



# 블록체인 및 관련 기술 설명

# 블록체인이란?

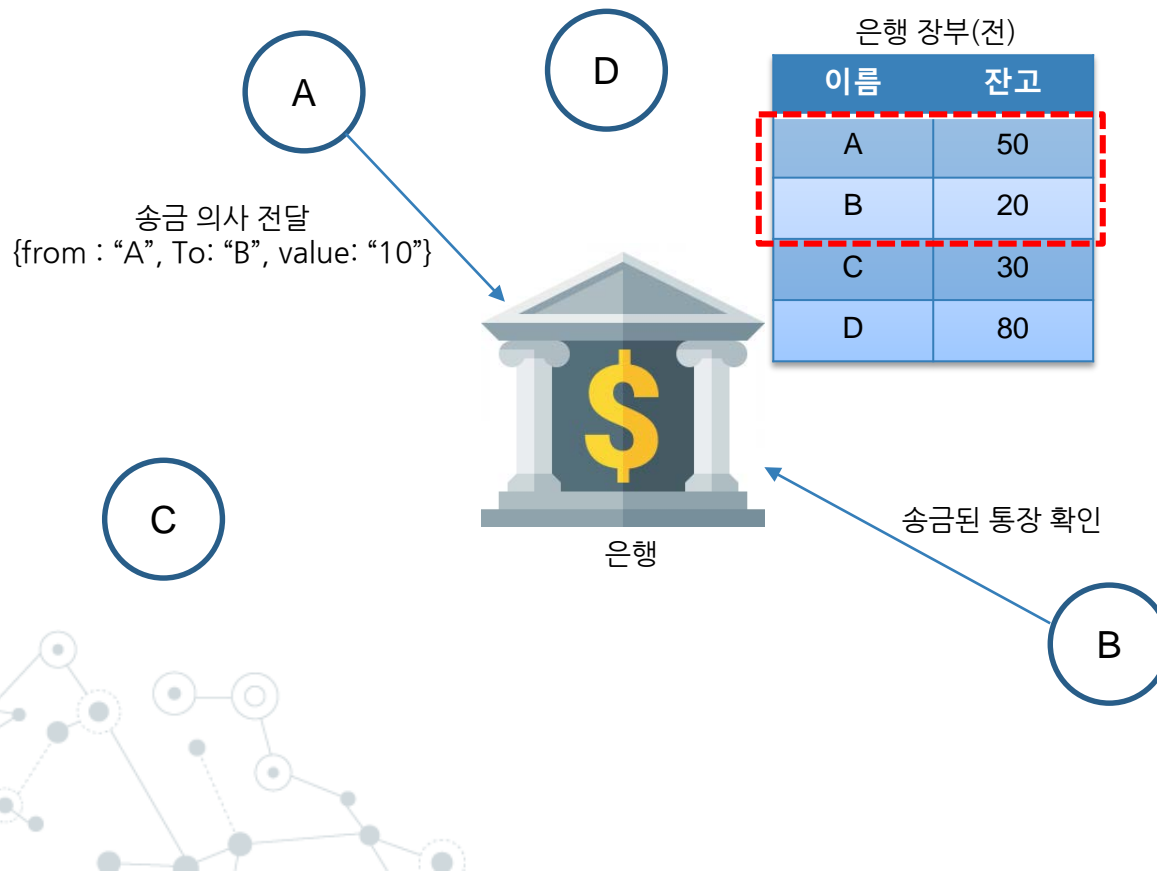
제3자의 개입없이(**Decentralized**) 네트워크의 참여자에 의해 모든  
이력을 투명하게 추적이 가능하도록 하며 이를 높은  
신뢰성(**Trustless**)으로 실현하기 위한 기술

# 블록체인이란?

-	현재 방식(중앙)	탈중앙화 방식(블록체인)
계좌 생성	은행	각 개인 지갑
송금의사 전달 (트랜잭션)	개인 -> 은행	개인 -> 블록체인 노드
장부 관리	은행	블록체인 노드
화폐 발행	(한국)은행	채굴 보상으로 자동 생성
사용자 확인	공인인증서, 아이디, 비밀번호, OTP, 전화번호 인증 등등	개인키 소유자

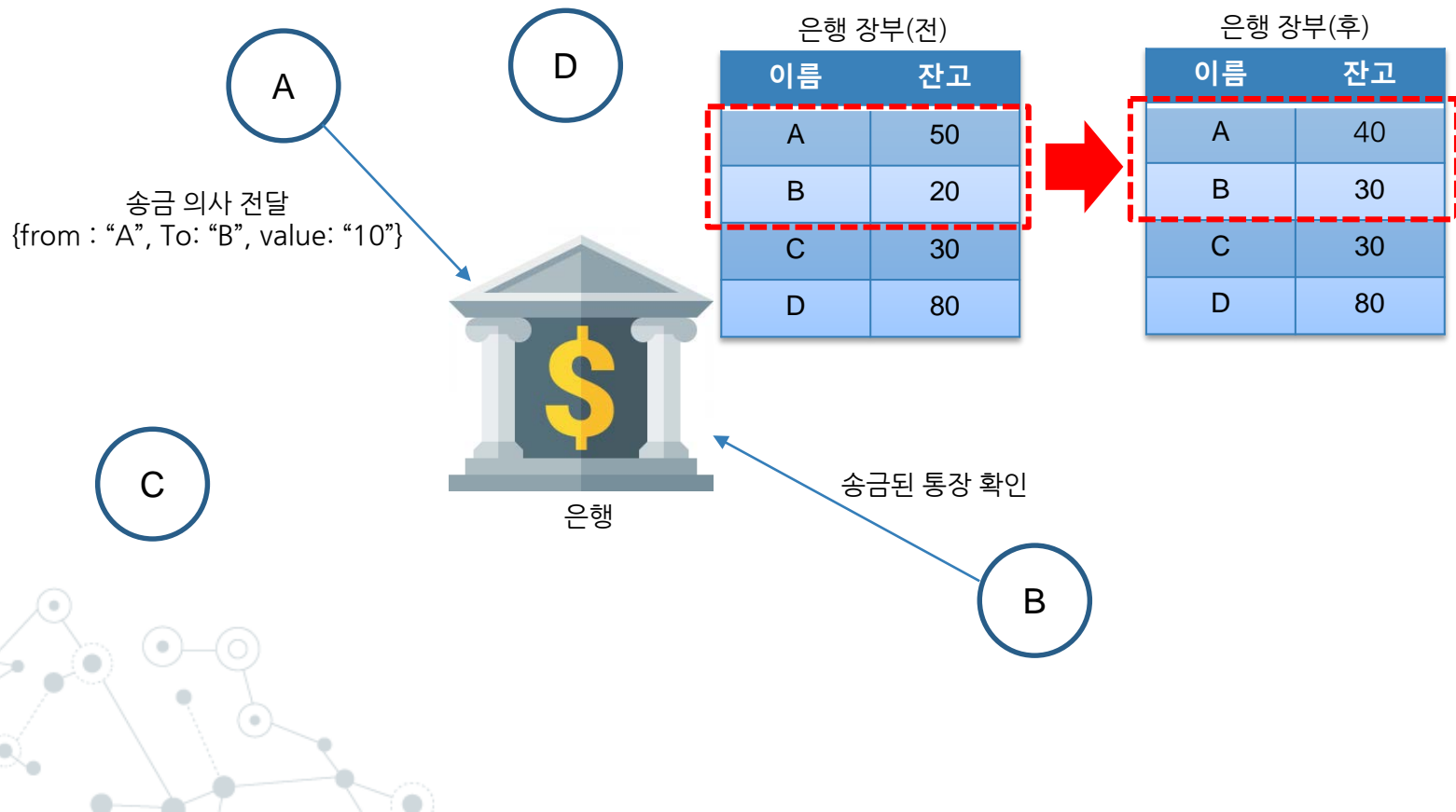
# 블록체인이란?

- ◎ A가 B에게 10원을 송금한다고 할 때에 처리 방법 (기존 방식, Centralized)
  - 데이터 형식으로 표현 : {from : "A", To: "B", value: "10"}
  - 트랜잭션(Tx) : 돈(코인)을 송금하기 위한 데이터



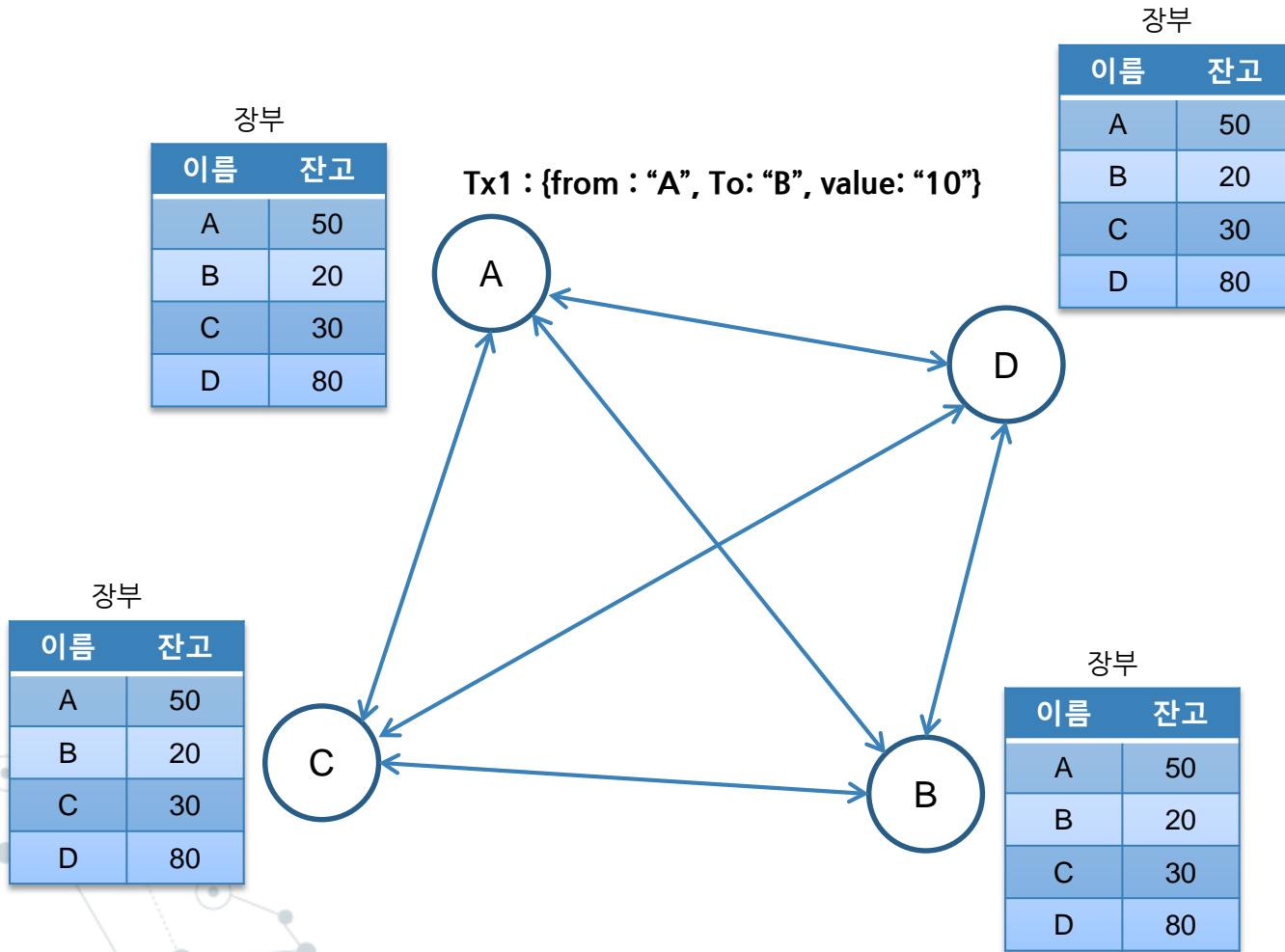
# 블록체인이란?

