠금을 해제해야 소비할 수 있음
  - 거래 출력 값(Transaction output): 하나의 거래에 의해서 출력 값으로 새롭게 생성되는 UTXO를 의미, 새로운 소유자의 비트코인 주소로 UTXO를 잠가둠

비트코인 구성 요소

- 거래(transaction)
  - 한 거래의 출력 값은 다음 거래의 입력 값
    - 이전 거래의 해시(트랜잭션 식별)와 출력 값의 번호(index)



비트코인 구성요소

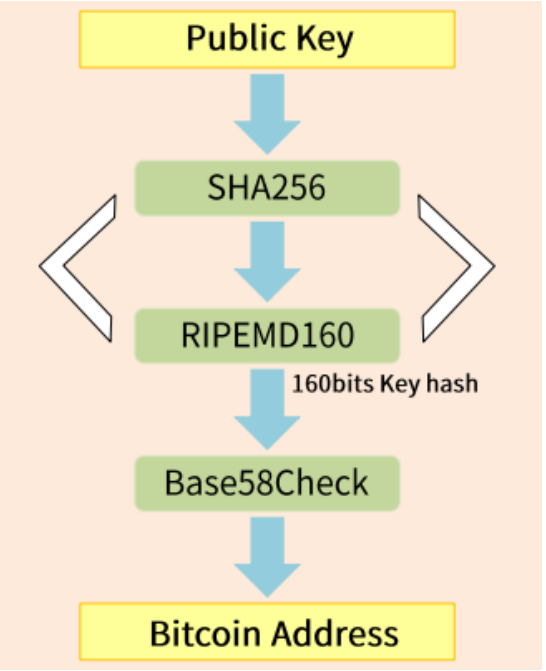
- 암호키와 비트코인 주소(Address)

	Public Key	Private Key
Similarity	Bank Account	Secret PIN number
Usage	Receive Bitcoin	Transfer Bitcoin
How to generate	Elliptic Curve Cryptography	Random Digit Extraction

- 개인키: 무작위 숫자 추출을 통해 생성
- 공개키
  - 개인 키로부터 타원곡선 암호법(Elliptic Curve Cryptography, ECC) 을 이용해 생성
- 비트코인 주소: 공개 키에 암호화 해시 함수 적용

