블록체인 실습 “암호”화폐

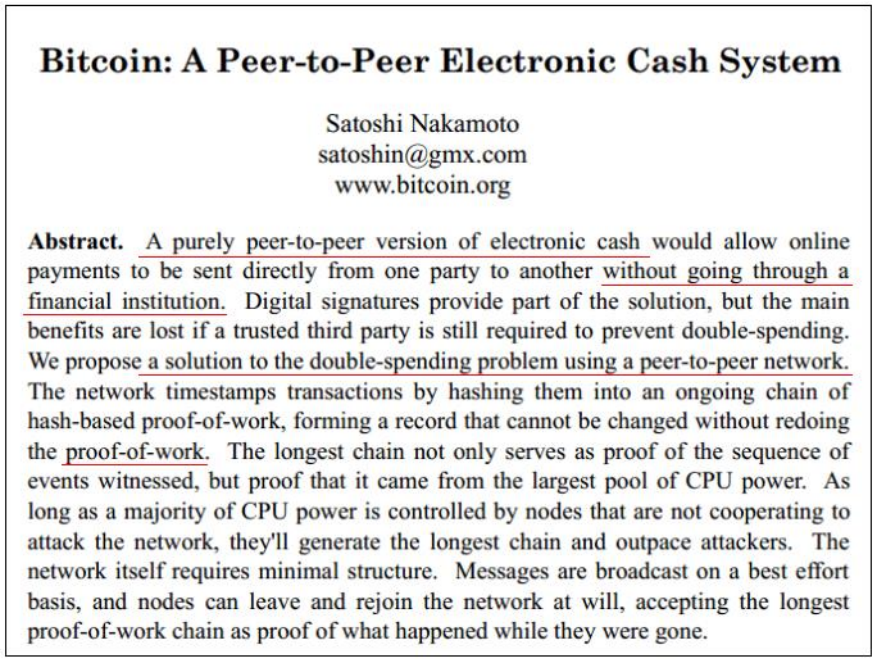
Module 0-0

한국항공대 채원부

Bitcoin Network Intro

비트코인의 탄생

- 비트코인은 2008년 10월 사토시 나카모토라는 정체 불명의 인물(혹은 그룹)이 만든 한편의 논문에서 시작 되었음
- 사토시는 이 논문을 Cypherpunk(암호학자)들의 메일링 리스트로 발송하였고, Cypherpunk들의 큰 관심을 받음
- 2009년 세계 여러 개발자들이 모여 사토시가 작성한 논문을 바탕으로 비트코인 네트워크 구현을 실현하고, 현재까지 운용 업그레이드 되기 시작함

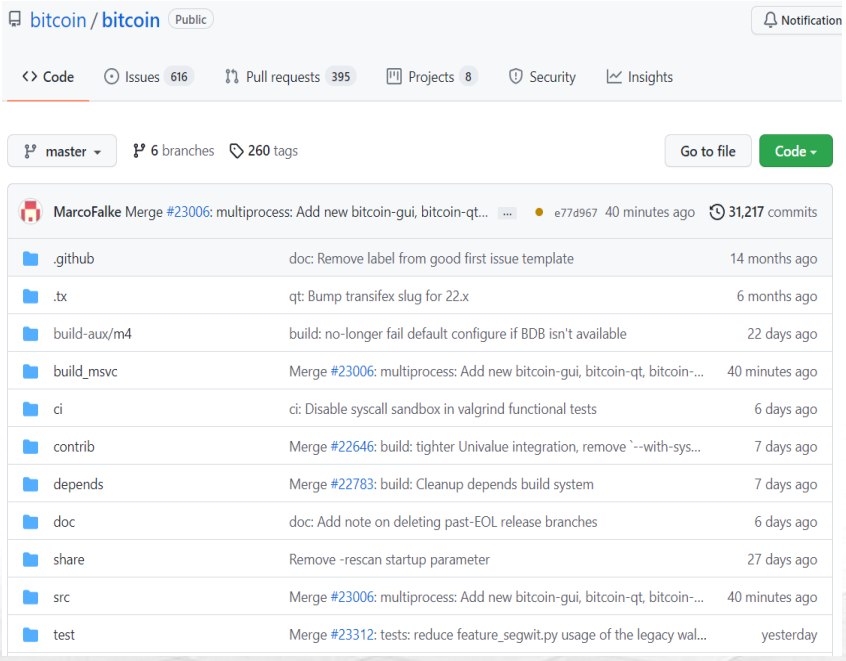


Bitcoin: A Peer-to-Peer Electronic Cash System

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.

https://bitcoin.org/bitcoin.pdf



https://github.com/bitcoin/bitcoin

Bitcoin Network Intro

비트코인 논문 주요내용

- 중앙 통제 시스템이 없는 peer-to-peer 네트워크임 (Decentralization)
- 이중 지불 문제를 방지함 (Double spending problem)
- 거래 내역은 네트워크에 공개되어 모든 노드들이 공유함 (블록체인, Blockchain)
- 네트워크의 각 노드들이 거래 원장을 검증할 수 있는 규칙(Deterministic)
- 블록체인에 저장된 거래원장을 신뢰할 수 있는 합의 시스템(Proof of Work)

금융 네트워크 설계 시 필요 조건

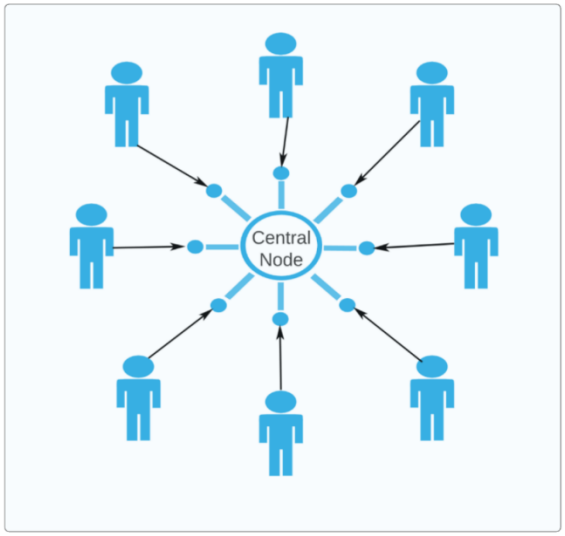
1. 돈을 전송하는 Transaction 발생 시 이를 처리해줘야 하는 “대리인” 필요
2. 거래내역이 이중 지불되지 않았음을 검증해주는 “검증자” 필요
3. 거래내역을 저장하는 “데이터베이스(DB)” 필요
4. 대리인, 검증자에 대한 “신뢰“ 필요

Bitcoin Network Intro

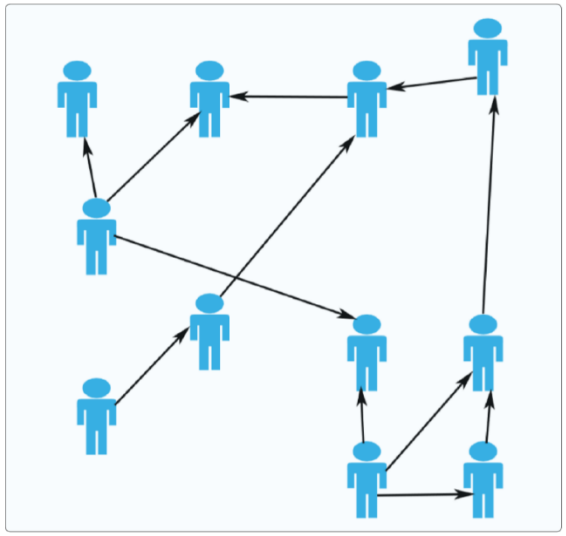
Centralized, Decentralized, Distributed Network

- 블록체인은 탈중앙화 분산 DB로서 참여한 모든 노드들이 같은 내용의 분산 공유 원장을 가지고 있고, 누구나 블록체인에 포함될 새로운 정보를 제안 할 수 있음
- 누구나 새로운 정보를 제안 할 수 있기 때문에 서로 다른 정보 중 누구의 정보를 블록체인에 포함시켜야 할지에 대한 결정인 합의 과정이 필요함
- 대다수의 블록체인은 합의하기 위해 작업증명(Proof of Work, PoW) 알고리즘을 사용함

