

블록체인 기술과 응용 서비스

1. 블록체인 개요
2. 블록체인 응용과 사례
3. 블록체인 보안
4. 비트코인 블록체인의 구조와 동작원리
5. 이더리움 블록체인의 구조와 동작원리
6. 가상전자 거래소, 전자지갑, 채굴
7. 블록체인 이슈와 전망



블록체인 기술과 응용 서비스

1주차

블록체인 개요

1교시 : 블록체인의 탄생과 P2P 네트워크

2교시 : 블록체인 유형과 합의 알고리즘

3교시 : 블록체인 응용분야와 진화 및 생태계



대구사이버대학교
DAEGU CYBER UNIVERSITY

1교시: 블록체인의 탄생과 P2P 네트워크

〈학습목표〉

- 블록체인의 정의 및 탄생 배경에 대하여 설명할 수 있다.
- P2P 네트워크의 기본 개념에 대하여 설명할 수 있다.

〈주요 용어 (1)〉

- **공유원장(분산원장)**

중앙 관리자나 중앙 데이터 저장소가 없으며, 피투피(P2P) 망 내 모든 참여자(Peer)가 거래 장부를 서로 공유하여 감시 관리하기 때문에 장부 위조를 막는다. 분산원장 기술이 사용된 대표적인 예가 블록체인이다.

- **트랜잭션**

데이터통신 시스템에서 관리의 대상이 되는 기본적인 정보를 기록한 기본파일(master file)에 대해서 내용의 추가, 삭제 및 갱신을 가져오도록 하는 행위(거래)를 트랜잭션이라 한다.

- **노드**

블록체인은 중앙 집중형 서버에 거래 기록을 보관, 관리하지 않고 거래에 참여하는 개개인의 컴퓨터들이 모여 네트워크를 유지 및 관리한다. 이 개개인의 컴퓨터, 즉 참여자를 노드라고 한다.

- **서버**

컴퓨터 네트워크에서 다른 컴퓨터에 서비스를 제공하기 위한 컴퓨터 또는 소프트웨어를 가리키는 용어이다.

〈주요 용어 (2)〉

- 클라이언트

서버에서 보내 주는 정보 서비스를 받는 측 또는 요구하는 측의 컴퓨터 또는 소프트웨어이다.

- P2P

기존의 서버와 클라이언트 개념이나 공급자와 소비자 개념에서 벗어나 개인 컴퓨터끼리 직접 연결하고 검색함으로써 모든 참여자가 공급자인 동시에 수요자가 되는 형태이다.

- 퓨어

순수, 자신 외에 다른 것이 가미되지 않은 상태이다.

- Host

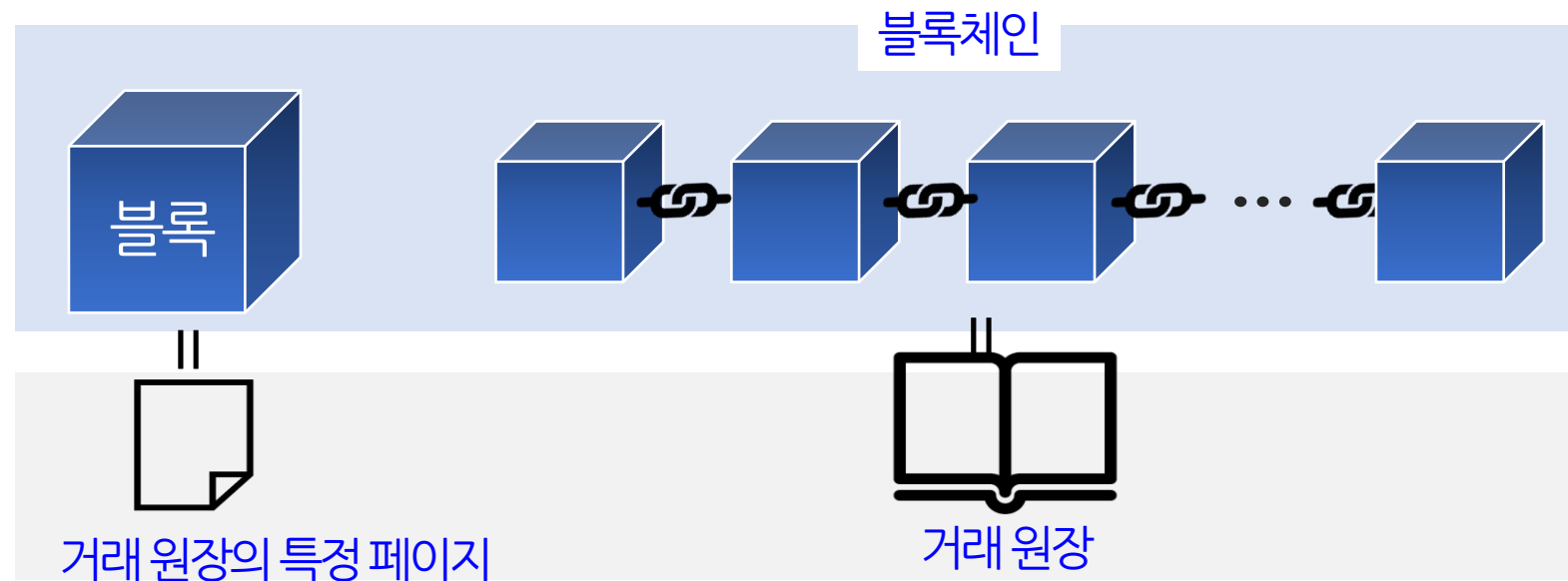
통신하는 시스템을 가리킨다. 인터넷 상에 연결된 개별적인 컴퓨터를 지칭하는 말이다.

블록체인-공유원장

- ❑ 비즈니스 네트워크에서 트랜잭션을 기록하고 유형 및 무형의 자산을 추적하는 프로세스를 효율화하는 **불변의 공유원장**

(IBM, <https://www.ibm.com/kr-ko/topics/what-is-blockchain>)

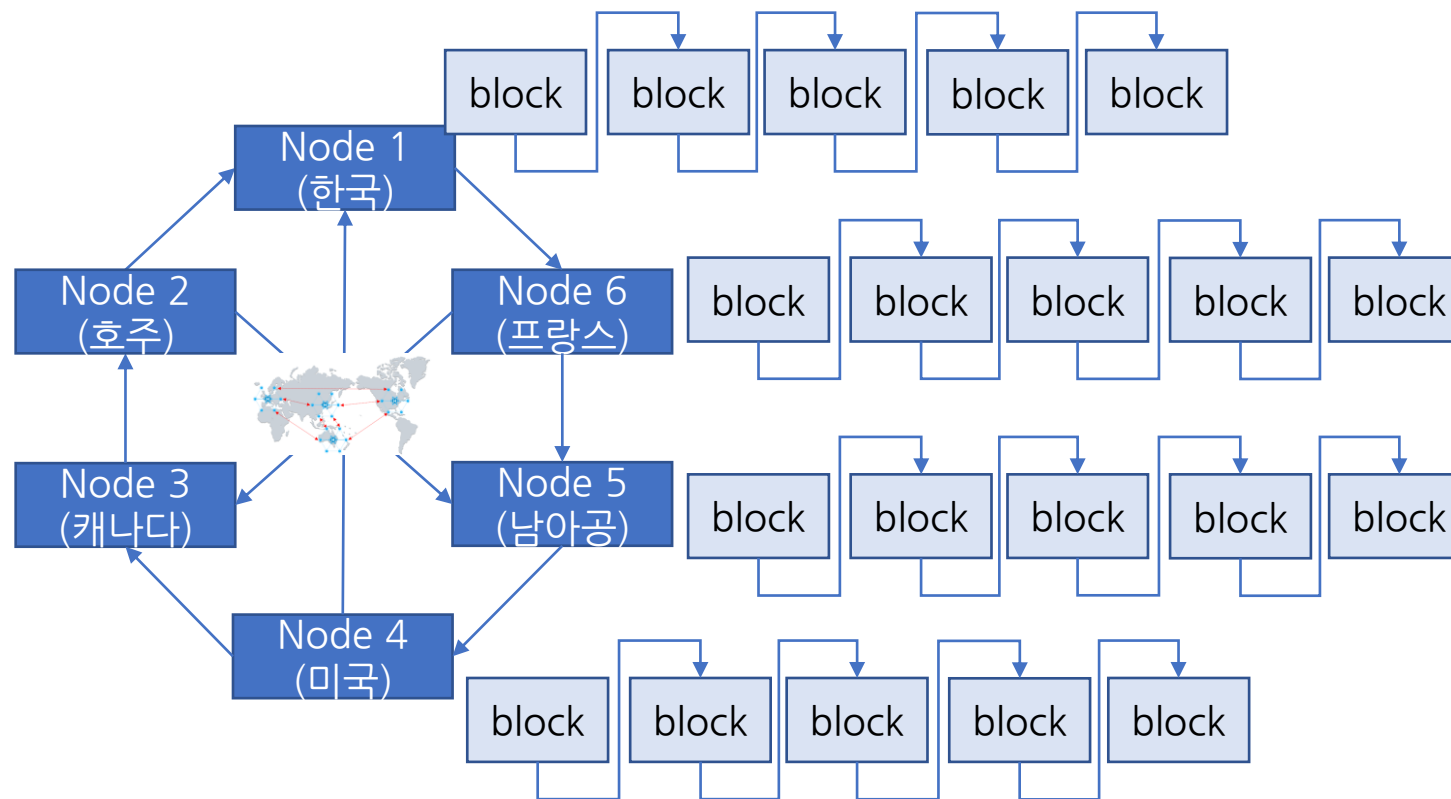
- ❑ 블록체인(blockchain)과 전통적인 원장



블록체인-분산컴퓨팅

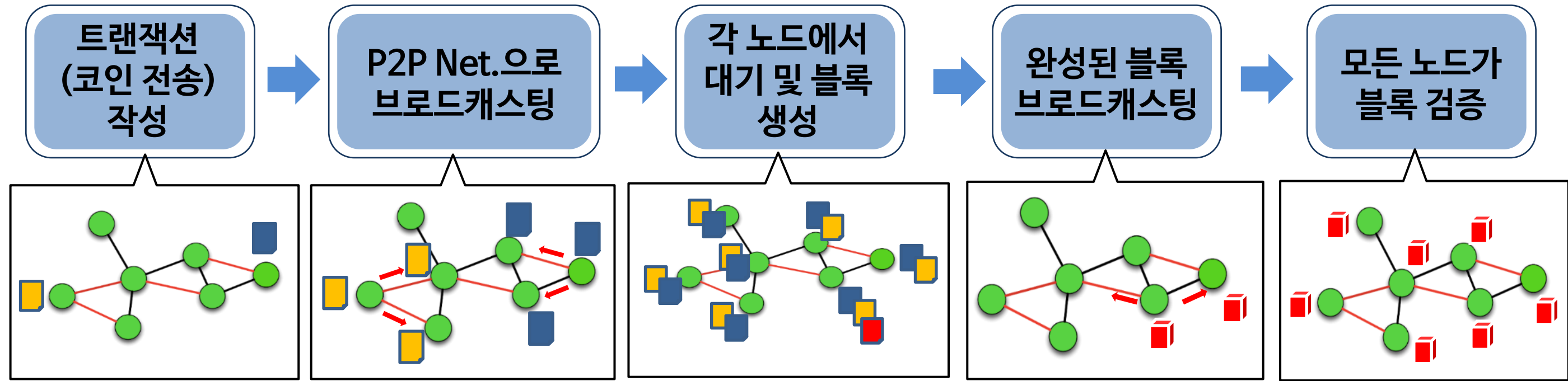
- ❑ 블록들이 P2P 방식으로 생성된 체인 형태의 분산 환경에 저장되며, 임의로 수정할 수 없고 누구나 변경 결과를 열람할 수 있는 **분산컴퓨팅 기반의 원장 관리 기술**(위키피디아)