- ◎ A가 B에게 10원을 송금한다고 할 때에 처리 방법 (기존 방식, Centralized)
  - 데이터 형식으로 표현 : {from : "A", To: "B", value: "10"}
  - 트랜잭션(Tx) : 돈(코인)을 송금하기 위한 데이터



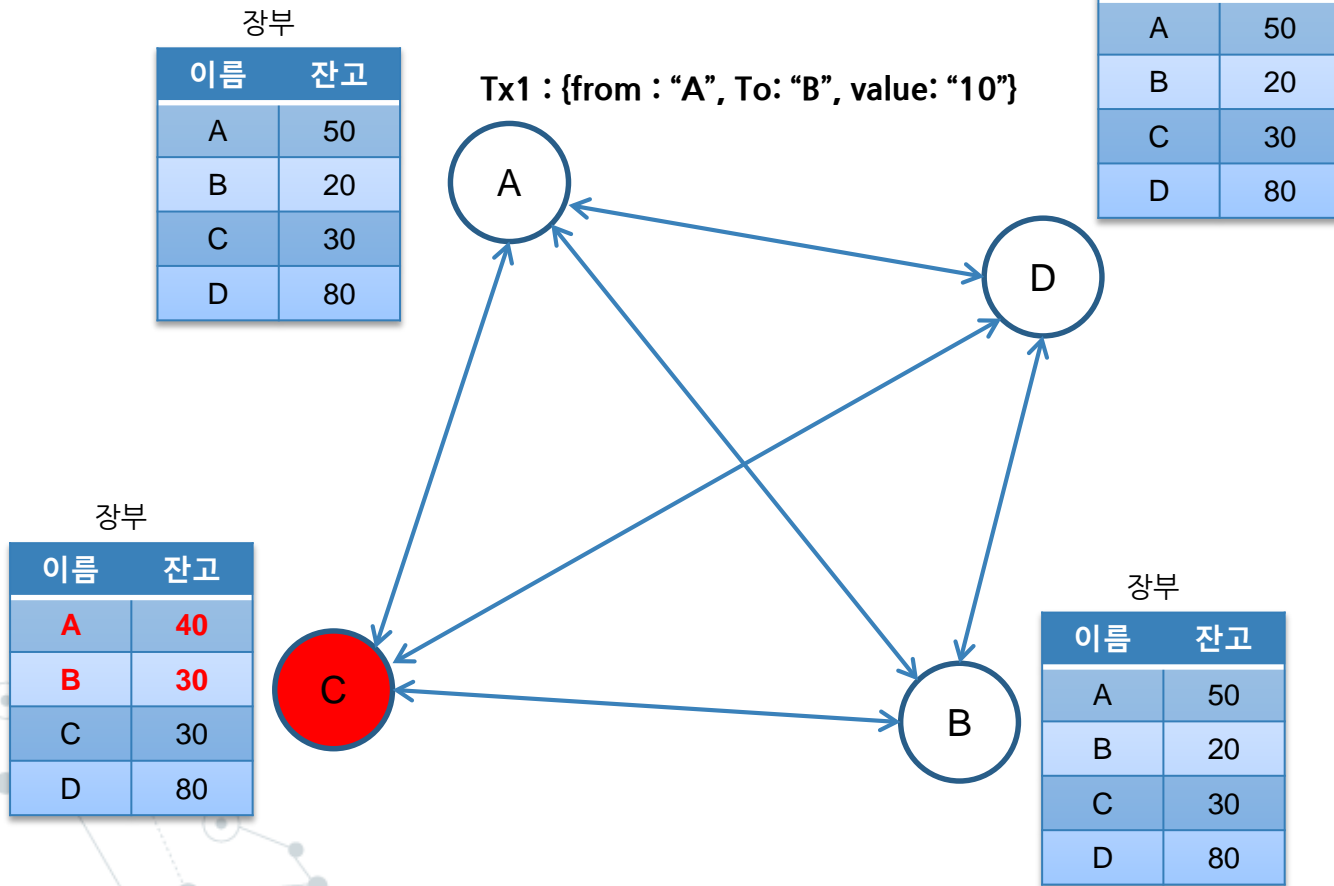
# 탈중앙화 방식

- ◎ A가 B에게 10원을 송금한다고 할 때에 처리 방법 (Decentralized)
  1. 송금 트랜잭션을 각 노드에 전파



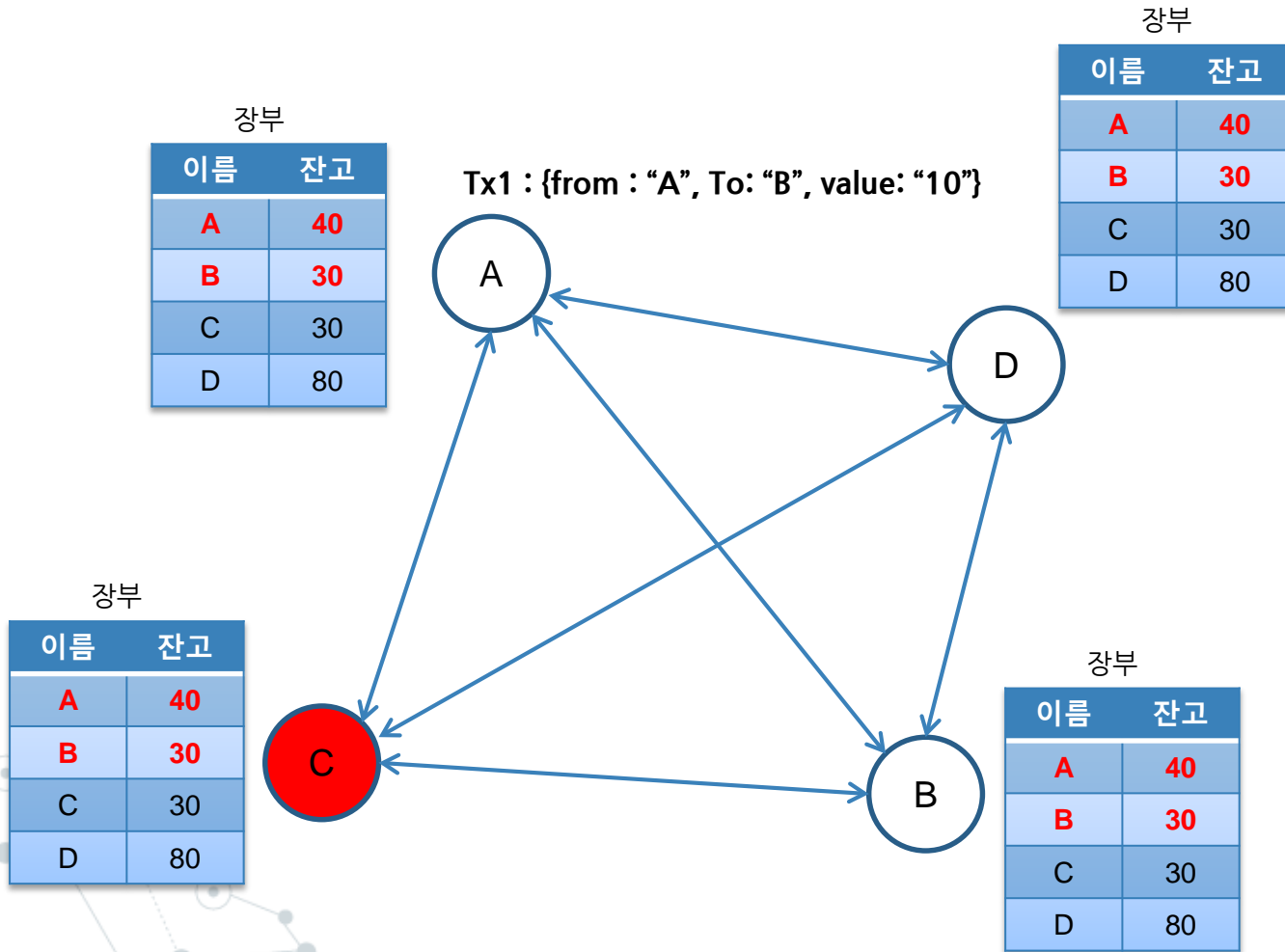
# 탈중앙화 방식

- ◎ A가 B에게 10원을 송금한다고 할 때에 처리 방법 (Decentralized)
1. 송금 트랜잭션을 각 노드에 전파
  2. 어느 한 노드가 해당 트랜잭션을 자신의 장부에 반영하여 반영된 장부를 전파



