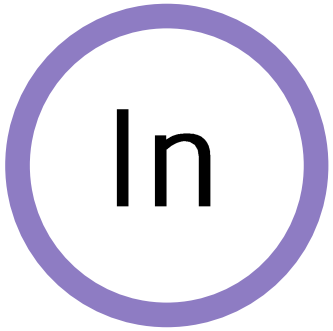
블록체인 개념 이해

블록체인이란



블록체인에 대한 이해

01 블록체인에 대한 정의

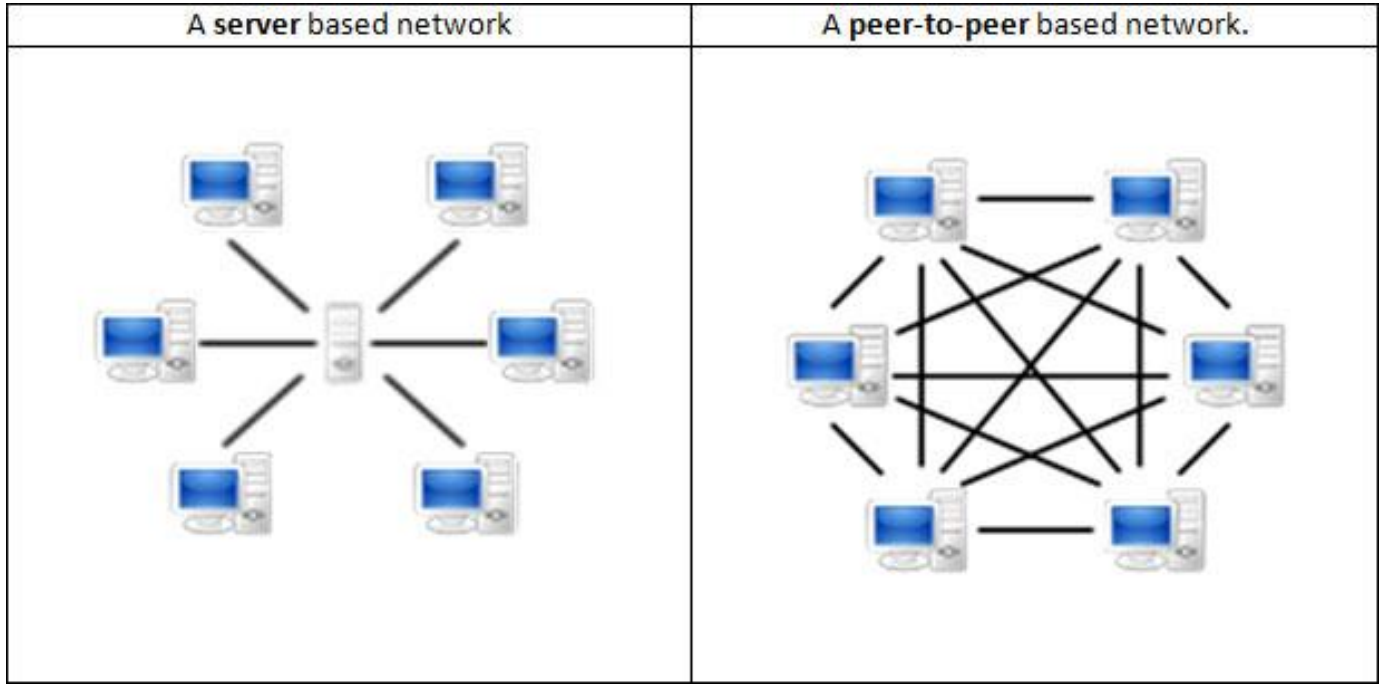
[위키백과]
블록체인은 관리 대상 데이터를 '블록'이라고 하는 **소규모 데이터들이 P2P 방식**을 기반으로 생성된 **체인 형태의 연결고리 기반 분산 데이터 저장 환경**에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 **분산 컴퓨팅 기술 기반의 원장 관리 기술**이다. 이는 근본적으로 **분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안**되었다. 블록체인 기술은 비트코인을 비롯한 대부분의 암호화폐 거래에 사용된다. 암호화폐의 거래과정은 탈중앙화된 전자장부에 쓰이기 때문에 블록체인 소프트웨어를 실행하는 많은 사용자들의 각 컴퓨터에서 서버가 운영되어, **중앙에 존재하는 은행 없이 개인 간의 자유로운 거래**가 가능하다.

[Oxford Dictionaries]
A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly.
비트코인 혹은 다른 암호화폐의 거래가 **순차적이고 공개적으로 기록되는 디지털 장부를 의미**

P2P방식, 순차적이고 공개적, 체인 형태, 분산 데이터 저장, 모든 참여 노드에 기록, 임의 조작 불가, 디지털 원장(장부), 중앙에 존재하는 은행 없이 개인 간 자유로운 거래

01 블록체인에 대한 정의

P2P(피투피)란 Peer to Peer(피어 투 피어)의 약자
인터넷에 연결된 다수의 개별 사용자들이 중개기관을 거치지 않고 직접 데이터를 주고받는 것
영어로 Peer란 '동료'라는 뜻
P2P란 인터넷에 연결된 한 동료가 다른 동료에게 데이터를 직접 전송하는 시스템을 말한다.



01 블록체인에 대한 정의

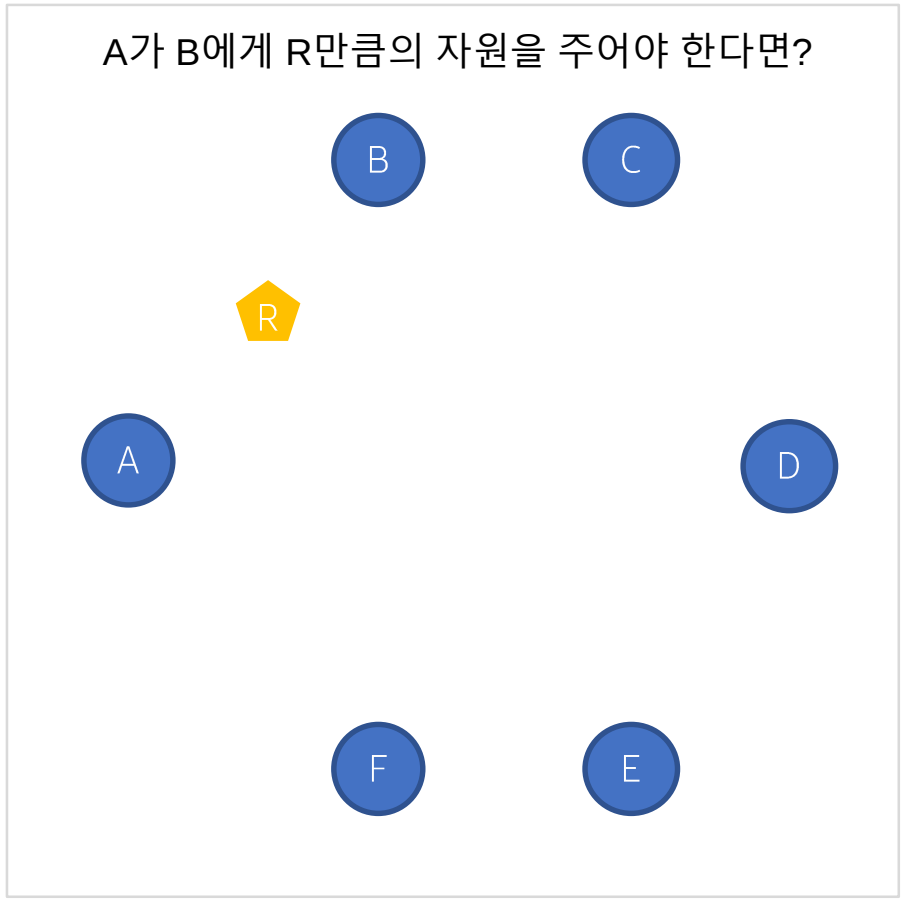
- P2P 방식은 기존의 서버-클라이언트 방식의 데이터 전송과는 본질적으로 다른 구조
- 서버-클라이언트(server-client) 구조
  - ➢개별적인 참여자는 우선 서버에 데이터를 올려야 하고, 다른 참여자가 해당 서버로부터 데이터를 받아오는 방식으로 작동
  - ➢서버-클라이언트 구조에서 서버는 중앙·중심·센터에 해당하고, 클라이언트는 서버에 연결된 종속적 위치에 놓이게 된다.
- P2P 방식은 중앙이나 중심 또는 센터가 없다.
  - ➢P2P 네트워크에 참여하는 모든 참여자들은 서로 평등

01 블록체인에 대한 정의

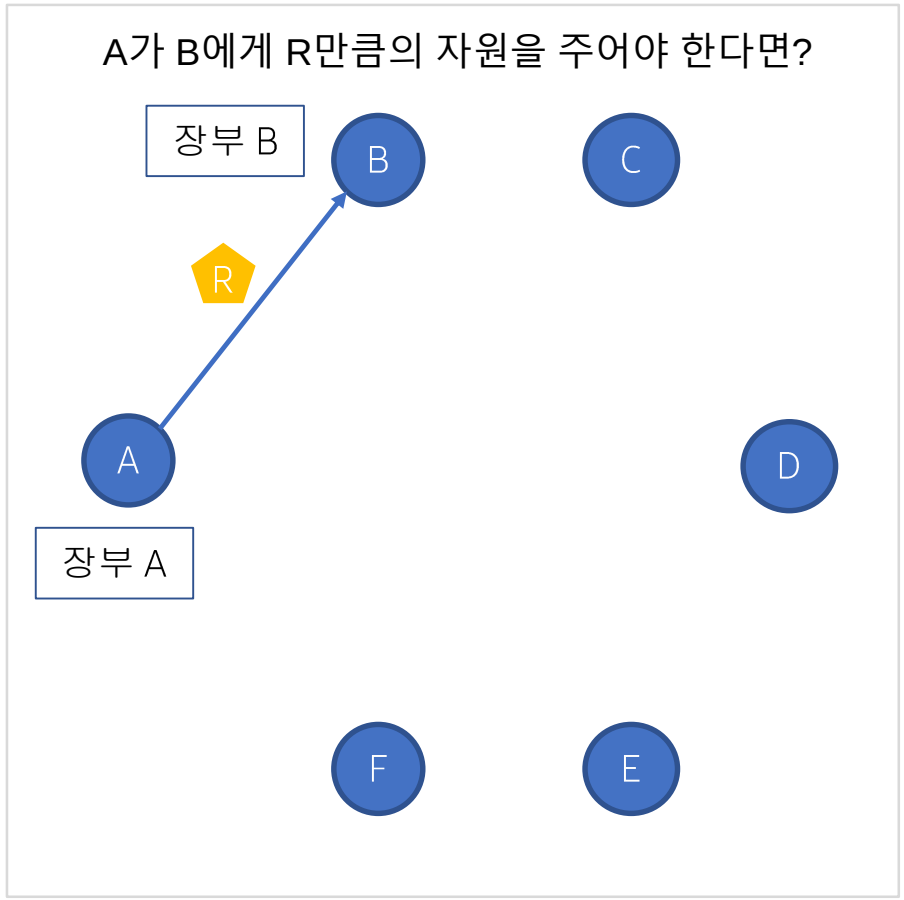
P2P는 다양하게 활용되고 있다.

- 음악 파일 공유 : 냅스터(Napster), 소리바다(soribada) 등
- 동영상 파일 공유 : 토렌트(Torrent)
- 암호화폐 : 비트코인(bitcoin), 이더리움(ethereum) 등

02 기존 금융 시스템



02 기존 금융 시스템



[직접 전달 – p2p]

각자의 장부에 자원을 받았다는 것과 자원을 주었다는 것을 기록하자.

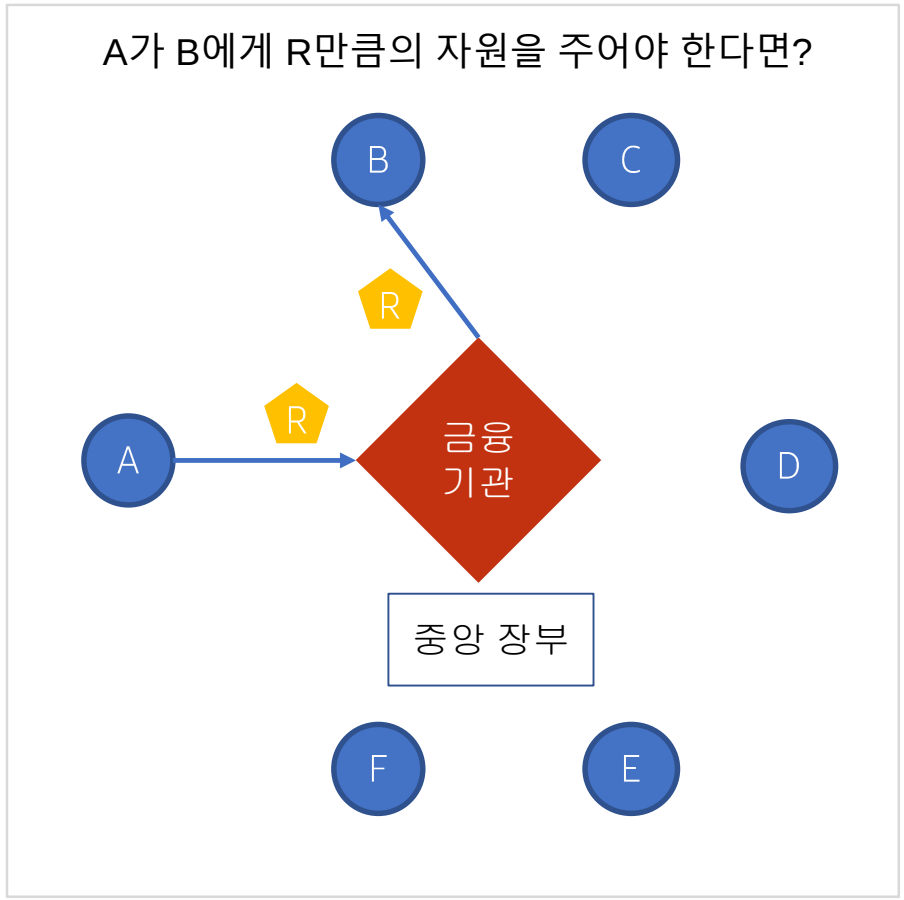
- A가 준 것을 잊고 기록하지 않고 또 보내면 어떡하지?
- B가 받은 것을 잊고 기록하지 않으면 어떡하지?
- B가 받지 않았다고 거짓말을 한다면 어떡하지?
- 인터넷 환경에서 신뢰가 필요한 거래에서 특히 부적절함.

→ 신뢰문제 발생
→ 이러한 분쟁을 중재 해 줄 기관이 필요

[장부A]
2021.01.02: C에게 R 2000을 받음
2021.01.03: D에게 R 5000을 받음
2021.01.04: B에게 R 1000을 전송

[장부B]
2021.01.02: C에게 R 3000을 받음
2021.01.03: D에게 R 2000을 전송
2021.01.04: A에게 R 5000을 받음

02 기존 금융 시스템



현재 대부분의 시스템

[신뢰받는 기관에 제 3자 역할을 맡기자]

신뢰받는 제3자 기관에 중앙에서 전달해 주도록 구축하자.
중앙기관이 받았다는 것과 전달했다는 것을 보증하자.

