http://blockchain2019.ieieweb.org

2019

블록체인으로 여는 미래사회 워크샵

일 시 : 2019년 6월 17일(월)~18일(화)

장 소 : 건설회관 3층 대회의실

주 최 : 대한전자공학회 통신/컴퓨터 소사이어티

IEIE 대한전자공학회
The Institute of Electronics and Information Engineers

I·N·V·I·T·A·T·I·O·N

초대의 글

4차 산업혁명의 최신 기술로 AI (Artificial Intelligence) 기술과 더불어 블록체인 기술이 최근 비약적으로 발전 중에 있습니다. 블록체인은 다른 어떤 기술보다도 산업계의 비즈니스 측면에서 중요도가 증가하고 있습니다. 특히 에너지, 의료, 법률, 광고, 금융, 컨텐츠, 디지털 신분증, Supply Chain Management, 스마트 팩토리, 스마트 시티 등 다양한 분야를 중심으로 사회 전반에 적용되고 있습니다. 블록체인은 현재의 물리적인 사회 및 경제를 디지털 형태의 사회 및 경제로 변환하는 데 있어서 혁신적인 기술로 앞으로도 기술 개발 및 응용의 가치는 매우 높다고 봅니다.

블록체인은 신뢰할 수 있는 분산 (탈중앙화) 어플리케이션 플랫폼을 제공하는 기술 (Decentralized Ledger Technology)로 비트코인을 통해 암호화폐로써 대중화되었으며, 이후 이더리움 등으로 확장 발전하고 있으며 위에 언급된 다양한 분야에서 응용되고 있습니다. 그러나 블록체인은 태생적으로 scalability, efficiency, resource consumption, security, interoperability 등 많은 문제를 가지고 있으며, 이러한 이슈는 학계, 연구계 및 산업계를 중심으로 다양한 시각에서 해결책이 모색되고 있습니다.

본 워크샵에서는 블록체인의 다양한 응용 사례 및 기술 개발 동향, 현재 진행되고 있는 DLT 연구 개발 이슈들을 폭넓게 살펴보고, 블록체인 구축 실습을 통해 경험과 지식이 부족한 일반인들에게 기본 동작 원리에 대한 이해를 제공하자고 합니다. 또한 블록체인이 우리 사회 전반에 걸쳐 영향을 미치게 됨에 따라 이를 법률 및 금융 산업, 산업계 하드웨어 개발 현황, AI 및 전자정부에 미치는 영향으로 나누어 살펴보고자 합니다.

이번 워크샵을 위해 귀중한 시간을 내어주신 발표자와 참석자 여러분, 그리고 차별화된 워크샵 준비를 위해 수고해주신 여러분들께 감사 드리며, 적극적인 참여와 발표, 토론을 통해 생동감 있는 워크샵이 될 수 있도록 많은 협조를 부탁 드립니다. 감사합니다.

2018년 6월

대한전자공학회 회장 최천원
워크샵 조직위원장 공준진
워크샵 프로그램위원장 이흥노, 황성운

워크샵 운영위원 (조직/프로그램)

조직위원장 공준진 학회 부회장 (삼성전자 마스터)

조 직 위 원 노원우 학회 상임이사 (연세대 교수)
이한호 학회 상임이사 (인하대 교수)
정찬호 학회 상임이사 (한밭대 교수)
김은원 학회 상임이사 (대림대 교수)

프로그램위원장 이흥노 학회 통신소사이어티 회장 (GIST 교수)
황성운 학회 상임이사 (홍익대 교수)

프로그램위원 이정우 학회 상임이사 (중앙대 교수)
이종혁 교수 (상명대)
권태경 교수 (연세대)
김현식 팀장 (KETI)
이원석 박사 (ETRI)

P·R·O·G·R·A·M

프로그램

첫째날 : 6월 17일 (월) : 건설회관 3층 대회의실

시 간	세부 프로그램	강연
09:30 ~ 10:00 (30분)	최신 국내외 산업계 주요 블록체인 응용 사례 소개	박세열 상무 (한국 IBM)
10:00 ~ 10:30 (30분)	개회사 환영사 격려사	최천원 회장 (대한전자공학회) 김기선 총장 (GIST) 오정근 회장 (한국 ICT 금융학회)
Part Ⅰ : 블록체인 정책		**좌장 : 황성운 교수 (홍익대학교)**
10:30 ~ 11:00 (30분)	블록체인 기술과 개발 방향	김종현 PM (IITP)
11:00 ~ 11:30 (30분)	최신 블록체인 기술 개발 동향 소개	이종혁 교수 (상명대학교)
11:30 ~ 12:00 (30분)	패널 토론 : 황성운, 김종현, 이종혁	–
Part Ⅱ : 최신 블록체인 기술 동향 (블록체인 확장성, 연결성, 개인정보)		**좌장 : 공준진 마스터 (삼성전자)**
13:00 ~ 13:30 (30분)	Scalable DeSecure Blockchain	이흥노 교수 (GIST)
13:30 ~ 14:00 (30분)	블록체인 플랫폼 간 연동을 위한 Interoperability 기술 개발 및 표준화 현황	이원석 박사 (ETRI)
14:00 ~ 14:30 (30분)	Lightning network	김형식 교수 (성균관대학교)
14:30 ~ 15:00 (30분)	How does PUF solve Blockchain problems?	김민석 대표 (㈜EpitomeCL)
15:00 ~ 15:30 (30분)	패널 토론 : 공준진, 이흥노, 이원석, 김형식, 김민석	–
Part Ⅲ : 블록체인 구축과 Smart Contract 실습		
15:40 ~ 18:00 (140분)	[실습] Ethereum 네트워크 구축 및 Smart Contract 구현 실습 * 노트북 필요 (지참)	최윤호 교수 (부산대학교)

둘째날 : 6월 18일 (화) : 건설회관 3층 대회의실

시간	세부 프로그램	강연
Part Ⅰ : 블록체인 응용 사례		**좌장 : 이정우 교수 (중앙대학교)**
09:00 ~ 09:25 (25분)	블록체인 현상과 응용사 례 (디지털 신분증, 의료, 법류, 광고, 금융, 컨텐츠)	고 란 기자 (조인디)
09:25 ~ 09:50 (25분)	블록체인과 Climate-Smart City	정순혁 부단장 (아태 핀테크그룹)
Part Ⅱ : 블록체인 정책 및 법적 이슈		**좌장: 구태언 테크앤로 부문장**
10:00 ~ 10:20 (20분)	전통적인 증권규제와 토큰 이코노미	이해붕 부국장 (금융감독원)
10:20 ~ 10:40 (20분)	블록체인 혁명에 대비한 주요국의 정책 동향	구태언 변호사 (법무법인 린)
10:40 ~ 11:00 (20분)	블록체인과 법적 이슈 동향 (규제혁신, 규제샌드박스, STO, 거래소 관련 법령 등)	정재욱 변호사 (법무법인 주원)
11:00 ~ 11:20 (20분)	국내외 블록체인 법제화 및 사법 시스템 이슈	김경환 변호사 (법무법인 민후)
11:20 ~ 12:00 (30분)	패널토론 : 고 란, 이해붕, 구태언, 정재욱, 정순혁, 김경환	-
Part Ⅲ : 블록체인경제와 금융		**좌장 : 오정근 건국대 교수**
13:00 ~ 13:25 (25분)	블록체인 혁명과 신 인류문명	오정근 교수 (건국대학교/ 한국 ICT금융 학회장)
13:25 ~ 13:50 (25분)	블록체인과 금융정책의 미래	김양우 교수 (수원대학교) (전)금융경제 연구원장
13:50 ~ 14:15 (25분)	블록체인 경제	홍기훈 교수 (홍익대학교)
14:15 ~ 14:40 (25분)	블록체인 : 디지털자산혁명	인 호 교수 (고려대학교)
14:40 ~ 15:20 (40분)	패널토론 : 오정근, 김양우, 홍기훈, 인 호	-
Part Ⅳ : 블록체인기술 및 전자정부 미래 전망		**좌장 : 주일택 소장**
15:30 ~ 15:55 (25분)	AI와 블록체인	이영환 대표 (㈜딜라이트체인)
15:55 ~ 16:20 (25분)	외부 정보 접근을 위한 Smart Contract Oracle 기술 개발	주일택 소장 (㈜ IoTrust)
16:20 ~ 16:45 (25분)	블록체인 하드웨어 가속기 및 지갑 개발 현황	현영권 대표 (㈜미디움)
16:45 ~ 17:10 (25분)	블록체인으로 여는 전자정부	민경식 박사 (한국인터넷진흥원)
17:10 ~ 17:50 (40분)	패널 토론 : 이영환, 정순형, 주일택, 현영권, 민경식	-
17:50 ~ 18:00 (10분)	폐회사	-

* 주최측의 사정으로 프로그램이 일부 변경될 수 있습니다.

C·O·N·T·E·N·T·S

목 차

둘째날 : 6월 18일 (화) : 건설회관 3층 대회의실

Part I : 블록체인 응용 사례

좌장 : 이정우 교수 (중앙대학교)

Part II : 블록체인 정책 및 법적 이슈

좌장: 구태언 테크앤로 부문장

Part III : 블록체인경제와 금융

좌장 : 오정근 건국대 교수

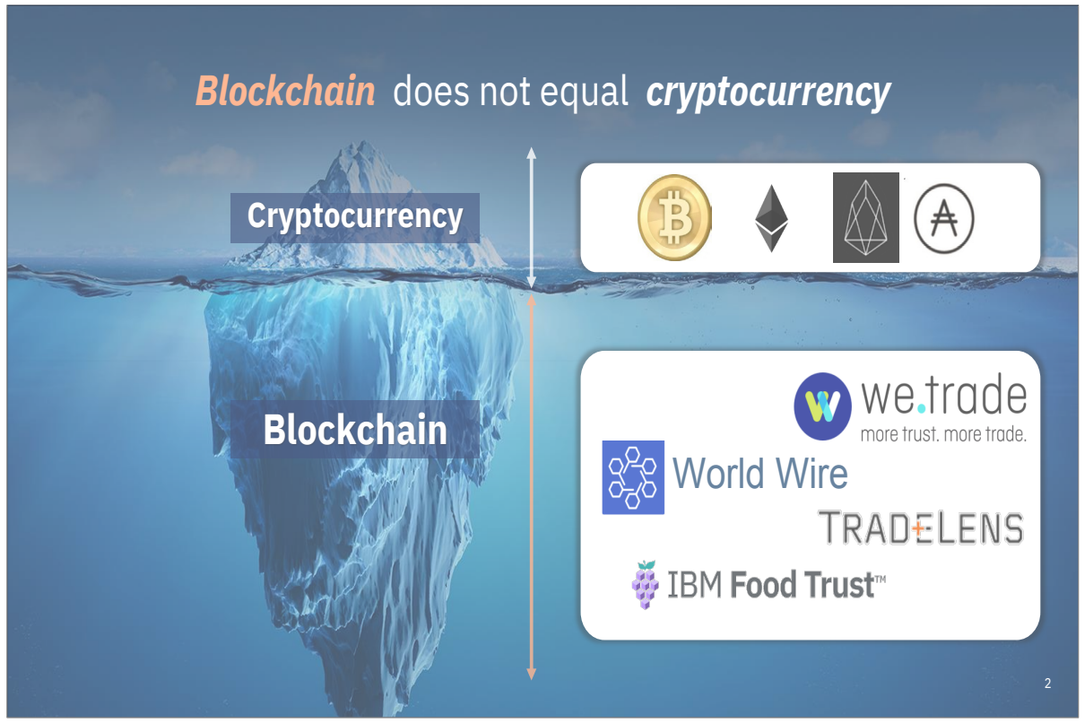
Part IV : 블록체인기술 및 전자정부 미래 전망

좌장 : 주일택 소장

최신 국내외 산업계
주요 블록체인 응용 사례 소개

박세열 상무
(한국 IBM)

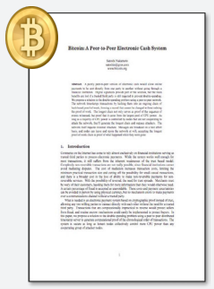

블록체인으로 여는 미래사회 워크샵
최신 국내외 산업계 주요
블록체인 응용사례 소개
2019년 6월 17일
IBM


Blockchain does not equal cryptocurrency
Cryptocurrency
Blockchain
we.trade
more trust. more trade.
World Wire
TRADELENS
IBM Food Trust™
2

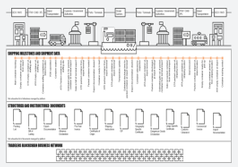
1. 블록체인 동향

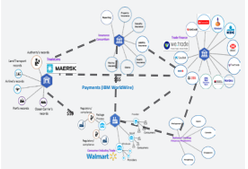
Blockchain 4.0 generation

Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Blockchain 4.0
비트코인	스마트 컨트랙트	산업생태계 모델	산업생태계 융합
• 비트코인 기반의 단순한 통화/화폐로서의 블록체인	• 스마트 컨트랙트 기능을 활용하여 필요한 참여자간 합의를 블록체인 기술로 실현	• 산업의 상용서비스로 블록체인 기술을 활용하여 자산추적, 불변성, 합의, 거래의 최종성(Finality)를 제공하는 산업생태계	• 다양한 산업생태계들 간의 융합으로 확산의 가속화 (Network of Networks) • 토큰(Token) 이코노미 확산



ethereum





3

1. 블록체인 동향

Blockchain in 2019

Technologies

- Bitcoin
- Ethereum
- Hyperledger
- CORDA
- Ripple
- BigChainDB
- Quorum
- Stellar
- +++

Topics

- Shared Ledger & smart contracts
- Public, private
- Permissioned, permission-less
- Tokens and incentive mechanisms
- Identity and Zero Knowledge
- Consensus mechanisms
- On-chain, off-chain
- Systems integration
- Inter-ledgering
- Physical-digital with IOT

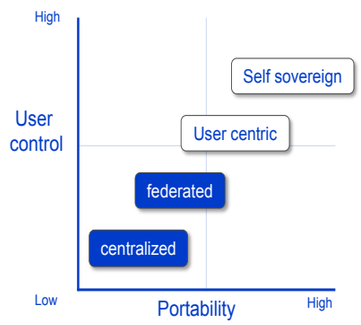
Communities

- Bitcoin
- Ethereum
- Linux Foundation / Hyperledger
- EEA
- ISO/TC 307 – Blockchain & DLT
- IEEE Blockchain
- W3C Blockchain Community
- Accord Project
- Sovrin
- DIF

4

1. 블록체인 동향

Self-Sovereign Identity



sovrin identity for all
Non-profit foundational network

DIF
Self sovereign identity providers

OPEN
Interoperability & standards

OASIS
Decentralized key management system

W3C®
Standards specification for specifying and verifying credentials

HYPERLEDGER
Linux Foundation: Project Indy
Open source implementation

5

1. 블록체인 동향

산업의 유스케이스

은행
- Supply chain and trade finance
- Know your customer
- Transaction banking, payments and digital currencies

자본시장
- Post trade
- Unlisted security and private equity funds
- Reference data
- Cross currency payments
- Mortgages

유통
- Supply chain
- Loyalty programs
- Information sharing (supplier – retailer)

공급망
- Workflow digitization
- Supply chain visibility
- Provenance and traceability

헬스케어
- Mediated health data exchange
- Clinical trial management
- Outcome based contracts
- Medicine supply chain

제조
- Supply chain
- Product parts
- Maintenance tracking

공공
- Asset registry
- Citizen identity
- Fraud and compliance

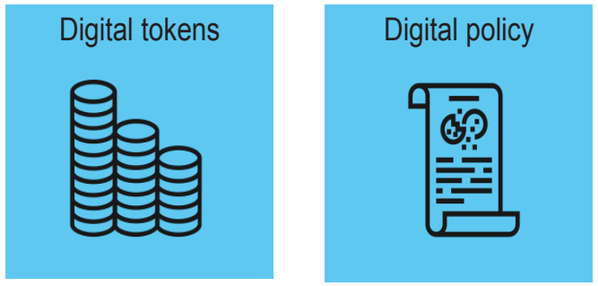
보험
- Complex risk coverage
- Group benefits
- Parametric insurance
- Asset usage history
- Claims filing

6

2. 토큰노믹스

기업 비즈니스를 위한

Token 기반 Permissioned Blockchain



2. 토큰노믹스

Stronghold USD Stable Coin

✓ 미국의 Stronghold 금융회사는 USD에 고정된 스테이블코인을 발행 및 관리를 통해 실시간 결제 네크워크를 구축

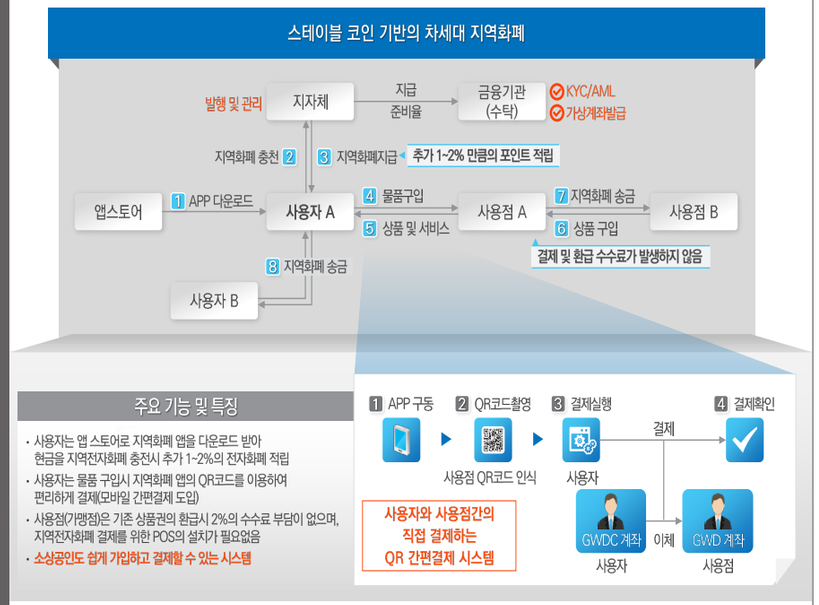
특징 및 시사점

- Stronghold USD는 은행의 예치금으로 뒷받침 됨
- 다른 스테이블코인에 비해 Stronghold USD는 US 은행에 의해 뒷받침 되며, AML 및 KYC 규정을 준수함
- 스텔라 프로토콜은 스텔라 네트워크에서 다양한 디지털 자산과 자산 클래스를 확장 가능하고 효율적으로 발행 할 수 있는 기능 제공
- Stronghold USD는 모든 거래 활동을 지원하는 실제 미국 달러에 대한 법적 대체 자산으로 활용됨

2. 토큰노믹스

차세대 지역화폐

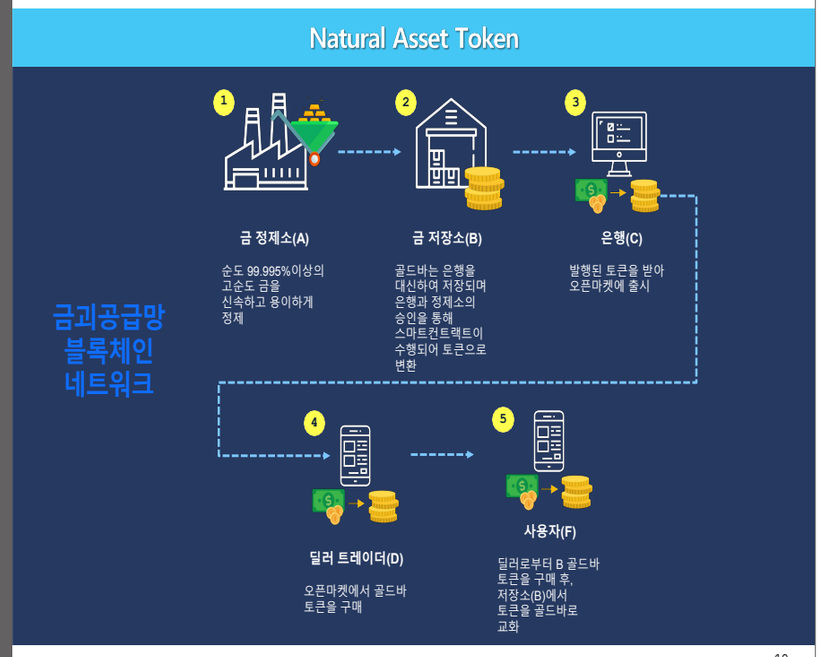
✓ 지자체/사용점/사용자 관점에서 지역경제를 활성화하기 위한 블록체인 기반의 차세대 지역화폐 플랫폼으로 법정화폐에 고정된 안전자산으로 사용이 편리하고 유통비용을 절감함



2. 토큰노믹스

Bullion Supply Chain

✓ 광산부터 소비자에 이르기까지의 공급망에서 자산의 투명한 추적



2. 토큰노믹스

Plastic Bank

- ✓ 아이티 국가에서 폐 플라스틱을 수집한 사람들에게 그에 대한 댓가로 디지털토큰으로 지불
- ✓ 사용자들은 디지털 토큰으로 교육비, 생활용품 구입 등의 용도로 활용

plasticbank

Utility Token

플라스틱 뱅크 | 아이티 국가(Haiti)

특징 및 시사점

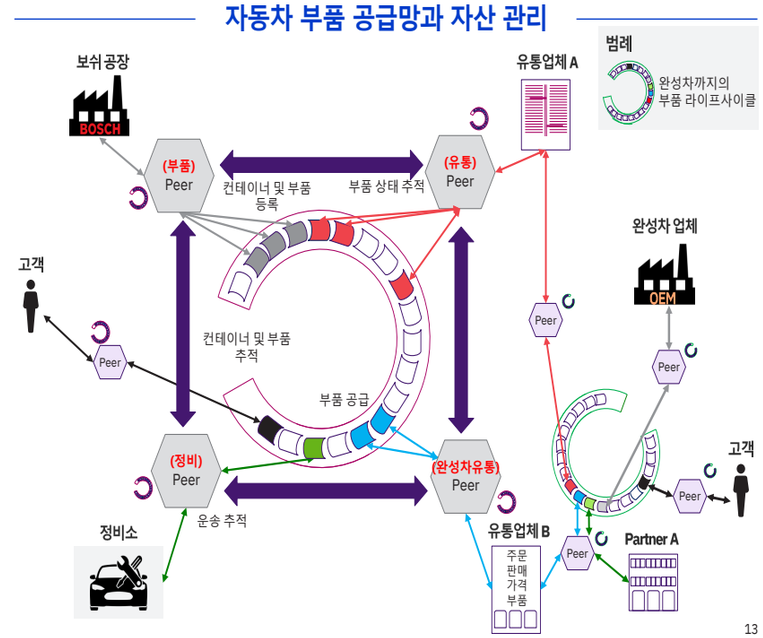
- 매년 약 800 만톤의 플라스틱이 우리 해양에 유입될 정도로, 플라스틱 폐기물은 사회적, 환경적 처리비용의 증가를 야기하고 있으며, 아울러 **폐플라스틱의 재활용과 재이용을 위한 혁신적인 기술개발에 많은 관심 집중**
- 플라스틱을 블록체인에 기반한 디지털 토큰으로 교환함으로써 플라스틱에 대한 가치를 표현함
- 사용자들은 스마트폰 앱의 디지털토큰을 통해서 상점에서 물품을 구입할 수 있으며, 교육비 납부, 의료보상 가입, 전기료 납부등 다양한 영역으로 확대됨
- 현금의 분실위험도 없으며, 활용이 매우 쉬움

3. 글로벌 사례

BOSCH 부품 공급망

- ✓ 보쉬는 블록체인을 활용한 자동차 부품이력관리 시스템을 구축

자동차 부품 공급망과 자산 관리



600 이상의 고객들과 블록체인 프로젝트를 진행중 ...

금융

- 무역금융: Bank of America Merrill Lynch, HSBC, we.trade
- 장외거래상품: DTCC, CLS
- KYC 신원확인: Crédit Mutuel ARKEA, SECURE KEY
- 채널 파이낸싱: IBM Global Financing

제조/에너지

- 원산지 추적/인증: everledger, BOSCH, BOEING
- 유효 재생에너지 관리: Tennet
- 제약제조 공급망관리: 合佳医药, Hebei Hejia Pharmatech Group Co., Ltd

유통/물류

- 식품안전: Walmart, Driscoll's, Tyson, McLane, Dole, Kroger, Nestlé, Unilever
- 글로벌 물류무역 디지털화: MAERSK LINE, PSA The World's Port of Call
- 물류무역: GOVERNMENT OF DUBAI

공공

- 건강정보 데이터교환: FDA, CDC
- 탄소배출권 관리 플랫폼: Chinese Energy-Blockchain Labs
- 공공자전거 등록/결제: RDW

3. 글로벌 사례

Cobalt 공급망 추적관리

- ✓ 콩고에서 열악한 노동환경 하에 아동을 포함한 노동자에 의해 채취된 코발트 사용을 스스로 금지
- ✓ '윤리적 코발트'를 활용을 위하여 블록체인 기술 활용

코발트 공급망 추적관리 블록체인 네트워크

3. 글로벌 사례

Re-imaging digital business processes

TRADELENS

- **물류 무역 생태계**
  선사, 항구 및 터미널, 세관, 육상운송업체등이 참여하는 물류무역 네트워크
- **실시간 정보 공유**

15%
물류무역 공급망의 비효율적인 프로세스를 개선

IBM Food Trust™

- **식품공급체인 관리**
  비용 및 리콜을 줄이고 문제가 된 식품의 원인 추적 가능
- **엔드 투 엔드 투명성 확보**

10%
매년 식중독으로 고생

World Wire

- **글로벌 외국환 송금/결제망**
  전 세계 47개 통화, 44개 은행 접점을 포함해 72개국이 참여하는 글로벌 외국환 송금/결제 네트워크
- **국가간 결제모델의 대안**

5천조원
하루에 일어나는 통화거래

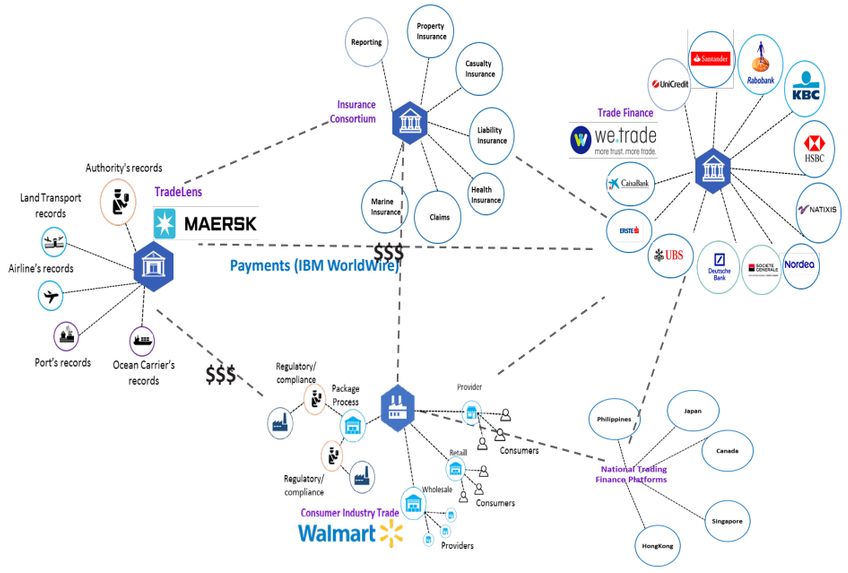
we.trade
more trust. more trade.

- **금융무역 플랫폼**
  유럽의 14개 은행이 참여하는 금융무역 컨소시엄
- **무역금융 기능 지원 및 효율화**

50%
중소기업들이 은행의 금융서비스 받기위한 인프라 부족

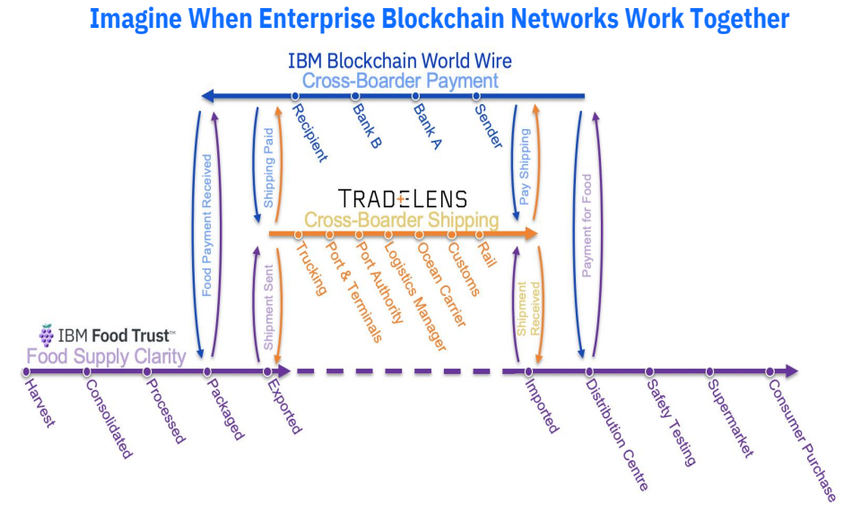
4. 블록체인의 미래

Blockchain 4.0 – 산업 생태계 융합



4. 블록체인의 미래

물류 무역 네트워크와 연동하는 타 네트워크



박 세열

- 現 IBM 블록체인 기술총괄(상무)
- 現 이화여자대학교 컴퓨터공학과 겸임교수
- 現 The Open Group Distinguished Architect

IBM

Mobile: +82-10-4995-7163

E-mail: sypark@kr.ibm.com or park.seyoul@ewha.ac.kr

The Open Group Open Certified
Distinguished Architect

첫째날

6월 17일(월)

건설회관 3층
대회의실

Part Ⅰ

블록체인 정책

좌장 : 황성운 교수
(홍익대학교)

블록체인 기술과 개발 방향

김종현 PM
(IITP)

블록체인 예타사업 2019

- 블록체인 예비타당성 조사 사업 추진 계획

블록체인·융합 PM
김 종 현

IITP

블록체인 기술의 의미

"블록체인은 세상을 바꾸는 기술이다"

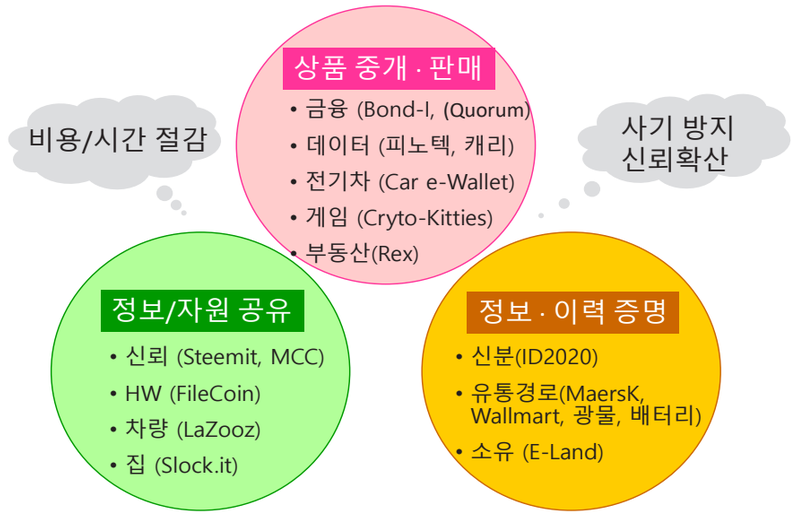
블록체인 인터넷 or 인터넷 컴퓨터 ?

- Trusted Network
  – 탈중앙화 기반의 제3자 신뢰 제공 기반
- Network Solution
  – 다양한 데이터를 공유하는 네트웍 솔루션
- Collaboration Tool
  – 개별 운영 시스템을 유지하면서 동등하게 협업이 가능한 툴

2

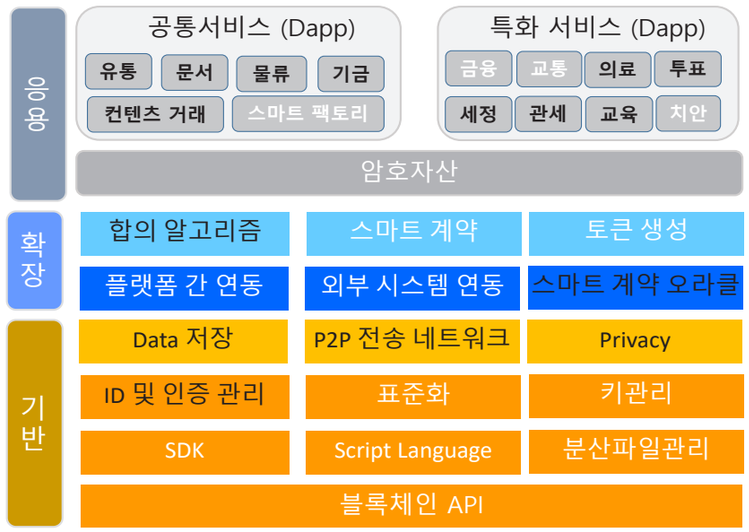
블록체인 기반 비즈니스 모델

- 블록체인은 Information Infrastructure 모델로 정보를 활용하는 모든 분야에 적용
  - 일반 공개 정보 또는 특정 그룹 대상 공개 가능한 정보이면서, 정보의 진위가 중요한 정보
  - 시간이 경과하면서, 축적되는 대량 데이터를 블록단위로 나누어 영구히 저장



블록체인 기술구조

- 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
  - 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

블록체인 예타 2019 주요 방향

- 3가지 분야 (기술성, 정책성, 경제성) 중 기술성, 경제성 분석 개선 필요

- 원천기술 전략과제(5개)에 비해 과중한 서비스 전략과제(7개) 비중 축소
  - 서비스 과제 축소와 동시에 전체 사업기간을 7년에서 5년으로 기간 단축
  - 서비스 개발후보로 민간주도로 하기 어려운 공공서비스 분야를 도출하고, 해당 부처 협업 강화

- 블록체인 기술에 대한 국가 R&D 투자 논리 보강
  - 다양한 서비스개발에 쉽게 적용할 수 있는 모듈형 블록체인 기술 개발
  - 기업체, 연구소 및 학교에서 개발 중인 기술과 중복성 배제 및 조화
  - 기술수요 조사에 기반한 필요기술 도출 및 기술분류 체계 정립과 기술개발 로드맵과 연계
    - ✓분상장부 기술에 맞는 네트워크 기술, 합의 기술 등 향후 10년 내 도입될 기술 분야 도출

- 기술 상용화와 글로벌 시장진출을 위한 성과목표 명확화
  - 블록체인 성능 지표 (거래처리속도, 데이터 처리용량 등) 개발 및 현실화
  - 국내외 특허 분석을 통한 향후 기술 개발 분야 도출과 특허 관련 성과목표 보강

- 산학연의 균형잡힌 기술 개발 계획과 과제도출의 타당성 강화
  - 산업 (오픈블록체인 협회, 블록체인 산업진흥협회)과 학회 (블록체인 학회, 한국통신학회) 협력 강화

예타사업 방향 2018 vs. 2019

2018 사업명

투명·신뢰 사회 실현과 4차 산업혁명을 선도하는 블록체인 중장기 기술 개발 사업

예산

총 사업비: 총 5,566억 원(7개년)
(국고 4,282억원, 지방비 120억원, 민자 1,164억원)

사업 목적

블록체인 기술·서비스·산업 분야 First Mover

- 기술수준 : '17년 76% → '26년 95%
- 글로벌 제품·서비스 점유율 : '17년 0% → '26년 5%
- 지자체 및 부처 연계 서비스 생태계 구축

주요 연구개발 내용

3대 핵심 분야 14개 전략과제

- 핵심원천기술 : 코어, 안전성, AI 융합 및 표준화 기술
- 검증기술 : 기술 검증 및 신뢰성 평가
- 서비스 및 생태계 : 7대 체인 서비스 및 생태계 구축

2019 사업명

신뢰사회 구현과 상용화 기술 개발을 위한 개방형 · 모듈형 블록체인 기술 개발 사업 (안)

예산

총 사업비: 총 5000여억원 규모 (5개년)
(국고 4,200억원, 민자 800억원)

사업 목적

블록체인 기술 선도국가

- 기술수준 : '18년 76% → '25년 90%
- 글로벌 제품·서비스 점유율 : '19년 0% → '25년 5%
- 다양한 산업분야의 블록체인 서비스에 활용

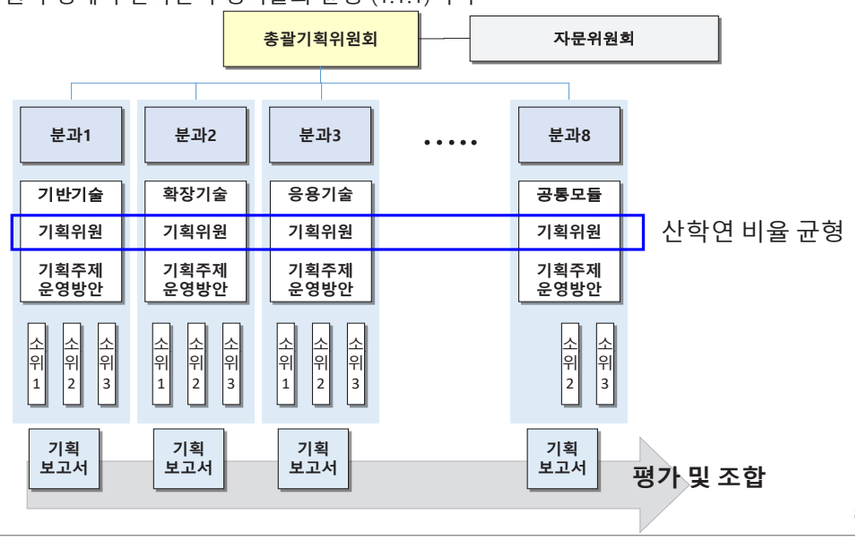
주요 연구개발 내용

3대 기술 분야 10여개 전략과제

- 원천기술 : 블록 생성, 전송, 합의 및 저장 기술
- 확장기술 : 블록체인 외부 연동, 플랫폼 및 표준화 기술
- 응용 서비스 기술

분과별 독립된 기획보고서 작성 후 전체 기획보고서 통합

- 분과별로 단독의 전략과제 보고서 작성 후 전체기획보고서로 통합
  - 분과는 산학연의 특성에 따라 구성 후 단독의 보고서 작성
  - 전체 분과위원 구성에서 산학연 구성비율의 균형 (1:1:1) 추구



기획보고서 작성 시 고려사항

문제 이슈 도출의 적절성

기획 위원 구성 비율 균형

- 산학연, 지역, 전문분야 등을 고려하여 편중되지 않게 전문가 구성

문제 및 이슈 해결 대안으로서의 과제 제시

- 현황 및 예측조사, 현안진단(이해관계자 설문조사, 간담회, 인터뷰, 문헌조사 등)을 통해 이슈 도출
- R&D사업이 다른 정책대안보다 효율적인 대안임을 제시

대형 R&D사업 추진 필요성/당위성 제시

- 민간에서 자율적으로 할 수 있는 사업이 아님을 제시

사업목표의 적절성

기술적 추세 및 기술수준을 고려한 R&D 사업 목표 제시

사업 목표가 달성되면 해당 문제/이슈가 어떻게 해결되는지 구체적으로 제시(as is → to be)

사업 목표의 효과성을 측정할 성과지표를 객관적/정량적으로 제시

사업성과에 대한 수혜자를 구체적으로 제시

세부 추진 전략의 적절성

과제도출 과정의 적절성

- 기술수요 및 활용수요조사를 바탕으로 적정한 근거에 기반하여 과제 풀을 도출하고,
- 객관적인 평가 절차 등을 거쳐 최종 과제를 도출(해당 절차 제시)

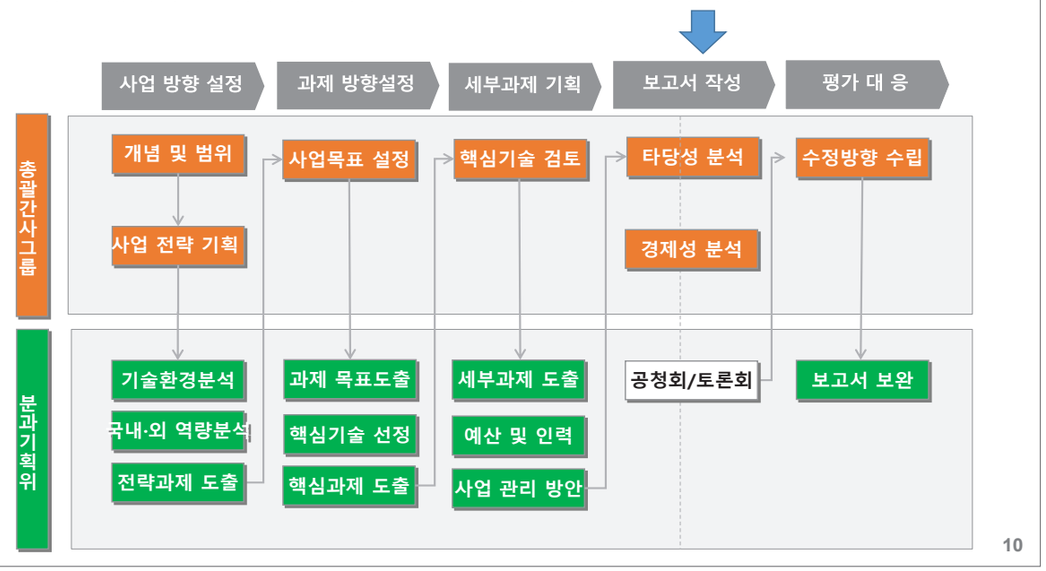
연구개발 특성을 고려한 주체별 추진체계 제시

- 과제 선정 기준 및 성과관리 방안 등을 구체적으로 제시
- 관계 부처/기관과 연계 및 협력 방안

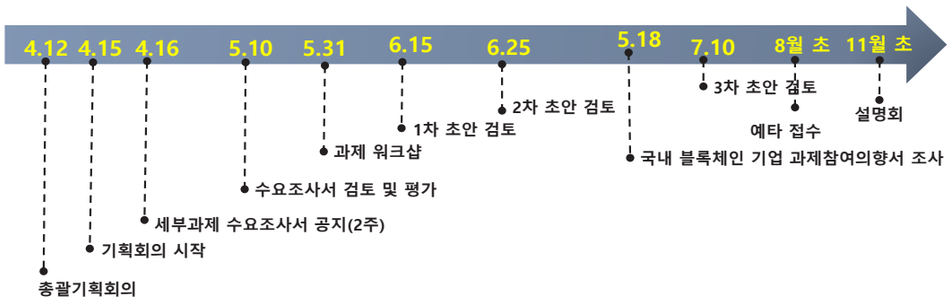
유사 중복사업에 대한 분석을 바탕으로 한 사업의 차별성 제시

기획 단계별 주요 추진 내용

- 분과별 세부과제 보고서와 전체기획보고서 작성 과정에서 특정작성자에 의존
  - 개별 세부과제 보고서의 자료 내용 불균형과 전체 논리 미흡으로 과다 시간 소요



기획 추진 일정



최신 블록체인 기술 개발 동향 소개

이종혁 교수
(상명대학교)

2019.06.17 @ 블록체인으로 여는 미래사회 워크샵 (대한전자공학회)

최신 블록체인 기술 개발 동향 소개
(확장성 이슈: 이더리움 오프체인 솔루션 중심으로)

Jong-Hyouk Lee, Protocol Engineering Lab., Sangmyung University
(jonghyouk@smu.ac.kr)

블록체인 확장성 이슈

Talk Abstract

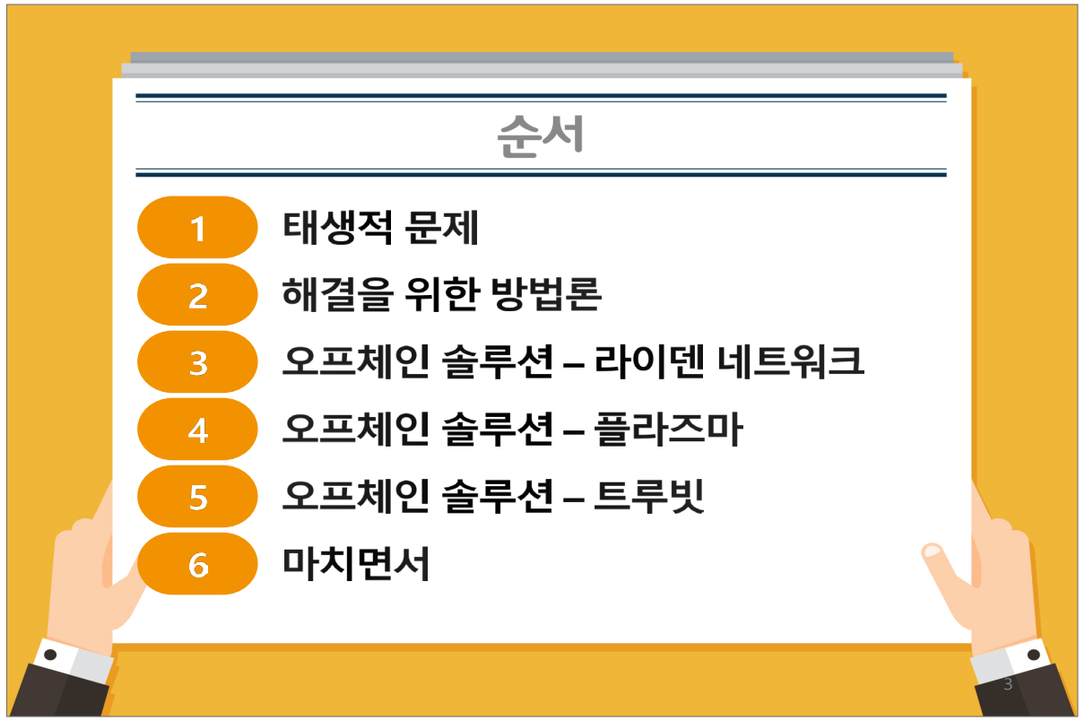
You may have heard about blockchain that is the underlying technology of Bitcoin and other cryptocurrencies. Blockchain is now considered as a big wave to revolutionize not just financial sectors, but any industry where data has to be safely and securely transferred over a non-trusted network like the Internet. However, nowadays the biggest hurdle for blockchain adoption is its scalability issue. In this talk, we focus on blockchain scalability issue. We pick Ethereum scaling solutions, especially off-chain solutions such as Raiden Network, Plasma, and TrueBit.

Speaker: Jong-Hyouk Lee, Ph.D.

- Assistant Professor, Sangmyung University, South Korea, 2013 – Present
- Assistant Professor, TELECOM Bretagne, France, 2012 – 2013
- Researcher, INRIA, France, 2009 – 2012
- Ph.D. from Sungkyunkwan University, South Korea

Blockchain related works

- 과제: 공개형 블록체인 환경에서의 합의 알고리즘 연구, 한국전자통신연구원, 2019
- 과제: 확장 가능한 허가형 블록체인 기반 신뢰 데이터 공유 체계 연구, 한국과학기술정보연구원, 2019
- 과제: 블록체인 기반 신뢰 데이터 공유 시스템 개발, 한국과학기술정보연구원, 2018
- 과제: 블록체인 기반 디지털 콘텐츠 DRM 응용 기술 개발, 한국저작권위원회, 2017-2018
- 과제: 클라우드에서 블록체인 서비스(Blockchain as a Service) 제공 분석 및 요구사항 개발, 한국전자통신연구원, 2017
- 과제: 마이크로그리드 환경에 적합한 블록체인 거래 핵심 기술, 사기업, 2017
- 논문: "Double-spending with a Sybil Attack in the Bitcoin Decentralized Network," *IEEE Transactions on Industrial Informatics*, accepted.
- 논문: "Rise of Anonymous Cryptocurrencies: Brief Introduction," *IEEE Consumer Electronics Magazine*, accepted
- 논문: "BIDaaS: Blockchain based ID as a Service," *IEEE Access*, vol. 6, pp. 2274-2278, 2018.
- 논문: "How the Blockchain Revolution Will Reshape the Consumer Electronics Industry," *IEEE Consumer Electronics Magazine*, 2017.
- 논문: "Blockchain based secure firmware update for embedded devices in an Internet of Things environment," *Journal of Supercomputing*, 2017.
- 논문: "마이크로그리드 환경에서의 스마트컨트랙트 기반 비공개 전력 경매", 한국통신학회, 2018년 6월 (우수 논문상)
- 논문: "이더리움 RLPx, Wire 프로토콜 분석", 한국통신학회, 2018년 1월 (우수 논문상)
- 논문: "블록체인 동작 과정에 따른 보안 분석", 한국정보보호학회, 2017년 6월 (한국전자통신연구원 원장상)
- 논문: "Whisper 기반의 안전한 모바일 메신저 설계", 한국통신학회, 2016년 11월 (우수 논문상)



태생적 문제 – 낮은 TPS

낮은 트랜잭션 처리율(TPS) 과연 언제 실시간 처리에 적합할 수 있을까?

태생적 문제 – 어떻게 TPS 높일까?

TPS 을 높이기 위한 방법? 블록 생성 속도 증가? 블록 크기 확대?

- TPS (Transaction Per Second): 초당 처리 할 수 있는 트랜잭션 (메시지) 의 수
  - 트랜잭션 (메시지) 는 블록에 담겨서 처리 됨
- 블록 생성 속도를 증가 시키려면? (즉, 블록 타임이 짧아지는 것을 의미)
  - 채굴의 난이도를 낮추어야 함
  - 채굴의 난이도가 낮아지면, 엉클 블록의 수가 증가하고 네트워크 보안성이 낮아짐
  - 또한, 엉클 블록의 수가 많아 진다는 것은 마이너의 기대 수익이 낮아지게 되고…이로 인해 높은 해시 파워를 가지는 마이닝 풀만이 살아 남기에 네트워크 중앙화가 가속됨
- 블록 크기 확대? (즉, 더 많은 트랜잭션을 블록에 담는다는 것을 의미)
  - 하나의 블록에 담길 수 있는 트랜잭션의 수가 증가하여, 네트워크 전파 속도가 낮아짐
  - 낮아진 네트워크 전파 속도로 인해, 엉클 블록의 수가 증가 할 수 있음
  - 또한, 블록의 크기가 크기에 해당하는 블록을 처리하기에 더 높은 컴퓨팅 파워가 요구되기에…성능이 좋은 컴퓨터로 마이닝 풀이 유리해 지며…결국 네트워크 중앙화가 가속됨

태생적 문제 – 단순 튜닝의 한계

TPS 을 높이기 위한 방법? 단순 파라미터 튜닝을 통해서는 안됨

- 네트워크 유효 처리량 (E_{th})
  - 블록 타임 내에 블록을 전파 받는 노드의 비율
    - 블록 타임 (block time) = 블록 인터벌 (block interval)
  - 90% 네트워크 유효 처리량이라면 (E_{th} = 90%), 블록 타임 내에 10%의 노드가 해당하는 블록을 받지 못 함
- 처리량 제한
  - 10분 혹은 더 짧은 블록 타임 동안 E_{th} = 90% 일 경우, 블록의 크기는 4 MB 를 넘지 못 함

$$\frac{\text{block size}}{\text{X \% effective throughput}} < \text{block interval}.$$

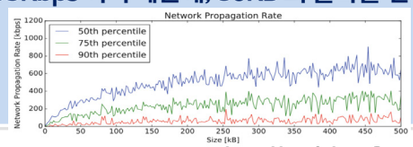
- 블록 타임 제한
  - E_{th} = 90% 일 경우, 유효 대역폭은 55Kbps 이기 때문에, 80KB 의 블록을 전파하기 위해서는 블록 타임이 12초가 요구 됨


On Scaling Decentralized Blockchains
(A Position Paper)

Kyle Croman[1,2], Christian Decker[3,IBM], Ittay Eyal[1,2], Adem Efe Gencer[1,2], Ari Juels[1,2], Ahmed Kosba[1,2], Andrew Miller[1,4], Prateek Saxena[5], Elaine Shi[1,2], Emin Gün Sirer[1,2], Dawn Song[1,6], and Roger Wattenhofer[3]

[1] Initiative for CryptoCurrencies and Contracts (IC3); Ithaca, USA
[2] Cornell University, Ithaca, USA
[3] Jacobs, Cornell Tech, New York, USA
[4] UMD, College Park, USA
[5] ETH, Zürich, Switzerland
{decker@tik.ee.ethz.ch
[6] UC Berkeley, Berkeley, USA
[7] NUS, Singapore, Singapore

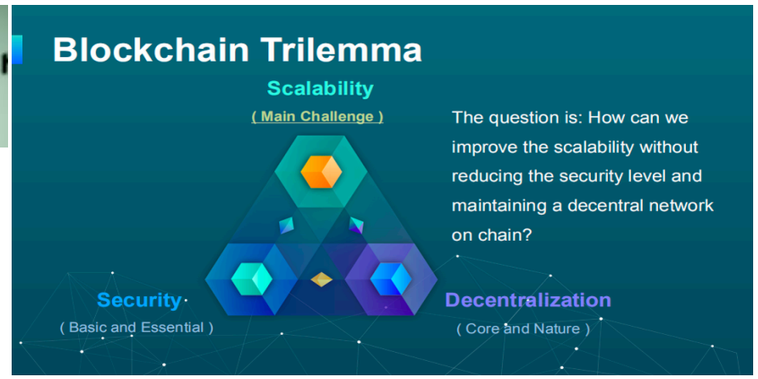
Abstract. The increasing popularity of blockchain-based cryptocurrencies has made scalability a primary and urgent concern. We analyze how fundamental and circumstantial bottlenecks in Bitcoin limit the ability of its current peer-to-peer overlay network to support substantially higher throughputs and lower latencies. Our results suggest that reparameterization of block size and intervals should be viewed only as a first increment toward achieving next-generation, high-load blockchain protocols, and major advances will additionally require a basic rethinking of technical approaches. We offer a structured perspective on the design space for such approaches. Within this perspective, we enumerate and briefly discuss a number of recently proposed protocol ideas and offer several new ideas and open challenges.



태생적 문제 – 트릴레마 문제로 귀결

블록체인 확장성 문제 어떤 것을 양보 할 것인가? 보안 vs. 분산

- Ethereum's Vitalik Buterin states that you can only have two out of either decentralization, scalability or security so trade-offs are almost inevitable.



해결을 위한 방법론

확장성 이슈를 해결하기 위한 방법 온체인 vs. 오프체인 솔루션

- 온체인 솔루션 (Layer-1 솔루션)
  - 블록체인 프로토콜의 자체를 변경함으로써 확장성 이슈를 해결
  - 대부분 하드 포크 필요
  - 예: 이더리움의 캐스퍼 (Casper), 샤딩 (Sharding)
- 오프체인 솔루션 (Layer-2 솔루션)
  - 블록체인 프로토콜의 동작을 변경하지 않고 외부에서 확장성 이슈를 해결
  - 하드 포크 불필요
  - 예: 라이덴 네트워크, 플라즈마, 트루빗

	Description	On/Off Chain	Potential Scaling Improvement	Release Date
Casper	Transition from proof-of-work algorithm to proof-of-stake algorithm.	On	2-5x	5/8/2018
Raiden Network	An off-chain token payment channel network.	Off	10-100x	2018
Plasma	An off-chain layer for smart-contract transacting.	Off	10-100x	2019
Sharding	A division of data amongst servers to prevent single servers from becoming bottlenecks.	On	10-100x	2019

SFOX

오프체인 솔루션 – 라이덴 네트워크 (1/2)

라이덴 네트워크가 필요한 이유? 모든 트랜잭션들이 메인넷에 몰리고 있다!