❑ P2P 방식의 블록 동기화





블록체인 동작원리



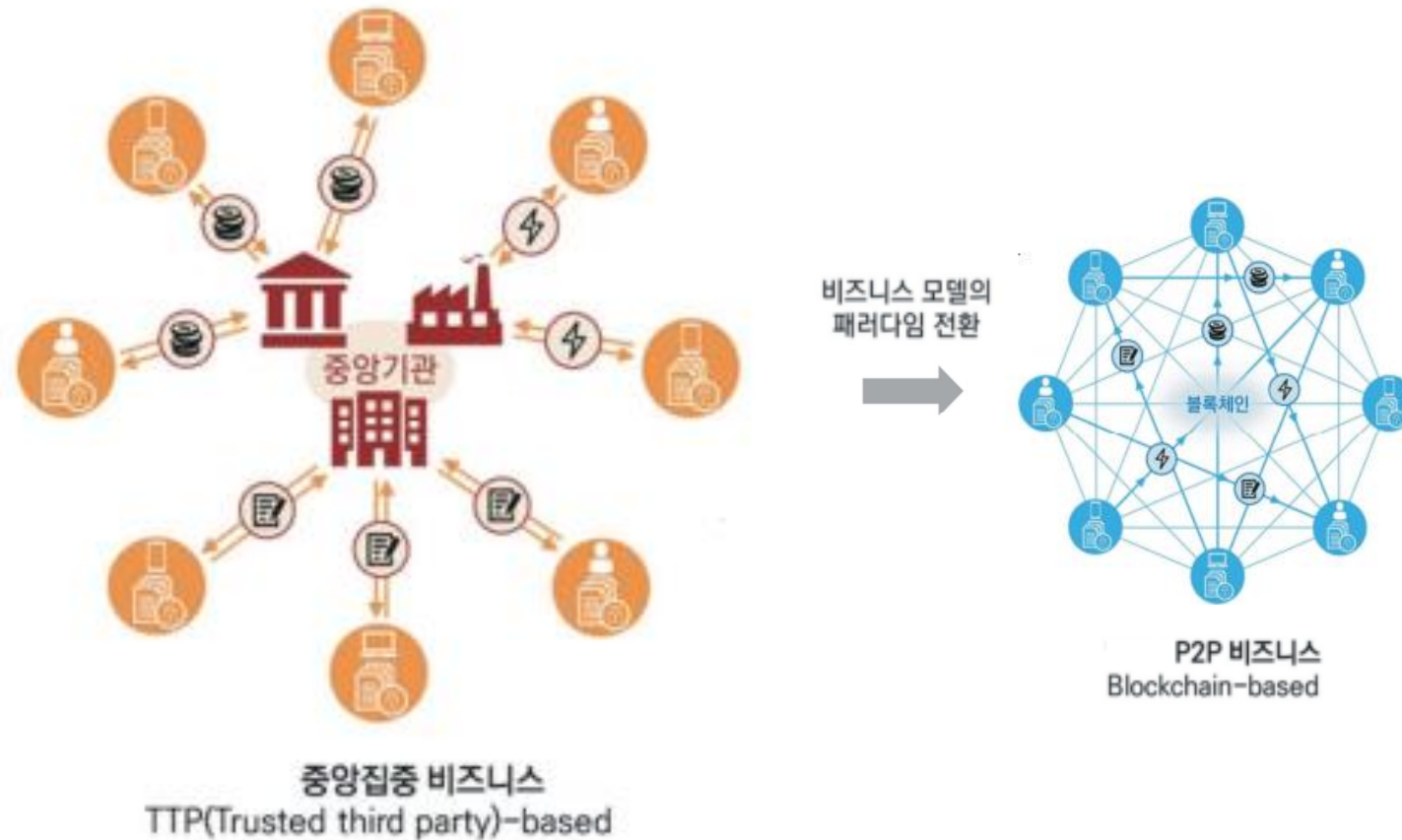
* 출처 : Hdac Blockchain Platform 교육 자료, 2019.10

블록체인의 탄생

- ❑ 2007-2008년 세계 금융 위기
- ❑ 사토시 나가모토가 기존 화폐의 위험성 인지
- ❑ 2008.10.31, “Bitcoin: A Peer-to-peer Electronic Cash System” 논문 발표
(<https://bitcoin.org/bitcoin.pdf>)
- ❑ 2009.1.3, 제너시스 블록 채굴
- ❑ 2010.5.22, 라스즐로가 10,000 BTC(당시 시세로 약 41달러)로 피자 2판 구매 → 최초의 실물 구매

중앙집중 비즈니스

- 중앙기관 집중 방식의 금융, 전자상거래 등은 중앙기관의 문제 발생 시 모든 이용자가 피해를 입는 구조로 **안전성 및 보안성에 한계**가 있음



블록체인 기반의 P2P 비즈니스

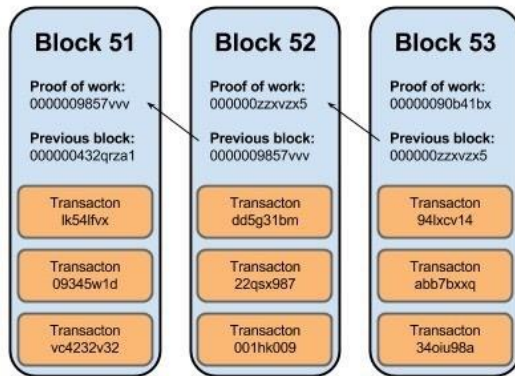
- 참여자간의 거래 기록이 공유/동기화되며, 보안에 안전한 원장 유지





블록체인 장점

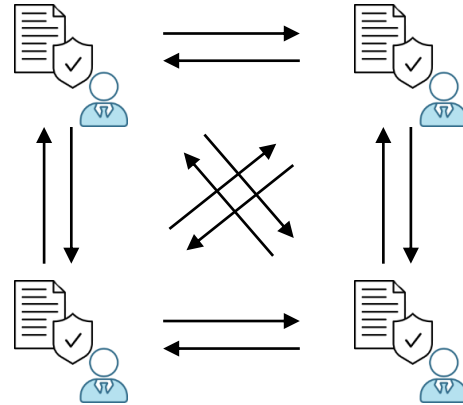
불가역성



체인 구조로 이전과
이후 데이터 모두 연결

위 · 변조 불가능

단일 장애점 방지



중앙시스템 관리가
아닌, 동일 데이터 공유

단일 장애 발생해도
정상 운영

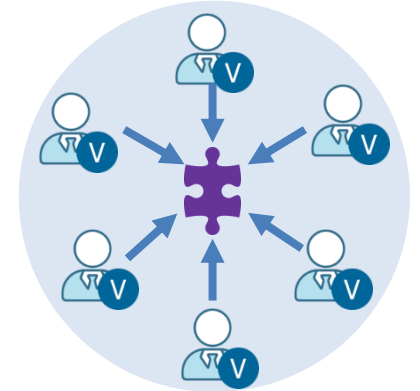
투명한 정보전달



모든 거래의 발생 시점부터
경로 추적 가능

블록체인의 모든 데이터
투명 관리

상호 감시 비즈니스



구성원들은 새로운
데이터를 상호 감시

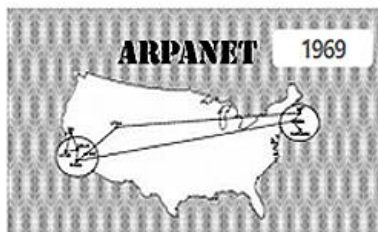
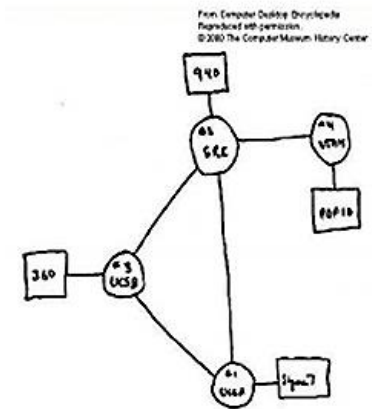
정당성 판단 및 비정상적
행위 차단

* 출처 : 블록체인 서비스 육성을 위한 제언, 주용완, KISA

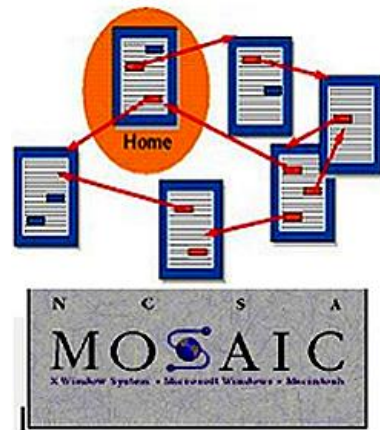


인터넷 역사 50년

분산 컴퓨터 연결성
Messaging, 복제



분산 데이터 연결성
Connectivity, 구조화



분산 컴퓨터 존재성
Existence, 복제



P2P 전송 프로토콜
▶ 분산 Hash 테이블
▶ Tracker, Peer(seeder)



데이터 신뢰성
Trust



블록체인 프로토콜
▶ 분산합의, 암호학적 검증
▶ Miner(Node), User

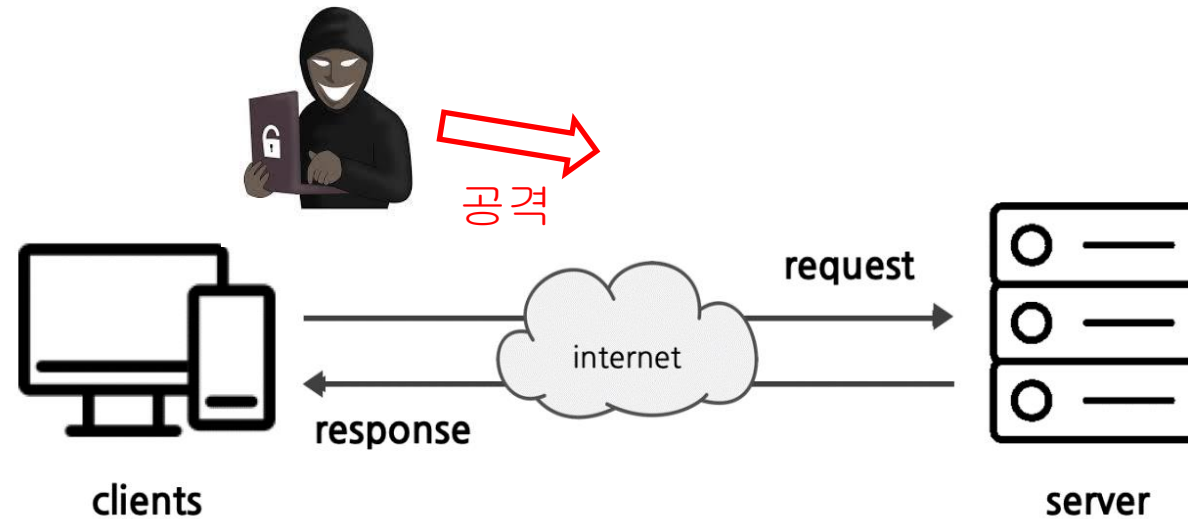


* 내용 출처: KT 이동훈, 2017

서버·클라이언트 네트워크

- 데이터 처리 및 관리하는 서버와 서버의 데이터를 이용하는 클라이언트로 구성
 - 서버가 집중 관리하므로 시스템의 설계, 기능 추가, 업데이트가 쉬움
 - 고사양 서버와 높은 대역폭 요구
 - 서버 장애가 발생할 경우 서비스 전체 중단

- 디도스 및 랜섬웨어와 같은 사이버 공격에 취약



출처: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQP9atDnvVY-FpZKMG9ZjPzjc4nYW-2i7xmVw&usqp=CA>