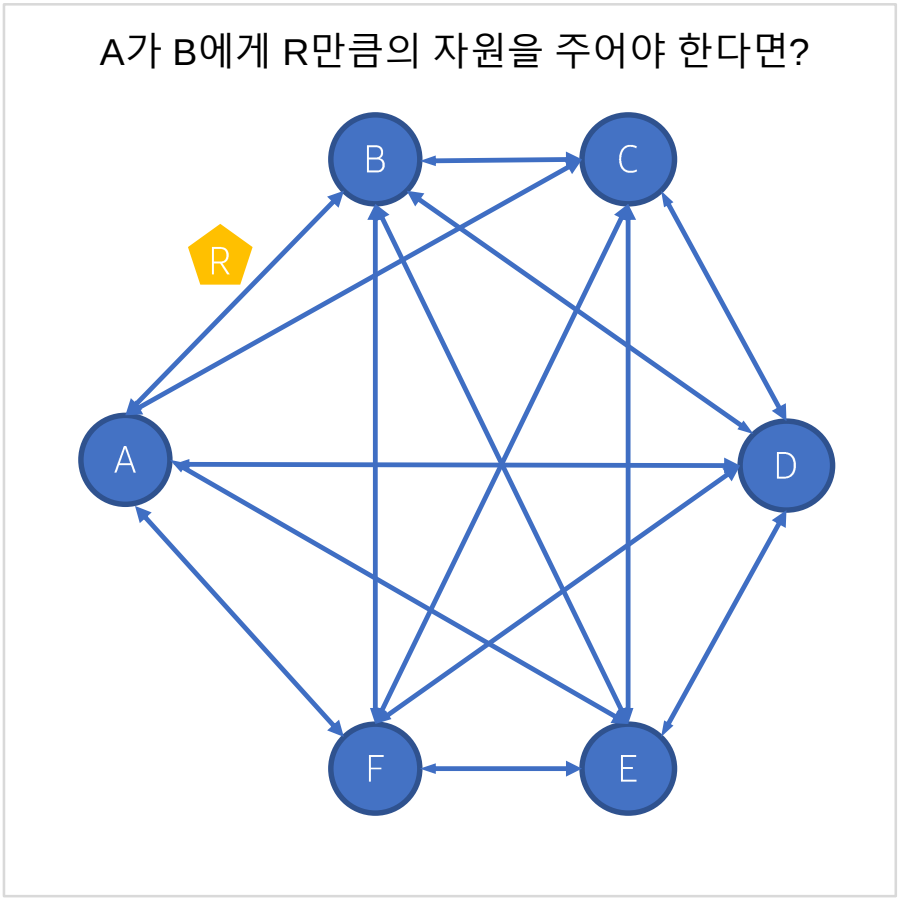
[중앙장부]
2021.01.02: C가 A에게 R 2000을 전송
2021.01.02: C가 B에게 R 2000을 전송
2021.01.03: D가 A에게 R 5000을 받음
2021.01.03: D가 A에게 R 2000을 받음
2021.01.04: A가 B에게 R 1000을 전송

- 신뢰 기반 모델의 태생적 약점
- 취소가능한 거래를 위한 금융기관의 분쟁 중재가 필요
- 중재비용은 거래 수수료를 올림
- 분쟁 예방을 위한 소액 거래의 가능성을 막음
- 회수가 불가능한 서비스에도 번복 가능한 지불로 인해 더 많은 비용 발생 가능

→ 각 개인에게 수수료 부과
→ 대리인 비용
→ 소액의 일상적 거래 가능성 제한
→ 분쟁 가능성

03 비트코인의 탄생

제 3자를 필요로 하지 않고 서로 직접 거래가 가능한 전자 화폐 시스템은 없을까?



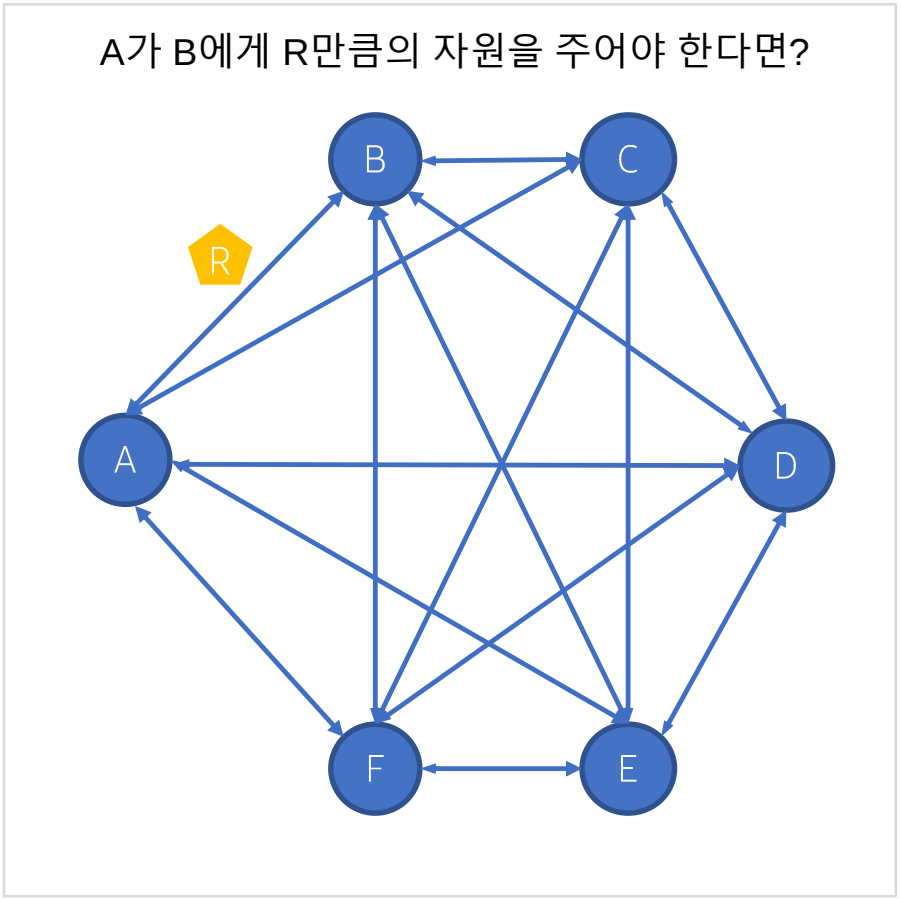
[P2P - 암호화 기술에 의한 전자지불 시스템]

목표:

- 자발적인 두 거래자가 제 3자인 금융기관 (신용기관) 없이도 직접적인 거래가 가능하도록 하자!
- 전산적으로 철회가 불가능한 거래를 통해 판매자를 보호하자.

03 비트코인의 탄생

제 3자를 필요로 하지 않고 서로 직접 거래가 가능한 전자 화폐 시스템은 없을까?



[P2P - 암호화 기술에 의한 전자지불 시스템]

목표:

- 자발적인 두 거래자가 제 3자인 금융기관 (신용기관) 없이도 직접적인 거래가 가능하도록 하자!
- 전산적으로 철회가 불가능한 거래를 통해 판매자를 보호하자.

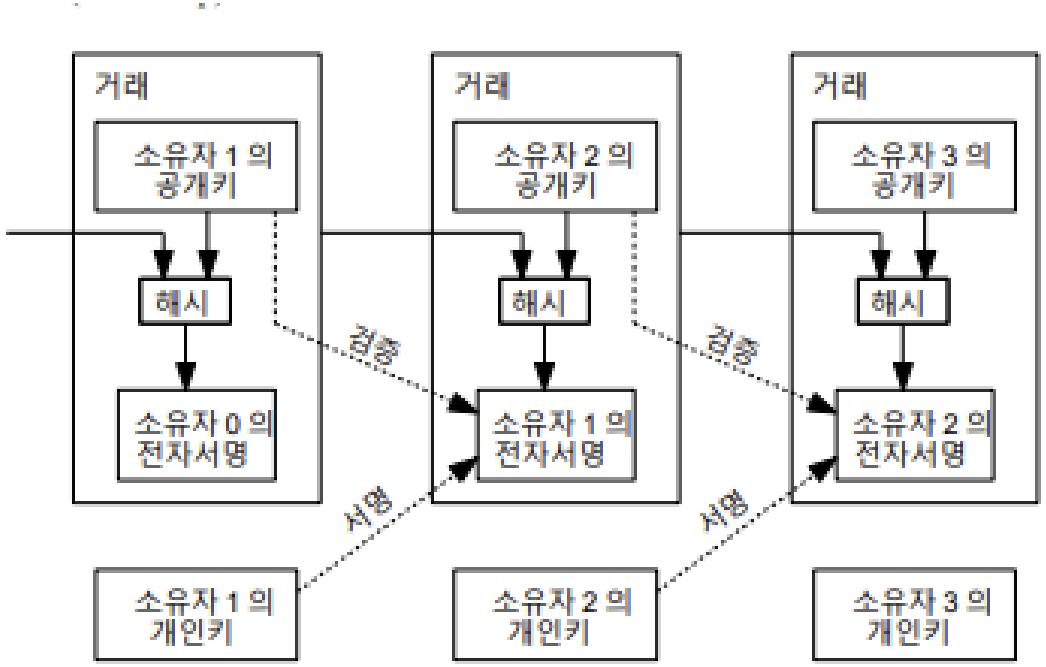
거래들의 **시간 순서를 전산적으로 입증하게 만들도록 하는 P2P 분산 네트워크 기반**을 이용하자

= 거래 시간순의 전산적 증명을 생성하는 P2P 분산 타임스탬프 서버

03 비트코인의 탄생

디지털 서명의 체인으로써 전자회폐를 정의

[P2P - 암호화 기술에 의한 전자지불 시스템]



- 각 개인키(private key) 소유자들은 먼젓번 거래 내역에 다음 소유자의 공개키의 해시값에 전자적으로 서명을 하고 이 정보를 이 화폐의 끝에 첨가한다.
- 거래내역을 + 거래내역의 해시값을 서명함.

암호화?
개인키?
공개키?
해시?
서명?

03 비트코인의 탄생

암호화? 서명? 공개키? 개인키?

[대칭키 암호]

- 하나의 비밀키를 양쪽(A & B)가 모두 같이 사용
- 암호화와 복호화에 사용하는 키가 같은 암호화 알고리즘
- 비밀키 하나만 알아내면 암호화된 내용을 해독 가능
- 비밀키 탈취 당할시에 안전 X

[공개키 암호]

- 비밀키 하나 만 가지는 대칭키 암호 방법과 달리, 공개키와 비밀키 두 개가 존재
- 비대칭 암호라고 불림
- 암호화와 복호화에 사용하는 키가 서로 다름
- 암호화할 때의 키는 공개키(public key), 복호화할 때의 키는 개인키(private key)
- 공개키는 누구나 알 수 있지만, 그에 대응하는 개인키는 키의 소유자만이 알 수 있음
- 특정한 비밀키를 가지는 사용자만이 내용을 열어볼 수 있도록 하는 방식.

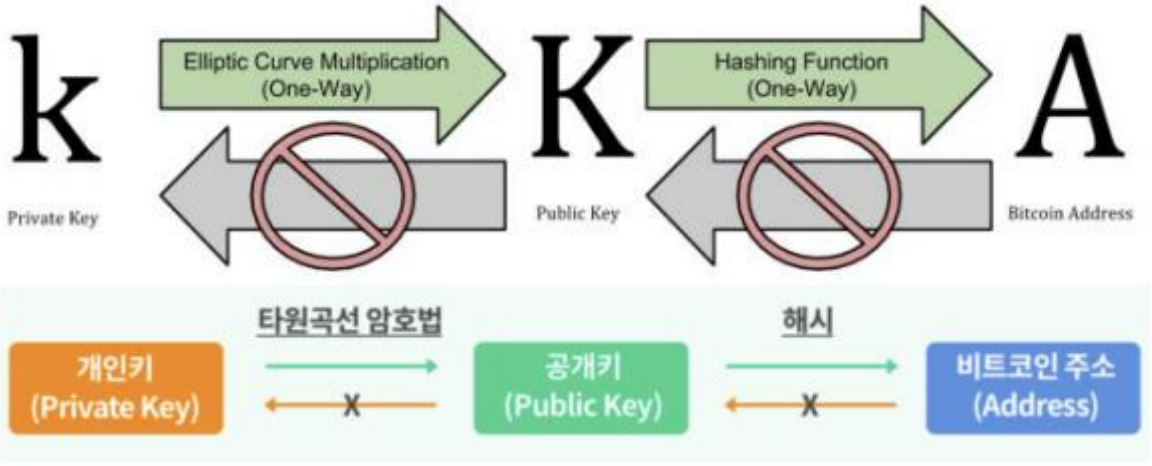
몇몇 알고리즘은 개인키로 암호화하고 공개키로 복호화도 가능함.

- RSA, ECDSA(ECC(타원곡선 Elliptic-curve cryptography))
- 공인인증서, ssl 등에 적용됨.

비트코인의 전자서명에는 양방향 공개키 방식인 ECDSA알고리즘 사용

03 비트코인의 탄생

암호화?



- ECDSA(Elliptic Curve Digital Signature Algorithm)으로 개인키(Private Key), 공개키(Public Key) 생성
- ECDSA 방식은 RSA(소인수분해문제) 알고리즘보다 훨씬 짧은 키 길이, 빠른 연산속도를 가지면서 비슷한 수준의 보안성 제공

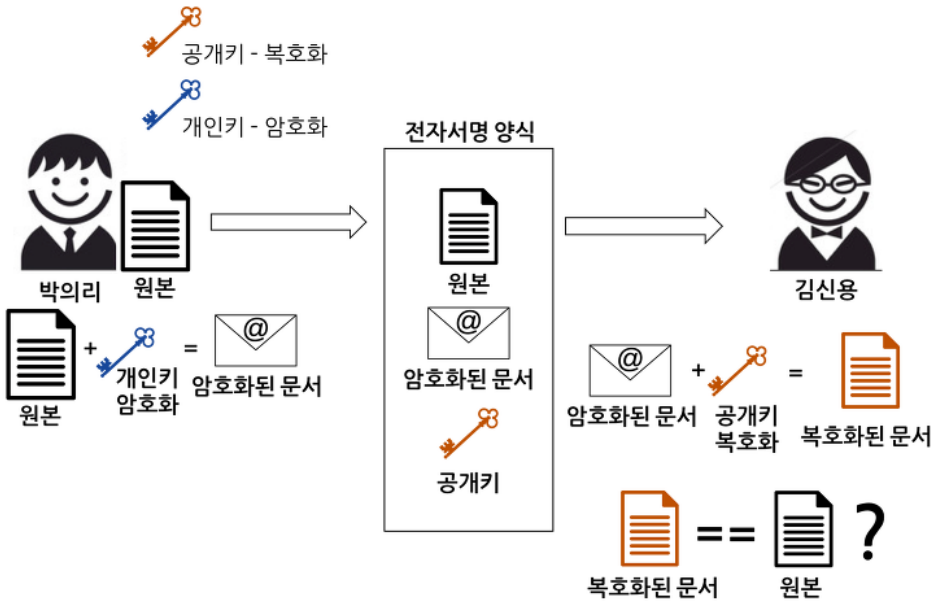


그림5. 전자서명을 위한 공개키 사용

출처: 공인인증서와 블록체인을 이용한 공동인증

03 비트코인의 탄생

해시 알고리즘?