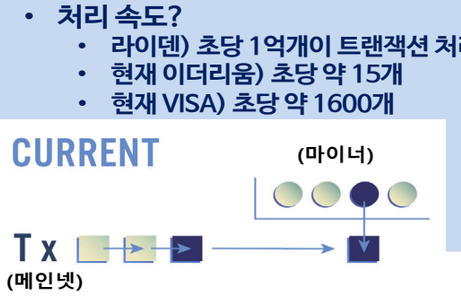
- 이더리움은 ERC-20, ERC-223, ERC-721 등 다양한 토큰을 제공하여, 블록체인이라는 기술을 제공하는 거대 플랫폼으로 성장하고자 함
  - ERC-20 를 통해 스마트 컨트랙트를 제공
- 대부분의 암호화폐는 ERC-20 토큰 기반이며 약 500 여개 이상의 프로젝트가 존재
  - 우리가 알고 있는 상위 100 위의 암호화폐 대부분이 ERC-20 기반으로 제작
- 수많은 ERC-20 토큰 기반 암호화폐, 프로젝트의 트랜잭션들이 모두 이더리움 메인넷으로 유입되며, 메인넷에서 처리를 해야 하는 상황
  - 이더리움이 블록체인 거대 플랫폼으로 성장 했다는 증거이지만, 확장성 문제
  - 트랜잭션들이 메인넷에 저장 되어야 함
  - 메인넷에서의 트랙잭션 처리 결과(지연 등)가 ERC-20 토큰 기반 암호화폐, 프로젝트에 직접적으로 영향

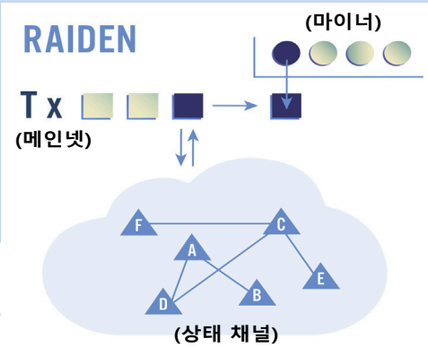
< 크립토키티 출시후 지연 상태에 있는 트랜잭션의 수 >

오프체인 솔루션 – 라이덴 네트워크 (2/2)

별도의 채널에서 토큰 처리 후 결과만 메인넷에 반영 라이트닝 네트워크?

- 상태 채널 (State channel)을 통해 외부에서 토큰 처리를 하고, 그 결과만을 메인넷에 반영하여 메인넷에 유입되는 트랜잭션의 양을 궁극적으로 줄임
  - 메인넷의 부하 (트랜잭션의 양, 트랜잭션의 처리 속도)가 줄어 듬
  - 각 상태 채널에서 필요한 동작을 수행하기에 다른 상태 채널과는 무관
  - 각 상태 채널에서 수행 된 과정는 블록체인과 될 필요 없음
- 처리 속도?
  - 라이덴) 초당 1억개이 트랜잭션 처리 가능
  - 현재 이더리움) 초당 약 15개
  - 현재 VISA) 초당 약 1600개

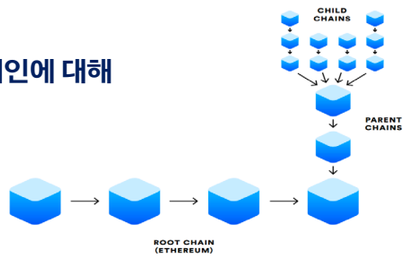




오프체인 솔루션 – 플라즈마 (1/2)

플라즈마 개발 이유? 손쉽게 블록체인을 생성하고 다양한 생태계 조성!

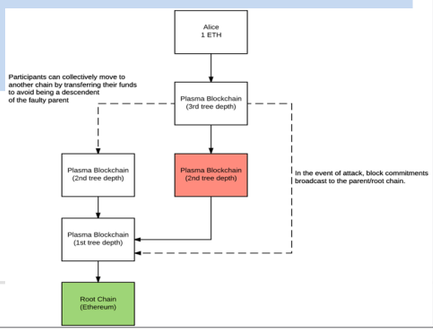
- 이더리움은 블록체인 기술을 제공하는 거대 플랫폼으로 성장하고자 함
  - 이더리움 메인넷은 하나의 블록체인 네트워크
  - 특정한 목적에 따라 개별적인 블록체인의 생성을 허용하여 서비스별 블록체인 허용
- 플라즈마는 블록체인(메인넷)에 연결 된 또 다른 블록체인이 가능케 함
  - 계층적인 구조를 가지는 블록체인들의 연결성 제공
  - 트리 형태의 블록체인 구조
- 블록체인(메인넷)에 연결 된 (무수히 많은) 블록체인에 대해 어떻게 확장성을 제공 할 것인가?



오프체인 솔루션 – 플라즈마 (2/2)

꼬리에 꼬리를 물고 있는 블록체인에게 어떻게 확장성을 제공할 것인가?

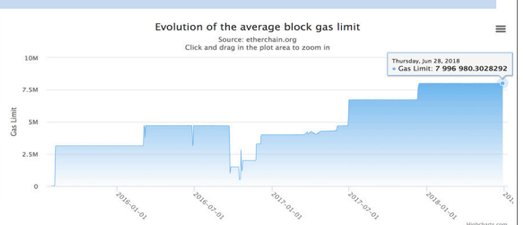
- 메인넷 블록체인 vs. 플라즈마 블록체인
  - 개별 서비스를 위한 플라즈마 블록체인을 트리 형태(부모-자식)로 구성
  - 메인넷 블록체인은 플라즈마 블록체인의 최상위 노드(최상위 부모 블록체인)과 연결
- 플라즈마 블록체인에서의 트랜잭션들은 어떻게 메인넷에 반영 되는가?
  - 하위 플라즈마 블록체인에서의 변경 사항은 상위 플라즈마 블록체인에게만 반영
    - 최상위 플라즈마 블록체인은 메인넷에 반영
  - 플라즈마 블록체인에서 3개의 블록이 생성 될 때 마다, 블록 해시 정보만을 상위에 저장



오프체인 솔루션 – 트루빗 (1/2)

트루빗 - Offchain computation solution TPS가 아닌 연산 능력!

- 스마트 컨트랙트의 명령어 별 가스(gas) 요금과 블록의 최대 가스(gas limit) 지정
  - 이를 통해 무분별한 스마트 컨트랙트의 실행 방지 및 메인넷 건전화
  - 스마트 컨트랙트 복잡도에 비례해 가스 비용이 증가
  - 크기가 큰 (복잡한) 스마트 컨트랙트 실행을 위해서는 큰 비용이 듬
  - 큰 비용을 지불 할 용이가 있다 할지라도 블록 최대 가스로 인해 이마저도 불가능
- 메인넷에서의 연산 한계 해결?
  - 블록 가스 제한(gas limit)을 높이는 방법으로 해결 할 수 있지 않을까?
  - 마이너(verifier)의 딜레마 발생
    - 블록에 탑재 된 코드를 검증?
    - 아니면, 검증하지 않고 진행?

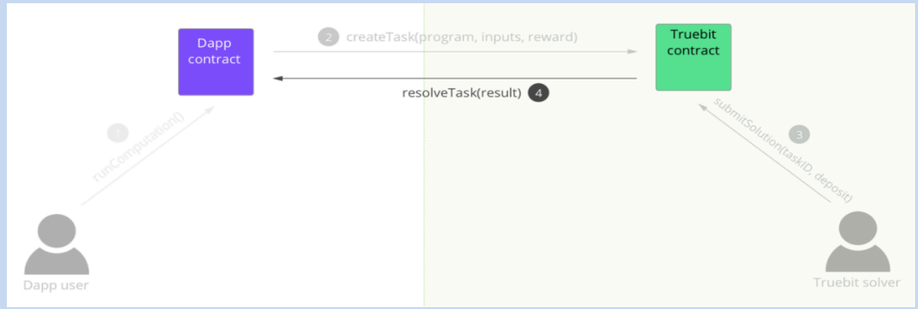


< 블록 가스 제한: 2018년 5월 기준 약 800만 – 매블록이 생성 될 때마다 변경 >

오프체인 솔루션 – 트루빗 (2/2)

복잡한 연산은 외부에서 처리! 복잡한 ML 연산은 클라우드에 맡기는 것처럼

- 블록의 최대 가스(gas limit)가 넘는 스마트 컨트랙트(Dapp) 의 연산을 대신 수행
  - 필요한 연산을 트루빗 네트워크에 참여하는 노드들에게 의지
  - 연산 된 결과만을 메인넷에 있는 스마트 컨트랙트에 반영

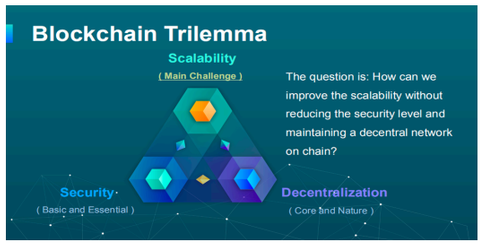


마치면서

블록체인 확장성 이슈는 해결 될까?

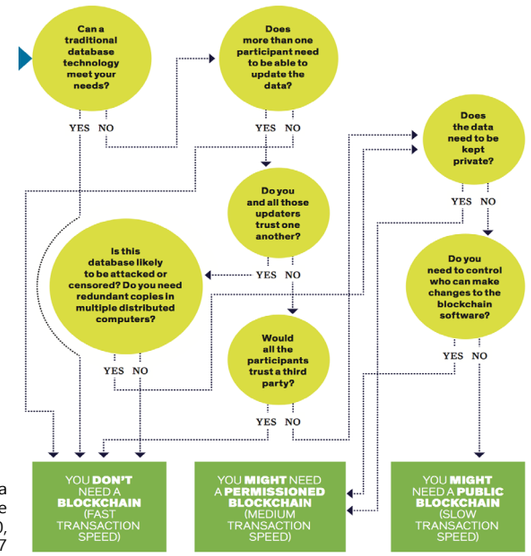
- 더딘 개발 속도
- 공개형 블록체인 vs. 비공개형 블록체인
- 실시간 프로세싱 (어플리케이션)vs. 비실시간 프로세싱이 요구되는 블록체인

블록체인 트릴레마?



부록1 – 정말 블록체인 도입이 필요한가?

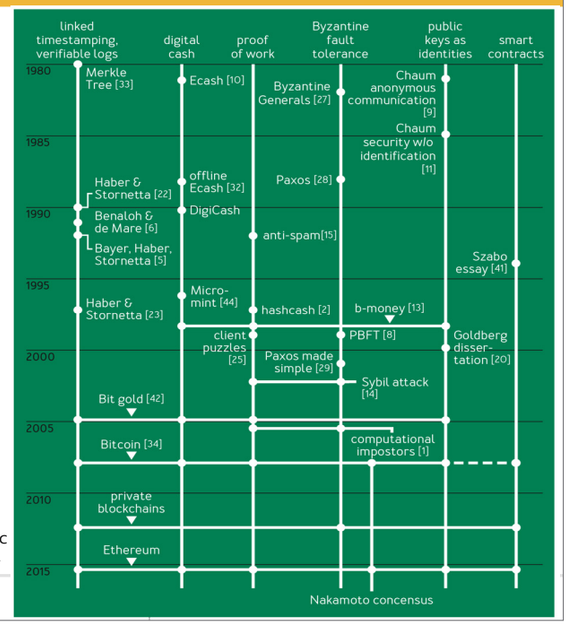
This chart will help you



Morgen E. Peck, "Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem," published in IEEE Spectrum, vol. 54, no. 10, September 2017

부록2 – 블록체인 핵심 기술의 발표 연대

The concept of cryptocurrencies is built from forgotten ideas in research literature



Arvind Narayanan and Jeremy Clark. 2017. Bitcoin's academic pedigree. Commun. ACM 60, 12 (November 2017), 36-45.

Part II

최신 블록체인 기술 동향
(블록체인 확장성, 연결성, 개인정보)

좌장 : 공준진 마스터
(삼성전자)

Scalable DeSecure Blockchain

이흥노 교수
(GIST)

Scalable DeSecure ECCPoW Blockchains

Presented @ IEIE Workshop Seoul

Future Society Ushered in via Blockchains
블록체인으로 여는 미래사회

Heung-No Lee, GIST, South Korea
Home page: http://infonet.gist.ac.kr
Facebook/Publication ID: Heung-No Lee
E-mail: heungno@gist.ac.kr

블록체인으로 여는 미래사회 워크샵

[2019년 6월 17일(월), 건설회관 3층 대회의실/ 서울 강남구 언주로 711 (7호선 학동역 10번출구)]

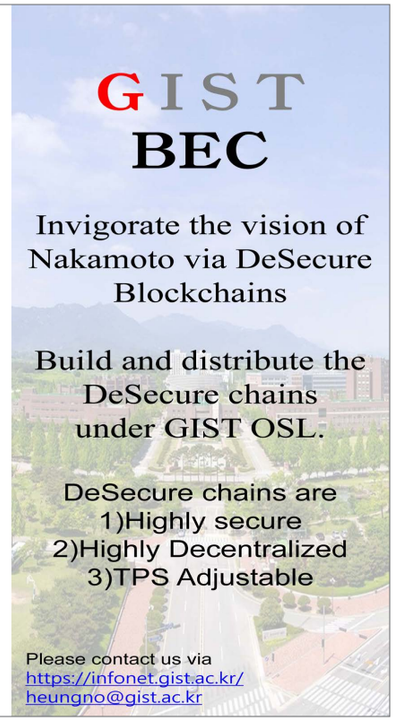
* 첫째날(6.17(월)) 실습에 참여하고자 하는 참가자는 노트북을 지참 바랍니다.

첫째날 : 6월 17일(월)

시간	세부 프로그램	강연
09:30 ~ 10:00 (30분)	최신 국내외 산업계 주요 블록체인 응용 사례 소개	박세열 상무 (한국 IBM)
10:00 ~ 10:30 (30분)	개회사 환영사 격려사	최천원 회장 (대한전자공학회) 김기선 총장 (GIST) 오정근 회장 (한국 ICT 융합학회)
Part I : 블록체인 정책 좌장 : 황성은 교수(홍익대)		
10:30 ~ 11:00 (30분)	블록체인 기술과 개발 방향	김종원 PM (IITP)
11:00 ~ 11:30 (30분)	최신 블록체인 기술 개발 동향 소개	이종혁 교수 (상명대학교)
11:30 ~ 12:00 (30분)	패널 토론 : 황성은, 김종원, 이종혁	-
Part II : 최신 블록체인 기술 동향 (블록체인 확장성, 연결성, 개인정보) 좌장 : 공준진 마스터(삼성전자)		
13:00 ~ 13:30 (30분)	Scalable DeSecure Blockchain	이흥노 교수 (GIST)
13:30 ~ 14:00 (30분)	블록체인 플랫폼 간 연동을 위한 Interoperability 기술 개발 및 표준화 현황	이원석 박사 (ETRI)
14:00 ~ 14:30 (30분)	Lightning network	김형식 교수 (성균관대학교)
14:30 ~ 15:00 (30분)	How does PUF solve Blockchain problems?	김민석 대표 (㈜EpitomeCL)
15:00 ~ 15:30 (30분)	패널 토론 : 공준진, 이흥노, 이원석, 김형식, 김민석	-
Part III : 블록체인 구축과 Smart Contract 실습		
15:40 ~ 18:00 (140분)	[실습] Ethereum 네트워크 구축 및 Smart Contract 구현 실습 * 노트북 필요(지참)	최은호 교수 (부산대학교)

Abstract

GIST Blockchain-Economy Center (BEC, Director Heung-No Lee) aims to introduce the Decentralized Secure(DeSecure) blockchains it has been developing since 2018. They aim to resolve the re-centralization problem of today's mining market. One of the key ideas is to have the proof-of-work (PoW) puzzle time-varying from block-to-block, using the error-correction-codes (ECC). Two new blockchains based on Bitcoin and Ethereum are to be developed using new consensus algorithm based on this new ECC-PoW. Time-varying puzzles make it very difficult to develop an ASIC mining chips. As the result, with the size of network growing, the difficulty level needs not be growing as well. As such, energy spent for mining can be controlled. The proposed ECC-PoW mechanism is to be explained in details. In addition, our plan to hardfork Bitcoin and Ethereum, by replacing the SHA based PoW with the proposed ECC-PoW, and by developing two new DeSecure blockchains, i.e. BTC-ECC and ETH-ECC, is discussed. The two DeSecure blockchains will be openly shared under an open source license at Github. We address how DeSecure blockchains can be used to resolving the issue of scalability. Our schedule to release the cores (C++ and Go) and technical meet-ups will be addressed.



Short Bio of Dr. Heung-No Lee

Heung-No Lee graduated from University of California, Los Angeles **(UCLA), U.S.A. with Ph.D., M.S., and B.S. degrees all in Electrical Engineering, 1999, 1994 and 1993** respectively. He has written more than 270 journal and conference publications. In the past, he worked at HRL Laboratory, Malibu, California, U.S.A., as Research Staff Member and as Assistant Professor at the University of Pittsburgh, Pittsburgh, Pennsylvania, U.S.A. He is currently a full tenured professor at Gwangju Institute of Science and Technology (GIST), Republic of Korea.

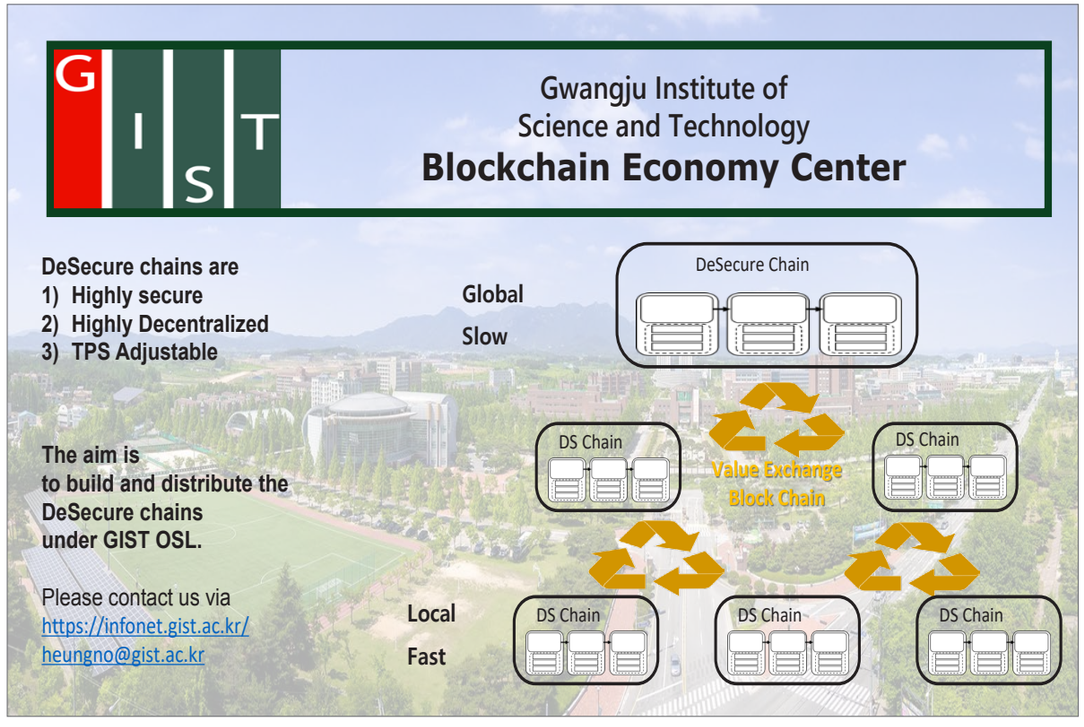
His research lies in the areas of Information Theory, Signal Processing Theory and their application to Communications and Networking systems, Biomedical systems, and Signal Processing systems.

Awards he has received recently include Top 50 R&D Achievements of Fundamental Research in 2013 (National Research Foundation), Top 100 National R&D Research Award in 2012 (the Ministry of Science, ICT and Future Planning) and This Month Scientist/Engineer Award (National Research Foundation) in January 2014.

He was the Director of Electrical Engineering and Computer Science within GIST College in 2014. Administrative positions he has held at GIST include the Dean of Research and the Director of GIST Research Institute.

Talk today

- DeSecure Blockchains
- Error Correction Codes based PoW
- Safe Transactions enabled by novel DS analysis
- Release Plan

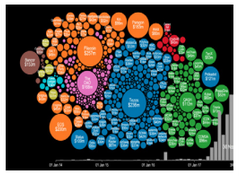


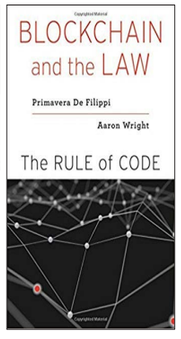
Bitcoin's Ideals

- Since birth in 2009, Bitcoin has never stopped breathing and alive currency system.
- It is a global digital currency which works beyond national boundaries.
- It was the time when trust on the banks and governments were severely degraded.
- Ideals around bitcoin are
  - Decentralization
  - Reforming Wall street
  - Unbundling big corporations
  - Reduction of inequality

7

Ethereum's Ideals





- Ethereum network allows not only coin TXs, but also doc files and computer codes.
- A *decentralized* app (Dapp) runs a front end code; a backend code runs in *the Eth Net*.
  - ✓ cf) For an ordinary app, the backend code is running on *a centralized server*.
- Smart contracts
  - ✓ A computer code can be executed and advanced to the next stage each time a contractual term matures.
- Decentralized autonomous organization has its bylaw written in smart contracts.
  - ✓ The organization spends tokens and makes governance decisions w.r.t. smart contracts.
- *Lex Cryptographia!*
- *Uprooting capitalism and democracy for a just society!*
- *Sharing Economy!*

8

Novel DeSecure Blockchains

- BTC and ETH are great BUT they are
  - Re-Centralized
  - Scalability Issue
  - Said to be too slow and small
- We aim to approach these two issues with DeSecure blockchains
  - Anti-ASIC ECC PoW
  - Ecosystem of DeSecure blockchains
- DeSecure blockchains uses novel Error-Correction Code PoW.
- We aim to provide two DeSecure blockchains, ETH-ECC and BTC-ECC.

They Have Sought Alternatives to SHA-PoW, BUT

	Pros	Cons	Coins within top 50 rank
PoW (Proof-of-Work)	• Strong security - Difficult to produce - Easy to verify	• Extreme computing power • 51% attacks • Transaction speed / Transaction throughput	Bitcoin, Ethereum
PoS (Proof-of-Stake)	• Energy & hardware efficiency • Much more expensive 51% attacks	• Recentralization • The rich-get-richer • "Noting at stake" problem	Qtum, Stratis
DPoS (Delegated PoS)	• Scalability and speed • Energy & hardware efficiency • Encouraging good behavior by real-time voting	• Recentralization • DDoS attacks	EOS, NEO smart economy
PoA (Proof-of-Activity)	• Much more expensive 51% attacks • Decentralization - Validators are randomly selected.	• Recentralization • Extreme computing power • The rich-get-richer	decred

Comparison to Existing Scalability Solutions

DeSecure Blockchain aims to resolve the re-centralization problem without sacrificing the securedness and decentralization!

Type	DeSecure	Bitcoin		Ethereum	
Name	Multi-level, multiple chains	Seg-Wit	Lightening Network	Plasma	Sharding
How	Many ECCPoW based chains can talk to each other via value-exchange service	Realize by modifying a block data structure	Allow off-chain transactions and record the end result of these transactions into the main blockchain	Allow transactions in child chains, TX records end up at the main chain are limited.	Divide BC DB with multiple shards
Pro	Many different services and levels of chains can co-work.	Easy to realize	Faster transactions Small TX fees	Faster transactions Small TX fees	Faster transaction
Con	No single chain solution Requires an ecosystem	Small improvement	The content of off-chain transactions lost	Some TX content lost Only full node can run this	Increased SW complexity

11

We aim to Replacing SHA-PoW with ECC-PoW!

Blockchain Core Program

Three key parts

1. Web server interface networking of peers
   - Node registration, get-address, give-address
   - Full node or light node
   - Communication among the wallets and the miners
2. Wallet for TX generations
   - Make private and public keys, address, store UTXOs, make TX, put signature, announce it to the neighbor, check to see if the TX is supported by the blockchain.
3. Consensus Mechanism — **Consensus Engine**
   - Data: Genesis block + regular blocks, one block every 10 min, block-size 1Mbyte
   - Protocol: consensus, block header, difficulty level adjustment, ...
   - Mining: Get the longest chain, validate it and all transactions within it, get transactions from mempool and form a block, run SHA repeatedly until you hit a good hash, put the proof into the block header, and attach the proofed block to the longest chain, and make announcement ASAP.

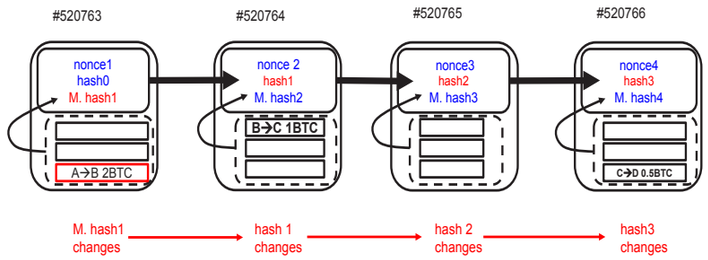
Program Suite

- C++, Python, Go, Java, Flask, http
- Download and run, then you have a blockchain server.

12

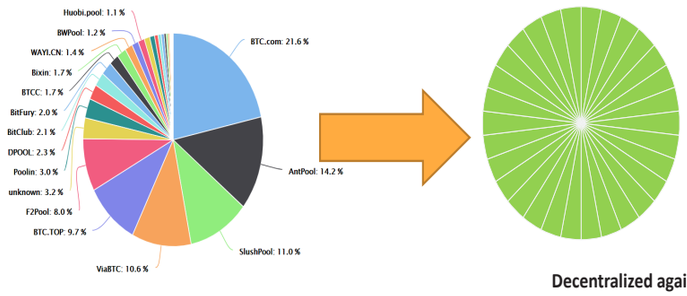
Pow is fundamental to OPEN blockchains!

- What happens when any alteration is made?
- Proof-of-Work (PoW)
- Immutability and openness allow transactions.
  - A → B 2 BTC
  - B → C 1BTC
  - C → D .5 BTC



ECC-PoW aims to resolve Recentralization Issue.

- ASIC → Mining Moguls → Discourage Average Miners
- Prone to Collusion, Censorship



Recentralized

Decentralized again

1. ASIC resistant
2. Vulnerability to DS attacks reduced

14

There are items to consider for a new PoW!

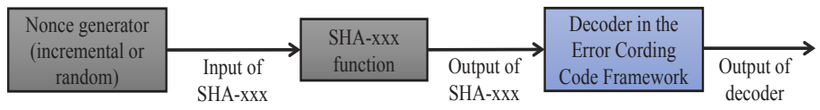
- A new puzzle generation system is capable of varying puzzles from block to block with the following properties:

  P1: Easy to verify but difficult to prove
  P2: Robust to detect block modification attacks
  P3: Controllable in changing the difficulty level
  P4: Open to anyone with a CPU
  P5: Unfixed and changeable from block to block

- The re-centralized problem can be resolved thanks to P5.

Novel Error Correction Codes PoW (ECCPoW)

- There are many one-way functions in Inverse Problems such as Error Correction Codes, Sparse-Signal Recovery, Space-Time Coding, Sphere-Decoding, Digital Communications Receiver algorithms.
- In these problems, encoding is easy but decoding is time-consuming!
- We combine a Error Correcting Code framework with SHA-xxx.

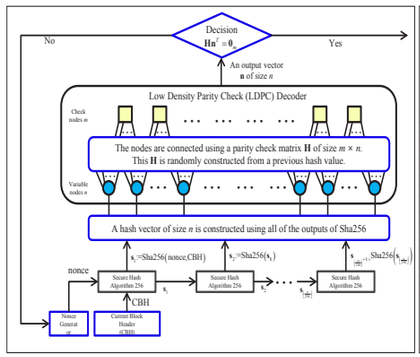


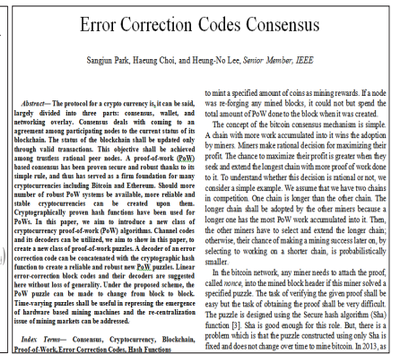
- The decision of mining success is made with the output of the above decoder.

Novel ECCPoW Consensus mechanism, how!

▣ ECCPoW Engine

- Compound code of SHA and LDPC decoder.
- Variable size of Parity Check Matrix (PCM) → Amt of resource (mem, comp) varies.
- PCM is varied by the hash of the previous block.





Error Correction Codes Consensus

Sangjun Park, Haeung Choi, and Heung-No Lee, *Senior Member, IEEE*

Abstract— The protocol for a crypto currency is, it can be said, largely divided into three parts: consensus, wallet, and networking overlay. Consensus deals with coming to an agreement among participating nodes to the current status of its blockchain. The status of the blockchain shall be updated only through valid transactions. This objective shall be achieved among trustless rational peer nodes. A proof-of-work (PoW) based consensus has been proven secure and robust thanks to its simple rule, and thus has served as a firm foundation for many cryptocurrencies including Bitcoin and Ethereum. Should more number of robust PoW systems be available, more reliable and stable cryptocurrencies can be created upon them. Cryptographically proven hash functions have been used for PoWs. In this paper, we aim to introduce a new class of cryptocurrency proof-of-work (PoW) algorithms. Channel codes and its decoders can be utilized, we aim to show in this paper, to create a new class of proof-of-work puzzles. A decoder of an error correction code can be concatenated with the cryptographic hash function to create a reliable and robust new PoW puzzles. Linear error-correction block codes and their decoders are suggested here without loss of generality. Under the proposed scheme, the PoW puzzle can be made to change from block to block. Time-varying puzzles shall be useful in repressing the emergence of hardware based mining machines and the re-centralization issue of mining markets can be addressed.

Index Terms— Consensus, Cryptocurrency, Blockchain, Proof-of-Work, Error Correction Codes, Hash Functions

to mint a specified amount of coins as mining rewards. If a node was re-forging any mined blocks, it could not but spend the total amount of PoW done to the block when it was created.

The concept of the bitcoin consensus mechanism is simple. A chain with more work accumulated into it wins the adoption by miners. Miners make rational decision for maximizing their profit. The chance to maximize their profit is greater when they seek and extend the longest chain with more proof of work done to it. To understand whether this decision is rational or not, we consider a simple example. We assume that we have two chains in competition. One chain is longer than the other chain. The longer chain shall be adopted by the other miners because a longer one has the most PoW work accumulated into it. Then, the other miners have to select and extend the longer chain, otherwise, their chance of making a mining success later on, by selecting to working on a shorter chain, is probabilistically smaller.

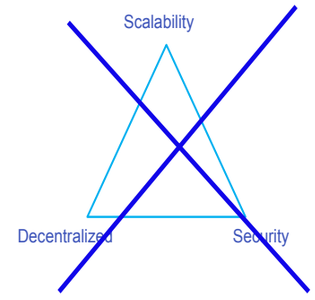
In the bitcoin network, any miner needs to attach the proof, called nonce, into the mined block header if this miner solved a specified puzzle. The task of verifying the given proof shall be easy but the task of obtaining the proof shall be very difficult. The puzzle is designed using the Secure hash algorithm (Sha) function [3]. Sha is good enough for this role. But, there is a problem which is that the puzzle constructed using only Sha is fixed and does not change over time to mine bitcoin. In 2013, as

※ 국제 학술지 IEEE trans. Information Forensics and Security에 제출예정

Blockchain Trilemma?

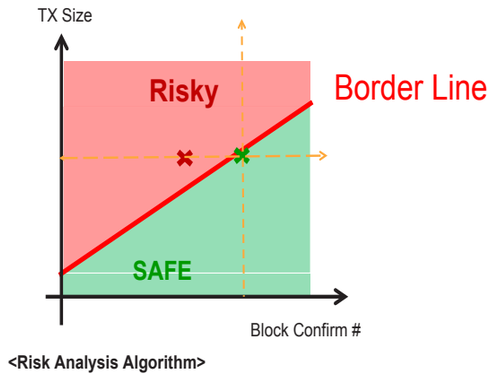
"
blockchain systems can only at most have two of the following three properties

- Vitalik Buterin, Sharding FAQ
https://github.com/ethereum/wiki/wiki/Sharding-FAQ
"

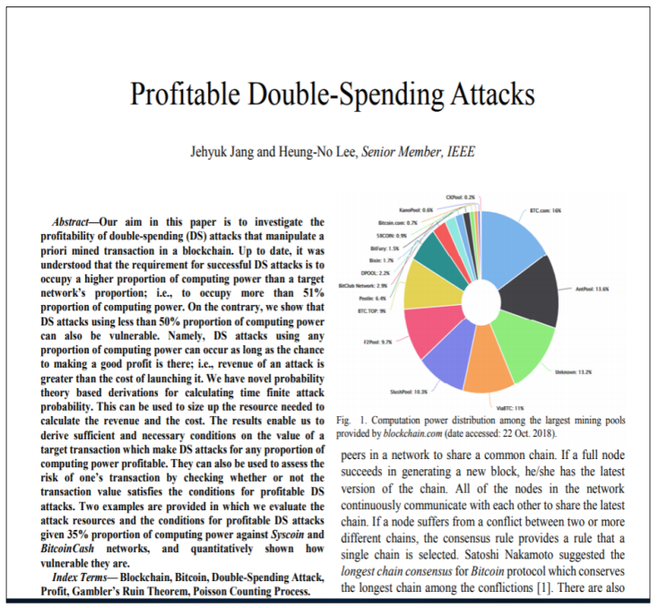


- Wrong approach!
- Not in a single blockchain, can it be achieved!
- *We shall promote many decentralized secure (DeSecure) blockchains and approach the scalability problem!*

Profitable DS Risk Analysis



<Risk Analysis Algorithm>



Profitable Double-Spending Attacks

Jehyuk Jang and Heung-No Lee, *Senior Member, IEEE*

***Abstract*—Our aim in this paper is to investigate the profitability of double-spending (DS) attacks that manipulate a priori mined transaction in a blockchain. Up to date, it was understood that the requirement for successful DS attacks is to occupy a higher proportion of computing power than a target network's proportion; i.e., to occupy more than 51% proportion of computing power. On the contrary, we show that DS attacks using less than 50% proportion of computing power can also be vulnerable. Namely, DS attacks using any proportion of computing power can occur as long as the chance to making a good profit is there; i.e., revenue of an attack is greater than the cost of launching it. We have novel probability theory based derivations for calculating time finite attack probability. This can be used to size up the resource needed to calculate the revenue and the cost. The results enable us to derive sufficient and necessary conditions on the value of a target transaction which make DS attacks for any proportion of computing power profitable. They can also be used to assess the risk of one's transaction by checking whether or not the transaction value satisfies the conditions for profitable DS attacks. Two examples are provided in which we evaluate the attack resources and the conditions for profitable DS attacks given 35% proportion of computing power against *Syscoin* and *BitcoinCash* networks, and quantitatively shown how vulnerable they are.**

***Index Terms*— Blockchain, Bitcoin, Double-Spending Attack, Profit, Gambler's Ruin Theorem, Poisson Counting Process.**

Fig. 1. Computation power distribution among the largest mining pools provided by *blockchain.com* (date accessed: 22 Oct. 2018).

peers in a network to share a common chain. If a full node succeeds in generating a new block, he/she has the latest version of the chain. All of the nodes in the network continuously communicate with each other to share the latest chain. If a node suffers from a conflict between two or more different chains, the consensus rule provides a rule that a single chain is selected. Satoshi Nakamoto suggested the *longest chain consensus* for *Bitcoin* protocol which conserves the longest chain among the conflictions [1]. There are also

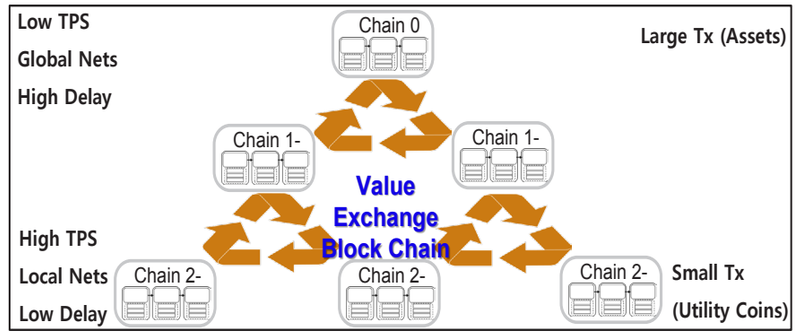
※ Jahyuk will present tomorrow afternoon!

※ 국제 학술지 IEEE trans. Information Forensics and Security에 제출됨

https://arxiv.org/ftp/arxiv/papers/1903/1903.01711.pdf

Provision of DeSecure chains, use ecosystem to solve Scalability issue!

- ▣ Global chains → national chains → local chains
- ▣ One chain is designed to hold only up to 20 DApps



<Multi-level DeSecure chains>

Block code

- A block code C(N, Rate, **G**, **F**, ENC, DEC, GF(q)) is well defined as a collection of codewords. When, $q = 2$, it is a binary system.
- N is the dimension of the code (e.g. $N = 512$)
- Rate = $(N - M)/N$ is the rate of the code, where M < N.
- For example, with $N = 1024$ and $M = 256$, Rate = 3/4.

- **G** is the Generator matrix with dimension $N \times (N - M)$.
- **F** is the Check matrix with dimension, $M \times N$.
- **G** and **F** are orthogonal to each other, i.e., $\mathbf{FG} = \mathbf{0}$.

- A message vector m is an $(N - M) \times 1$ vector.
- A codeword **c**, an N x 1 vector, is an element of the code and can be generated by multiplying a message vector m to the Generator matrix **G**, i.e., $\mathbf{c} = \mathbf{Gm}$.

- Galois Field of size q, GF(q), is used for addition and multiplication operations and storage of numbers in the system.

Block code, encoder and decoder

- ENC implies the encoder function, i.e., ENC takes the message vector **m** as the input and produces a codeword vector corresponding to it, e.g. **c** = ENC(**G**, **m**).
- DEC implies the decoding function; DEC takes an arbitrary vector e and returns a closest codeword **c**^, i.e., **c**^ = DEC(**F**, **e**).

$$\mathbf{s} = \mathbf{F}\,\mathbf{e}, \quad \mathbf{s} \in GF(q)^{M\times 1},\ \mathbf{F} \in GF(q)^{M\times N},\ \mathbf{e} \in GF(q)^{N\times 1}, \quad M < N$$

Encoder : Given $\mathbf{e}$, find $\mathbf{s} = Enc(\mathbf{e}, \mathbf{G})$

Decoder : Given $\mathbf{s}$, find $\hat{\mathbf{c}} = Dec(\mathbf{s}, \mathbf{F})$

Decoder

- DEC is to find a codeword **c**^ most close to the input word **e**.
- For the concept of distance, the Hamming distance can be used.
  For example, DH(**e**, **c**^) = $||\mathbf{e} - \mathbf{c}^{\wedge}||_0$ is the number of non-zero values in the (**e** – **c**^) vector.
- There are many ways to find **c**^ satisfying **Fc**^ = **0**.
- We propose to use the message passing graph decoder for its excellency in accuracy and superiority in decoding speed.
  This is to prevent a cheating attack in which a smart miner comes up with a new decoder algorithm of his own developed and outpaces the regular miners using the designated decoder. If this is allowed, a hidden advantage goes to the smart miner.

Geometrical Explanation

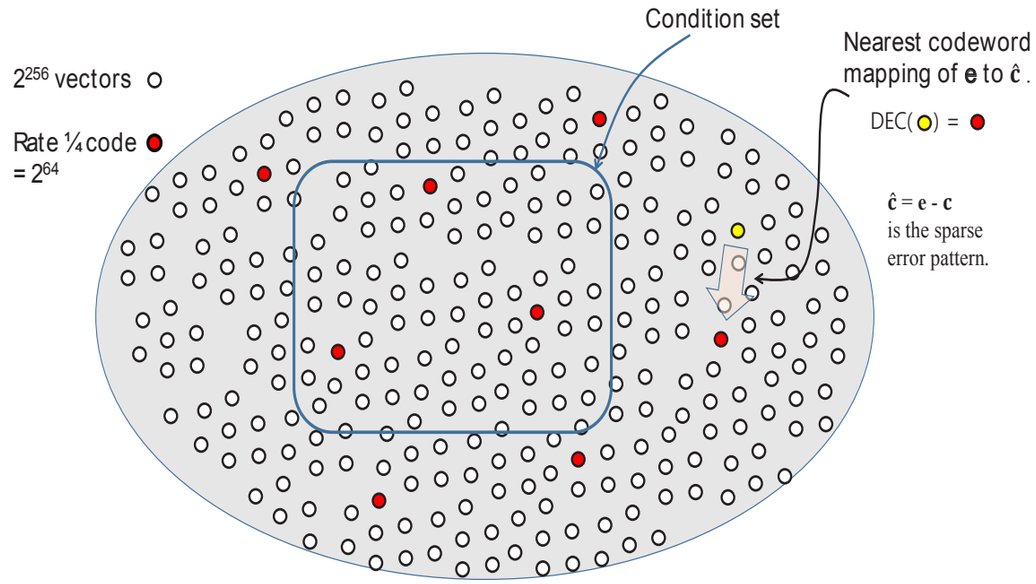
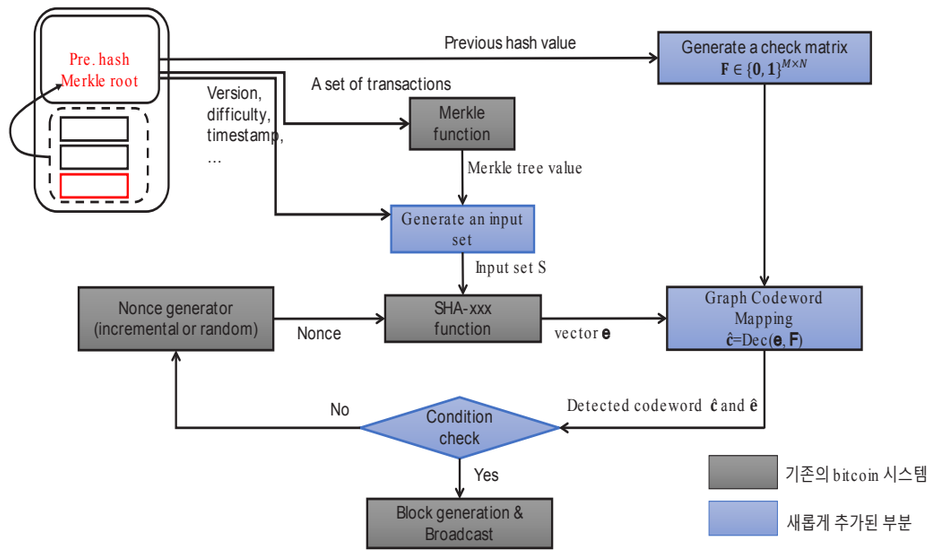
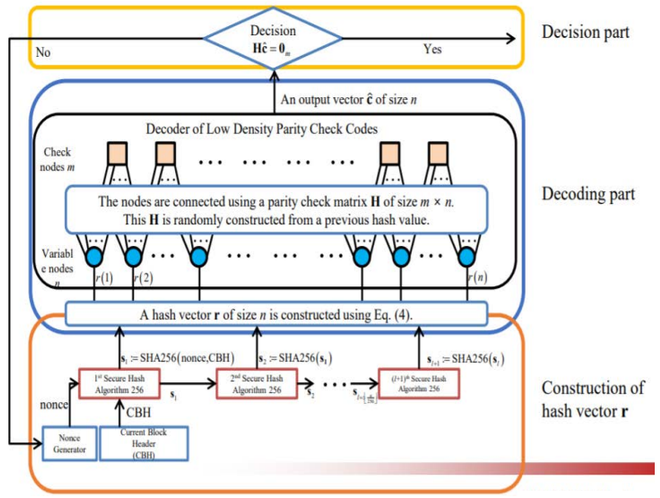


Diagram of ECCPoW

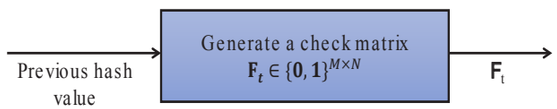


Big Picture of ECCPoW



Generate a Check Matrix

- Parameter set $S_t = \{h_{t-1}, \textit{code parameters}\}$;
- $\text{GenCheckMatrix}(S_t) = \mathbf{F}_t$
- Generate a check matrix $\mathbf{F}_t$ w.r.t. previous hash h_{t-1}.
- Takes the previous hash h_{t-1} as the input to this routine.
- That is, $\mathbf{F}_t$ changes from block to block.



Pseudo Code of the Decoder

- Input:
  - ✓ Hard decision of a priori LLR: $L_a^t = \mathbf{e}[t]$
- Iteration: repeat until converse
- Update variable-to-check node messages for $t = 1, 2, .., N$ and $\forall l \in Q1(t)$:

$$L^{t \to l} = \left[\sum_{l' \in Q1(t) \setminus l} (L_a^t \oplus L^{l' \to t}) \Big/ (j-1) \right]$$

- Update check-to-variable node messages for $l = 1, 2, .., M$ and $\forall t \in Q2(l)$:

$$L^{l \to t} = \oplus \sum_{t' \in Q2(l) \setminus t} L^{t' \to l}$$

- Output
  - ✓ Hard decision of a posteriori LLR:

$$L^{t \to l} = L_a^t \oplus \left[\sum_{l' \in Q1(t)} L^{l' \to t} \Big/ j \right] \rightarrow \hat{\mathbf{c}}[t]$$

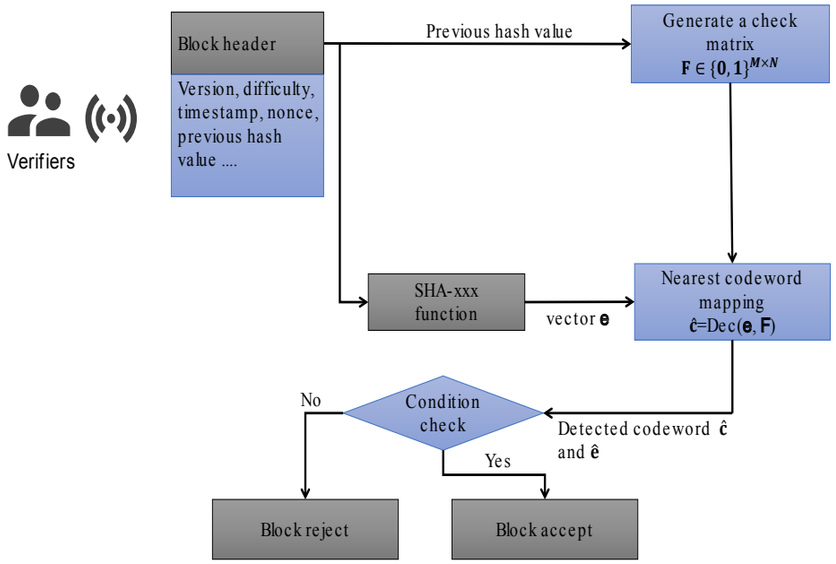
Implemented code in C

```
}
//Bit to Check Node Messages --> LRat!
for(i = 0; i < ITERATIONS; i++) {
    for(k = 0; k < COLUMNS; k++) {
        for(i = 0; i < COLUMN_WEIGHT; i++) {
            temp3 = LRit[k];
            for (m = 0; m < COLUMN_WEIGHT; m++) {
                if (m != i) {
                    temp3 += LRrti[k][Row_in_Column[m][k]];//LRat[ k][Row_in_Column[i][k] ] +  infinity_test(LRit[ k][Row_in_Column[i][k] ]);
                }
            }
            LRat[ k][Row_in_Column[i][k] ] =  (short) temp3;
        }
    }

    fprintf(out,"\n\n\nLRat! iteration %i\n",i);
    for(k=0; k <COLUMNS; k++) {
        fprintf(out,"\n");
        for(m=0;m<ROWS;m++)
            fprintf(out,"%i ",LRat[k][m]);
    }

    //Check to Bit Node Messages --> LRrti
    for(k = 0; k < ROWS; k++){
        for(i = 0; i < ROW_WEIGHT; i++){
            temp3 = 0.0;
            sign=1;
            for( m =0; m < ROW_WEIGHT; m++){
                if( m != i){
                    temp3 = temp3 + func_f( fabs( LRat[Column_in_Row[m][k]][k] ) );
                    if(LRat[Column_in_Row[m][k]][k] > 0.0)
                        temp_sign = 1;
                    else
                        temp_sign = -1;
                    sign=sign*temp_sign;
                }
            }
            magnitude =  func_f(temp3);
            LRrt[ Column_in_Row[i][k]] [k] =  (short) sign*magnitude;
        }
    }
    fprintf(out,"\n\n\nLRrt! iteration %i\n",i);
    for(k=0; k <COLUMNS; k++){
        fprintf(out,"\n");
        for(m=0;m<ROWS;m++)
            fprintf(out,"%i ",LRrt[k][m]);
    }
    //Last iteration get LR (pi)
    for(m =0; m < COLUMNS; m++){
        LRpt[m] = LRrt[m];
```

Diagram of New Verifiers



New Functions in ECCPoW

- New functions
  1. int **H = GenCheckMatrix(int n, int w_c, int w_r, int seed);
  2. bool DEC(int **H, int *e, int n, int w_c, int w_r, int *c);
  3. void Dec_Difficulty(int &n, int &wc, int &wr, int level);

- These functions are the key parts of the proposed solution.
  1. They are implemented in C++.
  2. They are used to implement a mining routine

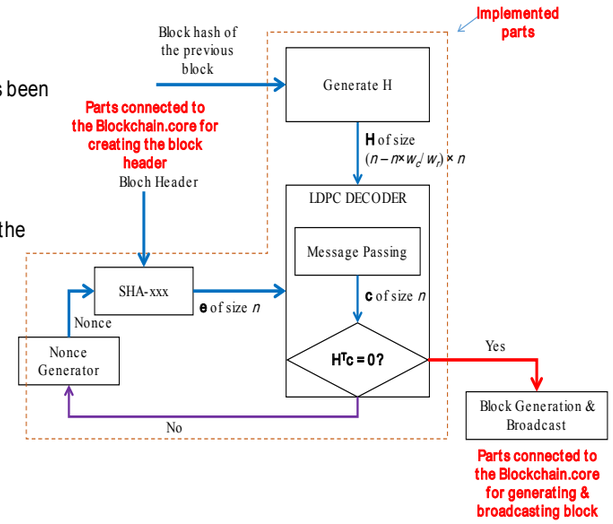
- An example of mining

1. generate block header with zero nonce.
2. Dec_Difficulty(&n,&wc,&wr,difficulty)
3. Seed = f(phv)
4. H = GenCheckMatrix(n, wc, wr, seed)
5. nonce = nonce + 1
6. e = SHA256(version, time, difficulty, nonce, mtv)
7. flag = DEC(H,e,n,wc,wr)
8. If flag == 0; go to step 4
9. Update chv and nonce.
10. Generate block and broadcast.

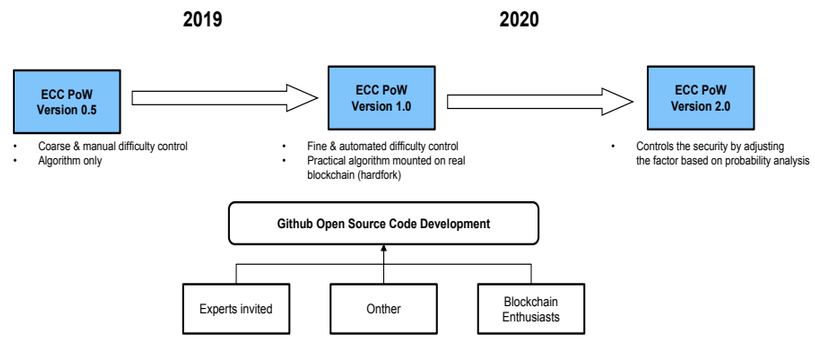
ECCPoW Hardfork

- New ECCPoW
  A new structure of the block header has been introduced and,
  three new functions are also have been introduced.

- We aim to link these functions to existing the blockchain. For example,
  mining function,
  chain validation function,
  consensus function and so on.



DeSecure Blockchain Release Plan



34

Impact of ECCPoW 1:
It is easier to start a new blockchain network.

- A large blockchain network is stable and not easy to disrupt.

- Today there are mining equipment renting sites.
- A new borne blockchain network needs to grow, but newbies are much more vulnerable to 51% attacks.

- DeSecure blockchain networks with ECCPoW do not suffer from such problems since there are no mining equipment available for ECCPoW.

Impact of ECCPoW 2:
One can make multiple blockchain networks

- It is easy to make a new blockchain with ECCPoW.

- Suppose hardforking a Bitcoin, and an Ethereum, with ECCPoW.
- Let us call them BTC-ECC and ETH-ECC protocols.

- Make the first blockchain network by running ETH-ECC over a network (Pusan coin)
- Make the second blockchain network by running BTC-ECC over other network (Gwangju coin)
- Make the third blockchain network by running ETH-ECC over another network (Seoul coin)
- Make the fourth blockchain network by running BTH-ECC over yet another network (Korea coin)

- Each cryptocurrency is independent with its own genesis block and random starting seed, and can be adjusted sufficiently strong for its regional requirement in the sense of scalability, security and decentralization.
- These blockchains are inter-connected at the local, regional, and national, transnational level.

Impact of ECCPoW 3:
Resolving the Scalability Trilemma

- Trilemma by V. Buterin is well known: Only up to **two out of the three** virtues such as Scalibility, Decentralization and Security **can be achieved simultaneously**.

- With ECC, each blockchain is already very strong in decentralization.
- Each EEC blockchain is flexible enough to fit into various settings of transaction speeds and security levels.
  - Campus ECC blockchain networks can be set to work very fast allowing up to 100s of thousands of TXs per second since the delay of the underlying communications network is very small.
  - Regional ECC blockchain networks can be set to work fast, i.e. allowing up to 10s of thousands of TXs per sec.
  - National ECC blockchain networks can be set sufficiently fast for covering inter-regional transactions.
  - Transnational ECC blockchain networks shall be set to work slow due to large delays.

- All these DeSecure chains started up with its own seed and decentralized levels are mutually independent and each one can be set to work at the required level of security and speed to serve its purpose.
- These DeSecure chains can be inter-connected via *distributed value-exchange* networks.
- The connected ECC blockchains can be named the ECC Blockchain International.
- *ECC Blockchain International* as a whole can serve to resolve the Scalability Trilemma.

Impact of ECCPoW 4:
It is safe to use a time-proven blockchain protocol.

- Bitcoin protocol has withstood the tough test of time.
- Thus, the networking part and the wallet part are robust enough.

- PoW is problem. Yes.
- But it is not the problem of PoW.
- It is the **fixedness** of the PoW puzzle.

- ECCPoW puzzles can be made to vary over time.

- The problematic consensus part with a fixed PoW can be replaced with the new ECC PoW consensus.

Impact of ECCPoW 5:
The complexity of ECCPoW puzzles can be set to grow very large; thus the cost for hardware acceleration is boundless.

- ECCPoW is a computer algorithm!
- Thus it is not impossible to find a hardware acceleration solution for it.

- ECCPoW puzzle can be represented as a randomly connected bipartite graph.
- In order to parallelize the algorithm, more memory and computation resource need to be allocated.
- The size of ECCPoW puzzle can grow very large.
- As the size of the puzzle grows, the more needed is the memory and computation resource.
- With ECCPoW puzzles, therefore, one can easily deter the emergence of hardware acceleration solution.

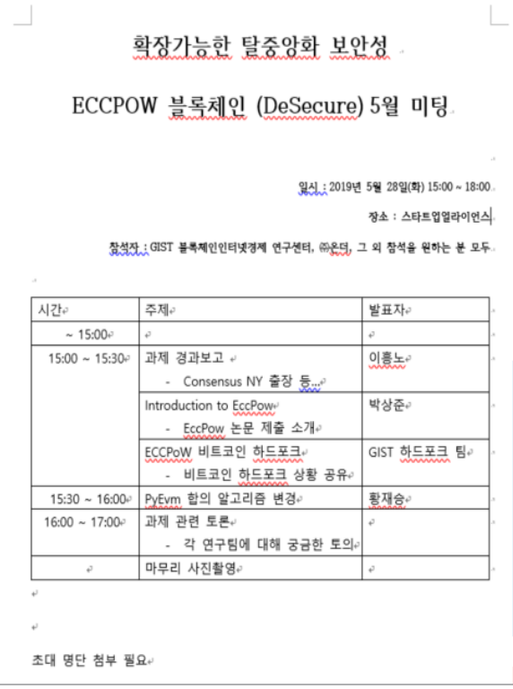
- Deterrence to hardware acceleration offers a blockchain network with small power consumption requirement.