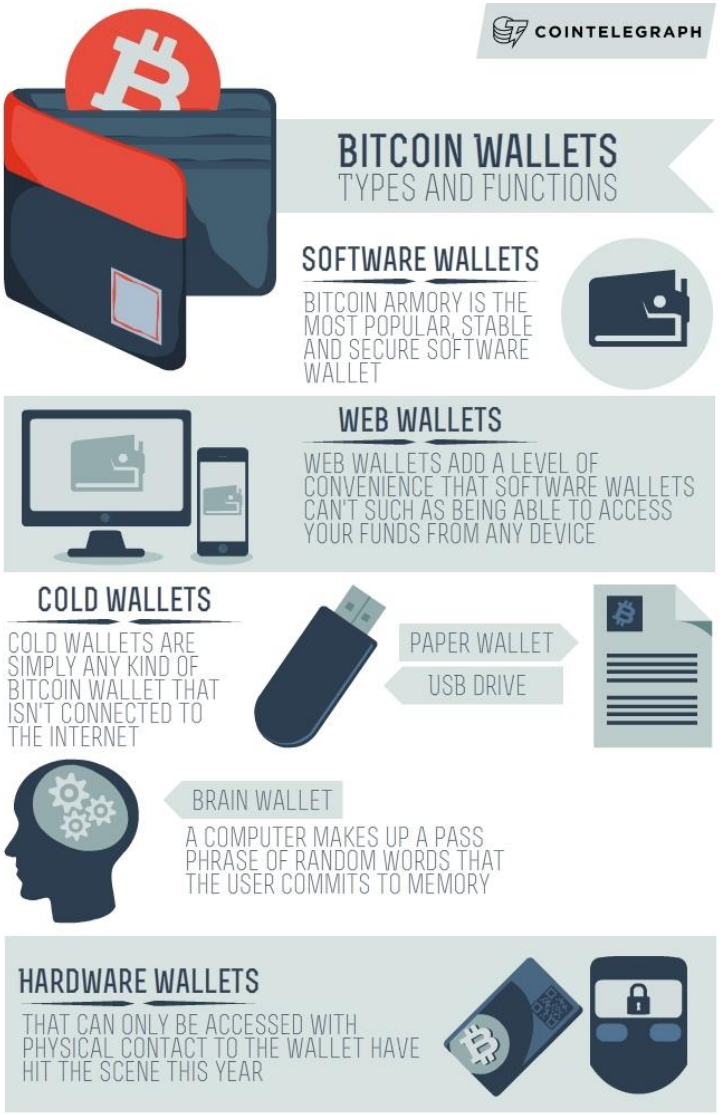
비트코인 구성요소

- 공개키로부터 비트코인 주소 생성
  - 공개키를 일방 암호화 해싱
    - SHA256 함수를 이용해 해싱하면 256bit 크기의 해시값, 이 값을 다시 RIPEMD160으로 해싱하면 160bit 크기의 해시값 생성
  - Base58check 인코딩을 통해 사용자가 읽을 수 있는 형태로 전환
    - 대문자, 소문자, 숫자 등을 사용
    - 자주 실수가 발생하거나 특정 글자체에서 동일하게 보일 가능성이 있는 몇몇 문자들을 제외한 58개의 문자를 이용하는 방식



비트코인 구성요소

- Wallet(지갑)
  - 개인 키와 공개키가 편의를 위해 한 쌍의 키 형태로 저장
  - 여러 개의 주소를 생성하고 관리
  - 비트코인 지갑은 비트코인이 아닌 키 관리
  - 사용자가 암호화폐를 보내고 받을 수 있게 하는 소프트웨어
  - 소프트웨어 지갑: 데스크톱, 모바일 또는 온라인
  - 하드웨어 지갑: USB와 같은 하드웨어 장치에 개인키 저장
  - 종이 지갑: 공개키 및 개인 키의 인쇄물