[SHA256] - Secure Hash Algorithm

- 비트코인은 해시(Hash) 함수 중 **하나인 SHA-256(Secure Hash Algorithm, 해시 값의 길이 256 비트)**을 사용하고 있음.
- SHA256은 미국 국가안보국(NSA)이 1993년에 SHA(Secure Hash Algorithm)를 설계하여 국가표준으로 정하였고, 이후 발전된 형태의 **SHA256(32바이트, 256비트, 16진수, 64자리)**은 많은 정보시스템에서 보안 프로토콜로 사용하고 비트코인도 이 방식을 채택하였음

[ASCII 코드]

ASCII	10진수	16진수	2진수
널(null)	0	0	0
헤더 시작	1	1	1
텍스트 시작	2	2	10
수직 탭	11	B	1011
용지 넘김	12	C	1100
캐리지 리턴(CR)	13	D	1101
시프트 아웃	14	E	1110
시프트 인	15	F	1111
데이터 링크 이스케이프	16	10	10000
장치 제어 1/Xon	17	11	10001
장치 제어 2	18	12	10010
장치 제어 3/Xoff	19	13	10011
장치 제어 4	20	14	10100
부정 응답	21	15	10101
동기식 유휴	22	16	10110
전송 블록의 끝	23	17	10111
취소	24	18	11000
미디어 끝	25	19	11001
파일의 끝(EOF)/대체	26	1A	11010
이스케이프	27	1B	11011
파일 구분자	28	1C	11100
그룹 구분자	29	1D	11101
레코드 구분자	30	1E	11110
단위 구분자	31	1F	11111

```
01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F
4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C
6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20
73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66
6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05
```

ASCII	10진수	16진수	2진수
공백	32	20	100000
!	33	21	100001
"	34	22	100010
+	43	2B	101011
,	44	2C	101100
-	45	2D	101101
.	46	2E	101110
/	47	2F	101111
0	48	30	110000
1	49	31	110001
2	50	32	110010
3	51	33	110011
4	52	34	110100
5	53	35	110101
6	54	36	110110
7	55	37	110111
8	56	38	111000
9	57	39	111001
:	58	3A	111010
;	59	3B	111011
<	60	3C	111100
=	61	3D	111101
>	62	3E	111110
?	63	3F	111111
@	64	40	1000000

ASCII	10진수	16진수	2진수
A	65	41	1000001
B	66	42	1000010
C	67	43	1000011
D	68	44	1000100
E	69	45	1000101
F	70	46	1000110
G	71	47	1000111
H	72	48	1001000
I	73	49	1001001
J	74	4A	1001010
K	75	4B	1001011
L	76	4C	1001100
M	77	4D	1001101
N	78	4E	1001110
O	79	4F	1001111
P	80	50	1010000
Q	81	51	1010001
R	82	52	1010010
S	83	53	1010011
T	84	54	1010100
U	85	55	1010101
V	86	56	1010110
W	87	57	1010111
X	88	58	1011000
Y	89	59	1011001
Z	90	5A	1011010
[	91	5B	1011011
₩	92	5C	1011100
]	93	5D	1011101
^	94	5E	1011110
_	95	5F	1011111
`	96	60	1100000

ASCII	10진수	16진수	2진수
a	97	61	1100001
b	98	62	1100010
c	99	63	1100011
d	100	64	1100100
e	101	65	1100101
f	102	66	1100110
g	103	67	1100111
h	104	68	1101000
i	105	69	1101001
j	106	6A	1101010
k	107	6B	1101011
l	108	6C	1101100
m	109	6D	1101101
n	110	6E	1101110
o	111	6F	1101111
p	112	70	1110000
q	113	71	1110001
r	114	72	1110010
s	115	73	1110011
t	116	74	1110100
u	117	75	1110101
v	118	76	1110110
w	119	77	1110111
x	120	78	1111000
y	121	79	1111001
z	122	7A	1111010
{	123	7B	1111011
|	124	7C	1111100
}	125	7D	1111101
~	126	7E	1111110
DEL	127	7F	1111111

03 비트코인의 탄생

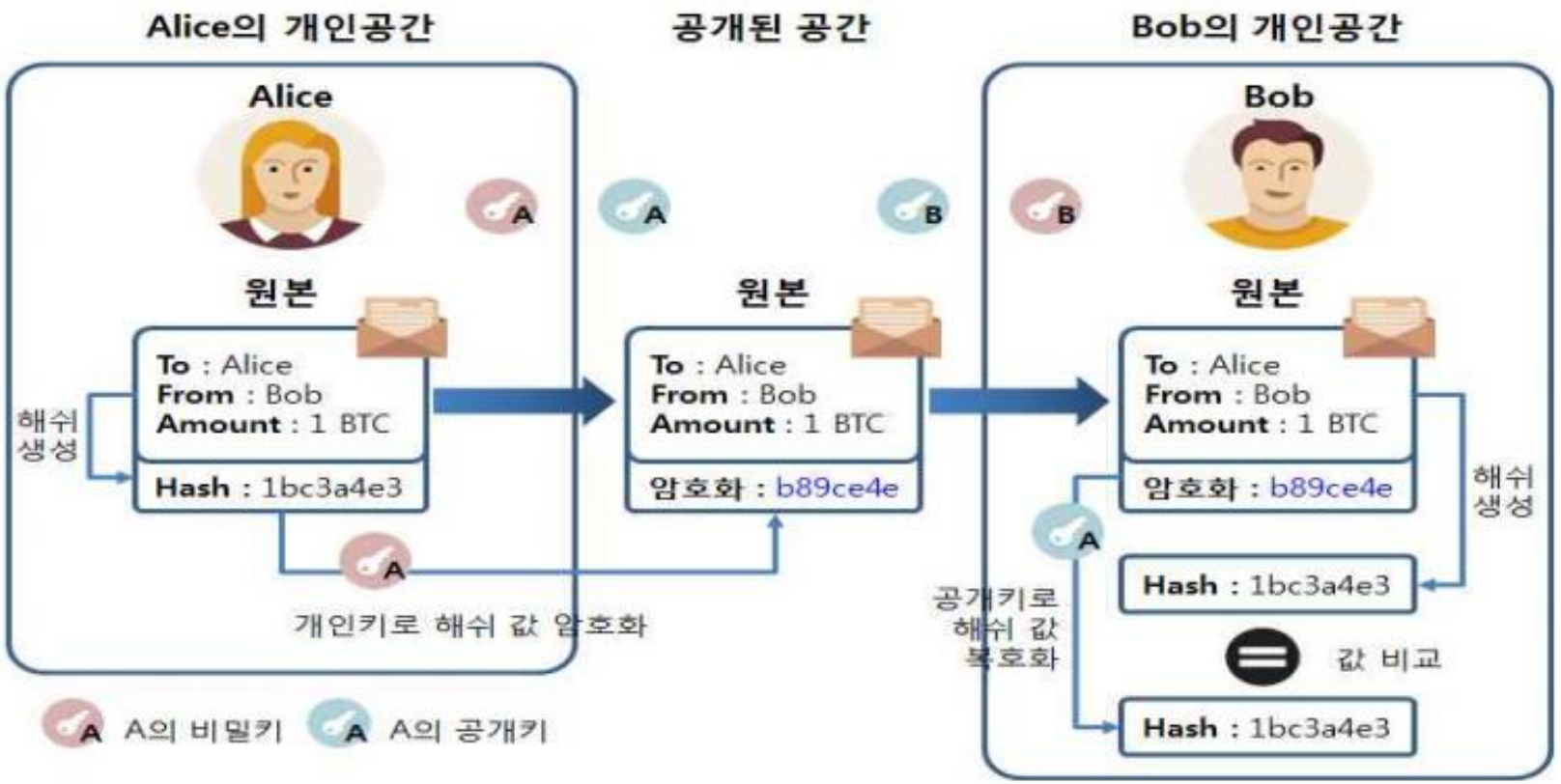
SHA256은 항상 임의의 입력 값에 매칭되는 고정된 출력 값(16진수, 64자리)을 갖고 암호화되며, 반대의 출력 값으로 입력 값을 찾는 복호화가 불가능한 단방향 특징

Input Data	Output Hash Value (SHA256)
0	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
1	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
01	938DB8C9F82C8CB58D3F3EF4FD250036A48D26A712753D2FDE5ABD03A85CABF4
A	559AEAD08264D5795D3909718CDD05ABD49572E84FE55590EEF31A88A08FDFFD
가	64EE5293D31BC58B72D76AE9A86A902E90442428E29F24F4ECB257BA841CDD36
A가	0C8DC5BB6E54005C98BBBEAC828250B7F79E29DC40DAA9CC2A7CB4A13AB83AE3
01A가	796C93436B73B7EDC2DD1F99C779C3F55577797451BBC1B6806658461F670D0B

Input Data	Output Hash Value (SHA256)
Attack at 9PM!	C53AE0B1DB6F94CE4177112D386C8BDF2F1B1D949F5A19F47D473A785DC97AFC
Attack at 9PM!0	8EB6977A5765FDA7CF7DE37E6BE6C420841CBA27B7EDE2B3C371AB6C9ADC41A0
Attack at 9PM!1	E3FB7A263A560F5B38A4B44FB394DFB3CD686944A906E76E28CEDDF481F815B8
Attack at 9PM!40	01F419F4C9FF3EAD7B79C646B14FB56DA73BA6267BE39B1C17A7828003164C62
Attack at 9PM!6541	000C007D99DB7909EAFCD9B39B7C92CB41410BF2A7E5D5E6D9873C240B36C312

03 비트코인의 탄생

디지털 서명의 체인으로써 전자회폐를 정의



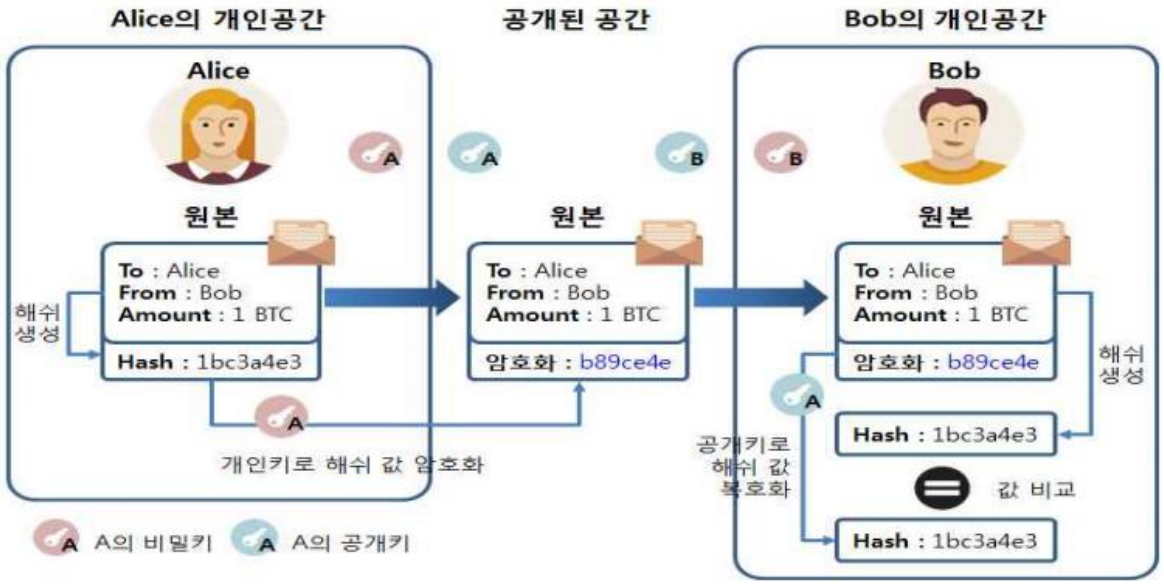
출처 : 금융보안원

- 메시지와 공개키 모두를 알 수 있다면 변조된 메시지를 보낼 수 있기 때문에, 실제로는 수신측의 공개키만을 사용하여 암호화하는 경우는 드물다.

- 송수신 양측의 키쌍을 사용하는 방법으로는 A의 개인키로 암호화 -> A의 공개키로 복호화로 구성된 방식이 일반적이다

03 비트코인의 탄생

디지털 서명의 체인으로써 전자회폐를 정의

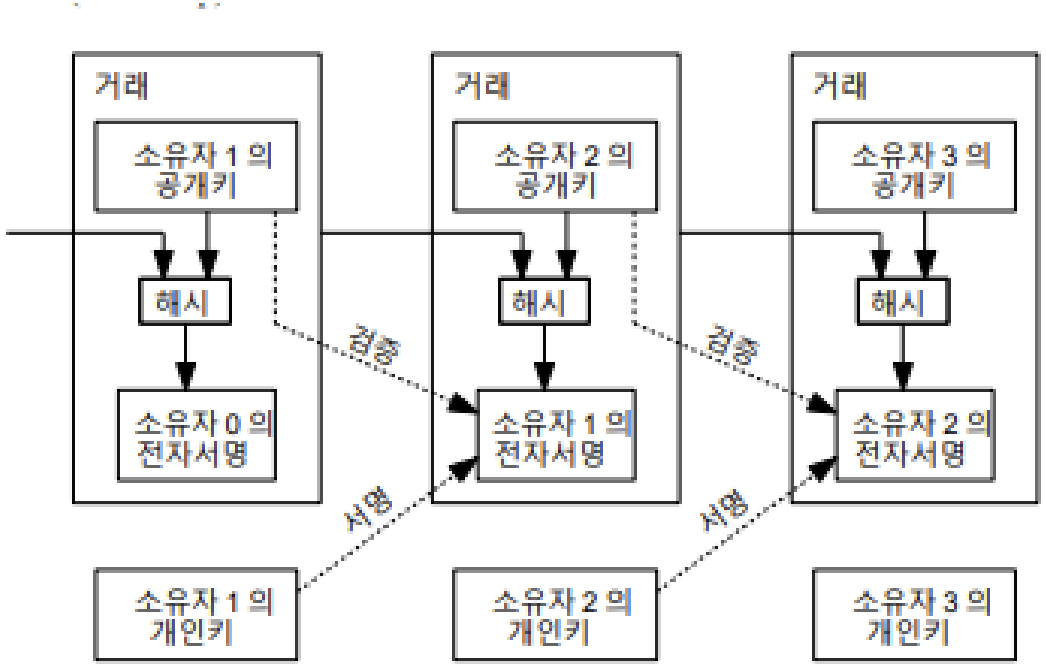


- Alice는 Bob에게 1BTC을 보내기 위한 거래 전문과 해시 값을 생성한 후 Alice의 개인키를 이용하여 해시 값을 암호화함
- 거래 전문과 암호화된 거래 전문의 해시 값을 Bob에게 전송
- Bob은 거래 전문 정보로 해시 값을 만들고, 암호화된 해시 값을 Alice의 공개키로 복호화 한 후 생성된 해시 값과 비교하여 무결성을 검증함

출처 : 금융보안원

03 비트코인의 탄생

디지털 서명의 체인으로써 전자회폐를 정의



[비트코인에서의 이중 거래 문제 발생 가능성]

- 이중 거래 문제를 해결하기 위해선 거래를 마칠 때 마다 제 3자가 검증을 해야한다.

목표:
- 자발적인 두 거래자가 제 3자인 금융기관 (신용기관) 없이도 직접적인 거래가 가능하도록 하자!

