캡스톤 디자인

- Rent GO -

허진영, 한석찬, 명세인, 채송현
상명대학교 컴퓨터 소프트웨어공학과

목차
INDEX

STEP I 블록체인 개념

정의

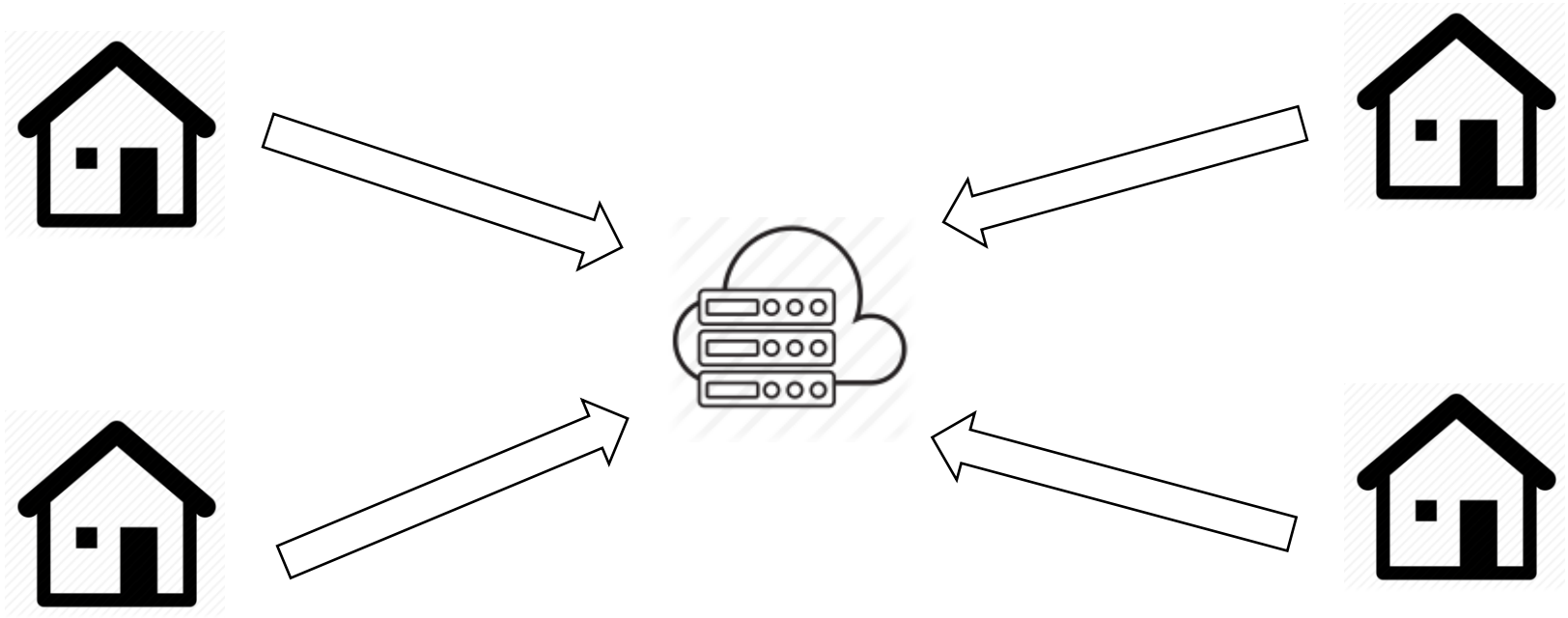
암호 화폐의 거래가 공개적으로 기록되는 디지털 장부

최초의 블록(Genesis Block)부터 시작해서, 개별블록이 이전 블록에 대한 정보를 가지고 있는 체인

모든 거래 정보 의미하는 블록체인은 여러 노드에 걸쳐 분산되어 저장 및 관리

STEP I 블록체인 개념

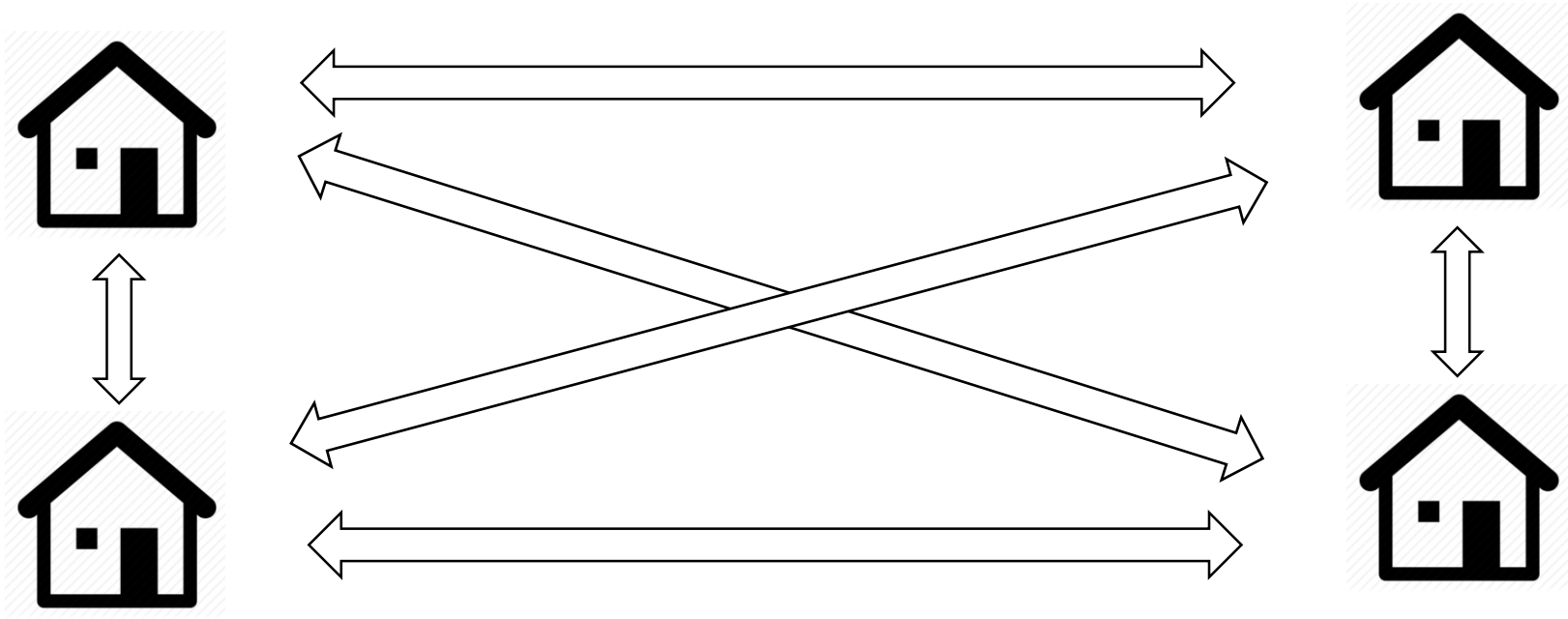
기존 중앙 집중형 거래



제 3자 신뢰기관과 개인의 거래
중앙 서버가 거래 공증 및 관리
사이버 공격에 대한 위협이 항상 있으며, 유지 관리비용이 필요

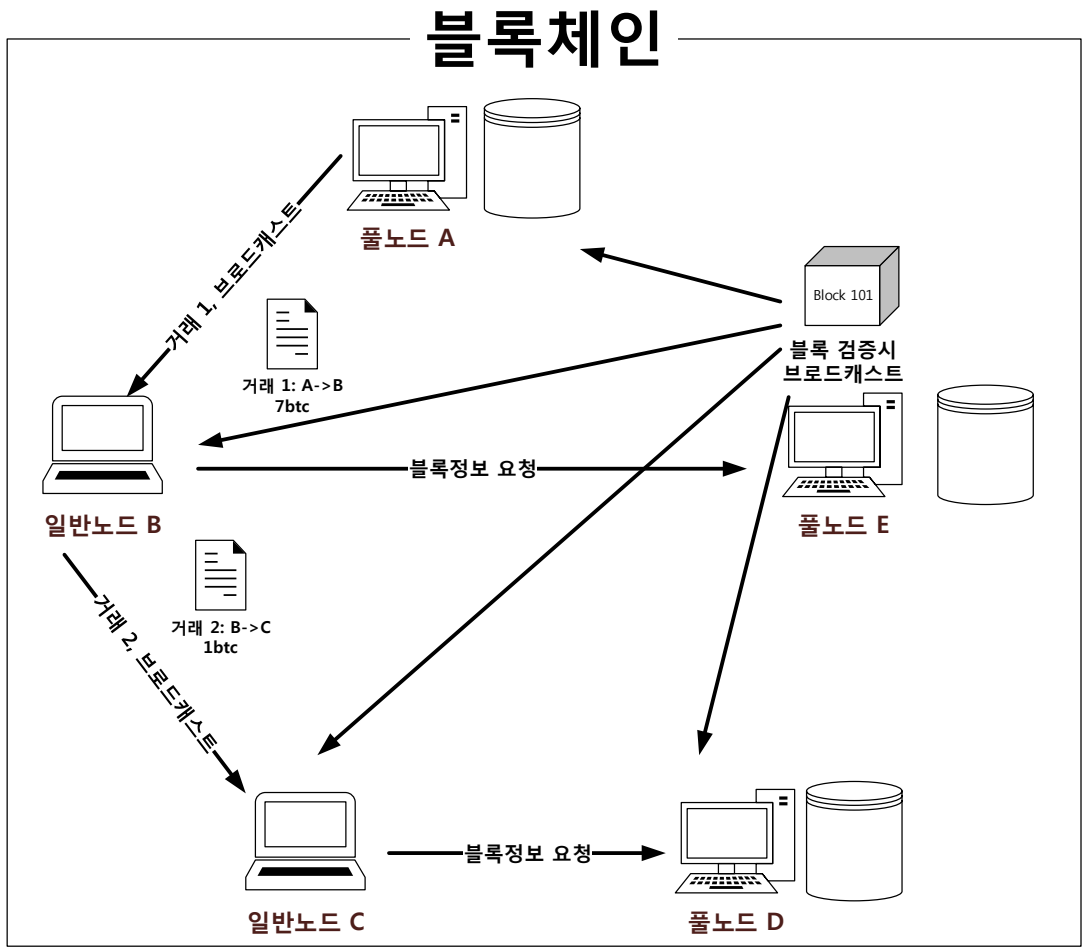
STEP I 블록체인 개념

블록 체인 기반 거래



거래내역이 모든 네트워크 참여자에게 공유 및 보관
개인간(P2P) 거래
거래정보의 투명성이 보장
해킹에 대한 위험성과 유지보수 비용이 줄어듦

STEP I 블록체인 개념
블록 체인 노드



- 일반 노드(라이트 노드) : 블록체인에 참여하여 거래를 수행하는 노드, 모든 블록정보를 가지고 있지 않으므로, 개별 거래에 대한 트랜잭션을 확인하기 위해 SPV를 수행
  - SPV(Simple Payment Verify): 거래를 검증하기 위해 일반 노드가 풀 노드에게 블록정보를 요청하여 머클 트리를 통해 이 거래가 검증된 거래인지를 확인

- 풀 노드 : 모든 블록체인 정보를 수집하고 저장하는 노드