# 탈중앙화 방식

- ◎ A가 B에게 10원을 송금한다고 할 때에 처리 방법 (Decentralized)
1. 송금 트랜잭션을 각 노드에 전파
  2. 어느 한 노드가 해당 트랜잭션을 자신의 장부에 반영하여 반영된 장부를 전파
  3. 전달받은 새로운 장부가 적절하게 만들어졌는 지 확인하고 자신의 장부를 갱신





# 블록체인

◎ A가 B에게 10원을 송금한다고 할 때에 처리 방법 (Decentralized)

1. 해당 트랜잭션을 포함한 블록을 생성(PoW)
2. 각 노드에 생성한 블록을 전파
3. 자신의 블록에 새롭게 생성된 블록을 갱신(연결)

장부

이름	잔고
A	50
B	20
C	30
D	80

장부

이름	잔고
A	45
B	30
C	25
D	80

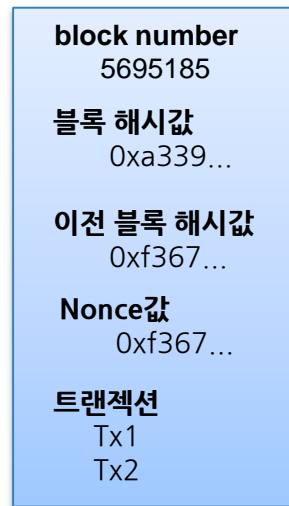
트랜잭션 Pool

Tx1 : {from : "A", To: "B", value: "10"}

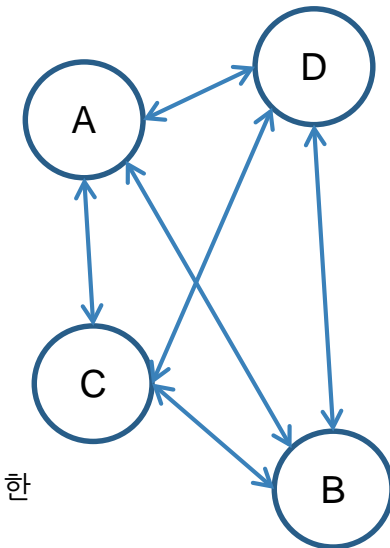
Tx2 : {from : "C", To: "A", value: "5"}

...

각각의 전자서명 값을 확인(A 및 C)



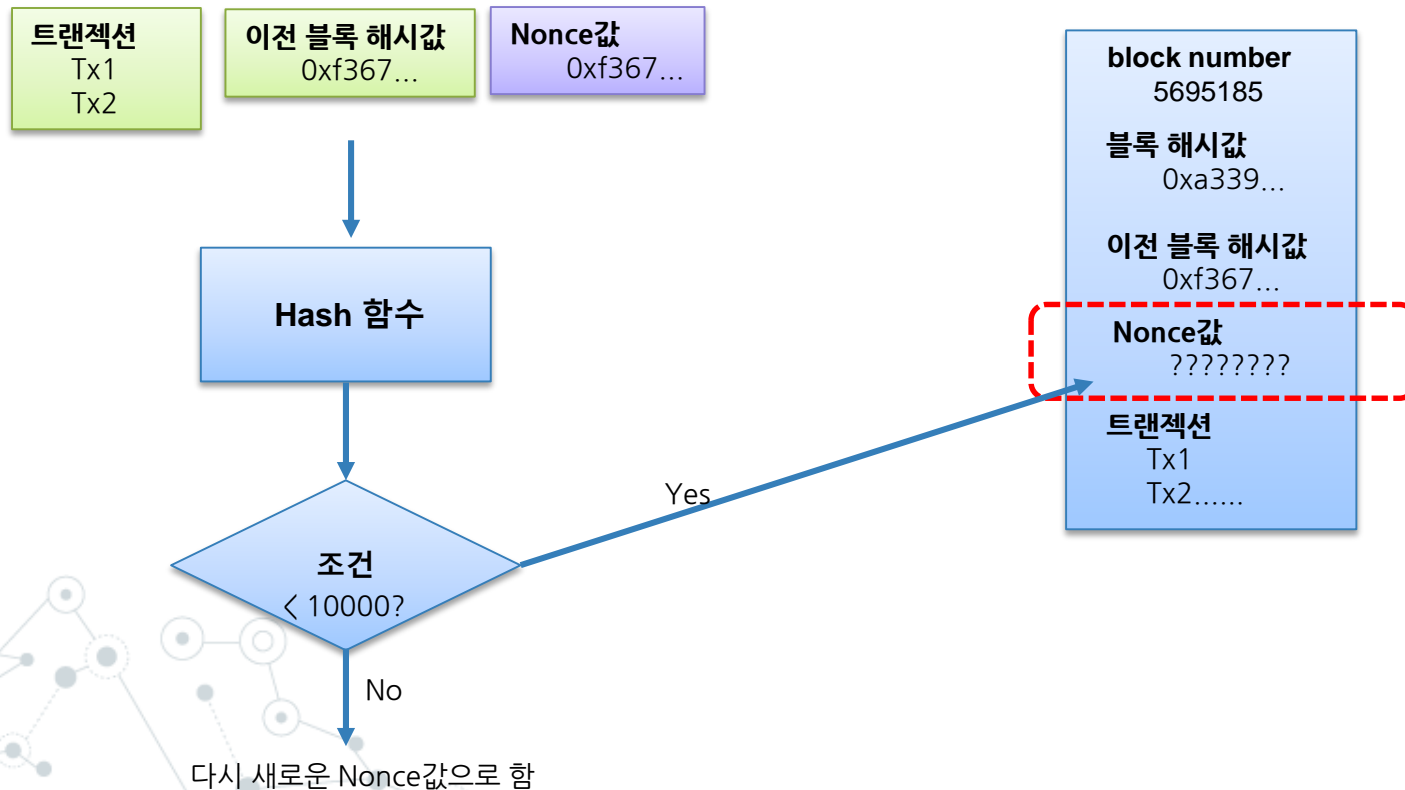
각 노드에 생성한  
블록을 전파



장부를 갱신함

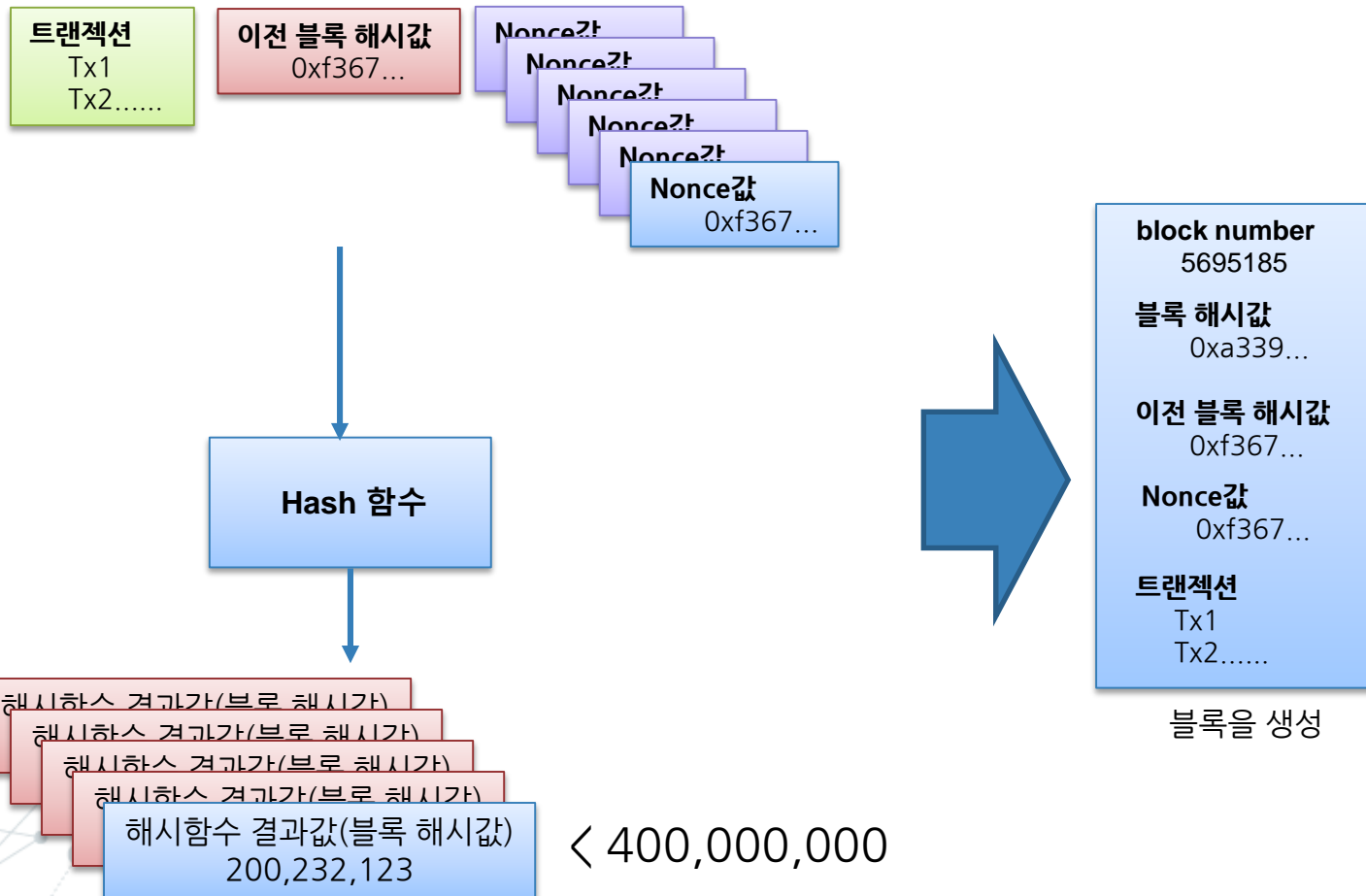
# 블록 생성 방법(PoW : proof of work)

- ◎ 일정 조건이 되도록 Nonce값을 찾는 것
  - 가능한 모든 경우의 Nonce값을 대입하여 Hash 함수를 계산
- ◎ Nonce값 이외의 값(데이터)는 고정, Nonce값만 찾으면 블록 데이터 완성