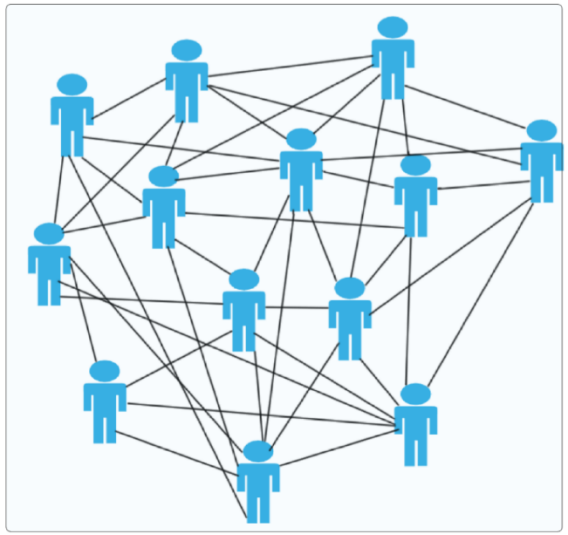
Centralized Network



Decentralized Network



Distributed Network



Bitcoin Network Intro

Centralized, Decentralized, Distributed Network

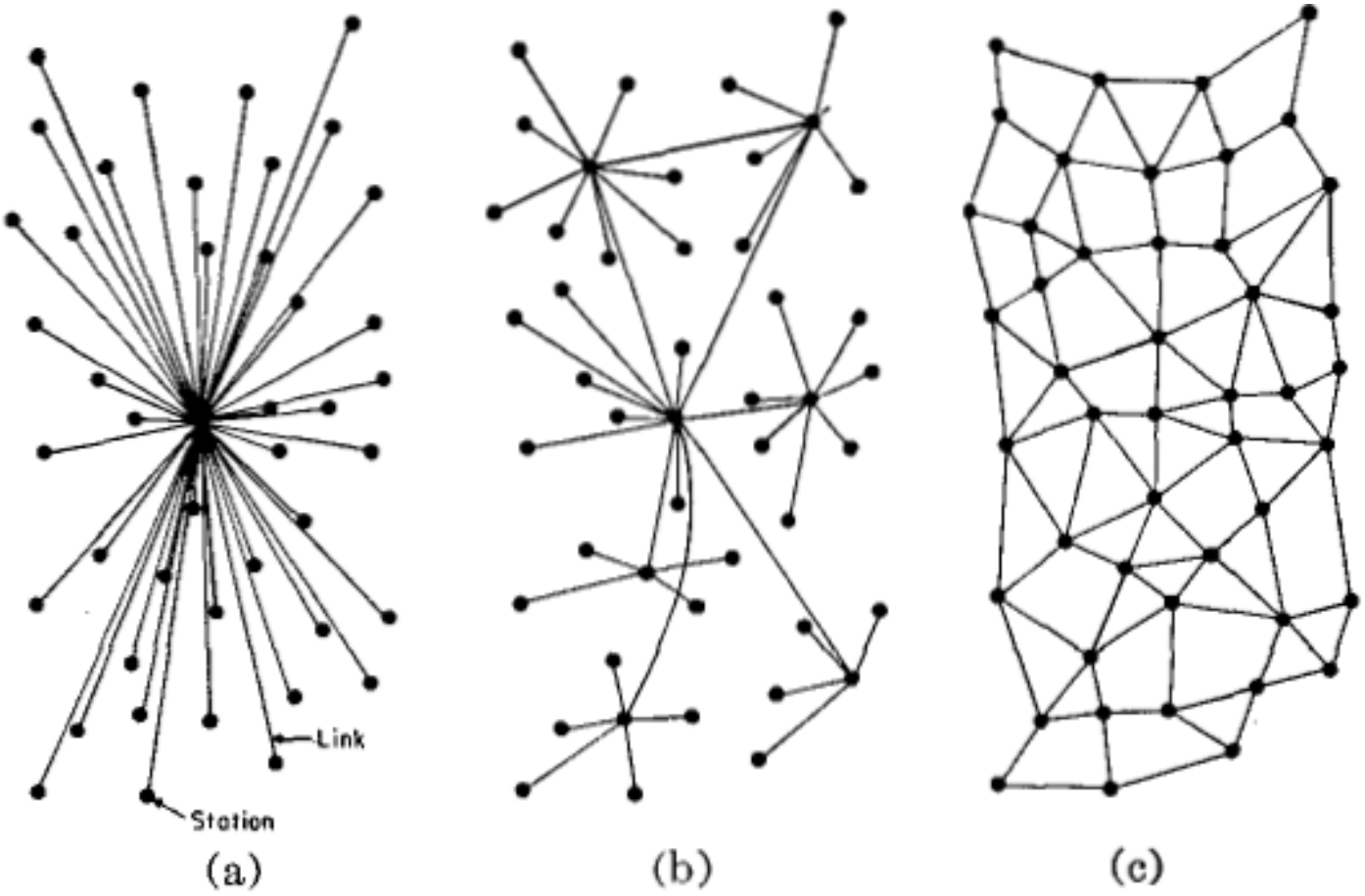
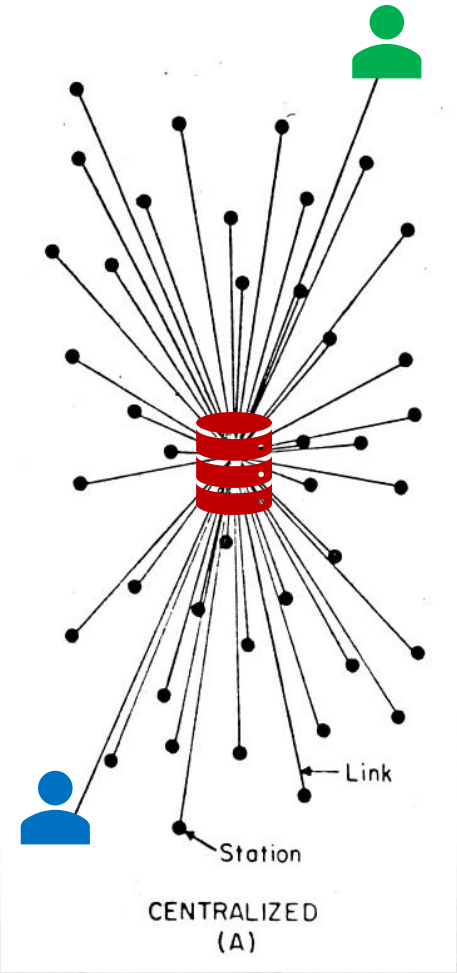


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

Bitcoin Network Intro

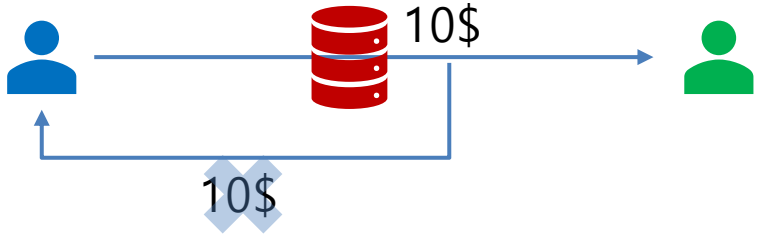
기존 금융 시스템 분석(Centralized Network)

- A 가 B 에게 10 달러를 송금하는 경우



- 기존 Centralized 서버가 Transaction 처리 대리인

- 기존 Centralized 서버가 이중지불을 방지



- 서버에 모든 거래내역 데이터를 저장
- 서버의 보안이 안전하다는 신뢰를 가져야함
  - 중앙화된 서버가 공격을 받아 해킹 당한다면?

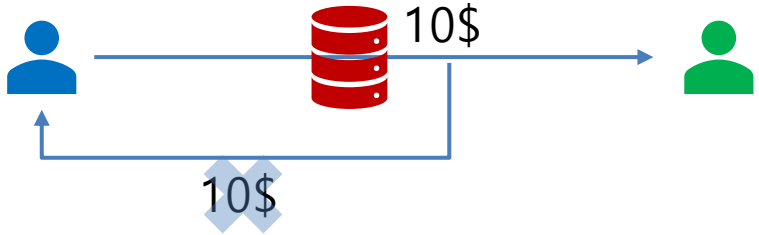
Bitcoin Network Intro

기존 금융 시스템 분석(Centralized Network)

- A 가 B 에게 10 달러를 송금하는 경우

- 기존 Centralized 서버가 Transaction 처리 대리인

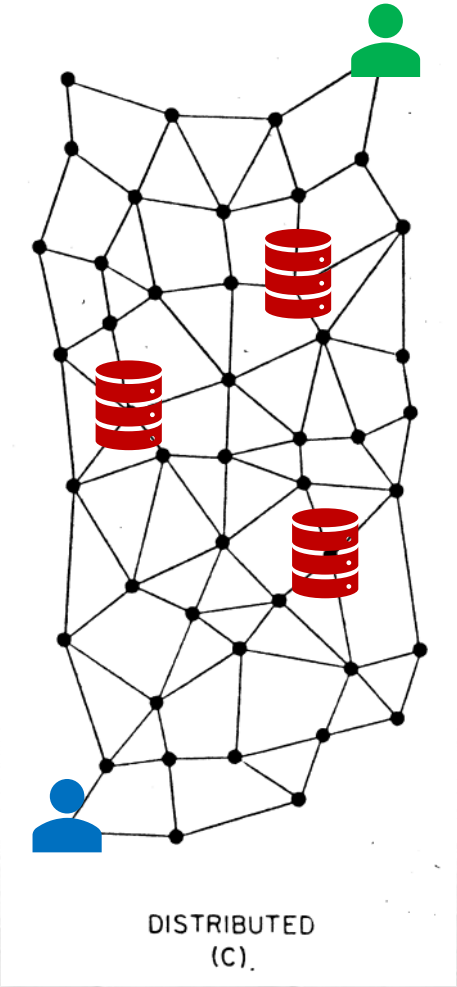
- 기존 Centralized 서버가 이중지불을 방지



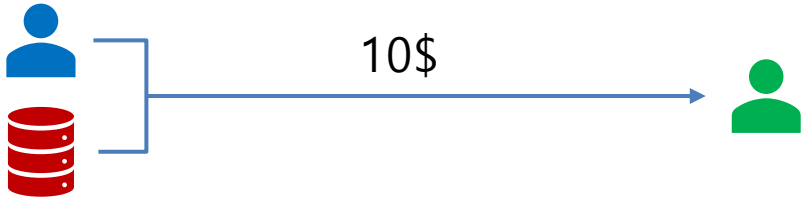
- 서버에 모든 거래내역 데이터를 저장
- 서버의 보안이 안전하다는 신뢰를 가져야함
  - 중앙화된 서버가 공격을 받아 해킹 당한다면?

Bitcoin Network Intro

- 기존 가상화폐 시스템 분석(Distributed Network)
  - A 가 B 에게 10 달러를 송금하는 경우



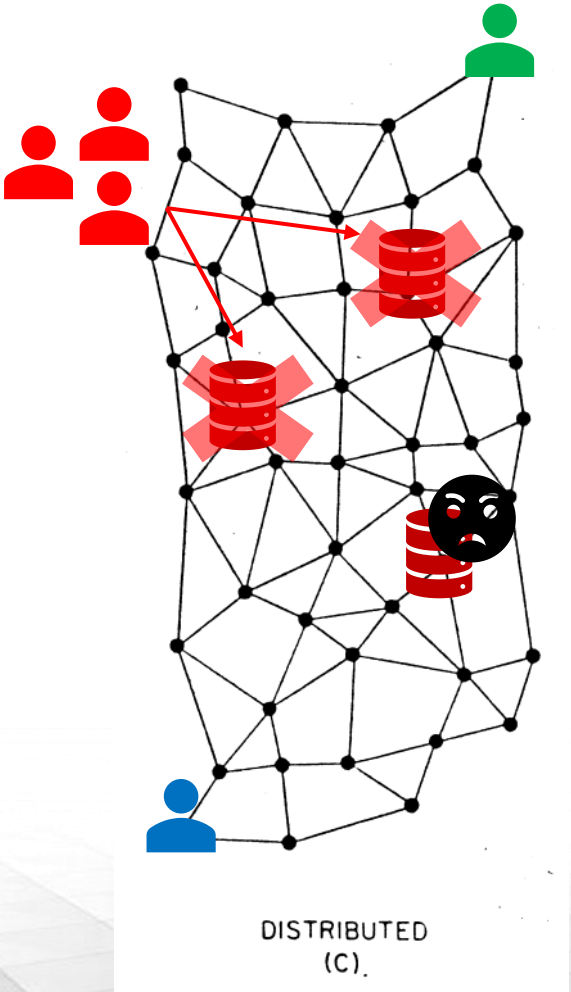
- 모든 Peer-to-Peer들이 연결되어 있고 3rd-Party 서버의 도움을 받아 함께 Transaction을 처리



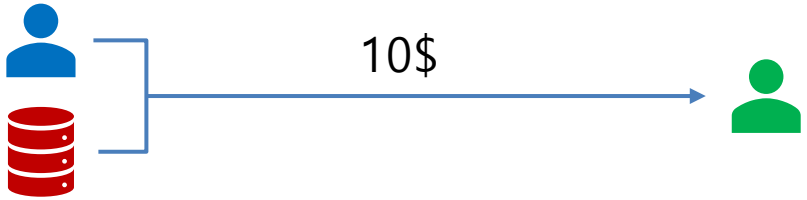
- 3rd-Party 서버가 Trusted 하다는 전제하에 금액 지불에 대한 내용을 보증
- 개인들이 모든 거래내역 데이터를 저장
- 3rd-Party 서버의 보안이 안전하다는 신뢰를 가져야함
  - 수가 적은 3rd-Party 중앙화된 서버가 공격을 받아 해킹 당한다면?
  - 3rd-Party 가 신뢰할 수 없다면?