  - 새로운 블록을 추가하기 위해 블록검증을 수행
  - 요청 받는 블록정보나 새롭게 검증된 블록들을 저장 및 관리

- 블록체인의 모든 메시지는 브로드캐스트

STEP I 블록체인 개념

블록 체인 장점

첫째, 탈 중앙화

P2P기반으로 중개기관 없이, 참여자 간의 직접적인 거래를 통해 특정 기관에 의존적이지 않고 중개 수수료를 절감

STEP I 블록체인 개념
블록 체인 장점

둘째, 보안성

**중앙 데이터베이스 한곳에 모든 자료를 저장하는 것보다
데이터보안 손실에 대한 보안성이 높음**

**수십~수천 개의 컴퓨터를 동시에 해킹하는 것은
매우 많은 비용이 들어가며, 현실적으로 불가능**

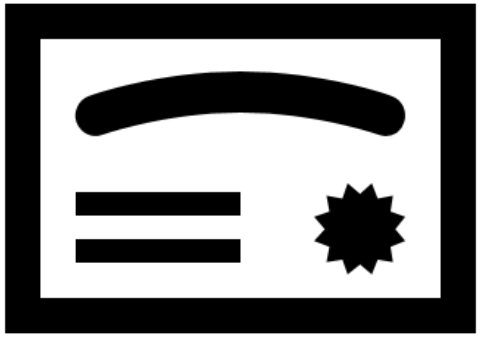
**또한 중앙집중 관리가 불필요하여, 내부자에 의한 조작
또는 정보 유출 위험 또한 크게 감소**

STEP I 블록체인 개념
블록 체인 장점

셋째, 투명성

블록체인은 모든 참여자들이 장부를 공유하는 공개성이 있어, 모든 거래기록에 공개적 접근이 가능

STEP I 블록체인 개념
블록 체인 장점



넷째, 안정성

일부 시스템에 오류 또는 성능저하가 발생하더라도 전체 네트워크가 타격을 입을 가능성이 희박 쉽게 복구가 가능

STEP I 블록체인 개념
블록 체인 단점

첫째, 처리 속도

시간당 거래 처리속도가 제한적

-> 이더리움은 약 10초에 한번 검증하여 단점을 보완

둘째, 저장 공간

모든 거래기록을 저장해야 하므로 저장공간이 점점 증가

-> 저장용량 문제가 나타날 소지가 있음
-> 공개성, 보안성을 이점으로 보완

STEP 2 블록체인 분류

Public BlockChain (퍼블릭 블록체인)