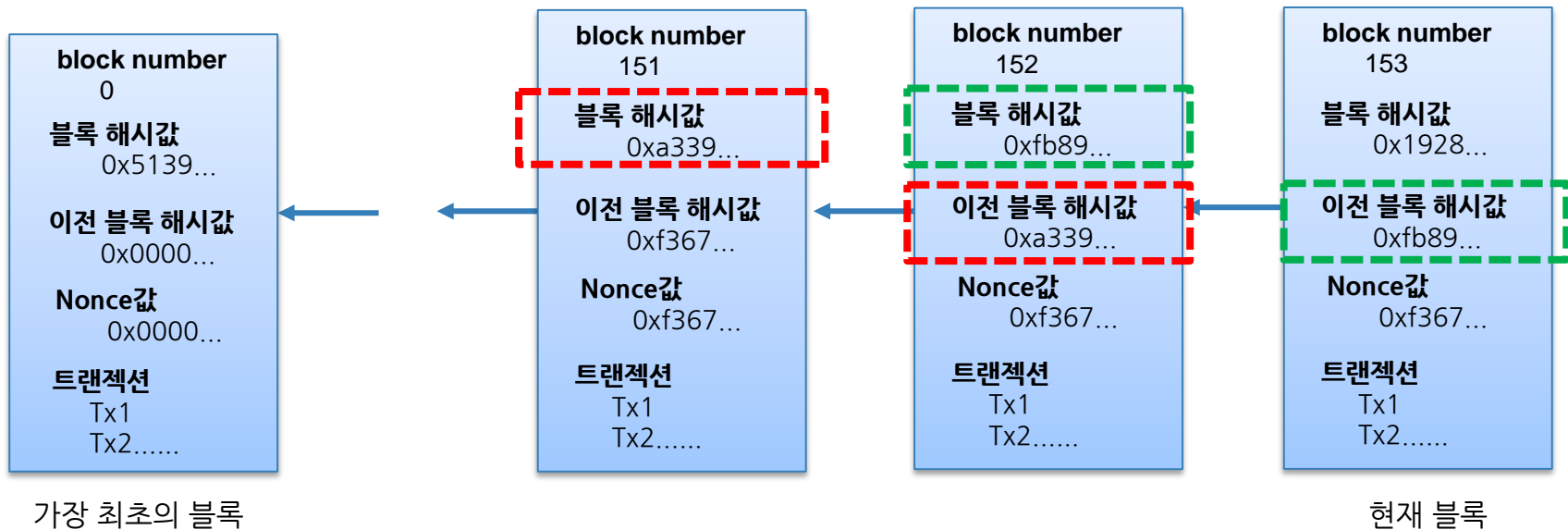
# 블록 생성 방법(PoW : proof of work)

- ◎ 일정 조건이 되도록 Nonce값을 찾는 것
  - 가능한 모든 경우의 Nonce값을 대입하여 Hash 함수를 계산



# 블록체인

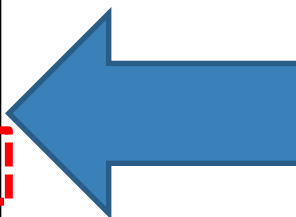
- ◎ 각 블록은 이전 블록을 참조
  - 최초의 블록, Genesis Block
  - 비트코인 : 약 10분간격, 이더리움 : 약 15초 간격으로 생성



# 블록체인

- ◎ 각 블록은 이전 블록을 참조
  - <https://etherscan.io/block/5825110>

Block Information	
Height:	< Prev 5825109 Next >
TimeStamp:	3 mins ago (Jun-20-2018 11:05:22 P
Transactions:	54 transactions and 1 contract interr
Hash:	0xd9d715a04f4ba8a36af599c2bb5b
Parent Hash:	0xa3a8d433a0a6ff45def09e281c7f4
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6cc
Mined By:	0x5a0b54d5dc17e0aadc383d2db43



Block Information	
Height:	< Prev 5825110 Next >
TimeStamp:	3 mins ago (Jun-20-2018 11:05:29 P
Transactions:	8 transactions and 0 contract interna
Hash:	0xcf49bbb9c4f63e32d46128ad9b7b7
Parent Hash:	0xd9d715a04f4ba8a36af599c2bb5b
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6cc
Mined By:	0xb75d1e62b10e4ba91315c4aa3fac

# 블록체인, TPS?

- ◎ Transaction Per Second의 약자로 초당 처리 가능한 트랜잭션 수
  - 비트코인 : 5 TPS
  - 이더리움 : 20 TPS
- ◎  $TPS = \text{한 블록에 포함될 수 있는 트랜잭션 수} / \text{블록생성 시간}$

**block number**  
5695185


**블록 해시값**  
0x1928...

**이전 블록 해시값**  
0xfb89...

**Nonce값**  
0xf367...

**트랜잭션**  
Tx1  
Tx2.....

**이더리움 :  $300\text{tx}/15\text{초} = 30 \text{ TPS}$**

 Blocks

[View All](#)

Block 5695688  
> 56 secs ago

Mined By [SparkPool](#)  
**106 txns** in 3 secs  
Block Reward 3.09184 Ether

Block 5695687  
> 59 secs ago

Mined By [miningpoolhub\\_1](#)  
**136 txns** in 9 secs  
Block Reward 3.10911 Ether

Block 5695686  
> 1 min ago

Mined By [Ethermine](#)  
**142 txns** in 10 secs  
Block Reward 3.11551 Ether

Block 5695685  
> 1 min ago

Mined By [Ethermine](#)  
**288 txns** in 7 secs  
Block Reward 3.077 Ether

Block 5695684  
> 1 min ago

Mined By [bw](#)  
**78 txns** in 27 secs  
Block Reward 3.31612 Ether

Block 5695683  
> 1 min ago

Mined By [Nanopool](#)  
**221 txns** in 0 sec

# 블록체인, TPS?

- ◎ Transaction Per Second의 약자로 초당 처리 가능한 트랜잭션 수
  - 블록사이즈가 커지면 포함시킬 수 있는 Tx 증가 -> TPS 증가

트랜잭션  
tx1, tx2, tx3, tx4,  
tx5.....

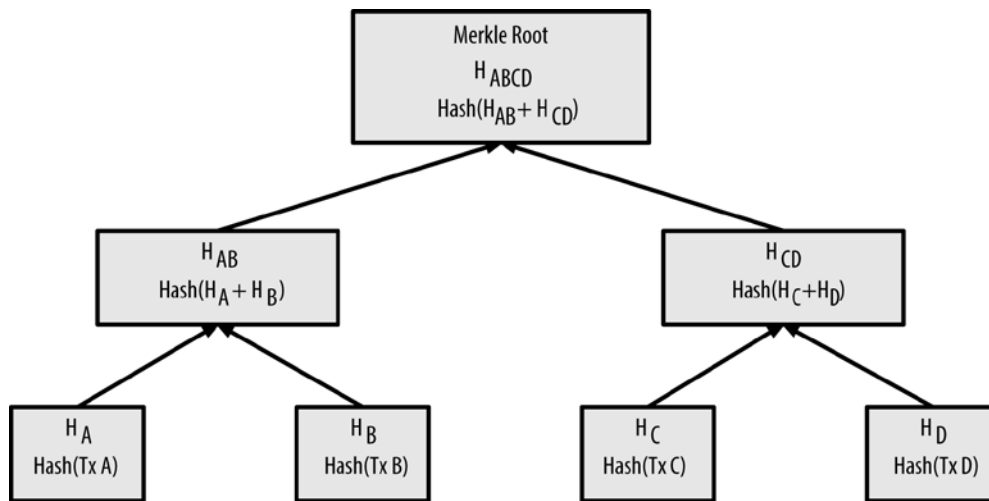
비트코인 블록사이즈 1M

트랜잭션  
tx1, tx2, tx3, tx4,  
tx5, tx6, tx7, tx8,  
tx9, tx10.....

