# 블록체인 기술의 이해와 응용
# (블록체인패러다임)

2017년 12월 1일

동국대학교 국제정보보호대학원 블록체인연구센터 박성준 센터장
( deb_blockchain@naver.com)

**오늘을 이야기 하는 것이 아님**

**내일을 이야기 하는 것임**

**그러나 모레를 이야기 하는 것은 아님**

***조속히 준비해야 함***

## 미래를 위한 핵심 기술

## “블록체인” & “인공지능”

농업사회 -> 공업사회 -> 정보사회 -> 지식사회 -> 지능사회

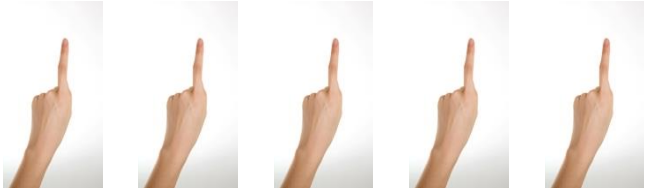
제1의 인터넷 인프라 -> 제2의 인터넷(블록체인) 인프라

# 탭스콧 부자 : 블록체인혁명
# (인공지능을 뛰어넘는 위대한 기술)

# 새로운 세상 = 블록체인 세상

블록체인 정의 및 개념
새로운 혁신(혁명)
컴플라이너스
법/제도/규제


성능 / 메모리
투기/투자
정보보호
거품



# 주요 내용

## 블록체인패러다임

- **개요** — 탄생배경 / 목적
- **비트코인과 이더리움** — 비트코인 / 이더리움
- **블록체인이란?** — 개념 / 정의 / 본질 / 기능
- **패러다임** — 사이버패러다임 / 블록체인패러다임
- **블록체인 분류** — 퍼블릿 / 프라이빗
- **블록체인 생태계** — 블록체인 1.0 / 2.0 / 3.0
- **법·제도** — 블록체인기본법 / 암호화폐법 / 스마트계약법
- **미래 세상** — 미래의 핵심인프라

# 개요

# *신뢰(Trust) 확보 모델*
# *제3의 신뢰기관, 중앙집중, 신뢰 중재자 등*

## □ 비트코인 탄생 배경

○ 현행 화폐시스템의 문제점

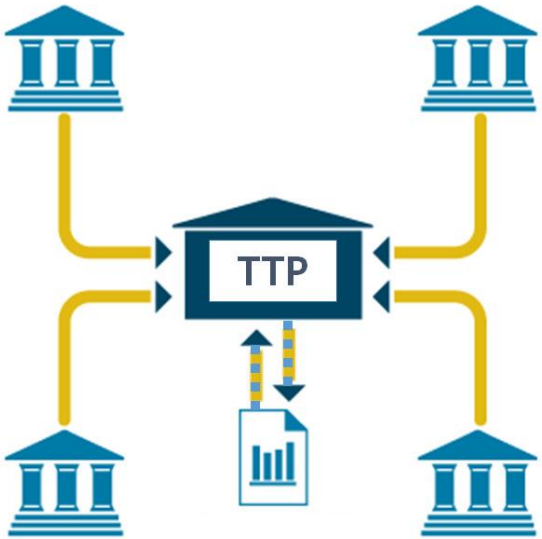
○ 중앙통제방식 = 신뢰기관 방식 => 역사적 문제점(신뢰성 담보 문제)

## □ 비트코인 개념의 확대 = 블록체인(신뢰 확보 기술)

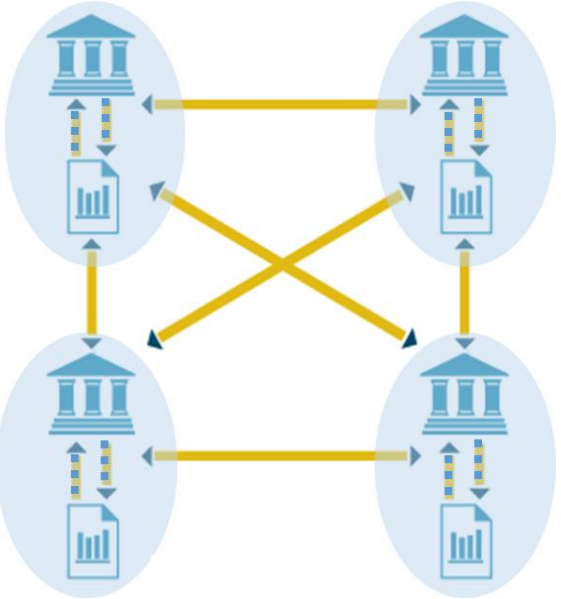
○ 정보의 집중 / 독점 = 신뢰의 독점

○ 정보의 불균형 = 신뢰 확보의 불균형

# P2P 신뢰(Trust) 확보 모델
## 제3의 신뢰기관, 중앙집중, 신뢰 중재자 개입 없이 신뢰성을 확보하는 모델



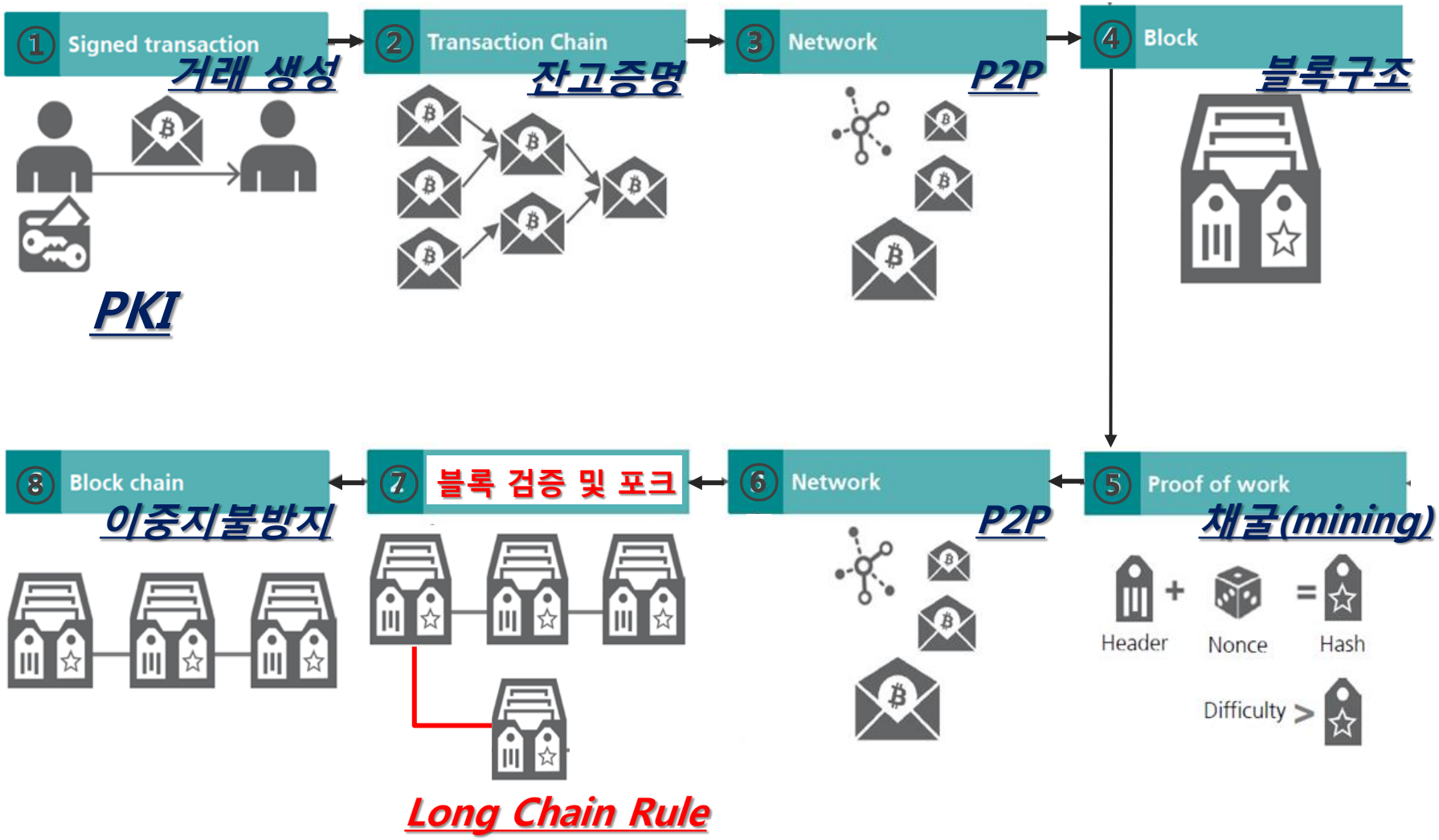

현재 신뢰 확보 모델



P2P 신뢰 확보 모델

# 비트코인과 이더리움

# 전체 흐름도




**비트코인은 블록체인 기술을 활용한 최초의 성공서비스**

# 계정 : 비트코인 지갑의 공개키/비밀키



지갑의 주소 : 공개키 또는 공개키의 해쉬값

# 거래(Transaction) 생성 및 종류

Alice

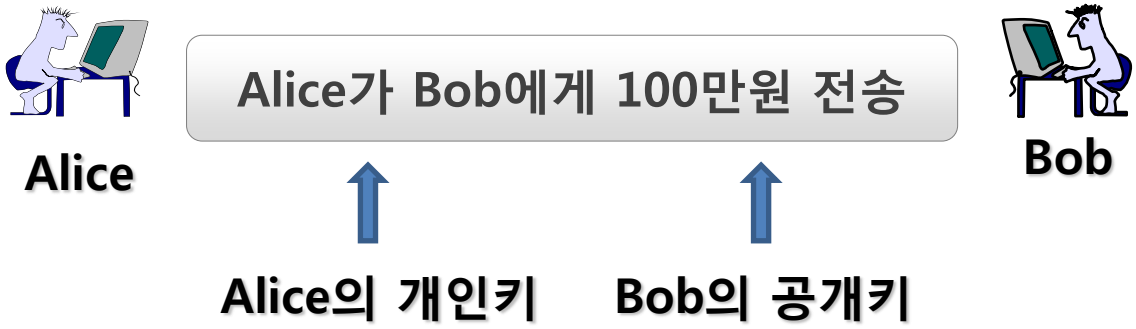
Alice가 Bob에게 100만원 전송

Bob

Alice의 개인키

Bob의 공개키

- **P2PKH** — Pay-To-Public-Key-Hash
- **P2PK** — Pay-To-Public-Key
- **다중서명** — Multi-Signature
- **P2SH** — Pay-To-Script-Hash
- ★ **Data Output** — OP_RETURN




**잔고증명 문제 발생(P2P임을 상기)**

Alice가 Bob에게 100만원을 보내기 위해서는 백만원의 돈을 소유하고 있어야 함 -> 어떻게 확인시켜 줄 수 있는가?

**잔고증명**

Alice는 누군가에게 100만원을 받았다는 것을 증명하면 됨

***현재의 화폐시스템에서는 은행 => P2P에서는 누가?***

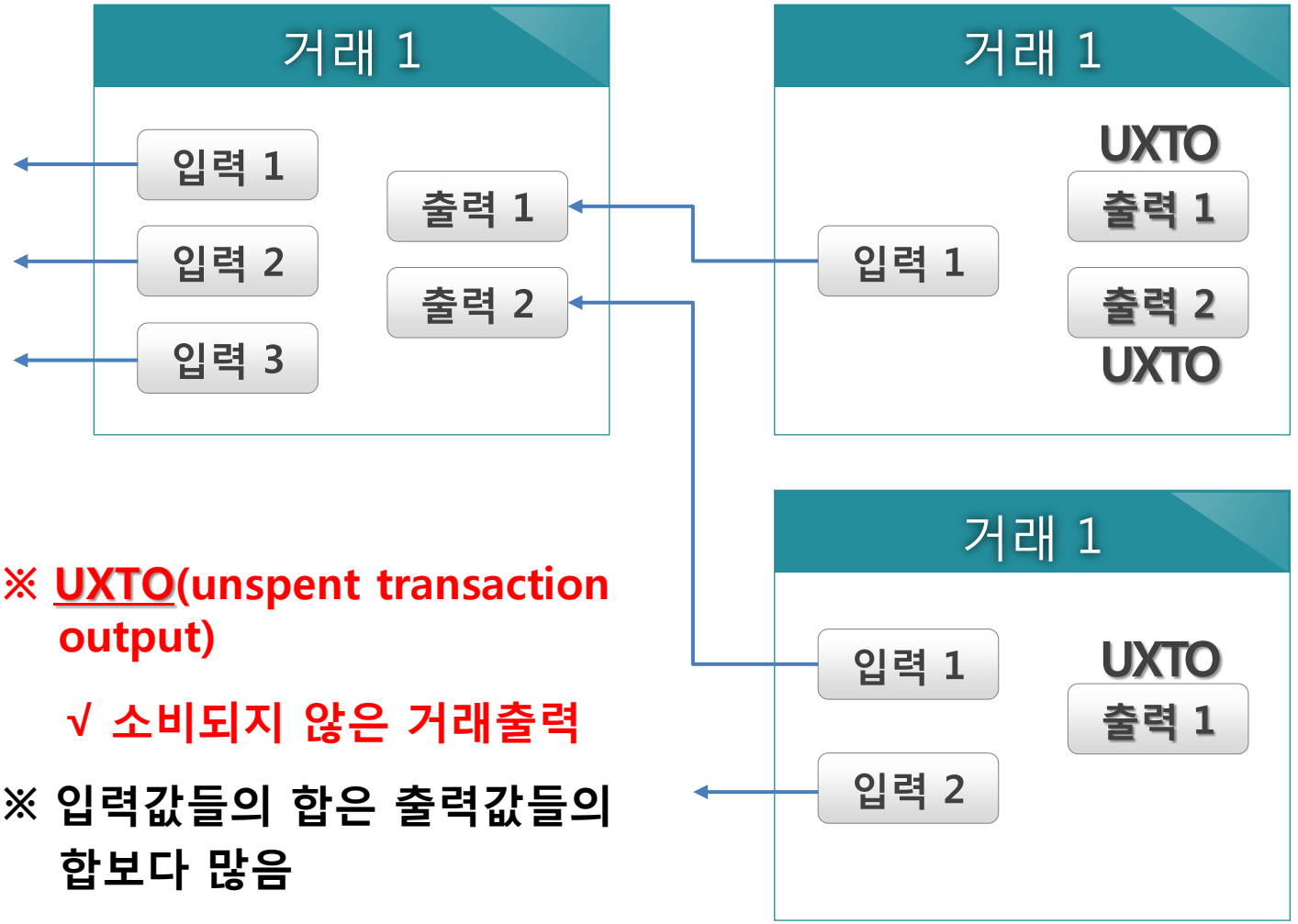

코인베이스 거래(Coinbase Transaction)

바트코인 화폐

디지털서명의 체인 또는 거래들의 체인

an electronic coin as a chain of digital signatures

# 일반적 구조(UXTO)

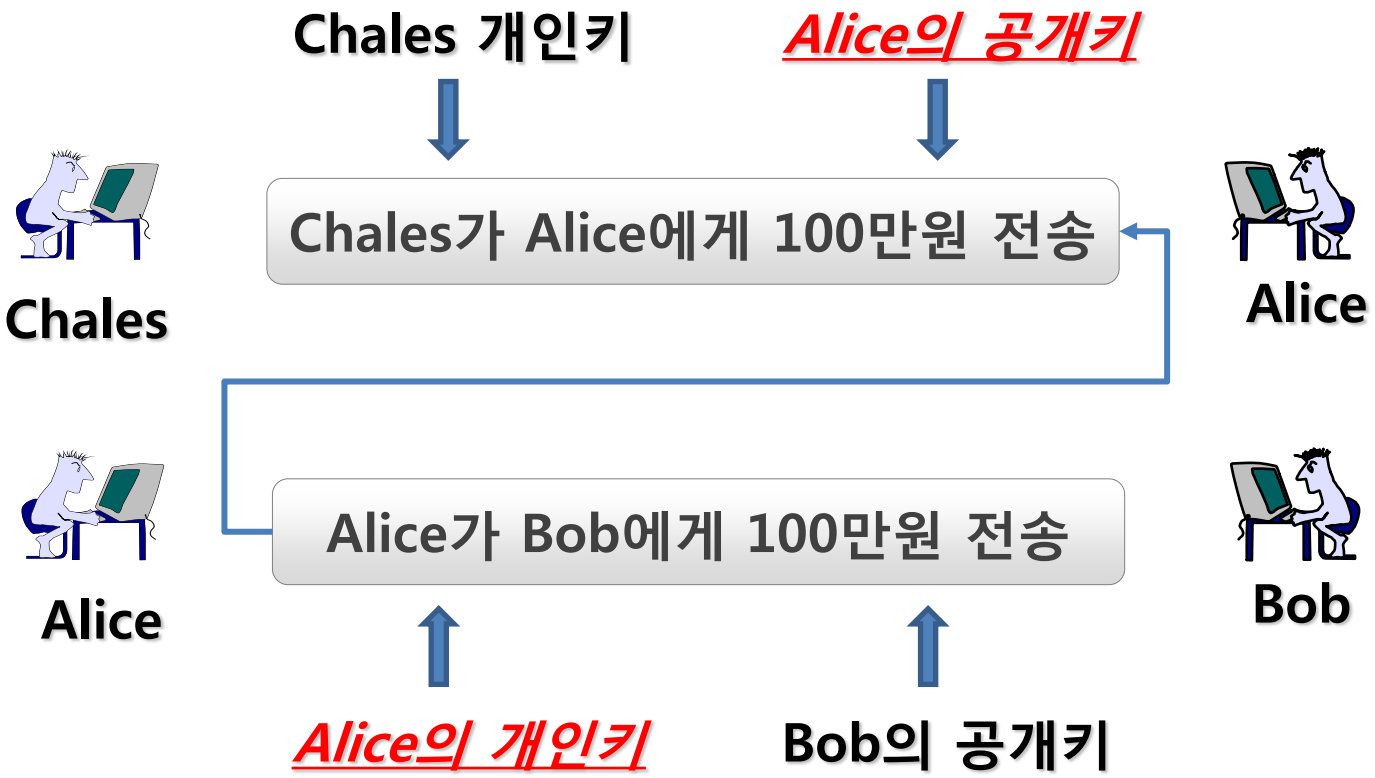



※ UXTO(unspent transaction output)