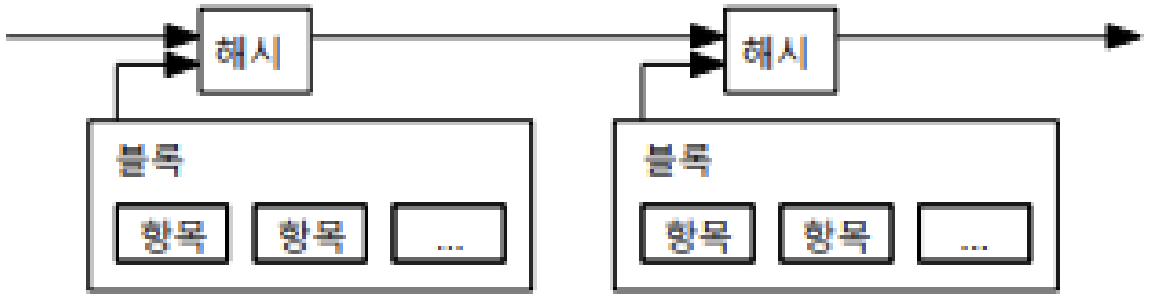
이중 거래 문제를 P2P로 해결하기 위해선, 모든 거래를 인식해야 함!

- 거래는 반드시 공개적으로 알려져야 한다
- 참가자들이 거래의 순서에 대한 단일 기록에 동의할 수 있는 시스템이 필요
- 수취인은 매 거래마다 과반수의 노드들이 그것이 첫 사용이라고 동의해주는 증명이 필요

최초의 블록 하나를 인정하고 모든 거래는 공개적으로 알려져야 하고, 참가자들에게는 그걸 받은 순서의 단일한 이력에 합의하는 시스템이 필요하다.

03 비트코인의 탄생

타임스탬프 서버



[비트코인에서의 이중 거래 문제 해법]

- 거래들의 시간 순서를 전산적으로 입증하게 만들도록 하는 P2P 분산 네트워크 기반을 이용
- 타임스탬프 서버를 이용

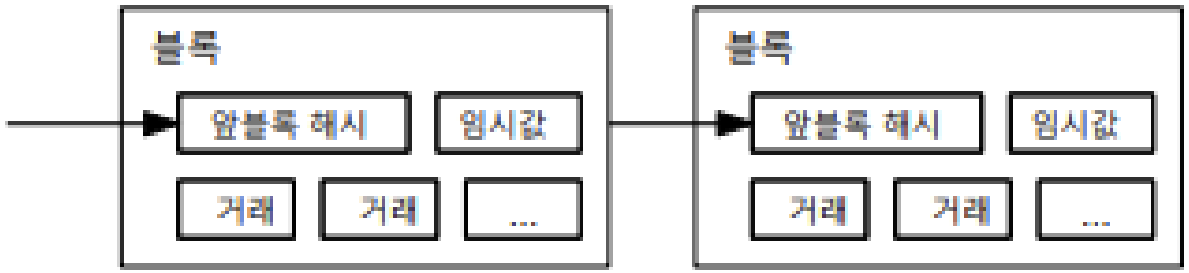
:

타임 스탬프가 찍힌 항목 블록의 해시를 계산해 넓게 퍼뜨리는 방식으로 동작.

- 해딩 시점에 그 데이터가 해시 계산에 들어가기 위해 명백히 존재했음을 증명
- 각 타임스탬프는 이전 타임스탬프를 해시에 포함하여 이전 타임스탬프들을 하나씩 연장하는 타임스탬프가 찍힌 체인을 생성

03 비트코인의 탄생

P2P기반의 분산 타임스탬프 서버



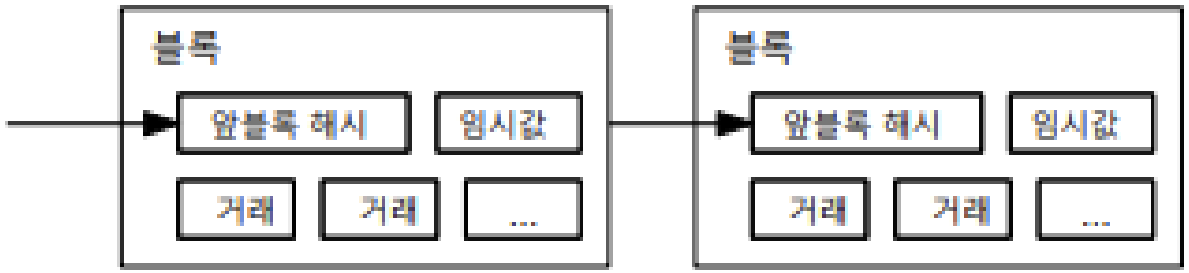
[작업증명 (PoW) 시스템이 필요함.]

P2P 기반에 분산 네트워크 타임스탬프 서버를 구현하기 위해서는 애덤 백의 해시캐시(Adam Back's Hashcash)와 유사한 **작업증명 시스템**이 필요 (컴퓨터의 작업량을 증명할 수 있는 시스템)
작업 증명은 **SHA256같은 걸로 해시 연산을 거친 결과가 0비트(zero bits) 여러 개로 시작할, 특정값을 찾는 작업을 수반**.
여기에 평균적으로 필요한 연산 과정은 0비트 개수에 따라 지수적으로 달라진다.

작업증명 시스템이 필요하다.
작업증명 Proof of Work (PoW)

03 비트코인의 탄생

작업증명 (Proof of Work) PoW

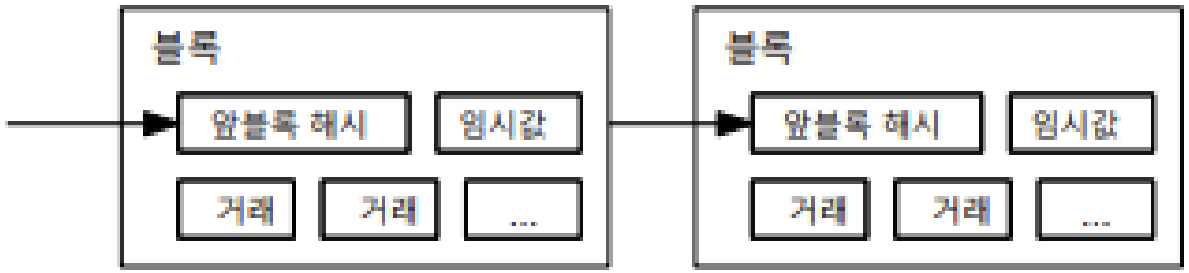


- 작업증명은 SHA256같은 해시 연산을 거친 결과가 0비트 여러 개로 시작할 특정 값을 찾는 작업
- 비트코인의 작업증명: 블록의 해시에 필요한 0비트를 주는 값이 발견될 때까지 블록 안에 임시값**(nonce)**을 증분하는 것으로 구현.
- 한 개의 CPU당 한번에 투표하는 구조.

노드들은 항상 가장 긴 체인을 올바른 것으로 간주하며 그 체인을 확장함

03 비트코인의 탄생

만약 공격자(위조자)가 이중거래를 요청하거나 변조한다면?



[다수결에 의한 의사결정]

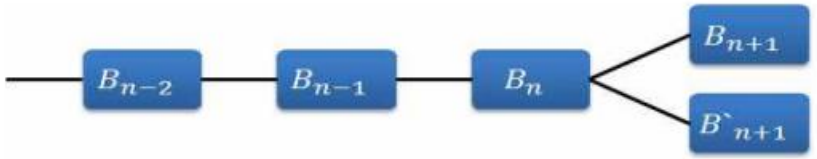
- IP하나당 1표라면 많은 IP를 할당할 수 있는 이에 의해 장악 될 수 있음. → CPU당 1표
- 다수결 의사가 의미하는 바 = 최다 작업증명 동작이 투입된 사슬 = 가장 긴 사슬
- **만약 다수 CPU 파워가 정직한 노드에 의해 통제된다면, 가장 정직한 사슬이 가장 빠르게 늘어나 다른 경쟁 사슬을 모두 압도.**

- **만약 과거 블록을 변경하려면 공격자는 그 블록과 그 뒤를 잇는 모든 블록의 작업증명을 재수행해야 하고, 정직한 노드들의 해시파워를 앞질러야함. (블록이 추가될 수록 지수적으로 감소)**

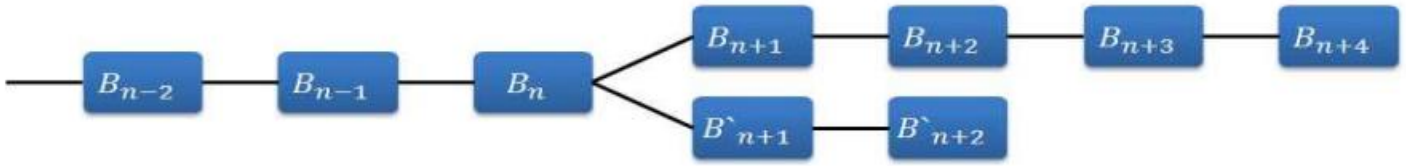
03 비트코인의 탄생

만약 공격자(위조자)가 이중거래를 요청하거나 변조한다면?

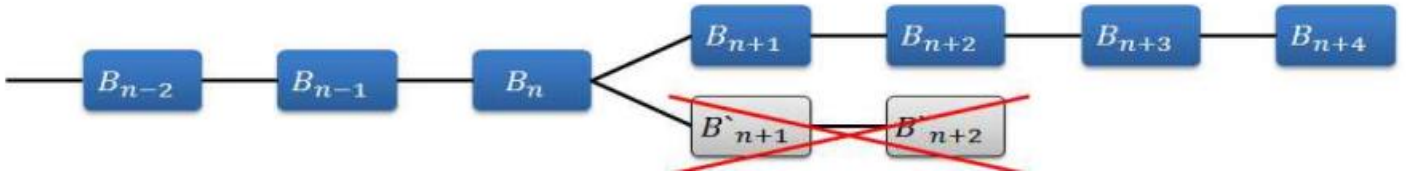
1) 이용자가 비트코인을 중복으로 사용하여 그 거래 내역이 서로 다른 노드들로 전송되면, 두 개의 블록이 생성됨



2) 채굴자들은 두 개의 블록을 가지고 경쟁적으로 다음 블록을 생성



3) 결국 경쟁에서 진 체인은 자연스럽게 소멸



03 비트코인의 탄생

비트코인 네트워크 동작 특징

[네트워크 실행 단계]

1. 새로운 거래가 모든 노드에 브로드캐스트 됨
2. 각 노드가 새로운 거래를 블록에 수집함
3. 각 노드가 그 블록에 맞는 난도의 작업증명을 찾기 시작
4. 노드가 작업증명을 찾은 시점에, 거기서 모든 노드로 그 블록을 브로드캐스트
5. 노드는 모든 거래가 유효하며 아직 지불되지 않았다는 조건에 맞을경우에 그 블록을 승인**(이중거래 문제 해결)**
6. 노드는 블록 승인을 표현하기 위해 먼젓번 해시로 승인된 블록의 해시를 사용해 사슬 안에 다음 블록을 생성함.

03 비트코인의 탄생

비트코인 네트워크 동작 특징

[네트워크 실행 단계]

1. 새로운 거래가 모든 노드에 브로드캐스트 됨
2. 각 노드가 새로운 거래를 블록에 수집함
3. 각 노드가 그 블록에 맞는 난도의 작업증명을 찾기 시작
4. 노드가 작업증명을 찾은 시점에, 거기서 모든 노드로 그 블록을 브로드캐스트
5. 노드는 모든 거래가 유효하며 아직 지불되지 않았다는 조건에 맞을경우에 그 블록을 승인**(이중거래 문제 해결)**
6. 노드는 블록 승인을 표현하기 위해 먼젓번 해시로 승인된 블록의 해시를 사용해 사슬 안에 다음 블록을 생성함.

- 노드들은 **항상 가장 긴 체인을 올바른 것으로 간주**하며 그 체인을 확장함
- **두 노드가 서로 다른 다음 블록을 동시에 브로드캐스트했다면, 노드들마다 서로 다른 블록을 먼저 받게 될 수 있음**
- 기본적으로 먼저 받은 것의 작업이 우선되지만 **다른 블록을 포함한 체인이 더 길어지는것에 대비하여 다른 브랜치도 보관**
- **다음 작업 증명이 발견되어 한 브랜치가 더 길어지면 노드들은 긴 브랜치의 작업으로 전환**됨

03 비트코인의 탄생

비트코인 네트워크 동작 특징

[네트워크 실행 단계]

1. 새로운 거래가 모든 노드에 브로드캐스트 됨
2. 각 노드가 새로운 거래를 블록에 수집함
3. 각 노드가 그 블록에 맞는 난도의 작업증명을 찾기 시작
4. 노드가 작업증명을 찾은 시점에, 거기서 모든 노드로 그 블록을 브로드캐스트
5. 노드는 모든 거래가 유효하며 아직 지불되지 않았다는 조건에 맞을경우에 그 블록을 승인**(이중거래 문제 해결)**
6. 노드는 블록 승인을 표현하기 위해 먼젓번 해시로 승인된 블록의 해시를 사용해 사슬 안에 다음 블록을 생성함.

- 새 거래들의 브로드캐스트가 꼭 모든 노드에 도달할 필요는 없음
- **많은 노드에 도달하면 결국 블록에 포함**됨
- **블록 브로드캐스트는 메시지 유실에도 취약하지 않음(**어떤 노드가 블록을 받지 못하면 다음 블록을 받았을 때 해당 블록이 다시 재요청함)

03 비트코인의 탄생

그럼 왜 노드들이 작업증명에 참여해야 하는가?
인센티브!

제네시스 블록: 최초블록
블록의 첫 거래내역은 약속에 의해 최초 블록을 생성한 사람에게 새로운 코인을 소유할 수 있게 해주는 특별한 거래.

- 화폐를 발행하는 중앙기관 없이 노드가 네트워크를 지원할 인센티브를 더해 주며 초기에 발행한 화폐를 유통할 방법을 제공
- 새 화폐를 일정량 꾸준히 추가하는 것 = 금 채굴자가 금 채굴을 위해 자원을 소비하는 것 = CPU 시간과 전기라는 자원 소비
- 인센티브 = 채굴 (소비 자원은 컴퓨팅 시간과 소비전기)

03 비트코인의 탄생

그럼 왜 노드들이 작업증명에 참여해야 하는가?
인센티브!

[인센티브 - 거래 수수료]

- 만약 거래에서 도출된 가치가 투입된 가치보다 작다면, 그 차이가 거래를 포함한 블록의 인센티브 가치에 더해질 **거래수수료**
- **애초 정해 놓은 수만큼의 화폐가 유통되면, 인센티브는 전부 거래 수수료로 바뀌어 인플레이션으로부터 자유로워짐**

03 비트코인의 탄생

그럼 왜 노드들이 작업증명에 참여해야 하는가?
인센티브!