P2P 네트워크

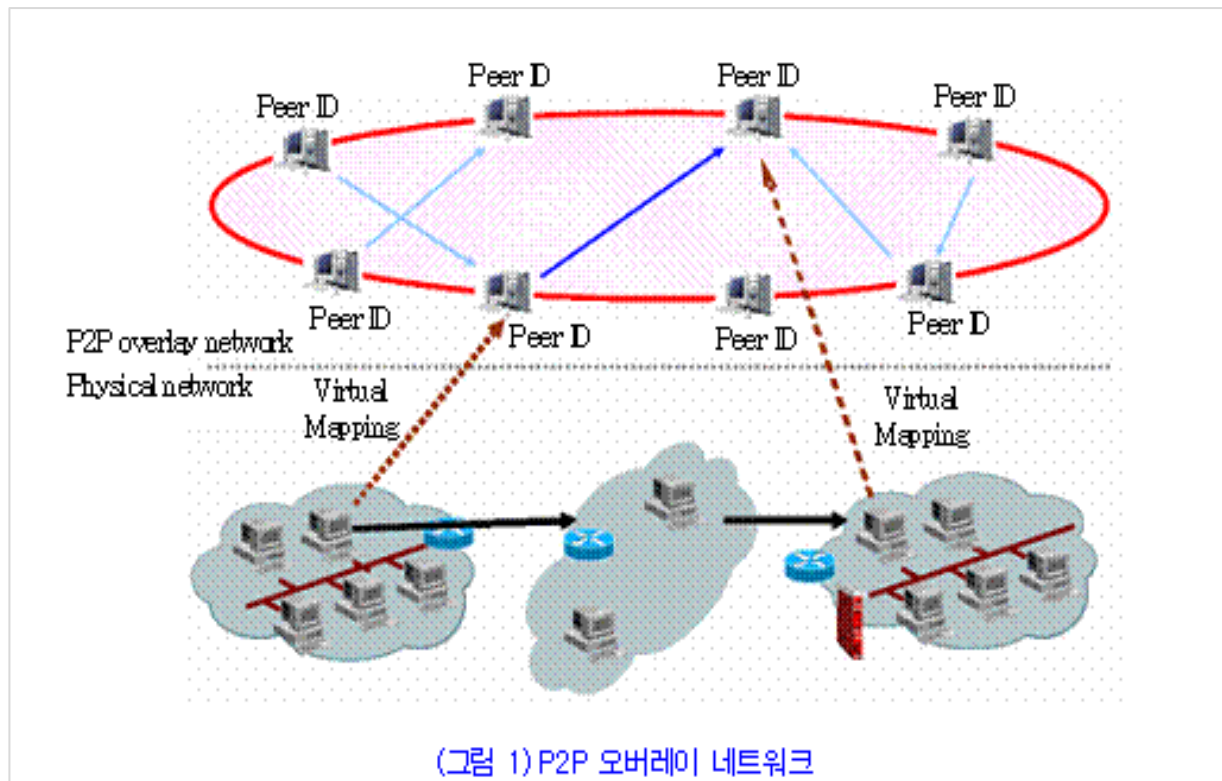
- 노드들이 동등한 입장에서 통신 → 각 노드는 서버이면서 클라이언트
 - 인스턴트 메시징: MSN 메신저, ICQ, JPPP
 - 파일 공유: Gnutella, Napster, 소리바다, 비트토렌트
 - 분산 컴퓨팅: SETI, KOREA@Home

* 출처: P2P 관련 국제 표준화 동향 (itfind.or.kr)



P2P 네트워크

- 인터넷에서 P2P 서비스에 등록된 노드들 간의 **P2P 오버레이 네트워크** 생성

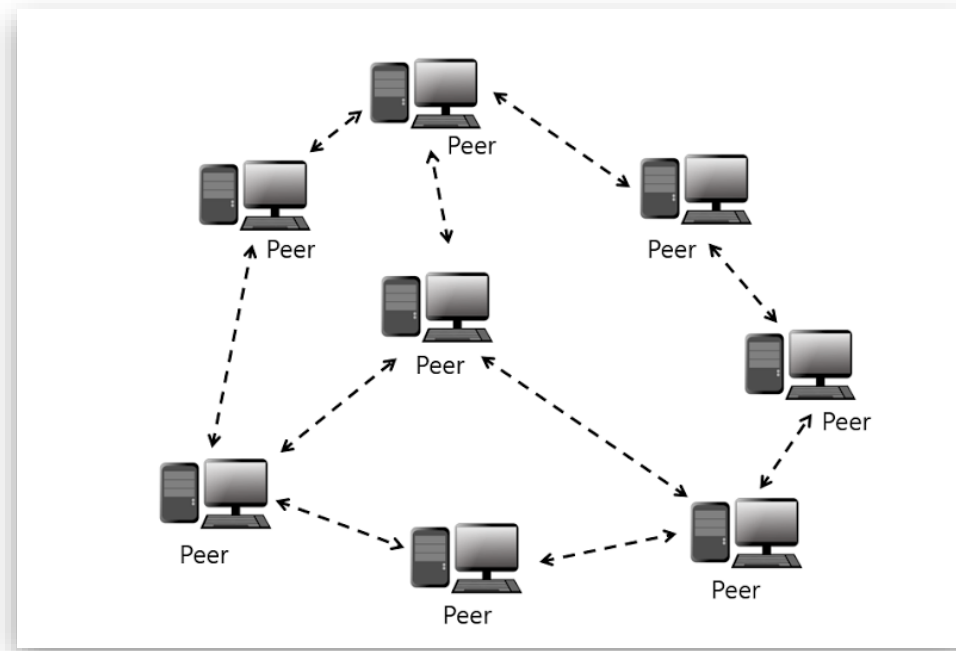


* 출처: P2P 관련 국제 표준화 동향 (itfind.or.kr)

퓨어 P2P 네트워크

❑ 모든 노드가 동등하게 연결

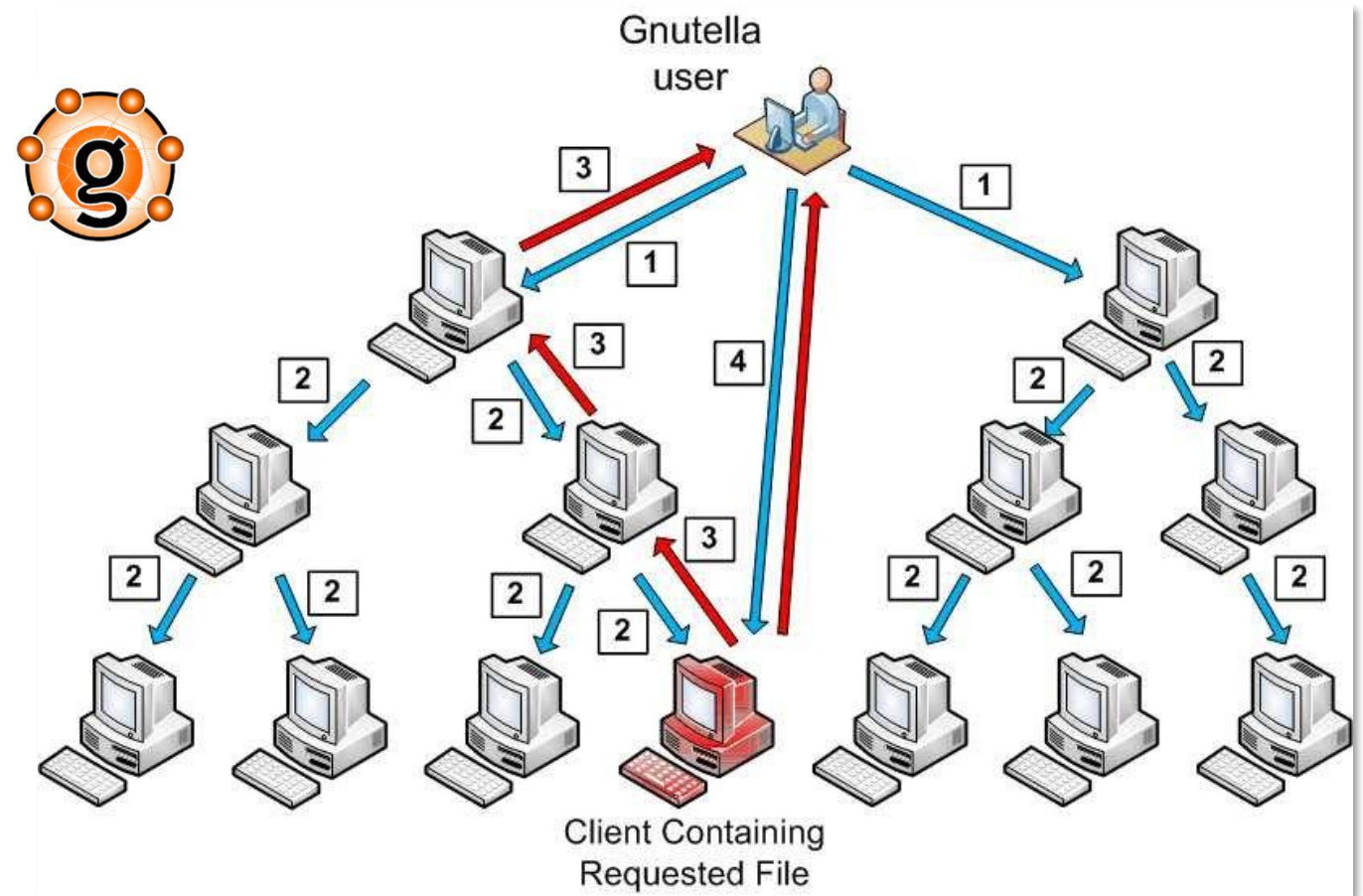
- 새로운 노드 추가(확장성)은 높으나 시스템 전반의 설계와 관리가 어려움
- 다른 노드들을 탐색할 수 있는 알고리즘 요구





퓨어 P2P - 그누텔라

- 서버 없이 파일 공유를 위한 분산 S/W 프로젝트
 - Host 정보 수집과 파일 공유를 위해 HTTP 사용
 - 이웃 노드에게 **브로드캐스트로 메시지 전파**



* 출처: https://www.researchgate.net/figure/How-to-Download-a-File-Using-the-Gnutella-Network_fig3_220080811



〈1교시〉 학습 정리

- 블록체인은 분산컴퓨팅 기반 불변의 공유원장 기술이다.
- 블록체인의 특징은 거래 내용의 불가역성, 투명한 관리와 상호 감시이며, 중앙시스템에 의한 관리가 아니므로 단일 장애에 의한 서비스 중단을 막을 수 있다.



〈1교시〉 학습 평가

1. 블록체인에 대한 설명 중 틀린 것은?

- 1) 사토시 나카모토가 기존 화폐의 위험성을 줄이기 위하여 비트코인 블록체인을 개발하였다.
- 2) 불가역성, 단일 장애점 방지 그리고 투명한 정보전달은 블록체인의 단점이다.
- 3) 블록체인은 거래원장 그리고 블록은 거래원장의 특정 페이지로 볼 수 있으며, 분산컴퓨팅 기반 불변의 공유원장 기술로 정의할 수 있다.
- 4) 2009년 1월 3일 비트코인의 제너시스 블록이 채굴되었다.

답) 2

해설) 불가역성, 단일 장애점 방지 그리고 투명한 정보전달은 블록체인의 장점이다.

2. P2P에 대한 설명 중 틀린 것은?

- 1) 블록체인은 인터넷과 같은 가상의 네트워크 위에 물리적인 P2P 오버레이 네트워크로 구성된다.
- 2) 스타크래프트와 같은 게임은 높은 성능을 위해 사용자 간에 P2P통신을 사용하며, 방을 만들고 검색, 조인하기 위해서 인덱스 서버를 활용한다.
- 3) 하이브리드 P2P 네트워크는 노드 정보들이 인덱스 서버에 기록되며, 데이터 교환은 P2P 통신으로 이루어진다.
- 4) 퓨어 P2P는 모든 노드가 동등하게 연결되는 네트워크로 시스템 전반의 설계와 관리가 어렵다.

답) 1

해설) 블록체인은 인터넷과 같은 물리적인 네트워크 위에 가상의 P2P 오버레이 네트워크로 구성된다.

2교시: 블록체인 유형과 합의 알고리즘

〈학습목표〉

- 블록체인의 유형과 비잔티움 장군 문제에 대하여 설명할 수 있다.
- 블록체인의 합의 알고리즘(PoW, PoS, DPoS)에 대하여 설명할 수 있다.

〈주요 용어 (1)〉

- **인덱스**

파일이나 레코드 같은 대량의 데이터 속의 특정한 요소를 인용하기 위한 순서 리스트로, 요소를 식별하고, 로케이트하며, 탐색 혹은 검색하기 위한 키세트와 어드레스를 나타낸 것

- **피어**

P2P 네트워크에 참여하는 다양한 형태의 노드로서 클라이언트와 서버의 역할을 동시에 수행한다.

- **시더(seeder)와 리처(leecher)**

파일을 조각으로 나누어 교환하는 비트토렌트 P2P에서 시더는 공유파일의 완전체이며, 리처는 일부 조각만 소유하는 피어노드를 의미한다.