어느 누구나 열람/송금이 가능한 공개된 형태의 블록체인

STEP 2 블록체인 분류

Public BlockChain (퍼블릭 블록체인)

- **Permission-less** : 네트워크 참여에 제한이 없음

- **누구든지** 블록체인의 데이터를 읽고, 쓰고, 검증 가능

- **비트코인**이 가장 대표적인 예

STEP 2 블록체인 분류

Public BlockChain (퍼블릭 블록체인)

단점

- 그 누구도 제어 하지 않기 때문에,
  허락 받을 필요가 없으므로, 돈세탁이나 밀수품 거래에 악용 가능

- 그 누구도 소유하지 않기 때문에,
  블록체인을 유지하려면 **경제적인 인센티브가 필요**(=채굴)

- 모두가 운영 주체이기 때문에,
  블록체인 **프로토콜을 변경**하는게 쉽지 않음
  (블록체인 네트워크의 51% 이상의 동의를 얻어야 함)

STEP 2 블록체인 분류

Private BlockChain (프라이빗 블록체인)

하나의 기관에서 독자적으로 사용하는 블록체인

완전히 개인화된 블록체인

STEP 2 블록체인 분류

Private BlockChain (프라이빗 블록체인)

- 한 중앙 기관이 모든 권한을 가지며,
  네트워크에 참여하기 위해선 해당 중앙기관의 허락이 필요

- 읽기, 쓰기, 합의 과정에 참여할 수 있는 참여자가 미리 지정되어 있고,
  필요에 따라 특정 주체가 새로 추가되거나 제거됨

- 해시 경쟁이 없는 알고리즘을 사용하는 이유
  비트코인처럼 해시 경쟁에 의존하는 보안성 없이도 충분한 가치를 제공
  서버를 분산 시키는 것 자체로 보안성 증가

- 대표적으로 금융기관에서 사용

STEP 2 블록체인 분류

Private BlockChain (프라이빗 블록체인)

장점

- 느린 거래 속도와 네트워크 확장성 문제 해소
- 퍼블릭 블록체인의 단점이나, 위험성을 보완

STEP 2 블록체인 분류

Consortium BlockChain(컨소시움 블록체인)

여러 기관들이 컨소시움(조합)을 이뤄 구성하는 블록체인

반 중앙형 블록체인

STEP 2 블록체인 분류

Consortium BlockChain(컨소시움 블록체인)

미리 선정된 노드에 의해서 컨트롤되는 반 중앙형 블록체인

- 미리 선정된 노드들이 권한을 가짐

- N개의 기관이 노드를 한 개 씩 운영하고
  각 기관의 노드 간 동의가 일어나야 거래가 생성

- 블록체인의 기록 열람 권리를 모든 참여자에게 부여 하거나
  기관에게만 제공하여 API를 통해 특정 인원에게만 공개

STEP 2 블록체인 분류

Consortium BlockChain(컨소시움 블록체인)

장점

- 분산형 구조를 유지하면서 제한된 참여를 통해 보안 강화
- 네트워크 확장이 용이하고 거래 속도가 빠름

STEP 2 블록체인 분류

블록체인 비교

	퍼블릭 블록체인	프라이빗 블록체인	컨소시움 블록체인
관리주체	모든 거래 참여자	중앙기관이 모든 관리	컨소시움에 소속된 참여자
네트워크 참여조건	없음	중앙기관이 관리	없거나 선별된 기관이 관리
거래속도	느림	빠름	빠름
식별성	익명성	식별가능	식별가능
거래 증명	작업증명(PoW) 알고리즘, 거래증명자가 누구인지 사전에 알 수 없음	중앙기관에 의해 거래증명이 이루어짐	거래 증명자가 인증을 거쳐 알려진 상태, 합의된 규칙에 따라 거래검증 및 블록 생성

STEP 3 블록체인의 합의

기존의 합의

중앙 집중형 방식에서의 합의는 서비스 제공자가 주체가 되어 사용자의 기록을 관리

장점

- **빠른 서비스 제공**

단점

- **중앙기관이 악의적인 의도로 기록 조작 가능**
- **악의적인 사용자는 중앙기관만 공격하면 기록 조작 가능**

STEP 3 블록체인의 합의

블록체인의 합의

중앙 집중형 에서 장단점이 있지만,
블록체인이 나오기 전까지는 P2P에서 공개적인 합의는 불가능한 것이 정설

- **블록체인으로 구현된 합의 알고리즘이 P2P에서의 거래정보, 데이터 정보들을 동기화하고, 모든 주체들이 믿을 수 있도록 함**

- **비트코인에서 블록을 합의하여 완전한 블록체인에 포함하기 위한 요소**
  - **작업증명블록을 검증**
  - **해당 거래에 대한 블록 검증 누적횟수(6-Confirmations)**

STEP 3 블록체인의 합의

합의 알고리즘

PoW(Proof of Work)

블록체인의 가장 기본적인 합의 알고리즘

- **거래승인 과정에 많은 컴퓨팅 파워가 필요한 어려운 작업을 수행**
- **가장 긴 블록체인을 합의하고 다른 기록은 폐기**
- **결국 블록체인을 조작불가능**

장점

- **데이터의 무결성 보장**

단점

- **채굴의 집중화와 독점화 문제**
- **과도한 에너지 소비와 같은 문제 발생**

STEP 3 블록체인의 합의
합의 알고리즘

PoS(Proof of Stake)

채굴 시스템에서 사용자의 소유 지분이 블록 생성권의 지분율을 나타냄

장점

- 블록의 생성 주기가 매우 짧아 독점화 현상 방지

단점

- 전체 네트워크의 노드 상태를 알아야함
- 지분율이 높은 사용자가 블록을 생성할 가능성이 높아 빈익빈 부익부 현상이 나타남

STEP 3 블록체인의 합의
합의 알고리즘

DPoS(Delegate Proof of Stake)

반 중앙화 된 방식
PoS방식을 기반, 모든 개인이 채굴을 하는 대신 101명의 선출된 Delegate(대표자)들 만이 블록 생성

- **대표자는 각 지분보유자가 자기 지분을 가지고 투표를 해서 선출**

- **대표자들끼리 서로 경쟁하게 함으로써 대표자들을 통해 실질적인 서비스 제공을 받을 수 있다는 장점**

STEP 3 블록체인의 합의
합의 알고리즘

PoI(Proof of Importance)

구글 검색 알고리즘이었던 Page Rank 알고리즘을 응용하여 개발됨

- **PoS와 유사하지만 계정의 잔액 규모에만 의존하지 않는다는 점이 다름**
- **빈익빈 부익부 현상을 막고자 계정의 잔액 규모가 아니라 많은 양의 코인을 빈번하게 거래할 수록 더 많은 보상을 가짐**