[인센티브의 필요성]

노드들이 정직함을 유지하는 것에 도움
- 공격자가 모든 정직한 노드들보다 더 큰 컴퓨팅 파워를 가졌을 때? (51% 공격)

선택A. 지불한 것들을 훔쳐서 사람들을 속이는 것
선택B. 새로운 코인을 생성하는 것(규칙대로 움직이는 것)

→ 시스템과 그가 보유한 부의 유효성을 해치는 것보다 신규 코인을 생성하는 규칙에 따라 행동할 확률이 높음

03 비트코인의 탄생

너무 많은 체인들이 쌓이면..
[저장공간 관리]

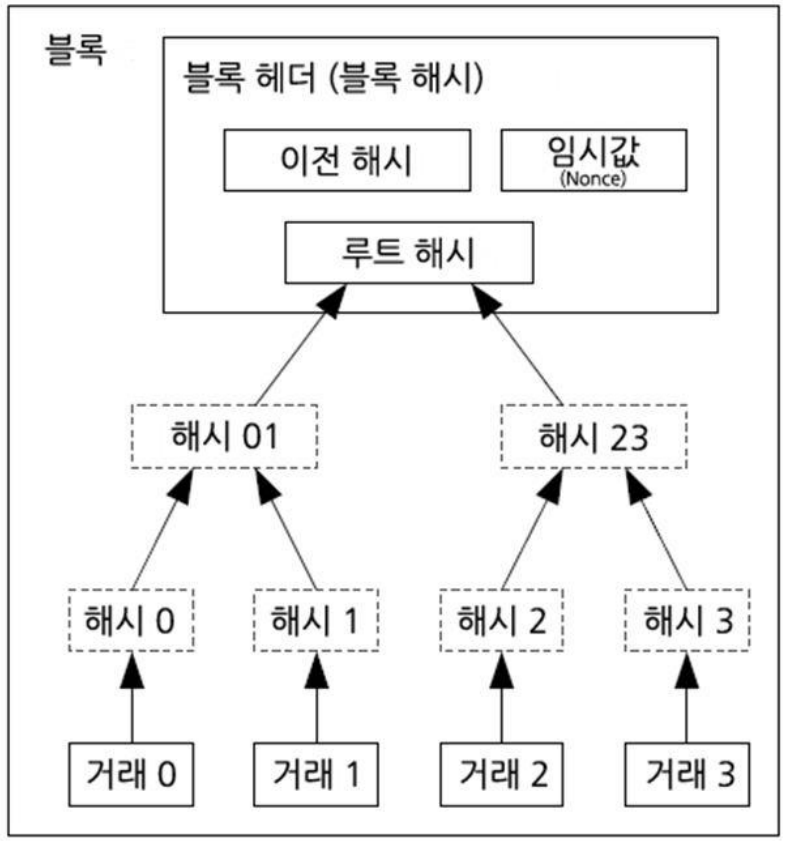
최종 거래가 많은 블록들에 묻히면, 그 이전에 사용된 거래는 저장공간 절약을 위해 폐기될 수 있음.

[블록 해시를 망가뜨리지 않고 해결하는 방법]

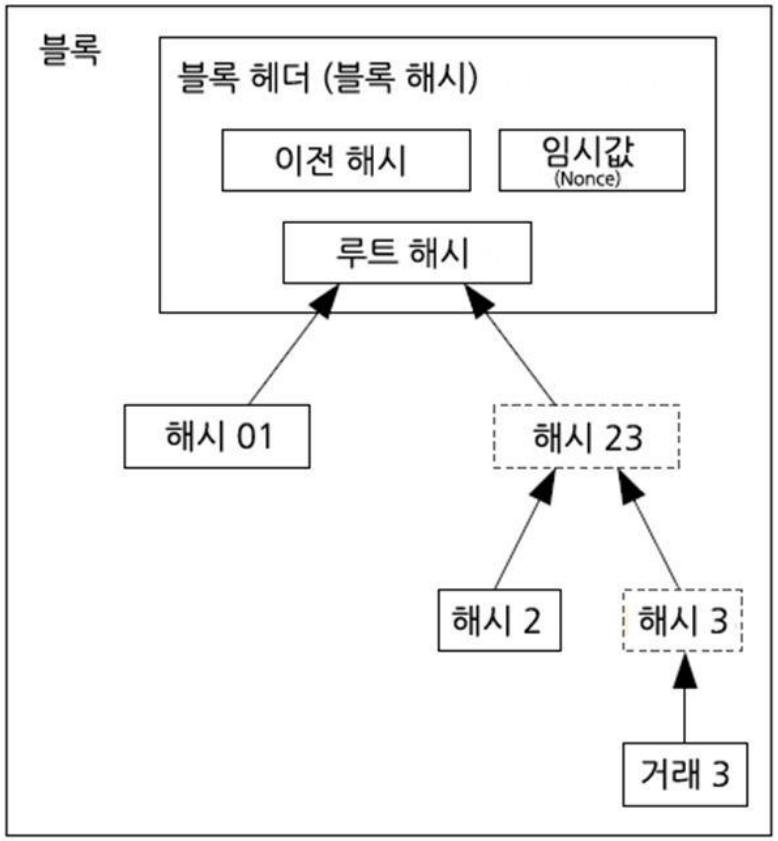
- 거래들은 **머클 트리(Merkle Tree)**안에 해시되어 저장되며, 루트(root)만 해당 블록의 해시에 포함
- 오래된 블록은 트리의 가지들을 잘라내고 결과적으로 압축됨

03 비트코인의 탄생

너무 많은 체인들이 쌓이면..
[저장공간 관리]



머클트리 구조로 해시된 거래 내역들



블록에서 거래 내역 0~2를 제거 후

03 비트코인의 탄생

전체 네트워크 노드를 구동하지 않고 검증이 가능

[가장 긴 작업증명 체인의 블록 헤더들의 사본만 유지]

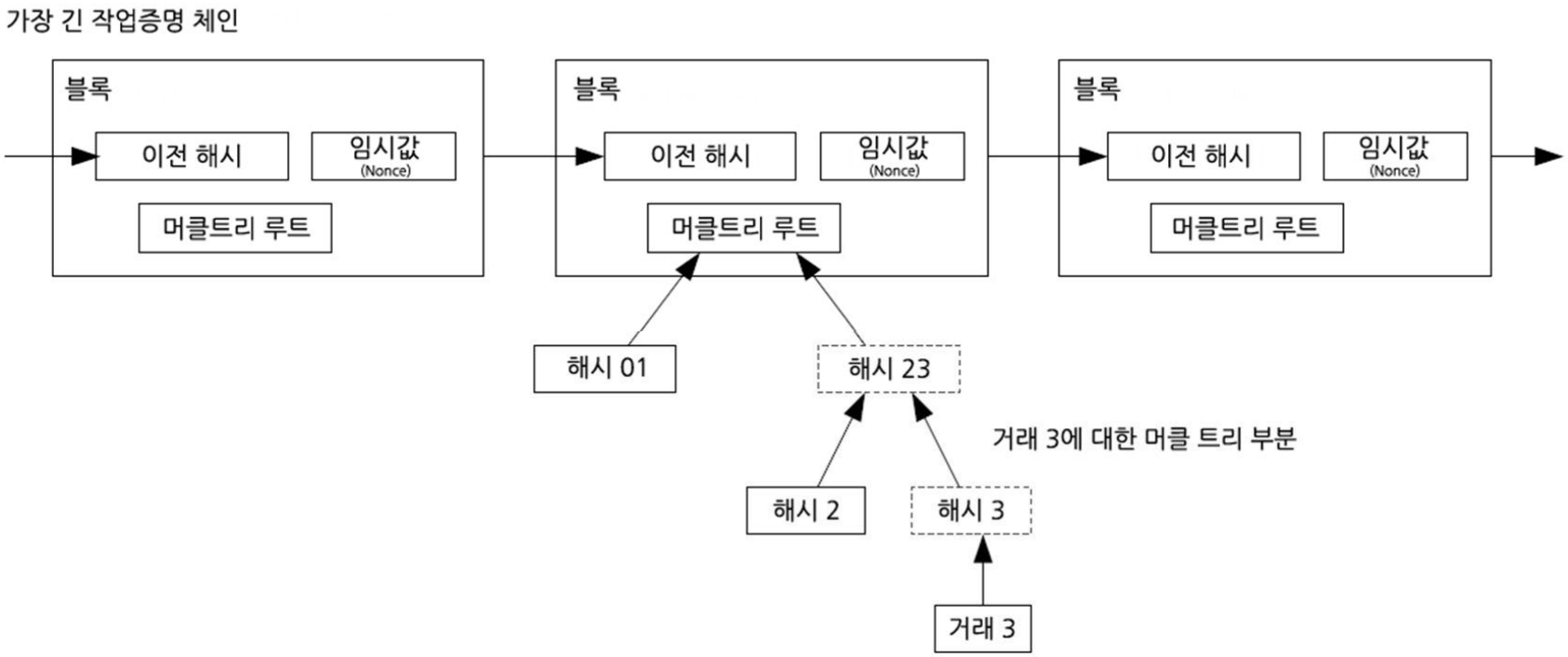
- 자신이 가장 긴 체인이라 확신할 때까지 네트워크 노드들에게 요청
- 그 거래내역이 기록된 블록에 연결된 머클트리 일부만 받아옴

[사용자는 스스로 거래내역 확인X]

- 체인의 한 부분에 연결함으로써 네트워크 노드가 해당 거래를 받아들이는지 확인 필요
- 그 후에 추가되는 블록들이 네트워크가 받아들이는지 추가로 확인

03 비트코인의 탄생

전체 네트워크 노드를 구동하지 않고 검증이 가능



필요한 건 머클트리뿐

03 비트코인의 탄생

금액 병합과 분할

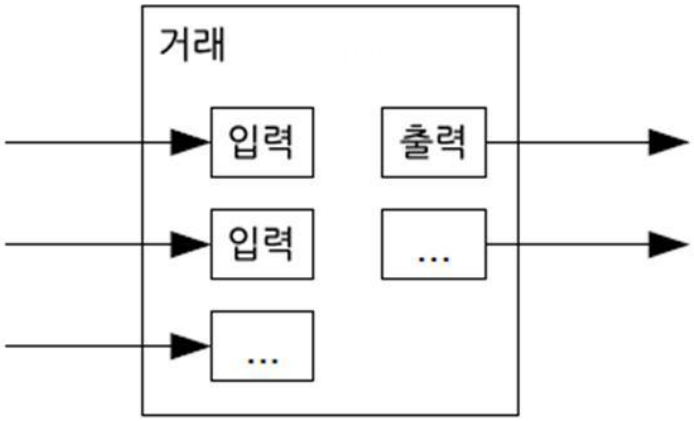
[개별적으로 다루는 것은 가능하지만 송금의 모든 잔돈을 개별적인 거래로 만드는 것은 어렵다]

- 금액을 나누거나 합치는 것이 가능하도록, 한 거래는 여러 개의 입출력을 포함
- 일반적으로 더 큰 이전의 거래로부터 오는 단일 입력 또는 작은 금액들로 구성된 여러 개의 입력 그리고 최대 두 개의 출력 존재. => 지불을 위한것 + 입금자에게 보낼 거스름돈

모든 거래를 개별거래로 만드는 것은 어렵다.
하나의 거래 내에서 병합과 분할이 가능토록하자!

03 비트코인의 탄생

금액 병합과 분할



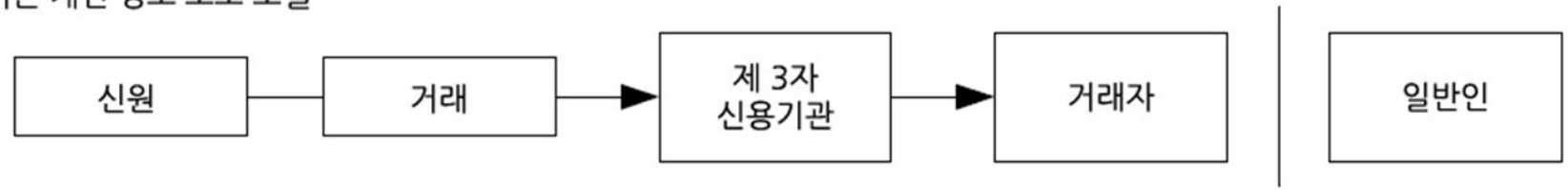
한 거래가 여러 개의 거래들에 의존되고 또 이들은 다시 더 많은 거래들에 의존되는 팬 아웃은 본 환경에서는 문제가 되지 않음

- 거래 내역의 완전한 독립사본을 추출해야 할 필요는 없음

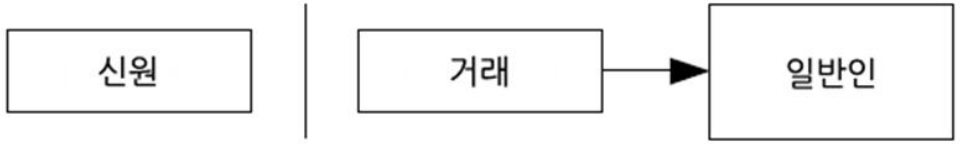
03 비트코인의 탄생

프라이버시는?

기존 개인 정보 보호 모델



새로운 개인 정보 보호 모델



- 전통적인 은행 모델은 정보 접근 권한을 거래 당사자들과 신뢰할 수 있는 제 3자에게만 제공
  - 모든 거래를 공개적으로 알려야 하는 본 백서의 방식 특성상 전통적 은행 모델 방식을 불가능하게 함
    - 하지만 정보의 흐름을 다른 면에서 차단함으로써 프라이버시 보호가 여전히 가능
    - Public은 누군가가 다른 누구와의 거래내역을 볼 수 있지만 특정인과의 연결지을 수 있는 정보가 없기 때문

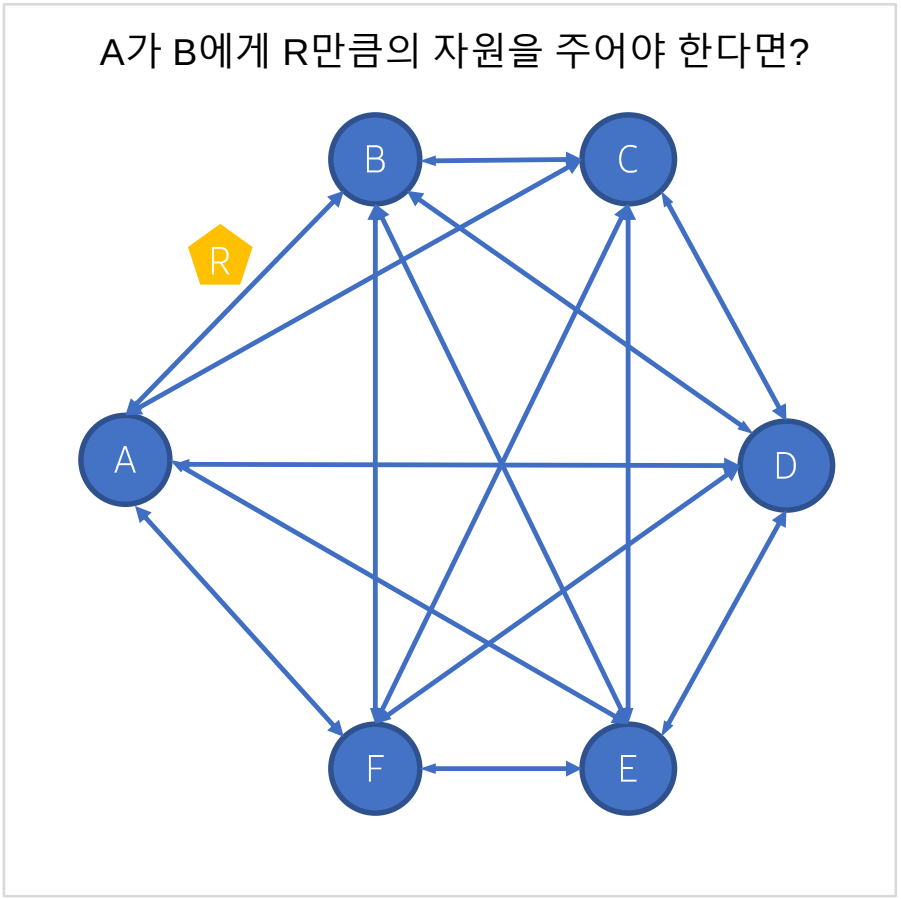
03 비트코인의 탄생

프라이버시는?