〈주요 용어 (2)〉

- **컨소시움**

공동 목적을 위해 조직된 협회나 조합이다.

- **항법장치**

항공기나 함정의 위치 정보를 제공하는 장치이다.

- **알고리즘**

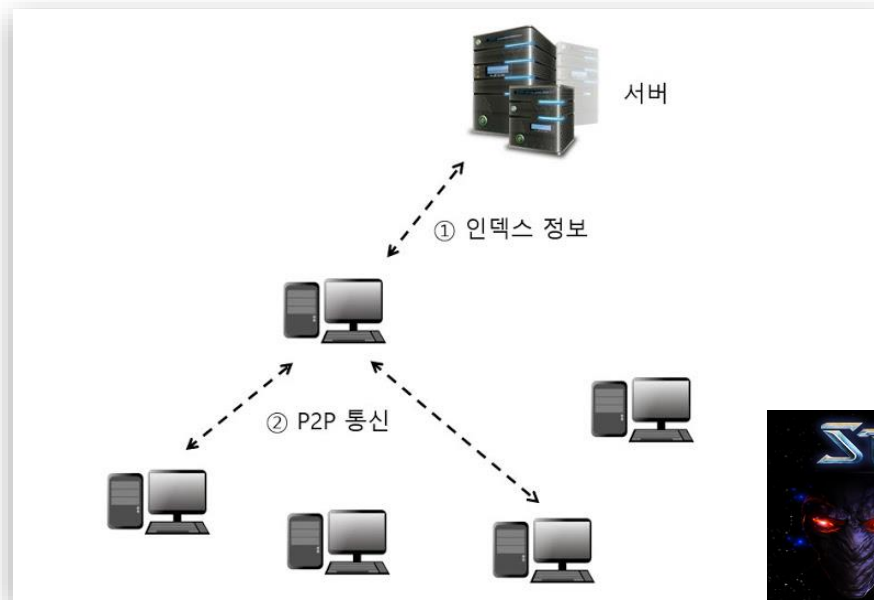
주어진 문제를 논리적으로 해결하기 위해 필요한 절차, 방법, 명령어들을 모아놓은 것이다.

- **스테이킹**

자신이 가지고 있는 암호화폐를 블록체인 네트워크에 예치한 뒤, 해당 플랫폼의 운영 및 검증에 참여하고 이에 대한 보상으로 암호화폐를 받는 것이다.

하이브리드 P2P 네트워크

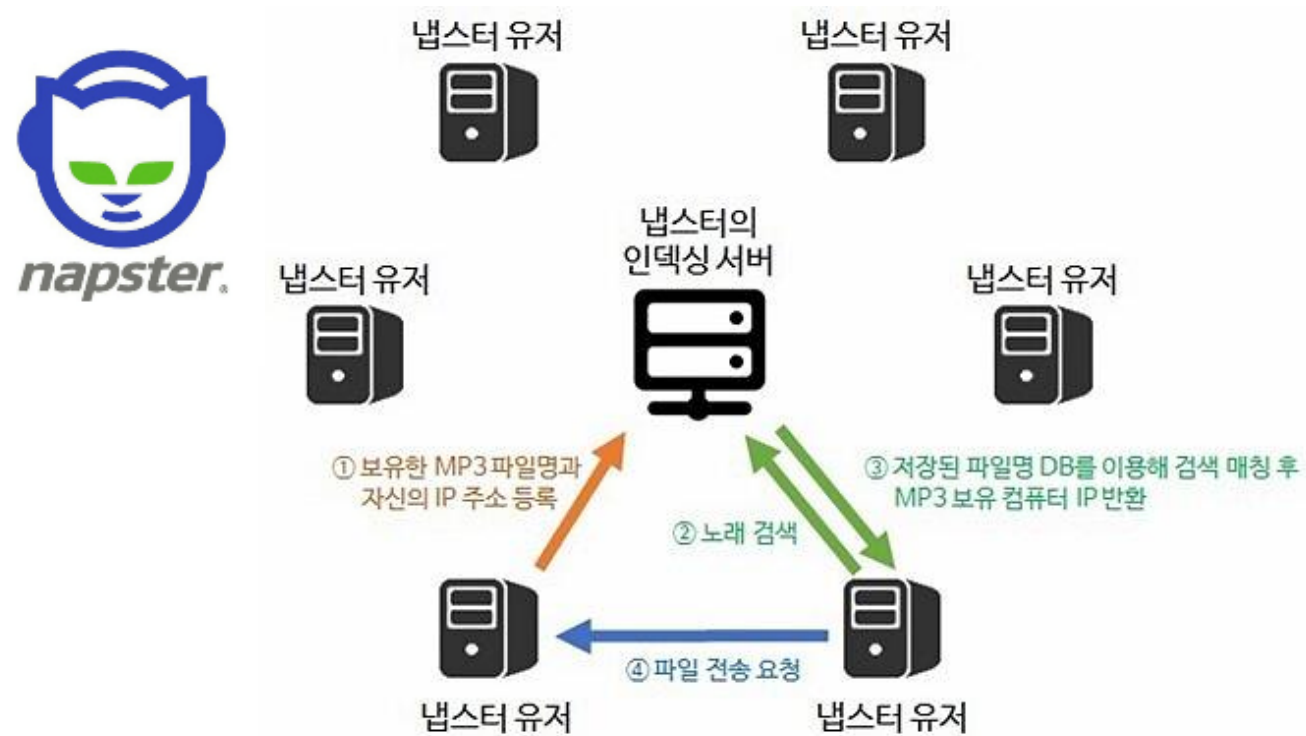
- ❑ 노드 정보들이 **인덱스 서버**에 기록되며, **데이터 교환**은 P2P 통신
 - 서버/클라이언트 구조처럼 설계와 관리가 용이하지만 **확장성 떨어짐**
- ❑ 스타크래프트와 같은 게임들이 하이브리드 P2P방식 사용
 - 높은 성능을 위해 사용자 간에 P2P통신 사용
 - 방을 만들고 검색, 조인하기 위해서 인덱스 서버 활용





하이브리드 P2P - 냅스터

- 손 패닝이 만든 온라인 음악 파일 공유 서비스
- 1999년 6월부터 2001년 7월까지 운영

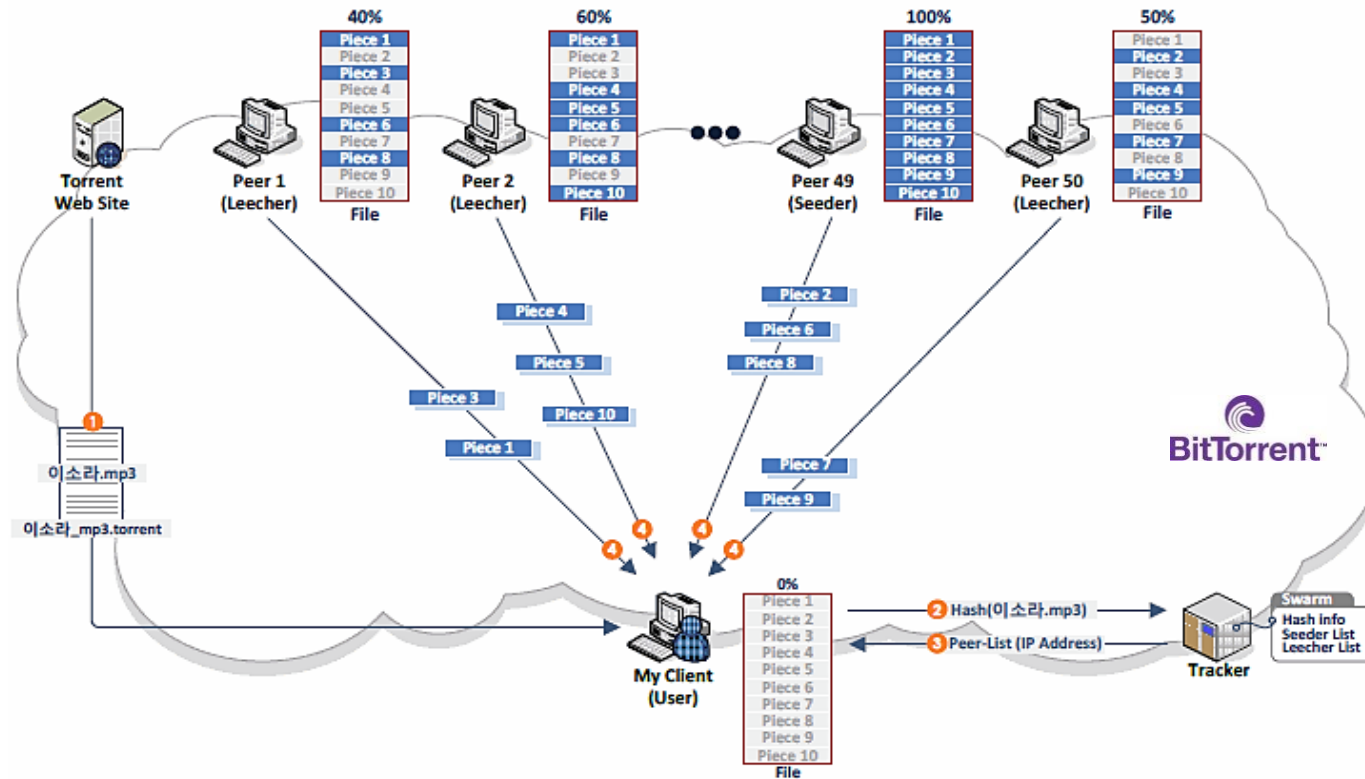


* 출처: <https://www.inven.co.kr/webzine/news/?news=164068>



하이브리드 P2P - 비트토렌트

- 2001년 7월에 발표된 P2P 방식의 파일 공유 S/W
 - 피어들의 정보를 관리하는 **Tracker**의 URL 정보는 .torrent 파일에 있음
 - 파일을 조각으로 나누어 교환** → 시더는 공유 파일의 완전체, 리처는 일부 조각만 소유



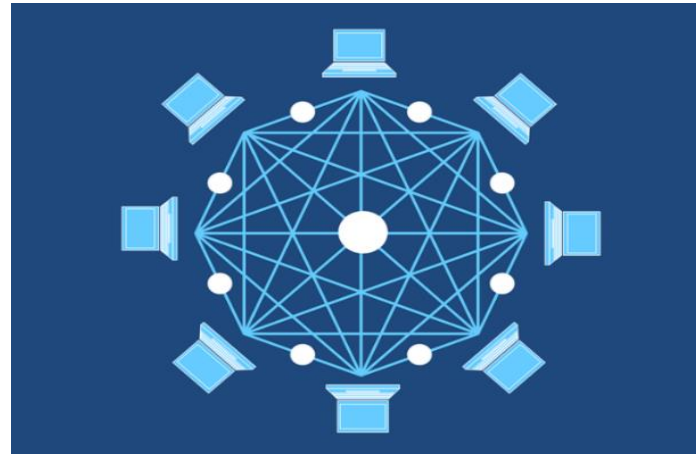
* 출처: <https://www.netmanias.com/ko/?m=view&id=techdocs&no=10644>

블록체인 유형

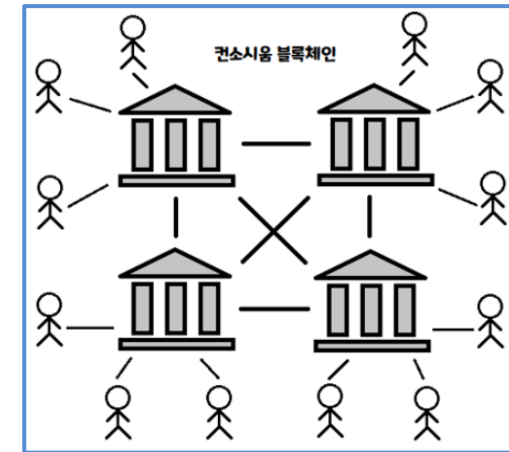
- ❑ 퍼블릭 블록체인: 누구나 거래를 생성하고 블록을 검증하며, 거래내역을 확인할 수 있는 개방형 → 퓨어 P2P
- ❑ 프라이빗 블록체인: 허가된 조직이나 개인만 참여할 수 있는 폐쇄형 → 서버가 존재하는 하이브리드 P2P
- ❑ 컨소시움 블록체인: 같은 목적을 갖는 여러 기관이 컨소시움을 구성하여 공정성과 확장성 보완



퍼블릭 블록체인



프라이빗 블록체인



컨소시움 블록체인



퍼블릭 블록체인

- 블록에 저장된 데이터의 **위조 및 변조가 거의 불가능**
- **암호화폐를 인센티브로 지급**하여 참여의 동기 부여 및 네트워크 유지
- 비트코인, 이더리움, 비트코인캐시, 이오스, 스텔라루멘, 스템, 모네로, ...