STEP 3 블록체인의 합의

합의 알고리즘

Consensus-by-bet

기존의 알고리즘과는 달리, 참여자의 동의 및 베팅을 통해서 블록체인의 거래를 승인하는 방식

- **동의를 통한 승인구조는 어느 한 사람이나 단체가 네트워크를 독점하기 어려움**
- **보증금을 걸고 승인에 참여하게 되는데 올바른 승인을 할 경우 보상을 해주고 그렇지 않은 경우 보증금을 돌려받지 못하는 패널티를 줌으로서 참가자가 올바른 블록을 승인 할 수 있도록 함**
- **올바른 블록을 많이 승인한 참가자일수록 신뢰할 수 있는 참가자로 간주하고 그 결과 거래의 타당성을 보장할 수 있게 됨**

STEP 4 블록체인 보안기술

해시함수

임의의 길이를 가진 어떤 임의의 데이터를 일정한 길이의 어떤 데이터로 바꿔주는 함수

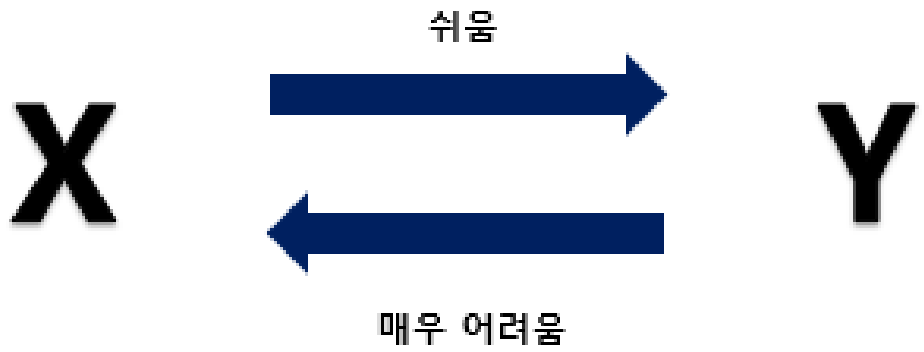
단 방향 함수

- 데이터로부터 해시 값을 구할 수는 있지만 해시 값으로 부터 데이터를 역산하는 것은 계산적으로 불가능
- 해시 출력 값이 같은 데이터를 추측 하는 것은 매우 어려움
    - 특정 해시 값이 나오는 데이터를 찾으려면 많은 경우의 수의 데이터 확인 필요

SHA-256

- 출력 값이 256비트인 해시함수

STEP 4 블록체인 보안기술
해시함수



EX) 특정 소수로 나눈 값의 나머지 함수
7로 나눈 나머지 함수 MOD7
X = 19일 때, Y= MOD7(19) = 5 -> 간단히 계산
Inverse-MOD7(5) = 5, 12, 19 … -> 무수히 많음

STEP 4 블록체인 보안기술
해시함수

- 한 글자만 바뀌었고, 비트단위로 보았을 때도 단 한 개의 비트만 바뀐 변화에서, 해시함수를 통해 전혀 다른 값이 산출
  - 데이터 변조의 유무를 검증하는 용도로 매우 적합한 함수

STEP 4 블록체인 보안기술
공개키 암호화

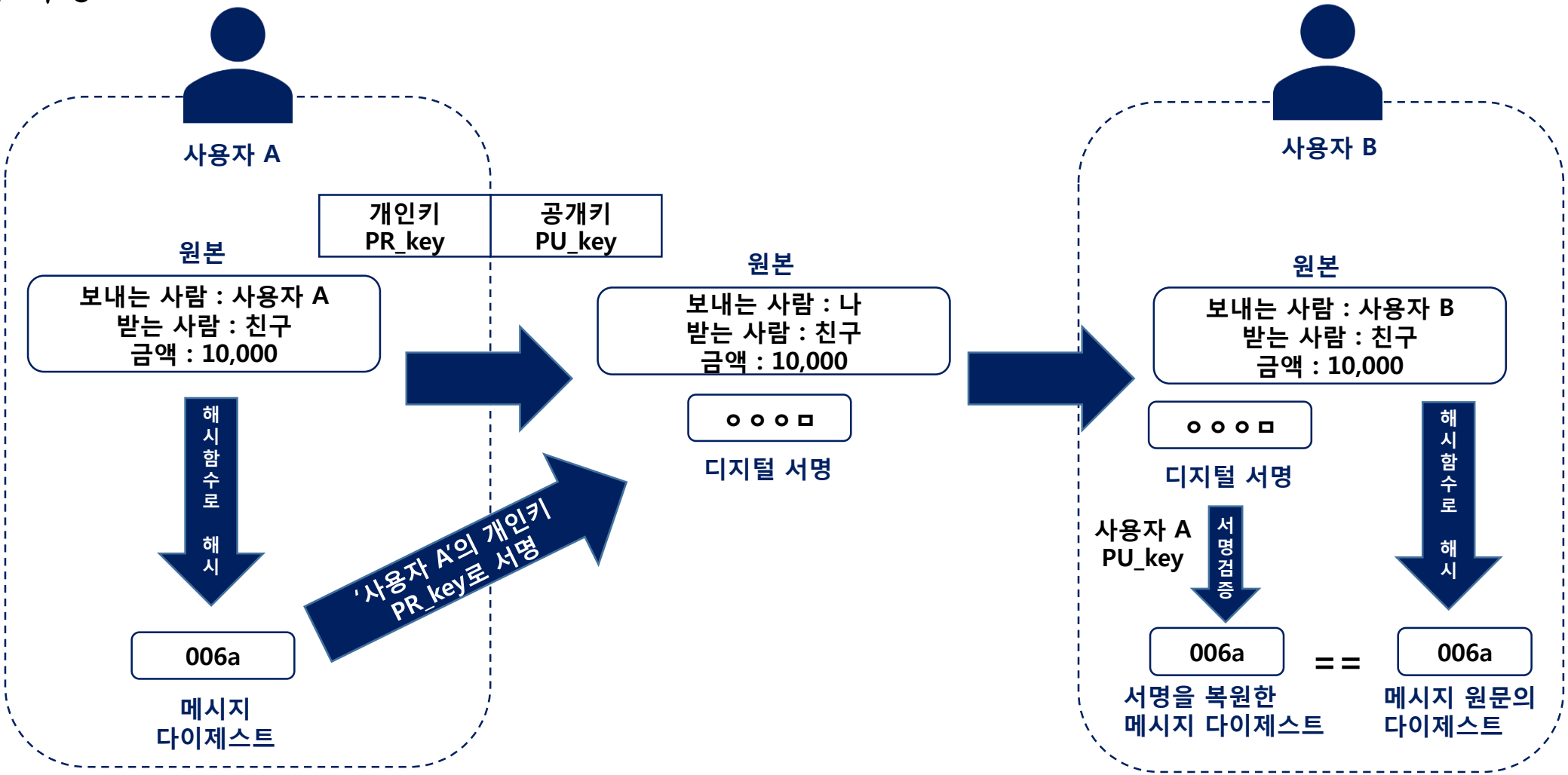
공개키(Public Key)와 개인키(Private Key) 쌍을 사용하는 암호화 방식