Bitcoin Network Intro

- 기존 가상화폐 시스템 분석(Distributed Network)
  - A 가 B 에게 10 달러를 송금하는 경우



- 모든 Peer-to-Peer들이 연결되어 있고 3rd-Party 서버의 도움을 받아 함께 Transaction을 처리



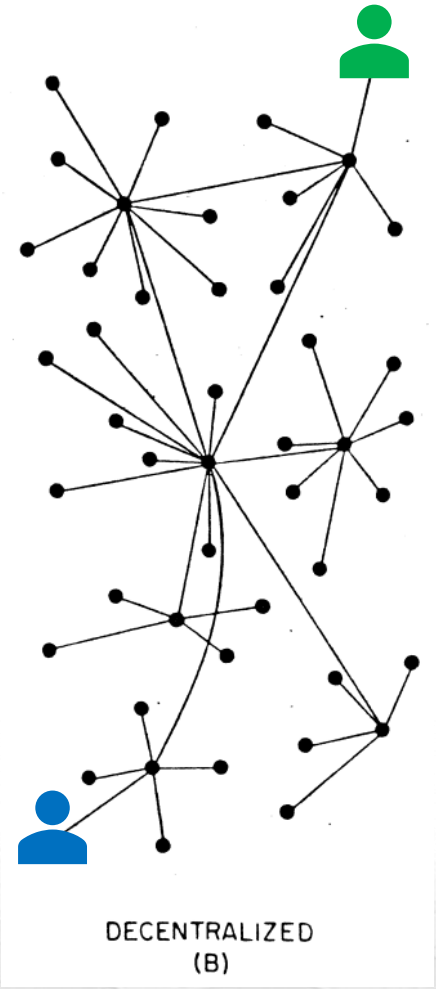
- 3rd-Party 서버가 Trusted 하다는 전제하에 금액 지불에 대한 내용을 보증

- 개인들이 모든 거래내역 데이터를 저장
- 3rd-Party 서버의 보안이 안전하다는 신뢰를 가져야함
  - 수가 적은 3rd-Party 중앙화된 서버가 공격을 받아 해킹 당한다면?
  - 3rd-Party 가 신뢰할 수 없다면?

Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

- A 가 B 에게 10 달러를 송금하는 경우

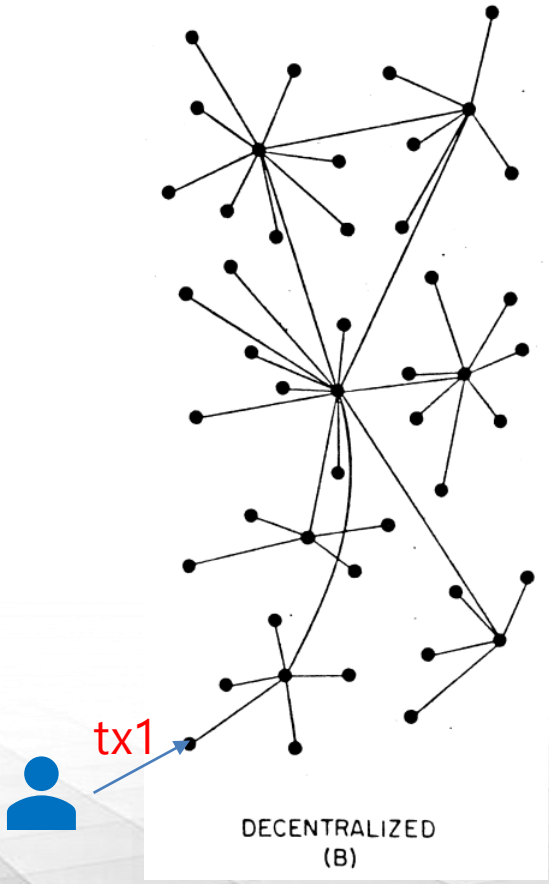


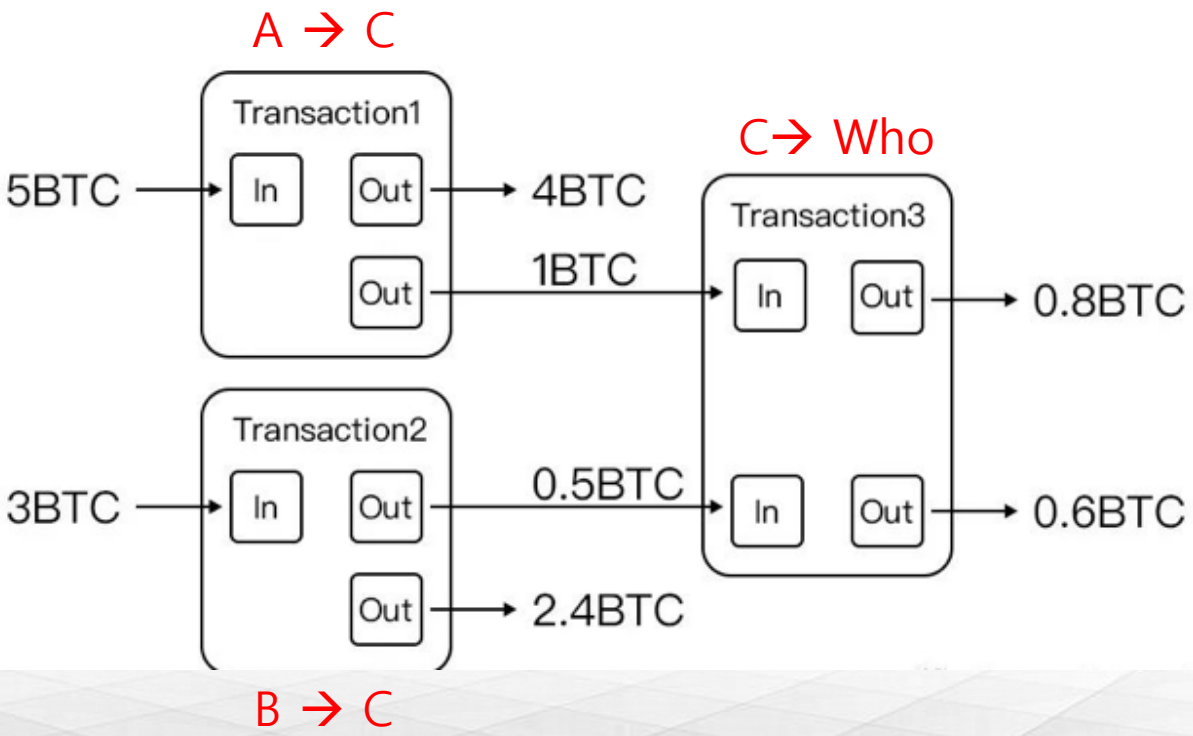
- 모든 Peer to Peer들이 연결되어 있고, 기존 Transaction을 처리해주는 "중앙화된 서버"가 없다.
  - (중앙을 찾을 수 없다 = Decentralied)
  - Transaction 을 처리해주는 대리인 필요
- 이중 지불을 방지해주는 Centralized Server가 없다
  - Transaction을 검증해주는 검증자 필요
  - 검증할 수 있는 규칙이 필요(해시 : HASH & 머클트리)
- 개인(노드)들이 모든 거래내역 데이터를 저장
  - 분산원장에 같은 데이터를 저장
- 대리인, 검증자에 대한 "신뢰" 필요
  - 작업증명 : Proof of Work

Bitcoin Network Intro

비트코인 은 존재 하는가?

