

# Blockchain Overview

Mooje Kong  
mooje.kong@gmail.com  
2018 3월

## 1. 블록체인 개념 이해하기

- 분산 원장의 개념
- 블록체인 구성 기술요소 이해하기 (P2P 네트워크, 합의 알고리즘, 전자 서명, 해시 함수 등의 개념) <-- 블록체인의 기반 기술에 대한 학습

## 2. 퍼블릭 블럭체인(이더리움) 기본

- 이더리움 개념
- 이더리움 스마트 컨트랙트 개발

## 3. 퍼블릭 블럭체인 클라이언트 개발

- 이더리움 Dapp 개발

## 4. 프라이빗 블럭체인의 이해

- Hyperledger Fabric 기술의 이해
- 블록체인 네트워크 구성 (런타임 환경 구성)

## 5. 프라이빗 블럭체인 개발

- 스마트 컨트랙트 개발
- SDK를 이용한 클라이언트 어플리케이션 개발

# 블록체인 기술

비즈니스 네트워크(Business Network)의 모든 참여자들이  
원장(Ledger)을 볼 수 있도록 해주는

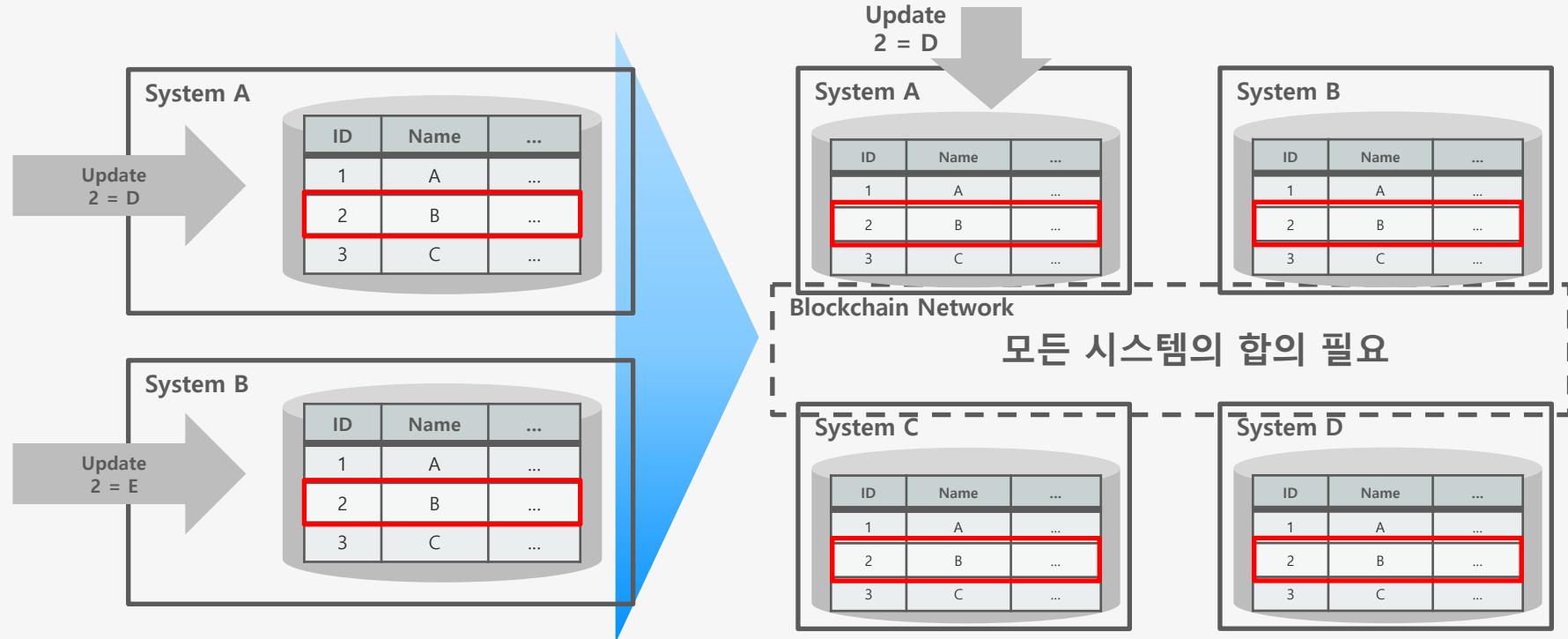
**공유 원장 기술  
(shared ledger technology)**

비즈니스 프로세스를 간소화하면서  
신뢰와 투명성을 확립하는

**차세대 트랜잭션 애플리케이션**을  
구축하기 위한 토대

# 분산원장

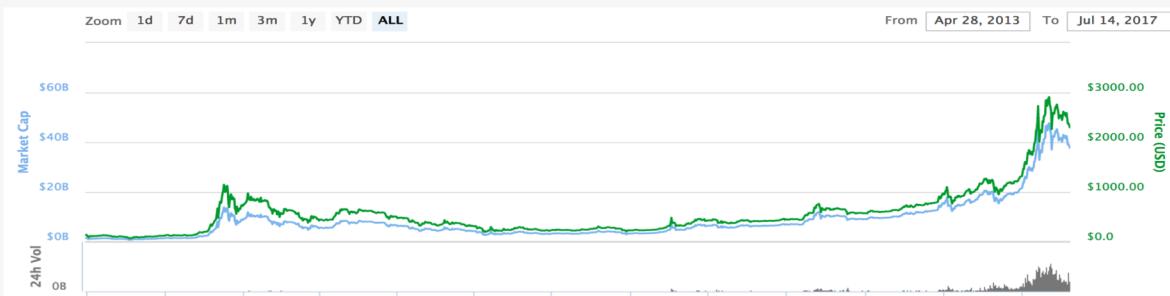
참여하고 있는 모든 시스템이 각자 원장 데이터를 보유하고 항상 동기화를 하는 것



# 블록체인의 시작 - 비트코인

블록체인은 비트코인을 구현하기 위해 만들어 졌음.

- 2008년 11월 사토시 나카모토의 논문에 의해 알려짐
- P2P 네트워크 상에서 구현한 최초의 가상화폐
- 2009년 1월 비트코인 소프트웨어 배포되어 운영
- 2009년 1월 3일 최초의 블록(genesis block)이 만들어진 이후 지금까지 가동되고 있음.



# 비트코인의 목적

사토시 나카모토의 논문 중...

"A purely peer -to -peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution ."

"전자 화폐를 순수 P2P (Peer to Peer)로 만들 수 있다면 금융 기관의 개입 없이 사용자끼리 직접 온라인으로 지불할 수 있게 된다."

## 온라인에서 사용자간 거래를 위한 기술적 해결해야 할 점

- 본인 보증, 부인 방지
- 제삼자 기간의 보증 대체
- 원장 데이터에 대한 위/변조 위험
- P2P 네트워크상에서의 비잔티움 장군 문제
- 등등

## 해결 방법

- 전자 서명
- 블록체인
- 해답 인센티브
- PoW

# 블록체인의 기술요소 구성

## 피어 투 피어(P2P) 네트워크

컴퓨터끼리 같은 목적으로 연결해 네트워크를 형성하는 방식이다. 어떤 컴퓨터도 같은 처리를 할 수 있기 때문에 1대가 정지해도 시스템 전체에는 영향을 주지 않는 특징을 가진다.