√ 소비되지 않은 거래출력

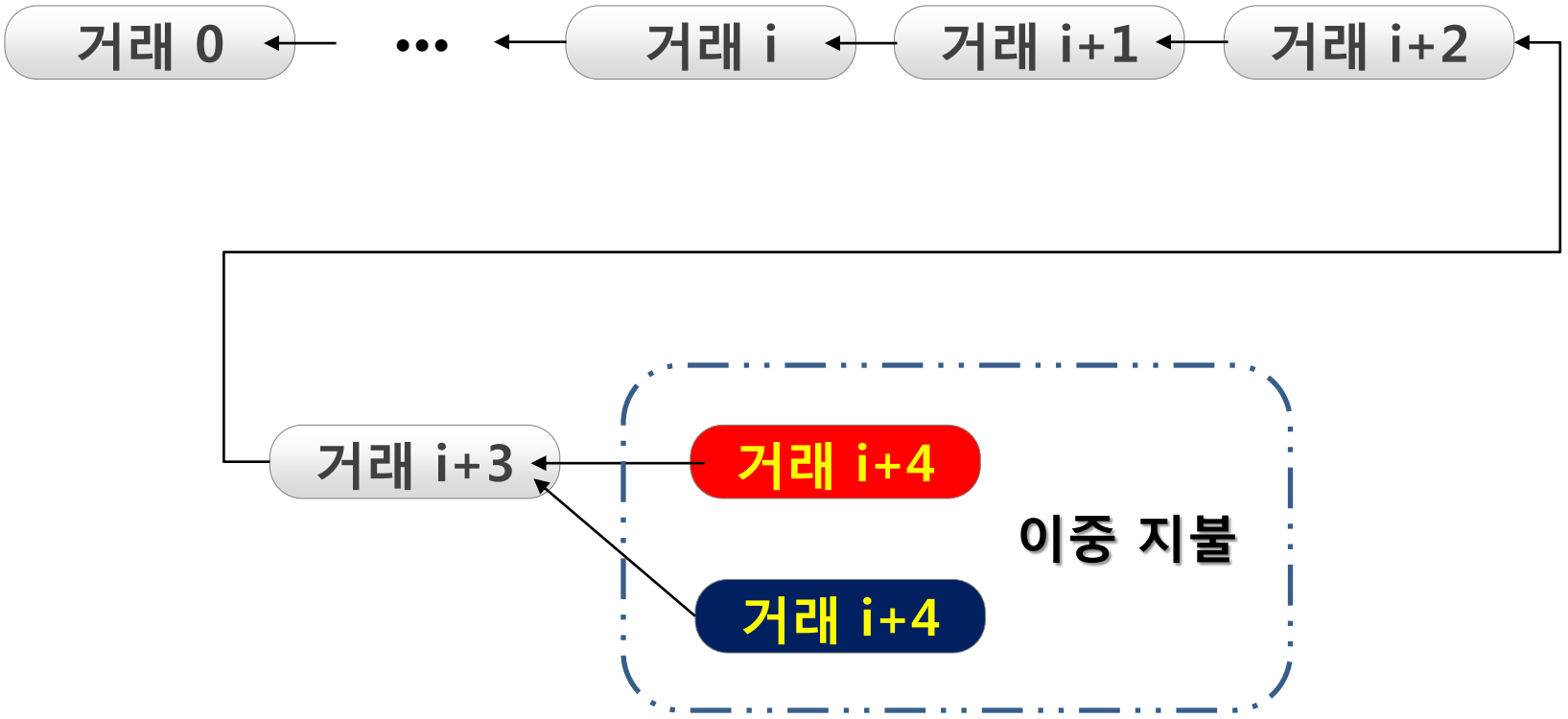
※ 입력값들의 합은 출력값들의 합보다 많음

# 거래 검증




**검증과정**

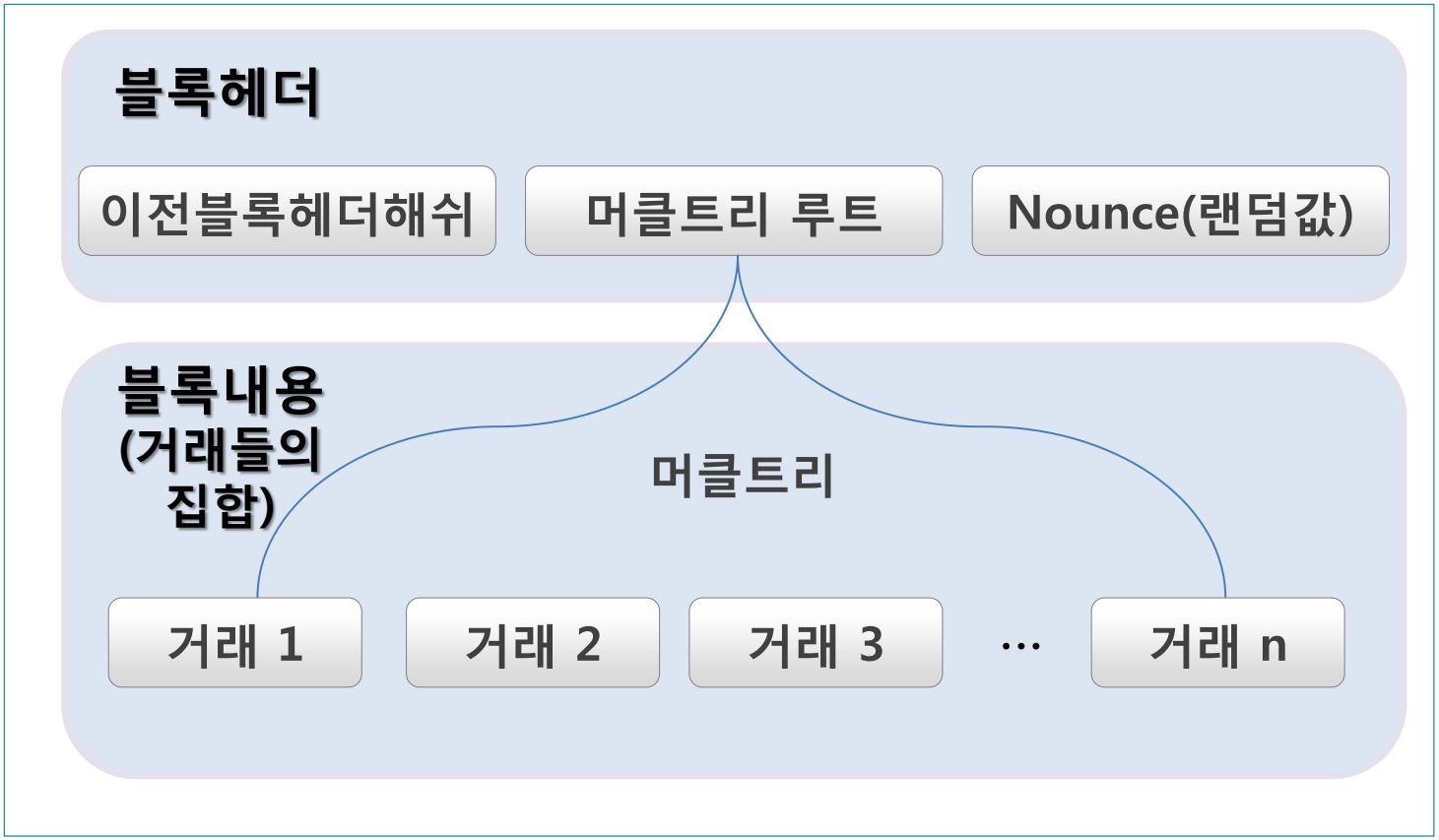
(1) Alice의 서명 검증
(2) 이전거래 존재여부 검증(해쉬값)
(3) 입력값의 합 ≥ 출력값의 합

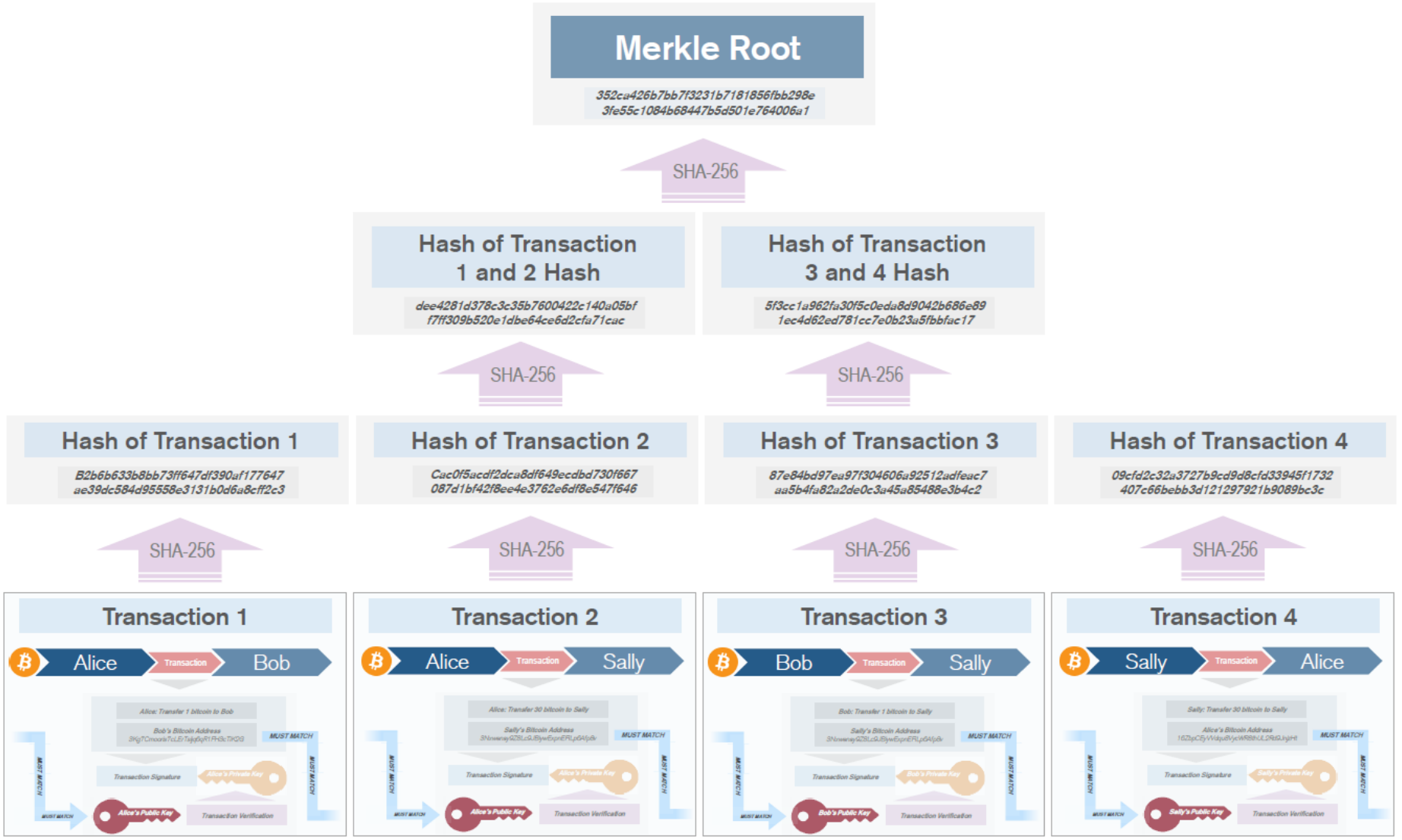



***거래(Transaction) 관점에서는 해결 방안 없음***

블록

√ 이중 지불 문제 해결
√ 블록헤더와 블록내용으로 구성
√ 블록체인의 구성 요소






※출처 : CREDIT SUISSE, Europe/United Kingdom Equity Research Technology, 2016년 8월

**채굴** : **이중사용방지를 위해 블록에 특별한 성질을 부여함**

※ 블록헤더의 해쉬값이 주어진 목표값보다 작은 랜덤값을 찾음

**H(이전블록헤더해쉬값, 머클트리루트, 랜덤값) < TV(Target Value)**

위의 계산에서 해쉬값이 목표값(TV : Target Value)보다 적어지는 **랜덤값을 찾는 과정을 채굴이라고 함**

***채굴 과정***

H(고정값, 고정값, 0) = 200 >(목표값 : 100)

H(고정값, 고정값, 1) = 102 >(목표값 : 100)

H(고정값, 고정값, 2) = 203 >(목표값 : 100)

⋮

H(고정값, 고정값, **97**) = 99 <(목표값 : 100)

***채굴 성공***

# 채굴(Mining) 및 보상_2

랜덤값을 찾는 과정을 **작업증명(PoW : Proof of Work)**이라 하며
비트코인은 평균적으로 10분이 소요되게 목표값을 정함

**보상** : 채굴에 대한 보상

채굴에 성공한 채굴자에게 보상

① 화폐발행(12.5BTC) + ② 거래수수료

**※ 채굴은 통화공급 역할(통화발행)**

비트코인의 총 통화량

① 화폐 발행량이 평균 4년마다 ½로 감소

② 총 통화량 : 2,100만 BTC(2140년 종료 예정)

***채굴이란 비트코인 화폐시스템의 안전성을 확보하는 과정***

**블록검증** : 블록의 해쉬값을 검증함으로서 채굴된 블록 검증

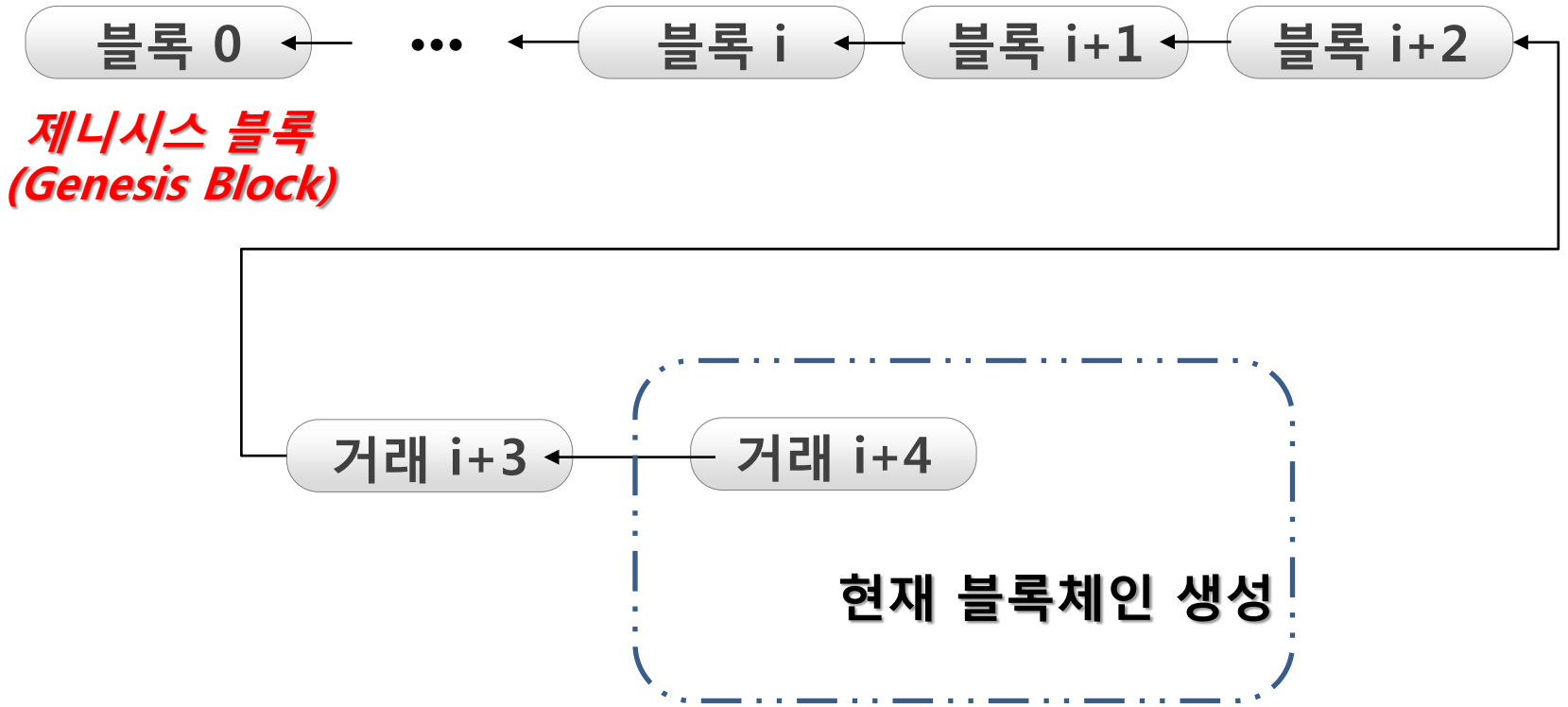
**검증과정**

(1) 이전블록 존재여부 검증(이전블록헤더해쉬값)

