

블록체인 기초 및 합의알고리즘

한국항공대학교 소프트웨어학과

박종서 교수

jspark1@gmail.com

박종서 교수 약력

- ❖ 1979-1983 : 한국항공대 통신공학 학사
- ❖ 1984-1986 : 미국 North Carolina State Univ. 석사
- ❖ 1987-1994 : 미국 Pennsylvania State Univ. 박사
- ❖ 1994-1996 : 미국 Pennsylvania State Univ. 조교수
- ❖ 1996-Present : 한국항공대 교수
- ❖ 1998년 7월 : 한국국제협력단 전문가로 미얀마 파견후 인생이 바뀜
- ❖ 1998-현재 : 네트워크 보안 전문가(비트코인 블록체인 전문)
- ❖ 2010-현재 : 드론 및 나노위성 응용 전문가

블록체인 기초 및 합의알고리즘

- 4차 산업 혁명과 블록체인
- 블록체인 개요 (비트코인중심)
- 블록체인 개요 (용어정리)
- 암호 알고리즘
- 합의 알고리즘

1

4차 산업혁명

4차 산업혁명이란?
4차산업혁명 기업

4차 산업혁명이란?

❖ World Economic Forum

- <https://www.youtube.com/watch?v=SCGV1tNBoeU>
- Cyber Physical System: 자동차 네비게이션
- Real Data(GPS, Physical) 지도(DB, Cyber)

❖ 분야

- 바이오, 나노, IT분야의 파괴적 혁신

AG 알파고 충격

❖ 알파고 리 (AlphaGo Lee)

- 48개의 TPU가 사용된 분산 버전이다. 2016년 3월 이세돌 9단과 대국에서 승리하였다. 수천만장의 기보 데이터 필요

❖ 알파고 제로 (AlphaGo Zero)

- 4개의 TPU가 사용된 단일 버전으로 알파고의 최종 버전
- 2017년 10월 19일 과학 저널인 네이처에 '인간 지식 없이 바둑을 마스터하기(Mastering the game of Go without human knowledge)'라는 제목의 논문 발표를 통해 소개되었다.
- 알파고 제로는 인간의 기보에 의존하는 지도학습 없이 바둑 규칙만으로 스스로 학습하며 기력을 향상시킨다.
- 빅데이터 학습이 필요없는 인공지능의 등장은 바둑과 달리 빅데이터 확보가 어려워 인공지능을 활용하기 어려웠던 분야에 해결책을 제시했다는 점에서 의미가 있다.

4차 산업혁명 기업(블록체인 AG)

❖ ENCORED Technologies(이하 인코어드)

- IoT 기반 에너지 빅데이터 서비스를 제공하는 기업으로 가정, 상가, 빌딩의 에너지 사용 패러다임을 바꿀 수 있는 기술가치를 인정받음
- 실리콘밸리 및 국내 유수의 벤처펀드 투자를 받아 EnerTalk이라는 빅데이터 서비스를 세계적 파트너들과 연계하여 Smart Home, Smart Building 글로벌 시장을 개척하고 있음
- 인코어드는 실리콘밸리의 글로벌 VC Formation 8의 투자를 받아 2013년 창업한 기업으로 Series A단계 국내 최고기록인 165억을 기업가치를 인정받고 \$6M USD의 투자를 받았음
- 2015년에는 소로스 펀드 매니지먼트가 운영하는 QSP(Quantum Strategic Partners Ltd) 및 LG유플러스로부터 \$10M 투자 유치
- 2016년부터는 국내는 물론 미국, 일본 등을 시작으로 본격적인 해외 진출을 추진하고자 합니다.
- 소프트뱅크의 손정의 회장 관심을 가지고 투자

❖ 세계에서 가장 많은 전력데이터 확보 → 블록체인으로 공유, AI적용

4차 산업혁명 기업

❖ IT분야가 선도 한다

- CPS(Cyber Physical System)
- Big Data 기반 혁신
- IOT
- 인공지능(AI), 딥러닝
- 비트코인, 알트(ALT)코인에 적용된 블록체인기술
 - 비트코인은 사라질 수 있어도 블록체인기술은 계속 진화할 것
 - 비트코인은 사라지지 않을것이다.
- 블록체인은 위의 모든 것을 묶어 비즈니스 모델을 만든다
 - 데이터 혁명



ICT 분야 4차 산업혁명

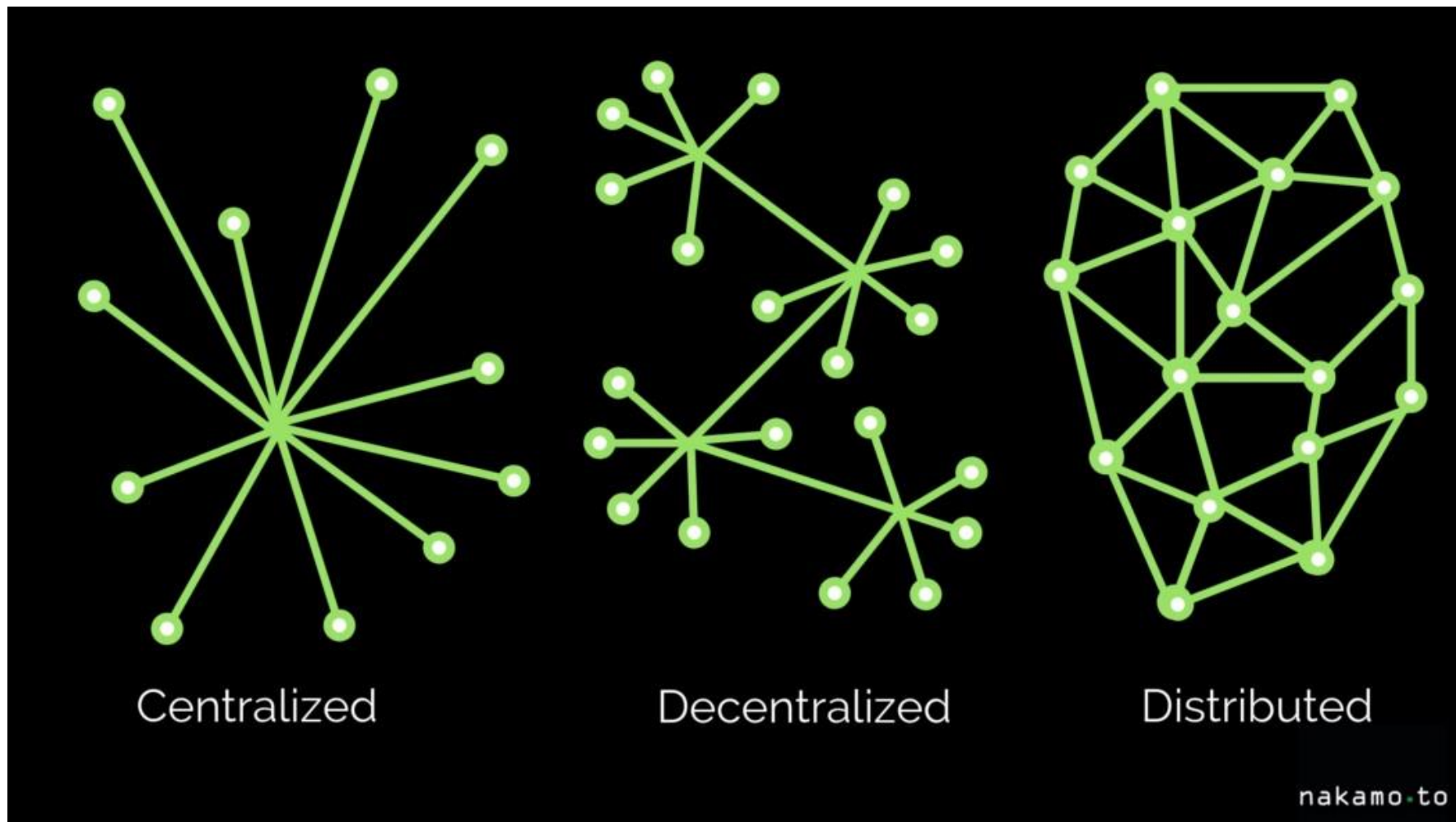
- ❖ IOT(엄청난 데이터 수집)
- ❖ Big Data(데이터 저장)
- ❖ Blockchain(데이터 공유)
- ❖ Deep Learning(데이터 처리 및 가치 창출)

1.1

블록체인 개요


비트코인 탄생
Client Server vs. P2P
블록체인 개념 및 특성
암호

분산 시스템 과 탈중앙 시스템



분산 시스템 필요성

- ❖ 분산 시스템의 필요성: 반도체 성능향상에 한계가 있으므로(적은 회로로 빠른 컴퓨터를 만들었다, 몇 년 전에 100nm에서 현재 3nm공정) 하나의 일을 여러 컴퓨터가 나누어 처리 필요, 그리고 고장감내 시스템의 필요성
- ❖ 하지만 지배구조는 중앙적(하나의 중앙 처리기가 모든 결정을 수립)



탈중앙화

- ❖ 중앙 집중식 시스템에서 제어는 단 하나의 엔티티 (예 : 개인 또는 기업)에 의해 실행됩니다. 탈 중앙화 시스템에서는 단일 제어 엔티티가 없습니다. 대신 여러 독립된 엔티티간에 제어가 공유됩니다.
- ❖ 비 분산 (또는 공존) 시스템에서는 시스템의 모든 부분이 동일한 물리적 위치에 있음. 분산 시스템에서 시스템의 일부는 별도의 위치에 있음.

예

- ❖ Microsoft Windows 운영 체제를 실행하는 PC에서 Microsoft Word 애플리케이션을 사용하여 문서를 작성한다고 가정.
- ❖ 이 설정은 중앙 집중식 및 비분 산식입니다. 하나의 엔터티 인 Microsoft가 애플리케이션과 운영 체제를 제어(중앙 집중식).
- ❖ 응용 프로그램과 운영 체제는 모두 PC, 즉 하나의 물리적 위치 (비 분산)에 있음.
- ❖ 이제 오픈 소스 워드 프로세싱 소프트웨어를 사용하여 PC에서 Linux와 같은 오픈 소스 운영 체제를 실행한다고 가정.
- ❖ 서로 다른 사람과 조직이 두 항목의 상태 변화에 기여 (이제 설정이 분산 됨). 반면에 모든 소프트웨어를 실행하기 위해 여전히 하나의 물리적 PC를 사용하고 있습니다 (아직 분산되지 않음).

중앙집중식 분산 시스템?

- ❖ 분산되었지만 중앙 집중식 시스템은 모순적으로 들릴 수 있지만 제어 및 위치에 따라 위의 정의를 사용하면 어떻게 작동하는지 알 수 있음.
- ❖ 데이터 저장 서비스를 제공하는 클라우드 서비스 제공 업체를 고려.
- ❖ 물리적으로 리소스 가용성 및 복원력 (분산)에 따라 다른 컴퓨터에서 데이터를 공유하고 복제 할 수 있음.
- ❖ 그러나 머신과 데이터 저장 시설이 어디에 있든 클라우드 서비스 공급자는 여전히 모든 것을 제어합니다 (중앙 집중식).

탈 중앙화 분산 시스템


- ❖ 마지막으로 탈 중앙화 분산 시스템이 남음.
- ❖ 비트 코인을 예로 사용함.
- ❖ 비트 코인은 하나의 중앙엔티티가 변경할 수 없는 블록 체인 시스템.
- ❖ 또한 전 세계에 분산 된 독립 컴퓨터의 피어 투 피어(Peer to Peer) 네트워크(Network)로 실행됨.
- ❖ 이 독립된 피어투 피어 네트워크에 연결된 분산 시스템의 상태는 하나의 중앙 엔티티가 결정 하는것이 아니라 합의(게임같은)에 의해서 결정됨

최초의 블록체인 기반 시스템 비트코인

- ❖ 세계 최초의 암호화폐인 비트코인(bitcoin)을 처음 만든 것은 **사토시 나카모토**라는 가명을 쓰는 사람임.
- ❖ 블록체인은 사토시 나카모토가 처음 제안했고, 이를 위해 2008년 11월 1일 <비트코인 : 개인 대 개인의 전자화폐 시스템>이라는 9쪽짜리 논문을 작성하고 <https://bitcoin.org/bitcoin.pdf>에 올렸음.
- ❖ 이는 자신의 제안을 구현한 최초의 블록체인 관리 프로그램 '비트코인 코어(Bitcoin Core)'이다. 그리고 자신의 아이디어를 담은 논문을 내려 받을 수 있는 사이트주소를 수백 명의 암호학 전문가들에게 전자우편으로 보냈다.

최초의 블록체인 기반 시스템 비트코인

- ❖ 그 메일에는 '저는 제3자의 신용보증인이 필요 없는 완전한 피투피(P2P) 전자 화폐 시스템을 개발해왔습니다.'라는 내용과 함께 비트코인 백서 링크를 첨부하였다.
- ❖ 이 논문은 비트코인과 블록체인의 기본 구조를 설명한다. 비트코인 코어는 암호화폐인 비트코인을 생성하고 비트코인 거래를 블록체인 형태로 기록하도록 설계됐다.
- ❖ 블록체인 기록을 검증한 대가로 주어지는 보상이 바로 새로 생성된 비트코인이다. 이렇듯 그는 블록체인 기술을 적용한 최초의 암호화폐인 비트코인(bitcoin)을 개발하고, C++ 언어로 작성한 소스 코드를 배포했다.
- ❖ 그 과정에서, 그는 피투피 네트워크를 이용하여 디지털 화폐에 대한 이중 지불 문제를 처음으로 해결했다. 2009년도에 비트코인 코어 프로그램이 공개되며 비트코인이 처음 발행되었다.



최초의 블록체인 기반 시스템 비트코인


- ❖ 2009년 1월 3일 오후 6시 15분 05초에 비트코인의 최초 블록인 제네시스 블록이 탄생한다.
- ❖ 이로 인해 50개 비트코인이 처음으로 채굴되었다. 그는 0번 블록에 '2009년 1월 3일, 은행을 위한 두 번째 긴급 구제 방안 발표 임박'이라는 의미심장한 메시지를 남겼다.
- ❖ 여기서 중앙화된 자본주의 시장의 폐해를 비트코인으로 해결하겠다는 의지를 볼 수 있다.
- ❖ 그러나 그 당시에는 사토시 나카모토 본인 외에는 전송할 사람도 없었고, 지불 수단으로도 쓰일 수 없었다.
- ❖ 그는 다른 사람들도 비트코인 네트워크에 참여하기 위해 다음과 같이 다시 메일을 전송하였다.

최초의 블록체인 기반 시스템 비트코인

- ❖ 메일에는 "첫 번째 비트코인이 만들어졌음을 발표합니다. 비트코인은 새로운 전자 화폐 시스템이며 피투피 네트워크를 사용함으로써 이중지불 문제를 해결했습니다."
- ❖ 그리고 다음과 같은 말을 덧붙였다. "중앙 서버도, 중앙집권화된 권력도 없는 완벽히 탈중앙화된 시스템입니다." 하지만 안타깝게도 당시 이메일을 수신한 사람들 중 비트코인에 관심을 보이는 사람이 없었다.
- ❖ 두 번째 비트코인 사용자인 할 피니만이 사토시 나카모토가 메일을 보낸지 일주일 뒤인 1월 10일에 관심을 보였고 사토시 나카모토가 보낸 이메일의 수신자 리스트에 있는 사람들에게 메일을 보냈다.