## 합의 알고리즘

P2P 네트워크와 같은 분산 네트워크에서 합의 형성을 수행하기 위한 알고리즘이다. 블록체인을 여러노드에서 공유하기 위한 가장 중요한 구조라고 할 수 있다.

## 전자 서명·해시 함수

트랜잭션(거래)을 발생시킨 사람의 정당성을 보증하거나 거래·블록체인 변조 방지, 암호화 등 보안과 관련된 기능이다.

## 스마트 계약

블록체인 네트워크에서 동작하는 프로그램을 가리킨다. 블록체인 기반 기술 중에서 가장 자유도가 높은 프로그램을 만들 수 있다.

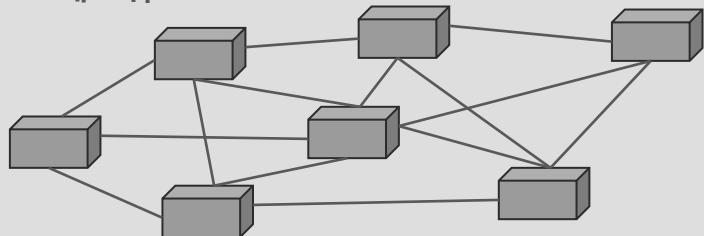
### 블록체인 기술

스마트 계약

전자서명 · 해시 함수

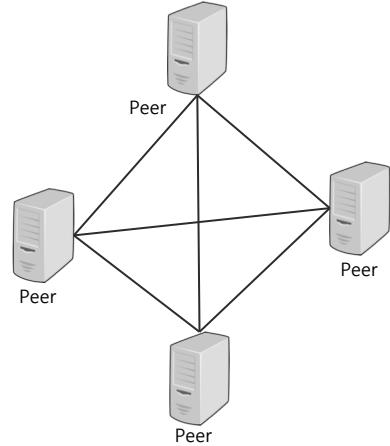
합의 알고리즘

### P2P 네트워크

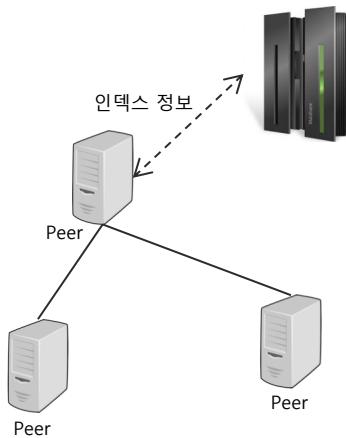


# 블록체인의 기술요소 – P2P 네트워크

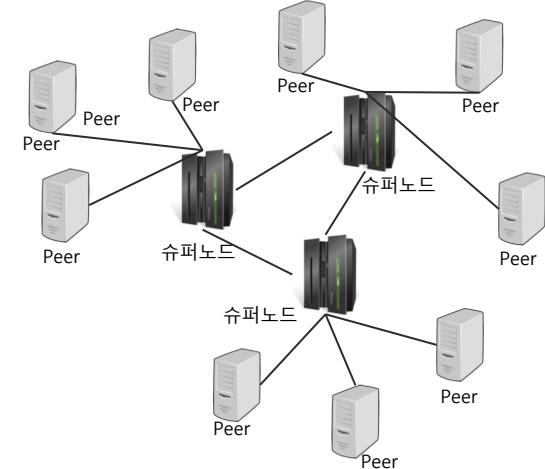
퓨어 P2P



하이브리드 P2P



슈퍼 노드형 P2P



- 노드간 직접적인 메시지 통신
- 노드 검색을 위한 알고리즘 구현 필요
- 확장성과 내결합성이 우수
- 비트코인, 이더리움

- 노드 탐색을 위해 인덱스 서버 사용
- 네트워크 설계, 관리가 용이
- 내결합성과 확장성이 떨어짐
- Hyperledger Fabric

- 계층적 노드 구성으로 ID 할당된 노드를 기준으로 메시지 통신
- 메시지 도착 가능성 및 확장성 높음
- 유연한 탐색은 불가능
- Hyperledger Fabric

# 블록체인의 기술요소 – 합의 알고리즘(1/4)

P2P 네트워크에서 정보의 지연과 미도달과 같은 환경을 극복하기 위해 하나의 결과에 대해 네트워크의 참여자가 합의를 얻기 위한 알고리즘

## 분산 시스템의 장애 모델

1. Fail Stop 모델 – 어떤 오류로 인해 중지된 서버는 깨끗이 퇴출하는 모델
2. Fail Recover 모델 – 한 번 정지한 서버가 부활하는 모델(지연과 중단을 구별하지 않음)
3. Byzantine Fault 모델 – 임의 노드가 악의적으로 실수를 일으키는 모델

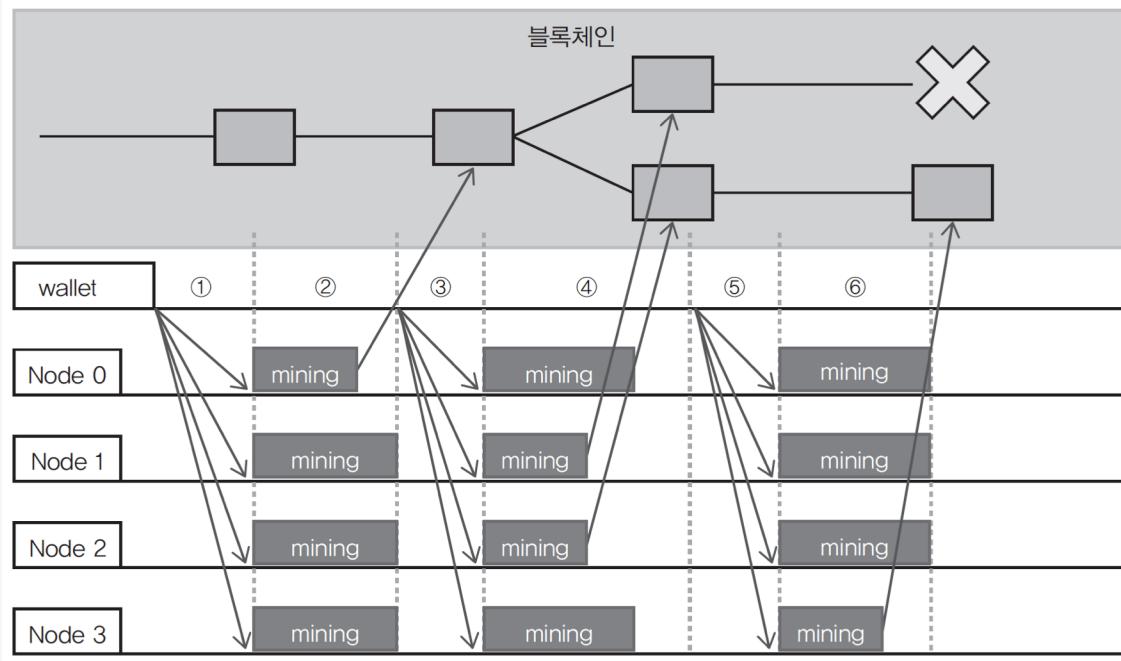
# 블록체인의 기술요소 – 합의 알고리즘(2/4)