Development Schedule

- Open research platform
  - Source codes github uploaded
  - Open development
- 2019 plan
  - ECCPoW 0.5 Version
  - Ethereum and Bitcoin Hardforks with ECCPoW 0.5v
  - Develop them into Ethereum ECCPoW 1.0v and Bitcoin ECCPow 1.0v
- 2020 plan
  - Network growth at least by 10,000 nodes worldwide
  - Co-working with Bitcoin and Ethereum communities

Plan to Offer DeSecure Chains and Meet-Ups

- May 28th, Tuesday, 2019
- Place: Startup Alliance
- 주소: Teheran-Ro 423, 7th floor of Hyundai Tower, 701Ho, Gangnam-Gu, Seoul (선릉역 10번 출구와 삼성역 7번 출구 사이)
- 시간: 15:00 ~ 17:00
- Anyone can attend, notify us at 정현준 junghj85@gmail.com appreciated.



확장가능한 탈중앙화 보안성

ECCPOW 블록체인 (DeSecure) 5월 미팅

일시 : 2019년 5월 28일(화) 15:00 ~ 18:00

장소 : 스타트업얼라이언스

참석자 : GIST 블록체인인터넷경제 연구센터, ㈜온더, 그 외 참석을 원하는 분 모두

시간	주제	발표자
~ 15:00		
15:00 ~ 15:30	과제 경과보고 - Consensus NY 출장 등...	이홍노
	Introduction to EccPow - EccPow 논문 제출 소개	박상준
	ECCPoW 비트코인 하드포크 - 비트코인 하드포크 상황 공유	GIST 하드포크 팀
15:30 ~ 16:00	PyEvm 합의 알고리즘 변경	황재승
16:00 ~ 17:00	과제 관련 토론 - 각 연구팀에 대해 궁금한 토의	
	마무리 사진촬영	

초대 명단 첨부 필요

Concluding Remarks

- PoW is fundamental for blockchains' immutability.
  - You put PoW to a block, you get the benefit of data immutability.
  - Recentralization issue is problem due to fixeness of PoW puzzles, not due to PoW itself.
- Trilemma by V. Buterin is well known. We seek to get two Security and Decentralization.
  - Flexible puzzles enabled by ECCPoW can resolve the recentralization problem;
  - PoW has shown to be the most secure.
- Scalability is left to the ecosystem of DeSecure blockchains.
  - Multiple layers of ECCPoW blockchains can operate simultaneously resolving the issues of scalability and thus breaking the trilemma.
- ECCPoW blockchains can play a crucial role in ushering in the ideals of blockchains and advance our society to the next level!

Selected References of GIST Blockchain Economy Center

- [Lee1] JH Jang and Heung-No Lee, "Profitable Double Spending Attacks," March 5th, 2019 submitted to IEEE Trans. Information Forensics and Securities, downloadable from https://arxiv.org/abs/1903.01711.
- [Lee2] 장재혁, 이흥노, "50%미만 이중 지불 공격", OSIA S&TR Journal, Vol. 32, No. 1, Mar. 2019. (pdf) (GIST 연구원 GRI 사업, 과학기술융합연구단 실용화사업)
- [Lee3] 정현준, 이흥노, "암호화폐 투자와 규제 현황", 한국정보과학회, 정보과학회지, 제 36권, 제 12호, pp. 49-56, Dec, 2018. (pdf)
- [Lee4] 박상준, 김형성, 이흥노, "Introduction to Error-Correction Codes Proof of Work," 블록체인경제 특집호, 대한전자공학회지, June 2019.
- [Lee5] Sangjun Park, HS Kim, Heung-No Lee, "Time-Variant Proof-of-Work Using Error-Correction Codes," to be submitted to IEEE Trans. Information Forensics and Securities.
- [Lee6] Mohamed Yaseen.J, Giljun Jung and Heung-No Lee."Decentralized Framework for Medical Images Based on Blockchain and Inter Planetary File System", The 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society(EMBC 2019), Berlin, Germany, Jul. 23-27, 2019.
- [Lee7] Please visit INFONET home page https://infonet.gist.ac.kr/?page_id=14 for more references.

- Thank you!

Heung-No Lee, GIST, South Korea
Home page: http://infonet.gist.ac.kr
Facebook/ Publication ID: Heung-No Lee
E-mail: heungno@gist.ac.kr

- Q&A

- We are actively looking for blockchain students to join us.
- Send me an e-mail!

블록체인 플랫폼 간 연동을 위한 Interoperability 기술 개발 및 표준화 현황

이원석 박사
(ETRI)

블록체인 플랫폼 간 연동을 위한 Interoperability 기술 개발 및 표준화 현황

2019.6.17

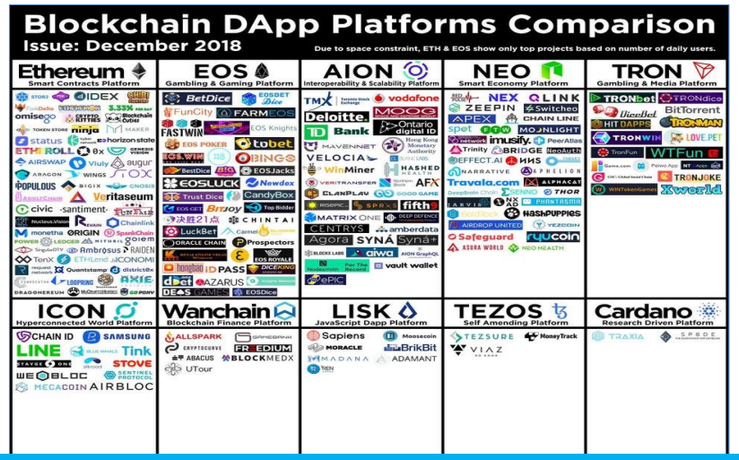
이원석 / ETRI 표준연구본부 / wonsuk.lee@etri.re.kr

블록체인 활용 분야

※ 출처 삼정 KPMG 경제연구원(2016), 블록체인이 가져올 경영 패러다임의 변화 금융을 넘어 전 산업으로

블록체인 기술은 금융 분야를 중심으로 시작으로 전 산업분야에서 활용 예상

블록체인 생태계의 파편화



새로운 블록체인 플랫폼들의 출현은 증가와 함께
블록체인 생태계의 파편화 이슈 또한 지속적으로 증가

〈Source: http://biz.chosun.com/site/data/html_dir/2018/04/18/2018041801090.html 〉

[2018 미래금융포럼] 스테판 토마스 리플 CTO "블록체인 간 상호운용성 높여야"

조선비즈 | 이승주 기자

입력 2018.04.18 11:19 | 수정 2018.04.18 12:10

"인터넷은 케이블로 연결하든 와이파이로 연결하든 위성을 사용하든 여러 다른 네트워킹 기술을 사용해도 서로 연결이 되는 시스템"이라며 "블록체인 기술도 일상에 큰 영향을 미칠만큼 주류가 되려면 인터넷과 같은 상호운용성이 있어야 한다."

스테판 토마스(Stefan Thomas) 리플(Ripple) 최고기술경영자(CTO)는 18일 조선비즈가 서울 소공동 웨스틴조선호텔에서 개최한 2018 미래금융포럼 기조연설에서 이같이 밝혔다.

일상에 큰 영향을 미칠만큼 주류가 되려면
인터넷과 같은 상호운용성 필요

EU, 블록체인 간 상호 운용성·확장성 표준 마련 촉구

김수찬 기자 | 입력 2019-03-12 16:42 | 수정 2019-04-11 11:51

'유럽연합 블록체인 관측 논의 기구'는 보고서를 통해 블록체인 간 디지털 신원인증과 상호 운용성을 위한 표준이 설립돼야 한다고 주장

〈Source: https://hkbnews.com/article/view/2289〉

Blockchain Interoperability Alliance (BIA)

- 블록체인이 해결해야 할 가장 큰 문제는 상호운용성
- 이종의 블록체인 플랫폼 간의 상호운용성 표준 개발 추진

〈Source: https://bitcoinexchangeguide.com/blockchain-interoperability-alliance/ 〉

블록체인 핵심 표준 중 하나는 블록체인 플랫폼 간의 상호운용성 표준

블록체인 상호운용성이란?

- 이종의 블록체인 플랫폼 간의 연동
- 이종의 암호화폐 간의 교환
- dApp 호환성
- ???

〈Source: https://www.intellectsoft.net/blog/blockchain-generations-cryptocurrencies-and-blockchain-platforms/〉

(e.g.)비트코인으로 스마트 컨트렉에 활용?

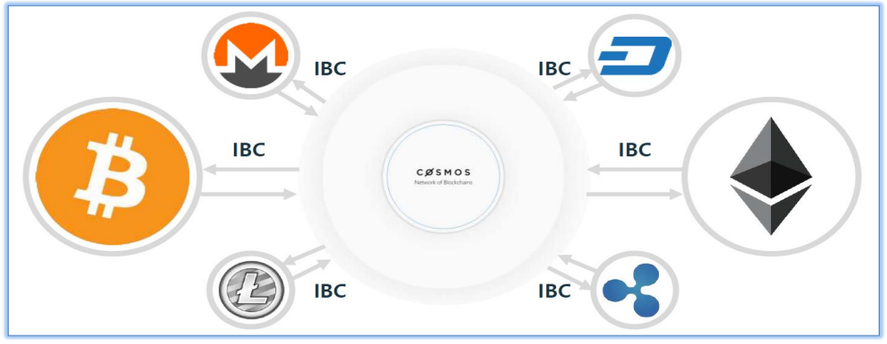
〈Source: https://www.slideshare.net/SungWanYun/1-74058385〉

Types of Blockchain Interoperability

- Notary schemes
  - Notary also known as witness mechanism, notary mechanism is essentially an intermediary way
  - Pros: It can flexibly support various block chains with different structures
  - Cons: There is a risk of centralization
- Side Chains/Relays
  - Side chain refers to another block chain that has the function of a chain
  - The relay chain is the combination of side chain and notary mechanism
- Hash-locking: Hashed Time Lock Contract (HTLC)
  - Hash locking technology mainly supports the exchange of atomic assets across chains, originating from the lightning network of Bitcoin
  - Pros: It is to achieve the atomic exchange of assets through time difference and shadow hash value
  - Cons: Hash locking can only be exchanged, but can not transfer assets or information

Side Chains/Relays (1/2)

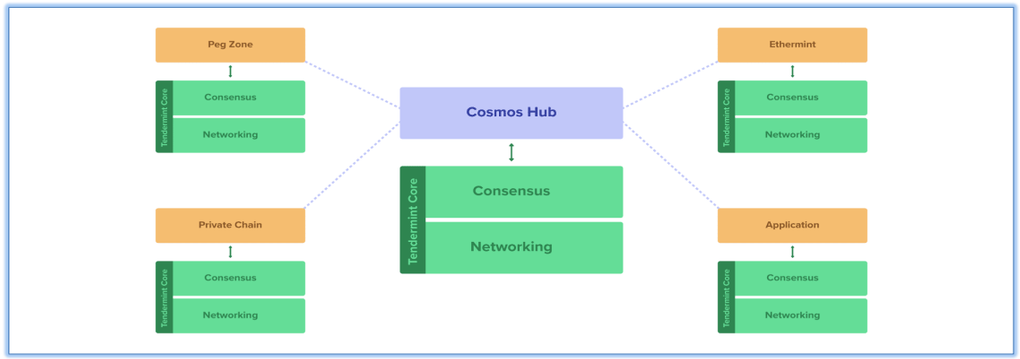
- Relay chain is essentially the integration and expansion of notary mechanism and side chain mechanism.



〈Source: https://www.slideshare.net/SungWanYun/1-83431803〉

Side Chains/Relays (2/2)

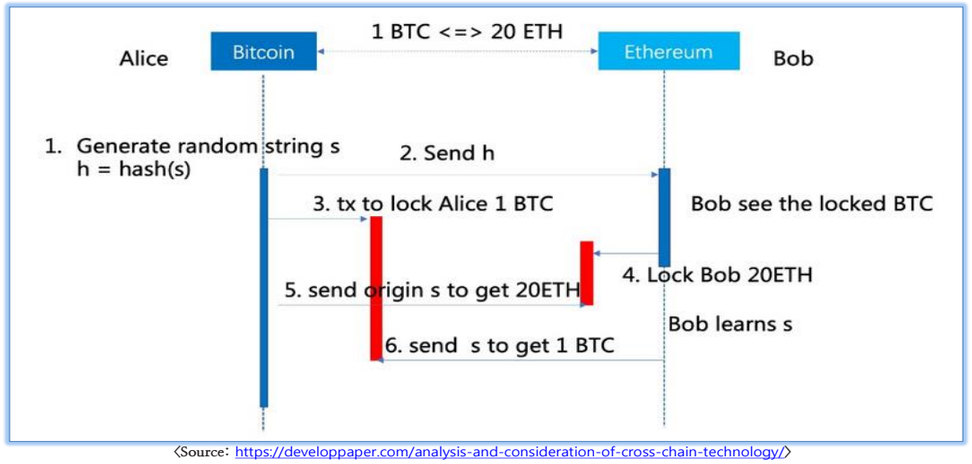
- Hubs on the network act as the central ledgers for each of the individual chains also called zones. Hubs are the ledgers for the token swapping between the zones



〈Source: https://befast.tv/what-is-cosmos-network-atom-a-beginners-guide-to-the-internet-of-blockchains/〉

Hash-locking

- Alice and Bob have the need for asset exchange, Alice wants to exchange one BTC and Bob for 20 ETH



〈Source: https://developpaper.com/analysis-and-consideration-of-cross-chain-technology/〉

Summary of Interoperability Types

	Notaries	Relays	Hash-locking
Interoperability types	All	All (if relays exist on both chains; otherwise one-way causality only)	Cross-dependency only
Trust model	Majority of notaries honest	Chains do not fail or get "51% attacked"	Chains do not fail or get "51% attacked"
Usable for cross-chain exchange?	Yes	Yes	Yes
Usable for cross-chain asset portability?	Yes (but requires universal long-term notary trust)[36]	Yes	No
Usable for cross-chain oracles?	Yes	Yes	Not directly
Usable for cross-chain asset encumbrance?	Yes (but requires long-term notary trust)	Yes	In many cases, but with difficulty
Ease of implementation	Medium	Hard	Easy

〈Source: https://medium.com/coinmonks/interoperability-the-holy-grail-of-blockchain-eb078e1a29cc〉

dApp Portability (1/2)

〈Source: https://www.cryptoglobe.com/latest/2019/05/new-blockchain-interoperability-standards-released-by-ethereum-enterprise-alliance/ 〉

dApp Portability (2/2)

Enterprise Ethereum Alliance Client Specification v4

Editor's Draft 10 June 2019

ENTERPRISE ETHEREUM ALLIANCE

ReSpec

Latest editor's draft:
https://entethalliance.github.io/client-spec/spec.html

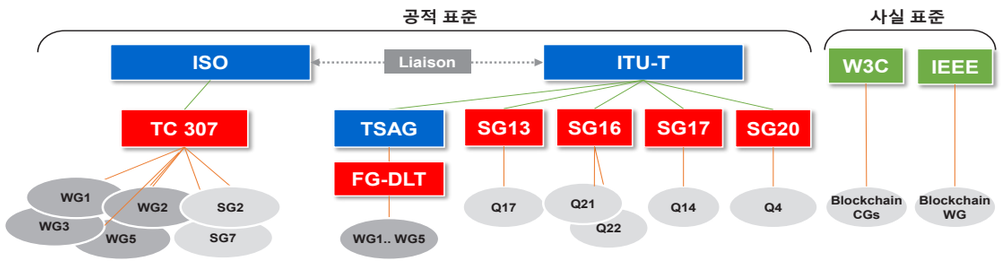
Editors:
Robert Coote (PegaSys)
Chaals Nevile (Enterprise Ethereum Alliance)
Grant Noble (PegaSys)
George Polzer (Everymans.ai)

Former editors:
Daniel Burnett (PegaSys)
David Hyland-Wood (PegaSys)

Contributors to this version:
Janie Baños (Dekra), Imran Bashir (JP Morgan Chase), Mark Bruening (BakerHostetler), Sara Feenan (Clearmatics), Ivaylo Kirilov (Web3Labs), Maya Konaka (Blockapps), Kieren James-Lubin (Blockapps), Chris McKay (PegaSys), Arash Mahboubi (PegaSys), George Ornbo (Clearmatics), Brianna Rich (EEA), Przemek Siemion (Banco Santander), Conor Svensson (Web3Labs), Clark Thompson (ConsenSys), Jim Zhang (ConsenSys), Weijia Zhang (Wanchain)

〈Source: https://entethalliance.github.io/client-spec/spec.html〉

블록체인 국제표준화 동향



- **TC 307/WG 1** –"Foundations"
- **TC 307/WG 2** –"Security, privacy and identity"
- **TC 307/WG 3** –"Smart contracts and their applications"
- **TC 307/WG 5** –" Governance "
- **TC 307/SG 2** – "Use Cases"
- **TC 307/SG 7** – "Interoperability of blockchain and distributed ledger technology systems"

- **ITU-T Q17/13** – Requirements, ecosystem, and general capabilities for cloud computing and big data
- **ITU-T Q21/16** – Multimedia framework, applications and services
- **ITU-T Q22/16** – Distributed ledger technologies and e-services
- **ITU-T Q14/17** – Security aspects for Distributed Ledger Technologies
- **ITU-T Q4/20** – e/Smart services, applications and supporting platforms

ISO/TC 307 WG7 상호운용성

- 상호운용성 WG 신설 조건부 승인 (2019/5/31)
  - 플랫폼, 데이터의 상호운용성을 중심의 연구를 기술적, 기업적, 관리 측면으로 전환하여 상호운용성 프레임워크 (Interoperability Framework) TS에 대한 투표를 통하여 WG 신설을 조건부로 승인

- 블록체인 및 분산 원장 시스템의 상호운용성에 대한 보고서 발간
  - Transport Interoperability, Syntactic Interoperability, Semantic data Interoperability, Behavioural Interoperability, Policy Interoperability
  - National/Regional Interoperability Frameworks

Comparison among projects aiming to increase intercommunication between DLTs

	Interledger	Virtualchain	Sidechain	Cosmos	Polkadot	Aion	Overledger
Purpose	Payments across different payment systems based on DLT	Ability to migrate from one DLT to another for fault tolerance	Add new innovative features to the main crypto currencies	Overcome Blockchain limits and transfer assets	Transfer assets and data (smart contract)	Solve Blockchain isolation problem	Build a messaging layer for multi-ledgers applications
Interoper-ability	1-C-1	1-C-1	1–1	N-C-N	N-C-N	N-C-N	N–N
Layer of comm.	Transaction Level	Over the transaction level	Transaction Level	Protocol based (transaction level for legacy ledger)	Protocol based (transaction level for legacy ledger)	Protocol based (transaction level for legacy ledger)	Over the transaction level
Connection Method	Two phase commit	Two phase commit like	Two phase commit (two way peg- SPV)	Two phase commit like (Tendermint)	Two phase commit (SPV)	Two phase commit	Two phase commit
Connection Speed	Notaries / Entity consensus	Migration time	Confirmation and Contest Period	Proportional to the validator number	Protocol time depended	Protocol time depended	Protocol (flexible) time depended
Scalability	Ledgers allow connectors to run nodes	Ledgers allow to write metadata	Ledger's compliance with two-way peg	Should implement IBF to talk with The Hub	Should implement the polka dot security consensus	Aion-compatible	Ledger's readability and/or writability
Fault tolerance	Depends on notaries or institutions that validates transactions	Depends on the two blockchains involved in the migration	Security faults on sidechain are confined in the sidechain itself.	Confined in the zones (User responsibility on where they move coins)	Para chains follow rules and consensus of Polkadot	Compatible blockchain Aion-1 follow rules and consensus of Aion-1	Protocol based

〈Source: ISO/TC 307 SG7 report in Dublin Plenary〉

참고문헌

- Analysis and Consideration of Cross-Chain Technology, https://developpaper.com/analysis-and-consideration-of-cross-chain-technology/
- Interoperability Overview, https://spec-rationality.com/news/interoperability-overview-dlt/
- Methods of Interoperability, https://spec-rationality.com/methods-interoperability/
- Blockchain Interoperability — Moving Assets Across Chains, https://medium.com/cryptronics/blockchain-interoperability-moving-assets-across-chains-e5203357d949

Lightning network

김형식 교수
(성균관대학교)

Robustness of Lightning Network

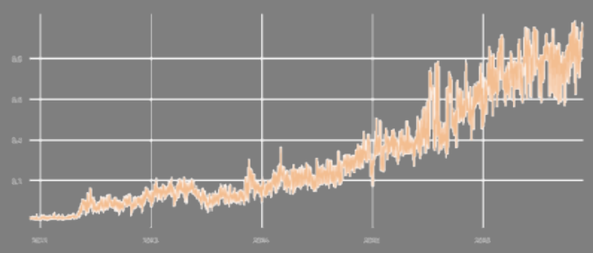
Hyoungshick Kim
Sungkyunkwan University

Why is Bitcoin so slow?

A winner node should be chosen among 15,000 nodes in a fair manner every time.

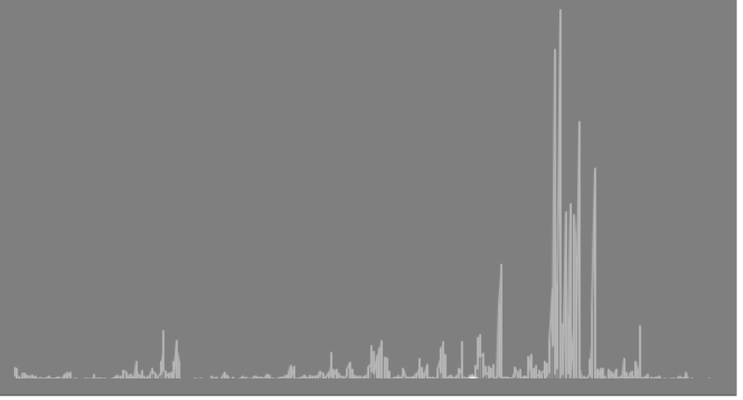
Scalability of Bitcoin

- Scaling limitations
  - 1 block = 1 MB max
  - 1 block ~ 2000 txns
  - 1 block ~ 10 min
  - So, 3-4 txns / sec
  - Log grows linearly



- VISA peak load comparison
  - Typically 2,000 txns / sec
  - Peak load in 2013: 47,000 txns / sec

The average time for one confirmation has recently ranged anywhere from 10 minutes to over 16 hours in extreme cases.



Micropayment don’t actually work

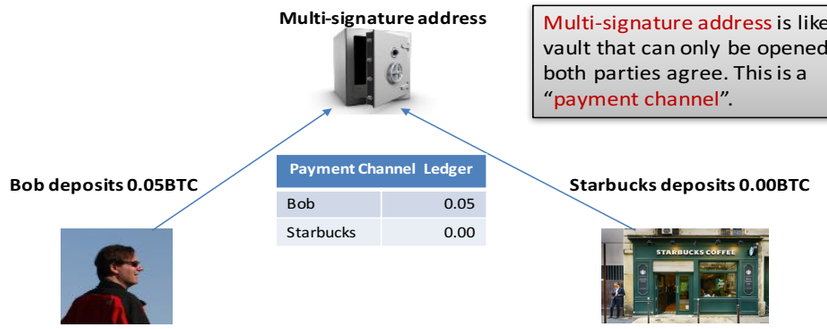
There's no easy fix

- Increasing block size improves throughput
  - Result: Bigger blocks take longer to propagate in the network
- Reducing the block interval reduces latency
  - Result: leads to instability where the system is in disagreement
- Introducing the second layer protocol (i.e., the lightning network)

Payment channels

Payment channel (1)

- Take small transactions out of the main blockchain (off chain)
- Suppose Bob buys a coffee regularly at Starbucks
- It is inefficient to use the main blockchain for small transactions
- The solution is to set up a multi-signature address that is shared by Bob and Starbucks

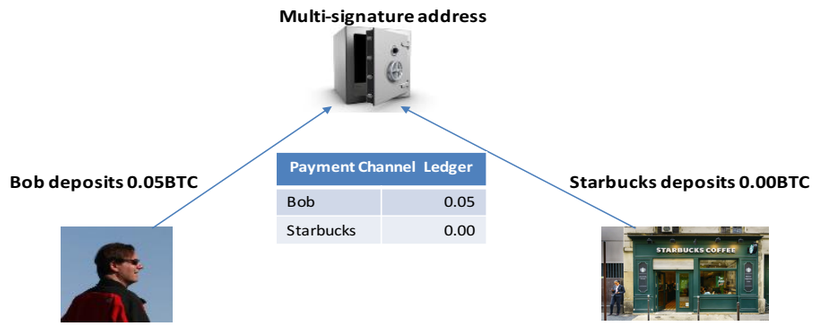


Payment channel (2)

scriptPubKeys

```
IF
        <expiry time> CHECKLOCKTIMEVERIFY DROP
        <Bob's pubkey> CHECKSIGVERIFY
        1
ELSE
        2
ENDIF
<Bob's pubkey> <Starbuck's pubkey> 2 CHECKMULTISIG
```

value: 0.05



Payment channel (3)

- Bob goes to Starbucks and orders an expresso which costs 0.005 BTC
- Payment channel ledger is updated off chain

Payment Channel Ledger	
Bob	0.05
Starbucks	0.00

- Starbucks signs the updated balance sheet and keeps a copy of the ledger
- There is no limit on the number of transactions per second because these transactions are happening off chain

Payment channel (4)

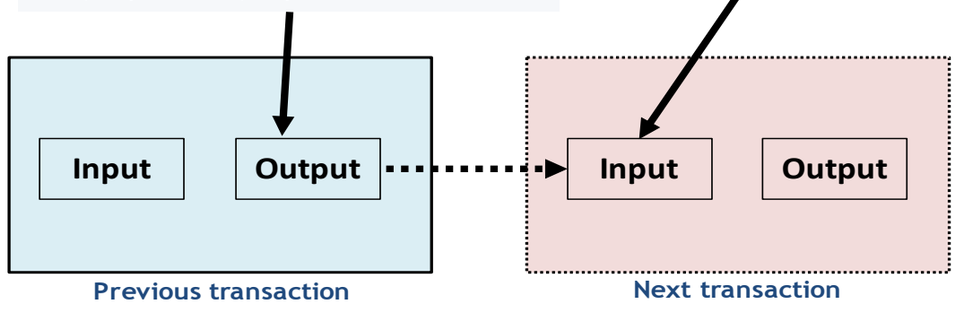
value: 0.05

scriptPubKeys

```
IF
        <expiry time> CHECKLOCKTIMEVERIFY DROP
        <Bob's pubkey> CHECKSIGVERIFY
        1
ELSE
        2
ENDIF
<Bob's pubkey> <Starbucks' pubkey> 2 CHECKMULTISIG
```

scriptSig

```
0 <Bob's signature> <Starbucks' signature>
```



Payment channel (5)

```
0 <Bob's signature> <Starbucks' signature>
```

```
IF
        <expiry time> CHECKLOCKTIMEVERIFY DROP
        <Bob's pubkey> CHECKSIGVERIFY
        1
ELSE
        2
ENDIF
<Bob's pubkey> <Starbucks' pubkey> 2 CHECKMULTISIG
```

nLockTime

2
<Starbucks' pubkey>
<Bob's pubkey>
<expiry time>
2
<Starbucks' signature>
<Bob's signature>
0

A bug in CHECKMULTISIG

Payment channel (6)

scriptPubKeys

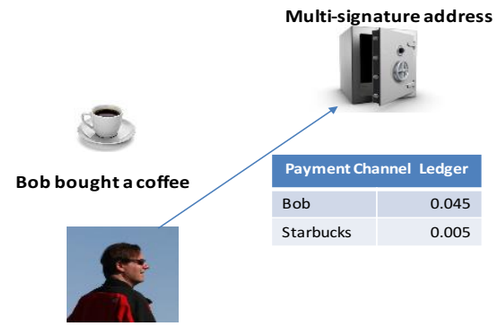
```
<Bob's pubkey> CHECKSIG
```

value
0.045

scriptPubKeys

```
<Starbucks' public key> CHECKSIG
```

value
0.005



Payment channel (7)

scriptPubKeys

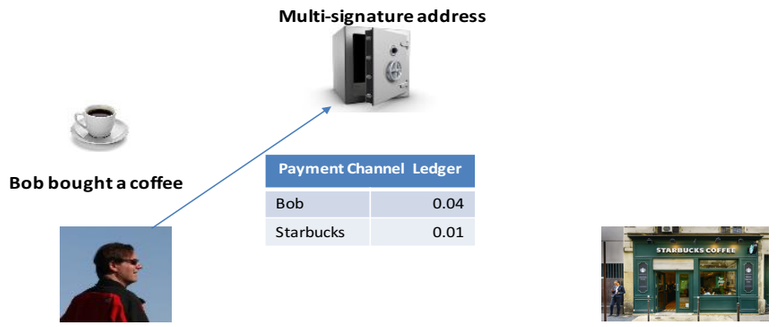
<Bob's pubkey> CHECKSIG

value
0.04

scriptPubKeys

<Starbucks' public key> CHECKSIG

value
0.01



Payment channel (8)

scriptPubKeys

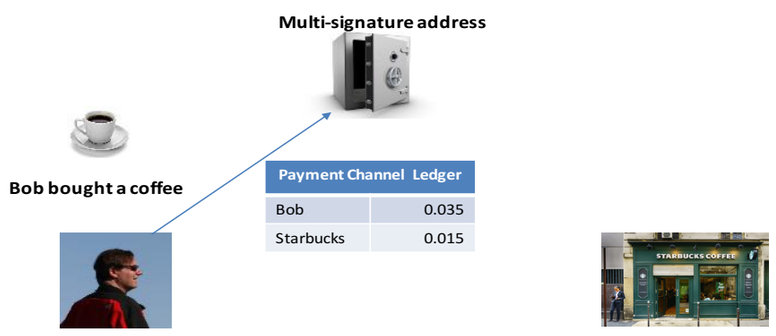
<Bob's pubkey> CHECKSIG

value
0.035

scriptPubKeys

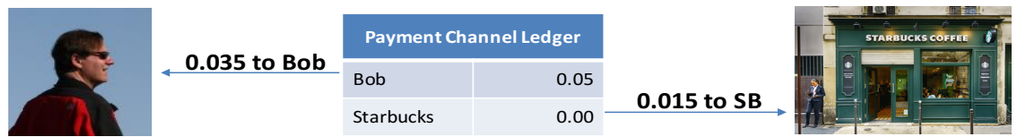
<Starbucks' public key> CHECKSIG

value
0.015



Payment channel (9)

- Payment channel can be closed at any time
- Either party simply needs to take the latest ledger which is signed by both parties and broadcast it to the network
- Miners verify the signatures on the ledger and then release the funds (single transaction to close). This is an on-chain transaction.



scriptPubKeys

<Bob's pubkey> CHECKSIG

value
0.035

scriptPubKeys

<Starbucks' public key> CHECKSIG

value
0.015

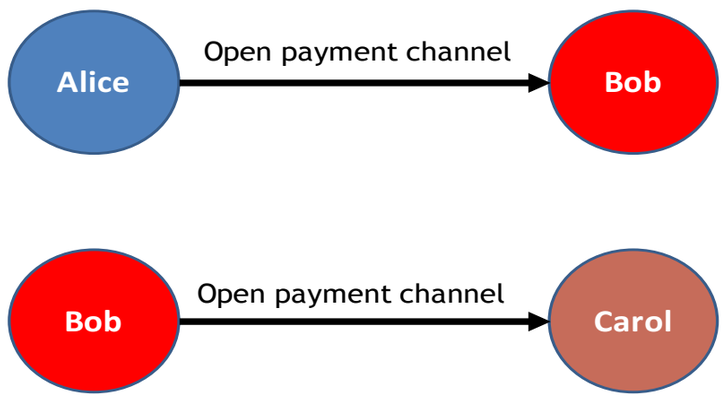
Applications

- Micropayments
  - Sending satoshis with small transaction fees
- Payment streaming
  - Sending small amount of money frequently
  - E.g., pay per second when watching video on YouTube
- Machine-to-Machine payments
  - Bandwidth, data, storage, CPU time, data can be traded
  - API endpoints usages

You can now play Pokémon on the blockchain

This Twitch game lets you play Pokemon with Lightning Network

Can we combine payment channels?

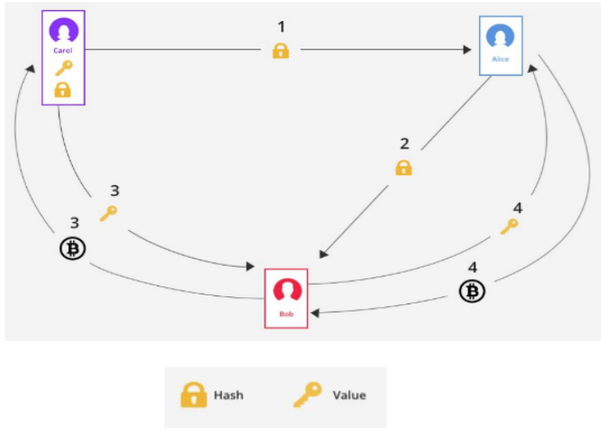


Can we combine payment channels?

1. Alice wants to send 1 BTC to Carol via Bob
2. Alice pays 1 BTC to Bob, Bob pays 1 BTC to Carol

Things that may go wrong here …

- Alice does not trust Bob or Carol
- Alice can pay Bob, Bob can choose not to pay Carol
- Bob can pay Carol, but Carol can claim that she did not receive the funds



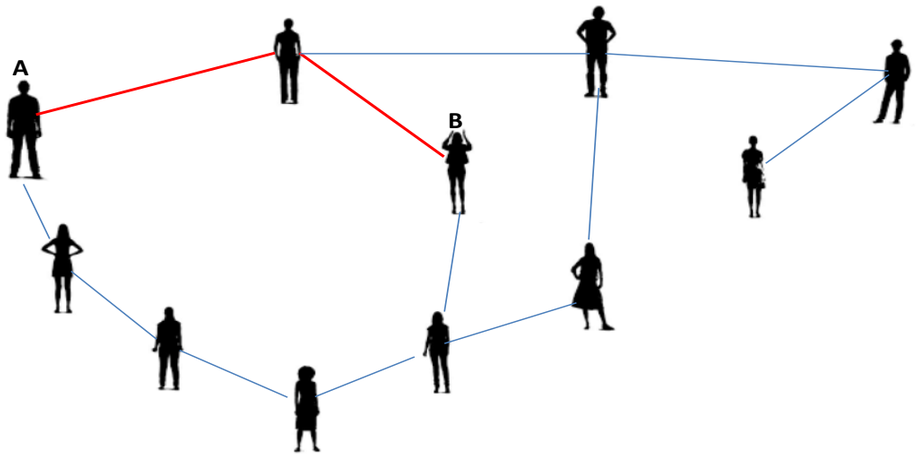
Alice wants to send 1 BTC to Carol via Bob

1. Carol needs to create an invoice consists of V_{rand} & $H(V_{rand})$; Carol sends $H(V_{rand})$ to Alice; Alice tells Carol to receive 1 BTC from Bob
2. Alice tells Bob that she will pay him 1 BTC if he can produce $H(V_{rand})$; Bob needs V_{rand}
3. Bob gives 1 BTC to Carol; Carol gives V_{rand} to Bob
4. Bob gives V_{rand} to Alice as a proof; Alice gives 1 BTC to Bob

We can achieve decentralized, instant, off-chain transfer of Bitcoin without Trust

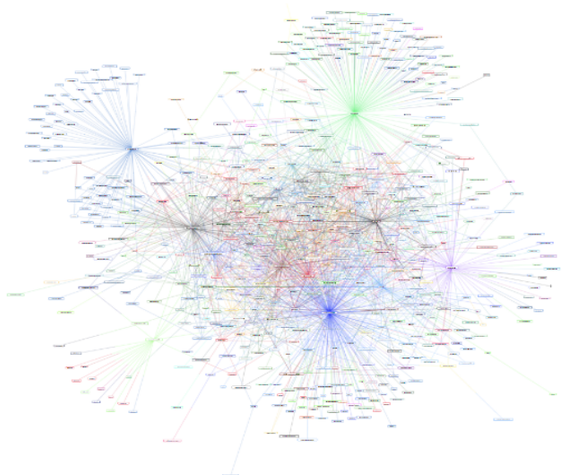
Lightning network

Network finds the fastest and cheapest way to connect A to B. It is also important that the channels have enough funds to do the transaction.



Lightning network mainnet

- Actual payments were used through payment channels
- June 24, 2018: 2295 nodes and 5065 channels

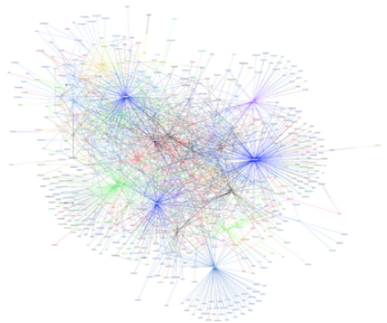


https://lnmainnet.gaben.win/

How reliable is lighting network

Lightning Network DDoS Sends 20% of Nodes Down

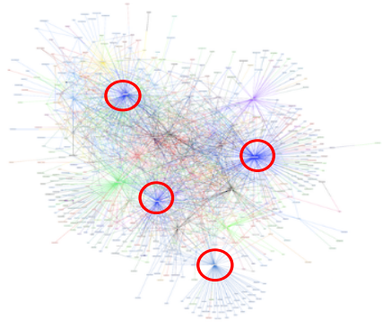
March 21, 2018 12:17 pm



Lightning Network (LN) nodes faced a Distributed Denial of Service (DDoS) attack yesterday that sent offline around 200 nodes, down from around 1,050 to 870.

How about targeted attacks?

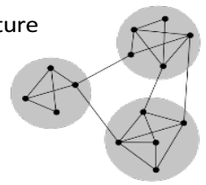
Lightning networks include a small number of highly connected **hub nodes** that are functionally valuable



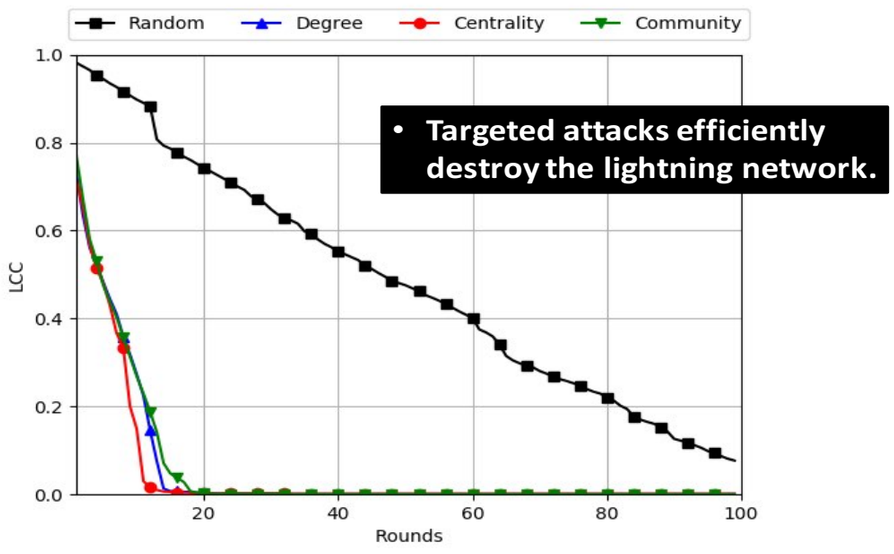
Targeted attacks might be much more effective

Attack strategies

- Random removal
  - Select nodes to be removed or connected, randomly
- High-degree removal
  - Select nodes to be removed or connected, according to their degree
- High-centrality removal
  - Select nodes to be removed or connected, according to their betweenness centrality
- Community based removal
  - Select nodes to be removed or connected using community structure



Effectiveness of targeted attack

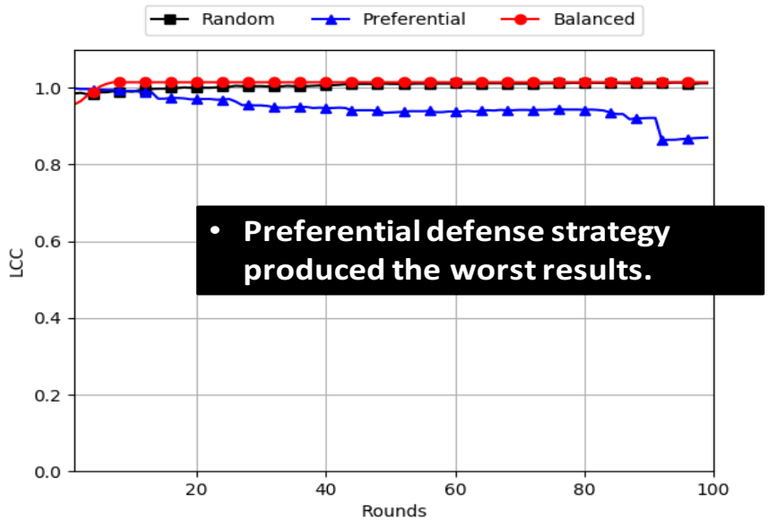


- **Targeted attacks efficiently destroy the lightning network.**

Defense strategies

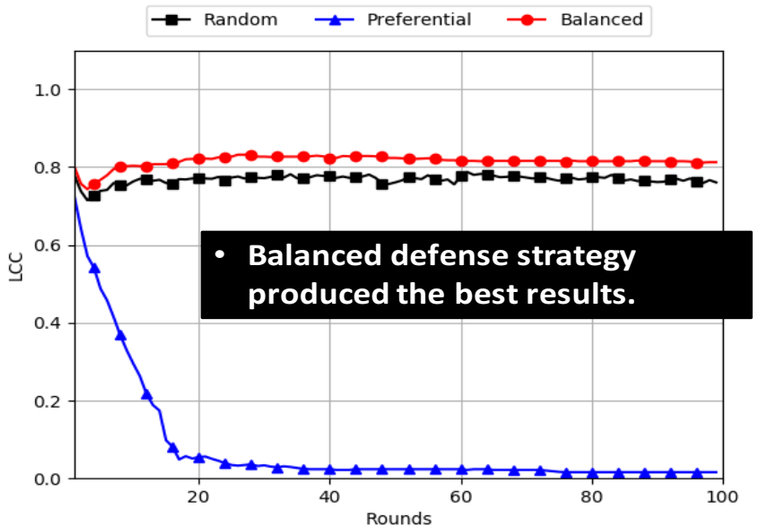
- Random replenishment
  - Create a node and add it to the network such that the node is connected to randomly selected different nodes
- Preferential replenishment
  - Create a node and add it to the network such that the node is connected to different nodes with probability proportional to their degree
- Balanced replenishment
  - Create a node and add it to the network such that the node is connected to different nodes with probability inversely proportional to their betweenness centrality

VS Random node attack



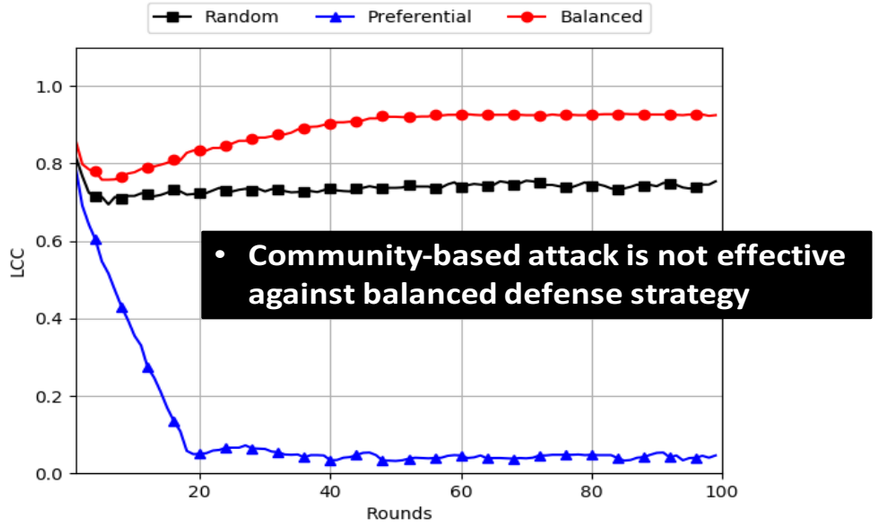
- **Preferential defense strategy produced the worst results.**

VS High-degree node attack



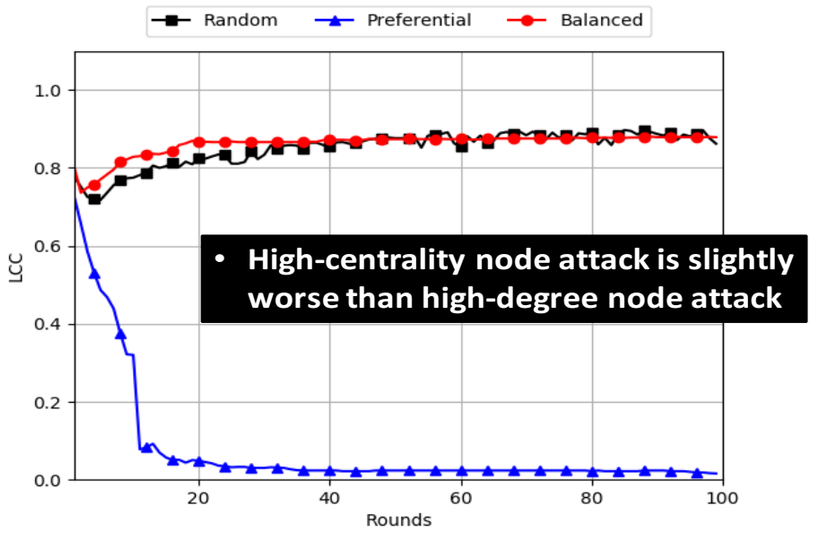
- **Balanced defense strategy produced the best results.**

VS Community-based attack



- **Community-based attack is not effective against balanced defense strategy**

VS High-centrality node attack



- **High-centrality node attack is slightly worse than high-degree node attack**

Summary

- Blockchain communities are trying to solve the scalability problem of blockchain
- Payment channel and/or Lightning network is a possible solution
- However, the current lightning network topology is highly centralized, which could be vulnerable to targeted DoS attacks
  - Balanced peer assignment is an effective defense strategy

Any questions?

How does PUF solve Blockchain problems?

김민석 대표
(㈜EpitomeCL)

블록체인 기술 개선을 위한 PUF의 활용

김민석

ICTK Holdings

epitomeCL

발표자

- 김민석
- 경력
  - 前 ALTIBASE (In-Memory DBMS)
  - 前 OnmirSoft (Distributed Database Module)
  - 前 SunjeSoft (In-Memory DBMS)
  - 前 Scalechain (Private Blockchain Protocol)
  - 現 epitomeCL (Blockchain/Cryptocurrency)
- 기타
  - OWDIN network (CDN/Network Service on Blockchain) Project Advisor
  - ICTK (VIA PUF)
  - AIoT (Crypto-Asset Custody solution)

목차

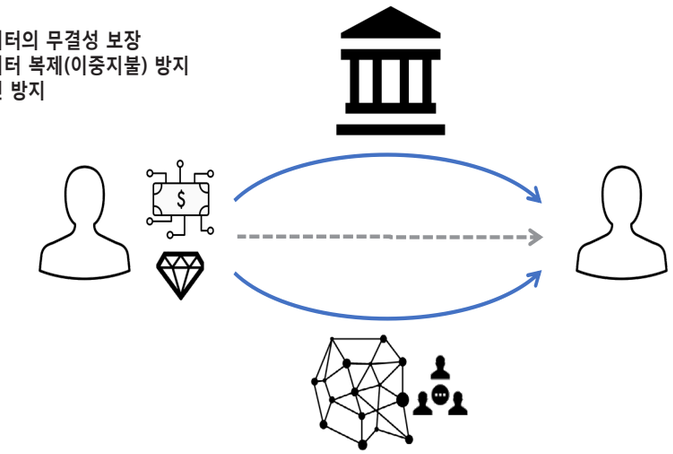
❖ 목차

- Blockchain 개요
  - Blockchain의 의의
  - Blockchain 기술 과제 및 발전 방향
- Blockchain 기술에서 PUF의 활용
  - VIA PUF 소개
  - Blockchain 기술에서 PUF의 활용 방법 제안 및 예시
- Appendix
  - Demo

블록체인의 개요

Blockchain

✓ 데이터의 무결성 보장
✓ 데이터 복제(이중지불) 방지
✓ 부인 방지



탈중앙화의 의의

- 장애 허용성/결함 감내성 (Fault tolerance) : 탈중앙화 된 시스템은 많은 수의 독립된 요소들로 이루어져 있기 때문에, 특정 사고로 인해 전체 시스템에 장애가 일어날 확률이 낮다.
- 공격 저항성 (Attack resistance) : 탈중앙화 된 시스템에는 중앙화되어 있는 급소가 없기 때문에, 시스템을 공격하거나 조작하는데 드는 비용이 매우 높다.
- 담합 저항성 (Collusion resistance) : 탈중앙화 된 시스템 내의 사용자들은 다른 사용자들에게 피해를 끼쳐서 자신의 이득을 취하는 행위를 하기 어렵다. 반면 중앙화 된 기업이나 정부의 리더들은 결속력이 비교적 약한 시민, 소비자, 직원들을 착취해서 이득을 얻는 경우가 많다.
- 크리스 딕슨 "Why Decentralization Matters"

  인터넷 서비스는 초기 성장단계에서는 양질의 서비스를 저렴하게 제공하여 사용자를 유혹하고, 열린 생태계를 만들어 참여하는 개발자나 사업체들과 협력하지만, 충분히 성장하고 난 뒤에는 네트워크의 힘이 너무나 강력해져서, 사용자들을 착취하고 서드파티 개발자나 사업체들과 경쟁하고 그들의 이익까지 빼앗기 시작함.

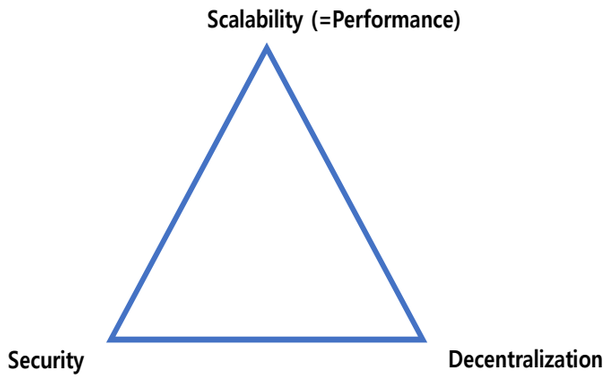
  블록체인 기반의 탈중앙화 된 시스템에서는 사용자와 개발자들이 토큰이라는 경제적 인센티브를 받고, 자발적으로 토큰의 가치 향상을 위해 협력하며 시스템을 성장시키게 되며, 만약 초기 개발팀이나 채굴자 등이 권력을 쥐게 되어 횡포나 착취를 하려고 해도 토큰 기반 투표와 같은 방법으로 참여자들이 목소리를 낼 수 있으며, 극단적인 상황에서는 시스템을 복제(Hardfork)하여 기존 데이터와 유저군을 그대로 유지한 채 권력자를 몰아낼 수도 있음.

  공리주의의 관점에서 볼 때 탈중앙화는 전체 네트워크가 제공하는 효용을 더 빨리 키울 수 있다고 주장.

합의 알고리즘

- **분산시스템에서 특정 데이터에 대하여 동일한 값을 유지하기 위해 고안된 개념.**
- **블록체인은 블록을 생성하여 체인처럼 연결하여 유지 관리하는 것**
- **블록체인에서의 합의 알고리즘**
  블록체인이 결국 공유원장/공유데이터저장소라고 생각한다면 저장되는 데이터를 여러 사람이 변경 또는 생산이 가능하다는 의미이고, 합의 프로세스는 이렇게 여러 사람이 변경하는 내용 중 **어떤 것을 사실로 받아들여서(결정 합의) 공유저장소에 기록하고 유지할 것인가(사실 합의)에 대한 프로세스**이며, 시스템이 이러한 방식으로 합의를 하여 **한 본의 기록 데이터를 유지하게 해주는 것이 합의 알고리즘**이다.
  즉, **(합의알고리즘의 목적)**은 **모든 노드가 동일한 하나의 체인을 가질 수 있도록 특정 메커니즘에 의하여 블록이 생성 및 연결되게 하는 것**
- **합의 알고리즘의 예제**
  공통으로 사용하는 한 문서를 여러사람이 동시에 작업하는 경우,
  (중앙화방식) 문서 변경 및 관리 책임자를 선택한 후 모든 문서 변경 작업은 책임자의 허가를 득 한 후 수행. 책임자는 변경된 내용이 충돌되지 않도록 잘 관리함.
  (탈중앙화방식) 문서를 변경하고자 하는 사람들이 모여서 가위바위보 게임을 수행한 후 승리한 사람이 문서를 변경하고 저장하는 것을 지속적으로 반복
- **탈중앙화 시스템으로써의 블록체인 기술에서는 탈중앙화 된 방식의 합의 알고리즘이 핵심기술 : 특정 노드에 의존하지 않으면서 동시에 신뢰를 제공하는 것**

Blockchain Trilemma



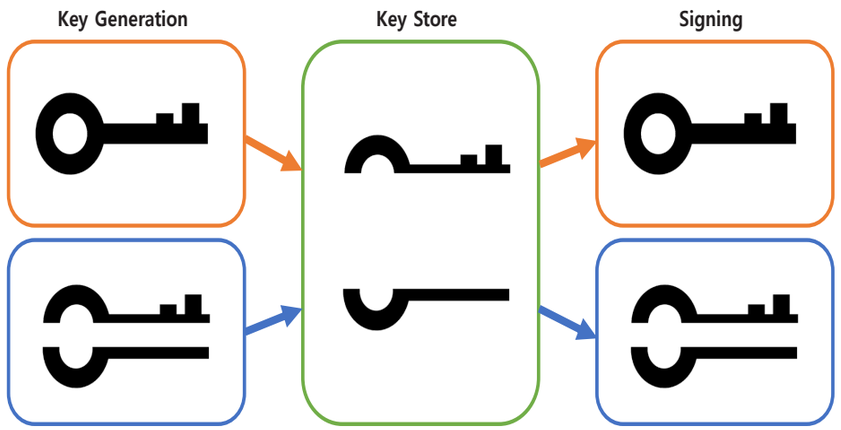
블록체인의 과제

- **공통적인 문제**
  - **관리의 어려움** - 사용자들의 **개인키 보관의 문제**. 개인키 분실 시 해당 자산을 복구할 수 있는 방법이 없음.
  - **확장성** - 높은 처리속도와 처리량이 매우 중요하다. 현재 실제 서비스들은 초 당 수천 건이 넘는 데이터 변경을 처리하는 경우가 대부분인데 이러한 속도를 처리할 수 있는 상용화 된 블록체인 프로토콜은 아직 존재하지 않음.
  - **익명성 및 투명성** - 모든 거래 내역이 공개되어 있고 추적이 가능하며, 주소가 익명성을 보장한다고 해도 사용자 식별이 될 수 있으므로 개인의 프라이버시를 침해할 가능성이 있음.
  - **합의구조** - POW의 다량의 전기를 소비하는 방식이 아니라 더 효율적이고 의미 있는 다른 작업증명 방식이 필요.
  - **오라클 문제** - 블록체인 외부에서 데이터를 참조해야 하는 경우, 외부 데이터를 신뢰해야 하는 문제 발생(중앙화, 보안)
- **비지니스 적용 관점의 문제 (Private Blockchain)**
  - 익명성 - 은행거래에서는 익명성을 허용하지 않으며, 거래가 비가역적이라는 부분도 이체 사고 발생 시 강제로 이체를 동결하거나 법정인도명령등에 따르기 위해 강제인도 등을 해야 할 경우 대응하지 못하는 문제가 있음
  - 투명성 - 모두가 다른 사용자의 잔고와 이체내역을 확인하는 것은 현재 규제와 금융 통념상 불가능 함.
  - **접속 권한 관리** - 퍼블릭 블록체인은 누구나 네트워크망에 접속하여 사용이 가능한데, 기관의 입장에서는 참여자의 선택적 진입과 권한 수준 설정 등의 기능이 필요함.