최초의 블록체인 기반 시스템 비트코인

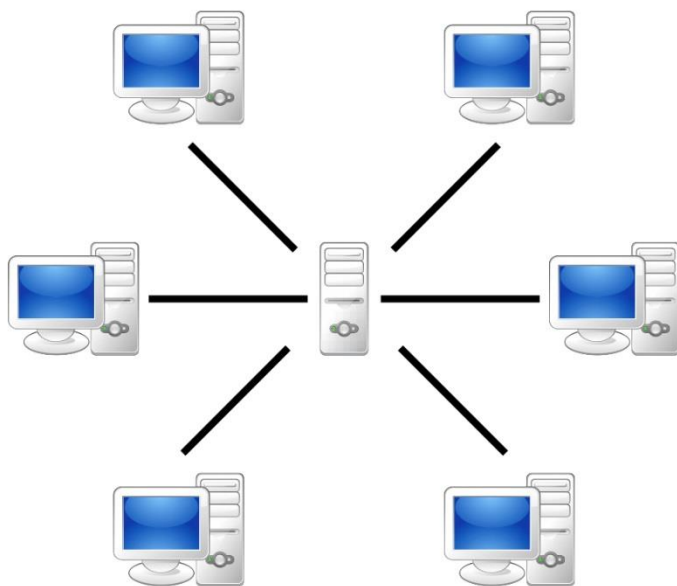
- ❖ 이후에 비트코인 사용자가 점점 늘었고, 사토시 나카모토는 자신이 논문을 올려둔 홈페이지(bitcoin.org)와 전자우편으로 다른 사람들과 소통하며 비트코인 네트워크를 확장했다.
- ❖ 이후 사토시 나카모토가 'bitcoin.org' 사이트에 개설한 IRC 채팅 채널은 비트코인 포럼이라는 이름으로 공식화되었다.
- ❖ 결국 사토시 나카모토는 기존의 P2P 통신 기술(BitTorrent, 소리바다 같은 파일공유 시스템), 합의 알고리즘(POW: Proof of Work, 작업증명), 공인 인증서 기술(비대칭키 암호, 해쉬 함수) 등을 혼합하여 블록체인 기술을 만들고 이를 비트코인으로 확인해 보인 것이다.



블록체인 기술의 최초 적용: Bitcoin 이란?

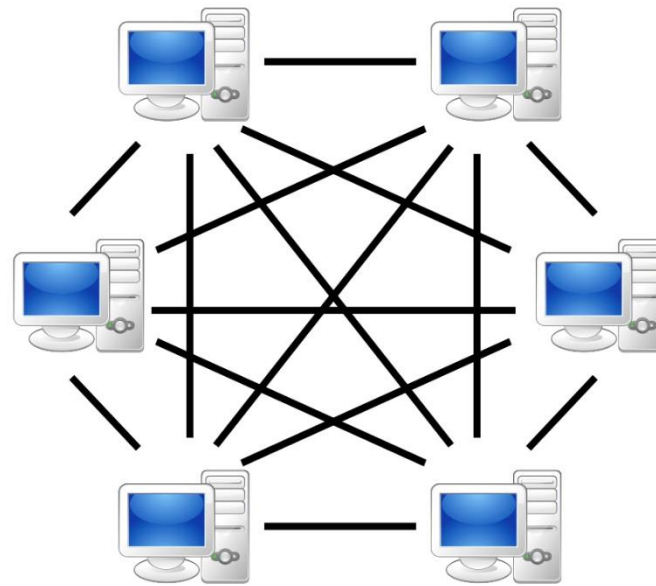
- 최초로 블록체인 기술을 활용해 성공적으로 만들어진 암호화폐
- 분산화된 P2P 기반의 디지털 가상화폐 (암호화폐)
- 국경 구분 없이 빠른 거래가 가능
- 송금 수수료가 매우 적음(액수에 관계없이 수백원)
- 채굴 시스템에 의해 사용자들이 자생적으로 관리
- 채굴되는 총량은 2100만 BTC로 제한되어 있음
- 10분마다 거래내역이 갱신되며 해킹 어려움

Client Server vs. P2P Network



Server-based

1% 공격 가능



P2P-network


51% 공격이 문제?

블록체인의 지속 가능성(역사적, 경제적 관점)

- ❖ [The four pillars of a decentralized society | Johann Gevers | TEDxZug](#)
- ❖ 레몬시장 이야기 : 정보의 비대칭성
- ❖ Deep Learning과의 연계성: Federated Learning(Blockchain + Deep Learning)

블록체인 개념

모든 거래 기록이 중앙 중개자 없이 숨김없이 오류없이 모두에게 확인된다

 **BLOCKCHAIN**

Home Charts Stats Markets API Wallet

Search


Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	134ZnmWpGDGSwU6AnkgSEqP3kZ2cKqruh <small>Public Bitcoin Address</small>	No. Transactions	2
Hash 160	169cded9e0b57f60018392d6cc98b0cc4c8fc533 <small>Cryptographic Hashed Address</small>	Total Received	\$ 6.63
Tools	Taint Analysis - Related Tags - Unspent Outputs <small>Discovery Tools</small>	Final Balance	\$ 0.00

Request Payment
Create a unique scannable QR code with amount

Donation Button
Create bitcoin donation widget for blogs/websites

Public Bitcoin Address scannable QR code




Transactions (Oldest First)

d2bb09337bda991846764d62e7770f3ec69831cdec425e770a1c14f604ddd77b Transaction Number

(Fee: \$ 0.05 - Size: 226 bytes) 2014-08-18 14:20:16

134ZnmWpGDGSwU6AnkgSEqP3kZ2cKqruh (\$ 6.63 - Output)
Public Bitcoin address funds are being sent from (\$)


Bitcoin Spent

1CNXMWGYuB2wn1f9UxKrKD7QmY7HzxJons - (Unspent) Public Bitcoin receiving address \$ 1.23

1JtCiHBcMB5cvR7mRr9vATFvSsqYNWtp - (Unspent) Sender's Public Bitcoin Change address \$ 5.35


6 Confirmations
of times validated on Bitcoin Network

\$ -6.63
Total funds sent

ac17ae4b8b4de054381ebaba7e38c6d64be2146805aca3cf2da41b9134a7b2bb

(Fee: \$ 0.05 - Size: 372 bytes) 2014-08-18 07:43:32

16Lr33nwoVx7C1cry9Bx8VyT996P2NyJld (\$ 6.33 - Output)
1LTtrFanRMQfsCp3jyZwEu7k81U6YXDYMF (\$ 5.04 - Output)


Bitcoin Received

134ZnmWpGDGSwU6AnkgSEqP3kZ2cKqruh - (Spent) \$ 6.63

1PX18cZmo5BMEavkQhT2Sr98RWMqCaUSFv - (Spent) \$ 4.68

51 Confirmations \$ 6.63

nipa 정보통신산업진흥원

KSA 한국표준협회
KOREAN STANDARD ASSOCIATION

KBCI 한국블록체인연구교육원
Korea Blockchain Institute

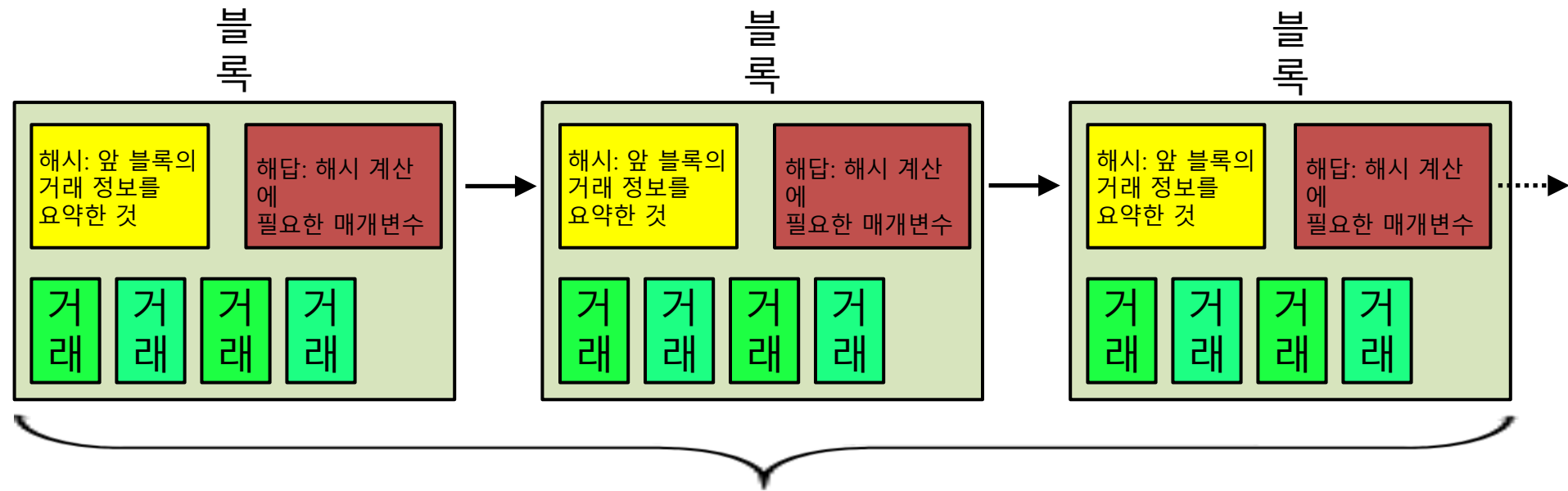
BLOCKCHAIN.INFO | @BLOCKCHAIN

25

블록체인 개념

❖ 블록체인의 기본 개념

- 거래가 담긴 블록이 사슬 모양으로 늘어선 것

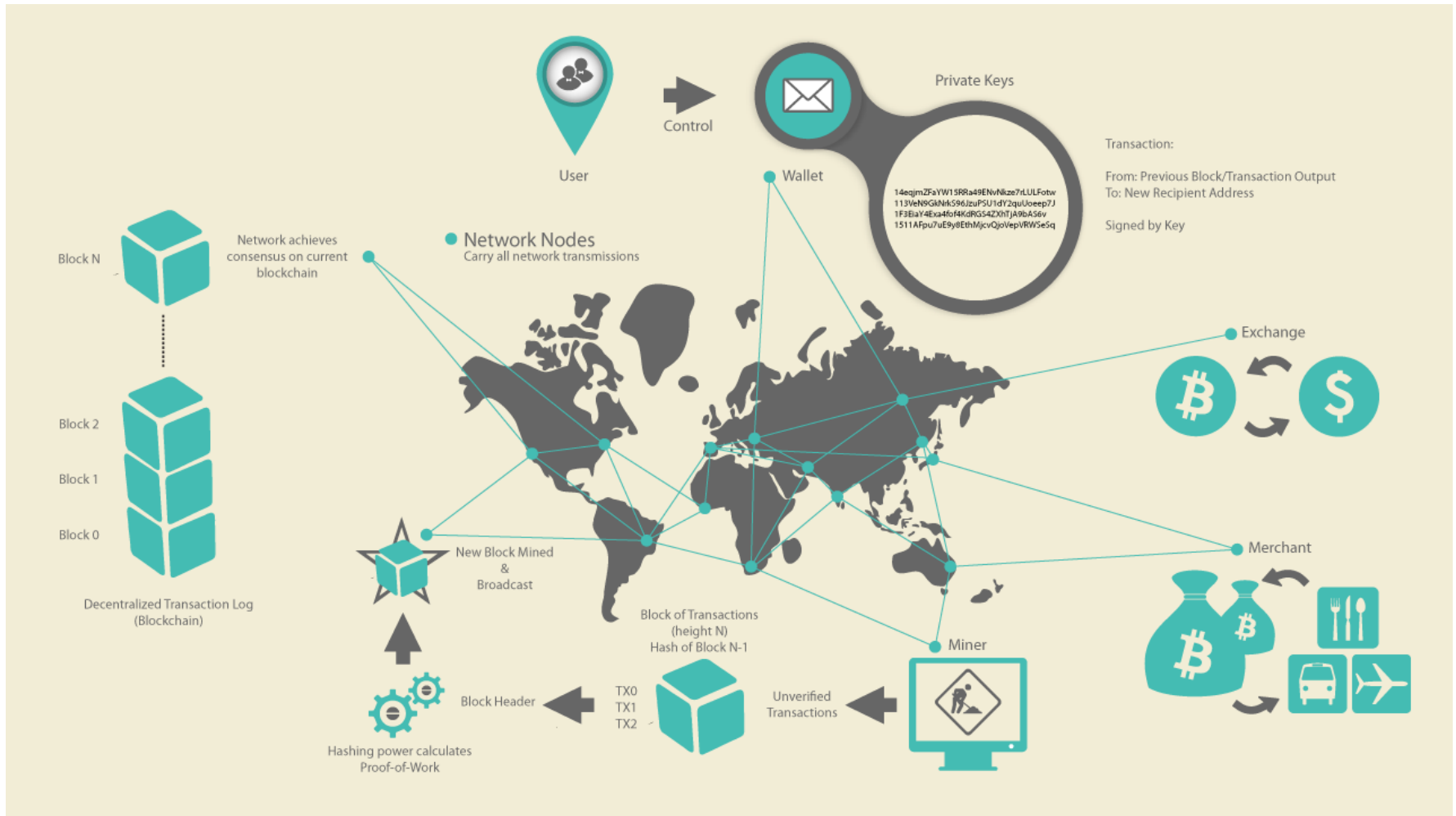


끝말 이어가기 빙고게임

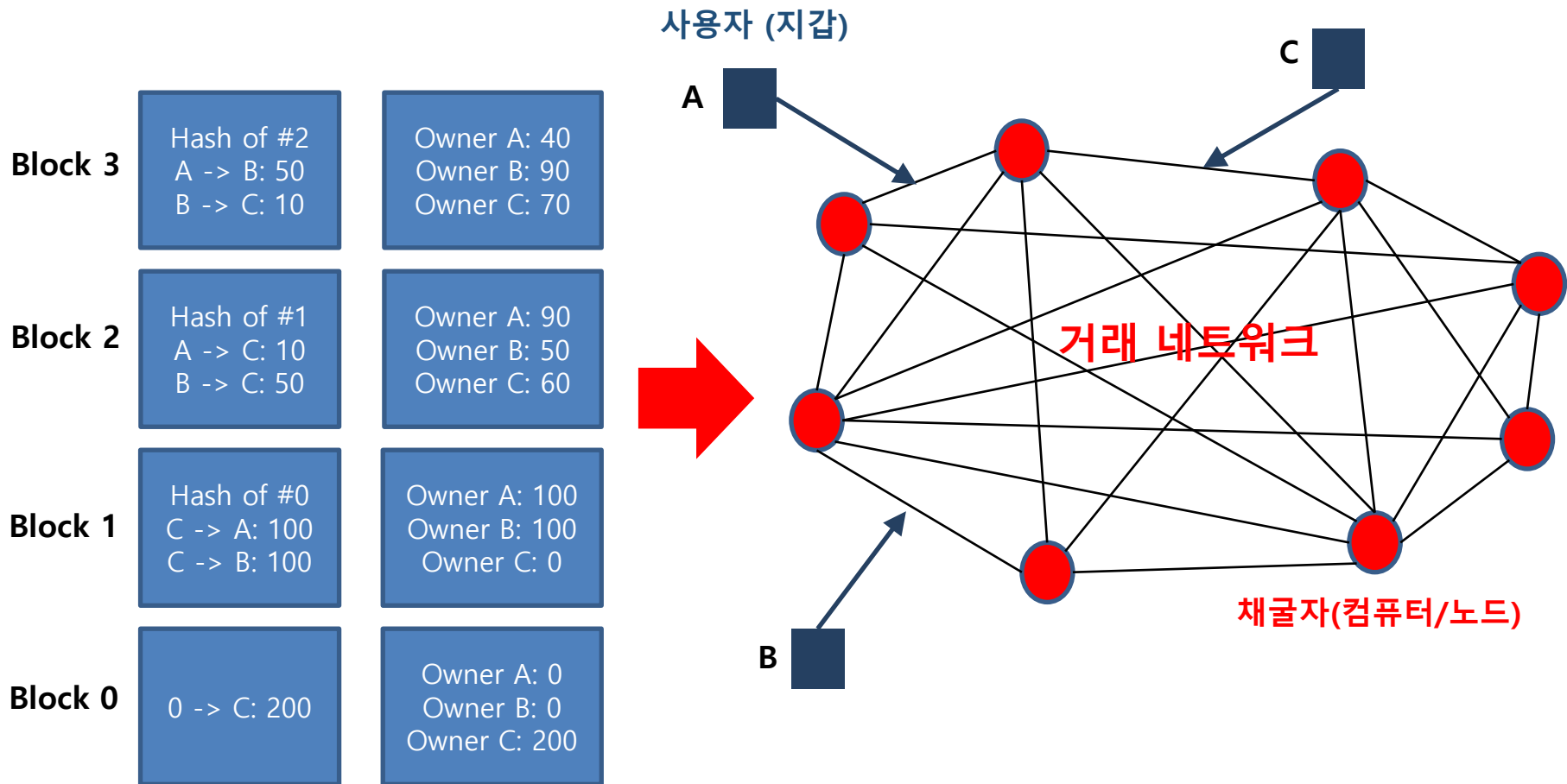
게임으로 합의에 도달

- ❖ 끝말이어가기 빙고게임
- ❖ 목적: 합의
- ❖ 목표: 인센티브(비트코인으로)
- ❖ 참가자: 전세계 마이너들(10,000개 정도 노드)
- ❖ 블록 해쉬값이 일정값 이하 되는 nonce 값 찾기
- ❖ 찾으면(끝말을) 바로 '블록(빙고)'를 피투피 네트워크를 통해 전세계로 보낸다
- ❖ 일정시간이 지나면 모든 참여자들이 똑같은 상태에 이른다(블록체인)