- 정답은 없다. 비트코인은 JSON 파일 속에 들어있는 문자열이다.
- 문자열 사용 기록이 이어져 있는게 블록체인

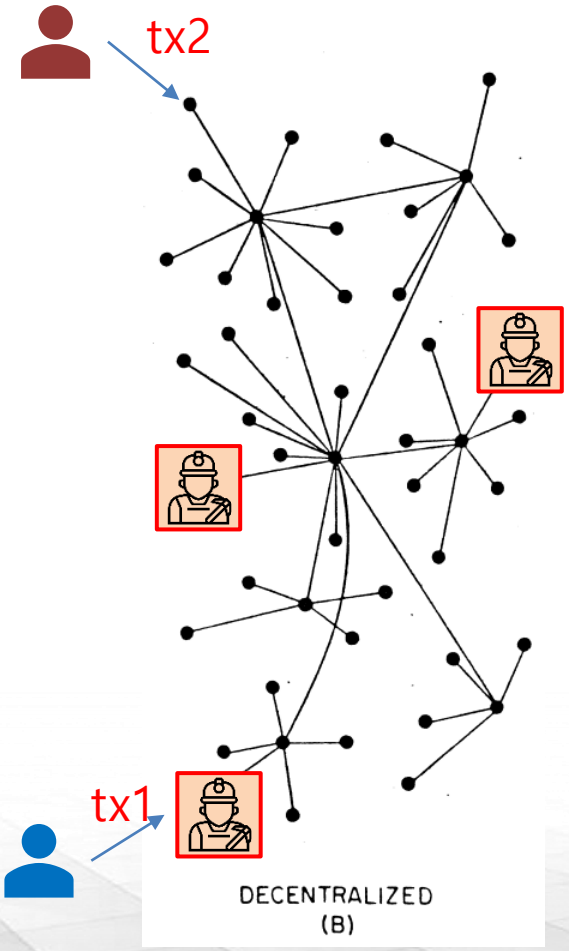


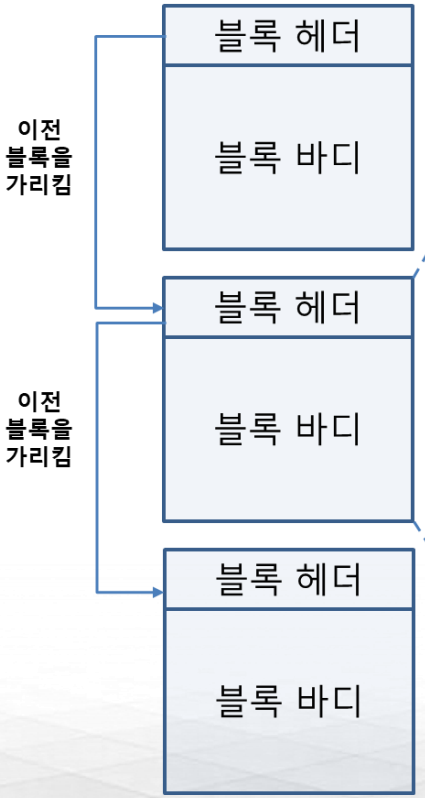


Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

비트코인 트랜잭션 생성





Version(4bytes)	현대버전	20400000
Previous Block Header Hash(32)	이전블록을 체인으로 연결하는 포인터	00000000000000002d1233fdsx23124312
Merkle Root(32)	**트랜잭션을 요약한 정보**	**5082jsn13kodjsmn3k2m2d5fklsm**
Timestamp(4)	블록생성시간	5c33093b08
Bits(4)	채굴의 난이도	172sa24d45
Nonce(4)	논스값	c567sd143c

머클트리 : 요약정보

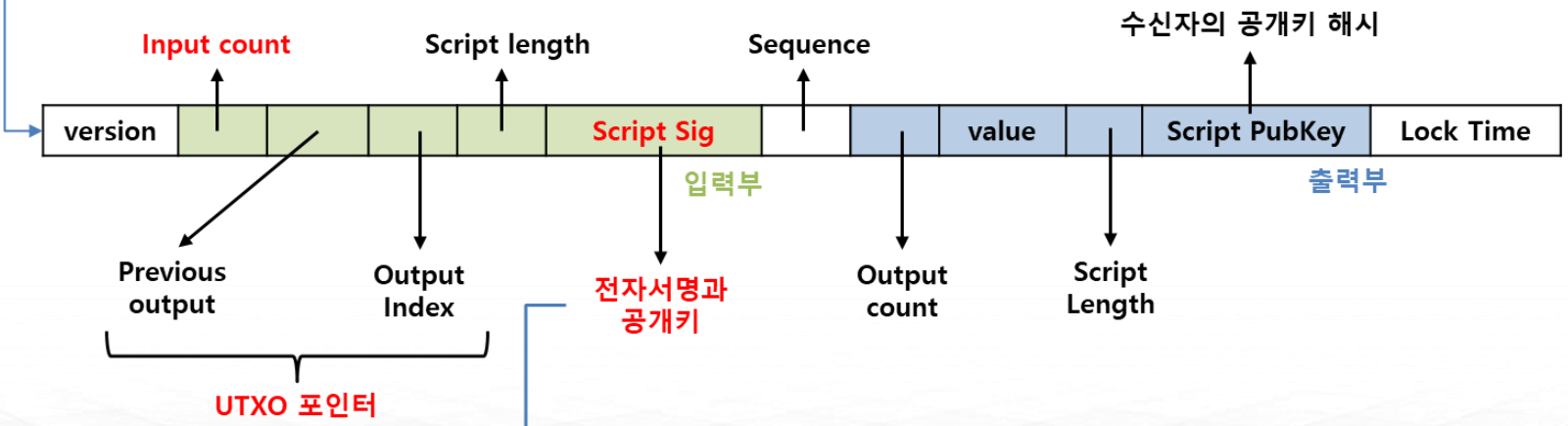
Transaction count(4)	블록바디에 들어있는 트랜잭션 수	0536
Coinbase transaction		
Transaction #1		
Transaction #2		
.....		
Transaction #133		

Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

비트코인 트랜잭션 생성

Transaction count(4)	블록바디에 들어있는 트랜잭션 수	0536
Coinbase transaction		
Transaction #1		
Transaction #2		
.....		
Transaction #133		



- 입력부 스크립트의 내용.
- 전자서명과 공개키를 포함해 서명을 검증 할 수 있는 데이터가 들어있음,
- UTXO의 자물쇠를 푼다는 의미로 언로킹(unlocking) 스크립트라 한다.

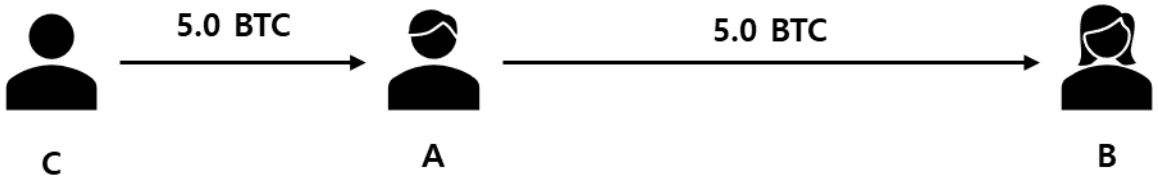
Bitcoin Network Intro

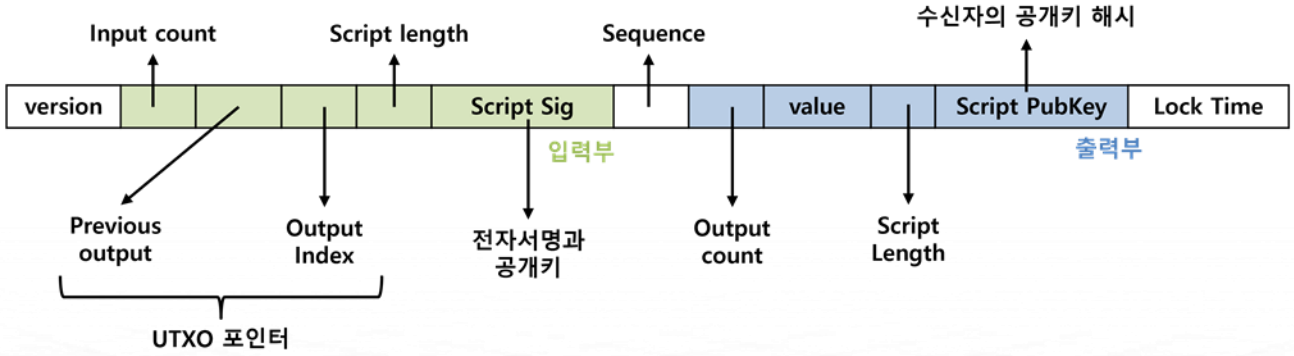
비트코인 시스템 분석(Decentralized Network)

- 비트코인 트랜잭션 생성

A라는 사람이 B라는 사람에게 5.0 BTC를 보내고자 함

- A 가 가지고 있는 5.0 BTC 가 하나의 입력부에 저장되어 있는 주소라면(C로 부터 받은 UTXO)
  “Prev output~Script Sig” 배열이 하나다!





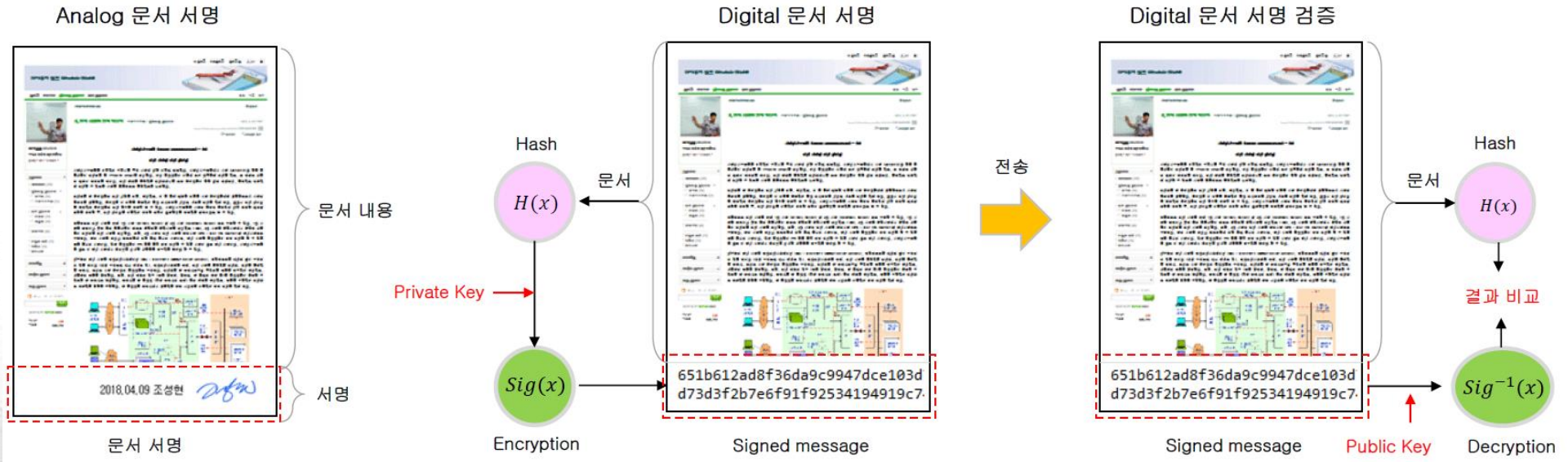
version	1	C의 5 BTC Tx 주소	1	*C	Sig-r(c), Sig-s(c), Pub(A)c		1	5.0 BTC (사토시)	*C	H(Pub(A)), OP_Code	Lock Time

Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

- 1) User는 본인의 Private Key로 TX에 대한 Hash값을 암호화
- 2) 다른 사람들은 서명한 사람의 Public Key로 암호문(전자 서명)을 풀 수 있고, 문서의 Hash 값을 계산한 후 전자서명과 비교
- 3) 비교시 일치 한다면 해당 문서는 서명자가 작성한 것이라는게 증명됨

- 비트코인 네트워크에서는 지갑의 소유자가 자신의 Private Key로 TX를 서명하는 절차가 필요함 → ECDSA (ECC기반 전자 서명 방식)



Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

- Miner 가 tx를 검증 해야함 = ECDSA(Eliptic Curve Digital Signature Algorithm)