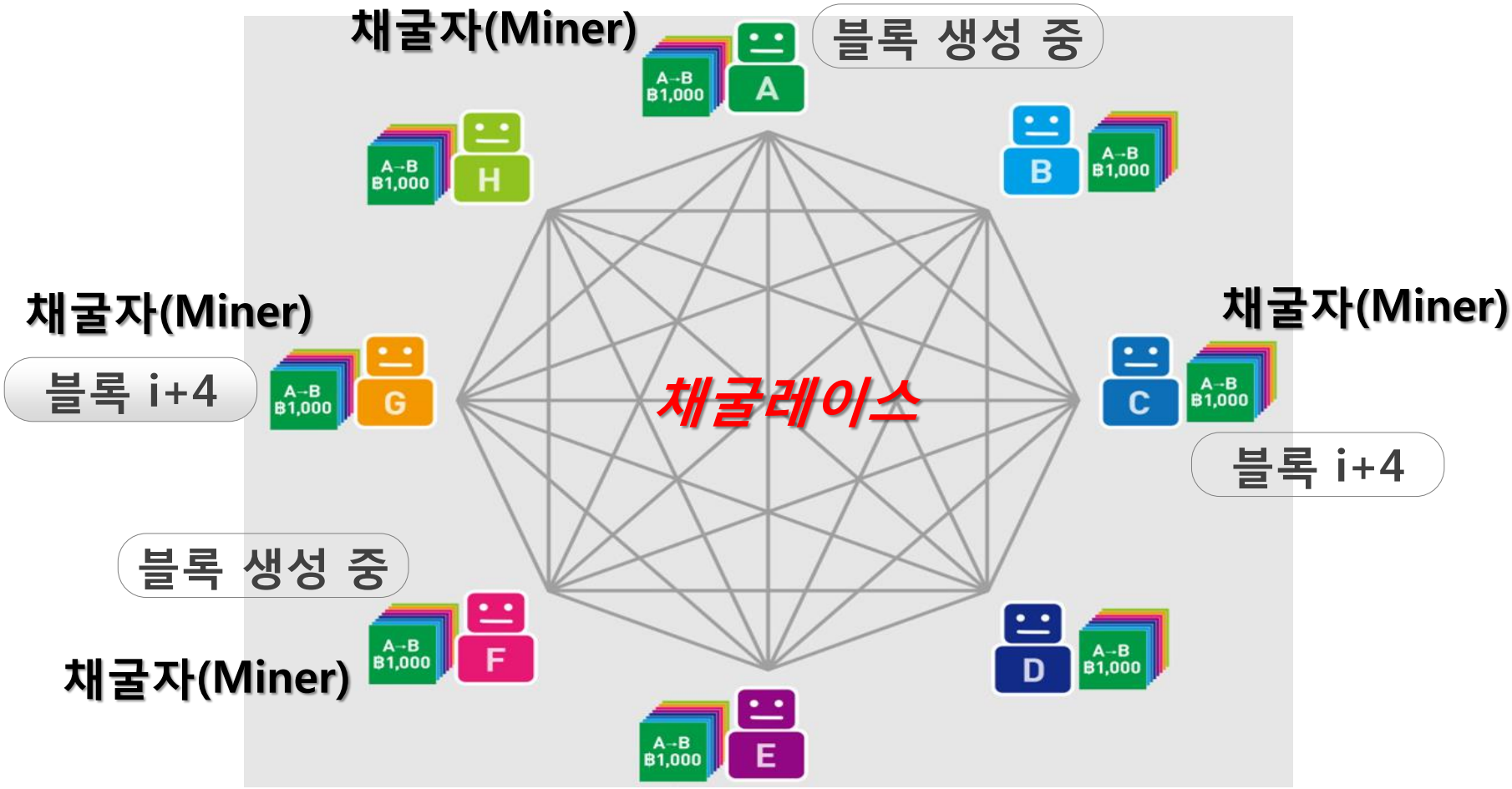
(2) 작업증명 검증

H(이전블록헤더해쉬값, 머클트리루트, 랜덤값)
< TV(Target Value)

**블록체인** : 블록이 검증되면 블록체인을 업데이트

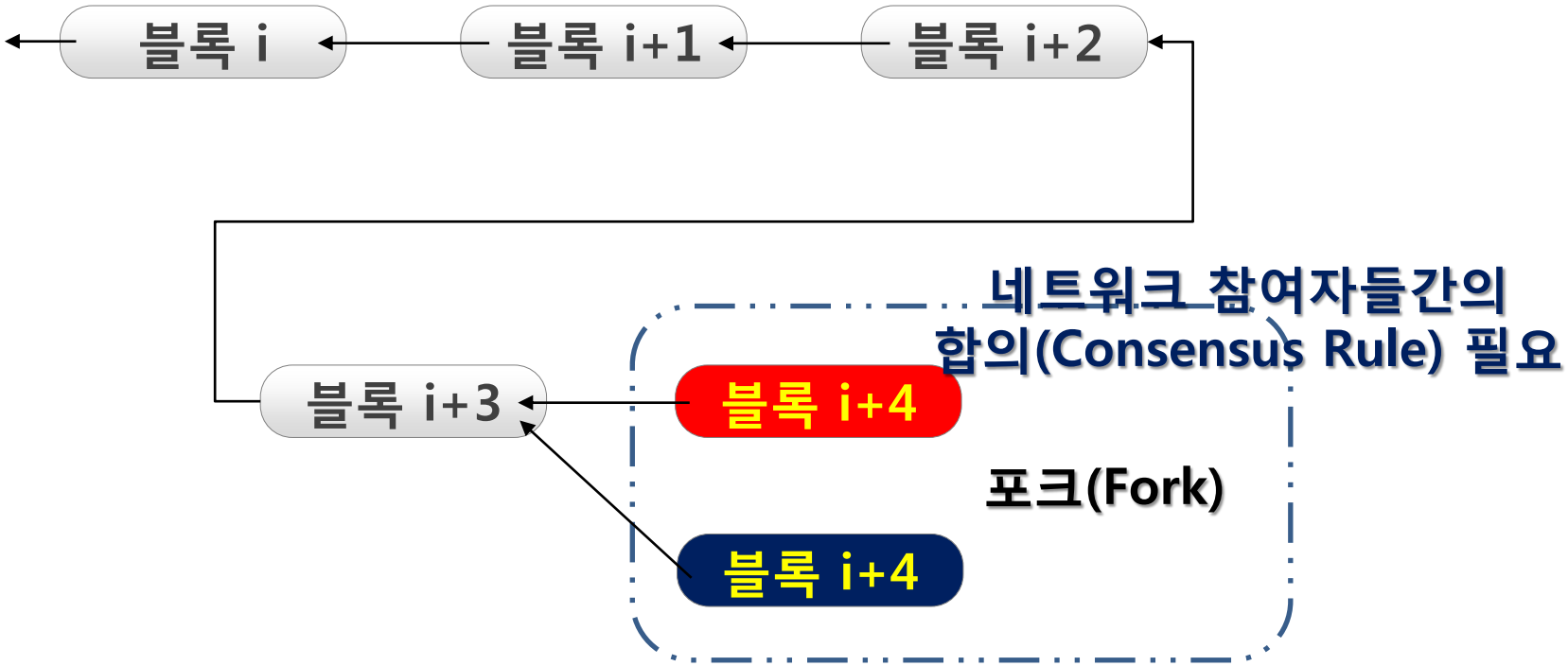


**포크 발생 이유** : P2P 네트워크에서 모든 참여자들이 **독립적으로 채굴**



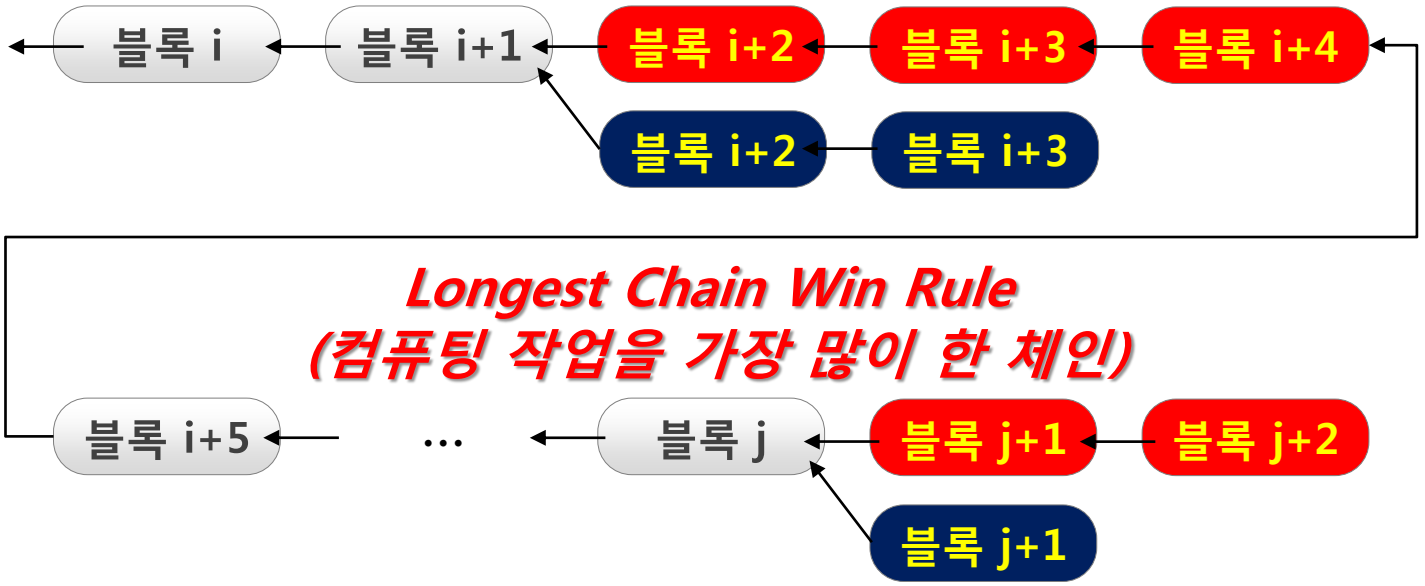

***비트코인 공격시에도 해커가 발생(이중 사용!!!)***

**포크** : 동일한 번호의 블록이 생성되는 현상




***분기(Fork)되는 블록체인 중 어떤 것을 선택할 것인가?***

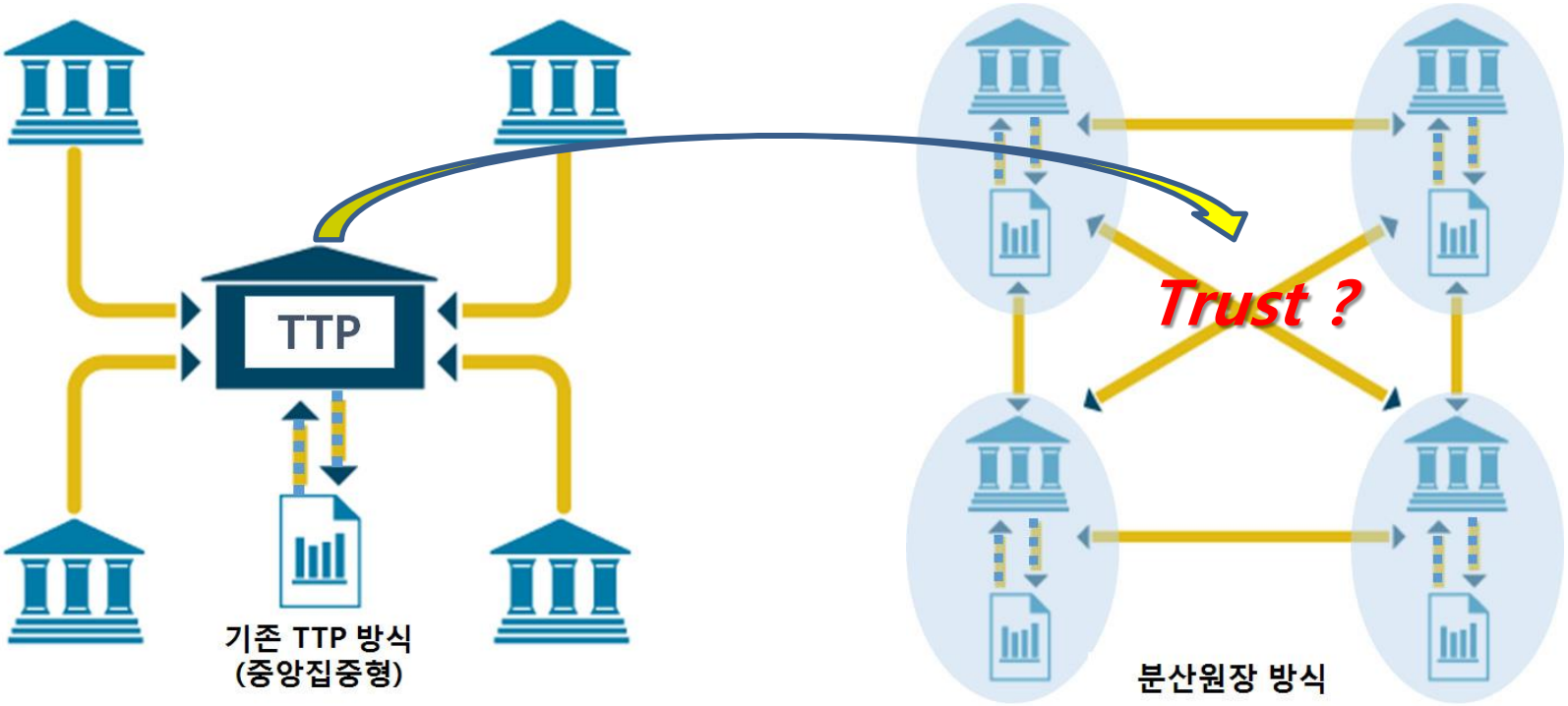
**긴체인(Longest Chain) 선택** : 번호가 긴 체인 선택




❖ Longest Chain : 길이가 가장 큰 체인


블록체인(Blockchain)
이중거래방지
합의 알고리즘 + 보상체계(암호화폐)
채굴
(Mining)
거래(Transaction)
잔고 증명(거래체인)
거래의 구성 및 연결(chain)
5가지 방법
계정(Account)
거래의 주체
공개키암호시스템: 비밀키, 공개키

## 비트코인은 분산화된 P2P 화폐시스템을 블록체인 개념으로 구현한 1번째 성공사례




## 블록체인 : P2P 신뢰네트워크

# 비트코인 한계

Alice

Alice가 Bob에게 100만원 전송

(Programable : S/W(script))

Bob

## 튜링 불완전성 (Turing-incompleteness)

- ✓ 하고 싶은 기능을 다 구현할 수 있는가?
- ✓ 해킹방지를 위해 제한함 (주로 DDoS 공격 방지)

## 제한적 상태 (Lack of state)

- ✓ 표현하고 싶은 상황을 다 표현할 수 있는가?
- ✓ 2가지 경우만 표현 (사용 또는 미사용)

## 거래 생성 주체

- ✓ 사람

## 블록체인 세상 구현

√ 다양한 블록체인 기반 서비스 구현을 위해 비트코인 기반 기술인 블록체인 기능의 확대가 필요
√ 블록체인 기술의 일반화가 필요함

## 이더리움 탄생

√ 비트코인의 한계점을 극복하고 다양한 응용서비스가 가능하도록 ***블록체인 기술의 일반화***

Alice

Alice가 Bob에게 100만원 전송

(Programable : S/W(script))

