블록체인 기술과 발전방향

- 블록체인 기술이슈와 해결

블록체인·융합 PM
김 종 현
girasong@iitp.kr

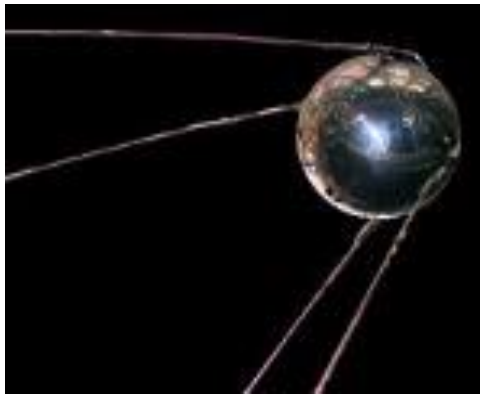
IITP

스푸트니크 충격 (Sputnik Crisis)과 GPS

- 스푸트니크 충격 (Sputnik Crisis): 1957년 10월 4일
  - 세계 최초 인공위성 스푸트니크 1호 (83.6kg, 직경 58cm)로 미국이 받은 과학기술·교육부문의 충격
    - ✓스푸트니크 2호(508.3kg)는 개 1마리를 실었고, 우주선 ·자외선 측정 (1957.11.3)

- GPS
  - 1957년 소련 스푸트니크위성의 신호를 추적한 존스홉킨스대 응용물리학연구소(APL)이 발표
  - 소련은 직접 쏘아올린 위성의 궤도를 추적할 기술은 수 없었음
  - 위성이 기지국 관찰자와 가까워지면 커지고, 멀어지면 작아지는 도플러원리를 이용해 위성 궤도 추론
  - 위성궤도를 통해 역으로 수신국 위치를 알아내는 방식으로 잠수함 위치를 확인하는 문제를 해결

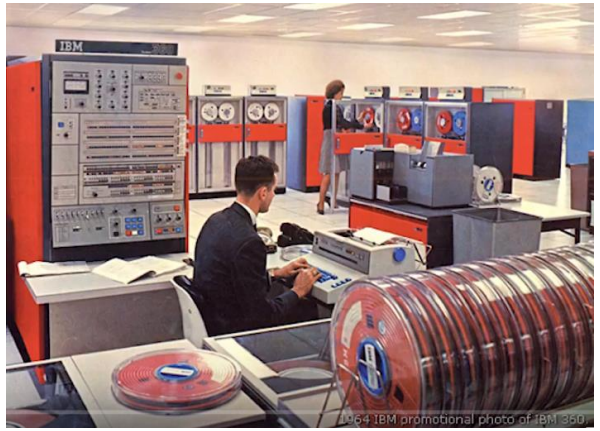
- 아폴로 11호 달 착륙 (1969.7.20)
  - "That's one small step for a man, one giant leap for mankind." by Neil Armstrong



소련의 스푸트니크(동반자) 인공위성

중앙집중 시스템과 분산시스템

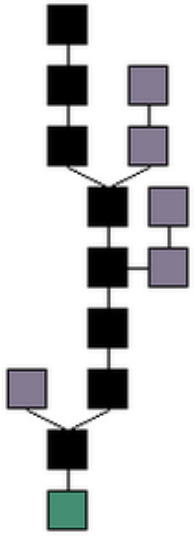
- ENIAC (1947) → Mainframe IBM 360 (1964)과 더미 터미널 (Dummy Terminal)
  → 애플컴퓨터 (1977)와 IBM PC 5150 (1981)
  → Thin Client or Zero Client by Cloud Computing 과 가상화