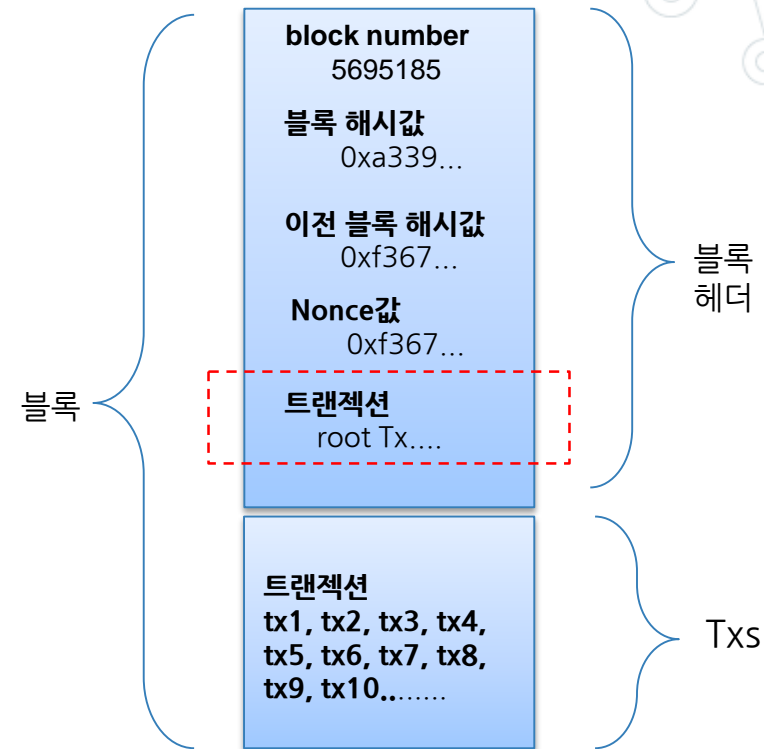
비트코인캐쉬 블록사이즈 8M

# 머클 트리

- ◎ 다수의 트랜잭션을 하나의 트랜잭션 해시로 묶어서 계산



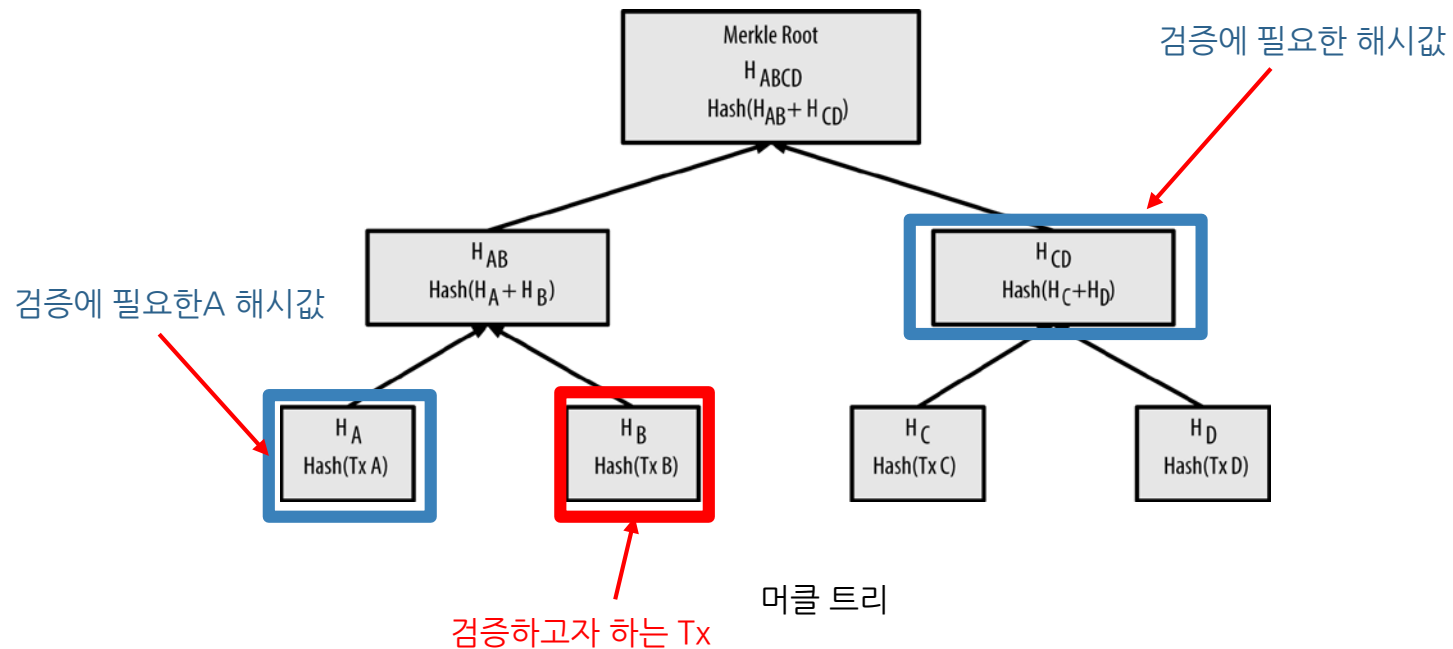
머클 트리





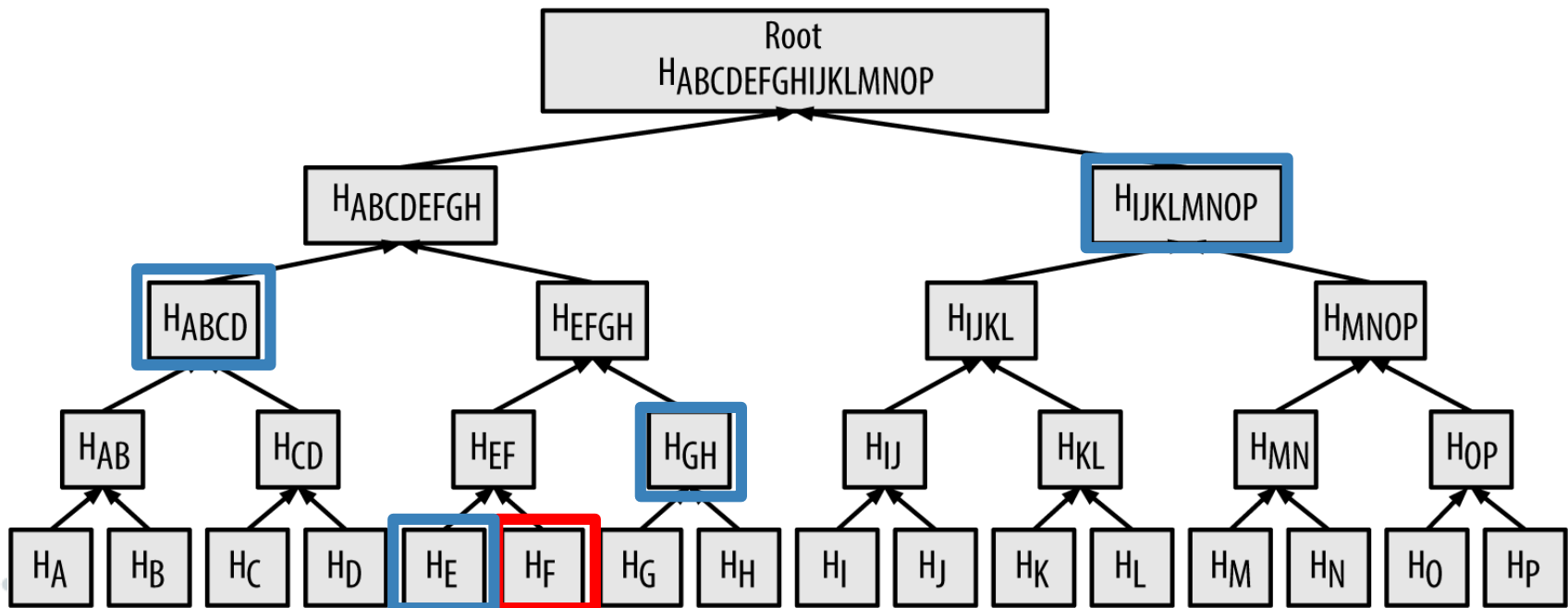
# 머클 트리

- ◎ 하나의 트랜잭션 검증이 효율적으로 가능함
  - 전체의 해시값 이외의 일부 해시값만 가지고 검증이 가능함

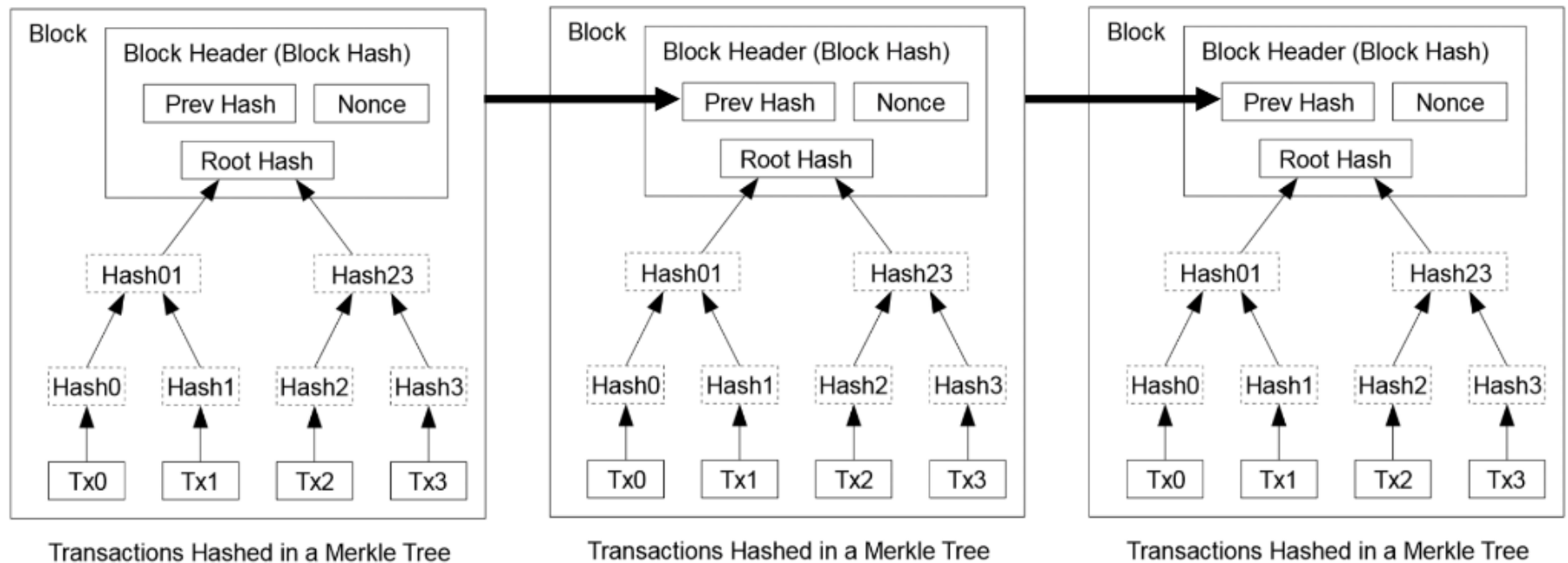


# 머클 트리

- ◎  $\log_2(N)$ 개의 32바이트 값이 필요
  - 전체로 했을 경우  $(N-1)$ 개의 32바이트 값



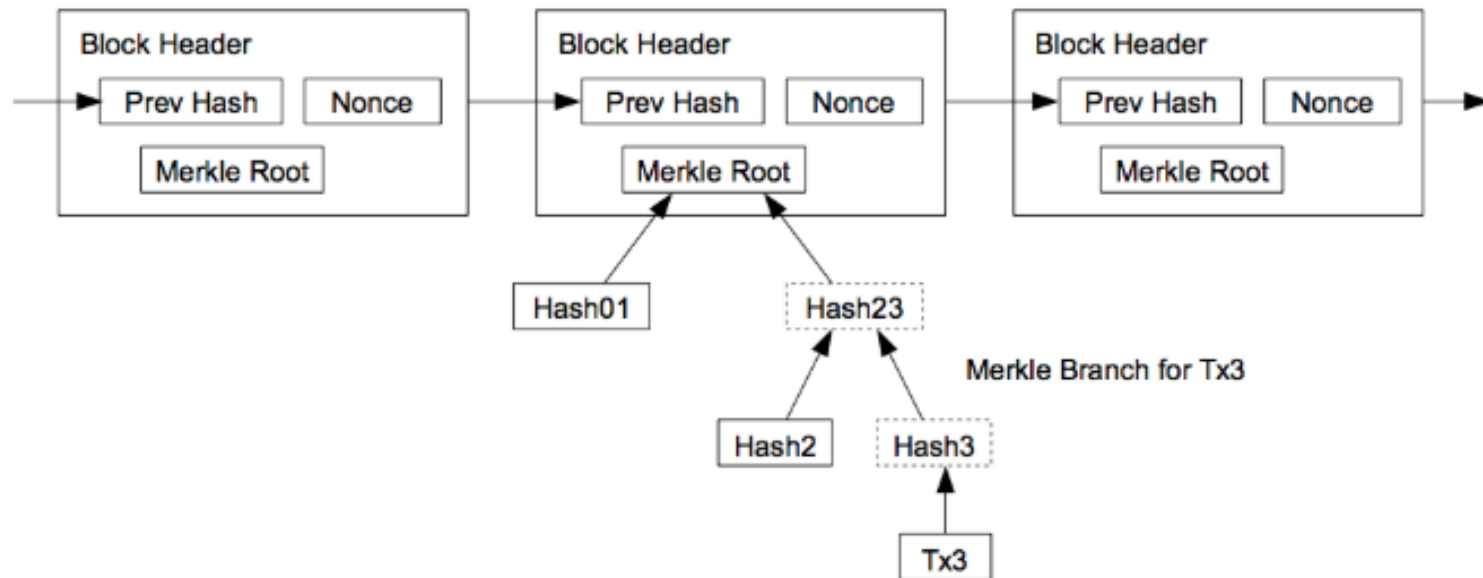
# 종합(머클트리 + 블록)