비트코인 네트워크

- 현재 전 세계 비트코인 노드들의 분포도

REACHABLE BITCOIN NODES
Updated: Sun Sep 8 11:11:42 2024 KST

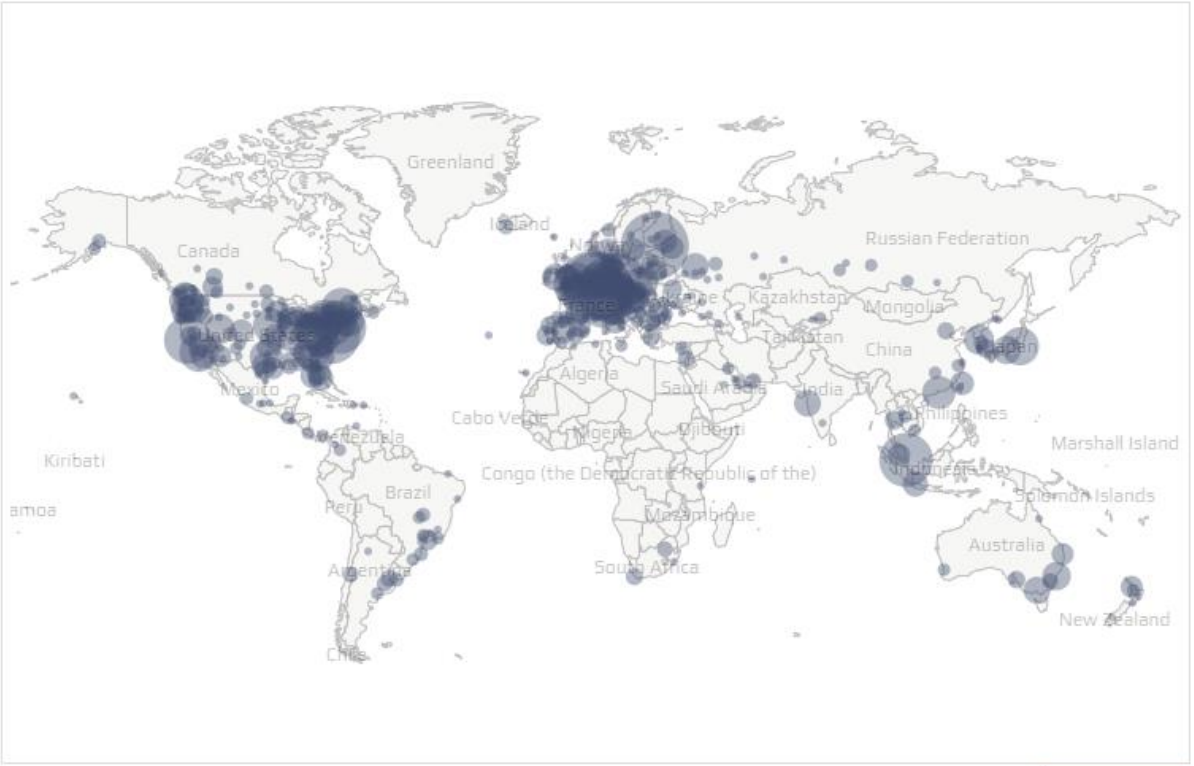
19141 NODES **CHARTS**

IPv4: -0.3% / IPv6: -7.4% / .onion: +12.2%

Top 10 countries with their respective number of reachable nodes are as follows.

RANK	COUNTRY	NODES
1	n/a	12144 (63.44%)
2	United States	1994 (10.42%)
3	Germany	1378 (7.20%)
4	France	441 (2.30%)
5	Finland	394 (2.06%)
6	Netherlands	341 (1.78%)
7	Canada	284 (1.48%)
8	United Kingdom	194 (1.01%)
9	Switzerland	176 (0.92%)
10	Singapore	169 (0.88%)

All (91) »

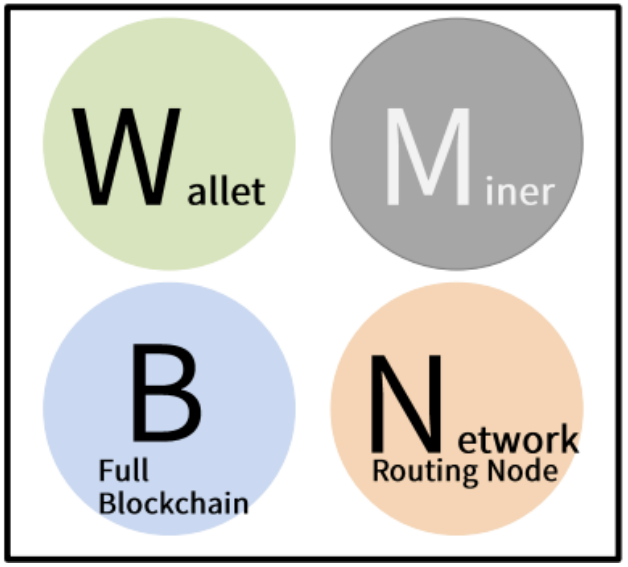


Map shows concentration of reachable Bitcoin nodes found in countries around the world. **LIVE MAP**

* https://bitnodes.io/

비트코인 네트워크

- 비트코인 네트워크: 비트코인 P2P 프로토콜을 실행하는 노드의 집합
- 블록체인에서 노드(node)
  - 블록체인 네트워크의 참여자를 의미, 엄밀히 말하면 참여자들이 사용하는 기계를 노드라고 부르며, PC부터 데이터를 저장할 수 있는 태블릿, 스마트폰 또한 노드가 될 수 있음
- 비트코인 블록체인의 노드의 역할
  - 지갑: 개인키/공개키 관리, 소유한 비트코인 송수신 및 잔고 확인
  - 채굴: 블록 생성, 합의, 화폐 발행
  - 블록체인(장부): 모든 장부 저장
  - 네트워크: 거래와 블록을 검증하고 전파하며, 이웃 노드들과의 연결을 유지



비트코인 네트워크

- 비트코인 노드
  - 풀노드(full node)
    - 거래와 블록을 검증하고 전파하며, 이웃 노드들과의 연결을 유지하는 역할
    - 비트코인 블록체인(장부)을 모든 거래내역들과 함께 완전한 최신 사본을 계속 유지하는 노드
    - 다른 노드로부터 데이터 제공 요청시 데이터를 제공
  - SPV(Simple Payment Verification) 노드 또는 라이트 웨이트(Light weight) 노드
    - 스마트폰이나 태블릿
    - 블록헤더만 다운로드하고 각 블록에 들어 있는 거래들은 다운로드하지 않는다
  - 마이닝 노드(Mining Node)
    - 새로운 블록을 생성하고 네트워크에 추가하는 채굴 기능을 수행하는 노드