안전한 Private key 관리 기술

- 암호 자산의 소유를 증명할 수 있는 개인의 private key 관리의 책임을 어떻게 감소시키는가?
  - 신뢰 할 수 있는 제3자에게 위임 : 현재 대부분의 사용자는 거래소에 자신의 키를 위임 시켜 놓음
  - 중앙화의 문제가 있으며, 결국은 자산이 커지면 이또한 진정한 해결책이 될 수 없음
  - 키에 대한 관리 책임을 한 곳에 집중하지 않고 여러 곳으로 분리하는 방향으로 발전
- Multi-signature Wallet & Threshold signature Wallet
  - 여러 개의 키를 이용하여 여러 개의 서명을 통해 디지털 자산의 소유권을 증명
  - N of M : 총 M개의 키 중 N개의 키로 생성된 서명이 있다면 소유권 증명 가능
  - 비트코인은 locking script, 이더리움은 스마트컨트랙트를 이용하여 지원
- Threshold signature Wallet
  - 여러 개의 키를 이용하여 여러 개의 서명을 통해 디지털 자산의 소유권을 증명
  - N of M : 총 M개의 키 중 N개의 키를 이용하여 하나의 서명을 생성하고 이를 통해 소유권을 증명
  - 블록체인과 무관하게 여러가지 암호 연산 기법을 통해 블록체인 외부에서 동작

Secret Sharing Vs Secure MPC



11

Secure MPC

- 동형암호학 (Homomorphic encryption)
  Homomorphic encryption is a form of encryption with an additional evaluation capability for computing over encrypted data without access to the secret key.
- Secret Sharing (Secret Splitting)
- Secure Multi-party Computation
- Threshold signature는 MPC 기법을 전자서명에 적용
  - ✓ Threshold ECDSA
  - ✓ Schnorr Signatures
  - ✓ BLS : Boneh-Lynn-Shacham signatures
- Muti-Signature의 경우 온체인 연산의 비용 문제, Threshold Signature의 경우 성능 및 사용자 간 사용성(참여자가 온라인으로 연결되어 있어야 함 등) 문제를 해결해야 함

12

블록체인 확장성 기술

- 블록체인 특성 상 채굴노드(마이너)의 수를 아무리 증가시켜도 처리속도가 늘어나지 않음. (비트코인 7TPS, 이더리움 14TPS)
- 블록체인이 가지고 있는 확장성(Scalability) 문제와 성능(Performance) 문제를 해결하고자 함
- 익명성 보장 문제도 함께 해결 가능
- 크게 3가지 형태로 시도.
  - ✓ On-Chain Solution (Layer1 Technology)
  - ✓ Off-Chain Solution (Layer2 Technology)
  - ✓ Inter-Chain Solution (Side-Chain)
- 블렉체인 간 또는 블록체인과 오프체인 간 상대의 상태/데이터의 무결성을 어떻게 신뢰할 수 있는가에 대한 문제가 남아있음

13

오라클(Oracle) 문제

- 스마트 컨트랙트를 동작시키는 요인이 블록체인 외부로부터 받아야 되는 경우 다음과 같은 사항들을 고려해야 함
  - ✓ 어떤 채널에서, 어떤 주체로 부터, 어떤 데이터를 수집할 것인가?
  - ✓ 데이터 전송 과정에서 위변조 가능성이 있는가?
  - ✓ 외부에서 가져온 데이터를 신뢰할 수 있는가? (데이터의 무결성)
- 스마트 컨트랙트는 주어진 데이터가 사실인지 아닌지를 판단할 수 없기 때문에 잘못된 데이터가 입력되어도 그대로 동작하며, 블록체인의 비가역적인 특성 때문에 한 번 실행된 결과는 되돌릴 수 없음
- 중앙화된 오라클에서 도덕적 해이가 발생할 경우 이를 방지할 수 없으며, 중앙화된 오라클이 고장 나거나 공격받을 경우 단일 실패 지점(Single Point of Failure)로 작용할 수도 있다는 문제가 생김
- 오라클의 구분
  - 해당 오라클의 정보가 객관적 사실 판단이 필요한 지 혹은 주관적 사실 판단이 필요한 지에 따라 구분할 수 있으며, 객관적 사실 판단이 필요한 경우는 다시 블록체인 내부에서 검증이 가능한지 아닌 지로 구분할 수 있음
  - ✓ Computational Oracle : 객관적인 사실을 다루면서 블록체인 내에서 연산을 진행하면서 검증이 가능한 정보를 처리하는 경우
  - ✓ Reporting Oracle : 객관적인 사실을 다루지만 블록체인 밖에서 일어난 사실 정보를 입력하는 경우
  - ✓ Jurying Oracle : 블록체인 밖에서 일어난 사건에 대해서 특정 참가자들이 주관적인 판단을 하고 그 결과를 입력하는 경우

14

탈중앙화 오라클 메커니즘

- Computational Oracle
  - ✓ 블록체인 외부에서 컴퓨터 연산을 진행하고 그 결과를 블록체인 상에 기록
  - ✓ 블록체인 외부에서 연산을 진행하는 이유는, 블록체인 상에서 연산 시 과도한 가스비가 예상되거나 가스비 최대 한계를 넘을 가능성 때문

- 외부 정보를 가져오는 방법
  - ✓ Single User Reporting Mechanism :
    특정 참여자를 선출하여 오라클 정보를 입력하도록 하고 다른 참여자들이 해당 정보를 감시하고 검증할 수 있도록 하는 방법 (challenge system 사용)
  - ✓ Voting Mechanism :
    서비스 참여자들은 자신이 생각하는 옳은 정답에 토큰을 걸고, 투표 기간이 끝난 이후에는 어떤 선택지가 가장 많은 토큰을 받았는지에 따라 오라클 결과가 결정

- 오라클 과정에 사용자들이 참여하도록 유도하고, 참여자들이 올바르게 행동하도록 하기 위한 인센티브 구조 (토큰이코노미) 설계가 필요하며 작동 과정이 너무 복잡하고 느릴 수 있다는 문제점이 여전히 있음

15

익명성 기술

❖ 거래추적 익명화
- 코인믹싱(Coin Mixing) / 코인조인 (Coin Join)
  - ✓ 여러 사람의 코인을 섞어서 익명성을 보장하는 기술
  - ✓ 믹싱에 참여하는 사람의 숫자와 코인의 수량이 늘어날수록 추적이 어려워짐
  - ✓ 코인 조인은 코인 믹싱에 의한 거래를 중계자 없이 P2P형태로 진행하는 것을 의미

- 스텔스(Stealth) 주소
  - ✓ 매 거래마다 자동으로 일회용 주소를 생성하는 기술.
  - ✓ 사용자의 본래의 주소를 일회용 주소로 감추어 익명성을 보장받음.

- 링(Ring)서명 / 링CT
  - ✓ 서명 시 사용자의 공개키 뿐만 아니라 다른 사용자의 공개키까지 사용하여 섞음으로써 정확한 송금자를 찾지 못하게 하는 기술

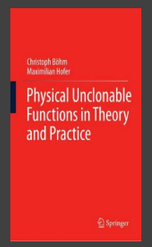
❖ 원장내용 익명화
- 영지식증명 (zero-knowledge proof, ZKP) : zk-SNARKS, zk-STARKS
  - ✓ 거래 결과에 대한 참, 거짓만 공개하고 거래의 내용은 비공개로 하는 선택적 익명성을 가진 기술.

16

VIA PUF 소개

PUF (Physical Unclonable Function)

❖ PUF: a Unique Physical Signature of Integrated Devices



PUF는 동일한 제조공정에서 생산되는 반도체의 미세구조 차이를 이용해 보안 키를 생성하고, 이를 활용하는 기술이다. 나노 단위의 반도체의 미세구조는 외부 난수값 주입(RNG) 없이 자체적으로 랜덤하게 생성되며, 사람의 지문처럼 고유성을 지니기 때문에 '반도체 칩 지문'으로도 불린다.
PUF의 가장 큰 특징은 랜덤하게 발생하는 반도체 미세구조의 특징상 복제가 불가능하다는 점이다. 미세구조 차이를 키 값으로 사용하기에 기기에 키 값이 저장되지 않아 해킹 당할 염려가 없으며, 고유 키 값을 사용한 전자서명 구조를 통해 부인 방지 기능이 강화돼 기기 인증에도 활용될 수 있다.

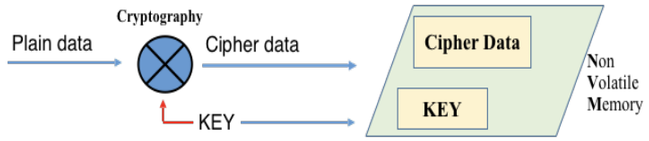
- **Why PUF?** *"IoT 장치는 유비쿼터스적 성격과 전력 등의 제약으로 하드웨어 보안에 독특한 문제를 지니고 있다. 따라서 기존 소프트웨어 및 암호화 방식은 개인키를 저장해야 하는 방식의 보안적 한계와 큰 전력을 소진하는 연산문제 때문에 IoT의 독특한 환경에는 적합하다고 볼 수 없다… …이에 비해 PUF는 반도체 생산 시 나타나는 임의의 물리적 현상에 따라 일정하게 생성되는 난수값을 필요시 키로 활용하는 방식이기에 주요정보를 저장할 필요가 없는 적합하고 안전한 방식이다."*

- Utilize micro tolerance of semiconductor process
- Same process & same design, but unique pattern on every chip
- Unclonable finger print on the chip

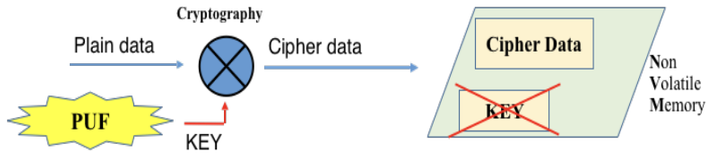
18

PUF 보안 방식의 장점

❖ 기존 방식



❖ PUF 사용 시



PUF 구현 방식

Table 1.1 Performance of different approaches

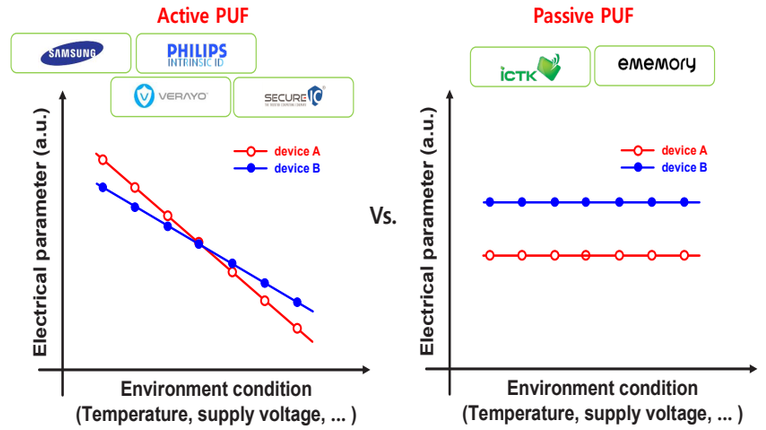
Approach	Ref.	Temp. (°C)	HD_{intra} (%)	HD_{inter}(%)
ID Cell	[44]	−25..125	5	50
Ring-oscillator PUF1[a]	[74]	20..120	0.48	46.15
Ring-oscillator PUF2[a]	[50]	25..65	<2	47.31
Arbiter PUF	[74]	20..120	9	23
SRAM PUF1	[21]	−20..80	12	50
SRAM PUF2	[27]	room	5	Bias to 1
Latch PUF	[73]	0..80	5.5	50
Inverter-based PUF[a]	[62]	20..125	0.4	50
Butterfly PUF	[37]	−20..80	6	50
D-flip-flop PUF1[b]	[49]	room	<5	50
D-flip-flop PUF2	[40]	−40..80	10	35
Glitch-based PUF	[75]	0..80	<8	40

[a]With kind of preselection (see Chap. 10)
[b]After bias compensation

출처 : physical unclonable functions in theory and practice

Active PUF vs. Passive PUF

✓ ECC(Error Correction Code) 필요 유무에 따라 Active PUF와 Passive PUF로 구분 가능

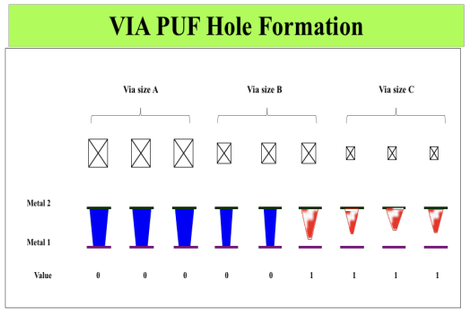


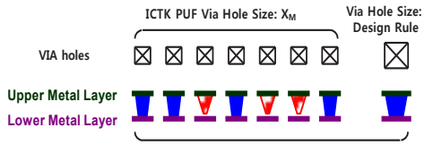
✓ Error Correction Code is required !

✓ No Error Correction Code

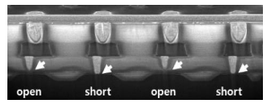
VIA PUF

- Utilize VIA holes between metal layers
- Certain hole size gives "open or short" randomly by recipe not by design
- The combination of this "open and short" generates VIA PUF





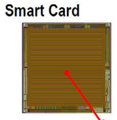
[Cross-sectional Views of ICTK VIA Hole Design Concept]

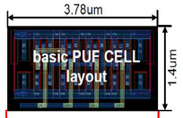


[Actual Sectional View of ICTK via PUF (SAM)]

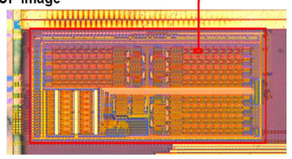
VIA PUF 기술의 우수성

Smart Card





PUF image



SAMSUNG

ISSCC, 2016

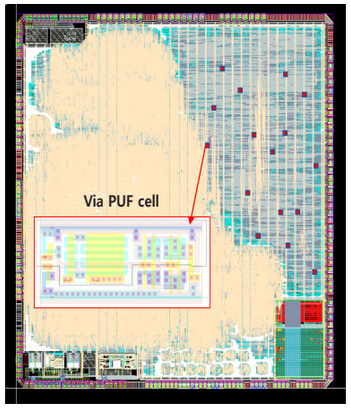
ememory

ISSCC, 2018

✓ PUF 기능을 위한 영역이 물리적으로 구분되어 있음.

Vs.

iCTK IRST1412



✓ Via PUF 셀은 스텐더드셀화 되어 일반 via hole 사이에 섞여 있어 구분 불가.
✓ 찾는다 하더라도 위에서 그 via PUF 값이 open/ short 구분이 불가.

23

PUF의 활용

ICTK PUF 제품 영업 현황

15

❖ Sales & Marketing Activities

Korea:
- "카"은행의 System Administration Security H/W (FlyHigh)
- "L"그룹 생활가전 thinQ, 유플러스 Access Point (AP), IoT WiFi 모듈의 H/W 보안인증모듈 (LG CNS)
- "S"전자 필요스펙 및 가격 검토 중 (G-Valley)
- "K" 이통사 위즈박스 (WizBox)의 망분리 보안 모듈
- "H"보안업체 제큐어 키 메니지먼트 Xecure Key Manager에 secure token 응용
- "C"체인 블록체인 서비스의 consensus algorithm 및 코인/토큰 운영 시스템 적용
- "H"社과 비디오 실시간 암호/복호화칩 공동 개발 중

China (Beijing & Shenzhen):
- "H"社(중국 가전 선두 업체)의 생활가전의 WiFi 모듈 데이터보호 및 인증용 적용(현재 수출형 도입, 중국 국내형 시험중)
- "B"社 (S/W 보안 업체) 차량용 T-box 통신 보안 모듈 공동 개발 협의 중
- "B"社 (중국 국영 전기 미터링 업체) 스마트 미터 지불보안칩 IP 가격 검토 중
- "A"社 (중국 인터넷 선두 업체)의 ID2 IoT H/W 인증 보안모듈 파트너 공식 등록

Europe:
- **Innovation Award** (혁신상) 수상: 2016 유럽 Smart Security Week, Digital ID/Hardware ID Security 부문 [IBM & ST Micro. 다른 카테고리 수상]
- 폴란드 2016 Krynica 경제포럼, IoT 보안정책 패널 참석
- 룩셈부르크 Internet Day 컨퍼런스 IoT Security 패널 참석

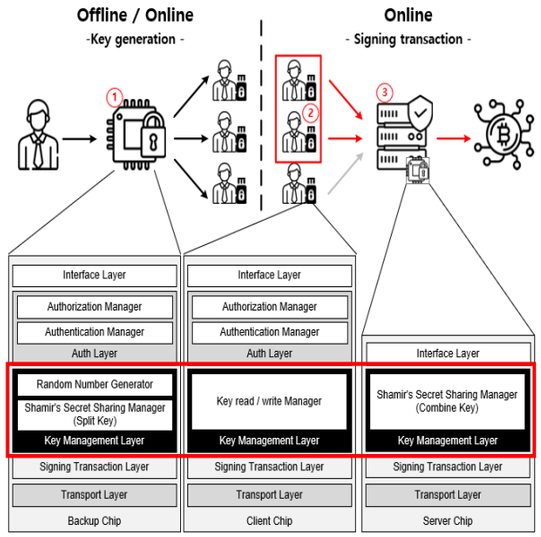
iCTK Holdings

PUF의 활용 : Off-chain Smart Contract & shared ledger

- 블록체인 스마트컨트랙트의 특징
  - 특정 입력 값에 대해 어떤 출력 값이 나올지 모두 알 수 있음
  - 누구도 임의로 로직을 바꾸지 못함 : 구현되어진 형태(=약속)대로 동작
  - 특정 조건이 만족되면 자동적으로 동작하며 누구도 동작을 임의로 제어하지 못함
- 블록체인 공유원장의 특징
  - 정해진 규칙에 따라 데이터가 생성되고 저장
  - 누구도 임의로 해당 데이터를 변경하지 못함 (삭제 포함)
  - 특정 데이터는 소유권을 증명(디지털서명) 할 수 있는 사람만 소비 가능
- PUF의 특성을 이용하여 강력한 보안칩(Secure Smart Chip)을 만들어서 해당 칩 내부에 누구도 임의로 변경할 수 없고, 정해진 규칙에 따라 동작하고 데이터를 처리하는 신뢰 가능한 실행 환경 및 신뢰 가능한 저장 환경을 구축할 수 있다면, 블록체인 상의 스마트컨트랙트와 공유원장의 특징을 만족하는 오프체인 환경을 구성할 수 있음
- 이와 같이 블록체인 외부에 신뢰 가능한 실행 환경을 만드는 것이 가능하다면, 1) 합의절차를 생략하고 2) 블록체인 상의 높은 연산 비용(예를 들어, 이더리움의 가스비 등)을 제거하는 것이 가능하게 되어, 보다 가볍고 빠르게 동작하며 보다 높은 확장성을 제공하는 것이 가능
- 이러한 기능을 하는 보안칩은 기존에 사용되던 형태에 비해 더 높은 가치를 다루게 되므로 상대적으로 높은 보안 요구사항을 가지게 됨

26

PUF 활용 예 #1 : 암호자산 보안지갑 & 커스터디 솔루션

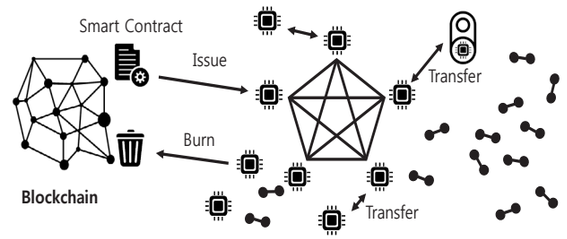


PUF 활용 예 #1 : 암호자산 보안지갑 & 커스터디 솔루션

❖ PUF를 활용한 Custody Service 구현 방안 및 장점

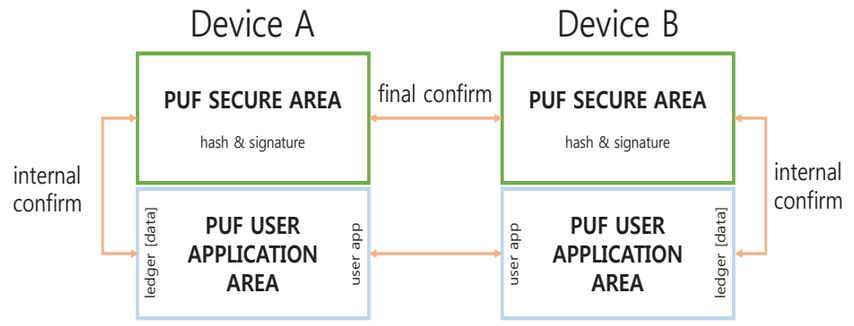
- 보안적 측면
  - ✓ 보다 간단한 로직으로 구현이 가능하므로 오 동작의 소지 및 로직 상의 공격 가능 지점이 적어짐
- 성능적 측면
  - ✓ 스마트컨트랙트 지갑 혹은 블록체인 스크립트 구현 방식에 비해 매우 가볍게 동작
  - ✓ 소프트웨어 구현 방식 지갑에 비해 간단한 로직으로 동작이 가능하며, 참여자 간 데이터 통신 횟수를 최소화 할 수 있어 빠르게 동작
- 기능적 측면
  - ✓ 오프체인에서도 스마트컨트랙트 지갑과 마찬가지로 다양하게 동작하는 유연성 확보가 가능

PUF 활용 예 #2 : PUF 보안칩을 이용한 2nd Layer 솔루션



- PUF 보안칩을 이용한 2nd Layer chain 구성
  - ✓ PUF 보안칩 내 신뢰 가능 실행 및 저장 환경을 이용하여, 모든 노드 간 제3자 합의 없이 빠르게 동작하면서도 해당 데이터의 무결성을 보장 (참여자 양자 합의)
  - ✓ 모든 노드가 무결성을 합의해야하는 블록체인의 경우 모든 노드들은 모든 데이터와 트랜잭션 정보를 저장하고 확인하여야 하지만, 이러한 방식은 굳이 모든 데이터를 저장하고 처리하지 않아도 됨 (해당 PUF보안칩/디바이스는 자신의 데이터만 처리)
  - ✓ 특정 거래는 외부에 독립적이므로 무한한 확장성
  - ✓ 거래 무결성 확인을 위한 거래 이력이 반드시 필요하지 않으므로 익명성 구현 가능

PUF 활용 예 #2 : PUF 보안칩을 이용한 2nd Layer 솔루션



<initial PUF key based digital signature exchange>

- ✓ 실행 로직은 PUF 보안칩 내부의 신뢰 실행환경에서 동작
- ✓ 해당 디바이스의 원장은 PUF 보안칩 내부의 신뢰 데이터 영역에 기록
- ✓ 거래 시작 전과 후에 서로 상대편 디바이스의 상태와 무결성을 점검하고 확정
- ✓ 필요한 경우 제3의 PUF 보안 디바이스를 이용하여 무결성 및 보안성 강화

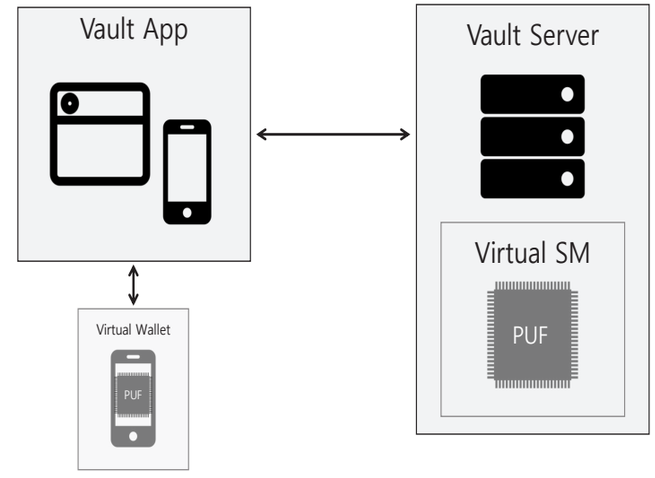
PUF 활용 : 남아있는 과제

- PUF 보안칩 인증 체계 (탈중앙화 된 방식)
- PUF Key의 복구 불가능한 특징을 고려 – 분실 또는 파손 시 PUF Key 처리 방안
- 이외에 기술 상용화 시점에 발생 가능한 모든 사항

Appendix : Demo

Demo #1 : Vault Service Demo

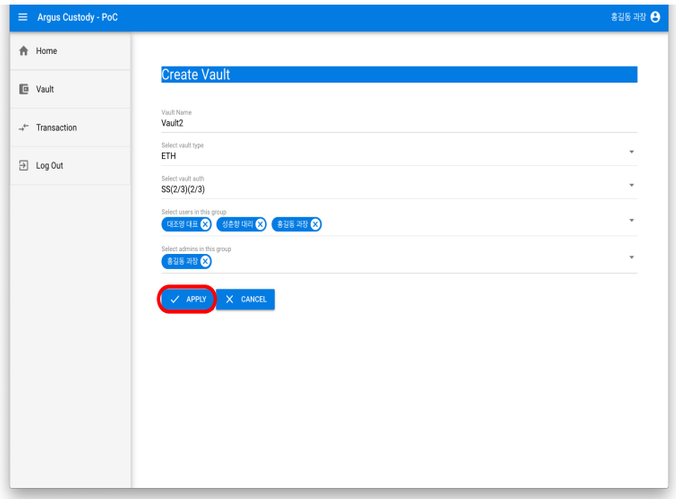
Demo Architecture



Demo Scenario

1. Create Vault
2. Create Private Key
3. Create Secret sharing Key
4. Save Secret Shared Key
5. Transfer Asset
   1) Start Txn
   2) Create Txn
   3) Txn wait for Confirm
   4) Plug Key & Confirm
   5) Check the Result

1. Create Vault



1. Create Vault

Vault 생성 요청

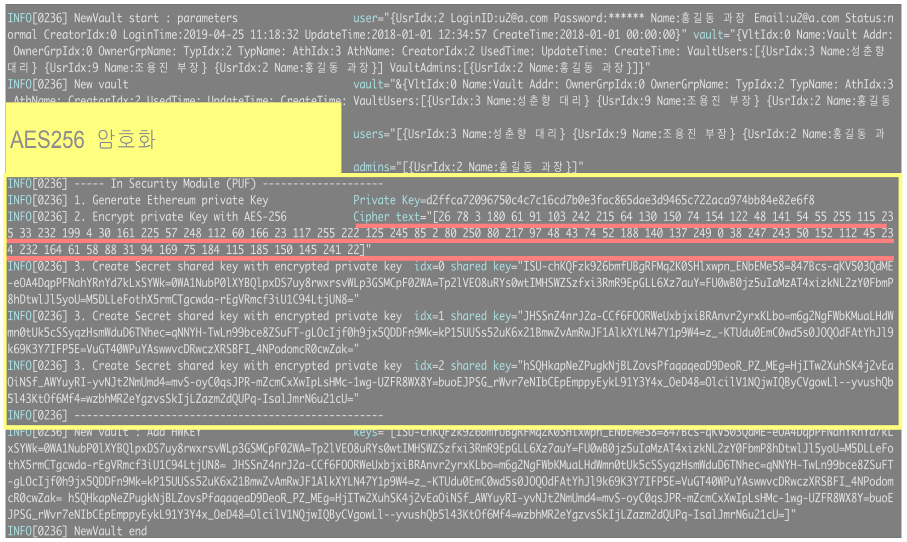
```
INFO[0236] New vault                                     user="{UsrIdx:2 LoginID:u2@a.com Password:****** Name:홍길동 과장 Email:u2@a.com Status:n
 AthName: CreatorIdx:2 UsedTime: UpdateTime: CreateTime: VaultUsers:[{UsrIdx:3 Name:성춘향 대리} {UsrIdx:9 Name:조용진 부장} {UsrIdx:2 Name:홍길동
 과장}] VaultAdmins:[{UsrIdx:2 Name:홍길동 과장}]}"
INFO[0236] New vault : Add vault users                   users="[{UsrIdx:3 Name:성춘향 대리} {UsrIdx:9 Name:조용진 부장} {UsrIdx:2 Name:홍길동 과
장}]"
INFO[0236] New vault : Add vault admins                  admins="[{UsrIdx:2 Name:홍길동 과장}]"
INFO[0236] ----- In Security Module (PUF) ----------
INFO[0236] 1. Generate Ethereum private Key              Private Key=d2ffca72096750c4c7c16cd7b0e3fac865dae3d9465c722aca974bb84e82e6f8
INFO[0236] 2. Encrypt private Key with AES-256           Cipher text="[26 78 3 180 61 91 103 242 215 64 130 150 74 154 122 48 141 54 55 255 115 23
5 33 232 199 4 30 161 225 57 248 112 60 166 23 117 255 222 125 245 85 2 80 250 80 217 97 48 43 74 52 188 140 137 249 0 38 247 243 50 152 112 45 23
4 232 164 61 58 88 31 94 169 75 184 115 185 150 145 241 22]"
INFO[0236] 3. Create Secret shared key with encrypted private key  idx=0 shared key="ISU-chKQFzk926bmfU8gRFMq2K0SHlxwpn_ENbEMe58=847Bcs-qKV503QdME
-eOA4DqpPFNahYRnYd7kLxSYWk=0WA1NubP0lXYBQlpxDS7uy8rwxrsvWLp3GSMCpF02WA=Tp2lVEO8uRYs0wtIMHSWZSzfxi3RmR9EpGLL6Xz7auY=FU0wB0jz5uIaMzAT4xizkNL2zY0FbmP
8hDtwlJl5yoU=M5DLLeFothX5rmCTgcwda-rEgVRmcf3iU1C94LtjUN8="
INFO[0236] 3. Create Secret shared key with encrypted private key  idx=1 shared key="JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdW
mn0tUk5cSSyqzHsmWduDGTNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP15UUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9
k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak="
INFO[0236] 3. Create Secret shared key with encrypted private key  idx=2 shared key="hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEa
OiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb
5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU="
INFO[0236] ------------------------------------------------
INFO[0236] New vault : Add HAKEY                         keys="[ISU-chKQFzk926bmfU8gRFMq2K0SHlxwpn_ENbEMe58=847Bcs-qKV503QdME-eOA4DqpPFNahYRnYd7k
LxSYWk=0WA1NubP0lXYBQlpxDS7uy8rwxrsvWLp3GSMCpF02WA=Tp2lVEO8uRYs0wtIMHSWZSzfxi3RmR9EpGLL6Xz7auY=FU0wB0jz5uIaMzAT4xizkNL2zY0FbmP8hDtwlJl5yoU=M5DLLeFo
thX5rmCTgcwda-rEgVRmcf3iU1C94LtjUN8= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduDGTNhec=qNNYH-TwLn99bce8ZSuFT
-gLOcIjf0h9jx5QDDFn9Mk=kP15UUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodom
cR0cwZak= hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEaOiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoE
JPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU="]
INFO[0236] NewVault end
```


2. Create Private Key

Private key 생성 (random)

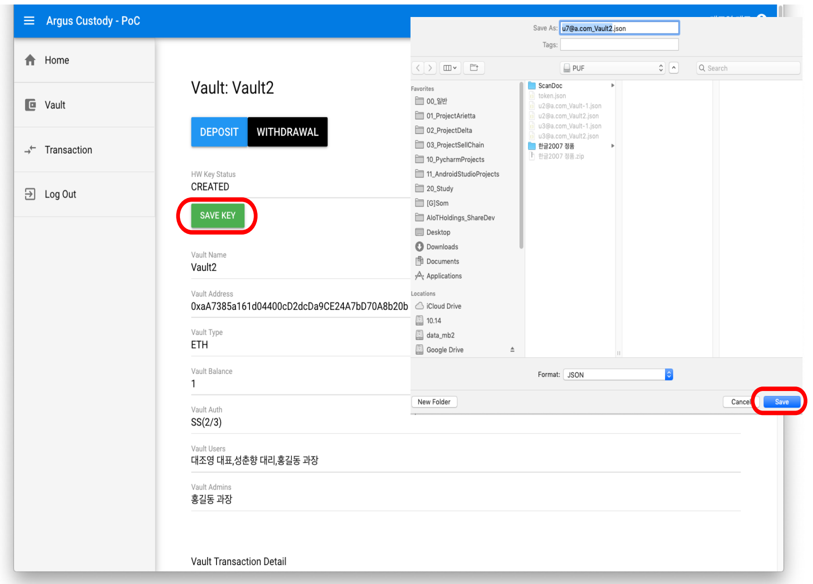
```
INFO[0236] NewVault start : parameters                   user="{UsrIdx:2 LoginID:u2@a.com Password:****** Name:홍길동 과장 Email:u2@a.com Status:n
ormal CreatorIdx:0 LoginTime:2019-04-25 11:18:32 UpdateTime:2018-01-01 12:34:57 CreateTime:2018-01-01 00:00:00}" vault="{VltIdx:0 Name:Vault Addr:
 OwnerGrpIdx:0 OwnerGrpName: TypIdx:2 TypName: AthIdx:3 AthName: CreatorIdx:2 UsedTime: UpdateTime: CreateTime: VaultUsers:[{UsrIdx:3 Name:성춘향
대리} {UsrIdx:9 Name:조용진 부장} {UsrIdx:2 Name:홍길동 과장}] VaultAdmins:[{UsrIdx:2 Name:홍길동 과장}]}"
INFO[0236] New vault                                     vault="&{VltIdx:0 Name:Vault Addr: OwnerGrpIdx:0 OwnerGrpName: TypIdx:2 TypName: AthIdx:3
 AthName: CreatorIdx:2 UsedTime: UpdateTime: CreateTime: VaultUsers:[{UsrIdx:3 Name:성춘향 대리} {UsrIdx:9 Name:조용진 부장} {UsrIdx:2 Name:홍길동
 과장}] VaultAdmins:[{UsrIdx:2 Name:홍길동 과장}]}"
INFO[0236] New vault : Add vault users                   users="[{UsrIdx:3 Name:성춘향 대리} {UsrIdx:9 Name:조용진 부장} {UsrIdx:2 Name:홍길동 과
장}]"
INFO[0236] New vault : Add vault admins                  admins="[{UsrIdx:2 Name:홍길동 과장}]"
INFO[0236] ----- In Security Module (PUF) ----------
INFO[0236] 1. Generate Ethereum private Key              Private Key=d2ffca72096750c4c7c16cd7b0e3fac865dae3d9465c722aca974bb84e82e6f8
INFO[0236] 2. Encrypt private Key with AES-256           Cipher text="[26 78 3 180 61 91 103 242 215 64 130 150 74 154 122 48 141 54 55 255 115 23
5 33 232 199 4 30 161 225 57 248 112 60 166 23 117 255 222 125 245 85 2 80 250 80 217 97 48 43 74 52 188 140 137 249 0 38 247 243 50 152 112 45 23
4 232 164 61 58 88 31 94 169 75 184 115 185 150 145 241 22]"
INFO[0236] 3. Create Secret shared key with encrypted private key  idx=0 shared key="ISU-chKQFzk926bmfU8gRFMq2K0SHlxwpn_ENbEMe58=847Bcs-qKV503QdME
-eOA4DqpPFNahYRnYd7kLxSYWk=0WA1NubP0lXYBQlpxDS7uy8rwxrsvWLp3GSMCpF02WA=Tp2lVEO8uRYs0wtIMHSWZSzfxi3RmR9EpGLL6Xz7auY=FU0wB0jz5uIaMzAT4xizkNL2zY0FbmP
8hDtwlJl5yoU=M5DLLeFothX5rmCTgcwda-rEgVRmcf3iU1C94LtjUN8="
INFO[0236] 3. Create Secret shared key with encrypted private key  idx=1 shared key="JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdW
mn0tUk5cSSyqzHsmWduDGTNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP15UUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9
k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak="
INFO[0236] 3. Create Secret shared key with encrypted private key  idx=2 shared key="hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEa
OiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb
5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU="
INFO[0236] ------------------------------------------------
INFO[0236] New vault : Add HAKEY                         keys="[ISU-chKQFzk926bmfU8gRFMq2K0SHlxwpn_ENbEMe58=847Bcs-qKV503QdME-eOA4DqpPFNahYRnYd7k
LxSYWk=0WA1NubP0lXYBQlpxDS7uy8rwxrsvWLp3GSMCpF02WA=Tp2lVEO8uRYs0wtIMHSWZSzfxi3RmR9EpGLL6Xz7auY=FU0wB0jz5uIaMzAT4xizkNL2zY0FbmP8hDtwlJl5yoU=M5DLLeFo
thX5rmCTgcwda-rEgVRmcf3iU1C94LtjUN8= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduDGTNhec=qNNYH-TwLn99bce8ZSuFT
-gLOcIjf0h9jx5QDDFn9Mk=kP15UUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodom
cR0cwZak= hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEaOiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoE
JPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU="]
INFO[0236] NewVault end
```

2. Create Private Key

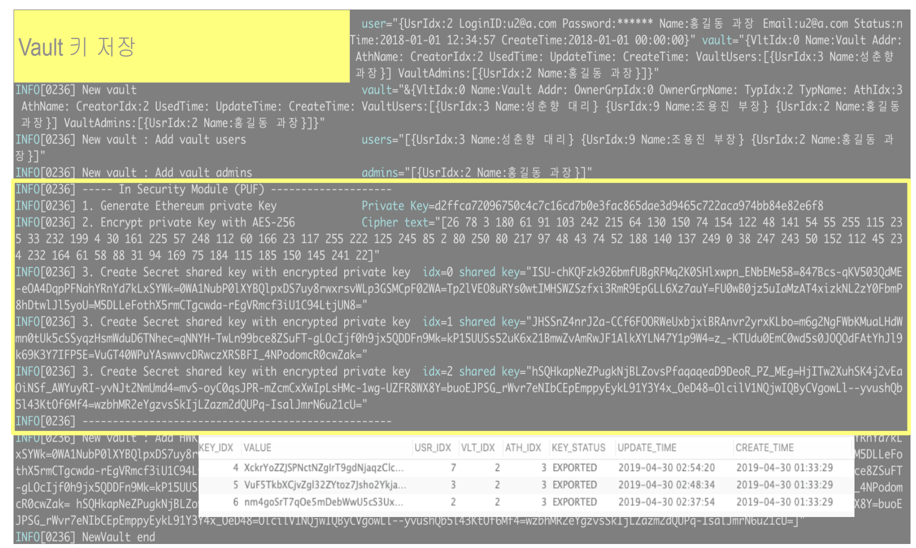


3. Create Secret sharing Key

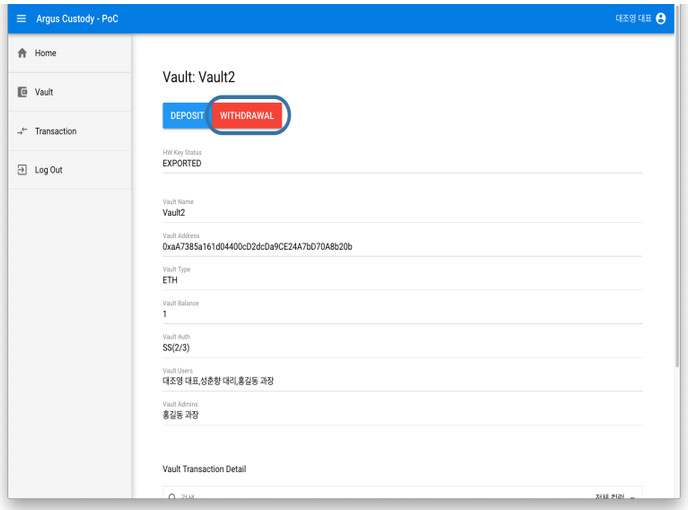
4. Save Secret Shared Key



4. Save Secret Shared Key

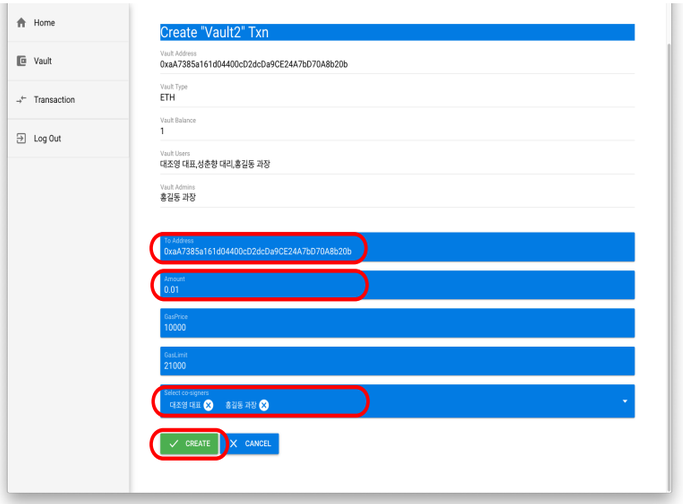


5. Transfer Asset : 1) Start Txn



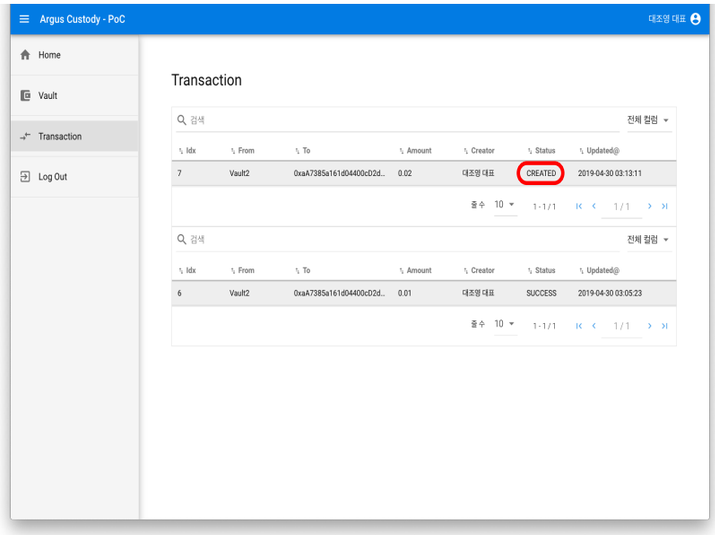
43

5. Transfer Asset : 2) Create Txn



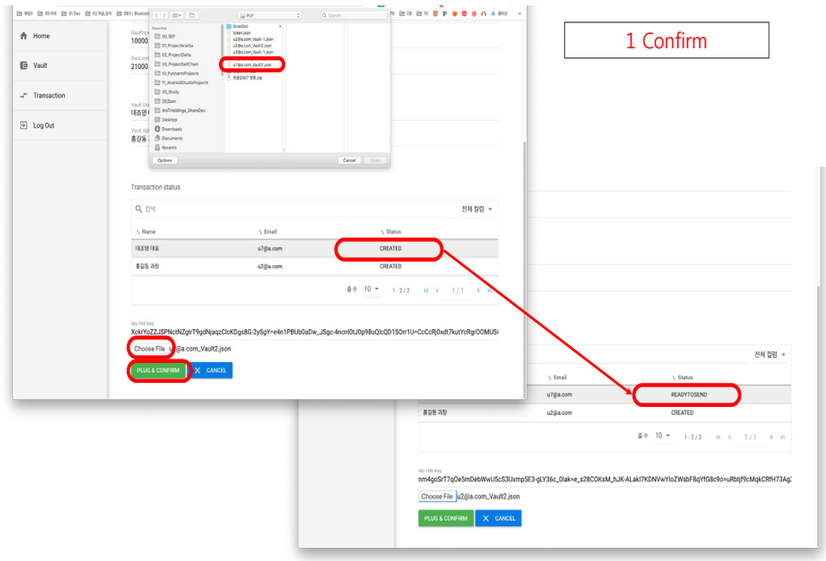
44

5. Transfer Asset : 3) Txn Wait for Confirm



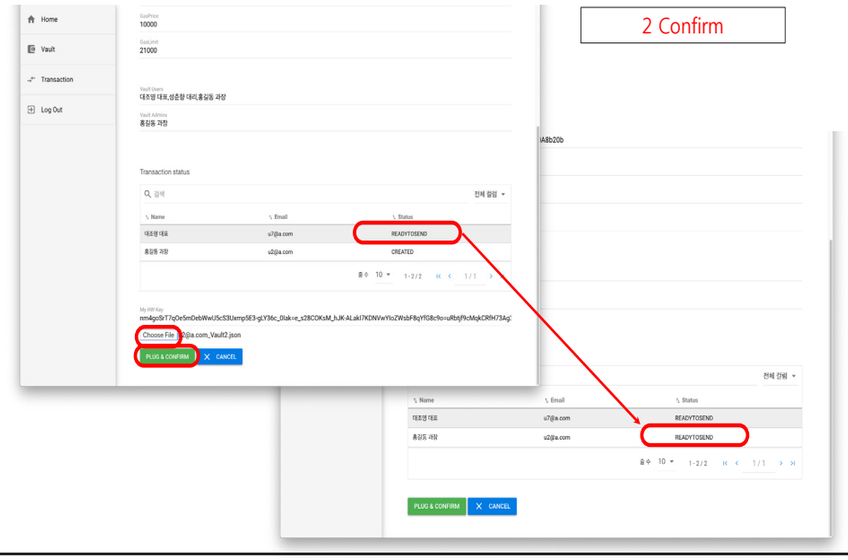
45

5. Transfer Asset : 4) Plug Key & Confirm



46

5. Transfer Asset : 4) Plug Key & Confirm



5. Transfer Asset : 4) Plug Key & Confirm

트랜잭션 생성

```
INFO[0133] ConfirmTxn start : parameters                 txnuserhwkey="{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrx
KLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}" user="{UsrIdx:9 LoginID:u9@a.com Password:****** Nam
1 LoginTime:2019-04-25 11:35:40 UpdateTime:2019-04-24 07:04:16 CreateTime:2019-04-24 07:04:
16}"
INFO[0133] Confirm txn                                   vault="&{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m
6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd
5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}"
INFO[0135] Request sign of ETH transaction               amount=10000000000000000 chainId=3 data="[]" gasLimit=21000 gasPrice=1000000000 nonce=0 s
haredKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEaOiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=bu
oEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CC
f6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1A
lkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1
0f477
INFO[0135] ----- In Security Module (PUF) -------------------
INFO[0135] 1. Combine Secret shared key                  result (encrypted key)="[26 78 3 180 61 91 103 242 215 64 130 150 74 154 122 48 141 54 55
 255 115 235 33 232 199 4 30 161 225 57 248 112 60 166 23 117 255 222 125 245 85 2 80 250 80 217 97 48 43 74 52 188 140 137 249 0 38 247 243 50 15
2 112 45 234 232 164 61 58 88 31 94 169 75 184 115 185 150 145 241 22]" sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEa
OiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb
5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=
qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAsww
vcDRwczXRSBFI_4NPodomcR0cwZak=]"
INFO[0135] 2. Decrypt private Key with AES-256           result (private key)=d2ffca72096750c4c7c16cd7b0e3fac865dae3d9465c722aca974bb84e82e6f8
INFO[0135] 3. Sign Tx                                    SingedTx="&{data:{AccountNonce:0 Price:0xc0003b2ae0 GasLimit:21000 Recipient:0xc000332240
 Amount:0xc0003b2ac0 Payload:[] V:0xc0003b2c80 R:0xc0003b2c20 S:0xc0003b2c40 Hash:<nil>} hash:{v:<nils>} size:{v:<nils>} from:{v:<nils>}}"
INFO[0135] ------------------------------------------------
INFO[0135] Send ETH transaction                          TxId=0x3ca6f3e547ea414e46be26d2478cadf8ea135a8b2a20f2f23febc27925d6fe88
INFO[0135] ConfirmTxn end
```


5. Transfer Asset : 4) Plug Key & Confirm

트랜잭션 서명 요청

```
INFO[0133] ConfirmTxn start : parameters                 txnuserhwkey="{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrx
KLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}" user="{UsrIdx:9 LoginID:u9@a.com Password:****** Nam
e:조용진 부장 Email:u9@a.com Status:CREATED CreatorIdx:1 LoginTime:2019-04-25 11:35:40 UpdateTime:2019-04-24 07:04:16 CreateTime:2019-04-24 07:04:
16}"
INFO[0133] Confirm txn                                   vault="&{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m
6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd
5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}"
INFO[0135] Request sign of ETH transaction               amount=10000000000000000 chainId=3 data="[]" gasLimit=21000 gasPrice=1000000000 nonce=0 s
haredKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEaOiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=bu
oEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CC
f6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1A
lkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1
0f477
INFO[0135] ----- In Security Module (PUF) -------------------
INFO[0135] 1. Combine Secret shared key                  result (encrypted key)="[26 78 3 180 61 91 103 242 215 64 130 150 74 154 122 48 141 54 55
 255 115 235 33 232 199 4 30 161 225 57 248 112 60 166 23 117 255 222 125 245 85 2 80 250 80 217 97 48 43 74 52 188 140 137 249 0 38 247 243 50 15
2 112 45 234 232 164 61 58 88 31 94 169 75 184 115 185 150 145 241 22]" sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITwZXuhSK4j2vEa
OiNSf_AWYuyRI-yvNJtZNmUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb
5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=
qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUSs52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAsww
vcDRwczXRSBFI_4NPodomcR0cwZak=]"
INFO[0135] 2. Decrypt private Key with AES-256           result (private key)=d2ffca72096750c4c7c16cd7b0e3fac865dae3d9465c722aca974bb84e82e6f8
INFO[0135] 3. Sign Tx                                    SingedTx="&{data:{AccountNonce:0 Price:0xc0003b2ae0 GasLimit:21000 Recipient:0xc000332240
 Amount:0xc0003b2ac0 Payload:[] V:0xc0003b2c80 R:0xc0003b2c20 S:0xc0003b2c40 Hash:<nil>} hash:{v:<nils>} size:{v:<nils>} from:{v:<nils>}}"
INFO[0135] ------------------------------------------------
INFO[0135] Send ETH transaction                          TxId=0x3ca6f3e547ea414e46be26d2478cadf8ea135a8b2a20f2f23febc27925d6fe88
INFO[0135] ConfirmTxn end
```

Secret share key combine

5. Transfer Asset : 4) Plug Key & Confirm

```
INFO[0133] ConfirmTxn start : parameters                txnuserhwkey="{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}" user="{UsrIdx:9 LoginID:u9@a.com Password:****** Name:조용진 부장 Email:u9@a.com Status:CREATED CreatorIdx:1 LoginTime:2019-04-25 11:35:40 UpdateTime:2019-04-24 07:04:16 CreateTime:2019-04-24 07:04:16]"
INFO[0133] Confirm txn                                  vault="&{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}"
INFO[0133] Request sign of ETH transaction              amount=10000000000000000 chainId=3 data="[]" gasLimit=21000 gasPrice=10000000000 nonce=0 sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITw2XuhSK4j2vEaOiNSf_AWYuyRI-yvNJt2NnUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1b6427
INFO[0135] ----- In Security Module (PUF) -------------------
INFO[0135] 1. Combine Secret shared key                 result (encrypted key)="[26 78 3 180 61 91 103 242 215 64 130 150 74 154 122 48 141 54 55 255 115 235 33 232 199 4 30 161 225 57 248 112 60 166 23 117 255 222 125 245 85 2 80 250 80 217 97 48 43 74 52 188 140 137 249 0 38 247 243 50 15 150 145 241 22]" sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITw2XuhSK4j2vEaOiNSf_AWYuyRI-yvNJt2NnUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1b6427
INFO[0135] 2. Decrypt private Key with AES-256          result (private key)=d2ffca72096750c4c7c16cd7b0e3fac865dae3d9465c722aca974bb84e82e6f8
INFO[0135] 3. Sign Tx                                   SingedTx="&{data:{AccountNonce:0 Price:0xc0003b2ae0 GasLimit:21000 Recipient:0xc000332240 Amount:0xc0003b2ac0 Payload:[] V:0xc0003b2c80 R:0xc0003b2c20 S:0xc0003b2c40 Hash:<nil>} hash:{v:<nil>} size:{v:<nil>} from:{v:<nils>}}"
INFO[0135] ------------------------------------------------
INFO[0135] Send ETH transaction                         TxId=0x3ca6f3e547ea414e46be26d2478cadf8ea135a8b2a20f2f23febc27925d6fe88
INFO[0135] ConfirmTxn end
```

AES256 복호화

51

5. Transfer Asset : 4) Plug Key & Confirm

```
INFO[0133] ConfirmTxn start : parameters                txnuserhwkey="{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}" user="{UsrIdx:9 LoginID:u9@a.com Password:****** Name:조용진 부장 Email:u9@a.com Status:CREATED CreatorIdx:1 LoginTime:2019-04-25 11:35:40 UpdateTime:2019-04-24 07:04:16 CreateTime:2019-04-24 07:04:16]"
INFO[0133] Confirm txn                                  vault="&{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}"
INFO[0133] Request sign of ETH transaction              amount=10000000000000000 chainId=3 data="[]" gasLimit=21000 gasPrice=10000000000 nonce=0 sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITw2XuhSK4j2vEaOiNSf_AWYuyRI-yvNJt2NnUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1b6427
INFO[0135] ----- In Security Module (PUF) -------------------
INFO[0135] 1. Combine Secret shared key                 result (encrypted key)="[26 78 3 180 61 91 103 242 215 64 130 150 74 154 122 48 141 54 55 255 115 235 33 232 199 4 30 161 225 57 248 112 60 166 23 117 255 222 125 245 85 2 80 250 80 217 97 48 43 74 52 188 140 137 249 0 38 247 243 50 15 150 145 241 22]" sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITw2XuhSK4j2vEaOiNSf_AWYuyRI-yvNJt2NnUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1b6427
INFO[0135] 2. Decrypt private Key with AES-256          result (private key)=d2ffca72096750c4c7c16cd7b0e3fac865dae3d9465c722aca974bb84e82e6f8
INFO[0135] 3. Sign Tx                                   SingedTx="&{data:{AccountNonce:0 Price:0xc0003b2ae0 GasLimit:21000 Recipient:0xc000332240 Amount:0xc0003b2ac0 Payload:[] V:0xc0003b2c80 R:0xc0003b2c20 S:0xc0003b2c40 Hash:<nil>} hash:{v:<nil>} size:{v:<nil>} from:{v:<nils>}}"
INFO[0135] ------------------------------------------------
INFO[0135] Send ETH transaction                         TxId=0x3ca6f3e547ea414e46be26d2478cadf8ea135a8b2a20f2f23febc27925d6fe88
INFO[0135] ConfirmTxn end
```

트랜잭션 서명

52

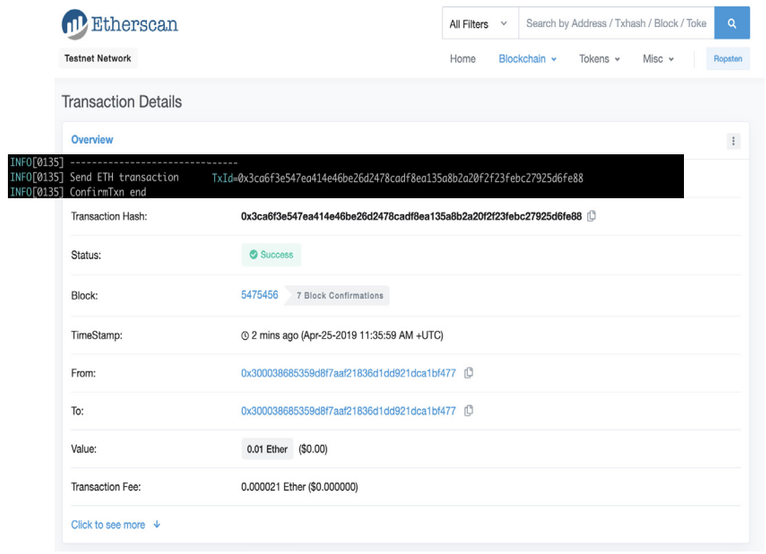
5. Transfer Asset : 4) Plug & Confirm

```
INFO[0133] ConfirmTxn start : parameters                txnuserhwkey="{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}" user="{UsrIdx:9 LoginID:u9@a.com Password:****** Name:조용진 부장 Email:u9@a.com Status:CREATED CreatorIdx:1 LoginTime:2019-04-25 11:35:40 UpdateTime:2019-04-24 07:04:16 CreateTime:2019-04-24 07:04:16]"
INFO[0133] Confirm txn                                  vault="&{TxnIdx:56 T2uIdx:75 UsrIdx:9 HWKey:JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak= UpdateTime:}"
INFO[0133] Request sign of ETH transaction              amount=10000000000000000 chainId=3 data="[]" gasLimit=21000 gasPrice=10000000000 nonce=0 sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITw2XuhSK4j2vEaOiNSf_AWYuyRI-yvNJt2NnUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1b6427
INFO[0135] ----- In Security Module (PUF) -------------------
INFO[0135] 1. Combine Secret shared key                 result (encrypted key)="[26 78 3 180 61 91 103 242 215 64 130 150 74 154 122 48 141 54 55 255 115 235 33 232 199 4 30 161 225 57 248 112 60 166 23 117 255 222 125 245 85 2 80 250 80 217 97 48 43 74 52 188 140 137 249 0 38 247 243 50 15 150 145 241 22]" sharedKeys="[hSQHkapNeZPugkNjBLZovsPfaqaqeaD9DeoR_PZ_MEg=HjITw2XuhSK4j2vEaOiNSf_AWYuyRI-yvNJt2NnUmd4=mvS-oyC0qsJPR-mZcmCxXwIpLsHMc-1wg-UZFR8WX8Y=buoEJPSG_rWvr7eNIbCEpEmppyEykL91Y3Y4x_OeD48=OlcilV1NQjwIQByCVgowLl--yvushQb5l43KtOf6Mf4=wzbhMR2eYgzvsSkIjLZazm2dQUPq-IsalJmrN6u21cU= JHSSnZ4nrJ2a-CCf6FOORWeUxbjxiBRAnvr2yrxKLbo=m6g2NgFWbKMuaLHdWmn0tUk5cSSyqzHsmWduD6TNhec=qNNYH-TwLn99bce8ZSuFT-gLOcIjf0h9jx5QDDFn9Mk=kP1SUUss52uK6x21BmwZvAmRwJF1AlkXYLN47Y1p9W4=z_-KTUdu0EmC0wd5s0JOQOdFAtYhJl9k69K3Y7IFP5E=VuGT40WPuYAswwvcDRwczXRSBFI_4NPodomcR0cwZak=]" to=0x300038685359d8F7aaF21836D1Dd921DCa1b6427
INFO[0135] ------------------------------------------------
INFO[0135] Send ETH transaction                         TxId=0x3ca6f3e547ea414e46be26d2478cadf8ea135a8b2a20f2f23febc27925d6fe88
INFO[0135] ConfirmTxn end
```