# 종합(머클트리 + 블록)

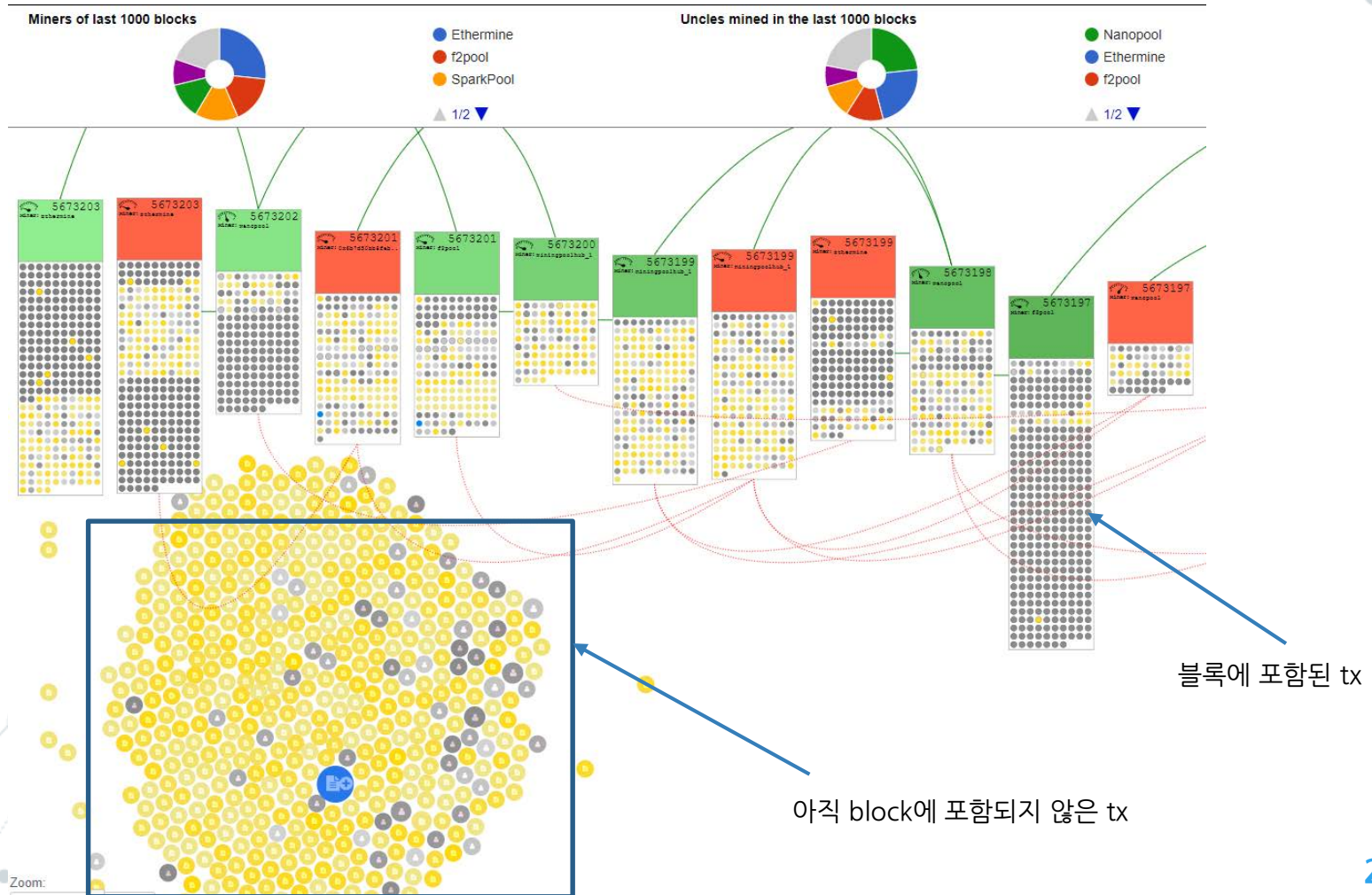
- ◎ SPV : Simplified Payment Verification
  - 스마트폰에서 모든 Tx를 다 저장해서 노드를 sync시키기에는 용량의 문제가 있음
- ◎ Tx3이 실제 블록에 포함됨을 확인
  - Hash2, Hash01값만으로 확인이 가능
  - 전체 모든 Tx을 받아오지 않고, 해시를 여러번 하지 않아도 확인이 가능

Longest Proof-of-Work Chain



# Visualize 블록체인

◎ <http://ethviewer.live/>



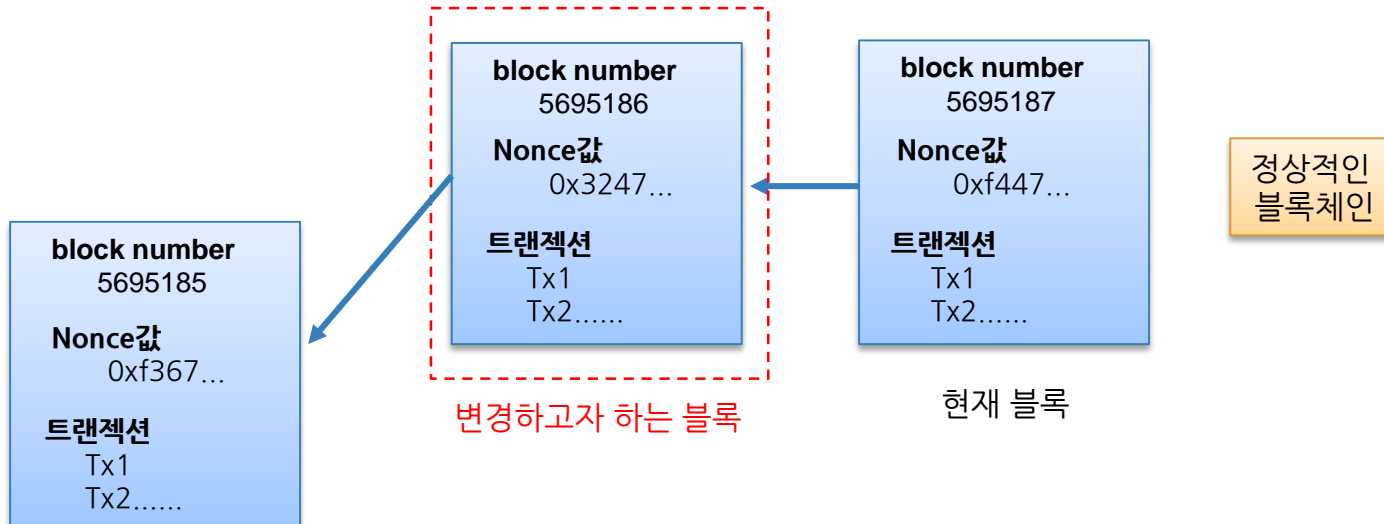
# 실제 블록체인 정보

- ◎ <https://etherscan.io/> (이더리움)
- ◎ <https://blockchain.info/> (비트코인)

Blocks	View All	Transactions	View All
<div>Block 5673239</div> <div>&gt; 11 secs ago</div>	Mined By <a href="#">Ethermine</a> 53 txns in 11 secs Block Reward 3.03685 Ether	<div>TX# 0X2BC58B08CFF72618609F394...</div> <div>&gt; 11 secs ago</div> <div>From 0xad5b87eebb0635... To 0x3f9c0a5773817fa...</div> <div>Amount 0 Ether</div>	
<div>Block 5673238</div> <div>&gt; 22 secs ago</div>	Mined By <a href="#">Nanopool</a> 169 txns in 33 secs Block Reward 3.38014 Ether	<div>TX# 0X642CB5814AFC2E1452510AD...</div> <div>&gt; 11 secs ago</div> <div>From 0xeb4b3106b76dd4f... To 0xf230b790e05390f...</div> <div>Amount 0 Ether</div>	
<div>Block 5673237</div> <div>&gt; 55 secs ago</div>	Mined By <a href="#">Nanopool</a> 187 txns in 15 secs Block Reward 3.10259 Ether	<div>TX# 0XF369E448824D9A1B321D08F...</div> <div>&gt; 11 secs ago</div> <div>From 0x8f4d6a9c259c0fe... To 0x228ba514309ffdf0...</div> <div>Amount 0 Ether</div>	
<div>Block 5673236</div> <div>&gt; 1 min ago</div>	Mined By <a href="#">Ethermine</a> 147 txns in 3 secs Block Reward 3.27025 Ether	<div>TX# 0X556BF3D81CC7011AE618F1C...</div> <div>&gt; 11 secs ago</div> <div>From 0x308edde9ae4c82f... To 0xf20f321cab9370b...</div> <div>Amount 0.0006 Ether</div>	
<div>Block 5673235</div> <div>&gt; 1 min ago</div>	Mined By <a href="#">f2pool_2</a> 259 txns in 16 secs Block Reward 3.63194 Ether	<div>TX# 0X8C3F2FBD1FC3210294E3955...</div> <div>&gt; 11 secs ago</div> <div>From 0x3dec67afd79eed7... To 0xee014a07e0a5dd...</div> <div>Amount 0.0006 Ether</div>	
<div>Block 5673234</div> <div>&gt; 1 min ago</div>	Mined By <a href="#">miningpoolhub_1</a> 77 txns in 4 secs Block Reward 3.08418 Ether	<div>TX# 0X736832C192C00E9A75C73CB...</div> <div>&gt; 11 secs ago</div> <div>From 0x632652d27c0313... To 0x7d8b9f24320dab5...</div> <div>Amount 0 Ether</div>	