Bob

**튜링 완전성 (Turing-completeness)**

✓ 하고 싶은 기능을 다 구현할 수 있도록 함

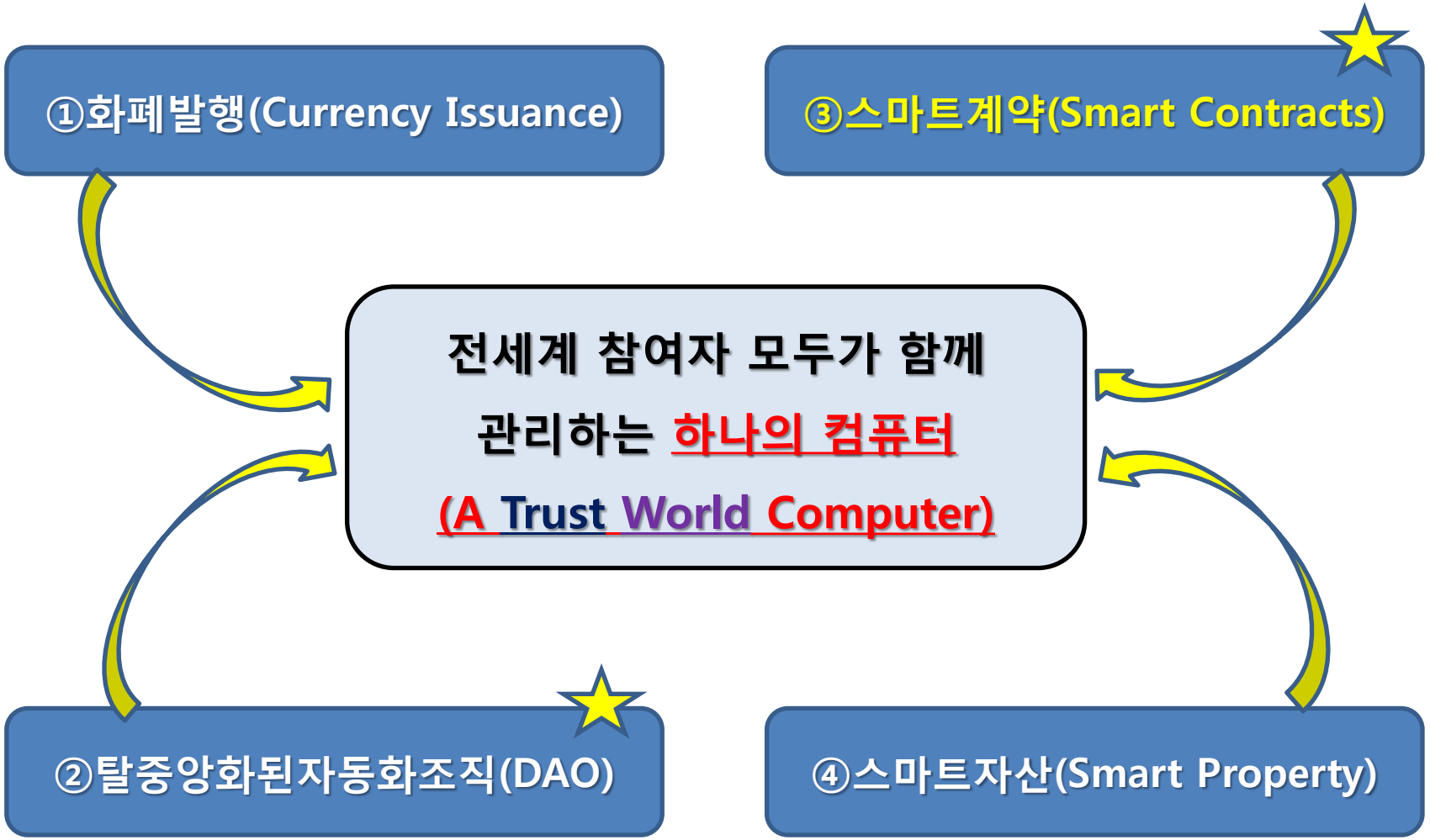
**컴퓨터**

✓ 다양한 표현 가능

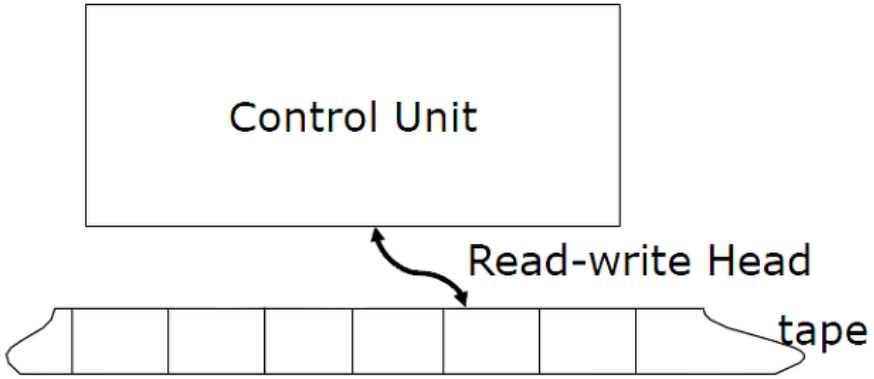
**거래 생성 주체**

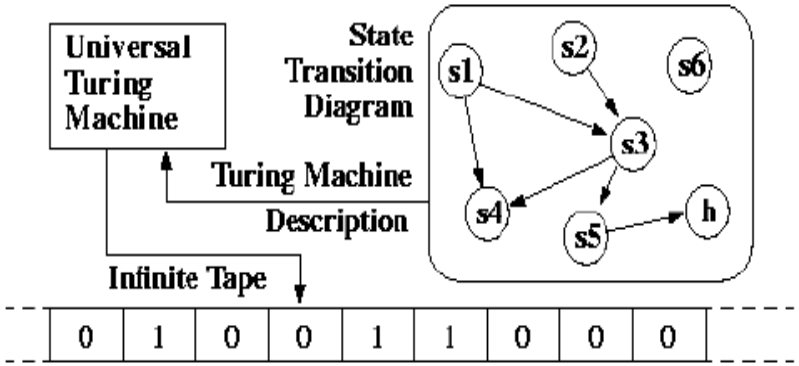
✓ 사람
✓ S/W

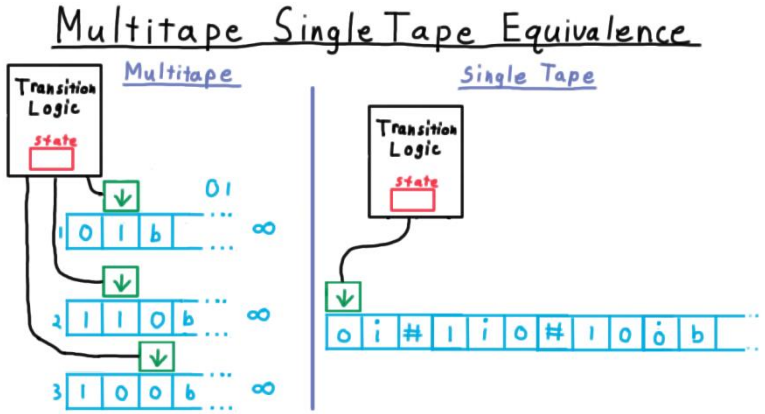
***비트코인의 4가지 미비점을 모두 극복하여***
***모든 응용서비스가 가능한 공통의 블록체인플랫폼 개발***