[**각 거래마다 새로운 키 쌍이 사용되면 그게 어떤 공통된 소유자에게 연결되는 일을 피할 수 있음**.]
- 여러 개의 입력을 가지는 거래의 경우에는 해당 입력들이 동일한 소유자의 것임이 드러날수밖에 없음

03 비트코인의 탄생

제 3자를 필요로 하지 않고 서로 직접 거래가 가능한 전자 화폐 시스템 탄생



[P2P - 암호화 기술에 의한 전자지불 시스템]

목표:

- 자발적인 두 거래자가 제 3자인 금융기관 (신용기관) 없이도 직접적인 거래가 가능하도록 하자!
- 전산적으로 철회가 불가능한 거래를 통해 판매자를 보호하자.

거래들의 **시간 순서를 전산적으로 입증하게 만들도록 하는 P2P 분산 네트워크 기반**을 이용하자

= 거래 시간순의 전산적 증명을 생성하는 P2P 분산 타임스탬프 서버

03 비트코인의 탄생

[블록체인의 정의]

- 데이터 분산 저장 기술의 일종
- block 단위의 데이터를 chain처럼 연결하여 저장
- 저장된 데이터를 모든 사용자에게 분산하여 저장
- 이러한 **분산저장** 특성 때문에 분산원장기술 (분산장부기술, Distributed Ledger Technology) 이라고 불리기도 함

[비트코인의 목표값 및 해시값 검증]

- 데이터 분산 저장 기술의 일종
- block 단위의 데이터를 chain처럼 연결하여 저장
- 저장된 데이터를 모든 사용자에게 분산하여 저장
- 이러한 분산저장 특성 때문에 분산원장기술 (분산장부기술, Distributed Ledger Technology) 이라고 불리기도 함

03 비트코인의 탄생

[위키백과]
블록체인은 관리 대상 데이터를 '블록'이라고 하는 **소규모 데이터들이 P2P 방식**을 기반으로 생성된 **체인 형태의 연결고리 기반 분산 데이터 저장 환경**에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 **분산 컴퓨팅 기술 기반의 원장 관리 기술**이다. 이는 근본적으로 **분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안**되었다. 블록체인 기술은 비트코인을 비롯한 대부분의 암호화폐 거래에 사용된다. 암호화폐의 거래과정은 탈중앙화된 전자장부에 쓰이기 때문에 블록체인 소프트웨어를 실행하는 많은 사용자들의 각 컴퓨터에서 서버가 운영되어, **중앙에 존재하는 은행 없이 개인 간의 자유로운 거래**가 가능하다.

[Oxford Dictionaries]
A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly.
비트코인 혹은 다른 암호화폐의 거래가 **순차적이고 공개적으로 기록되는 디지털 장부를 의미**

P2P방식, 순차적이고 공개적, 체인 형태, 분산 데이터 저장, 모든 참여 노드에 기록, 임의 조작 불가, 디지털 원장(장부), 중앙에 존재하는 은행 없이 개인 간 자유로운 거래

04 블록체인의 기술의 등장 배경

[등장 배경]

- PC와 스마트폰을 통한 온라인 거래가 보편화되고 사물인터넷(IoT) 기반이 확충되어 온라인-오프라인(O2O) 거래도 증가하면서 금융과 정보통신(ICT)가 접목된 핀테크(Fintech)에 이어 해킹과 위조·변조가 거의 불가능한 거래시스템에 대한 사회적 요구 증대

[암호화폐 출현]

디지털 가상화폐인 '비트코인(Bitcoin)'에 적용된 블록체인(Blockchain) 기술을 금융 거래뿐만 아니라 산업 전반에 적용하려는 새로운 비즈니스 모델 확산

[개념 정의]

- 블록체인은 다양한 정보를 기록한 원장(ledger)을 모든 구성원(node/peer)이 각자 분산(distributed) 관리하고, 주기적 및 새로운 거래가 발생할 때마다 암호방식으로 장부를 검증 및 업데이트하여, **개념적으로는 탈중앙, 보안성, 익명성, 투명성이 강력한 디지털 공공장부 또는 분산원장(distributed ledger)**이라 말할 수 있음.

금융의 경우 비트코인이 등장하기 이전에는 P2P(Peer-to-Peer)에서 구동되는 분권적 금융거래 시스템이 불가능하였는데, **블록체인의 작업증명(Proof of Work)과 분산장부 기술**로 해결

04 블록체인의 기술의 등장 배경

[생각의 확장]

- 블록체인은 컴퓨터 프로그램으로 암호기술을 이용하여 설계한 블록(Block)에 **다양한 정보(거래 내역 뿐만 아니라)를** 담아 체인(Chain)처럼 연결한 것을 말하고, 비트코인은 이를 실제 적용하여 구현한 대표적 사례임

비트코인은 안전한 해시 알고리즘(SHA) 중의 하나인 SHA256 암호방식으로 다수의 참여자 (노드)가 작업증명(Proof of Work)을 통해 블록체인을 만든 것으로 이를 암호화폐(BTC)라 부르며, 새로운 블록이 생성될 때마다 보상(6.25BTC)을 지급함

비트코인의 반감기는 그 채굴량이 절반으로 줄어드는 주기로, 약 4년마다 돌아온다. 2012년 11월 첫 반감기 블록에 대한 보상이 50BTC에서 25BTC로 감소했다. 이후 2016년 25BTC에서 12.5BTC, 2020년 12.5BTC에서 6.25BTC로 줄었다.

05 PoW의 이해

새로운 화폐가 생성되는 과정(조폐)에서, 생성자들(채굴자들)에게 "일을 했다는 것을 증명(proof of work)"하는 것을 강제하여 화폐의 가치와 보안을 보장하는 방식

- 장점: 안정성 - 최초의 P2P방식의 분산원장 방식, Bitcoin Core는 아직 해킹되지 않았음.
- 단점: 거래량/거래속도의 제한, Bitcoin은 3~4 tps, Ethereum 20 tps, paypal 200 tps, Visa Card: 2~40,000 센, 에너지소모 과다, 빈익빈부익부

05 PoW의 이해

[PoW - 작업증명]

비트코인: 최초의 블록체인 기술이 적용된 시스템
합의 알고리즘으로 작업 증명(Proof of Work: PoW)과 가장 긴 체인(Longest Chain)을 선택하는 방법 사용
최대 7 TPS밖에 처리할 수 없는 성능의 한계
작업증명으로 인해 많은 에너지낭비

작업증명으로 부르기도 하며 풀기 어려운 문제를 빨리 해결한 사람에게 블록을 생성할 수 있는 권한을 주고 그 보상으로 코인을 제공

비트코인의 경우 해시 함수의 결과값이 특정 값보다 작아지도록 하는 입력 값(Nonce)을 찾는 문제
비트코인의 경우 약 10분 정도 걸려 풀릴 수 있도록 난이도 조절
비트코인은 Nonce값을 만드는데 SHA-256이라는 알고리즘 사용
SHA(Security Hash Algorithm)은 미국 표준 기술 연구소(NIST)에 의해 공표된 해시 알고리즘
SHA-256은 256비트로 구성되어 64자리 문자열을 반환

PoW코인들
비트코인, 라이트코인 등

05 PoW의 이해

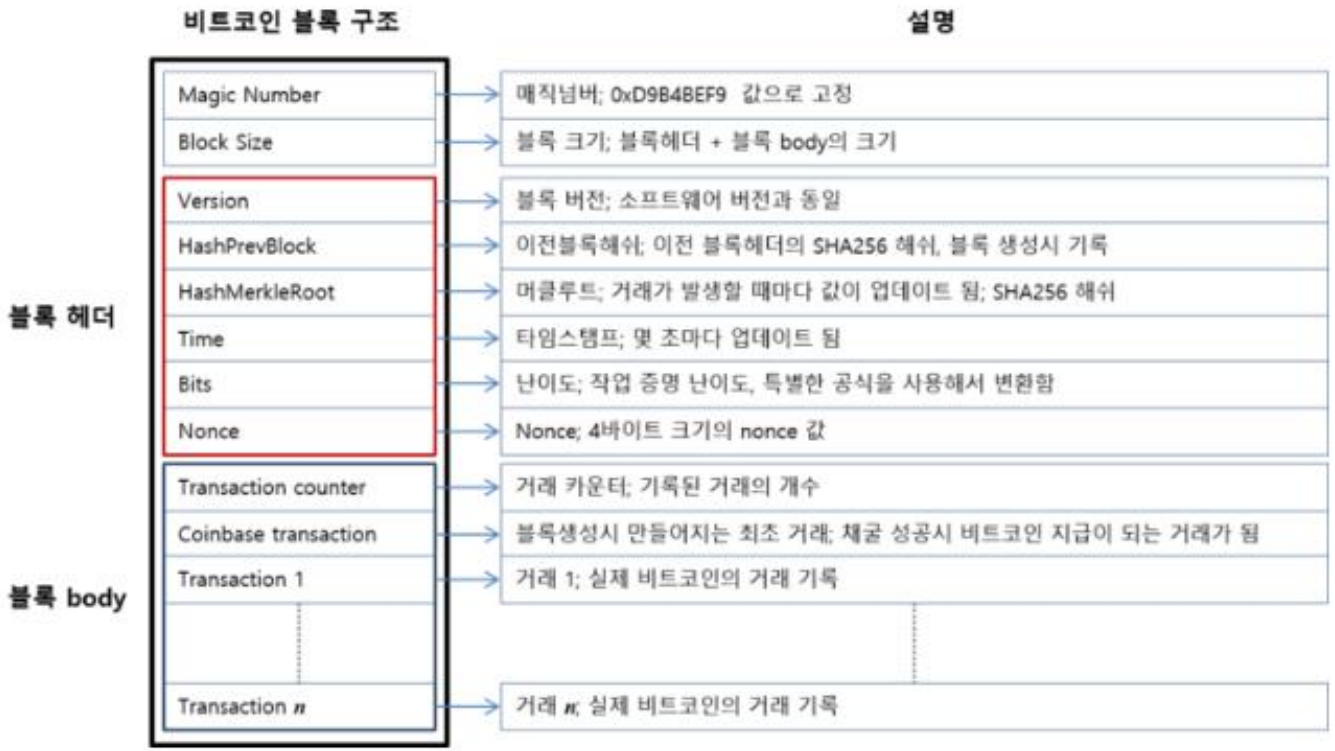
[PoW - 작업증명]

- 채굴자들이 CPU, GPU같은 장비를 통해 해시 함수의 출력 값을 구함
- 해시 함수는 단방향 암호화 기술이므로 결과값으로 입력 값을 찾을 수 없음
  →결과가 나올 때까지 입력 값을 바꿔 지속적으로 실행 해야함
- Nonce값을 구해서 블록해쉬 값을 구하고 이 블록 해쉬값을 식별자로 가지는 유효한 블록을 만들어 내야함
- Nonce값은, 이 Nonce값을 입력값 중의 하나로 해서 계산되는 블록 해쉬값이 특정 숫자보다 작아지게 하는 값을 말한다

05 PoW의 이해

[PoW - 작업증명]

- 작업증명은 SHA256 알고리즘에서 특정 목표값보다 작은 해시값을 구하는 작업(계산)에 참여하고 완결(증명)하는 행위를 의미하며, 비트코인은 수학적으로 약 10분 정도 걸려야 풀 수 있는 (해시의 앞자리 숫자가 0으로 시작되고, 0의 갯수를 조절하는) 난이도 등을 통해 목표값보다 작은 해시값이 되도록 넌스(Nonce)를 찾는 것을 말함



COINBASE TRANSACTION:
새로운 블록이 생성될때 최초로 기록되는 정보

- 무의미한 값 ➔ 작업 증명이 성공시 성공 노드의 비트코인 주소로 입금하는 정보로 변경.

version : 소프트웨어/프로토콜 버전
previousblockhash : 블록 체인에서 바로 앞에 위치하는 블록의 블록 해쉬
merklehash : 개별 거래 정보의 거래 해쉬를 2진 트리 형태로 구성할 때, 트리 루트에 위치하는 해쉬값
time : 블록이 생성된 시간
bits : 난이도 조절용 수치
nonce : 최초 0에서 시작하여 조건을 만족하는 해쉬값을 찾아낼때까지의 1씩 증가하는 계산 회수

https://www.blockchain.com/btc/block/538695

05 PoW의 이해

Bitcoin Block Height #538695 Blocks at depth 538695 in the bitcoin blockchain

Summary	
Height	538695 (Main chain)
Hash	00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda
Previous Block	00000000000000000002669a90eec10d534c158eabe4ef8bd7f6133601f0ab116
Next Blocks	00000000000000000009ef223af6652bbc8736e756e1b276dd429298eb4a3198
Time	2018-08-27 08:37:26
Received Time	2018-08-27 08:37:26
Relayed By	BTC.TOP
Difficulty	6,727,225,469,722.53
Bits	388618029
Number Of Transactions	1614
Output Total	3,587.8337015 BTC
Estimated Transaction Volume	330.50932894 BTC
Size	1241.455 KB
Version	0x20000000
Merkle Root	e0e5c1e24465805b97c359d9f0f5271a014b766853073f516bc6bc4f3be29bd7
Nonce	664909101
Block Reward	12.5 BTC
Transaction Fees	0.08705715 BTC

목표값(target) Bits의 계산 공식

= coefficient * 2^ { 8 * (exponent-3) }

블록 #538695의 목표값의 계산을 위해
Bits값 "388618029"를 16진수로 변환하면 "0x1729d72d"
처음 2자리 "17"은 지수, 나머지 6자리 "29d72d"는 계수

목표값(16진수)
= 0x29d72d * 2^ { 0x08 * (0x17-0x03) }

목표값(10진수)
= 2,742,061 * 2^ { 8 * (23-3) }
= 2,742,061 * 2^ 160
= 2,742,061 *
1.461501637330902918203684832716 3e+48
= 4.007526641161212986792514236082 8e+54
= 400752664116121442460608062048820646620266244862068 6086

블록 #538695의 목표값을 실제 해시값과 비교하면,
해시값 : 0x00000000000000000000d8b4025c6356088d75a7f3e6818411bab2b748947dcda
목표값 : 0x00000000000000000029d72d0000000000000000000000000000000000000000

이를 10진수로 변환하면, #538695의 해시값이 목표값보다 작은 것을 알 수 있음
해시값 : 1297252452973963204084200844082660268606420482246480888
목표값 : 400752664116121442460608062048820646620266244862068 6086

Bits: 작업증명을 위한 대상값(target)

목표값: 이 target값이 작업 증명의 대상.