비트코인 전체그림



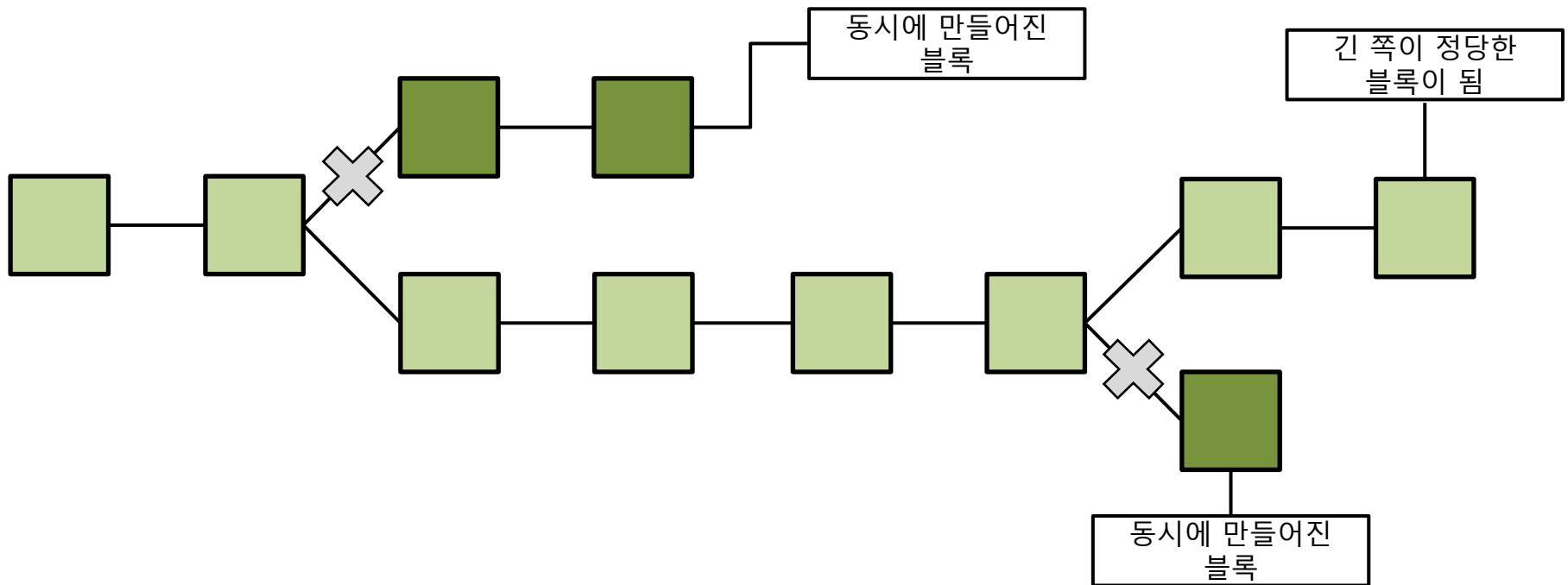
거래 기록 과 채굴

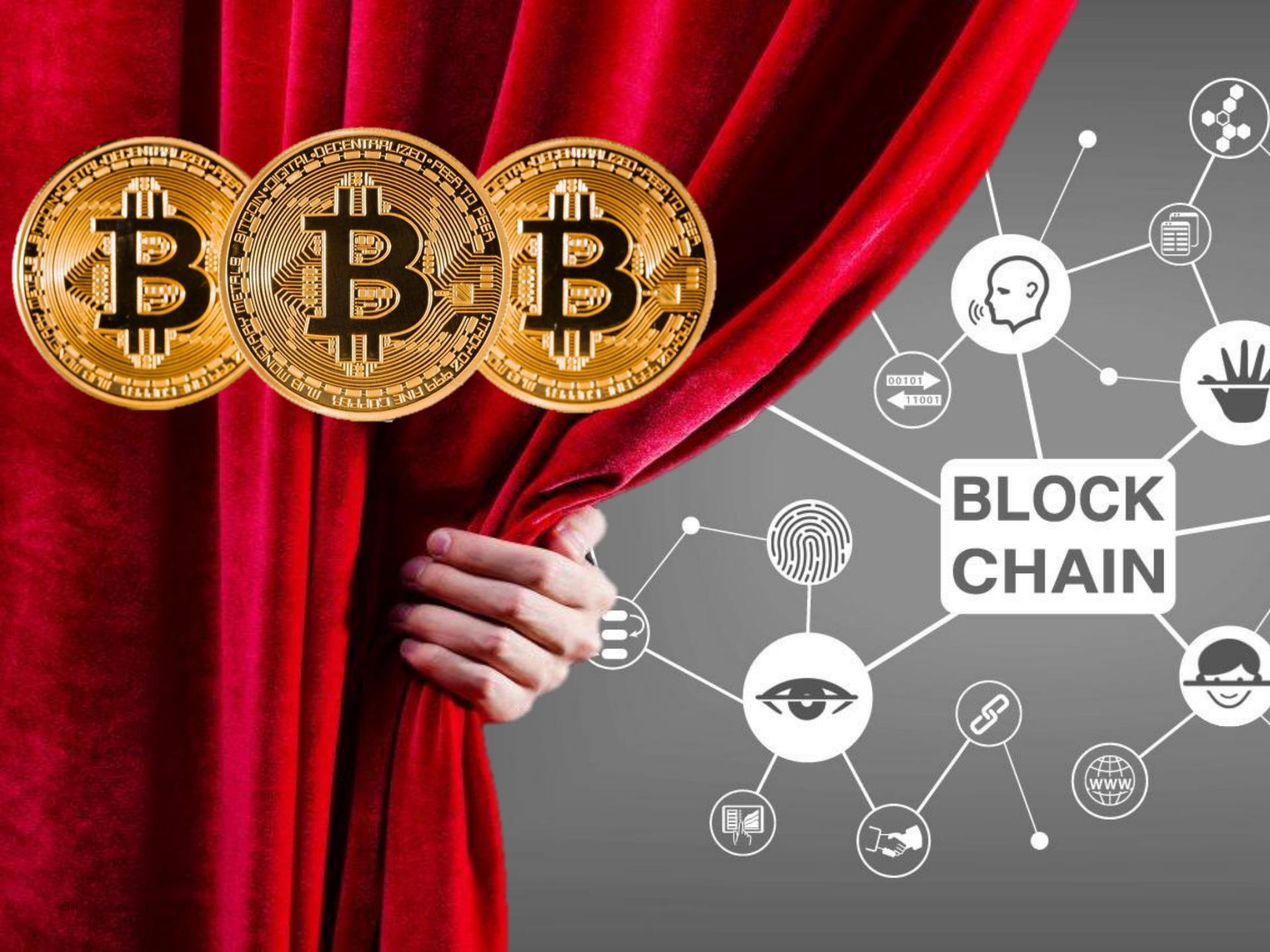


블록체인 개념(이중지불 방지)

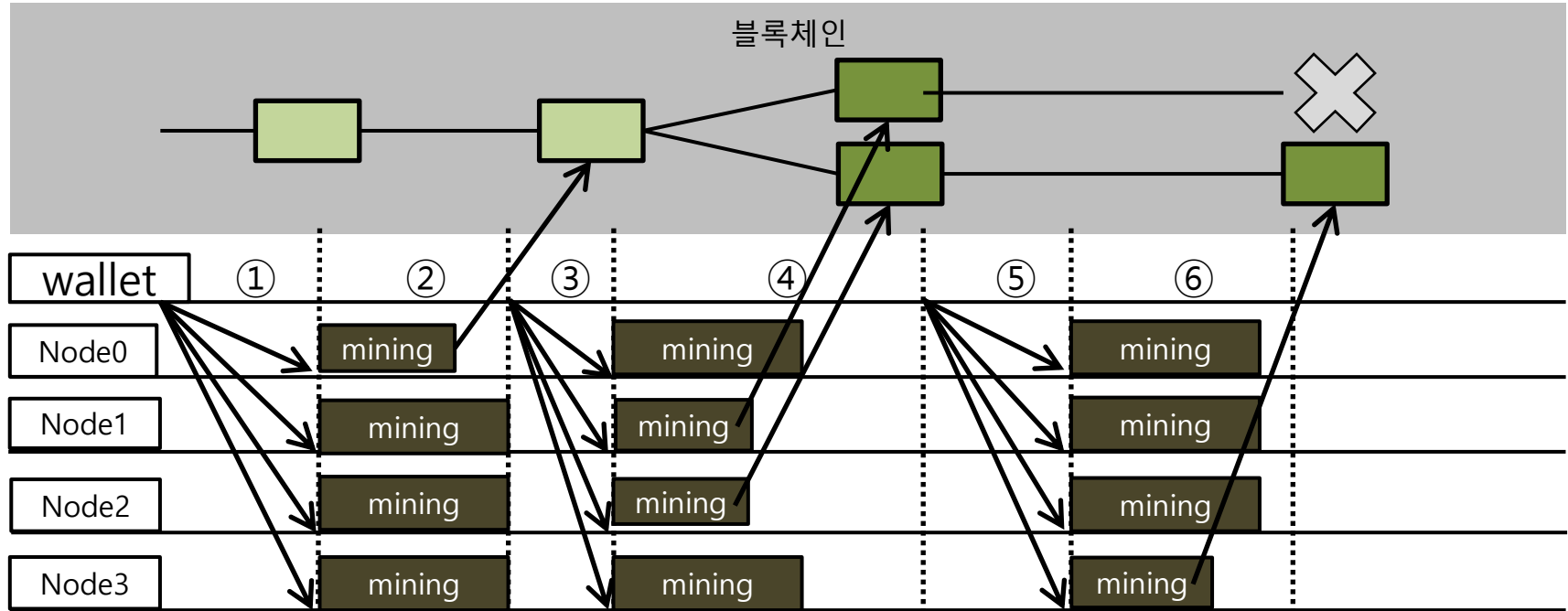
❖ 정당한 블록 찾기

- 가장 긴 체인이 정당하다(Double Spending 문제를 긴 체인으로 해결)





블록체인 개념 (합의: PoW 구조)



Pow 처리 절차

- ① wallet이 트랜잭션을 발행하고 참가자 전원에게 브로드캐스트
- ② 받은 승인자가 해시를 계산함. 여기서는 Node0이 먼저 발견했기 때문에 Node0이 만든 블록이 블록체인에 추가됨
- ③ wallet이 다른 트랜잭션을 발행하고 참가자 전원에게 브로드캐스트
- ④ 받은 승인자가 해시를 계산함. 여기서는 Node1 과 Node2가 동시에 발견했기 때문에 블록체인이 분기됨
- ⑤ wallet이 다른 트랜잭션을 발행하고 참가자 전원에게 브로드캐스트
- ⑥ 받은 승인자가 해시를 계산함. 여기서는 Node3이 발견해서 Node2의 블록 뒤에 추가한 것으로 함. 이 경우 아래의 블록체인이 올바른 것(*)이 됨.

* -> 네트워크 상태에 따라서 이후에 위의 블록체인에 추가된 것이 더 길어지게 된다면 위의 것이 올바른 것으로 변경 된다.

비트코인 개념

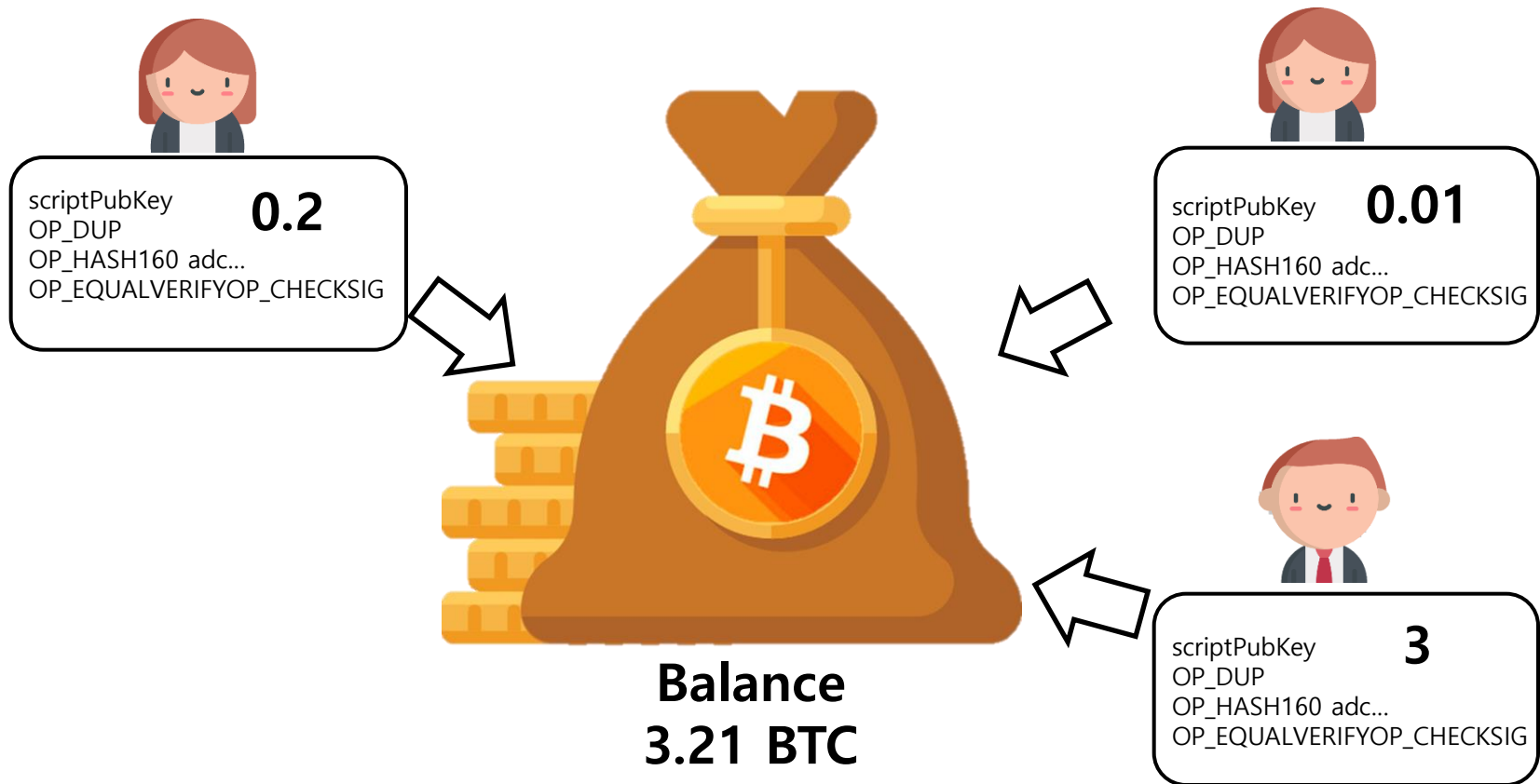
❖ 거래와 기록 장부

- 거래는 지갑 software/app 에서 발생 시킴
 - 소유주(송신자)가 개인키(열쇠)를 사용하여 거래를 생성하고 그의 공개키(열쇠)와 수신자 주소를 함께 네트워크에 방송
- 거래 처리자(채굴자)
 - 정상적인 돈인지 검증 (위조 X, 변조 X)
 - (동봉된 공개키로) 소유주 입증
 - 이 거래 내용이 공개 장부에 기록되면 송신종료
 - 돈을 수신자에게 직접 주는 것 이 아니다!!!
- 수신자 수령
 - 수신자는 공개장부에 접근하여 입금과 잔고 확인