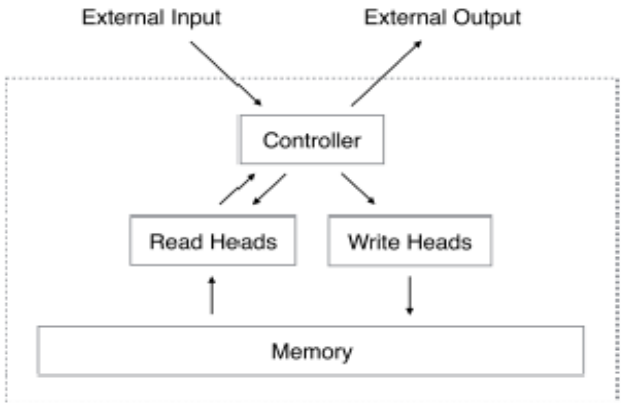


# 컴퓨터 : 메모리관리시스템으로 추상화(Turing Machine)

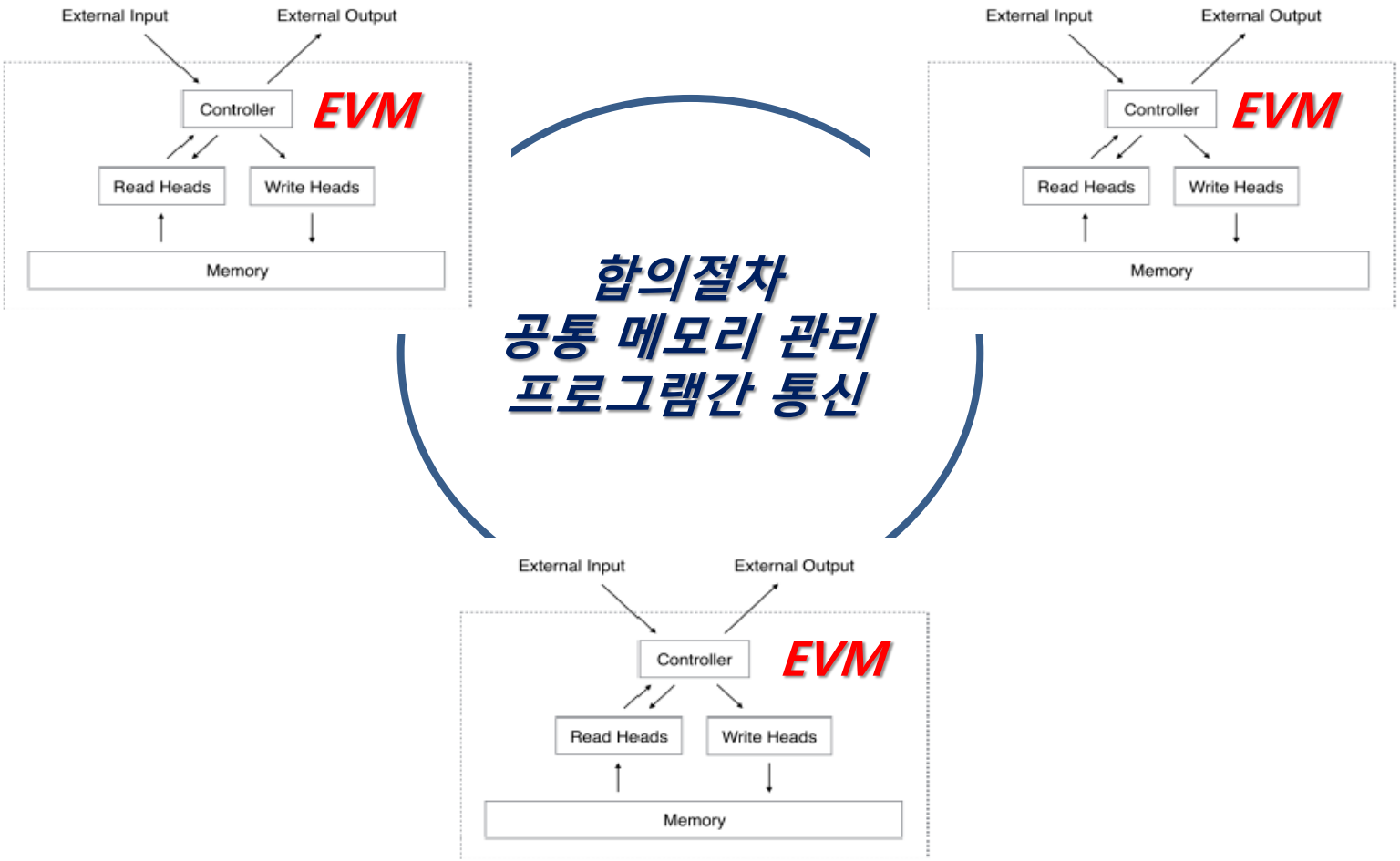


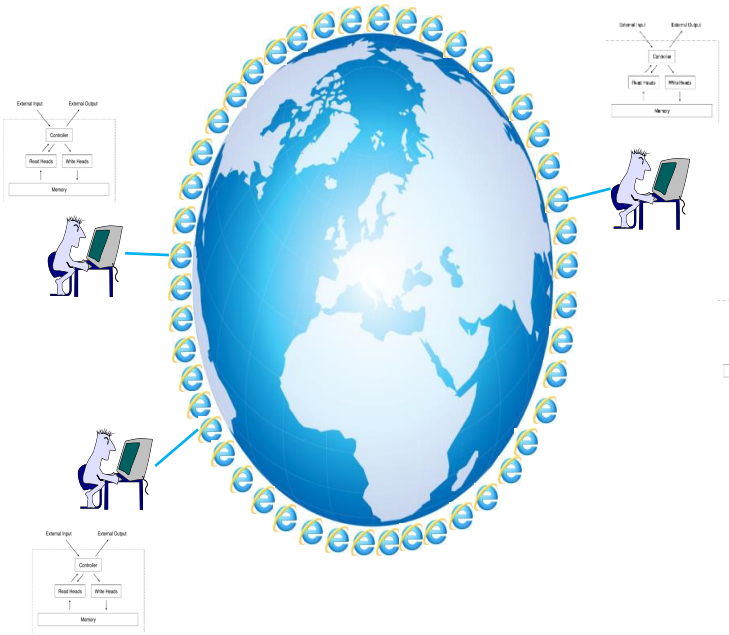



# 이더리움 : 확장된 블록체인(비트코인 블록체인 + 컴퓨터)



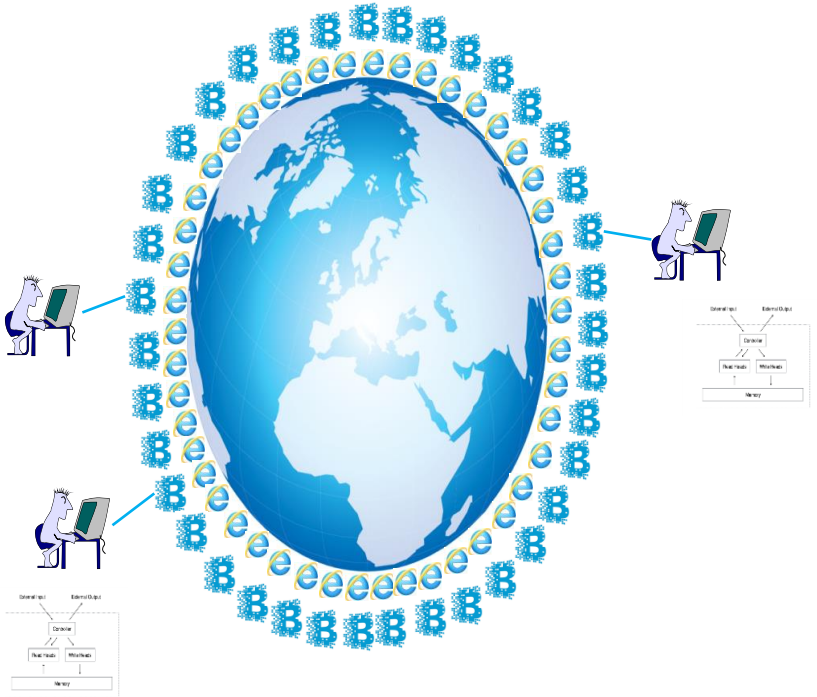
# *이더리움 : 전세계 참여자 모두가 함께 관리하는 하나의 컴퓨터*

*인터넷에 연결된 모든 컴퓨터는*
*독립 주체들임*

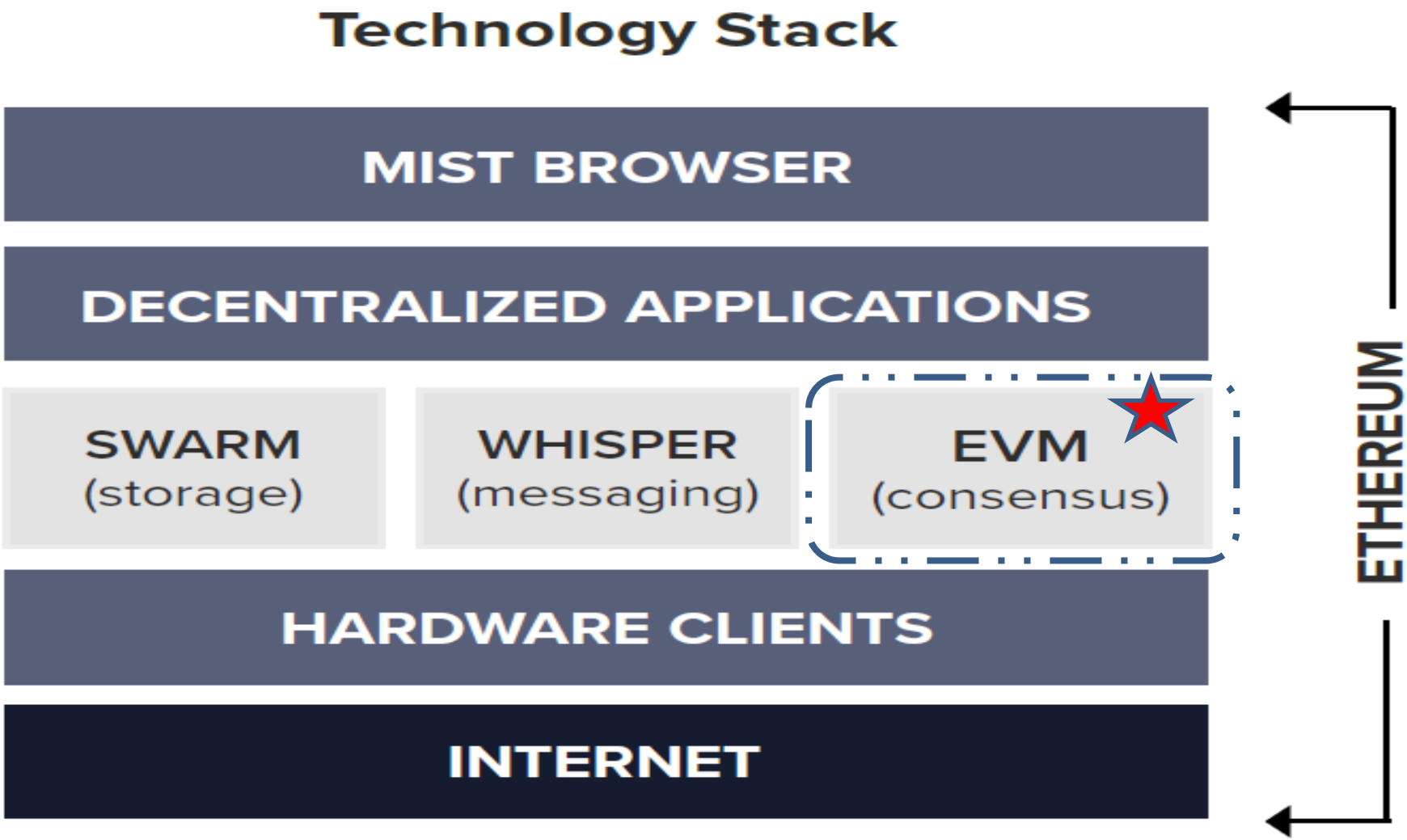


*인터넷 세상*

*이더리움에 연결된 모든 컴퓨터는*
*이더리움 컴퓨터의 객체(부분)*

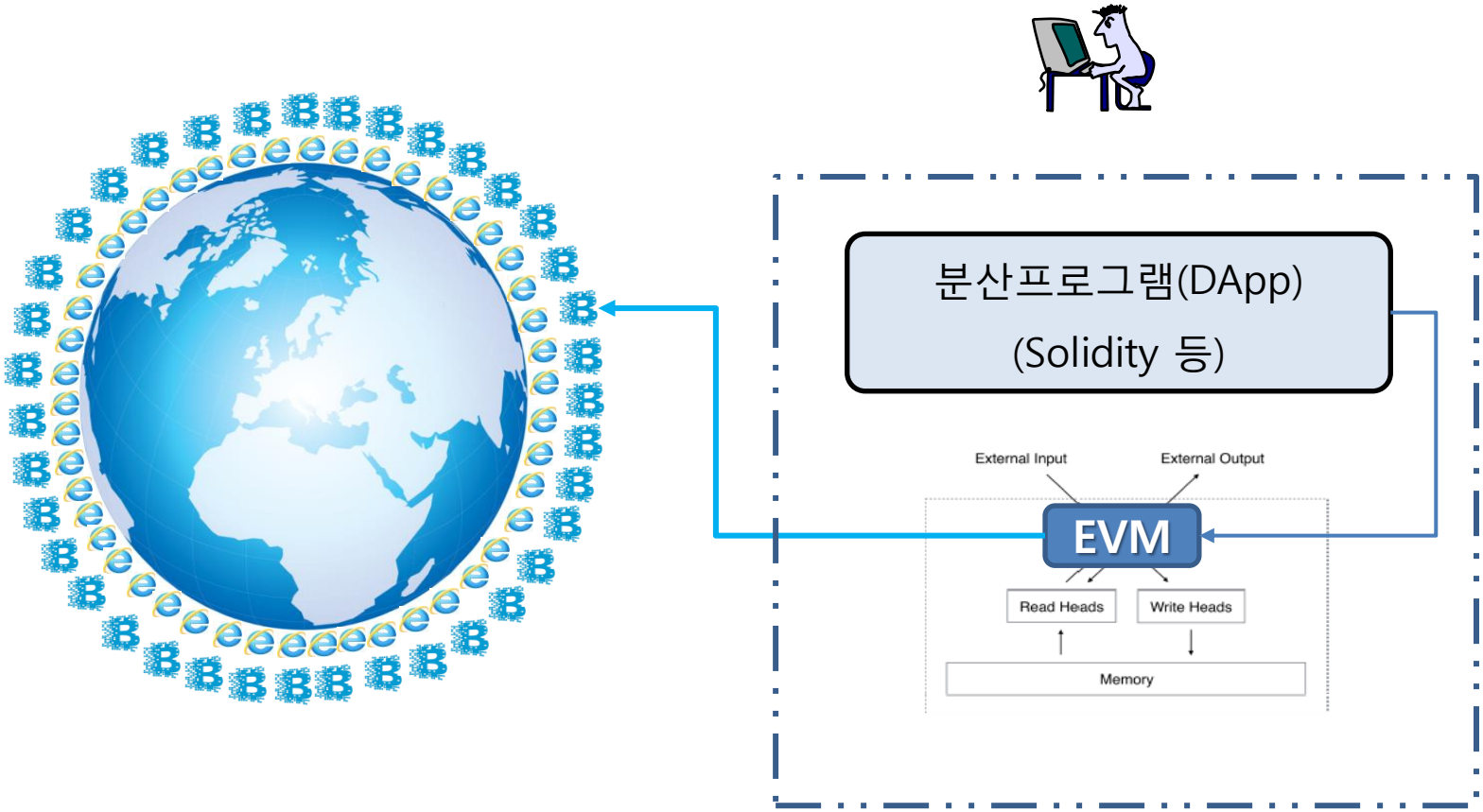


*블록체인 세상*




**참조 : 지속적으로 업데이트 등 진행 중**

# 이더리움 언어(컴퓨터 언어)



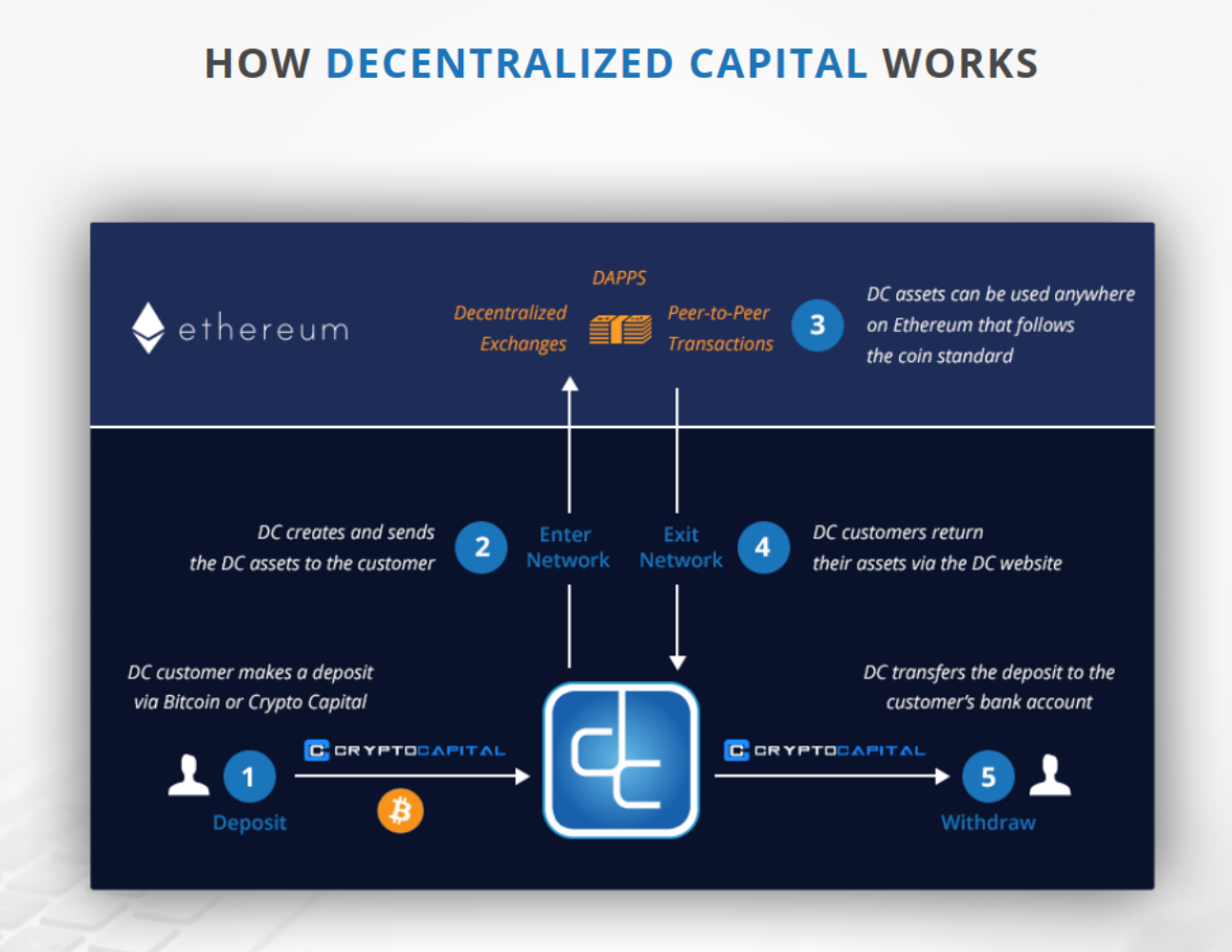
# 이더리움 응용 서비스


http://dapps.ethercasts.com/
이더리움 : 네이버 통합검색
State of the Dapps
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
국세청 홈택스
TERAROSA COFFEE
문화콘텐츠닷컴 - 문화원...
디지털 폰트의 글로벌 리...
웹 조각 갤러리
STATE OF THE ĐAPPS
Search
EtherGit
Miles Albert
Verity
Matt Goldenberg
Everex
Chainy.Link
SmartToken
Nikita Dubrovin
PixelMap
Ken Erwin
Dragoo
Gabriele Rigo
Time Clock
Daniel Moscufo
AuctionHouse
Doug Petkanics, Eric Tang
Project Entropy
Joran Kikke
BitVault
Nikita Dubrovin
Etherization
Vedran Kajic
smart-lease
Marie
Costring
Manuel
KeyPal
Paul Hensel
Zonafide
Paul Worrall
ETH Notifier
U-Zyn Chua
File Storage Marketpl...
Andriian Chestnykh
etherslots.win
Ignas Mangevicius and DEV. team
ReGa
Sergei Sevriugin
godzillion
Rodrigo Sainz
Decentralized Ether...
Yaron Velner
Ethrex
Ethrex
BlockCDN
Tony Long
SafeEther
Sergey Leschenko
PriceGeth
Shayan Eskandari
Velocity Options Cont...
Shayan Eskandari
EtherLovers
Lukas
TokenCard
Monolith Studio
Status
Jarrad Hope
Tinypay
MustWin.com
Bitualcard
John Lee
RockPaperScissors
HashFairGames
TheEthereumLottery
HashFairGames
Donamin
Zoltán Tápi
emojillionaire
Matus Lestan
Interdimensional Juke...
controtie
blockchainmail.net
Eamonn Hynes
earthlottery.com
Eamonn Hynes
GrünStromJeton
Thorsten Zoerner
The Rudimental
Troy Murray
Community-Currency
Rogelio Segovia
Lottereo
Daniel Mermelstein / Glynn Bird
Free Ftopia
Phil
Pray4Prey
Julia Altenried, Stefan Hoeller
DTE
Yampi
YouChoo
Billy Williams
Crystal Mines
Yampi
Transaction Relay
iuri matias
Melonport
Reto Trinkler, Mona El Isa
FlightAssure
Ai-London
COAKT
Nick Barba, Kevin Kriss
War On Ether
Kobi Gurkan
Reputation Manager
James Sangalli
PredictionToken
Etherboost
OpenRep
James Sangalli
Cetas
Algorythmix
Ethereum Lottery
iFA
Etherandom
Etherandom
Etherplay
wighawag
etherfaces
Sridhar
FarmShare
William E Bodell III
ARK
MonkeysCage
Decentralized Capital
Alex Wearn
OutcomeCoin
Etherboost
Hash DB
Metaspace
Flight Delay Insurance
Christoph Mussenbrock
FirstBlood.io
Joe & Zack
Smart Identity
Deloitte
Everex Transfer
Everex
Ethplorer
Everex
Raiden Network
brainbot technologies
SafeContracts - TREX
Rocky Fikki
HydraChain
brainbot technologies
Rex
Stephen King & Russell McLernon
TheGrid
Vasco Yannic Lange
Sustainy
Jonathan Bean
otlw-forum
otlw
KingOfTheEtherThrone
Kieran Elby
Sell ETC Safely
Viktor Novak
The-Pitts-Circus-Famil...
Ken Evil
Etherplan
Donald McIntyre
tax spendings
siddharth patel
Microtick
Mark Jackson
EtherDelta
Etherboost

# 이더리움 응용 서비스 예


Decentralized Capital
HOME
FAQ
ABOUT US
SIGN UP
LOGIN
Government Currencies
on the Ethereum Blockchain
PURCHASE DC ASSETS

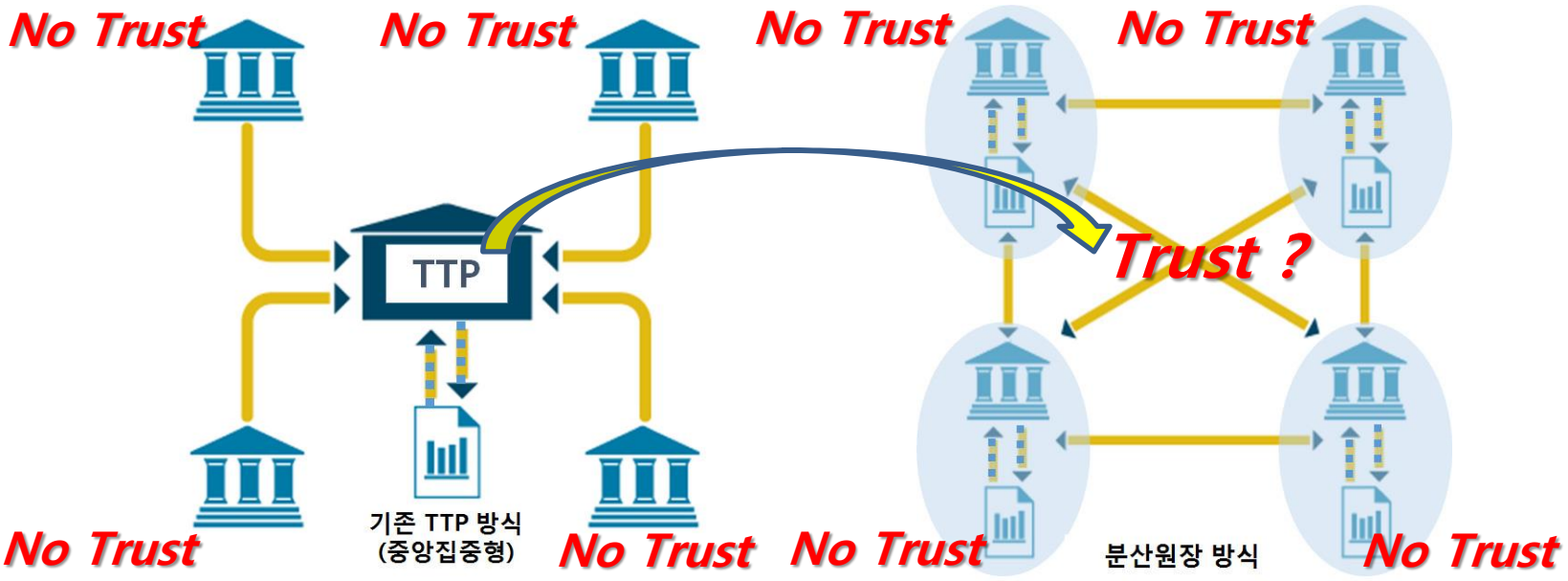
# 이더리움 응용 서비스 예


HOW DECENTRALIZED CAPITAL WORKS
ethereum
DAPPS
Decentralized Exchanges
Peer-to-Peer Transactions
3
DC assets can be used anywhere on Ethereum that follows the coin standard
DC creates and sends the DC assets to the customer
2
Enter Network
Exit Network
4
DC customers return their assets via the DC website
DC customer makes a deposit via Bitcoin or Crypto Capital
DC transfers the deposit to the customer's bank account
CRYPTOCAPITAL
CRYPTOCAPITAL
1
Deposit
5
Withdraw

# 블록체인이란?

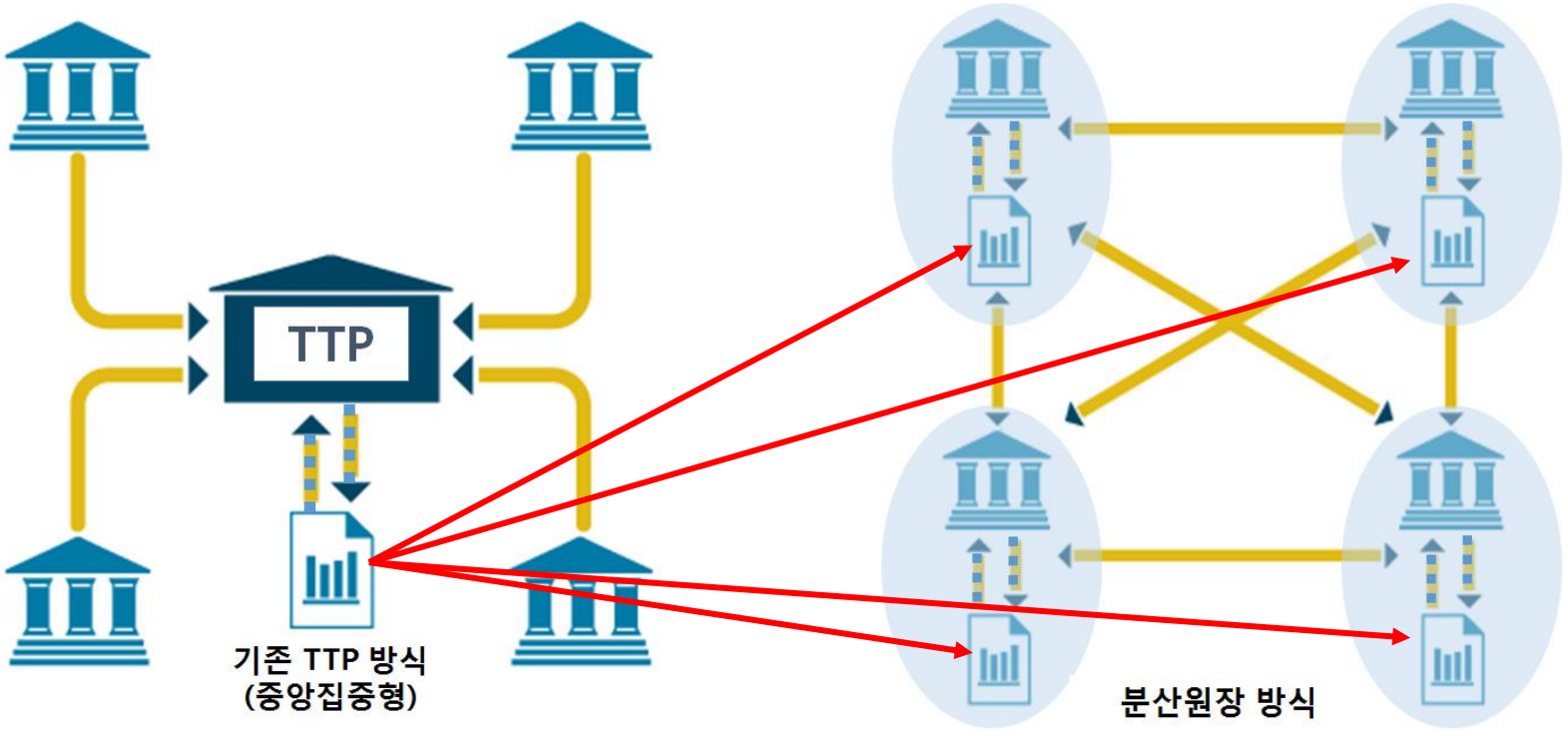
**블록체인**

분산원장(Distributed Ledger) 기술은 거래정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 P2P(Peer-to-Peer)네트워크에 분산하여 참가자가 ***공동으로 기록하고 관리하는 기술을*** 의미함(한국은행)




※ TTP : Trust Third Party의 약자로 제3의 신뢰기관

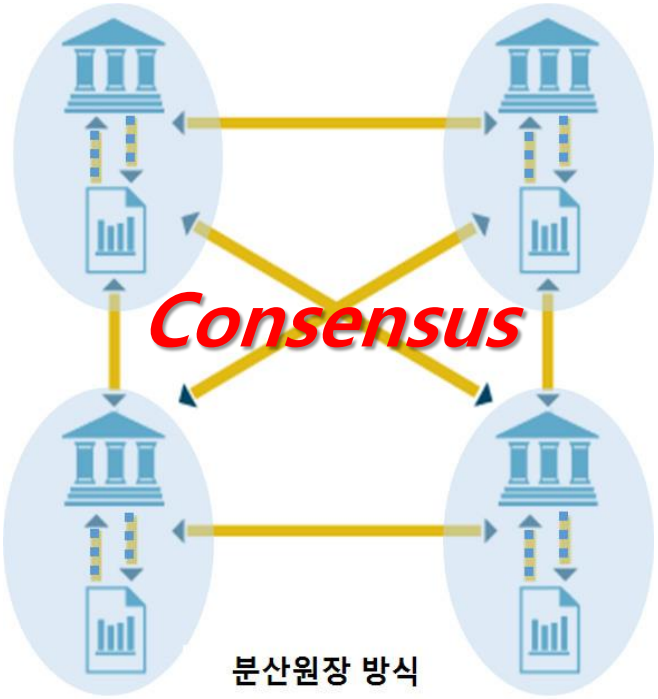
# 기존 모델과의 차이점 = 분산장부 개념




***Trust : TTP 역할***

***Trust : 누가 보증***

# *Where is Trust : 분산 장부들의 합의(무결성)*




네트워크 참여자들의
합의(Consensus)