1964

1977

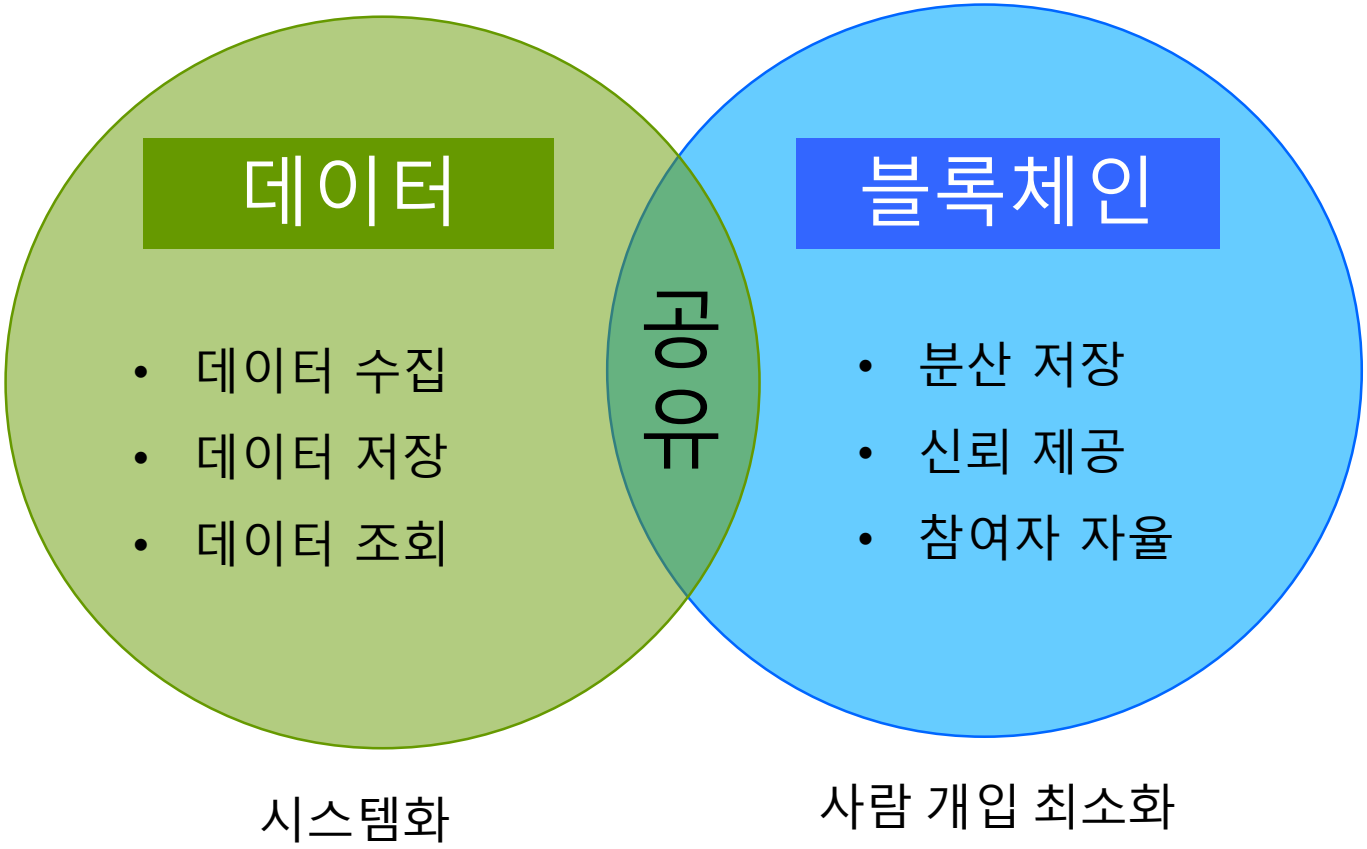
2010



2017

블록체인 역할 3가지

1. 신뢰할 수 있는 데이터
2. 투명한 정보 공개
3. 자율 기반 거버넌스



블록체인의 오해와 진실

오 해	진 실	무엇을 할 수 있나?
보안 강화	위변조 방지	제3자 신뢰 제공
자동화	디지털화	직거래
가상화폐	탈중앙화 협업도구	집단 지성 기반 평가

Q & A

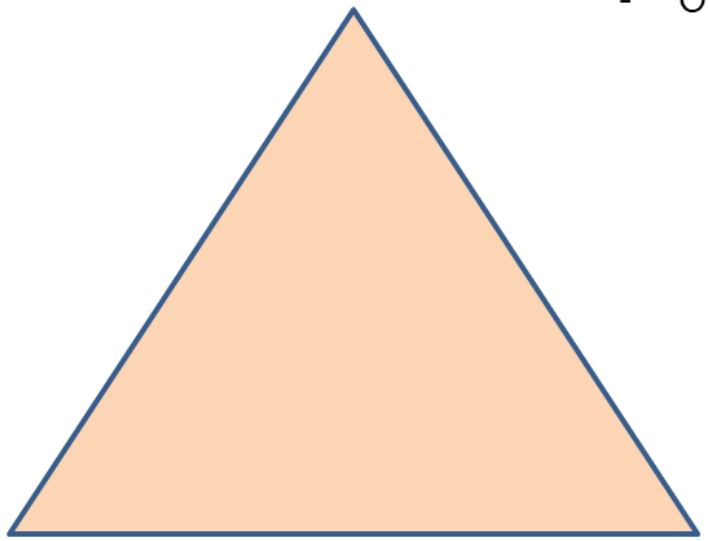
- 블록체인은 데이터를 자동으로 공유 ?
- 블록체인은 개인 프라이버시를 보호 ?
- 블록체인 기반 식품이력관리는 소요시간을 감소 ?
- 블록체인은 신분증명을 편하게 ?
- 블록체인 기반 실손보험 소액청구는 처리절차가 간편 ?