비트코인 개념

❖ 내 지갑(통장)의 코인 잔고

- 실제 코인이 들어 있는 것이 아니라 잔고만 보여줌



비트코인 개념

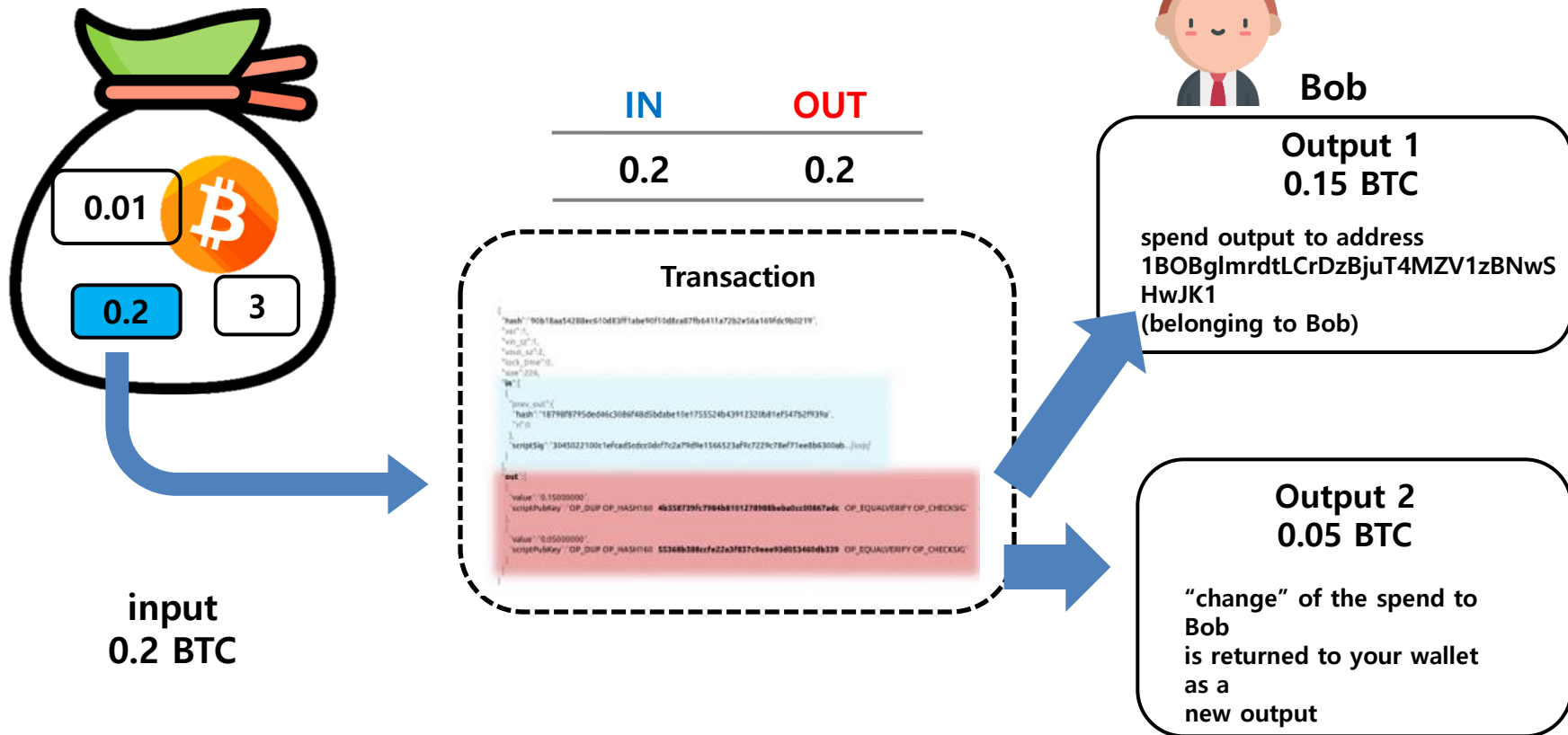
❖ 내 주소로 받은 모든 코인량이 독립적으로 존재



실제 돈이 아니라
기록 3개가 있는 것임

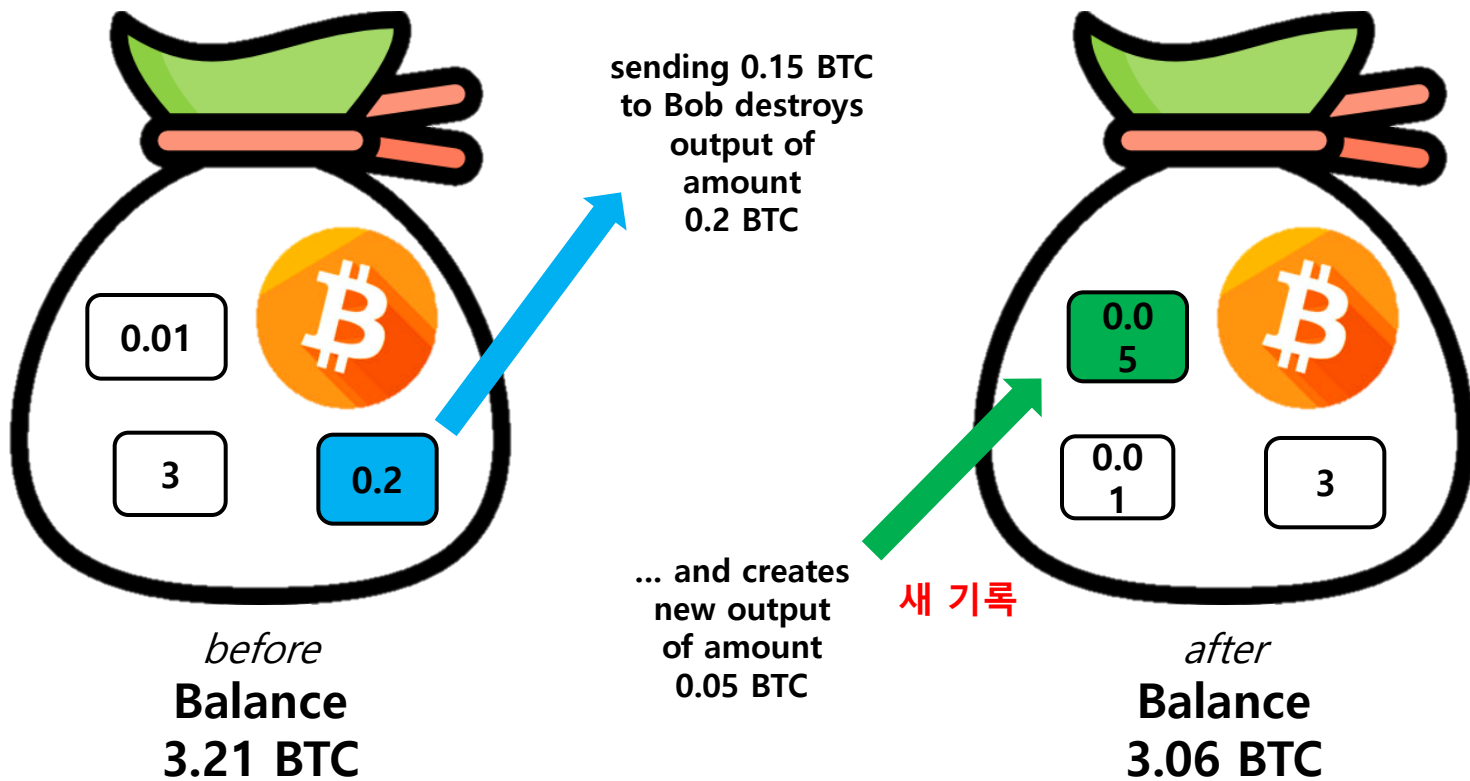
비트코인 개념

- ❖ 코인 사용 (0.15 BTC 를 사용할 때)
 - 과거 기록을 꺼내서 새로운 기록을 만듦



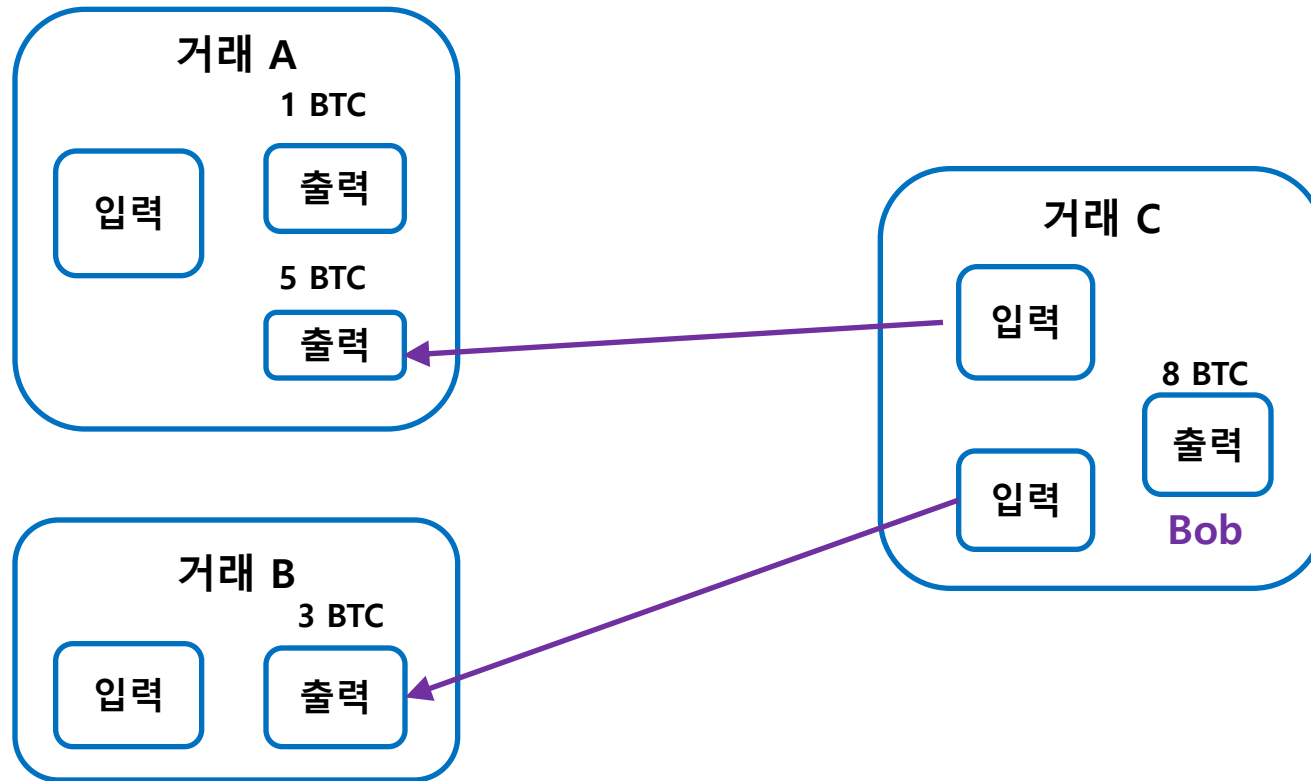
비트코인 개념

❖ 코인 사용 (0.15 BTC 사용 후 잔고)



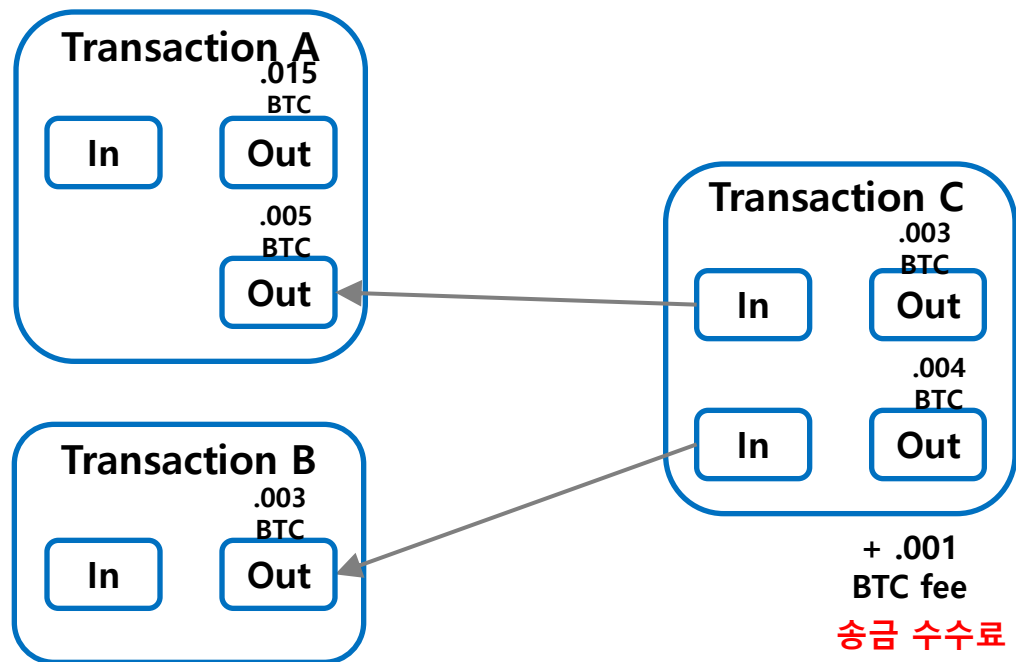
비트코인 개념

- ❖ 과거 거래로 부터 → 새로운 거래
 - 이전 거래 기록을 참조하여 송금



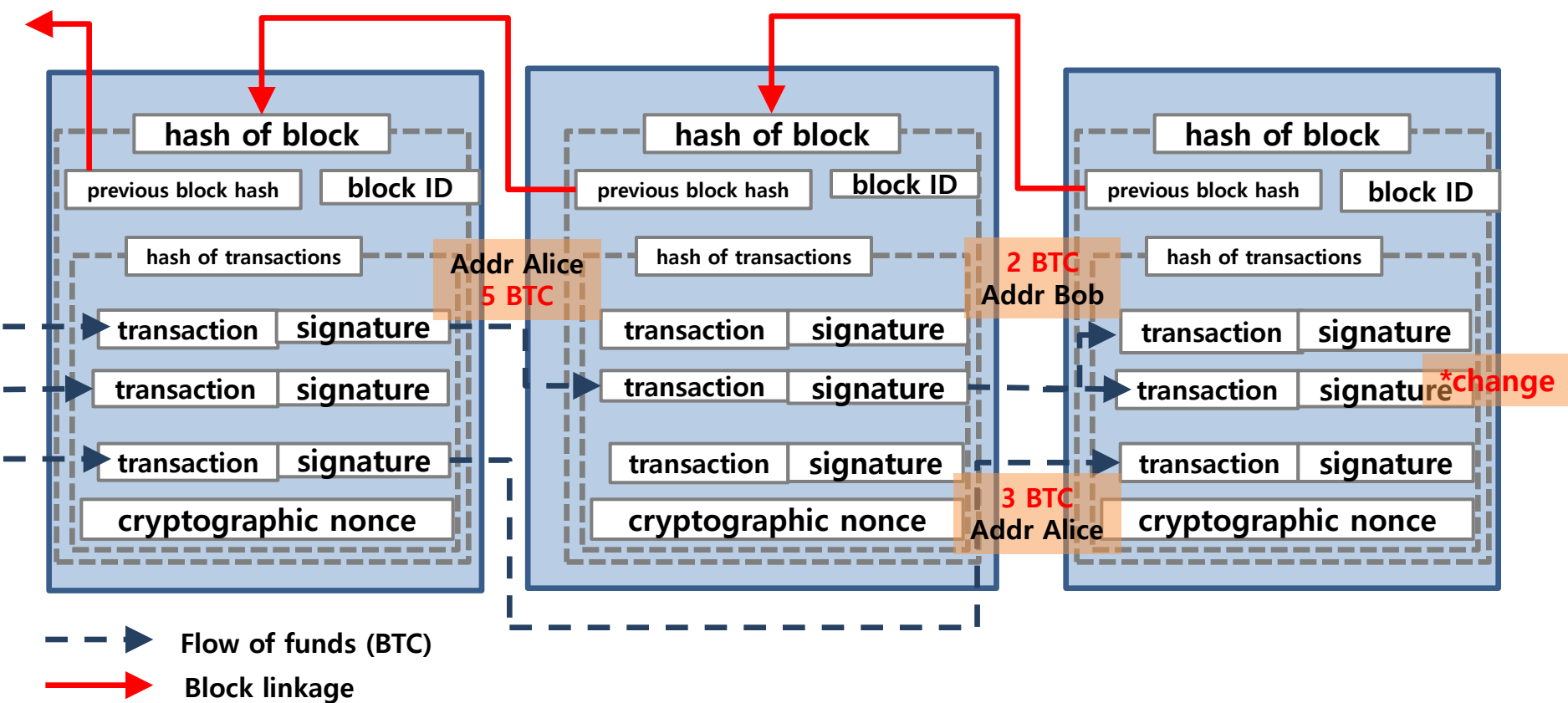
비트코인 개념

❖ 과거 거래로 부터 → 새로운 거래



비트코인 개념

❖ 과거와 현재 거래의 연결(블록, 트랜잭션)



비트코인 개념


❖ 거래

- 내 계정(내 주소)에서 내가 가진 코인 기록을 지움
- 송금액 만큼의 수신인의 새 코인 기록을 만듦
- 잔액만큼의 내 코인 기록도 새로 만듦
- 수신인의 비트코인 주소에 들어간 금액 기록 (출력 1)
- 내 비트코인 주소에서 빠져나간 잔액기록 (출력 2)
- 출력으로는 출력인덱스, 코인량(금액), 수신자주소(공개키해쉬)를 기록한다.
- 이렇게 수신된 코인을 UTXO 라 부른다.(Unspent Transaction Output)
 - 따라서 지금 사용 가능한 모든 코인은 다 UTXO 이다.