## 합의 알고리즘 특징 비교

	Paxos/Raft	PBFT	PoW	PoS
장애 모델	Fail-Stop, fail-recover는 대응하지만 Byzantine Fault는 대응하지 않음	Byzantine Fault 대응	Byzantine Fault 대응	Byzantine Fault 대응
통신 비용	리더를 중심으로 통신하기 때문에 PBFT보다 통신 비용 낮음, PoW, PoS 와 비교하면 전체적으로 비용은 같지만 리더 1대의 통신 비용이 높아짐	각 서버간 통신을 수행하기 때문에 비용은 높음	참가 서버 전체가 아닌 로컬 통신만으로 문제 없음. 로컬 통신은 비용이 낮음	참가 서버 전체가 아닌 로컬 통신만으로 문제 없음. 로컬 통신은 비용이 낮음
결합 허용 대수	$\frac{1}{2}$ 미만은 문제 없음(정확히 $\frac{1}{2}$ 인 경우 대응 불가) PBFT 보다 적은 대수로 가능	1/3 미만까지 보증(정확히 1/3인 경우 대응 불가)	1대로 남아 있다면 문제 없음	1대로 남아 있다면 문제 없음
다수결 대신이 되는 것	다수결	다수결	CPU 계산량	보유한 자산의 크기
CPU 연산 비용	낮음	낮음	높음	중간정도. PoW 보다 낮지만 나름대로의 해시 계산을 수행
권한의 분산	리더에게 강한 권한이 있으나 교체될 수 있음	참가 서버 모두가 평등	전기세가 낮은 지역에 집중될 가능성이 있음	일반적으로 화폐 보유는 집중될 가능성이 높음
참가 서번의 조건	신뢰된 서버만 참가	신뢰된 서버만 참가	어떤 서버도 참가 가능	어떤 서버도 참가 가능
비밀 보호를 위한 인증	특별히 없음	사전에 서로 신뢰한 공개 암호화 키를 사용	참가시 준비한 공개 암호화 키를 사용	참가시 준비한 공개 암호화 키를 사용

# 블록체인의 기술요소 – 합의 알고리즘(3/4)

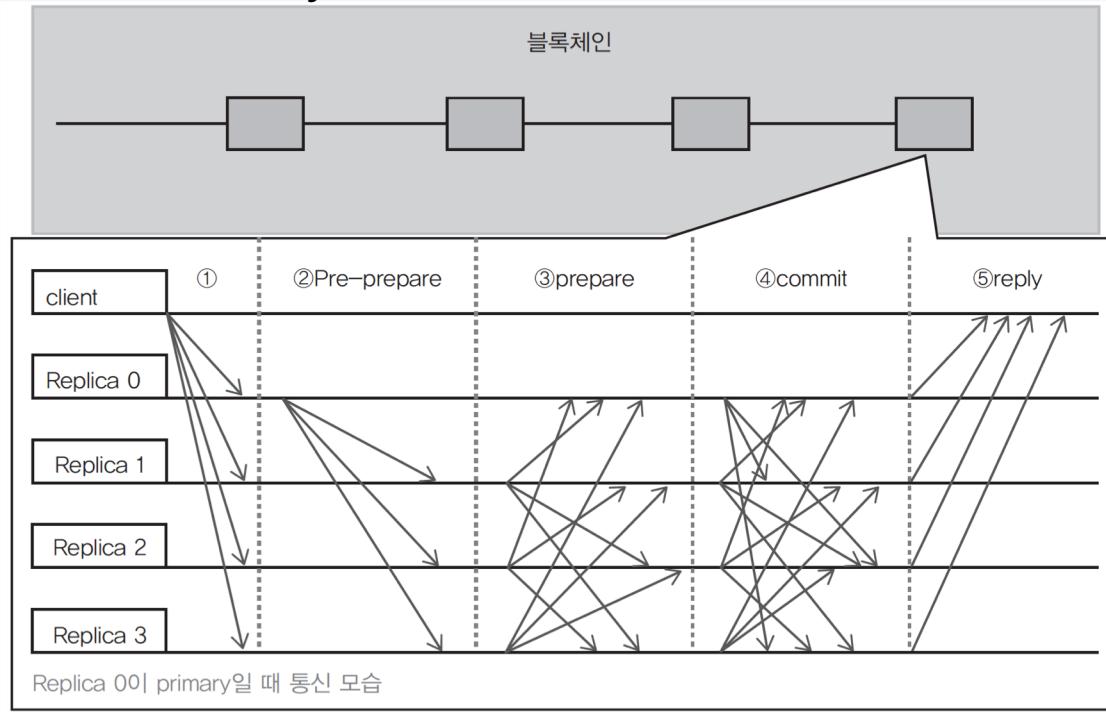
## 작업 증명(Proof of Work, PoW) 알고리즘



- 1) Wallet이 트랜잭션을 발행하고 참가자 전원에게 브로드 캐스트
- 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 Node1과 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 것이 됨

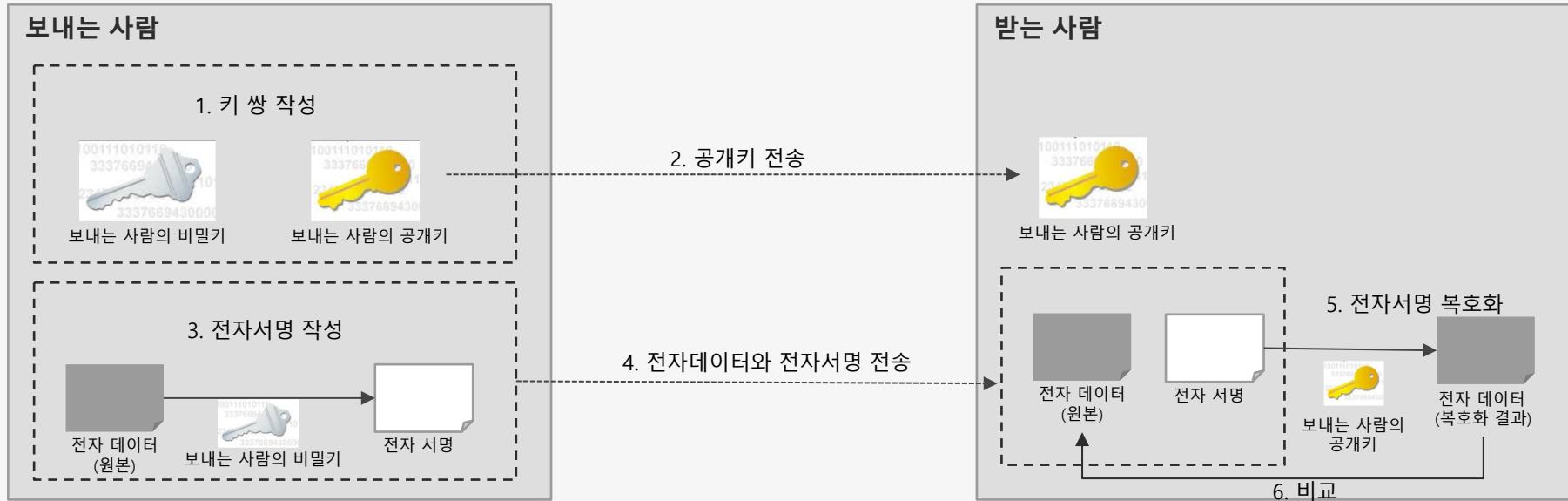
# 블록체인의 기술요소 – 합의 알고리즘(4/4)