블록체인 기술의 주요 이슈

- 블록체인 기술 한계
  - 데이터 중복 저장의 비효율성
  - 거래속도 증가를 위해, 일부 선정 노드만 합의에 참가하는 DPOS의 중앙화 문제
  - 빅데이터 활용을 위한 대용량 컨텐츠의 분산장부 처리 · 저장
  - 메인넷에 접근하기 위한 클라이언트 SW 및 UI/UX
  - 분산장부의 개인정보 저장 · 삭제 및 보호
  - 과거 거래 내역의 수정

- 차세대 블록체인 기술개발 방향
  - 진정한 탈중앙화 거버넌스를 위한 합의 알고리즘
  - 거래데이터 고속처리에 적합한 블록구조
  - 데용량 데이터 분산 저장 기술 개발

• Decentralization, Scalability, Security & Privacy 동시 해결 기술



블록체인은 진화 중

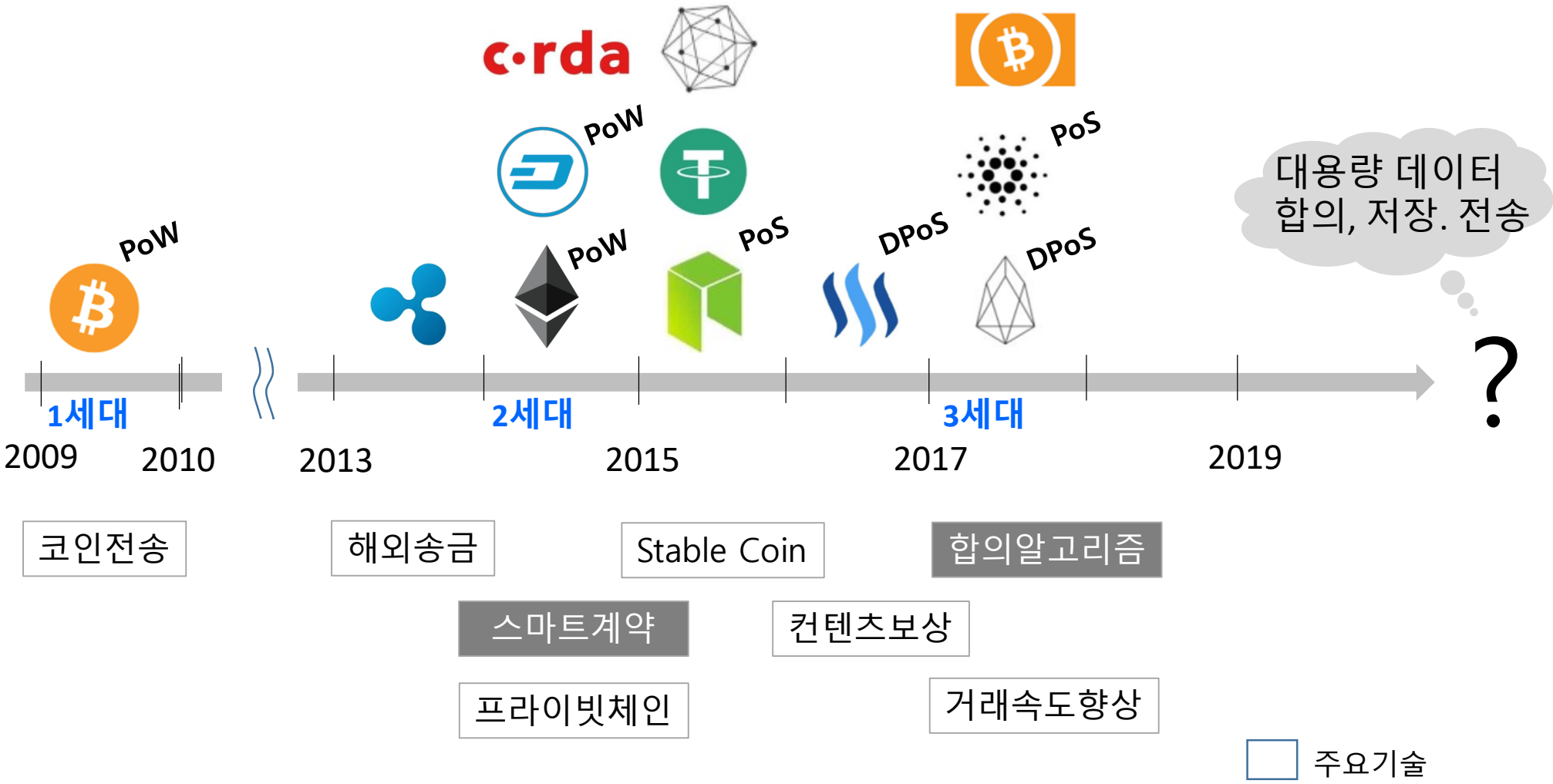
- 지금까지 소개된 기술은 빙산의 일각 !!! → 대용량 데이터 고속 처리기술과 합의 알고리즘