# 위변조가 왜 어려운가?

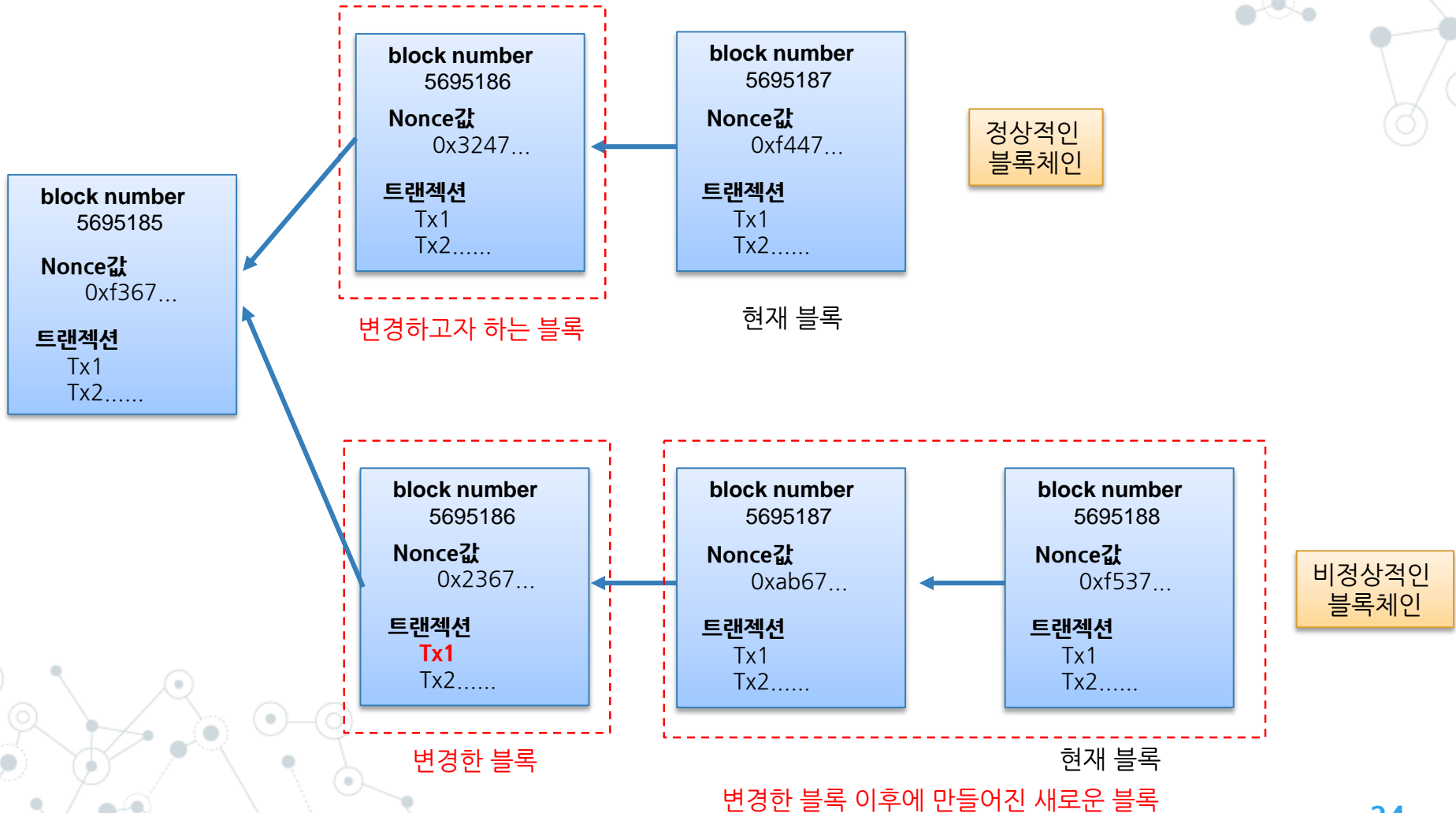
- ◎ confirmation : 뒤에 붙은 블록의 개수
  - 임의로 내용을 변경하고자 하는 블록을 생성하고(새로운 Nonce값을 찾고) 그 뒤에도 새로운 블록을 또 찾고..
  - 전체 네트워크의 약 51% 이상의 계산 파워가 없으면 실질적으로 불가능함



# 위변조가 왜 어려운가?

◎ confirmation : 뒤에 붙은 블록의 개수

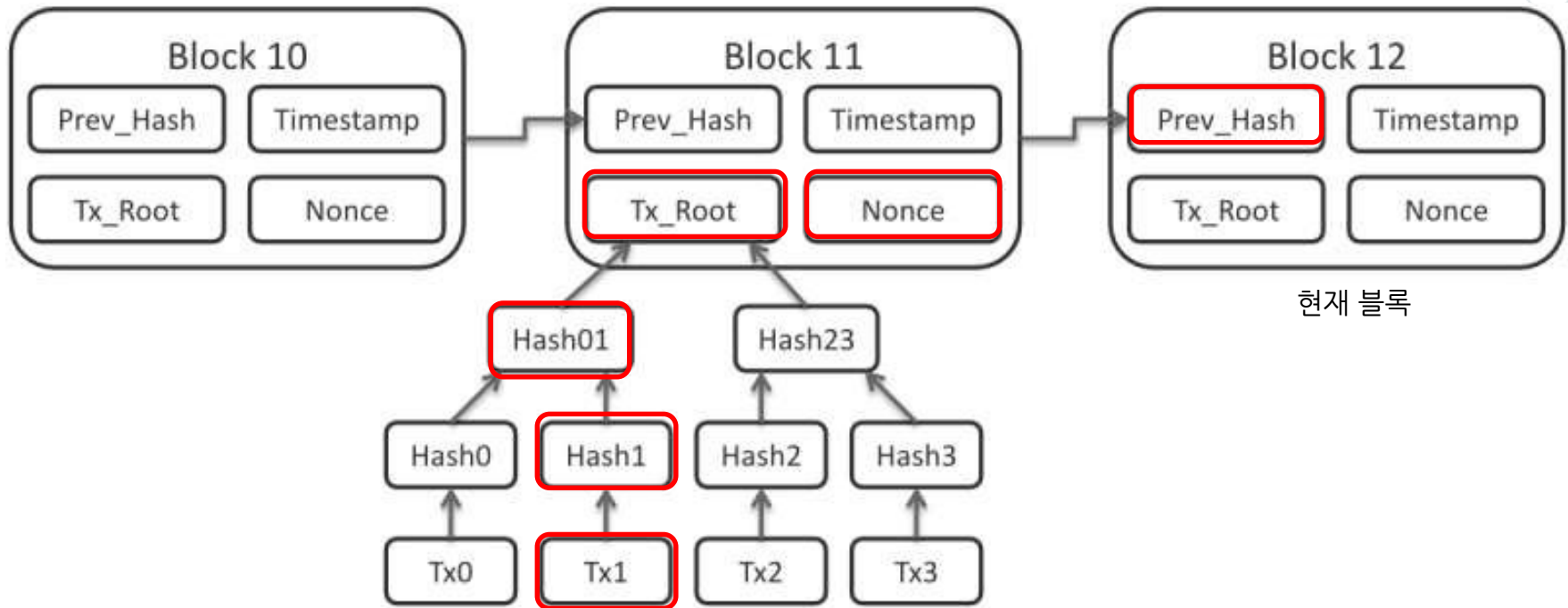
- 임의로 내용을 변경하고자 하는 블록을 생성하고(새로운 Nonce값을 찾고) 그 뒤에도 새로운 블록을 또 찾고..
- 전체 네트워크의 약 51% 이상의 계산 파워가 없으면 실질적으로 불가능함





# 위변조가 왜 어려운가?

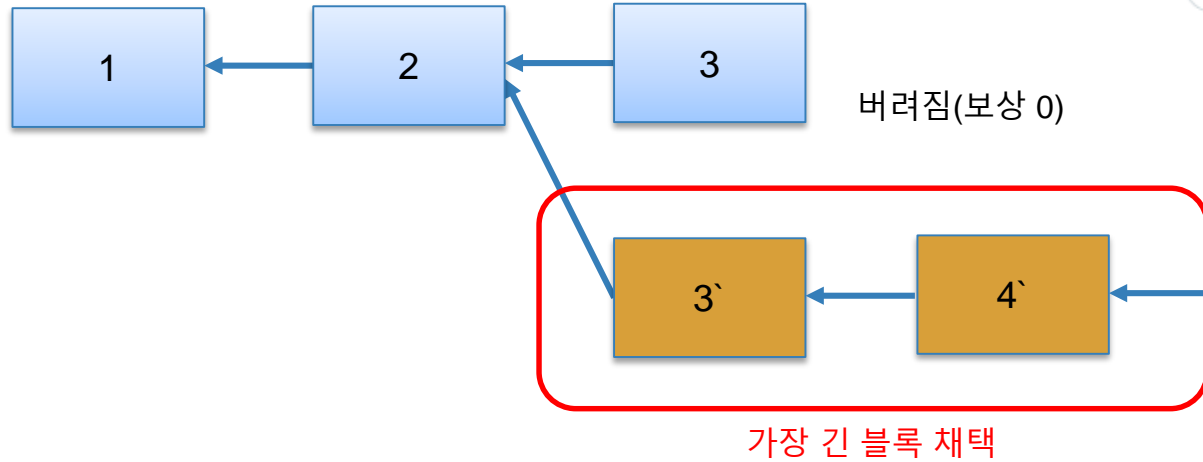
- ◎ confirmation : 뒤에 붙은 블록의 개수
  - 임의로 내용을 변경하고자 하는 블록을 생성하고(새로운 Nonce값을 찾고) 그 뒤에도 새로운 블록을 또 찾고..
  - 전체 네트워크의 약 51% 이상의 계산 파워가 없으면 실질적으로 불가능함