<ECC 표준 문서에 정의된 도메인 파라미터>
P = Prime number
G = Generator
n = order of G

d ∈ {2, 3, …., n-1}
Q(서명자의 공개키) = d*G

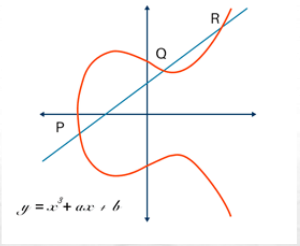
K ∈ {2, 3, …., n-1}
(x, y) =k*G

Sig-r = x
Sig-s ={h(m)+d*r}*(k^-1) mod n

디지털 문서 서명자

전자서명(Sig-r, Sig-s)을 만듬

- M (문서, A가 B에게 5BTC 보냄)
- Q (서명자의 공개키)
- Sig-r (ecc의 x좌표)
  → y좌표는 바로 대응됨
- Sig-s (전자서명 해시한 값)



w = (Sig-s)^-1 mod n
u1 = w*h(m) mod n
u2 = w*r mod n
(x, y) = u1*G + u2*Q
→ X 를 직접 계산함

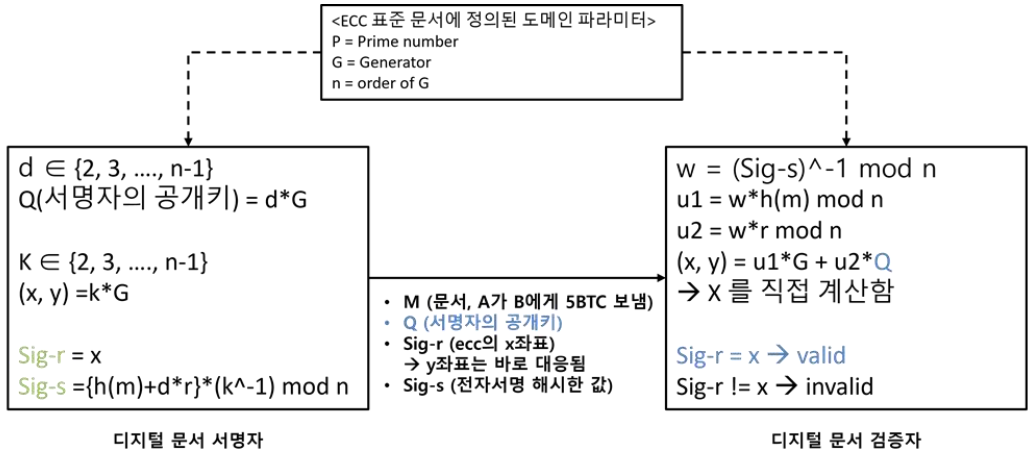
Sig-r = x → valid
Sig-r != x → invalid

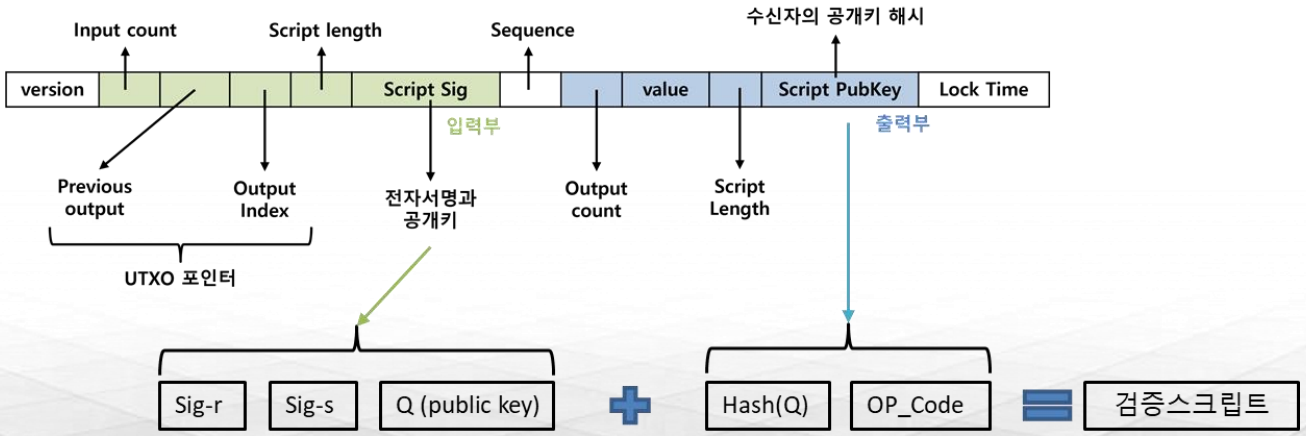
디지털 문서 검증자

Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

Miner 가 tx를 검증 해야함 = ECDSA(Eliptic Curve Digital Signature Algorithm)





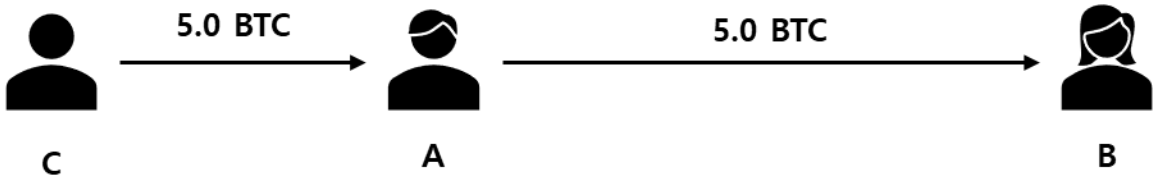
Bitcoin Network Intro

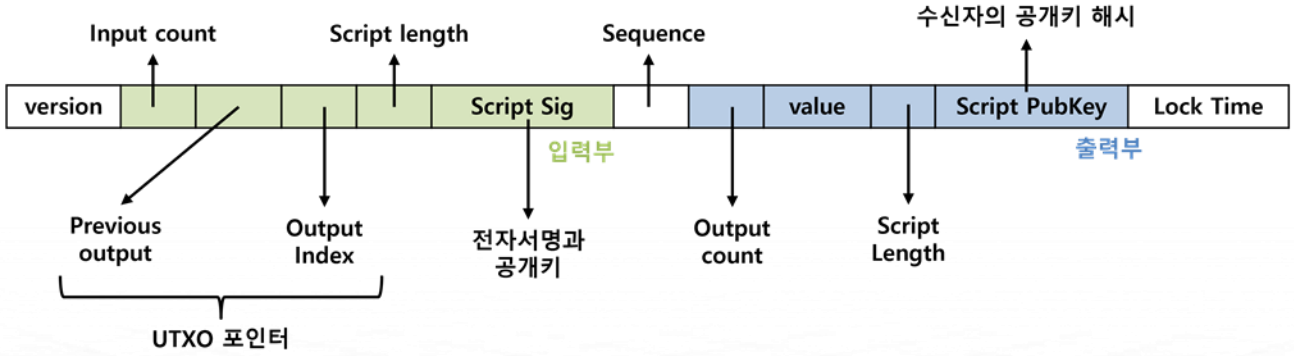
비트코인 시스템 분석(Decentralized Network)

- 비트코인 트랜잭션 생성

A라는 사람이 B라는 사람에게 5.0 BTC를 보내고자 함

- A 가 가지고 있는 5.0 BTC 가 하나의 입력부에 저장되어 있는 주소라면(C로 부터 받은 UTXO)
  “Prev output~Script Sig” 배열이 하나다!



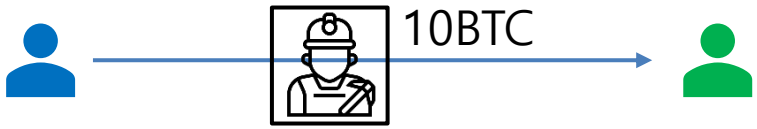


version	1	C의 5 BTC Tx 주소	1	*C	Sig-r(c), Sig-s(c), Pub(A)c		1	5.0 BTC (사토시)	*C	H(Pub(A)), OP_Code	Lock Time

Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

- A 가 B 에게 10BTC를 송금하는 경우



Miner(채굴자)

- User의 Transaction 을 처리해주는 “대리인” (기존 서버의 역할)
- Transaction 을 처리해주면 보상(12.5btc)을 획득 (네트워크 참여를 위해)
- 대리인의 자격을 공평하게 가지는 방법 = 작업증명 (Proof of Work; PoW)