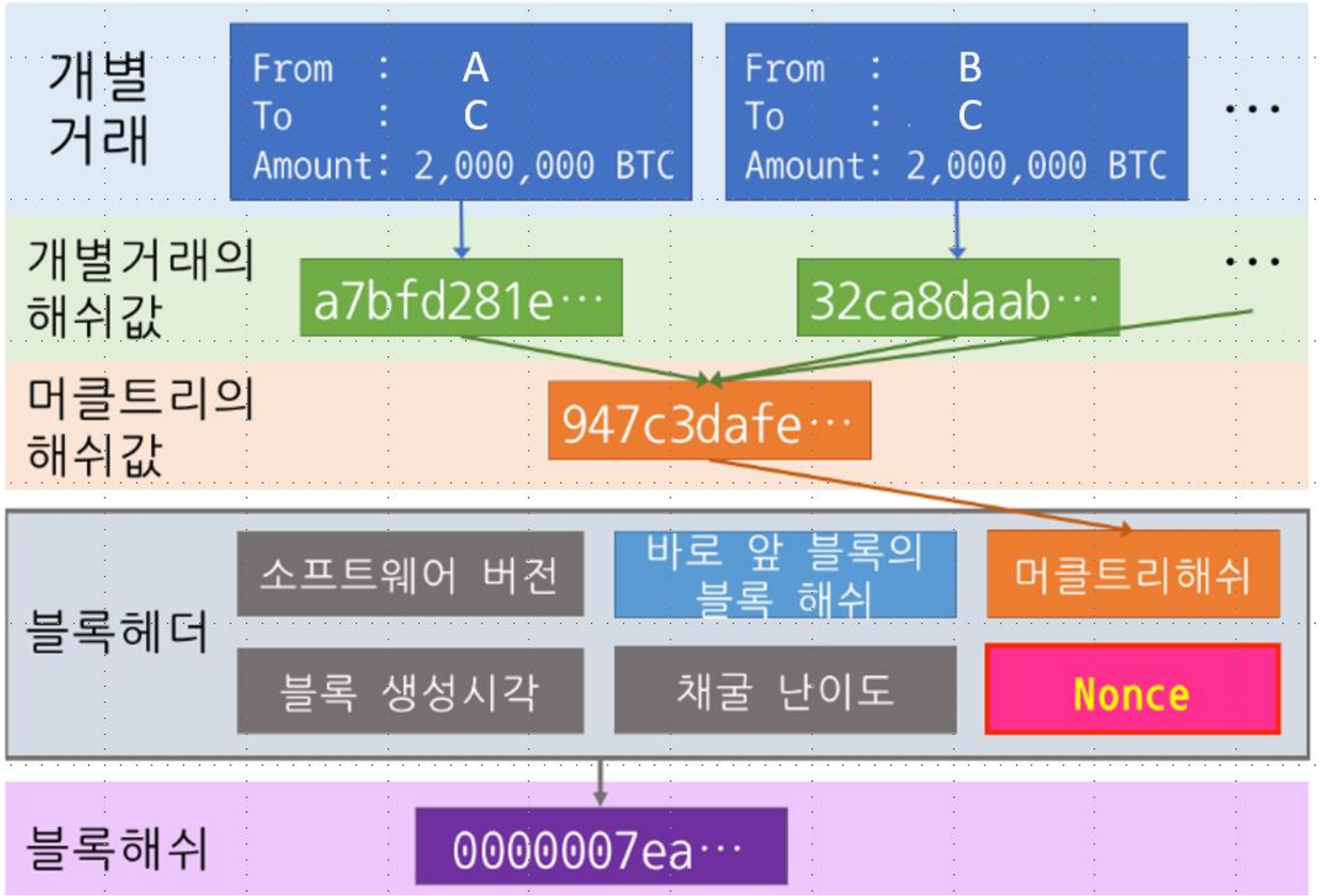
비트코인 블록 헤더의 SHA256 해쉬값이 이 값보다 작거나 같은 해쉬값이 나오는 Nonce를 구하게 되는 것이 채굴 성공!

보다 작게 나오는 **블록 헤더의 해쉬값**이 되도록 Nonce를 구하는 것.

➔ Target값의 0이 많으면 많을수록 난이도 상승

https://www.blockchain.com/btc/block/538695

05 PoW의 이해

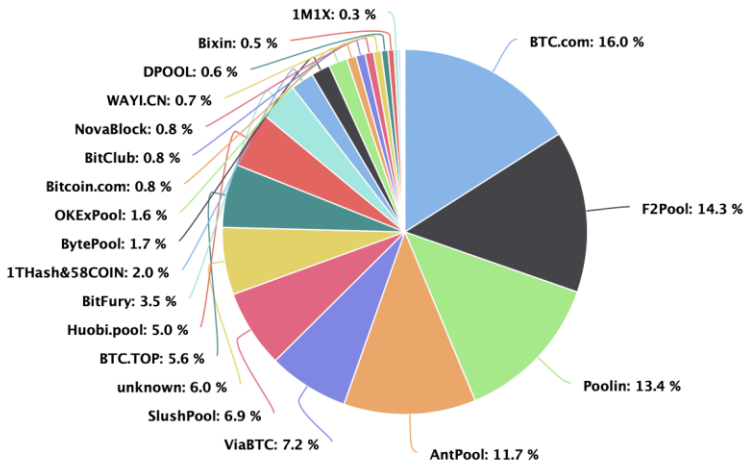

개별 거래
From : A
To : C
Amount: 2,000,000 BTC
From : B
To : C
Amount: 2,000,000 BTC
…
개별거래의 해쉬값
a7bfd281e…
32ca8daab…
…
머클트리의 해쉬값
947c3dafe…
블록헤더
소프트웨어 버전
바로 앞 블록의 블록 해쉬
머클트리해쉬
블록 생성시각
채굴 난이도
Nonce
블록해쉬
0000007ea…

05 PoW의 이해

해쉬레이트 비교

Pool Distribution (calulate by blocks)

All | 1 Y | 3 M | 1 M | 1 W | 3 D | 24 H



	Pool	Hashrate Share	Blocks Mined	Empty Blocks Count	Empty Blocks Percentage	Avg. Block Size (Bytes)	Avg. Tx Fees Per Block (BTC)	Tx Fees % of Block Reward
0	NETWORK	100.00 %	54,488	245	0.45 %	1,075,171	0.36107546	2.89 %
1	BTC.com	16.00 %	8,716	88	1.01 %	1,070,387	0.39285490	3.14 %
2	F2Pool	14.35 %	7,819	49	0.63 %	1,062,840	0.33074775	2.65 %
3	Poolin	13.38 %	7,289	1	0.01 %	1,071,114	0.31392462	2.51 %
4	AntPool	11.69 %	6,369	43	0.68 %	1,083,524	0.37521971	3.00 %
5	ViaBTC	7.15 %	3,898	7	0.18 %	1,074,428	0.36440992	2.92 %
6	SlushPool	6.88 %	3,751	14	0.37 %	1,099,394	0.42211445	3.38 %
7	unknown	5.96 %	3,247	3	0.09 %	1,073,761	0.34666090	2.77 %
8	BTC.TOP	5.65 %	3,076	13	0.42 %	1,100,432	0.43761674	3.50 %

05 PoW의 이해

블록의 첫 거래는 채굴자에게 보상을 주는 거래로 시작

- 새로 발행된 비트코인은 최초 50BTC에서 시작
- 블록이 21만개(대략 4년?) 추가될때마다 절반으로 줄어듬
- 2018년 현재 12.5BTC를 보상으로 받음
- 2020년 6.25BTC로 반감될 예정

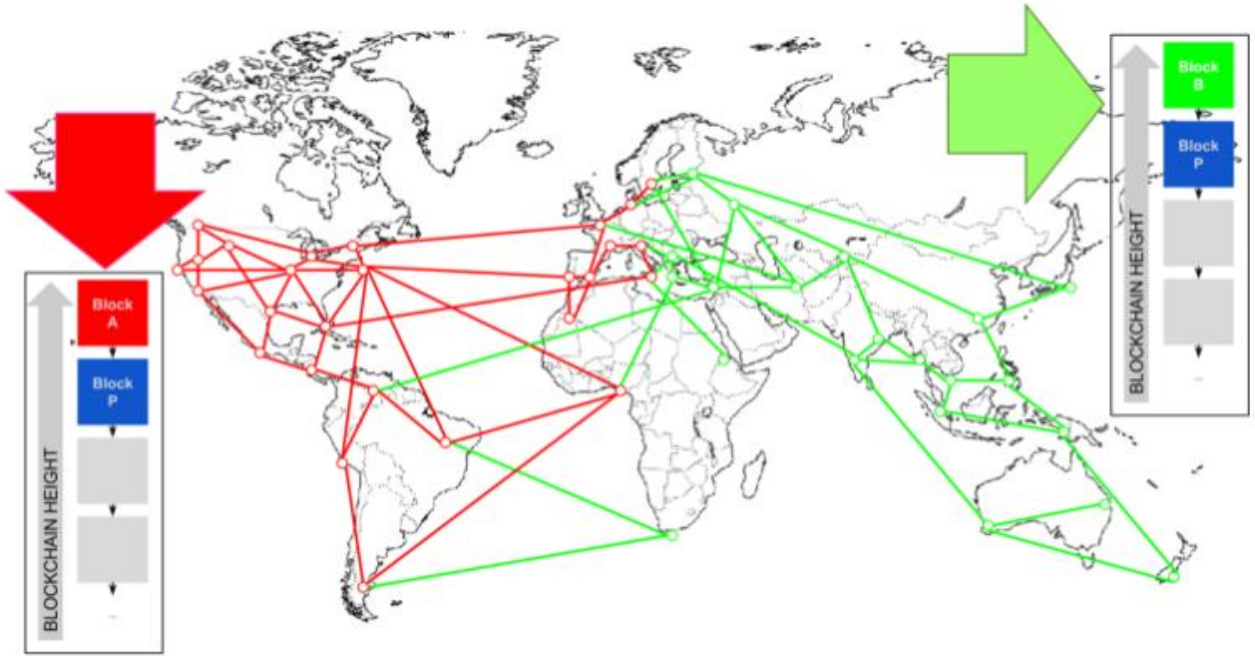
05 PoW의 특징

- 블록 거래 내용 변경을 위해 많은 자원이 필요해 위변조가 어려워 보안성이 좋음
- 이중지불 문제 해결
- 채굴 난이도가 높아질수록 연산에 고사양 장비들이 필요하게 됨
- 반복적인 연산을 계속해서 불필요한 연산을 많이 하게 되며 전기같은 리소스 낭비가 심함
- 노드들이 트랜잭션을 검토해야 하기 때문에 모든 블록 정보를 보유해야함

06 블록체인의 분기 과정

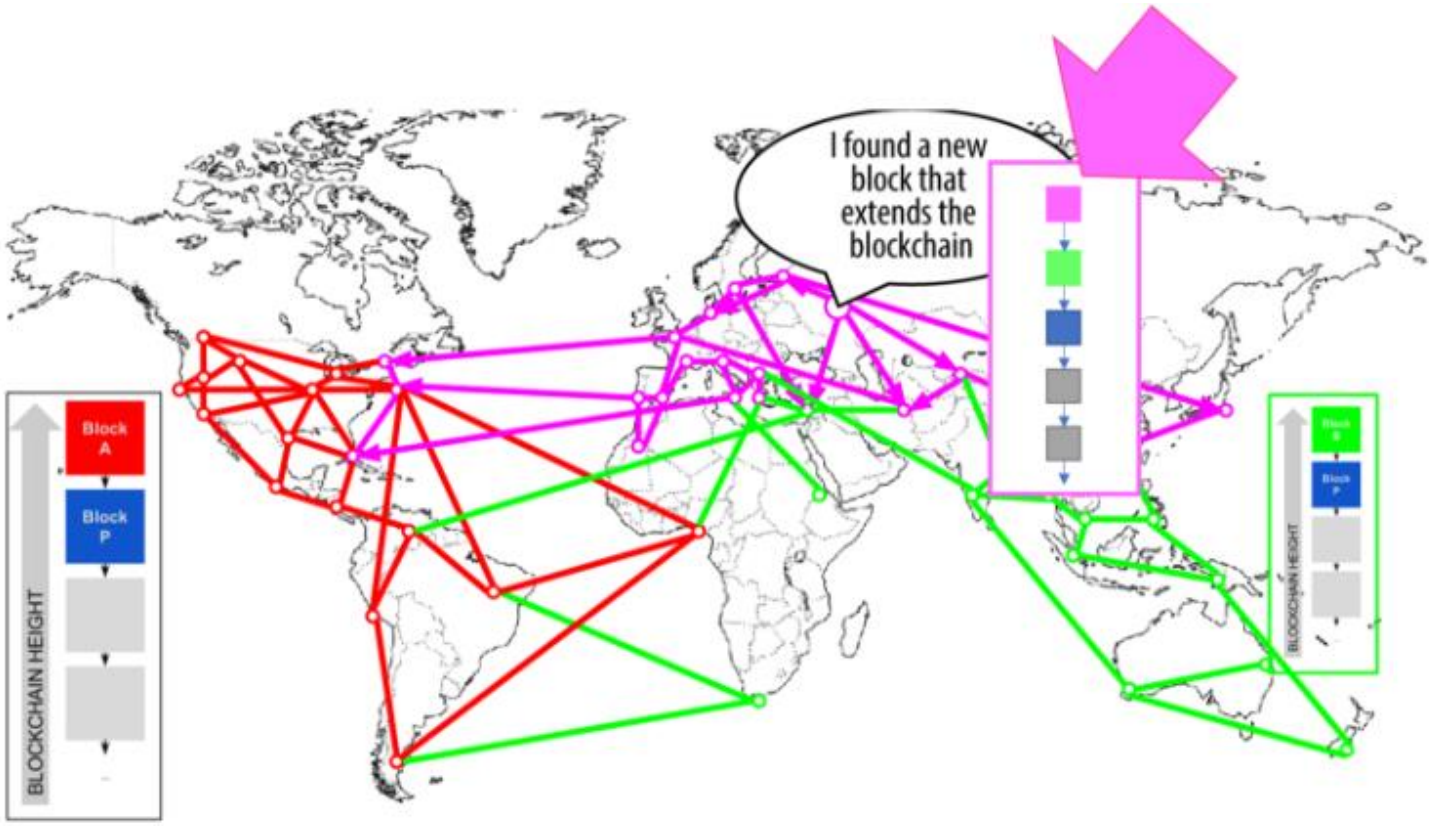
1. 물리적으로 거리가 먼 노드들이 거의 동시에 Nonce값을 찾아 마지막 블록 이였던 P에 각각 새로운 블록을 추가하며 인접 노드들에게 전파