비트코인 개념

❖ UTXO 코인 사용 (새 거래 생성)

- 입력 : 이전의 본인 UTXO 코인 (출력) 정보 (이전 거래 ID, 출력 번호, 코인량)를 참조
- 출력 : 출력번호, 수신자 + 송금액 을 기록
- 생성된 거래를 비트코인 네트워크에 방송
- 이때 받는 사람은 송금이 시작되었다는 것을 알게되지만, 아직 확인(확정, 블록 등록)은 되지 않았음
- 송금 수수료 = 입력 금액의 합 - 출력 금액의 합



PKS 개념

- ❖ 인터넷은 단순히 필요로 하는 정보를 공유하거나 찾아보는 수단을 넘어서서 매우 다양한 용도로 활용되기 시작

인터넷 쇼핑

인터넷 बैंकिंग

인터넷 영화관

사이버대학

사이버관공서

PKI 개념

❖ 안전한 커뮤니케이션 환경의 필요성

- 예: 인터넷쇼핑
- 인터넷 쇼핑 사이트를 어떻게 신뢰할 수 있는가?
- 주문한 고객을 어떻게 믿을 수 있는가, 정말 본인이 주문한 것인가?
본인이 주문해 놓고도 부인하면 어떻게 하는가?
- 거래 내용은 비밀이 보장되는가? 누군가 거래 내용을 도청할 수
있지 않은가

❖ 이러한 문제들을 효과적으로 해결해 줄 수 있는 대안이 바로 공개키 기반 구조(Public Key Infrastructure, PKI)

PKI의 기본구조

❖ PKI

- 전자상거래나 정보유통의 안전성과 신뢰성을 확보하기 위한 시스템으로, 상대방의 신원을 확인하고 비밀 유지기능(정보 내용의 변경확인)과 부인봉쇄 기능을 제공.
- 기술적인 차원에서 보면
 - 공개키 알고리즘을 통한 암호화 및
 - 전자 서명을 제공하는 복합적인 보안시스템 환경
- 암호화와 복호화키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털인증서(전자서명)를 통해 사용자를 인증하는 시스템

PKI의 기본구조

❖ PKI

- 공개키 암호화나 전자서명이 안전하게 사용되기 위해서는 키의 생성과 인증, 그리고 분배와 안전한 관리를 위한 믿을 수 있는 체계가 필요한데 이것이 공개키 기반 구조(정부, 민간단체의 참여 필요)
- 가장 핵심은 공개키가 정말 맞는지 확인 해주는 구조이며 중심에 CA(Certificate Authority)가 있다
- 그런데 퍼블릭 블록체인에서는 PKI가 필요 없고 전자서명 개념만 사용된다.
- 왜냐하면 공개키는 결국 주소로 쓰이게 되며 거래를 생성하는 사람이 주소를 조작하면 본인의 손해가 되기 때문
- 하지만 프라이빗 블록체인 에서는 PKI가 꼭 필요하다.

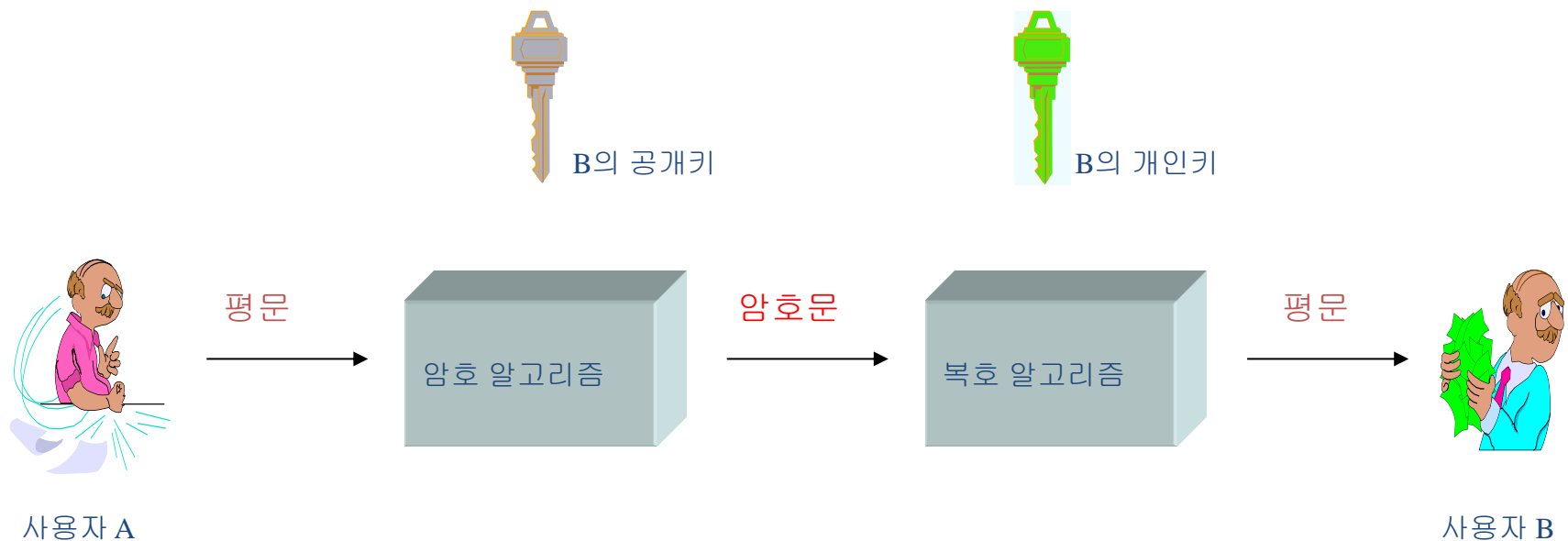
공개키(비대칭키) 암호

❖ 관용 암호와 공개키 암호 비교

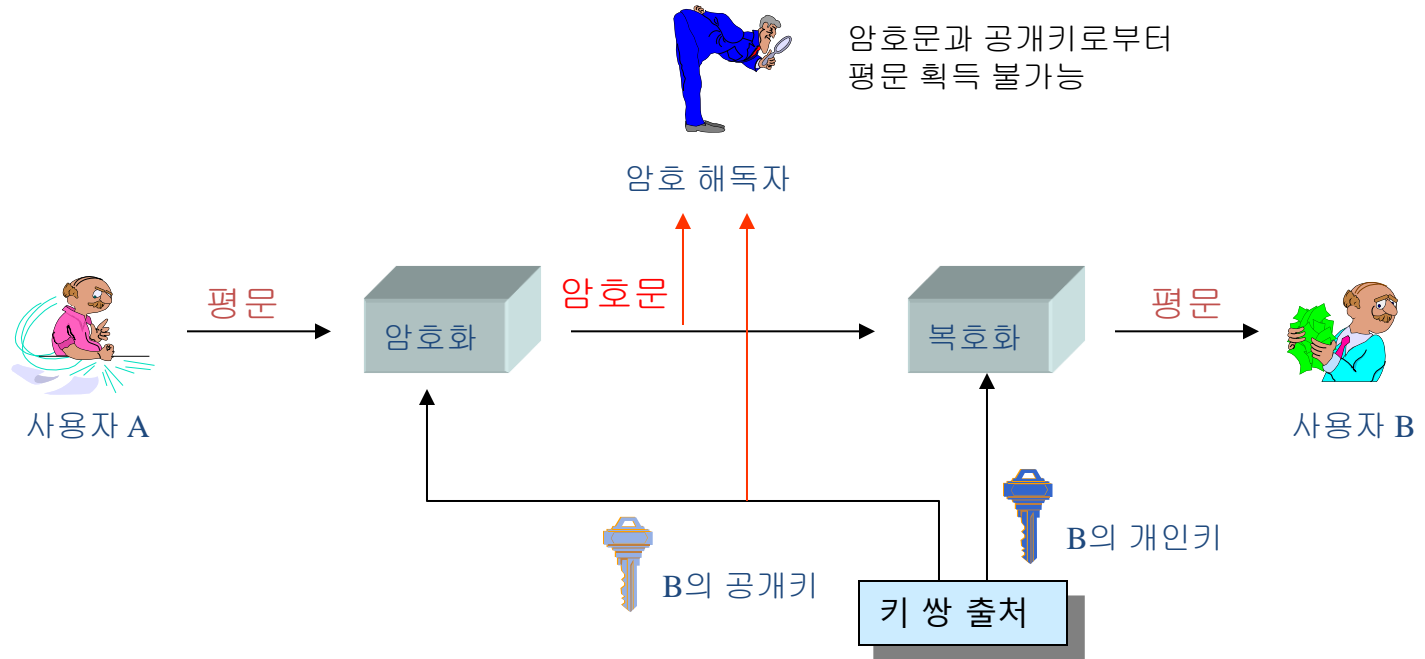
관용 암호 (대칭키)	공개키 암호
암호/복호에 동일한 키와 동일한 알고리즘 사용	암호/복호에 각각 서로 다른 키와 동일한 알고리즘 사용
수신자와 송신자는 키를 교환해야 함	수신자와 송신자는 연관된 키쌍 중 하나를 알아야 함
공유한 키(비밀키)는 비밀로 유지	키 쌍중 하나(개인키)를 비밀로 유지 공개키를
키 분배의 어려움	공개키를 공개
디지털 서명 불가능	디지털 서명 가능
속도가 빠름	속도가 느림

공개키(비대칭키) 알고리즘 &CC

❖ Elliptic Curve Cryptography & Diffie-Hellman Youtube



공개키 사용한 암호

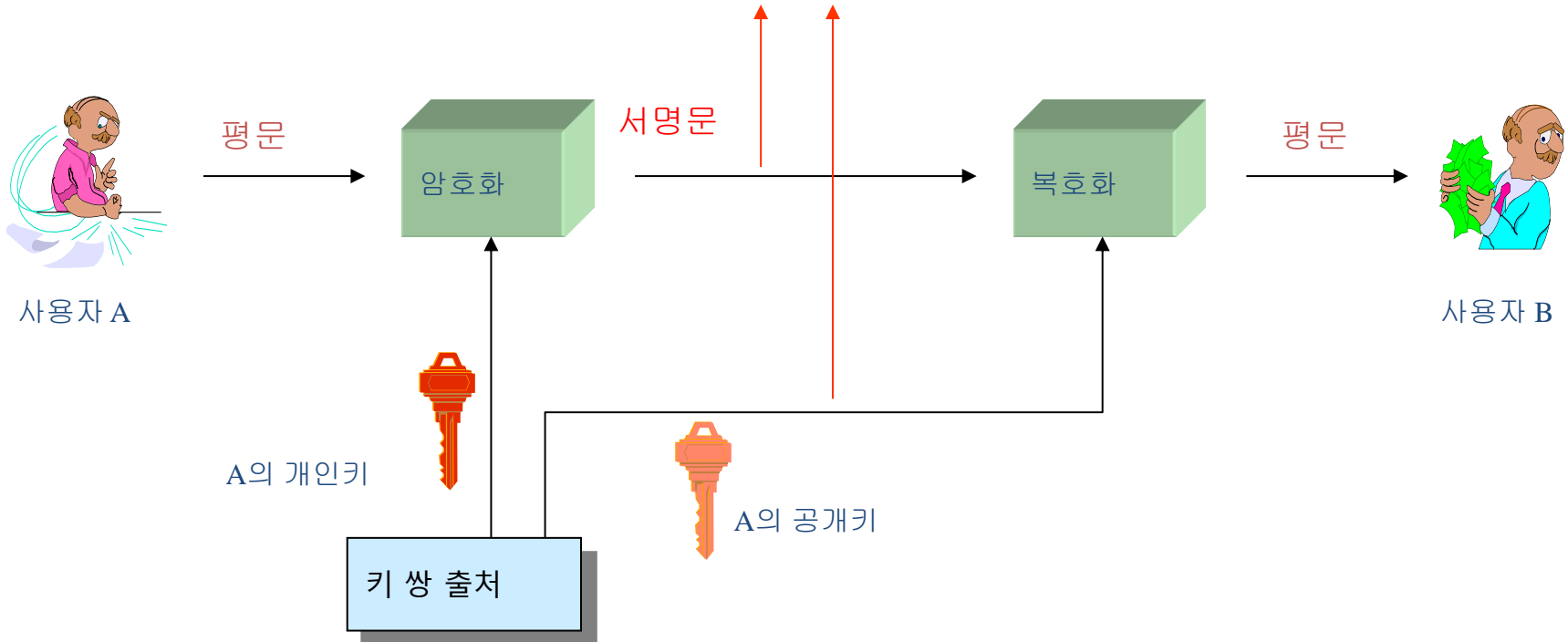


공개키 사용한 인증



개인키를 알 수 없음으로
위조된 서명문 작성 불가능
(평문은 알 수 있음)

암호 해독자



해쉬함수 특성



사용자 패스워드

8바이트

일방향 해시함수
(SHA-1)

43 B0 4C 54 3B
67 A2 23 3F 7D
36 2B 7A 2B 49
3C D3 AF 27 4A

해시값 20바이트



스캐너로부터의
영상 데이터

512 킬로바이트

일방향 해시함수
(SHA-1)

73 BF 4C 34 3B
67 A2 45 23 76
3F 76 D2 37 F6
44 47 8F 93 D2

해시값 20바이트



플로피 디스크의
모든 파일

1.4메가바이트

일방향 해시함수
(SHA-1)

54 3B 4C 34 3B
62 3C D3 AF A2
45 67 A2 23 3F
7D 43 B0 4C 19

해시값 20바이트



하드 디스크의
모든 파일

80기가바이트

일방향 해시함수
(SHA-1)

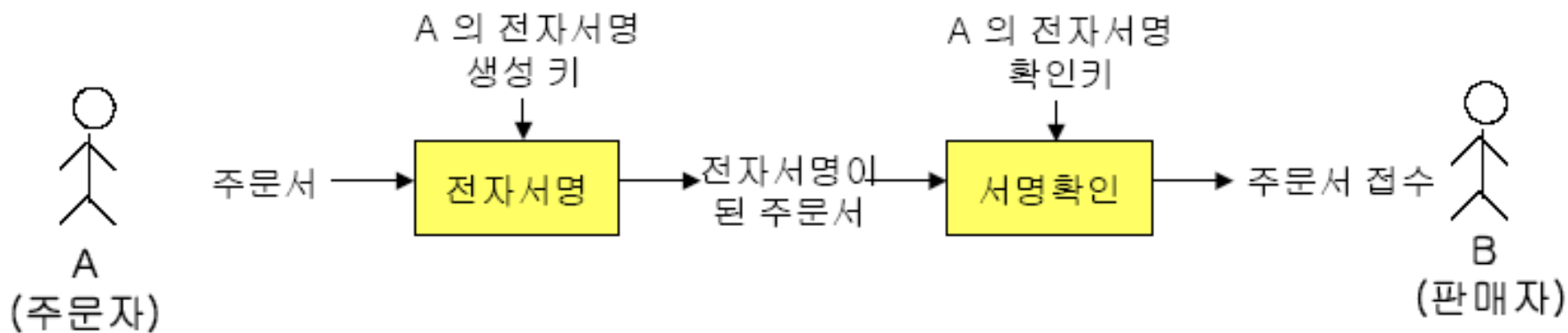
32 2B 23 70 7A
2B 4F 43 B0 4C
54 3B 49 28 67
A2 23 8F 7D 36