서로 **신뢰하지 않는**
네트워크 참여자들간의
신뢰 확보 방법

## *P2P 신뢰모델 : 네트워크 참여자들의 공동*

# 블록체인 : 분산장부 이상의 개념

**분산장부**

√ 장부의 의미
=> 저장 정보?
√ 장부의 공동 관리(분산)
√ 공동관리 방식

글로벌 신뢰장부

일반화

**블록체인**

√ 장부의 개념 확장
=> 저장 정보의 확장
=> 메모리 + CPU
√ 새로운 컴퓨터
=> 글로벌(공동 작업)
√ 새로운 네트워크
=> 기본 구성 요소

글로벌 신뢰컴퓨터

# 국내 금융권 블록체인 정의

## 한국은행

√ '블록체인(Blockchain)'을 '**분산원장(Distributed Ledger)기술**'이라고 소개

√ 거래정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 P2P(Peer-to-Peer) 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하는 기술

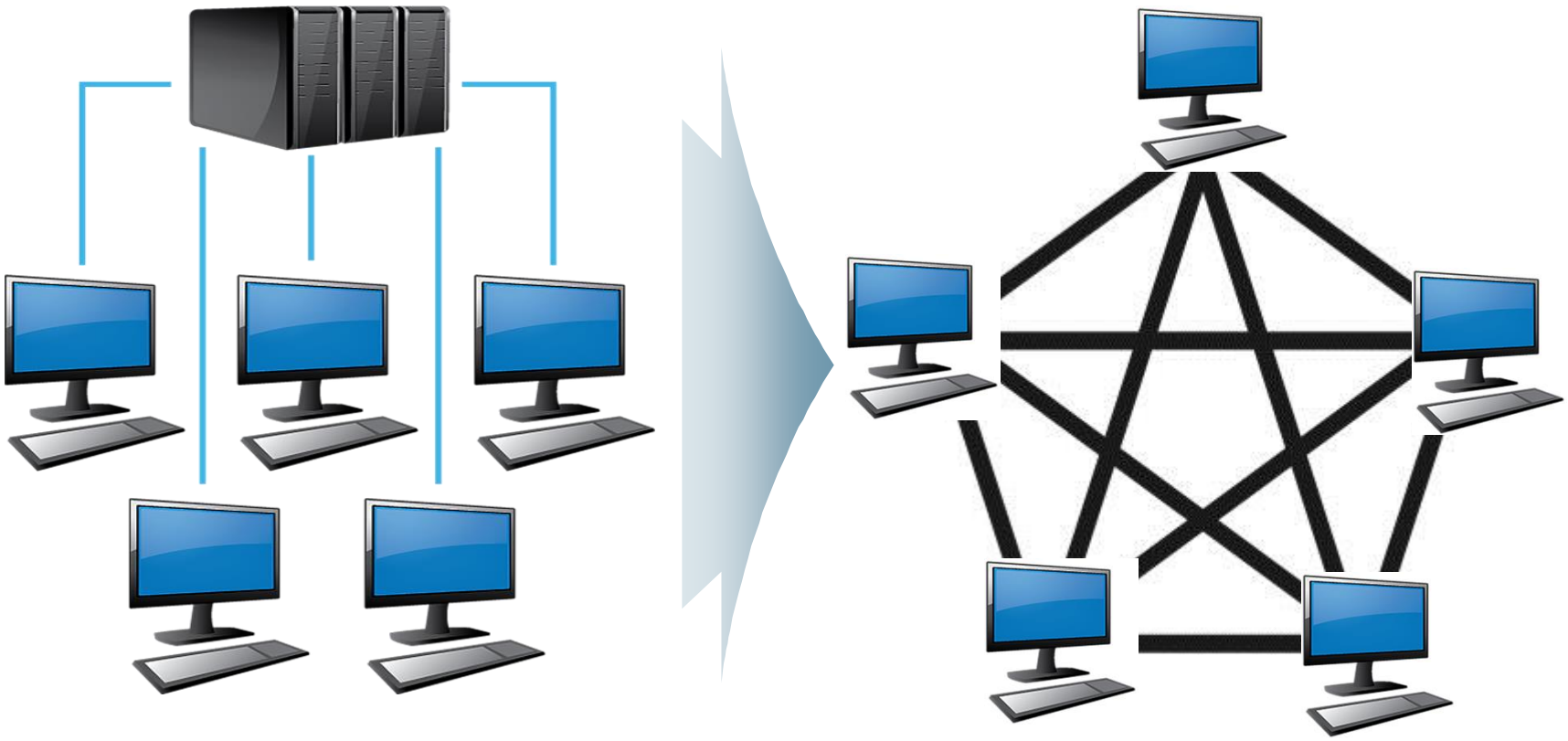
## 금융위원회/금융감독원

√ '블록체인(Blockchain)'이란 거래 데이터를 중앙집중형 서버에 기록, 보관하는 기존 방식과 달리 거래 참가자 모두에게 내용을 공유하는 **분산형 디지털 장부**를 의미

## 금융결제원

√ '블록체인(Blockchain)'이란 **분산된 네트워크의 컴퓨팅 자원을 모아 거대한 연산 능력을 확보**하고, 이를 기반으로 중앙서버 없이 모든 작업을 처리하고 검증하는 기술

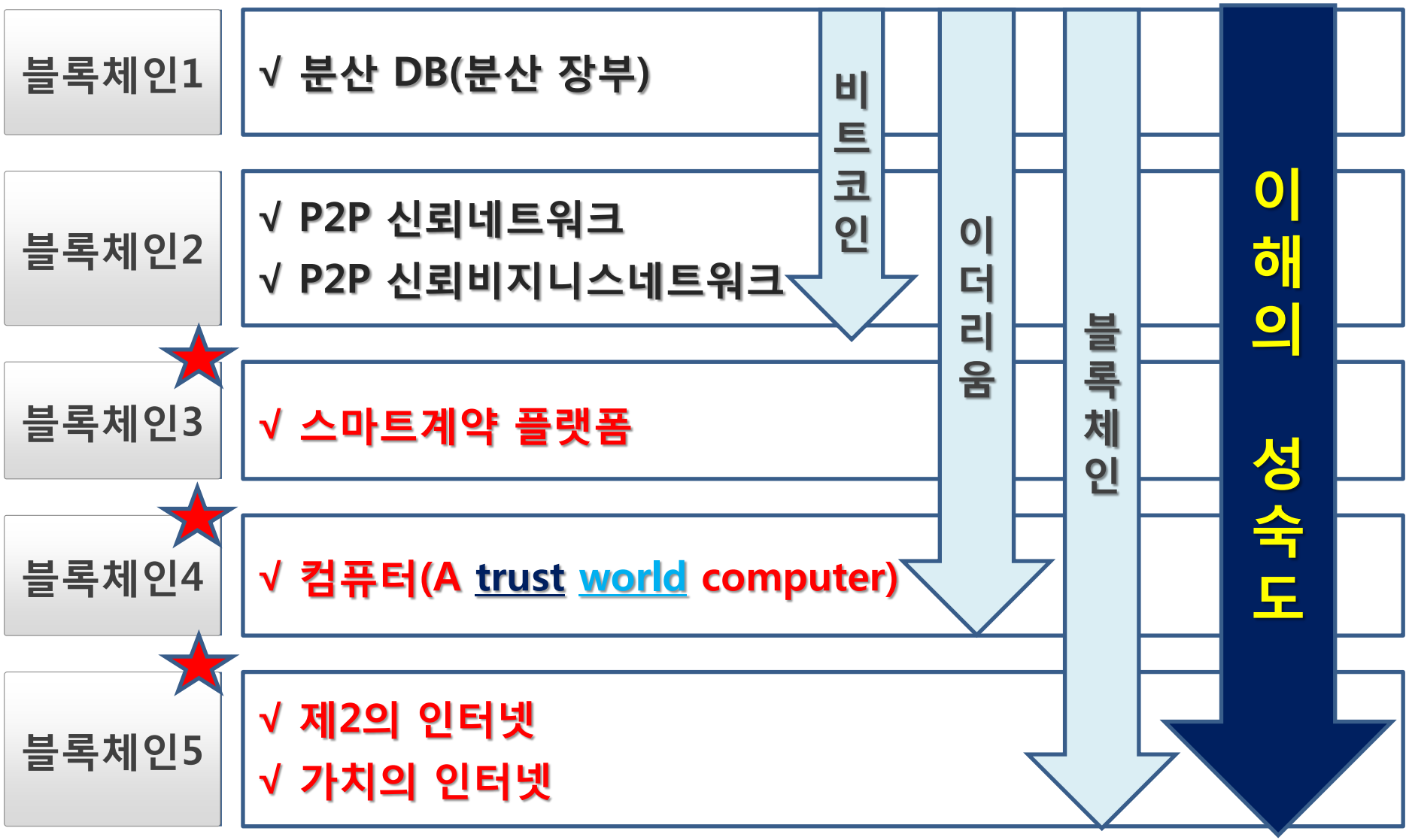
# 블록체인 개념 = 분산장부 개념에서 모든 것의 공동 작업



***블록체인의 현실적 모델***
***P2P 공유모델 : 토렌토 + CPU(S/W)***

**※ 참고 : 우리가 현재 쓰고 있는 컴퓨터조차도 블록체인 컴퓨터임**

# 다양한 블록체인 정의




※ 스마트계약 : 블록체인 컴퓨터에서 실행하는 소프트웨어

# 새로운 *컴퓨터* & *네트워크*

현재 : 컴퓨터와 네트워크(인터넷)

***블록체인* : 새로운 *컴퓨터&네트워크***

**A trust world computer**

# 블록체인의 본질

가정
① 상호 신뢰하지 않는 참여자(사람 또는 사물)들이

정치 / 행정 / 경제 / 금융 / 물류 / 의료
② 어떤 목적을 가지고

생태계
③ 커뮤니티를 구성하였을 때

정부 / 은행 / 카드회사 / 변호사 / 세무사
④ 신뢰기관이나 신뢰 중재자 없이

갑과 을이 없는 세상 / 공유경제 / 불균형성 해소 / 불평등 해소
⑤ (차별 없이 공정하고 합리적으로) 참여자들이 함께 신뢰성을 확보하면서
함께(공정한 합의)

⑥ ***추구하는 목적을 달성할 수 있도록 해주는 기술***

# 참여자 모두가 함께 공동 작업 수행

*인터넷에 연결된 모든 컴퓨터는*
*독립 주체들임*


*인터넷 세상*

*블록체인에 연결된 모든 컴퓨터는*
*하나의 컴퓨터 처럼 동작(글로벌)*


*블록체인 세상*

# P2P 커뮤니티생태계 인프라

## 블록체인 주요 기능

### 3대 기본 기능

안전한 데이터 저장 | 암호화폐 | 스마트계약

기본적으로 PKI 내재되어 있음

**블록체인 특징**

정보공유 및 투명성, 보안성(원본 보장, immutability)

*4대 정보보호서비스 : 비밀성, 인증, 무결성, 부인봉쇄*

**정보보호 문제 발생**

비밀성(confidentiality), 인증, 부인봉쇄 및 개인정보호(privacy)

## *CryptoBlockchain(암호블록체인)*

블록체인 오픈 플랫폼 + 융합 + 암호기술 오픈 플랫폼

# (암호)블록체인 탄생

## 암호기술 플랫폼

기밀성 | 인증 | 무결성 | 부인방지 | 프라이버시

Hash | Encryption/ Signature | Zero Knowledge | Multi-party Computation

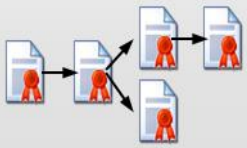
블록체인 공격 모델 | 블록체인 안전성 분석 모델

융합

## 블록체인 플랫폼

public permissionless blockchain | private permissioned blockchain

P2P Network | Distributed Ledger | Consensus



암호 블록체인

## 블록체인 생태계

**Blockchain 3.0 (Everything)**

- 금융 / 비금융 전 분야
- **사물인터넷** 등

→ 블록체인 + Everything

**Blockchain 2.0 (Smart Contract / DAO)**

- 스마트 계약 / 탈중앙화
- 스마트 자산 등

**Blockchain 1.0 (Cryptocurrency)**

- 디지털 화폐
- 화폐 전송 / 송금

# 안전한 P2P 커뮤니티생태계 인프라

## (암호)블록체인 주요 기능

### 3대 기본 기능

- 안전한 데이터 저장
- 암호화폐
- 스마트계약

### 정보보호 기능

- 비밀성
- 인증
- 무결성
- 부인방지
- 개인정보보호(Privacy)

# 블록체인이 가져다 줄 새로운 세상

***(탈중앙화, P2P, 공정, 신뢰, 프라이버시)***

***(개방/공유/투명, 실시간 감사, 효율화)***

***(새로운 경제 : 암호화폐와 암호경제)***

# 블록체인의 장·단점

| 구분 | 특징 | 내용 | 효과/제약사항 |
|---|---|---|---|
| ★ 장점 극대화 | 탈중앙화 | P2P 기반으로 중개기관 없이 참여자 간 직접거래 가능 | 인프라 구축비용 및 중개수수료 절감 |
| | 보안성 ★ | 다수의 참여자가 거래 정보를 공유하여 해킹이 어려움 | IT 보안비용 절감 |
| | 확장성(오픈소스) | 오픈소스를 이용해 구축, 연결, 확장 가능 | IT 구축비용 절감 |
| | 투명성 | 모든 거래기록에 공개적 접근 가능 | 관리감독 및 규제비용 절감 |
| | 신속성 | 거래의 승인 및 기록이 자동적으로 실행됨 | 신속성 향상 |
| ★ 단점 해결 | 확장성(처리속도) | 시간당 거래 처리속도가 제한적 | 주식시장에서와 같은 대량거래 구현이 어려움 |
| | 확장성(저장공간) | 모든 거래기록을 저장해야 하므로 저장공간이 점점 증가 | 저장용량 문제가 나타날 소지가 있음 |
| | 비가역성 | 한 번 집행된 거래는 다시 되돌릴 수 없음 | 이전된 자산이 강제로 반환될 수 없음 |

장점은 극대화하고 단점은 해결

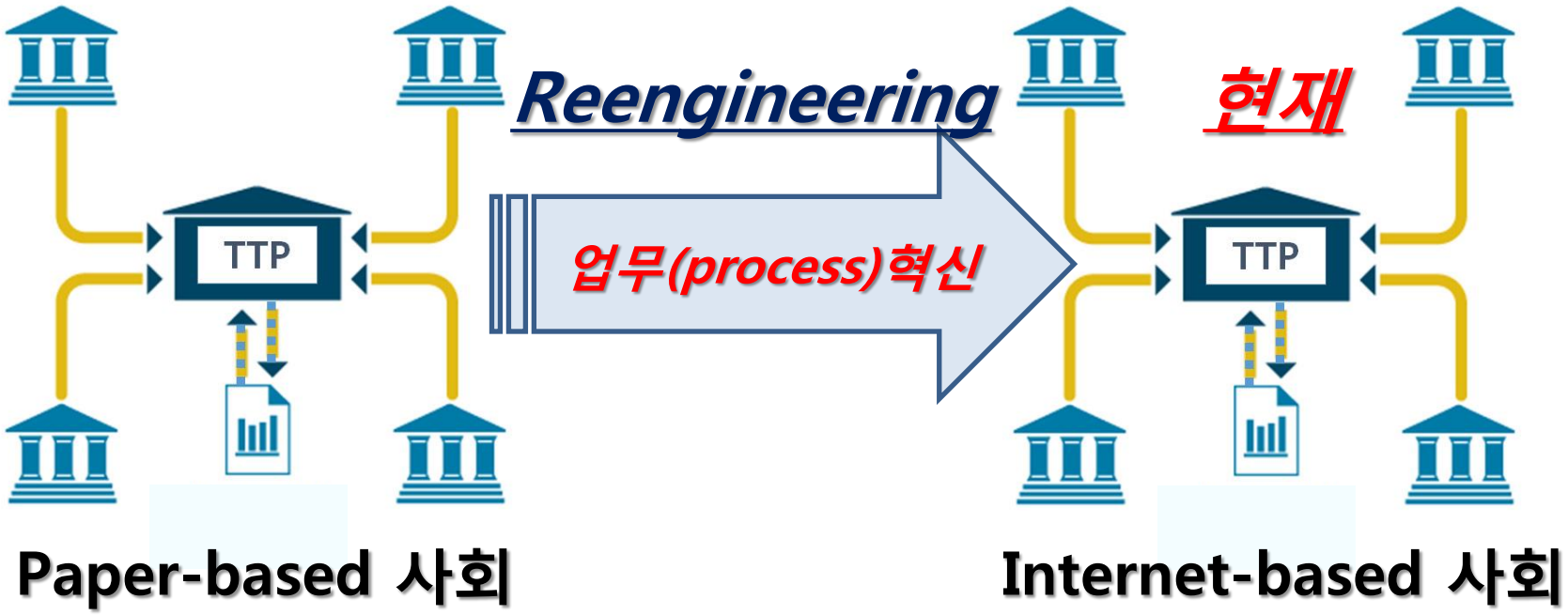
자료 : Santander InnoVentures, KB금융지주 경영연구소, 한국은행, 신영증권 리서치센터

# 패러다임


새로운 커뮤니티생태계 탄생
사이버세상
블록체인세상
안전한 P2P 생태계 인프라
블록체인 다양성
참여자 / 합의 방식(Consensus Protocol) / 특성
블록체인 = 분산원장 : Trust(immutability)
Internet +P2P Network(Without TTP) : Not Trust
(Synchronous / Asynchronous, etc)
암호블록체인 : 안전한 P2P 신뢰네트워크

## 사이버패러다임(1996년 전후)

(*Real World의 모든 업무를 인터넷 기반의 Cyber World 로 전환하는 것*)