비트코인



이더리움



비트코인 캐시



이더리움



스텔라루멘



스팀



모네로



1. 거래 생성
(송금/스마트 계약)



누구나 거래를 생성할 수 있음



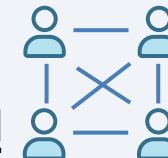
2. 블록에 데이터 저장



3. 블록 검증 및 암호화



4. 분산된 네트워크에
보상 분배 및 거래 승인



블록 검증자는 누구나 될 수 있음
거래 내용 확인은 모두가 가능



5. 거래 완료



* 출처: <https://velog.io/@chb1828/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%9D%98-%EC%9C%A0%ED%98%95%EB%93%A4>



프라이빗 블록체인

- 블록체인 개발자의 규칙에 따라 **허가 받은 노드만 거래 생성, 열람 및 검증자**가 될 수 있음
- 처리 속도가 빠르나 중앙결정화 되어 **공정성과 투명성**이 떨어질 수 있음
- 암호화폐 발행이 필수이지 않으며, 참여자들이 컴퓨터 운영 비용을 부담
- 하이퍼레저 패브릭, R3코다, 삼성 SDS의 넥스레저, 국제 송금을 위한 리플, ...

1. 거래 생성
(송금/스마트 계약)



허가 받은 사람만이
거래를 생성할 수 있음

2. 블록에 데이터 저장



3. 블록 검증 및 암호화



4. 분산된 네트워크에
보상 분배 및 거래 승인



허가를 받아야만 거래 내용을
확인할 수 있음

허가를 받아야만
블록 검증자가 될 수 있음

5. 거래 완료



컨소시엄 블록체인

□ 중간 형태인 하이브리드 블록체인

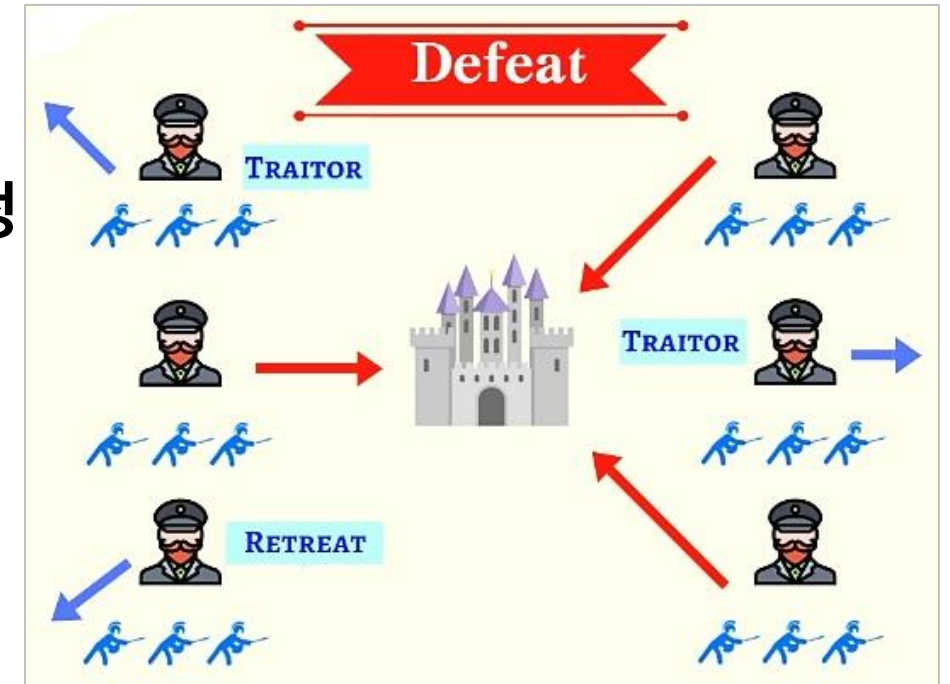
- 선별된 노드들만 합의 과정에 참여, 다른 노드들은 거래를 생성하거나 확인
- 16개 은행과 금융결제원, 금융보안원이 구축한 블록체인 기반의 BankSign
- 블록체인 기반 식품 추적 네트워크인 IBM 푸드 트러스트 등이 있음

블록체인 유형	퍼블릭	<u>프라이빗</u>	컨소시엄
허가가 필요한가?	X	O	O
누가 읽을 수 있나?	누구나	초대된 사용자만	경우에 따라 다름
누가 쓸 수 있나?	누구나	승인된 참여자만	승인된 참여자만
소유자	아무도 아님	단일 주체	복수 주체
참여자를 알 수 있나?	<u>아니오</u>	네	네
트랜잭션 속도	느림	빠름	빠름



비잔티움 장군 문제

- 분산컴퓨팅 시스템의 **신뢰성 문제**에 대한 논리적 딜레마, “The Byzantine Generals Problem, 1982”에서 처음 언급
- 기본 전제
 - 여러 부대가 성을 둘러싸고 있으며 각 장군들은 합의를 통해 공격 결정
 - 장군 중 한 명이 공격이나 후퇴를 결정하여 다른 장군들에게 전달
 - 메시지를 받은 장군은 나머지 장군들에게 전달
 - 일정 시간 후 각 장군은 자신이 받은 메시지를 종합하여 명령 이행
- 합의를 방해하는 요소 → **비잔티움 장군 문제의 딜레마**
 - 메시지 전달의 실패 확률이 있음
 - 배신자가 존재할 수 있음



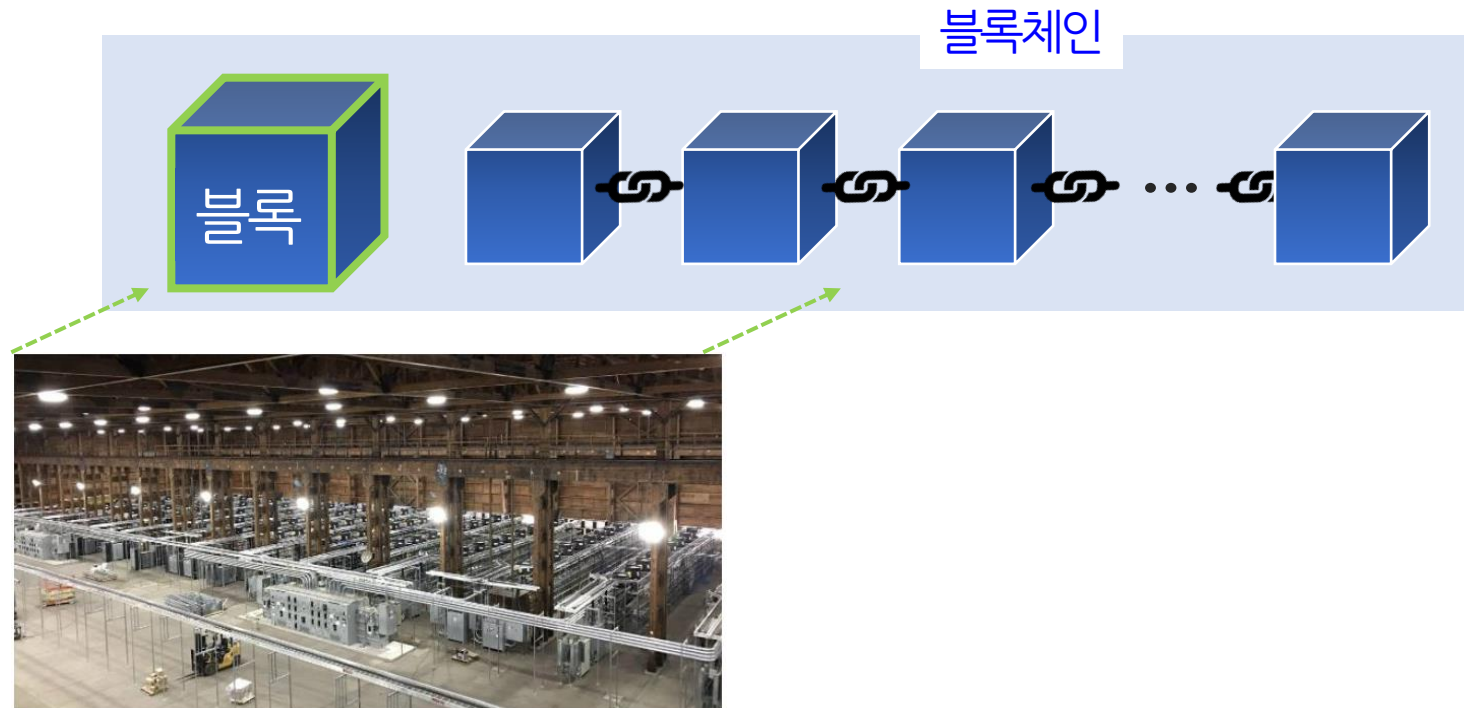
* 출처: <https://blockchain-baam.tistory.com/26>

비잔티움 장애허용

- ❑ BFT(Bizantine Fault Tolerance)은 비잔티움 장군문제에서 파생된 장애허용 연구의 한 분야
- ❑ 비트코인 이전의 BFT: 장군 중에 잘못된 메시지를 보내는 경우에도 전체 시스템이 돌아가도록 함
 - 당시 학자들은 BFT의 기본 전제가 최소 3분의 2 참여자가 정상 작동하여야 함을 규명함
 - 항법장치 분야에 처음 적용 → 항법장치 센서 3 개 중 2 개가 정상 작동한다면 하나의 신호를 무시해도 승객들은 무사히 목적지에 도착
- ❑ 사토시는 항공기 분야 해결책과 다르게 참여자 모두가 최신의 원장을 동일하게 보유하도록 수학적으로 보장함
 - BFT 시스템 구축에 다양한 방식 → 블록체인은 합의 알고리즘 도입

합의 알고리즘

- 참여자들의 통일된 의사결정을 위해 사용하는 알고리즘이며, 합의를 통해 검증된 블록이 체인에 연결
- 대표적인 합의 알고리즘
 - 작업증명(PoW, Proof of Work)
 - 지분증명(PoS, Proof of Stake)
 - 위임지분증명(DPoS, Delegated Proof of Stake), ...



Unlimited Bitcoin mining pool [출처: <https://news.bitcoin.com>]

작업증명(PoW, Proof of Work)

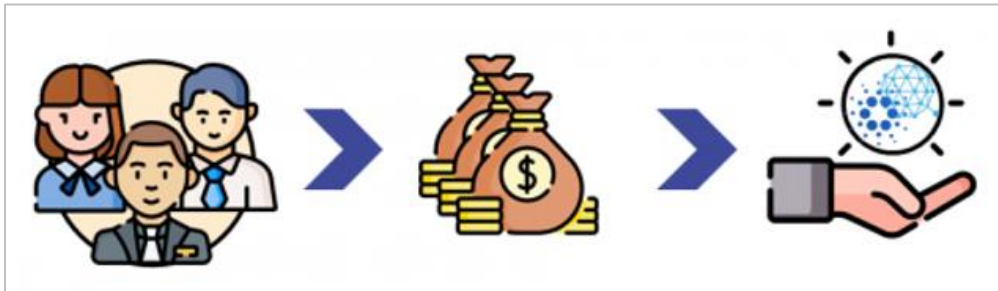
- ❑ 복잡한 문제(예, 해시함수)를 먼저 해결한 노드에 블록의 생성 권한 부여
 - 증명 방식: 하나씩 대입해야 풀 수 있는 문제의 답을 찾음
 - 채굴 보상: 암호화폐
 - 비트코인, 이더리움1.0 등에서 사용
 - ASIC, GPU 사용 및 높은 전력소모



First Solve, FirstServed!