## PBFT(Practical Byzantine Fault Tolerance) 알고리즘

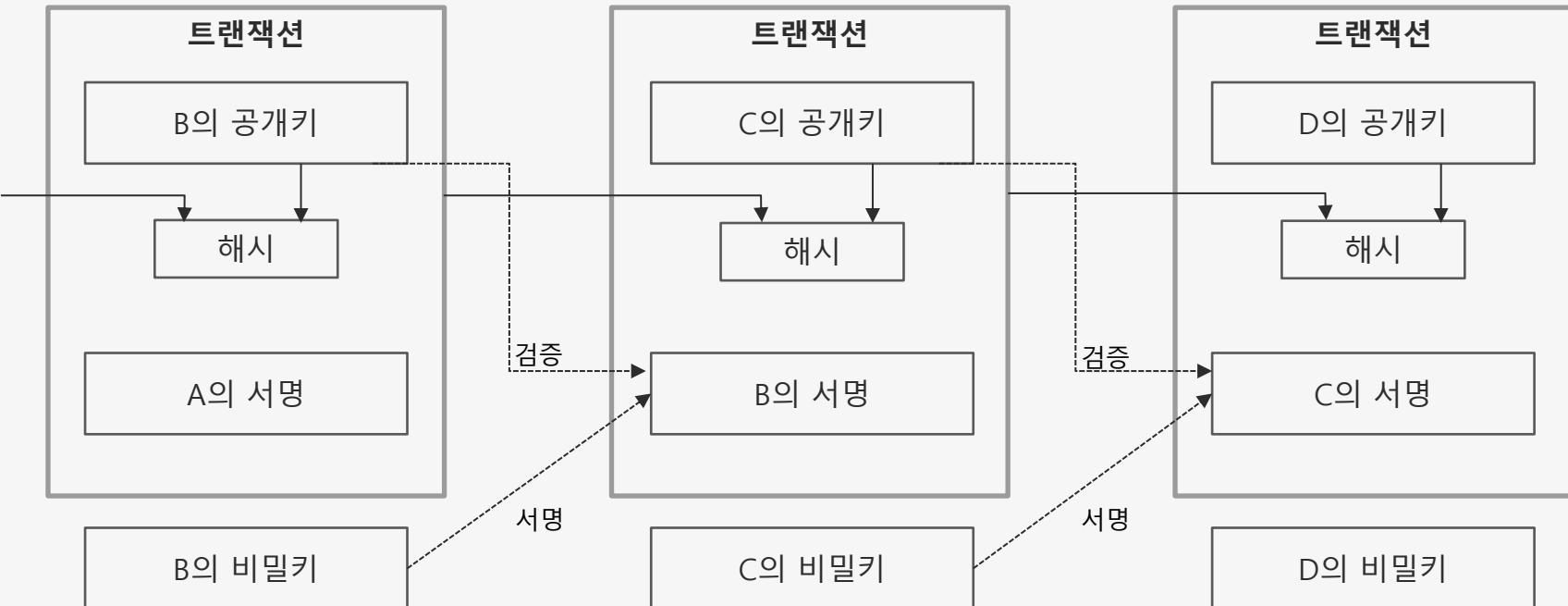


- 1) 클라이언트가 모든 노드에 요청을 브로드캐스트
- 2) Replica0이 primary(리더)가 되고 순차적으로 명령을 다른 노드에 전달
- 3) 각 노드는 2)의 명령을 받으면 primary(Replica0)를 포함한 모든 노드에 수신한 신호를 전송
- 4) 각 노드는 3)에서 전달된 명령을 일정 수 이상(2f) 수신하면 primary(Replica0)를 포함한 모든 노드에 수신한 신호를 전송
- 5) 각 노드는 4)에서 보낸 명령을 일정 수 이상(2f) 수신하면 명령을 실행하고 블록을 등록해 client에 replay를 반환

# 블록체인의 기술요소 – 전자 서명(1/2)



# 블록체인의 기술요소 – 전자 서명(2/2)

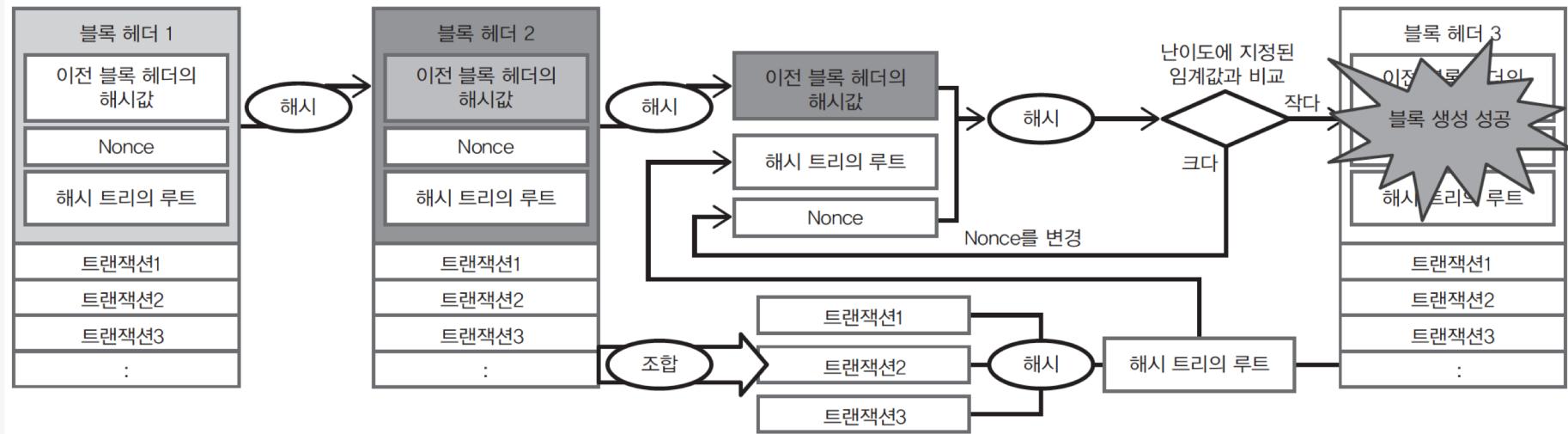


# 블록체인의 기술요소 – 해시 함수(1/2)

## 해시 함수의 특징

- 전자 데이터의 고유한 해시를 생성함
- 전자 데이터의 길이(비트 길이)와 상관없이 고정된 크기의 해시를 생성함(해시 사이즈는 사용하는 해시 함수가 결정)
- 전자 데이터가 1비트라도 변하면 완전히 다른 해시가 만들어짐(해시는 전자 데이터의 내용에 따라 고유한 값을 가짐)

# 블록체인의 기술요소 – 해시 함수(2/2)



[출처 : 블록체인 구조와 이론]

# 이더리움이란?

- 이더리움은 2015년 출시된 차세대 스마트 계약 분산 응용프로그램(Dapp : decentralized applications) 기술
- 비트코인과 함께 대표적인 퍼블릭 블록체인 중 하나로 스위스의 비영리 단체인 이더리움 재단(Ethereum Foundation)에서 개발한 오픈소스 프로젝트
- Solidity 등의 튜링완전성(Turing-Completeness) 을 갖춘 확장용 언어를 갖춰 스마트 계약을 쉽고 간단하게 프로그래밍 가능