분산장부 저장기술

블록체인 확장기술

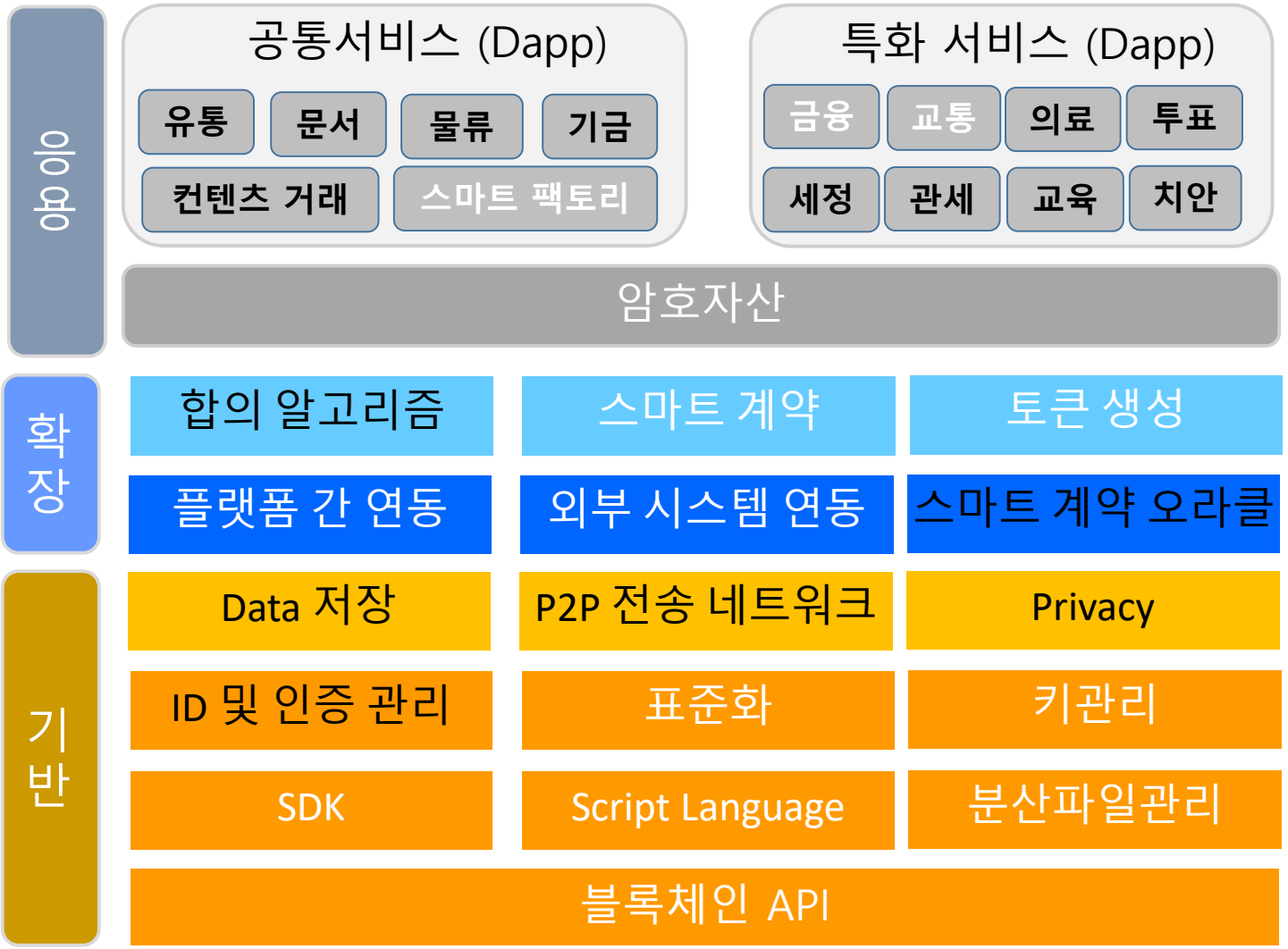
블록체인 기술 진화

- 채굴 (PoW 방식. 비트코인, 이더리움)에서 PoS 방식(스팀잇, EOS. Cardano)으로 발전
- 대용량 데이터, 거래량 증가에 따른 합의알고리즘 개선



블록체인 기술구조

- 과기정통부 2018 블록체인 기술 로드맵 기준에 따른 기술 분류



(흰색 글씨 기술은 R&D 미포함 분야)