예, Tx1를 변경하고자하면 결국 Hash1 -> Hash01 -> Tx\_Root가 변경됨  
Block11을 변경하려면 이를 참조하고 있는 Block12도 변경해야함  
(->새로운 Nonce값을 찾는 것)

# 비트코인의 블록 체인

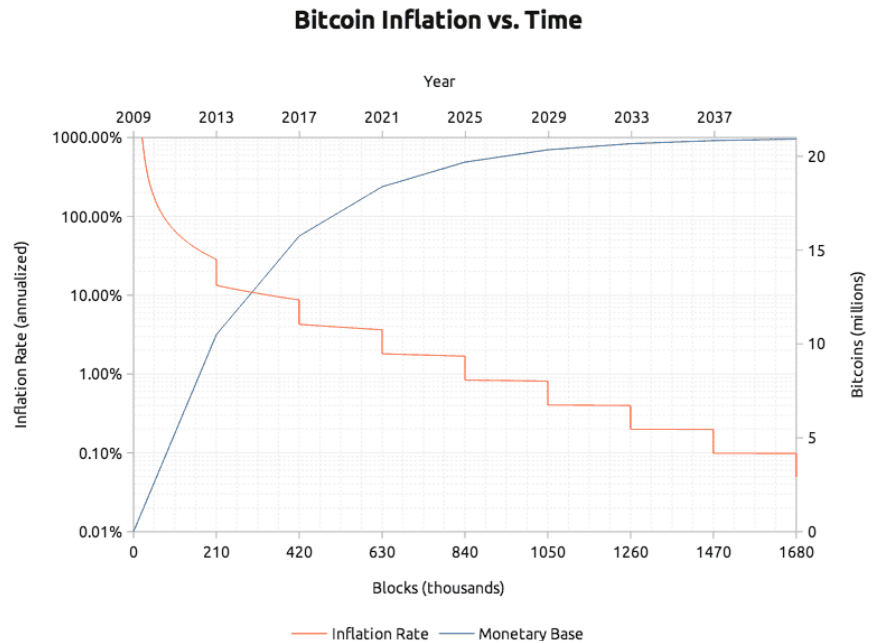
- ◎ 가장 길이가 긴 것을 채택(유효한 블록 -> 보상 지급)
  - 블록보상 12.5 BTC



# 비트코인의 블록 체인

- ◎ 가장 길이가 긴 것을 채택(유효한 블록 -> 보상 지급)
  - 블록보상 12.5 BTC

크기	1015.57 KB
번역	0x20000000
Merkle Root	026c593460ee2d4a3
해시 난수(Nonce)	2572966032
블록 보상	12.5 BTC
거래 수수료	3.10783096 BTC

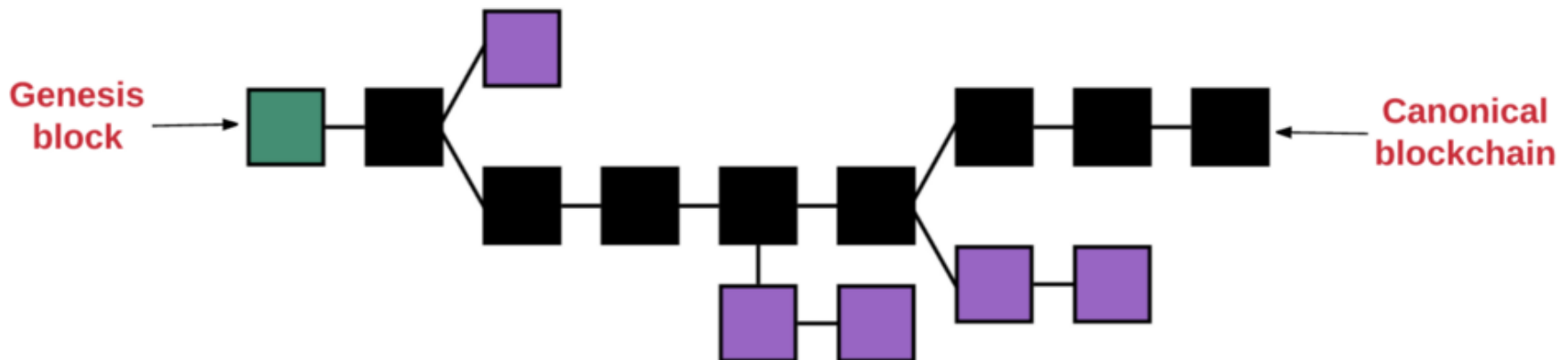


총 발행량이 정해져 있음

# 이더리움의 블록 체인

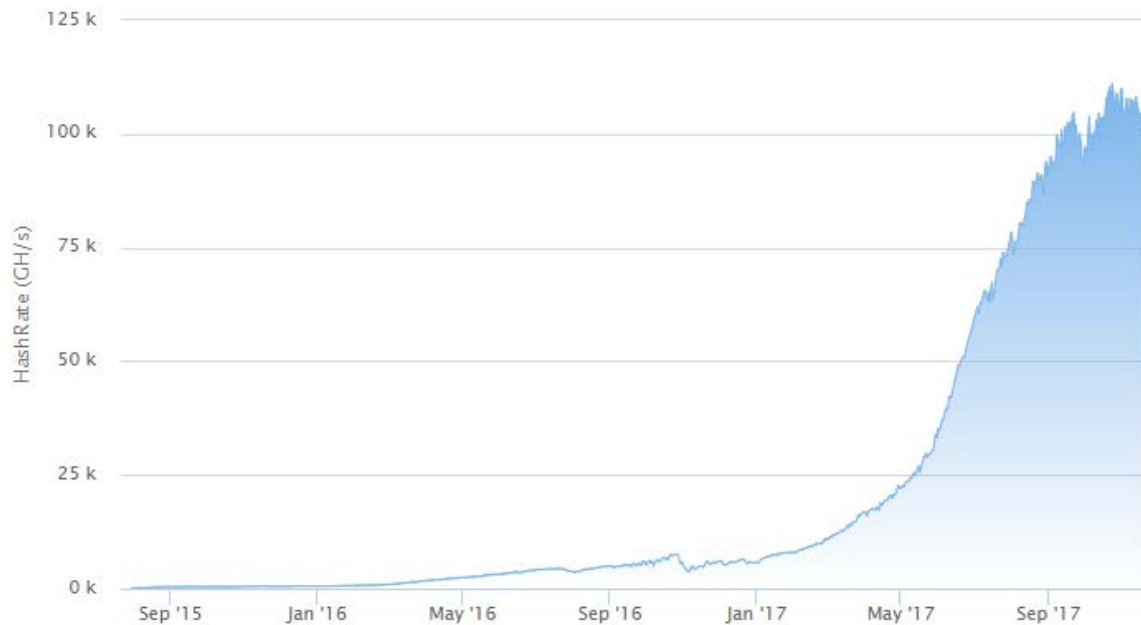
- ◎ 이더리움은 포크가 발생할 확률이 높음
- ◎ **GHOST\* = Greedy Heaviest Observed Subtree**
  - 블록보상 : 3 eth
  - 가장 긴 Path를 고름
  - 블록에 uncles을 포함시킴 -> 포함된 uncle block의 난이도를 합쳐서 메인 블록체인을 정함
  - uncle(최대 7/8)과 nephew(1/32)에 대해서도 보상

Block Reward:	3.214233108837901391 Ether (3 + 0.120483108837901391 + 0.09375)
Uncles Reward:	2.25 Ether (1 Uncle at Position 0)



# 공격이 가능한가?

- ◎ Ethereum Public Nextwork(대표적인 블록체인)를 해킹하는 것과 동일한 Cost
- ◎ 현재 Hashrate = 11246GH/s (1초당 11,246,000,000,000번의 연산량)
- ◎ 해킹을 위해 동등 수준의 Hashrate 파워가 필요함
- ◎ 결국  $11246\text{GH} / 35\text{MH} \times \$1,000 = \text{\$321,314,000(3억달러)}$ 가 필요함



Ethereum Network Hashrate (전체 노드 파워)

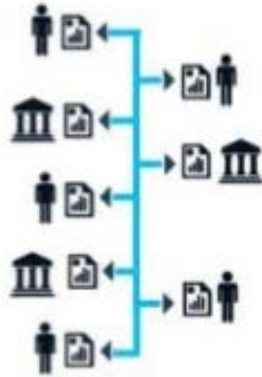
GTX 1080ti으로 현재  
약 **30만대** 규모



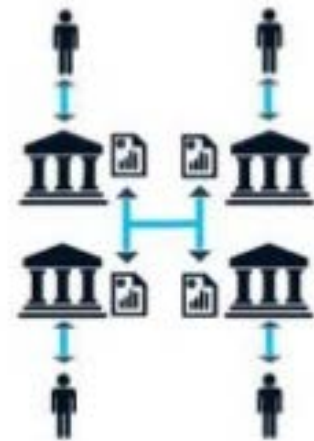
Model : GTX1080ti GPU  
Price : \$1,000  
Hashrate : 35MH/s

# 블록체인 네트워크 종류

- ◎ 퍼블릭 네트워크=퍼블릭 체인(비트코인, 이더리움 등등)
  - 누구나 열람이 가능하고 네트워크에 참여가 가능함
  - 속도는 낮음(PoW)
- ◎ 프라이빗 네트워크=프라이빗 체인(리플 등등)
  - 권한을 가지는 기관 및 회사 등만 참여가 가능한 네트워크
  - 트랜잭션 또한 허가된 노드만 가능
  - 속도는 빠름 (PoS, PBFT, PoA 등)
- ◎ 테스트 네트워크
  - 실제 네트워크를 동작시키기 전에 테스트를 위한 용도의 네트워크
  - 이더리움은 ropsten, rinkeby 등이 있음



퍼블릭 네트워크



프라이빗 네트워크

# 종합

- ◎ 트랜잭션
  - 사용자가 블록체인 상에 보내는 송금 요청 등을 말함
- ◎ 블록
  - 트랜잭션의 집합
- ◎ 블록 생성(마이닝)
  - 블록의 해시값이 일정 조건을 만족하는 Nonce값을 찾는 과정
  - Nonce값이 찾아져야 블록이 생성되고 각 노드에 전파가 되어 블록에 포함된 트랜잭션이 유효한 트랜잭션으로 됨