- 디지털 서명에 응용

공개키는 모든 사람에게 공개하는 것이고 개인키는 비밀로 유지하는 것

공개키로 암호화된 정보는 개인 키로만 복호화 할 수 있고,
개인키로 암호화된 정보는 공개 키로만 복호화 가능

STEP 4 블록체인 보안기술
디지털 서명



STEP 5 작업증명
의미

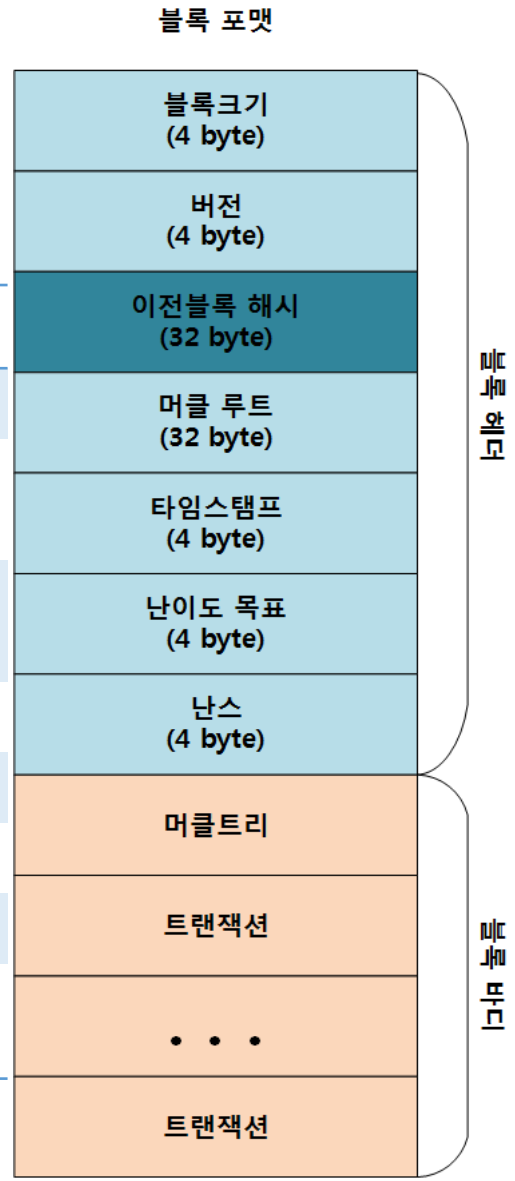
새로운 블록에 대해 검증 작업을 완료했음을 증명

- 새로운 블록의 해시를 계산 할 때, 조건에 맞는 해시를 계산해내려면 Nonce값을 변경하며 계산

결론적으로 조건을 만족하는 Nonce값을 구하는 것이 바로 작업 증명

STEP 5 작업증명
블록의 구조

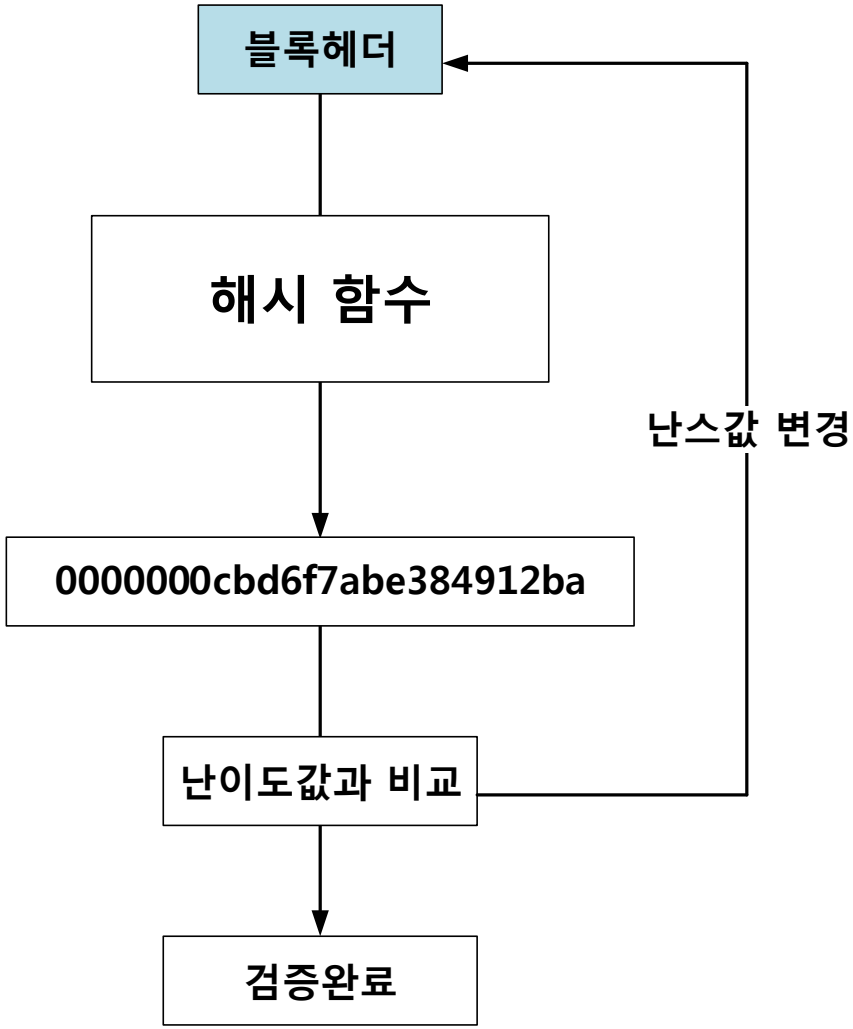
구성	명칭	설명
블록 헤더 (Block Header)	버전(version)	데이터구조의 버전
	이전해시블록	블록의 체인구조에서 이전블록(부모블록)에 대한 해시 참조 값
	머클루트 (Merkle Root)	해당 블록에 포함된 거래로부터 생성된 머클트리의 루트에 대한 해시(블록에 들어있는 모든 거래의 요약본)
	타임스탬프	블록의 생성 시간
	난이도 목표	Bit값으로 블록의 작업증명 알고리즘에 대한 난이도 목표
	난스(Nonce)	작업증명 알고리즘에 사용되는 카운터
블록 바디 (Block body)	트랜젝션(tx)	10분 동안 수집한 거래내역
	머클트리 (merkle tree)	거래내역을 트리 형태로 만든 데이터