블록체인 기술 이슈

기반

- 확장성 (Transaction & Node Scalability)
  - 빈번하게 발생하는 금융거래 (VISA는 최고 50,000 tps) 와 같은 거래 적용이 어려움
    - ✓낮은 처리 속도 (비트코인은 ~2 tps(transactions per second), hyperledger fabric은 150 tps)
  - 프라이빗 블록체인의 복잡성(complexity)이 참여 노드 수의 제곱에 비례하여 제한
- 트랜잭션의 지연시간 (Transaction Latency)
  - 트랜잭션의 확정(confirmation)에 걸리는 시간 지연 (비트코인은 약 60분(6 confirmations))

확장

- 최종성 (Transaction Finality)
  - 51% 공격에 취약
- 상호운영성 (Interoperatbility or Service Fragmentation)
  - 블록체인 플랫폼에 따라 Dapp이 개별적으로 구현되고, 블록체인 간 정보 교환이 어려움

응용

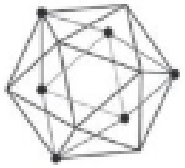
- 신원 증명 및 관리의 부재 (Lack of Identification and Management)
  - 계정의 신원(identity) 확인이 어렵고 키의 분실의 경우 계정 복구가 불가능

거래 속도

- 초당 거래속도 TPS (Transaction Per Second) 비교

7

100



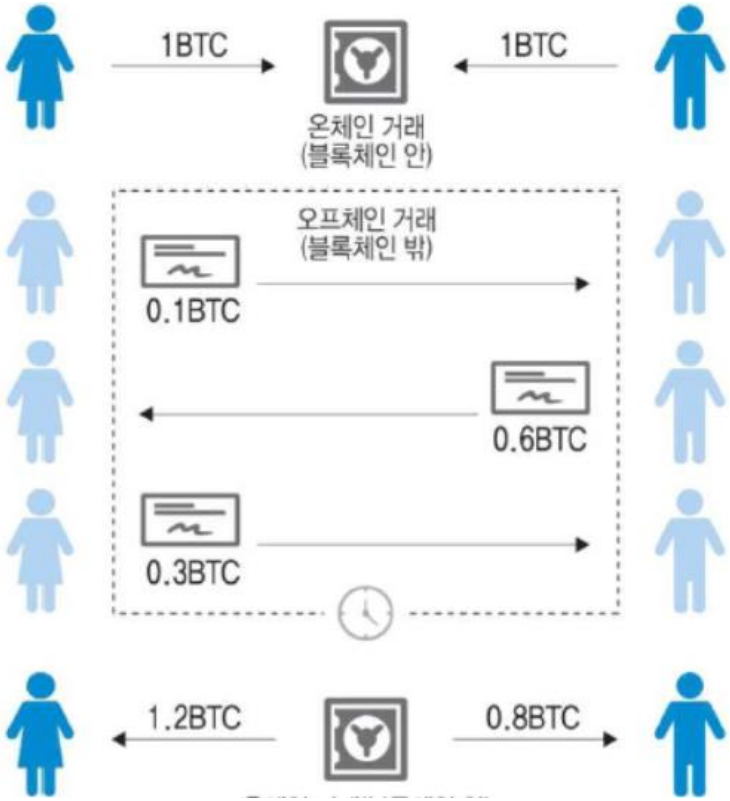
150

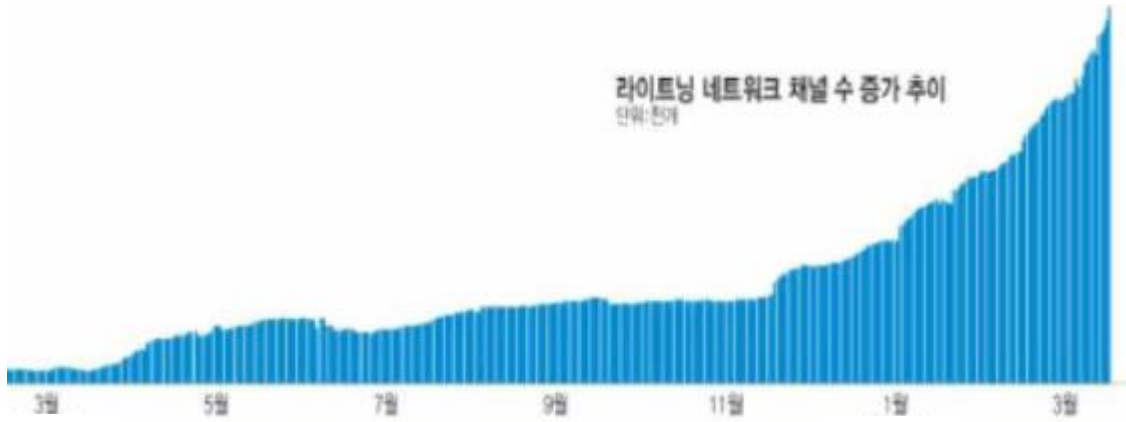
2400

4500

비트코인 라이트닝 네트워크

- 확장성과 속도 향상 (초당 10만건 목표) 솔루션 (조셉 푼과 태지 드리자 논문, 2015.2)
  - 라이트닝 네트워크 거래 채널 수 39,266개, 1064 BTC (2019.3.18):
    - ✓거래자들 사이에 결제 채널을 만들고, 온체인에 일정량의 비트코인을 예치하고 거래를 진행함.
    - ✓채널이 열린 동안 발생한 거래내역은 블록체인에 직접 기록되지 않고, 최종적인 결제 결과가 온체인에 기록





출처: 블록체인 데이터 모니터링 사이트 1ML

블록체인협회, BLOCKCHAIN 동향과이슈, 2019.4월 제6호

이더리움 개발동향

- 기반기술 개선: 처리속도 향상을 위한합의 알고리즘 Casper (PoW와 PoS 동시 사용) 개발 중
  - Casper FFG (Friendly Finality Gadget) 업데이트를 통한 최종성(Finality) 개선이 중앙화 문제로 연기
    - ✓매 100블록마다 PoS 합의를 통해 Checkpoint를 생성하고 블록체인의 최종성 지점으로 고려하면서 대량의 이더리움 보유자들에게 권한이 집중되는 문제가 발생
  - 사이드체인의 안전성을 개선한 플라즈마(Plasma) 및 플라즈마의 효율성을 개선한 플라즈마 캐시

- Constantinople 하드포크 ('19.3.1)와 Smart Contract 실행 효율성 개선 (가스비 절약)