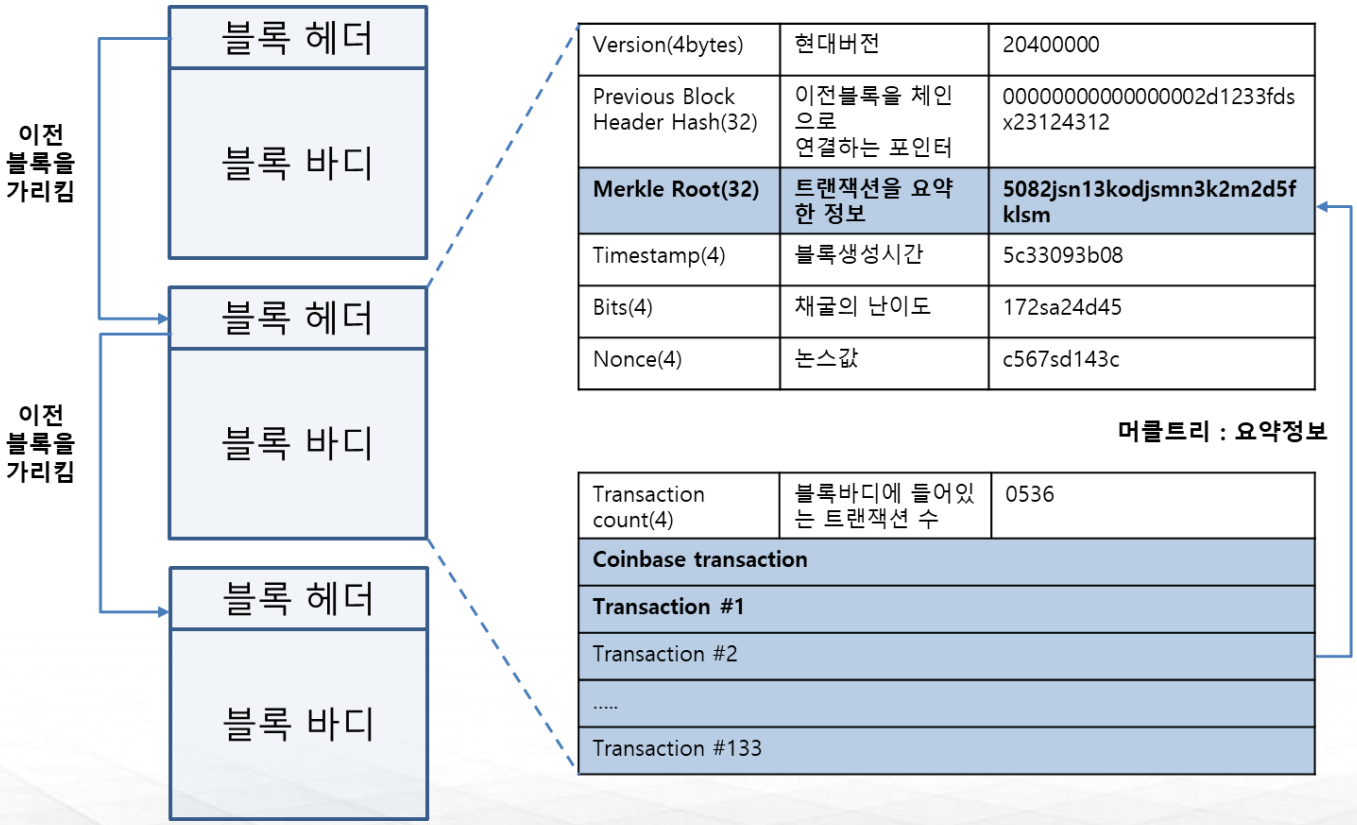
개인 Miner 가 처리한 Transaction 검증과정 필요

- 탈중앙화 네트워크에서 서로 다른 Peer들이 이중지불이 안되었다는 공통의 검증(합의) 필요
- 분산원장 = 모든 노드들이 같은 내용의 데이터를 가짐
- 해시(HASH) = Miner가 처리한 TX Block이 올바르다는 것을 모두가 검증하는 과정

Bitcoin Network Intro

비트코인 시스템 분석(Decentralized Network)

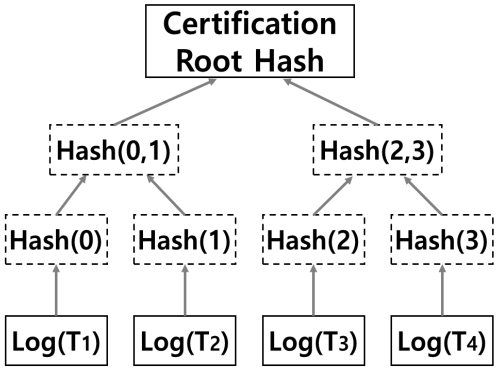
비트코인 트랜잭션 생성



Version(4bytes)	현대버전	20400000
Previous Block Header Hash(32)	이전블록을 체인으로 연결하는 포인터	00000000000000002d1233fds x23124312
Merkle Root(32)	**트랜잭션을 요약한 정보**	**5082jsn13kodjsmn3k2m2d5f klsm**
Timestamp(4)	블록생성시간	5c33093b08
Bits(4)	채굴의 난이도	172sa24d45
Nonce(4)	논스값	c567sd143c

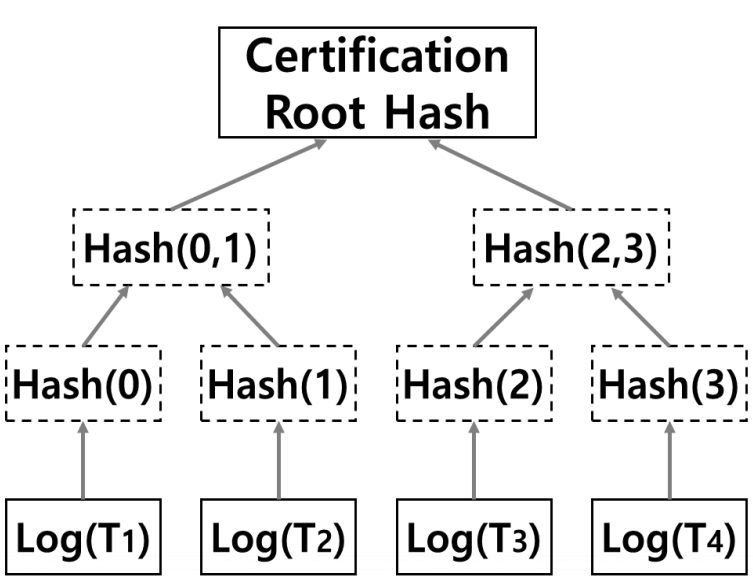
머클트리 : 요약정보

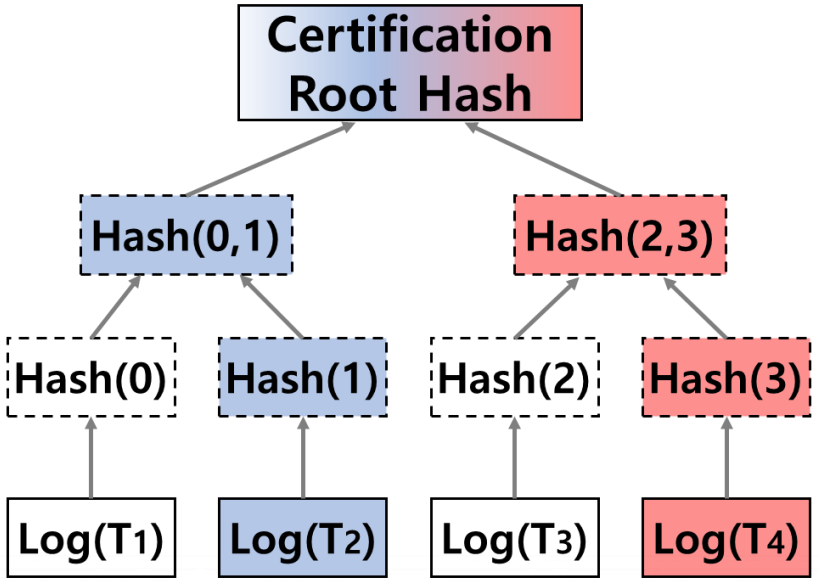
Transaction count(4)	블록바디에 들어있는 트랜잭션 수	0536
Coinbase transaction		
Transaction #1		
Transaction #2		
.....		
Transaction #133		



Bitcoin Network Intro

- 비트코인 시스템 분석(Decentralized Network)
  - 머클트리 실습





Proof of Work

연결할 수 있는(블록생성) 권한획득

- Hash(Version + Prev Block Hash + Merkle Root +Timestamp + Bits + **Nonce**) < Target
- Hash(20400000 + 0000000000000002d1233fdsx23124312 + **5082jsn13kodjsmn3k2m2d5fklsm** + 5c33093b08 + 172sa24d45 + **Nonce**) < Target
- **이걸 만족한 Nonce값을 찾는 마이너에게 블록생성 권한을 줌**
  http://www.bagill.com/text-converter.php

Hash	00000000000000000005c0a28631ba795a1b34511b4db2a3e12f42272efd84d7
Confirmations	1
Timestamp	2021-10-27 11:24
Height	706874
Miner	AntPool
Number of Transactions	28
Difficulty	20,082,460,130,830.84
Merkle root	2cec11f12d7d42521fd55f39b6560963ccee82230fb4c881b495eeb137dacba5

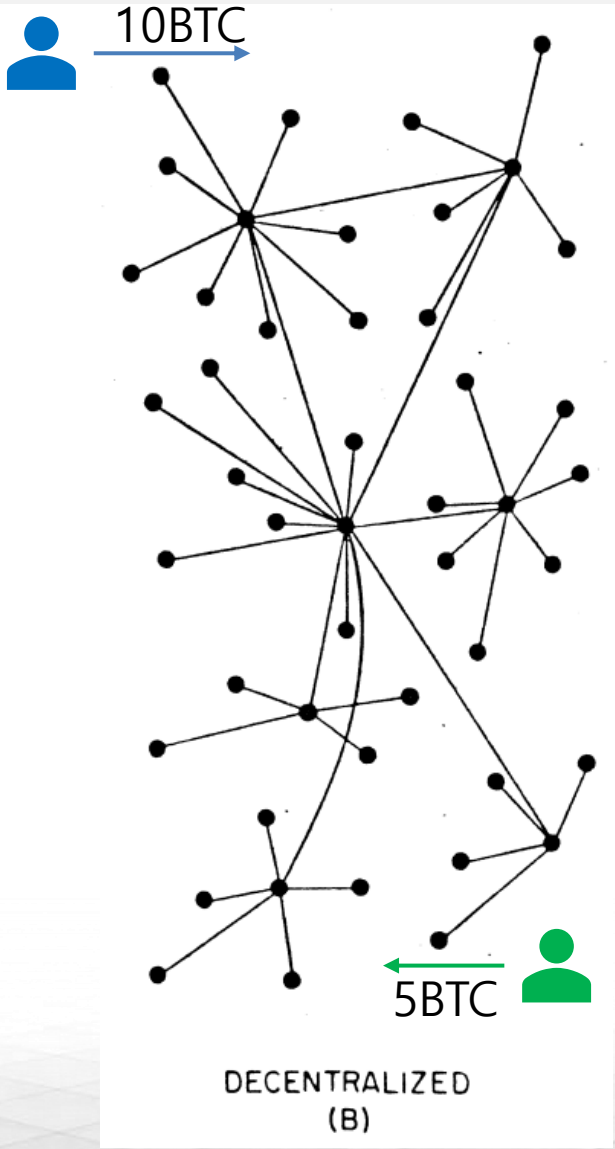
Proof of Work

작업증명(Proof of Work)

- 거래 1 : A 가 B 에게 10BTC를 송금
- 거래 2 : C 가 D 에게 5BTC를 송금

작업증명(PoW) 과정

- User A, C는 블록체인 네트워크로 처리하고자 하는 TX 를 전송
- 블록체인에 연결된 노드들은 인접한 노드들에게 받은 TX를 전송
- 블록체인상 모든 Full노드(Miner) 에게 TX가 전파됨