STEP 5 작업증명
과정

기본동작

- 블록헤더를 해시하여 해시 값을 난이도 값과 비교
- 난이도 값에 맞지 않으면 난스 값을 변경
  - 난이도 값은 출력된 해시 값의 0배열의 개수
- 난이도 값에 맞는 해시 값을 찾으면 블록체인에 추가



STEP 5 작업증명

Nonce

입력 값인 블록헤더 중 유일하게 변경할 수 있는 값

- 계산되는 블록 해시 값이 특정 숫자 배열을 찾기 위해 변경
- nonce는 0에서 시작해서 작업 증명이 될 때까지 반복할 때마다 1씩 증가
  - 오버플로우 발생 시 블록 바디를 다시 구성(추가된 트랜잭션 포함)하여 0부터 시작

해시 함수의 특성을 이용

- 해시 결과를 예측할 수 없으므로, Nonce값을 변경하여 난이도에 맞는 해시 값을 계산
  - Hashcash

STEP 5 작업증명
난이도

블록 생성 난이도를 조절

목표
- 2016개의 블록을 생성하는데 2주(2016블록*10분=2주)가 유지

난이도 조정방법
- **목표치를 초과/미달하는 부분만큼 목표 값(target value)의 난이도가 변경되는 것**
- **2016개의 블록이 만들어지는 시점에서 블록체인의 2016개의 블록을 거슬러 시간 값을 확인하여 난이도 조정**