  - 5개 EIP 개선: 스마트 컨트랙트 보안 개선, EVM(Ethereum Virtual Machine) 성능향상, 채굴 보상 감소
  - EVM 성능 (가스비 절약)을 위한 함수 OPCODE (Bitwise SHIFT 연산, EXTCODEHASH, SSTORE) 추가
    - ✓SSTORE: state 값구분을 세분화 (originValue, currentValue, newValue)하여 변화가 없는 경우, DB 저장과정을 생략

- 확장성 개선 (병렬처리를 위한 Sharding 업데이트)
  - '18년 중반기 예정이던 Main Chain과 Shard Chain 분리가 트리 기반 다단계 블록체인 구조 문제로 연기('19.3.8 기준)

- 탈중앙화를 저해 거래 검증 구조 개선
  - Constantinople 업데이트 시 Validator를 통해야만 블록의 최종성이 보장되는 일부 중앙화된 구조

블록체인 플랫폼의 의미

- 블록체인 개발 현황과 문제점
  - 다양한 블록체인 플랫폼들이 산재하여 서비스 개발 시 선택이 어려움
    - ✓전세계 2099개 블록체인 플랫폼 (출처: coinmarketcap.com, 2018.10.18.)
  - 외산 공개소스 기반의 블록체인 솔루션은 거래 당 수수료, 보안성, 유지보수 및 기술 종속 우려
  - 각 부처별로 진행되는 블록체인 서비스실증 사업은 향후 업무 연계 또는 데이터 공유가 어려움
  - 정부/민간 영역에서 각각 서로 상이한 블록체인 플랫폼 개발로 인한 중복 투자

- 블록체인 플랫폼 개발의 중요성
  - 블록체인 플랫폼은 다양한 서비스 개발에 활용이 가능하여 중소벤처기업 육성이 용이함
    - ✓코어 기능 및 서비스 기능의 모듈화를 통한 레고타입의 블록체인 모듈개발
  - 모바일 플랫폼(Android, iOS 등) 준비미비로 뺏긴 앱 주도권 회복 기회
  - MS, 아마존, 구글 클라우드 시장에 잠식당하고 있는 국내 블록체인 클라우드 서비스(BaaS) 시장 창출

국외 블록체인 vs. 국내 블록체인

2017 2018 2019

블록체인 기술 이슈와 해결 방향

• 블록체인 상용화를 위해 탈중앙화, 빅데이터 저장, 고속합의, UX, 개인정보저장 기능개선

	 As Is	 To-Be
기반	• 저속 합의구조 (PoW) • 저신뢰 합의구조 (DPoS) • 저속 P2P 네트워킹	• 효율적/유연한 합의구조 • 탈중앙화 분산 합의구조 • 저지연 P2P 네트워킹
확장	• 저속 On-Chain 거래 • 키 / 암호 분실 위험 • 취약한 컨텐츠 보안	• Side Chain/Off-Chain/병렬처리 • 분산 키 관리 • 프라이버시 보장 기술/IPFS
응용	• 블록체인 평가체계(없음) • 단일 블록체인 종속 SW개발환경 • 단일 블록체인 기반 플랫폼 구조 • 블록체인 플랫폼의 난립 • 개발자 기반 스마트 컨트랙트	• 블록체인 기술/성능 평가 • 유연한 SW개발 환경과 UX • 블록체인 플랫폼 간 상호운영성 • 블록체인 표준화 (산업/서비스) • 사용자 기반 스마트 컨트랙트