해시값 20바이트

PKI의 기본구조

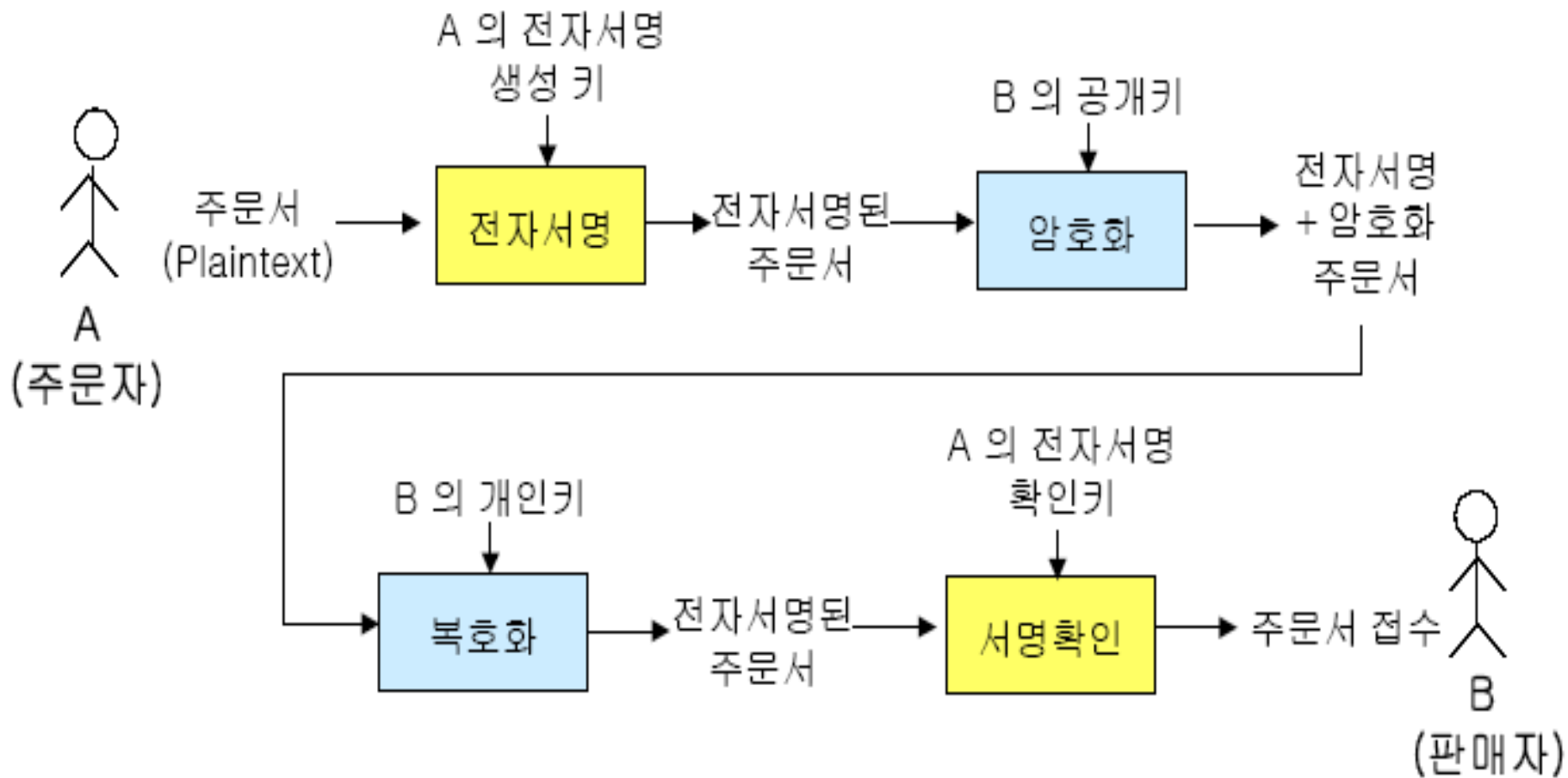
❖ 전자서명

- 주문서가 A가 보낸 것임을 증명
- A는 주문서를 보내지 않았다고 부인할 수 없다



PKI의 기본구조

❖ PKI : 공개키 암호화 + 전자서명



전자서명

❖ 전자서명(Digital Signature)

- 현실 세계에서 상거래시, 계약시 인감을 찍으면 법적 효력이 있음
- 전자서명은 인터넷 상에서 인감의 역할을 하며 역시 법적인 효력을 갖는다.
- 국내의 전자서명법
 - 1998년부터 제정 작업 추진
 - 1999년 2월 5일: 전자서명법 공포(법률 제5792호)
 - 1999년 6월 30일: 전자서명법 시행령 발표(대통령령)
 - 1999년 7월 1일: 전자서명법 발효
 - 1999년 7월 7일: 전자서명 인증관리센터 설립(한국정보보호센터내)

전자서명

❖ 전자서명(Digital Signature)

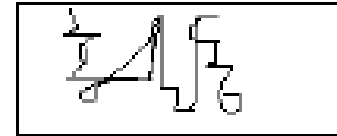
■ 해외의 전자서명법 현황

국가	법제정년도	공인인증기관
미국(유타주)	1995	DST, Arcanvs, USERTrust
독일	1997	도이치 텔레콤
말레이시아	1997	-
이탈리아	1998	-
싱가포르	1998	-

전자서명

❖ 전자서명의 개념

- 광의의 전자서명(electronic signature)
 - 전자펜을 이용한 그래픽 기반의 서명방식(수기서명과 비슷)
 - 위조가능, 변조가능, 부인가능



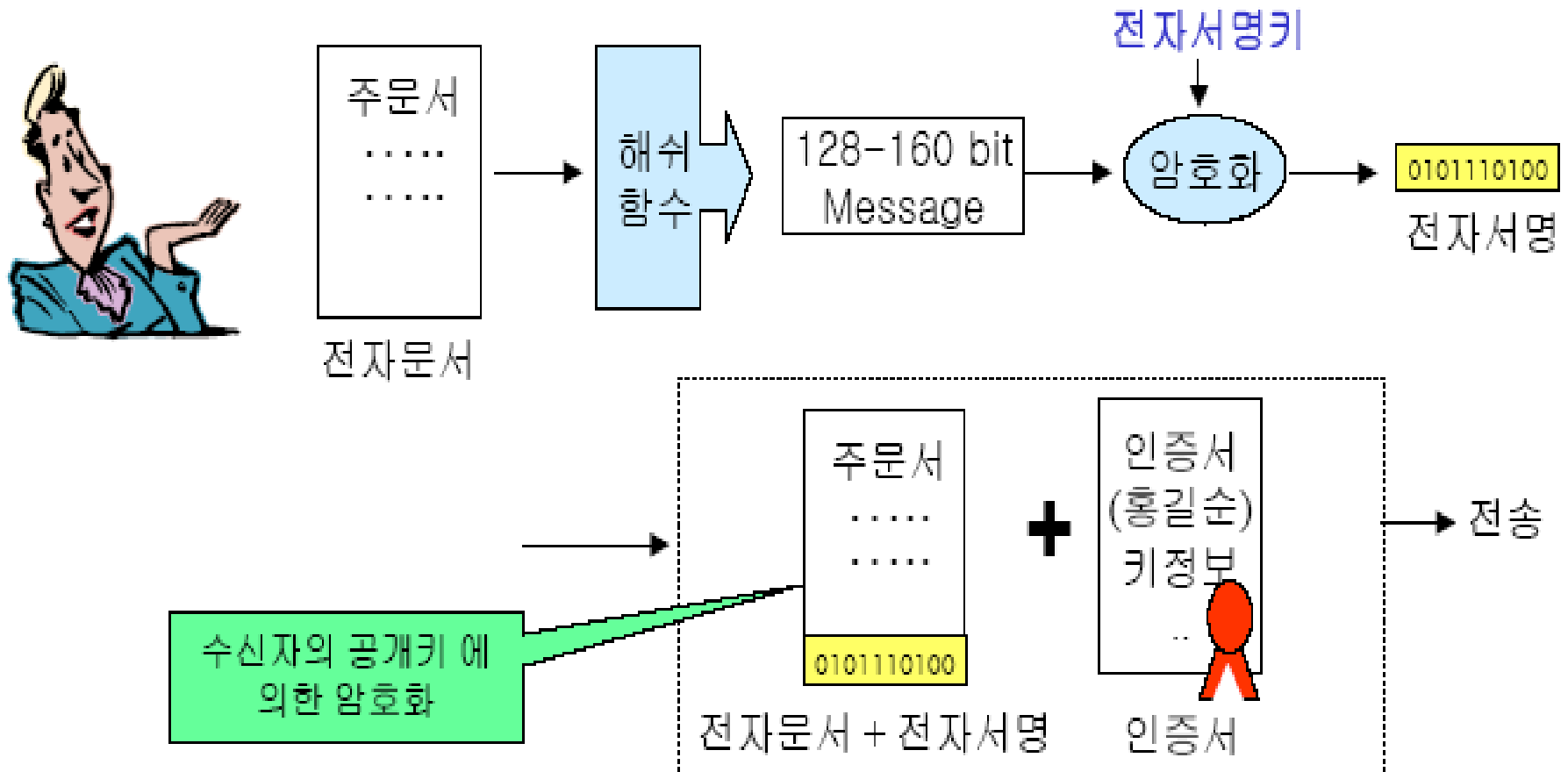
- 협의의 전자서명(digital signature)
 - 디지털 데이터 스트림으로 구성된 서명키 이용방식
 - 위조불가, 변조불가, 부인불가

AX1028B40612DSF084QW

전자서명

❖ 전자서명 체계

- 송신자



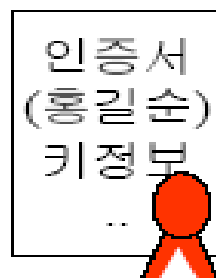
전자서명

❖ 전자서명 체계

- 수신자



인증기관에
확인



전자서명
검증키

전자서명 분리
(수신자 개인키로 복호화)

0101110100

주문서
.....

복호화

해쉬
함수

H1

H2

$H1 = H2$: Verified



PKI 구성요소

❖ 공개키 알고리즘

- 비대칭키 암호화 알고리즘으로 메시지의 암호화 및 서명에 사용됨.

❖ 공개키 인증서(Public-key Certificate, Certificate)

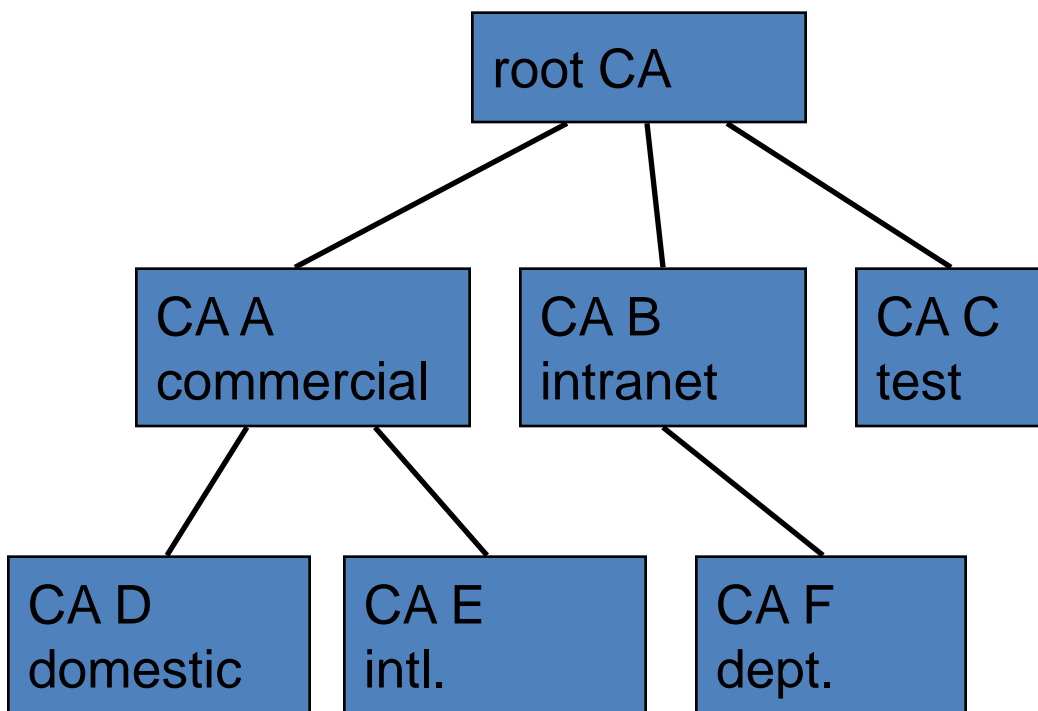
- 공개키에 관한 정보와 인증기관의 서명
- 공개키의 무결성, 신빙성을 보증함
- X.509 형식

❖ 인증기관 (Certificate Authority, CA)

- 인증 객체에 대한 인증서를 발급(또는 폐기)함
- 신뢰된 인증기관에서 발급한 인증서는 공개키와 공개키의 주체를 연결시켜주는 고리가 됨
- 공개된 Certificate Directory (인증서 보관 장소)에 인증서를 저장하여 둠.

CA 계층구조

- ❖ 하나의 공증 사무소가 인터넷의 모든 호스트를 증명할 수 없다.
- ❖ 공증 사무소가 공증 사무소를 증명
- ❖ 중앙 CA 존재



2

블록체인 용어정리

기본 용어정리
기술 용어 정리
기타 참고사이트


블록체인 기본용어

❖ 블록체인(Blockchain)

데이터를 '블록'에 담아 체인 형태로 연결하고, 이를 여러 대의 컴퓨터에 복제하여 저장하는 분산형 데이터 저장 기술이다. 중앙 집중형 서버에 거래 데이터를 보관하지 않고, 모든 사용자가 거래 기록을 공유/대조하도록 하여, 데이터 위조나 변조를 할 수 없게 되어 있다. 일종의 '분산식 공공장부'의 개념으로 널리 알려져 있다.

퍼블릭 블록체인(Public Blockchain)

공개형 블록체인이라고 불리기도 하며, 전 세계의 누구나 모두 읽고 거래 정보를 발송하고 거래가 유효한지 확인할 수 있으며, 누구나 합의 과정의 블록체인에 참여할 수 있다. 통상적으로 완전한 탈중앙화 시스템으로 여겨진다.



블록체인 기본용어

프라이빗 블록체인(Public Blockchain)

폐쇄형 블록체인이라고도 불리기도 하며, 기관 또는 조직에서 권한을 통해 관리되는 블록체인을 말한다. 이 해당 네트워크에 참여하기 위해서는 고유의 인증 방식을 통과해야 한다.


컨소시엄 블록체인(Consortium Blockchain)

미리 선정된 노드에 의해서 제어되는 퍼블릭과 프라이빗 블록체인 사이의 반 중앙형 블록체인이다. 미리 선정된 기관이 노드를 한 개씩 운영하고 각 기관의 노드 간 동의가 일어나야 거래가 생성된다. 블록체인의 기록 열람 권리를 퍼블릭 블록체인처럼 대중에게 부여할 수도 있지만, 특정 기관에만 제공하거나 API를 통해 특정 인원에게만 공개할 수도 있다.

블록체인 기본용어

❖ 블록(Block)

유효한 거래 정보의 묶음을 말하며, 데이터를 저장하는 단위이다. 일정 기간의 거래 데이터를 블록에 분산 저장하는데, 블록체인 네트워크마다 블록 안의 거래 데이터는 조금씩 다르다. 블록은 블록 헤더와 거래 정보, 기타 정보로 구성되며, 비트코인의 경우 블록 하나에 약 1,800 ~ 4,200 건의 거래 정보가 포함될 수 있다.




블록체인 기본용어

머클 트리(Merkle tree)

블록에 포함된 거래의 요약을 나무 형태로 만들게 된다. 해시 트리(Hash tree)라고도 하며, 랄프 머클의 이름을 따서 머클 트리라고도 불린다. 해시 함수를 통해 2개의 거래 데이터를 하나의 데이터로 묶는 방식을 통해 용량을 절약한다.