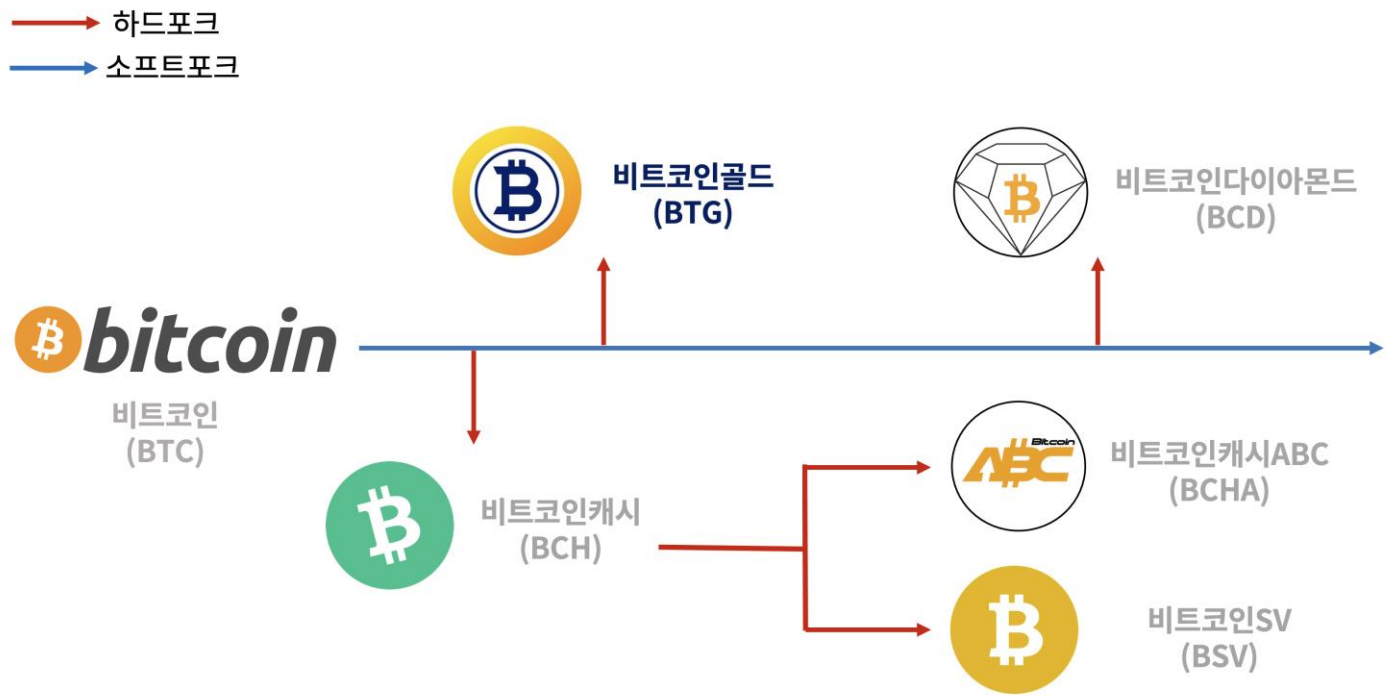
블록체인 포크(Fork)

- 하드 포크(Hard Fork)와 소프트 포크(Soft Fork)
  - 블록체인 프로토콜에 대한 업데이트나 개선
  - 하드 포크 (Hard Fork)
    - 기존 블록체인 프로토콜에 대한 중요한 변경사항을 포함하는 업데이트
    - 이전 버전의 노드와 새 버전의 노드 간에 비호환
    - 예시: Ethereum의 하드 포크 중 하나인 "The DAO Hard Fork"는 이전에 발생한 스마트 계약 공격으로부터 회복하기 위해 실행
    - 예시: Bitcoin Cash (비트코인 캐시), 블록 크기가 1MB에서 8MB로 확장
  - 소프트 포크 (Soft Fork)
    - 이전 버전의 노드와 새 버전의 노드 간에 호환성을 유지하는 업데이트
    - 예시: Bitcoin의 소프트 포크 중 하나인 "Segregated Witness (SegWit)"는 트랜잭션 유효성 검사를 개선하고 블록 크기 제한을 늘리기 위해 실행

블록체인 포크(Fork)

- 비트코인 하드포크
  - 비트코인캐시가 비트코인 블록체인 네트워크의 처리속도 개선을 목표
  - 비트코인골드는 비트코인의 채굴방식 개선을 목표