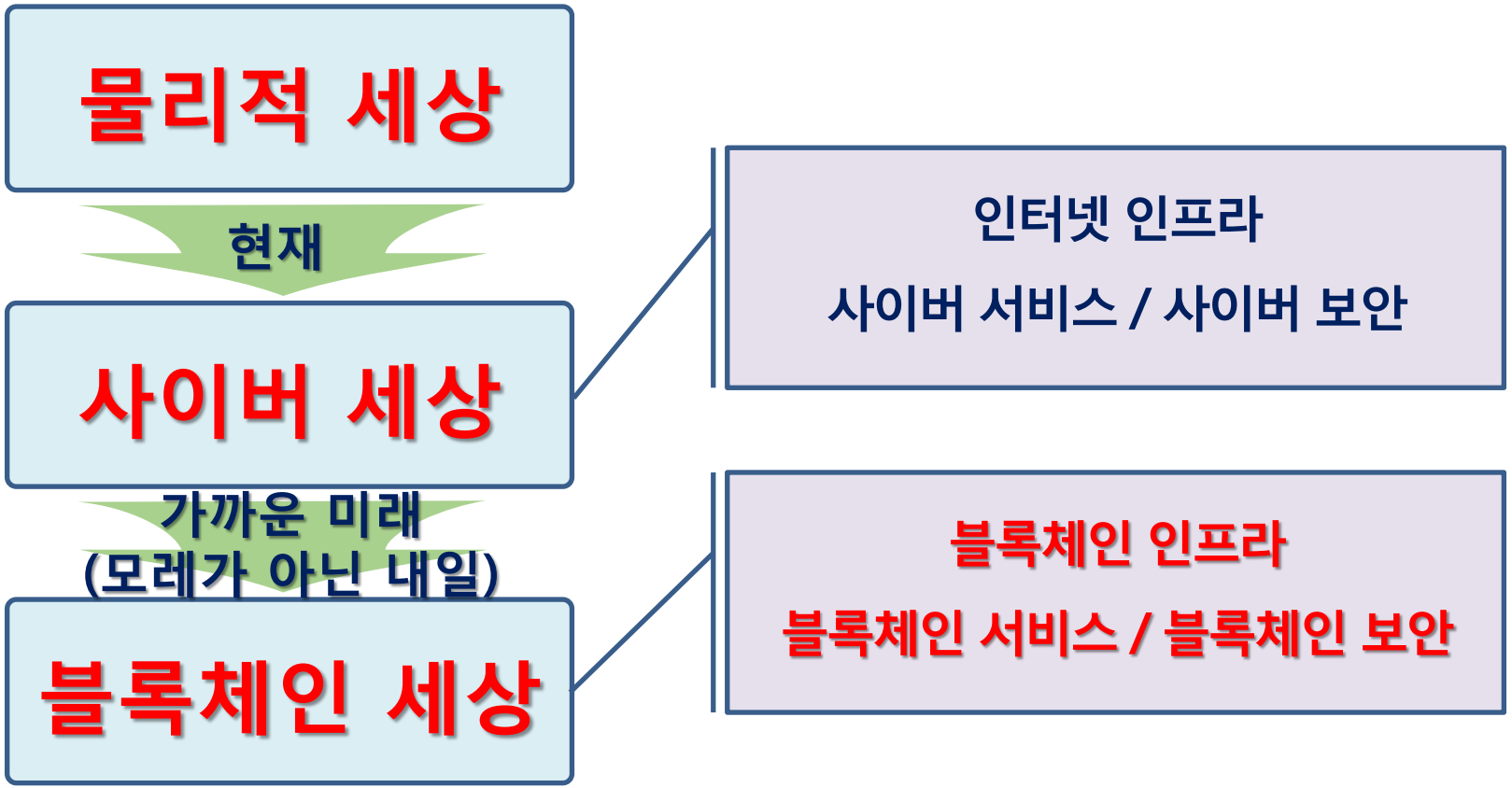



***사이버세상 및 사이버보안 탄생***

## 블록체인패러다임(2015년 전후)

(*TTP 기반의 모든 업무를 Blockchain-based 기반으로 전환하는 것*)


***사이버세상 및 사이버보안에서***
***블록체인세상 및 블록체인보안으로 전환***




**해야 하는가의 문제 => 언제 하는가의 문제**

**시작할 때가 지남★**

# 새로운 블록체인 세상(블록체인패러다임 실현분야)

정부·공공 | 정치 | 경제 | 교육

물류 | 금융 | 의료 | 에너지

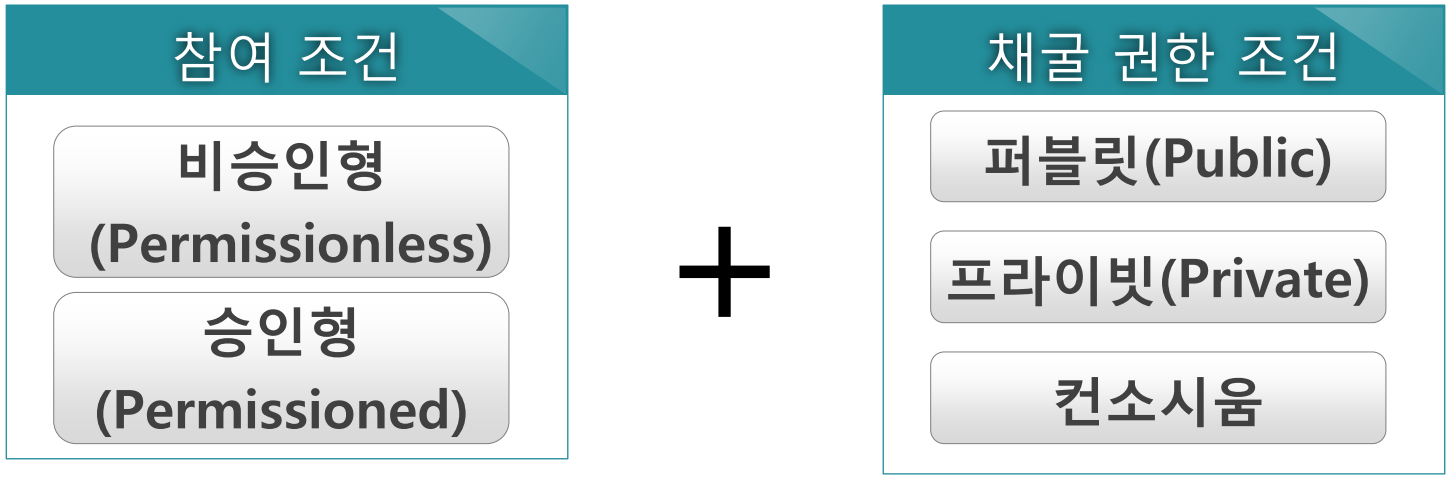
**안전한 P2P 커뮤니티생태계**

## (암호)블록체인 주요 기능

| | | | |
|---|---|---|---|
| 3대 기본 기능 | 안전한 데이터 저장 | 암호화폐 | 스마트계약 |
| 정보보호 기능 | 정보보호 4대 서비스 (비밀서, 인증, 무결성, 부인방지) | | 개인정보보호 |

# 블록체인 분류

# 블록체인의 다양성_1



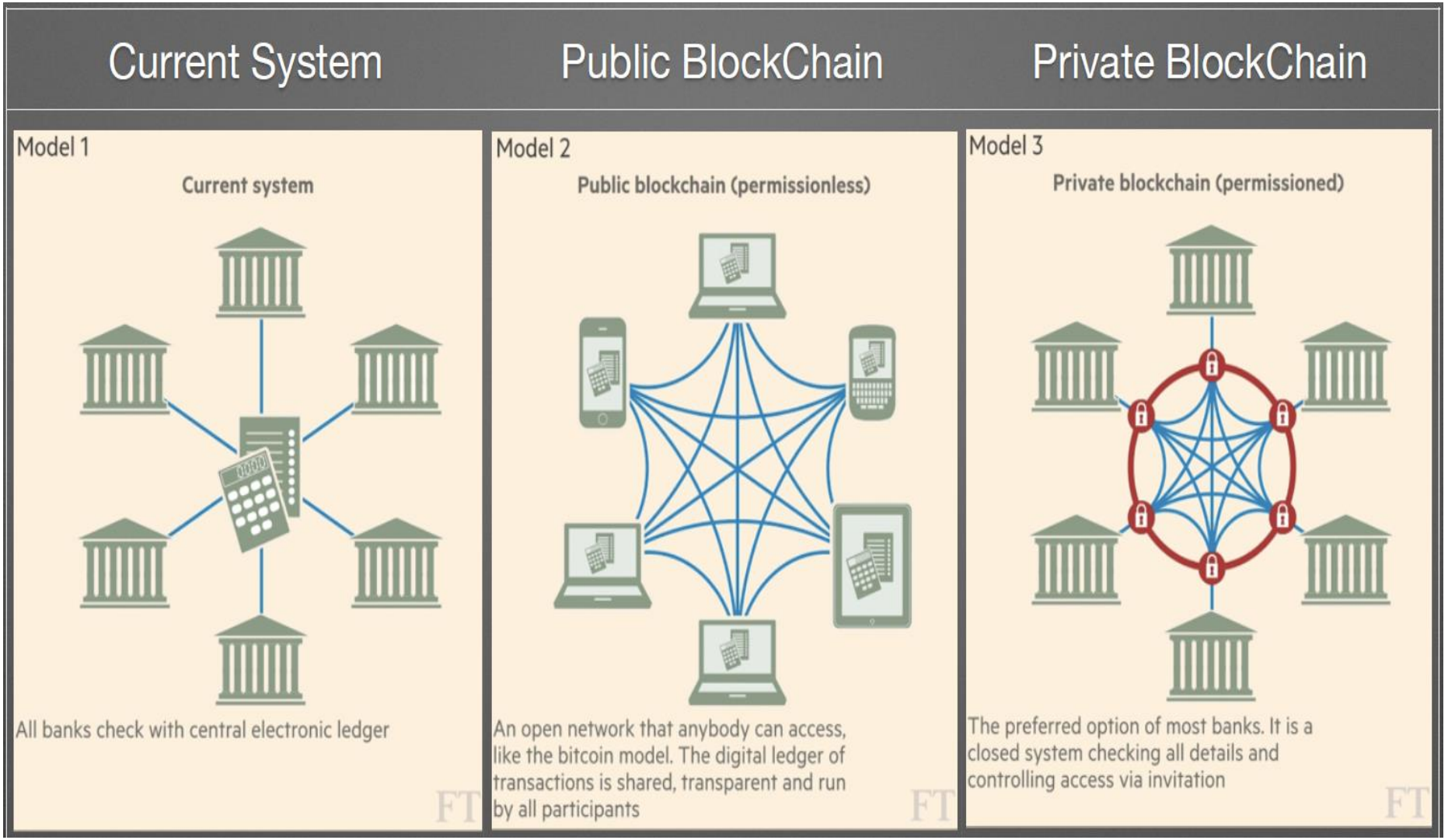

***퍼블릿블록체인(Public Permissionless Blockchain)***

Public Permissioned Blockchain

Private/Consortium Permissionless

***프라이빗블록체인(Private/Consortium Permissioned)***

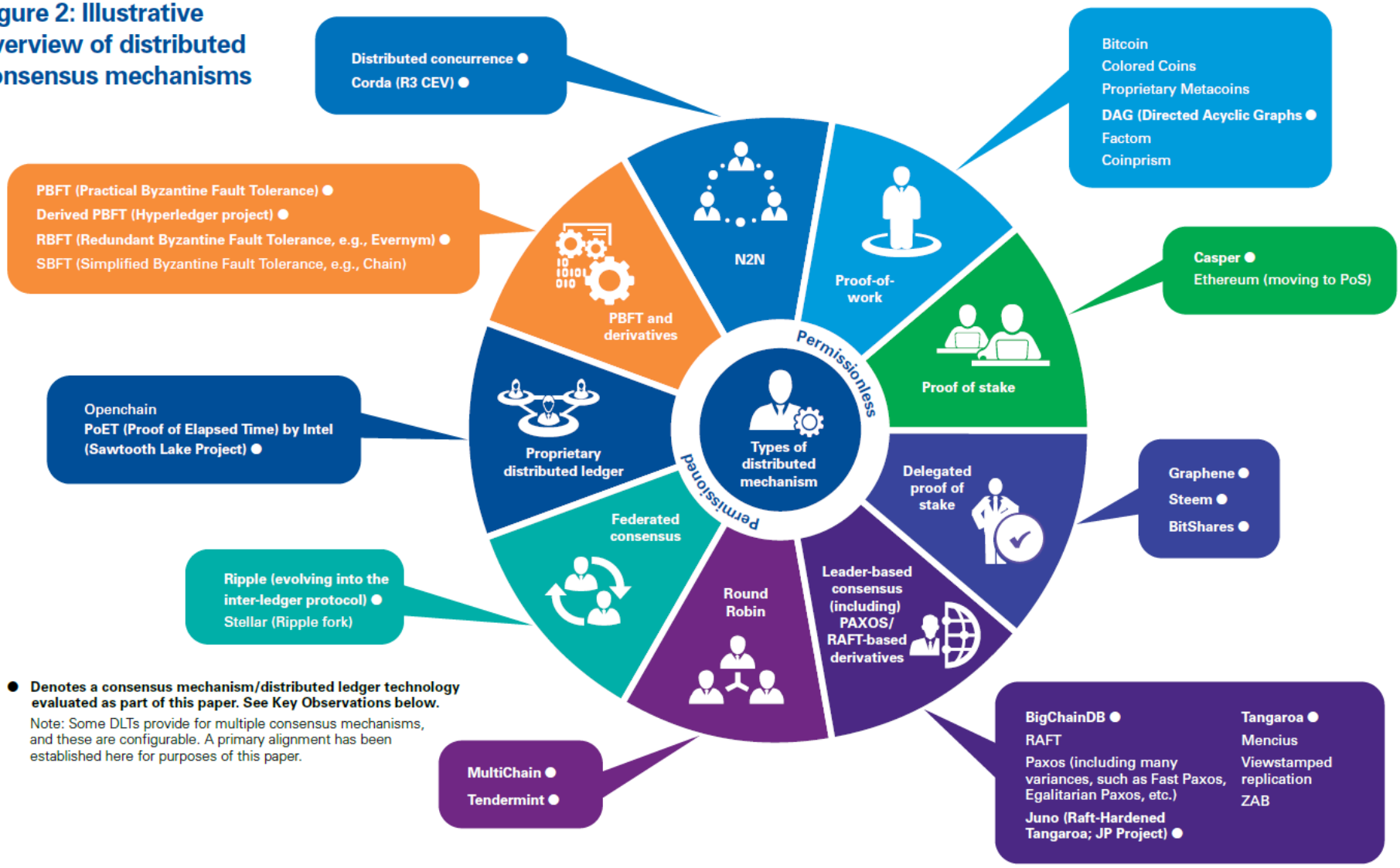
# 블록체인의 다양성_2




※출처 : 구글 이미지

# 블록체인의 다양성_3

**Figure 2: Illustrative overview of distributed consensus mechanisms**

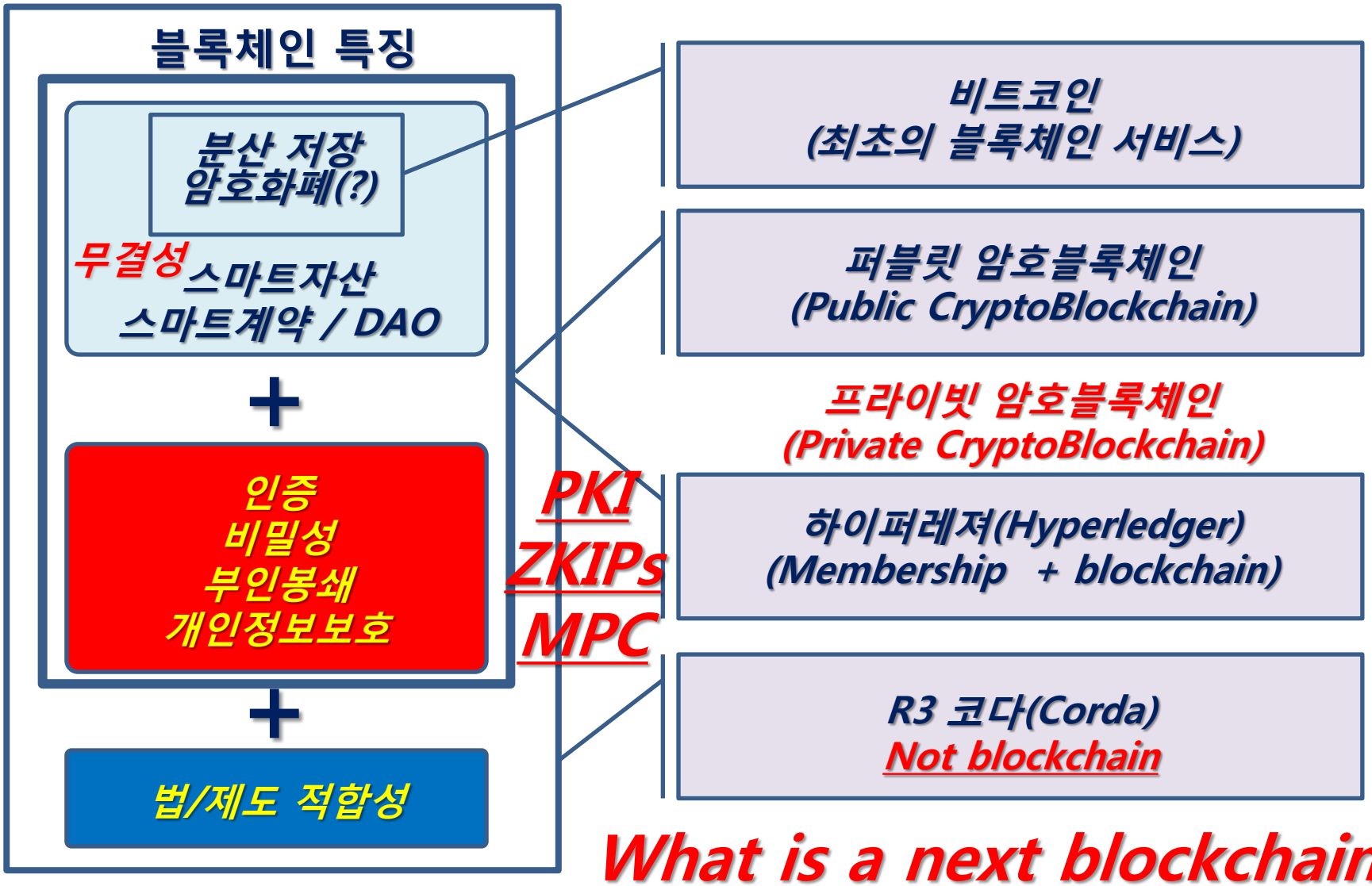



● **Denotes a consensus mechanism/distributed ledger technology evaluated as part of this paper. See Key Observations below.**

Note: Some DLTs provide for multiple consensus mechanisms, and these are configurable. A primary alignment has been established here for purposes of this paper.