트랜잭션 전송

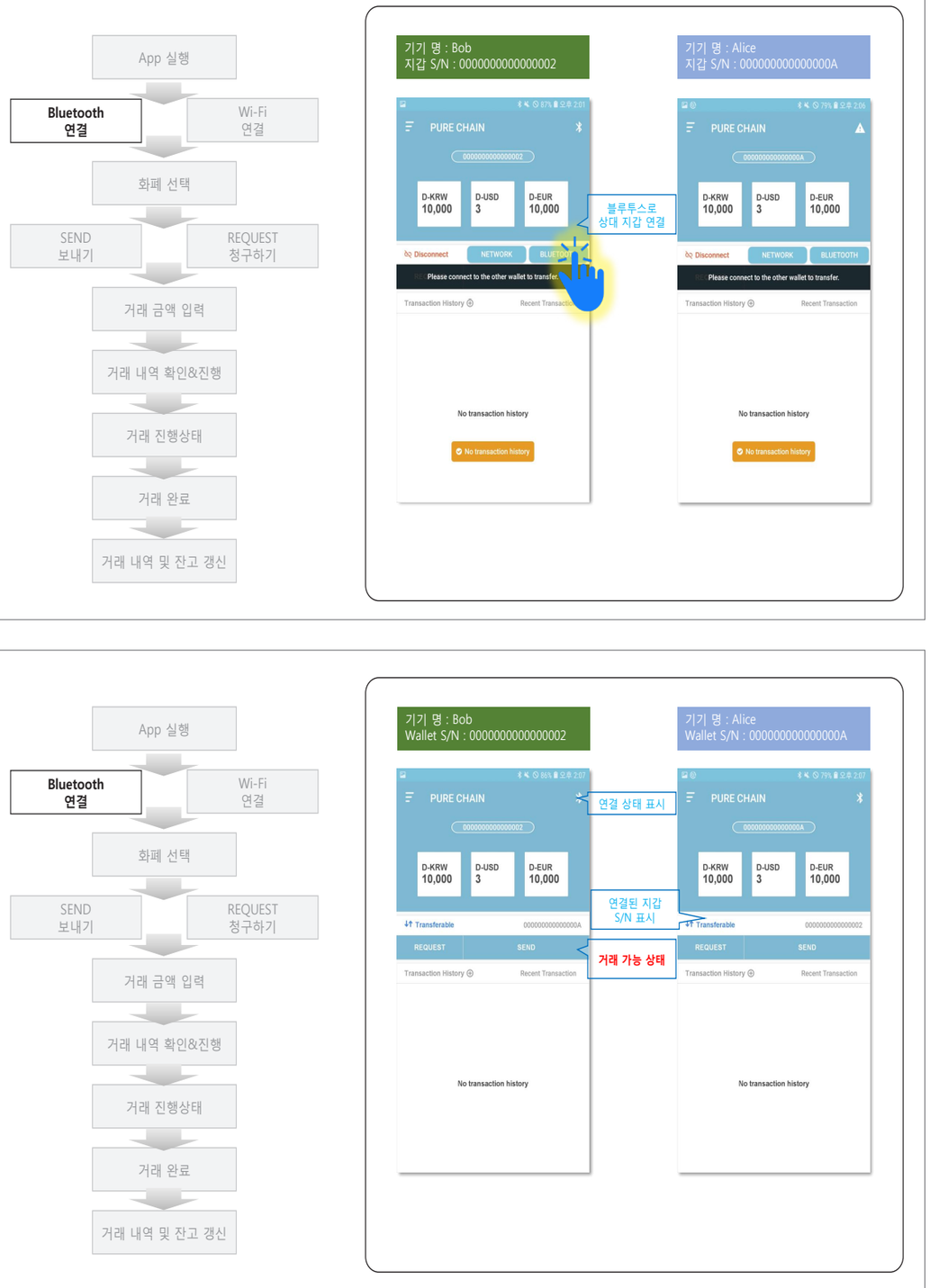
53

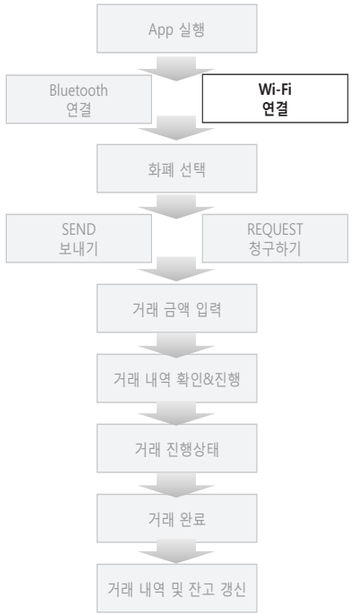
5. Transfer Asset : 5) Check the Result

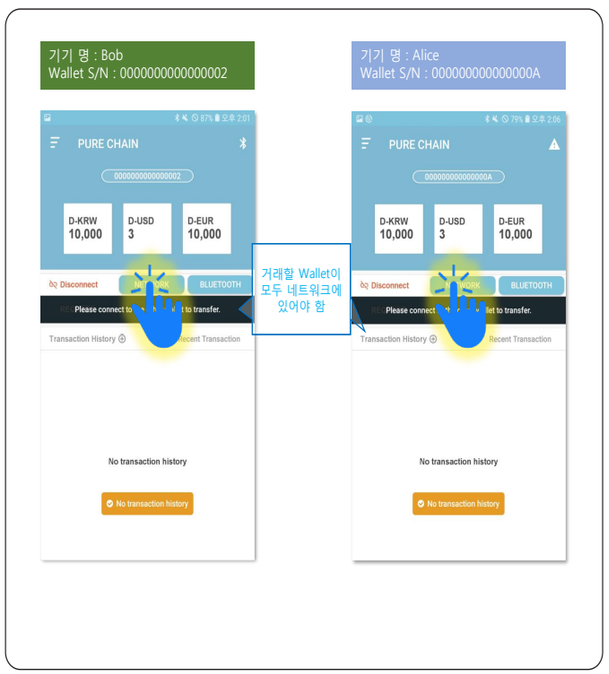


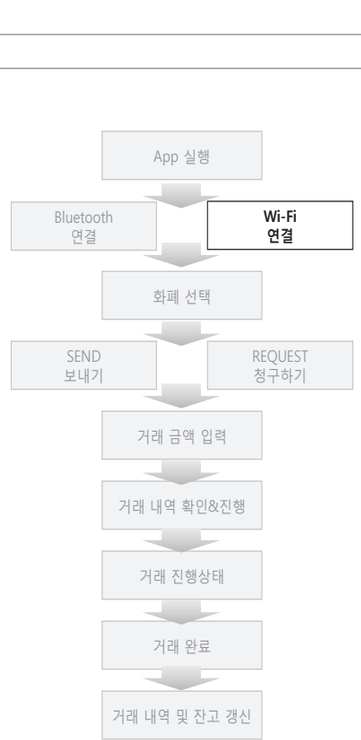
54

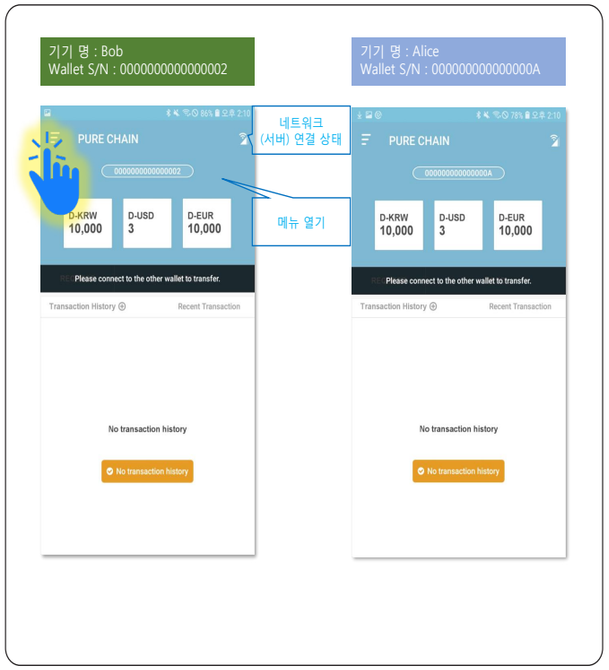
Demo #2 : purechain (PUF-Chain) Demo

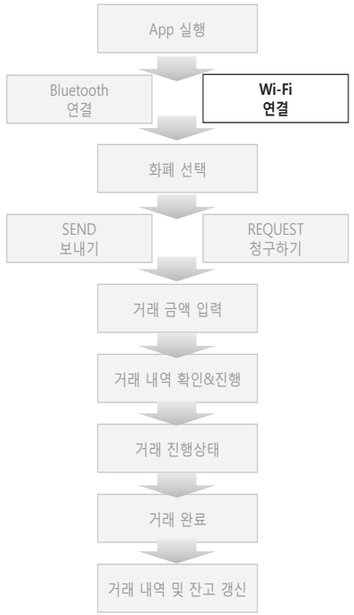


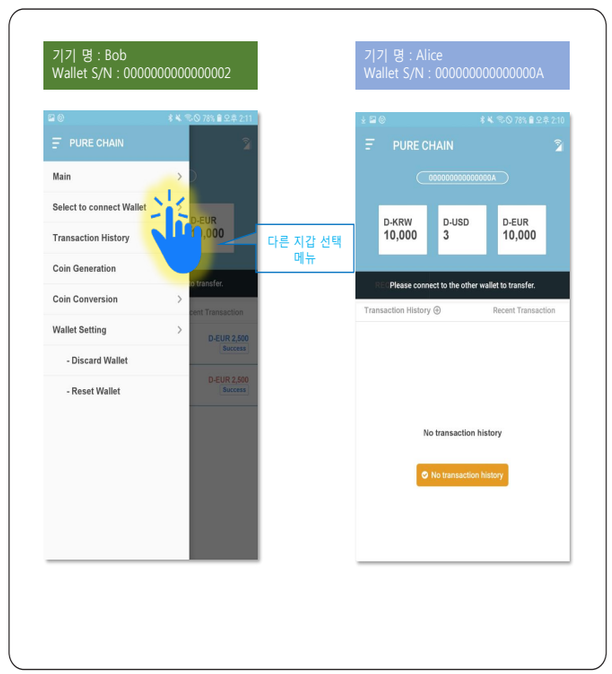

App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

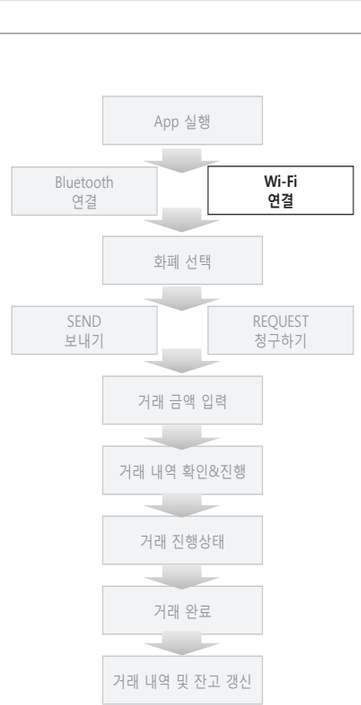

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
PURE CHAIN
D-KRW 10,000
D-USD 3
D-EUR 10,000
Disconnect
BLUETOOTH
Please connect to the other wallet to transfer.
Transaction History
Recent Transaction
No transaction history
거래할 Wallet이 모두 네트워크에 있어야 함

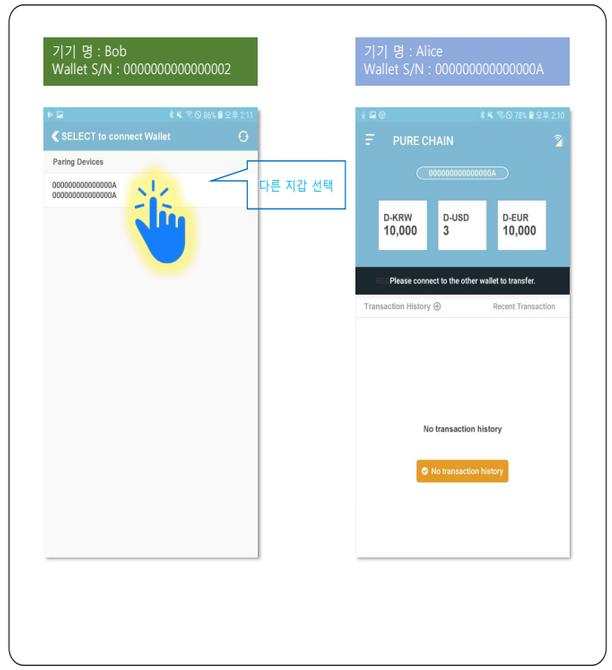

App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

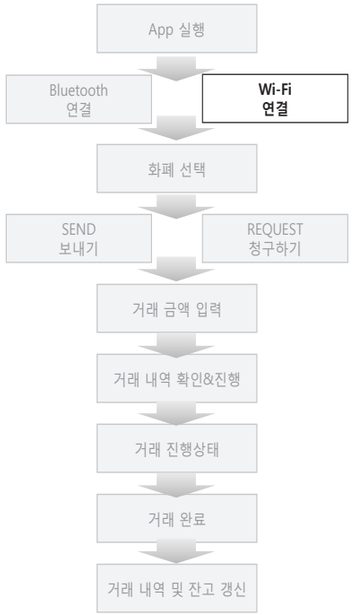

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
PURE CHAIN
D-KRW 10,000
D-USD 3
D-EUR 10,000
Please connect to the other wallet to transfer.
Transaction History
Recent Transaction
No transaction history
네트워크 (서버) 연결 상태
메뉴 열기


App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

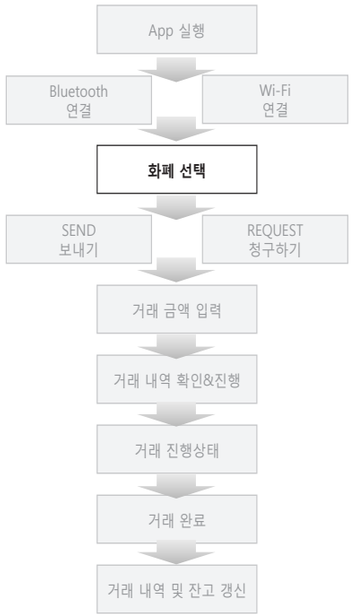

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
PURE CHAIN
Main
Select to connect Wallet
Transaction History
Coin Generation
Coin Conversion
Wallet Setting
- Discard Wallet
- Reset Wallet
D-KRW 10,000
D-USD 3
D-EUR 10,000
Please connect to the other wallet to transfer.
Transaction History
Recent Transaction
No transaction history
다른 지갑 선택 메뉴


App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

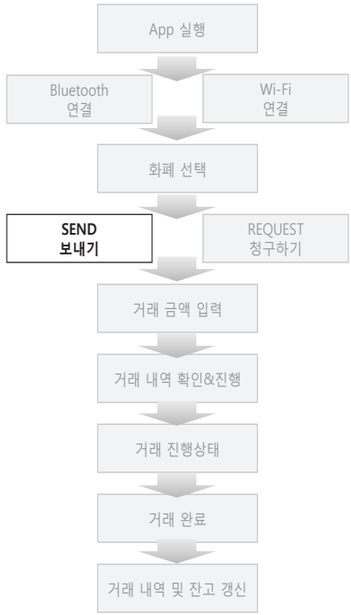

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
SELECT to connect Wallet
Paring Devices
000000000000000A
000000000000000A
PURE CHAIN
D-KRW 10,000
D-USD 3
D-EUR 10,000
Please connect to the other wallet to transfer.
Transaction History
Recent Transaction
No transaction history
다른 지갑 선택

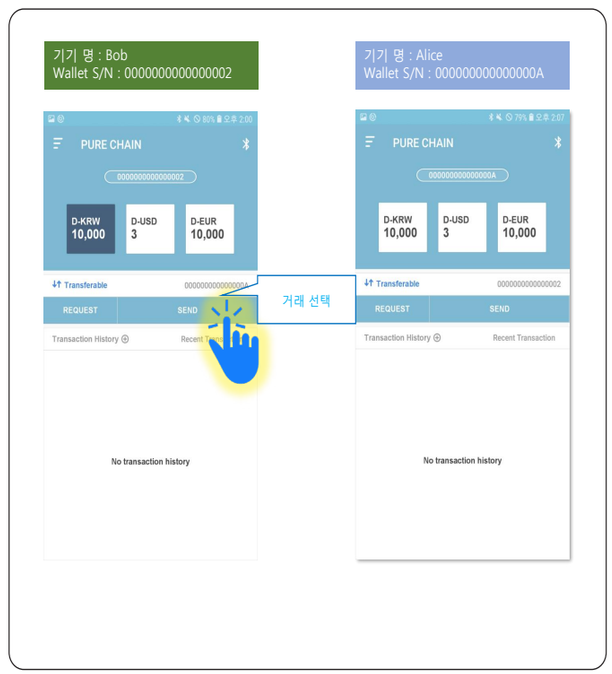

App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

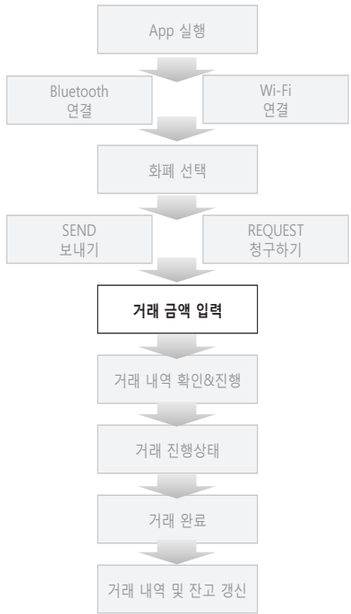

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
PURE CHAIN
D-KRW 10,000
D-USD -
D-EUR -
D-KRW 10,000
D-USD 3
D-EUR 10,000
Transferable
REQUEST
SEND
Transaction History
Recent Transaction
No transaction history
Successfully connected to the other wallet.
연결된 지갑 S/N 표시
거래 가능 상태


App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

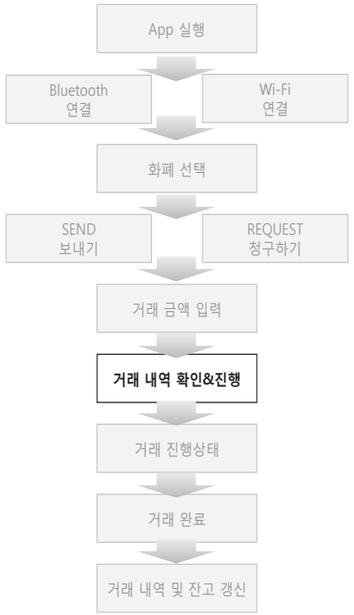

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
PURE CHAIN
D-KRW 10,000
D-USD 3
D-EUR 10,000
Transferable
REQUEST
SEND
Transaction History
Recent Transaction
No transaction history
거래할 화폐 선택


App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

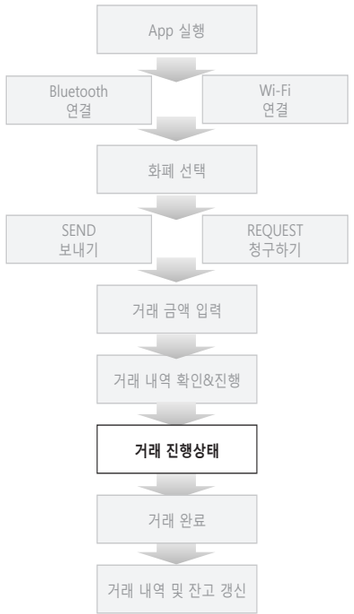

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
PURE CHAIN
D-KRW 10,000
D-USD 3
D-EUR 10,000
Transferable
REQUEST
SEND
Transaction History
Recent Transaction
No transaction history
거래 선택

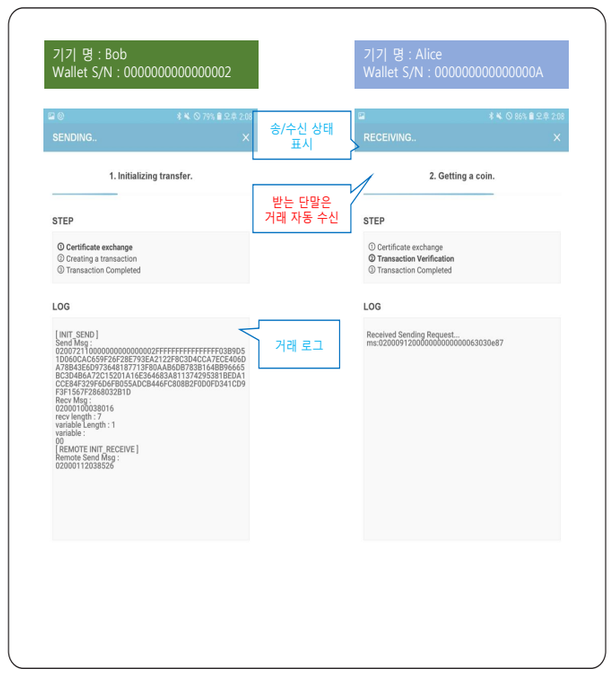

App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

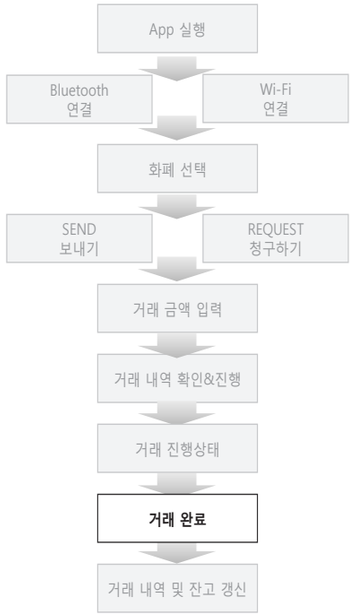

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
SEND
D-KRW 10,000
Wallet Name
0000000000000002
D-KRW Sending Amount
2500
Receiver
000000000000000A
SEND
PURE CHAIN
D-KRW 10,000
D-USD 3
D-EUR 10,000
Transferable
REQUEST
SEND
Transaction History
Recent Transaction
No transaction history
거래할 금액 입력

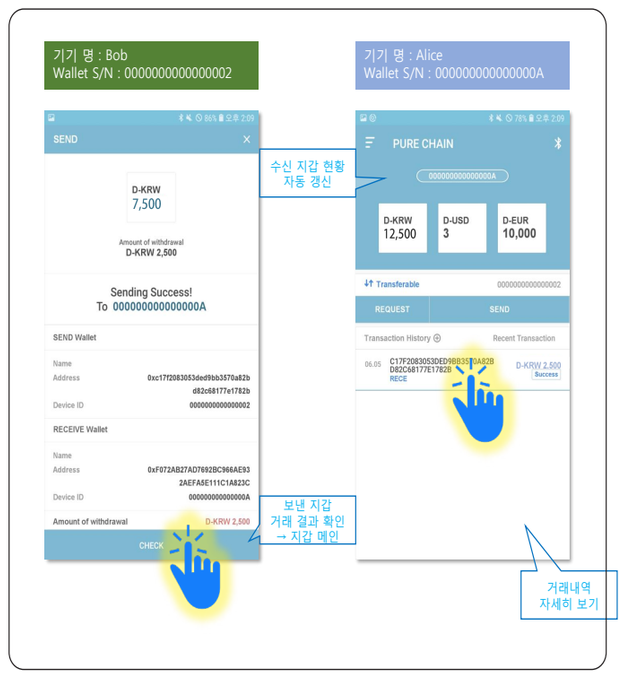

App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신

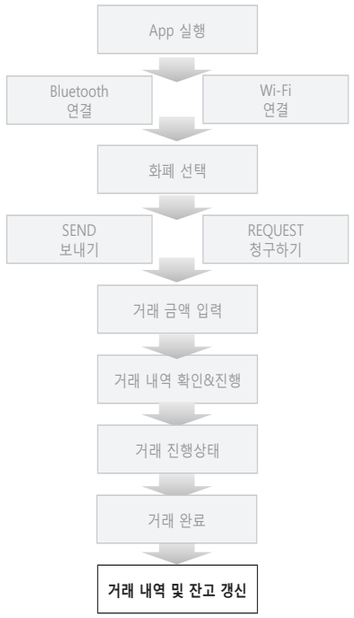

기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
SEND
Do you want to send to 000000000000000A?
SEND Wallet
Name
Address
0xc17f2083053ded9bb3570a82b d82c68177e1782b
Wallet S/N
0000000000000002
RECEIVE Wallet
Name
Address
0xF072AB27AD7692BC966AE93 2AEFA5E111C1A823C
Wallet S/N
000000000000000A
Sending Amount
D-KRW 2,500
NO
YES
보낼 지갑 주소 & S/N & 거래 금액 확인
PURE CHAIN
D-KRW 10,000
D-USD 3
D-EUR 10,000
Transferable
REQUEST
SEND
Transaction History
Recent Transaction
No transaction history

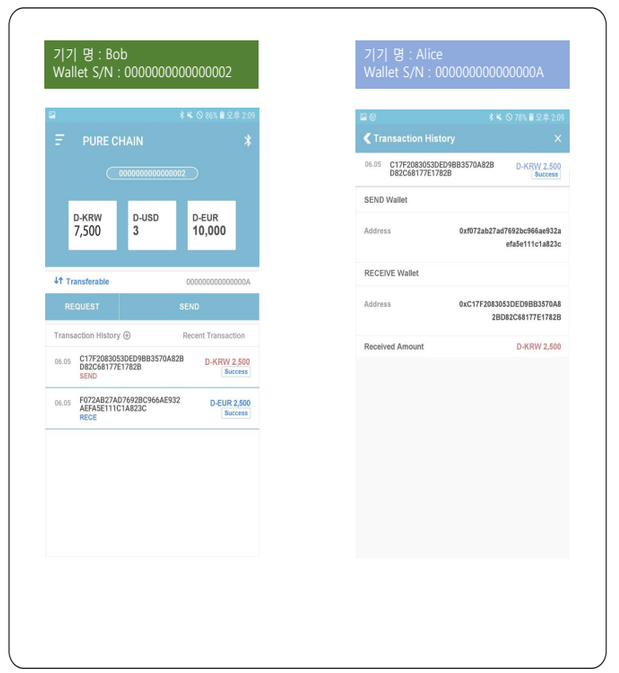

App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신


기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
SENDING..
RECEIVING..
송/수신 상태 표시
1. Initializing transfer.
2. Getting a coin.
STEP
Certificate exchange
Creating a transaction
Transaction Completed
Certificate exchange
Transaction Verification
Transaction Completed
받는 단말은 거래 자동 수신
LOG
[INIT_SEND]
Send Msg :
02007211000000000000000002FFFFFFFFFFFFFFFF03B905 1D060CAC659F26F2BE793EA2122F8C3D4CCA7ECE406D A78B43E6D97364818771 3F80AAB6DB783B164BB96665 BC3D4B6A72C15201A16E364683AB11374295381BEDA1 CCE84F329F6D6FB055ADCB446FC808B2F0D0FD341CD9 F3F1567F2868032B1D
Recv Msg :
02000100038016
recv length : 7
variable Length : 1
variable :
00
[REMOTE INIT_RECEIVE]
Remote Send Msg :
02000112038526
거래 로그
Received Sending Request...
ms:02000912000000000000063030e87


App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신


기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
SEND
D-KRW 7,500
Amount of withdrawal
D-KRW 2,500
Sending Success!
To 000000000000000A
SEND Wallet
Name
Address
0xc17f2083053ded9bb3570a82b d82c68177e1782b
Device ID
0000000000000002
RECEIVE Wallet
Name
Address
0xF072AB27AD7692BC966AE93 2AEFA5E111C1A823C
Device ID
000000000000000A
Amount of withdrawal
D-KRW 2,500
CHECK
수신 지갑 현황 자동 갱신
보낸 지갑 거래 결과 확인 → 지갑 메인
PURE CHAIN
D-KRW 12,500
D-USD 3
D-EUR 10,000
Transferable
REQUEST
SEND
Transaction History
Recent Transaction
06.05
C17F2083053DED9BB3570A82B D82C68177E1782B
RECE
D-KRW 2,500
Success
거래내역 자세히 보기


App 실행
Bluetooth 연결
Wi-Fi 연결
화폐 선택
SEND 보내기
REQUEST 청구하기
거래 금액 입력
거래 내역 확인&진행
거래 진행상태
거래 완료
거래 내역 및 잔고 갱신


기기 명 : Bob
Wallet S/N : 0000000000000002
기기 명 : Alice
Wallet S/N : 000000000000000A
PURE CHAIN
0000000000000002
D-KRW 7,500
D-USD 3
D-EUR 10,000
Transferable
000000000000000A
REQUEST
SEND
Transaction History
Recent Transaction
06.05
C17F2083053DED9BB3570A82B D82C68177E1782B
SEND
D-KRW 2,500
Success
06.05
F072AB27AD7692BC966AE932 AEFA5E111C1A823C
RECE
D-EUR 2,500
Success
Transaction History
06.05
C17F2083053DED9BB3570A82B D82C68177E1782B
D-KRW 2,500
Success
SEND Wallet
Address
0xf072ab27ad7692bc966ae932a efa5e111c1a823c
RECEIVE Wallet
Address
0xC17F2083053DED9BB3570A8 2BD82C68177E1782B
Received Amount
D-KRW 2,500

Part III

블록체인 구축과 Smart Contract 실습

좌장 : 최윤호 교수
(부산대학교)

Ethereum 네트워크 구축 및 Smart Contract 구현 실습
- 대한전자공학회 블록체인 워크샵

Ethereum
스마트 계약 개발 환경 구축

2019.06.17
부산대학교 최윤호교수

PUSAN NATIONAL UNIVERSITY
SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Software & System Security Laboratory

개요

I 스마트 계약 소개 ▸▸

II 개발 환경 구축 ▸▸

스마트 계약 소개

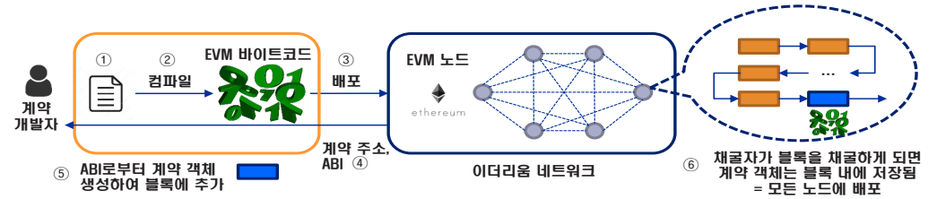
- 스마트 계약 개요
- 스마트 계약 동작 과정
- 스마트 계약 작성
- 스마트 계약 개발 도구

스마트 계약 개요

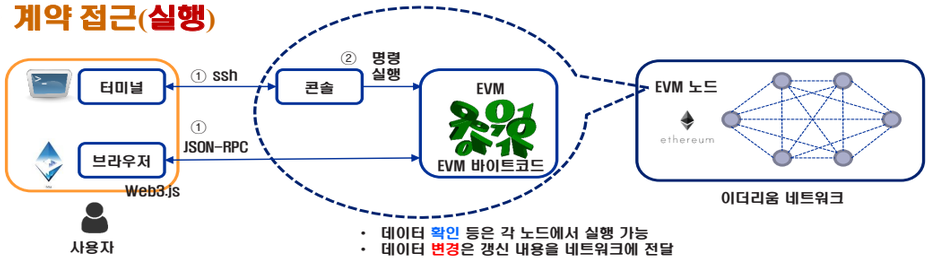
◆ 스마트 계약(Smart Contract) 이란?
- 특정 계약을 스스로 수립, 검증, 이행하기 위한 프로토콜 – 위키피디아
- 블록체인에서 동작하는 응용프로그램의 단위. 즉, EVM 바이트코드
  - EVM (Ethereum Virtual Machine)
  - EVM 바이트코드: EVM 고유의 바이너리 형식 (응용프로그램)
- 스마트 계약의 개발 및 이용 흐름은 웹 응용 프로그램과 동일
  - 개발자: (계약)코드 작성 → 블록체인에 배포 (웹에서는 웹 서버에 배포)
  - 사용자: 브라우저를 통해 서버에 접근하고, 목적한 일을 수행함
- 스마트 계약의 목적
  - 기존의 법률적 계약보다 우수한 보안성을 제공
  - 기존의 계약보다 저렴한 처리 비용을 제공
- 실용적인 측면
  - 에스크로(escrow)에 자산을 보유하고 계약 기간이 만료될 때 이를 이동시킬 수 있는 권한이 부여됨 *escrow: 결제 대금 예치 서비스

스마트 계약 동작과정

◆ 계약 개발 및 배포 = 바이트코드의 블록 내 저장



◆ 계약 접근(실행)



스마트 계약 작성 (1/3)

◆ 상태 변경과 데이터 저장이 가능한 튜링 완전한 고급 언어로 계약을 작성함
- Solidity: 자바스크립트와 문법이 유사하며 가장 광범위하게 사용됨
  - http://solidity.readthedocs.io/en/develop/index.html
- Serpent: 파이썬과 문법이 유사함
- LLL: 어셈블리와 유사한 저수준 언어 (Low Level OPCODE)
- Mutan: C와 유사하나 더 이상 사용하지 않음

◆ 튜링완전언어: 모든 수학문제를 풀 수 있는 일반적인 알고리즘을 만들어낼 수 있는 컴퓨터언어
- 조건 1) 프로세스를 충분히 분할할 수 있을 만큼 작은 단위를 사용할 수 있어야 한다.
- 조건 2) 조건설정과 반복 명령어가 있어야 한다.
- cf.) 비트코인의 스크립트 언어는 조건설정 만을 지원함

◆ 블록체인내에 상태 정보로 존재하고 EVM 노드에서 작동되어 이더리움의 상태 전이를 유발함

스마트 계약 작성 (2/3)

◆ 스마트 계약 컴파일

```
1  pragma solidity ^0.4.0;
2
3  contract MyContract {
4      uint i = (10 + 2) * 2;
5  }
```

```
01010110111001111110
01011110101111000010
1100101010100101.....
.....
```

◆ 함수와 시그너처

```
1  contract Calculator {
2    function sumAndReturn(int a, int b) returns (int) {
3      sum = a + b;
4      return sum;
5    }
6  }
```

파라미터와 반환값의 형태를 합쳐서 함수의 시그니처(특징)라고 얘기한다.

: sumAndReturn 함수의 시그니처는 (int, int) returns (int)

스마트 계약 작성 (3/3)

◆ 스마트 계약 구성

항목	설명
version pragma	• Solidity 컴파일러 버전의 호환성을 지정함
state variable	• 계약에 저장할 상태 변수들을 선언함
constructor	• 계약의 생성자. 계약이 생성될 때 딱 1번 실행됨.
function	• EOA나 계약, 계약 내부에서 호출할 수 있는 함수를 정의함
function modifier	• 반복적으로 사용되는 조건을 정의함

```
pragma solidity ^0.4.0;                                          ← verision pragma

contract MyToken {
   address public creator;
   uint256 public totalSupply;
   mapping (address => uint256) public balances;                 ← state variables

   function MyToken() public {                                   ← constructor
      creator = msg.sender;
      totalSupply = 10000;
      balances[creator] = totalSupply;
   }

   function balanceOf(address owner) public constant returns(uint256){   ← function
      return balances[owner];
   }
            ...
}
```


스마트 계약 개발 도구

◆ 기본 도구

- Mist & Browser-Solidity – 이더 전송, 계약 배포, 개발이 가능
- Geth & Eth – 이더리움 네트워크 구성, 관리 및 운영, 개발을 위한 라인 인터페이스
- Remix IDE – Web based Solidity IDE
- web3.js – Ethereum Compatible JavaScript API

◆ 선택적 도구

- 자바스크립트 testRPC – 이더리움 풀노드를 애뮬레이션
- Solc – solidity컴파일러
- Parity – 이더리움 클라이언트 & 지갑
- Tupple – 이더리움 개발 및 테스팅 프레임워크
- Embark, OpenZeppelin – 안전하고 재사용 가능한 솔리디티 스마트 계약 프레임워크
- Metamask – 크롬 브라우저 확장

개발 환경 구축

- Geth 구동 환경 구축
- 이더리움 기본 동작 실습
- 스마트 계약

Geth 구동 환경 구축

◆ OS별 Geth 클라이언트 설치

- https://geth.ethereum.org/downloads/ 에 접속 후, 운영체제에 맞게 Geth 클라이언트 프로그램 다운

- **윈도우**
  - Geth 클라이언트 프로그램 파일(exe) 실행 후 설치

- **리눅스**
  - 다운받은 Geth 클라이언트 실행 프로그램을 설치 없이 다운 받은 위치에서 구동

Geth 구동 환경 구축

◆ 테스트 네트워크에서 Geth 구동

1. 아래의 명령어를 참고하여 초기화된 Geth를 실행한다.

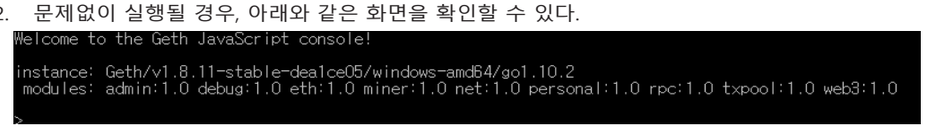
```
geth --networkid 4649 --nodiscover --maxpeers 0 --datadir "C:\Program Files\Geth\data_testnet" console 2>>
"C:\Program Files\Geth\data_testnet\geth.log"
```

데이터 디렉터리 경로

❖ 각 옵션이 의미하는 내용

옵션	의미
--networked 4649	네트워크 식별자, 0~3은 예약된 숫자이므로 그 밖의 정수인 4649를 지정하였다.
--nodiscover	생성자의 노드를 다른 노드에서 검색할 수 없게 하는 옵션이다. 노드 추가를 수동으로 해야한다.
--maxpeers 0	생성자의 노드에 연결할 수 있는 노드의 수를 지정한다. 0을 지정하였으므로 다른 노드와 연결하지 않는다.
console	대화형 자바스크립트 콘솔을 기동한다.
2>> "데이터 디렉터리 경로₩geth.log"	로그 파일을 만들 때 사용할 옵션으로, 에러를 geth.log 파일에 저장한다.

2. 문제없이 실행될 경우, 아래와 같은 화면을 확인할 수 있다.



이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (1/8)

- 이더리움에는 **EOA(Externally Owned Account) 계정**과 **Contract 계정**이 존재한다.

  EOA : 일반 사용자가 사용하는 계정으로 비밀키에 의해 관리된다. 주로, Ether를 송금하거나 계약을 실행한다.
  Contract : 계약을 배포할 때 만들어지는 계정으로 블록체인에 존재한다. 다른 계정으로부터 수신한 메시지를 이용해 코드를 실행한다.

- Geth 콘솔에서 personal.newAccount 명령을 이용하여 EOA를 생성할 수 있다.

```
> personal.newAccount("pass0")
"0xf7abe3614faaaf0732a3ffc737964683b2b4b387"
```

"pass0"는 사용자 지정 패스워드이며, 40바이트의 계정 주소가 생성된다.

- eth.accounts 명령을 이용하여 해당 노드가 관리하고 있는 계정의 주소를 확인할 수 있다.

```
> eth.accounts
["0xf7abe3614faaaf0732a3ffc737964683b2b4b387"]

> personal.newAccount("pass1")
"0xbd014aaf96216f62b59c1544013f8aad73fd0545"

> eth.accounts
["0xf7abe3614faaaf0732a3ffc737964683b2b4b387", "0xbd014aaf96216f62b59c1544013f8aad73fd0545"]
```


이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (2/8)

- 아래와 같이 인덱스 형태로 지정해 각 계정을 확인할 수 있다.

```
> eth.accounts[0]
["0xf7abe3614faaaf0732a3ffc737964683b2b4b387"]
> eth.accounts[1]
["0xbd014aaf96216f62b59c1544013f8aad73fd0545"]
```

- 콘솔이 아닌, 셸에서 geth 명령으로 계정을 만들거나 확인할 수 있다.

데이터 디렉터리 경로

```
C:\Program Files\Geth > geth --datadir "C:\Program Files\Geth\data_testnet" account new
INFO [06-19|19:09:41] Maximum peer count                       ETH=25 LES=0 total=25
Your new account is locked with a password. Please give a password. Do not forget this password.
Passphrase: (패스워드 입력)
Repeat passphrase: (패스워드 입력)
Address: {80b615b785ec07494ead4f24a442b2eee73f6922}
```

생성된 계정 주소

```
C:\Program Files\Geth > geth --datadir "C:\Program Files\Geth\data_testnet" account list
INFO [06-19|19:10:08] Maximum peer count                       ETH=25 LES=0 total=25
Account #0: {f7abe3614faaaf0732a3ffc737964683b2b4b387} keystore://C:\Program Files\Geth\data_testnet\keystore\UTC--2018-06-19T08-13-25.805849700Z--f7abe3614faaaf0732a3ffc737964683b2b4b387
Account #1: {bd014aaf96216f62b59c1544013f8aad73fd0545} keystore://C:\Program Files\Geth\data_testnet\keystore\UTC--2018-06-19T08-28-22.438524500Z--bd014aaf96216f62b59c1544013f8aad73fd0545
Account #2: {80b615b785ec07494ead4f24a442b2eee73f6922} keystore://C:\Program Files\Geth\data_testnet\keystore\UTC--2018-06-19T10-09-47.581175400Z--80b615b785ec07494ead4f24a442b2eee73f6922
```

이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (3/8)

- 이전과 동일한 옵션을 사용하여 Geth를 시작한다.

```
geth --networkid 4649 --nodiscover --maxpeers 0 --datadir "C:\Program Files\Geth\data_testnet" console 2>>
"C:\Program Files\Geth\data_testnet\geth.log"
```

데이터 디렉터리 경로

- 이더리움에서 채굴에 성공했을 때 보상받을 계정을 Etherbase라고 한다. 일반적으로 eth.account[0]가 Etherbase의 디폴트값이다.

```
> eth.accounts                                    0번째 인덱스
["0xf7abe3614faaaf0732a3ffc737964683b2b4b387", "0xbd014aaf96216f62b59c1544013f8aad73fd0545",
"0x80b615b785ec07494ead4f24a442b2eee73f6922"]

> eth.coinbase
"0xf7abe3614faaaf0732a3ffc737964683b2b4b387"
```


이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (4/8)

- Etherbase는 miner.setEtherbase 명령으로 변경할 수 있다.
  (이후 과정은 Etherbase가 eth.accounts[0]인 상태로 진행)

```
> eth.accounts                                    1번째 인덱스
["0xf7abe3614faaaf0732a3ffc737964683b2b4b387", "0xbd014aaf96216f62b59c1544013f8aad73fd0545",
"0x80b615b785ec07494ead4f24a442b2eee73f6922"]

> miner.setEtherbase(eth.accounts[1])
true

> eth.coinbase
"0xbd014aaf96216f62b59c1544013f8aad73fd0545"

> miner.setEtherbase(eth.accounts[0])

true
> eth.coinbase
"0xf7abe3614faaaf0732a3ffc737964683b2b4b387"
```


이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (5/8)

- eth.getBalance 명령으로 계정의 잔고를 확인할 수 있다. 이 때, 인수는 계정의 주소이다.

```
> eth.getBalance(eth.accounts[0])
0
> eth.getBalance(eth.accounts[1])
0
> eth.getBalance(eth.accounts[2])
0
> eth.getBalance("0xf7abe3614faaaf0732a3ffc737964683b2b4b387")
0
```

- eth.blockNumber 명령으로 블록체인에 연결된 블록의 개수를 확인할 수 있다.

```
> eth.blockNumber      아직 채굴을 시작하지 않았기 때문에 블록 개수가 0이다.
0
```

- miner.start(thread_num) 명령으로 채굴을 시작할 수 있다. 이 때, thread_num은 채굴에 사용할 스레드 개수이다.

```
> miner.start(1)
null
```


이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (6/8)

- eth.mining : 채굴이 진행되고 있다면 True, 진행되고 있지 않다면 False 출력한다.
- eth.hashrate : 채굴하는 데 사용하는 연산력을 나타내는 해시 속도를 출력한다.
- miner.stop() : 채굴을 중지하는 명령이다.

```
> eth.mining
true          채굴 중이기 때문에 True가 출력됨
> eth.hashrate
1087190
> eth.blockNumber
0
> eth.blockNumber
6
> eth.blockNumber
11
> miner.stop()
true          채굴을 중지함
> eth.mining
false         채굴 중이 아니기 때문에 False가 출력됨
```

이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (7/8)

- 채굴 보상을 받는 계정인 eth.account[0]의 잔고를 확인한다.

```
> eth.getBalance(eth.accounts[0])
85000000000000000000
> eth.getBalance(eth.coinbase)
85000000000000000000
```

출력되는 값은 이더리움에서의 최소 단위인 wei 단위이다.

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

- **85,000,000,000,000,000,000wei를 ether 단위로 환산하면?**

이더리움 기본 동작 실습

◆ 계정 생성과 채굴 (8/8)

- 아래와 같은 명령을 사용하여 ether 단위로 환산한 값을 출력할 수 있다.

```
> web3.fromWei(eth.getBalance(eth.accounts[0]), "ether")
85
```


이더리움 기본 동작 실습

◆ Ether 송금 (1/6)

- sendTransaction 명령으로 eth.accounts[0]에서 eth.account[1]로 20ether를 송금한다.

```
> eth.sendTransaction({from:eth.accounts[0], to:eth.accounts[1], value:web3.toWei(20,"ether")})
Error: authentication needed: password or unlock
    at web3.js:3143:20
    at web3.js:6347:15
    at web3.js:5081:36
    at <anonymous>:1:1
```

- 이더리움에서는 잘못된 실행 방지를 위해 항상 계정을 잠금 상태로 유지한다.
  따라서, personal.unlockAccount 명령으로 계정 잠금을 해제해야 한다.

```
> personal.unlockAccount(eth.accounts[0], "pass0", 0)
true
```

인수는 각각 잠금 해제할 계정, 비밀번호, 잠금 해제 유효 시간(초단위) 이다.
잠금 해제 유효 시간 인수는 기본적으로 300초이며, 0을 입력하면 Geth 프로세스가 종료되기 전까지 잠금해제가 유지된다.

이더리움 기본 동작 실습

◆ Ether 송금 (2/6)

- sendTransaction 명령으로 eth.accounts[0]에서 eth.account[1]로 20ether를 다시 송금한다.

```
> eth.sendTransaction({from:eth.accounts[0], to:eth.accounts[1], value:web3.toWei(20,"ether")})
"0x117da0529843cde4b5b19c7d45158febf435fc441878736df90dffb614f40652"
> eth.getBalance(eth.accounts[0])
85000000000000000000
> eth.getBalance(eth.accounts[1])
0
```

트랜잭션 ID 값

- sendTransaction 명령을 수행했으나 eth.account[1]의 잔고가 0 wei임을 확인할 수 있다.

이더리움 기본 동작 실습

◆ Ether 송금 (3/6)

- eth.getTransaction 명령으로 트랜잭션 상태를 확인할 수 있다.

```
> eth.getTransaction("0x117da0529843cde4b5b19c7d45158febf435fc441878736df90dffb614f40652")   트랜잭션 ID 값

{
  blockHash: "0x0000000000000000000000000000000000000000000000000000000000000000",
  blockNumber: null,  트랜잭션이 어떠한 블록에도 포함되지 않았다.
  from: "0xf7abe3614faaaf0732a3ffc737964683b2b4b387",  보내는 주소 (eth.accounts[0])
  gas: 90000,
  gasPrice: 18000000000,
  hash: "0x117da0529843cde4b5b19c7d45158febf435fc441878736df90dffb614f40652",
  input: "0x",
  nonce: 0,
  r: "0x3f52594d2ddc63f0e563bb9ceeed5751c5949953aed282d15498048894e0351c",
  s: "0x66d827dd418810839fa345ad8c2dd6b00aad2f0ea3cd756d972d45c85aef7b13",
  to: "0xbd014aaf96216f62b59c1544013f8aad73fd0545",   받는 주소 (eth.accounts[1])
  transactionIndex: 0,
  v: "0x18ae",
  value: 20000000000000000000
}
```

23

이더리움 기본 동작 실습

◆ Ether 송금 (4/6)

- 미처리된 트랜잭션을 처리하기 위해 채굴을 시작하여 블록을 생성한다.

```
> miner.start(1)
null
```

- 다시 eth.getTransaction 명령으로 트랜잭션 상태를 확인한다.

```
> eth.getTransaction("0x117da0529843cde4b5b19c7d45158febf435fc441878736df90dffb614f40652")   트랜잭션 ID 값

{
  blockHash: "0xbd5ff484d255d78540d60f82f1a95e7ce414d3d7d4f6b207c7e2a04eeabea42d",  18번째 블록의 해시값
  blockNumber: 18,   트랜잭션이 18번째 블록에 포함되었다.
  from: "0xf7abe3614faaaf0732a3ffc737964683b2b4b387",  보내는 주소 (eth.accounts[0])
  gas: 90000,
  gasPrice: 18000000000,
  hash: "0x117da0529843cde4b5b19c7d45158febf435fc441878736df90dffb614f40652",
  input: "0x",
  nonce: 0,
  r: "0x3f52594d2ddc63f0e563bb9ceeed5751c5949953aed282d15498048894e0351c",
  s: "0x66d827dd418810839fa345ad8c2dd6b00aad2f0ea3cd756d972d45c85aef7b13",
  to: "0xbd014aaf96216f62b59c1544013f8aad73fd0545",   받는 주소 (eth.accounts[1])
  transactionIndex: 0,
  v: "0x18ae",
  value: 20000000000000000000
}
```

24

이더리움 기본 동작 실습

◆ Ether 송금 (5/6)

- 미처리된 트랜잭션을 처리하기 위해 채굴을 시작하여 블록을 생성한다.

```
> eth.getBlock(18)
{
  difficulty: 131072,
  extraData: "0xda8301080b846765746888676f312e31302e328777696e646f7773",
  gasLimit: 131877941,
  gasUsed: 21000,
  hash: "0xbd5ff484d255d78540d60f82f1a95e7ce414d3d7d4f6b207c7e2a04eeabea42d",
  logsBloom:
"0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",
  miner: "0xf7abe3614faaaf0732a3ffc737964683b2b4b387",
  mixHash: "0xa0399563ed0368919321f408603efb368ba59376b577a97156c02961955689cd",
  nonce: "0x1ac2c567aad218b4",
  number: 18,
  parentHash: "0x2b6544a6fcf464c4b9a00db9e3b0c88821f4e046aefc5b8f758f13b0b1aaa85a",
  receiptsRoot: "0xefb734962f223d68c51454edaf554d5d1ccdab9d535e10e156c59f45c386ddcd",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  size: 656,
  stateRoot: "0xef757db5954bd793d7b52c12fd449e40a8e7486bab96476cfa364ad56dc86397",
  timestamp: 1529410024,
  totalDifficulty: 2382848,
  transactions: ["0x117da0529843cde4b5b19c7d45158febf435fc441878736df90dffb614f40652"],
  transactionsRoot: "0x7052f560fa131e1ce77c4d6458e225054f08ed936faab9061fddeaf16fbcf730",
  uncles: []
}
```

25

이더리움 기본 동작 실습

◆ Ether 송금 (6/6)

- 트랜잭션이 블록에 포함된 것을 확인한 다음, eth.accounts[1]의 잔고를 확인하면 송금이 완료된 것을 확인할 수 있다.

```
> eth.getBalance(eth.accounts[1])
20000000000000000000
> web3.fromWei(eth.getBalance(eth.accounts[1]), "ether")
20
```

- eth.pendingTransactions 명령을 사용하여 현재 처리되지 않은 트랜잭션 내용들을 확인할 수 있다.

```
> eth.pendingTransactions
[]
```

26

이더리움 기본 동작 실습

◆ 거래 수수료 (1/2)

- eth.accounts[1]의 잠금을 해제하고, eth.accounts[1]에서 eth.accounts[2]로 송금을 한다.

```
> personal.unlockAccount(eth.accounts[1], "pass1", 0)
true
> eth.sendTransaction({from:eth.accounts[1], to:eth.accounts[0], value:web3.toWei(10,"ether")})
"0xc857b28f7a855f0632dc0e5ab7cf135ce340639616d72f1ea316bfb7b51b9843"
> miner.start(1)
null
> eth.pendingTransactions
[]
> miner.stop()
true
```

- eth.account[1]과 eth.account[2]의 잔고를 확인한다.

```
> eth.getBalance(eth.accounts[2])
10000000000000000000
> web3.fromWei(eth.getBalance(eth.accounts[2]), "ether")
10                                                    eth.accounts[1]이 보낸 10ether
> eth.getBalance(eth.accounts[1])
9999622000000000000
> web3.fromWei(eth.getBalance(eth.accounts[1]), "ether")
9.999622                                              기존 잔고 20ether에서 10ether를 송금했는데 잔고가 10ether보다 작다.
```


이더리움 기본 동작 실습

◆ 거래 수수료 (2/2)

- 채굴을 했던 eth.accounts[0]의 잔고를 확인하면 eth.accounts[1]에서 줄어든 0.000378ether가 eth.accounts[0]에게 전달되었음을 확인할 수 있다.

```
> eth.getBalance(eth.accounts[0])
135000378000000000000
> web3.fromWei(eth.getBalance(eth.accounts[0]), "ether")
135.000378
```

- 이 때, 0.000378ether는 트랜잭션을 처리하기 위한 수수료(Gas)이며, 블록 채굴자(eth.accounts[0])에게 지불되었다.