# 이더리움이란?

- 이더리움은 2015년 출시된 차세대 스마트 계약 분산 응용프로그램 기술
- 이더리움은 스마트 계약이라는 사용자가 제작한 어플리케이션을 구동할 수 있는 블록체인 기반의 플랫폼
- 비트코인이 블록체인의 기술을 활용하여 화폐 거래를 위한 기능 위주로 구성이 되어 있는 반면 이더리움의 스마트 계약은 사용자의 요구에 따라 무한 확장되는 어플리케이션 환경을 제공해 준다는데 큰 의미가 있음
- 비트코인과 함께 대표적인 퍼블릭 블록체인 중 하나로 스위스의 비영리 단체인 이더리움 재단(Ethereum Foundation)에서 개발한 오픈소스 프로젝트
- Solidity 등의 튜링완전성(Turing-Completeness) 을 갖춘 확장용 언어를 갖춰 스마트 계약을 쉽고 간단하게 프로그래밍 가능

# 이더리움 특징 – 블록체인 네트워크

- **라이브 네트워크**

전 세계적으로 공개된 네트워크이다. 누구라도 공개된 네트워크에 노드를 추가하여 참가 할 수 있음

- **테스트 네트워크**

테스트를 위한 네트워크로 전 세계적으로 참가하여 테스트 가능한 “Morden 테스트 넷”이 있으며 사용자가 개발을 위해 한정된 환경(개발 PC 등)에 설치해서 테스트 가능한 사설 테스트 네트워크가 있음

# 이더리움 특징 – 화폐단위

이더리움의 화폐단위는 “ether”이다. 이는 여러 단위로 나누어 관리 할 수 있으며 그 단위는 아래와 같다.

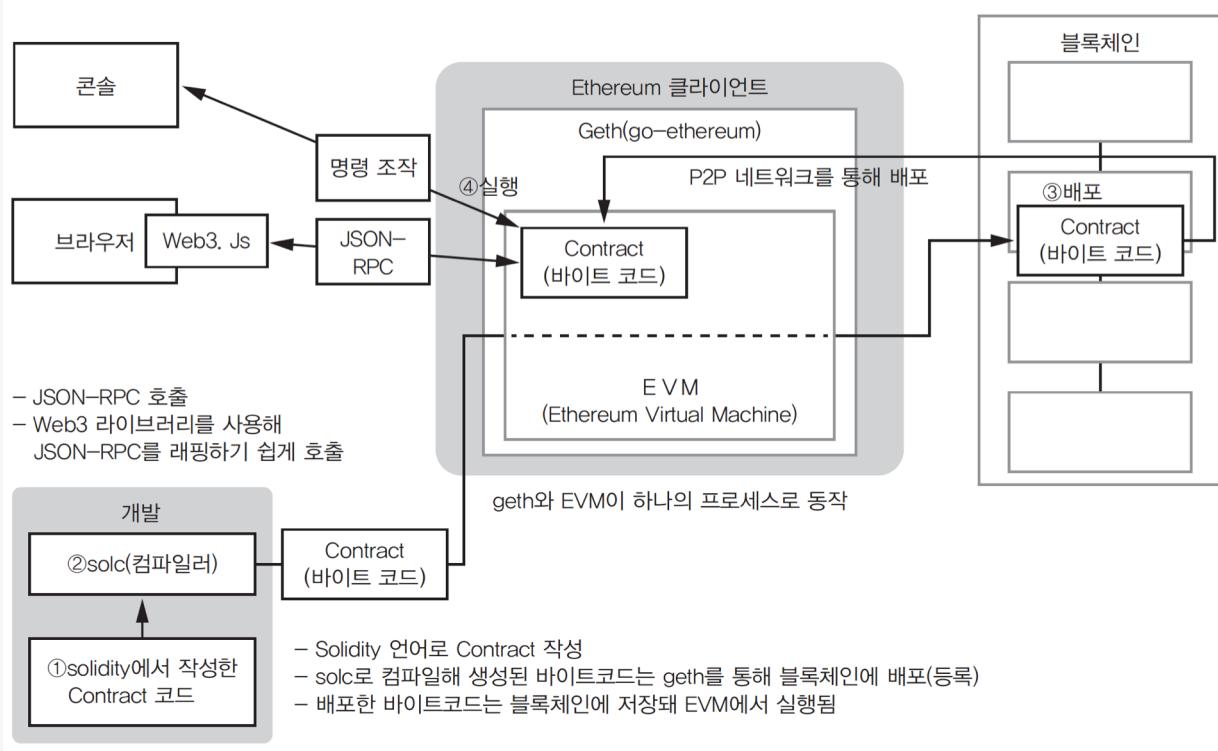
단위	Wei 가치	Wei
wei	1 wei	1
Kwei(babbage)	$10^3$ wei	1,000
Mwei(lovelace)	$10^6$ wei	1,000,000
Gwei(Shannon)	$10^9$ wei	1,000,000,000
microether(Szabo)	$10^{12}$ wei	1,000,000,000,000
milliether(finney)	$10^{15}$ wei	1,000,000,000,000,000
ether	$10^{18}$ wei	1,000,000,000,000,000,000

# 이더리움 특징 – Gas

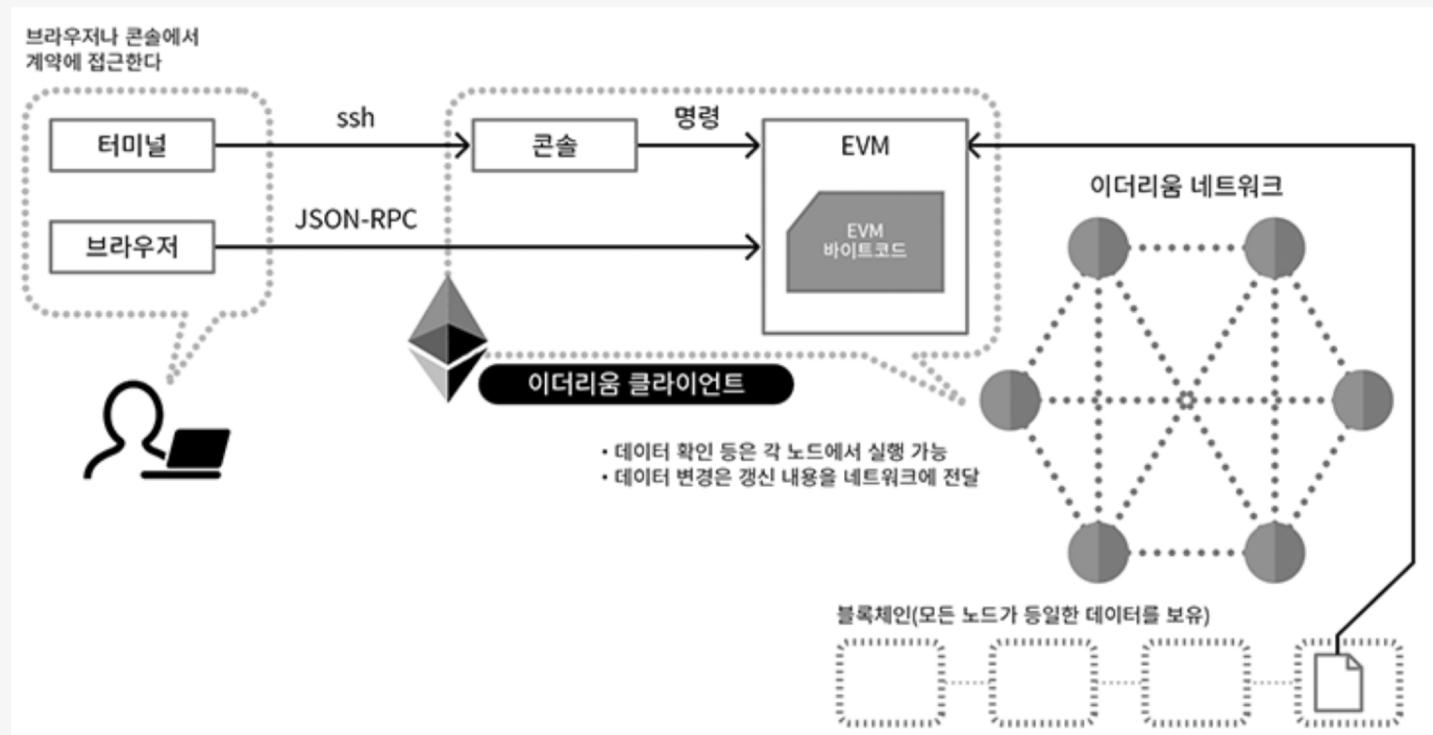
이더리움에서 거래를 위해서는 수수료를 Ether로 지불해야 하며, 이 것을 'Gas'라고 함.  
사용자는 이더리움을 사용한 수수료를 채굴자에게 Gas를 지불하며, 지불되는 Gas의 양은  
수수료(Gas fee)와 현재 Gas 가격(Gas price)에 의해 결정 됨