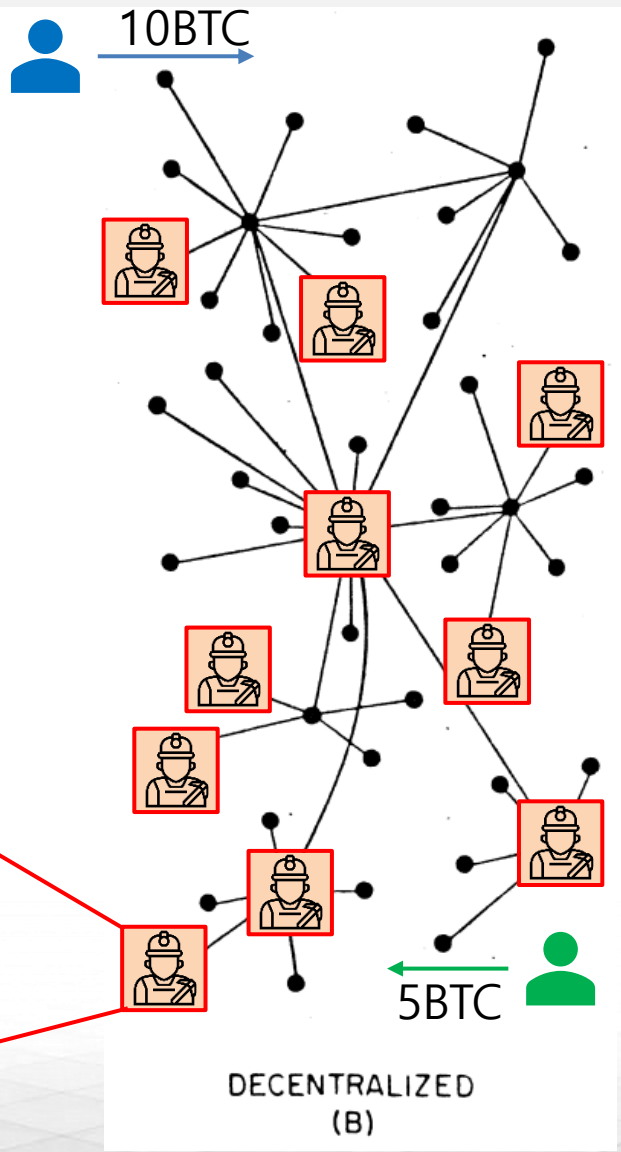
Proof of Work

작업증명(Proof of Work)

- 거래 1 : A 가 B 에게 10BTC를 송금
- 거래 2 : C 가 D 에게 5BTC를 송금

작업증명(PoW) 과정

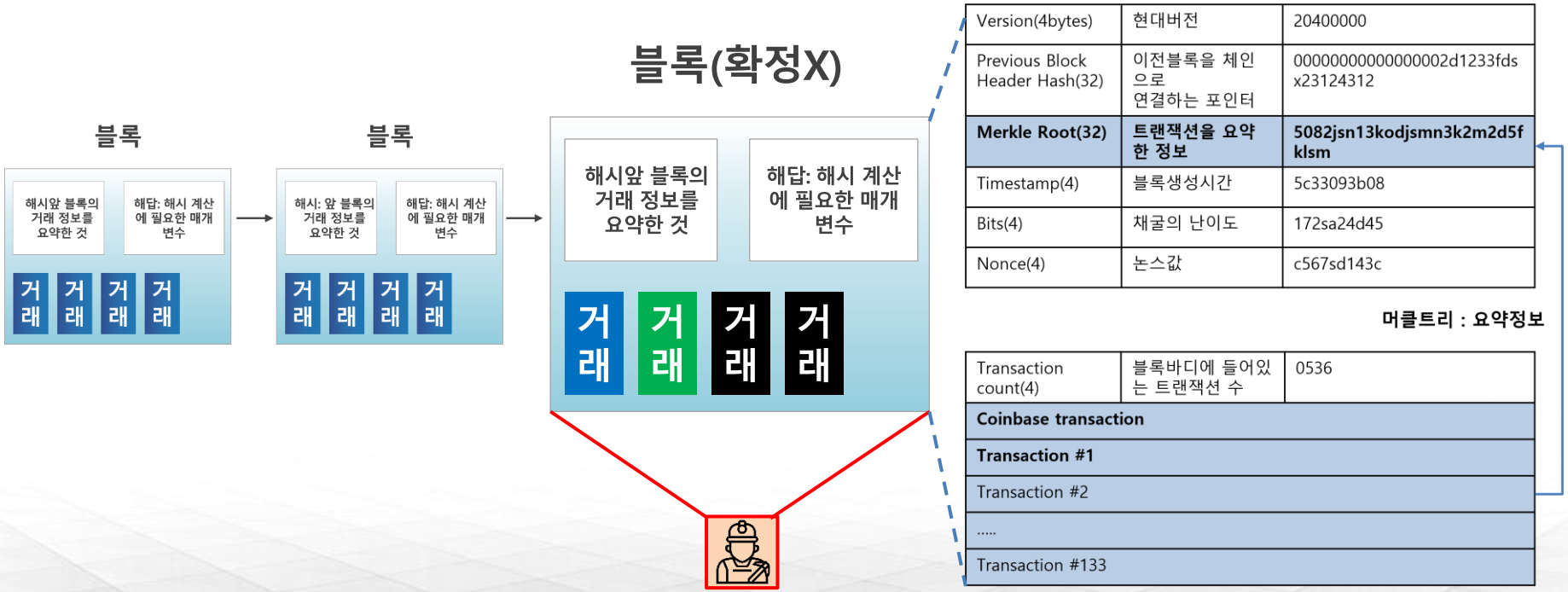
- 블록체인상 모든 Full노드(Miner) 에게 TX가 전파됨
- Miner들은 전파 받은 Transaction을 자신의 local mempool(컴퓨터)에 담아 블록을 생성



Proof of Work

작업증명(Proof of Work)

- 블록체인상 모든 Full노드(Miner) 에게 TX가 전파됨
- Miner들은 전파 받은 Transaction을 자신의 local mempool(컴퓨터)에 담아 블록을 생성
- Miner들은 보상을 받고 TX를 처리하기 위해 기존 블록체인에 자신이 만든 블록을 연결하기 원함!



Proof of Work

작업증명(Proof of Work)

- 블록체인상 모든 Full노드(Miner) 에게 TX가 전파됨
- Miner들은 전파 받은 Transaction을 자신의 local mempool(컴퓨터)에 담아 블록을 생성
- Miner들은 보상을 받고 TX를 처리하기 위해 기존 블록체인에 자신이 만든 블록을 연결하기 원함!

연결할 수 있는(블록생성) 권한과 생성된 블록 검증

- 중앙화된 "대리인"이 없기 때문에 TX를 처리할 수 있는 권한(블록생성 권한)을 공평하게 획득해야 한다.
- 공평하게 블록생성 권한을 획득하는 방법 = 작업증명(Proof of Work)
- 권한을 획득한 Miner가 생성한 블록을 모든 노드가 검증 가능 해야한다.
  결정론적 방법(Deterministic) = 해시 HASH

Proof of Work

연결할 수 있는(블록생성) 권한획득

- Hash(Version + Prev Block Hash + Merkle Root +Timestamp + Bits + **Nonce**) < Target
- Hash(20400000 + 0000000000000002d1233fdsx23124312 + **5082jsn13kodjsmn3k2m2d5fklsm** + 5c33093b08 + 172sa24d45 + **Nonce**) < Target
- **이걸 만족한 Nonce값을 찾는 마이너에게 블록생성 권한을 줌**
  http://www.bagill.com/text-converter.php

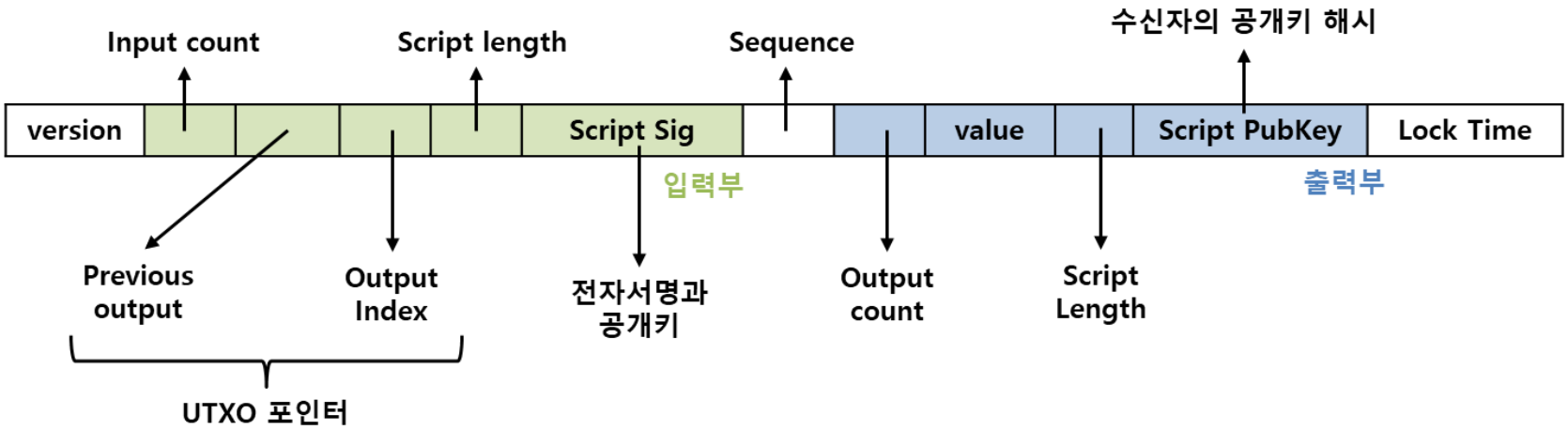
Hash	00000000000000000005c0a28631ba795a1b34511b4db2a3e12f42272efd84d7
Confirmations	1
Timestamp	2021-10-27 11:24
Height	706874
Miner	AntPool
Number of Transactions	28
Difficulty	20,082,460,130,830.84
Merkle root	2cec11f12d7d42521fd55f39b6560963ccee82230fb4c881b495eeb137dacba5

Proof of Work

- 연결할 수 있는(블록생성) 권한획득
  - Hash(Version + Prev Block Hash + Merkle Root +Timestamp + Bits + **Nonce**) < Target
  - Hash(20400000 + 0000000000000002d1233fdsx23124312 + **5082jsn13kodjsmn3k2m2d5fklsm** + 5c33093b08 + 172sa24d45 + **Nonce**) < Target
  - **이걸 만족한 Nonce값을 찾는 마이너에게 블록생성 권한을 줌**
    http://www.bagill.com/text-converter.php
  - 검증은 다른 노드들이 Nonce값을 넣어 보기만 하면 검증 완료

Hash	00000000000000000005c0a28631ba795a1b34511b4db2a3e12f42272efd84d7
Confirmations	1
Timestamp	2021-10-27 11:24
Height	706874
Miner	AntPool
Number of Transactions	28
Difficulty	20,082,460,130,830.84
Merkle root	2cec11f12d7d42521fd55f39b6560963ccee82230fb4c881b495eeb137dacba5