참고 문헌

- 아카하네 요시하루 외 1인, “블록체인 구조와 이론 ,” 위키북스
- 박제현 외 2인, “코어 이더리움 프로그래밍,” 제이펍
- 와타나베 이츠시 외 3인, “블록체인 애플리케이션 개발 실전 입문,” 위키북스
- 이더리움 가상 머신, https://res.cloudinary.com/hzpbl0kap/image/upload/v1521022316/03-EVM.pdf
- 윌리엄 무가야, 비즈니스 블록체인, 한빛미디어

Ethereum 네트워크 구축 및 Smart Contract 구현 실습
- 대한전자공학회 블록체인 워크샵

Smart Contract 구현 실습

2019.06.17

부산대학교 최윤호교수

PUSAN NATIONAL UNIVERSITY
SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Software & System Security Laboratory

개요

I Browser-Solidity를 활용한 계약 개발 ▸▸

II 스마트 작성, 실행 및 배포 ▸▸

Browser-Solidity를 활용한 계약 개발

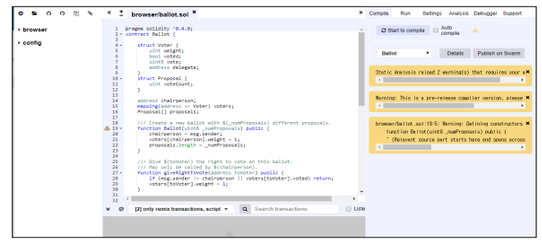
- Browser-Solidity 소개
- Browser-Solidity를 통한 계약 생성 및 배포

Browser-Solidity를 활용한 계약 개발

Software & System Security Laboratory

◆ Browser-Solidity 소개

- Browser-Solidity는 웹 브라우저 기반의 Solidity 언어 전용 통합 개발 환경이다.
- 웹 브라우저에서 계약 코드 작성, 컴파일, 배포, 계약 메서드 실행이 가능하다.
- Browser-Solidity는 두가지 방법으로 이용할 수 있다.
  1. http://remix.ethereum.org 에 접속하여 온라인으로 사용하는 방법
  2. 깃허브(https://github.com/ethereum/remix-ide)를 통해 설치 후, 오프라인으로 사용하는 방법



Browser-Solidity를 활용한 계약 개발

◆ Browser-Solidity와 Geth 연결 (JSON-RPC)

- HTTP-RPC 서버를 활성화하여 Browser-Solidity와 Geth가 연동되도록 JSON-RPC 옵션으로 구동한다.

```
C:\Program Files\Geth>geth --networkid 4649 --nodiscover --maxpeers 0 --datadir "C:\Program Files\Geth\data_testnet"
--rpc --rpcaddr "0.0.0.0" --rpcport 8545 --rpccorsdomain "*" --rpcapi
"admin,db,eth,debug,miner,net,shh,txpool,personal,web3" console 2>> "C:\Program Files\Geth\data_testnet\geth.log"
```

사용자에 맞게 수정

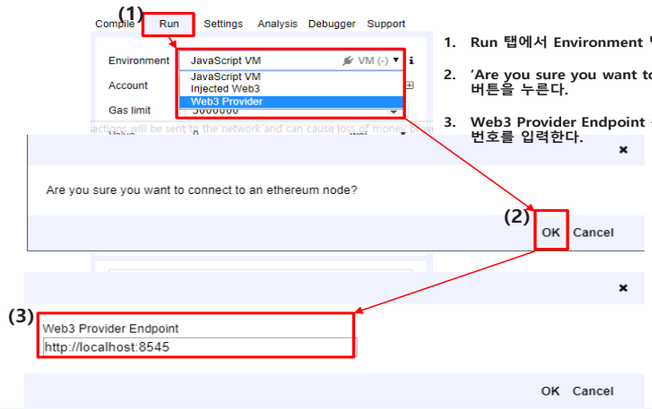
❖ 각 옵션이 의미하는 내용

옵션	의미
--rpc	HTTP-RPC 서버를 활성화한다.
--rpcaddr "0.0.0.0"	HTTP-RPC 서버의 수신 IP주소를 지정한다. 기본값은 "localhost"이고 "0.0.0.0"은 어떤 인터페이스에서의 접근도 수신한다는 것을 의미한다.
--rpcport 8545	활성화한 HTTP-RPC 서버가 사용하는 포트를 지정한다.
--rpccorsdomain "*"	자신의 노드에 RPC로 접속을 허가할 IP주소를 지정한다. "*"는 모든 IP를 의미한다.
--rpcapi "admin,db,eth,debug,miner,net,shh,txpool,personal,web3"	RPC를 허가할 명령을 지정한다. 기본값은 "eth, net, web3"이다.

Browser-Solidity를 활용한 계약 개발

◆ Browser-Solidity 설정

- Browser-Solidity를 통해 현재 구동 중인 이더리움 노드에 접속하기 위해 아래의 동작을 수행한다.

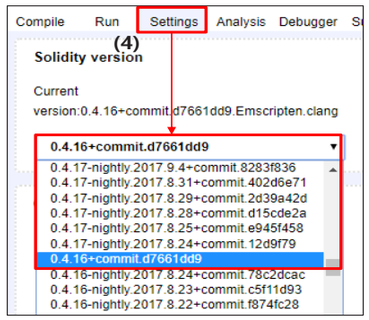


1. Run 탭에서 Environment 박스에서 Web3 Provider를 선택한다.
2. 'Are you sure you want to connect to an Ethereum node?' 알림에 확인 버튼을 누른다.
3. Web3 Provider Endpoint 주소에 Geth를 실행 중인 IP주소와 지정한 포트 번호를 입력한다.

Browser-Solidity를 활용한 계약 개발

◆ Browser-Solidity 설정

- 이후 실습 코드와의 호환을 위해 Browser-Solidity의 Solidity 컴파일러 버전을 변경한다.



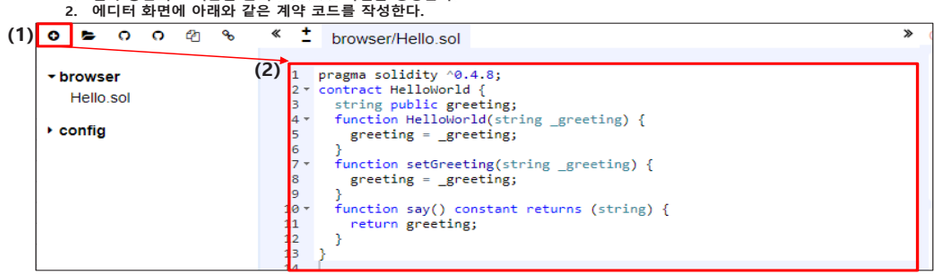
4. Settings 탭에서 Solidity version 박스에서 컴파일러 버전을 0.4.16+commit.d7661dd9 버전으로 변경한다.

Browser-Solidity를 활용한 계약 개발

◆ Browser-Solidity에서 계약 생성

- Browser-Solidity에서 Hello World를 출력하는 계약 생성

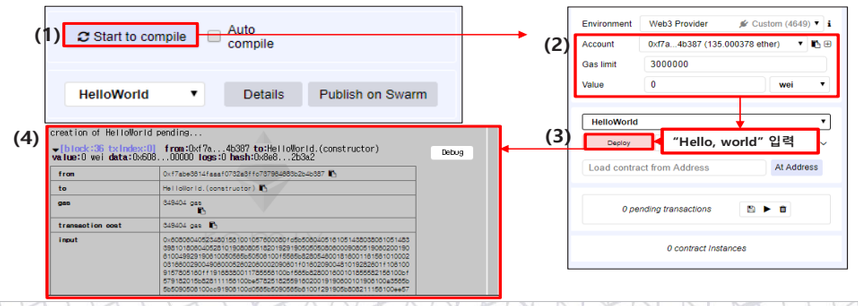
1. 왼쪽 상단의 + 버튼을 눌러 Hello.sol 파일을 생성한다.
2. 에디터 화면에 아래와 같은 계약 코드를 작성한다.



Browser-Solidity를 활용한 계약 개발

◆ Browser-Solidity에서 계약 배포

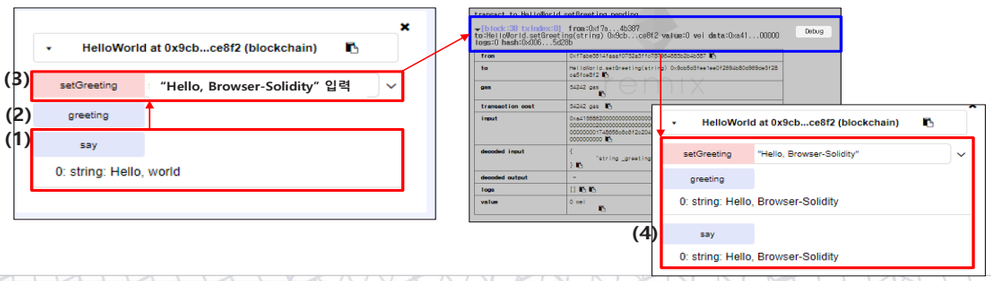
1. Compile 탭에서 Start to compile 버튼을 클릭하여 컴파일을 수행한다.
2. 계약을 배포하는 계정(현재는 eth.accounts[0])과 Gas limit를 설정한다.
   (단, 이 때 배포하는 계정은 잠금 해제된 상태여야 한다.)
3. Deploy 버튼 옆의 빈칸에 "Hello, world"를 입력하고 Deploy 버튼을 클릭한다.
   ("Hello, world"가 생성자에 들어가는 인수이다.)
4. 새롭게 채굴된 블록에 계약을 배포하는 거래가 포함된다.
   (계약의 주소와 계약의 메서드를 확인할 수 있다.)



Browser-Solidity를 활용한 계약 개발

◆ Browser-Solidity에서 배포한 계약의 동작 확인

1. say 버튼을 클릭하여 say 메서드를 동작시키면 생성자의 인수로 입력하였던 "Hello, world"가 출력된다.
2. greeting 버튼을 클릭하면 greeting 변수의 현재 값을 알 수 있다.
3. greeting 변수 값을 변경하는 setGreeting 메서드를 동작시키기 위해, 빈칸에 "Hello, Browser-Solidity"를 입력하고 setGreeting 버튼을 클릭한다.
   (이 메서드의 호출으로 계약의 state가 바뀌기 때문에 거래가 발생한다. 이 거래는 새로 채굴되는 블록에 포함된다.)
4. say 메서드를 다시 동작시키면 "Hello, Browser-Solidity"가 출력되는 것을 확인할 수 있다.



Browser-Solidity를 활용한 계약 개발

◆ Browser-Solidity를 활용하여 기존 계약에 접근

1. 실습의 편의를 위해, 이전 단계에서 배포했던 계약의 주소를 복사하고, X 버튼을 클릭한다.
2. 복사한 계약의 주소를 "Load contract from Address"가 적힌 빈칸에 붙여넣고 "At Address" 버튼을 클릭한다.
3. 이전 단계에서 배포하고, greeting 변수 값을 "Hello, Browser-Solidity"로 변경하였던 계약이 다시 호출된다.
   (greeting, say 버튼을 클릭하면 "Hello, Browser-Solidity"가 출력된다.)

스마트 계약 실행 및 배포

- 가상 화폐 계약
- 블랙리스트 기능 추가

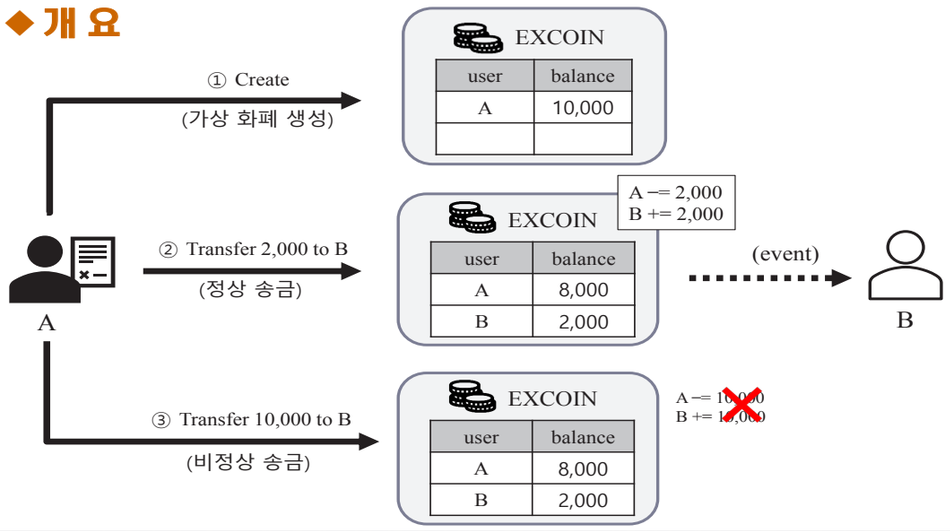
가상 화폐 계약

◆ 개 요

- **토큰(token)**이란 비트코인이나 Ether처럼 특정 계정에 연결되어 관리된다.
- 또한, 임의의 계정에 임의의 양을 전달할 수 있는 화폐보다 추상적인 개념이다.
- 가상화폐 계약 작성을 통해 토큰을 작성하고 배포한다.

가상 화폐 계약

◆ 개 요



가상 화폐 계약

◆ 계약 작성

```
1  pragma solidity ^0.4.8;
2
3  contract OreOreCoin {
4      string public name;
5      string public symbol;
6      uint8 public decimals;
7      uint256 public totalSupply;
8      mapping (address => uint256) public balanceOf;
9
10     event Transfer(address indexed from, address indexed to, uint256 value);
11
12     function OreOreCoin(uint256 _supply, string _name, string _symbol, uint8 _decimals) {
13         balanceOf[msg.sender] = [          ];
14         name = [      ];
15         symbol = [          ];
16         decimals = [              ];
17         totalSupply = [          ];
18     }
19
20     function transfer(address _to, uint256 _value) {
21         if (balanceOf[msg.sender] < [      ]) throw;
22         if (balanceOf[_to] + _value < balanceOf[_to]) throw;
23         balanceOf[msg.sender] -= [      ];
24         balanceOf[_to] += [      ];
25         Transfer(msg.sender, _to, _value);
26     }
27 }
```

(1) 상태 변수 선언
- **line 4 : 토큰 이름**
- **line 5 : 토큰 단위**
- **line 6 : 소수점 이하 자리수**
- **line 7 : 토큰 총량**
- **line 8 : 각 주소의 잔고**

가상 화폐 계약

◆ 계약 작성

```
1  pragma solidity ^0.4.8;
2
3  contract OreOreCoin {
4      string public name;
5      string public symbol;
6
7
8
9
10     event Transfer(address indexed from, address indexed to, uint256 value);
11
12     function OreOreCoin(uint256 _supply, string _name, string _symbol, uint8 _decimals) {
13         balanceOf[msg.sender] = [          ];
14         name = [      ];
15         symbol = [          ];
16         decimals = [              ];
17         totalSupply = [          ];
18     }
19
20     function transfer(address _to, uint256 _value) {
21         if (balanceOf[msg.sender] < [      ]) throw;
22         if (balanceOf[_to] + _value < balanceOf[_to]) throw;
23         balanceOf[msg.sender] -= [      ];
24         balanceOf[_to] += [      ];
25         Transfer(msg.sender, _to, _value);
26     }
27 }
```

(2) 이벤트 알림
- **event는 거래의 로그를 출력하는 기능이다.**

가상 화폐 계약

◆ 계약 작성

```
1  pragma solidity ^0.4.8;
2
3  contract OreOreCoin {
4      string public name;
5
6
7
8
9
10
11
12     function OreOreCoin(uint256 _supply, string _name, string _symbol, uint8 _decimals) {
13         balanceOf[msg.sender] = _____;
14         name = _____;
15         symbol = _____;
16         decimals = _____;
17         totalSupply = _____;
18     }
19
20     function transfer(address _to, uint256 _value) {
21         if (balanceOf[msg.sender] < _____) throw;
22         if (balanceOf[_to] + _value < balanceOf[_to]) throw;
23         balanceOf[msg.sender] -= _____;
24         balanceOf[_to] += _____;
25         Transfer(msg.sender, _to, _value);
26     }
27 }
```

(3) 생성자 , line 12-18
- 계약이 배포될 때 실행되는 함수이다.
- 인수로 받은 값들을 계약의 상태 변수로 설정한다.
- 현재는 계약 생성 시 계약 생성자가 모든 토큰을 가지고 있다.

가상 화폐 계약

◆ 계약 작성

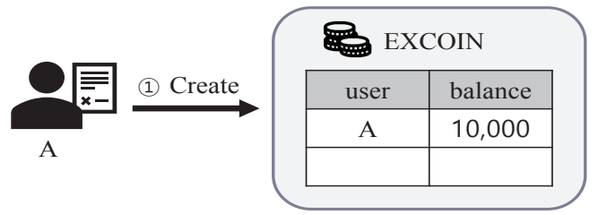
```
1  pragma solidity ^0.4.8;
2
3  contract OreOreCoin {
4      string public name;
5      string public symbol;
6      uint8 public decimals;
7      uint256 public totalSupply;
8      mapping (address => uint256) public balanceOf;
9
10
11
12                                                          {
13
14
15
16
17
18
19
20     function transfer(address _to, uint256 _value) {
21         if (balanceOf[msg.sender] < _____) throw;
22         if (balanceOf[_to] + _value < balanceOf[_to]) throw;
23         balanceOf[msg.sender] -= _____;
24         balanceOf[_to] += _____;
25         Transfer(msg.sender, _to, _value);
26     }
27 }
```

(4) 송금 함수
- 송금받을 주소(_to)와 금액(_value)를 인수로 받는다.
- line 21 : 송금하는 주소에 송금액만큼 잔고가 없는 경우 예외처리
- line 22 : 송금으로 인한 오버플로우가 없는지 확인하는 예외처리
- line 23-24 : 송금하는 주소와 송금받는 주소에 대한 잔고 갱신
- line 25 : 송금 처리에 대한 이벤트 호출(로그 출력)

가상 화폐 계약

◆ 계약 생성

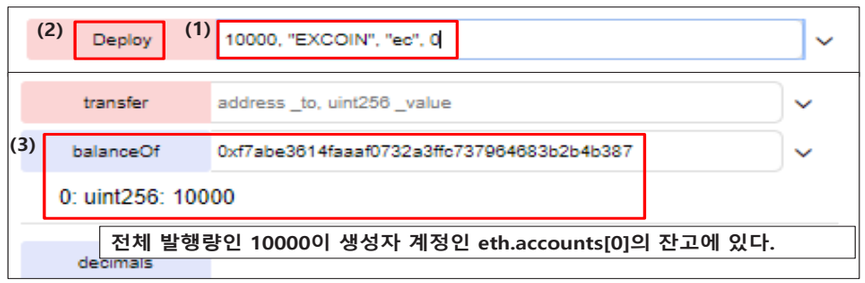
- A(eth.accounts[0])에 의해 전체 발행량이 10,000인 상태로 계약을 생성한다.



가상 화폐 계약

◆ 계약 생성

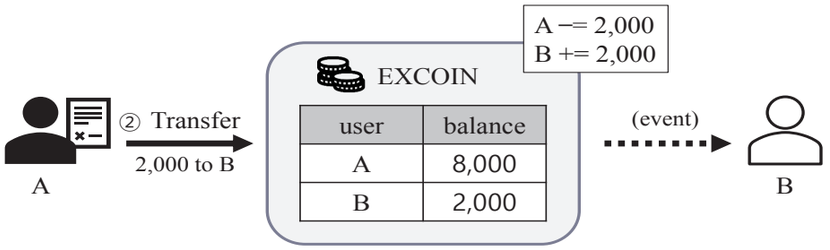
1. eth.accounts[0]이 토큰을 만든다. Browser-Solidity에서 Run 탭의 "Deploy" 버튼 옆의 빈칸에 10000, "EXCOIN", "ec", 0을 입력한다.
2. "Deploy" 버튼을 클릭하여 계약을 배포한다.
3. eth.accounts[0]의 주소를 "balanceOf" 버튼 옆의 빈칸에 붙여넣고, "balanceOf" 버튼을 클릭한다.



가상 화폐 계약

◆ 정상 송금

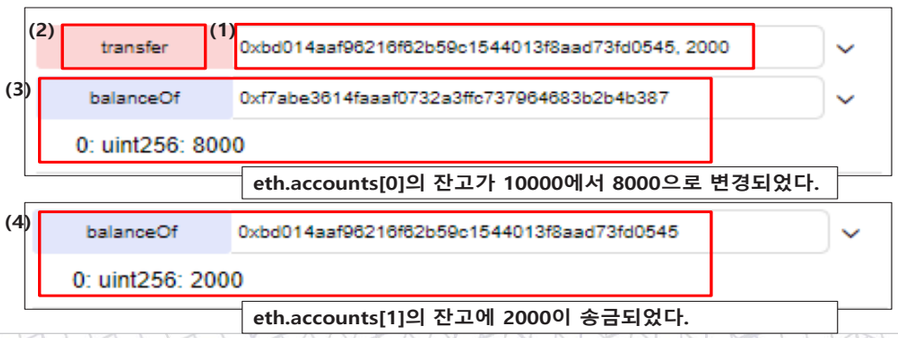
- A(eth.accounts[0])가 B(eth.accounts[1])에게 송금(2000)한다.



가상 화폐 계약

◆ 정상 송금

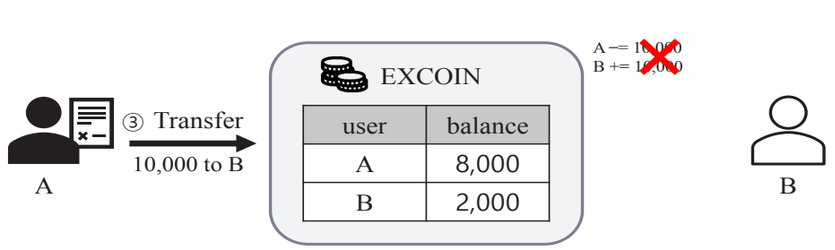
1. Browser-Solidity에서 Run 탭의 "transfer" 버튼 옆의 빈칸에 송금할 주소, 송금액을 입력한다.
2. "transfer" 버튼을 클릭하여 송금한다.
3. eth.accounts[0]의 주소를 "balanceOf" 버튼 옆의 빈칸에 붙여넣고, "balanceOf" 버튼을 클릭한다.
4. eth.accounts[1]의 주소를 "balanceOf" 버튼 옆의 빈칸에 붙여넣고, "balanceOf" 버튼을 클릭한다.



가상 화폐 계약

◆ 비정상 송금

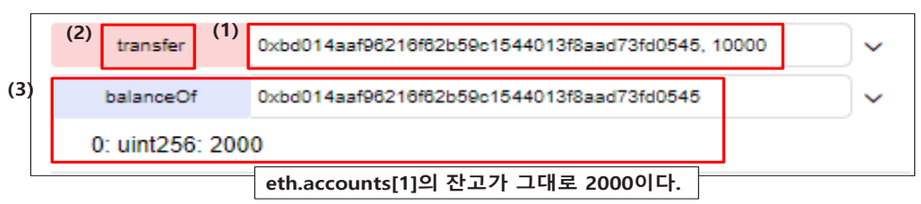
- A(eth.accounts[0])가 B(eth.accounts[1])에게 자신의 잔고(8000)보다 큰 금액(10000)을 송금한다.
- 이 경우 잔고가 부족하기 때문에 예외가 발생하며 잔고는 변경되지 않는다.



가상 화폐 계약

◆ 비정상 송금

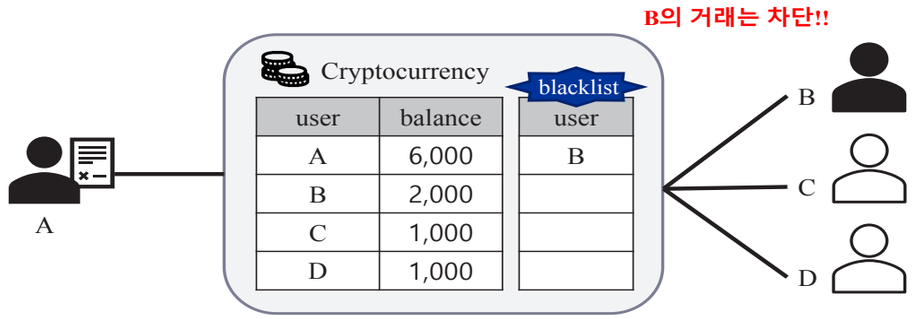
1. Browser-Solidity에서 Run 탭의 "transfer" 버튼 옆의 빈칸에 송금할 주소, 송금액을 입력한다.
2. "transfer" 버튼을 클릭하여 송금한다.
3. eth.accounts[1]의 주소를 "balanceOf" 버튼 옆의 빈칸에 붙여넣고, "balanceOf" 버튼을 클릭한다.



가상 화폐 계약 – 블랙리스트

◆ 개 요

- 앞에서 만든 가상 화폐 계약에 대해 '블랙리스트'에 기록된 사용자의 거래를 차단하는 기능을 추가한다.
- 단, 계약 생성자만이 블랙리스트를 관리할 수 있도록 구현한다.



가상 화폐 계약 – 블랙리스트

◆ 계약 작성

```
1  pragma solidity ^0.4.8;
2
3  contract OreOreCoin {
4      string public name;
5      string public symbol;
6      uint8 public decimals;
7      uint256 public totalSupply;
8      mapping (address => uint256) public balanceOf;
9      mapping (address => int8) public blackList;
10     address public owner;
11
12     modifier onlyOwner() { if (                    ) throw; _; }
13
14     event Transfer(address indexed from, address indexed to, uint256 value);
15     event Blacklisted(address indexed target);
16     event DeleteFromBlacklist(address indexed target);
17     event RejectedPaymentToBlacklistedAddr(address indexed from, address indexed to, uint256 value);
18     event RejectedPaymentFromBlacklistedAddr(address indexed from, address indexed to, uint256 value);
19
20     function OreOreCoin(uint256 _supply, string _name, string _symbol, uint8 _decimals) {
21         balanceOf[msg.sender] = _supply;
22         name = _name;
23         symbol = _symbol;
24         decimals = _decimals;
25         totalSupply = _supply;
26         owner =           ;
27     }
```

(1) 상태 변수 추가
- line 9 : 블랙리스트 정보를 저장할 매핑 값이 0이하면 정상, 1이상이면 블랙리스트
- line 10 : 계약 소유자 주소

가상 화폐 계약 – 블랙리스트

◆ 계약 작성

```
1  pragma solidity ^0.4.8;
2
3  contract OreOreCoin {
4      string public name;
5      string public symbol;
6      uint8 public decimals;
7      uint256 public totalSupply;
8      mapping (address => uint256) public balanceOf;
9      mapping (address => int8) public blackList;
10     address public owner;
11
12     modifier onlyOwner() { if (                    ) throw; _; }
13
14     event Transfer(address indexed from, address indexed to, uint256 value);
15     event Blacklisted(address indexed target);
16     event DeleteFromBlacklist(address indexed target);
17     event RejectedPaymentToBlacklistedAddr(address indexed from, address indexed to, uint256 value);
18     event RejectedPaymentFromBlacklistedAddr(address indexed from, address indexed to, uint256 value);
19
20     function OreOreCoin(uint256 _supply, string _name, string _symbol, uint8 _decimals) {
21         balanceOf[msg.sender] = _supply;
22         name = _name;
23         symbol = _symbol;
24         decimals = _decimals;
25         totalSupply = _supply;
26         owner =           ;
27     }
```

(2) 수식자 선언
- 수식자는 메서드를 실행하기 전에 동작 조건을 확인하고 메서드 실행을 제어할 수 있다.

가상 화폐 계약 – 블랙리스트

◆ 계약 작성

```
1  pragma solidity ^0.4.8;
2
3  contract OreOreCoin {
4      string public name;
5      string public symbol;
6      uint8 public decimals;
7      uint256 public totalSupply;
8      mapping (address => uint256) public balanceOf;
9      mapping (address => int8) public blackList;
10     address public owner;
11
12     modifier onlyOwner() { if (                    ) throw; _; }
13
14     event Transfer(address indexed from, address indexed to, uint256 value);
15     event Blacklisted(address indexed target);
16     event DeleteFromBlacklist(address indexed target);
17     event RejectedPaymentToBlacklistedAddr(address indexed from, address indexed to, uint256 value);
18     event RejectedPaymentFromBlacklistedAddr(address indexed from, address indexed to, uint256 value);
19
20     function OreOreCoin(uint256 _supply, string _name, string _symbol, uint8 _decimals) {
21         balanceOf[msg.sender] = _supply;
22         name = _name;
23         symbol = _symbol;
24         decimals = _decimals;
25         totalSupply = _supply;
26         owner =           ;
27     }
```

(3) 이벤트 추가
- 블랙리스트에 추가/삭제하는 이벤트
- 블랙리스트에 포함된 주소에 대해 입출금 거부 이벤트

(4) 생성자 수정
- 상태 변수 owner에 소유자 주소를 설정한다.

가상 화폐 계약 – 블랙리스트

◆ 계약 작성

```
29  (5) function blacklisting(address _addr) onlyOwner {
30          [          ] = 1;
31          Blacklisted(_addr);
32      }
33
34  (6) function deleteFromBlacklist(address _addr) onlyOwner {
35          [          ] = -1;
36          DeleteFromBlacklist(_addr);
37      }
38
39      function tra
40          if (bala
41          if (bala
42          if (blac
43              Reje
44          } else i
45              Reje
46          } else {
47              bala
48              bala
49              Transfer(msg.sender, _to, _value);
50          }
51      }
52  }
```

(5) 블랙리스트 추가 메서드
- 이 메서드는 수식자(onlyOwner)에 의해 계약 소유자 주소만이 실행할 수 있다.
- 블랙리스트에 추가할 주소에 대한 값을 1로 변경하고 이벤트를 발생시킨다.

(6) 블랙리스트 삭제 메서드
- 이 메서드는 수식자(onlyOwner)에 의해 계약 소유자 주소만이 실행할 수 있다.
- 블랙리스트에 추가할 주소에 대한 값을 -1로 변경하고 이벤트를 발생시킨다.

가상 화폐 계약 – 블랙리스트

◆ 계약 작성

```
29      function blacklisting(address _addr) onlyOwner {
30          [                ] = 1;
31          Blacklisted(_addr);
32      }
33
34      function deleteFromBlacklist(address _addr) onlyOwner {
35          [                ] = -1;
36          DeleteFromBlacklist(_addr);
37      }
38
39      function transfer(address _to, uint256 _value) {
40          if (balanceOf[msg.sender] < _value) throw;
41          if (balanceOf[_to] + _value < balanceOf[_to]) throw;
42          if (blackList[msg.sender] > [ ]) {
43              RejectedPaymentFromBlacklistedAddr(msg.sender, _to, _value);
44          } else if (blackList[_to] > [ ]) {
45              RejectedPaymentToBlacklistedAddr(msg.sender, _to, _value);
46          } else {
47              balanceOf[msg.sender] -= _value;
48              balanceOf[_to] += _value;
49              Transfer(msg.sender, _to, _value);
50          }
51      }
```

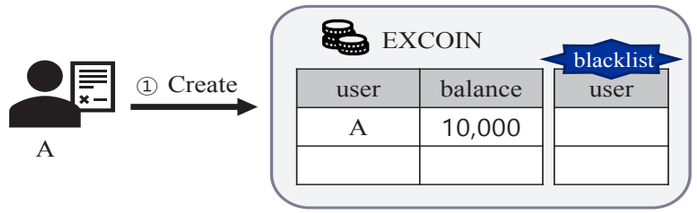
(7) 블랙리스트 주소에 대한 입출금 차단
- 송금에 대해 잔고를 변경하기 전에 블랙리스트 검사를 수행한다.
- 보내거나 받는 주소가 블랙리스트(값이 1이상)이면 이벤트만 발생하고, 잔고는 변하지 않는다.

가상 화폐 계약 – 블랙리스트

◆ 계약 생성

- 이전과 동일하게 A(eth.accounts[0])에 의해 전체 발행량이 10,000인 상태로 계약을 생성한다.
- 계약이 정상적으로 동작하는지 확인하기 위해서 eth.accounts[0]에서 eth.accounts[1]으로 2000을 송금한다.

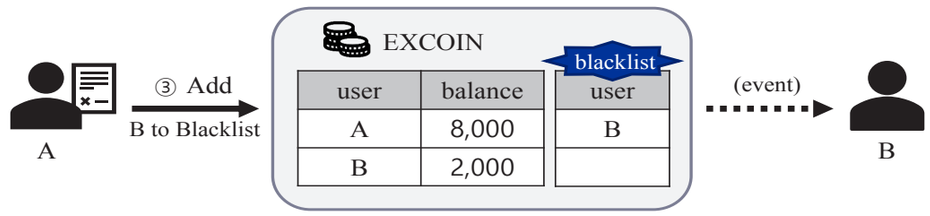
(2) Deploy (1) 10000, "EXCOIN", "ec", 0



가상 화폐 계약 – 블랙리스트

◆ 블랙리스트 추가 및 송금

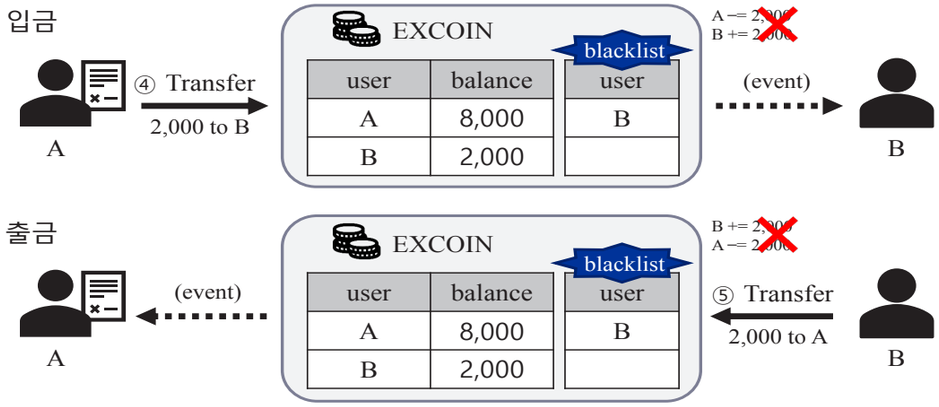
- 사용자 B(eth.accounts[1])를 블랙리스트에 등록한다.



가상 화폐 계약 – 블랙리스트

◆ 블랙리스트 추가 및 송금

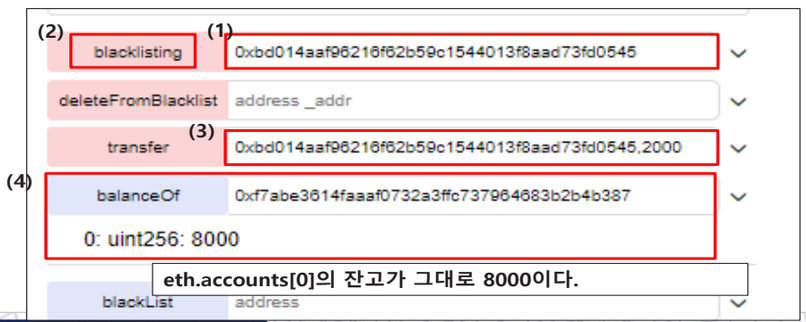
- 사용자 B(eth.accounts[1])가 블랙리스트에 추가되었기 때문에 입출금이 모두 차단된다.



가상 화폐 계약 – 블랙리스트

◆ 블랙리스트 추가 및 송금

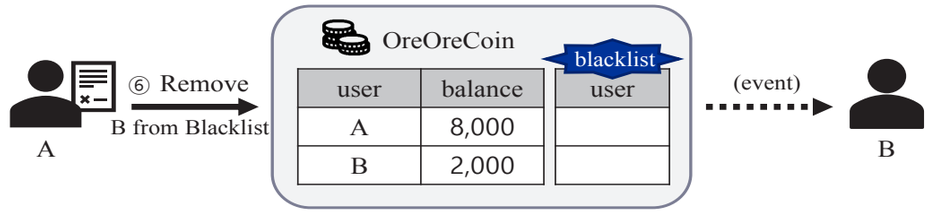
1. Browser-Solidity에서 Run 탭의 "blacklisting" 버튼 옆의 빈칸에 블랙리스트에 추가할 eth.accounts[1]의 주소를 입력한다.
2. "blacklisting" 버튼을 클릭하여 eth.accounts[1]을 블랙리스트에 추가한다.
3. eth.accounts[0]이 eth.accounts[1]의 주소에 2000 코인을 송금한다.
4. eth.accounts[0]의 잔고를 확인한다.



가상 화폐 계약 – 블랙리스트

◆ 블랙리스트 제거

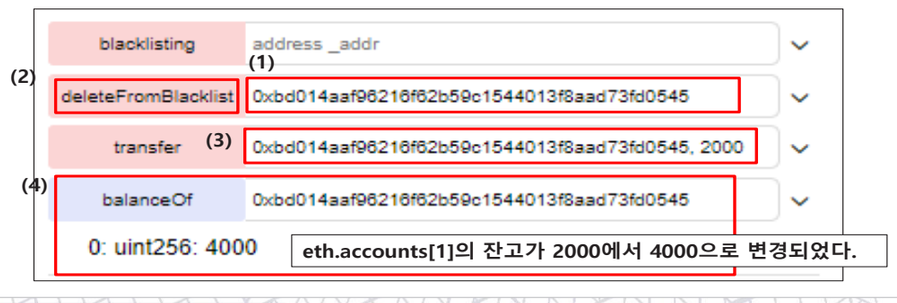
- 사용자 B(eth.accounts[1])를 블랙리스트에서 제거하고 송금이 제대로 동작하는지 확인한다.



가상 화폐 계약 – 블랙리스트

◆ 블랙리스트 제거

1. Browser-Solidity에서 Run 탭의 "deleteFromBlacklist" 버튼 옆의 빈칸에 블랙리스트에서 삭제할 eth.accounts[1]의 주소를 입력한다.
2. "deleteFromBlacklist" 버튼을 클릭하여 eth.accounts[1]을 블랙리스트에서 삭제한다.
3. eth.accounts[0]이 eth.accounts[1]의 주소에 2000을 송금한다.
4. eth.accounts[1]의 잔고를 확인한다.



참고 문헌

- 아카하네 요시하루 외 1인, “블록체인 구조와 이론 ,” 위키북스
- 박제현 외 2인, “코어 이더리움 프로그래밍,” 제이펍
- 와타나베 이츠시 외 3인, “블록체인 애플리케이션 개발 실전 입문,” 위키북스
- 이더리움 가상 머신, https://res.cloudinary.com/hzpbl0kap/image/upload/v1521022316/03-EVM.pdf
- 윌리엄 무가야, 비즈니스 블록체인, 한빛미디어

둘째날

6월 18일(화)

건설회관 3층
대회의실

Part Ⅰ

블록체인 응용 사례

좌장 : 이정우 교수
(중앙대학교)

블록체인 현상과 응용사례

(디지털 신분증, 의료, 법류, 광고, 금융, 컨텐츠)

고 란 기자
(조인디)

Blockchain Era
The Rise of Sovereignty

블록체인 현상과 응용 사례

JOIN :D 고란 기자 neoran@joongang.co.kr

(2019년 6월 18일)

WHO IS SPEEKER

중앙일보 기자: 2003년~
Join:D(블록체인 미디어) CCO
'고란의 어쩌다 투자'
『넥스트 머니』(2018, 다산북스)
'고란TV' '조인디' (youtube 채널)

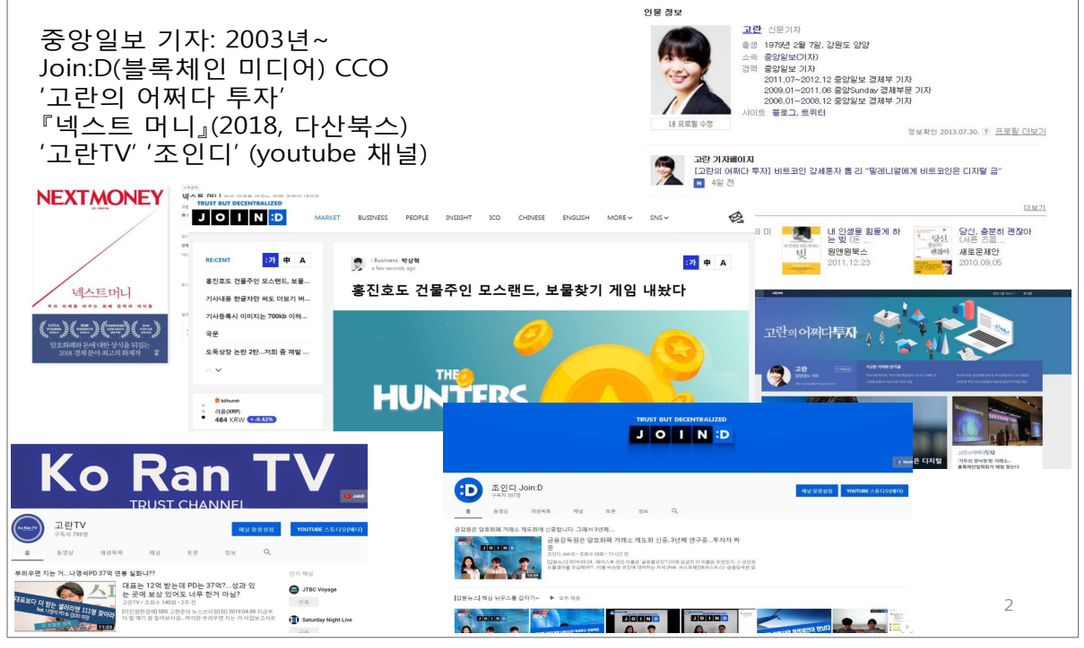


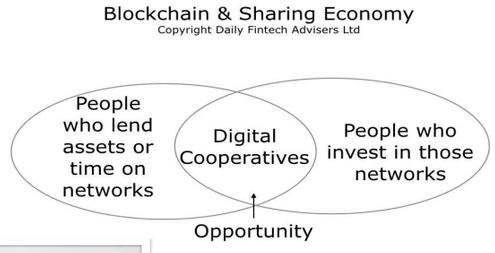
TABLE of CONTENTS

0. 공용경제(Sharing Economy) 시대의 개막

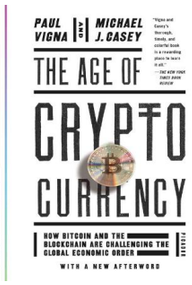
sharing economy

NOUN

An economic system in which assets or services are shared between private individuals, either free or for a fee, typically by means of the internet.



1. 금융: 인간의 자유는 경제적 자립에서부터



Paul Vigna, Michael J. Casey,
『 The Age of Cryptocurrency』(2016)

Roya Mahboob,
CEO of the Afghan Citadel Software Company

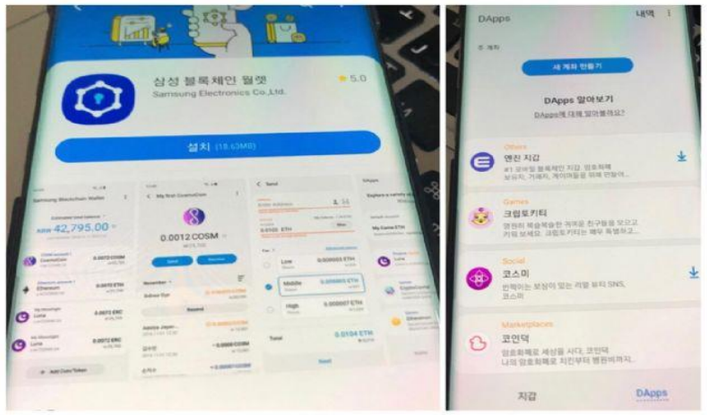
1. 금융: 인간의 자유는 경제적 자립에서부터

케냐

남아프리카공화국

보다폰

1. 금융: 인간의 자유는 경제적 자립에서부터



연도	판매량(대)
2010년	2390만
2011년	9740만
2012년	2억1300만
2013년	3억2930만
2014년	3억1720만
2015년	3억1970만
2016년	3억940만
2017년	3억1750만
2018년	2억9460만

1. 금융: 인간의 자유는 경제적 자립에서부터

Viktor Radchenko
@vikmeup

Apple announced CryptoKit for iOS 13, only a few steps away before you can turn your phone into a hardware wallet.developer.apple.com/documentation/…

♡ 725 1:52 PM - Jun 4, 2019

273 people are talking about this

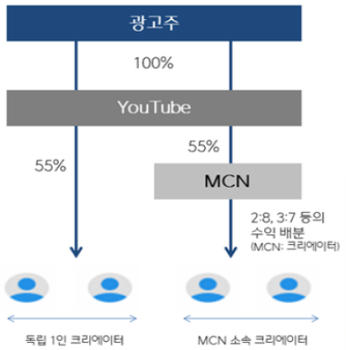
1. 금융: 인간의 자유는 경제적 자립에서부터

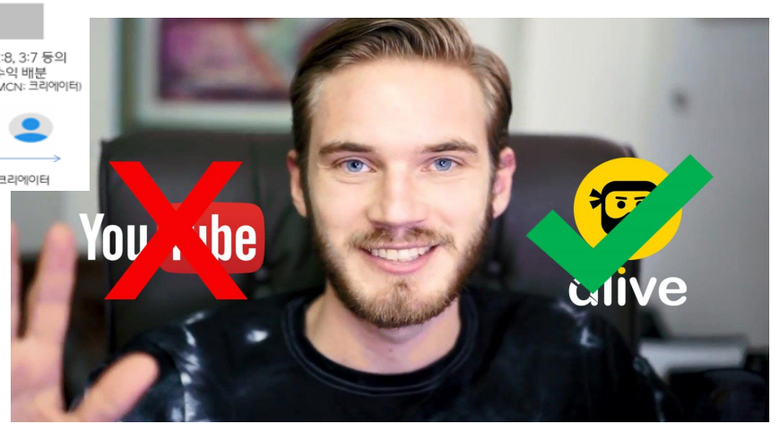
2. 콘텐츠: 유통의 지배를 창작자의 권리로 끝내라

	2007년	2017년	2018년
1	교사	교사	운동선수
2	의사	운동선수	교사
3	연예인	의사	의사
4	운동선수	요리사(셰프)	조리사(요리사)
5	교수	경찰	인터넷방송 진행자(유튜버)

〈자료: 교육부〉

2. 콘텐츠: 유통의 지배를 창작자의 권리로 끝내라





2-1. 게임: 돈이 나오니 밥이 나오니...코인이 나온다

[세계기행] 빈약한 틀, 유저 드라마가 채운 세계관 '리니지'

게임메카 이세벽 기자 2017.04.20 23:24

▲ 초창기 '리니지' 커버 아트 (사진출처: 공식 홈페이지)

세상의 부모님께 고함...게임을 하면 돈이 나옵니다

우주적 관찰자 시점: ④이오스타워게임(상) 가장 많은 아류작을 양산, 기네스북에 오른 게임 테트리스. 이것은 미군의 군사력을 약화시키기 위한 소련군의 음모? 그만큼 중독성이 있다. 그 테트리스를 탑은, 아니 그것보다 더 단순해 더 중독성이 있는 이오스타워게임. 게임하면 돈이 나오니 밥이 나오니 했던 전국의 부모님들이여 반성하라. 게임 했더니 코인이 나온

2. 콘텐츠: 유통의 지배를 창작자의 권리로 끝내라

블록체인 미디어 사례 1. 스팀-스팀잇

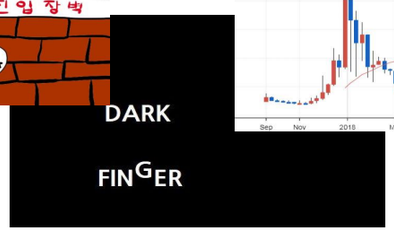
스팀잇의 매력

글을 쓰면
암호화폐로 보상을 받는다!

스팀잇 암호화폐 3종

1. 스팀
2. 스팀파워
3. 스팀달러

< 출처: https://steemit.com/kr/@mechuriya/4-steem-token-economy

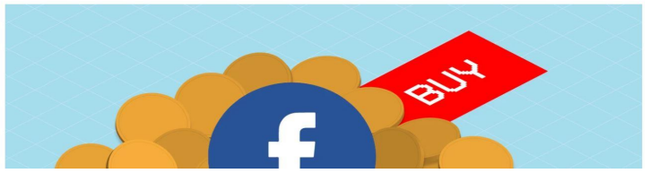


3. DID: 가이사의 것은 가이사에게, 플랫폼 데이터는 주인에게

Facebook plans June 18th cryptocurrency debut. Here's what we know

Josh Constine @joshconstine / 2 days ago

Comment



3. DID: 가이사의 것은 가이사에게, 플랫폼 데이터는 주인에게

Although these events are taking place across a variety of contexts and industries, I would argue that there is a common trend at play. And the trend is this: **control over users' data and digital possessions and activity is rapidly moving from an asset to a liability**. Before, every bit of control

3. DID: 가이사의 것은 가이사에게, 플랫폼 데이터는 주인에게

Microsoft: Forget Google, Facebook – log in with our new blockchain ID

Microsoft has improved the scalability of its ION bitcoin blockchain-based distributed identity system. But it's still early days.

By Liam Tung | May 14, 2019 -- 13:28 GMT (21:28 GMT+08:00) | Topic: Security

Microsoft To Launch Decentralized Identity Solution Based On The Bitcoin Blockchain

By Samantha Mitchell · May 14, 2019

Share

Microsoft

Microsoft Looking To Build Decentralized Identity Network On Top Of Bitcoin Blockchain

Darryn Pollock Contributor
Crypto & Blockchain

Microsoft CEO Satya Nadella delivers the keynote address at Build, the company's annual conference for software developers Monday, May 6, 2019, in Seattle. (AP Photo/Elaine Thompson)
ASSOCIATED PRESS

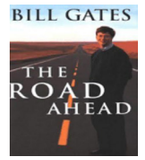
4. 기타(의료・광고・물류 등): 공용경제 기여자를 생각한다

5. The Road Ahead

"We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don't let yourself be lulled into inaction."

"우리는 앞으로 2년 뒤에 닥쳐올 변화에 대해서는 과대평가하지만 10년 뒤에 올 변화는 과소평가하는 경향이 있다. 그렇다고 스스로를 나태함으로 이끌지는 마라."

빌 게이츠,『미래로 가는 길(The Road Ahead)』(1995)



블록체인과 Climate-Smart City

정순혁 부단장
(아태 핀테크그룹)

Part II

블록체인 정책 및 법적 이슈

좌장 : 구태언 부문장
(테크앤로)

전통적인 증권규제와 토큰 이코노미

이해붕 부국장
(금융감독원)

블록체인으로 여는 미래사회 워크샵

Part II-블록체인 정책 및 법적 이슈

전통적인 증권규제와 토큰 이코노미

본 발표내용은 관계당국의 공식적인 입장과 무관하며,
개인적 견해임을 밝혀둡니다.

李 海 鵬

반갑습니다!

2

- 증권감독원/금융감독원 (1990~現)
  * 기업공시, 법제조사, 자본시장 불공정거래 조사
- 법학 석사 (상법)
- 핀테크 현장자문단 (2017.5~現)
- 「블록체인 전략 전문경영자 과정」 제1기 수료 (2018.9-2019.2)
- 비트코인 백서 번역; 글로벌 주요 금융당국의 최근 동향 분석 (미국, 일본, 스위스, 호주, 프랑스, DBGM 등)

한국전자공학회 워크샵(2019.6.18)

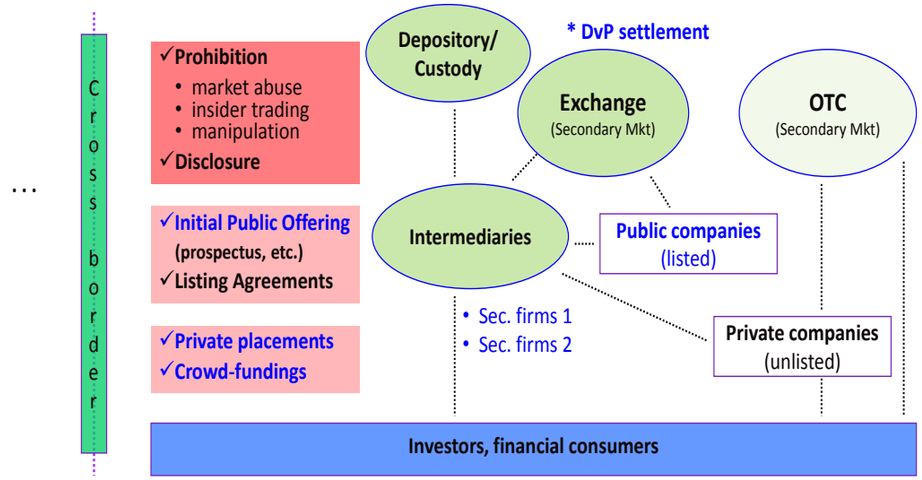
Key Words 1

3

- 전통적 증권시장 구조와 규제 요소
- 소비자(consumer) vs. 투자자(investor)
- 상거래/투자와 정보 비대칭 문제
  - Caveat Emptor (contract law)
  - Informed Investment (securities law)
- Blockchainism, Token economy
- ICO와 증권규제 적용 판단
  - Howey Test, etc.

전통적 증권시장 구조 – 증권 취급규제 관련 제반 요소

4



전통적 증권시장 규제 요소

5

- **금융투자상품 정의** (shares, debentures, units in a CIS, etc.)
- **금융투자상품 중개업** (intermediaries–dealer, broker, exchange, etc.)
- **발행인/권유대상물 등록** (securities registration statement, prospectus)
- **공모/사모 규제 차등** (public offering, private placement)
- **부정거래등 금지** (market misconducts, manipulation, frauds, *class action*)
- **보관/예탁/결제 규칙** (custody, depository, DVP settlement)

소비자와 투자자 – Consumer vs. Investor

6

- ***Customer*** buys a **product** that will satisfy his/her needs

  "소비자는 자신의 사용목적을 만족시켜 줄 제품을 사고"

  * *personal use product/property*

- ***Investor*** buys a **promise** of financial return

  "투자자는 금융수익에 대한 약속을 산다"

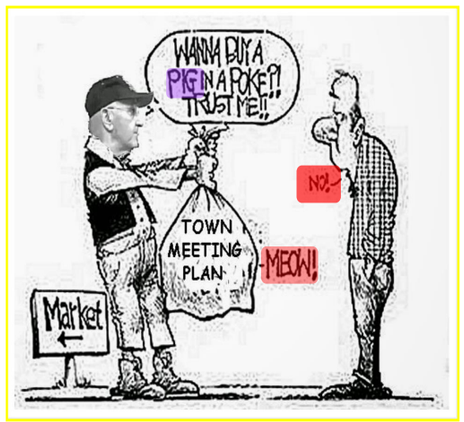
  * *investment, transferable*

WHO sell & promise WHAT ?
Doing as well ?
Done as promised ?

* re: France: ICO regulation objective for the AMF! – *Steemit.com*

정보 비대칭 문제 – 개인용도 물품을 사고 팔 때 (contract law) 7

❖ *Buying without knowing, without a full understanding of its true nature or value ?*



*출처: Ken O'Brien(03/27/2014)
http://ozonesouthbridge.blogspot.com/2014/04/dont-vote-for-pig-in-poke.html

매도자-매수자 간 정보 비대칭 문제 대응

✓ *Guarantee a buyer the right to inspect goods before purchase*

Caveat Emptor=Let the buyer Beware

– *guiding principle of commerce*

(적용) 구매자의 reasonable due diligence 실행으로도 제거되지 못할 정도로 판매자가 분명한 정보 우위에 있을 때

정보 비대칭 문제 – 투자상품을 사고 팔 때 (securities regulation) 8

❖ **informed investment – 글로벌 증권법규, 행위규칙 제도화**

- require to disclose material information
- prohibit misleading or deceptive conduct

❖ **글로벌 증권 규제당국 역할**

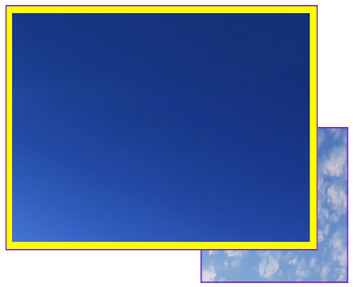
- Facilitate capital formation
- Promote fair, orderly, and efficient markets
- Protect investors

• Investors' Advocate

Informed investment 여건 확보 – 증권 발행/유통 행위 규칙 9

❖ **Blue Sky law & 33년/34년 증권법**

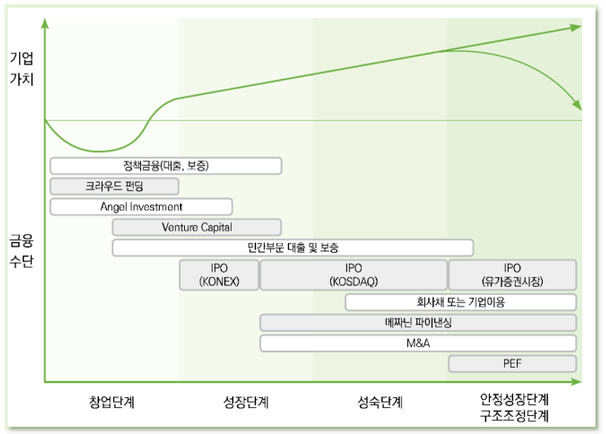
- **U.S. state securities laws named after the term, requiring sellers to**
  - ✓ *register their offerings*
  - ✓ *provide material information, etc.*
- **Safeguards to**
  - ✓ *protect investors from fraud making lofty promise of greater profits to come, hiding details fraudulently*
  - ✓ *stop the sale of stock exploiting fraudulently investors' lack of experience or knowledge about the security*



- *Metaphor: fraudulent basis of some securities, 'speculative schemes' with no more basis than do many feet of empty 'blue sky'*

기업공개(Initial Public Offering) 10

❖ **성장단계에 접어든 기업의 상장 과정 – 주식공개, 자금조달**



- Highly standardized
- Lawyer–heavy orchestration
- Underwriting
- Exit (v/c, etc.)