난이도 조정시점
- 매 2016번째 블록마다 이루어짐

STEP 5 작업증명
머클트리와 머클루트

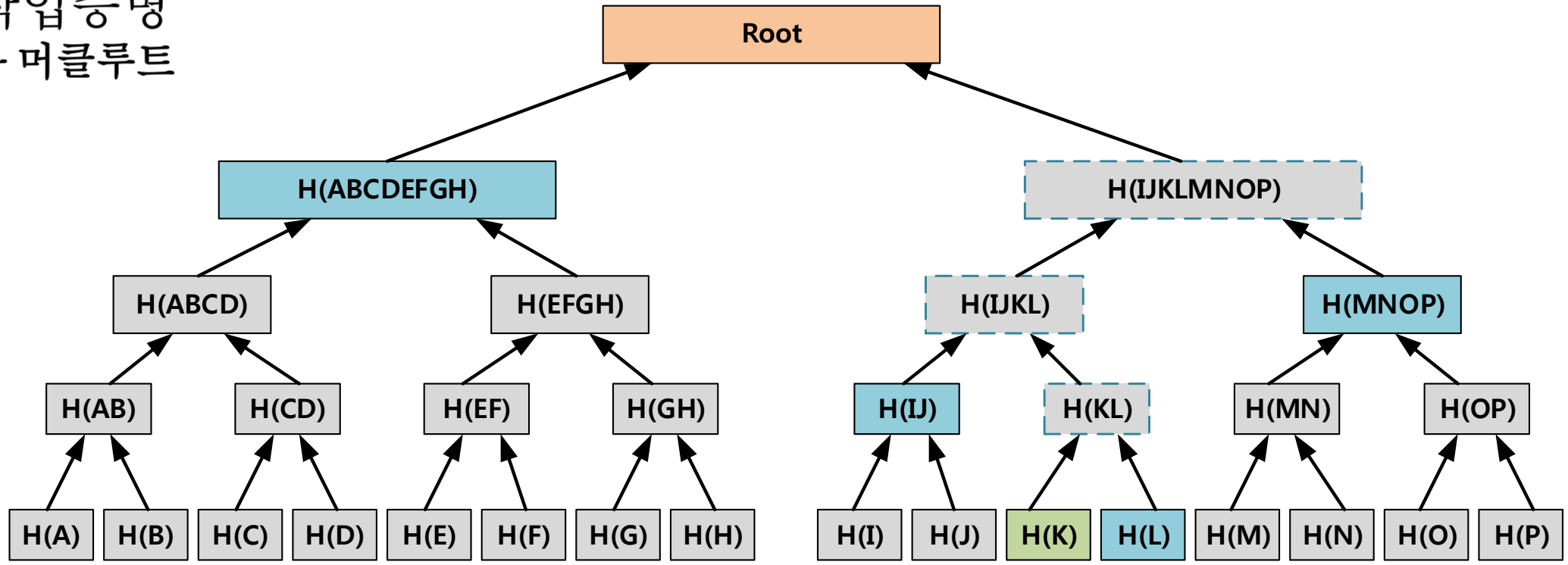
특정 파일의 변조 유무 검증

대량의 데이터 중, 일부 데이터가 손상될 경우 어떤 데이터가 손상되었는지 찾아냄
- 손상된 데이터를 다시 전송 받기 위한 자료구조

블록체인에서의 사용 용도

블록체인 사용자가 작성한 트랜잭션이 변조되지 않고, 블록에 포함되었음을 확인하기 위함

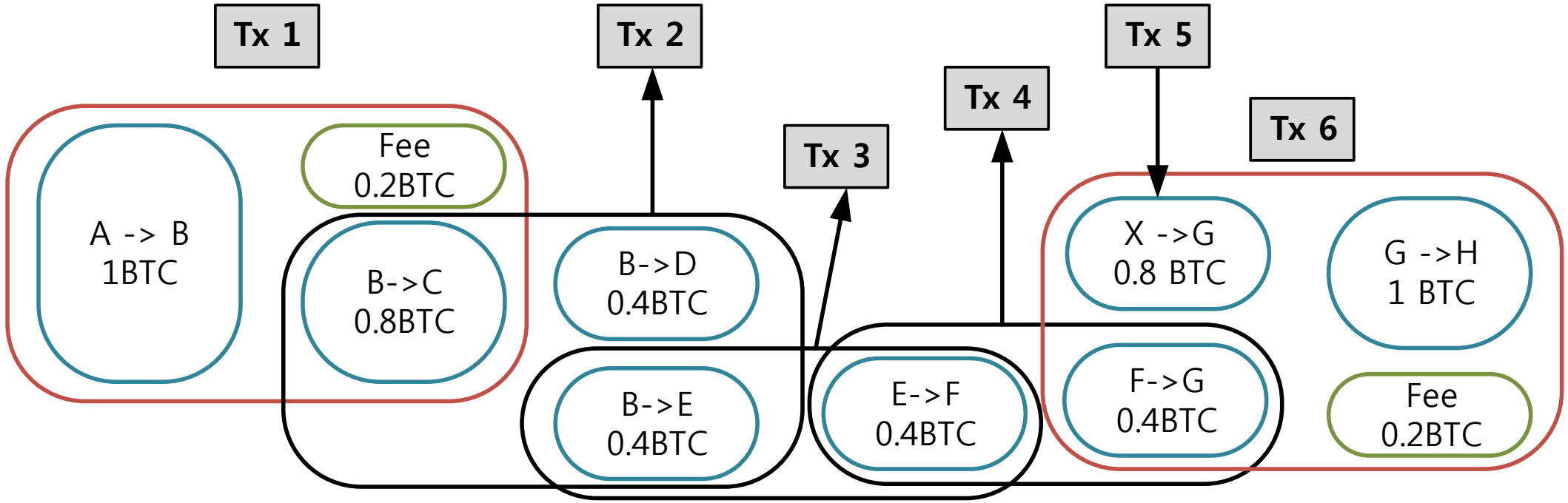
STEP 5 작업증명
머클트리와 머클루트



트랜잭션 A~P를 해시하여 머클트리 구성후 트랜잭션 K가 머클트리에 포함되었는지 확인

- 확인할 트랜잭션: 초록색 노드
- 확인하기 위해 알아야 할 트랜잭션: 파란색 노드
- 노드를 해시하여 루트까지 구해질 노드: 파란 점선노드

STEP 5 작업증명
트랜잭션 수수료

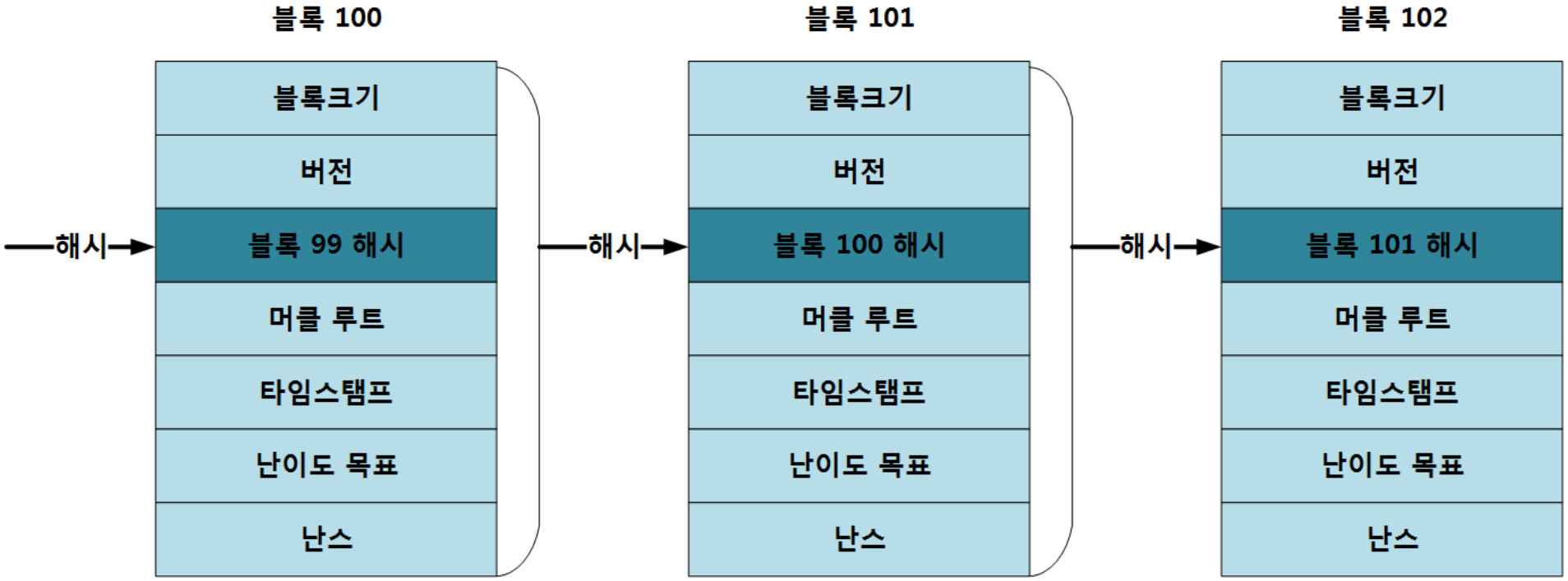


트랜잭션은 인풋과 아웃풋으로 구성

- **인풋의합 ≥ 아웃풋의합**
- **인풋과 아웃풋의 차는 수수료로 지급(지급하지 않으려면 자신에게 전송)**
- **트랜잭션 1, 6은 수수료를 지급하는 트랜잭션**
- **트랜잭션 2,3,4는 수수료가 없는 트랜잭션**