머클 루트(Merkle root)

블록에 저장되어 있는 모든 거래의 요약본으로 해당 블록에 포함된 거래로부터 생성된 머클 트리의 루트에 대한 해시를 의미한다




블록체인 기본용어

제네시스 블록(Genesis Block)

블록체인 네트워크의 시작을 상징하는 첫 번째 블록이다. 첫 번째 블록이 생성된 이후 다음 블록이 지속적으로 연결된다. 블록이 생성된 순서는 높이로 표현하며, 0번 블록은 네트워크가 최초에 시작될 때 만들어진 제네시스 블록이 된다.

블록 높이(Block Height)

제네시스 블록으로부터 현재 블록까지 블록이 만들어진 양을 나타내며, 이 수치를 높이로 표현한다.




블록체인 기본용어

블록 헤더(Block Header)

블록 해시, 거래정보, 머클루트, 난수 등 블록의 주요 데이터를 담고 있다. 블록체인 네트워크마다 헤더 안의 데이터는 다를 수 있다.

블록 보상(Block Reward)

컴퓨팅 파워를 투입해서 가장 먼저 작업증명을 달성한 채굴자에게 주어지는 보상이다. 작업증명을 위해서 전기와 같은 비용이 들기에 블록 보상은 네트워크가 보상의 개념으로 새로운 블록 각각에 포함되어있다.



블록체인 기본용어

블록 타임(Block Time)

일정한 블록이 생성되는데 걸리는 시간으로 비트코인의 경우 평균적으로 10분에 하나의 블록이 만들어지도록 설계되어 있다. 블록 타임을 유지하기 위해서 채굴 난이도가 조정된다.

블록 탐색기(Block Explorer)

거래 내역, 주소, 특정 블록에 대한 정보 등을 보여주는 탐색기로써, 각각의 블록체인에 따른 블록 탐색기가 존재한다. 대표적인 블록 탐색기는 <https://blockexplorer.com>, etherscan.io 등이 있다.

블록체인 기본용어

❖ 주요 체인(Main chain)

제네시스 블록으로부터 가장 최근의 블록까지 연결되어 있는 체인을 말한다. 주요 체인 또는 최장 체인이라 부르며, 가장 많은 해시 파워가 투입되는 체인에 다음 블록이 연결된다.

❖ 댕(DAPP, Decentralized Application)

블록체인 기반 플랫폼 위에서 작동하는 탈중앙화된 어플리케이션이다. DAPP의 참여자가 많아질수록 해당 토큰에 대한 수요가 늘어나며 DAPP을 사용하는데 필요한 플랫폼의 가치는 증가한다.

블록체인 기본용어

암호화폐(Cryptocurrency)

디지털 자산의 한 종류로 블록체인 기술을 활용하는 분산형 시스템 방식으로 처리된다.
보안을 위해 암호화를 사용하여 거래 내역을 검증하는 시스템으로 이루어져 있으며, 최초의 암호화폐는 2009년 출현한 비트코인이다.

암호화폐 주소(Cryptocurrency Address)

암호화폐를 지갑에 보관하기 위한 주소이다. 여러 복잡한 숫자/영문 대소문자의 조합으로 암호화폐를 보내고 받기 위해 필요하다. 주소를 통해 수신인과 발신인을 확인할 수 있으며 비트코인(BTC), 이더리움(ETH) 등 여러 방식의 암호화폐 주소가 존재한다. 최근에는 거래소에서 편리하게 암호화폐 주소를 생성하여 이용할 수 있다.



블록체인 기본용어


암호화폐 거래소(Cryptocurrency Exchange)

블록체인 기술을 활용하는 디지털 자산인 비트코인 등 암호화폐를 사용자들이 교환할 수 있는 거래소를 암호화폐 거래소(Cryptocurrency Exchange)라 한다. 증권 거래소와 비슷한 방식으로 운영된다. 이용자들 사이에서 발생하는 거래 수수료를 주요한 비즈니스 모델로 가지고 있다.

탈중앙화 거래소(Decentralized Exchanges : DEX)

중앙집권형 거래소가 가지고 있는 해킹 위험을 감수하지 않고 거래소의 중개 없이 개인간 직거래를 할 수 있도록 네트워크의 노드가 거래소의 시스템을 형성하는 거래소를 의미한다. 암호화폐 개인 지갑을 통해 자유롭게 거래하며 누구나 지갑을 만들고 참여할 수 있는 암호화폐의 성격을 그대로 반영한 거래시스템이다. CryptoBridge, EtherDelta, Bitshares, OpenLedger 같은 거래소가 있다.





블록체인 기본용어

비트코인(Bitcoin)

비트코인(BTC)은 결제 시스템으로, 중앙은행 또는 단일 관리자 없이 작동하는 최초의 분산형 암호 화폐다. 네트워크는 Peer to Peer(P2P) 방식이며 중개자 없이 사용자 간에 직접적인 트랜잭션이 발생한다. 이러한 거래는 암호화를 통해 네트워크 노드에 의해 검증되고 블록체인이라고 하는 공개적인 분산 원장에 기록된다. 비트코인은 사토시 나카모토 라는 알려지지 않은 개인 혹은 그룹에 의해 발명되어 2009년 오픈 소스 소프트웨어로 출시되었다.

블록체인 기본용어

스테이블코인(stable coin)

법정화폐 또는 실물 자산을 기준으로 가격이 연동되는 암호화페를 뜻한다. 기존의 암호화페는 특유의 가격 변동성 때문에 통화로써 사용되기에는 안정성이 떨어진다는 평가를 받는 반면 USDT와 같은 코인은 가치가 달러에 고정되기에 기존의 변동성이 높은 암호화페에 비해 가격 안정성이 높다.

이더리움(Ethereum)

이더리움은 튜링 완전성을 지원하며 프로그래밍이 가능한 블록체인 기술 기반의 분산 컴퓨팅 플랫폼이다. 이더리움은 비트코인과 같이 블록체인을 기반으로 하지만, 튜링 완전성을 지원하는 프로그래밍 언어의 접목을 통해 스마트 계약과 범용적인 목적의 분산된 어플리케이션(Dapp)의 개발 및 실행 환경을 지원한다.

블록체인 기본용어

가스(Gas)

가스는 모든 이더리움 플랫폼에서 트랜잭션을 실행하기 위한 네트워크 수수료의 단위이다. 이더리움(ETH)을 전송할 때 네트워크의 모든 노드가 같은 계산을 수행하고 같은 값을 저장해야 하는 작업이 필요한데, 이러한 작업량을 GAS 혹은 특정 금액으로 환산하게 된다.

이더리움 가상 머신(EVM)

이더리움은 이더리움 가상 머신(EVM : Ethereum Virtual Machine)을 통해 원활한 스마트 계약 활용을 지원한다. 이더리움 가상머신이란, 이더리움 블록체인 네트워크의 노드들이 공유하는 가상환경이자 자체 중개 시스템 역할을 수행하는 트랜잭션 프로토콜을 의미한다.

블록체인 기본용어

ERC(Ethereum Request for Comment)

이더리움 블록체인 네트워크에서 발행되는 토큰의 호환성을 보장하기 위한 표준 사양이다. 이더리움 블록체인 네트워크에서 구현되기 위해 만들어진 일련의 표준들을 설명하며, 대표적으로 ERC20 토큰 표준이 있다.

ERC20(Ethereum Request for Comment 20)

Ethereum Request for Comment 20를 줄여 ERC20이라 부른다. 이더리움 블록체인 네트워크에서 발행되는 토큰의 표준으로 필요한 이더리움과 호환성이 있는 모든 요구 사항을 충족시키는 표준은 ERC20으로 간주된다. ERC20 토큰은 이더리움과 교환 가능하며 이더리움 지갑으로 전송이 가능하다.


블록체인 기본용어

토큰(Token)

독립된 블록체인 네트워크(메인넷)가 아닌 이더리움과 같은 플랫폼을 이용하여 발행할 수 있는 암호화폐이다. 독립된 블록체인 네트워크를 소유한 경우에는 코인으로 부르며, 비트코인, 이더리움, 퀀텀, 스팀 등이 있다. 코인과 같이 메인넷 시스템을 한 번에 구축하는 것은 어렵기 때문에 먼저 이더리움과 같은 플랫폼 위에 토큰을 발행한 뒤 개발을 통하여 코인으로 전환하게 된다.

테스트넷(Testnet)

기존의 플랫폼으로부터 독립된 자체 메인넷 블록체인을 구축하기 위한 작업이다. 테스트넷(Testnet: 일종의 베타 서비스) 과정을 통해 블록체인 및 지갑의 안정성이 검증되며 최종적으로 독립된 블록체인을 구현하는 메인넷이 출시된다.



블록체인 기본용어

메인넷(Mainnet)

메인넷은 기존에 존재하는 플랫폼에 종속되지 않고, 독립적인 플랫폼으로 새로운 생태계를 구성하고 자체 지갑을 생성하는 것이다. 안정성이 검증된 메인넷을 갖는 것은 난이도가 상당하며 그만큼의 기술력을 필요로 한다.

트랜잭션(Transaction)

암호화폐를 송금하는 이체 거래 과정에서 전송되는 서명된 정보를 의미하며 하나의 문자열로 생성된다.

블록체인 기본용어

트랜잭션 ID(TxID : Transaction ID)

TxID는 트랜잭션 데이터 전체에 대한 해시값(데이터를 문자열로 치환)이다. 해시값은 데이터가 조금만 달라져도 전혀 다른 값이 되며 이를 이용해 트랜잭션에 대한 블록체인 네트워크의 기록을 조회 및 식별할 수 있다. 지갑 주소, 수량, 컨펌 수, 시간 등의 확인이 가능하다.

트랜잭션 수수료(Transaction Fee)

암호화폐를 전송할 때 노드(Node)에게 지불되는 수수료를 의미한다. 거래가 블록에 포함되기 위해서는 증명 작업이 필요하다. 노드들이 이 검증과 증명을 대신 해주는 대가로 블록 보상과 함께 수수료를 받는다. 수수료는 암호화폐 네트워크가 노드에게 제공하는 경제적 유인이다. 즉, 트랜잭션을 만든 사람이 채굴자에게 지불하는 비용이며 일반적으로 수수료는 트랜잭션의 우선순위에 영향을 준다.


블록체인 기본용어

컨펌(Confirm)

암호화폐는 거래 시 인증받는 과정을 컨펌이라고 한다. 거래가 블록에 포함되어 발행되었는가를 확인하는 것이다. 예를 들어 1컨펌이 출력되면 블록이 한 개 쌓였음을 의미한다. 블록 위에 블록이 쌓일 때마다 컨펌의 수도 증가한다.

컨펌 숫자(Confirmation Number)

주요 체인으로부터 해당 트랜잭션이 거절(reject)될 가능성을 측정하는 단위이다. 제로 컨펌이라는 의미는 해당 트랜잭션이 컨펌되지 않은 것을 의미하며, 1컨펌은 해당 트랜잭션이 주요 체인의 가장 최근 블록에 속해 있음을 의미한다. 이러한 방식으로 N컨펌을 설명할 수 있으며, 더 많은 블록이 추가됨으로써 트랜잭션이 역방향으로 수행될 가능성(이중지불)은 극히 낮아지게 된다.



블록체인 기본용어

스마트 컨트랙트(Smart contract)

스마트 컨트랙트는 블록체인에서 거래의 일정 조건을 만족시키면 자동으로 거래가 체결되는 기술이다. 블록체인 기반으로 금융부터 부동산 공증 등 다양한 형태의 계약을 체결하고 이행할 수 있으며 스마트 컨트랙트를 작동시키려면 모든 사용자가 동일한 권리를 갖는 분산된 네트워크가 필요하다.

블록체인 기본용어


합의 알고리즘(Consensus Algorithm)

생성된 블록의 유효성을 검토하여 블록체인에 반영 여부를 의사결정하는 방식을 의미한다.

대표적으로 작업 증명(PoW), 지분 증명(PoS), 위임 증명(DPoS) 방식이 있다.

작업 증명(PoW : Proof of Work)

컴퓨터 연산 작업을 수행하여 블록체인에 기여하는 대가로 보상을 받는 방식이다. 연산을 위해서는 성능이 우수한 장비를 필요로 한다. P2P 네트워크에서 시간과 비용을 들여 수행된 컴퓨터 연산 작업을 신뢰하기 위해 참여당사자 간에 간단히 검증하는 방식이다.



블록체인 기본용어

지분 증명(PoS : Proof of Stake)

노드에 기여하는 대가로 보상을 받는 방식이다. 채굴 파워가 아닌 지분에 따른 정당한 의사결정이 이루어지며 채굴 파워에 의한 중앙화를 방지하며 에너지 낭비를 최소화한 친환경적인 방식이다. 지분에 비례한 공정한 보상 지급을 통해 작업 증명 방식의 단점을 보완한다.

위임 증명(DPoS : Delegated Proof of Stake)

자격을 갖춘 선택된 증인이 참여자들이 보유하고 있는 지분을 위임받아 블록을 검증하는 방식이다. 이중 채굴과 그라인딩 어택에 대해 내성을 갖는 합의 프로토콜이라 평가받는다. 모든 참여자가 블록을 검증하는 것이 아닌 소수의 증인만이 블록을 검증하기 때문에 증명 속도가 빠르다는 장점이 있다.

블록체인 기술용어

노드(Node)

블록체인 분산원장 네트워크 노드이다. 블록체인은 중앙 집중형 서버에 거래 기록을 보관, 관리하지 않고 거래에 참여하는 개개인의 서버들이 모여 네트워크를 유지 및 관리하는데 이 개개인의 서버, 즉 참여자를 노드라고 한다. 비트코인은 채굴자부터 일반 사용자까지 모두 비트코인 네트워크 중 하나의 노드로 볼 수 있다. 다만 비트코인은 다중심화 특징을 갖고 있어 '비트코인 풀 노드'라는 중역할을 하는 노드가 필요하다. 네트워크의 데이터를 보관하며 생성된 거래마다 정보를 수신하는 노드는 거래에 대해 검증하고 다른 노드에 전송을 한다. 때문에 데이터가 한번 생성되면 이를 변조할 수 없고 노드의 수가 많을수록 블록체인 네트워크는 더 안전하다고 할 수 있다. 피어(Peer)라는 이름과 유사하게 사용된다.

블록체인 기술용어

풀 노드(Full Node)

풀 노드는 모든 블록체인 원장을 가진 노드로 블록체인 데이터를 동기화하기 위해 메모리를 사용한다. 모든 거래를 검증하고 실시간으로 데이터를 업데이트할 수 있으며 분산 원장 중 블록체인 거래를 전송 및 수신하고 확인하는 중요한 역할을 담당한다. 비트코인에서는 비트코인 클라이언트를 통해 완전한 블록체인 데이터를 다운로드하고 보존한다.

❖ OKCOIN 용어사전 참조



다른 용어 정리 사이트

- ❖ 쉽게 설명하는 블록체인 : 블록체인 용어 정리
- ❖ 블록체인 용어 정리 - 브런치
- ❖ 블록체인 용어 사전!! - Steemit



블록체인 애니메이션 데모

❖ 블록체인 데모:

<https://andersbrownworth.com/blockchain/>

❖ 리얼 비트코인 트랜잭션 애니메이션:

<https://blocks.wizb.it/>

❖ 비트코인 이더리움 탐색기

<https://www.blockchain.com/>

3

합의 알고리즘

PoW

PoS

DPoS

합의 알고리즘(Consensus)

❖ 블록체인 합의

- P2P 네트워크에서는 클라이언트 서버 구조와 달리 정보의 지연과 미 도달 사태를 피할 수 없음
- 데이터를 변조할 의도가 없다 해도 이중 송신에 따른 처리 중복이나 잘못된 정보에 의한 오작동 등의 위험이 있어 정확한 정보를 공유하는데 어려움이 있음

❖ 합의 알고리즘

- P2P 네트워크 시스템에서 각 노드간 정보 도달의 시간 차이가 있음
- 생성된 블록의 정당성을 검토하고 해당 블록을 블록체인에 연결하기 위해 네트워크 참가자들의 합의를 위한 알고리즘이 필요

합의 알고리즘의 종류

❖ 작업증명 (Proof of Work, PoW)

- 블록체인에서 가장 보편적으로 사용중인 합의 알고리즘으로 컴퓨팅 파워를 이용하여 특정 난이도의 해시값을 역함수를 해시화 하여 Nonce 값을 계산해내고 이를 검증하는 것으로 합의를 도출한다.