- **Gas Fee**  
가스 수수료는 이더리움에서 요구하는 자원의 양과 복잡도에 따라 가치가 결정되는 수수료
- **Gas Price**
  - 1Gas당 가격, 단위는 wei/Gas
  - 채굴자는 가스 가격이 높은 트랜잭션 부터 실행
- **Gas Limit**
  - 트랜잭션 처리에 드는 최대값, 즉 트랜잭션 처리에 드는 Gas의 추정치
- **Block Gas Limit**
  - 한 블록에 담을 수 있는 최대 Gas limit의 갯수

# 이더리움의 아키텍처



# 이더리움의 아키텍처



[출처 : 블록체인 애플리케이션 개발 실전 입문]

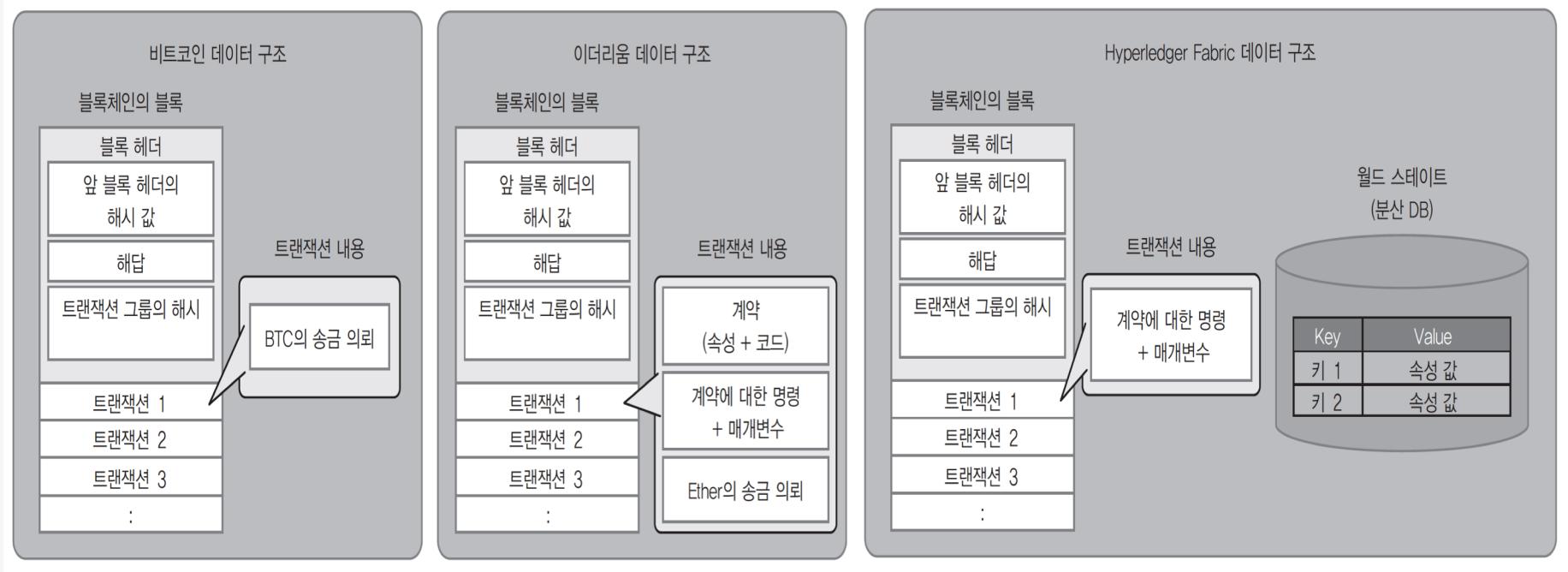
# 블록체인 기반 기술의 분류

	공용(Public) 형	컨소시엄형 (여러 조직에서 운영)	개인(Private)형 (단일 조직에서 운영)
(마이닝) 노드형	제한 없음	제한 가능	제한 가능
블록체인 검색	제한 없음	제한 가능	제한 가능
블록 생성시	높은 난이도 필요	임의	임의
마이닝 보수	필요	임의	임의

# 블록체인 기반 기술 비교

분류	하이퍼레저 (Hyperledger)	이더리움 (Ethereum)	리플 (Ripple)	비트코인 (Bitcoin)
소개	모든 산업에서 사용할 수 있는 Blockchain 기술의 표준화	일반적인 사용을 위한 Blockchain	페이먼트 Blockchain	페이먼트 Blockchain
거버넌스	리눅스 재단	이더리움 개발자	리플 랩(Ripple Labs)	비트코인 개발자
합의 네트워크	플러거블 : PBFT (Practical Byzantine Fault Tolerance)	マイ닝	리플 프로토콜	マイ닝
네트워크	프라이빗 또는 퍼블릭	퍼블릭 또는 프라이빗	퍼블릭	퍼블릭
프라이버시 (Privacy)	오픈 원장 부터 사설 원장 지원	오픈 원장	오픈 원장	오픈 원장
스마트 컨트랙 (Smart Contracts)	멀티 프로그래밍 언어 (Go, Java, Node.js)	'Solidity' 프로그래밍 언어	없음	가능하지만 분명하지 않음
통화	통화기반이 아님(UTXO API 활용하여 구현 가능)	Ether	XRP	BTC
マイ닝 보상	관련없음	있음	없음	있음
State	키-밸류 데이터베이스	계좌(Account) 데이터	없음	거래(Transaction) 데이터

# 블록체인 데이터 모델 비교



# 블록체인의 특징

## 1. 블록은 시간 별로 정렬돼 있다.

- 거래 기록이 블록으로 시간별로 어어져 있음

## 2. 분산형 원장 구조다

- 변조가 어려움
- 거래 기록의 작성 시점을 객관적으로 알 수 있음
- 분산형 시스템이기 때문에 큰 중앙 시스템이 필요 없음
- 거래 기록의 타당성을 모든 참여자에게 검증받음