지분증명(PoS, Proof of Stake)

- 네트워크 상에 일정량의 코인을 자신의 지분으로 **스테이킹**
 - 스테이킹한 노드들 중에 다음 블록의 **검증자 노드** 선택
 - 검증자 노드에게 블록에 있는 트랜잭션들의 수수료 지급
 - **에이다, 이더리움2.0** 등에서 사용
 - **친환경**: 유지비용 최소화(PC 1대 + 인터넷이 전부)



With great power comes great responsibility

가상 화폐별 전력 소모량 (2021.6 기준)

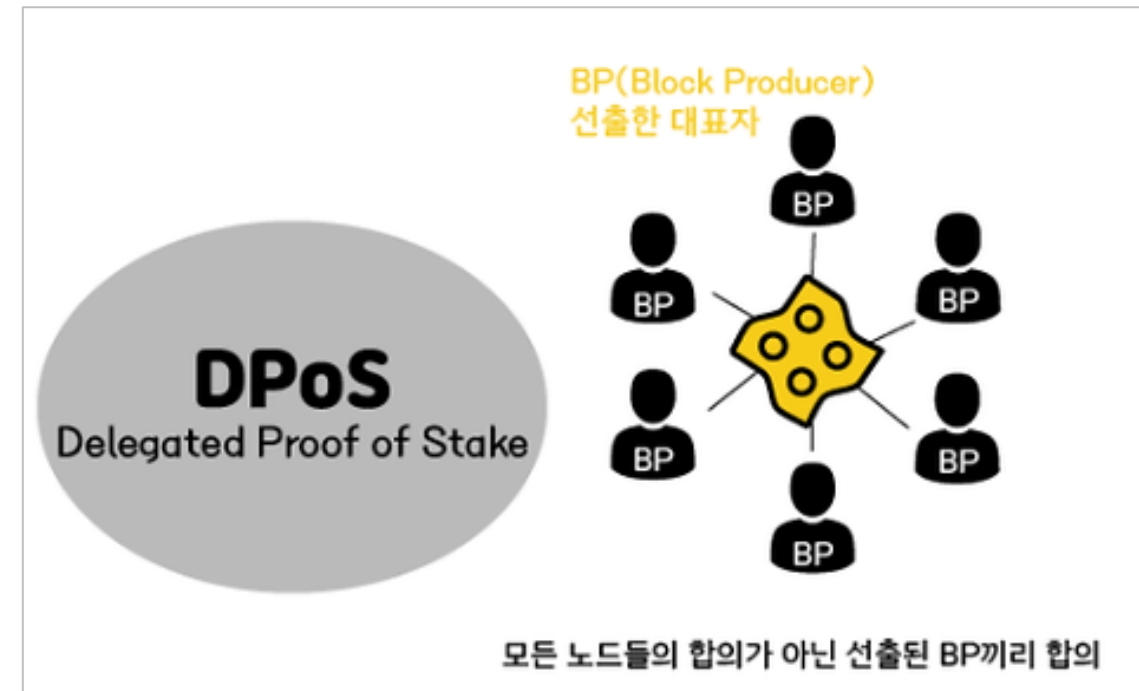
가상 화폐	블록체인 유지 방식	비트코인 대비 전력 소비량(%)
1위 비트코인	작업증명	-
2위 이더리움	작업증명	8.849%
4위 비트코인캐시	작업증명	2.681%
5위 카르다노(에이다)	지분증명	0.077%
6위 XRP(리플)	지분증명	0.001%



위임된 지분증명 (DPoS)

- Delegated Proof of Stake → **토큰 민주주의**

- 기존 PoS 방식에 **투표가 결합된 방식**
- 루나, 이오스 등에서 사용**
- 투표로 뽑은 **대표 노드에게 증명 위임**
→ 대표 노드는 수익 배분



*출처: <https://m.blog.naver.com/bodoblock00/221657805838>

암호화폐 별 합의 알고리즘

구분	PoW	PoS	DPoS
채굴 방법	복잡한 수학 문제 연산	지갑에 예치	투표로 뽑은 대표자에게 증명 위임
보상 기준	작업량	보유 지분에 비례	대표자 수익 배분
장점	보안성	친환경	빠른 처리 속도
단점	막대한 전기 소모	코인 쓸림 현상	네트워크 공격 취약
주요 코인	 비트코인(BTC)	 에이다(ADA)	 트론(TRX)
	 이더리움(ETH)	 알고랜드(ALGO)	 이오스(EOS)
	 라이트코인(LTC)	 테조스(XTZ)	 루나(LUNA)
	 모네로(XMR)	 셀로(CELO)	 리스크(LSK)



〈2교시〉 학습 정리

- 블록체인의 유형은 퍼블릭, 프라이빗 그리고 컨소시엄 블록체인으로 구분된다.
- 비잔티움 장군 문제는 분산컴퓨팅 시스템의 신뢰성 문제에 대한 논리적 딜레마이다.
- 블록체인의 대표적인 합의 알고리즘에는 PoW, PoS, DPoS가 있으며, 합의를 통해 검증된 블록이 체인에 연결된다.



〈2교시〉 학습 평가

1. 블록체인 유형에 대한 설명 중 틀린 것은?

- 1) 퍼블릭 블록체인은 누구나 거래를 생성하고 블록을 검증하며, 거래내역을 확인할 수 있는 개방형으로 퓨어 P2P를 주로 이용한다.
- 2) 프라이빗 블록체인은 허가된 조직이나 개인만 참여할 수 있는 폐쇄형이며, 서버가 존재하는 하이브리드 P2P를 주로 이용한다.
- 3) 비트코인, 이더리움, 비트코인캐시, 이오스는 퍼블릭 블록체인에 해당한다.
- 4) 16개 은행과 금융결제원 등이 구축한 BankSign과 IBM 푸드 트러스트는 프라이빗 블록체인에 해당한다.

답) 4

해설) 16개 은행과 금융결제원 등이 구축한 BankSign과 IBM 푸드 트러스트는 컨소시엄 블록체인에 해당한다.

2. 합의 알고리즘에 대한 설명 중 틀린 것은?

- 1) 비트코인, 이더리움 1.0은 높은 전력이 소모되는 PoW 방식을 사용한다.
- 2) 이더리움 2.0의 작업증명 방식에서는 스테이킹한 노드들 중에서 다음 블록의 검증자 노드가 선택된다.
- 3) 루나, 이오스 등에서 사용되는 DPoS는 기존 PoS 방식에 투표가 결합된 방식이며, 투표로 뽑은 대표 노드에게 증명을 위임한다.
- 4) 합의 알고리즘은 참여자들의 통일된 의사결정을 위해 사용하는 알고리즘이며, 합의를 통해 검증된 블록이 체인에 연결된다.

답) 2

해설) 이더리움 2.0의 지분증명 방식에서는 스테이킹한 노드들 중에서 다음 블록의 검증자 노드가 선택된다.

3교시: 블록체인 응용분야와 진화 및 생태계

〈학습목표〉

- 블록체인 응용분야와 진화에 대하여 설명할 수 있다.
- 블록체인의 생태계에 대하여 설명할 수 있다.

〈주요 용어〉

- 해시레이트

초당 해시값 계산 횟수의 총합으로 해시레이트는 주어진 채굴기가 작동하는 속도로 정의 내릴 수 있다.

- 스크립트

응용 프로그램의 명령 집합으로 구성된 프로그램의 한 유형. 스크립트는 일반적으로 응용 프로그램의 규칙 및 구문을 사용하여 나타낸 명령과 간단한 제어 구조가 결합되어 이루어진다.

- 플랫폼

특정 장치나 시스템 등에서 이를 구성하는 기초가 되는 틀 또는 골격을 지칭하는 용어이다.

- 액셀러레이터

가속장치 (Accelerator)라는 말에서 따온 것으로, 창업 초기 기업이 빨리 성장 궤도에 오를 수 있도록 자금과 멘토링 지원을 하는 프로그램을 말한다.

사토시의 비트코인 주소


❑ 사토시가 2009년 1월 3일 만든 **비트코인 지갑 주소**
(<https://blockchair.com/explorers?from=bitcoin.com>)

❑ 2009.1.3 제네시스 블록 채굴(50BTC)

Genesis Block

블록 #0


요약	
거래 수	1
출력 합계	50 BTC
예상된 거래량	0 BTC
거래 수수료	0 BTC
높이	0 (주요 체인)
타임 스탬프	2009-01-03 18:15:05
수신 시간	2009-01-03 18:15:05
릴레이된 곳	Unknown
난이도	1
Bits	486604799




FF 4D 04 FF FF 00 1D
6D 65 73 20 30 33 2F
43 68 61 6E 63 65 6C
69 6E 6B 20 6F 66 20
69 6C 6F 75 74 20 66
FF FF FF 01 00 F2 05
8A FD B0 FE 55 48 27
D6 A8 28 E0 39 09 A6

.....yyyyM.yy..
..EThe Times 03/
Jan/2009 Chancel
lor on brink of
second bailout f
or banksyyyy..ò.
*....CA.gSÿ°pUH'
.gñ|q0°. \Ö" (à9. |

비트코인 제네시스 블록과 런던 타임지 1면

 BLOCKCHAIR

 Address
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Balance

68.52163703 BTC · 3,224,833.80 USD

Total received

68.52163703 BTC · 24,205.21 USD

Total spent

0 BTC · 0 USD

Transaction history

Show inputs and outputs

Received

Confirmed

0.00000558 BTC · 0.26 USD

Sep 1, 2021, 2:59 AM UTC

Transaction hash: b48615b914df709c3a971e114e4e8132908de139cb05767d786ab929050cfe89

Senders: 1 Recipients: 2

Received

Confirmed

0.00000558 BTC · 0.26 USD

Aug 31, 2021, 11:34 AM UTC

Transaction hash: 8a61e526636bcf3943356ed349e6dcd1f606712a82ba5a5886d1dd9bb15e5e4d

Senders: 1 Recipients: 2

Received

Confirmed

0.0000072 BTC · 0.35 USD

Aug 30, 2021, 1:50 PM UTC

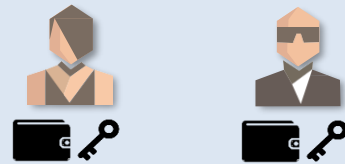
Transaction hash: 3980ad2d406e2917c8b272d4114411fbb85ab3519e76946492cfd8e0888b83d2

Senders: 1 Recipients: 1



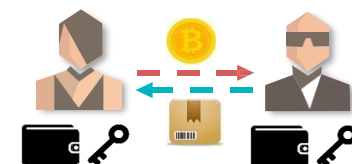
비트코인 거래과정

① 비트코인 지갑 생성



A와 B는 비트코인 지갑 생성
→ 주소와 개인키 확보

② 상호거래



A는 100BTC를 주고 B에게 물건 구매
→ 송금정보를 지갑에 저장

③ 거래내역 배포

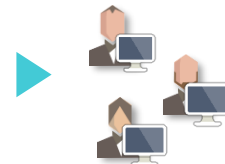
[거래 #9523]
A가 B에게 100BTC 전송
A개인키



거래를 개인키로 서명하고 공표

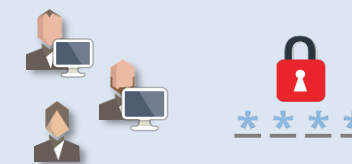
④ 채굴자 전달

[거래 #9523]
A가 B에게 100BTC 전송
A개인키



거래내역은 임의의 채굴자 노드로 전달

⑤ 블록 검증



채굴자들은 10분간 거래를 새로운
블록으로 통합 → 암호해시 연산으로 검증

⑥ 정상확인



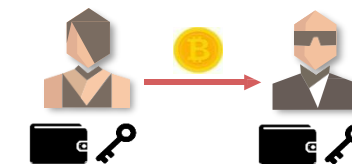
채굴자 X가 가장 먼저 A의
거래내역(블록)이 정상임을 확인

⑦ 보상지급



검증에 성공한 X에게 비트코인 지급

⑧ 거래 종료



A의 지갑 프로그램은 지불을 완료하고
100BTC를 B의 지갑에 적립



비트코인 반감기

- 2009년 1월 부터 2140년 까지 **총 2,100만개**의 비트코인 발행
- 21만개의 블록이 추가되는 **약 4년마다** 보상금이 **절반**으로 감소
- 2020년 **93.8%**의 비트코인 발행

기간	블록 넘버	보상금 (BTC)	비트코인 발행량	비중
1기 (2009-)	0	50	10500000	50%
2기(2013-)	210000	25	15750000	75%
4기(2020-)	630000	6.25	19687500	93.8%
5기(2024-)	840000	3.125	20343750	96.9%
24기(2100-)	4830000	0.00000596	20999998.7	99.9%
34기(2140-)	6930000	0.00000000	20999999.9	100.0%

* 자료: https://en.bitcoin.it/wiki/Controlled_supply, 신상화(2015)



*출처: <https://blog.naver.com/mpjzfuvyby/221550182029>



비트코인 주요 차트

- **비트코인 통계:** <https://www.blockchain.com/ko/charts> (2021.8.30)
- **이더리움 통계:** <https://etherscan.io/charts> (2021.8.30)



시장 가격(USD)	평균 블록 크기(MB)	일일 거래
\$47,575.42 USD	1.26 메가바이트	266,220 업무
ETH-\$3,475.17 주요 비트코인 거래소의 평균 USD 시장 가격.	ETH-86,981바이트 지난 24시간 동안의 평균 블록 크기(MB)입니다.	ETH-1,206,314 지난 24시간 동안 확인된 트랜잭션의 총 계입니다.