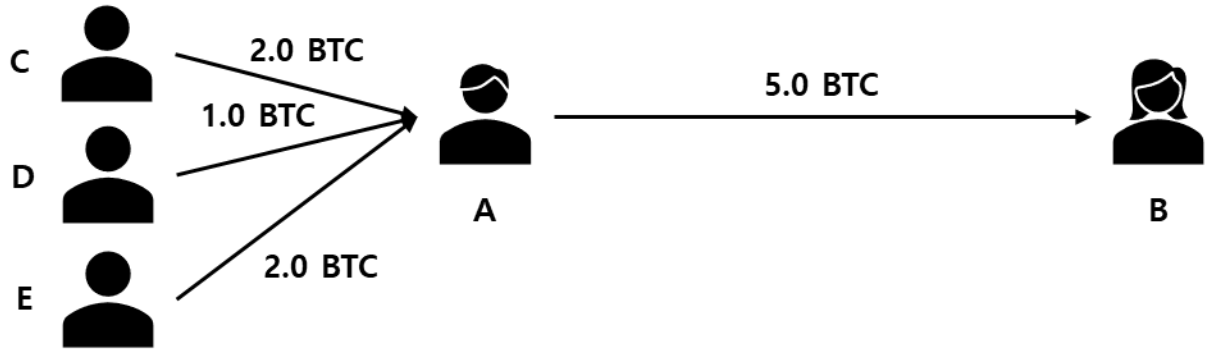
비트코인이 느려터진 이유

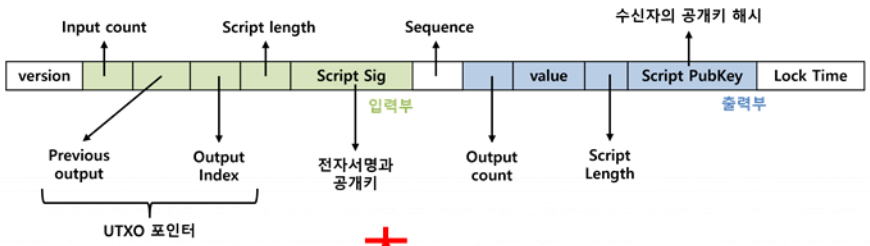


Version	트랜잭션의 버전
Input count(4)	입력부의 개수(입력부는 여러 개 있을 수 있다)
Previous output(C)	이전 출력부의 트랜잭션 ID
Output index(32)	이전 출력부들 중 잔액을 사용할 출력부 번호
Script length(C)	입력부 스크립트의 길이
Script Sig(Var)	입력부 스크립트의 내용, 전자서명과 공개키를 포함해 서명을 검증할 수 있는 데이터가 들어있다.
Sequence(4)	현재는 쓰이지 않는 시퀀스 번호(0xffffffff)
Ouput count(C)	출력부의 개수(여러 사람에게 송금하는 경우 여러 개의 출력부가 존재할 수 있음
Value(8)	송금할 금액 단위=1사토시(Satoshi), 1btc= 10^8사토시, 1사토시는 트랜잭션의 최소단위
Script length(C)	출력부 스크립트의 내용
Script Pubkey(Var)	수신자의 공개키 해시 값
Lock Time(4)	채굴자가 이 트랜잭션을 언제 선택 할 수 있는지 표시 (0이면 아무때나 사용가능),트랜잭션 지연시킬때 사용함

비트코인이 느려터진 이유

- 입력부가 여러 개일 때는 Previous output부터 Script Sig가 여러 번 반복된다 (배열구조)
- Var = 가변크기, 전자서명의 크기는 트랜잭션마다 달라질 수 있음
- A라는 사람이 B라는 사람에게 5.0 BTC를 보내고자 함
  - A 가 가지고 있는 5.0 BTC 가 여러 사람에게 받은 거여서 입력부가 여러 개라면?





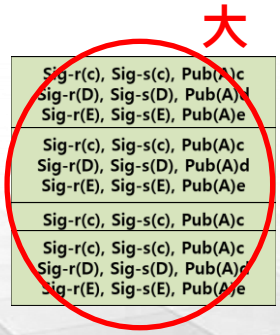
大

version	1	C의 2 BTC Tx 주소 D의 1 BTC Tx 주소 E의 2 BTC Tx 주소	1 2 3	*C	Sig-r(c), Sig-s(c), Pub(A)c Sig-r(D), Sig-s(D), Pub(A)d Sig-r(E), Sig-s(E), Pub(A)e		1	5.0 BTC (사토시)	*C	H(Pub(A)c), OP_Code H(Pub(A)d), OP_Code H(Pub(A)e), OP_Code	Lock Time

- 5.0 BTC 를 보내는데 TX 의 서명 부분이 가변크기라 너무 커진다

비트코인이 느려터진 이유

- 지갑에 1BTC 가 있는데 10개의 주소에 0.1BTC 가 나눠져 있는 경우에 0.95 BTC를 보내려고 한다면?
  - 트랜잭션은 10개의 Input과 1개의 Output으로 구성됨
  - 10개에 해당되는 전자서명이 너무 많은 크기를 차지함



A→B 10 BTC 보내는 서명

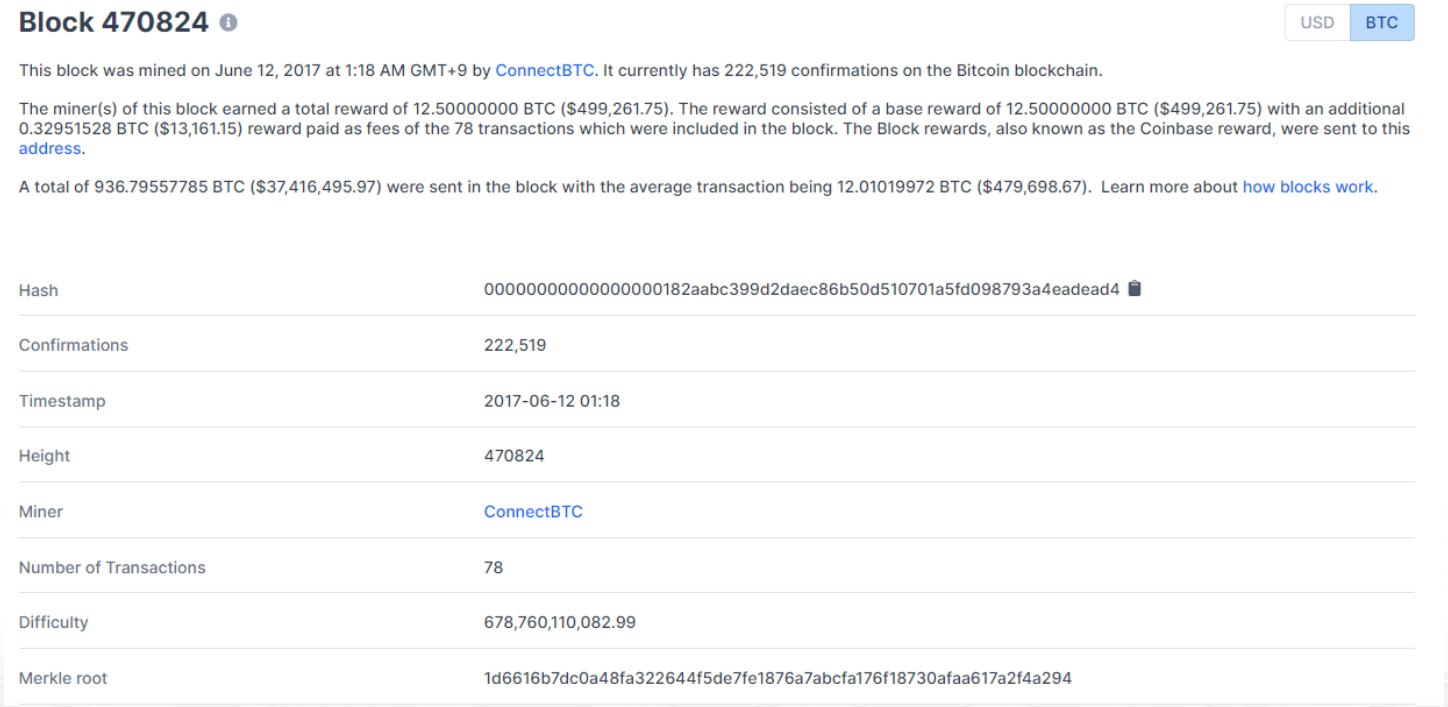
Version(4bytes)	현대버전	20400000
Previous Block Header Hash(32)	이전블록을 체인으로 연결하는 포인터	00000000000000002d1233fdsx23124312
Merkle Root(32)	**트랜잭션을 요약한 정보**	**5082jsn13kodjsmn3k2m2d5fklsm**
Timestamp(4)	블록생성시간	5c33093b08
Bits(4)	채굴의 난이도	172sa24d45
Nonce(4)	논스값	c567sd143c

머클트리 : 요약정보

Transaction count(4)	블록바디에 들어있는 트랜잭션 수	0536
Coinbase transaction		
Transaction #1		
Transaction #2		
.....		
Transaction #133		

스팸어택에 대한 저항력

- 2017년 6월 17일에 있었던 아래의 블럭은 1메가 한계가 꽉 찼는데 고작 78개의 트랜잭션 만을 가지고 있었음
  - 전자서명 필드가 너무 커짐
  - 이를 해결하기 위해 적용된 기술
    (2017 = Segwit(비트코인 하드포크), (2021/11월 = Taproot(영지식 Shnorr적용)



Block 470824

USD BTC

This block was mined on June 12, 2017 at 1:18 AM GMT+9 by ConnectBTC. It currently has 222,519 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 12.50000000 BTC ($499,261.75). The reward consisted of a base reward of 12.50000000 BTC ($499,261.75) with an additional 0.32951528 BTC ($13,161.15) reward paid as fees of the 78 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 936.79557785 BTC ($37,416,495.97) were sent in the block with the average transaction being 12.01019972 BTC ($479,698.67). Learn more about how blocks work.

Hash	00000000000000000182aabc399d2daec86b50d510701a5fd098793a4eadead4
Confirmations	222,519
Timestamp	2017-06-12 01:18
Height	470824
Miner	ConnectBTC
Number of Transactions	78
Difficulty	678,760,110,082.99
Merkle root	1d6616b7dc0a48fa322644f5de7fe1876a7abcfa176f18730afaa617a2f4a294

감 사 합 니 다

한국항공대학교