✓ Corporate track record
✓ Offerings rights
✓ Tradable products

U.S. 증권규제법에서의 책임 가중

11

common law, caveat emptor	securities regulation
• **Principles of commerce** ✓ let the buyer *Beware* ✓ right to inspect before purchase	• **Enhanced disclosure requirements** ✓ registration of pub. offered security ✓ prospectus (risks, material information)
• **Common law fraud elements** ✓ material misrepresentation/omission ✓ made with knowledge (reckless disregard) of its falsity ✓ intention to induce the victim to rely ✓ justifiable reliance by the victim ✓ damages → tort, rescission, restitution, etc.	• Elements of common law fraud + **More protective civil remedies** ✓ lower requirements for recovery (negligence, shift burden of proof) → civil & criminal liability, injunction, administrative remedies

한국전자공학회 워크샵(2019.6.18)

Blockchainism, Token economy – radical ideas came to real world

12

- **Decentralized Autonomous Eco-system** (developers, users, investors)
  - governance, transparency, accountability, etc. are ensured via protocols
  - philosophical insights, embracing the ideas – distributed records & power, distributed capitalism, etc.
- **Suggest solutions for issues human society confront, impacting real life economically & socially**
  - crypto-economies are created as environments, and
  - scaling up the scope of applicability
- **Eco-system ≒ community, SUSTAINABLE**

한국전자공학회 워크샵(2019.6.18)

Bitcoin: A Peer-to-Peer Electronic Cash System

13

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

<Contents>

electronic payment system *trusted third party* *without* *transaction cost* *sent directly* *financial institution* *purely peer-to-peer version* *distributed* *longest chain* *electronic cash* *We propose* *timestamp server* *prevent double-spending* *nodes* *outpace attackers* *majority cooperating* *online payment* *solution* *transaction* *ongoing chain of hash-based proof-of-work* *proof of the sequence of events witnessed* *honest nodes collectively control* *digital signature* *computational proof* *timestamp network* *messages broadcast* *chronological order of transactions* *hash timestamped* *non-reversible transactions* *minimal structure*

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

한국전자공학회 워크샵(2019.6.18)

Bitcoin: A Peer-to-Peer Electronic Cash System

14

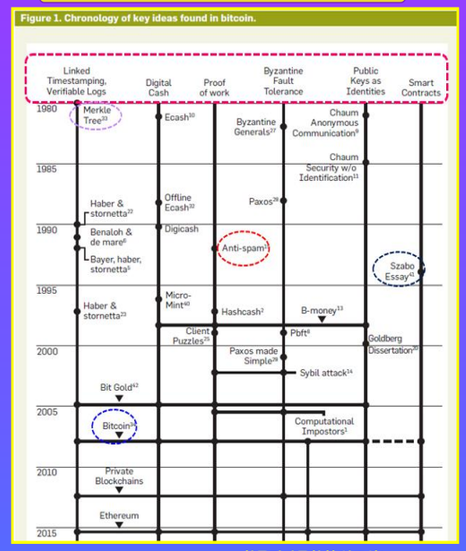
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

- The first application program, adapting the concept of blockchain to a specific field of crypto-currency
- The concept of crypto-currency is built from forgotten ideas in research literature
- Making a *radically* different proposal for a decentralized crypto-currency that did not need the banks

Collaboration

→ "We propose ..."

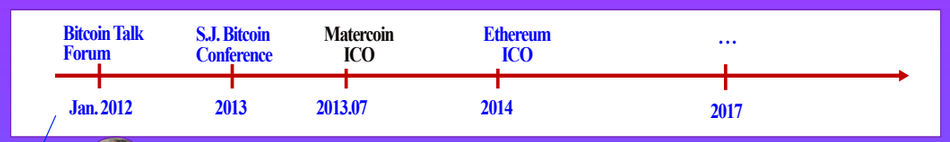
Bitcoin's Academic Pedigree



한국전자공학회 워크샵(2019.6.18)

첫 번째 ICO – J.R. Willett의 아이디어

15



- Mastercoin: A Second Generation Protocol on the Bitcoin Blockchain

"The Second Bitcoin White Paper"

We claim that the **existing bitcoin network** can be used as a protocol layer, on top of which new currency layers with new rules can be built …., … will **provide initial funds to hire developers** to build software which implements the new protocol layers, … **will richly reward early adopters** of the new protocol."

- Seattle s/w engineer meetup -

J.R. Willett @San Jose Bitcoin Conference (2013)

16

"If you wanted to, today, start a new protocol layer on top of Bitcoin, …, you could do it **without going to a bunch of venture capitalists** and instead of saying, hey, I've got this idea, you can — you're familiar with Kickstarter I assume? …

… here's my pitch, here's **my group of developers** — lot of developers in this room. If you get a **bunch of trustworthy guys together** that people have heard of and say, okay, we're going to do this. We're going to make a new protocol layer… on top of bitcoin, and **here's who we are** and here's our plan, and here's our bitcoin address, **and anybody who sends coins to this address owns a piece of our new protocol**. … I've been telling people this for at least a year…. I don't have a ton of coins, but that's where I want to invest my coins. … Does **anybody in this room** want my bitcoins because I want to—"

"**I'll take them**," someone shouts

- VC들한테 머리 조아리며 설명할 필요 없잖아요
- Kickstarter와 비슷해요

- 여기 이 방에 있는 개발자들
- 우리끼린 서로 믿을만 하잖아요
- 다들 그러고 싶을 겁니다

- 나한테 보내줘요!

Initial Coin Offering – 공개적 판매권유 행위…

17

public

❖ ***Wisdom of the crowd?***

- **Cap, Price (pre-sale, crowd-sale)**
- **Whales (large investors)**
- **Listing & trading**
- **노드 보상용, 자금모집 목적의 판매용으로 변질?**
- **Interactive Coin Offering (Vitalik)**

- 문제는 대부분 토큰 모집이 마치 도서명, 저자, 배포망 이런 것들 모두가 앞으로 정해질, 아직 설립도 되지 않은 출판사의 지분에 투자하라는 것과 유사하다. 2차 유통시장에서 오른 가격에 팔 수 있을 거라 기대하고 가치 상승 가능성만 보고 투자하라는…

Many token offerings are more analogous to interests in a **yet-to-be-built** publishing house with the authors, books and distribution networks all to come.

– SEC Chairman, *Statement on Cryptocurrencies and ICOs* –

"If you want investors to empty their pockets, tell them that you are using blockchain."

– PM of India, 2018, at Singapore Fintech Festival

rampant Scams cast a dark shadow over Play Grounds

18

● Blockchain Exchange Commission ?

Headquarter Address: "SEC = BEC"

100 F Street Northeast, Washington, D.C. 20549

Sale–Crypto/digital Assets

Unregulated

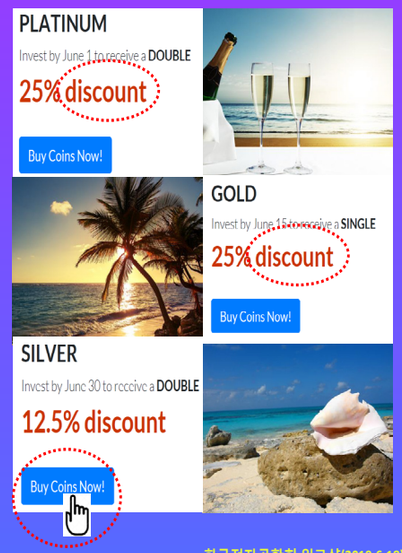
- Offering promises/rights?
  - ✓ Alerts, no recourse
  - ✓ Guidance (taxonomy…)
  - ✓ Consultation process
  - ✓ Regulatory framework

19

HOWEYCOINS

DON'T MISS THIS EXCLUSIVE OPPORTUNITY TO PARTICIPATE IN HOWEYCOINS TRAVEL NETWORK NOW!

- HoweyCoins are officially registered with the U.S. gov.
- You can trade on an SEC-compliant exchange for profit
- Can be used with existing points programs
- Can be exchanged for cryptocurrencies and cash
- Can be spent at any participating airline or hotel ...



한국전자공학회 워크샵(2019.6.18)

20

HOWEYCOINS

Investor.gov
U.S. SECURITIES AND EXCHANGE COMMISSION

ICO - HOWEYCOINS

If You Responded To An Investment Offer Like This, You Could Have Been Scammed – HoweyCoins Are Completely Fake!

- RED FLAG: CLAIMS OF HIGH, GUARANTEED RETURNS √
- RED FLAG: CELEBRITY ENDORSEMENTS √
- RED FLAG: CLAIMS OF "SEC-COMPLIANT"
- RED FLAG: INVESTING WITH A CREDIT CARD
- RED FLAG: PUMP AND DUMP SCAMS

한국전자공학회 워크샵(2019.6.18)

21

ICOs, 적용될 규칙은?

ICO 시조새의 생각? (J.R. Willett, 인터뷰) 12/14/2018

Q: ICO는 '눈먼 돈'을 모은다는 지적도 받습니다. 가장 시급하고 중요한 규칙은 무엇일까요?

A: ICO에서 가장 중요한 규칙은 캐비엇 엠토르(caveat emptor)입니다. 사는 자와 파는 자 모두 스스로 경계를 게을리 하지 말아야 한다는 라틴어 표현입니다…. 아무도 사기성 ICO 출시를 막을 수는 없어요. 규제당국은 사기가 발생한 후에 이에 대응할 뿐입니다.

안타깝게도 사전판매(pre-sale)를 하지 않는 ICO는 보기 드뭅니다. 사전판매에서 부유한 사람들과 내부자가 대량의 토큰을 제공받은 뒤 개인 투자자가 희생됩니다. 업OO이 사전판매를 하지 말아야 한다고 주장한 이유이기도 합니다. 저는 내부자이지만 업OO을 시중가로 구입했습니다.

*출처: Blockinpress(2018.12.14), "비트코인 250원 시절 입문해 'ICO 창시자'…."

한국전자공학회 워크샵(2019.6.18)

22

ICO/crypto-asset – 증권성 판단, Howey Test (예시)

❖ √ 경제적 실질이 증권&공모행위와 같다면 ?

- Digital asset itself is a simply code, all by itself is not a security
- If an ICO represents a set of rights & financial interest, then the *economic substance* is the same as a securities offering

→ **securities laws (regulatory principles) are applied**

- **Investment Contract**(securities) – **Howey Test**
  1) invest of money, 2) in a common enterprise, 3) with an expectation of profit, 4) derived from the efforts of others

✓ "**Form is disregared for substance** *and the emphasis is placed upon* ***economic reality***" *(SEC v. Howey, 1946)*

• flexible

한국전자공학회 워크샵(2019.6.18)

Regulatory framework for ICOs & token generation events

23

❖ 해외 증권당국의 입장 (예시) – ASIC

"ASIC has been clear that for ICOs, regardless of the structure, there is one law that will always apply – you can't make misleading or deceptive statements about the product. This is a key focus for ASIC. …law prohibiting misleading or deceptive conduct will apply in this space, regardless of whether there is a financial product involved.

While ICOs are highly speculative investments, they may involve similar risks to other existing financial products. Therefore we believe the existing laws can continue to be applied to ICOs in a technologically-neutral manner.

However as the crypto-asset market evolves, there may be further opportunities to modify the regulatory framework.

– c2019-t353604-asic.pdf . Submission to the Treasury Issue Paper on Initial Coin Offerings –

Key Words 2

Reasoning, Guidance & Regulatory Frameworks are converging globally

24

- 연구(위탁)/조사/협업, 그 결과를 공표하고
  * HKMA/ASTRI, SEC, AMF, JFSA, …
- 공개적으로 주의경고, 입장, 가이드라인을 밝히며
  * SEC, JFSA, HKSFC, …
- 금지할건 금지, 되돌려 주라는 명령 내리고
  * SEC, HKSFC, MAS, …
- 접촉/입장표명 창구를 일원화 하며
  * FinHub; Crypto-Mom/Czar/Daddy …
- 공개 의견수렴 절차 진행, 그 회신도 공개하고
  * AUS Treasury, AMF, …
- 필요한 규제의 틀을 갖추어 나가다
  * JFSA, AMF, FSRA-ADGM …; FATF; IOSCO

미국 – IRS Guidance, SEC Report/Statements/Framework

25

헤드라인	비고
• IRS, "IRS Virtual Currency Guidance" (03/25/14)	• Property; 교환거래 손익 증빙
• 뉴욕주, BitLicense(→Virtual Currency License)법 (06/03/15)	
• SEC, "The DAO Investigation Report" (07/25/17)	• 오래된 증권규제원칙 적용
• SEC Chairman, "Statement on Cryptocurrencies and ICOs" (12/11/17)	* **Howey Test (1946)**
• 뉴욕주(의회), '암호화폐 규제 원점 재검토 TF' 출범 (06/02/18)	* investment contract
• SEC, "Digital Asset Transactions: When Howey met Gary" (06/14/18)	• W. Hinman Remarks
• 트럼프(행정명령), '사이버/가상통화 사기 대응 TF' (07/13/18)	• 법무부, SEC, CFPB 등
• 뉴욕주(검찰), 'Virtual Markets Integrity Initiative Report' (09/18/18)	• trading platforms 조사결과
• 양원, 'Blockchain Promotion Act of 2018' 제출 (10/03/18)	• 블록체인 정의 명확화 요구
• SEC(기업재무국등 3개부서장), 'Statement on Digital Asset Securities Issuance and Trading' 발표 (11/16/18)	• 기업재무국, 투자관리국, 시장국
• SEC, "Framework for 'Investment Contract' Analysis of Digital Assets" (04/03/19)	• 토큰 비조치의견서도 공표

미국 SEC

26

- *DAO Investigation Report (17.07.25)*

Howey Test – investment contract
- securities law principles -

– DAO tokens are 'securities'(증권)

- DAO 투자자들은 '타인의 경영노력'(managerial efforts)으로부터 나오게 될 '수익에 대한 합리적 기대'(reasonable expectation of profits) 하에 '금전을 투자'한 것

- *Framework for 'Investment Contract' Analysis of Digital Assets (19.04.03)*

- Virtual currency, crypto currency 용어를 'digital assets'으로 변경
- 권유행위의 본질에 따라, 연방증권법상 증권(security) 유형인 '투자계약' 해당여부 분석 기준 구체화
  – **(적용범위)** offering, selling, distributing; marketing, promoting; buying, selling, trading; facilitating exchanges; holding, storing; offering financial services-management, advice; other professional services

일본 – 투자자 경고, 지급수단/거래 제도화, 투기대응 규제 강화

27

헤드라인	비고
• 개정 자금결제법*, 범죄수익은닉법 등 본격 시행 (09/30/17) * (1989년 제정) '선불식 증표의 규제등에 관한 법률'(프리페이드법) 토대로 개정	• 가상통화 정의, 지급결제 수단, 가상통화교환업
• 금융청, ICO에 관한 성명서 (10/27/17)	• 규제관점 명확화, 위험 경고
• 금융청, '가상통화교환업 등에 관한 연구회' 설치 운영 (03/18~11/18)	• **회의록, 설명자료 등 공개**
• ICO 비즈연구그룹(타마 대학), 금융청에 ICO 규제방안 요청 제안 (04/05/18)	• **ICO 가이드라인 초안**
• 금융청, 일본가상통화교환업협회(JVCEA) 認定 자율규제기관 승인 (10/18)	
• 금융청, 「자금결제법등 개정법률안」 의회 통과 (법안제출 03/15/19, 의회 통과 05/31/2019) * 암호자산 중 투자형토큰 – 금융상품거래법, 금융상품판매법도 적용 * 2020.4월 시행; 2020.1월부터는 소득세 적용(재산채무조서에 암호자산 포함)	• '암호자산'으로 변경, 가격조작 금지, 적용법 확대

한국전자공학회 워크샵(2019.6.18)

홍콩 – 연구위탁 발표, 성명서, 가이드라인, 규제방안

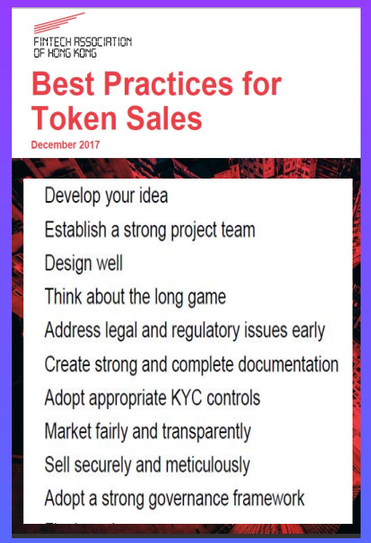
28

헤드라인	비고
• HKMA/ASTRI, "Whitepaper on Distributed Ledger Technology" (11/11/16)	• 분산원장기술(DLT) 연구물 공표 약속 이행
• HKMA/ASTRI, "Whitepaper 2.0 & ANNEX on DLT" (10/25/17)	
• HKSFC, "Statement on Initial Coin Offerings" (09/05/17)	• 증권형 - 증권법 적용
• FTAHK(홍콩핀테크협회), "Best Practices for Token Sales" (12/17)	• 자율규제
• HKSFC, "Statement on regulatory framework for virtual asset portfolios managers, fund distributors and trading platform operators" (11/08/18)	• 가상통화 투자펀드 등록 및 가입 제한, VA 펀드 운용사 면허조건, 가상통화 거래소 규제샌드박스 또는 면허요건

한국전자공학회 워크샵(2019.6.18)

HongKong – Self-regulation and HKSFC

29



HK Securities and Futures Commission

- Halted an ICO that the structure was to constitute a 'collective investment scheme' under HK SFO, to unwind and return tokens to the HK investors
- Warned seven HK-based or connected crypto exchanges, seven ICO issuers against unlicensed, unauthorized handling of cryptocurrency that constitute 'securities'

한국전자공학회 워크샵(2019.6.18)

싱가포르 – 가이던스, 지급결제법, 불법행위 금지

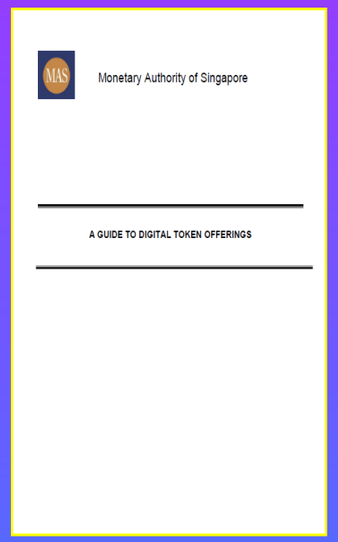
30

헤드라인	비고
• MAS, "A Guide to Digital Token Offerings" (11/14/17)	• 자본시장 상품형 → 증권법
• MAS, "A Guide to Digital Token Offerings" (updated, 11/30/18)	
• MAS, "PSA, Payment Services Act" 제정 (2019.2.25 제정, 하반기 시행 예정) * 기존 지급시스템법/환전송금업법 대체; digital payment service 라이선스 * Definitions: currency; money(e-money); digital payment token, service provider …	• 암호화폐 규제법

한국전자공학회 워크샵(2019.6.18)

Singapore (MAS)

31



- application of Securities Laws on offers or issues of digital tokens in Singapore which constitute 'capital market products'
  - ✓ Capital markets products: Share, debenture, unit in a CIS
  - ✓ Offerors of digital tokens securities or unit in a CIS
  - ✓ Intermediaries, facilitate offers / issues of digital tokens
- Warned digital token exchanges the need to seek authorization as a approved if the token traded constitute 'securities'
- Warned a ICO issuer to stop offering tokens that are considered to constitute 'securities' to Singapore-based investors, and return all funds raised

스위스, 영국, 지브롤터, 몰타 – 가이드라인, 의견수렴, 관련입법

32

헤드라인 (스위스)	비고
• FINMA, "Regulatory treatment of ICO" (09/29/17) • FINMA, "Guidelines for enquiries regarding the regulatory framework for ICO" (02/16/18) • CVA(크립토밸리협회), "ICO Code of Conduct" (01/18/18)	• 토큰 개별 특성(양도성, 기능) 평가→ 3개 유형 (Payment/Utility/Asset형); • AML/블록체인 혁신기술성
헤드라인 (영국)	**비고**
• 의회(Treasury Committee), 가상화폐 및 분산원장기술 연구 실시 (02/22/18) • FCA, Guidance on Cryptoassets (consultation 기초문건) 발표	• 혁신적 비즈 기회 창출 등 잠재적 이득, 리스크 연구
헤드라인 (지브롤터-영국령)	**비고**
• GFSC, 'Financial Services (DLT Providers) Regulations 2017' and 'DLT Provider Guidance Notes 1~9' 발표 (10/12/17)	• 금융서비스업으로 규제
헤드라인 (몰타)	**비고**
• 의회, 블록체인, 가상통화, DLT 관련 3개 법안 입법 (0626/18) * ICO 규제 가상금융자산법(VFA), 전담조직 몰타 디지털혁신기구법(MDIA), 관련기업 설립법(ITASA)	• 블록체인 관련산업 규제틀

Switzerland – FINMA ICO Guideline (02/16/2018)

33

The table below illustrates the key factors:

	Pre-financing and pre-sale / The token does not yet exist but the claims are tradeable	The token exists
ICO of payment tokens	= Securities ≠ subject to AMLA	≠ Securities = means of payment under AMLA[3]
ICO of utility tokens[4]		≠ Securities, if exclusively a functioning utility token = Securities, if also or only investment function ≠ means of payment under AMLA
ICO of asset tokens[4]		= Securities ≠ means of payment under AMLA

- Payment, Utility, **Asset tokens** (securities)
- Have to make an Inquiry to FINMA with information FINMA requires, including law firm's review
- FINMA monitoring closely and cracking down on fraudulent activities
- Self-Regulation (Cryptovalley Association)

프랑스 – 의견수렴, 결과발표, 규제체계 마련

Avant garde

34

헤드라인	비고
• AMF, launched *a public consultation on ICOs* (10/26/17~12/22/17) • AMF, "Summary of replies to the public consultation on Initial Coin Offerings and update on the UNICORN Programme" (02/22/18) * UNICORN : Universal Node to ICO's Research & Network • 의회, 'Business Growth and Transformation Bill'(PACTE) (06/19/18 하원, 09/14/18 통과; 04/11/2019 의회 최종독회 통과) * AMF에 ICO 관련 정보 심사, 승인권한 부여	• ICO에 관한 규제필요성 등 관련 의견 공개적 요청 • ICO/DASP 규제체계 법안 - Optional VISA for ICOs - Optional license for DASP

France – AMF (Authorité des Marchés Financiers)

35

Summary of Replies to the Public Consultation on ICOs … (02/22/2018)

I – UNICORN Programme Update – ICO projects presented to the AMF; Token issued as part of an ICO; Comments on the information documents provided to token purchasers at the pre-issue stage (whitepaper)

II – Respondents' opinions on the AMF's legal analysis of ICOs – ICOs & financial instruments; ICOs & intermediation in miscellaneous assets; ICOs & collective investments; ICOs & crowd-funding; Other possible legal qualifications; Other items to consider in the legal analysis

III – Respondents' opinions on white papers & the duties of project initiators – Minimum information that respondents agree should be provided; Information on the projects developers; W/P approval by an authority, professional association or other reference institution; W/P validation by independent experts; Sale & pre-sale transparency; W/P standardization; Warning about the risks arising from the unregulated nature of ICOs; Other W/P good practices mentioned by respondents; Escrow of funds raised; AML/CFT; Token valuation . . .

IV – Regulation options preferred by respondents

V – Main results of the public consultation

한국전자공학회 워크샵(2019.6.18)

호주 – 가이드라인, 공개의견수렴, 접수의견 공표…

36

헤드라인	비고
• ASIC, "Information Sheet 225 ICOs and crypto-assets" (09/2017, updated 05/30/2018, 19-121MR) – ICO를 통해 크립토에셋을 권유할 때 고려할 사항 – ICO나 크립토에셋과 관련하여 오해를 유발하거나 사기적인 행위가 되는 경우는 – 어떤 경우 ICO가 금융상품이 되거나 이를 포함하게 되는지 – 크립토에셋 트레이딩 플랫폼이 금융시장이 되는 경우는 – 크립토에셋을 참조하는 금융상품에 대하여 – 해외에서의 크립토에셋 범주가 호주에서는 …	• ICO, 암호자산 가이던스 (회사법, 증권투자법 관계)
• Treasury, *public consultation process on ICOs* (01/2019~02/2019) * Issues Paper: INITIAL COIN OFFERINGS (토큰 범주, ICO시장 동력, 기회요인/리스크요인, 호주의 현행 규제체계 및 개선 필요성, 조세 취급방안)	• 재무부의 이슈검토문 제공 및 질문; 공개 의견수렴; 제출의견서 공개

한국전자공학회 워크샵(2019.6.18)

아부다비 국제금융센터(ADGM) – 규제체계 제도화

37

헤드라인	비고
• FSRA, Guidance-Regulation of Initial coin/Token Offerings and Crypto Assets under the Financial Services and Markets Regulations (06/25/2018) • FSRA, Guidance-Regulation of Crypto Asset Activities in ADGM (06/25/18) * 암호자산취급업(OCAB) 인가; OCAB 규제조건 (유형, 인정 암호자산, 자본금 요건, AML/CFT, TAX); Technology governance & control; crypto asset risk disclosures; market abuse, transaction reporting; crypto asset exchange; crypto asset custodian…	• ICO에 관한 규제필요성 등 관련 의견 공개적 요청 • OCAB 규제 조건 • 암호자산 거래소 • 암호자산 보관/수탁 등

한국전자공학회 워크샵(2019.6.18)

prayer for developers . . .

38

"Were you HONEST in your business dealings ?"

– Babylonian Talmud, Shabbos 31a –

• Community
• Collaborative efforts

THANK YOU!

블록체인 혁명에 대비한 주요국의 정책 동향

구태언 변호사
(법무법인 린)

블록체인 혁명에 대비한 주요국 정책동향

2019. 6. 18.
법무법인 린
테크앤로 부문장 구태언

목차

I. 각국 블록체인 산업 관련 규제 최신 동향

2018년 각국 블록체인(암호화폐) 규제 현황 일람표 I

나라	ICO 허용 여부	암호화폐 거래 허용 여부	암호화폐거래소 라이선스 유무	ICO 가이드라인 유무
싱가포르	O	O	O	O
스위스	O	O	O	O
중국	X	X	N/A	N/A
한국	X	O	X	X
미국	O	O	O	X
일본	O	O	O	X
영국	O	O	O	X
프랑스	O	O	X	O
몰타	O	O	X	X
루마니아	O	O	X	X

2018년 각국 블록체인(암호화폐) 규제 현황 일람표 II

나라	ICO 허용 여부	암호화폐 거래 허용 여부	암호화폐거래소 라이선스 유무	ICO 가이드라인 유무
우크라이나	O	O	X	X
캐나다	O	O	O	X
유럽연합	O	O	X	X
독일	O	O	O	O
호주	O	O	O	O
태국	O	O	O	O
브라질	O	O	X	X
러시아	O	O	X	O
베네수엘라	O	O	O	X
에스토니아	O	O	O	X

미국

새롭고 중앙화된 증권 규제

- SEC는 토큰이 증권일 경우 증권법에 따른 규제를 받아야 하며, 기존 모든 토큰은 증권일 가능성이 있으니 면밀한 주의 당부
- 증권이 아닐 경우에는 별다른 규제 없으며, 암호화폐 거래소도 상장시 토큰이 증권이 아니라는 로펌 의견서 요구

암호화폐 & 거래

- 50개 주가 모두 각자의 규정을 만들 수 있음(예, BitLicense)
- SEC는 증권형 토큰의 정의 및 ICO 에 대한 관할권을 보유
- FinCEN - 모든 거래소가 등록해야 함

ICO

- 엄격한 SEC 규정으로 인해 ICO를 발행하는 회사들이 미국 내 참가자들에게로부터 자본 모집을 하지 못함
- 증권의정의의 범위가 매우 넓음(예, 투자계약증권 - Howey Test)
- 최근 적격투자자(연소득20만불이상)로 참가자를 한정하는 사례 有

시사점

- 증권형 토큰 ICO(STGE)도 등장
- 센트라코인 등 사회적 피해가 큰 토큰에 대해서는 SEC, USAO 등이 적극적 법적용

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets (4)

- **타인의 노력으로부터 발생하는 이익에 대한 합리적인 기대(Reasonable Expectation of Profits Derived from Efforts of Others)가 있었는지 판단하는 구체적 기준**
  - **2. Reasonable Expectation of Profits**
    - 이익은 초기 투자나 사업 개발로부터 자본 이득이나 구매자의 자금의 사용의 결과로 얻어지는 이익에 대한 참여가 포함되며, 전적으로 수요와 공급에 영향을 주는 시장 외부적 요인에 의한 가격상승은 Profit에 대한 기대에 포함되지 않음.
    - ①디지털 자산이 소유자에게 회사의 수입이나 이익을 나눌 권리를 주거나 디지털 자산의 가격상승으로 인한 이익을 현실화할 기회를 주는 경우, ②디지털 자산이 이동 가능하고 플랫폼이나 2차 시장에서 거래 가능하거나 장래에 그럴 것으로 기대되는 경우, ③그 타인들이 네트워크나 디지털자산의 가치를 증대시키기 위해 지속적으로 돈을 쓰는 경우 등에 해당하면 Reasonable Expectation of Profits가 있는 것으로 해석될 가능성 높음.

7

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets

- ICO를 진행할 때는 미국 연방 증권법이 적용되는지 확인하여야 함.
- ICO를 진행하는 코인이 미국 연방 증권법상 "증권"(Security)의 정의에 부합하면 미국 연방 증권법이 적용됨.
- 증권의 개념에는 주식, 채권뿐만 아니라 "투자계약증권"(Investment contract)도 포함됨.
- 디지털 자산이 증권에 해당하면 증권을 제공하거나 판매할 때 SEC에 등록하여야 함.
- **이 SEC 가이드는 디지털 자산이 투자계약증권인지 여부, 그리고 디지털 자산에 대한 제공이나 판매가 증권거래인지 여부를 판단하는 기준을 제공하는 것임.**
- **투자계약증권 해당여부를 판단할 때 Howey Test를 기준으로 삼는 것은 기존의 미국 연방 대법원 입장과 같으나, 그 구체적인 기준들을 제시하였다는 데에 의미가 있음.**
- 기존의 미국 SEC의 입장에서 크게 진보한 것은 아님.

8

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets

- **원문 URL :** https://www.sec.gov/files/dlt-framework.pdf
- **투자계약 증권 해당여부 판단 기준 : Howey test**
  - **투자계약 증권 : 타인의 노력으로부터 발생하는 이익을 합리적으로 기대하면서 공동의 사업에 금전을 투자할 때 투자계약이 존재함.**
  - **1. 금전의 투자(The Investment of Money)**
    - 디지털 자산을 현실 통화나 다른 디지털 자산 등을 통해 구매하면 이 요건이 충족됨.
    - 대부분 디지털 자산의 경우 이 요건을 충족함.
  - **2. 공동의 사업(Common Enterprise)**
    - 법원은 공동의 사업 요건은 투자계약의 특유한 요건으로 분석하고 있음.
    - 대부분 디지털 자산에서 공동의 사업 요건도 충족함.

9

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets (2)

- **투자계약 증권 해당여부 판단 기준 : Howey test**
  - **3. 타인의 노력으로부터 발생하는 이익에 대한 합리적인 기대(Reasonable Expectation of Profits Derived from Efforts of Others)**
    - 구매자가 타인의 노력으로부터 발생할 이익(또는 다른 금전적인 보상)에 대한 합리적인 기대가 있었는지 여부로, 보통 Howey test에서 가장 중요한 부분임.
    - 홍보자나 스폰서나 제3자들이 사업 성공에 필요한 경영적 노력을 제공할 때 투자자들은 이익에 대한 합리적인 기대를 하게 되고, 이 조건이 충족됨.
    - 이 요건 충족여부를 판단할 때에는 거래시 경제적 현실이 어떠한지, 어떠한 경제적 유인이 고객에게 전달되는지 등을 고려함.
    - 즉 이 요건은 거래 자체와 디지털 자산이 어떻게 제공되고 판매되는지에 관련된 것임.

10

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets (3)

- **타인의 노력으로부터 발생하는 이익에 대한 합리적인 기대(Reasonable Expectation of Profits Derived from Efforts of Others)가 있었는지 판단하는 구체적 기준**
  - **1. Reliance on the Efforts of Others**
    - 구매자가 합리적으로 타인의 노력에 의지할 것을 기대할 수 있었는지 여부를 고려함
      - 디지털 자산의 네트워크 완성을 위해 타인의 노력이 필수적인 경우, 그 타인이 디지털 자산과 네트워크의 가치증대를 위해 노력할 것을 기대할 수 있는 경우 등을 고려하여 판단
    - 그 노력이 사업 성패에 영향을 미칠만한 부인할 수 없는 중요한 필수적인 경영 노력인지 여부를 고려함.
  - **2. Reasonable Expectation of Profits**
    - 이익은 초기 투자나 사업 개발로부터 자본 이득이나 구매자의 자금의 사용의 결과로 얻어지는 이익에 대한 참여가 포함됨.
    - 전적으로 수요와 공급에 영향을 주는 시장 외부적 요인에 의한 가격상승은 포함되지 않음.

11

미국

TKJ 토큰에 대한 '비규제 조치 의견서'(No-Action Letter) 발행

- 원문 URL : https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm
- SEC는 항공 서비스업체 TurnKey Jet가 ICO를 통해 발행한 TKJ 토큰에 관하여 '비규제 조치의견서'(No-Action Letter)를 발행함
- TKJ는 '비규제 조치 의견서'를 받기까지 SEC 담당자와 50회 가량 통화하는 등 노력을 기울임
- 비규제 조치 의견서를 발행한 것은 규제의 명확성 측면에서 바람직한 일임

12

캐나다

암호화폐 규제 법률 초안 발표

암호화폐 & 거래

- 캐나다 정부가 지난 2015년~2016년 자금세탁방지국제기구를 통해서 자금세탁 및 금융테러방지관리라는이름으로 암호화폐 산업에 대한 조사 시행
- 2년 간의 조사 결과를 바탕으로 2018년 6월 초 암호화폐 거래소 및 암호화폐 결제 처리업체를 현금 서비스 사업체로 규정하고, 이들로부터 철저한 보고 체계를 갖추는 법률 초안 발표
- 업체들은 미화 약 1만 달러(한화 1073만원)를 초과하는 거래는 당국에 보고해야 하며, KYC로 고객에게 미화 약 770달러(한화 82만원)의 초기 금액 증명을 요구해야 함
- 비용편익분석을 하기 위해서 정부가 향후 10년 동안 약 4700만 달러(한화 504억원)를 투자할 계획

13

영국

글로벌 금융 혁신 네트워크GFIN 창설

암호화폐 파생 상품에 대한 거래 및 자문이 EU가 발표한 금융 정책에서 언급된 금융도구 지침 시장 II(MiFID 2)에 속함.

암호화폐 파생상품은 거래 허가를 받아야 한다고 함.

--영국 금융업무 행위감독기관(FCA, Financial Conduct Authority)

GFIN(Global Financial Innovation Network 글로벌 금융혁신 네트워크) 8월 창설됐음

- **FCA가 주도해 11개국 금융규제기관들이 협력해 만든 단체**
- **각국 금융 당국과의 밀접한 의사소통 지원 목표**
- **블록체인의 분산 원장 기술 및 인공지능 증권 ICO 자금세탁방지 등 글로벌 협력이 필요한 분야에서 가시적 성과를 낼 예정**
- **FCA를 비롯해 프랑스금융감독기관, 아부다비글로벌마켓,미국 소비자금융보호국, 두바이 금융서비스국, 건지금융서비스국, 홍콩 통화 당국, 싱가포로 통화당국, 캐나다 온타리오증권위원회 등 총 11개국이 회원으로 등록했음**
- **GFIN 회원국 중 싱가포르통화청(MAS), 홍콩통화 당국(HKMA), 아부다비글로벌마켓(ADGM) 등 일부 국가들은 DLT 기반으로 구축된 해외 송금 결제가 운영되고 있음**

14

스위스

ICO 생태계 구축 집중

- 증권형 토큰이 아니면 특별한 규제를 하지 않는 태도
- 비영리법인을 통한 ICO를 허용해 많은 ICO프로젝트가 집중됨(기부 방식으로 모금 가능하므로)

암호화폐 & 거래

- 암호화폐 비즈니스를 위한 특별한 라이선스가 필요하지 않음
- 스위스 자금 세탁방지법 (Swiss Anti-Money Laundering Act)에 따른 호의적인 대우

ICO

- 스위스 금융 시장 감독 관리 당국 (Swiss Financial Market Supervisory Authority, FINMA)이 새로운 ICO를 검토하여 허가
- AML 및 증권 규정에 집중
- 규정은 토큰의 기능 (지불형, 유틸리티형 또는 자산형/증권형 토큰)에 따르며 증권형이 아닌한 허용적 태도

시사점

- 크립토밸리로 잘 알려진 Zug/ Zurich
- 많은 ICO 프로젝트들 (특히 EU와 아시아 기반 프로젝트)이 선호하는 나라

15

독일

암호화폐 과세 가이드라인 공개

2018년 2월 27일 독일 연방 당국은 유럽사법재반소가 지난 2015년 내린 결정문을 바탕으로 암호화폐 과세 가이드라인을 공개했음

- 독일연방재무부는 독일에서 비트코인 등 암호화폐로 서비스나 물건을 사서 결제하는 경우 암호화폐를 법적인 결제 수단으로 인정했음
- 암호화폐가 결제 수단으로 쓰는 경우 별도의 과세 대상이 되지 않음
- 결제 서비스를 제공하는 지갑업체 등이 결제 수수료를 받게 된 경우 과세 대상이 됨
- 채굴을 자발적으로 행해지는 서비스로 규정하므로 암호화폐 채굴자가 블록은 생성한 보상으로 받은 암호화폐가 면세대상이 됨

16

독일

암호화폐의 영향력에 대한 정부의 입장

- 암호 토큰이 돈의 세가지 기능을 구비하지 않으므로 통화가 아니라 암호 토큰으로 여긴다.
- 암호 토큰은 일상 생활, 가치 저장고 또는 단위에서 지불 수단으로 사용되지 않는 다고 보았다.
- 암호화폐를 금융 안정성을 위협하는 것으로 보지 않지만 암호 토큰의 높은 성장률로 인해서 이 분야의 발전을 모니터 할 계획이다. 이를 통해서 향후 비트코인 선물 계약 등 제도권 상품 거래가 확립될 경우 엄격한 개입을 예고했다.
- 암호 화폐 거래 시장은 아직 규모가 작기 때문에 가격 변동성이 높고 시가총액이 급증했지만 암호화폐가 국가의 재정적 안보에 위협이 되지 않는다.

--독일 재무안정위원회(Financial Stability Committee)

암호화폐 거래 규모가 매우 작기 때문에 암호화폐가 글로벌 금융시스템에서 중요한 역할을 하지 않는다.

--독일 연방정부 대표

17

프랑스

암호화폐 정책 방향 급선회 중

암호화폐 강력 규제 ➡ **블록체인과 암호화폐 선도주자**

7월 4일 프랑스 암호화폐 규제 TF는 재정부에 제출한 보고서를 통해서 암호화폐 중요성을 강조했다

블록체인은 스타트업(창업초기기업)에게 새로운 기회를 제공할 것이다. 스타트업은 암호화폐공개(ICO)를 통해 토큰(암호화폐)을 발행함으로써 자금조달을 할 수 있다.

블록체인 혁명은 중개자 없이 '신뢰의 네트워크'를 구축해 우리 경제를 더욱 효율적으로 만들 것이다.

프랑스는 블록체인 혁명을 놓치지 않겠다. 지난해 12월 금융증권 전송에 블록체인기술 활용을 허용한 바 있다. 여기서 멈추지 않고 암호화폐 영역에서도 앞서나갈 것이다.

18

프랑스

ICO 신규 법안 정부 승인 : PACTE 법안 제26조

ICO 법안의 목적

프랑스 시장에서 ICO를 통해서 자금을 모집하고자 하는 회사가 프랑스의 관련 규칙을 준수하고 시장을 남용하지 않고 투자자를 보호해 줄 수 있으면 AMF에서 이런 회사에게 ICO를 발행할 수 있게 하는 허가를 발급함

토큰의 정의

any intangible asset representing, in a digital form, one or more rights, that can be issued, registered, kept or transferred using a shared electronic registration device through which it is possible to identify, either directly or indirectly, the owner of said asset

ICO의 법적 프레임워크가 될 법안이 프랑스 의회 소관 상임위원회에서 통과됐다
이 법은 세계의 블록체인 혁신가들을 끌어들일 수 있을 것이다
-프랑스의 브루노 르메리 재무장관

프랑스

ICO 신규 법안 정부 승인 : PACTE 법안 제26조

허가를 받을 수 있는 조건

- 토큰의 pre-sale단계 진행 전 미리 발급받아야 하지만 private sale단계 진행 후 발급받아도 됨
- 발행인의 의무 아니라 자원해서 신청하는 방식 도입 구체적인 조건은 곧 발표할 RGAMF에 포함시킴
- AMF는 백서의 내용과 정보를 리뷰하며 발행인의 다른 교류 문건과 담보를 주는 지원 문건을 모두 리뷰함

발행인의 의무

- 발행인은 프랑스에서 설립된 법인이어야 함며 조달한 자금을 감독하고 보장하는 에스크로 계좌 같은 메커니즘을 구축해야 함
- 백서에 대중에게 발행과 발행인의 정보를 포함한 유용한 정보를 포함해야 함. ICO에 대한 정보, 문건과 홍보에 관한 소통은 정확하고, 명확하고, 오도하는 의도가 없어야 함. 또한 발행의 리스크도 포함시켜야 함.

프랑스

ICO 신규 법안 정부 승인 : PACTE 법안 제26조

AMF의 권한

- AMF는 허가를 발급받은 토큰의 발행인에게 화이트 리스를 발급할 것임.
- AMF는 일반적 규정에 따라 새로운 구매나 발행을 정지시킬 수 있으며 발행에 관한 모든 홍보에 대한 소통을 중지시킬 수 있음.
  하지만 이런 권한은 이미 허가를 받은 발행인에 한하며 외국인 발행인에 적용하지 않음

비주

- 허가를 받지 않은 ICO는 금지되지 않을것임.
- 하지만 허가를 가지면 발행인은 자금 모집의 사용에 대해서 투자자에게 특정의 담보를 제공해야 함을 뜻함

대한민국

정부 발표 이슈	일시	분류	경과
가상화폐 이용 유사수신행위 처벌	2017.9.4	입법필요사항	입법 안됨
ICO 전면금지	2017.9.29	입법필요사항	입법 안됨
가상화폐 거래시 실명계좌 사용 의무화	2017.12.28	정부시행가능사항	시행됨
거래소 폐쇄를 위한 특별법 제정	2017.12.28	입법필요사항	입법 안됨
가상화폐 거래에 세금 부과	입장 없음	개인소득세 :입법필요 상속증여, 법인세 즉시 부과가능	입법 안됨

II. 각국의 블록체인 규제 요약

각국의 블록체인(암호화폐) 규제 요약

[세계 각국]

- 블록체인의 대표적 서비스인 암호화폐에 대해 관망적 자세를 취함
- 시장경제국가는 ICO를 금지하는 정책을 취하고 있지 않음
- 이용자의 디지털 자산을 보관, 거래하는 거래소는 라이센스제를 취하는 나라 많음
- 나아가, ICO와 참여자 보호를 위해 절차/지침을 가이드라인 또는 법률로 규정한 나라도 상당수
- 이용형 토큰과 증권형 토큰을 구별해 증권형 토큰에 증권법을 적용하는 나라 다수
    - 미국은 증권형 토큰을 넓게 인정해 대부분 ICO는 증권발행으로 보는 입장이나, ICO를 금지하는 것이 아니라 증권발행 절차를 따르라는 입장
    - 미국을 제외한 주요 나라는 이용형 토큰이라면 특별한 규제 없이 발행 허용

[한국]

- 암호화폐의 거래는 인정하면서 ICO를 전면 금지하는 나라는 한국 외에 없음
- ICO 금지 이외에 과세정책에 대해서도 아무런 입장을 밝히지 않는 나라도 한국 외에 없음
- 정부가 준비 중인 거래소의 AML 규제까지 실행되면 전세계에서 가장 강력한 규제국가가 될 전망

IV. 바람직한 블록체인 규제정책

블록체인의 필수요소인 암호화폐의 속성을 분류해야

암호화폐는 이미 다양한 형태로 진화, ICO를 통한 자금조달을 하지 않는 경우도 등장

1. 화폐	Bitcoin, Litecoin, Bitcoin Cash 등
2. 플랫폼	Ethereum, NEO 등
3. 핀테크	Bancor, Bancera, Crypterium 등
4. 지불	Ripple, Stellar Lumens, Request Network 등
5. 익명성	Monero, ZCash, Dash 등
6. 응용	Vechain, IOTA, Cardano 등
7. 가치교환	Steemlt, MaidSafe, iExec 등

➢ 블록체인산업 관련 법률을 제정함에 있어 통일적인 규율이 아닌, 각 암호화폐의 속성에 따라 법률상 달리 취급해야 함

➢ 증권형이 아닐 경우 발행한 암호화폐 거래를 금융통화상품으로 취급해야 할 필연성이 적음

암호화폐의 속성 및 ICO의 목적에 따른 구별

암호화폐의 속성 및 발행단계에 따른 구별 → 규제 설계에 반영

토큰의 분류	ICO	IEO	트레이드 마이닝 토큰	법적 규제
지불형	지불형/유틸리티형은 자본시장법 적용 안됨. 금융통화상품도 아님(정부 입장) 단, 비증권형이라도 블록체인 서비스 개발 자금을 공모하는 ICO는 일정한 규율 필요 • 1안) 전자금융거래법에 금융위원회가 인가할 경우 ICO를 할 수 있도록 근거와 인가제를 도입하는 방안 • 2안) 전자금융거래법에 ICO를 정의하고, 금융위원회가 정하는 고시에 따라 할 수 있도록 하는 방안(금융위원회는 시정명령 등 행정제재) • 3안) 디지털토큰에 관한 특별법 제정 / ICO를 허용 • 4안) 정부 가이드라인으로 허용하는 방안 • 5안) 기 제출 법률안처럼 금융위 인가/등록제	IEO: 개발완료된 서비스의 토큰을 판매하는 것 개발자금을 미리 공모하지 않으므로 단순한 상품 또는 이용권의 판매로서, 전자상거래법 적용	해당 없음	전자상거래법 적용
유틸리티형				
증권형	자본시장법 적용 • 1안) 전자금융거래법에 금융위원회가 인가할 경우 ICO를 할 수 있도록 근거와 인가제를 도입하는 방안 • 2안) 전자금융거래법에 ICO를 정의하고, 금융위원회가 정하는 고시에 따라 할 수 있도록 하는 방안(금융위원회는 시정명령 등 행정제재) • 3안) 디지털토큰에 관한 특별법 제정 / ICO를 허용 • 4안) 정부 가이드라인으로 허용하는 방안 • 5안) 기 제출 법률안처럼 금융위 인가/등록제	자본시장법 적용(금융위원회 발행 허가)	자금의 공모가 없으므로 증권발행 아님. 자본시장법 적용 안됨	자본시장법 적용

블록체인과 법적 이슈 동향

(규제혁신, 규제샌드박스, STO, 거래소 관련 법령 등)

정재욱 변호사
(법무법인 주원)

블록체인
법적 이슈 동향

2019. 06. 18. | 정재욱 법무법인(유한) 주원 파트너 변호사

JOOWON
법무법인(유한)주원

발제자 소개

JOOWON
법무법인(유한)주원

정재욱 법무법인(유한) 주원 파트너변호사

T. 02 6710 0342
F. 02 6710 0310
E. jwjeong@joowonlaw.com

주요 경력

법무법인(유한) 주원 파트너 변호사
대한변호사협회 IT 블록체인 특별위원회 부위원장
대한변호사협회 상임이사(교육이사)
사단법인 블록체인법학회 발기인, 학술이사
한국블록체인협회 자문위원
서울대학교 법과대학 대학원 박사과정(사회경제법 전공)
前 법무법인 세종(SHIN & KIM) 변호사
前 서울지방변호사회 상임이사(법제이사)
前 서울지방변호사회 비상임이사, 법제위원

블록체인으로 여는 미래사회 워크샵
법무법인(유한) 주원 정재욱 변호사

JOOWON 법무법인(유한)주원

CONTENTS

JOOWON 법무법인(유한)주원

I. ICO, IEO, STO 규제 동향

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

1. ICO 전면금지 방침

가. 2017년 9월 4일자 보도자료

대한민국 금융위원회, 국무조정실, 공정거래위원회, 법무부, 방송통신위원회, 국세청, 경찰청, 한국은행, 금융감독원, 인터넷진흥원 등 유관기관 담당자들로 구성된'가상통화 관계기관 합동TF'는 2017. 9. 4. 보도자료 발표

· 배경

○ 가상통화를 악용한 불법거래, 가상통화 투자를 빙자한 유사수신·다단계 등 사기범죄 발생으로 소비자 피해가 우려

○ 현 시점에서 가상통화는 화폐·통화나 금융상품으로 보기는 어려우나, 가상통화거래가 무분별하게 이루어질 경우 금융거래질서에 부정적 영향을 미칠 우려가 있기 때문에 세심한 대응이 필요

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

1. ICO 전면금지 방침

가. 2017년 9월 4일자 보도자료

· 주요 내용

(1) 관련 제재 근거의 마련

○ 가상통화 투자를 사칭한 유사수신행위에 대해 유사수신행위규제법상 근거를 명확화하고, 처벌 수준을 강화하는 등 처벌의 실효성을 높여나갈 예정

○ 가상통화의 가치를 정부·금융기관이 보장해 줄 수 없으므로 가상통화거래를 금융업으로 포섭하여 공신력을 부여하기는 어려우나, 유사수신행위규제법의 적용범위를 확대하여, 기존 유사수신행위 외 '가상통화거래행위'에 대해서도 규율체계를 마련할 예정

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

1. ICO 전면금지 방침

가. 2017년 9월 4일자 보도자료

· 주요 내용

(2) 증권발행 형식의 ICO 제재

○ 지분증권·채무증권 등 증권발행 형식으로 가상통화를 이용하여 자금조달(ICO)하는 행위에 대해서는 자본시장법 위반으로 처벌

(3) 향후 대응방향

○ 가상통화 취급업자의 성격이나 인가 문제, 과세 문제 등 국제적인 공감대가 확립되지 않은 사안에 대해서는 각국 정부, 국제기구 등의 논의·규제 동향을 보면서 면밀히 분석하고 충분한 논의를 통해 대응방안을 강구해나갈 예정

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

1. ICO 전면금지 방침

나. 2017년 9월 29일자 보도자료

합동 TF는 2017. 9. 29. 최근 국내외 시장·규제 동향에 대한 대응조치를 논의하고, 지난 9.1일 발표한 '가상통화 대응방향'의 관계기관별 추진현황을 점검하여 관련 대응방침 보도자료 배포

· 발표 배경

○ 시중자금이 비생산적·투기적인 방향으로 몰리는 현상이 나타나고 있는 데 대해 심각한 우려를 표명하고, 이에 따라 생산적 투자로 전환할 수 있도록 추가적인 조치가 불가피한 상황이라고 판단

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

1. ICO 전면금지 방침

나. 2017년 9월 29일자 보도자료

· 주요 내용

(1) ICO 전면금지 방침

○ ICO가 프로젝트에서 나오는 수익을 배분하거나 기업에 대한 일정한 권리·배당을 부여하는 방식(속칭 '증권형') 뿐만 아니라, 플랫폼에서의 신규 가상통화를 발행하는 방식(속칭 '코인형') 등 다양한 유형으로 이루어지고 있음. 이에 ICO를 앞세워 투자를 유도하는 유사수신 등 사기위험 증가, 투기수요 증가로 인한 시장과열 및 소비자피해 확대 등 부작용이 우려되는 상황

○ 기술·용어 등에 관계없이 모든 형태의 ICO를 금지할 방침

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

1. ICO 전면금지 방침

나. 2017년 9월 29일자 보도자료

· 주요 내용

(2) 관련 범죄 집중단속, 처벌 사례

○ 가상통화를 이용한 마약거래, 유사수신·다단계 사기범죄에 대한 단속을 강화하고, 각각 마약류관리법 및 유사수신행위규제법·방문판매법 위반 등으로 기소(검찰)

(3) 관련 법안 마련 계획

○ 가상통화 관련 유사수신행위 규제 명확화, 처벌 강화를 위한 유사수신행위규제법 개정안 마련(가칭 '유사수신행위 등 규제법', 금융위). '가상통화거래행위'를 규정하고, ICO·신용공여·시세조종·표시광고 등 금지행위를 명확히 규정

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

2. ICO 실태점검 실시

가. 2018년 8월, 실태점검 실시 결정

○ 가상통화 관계차관회의에서 ICO 실태점검 실시 및 그 결과를 바탕으로 대응방안을 논의하기로 결정

나. 2018년 9월 ~ 11월, 실태점검 실시

○ (점검대상) 22사 (언론.인터넷 등을 통해 확인): 국내에 있는 블록체인기술 개발회사를 대상으로 점검 실시

○ (점검방식) 서면점검: 회사의 임의 협조(일반기업 조사근거 부재)를 얻어 질문서에 대한 답변서 징구 및 백서.홍보자료(웹사이트 등) 점검

○ 질문내용(6개 부문, 52개 문항을 기초): ①회사개황, ②프로젝트 내용, ③ICO 내역, ④투자자 부여혜택(권리), ⑤국내투자자 대상 홍보내역, ⑥기타 사항

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

2. ICO 실태점검 실시

다. 2019년 1월 31일, 실태조사 결과 및 향후 대응방향 발표

(1) 실태조사 결과

○ 국내 기업은 ICO 금지 방침을 우회하여 싱가포르 등 해외에 페이퍼 컴퍼니를 설립하여 형식만 해외ICO 구조로 대부분 진행

- 해외 페이퍼 컴퍼니는 「ICO 자금모집」 이외 다른 업무는 없는 것으로 보이며, 국내기업이 개발•홍보 등 업무를 총괄 / 페이퍼컴퍼니와 국내기업간 용역 계약을 통해 이더리움 등을 현지 환전하여 송금

○ 해외에서 실시한 ICO이지만, 한글백서 및 국내홍보 등 고려시 사실상 국내 투자자를 통한 자금모집이 이뤄진 것

- ICO를 통한 자금모집은 모두 '17년 하반기 이후 진행되었고, 총 규모는 약 5,664억원, 1개사 평균 330억원 수준

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

2. ICO 실태점검 실시

다. 2019년 1월 31일, 실태조사 결과 및 향후 대응방향 발표

(1) 실태조사 결과

○ ICO 관련 중요한 투자판단 정보(회사개황, 사업내용, 재무제표 등)가 공개되어 있지 않으며, 개발진 현황 및 프로필 또한 미기재 또는 허위 기재 우려

○ ICO를 통해 계획한 프로젝트는 금융, 지불·결제, 게임 등이 있었으나, 실제 서비스를 실시한 회사는 없었으며 사전테스트 단계 또는 플랫폼 개발 중인 상황으로 확인

○ 모든 신규 가상통화 가격이 하락, 이에 따른 피해 또한 우려되는 상황

○ P2P대출 유동화 토큰 발행·거래, 가상통화 투자펀드 판매 등 자본시장법상 무인가 영업행위, 중요사항을 과다하게 부풀려 광고하는 사기죄 등 법 위반 소지가 있는 사례

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

2. ICO 실태점검 실시

다. 2019년 1월 31일, 실태조사 결과 및 향후 대응방향 발표

(2) 대응 방향

○ ICO에 대한 투자 위험이 높고 국제적 규율체계도 확립되어 있지 않은 상황임을 감안하여 정부는 ICO 제도화에 대한 신중한 입장을 견지

○ 정부가 ICO 가이드라인 등을 제시하는 경우 투자 위험이 높은 ICO를 정부가 공인한 것으로 이해될 수 있어 투기과열 현상 재발과 투자자 피해가 확산될 우려

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

3. 최근 정부 방침

2019년 5월 28일, 가상통화 관련 관계부처 회의 결과 발표

아래와 같은 기존 입장 재확인

○ 가상통화는 법정화폐가 아니며 어느 누구도 가치를 보장하지 않기 때문에 불법행위•투기적 수요, 국내외 규제환경 변화 등에 따라 가격이 큰 폭으로 변동하여 큰 손실이 발생할 수 있다는 점에서, 가상통화 투자 등 일련의 행위는 자기책임하에 신중하게 결정할 필요가 있음을 다시 한번 강조

○ ICO(Initial Coin Offering) 조사결과('19.1) 및 국제동향 등을 고려하여 자금세탁방지 등을 위해 국회에 계류되어 있는 「특정금융정보법」 개정안이 조속히 통과되기를 바라며, 이를 위해 정부도 최대한 노력

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

4. 검토

나. ICO, IEO, STO 금지 조치의 법적 근거

(1) ICO, IEO의 경우

○ 현재까지도 유사수신행위의 규제에 관한 법률이 개정되거나, 관련 특별법이 제정된 바는 없음.