STEP 5 작업증명

블록 검증 후 구성된 블록체인



머클 루트는 트랜잭션의 정보를 요약

블록헤더만 해시 하여도 전체 블록체인의 정보들을 요약한 효과

STEP 5 작업증명

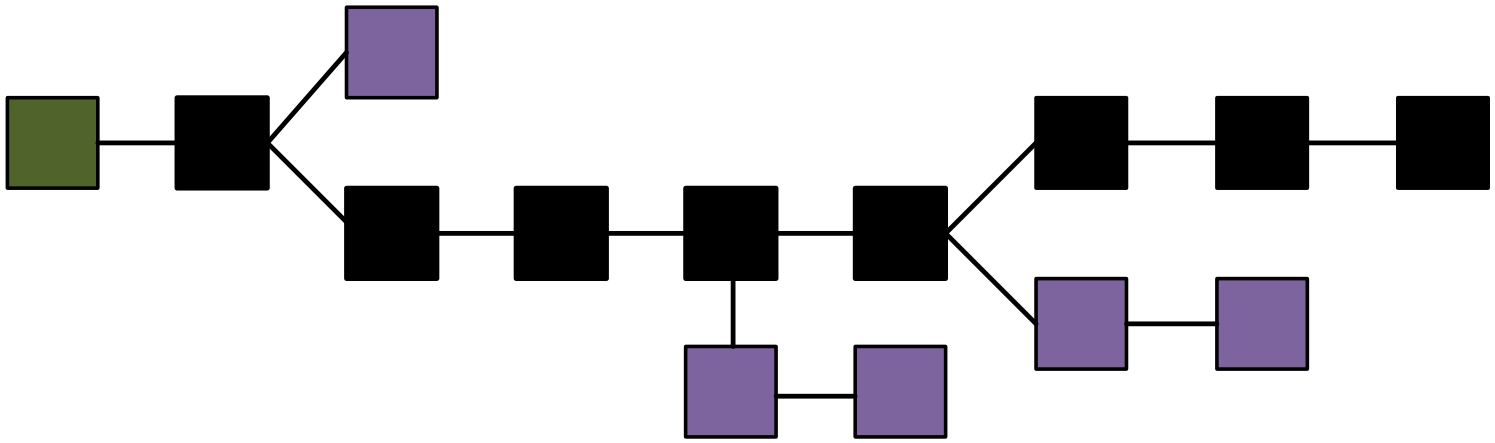
Fork

메인 블록체인에서 두 개 이상의 블록에 대한 작업증명이 이루어져 분기가 발생하는 경우

- 블록체인은 P2P네트워크이며, 블록검증이 완료되면 브로드캐스트
- 검증된 블록을 개별 노드가 동시에 수신하는 것은 물리적으로 불가능

결과적으로 가장 긴 체인을 이루는 블록을 메인 블록체인에 포함

- 모든 노드가 정보를 동기화

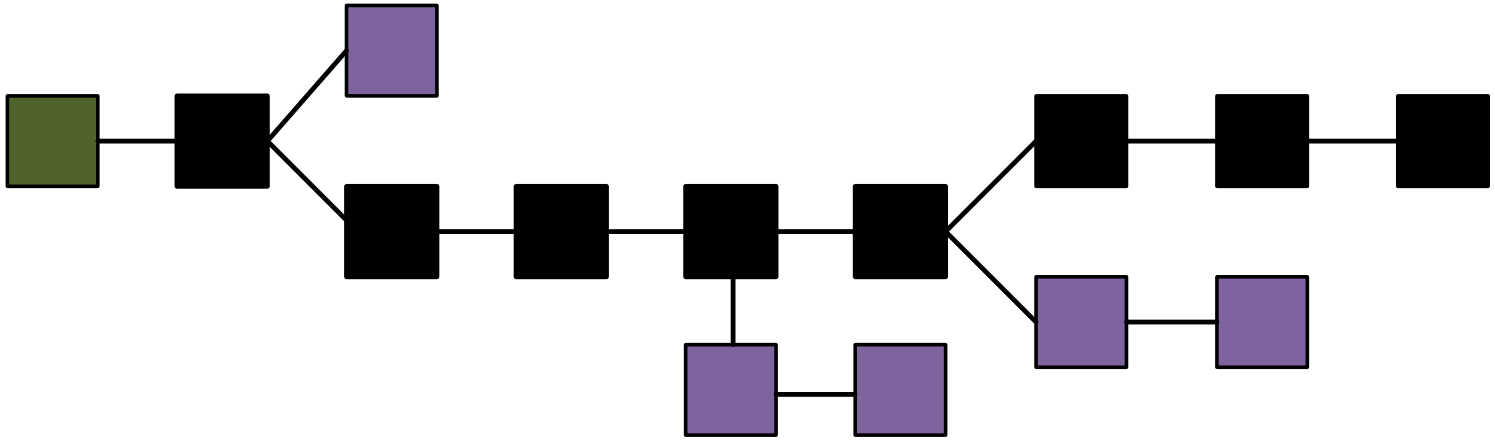


STEP 5 작업증명
이중지불

악의적인 목적으로 두 번 지불하거나, 지불된 금액을 회수하려는 경우

- 부정한 트랜잭션이 포함된 분기에 작업증명을 수행하여 메인 블록체인으로 만들 경우 이중지불이 발생할 수 있음

- 51%이상의 해시파워를 소유해야 함



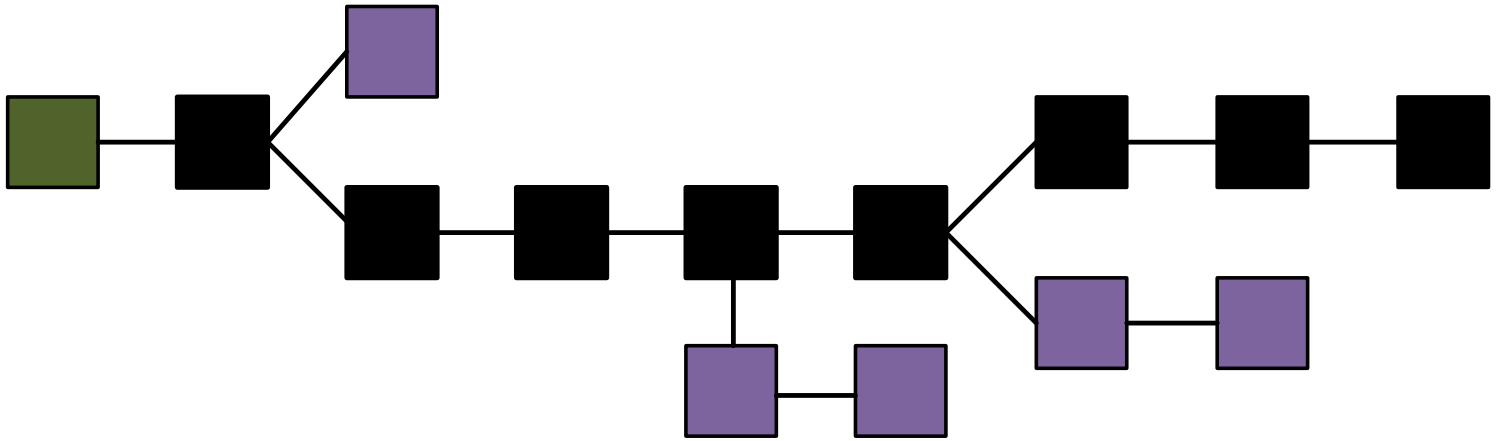
STEP 5 작업증명

51% ATTAK 사례

2014년 6월 마이닝 풀 중 하나인 Ghash.IO가 전체 해시의 51% 를 넘은 사례

- **51%를 이용하여 비트코인을 공격할 수 있었지만, 비트코인 시스템을 보존 하려고 함**

- **51%를 이용해 다른 사용자의 비트코인을 훔치거나, 새로운 블록을 생성하여 코인을 획득가능**



STEP 6 블록체인 활용 가능 분야

전자화폐	• 제 3자 신용기관 없이 사용자 간 인증을 통해 안전하게 유통이 가능 하도록 한 가상화폐 • 예)비트코인
해외송금	• 해외 송금 수수료를 획기적으로 낮출 수 있음 • 비트코인과 문자메시지(SMS)를 결합한 해외송금서비스 • 예)37Coins
데이터 저장 및 보호	• 국가토지대장을 블록체인을 통해 기록하여 해킹 및 조작을 원천적으로 방지 • 예)온두라스의 국가 토지 대장
메시지 보호 및 저장	• 사용자가 만든 P2P 네트워크상에서 상호 주고 받는 메시지를 암호화 및 메시지를 보내고 받는 당사자의 주소도 추적할 수 없는 형태가 됨 • 예)비트 메시지

STEP 7 참고자료

비트코인 기반기술, 블록체인의 원리

- https://www.slideshare.net/skimaza/ss-57356762

IITP Tech and Future Insight: 블록체인 콘서트 발표자료

- http://www.iitp.kr/kr/1/notice/notify/view.it?ArticleIdx=1995&count=true&page=1

블록체인의 기술적 이해 및 도입을 위한 첫걸음

- http://zzibal.printf.kr/wp-content/uploads/2016/03/Korbit-White_Paper-Block_Chain_Primer-1.pdf

Bitcoin, Blockchain and the Crypto Contracts

-https://www.slideshare.net/prithwis/bitcoin-blockchain-and-the-crypto-contracts-part-2

Bitcoinwiki, maintained by bitcoin community

-https://en.bitcoin.it/wiki/Main_Page

THANK YOU

감사합니다