해시레이트(Hash Rate)

지난 24시간 동안 비트코인 네트워크가 수행한 예상 초당 테라해시 수입입니다.



- 해시레이트가 높을수록 채굴 난이도 상승 → 더 많은 전력과 시간이 소요되어 암호화폐 가격 상승



해시레이트(Hash Rate)

지난 24시간 동안 비트코인 네트워크가 수행한 예상 초당 테라해시 수입입니다.

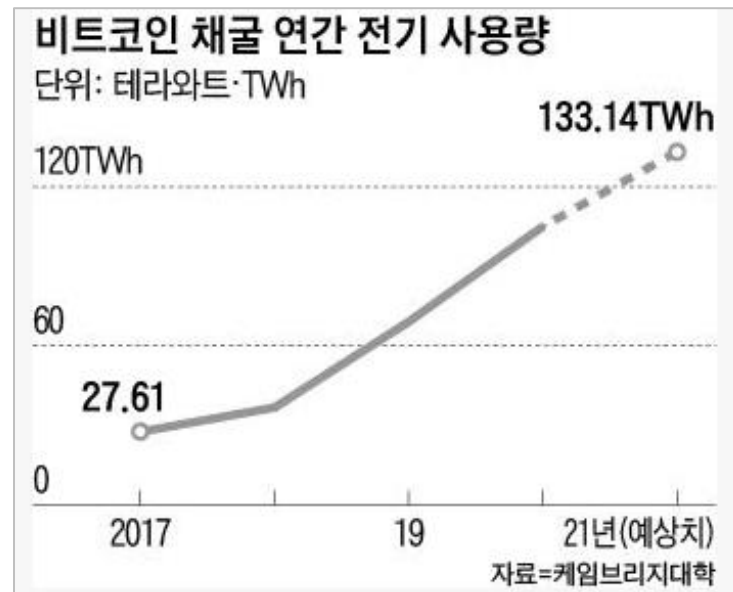


중국의 채굴 업체
90% 이상 폐쇄

- 전 세계 비트코인 채굴장의 65%가 있는 중국에서 채굴 업체의 90% 이상 폐쇄
(중국 글로벌타임스, 2021년 6월 20일)

비트코인 채굴의 전기 사용량

- ❑ 비트코인 채굴의 전기 사용량이 **스웨덴의 1년 사용량 보다 많음**
- ❑ 채굴 순위 6위의 이란도 '20년 말부터 대규모 정전 발생 → '21년 1월 **1,620개의 채굴장 강제 폐업**
- ❑ 압하지야 자치공화국 법안('21년 4월) : '22년 5월까지 모든 암호화폐 채굴 행위를 금지하고, 이를 어길 시 **최대 3년의 징역형** 선고



세계의 연간 전기 사용량
2일 기준, 단위: 테라와트·TWh

1위 중국	6453.17TWh
2위 미국	3989.57
8위 한국	527.036
26위 말레이시아	147.209
27위 비트코인 채굴	133.14
28위 스웨덴	131.798

※국가별 전기 사용량은 2019년, 비트코인은 2일 기준 2021년 예상



비트코인 - 블록체인의 한계점

- **느림**: 블록 생성 간격 10분 → 블록체인에 거래의 기록 여부를 확인하려면 길게는 수 십분 대기
- **Only Bitcion**: 비트코인만 이체 가능
- **Only Bitcoin Script**: 스크립트 기능이 제한적 → 고급이체 조건 설정 또는 스마트 컨트랙트 코딩이 불가능
- **높은 보수성**: 비트코인의 버전 업그레이드가 느림
- **거래 공개**: 비트코인 상의 거래가 모두에게 공개

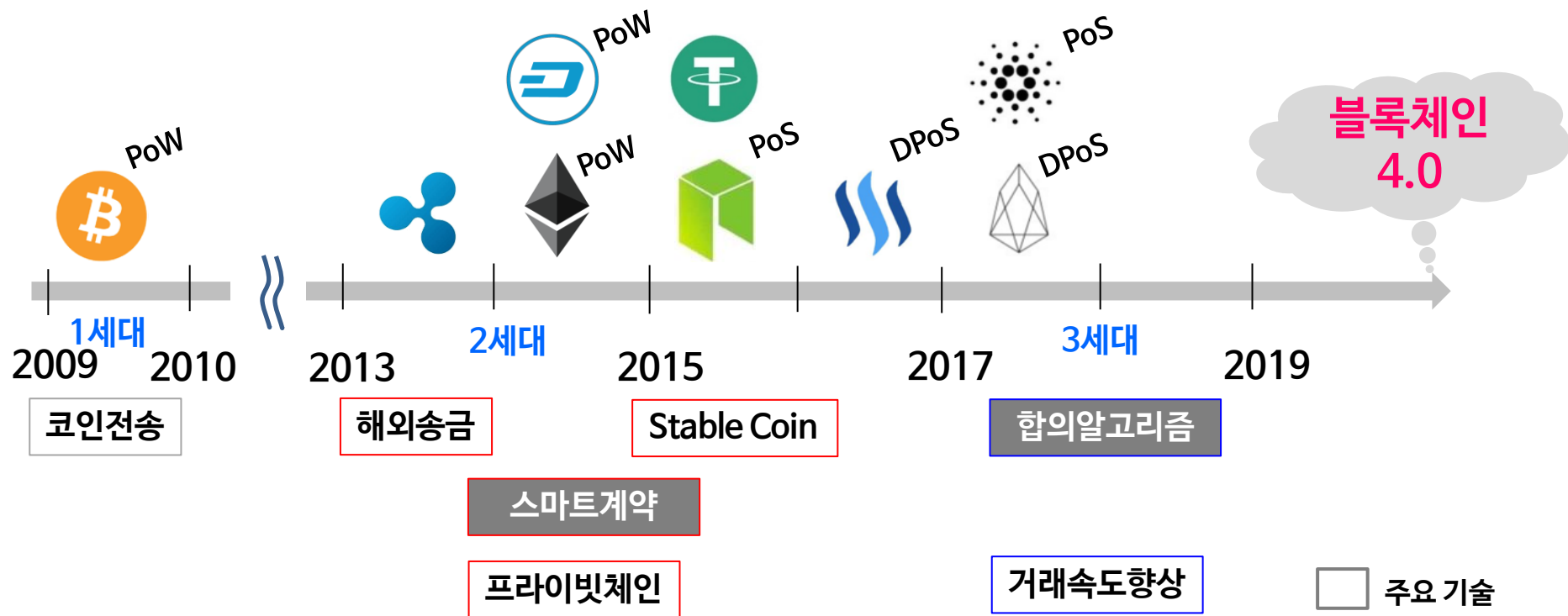


* 출처: howmuch.net/articles/crypto-transaction-speeds-compared, 10 Jan 2018



블록체인 기술 진화

- 대용량 데이터, 거래량 증가에 따른 합의알고리즘 개선 → PoW에서 PoS 및 DPoS 방식으로 발전
- **블록체인 4.0**: 블록체인 생태계가 서로 연결되어 새로운 시장 탄생 (IBM의 디지털 거래 슈퍼하이웨이)





국내외 블록체인 활용 현황(1)

분야	기업	주요내용
물류 /유통	IBM (미국)	‘17년 8월 금융, 유통, 보건 등의 분야에 적용되는 통합형 생산 블록체인 플랫폼 공개(월마트와 네슬레가 식품 유통 이력 추적에 활용)
	알리바바 (중국)	‘19년 말 인수한 수입 e-커머스 플랫폼 Koala가 QR 코드와 위조방지 지문서명 기능이 추가된 블록체인 추적 시스템 도입
게임	텐센트 (중국)	자체 블록체인 플랫폼(트러스트SQL)으로 제작한 블록체인 게임 “Let Us Hunt Monster”가 ‘19년 4월 중국 아이폰 앱스토어의 무료게임 분야 다운로드 1위
저작권	코닥 (미국)	블록체인 기반 저작권 보호 플랫폼 KodakONE을 활용하여 거래 시 코닥코인으로 체결
	Tune Company (미국)	뮤지션들의 저작권 보호를 위해 블록체인 기술로 로열티 부분의 불투명성을 관리하는 Tune Token 플랫폼 개발



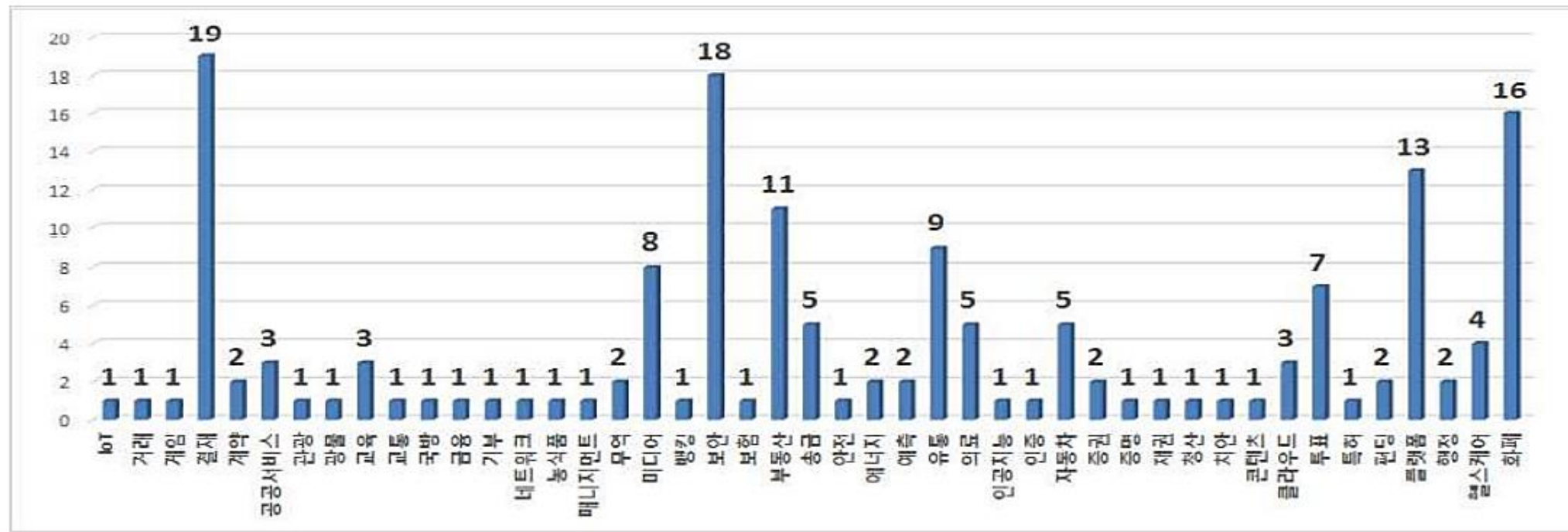
국내외 블록체인 활용 현황(2)