**※출처 : Consensus : Immutable agreement for the Internet of value, KPMG, 2016년**

# 블록체인 발전 방향

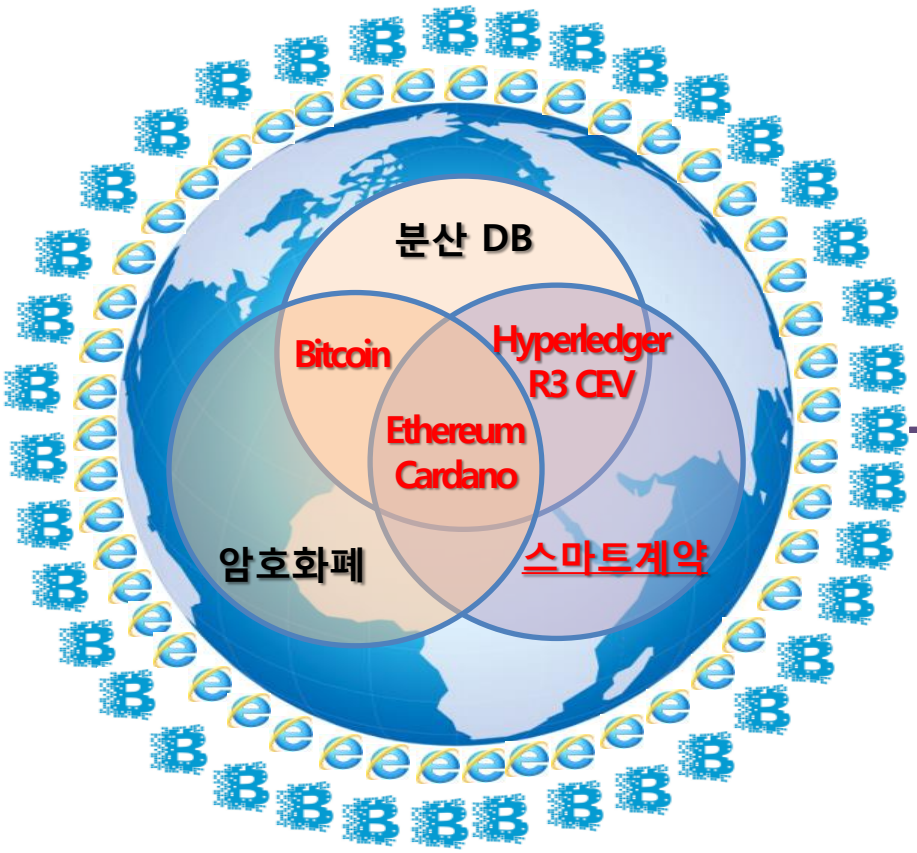



**What is a next blockchain?**

**CryptoBlockchain(암호블록체인)**

# 블록체인 생태계

# 블록체인패러다임과 생태계_1




**블록체인 1.0**

암호화폐

**블록체인 2.0**

스마트계약

**블록체인 3.0**

Everything !!!

# 블록체인패러다임과 생태계_2

## Blockchain 1.0

- 암호화폐 (cryptocurrency)
- 화폐전송 (currency transfer)
- 외환송금 (remittance)
- 전자지불 (digital payment system)

**Cryptocurrency**

## Blockchain 2.0

- 증권(stock) / 채권(bonds)
- 대출(loans) 모기지(mortages)
- 부동산소유권 (titles)
- 스마트계약 (smart contract)
- 스마트자산 (smart property)
- 탈중앙화자율조직 (DAO)

**Smart Contract / DAO**

# 블록체인패러다임과 생태계_3

## Blockchain 3.0

- 정부(government)
- 국방(national defence)
- 보건(health)
- 과학(science)
- **문화(culture) / 예술(art)**
- **IoT / 물류(SCM -> DCM)**
- 농·축산식품 관리

**미래 적용(서비스) 분야에 따른 분류 블록체인 3.0**

***Change Everything (혁명적/파괴적 기술)***

**국외 동향 : 블록체인 3.0**
**국내 동향 : 블록체인 1.5**

# 국내 생태계 현황

정부·공공 : 새로운 아젠다(블록체인 기반 행정·공공 서비스) 발표

금융권 : 핀테크 / 블록체인 인증서 / 암호화폐

IT 기업 : 블록체인 전문 기업체로서의 전환 추진(IoT, 물류 등)

벤쳐기업 : 암호화폐 / 거래소 / 외환송금 / 개발 용역

유망 산업분야 : IOT / 에너지 / 물류·유통 / 의료

**국내 현황 : 블록체인 1.5 정도**

**아직도 의미 없는 논쟁 중**

# 국내 블록체인 금융생태계 현황_1

## KB 국민은행

√ 핀테크 업체 '코인플러그(coinplug)'에 15억 원 투자, 인증 및 송금 서비스 관련 파트너쉽 체결('15.9.)
√ 비대면 실명확인 증빙자료 보관시스템 구축('16.4.)
√ KB국민카드는 국내 금융사 중 최초로 블록체인 기술을 활용한 간편 개인인증 시스템을 도입('16.10.)

## 신한은행

√ 블록체인 외환송금 서비스 개발 스타트업 '스트리미(Streami)'와 협업('16.7.)
√ '신한 골드 안심 서비스' 출시를 통해 금 실물거래가 이뤄질 때 블록체인 기술을 바탕으로 구매 교환증과 보증서 발급('16.8.)

## NH 농협은행

√ FIDO(Fast Identity Online)기반의 공인인증서 대체 기술 및 생체인증 솔루션을 자사 전체 금융 플랫폼에 탑재('16.8.)
√ 기존의 지문인증 서비스에 블록체인 기술을 결합해 보안성을 높여 인터넷 뱅킹으로까지 확대('16.10.)

# 국내 블록체인 금융생태계 현황_2

## IBK 기업은행

√ 블록체인 전문기업 '블로코(Blocko)'와 협력하여 장외주식 거래를 위한 'KSM(KRX Startup Market) 시스템' 개발('16.9.)
√ 블록체인 기술 발전을 위한 글로벌 협력조직인 '하이퍼레저 (Hyperledger)' 가입('17.4.)

## IBK 기업은행

√ 핀테크 기업 '코빗(Korbit)'과 협력해 블록체인 기반 금융서비스 개발 착수('16.3.)
√ 유럽과 아프리카간 비트코인 송금서비스를 제공하는 케냐의 비트코인 스타트업 '비트페사(BitPesa)'와 공동협력을 위한 업무협약 체결('16.7.)

## KRX 한국거래소

√ 미국 송금 전문업체 '머니그램(MoneyGram)'과 협약해 전 세계 200여 개국으로 24시간 송금 가능한 서비스 개시('17.2.)
√ 디지털전략부 신설을 통해 블록체인과 접목한 사업모델 개발 계획 ('17.4.)

# 국내 블록체인 금융생태계 현황_3

## KEB 하나은행

√ 핀테크 스타트업 인큐베이팅 센터인 '원큐랩(1Q Lab)'을 통해 센트비 등 핀테크 기업과 함께 블록체인 기술을 활용한 해외송금 서비스 구축 ('15.6.)

√ 국내 지급 결제 및 인증 관련 프로젝트를 진행하고 기술검증을 완료 ('16.11.)

**√ 기존 포인트 제도인 하나머니를 블록체인 기반의 암호화폐로 전환 예정. 특히, 하나머니의 글로벌 제휴처 확대 주력**

## 우리은행

√ 미국 송금 전문업체 '머니그램(MoneyGram)'과 협약해 전 세계 200여 개국으로 24시간 송금 가능한 서비스 개시('17.2.)

√ 디지털전략부 신설을 통해 블록체인과 접목한 사업모델 개발 계획 ('17.4.)

**√ 국내 은행 최초로 암호화폐 발행 사업 추진('17.8.)**

**※ 암호화폐 : 선불형전자지불수단**

# 국내 블록체인 금융생태계 현황_4

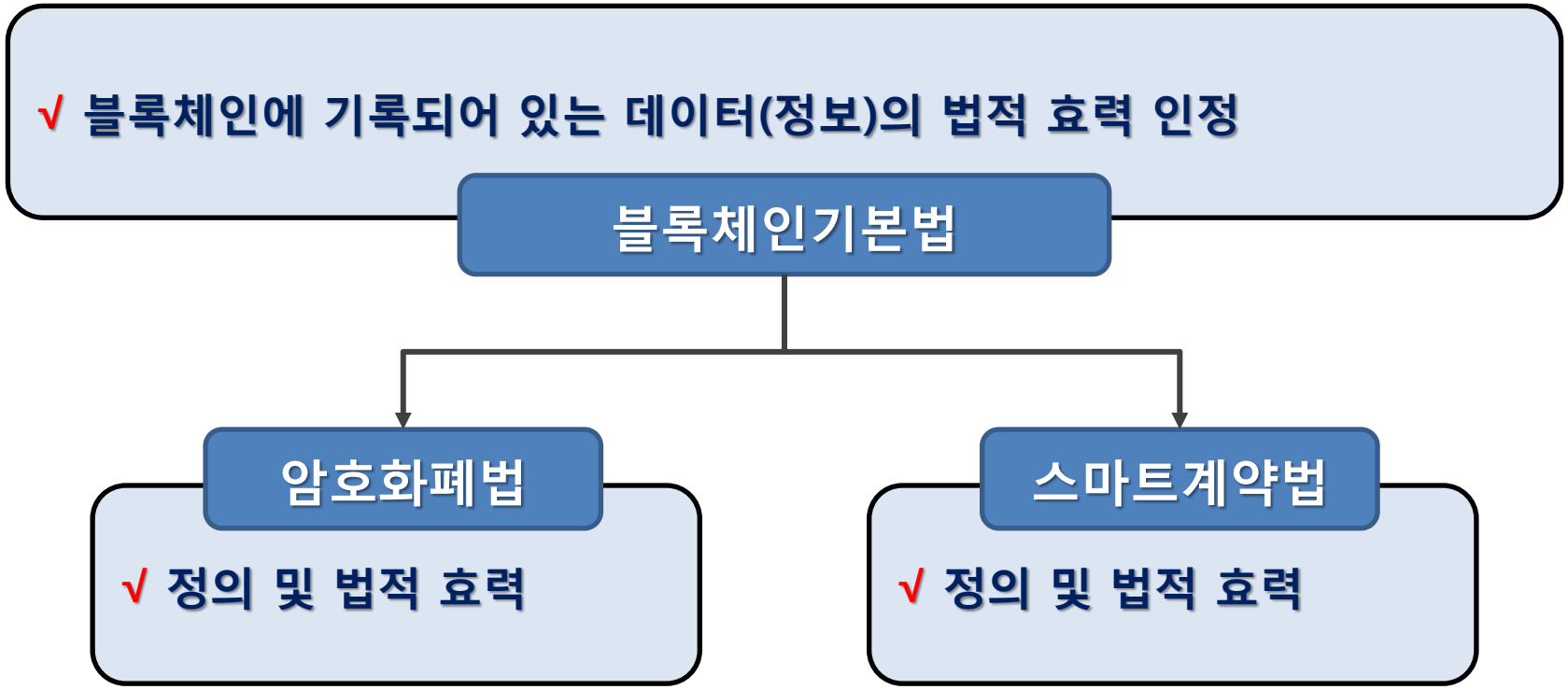
## 은행연합회

√ 은행권 블록체인 컨소시엄
√ 16개 사원은행 및 2개 협력기관
√ 은행 공동 블록체인 플랫폼(2018년 2월 예정)
√ **은행 공동 사설인증서비스**

## 금융투자협회

√ 주로 증권사 위주의 블록체인 컨소시엄
√ 미래에셋대우, NH투자증권, KB증권 등 증권사 21곳과 데일리인텔리전스, 더루프 등 5개 기술 파트너
√ 공동 블록체인 플랫폼(올해 서비스 목표 예정)
√ **모바일트레이딩시스템(MTS)의 사설인증서비스**

# 법·제도




***가상화폐 : 전자금융거래법 개정 ?***

# 국내 소액해외송금업 제도 도입

## 외국환거래규정을 개정하여 비 금융기관의 외국환업무 중 소액해외송금업 등록 허용 (2017. 7. 18.부터 시행)

### 등록 요건

**√ 재무요건**

- 자기자본 20억원 이상일 것
- 자기자본 대비 부채비율 200% 이내일 것

**√ 시설요건**

- 전산시설, 자금세탁방지체계를 구축할 것
- 한국은행과 외환전산망을 연결할 것

**√ 인력요건**

- 외환전문인력을 확보할 것
- 정보보호최고책임자를 지정할 것

### 업무 범위

**√ 거래한도**

- 건당 지급·수령한도는 미화 3천불
- 동일인이 동일 업자를 통해 지급·수령할 수 있는 연간 누계한도는 미화 2만불

**√ 업무방식**

- 소액해외송금업용 은행 계좌를 지정하여 동 계좌를 통해서만 고객의 자금 지급·수령

## 전자금융거래법 개정안 발의 (더불어민주당 박용진 의원실), 2017. 7 .31.

### 주요 내용

√ **가상통화취급업의 분류 및 인가(5개 업무로 분류)**

- 가상통화매매업
- 가상통화거래업
- 가상통화중개업
- 가상통화발행업
- 가상통화관리업

√ **가상통화거래업자의 의무**

- 가상통화거래소를 운영하는 가상통화거래업자에 대해서는 더욱 강하게 규제
- 가상통화예치금을 예치기관에 예치하거나 피해보상계약을 체결할 의무

# 미래 세상

# 암호블록체인


인터넷 세상
인터넷

블록체인 세상
블록체인인터넷

모든 것의 혁명
(가치의 인터넷 탄생)

# 미래 세상의 특징
# 새로운 탈중앙화된 P2P 생태계 세상

***관련 법체계 정비(블록체인 세상 기반조성)***

**암호블록체인패러다임**

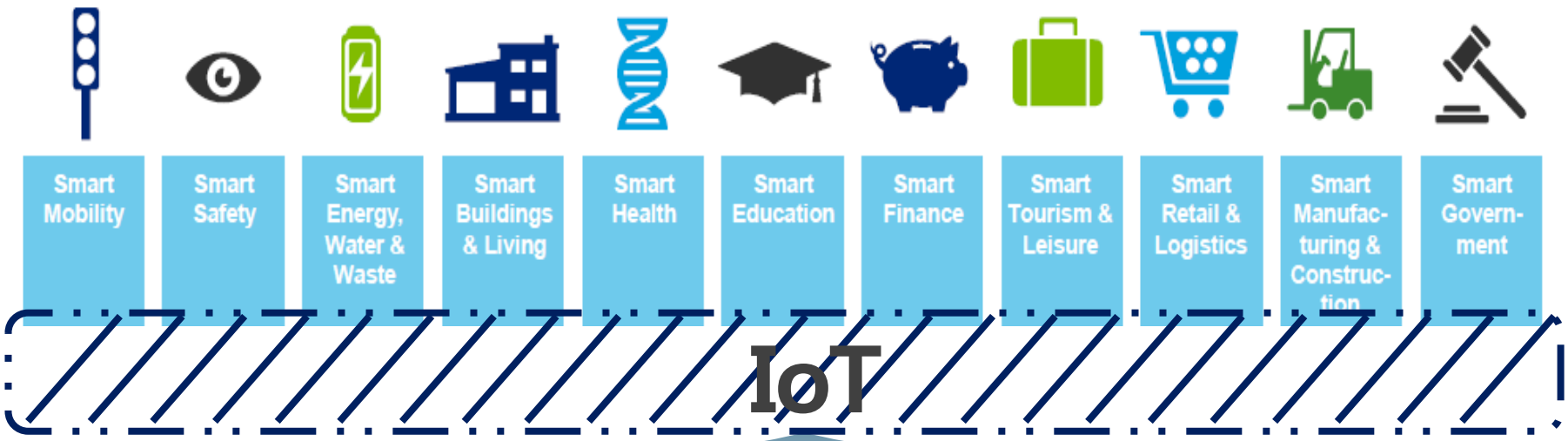
***CryptoBlockchain Open Platform***

***(비밀성, 인증, 무결성, 부인방지, 개인정보보호)***

***Blockchain Open Platform***

***인터넷+파괴적 기술들의 융합***

# 미래 블록체인 세상




**관련 법체계 정비(블록체인 세상 기반조성)**

**블록체인패러다임**

**CryptoBlockchain Open Platform**

**(암호블록체인 + 정보보호)**

**P2P 분산 초연결 신뢰네트워크(S/W, H/W)**

*(latency, Throught, Scalability, Fault tolerance)*

**사이버 세상**

①현재 어떤 문제를 가지고 있는가?
②미래 산업 예측?

생산성/경쟁력/신사업
새로운 경제생태계 대비

**블록체인 세상**

①문제 해결의 효율적인 방법 제공
②선도적인 신사업 창출을 통한
암호경제의 주도권 확보

**새로운 경제생태계(암호경제)**

**대응 전략 필요**

# 결언 : 블록체인 본질에 대한 본질 상기

## 블록체인의 본질

가정
① 상호 신뢰하지 않는 참여자(사람 또는 사물)들이

정치 / 행정 / 경제 / 금융 / 물류 / 의료
② 어떤 목적을 가지고

생태계
③ 커뮤니티를 구성하였을 때

정부 / 은행 / 카드회사 / 변호사 / 세무사
④ 신뢰기관이나 신뢰 중재자 없이

갑과 을이 없는 세상 / 공유경제 / 불균형성 해소 / 불평등 해소
⑤ (차별 없이 공정하고 합리적으로) 참여자들이 함께 신뢰성을 확보하면서
함께(공정한 합의)

⑥ *추구하는 목적을 달성할 수 있도록 해주는 기술*

# 결언 : 미래 세상의 합의

## 전략적 합의

새로운 질서의 가치 판단?

헌법적 가치 / 우리가 합의하는 가치

*새로운 질서의 최소한의 기준 확립*

## 전술적 합의

새로운 질서(rule) 필요

블록체인 생태계 = 탈중앙화된 P2P 생태계

새로운 정치 / 새로운 경제 / 새로운 금융