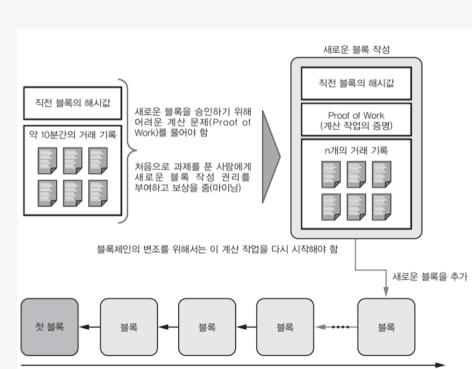
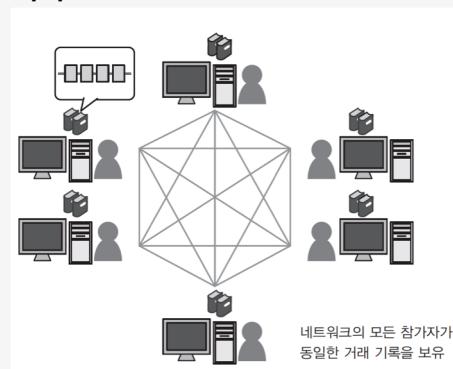
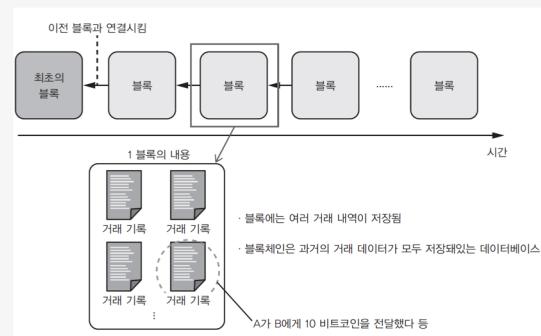
# 블록체인의 응용 – 결제 및 거래

## 화폐의 기능을 위한 블록체인

1. “누가 누구에게 얼마만큼 전달했다”라는 거래 기록을 블록 단위로 기록해 연결하여 시간순으로 관리
2. 임의로 화폐량을 부풀릴 수 없음

## 대표적인 가상화폐

- 비트코인, Litecoin, Namecoin, Ripple 등

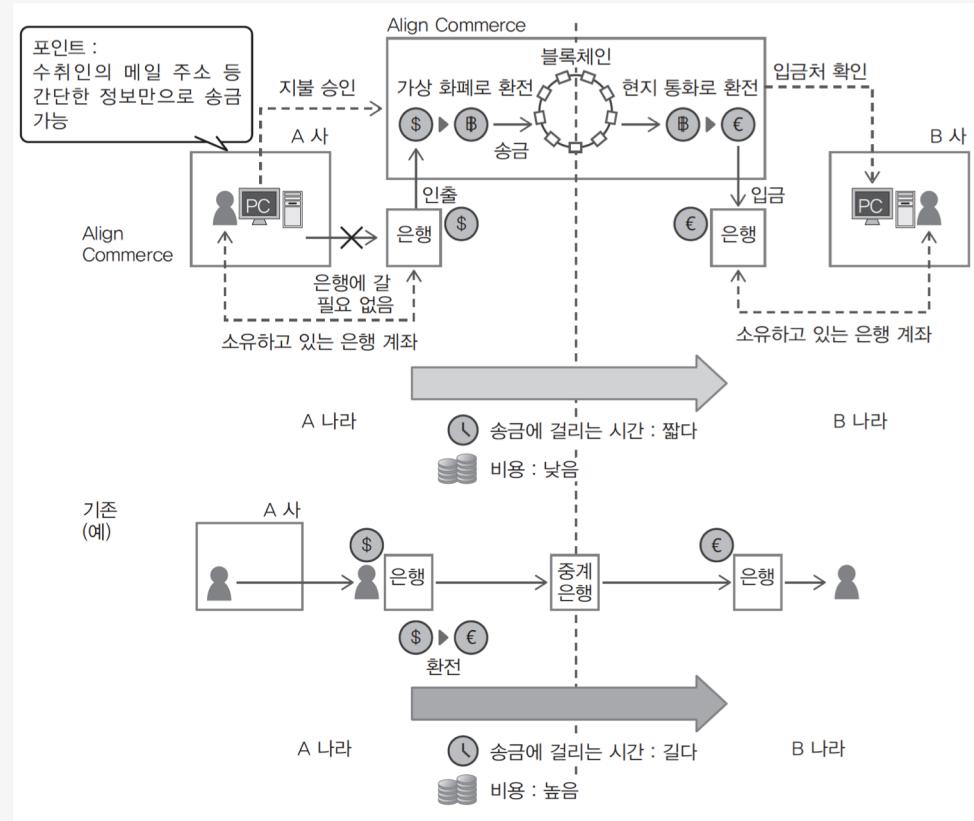


# 블록체인의 응용 – 송금·결제

블록체인을 이용한 송금·결제는 다양하게 시도하거나 서비스 중

미국의 Align Commerce 사례

- 송금 절차를 가상화폐를 이용
- 서비스 가능한 국가 : 60개국
- 송금/수취 : 24개국
- 송금 절차 간략화, 낮은 수수료, 처리과정 투명화