비트코인 하드포크 히스토리



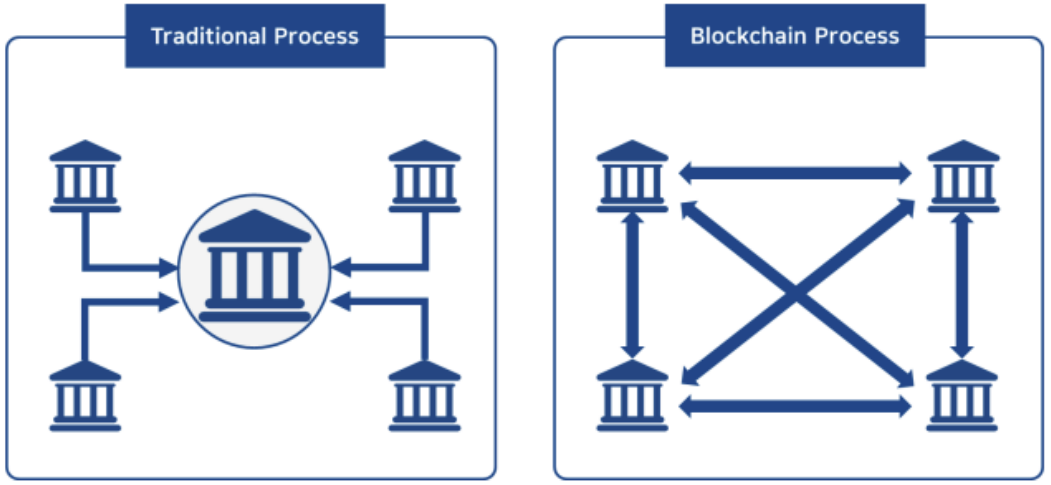
* https://m.upbitcare.com/academy/research/236

비트코인 블록체인

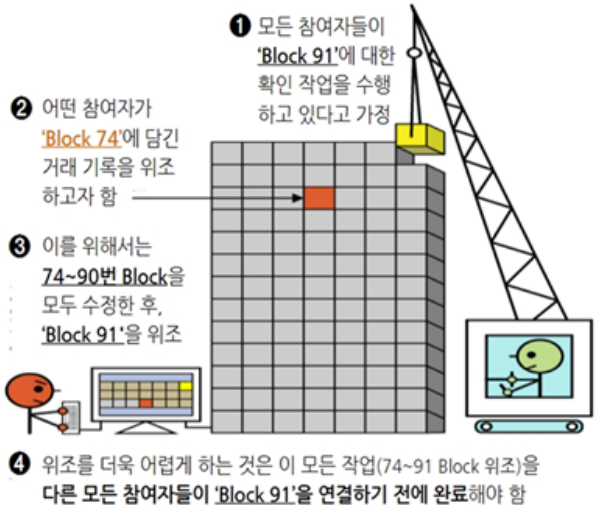
- 비트코인의 한계
  - 실시간성이 낮다
    - 거래가 완료되기 까지 최소 10분
  - 확장성 문제
    - 비트코인의 초당 거래량은 초당 약 7개 정도
  - 에너지 소모 문제
  - 미비한 스마트 계약 기능
    - 암호화폐 거래를 위해 제안된 전자 지불 시스템
    - 여러 산업에 적용하기 어려운 이유

블록체인의 특징

- 탈중앙화
  - 관리의 분권화
  - 데이터의 투명성



- 데이터의 불변성
  - 위변조 어려움



블록체인 요소 기술

- 해시 함수: 비트코인의 보안, 데이터 무결성, 그리고 네트워크의 신뢰성을 유지하는 데 핵심적인 역할
  - 블록의 해시 생성: 각 블록은 이전 블록의 해시값을 포함
    - 블록 헤더는 블록의 중요한 정보를 담고 있으며, 해시함수를 통해 헤더의 해시값 생성
    - 이 해시값은 블록의 고유한 식별자로 사용되며, 블록 간의 순서를 보장하는 역할
  - 작업 증명(Proof of Work, PoW):
    - 채굴자들이 특정 조건을 만족하는 해시값을 찾기 위해 연산을 수행
  - 트랜잭션 무결성 검증:
    - 트랜잭션 데이터의 해시값을 사용하여 무결성을 검증
  - 머클 트리(Merkle Tree):
  - 주소 생성: 사용자의 공개 키로부터 해시함수를 적용해 생성