❖ 지분증명 (Proof of Stake, PoS)

- PoW의 컴퓨팅 파워 낭비 문제를 해결하고자 개발된 합의 알고리즘으로 노드가 보유한 자산을 기준으로 권한을 분배 하여 합의를 도출하고 보상을 분배하는 알고리즘이다.

❖ 이외에도 Proof of Elapsed Time (PoET) 등의 다양한 알고리즘 존재

합의 알고리즘(Consensus)-PoW

❖ 작업증명(PoW, Proof of Work)

- Bitcoin 창시자인 Satoshi Nakamoto의 뛰어난 업적은 분산 네트워크에서 간의 합의를 달성하기 위한 작업 증명 프로토콜을 활용하는 것
- 여러가지 존재하는 기술을 융합시켜 블록체인이라는 혁명적 기술을 세상에 선 보임

❖ 시장 경제학적 솔루션

- 공학적 솔루션이 아닌 이기 때문에 매우 다양한 합의알고리즘이 제안되고 있음
(51%공격을 감행할 수 있는 주체는 마이너들인데 마이너들이 비트코인 생태계에 좋지않은 공격을 할리가 없다)

합의 알고리즘(Consensus)-PoW

Proof of Work



*proof of work is a requirement to define
an expensive computer calculation,
also called mining*

<https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

합의 알고리즘(Consensus)-PoW

❖ 작업증명

- Bitcoin의 합의 프로토콜
- 이 프로세스를 '마이닝'이라고 하며 네트워크의 노드를 '광부'라 함
- "작업 증명"은 도착하기 위해 상당한 노력이 필요한 수학적 문제에 대한 답을 해결하는 과정
- 비트코인은 가장 긴 체인(Longest Chain)을 선택하는 방법을 사용
- 풀기 어려운 문제를 빨리 해결한 사람에게 블록을 생성할 수 있는 권한 부여하고 보상으로 코인을 제공
- 문제는 해시 함수의 결과값이 특정 값보다 작아지도록 하는 입력 값 (Nonce)을 찾는 것
- Nonce 값을 만드는 데에는 SHA-256 알고리즘 사용
- 비트코인은 약 10분 정도 걸려 풀릴 수 있는 난이도

합의 알고리즘(Consensus)-PoW

❖ 해시

- *SHA(Security Hash Algorithm)은 미국 표준 기술 연구소(NIST)에 의해 공표된 해시 알고리즘
- SHA-256은 256비트로 구성되어 64자리 16진수(4 비트) 열을 반환한 값
- 해시 함수는 단방향 암호화 기술이므로 결과값으로 입력 값을 찾을 수 없음
- 블록 해쉬값이 특정 숫자보다 작아지게 하는 nonce값을 찾는 것이 마이닝

❖ 마이너

- CPU, GPU같은 장비를 통해 해시 함수의 출력 값을 구함
- 결과값이 나올 때까지 입력 값을 바꿔 지속적으로 실행 해야함
- Nonce값을 구해서 블록해쉬 값을 구하고 이 블록 해쉬값을 식별자로 가지는 유효한 블록을 만들어 내야함

합의 알고리즘(Consensus)-PoW

❖ 마이닝

- 블록(B)의 해쉬값은 $\text{Hash}(B) \leq M/D$ 로 정의
- D : 난이도 (Difficulty)
- M : 난이도 D의 최대 값($2^{256} - 1$)

❖ 보상

- Nonce값을 구하기 위해서는 많은 작업 비용이 들며 이러한 행위의 보상이 없다면 아무도 채굴하지 않을 것
- 비트코인에서 보상은 새로 발행되는 비트코인과 해당 블록에 포함된 거래의 거래 수수료의 합

합의 알고리즘(Consensus)-PoW

❖ 특징

- 블록 거래 내용 변경을 위해 많은 자원이 필요해 위,변조가 사실상 어려워 보안성이 좋다고 할 수 있음
- 채굴 난이도가 높아질 수록 연산에 고 사양의 장비들이 필요하게 됨
- 반복적인 연산을 통해 불필요한 연산을 하게 되면 전기와 CPU와 같은 리소스 낭비가 심함
- 노드들이 트랜잭션을 검토해야 하기 때문에 모든 블록 정보를 보유해야 하며, 이를 통해 이중 지불 문제를 해결

❖ 문제점

- 51%의 공격 : PoW의 경우 악의적인 참여자가 절반 이상의 해시 파워를 가지게 된다면 블록 내용의 조작이 가능

합의 알고리즘(Consensus)-PoW

❖ PoW 파이널리티 불확실성

- PoW는 블록체인이 분기하게 되는 경우 긴 체인이 올바른 것으로 판단
- 짧게 체인이 버려지는 경우 트랜잭션이 미확인 풀로 들어가므로 합의 시간이 매우 길어질 확률이 있으나 결국은 블록에 들어가게 됨
- 이때 고의적인 이중지불(double spending) 문제가 발생할 수 있기 때문에 비트코인의 경우 이런 현상을 방지하기 위해 트랜잭션이 블록에 올라 가도 6블록(1시간) 이상 기다리는 것이 안전함

❖ PoW 성능 한계

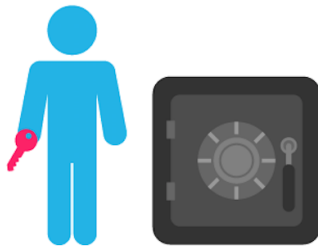
- P2P 네트워크에서 단일 정보를 공유하는 구조상 네트워크에 확산되는 시간을 없애는 것은 불가능
- 여러 노드간의 합의를 통해 정보의 신뢰성을 담보하기 때문에 합의에 걸리는 시간이 필요

합의 알고리즘(Consensus)-PoS

❖ 지분증명(PoS, Proof of Stake)

- 블록체인 기술에서 일반적으로 사용되는 합의 프로토콜
- 지분증명은 암호화폐가 블록을 검증하는 데 사용하는 합의 알고리즘
- 2011년에 처음 제안되었으며, 2012년 Peercoin이 최초
- 주요 장점은 에너지 효율성과 보안

Proof of Stake



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

<https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

합의 알고리즘(Consensus)-PoS

❖ 지분증명(PoS)

- 는 참여자의 코인 지분을 기준으로 블록을 생성
- 참여자의 코인 지분이 많을 수록 유리해 지는 방식
- 다음 블록의 생성자는 부분적으로 사용자가 보유하고있는 암호화폐의 수량 또는 어떤 경우에는 그 특성을 보유하고 있는 기간에 의해 무작위 시스템에 의해 결정
- 무작위 추출은 중앙 집중화를 예방할 수 있음
: 시스템의 부유한 개인이 항상 다음 블록을 만들고 지속적으로 부를 창출하면 결과적으로 시스템을 통제하게 됨

합의 알고리즘(Consensus)-PoS

- ❖ PoW보다 훨씬 적은 에너지를 사용하여 효율적
 - Bitcoin의 2주 전기 사용량 = 네덜란드 가정의 평균 전기 요금
→ 비 효과적이거나 지속 불가능 하게 될 수도
 - PoS는 훨씬 적은 전기 사용량을 필요로 하기 때문에 우수한 합의 프로토콜로 간주 될 수 있음
 - 시스템이 훨씬 효율적이기 때문에 네트워크를 유지하기 위해 마이너에게 인센티브를 부여하는 수단으로 너무 많은 새로운 코인을 발급해야 할 필요성이 적음
 - 이것은 특정 코인의 가격을 보다 안정하게 유지하는 데 도움
 - PoS는 비잔틴 결함 허용 문제를 해결하는데 특히 적합함
: 모든 유효성 검사가 네트워크에 의해 추적되고 ID(지갑주소)의 신원을 알고 있기 때문

합의 알고리즘(Consensus)-PoS

❖ 특징

- PoW의 단점을 극복하기 위한 알고리즘 중 하나이며 해시 파워가 필요하지 않아 경제적이다
- PoW에서 **51% 해시파워**를 가지는 비용 vs PoS에서 **전세계 자산의 51%** : PoS방식의 비용이 더 높음
- 중앙집권화가 더 어려워 분산화가 보장됨

❖ 문제점

- 참여한 노드들이 이자를 받으려고 코인을 묶어 두려할 경우 시중 코인의 유통량 감소로 이어질 수 있음
- 코인을 많이 보유한 사람이 너무 강한 권력을 가지게 됨

합의 알고리즘 - BFT 기반 PoS

❖ BFT algorithm

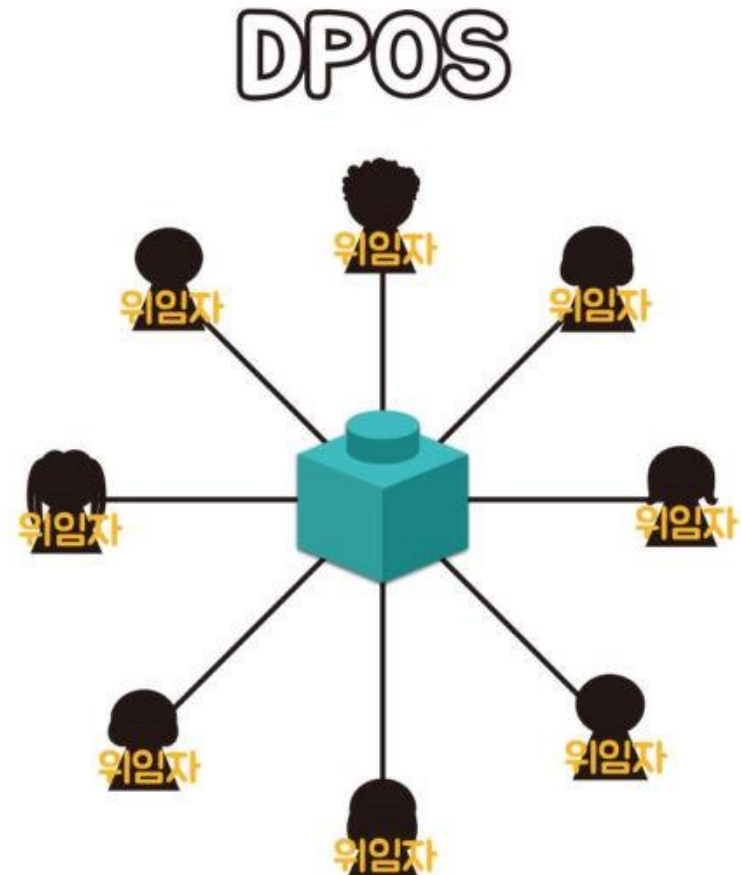
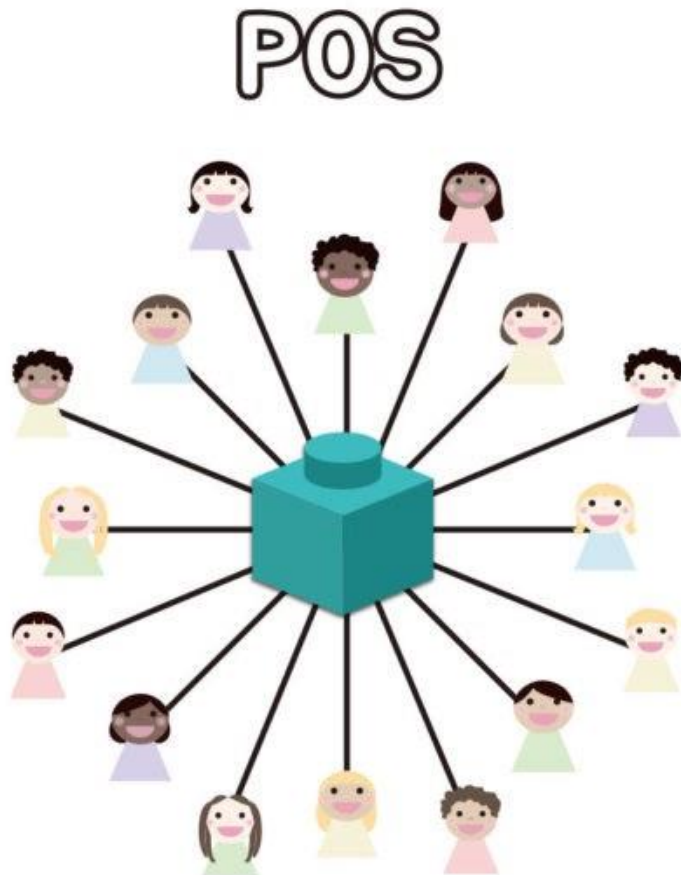
- 네트워크의 1/3보다 적은 노드가 적대적이라도 합의가 가능
- Chain기반이 아니므로 합의 및 검증이 매라운드마다 이루어짐
- BFT Consensus 알고리즘은 일관성있게 가용성을 유지하기 때문에 비동기 네트워크 모델로 관리 할 수 있음
- Tendermint, Ripple, Stellar 등이 해당 됨

합의 알고리즘 - DPoS

❖ 위임 지분 증명(DPoS, Delegated Proof of Stake)

- 특정 인원에게만 PoS를 할 수 있도록 권한을 위임하는 알고리즘
- 네트워크상 노드들의 투표 결과로 선출된 상위 노드에게 권한을 위임하여 일종의 대표자의 역할 수행
- 위임한 대표자와 수익을 배분

합의 알고리즘 - DPoS



<http://www.mobiinside.com/kr/2018/07/28/blockchainpepp-powposdpos/>

합의 알고리즘 - DPoS

❖ DPoS 코인 종류

- Ark, Lisk, Waves, Tezos, BOScoin, Steem, EOS, Rise 등

❖ DPoS 블록 대표자(생산자) 수 case

- EOS : 21
- Bitshares : 101
- Steemit : 21
- Lisk : 101
- Ark : 51

합의 알고리즘 정리

관리주체	관리자가 없음	여러조직	단일조직
네트워크 형태	퍼블릭(Public) 형	컨소시움(Consortium) 형	프라이빗(Private) 형
참여자	자유적	허가적(Permissioned)	
	불특정 사용자가 참여할 수 있기 때문에, 악의를 가진 사용자가 참여할 수 있음	참여자의 신원이 확인되고, 신뢰할 수 있음	
분산합의 알고리즘 (Consensus)	작업증명(Proof of work) 및 지분증명(Proof of stake) 알고리즘 (마이닝)	특정 노드(검증자)에 의한 검증 (분산합의 알고리즘)	
	<ul style="list-style-type: none"> ✓ 전력소비가 많음 ✓ 최종성이 없음 ✓ 51% 공격 문제 	<ul style="list-style-type: none"> ✓ 전력소비를 최소화 ✓ 최종성이 있음 ✓ 경량화 되어 있으며, 빠르게 처리됨 	
트랜잭션 처리시간	상대적으로 오래걸림 (비트코인:10분, 이더리움:10초)	빠르게 트랜잭션 처리 (수초에서 실시간)	
유즈 케이스	디지털 화폐	은행 송금, 증권 거래 등 비즈니스 네트워크에서 사용	
구현 예	비트코인(Bitcoin), 이더리움(Ethereum)	리플(Ripple), 하이퍼레저(Hyperledger)	

업무사용의 중요성 : 비즈니스 유스케이스에 따라 분산합의 알고리즘을 목적에 맞게 사용할 수 있음

모바일 앱 지갑을 이용한 비트코인 주고받기

- ❖ 모바일에서 Play 스토어 가서서 Mycelium 앱 설치
- ❖ 프라이빗 키 백업 하지 마시고(backup later) 수신 선택 하세요(주소는 Legacy로 선택). 주소를 클립보드에 복사 하셔서 제게 메일(jspark1@gmail.com)로 보내주세요.
- ❖ 유튜브 머니머니해도 건강 채널에 가서서 구독 좋아요, 하시면
- ❖ 그럼 제가 아주 적은(나중에?) 비트코인과 블록체인 비즈니스 밴드 가입 부탁 메일 보내 드립니다.
- ❖ 이 유튜브 채널을 통해 블록체인 인공지능 다이어트 당뇨 관리 해 드릴것입니다!

MUSELUM 화면