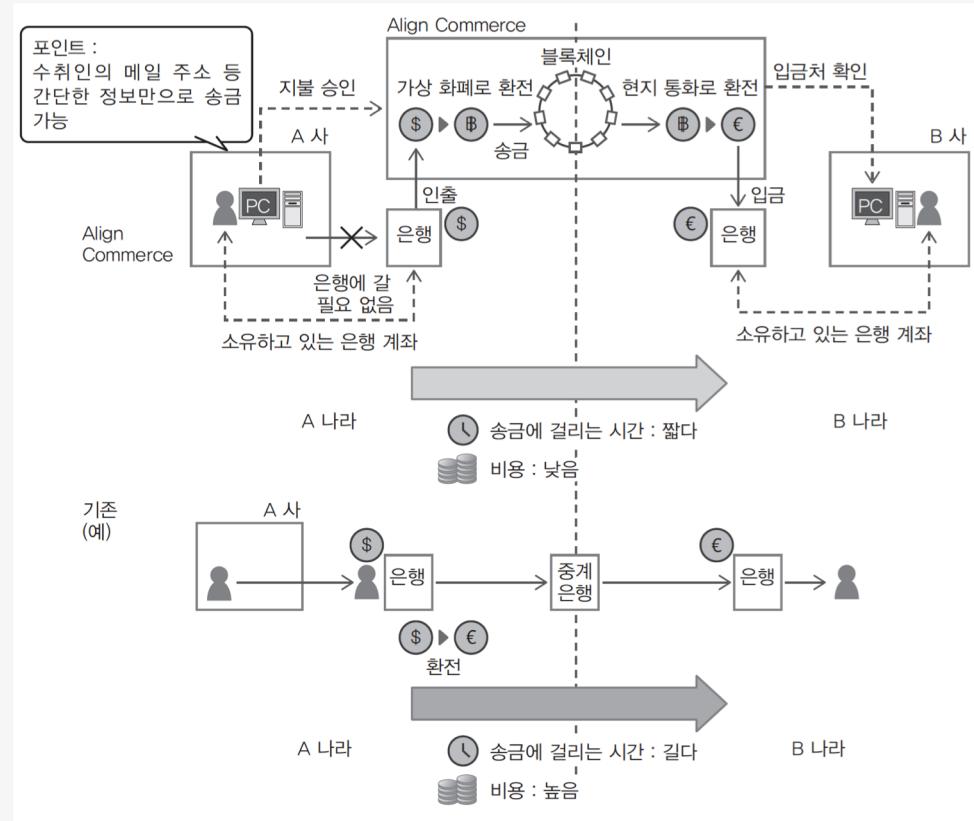


# 블록체인의 응용 – 송금·결제

블록체인을 이용한 송금·결제는 다양하게 시도하거나 서비스 중

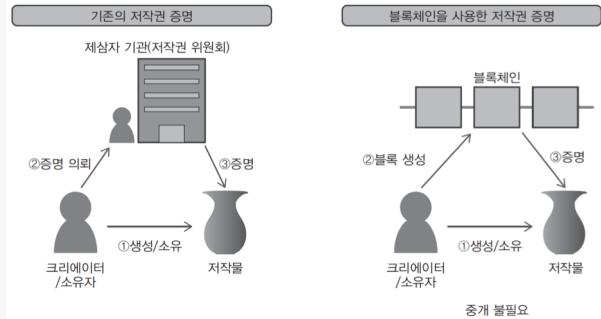
미국의 Align Commerce 사례

- 송금 절차를 가상화폐를 이용
- 서비스 가능한 국가 : 60개국
- 송금/수취 : 24개국
- 송금 절차 간략화, 낮은 수수료, 처리과정 투명화

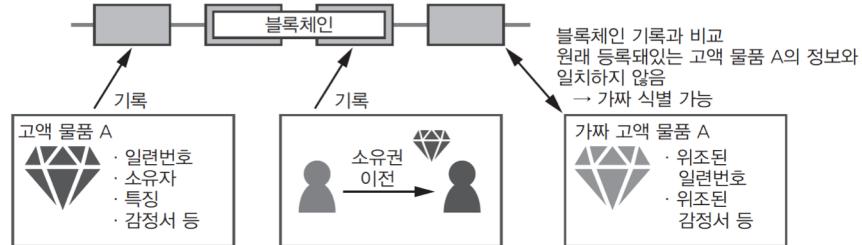


# 블록체인의 응용 – 서명 및 증명

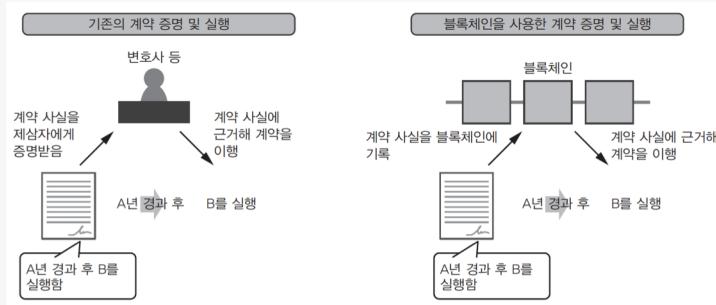
## 저작권 관리



## 고액 물품 거래 추적



## 계약 관리 및 실행



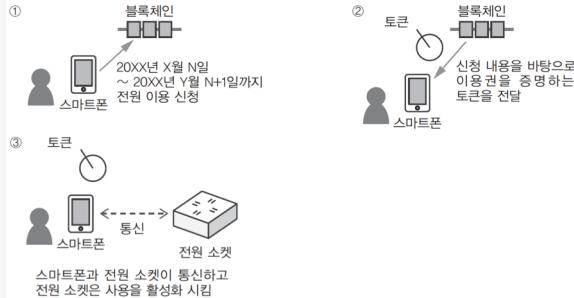
Welcome to the digital vault of the future.

Everledger is a global startup that uses the best of emerging technology including blockchain, smart contracts and machine vision to assist in the reduction of risk and fraud for banks, insurers and open marketplaces.

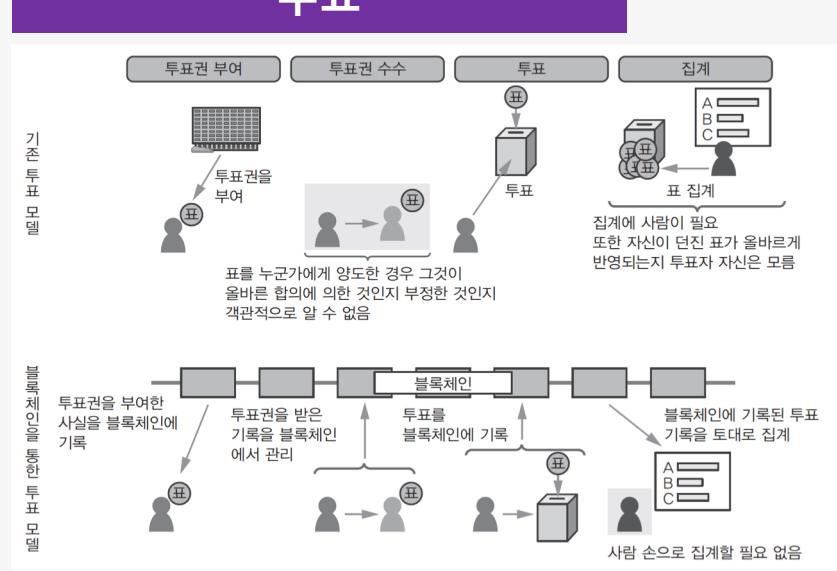
FIND OUT MORE

# 블록체인의 응용 – 신규 서비스

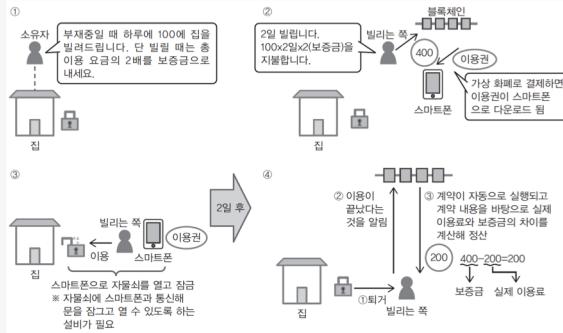
## IoT – Nayuta 전원 소켓



## 투표



## IoT – Slock 임대/판매/공유



감사합니다.

# Gas cost

- 21000 gas는 모든 트랜잭션의 기본 요금. 이 값은 서명에서 발신자 주소를 복원하는 elliptic curve 연산과 트랜잭션의 저장을 위한 디스크와 네트워크 비용임
- 트랜잭션은 무제한의 데이터를 가질 수 있음. 데이터에 대한 비용은 값이 0인 바이트의 경우 4 gas, 그렇지 않은 경우 68gas.
- SSTORE 연산 (값을 계정의 스토리지에 보관)은
  - 0인 값을 0이 아닌 값으로 변경할 때 20000gas
  - 0에서 0으로, 또는 0이 아닌 값에서 0이 아닌 값으로 변경시 5000gas
  - 0이 아닌 값에서 0으로 변경시 5000gas
  - 성공적으로 트랜잭션 실행이 종료되면 20000gas 환불 (환불은 사용한 전체 gas의 50% 캡을 가지고 있음. 트랜잭션의 전체 소모 gas가 30,000이면 15,000이 환불 한계)
- 컨트랙트가 제공하는 데이터의 메시지에는 과금 없음
- 메모리는 무한히 확장 가능한 배열임. 하지만 32바이트당 1gas가 소모됨
- 인자의 값에 따라 연산 시간이 크게 달라지는 opcode의 경우 (예: EXP) 인자의 값에 따라 소모되는 gas가 달라짐