2018년 과기정통부 R&D 과제

과제명	과제 내용
실시간 대용량 데이터 유통을 위한 온-오프 하이브리드 블록체인 기술 개발	• 하이브리드 블록체인 및 대용량 데이터 유통을 위한 합의알고리즘 설계 진행, 온-오프체인 연동 CID(Content Identifier) 기술 개발
마이크로그리드 보안 및 운영 효율성을 위한 블록체인 기반 임베디드 기기 및 플랫폼 개발	• 블록체인 플랫폼 소프트웨어 구조, IoT와 블록체인 연동을 위한 디바이스 및 실시간 통신·제어 프로토콜 설계
블록체인의 트랜잭션 모니터링 및 분석 기술개발	• 블록체인 트랜잭션 모니터링 및 분석 시스템 구현, 블록체인 모니터링 네트워크 구축(안) 마련
위치기반 블록체인 시스템 개발	• KAILOS(KAIST Indoor Positioning System) 위치기반 블록체인 시스템 원형 구현 및 위치기반 블록체인의 도시범위 적용을 위한 도시 라디오맵 구축 시스템 개발
블록체인 시스템의 상호 연동을 위한 HCB-Net 개발	• Circle Chain 설계 및 모듈 개발, 블록체인 Connect 프로토콜 및 알고리즘 개발