각 A, B 블록을 받은 후에 받는 블록들은 무시됨
->A블록을 이었으면 B블록을 무시, 반대의 경우도 마찬가지



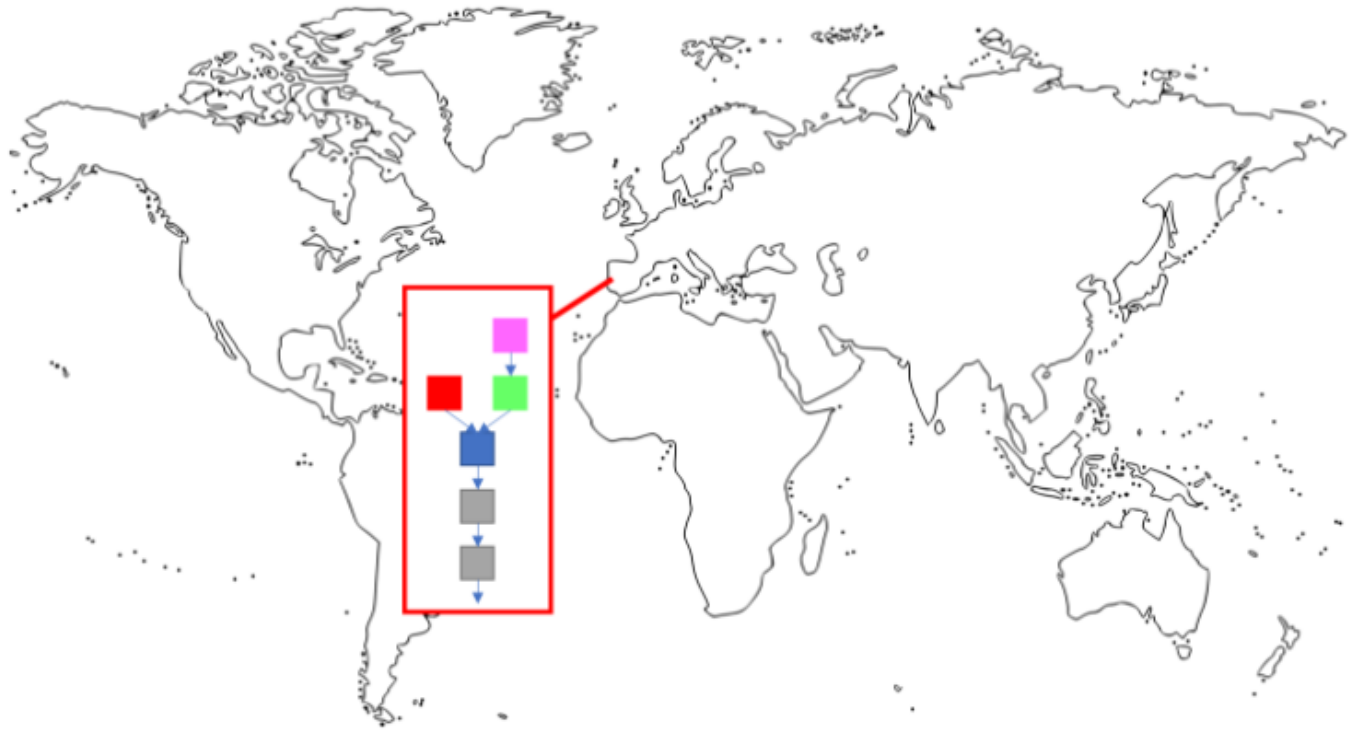
06 블록체인의 분기 과정

1. B블록을 이어받은 노드에서 Nonce값을 구해 새로운 블록 생성을 위해 인접 노드로 전파



06 블록체인의 분기 과정

3. 빨간색 노드인 A블록을 이었던 노드들은 더긴 노드 초록-보라 노드가 있으므로 교체됨

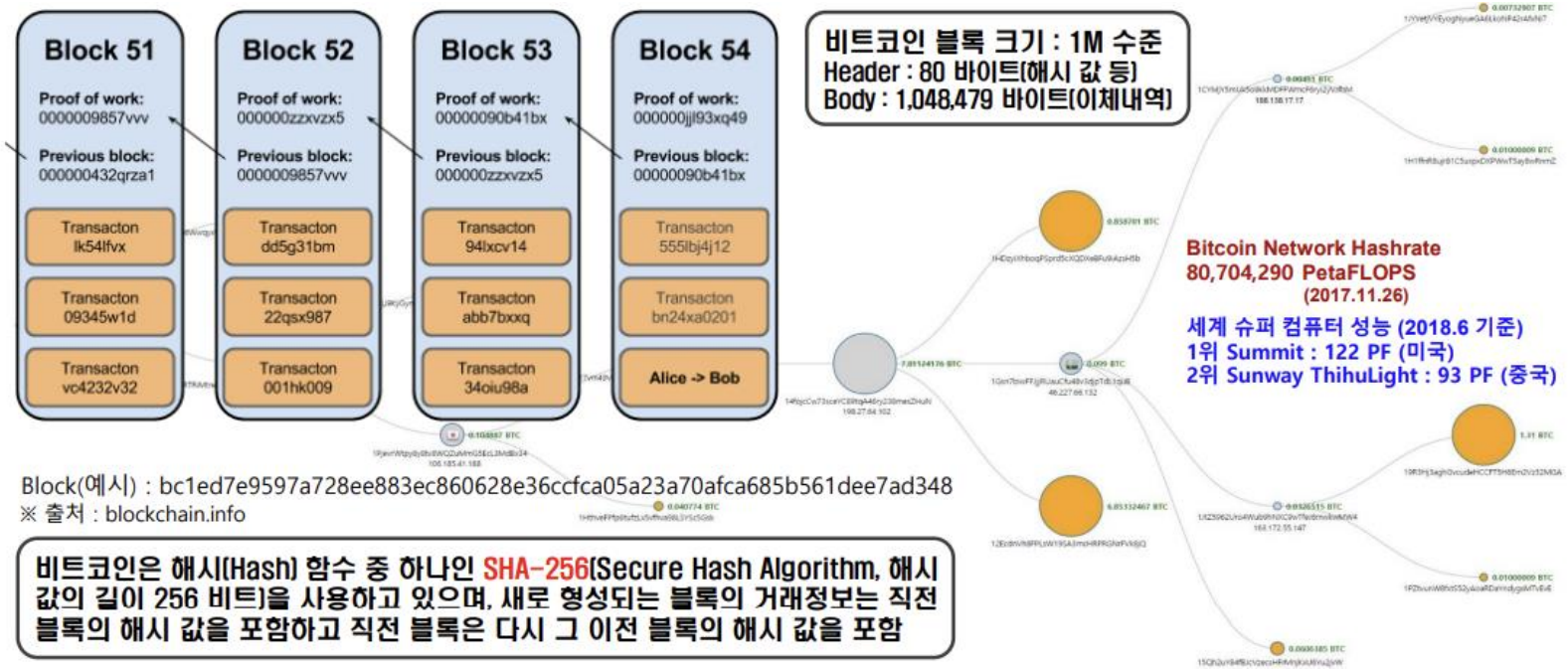


05 블록체인 기술의 구조 및 특성

[기술 구조]

블록체인은 P2P 네트워크에서 일정 시간마다 새로운 거래내역을 담은 신규 블록 (block)이 형성되어 기존 블록에 계속 연결(chain)되는 데이터베이스 구조를 가지며, **원천적으로 이중지불(double spending) 방지 및 이체 불가역성(irreversibility)**

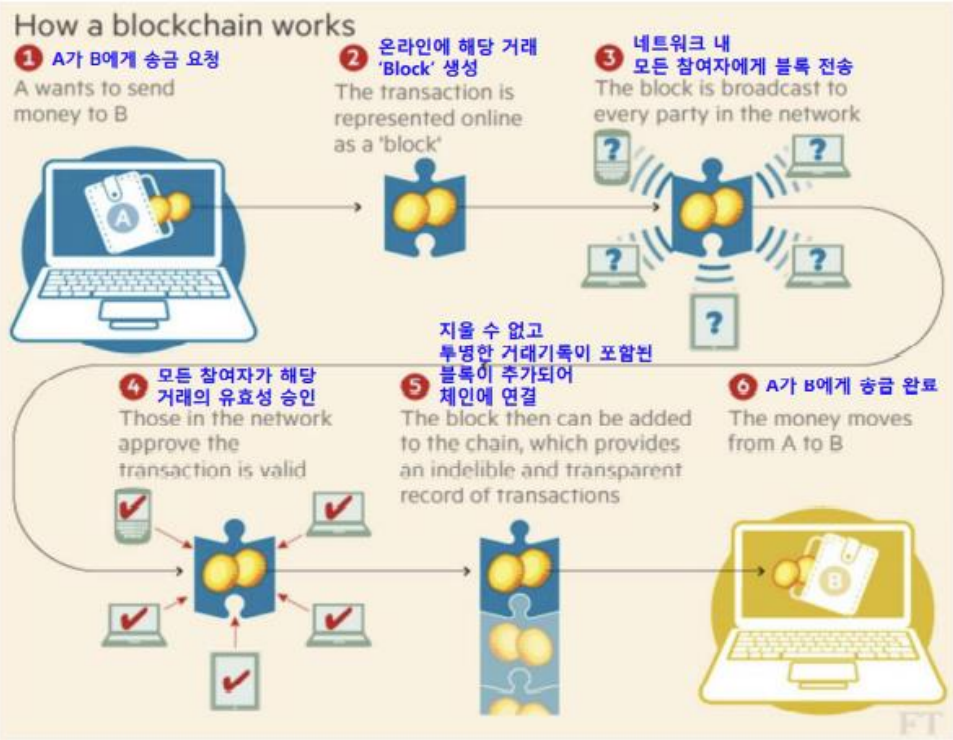
작업증명(Proof of Work)을 도입하여 네트워크 참가자에게 거래서비스 요청시 많은 자원을 소모하는 작업을 함께 수행할 것을 요구함으로써, 네트워크에 대한 공격을 예방하고 거래 위변조 시도를 방지

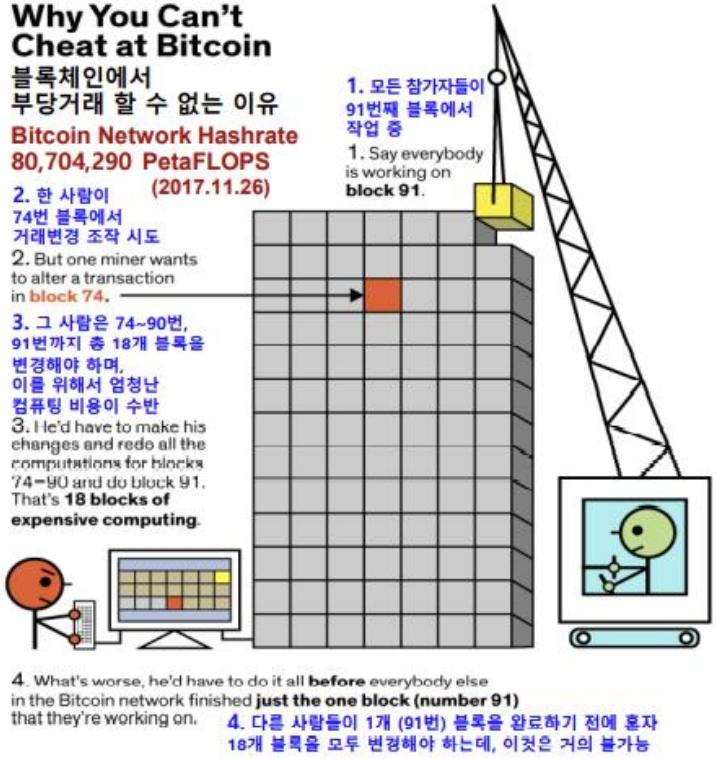


05 블록체인 거래의 안정성

[블록체인 거래]

- 블록체인에서 거래란 실물화폐를 주고받는 것이 아니고 기존 중앙은행이 관리하는 **전자화폐와 달리 온라인에서 화폐가치 이동의 기록(실질적으로는 입출력 값 변화(장부의 변화))**
- 거래가 발생할 때마다 해당 거래기록의 블록(block)이 생성되어 연결(chain)되며 모든 참여자에게 전송되어 거래의 유효성이 승인되는 방식이고, 거래내역을 중앙서버에 저장하는 일반금융과 달리 블록 체인은 모든 참여자의 컴퓨터에 저장



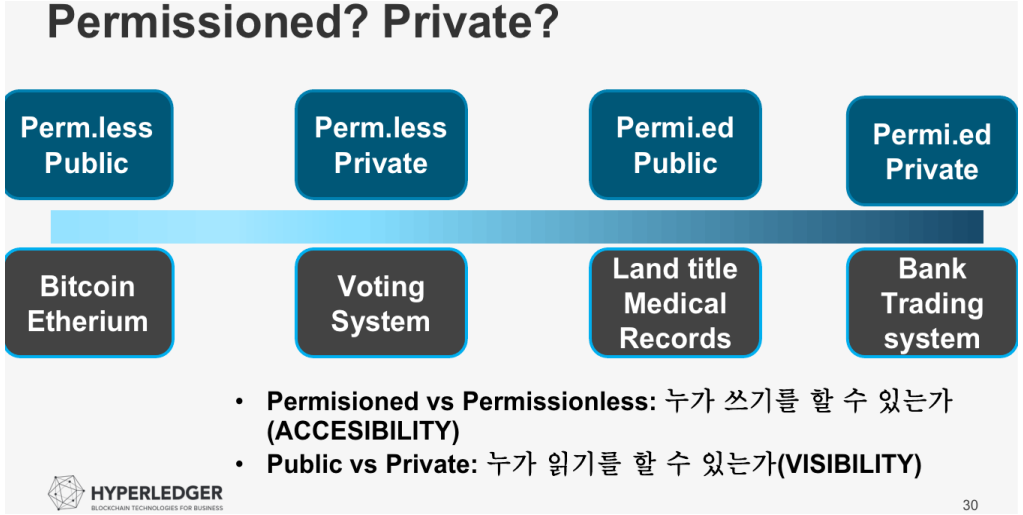


06 블록체인의 종류

	퍼블릭 블록체인	프라이빗(컨소시움) 블록체인
읽기 권한	누구나 열람 가능	허가된 기관만 열람 가능
거래 검증 및 승인	누구나 네트워크에 참여하면 거래 검증 및 승인을 수행	승인된 기관과 감독 기관
트랜잭션 생성자	누구나 트랜잭션을 생성	법적 책임을 지는 기관만 참여
합의 알고리즘	부분 분기를 허용하는 작업증명이나 지분증명 알고리즘	부분분기를 허용하지 않는 BFT계열의 합의 알고리즘
속도	7~20 TPS	1000 TPS이상의 고성능
권한 관리	누구나 모두가 모든 일을 할 수 있음	Private Channel, Tierd System등을 통해 읽기 쓰기 권한 관리가 가능
예시	비트코인, 이더리움	IBM Fabric, LoopChain, R3 Corda

bloter.net

- 퍼블릭: 이미 전개된 퍼블릭 블록체인에서 스마트컨트랙트를 자유롭게 작성하고 사용할 수 있음
- 프라이빗(컨소시엄): 기관(산업)이나 이해 당사자들이 블록체인을 직접(또는 임대) 운용하며 업무를 수행
- 퍼블릭-프라이빗은 용도에 따라 선택하는 것이 효율적임. (비유: 퍼블릭-프라이빗 클라우드, 공공-개인 운송수단)



Decentralization, Marta Piekarska, Hyperledger

06 전통적인 방식 vs 블록체인

모델	레거시	블록체인
패러다임	TTP (Trusted Third Party)	신뢰자들 시스템 (Trusty System)
아키텍쳐	센트럴 서버	P2P 네트워크
데이터베이스	싱글카피	멀티플카피
시큐리티	접근제어	암호학
가격	중계	합의
엑세스	프라이빗	퍼블릭

07 DApp의

보안

대칭키, 비대칭키(암호화, 서명)

해시

PKI, SSL, TLS

네트워크

p2p

서버-클라이언트

DB

파일db

JSON

웹서비스

nodejs

반응형 웹페이지

프로그래밍

스마트컨트랙트