분야	기업	주요내용
부동산	이취치예지탄 (중국)	‘19년 1월 부동산거래, 정보서비스, 자산운용 등 4 가지 기능을 갖춘 중국자산정보컨설팅서비스(CIAC) 플랫폼 운영 시작
의료	메디블록 (한국)	의료, 관광, 금융을 통합해 양질의 의료 서비스를 제공하는 블록체인 기반의 의료관광 모바일 결제 플랫폼 메디토 개발
	상하이체육국 (중국)	블록체인 기반 위챗 애플릿을 출시하여 온라인으로 일대일 헬스 수업을 받을 수 있는 ‘홈 헬스’ 서비스 제공
금융	삼성(한국)	갤럭시 S10에 전자지갑을 탑재하여 암호화폐를 저장 및 송금
	연방준비은행 (미국)	IBM과 함께 블록체인을 응용한 지급 결제 시스템 개발



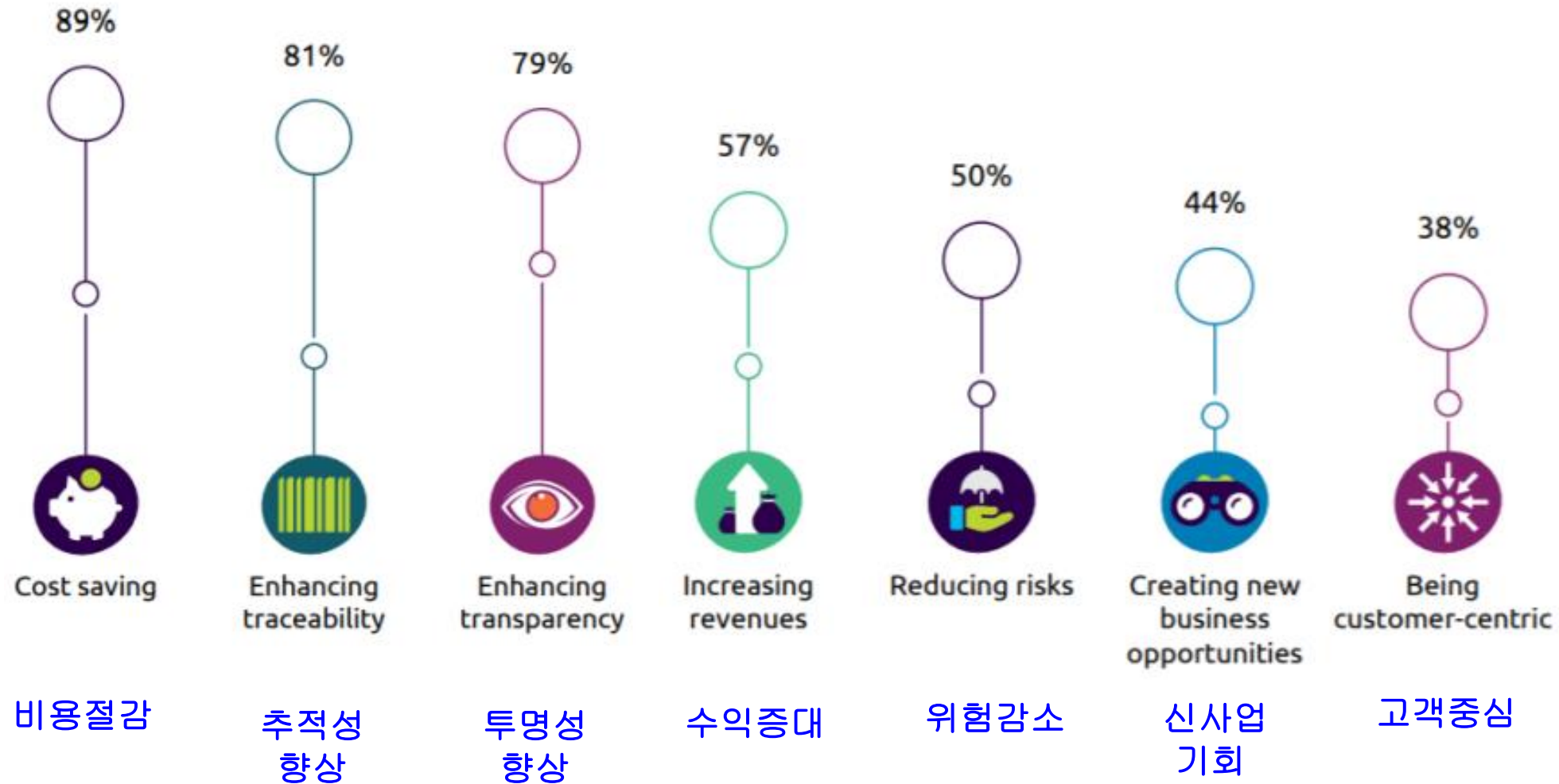
블록체인 응용 분야별 분포

- 초기에 적용된 금융(결제, 화폐, 보안 등) 뿐만 아니라 다양한 산업에서 블록체인의 적용 시도가 활발
- 총 45개 응용분야 조사
 - 10개 이상: 결제·보안·화폐·플랫폼·부동산
 - 5개 이상: 유통·미디어·투표·송금·의료·자동차



※ 주 : 5대 분석대상별 조사된 응용 분야에 대한 분석 결과값임 (n=166)

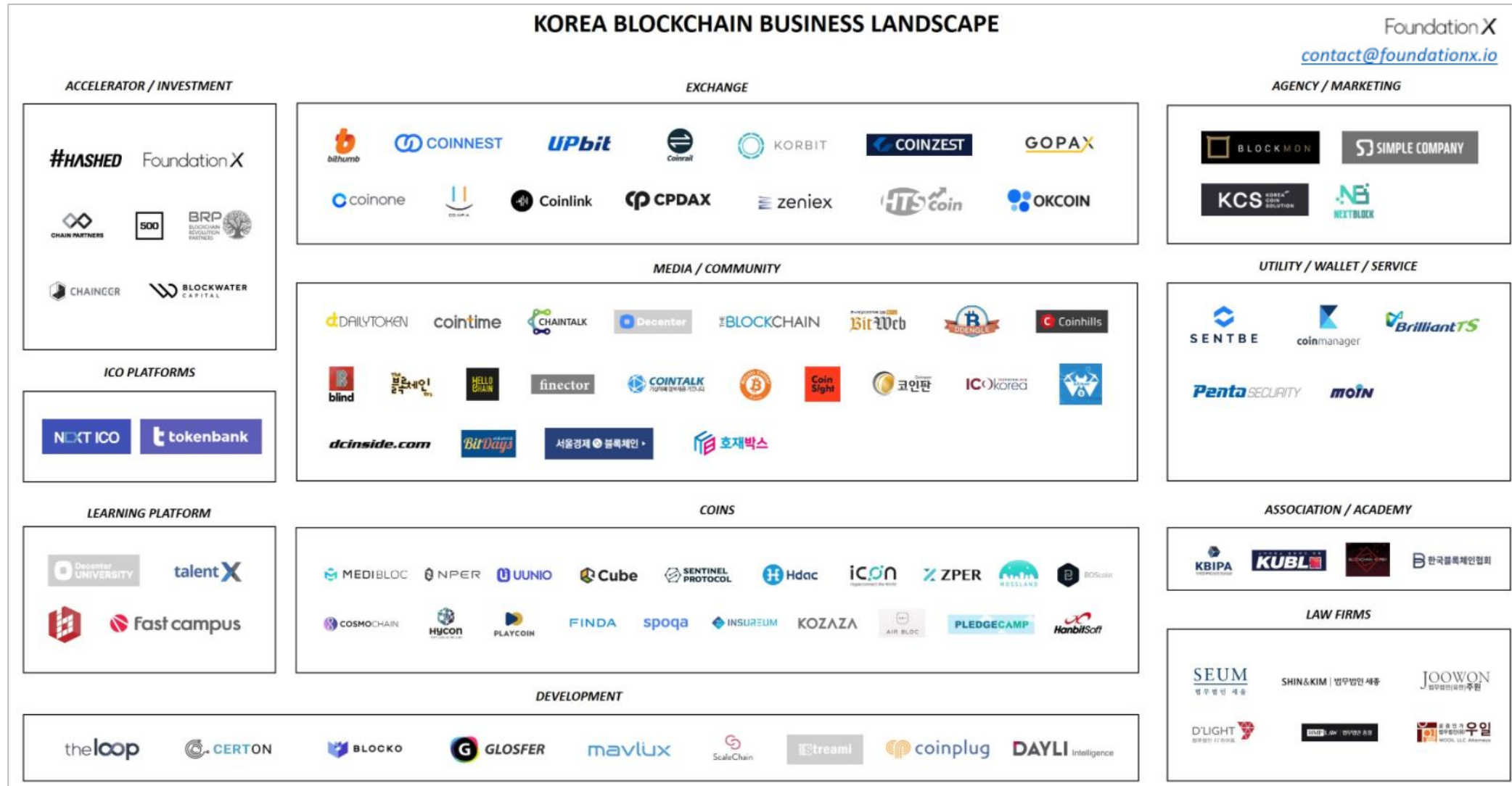
블록체인의 사용 동인



Source: Capgemini Research Institute, Blockchain Survey; April–May 2018, N=447 organizations.

블록체인 생태계(1/3)

□ 블록체인 관련 조직과 그룹의 구성을 나타내는 지도



블록체인 생태계 지형도(2/3)

- ❑ 개발사: ICON Loop, CertOn, Bloko, Glosfer
- ❑ 암호화폐 거래소: 업비트, 빗썸
- ❑ 지갑 서비스: 그라운드X의 모바일 지갑 Klip, 차일드리의 비둘기지갑
- ❑ 암호화폐공개(ICO: Initial Coin Offering) 플랫폼: Next ICO, TokenBank
 - 새로운 암호화폐를 만들기 위해 투자자들로부터 개발 자금을 모집하고 코인을 나눠주는 행위

블록체인 생태계 지형도(3/3)

- ❑ ICO 기업을 위한 마케팅 및 컨설팅: NextBlock, Blockmon
- ❑ 투자 및 액셀러레이터: Chain Partners, FoundationX
- ❑ 블록체인 관련 미디어(코인타임, 데일리토큰)와 커뮤니티(Coinpan, Bitdays)
- ❑ 학회 및 단체: 한국블록체인협회
- ❑ 법률사무소: 세움, 세종, 우일



〈3교시〉 학습 정리

- 대용량 데이터, 거래량 증가에 따라 합의 알고리즘이 PoW에서 PoS 및 DPoS 방식으로 발전한다.
- 초기에 적용된 금융(결제, 화폐, 보안 등) 뿐만 아니라 다양한 산업 분야(결제·보안·화폐·플랫폼·부동산·유통·미디어·투표·송금·의료·자동차)에서 블록체인의 적용 시도가 활발이 전개되고 있다.
- 블록체인 생태계에는 개발사, 암호화폐 거래소, 지갑서비스, 암호화폐공개 플랫폼, 투자 및 액셀러레이터, 블록체인 관련 미디어와 커뮤니티 등이 포함된다.



〈3교시〉 학습 평가

1. 해시레이트 및 암호화폐에 대한 설명 중 틀린 것은?

- 1) 비트코인은 스크립트 기능이 충분하여 고급이체 조건 설정 또는 스마트 컨트랙트 코딩이 가능하다.
- 2) 해시레이트가 높을수록 채굴 난이도가 상승하며 더 많은 전력과 시간이 소요되어 암호화폐 가격 상승한다.
- 3) 2140년 까지 총 2,100만개의 비트코인 발행되며, 21만개의 블록이 추가되는 약 4년마다 보상금이 절반으로 감소한다.
- 4) 대용량 데이터, 거래량 증가에 따라 합의 알고리즘이 PoW에서 PoS 및 DPoS 방식으로 발전한다.

답) 1

해설) 비트코인은 스크립트 기능이 제한적이어서 고급이체 조건 설정 또는 스마트 컨트랙트 코딩이 불가능하다.

2. 블록체인 생태계가 무엇인지 그리고 생태계에 포함되는 것은 어떠한 것들이 있는지 설명하시오.

해설) 블록체인 생태계는 블록체인 관련 조직과 그룹의 구성을 나타내는 지형도이며, 개발사, 암호화폐 거래소, 지갑서비스, 암호화폐 공개 플랫폼, 투자 및 액셀러레이터, 블록체인 관련 미디어와 커뮤니티 등이 포함된다.