2019년 과기정통부 R&D 신규과제

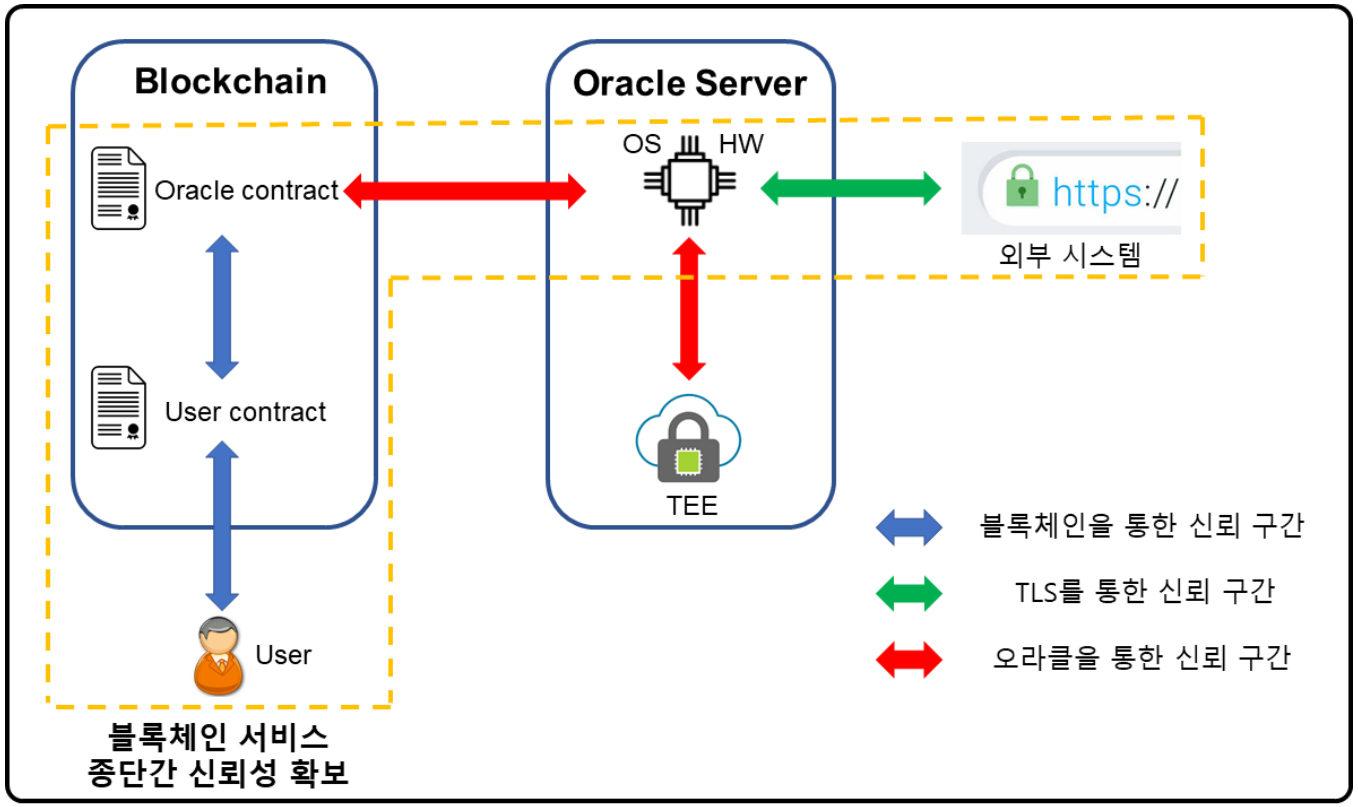
• 과제 12개 예산 : 78억원, 연구기간 2년

(백만원)

번호	과 제 명	예산	공모 방식
1	블록체인을 활용한 분산형 자기주권 신원정보 관리 기술 개발	1,200	지정 공모
2	블록체인 외부 정보 접근을 위한 스마트 컨트랙트 오라클 기술 개발	600	지정 공모
3	블록체인간 트랜잭션 및 블록 전파 지연 문제 해결	800 (400*2개)	자유 (문제)
4	블록체인 트랜잭션에 따른 최적 합의 알고리즘 문제 해결	800 (400*2개)	자유 (문제)
5	블록체인의 개인 콘텐츠 추적과 소멸 수정을 위한 잊혀질 권리 문제 해결	800 (400*2개)	자유 (문제)
6	스마트 컨트랙트 정형명세 블록체인 핵심 기술	600	자유 공모
7	부정거래/수급 특화 블록체인 응용 플랫폼	500	자유 공모
8	학술논문 특화 블록체인 응용 플랫폼	500	자유 공모
9	전자문서 특화 블록체인 응용 플랫폼	500	자유 공모
10	콘텐츠 특화 블록체인 응용 플랫폼	500	자유 공모
11	공유경제 특화 블록체인 응용 플랫폼	500	자유 공모
12	물류 특화 블록체인 응용 플랫폼	500	자유 공모

스마트 컨트랙트 오라클(Oracle)

- 블록체인 외부 데이터를 사용하는 스마트 컨트랙트 수행 시, 입력데이터의 신뢰성을 제공
  - TEE(Trusted Execution Environment)를 활용한 Enclave (보안 구역)를 통해 데이터 신뢰성 보장
  - 블록체인 처리 데이터의 검증 또는 스마트계약의 계약조건 매칭여부를 판단하기 위해 사용됨
  - 스마트 컨트랙트에 기술된 계약조건에 해당하는 블록체인 외부 데이터 또는 API (Application Program Interface)를 통해 필요한 시스템에 연계할 경우 데이터 무결성을 보장
  - 오라클(Oracle) 솔루션: 오라클라이즈(Oraclize), 체인링크(Chainlink), 아이캐시(iCash), 톰슨로이터원



국내 블록체인 기술개발 방향

- 글로벌 거대자본과 대응하는 국내 벤처기업의 경쟁력 강화
  - 확장성, 탈중앙화, 프라이버시 문제를 동시 해결하는 플랫폼 개발은 리스크가 있는 도전적인 과제임

- 다양한 서비스 요구사항에 대응하기 위한 블록체인 코어 기술의 체계적인 개발
  - 개별 블록체인 기업의 공통 개발 요구사항을 반영한 공동개발 기술 도출
  - 업계의 서비스별 기술이 선택 가능한 적응형 (Adaptive) 모듈방식 기능 제공
  - 블록체인 솔루션의 목적별 특화된 서비스 및 플랫폼 난립으로 인한 Silo 현상 극복
    - ✓전세계 블록체인 플랫폼 수는 2099개(출처: coinmarketcap.com, 2018.10.18.)

- 이기종 블록체인 간 연계를 위한 상호운용기술 개발
  - Interchain 또는 Interledger와 같은 상호운용성 기술과 모듈관리 툴 개발
  - 기업 또는 사용자의 블록체인 정보 접근성을 위한 공통 인터페이스 (API) 개발

- 공통 응용을 위한 블록체인 플랫폼으로 업무 연계 또는 데이터 공유 이슈 개선
  - 관세청 블록체인 3개 사업에서 3가지 사업자의 솔루션 적용 (삼성 SDS, 아이콘 루프, 마크애니)
  - 2018년 시범사업에 3개의 상이한 플랫폼 기반 서비스 실증 (하이러레저, 아이콘루프, 블로코)
  - 각 부처별, 부처내 블록체인 서비스 개발에 따른 중복투자 개선