○ ICO를 명시적으로 금지하는 법령이 없기 때문에 ICO를 한다는 것 그 자체만으로 어떠한 형사처벌을 받지는 않음(죄형법정주의)

○ 그러나 ICO의 구체적인 목적, 구조, 절차, 방식 등에 따라 형법, 자본시장 및 금융투자업에 관한 법률(이하 '자본시장법'), 유사수신행위규제법 등 현행법령이 적용될 여지

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

4. 검토

가. IEO, STO의 등장

(1) IEO

○ Initial Exchange Offering의 약자로 통상 프로젝트 팀이 암호화폐를 발행할 때(또는 발행 직전 단계에서) 암호화폐 거래소와 위탁판매계약을 체결한 후 거래소가 암호화폐를 대신 판매해 주는 것을 의미. 암호화폐 거래소에서 해당 암호화폐를 매수한 후 이를 직접 투자자에게 판매하는 경우도 있음

(2) STO

○ 증권발행 형식의 ICO를 의미하며 Security Token Offering의 약자임. 증권형 토큰(Security Token)이란 블록체인을 기반으로 부동산, 천연자원, 콘텐츠 등의 자산을 토큰으로 유동화하고 프로젝트의 성공 여부에 따라 투자자에게 그 수익을 배분하는 토큰이나 지분권 등을 말함

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

4. 검토

나. ICO, IEO, STO 금지 조치의 법적 근거

(2) STO의 경우

○ STO와 관련하여서는 자본시장법이 적용될 수 있을 것

○ 다만, STO에 대하여 자본시장법이 적용될 수는 있겠지만, STO가 자본시장법에 따라 금지된다고 볼 수 있는지 의문

- 현행 자본시장법은 정부로 하여금 개별 증권의 발행과정을 모두 심사하여 해당 증권의 가치를 정부가 심사하도록 하고 있지 않고, 단지 발행자로 하여금 증권에 대한 정보를 제대로 공시하도록 함으로써 투자자가 본인의 책임 하에 해당 증권의 가치를 판단하도록 유도

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

I. ICO, IEO, STO 규제 동향

JOOWON 법무법인(유한)주원

4. 검토

나. ICO, IEO, STO 금지 조치의 법적 근거

(2) STO의 경우

- 일반 공모: 발행인이 50명 이상의 투자자에게 청약을 권유해 증권을 모집할 경우 모집가액 또는 매출가액 각각의 총액이 10억원 이상일 때는 금융위원회에 증권신고서 및 투자설명서 등 27종의 서식을 금융위원회에 제출, 비치해야 하는 등 규정이 엄격

- 소액 공모: 단 10억원 미만의 소액공모의 경우에는 증권신고서 제출 대신 소액공모공시서류를 제출하면 됨. 현행법상으로는 10억이 기준이나 2018년 11월 정부 발표에 따르면 소액공모 상한을 10억원에서 30억원으로 늘릴 예정

- 크라운드 펀딩: 한편 온라인소액투자중개업의 요건에 부합해 크라우드펀딩으로 증권을 발행할 수도 있음(조달 한도는 7억원 이하였으나 최근 15억원으로 확대)

○ 단, 실제 추진 가능하기 위해서는 정부의 창구규제가 개선되어야

JOOWON 법무법인(유한)주원

II. 암호화폐 거래소 규제 동향

II. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

1. 2017년 규제 동향

가. 2017년 9월 4일자 보도자료

○ 가상통화의 국내거래에 대해서도 주요국의 자금세탁방지 규제강화 추세 등을 감안하여 규제도입을 추진할 계획(특금법 개정)

○ 가상통화 취급업자에 맡긴 고객자산의 별도 예치 등 소비자보호 사항을 취급업자가 마련할 자율규제안에 반영토록 권고 추진

II. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

1. 2017년 규제 동향

나. 2017년 9월 29일자 보도자료

(1) 신용공여 금지

○ 소비자가 가상통화 취급업자로부터 매매자금 또는 가상통화를 빌려 매매(속칭 '코인 마진거래')하는 등 사실상 신용공여행위가 이루어지고 있거나 준비중

○ 가상통화 취급업자의 신용공여행위를 허용하지 않을 방침. 규제입법 이전에 가상통화 취급업자의 신용공여 현황 및 대부업법 등 관련법 위반 여부를 조사하고, 위반시 엄정 제재할 계획

(2) 고객정보 유출사고 조사, 제재

○ 신고된 가상통화 취급업자의 고객정보 유출사고에 대해 조사중이며, 조사결과에 따라 법 위반사항에 대해서는 엄정 제재(정보통신망법)

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

1. 2017년 규제 동향

나. 2017년 9월 29일자 보도자료

(3) 이용자 확인

○ 은행 가상계좌를 통한 이용자 본인확인 프로세스 관련 의견 수렴

○ 이용자 본인계좌에서만 입·출금 가능하도록 통제, 이용자 1인 1가상계좌 부여 원칙 적용, 은행의 가상통화취급업자 실사기준 마련 등

(4) 자금세탁방지

○ 은행권을 통해 가상통화 취급업자의 계좌개설·고객확인 현황 및 의심거래 유형을 추가로 파악하고(금융위), 은행권에 고객확인·의심거래보고를 강화하도록 지도(공문시행, 9.28일)

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

2. 가상통화 투기근절을 위한 특별대책

2017년 12월 28일, 특별대책 발표

정부는 2017. 12. 28. 관계부처(기획재정부, 법무부, 금융위원회, 과학기술정보통신부, 공정거래위원회, 방송통신위원회 등) 차관회의를 개최하여, 가상통화 투기를 근절하기 위한 특별대책 발표

(1) 가상통화 거래 실명제 실시

○ 가상통화 거래소에 대한 은행의 가상계좌 신규발급이 즉시 전면 중단

○ 세부방안이 마련되는 대로 기존 가상계좌 거래소의 신규회원에 대한 가상계좌 제공이 중단되고, 기존 가상계좌의 이용자 역시 실명인증을 거친 본인의 거래 은행으로만 입출금을 할 수 있도록 계좌이전 작업 진행

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

2. 가상통화 투기근절을 위한 특별대책

2017년 12월 28일, 특별대책 발표

(2) 가상통화 거래소에 대한 은행의 자금세탁방지 의무 강화

○ 가상통화 거래소의 실명거래방식이 확립되기 전까지, 은행이 거래소를 식별하고 특별히 관리할 수 있도록 고객확인의무(CDD)와 의심거래보고의무(STR)를 강화하여 이행

○ 가상통화 거래소의 거래가 의심거래로 보고되는 경우 금융거래정보분석원(FIU)은 이를 집중분석하여 자금원천이 불분명하거나 자금세탁이 의심되는 경우 국세청 등 법집행기관에 적극적으로 자료를 제공할 예정

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

2. 가상통화 투기근절을 위한 특별대책

2017년 12월 28일, 특별대책 발표

(3) 공정거래위원회 불공정약관 조사

○ 공정거래위원회는 주요 가상통화 거래소 4개 업체(빗썸, 코인원, 코빗 및 코인플러그)의 약관을 중심으로 불공정약관사용여부를 조사 중

○ 향후 조사 가능한 모든 가상통화 거래소를 대상으로 직권조사를 확대 실시하여, 불공정 약관에 대해서는 시정명령·과태료 등 관련 법 규정에 따라 엄격히 조치할 예정

(4) 가상통화 거래소 폐쇄 검토

○ '가상통화 거래소 폐쇄를 위한 특별법' 제정을 통한, 가상통화 거래소의 폐쇄 검토

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

3. 가상통화 관련 자금세탁방지 가이드라인

2018년 1월 23일, 자금세탁방지 가이드라인 시행

○ 가이드라인은 가상통화 관련 금융거래에 관하여

①「특정 금융거래보고 및 이용 등에 관한 법률」(이하 '특금법')과 그 하위법령의 시행에 필요한 사항을 명확히 하고

②자금세탁 및 공중협박자금 조달 행위(이하 '자금세탁등')를 효과적으로 방지하기 위해 금융회사등의 준수가 필요한 사항을 규정

○ 금융회사 등에 적용되는 것으로 암호화폐 거래소를 직접적으로 규율하는 가이드라인은 아님

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

3. 가상통화 관련 자금세탁방지 가이드라인

2018년 1월 23일, 자금세탁방지 가이드라인 시행

(1) 금융회사등은 고객이 취급업소 인지 여부를 식별하기 위한 절차를 운영

(2) 취급업소로 인식한 경우 일정한 조치

(고객확인 강화) 금융회사등은 취급업소를 자금세탁등의 위험이 높은 고객으로 고려하여 취급업소에 대해 업무규정이 열거한 추가적 확인사항(업무규정 제42조제2항.제3항)과 다음 각 호의 정보를 확인

1. 취급업소가 제공하는 서비스의 내용 / 2. 취급업소의 실명확인 입출금계정서비스 이용여부 및 이용계획 등 (이하 생략)

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

3. 가상통화 관련 자금세탁방지 가이드라인

2018년 1월 23일, 자금세탁방지 가이드라인 시행

(취급업소가 법인·단체 또는 개인의 계좌[실명확인 입출금계정서비스를 이용하지 않는 경우]를 통해 가상통화관련 금융거래를 하는 경우) 금융회사등은 자금세탁등을 효과적으로 방지하기 위하여 다음 각 호의 사항을 이행

1. 취급업소의 임직원 계좌가 가상통화관련 금융거래에 활용되는 것으로 의심되는 경우 임직원 명의 계좌에 대한 강화된 고객확인 및 금융거래모니터링 강화

2. 금융회사등의 고객 중 민법상 미성년자, 외국인 등의 가상통화관련 금융거래를 식별

3. 금융회사등은 취급업소 이용자의 금융거래내역 관리를 대행하거나 실시간 관리가 가능하도록 하는 등 취급업소의 가상통화관련 금융거래내역 관리에 편의성을 제공하는 용역 행위를 자제

4. 기타 금융회사등에서 자금세탁등의 방지를 위해 필요하다고 인정되는 사항

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅱ. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

3. 가상통화 관련 자금세탁방지 가이드라인

2018년 4월, 은행권 현장 점검

금융정보분석원·금융감독원은 동 가이드라인의 이행실태를 점검하기 위해 3개 은행에 대한 현장점검(농협, 국민, 하나은행)을 실시(4.19~25일)

2018년 7월 10일, 가이드라인의 개정

(1) 비집금계좌에 대한 모니터링 강화

금융회사는 취급업소의 '비집금계좌'의 거래에 대해서도 모니터링을 강화하고, 이상거래가 발견되는 경우 취급업소에 대해 '강화된 고객확인'을 실시

(2) 해외 가상통화 취급업소 목록 공유

(3) 거래거절 시점 명시 및 거래거절 사유 추가

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

II. 암호화폐 거래소 규제 동향

JOOWON 법무법인(유한)주원

4. 검토

직접적인 규율의 부재

○ 뚜렷한 법적 규제나 규율도 없는 상황. 시세조종, 봇거래, 자전거래 등이 빈번하게 발생. 기본적으로 암호화폐 시장의 폐쇄성, 정보의 비대칭으로 인해 발생하는 문제

○ 거래소가 직간접적으로 시세조종을 하거나 거래량 부풀리기를 했을 경우에는 사후적으로 사기 등을 문제 삼고 민, 형사 소송을 제기하여 손해를 보전 받을 수도 있겠지만, 실제로 이를 실현하기 위해서는 많은 시간과 비용 소요

○ 암호화폐 시세조종, 내부자거래에 대해 현행 자본시장법을 적용하기는 어려운 측면

자금세탁 방지 가이드라인 자체의 문제

○ 규율체계의 문제

○ 실제 관련 분쟁 사례 발생(입금정지조치금지가처분 사례)

JOOWON 법무법인(유한)주원

III. 크립토 펀드 및 외국환 관련 법적 이슈

III. 크립토 펀드 및 외국환 관련 법적 이슈

JOOWON 법무법인(유한)주원

1. 크립토 펀드 관련 법적 이슈

자본시장법의 적용 가능성

○ 암호화폐의 재산적 가치 인정

수원지방법원 2018. 1. 30. 선고 2017노7120 판결 / 대법원 2018. 5. 30. 선고 2018도 3619 판결

"비트코인은 재산적 가치가 있는 무형의 재산이라고 보아야 한다. 그 이유는 다음과 같다. ① 비트코인은 경제적인 가치를 디지털로 표상하여 전자적으로 이전, 저장 및 거래가 가능하도록 한, 이른바 '가상화폐'의 일종이다. ② 피고인은 음란물유포 인터넷사이트인 "○○○○○○○.com"(이하 '이 사건 음란사이트'라 한다)을 운영하면서 사진과 영상을 이용하는 이용자 및 이 사건 음란사이트에 광고를 원하는 광고주들로부터 비트코인을 대가로 지급받아 재산적 가치가 있는 것으로 취급"

JOOWON 법무법인(유한)주원

III. 크립토 펀드 및 외국환 관련 법적 이슈

1. 크립토 펀드 관련 법적 이슈

자본시장법의 적용 가능성

○ 자본시장법상의 규정

- 집합투자: 2인 이상의 투자자로부터 모은 금전등을 투자자로부터 일상적인 운용지시를 받지 아니하면서 재산적 가치가 있는 투자대상자산을 취득·처분, 그 밖의 방법으로 운용하고 그 결과를 투자자에게 배분하여 귀속시키는 것(자본시장법 제6조 제5항)

- 금전등: 금전, 그 밖의 재산적 가치가 있는 것(자본시장법 제3조)

Ⅲ. 크립토 펀드 및 외국환 관련 법적 이슈

JOOWON 법무법인(유한)주원

1. 크립토 펀드 관련 법적 이슈

실제 사례와 정부의 방침

○ 실제 사례

○ 정부의 방침: 2018년 10월 24일자 보도자료

- 일명 "가상통화펀드"는 집합투자업의 외형구조를 갖추고 펀드라는 명칭을 사용하고 있어 일반투자자들이 자본시장법상 적법하게 설정된 펀드로 오인할 소지가 있으나

- "가상통화펀드"는 금융감독원에 등록된 사실이 없고, 홈페이지에 게시하고 있는 투자설명서는 금융감독원의 심사를 받은 사실이 없으며 해당 운용사·판매회사·수탁회사 등은 금융위원회의 인가를 받은 사실이 전혀 없음

- "가상통화펀드"는 자본시장법 위반소지가 있는 만큼, 투자자들은 자본시장법상 투자자보호를 위한 각종 제도가 적용되지 않는 점을 충분히 인식하고, 투자에 각별히 유의할 필요

Ⅲ. 크립토 펀드 및 외국환 관련 법적 이슈

JOOWON 법무법인(유한)주원

2. 외국환 관련 법적 이슈

암호화폐 이용한 환치기, 재정거래 등에 대한 처벌

○ 법원의 태도

- 외국환거래법 제3조에서는 대한민국과 외국간의 지급, 추심 및 수령을 외국환업무라 규정하고 있을 뿐 외국환업무가 지급수단에 의해야 한다고 규정하고 있지는 않음.

- 비트코인은 피고인이 외국환거래법위반죄를 회피 하기 위한 수단으로 사용된 것일 뿐 환전의뢰인이 비트코인을 보유할 목적이나 비트코인의 시세 차익을 얻을 목적으로 피고인에게 비트코인 매매를 중개한 것으로 보이지는 않음

- 해외 비트코인 거래소로부터 국내 비트코인 거래소로 비트코인을 전송받는 행위 자체는 외국환거래법 상 외국환 업무에 해당하지 않는다고 볼 여지

- 그러나 피고인이 국내 비트코인 거래소에서 비트코인을 한화로 매도한 후 그 대금을 환전의뢰인이 지정한 계좌로 송금하는 행위는 외국환거래법상 외국환 업무에 해당

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅲ. 크립토 펀드 및 외국환 관련 법적 이슈

JOOWON 법무법인(유한)주원

3. 검토

모호한 규제가 범죄자를 양산할 우려

(1) 크립토 펀드 관련

○ 암호화폐, 펀드 투자자산으로 편입 불가능한지 의문

○ 요건 갖추어 인가, 등록 신청시 받아들일지 여부

(2) 외국환 관련

○ 소액해외송금업체들이 해외송금의 수단으로 암호화폐를 활용할 수 있도록 허용해야 (불허할 법적 근거는 무엇인지)

○ 암호화폐 거래가 외국환거래법 적용대상인지 불분명한 측면

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

JOOWON 법무법인(유한)주원

Ⅳ. 규제 샌드박스와 블록체인 비지니스

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅳ. 규제 샌드박스와 블록체인 비지니스

JOOWON 법무법인(유한)주원

1. 규제 샌드박스 제도의 체계

정부는 2018년 9월경 이른바 '규제 샌드박스 5법 ' 을 국회에 제안

법령명	소관부처	제·개정	추진현황
정보통신 진흥 및 융합 활성화 등에 관한 특별법	과학기술정보통신부	일부개정	'18. 10. 16. 공포 '19. 1. 17. 시행
산업융합촉진법	산업통상자원부	일부개정	'18. 10. 16. 공포 '19. 1. 17. 시행
지역특화발전특구에 대한 규제특례법	중소벤처기업부	일부개정	'18. 10. 16. 공포 '19. 4. 17. 시행
금융혁신지원 특별법	금융위원회	제정	'18. 12. 31. 공포 '19. 4. 1. 시행
행정규제기본법	국무조정실	일부개정	18. 4. 17. 개정 18. 10. 18 시행

○ 정확히는 '규제 샌드박스 법 4 + 1'로, 행정규제기본법은 규제 샌드박스를 총괄하는 법률로서의 지위

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅳ. 규제 샌드박스와 블록체인 비지니스

JOOWON 법무법인(유한)주원

2. 규제 샌드박스 제도와 블록체인 비지니스

금융 규제 샌드박스: 블록체인 관련 혁신금융서비스 지정

(1) '개인투자자간 주식대차 플랫폼'

○ 블록체인 기반의 주식대차 거래 플랫폼을 통해 개인투자자에게 자유로운 주식대여와 차입기회를 제공

- 개인투자자가 보유하고 있는 주식을 일정기간 빌려주고 이에 대한 대여이자(수수료)를 받는 한편, 해당 주식을 빌려간 또 다른 개인투자자는 기관투자자처럼 공매도를 이용한 투자 전략을 펼칠 수 있도록 하는 것

○ 자본시장법에서 정하는 금융투자업자로서 인가를 받지 않더라도 증권대차의 중개업무를 허용하는 것으로 규제 특례를 허용함(자본시장법 제11조, 제40조 관련)

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅳ. 규제 샌드박스와 블록체인 비지니스

JOOWON 법무법인(유한)주원

2. 규제 샌드박스 제도와 블록체인 비지니스

해외송금 비즈니스, ICT 융합 규제 샌드박스

○ A 소액해외송금업체, 블록체인 기반 해외송금서비스

- ICT 융합 규제샌드박스가 사전 신청을 받기 시작한 첫날인 2019. 1. 17. 곧바로 임시허가와 실증특례를 신청

- 임시허가: 신기술·서비스에 대한 근거법령이 없거나 명확하지 않은 경우 신속한 사업화가 가능하도록 임시로 허가
- 실증규제특례: 신기술·서비스가 규제로 인해 사업 시행이 불가능한 경우, 규제를 적용하지 않고 실험·검증을 임시로 허용

- 현재까지 3차례에 걸친 신기술·서비스 심의위원회가 개최되었는데(1차는 2019. 2. 14., 2차는 2019. 3. 6., 3차는 2019. 5. 9. 각 개최됨), A 업체의 경우는 기획재정부와 법무부의 '투기 조장' 우려로 인하여 현재까지 진행된 심의에서 모두 제외

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅳ. 규제 샌드박스와 블록체인 비지니스

JOOWON 법무법인(유한)주원

2. 규제 샌드박스 제도와 블록체인 비지니스

금융 규제 샌드박스: 블록체인 관련 혁신금융서비스 지정

(2) '디지털 부동산 수익증권 유통 플랫폼'

○ 부동산 유동화 수익증권을 블록체인 기반의 디지털 방식으로 일반 투자자에게 발행·유통하는 서비스

- 부동산 소유자가 신탁회사와 신탁 계약을 맺으면 신탁회사는 수익증권을 공모·발행, 이때 발행한 수익 증권 원본을 신탁회사가 보관하고, 투자자는 수익증권에 대한 반환청구권을 표시한 전자증서를 받게 되며 투자자는 B사 플랫폼에서 다자간 매매체결 방식으로 전자증서를 거래한다는 취지의 서비스

○ 금융위원회 ① 부동산 신탁 계약에 의한 수익증권 발행 허용(자본시장법 제110조 제1항), ② 플랫폼 개설을 위한 거래소 허가 규정에 대한 예외 인정(자본시장법 제373조), ③ 증권거래 중개를 위한 투자중개업 인가에 대한 예외를 인정 방향으로 규제 특례 허용

블록체인으로 여는 미래사회 워크샵
법무법인(유한)주원 정재욱 변호사

Ⅳ. 규제 샌드박스와 블록체인 비지니스

JOOWON 법무법인(유한)주원

2. 규제 샌드박스 제도와 블록체인 비지니스

금융 규제 샌드박스: 블록체인 관련 혁신금융서비스 지정

(3) '비상장기업 주주명부 및 거래활성화 플랫폼'

○ 비상장 초기 혁신·중소기업의 주주명부 관리 및 장외 거래 편의성 제고를 위한 서비스

- 현재 비상장 기업은 PC, 엑셀 등 수기 작업으로 주주명부를 관리하고 비상장 주식의 장외 거래는 불투명한 1:1 거래 외에는 별다른 방법이 없는데, 블록체인을 활용하여 주주명부의 변동을 실시간으로 확인할 수 있도록 하고, 블록체인을 통해 장외 1:1 거래를 지원한다는 취지의 서비스

○ 자본시장법상 투자중개업 인가의 예외를 인정해주는 내용으로 규제특례를 허용

JOOWON 법무법인(유한)주원

Ⅴ. 검토 및 제언

Ⅴ. 검토 및 제언

JOOWON 법무법인(유한)주원

블록체인, 암호화폐에 대한 규제의 필요성

규제의 공백으로 인한 부작용

○ 암호화폐 열풍이 다소 주춤해졌다고는 하나 시장에서는 여전히 많은 자금이 IEO, 거래소 등에 모이고 있고, 암호화폐 관련 사기, 다단계, 유사수신 범죄의 발생도 심각한 수준

- 금융감독원에 의하면 지난해 수사가 의뢰된 유사수신 139건 중 44건(31.7%)이 암호화폐 관련 유형

○ 규제의 공백, 모호함은 한편으로는 제대로 사업을 해보려는 기업의 앞날을 가로막고 있고, 다른 한편으로는 관련 범죄의 양산을 방치

Ⅴ. 검토 및 제언

JOOWON 법무법인(유한)주원

블록체인, 암호화폐에 대한 규제의 필요성

사업자는 해외로 떠나고, 국내 투자자들은 위험에 노출

○ ICO(IEO, STO포함)라는 새로운 자금모집수단을 활용하여 제대로 사업을 해보려는 사업자들은 해외로 내몰리고 있음

○ 반대로 ICO를 빙자한 사기, 다단계, 유사수신 범죄가 기승을 부리고 있음에도 불구하고, 사후 처벌만 이루어질 뿐 사전 예방 조치는 전혀 이루어지지 않고 있음

- 사전에 국민, 투자자에게 제대로 된 투자 정보를 제공하게 ICO 기업에게 강제하거나, 일정한 요건을 충족한 기업만 ICO를 하게 할 수 있음에도 불구하고 이러한 조치는 전혀 이루어지지 않고 있음

- 정보의 비대칭 문제로 인하여 일반 국민 내지 투자자 입장에서는 어떠한 ICO, IEO, STO가 제대로 된 것인지 판별하게 어려운 위치에 놓여져 있음.

Ⅴ. 검토 및 제언

JOOWON 법무법인(유한)주원

블록체인, 암호화폐에 대한 규제의 필요성

방치는 해법이 될 수 없어

○ 암호화폐 거래소와 관련하여서도 해킹, 오입금 등의 사고가 빈번하게 발생하고 있고, 그 피해액수가 상당함에도 불구하고, 정부 차원에서의 관리 조치는 유명무실한 상황

○ 블록체인, 암호화폐를 활용한 해외송금, 해외결제 서비스의 경우 기존의 은행의 swift 망, PG사 등을 통하는 것에 비하여 혁신적 요소. 규제의 불분명함, 정부의 금지 방침 등으로 인하여 시장에 제대로 출시되지 못하고 있거나 출시되어도 취소 빈번

○ 암호화폐 시장 규모가 축소되고 국민적 관심이 줄어들었기 때문에 더 이상 어떤 조치가 필요하지 않다고 보는 시각도 다수. 암호화폐 거래 내지 거래소의 방치가 블록체인 산업의 발전을 가로막는 것은 차치하더라도 다수의 피해자들을 양산해 왔던 것은 아닌지, 혁신적 사고를 바탕으로 새로운 서비스를 제공하려는 건전한 사업자 마저 잠재적 범죄자로 만들어 버리거나, 해외로 내몰았던 것이 아닌지 되돌아볼 필요

국내외 블록체인 법제화 및 사법 시스템 이슈

김경환 변호사
(법무법인 민후)

국내·외 블록체인 법제화 및 사법 시스템 이슈

-국외(일본) 법제화 동향을 중심으로-

김경환 대표변호사

법무법인 민후

Contents

법무법인 민후

1.개괄

법무법인 민후

개괄

법무법인 민후

① 블록체인에 대한 규제 입법은 없고, 진흥 입법은 많이 발견됨

② 다만 미국의 일부 주는, 블록체인 기록에 대한 증거능력 인정이나 문서 · 주주명부 등으로서의 법적 효력 인정 등에 대한 입법을 한 적이 있음

③ 암호화폐나 ICO에 대하여는 몰타, 일본 등 입법이 몇 가지 발견되며, 많은 나라에서는 가이드라인을 발표하였음

④ 본 발표에서는, 우리나라와 법체계가 가장 유사한 일본 사례를 설명하고 이를 근거로 우리나라의 법제도 방향을 제시하고자 함

2.일본의 법제도

법무법인 민후

자금결제법

법무법인 민후

❖ 2017. 4. 시행, 하위법령으로는 '내각법령', '사무지침'이 있음

❖ 배경 : 2014년 세계 최대의 거래소였던, MTGOX 해킹 및 파산을 계기로 자금결제법이 제정

1) 가상통화의 정의(2조5항)

- 물품을 구입 혹은 임차 또는 용역의 제공을 받는 경우에 그 대가의 변제를 위해 불특정인에게 사용할 수 있으며, 또한 불특정인을 상대방으로 구입 및 판매할 수 있는 재산적 가치(전자 기타의 물건에 전자적 방법으로 기록된 것에 한하며, 본방 통화와 외국 통화 및 통화 건설 자산을 제외)이며, 전자 정보 처리 조직을 이용하여 이전 할 수 있는 것
- 불특정인을 상대방으로 전 호와 상호 교환할 수 있는 재산적 가치이며, 전자 정보 처리 조직을 이용하여 이전 할 수 있는 것

* ① 불특정성, ② 재산적 가치, ③ 전자적 기록, ④ 비법정통화 / ① 교환가능성, ② 전자적기록

* 가상통화를 '물건'으로 취급하면 8%의 소비세가 붙지만, 자금결제법에 따르면 '지급수단'으로 보기 때문에 2017. 7.부터 소비세가 부과되지 않음

자금결제법

법무법인 민후

2) 가상통화교환사업(2조7항) : 아래 업무를 '업으로' 하는 경우

- ① 가상통화의 매매 또는 다른 가상통화의 교환 {판매소, 교환소 등}
- ②① 행위의 매개, 중개 또는 대리 {거래소 등}
- ③①, ② 행위에 대하여 이용자의 금전 또는 가상통화 관리 {단순한 보관업무는 제외}

* 가상통화의 매매 등을 실시하지 않고, 이용자의 가상통화를 관리하여 지시에 따라 이용자가 지정하는 주소에 가상통화를 이전하는 '가상통화 수탁업무'는 적용대상이 아님

* 자금결제법상 '가상통화'를 ICO하는 경우는 가상통화교환사업의 등록을 마쳐야 함. 다만 거래소에 ICO를 위탁하는 경우 즉 IEO는 등록이 없이도 ICO가 가능하다고 보고 있음

자금결제법

법무법인 민후

3) 등록제

- 내각총리 대신에 대한 등록 필수(63조의2)
- 외국법에 의하여 등록한 업자로도 일본에서 다시 등록을 해야 함(63조의22)
- 등록요건(63조의5) : 1,000만엔(한화 약 1억원)의 최저자본금 + 순자산액이 마이너스가 아닐 것
- 2019. 4. 현재 19개의 업체가 등록되어 있음

4) 등록업자의 재무규제

- 외부감사 실시 의무화(63조의14)

자금결제법

법무법인 민후

5) 등록업자의 행위규제

- 명의대여 금지(63조의7)
- 정보의 안전관리(63조의8)
  * 전사적인 리스크 관리, 사이버보안 대책 수립, 독립 감사 부서의 감사, 장애발생시 대응방안수립 등
- 위탁처에 대한 지도(63조의9)
- 이용자보호(오인방지 등을 위한 설명 및 정보제공 의무, 63조의10)
  * 내각부령 : 취급 가상통화는 법정통화가 아님, 취급 가상통화 가치의 변동을 직접적인 원인으로 손실이 발생할 우려가 있는 때에는 그 취지 및 이유, 불만처리 연락처 등
- 이용자 재산의 분별 · 관리의무(63조의11)
  * 법률 : 이용자의 금전 또는 가상통화를 등록업자의 금전 또는 가상통화와 분별 · 관리해야 함, 공탁 · 신탁을 맡길 의무는 없음. 위반시 2년 이하 징역 등 제재
  * 다만 일본 금융심의회는 가상통화의 공탁이나 신탁에 대하여 부정적 견해를 밝힌 바 있음
  * 내각부령 : 이용자끼리는 '장부상' 이용자마다 구분 관리하되, 개별적으로 주소를 부여하고 관리할 필요는 없음. 분별 · 관리 상황에 대한 외부 감사 의무화

자금결제법

법무법인 민후

6) 등록업자에 대한 감독규제

- 장부 서류의 작성 보관 의무 (자금결제법 63조의13)
- 보고서 제출 의무 (법 63조의14)
- 현장 검사 등 (동법 63조의15)
- 업무 개선 명령 (동법 63조의16)
- 등록 취소 등 (동법 63조의17)
- 등록 말소 (동법 63조의18)
- 감독 처분의 공고 (동법 63조의19)
- 폐지의 신고 등 (동법 63조의20)

범죄수익의 이전방지에 관한 법률(or 마네론 규제법)

법무법인 민후

가상화폐교환업자는 범수법상 '특정사업자'에 해당하므로 다음의 의무를 부담함(2조2항31호)

① : 계좌 개설시 거래시 확인 의무 (犯収法 4조)

② : 확인 기록 · 거래 기록 등의 작성 · 보존 의무 (동법 6조, 7조)

③ : 혐의 거래 신고 의무 (법 8조)

④ : 내부 관리 체제의 정비 (직원 교육, 총괄 관리자의 선임 위험 평가서의 작성, 감사 등) (동법 11조)

3.일본 법원의 판결

법무법인 민후

도쿄지법 2015. 8. 5. 판결

법무법인 민후

[사안의 개요]

파산회사(주식회사 MTGOX)가 운영하는 비트코인 거래소를 이용하고 있던 고객(원고)가 파산관재인(피고)에 대해 피고가 점유하고 있는 원고의 비트코인의 인도 등을 요구한 사안

[판결]

비트 코인은 "디지털 통화" 또는 "암호학적 통화'라고되어 있으며, 그 구조나 기술은 독점적으로 인터넷 네트워크를 이용한 것으로서 비트코인은 공간의 일부를 차지하는 것이라고 볼 수 없다.

비트코인 주소의 비트코인의 잔량은 블록체인에 기록되어 있는 이 주소와 관계 비트코인의 모든 거래를 차감 계산한 결과 산출되는 수량이며, 해당 비트코인 주소에 잔량에 해당하는 비트코인 자체를 표상하는 전자적 기록은 존재하지 않는다. 위와 같은 비트코인의 구조 등에 비추어 보면, 원고가 비트코인을 독점적으로 지배하는 것으로는 인정되지 않는다.

[시사점]

비트코인 등 가상통화는 소유권의 대상이 되지 않는다는 판결임
{소유권 이외 채권자 권리까지 부정한 것은 아님에 유의}

요코하마 지방법원 2019. 3. 27. 판결

법무법인 민후

[사안의 개요]

마이닝 스크립트('코인하이부')가 구현된 사이트를 방문하면 방문자의 PC의 시스템 전력의 일부가 자동으로 가상 통화 MONERO(모네로) 마이닝에 필요한 계산을 제공하고, 마이닝에서 얻은 보상의 일부는 사이트 운영자 측에 지불됨

[판결]

이 스크립트는 잘못된 지령을 주는 프로그램에는 해당하지 않는바, 컴퓨터 바이러스로 볼 수 없기 때문에 무죄를 선고함

4.자금결제법 · 금융상품거래법 · 금융상품판매법 개정안

법무법인 민후

자금결제법 · 금융상품거래법 · 금융상품판매법 개정안

법무법인 민후

- ❖ 배경 : 가상통화 유출 사안이 많이 발생함, 가상통화가 결제수단으로 사용되는 것보다 투기거래에 이용되는 경우가 많아짐
- ❖ 3. 15. 정부가 2018. 3. 금융기관을 중심으로 만들어진 '가상화폐교환사업 등에 관한 연구회'의 논의 결과를 바탕으로, 가상통화를 암호화자산으로 명칭을 변경하는 등의 '정보통신 기술의 진전에 따른 금융거래의 다양화에 대응하기 위한 자금결제에 관한 법률 등의 일부를 개정하는 법률안'을 의결하고 중의원에 제출함
- ❖ 중의원이 5. 21. 개정안을 가결함
- ❖ 참의원이 원인으로 접수받아 심의를 개시하였고, 순조롭게 진행된다면 2020. 6.경 시행 예정임
- ❖ 개정대상 : 자금결제법, 금융상품거래법, 금융상품판매법

자금결제법 · 금융상품거래법 · 금융상품판매법 개정안

법무법인 민후

1) FAFT 등의 국제동향을 감안하고 가상통화가 법정통화로 오인될 염려가 있기에, 법령상의 '가상통화'의 명칭을 '암호화자산'으로 변경하였음(자금결제법안 2조5항)
2) 핫지갑(온라인)에서 관리되던 암호화자산의 유출이 잇따르자, 업자의 암호화자산 분별 관리 의무를 강화하여 업무의 원활한 수행 등을 필요한 경우를 제외하고는 콜드 지갑으로 관리하는 것을 의무화하고, 인터넷으로 관리하는 고객의 암호화자산에 대하여 변제 재원의 확보를 의무화함(자금결제법안 63조의11)
3) 업자의 분별 관리 의무를 확대하여 이용자의 금전에 대한 신탁을 의무화함(자금결제법안 63조의11)
4) 사업자의 과도한 광고 · 권유에 대한 대응으로써, 허위 표시나 과대광고의 금지, 투기를 조장하는 광고 · 권유의 금지 등의 규제를 정비함(자금결제법안 63조의9의2, 3)
5) FAFT 권고 및 암호화자산 수탁업자의 유출위험 · 돈세탁 우려 등이 문제됨에 따라, 자금결제법의 적용을 받지 않던 '암호화자산 수탁업자'를 적용대상으로 포함하고, 본인확인 의무와 암호화자산의 분별 관리 의무를 규정함(자금결제법안 2조7항4호)
6) 돈세탁 악용이나 익명성 문제를 극복하기 위해서, 업자가 취급 암호화자산이나 업무의 변경을 사전 신고하고 문제가 없는지를 확인하는 구조를 정비함(자금결제법안 63조의6)

자금결제법 · 금융상품거래법 · 금융상품판매법 개정안

법무법인 민후

7) 이용자 보호를 위해서, 업자가 이용자에게 신용을 공여하는 경우에는 계약 내용에 대한 정보 제공 등의 조치를 취해야 함(자금결제법안 63조의10)
8) 이용자 보호를 위해서, 도산시 이용자는 업자가 분별 관리하는 이용자의 암호화자산 및 이행보증 암호화자산에 대하여 우선변제권을 가짐(자금결제법안 63조의19)
9) 금상법이 적용되는 암호화자산을 규정하였는바, 전자 기록 이전 권리 즉 '전자 정보 처리 조직을 이용하여 이전할 수 있는 재산적 가치(전자 기타의 물건에 전자적 방법으로 기록된 것에 한함)에 표시되는 것'이라는 개념을 도입하여 금상법의 적용대상이 되는 금융상품으로서의 토큰의 범위를 명확히 하고(금상법안 2조3항), 동시에 위 토큰이 자금결제법 적용대상이 아님을 명확히 함

* 자금결제법의 가상통화의 ICO 실시는 가상화폐교환업무에 해당하고 자금결제법의 규제 대상이었음

* 다만 금상법이 적용되는지에 대하여는 해석과 당국의 태도가 명확하지 않았으나 금상법 개정안을 통해서 이를 명확히 정리함 {다만 2017. 10. 27. 금융청은 ICO가 투자로서의 성격이 있는 경우, 금상법이 적용되므로 금상법상 등록을 요한다고 발표한 적이 있음}

* 가상통화 투자펀드 운용의 경우에도 금상법상 등록이 필요함

자금결제법 · 금융상품거래법 · 금융상품판매법 개정안

법무법인 민후

10) 암호화자산을 이용한 새로운 거래에 대한 대응으로서, 금융지표 등을 대상으로 하는 파생상품 거래 · 옵션거래 · 스왑거래, FX마진(FX거래)를 하는 업체에 대하여 금상법상 등록의무를 부과함 (금상법안 2조24항 등)

11) 레버리지 거래(증거금 거래)에 대하여, 향후 정부령의 개정에 따라 증거금 배율을 원칙적으로 4배 이하로 둘 가능성이 있다고 함

12) 시장 안정화를 위해서, 허위사실의 유포 또는 가격조작, 시세조종 등의 불공정행위 금지 규정을 ICO나 암호화자산을 이용한 금융상품에도 적용함(금상법안 185조의22, 23, 24)

13) 암호화자산 판매시 금판법의 규제가 적용됨(금판법안 3조등)

14) 형사소송법 등뿐만 아니라 금융상품 거래법 위반 사안의 조사에서 전자적으로 저장된 데이터의 압류 등을 가능하게 하는 규정을 정비함

* 일본의 ICO 규제 정리

- 자금결제 목적의 ICO : 자금결제법상의 '가상통화'에 해당하면 자금결제법상의 등록이 필요함
- 금융투자 목적의 ICO : 금상법 및 금판법 적용대상으로서 금상법상 등록이 필요함

5.우리나라 법원의 암호화폐 판결 등

법무법인 민후

우리나라 법원의 암호화폐 판결 등

법무법인 민후

대법원 2018. 5. 30. 선고 2018도3619 판결

비트코인은 경제적인 가치를 디지털로 표상하여 전자적으로 이전, 저장 및 거래가 가능하도록 한, 이른바 '가상화폐'의 일종인 점, 피고인은 위 음란사이트를 운영하면서 사진과 영상을 이용하는 이용자 및 음란사이트에 광고를 원하는 광고주들로부터 비트코인을 대가로 지급받아 재산적 가치가 있는 것으로 취급한 점에 비추어 비트코인은 재산적 가치가 있는 무형의 재산이라고 보아야 하고, 몰수의 대상인 비트코인이 특정되어 있다는 이유로, 피고인이 취득한 비트코인을 몰수할 수 있다

서울중앙지방법원

- 암호화폐에 대한 가압류는 인정되지 않으나, 암호화폐 반환청구권에 대한 가압류는 인정됨
- 암호화폐(비트코인)는 전자금융거래법상 선불전자지급수단에 해당하지 않음

우리나라 법원의 암호화폐 판결 등

법무법인 민후

기타 법원

- 암호화폐 빌려준 후 돌려받을 때 가격 기준은 변론종결 시로 보아야 함 (남부지법, 부산지법 서부지원)
  > 암호화폐에 대한 강제집행이 불가능하므로
- 거래소 착오로 지급된 암호화폐를 처분해도 횡령죄는 아님 (부산지검 서부지청)
  > 암호화폐는 형태가 있는 유체물 또는 관리 가능한 동력이라고 보기 어려우므로
- 외국 소재 거래소에 미화를 보낸 것은 외국환거래법의 '예금거래'에 해당하지 않음. 따라서 미신고 해외예금거래로 볼 수 없음(서울북부지검, 서울서부지검)

6.우리나라의 입법 방향

법무법인 민후

우리나라의 입법 방향

법무법인 민후

블록체인

- 진흥 입법이 시급하게 필요함 (송희경 의원안, 이상민 의원안 등)

암호화폐 : 혁신달성 또는 피해자 보호를 위해서 조속한 입법이 필요함

- 좋은 아이디어가 있어도 암호화폐 법제도화가 늦추어짐에 따라 이를 실현할 수 없음
- 입법이 없는 상황을 틈타 사기행위 등이 빈번하게 발생하고 있음
- 법제도 도입이 늦어짐에 따라 피해자가 속출하고 있지만 구제를 받지 못하는 상황임

암호화폐 입법방향

- 금융상품으로서의 암호화폐 : 자본시장법 적용대상
- 지급수단으로서의 암호화폐 : 전자금융거래법 적용대상
- 기타 암호화폐 : 규제 대상 아님

Part III

블록체인경제와 금융

좌장 : 오정근 교수
(건국대학교)

블록체인 혁명과 신 인류문명

오정근 교수
(건국대학교/한국 ICT금융 학회장)

블록체인과 금융의 미래

2019. 6. 18

오정근
(한국금융ICT융합학회 회장)

약력

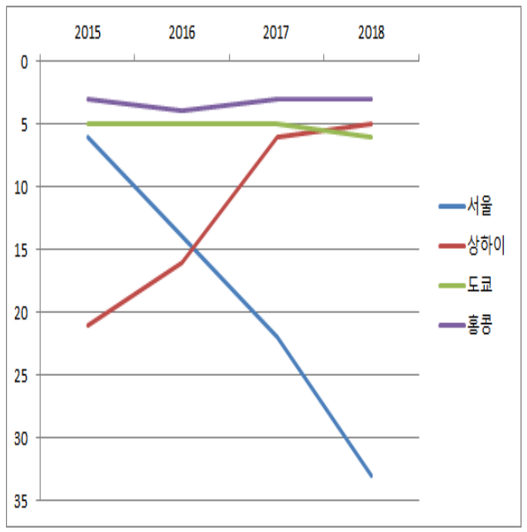
- 고려대 경제학 학사 석사
- 영국 맨체스터대 경제학 석사 박사

- 한국금융ICT융합학회 회장

- 前 한국은행 금융경제연구원 부원장
- 동남아중앙은행 조사국장
- 고려대 경제학과 교수
- 건국대 금융IT학과 특임교수
- 한국국제금융학회 회장
- 아시아금융학회 회장

추락하는 한국금융산업

한국, 세계금융중심지 순위 급락
아시아 주요도시 금융중심지 순위



자료: 영국 컨설팅그룹 지엔

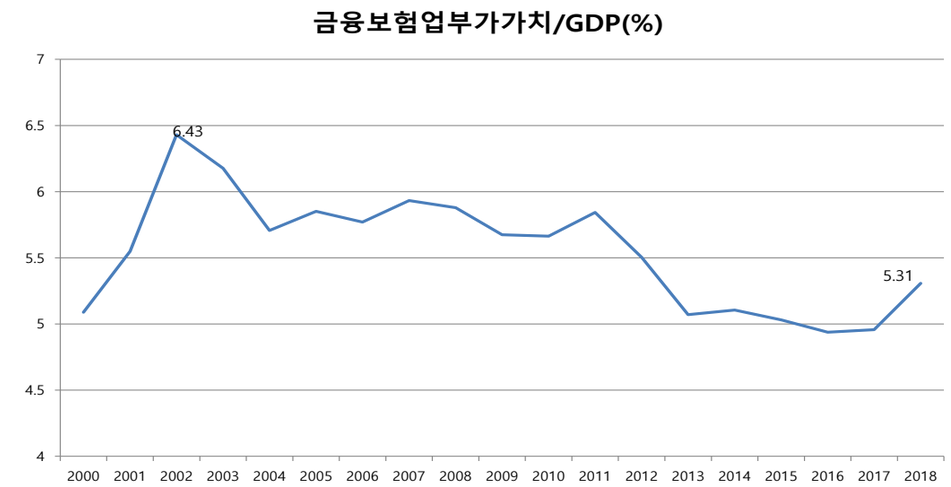
노무현정부시절 2003년 12월 '동북아금융허브 구상'을 발표.

2012년 11월 여의도에 55층 짜리 국제금융센터를 완공
현재 35% 정도가 공실. 입주기업 142곳 중 외국계 금융사는 25곳에 불과. 외국계 금융사 본사는 전무.

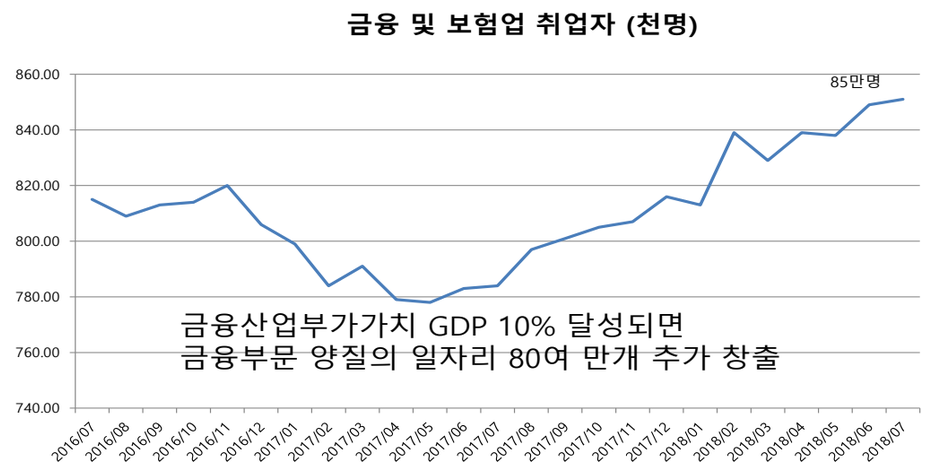
높은 법인세와 갖은 규제로 오히려 외국금융회사들이 한국을 떠나고 있는 실정.

금융중심지 순위:
서울은 2015년 5위, 2016년 14위, 2017년 22위, 2018년 33위 2019년 36위로 급전직하 추락

금융산업 부가가치 10년 내 GDP 10% 달성하겠다던 "10-10정책" 무색



금융산업 양질의 일자리 창출 제약



‘2019년 세계 100대 은행
스탠더드앤드푸어스(S&P)글로벌마켓인텔리전스

자산 기준 글로벌 은행 톱10 (단위: 억 달러)

올해 순위	작년 순위	은행명	국가	총자산
1	1	중국공상은행	중국	4조274
2	2	중국건설은행	중국	3조3765
3	3	중국농업은행	중국	3조2874
4	4	중국은행(BOC)	중국	3조922
5	5	미쓰비시UFJ파이낸셜그룹	일본	2조8129
6	6	JP모건체이스	미국	2조6225
7	7	HSBC홀딩스	영국	2조5581
8	9	뱅크오브아메리카	미국	2조3545
9	8	BNP파리바	프랑스	2조3367
10	10	크레디트아그리콜	프랑스	2조1236

한국에서는 총 6곳이 세계 100대 은행 순위에 랭크.
KB금융그룹이 64위, 신한금융그룹이 65위, NH농협은 72위, 하나금융그룹이 77위, 우리금융그룹이 85위, 산업은행이 94위

한국, 신금융에서도 낙후
2018년 세계 100대 핀테크산업(KPMG)

- 미국 18
- 영국 12
- 중국 11
- 호주 7
- 싱가포르 6
- 한국은 28위의 비바리퍼블리카와 63위의 데일리금융그룹 두 개만 랭크

- 세계 10위 핀테크기업
  - 중국은 알리바바그룹의 금융지주회사인 앤트파이낸셜이 1위, 징둥금융이 2위, 바이두가 4위, 루팍스가 10위로 4개가 랭크. 미국의 3개를 앞지르고 있음

2018년 세계 50대 핀테크산업(KPMG)

Leading 50

#01	Ant Financial	#17	Adyen	#34	Future Finance
#02	JD Finance	#18	Policybazaar	#35	Neyber
#03	Grab	#19	Klarna	#36	ZhongAn
#04	Du Xiaoman Financial (Baidu Financial)	#20	ACORN Oaknorth Holdings	#37	TransferWise
#05	Sofi	#21	Kreditech Holding	#38	Pushpay
#06	Oscar Health	#22	Monzo	#39	League Inc.
#07	Nubank	#23	WeLab	#40	Circle
#08	Robinhood	#24	Number26 (N26)	#41	Lendingkart
#09	Atom Bank	#25	WealthSimple	#42	Opendoor
#10	Lufax	#26	AfterPay Touch	#43	Metromile
#11	OneConnnect Financial Technology	#27	Dianrong	#44	Folio
#12	51 Credit Card Manager	#28	VivaRepublica (Toss)	#45	Lendix
#13	Revolut	#29	QUOINE	#46	GuiaBolso
#14	Compass	#30	Kabbage	#47	Starling Bank
#15	Stripe	#31	Affirm	#48	Coinbase
#16	Clover Health	#32	OurCrowd	#49	Airwallex
		#33	SolarisBank	#50	Lemonade

주목할 핀테크 기업

- 1위 앤트파이낸셜: 전자상거래회사 알리바바의 금융지주회사
  - 은행 증권 보험 카드 신용평가 전방위 금융업 영위

- 3위 그랩 파이넨셜: 공유자동차 그랩의 금융지주회사
  - QR코그 결제 그랩페이, 보험, 소액대출
  - 2012년 말레이시아 창업, 2014년 싱가포르 이전, 현재 동남아 6개국 1억 4400만 명 지난해 매출 10억 달러 달성 유니콘 진입

금산분리 제한 없이 산업자본이 금융업 진출해 유니콘으로 성장

주목할 핀테크 기업

- 9위 Atom Bank: 영국 인터넷전문은행
- 13위 Revolut: 영국 수수료 없는 실시간 환전회사
- 22위 Monzo: 영국 셀카 본인인증 도입한 인터넷은행
- 27위 Dianrong: 중국 P2P 금융회사
- 26위 Zhongan: 중국 인슈어테크 회사
- 37위 Transferwise: 영국 환전연결 P2P 회사
- 48위 Coinbase: 미국 최대 암호화폐거래소

무엇이 문제인가

- 모바일혁명과 금융빅뱅 몰이해
- 인터넷전문은행 메기역할 상실
- 빅데이터 심사분석 실종
- 인공지능과 금융 접목 지연
- 블록체인과 암호화폐, 무법규제로 질식

4차 산업혁명 화폐금융빅뱅 9대 기술

- **모바일** : 점포=> 모바일 (글로벌 모바일 네크워크)
- **모바일 결제**: 카드 =>모바일 =>QR코드
- **비대면인증**: 대면 거래=> 비대면 거래
- **빅데이터**: 심사분석=>빅데이터분석
- **클라우드**: 빅데이터 저장
- **인공지능(AI)**: 인간분석=>인공지능 머신/딥러닝분석

시공간 제약 없는 초연결 **모바일 금융**

신 신용분석 => 정보비대칭성 완화

- **암호화기술:** 프라이버시 보장 익명거래 가능
- **암호화폐**: 페이퍼화폐=>디지털화폐
- **블록체인**: 중앙집중결제보안=>디지털분산원장

신 화폐금융 제도

신 보안체계
신 결제제도

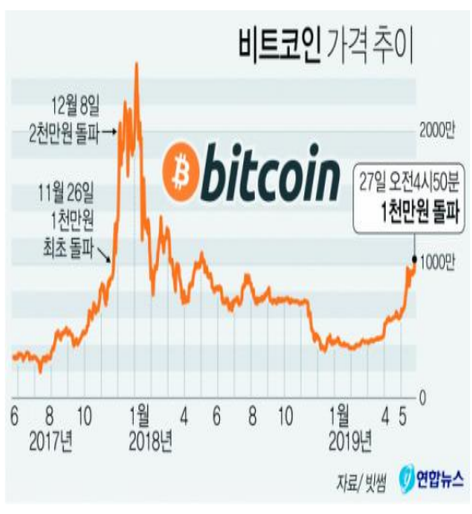
4차 산업혁명시대 기술혁신 신 화폐금융제도 빅뱅

- 신 화폐금융제도
- 신 모바일 금융제도

신 화폐금융제도

- 금융의 본질
- 블록체인과 금융
- 화폐의 기능과 암호화폐
- 암호화폐와 국제금융제도

비트코인 가격 동향



글로벌 금융회사 기업들 암호화폐시장 진입과 가격 재반등

비트코인 가격 재반등 배경

- 글로벌 금융회사 기업들 암호화폐시장 진입
  - 투자자들에게 암호화폐 재인식 계기
- 글로벌 금융시장 불안 증대
  - 안전자산으로 비트코인, 금 선호현상 대두
- 비트코인 4번 째 반감기 도래
- 시장에서 가격 저점으로 인식

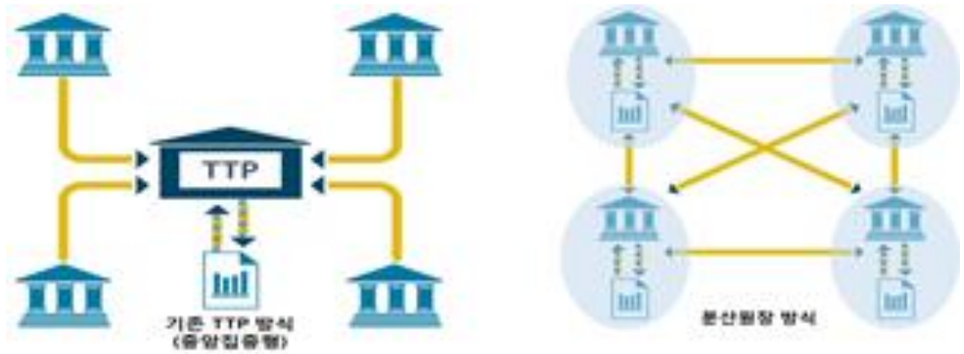
금융의 본질

- 금융거래당사자, 즉 돈을 지급하는 측과 돈을 받는 측 간의 신뢰를 해결하기 위한 방법으로 제3의 신뢰기관(Trusted Third Party: TTP)을 설립하고 해당 기관에 대한 신뢰를 토대로 금융거래
  - 예금과 대출을 중개하는 신뢰기관으로 은행이 탄생
  - 은행과 은행 간의 거래를 중개하는 신뢰기관으로 금융결제원 설립
  - 은행과 은행 간의 거래과정에서 일시적 최종대부자(lender of last resort) 기능을 하는 중앙은행 탄생
  - 자본시장의 주식과 채권을 받고 대금을 지급하는 신뢰기관으로 예탁결제원 설립

제3 신뢰기관 (TTP) 불신 대두

- 2008년 9월 15일 세계적인 투자은행 리만 브라더스(Lehman Brothers Holdings Inc.)의 파산과 그 결과 뒤따른 글로벌 금융위기
  - 제3의 신뢰기관을 바탕으로 한 금융제도가 얼마나 위험한 것인가를 여실히 노정
- 그 후 기축통화국의 무한정한 양적 완화 통화정책은 신흥시장국들에게 로운 금융불안요인 제공

블록체인과 금융



분산원장 기술은 기존 중앙집중형 시스템에 비해 (1) 효율성(efficiency), (2) 보안성(security), (3) 시스템 안정성(resilience), (4) 투명성(transparency) 측면에서 장점

화폐의 기능

- 첫째, 지급결제수단,
- 둘째, 교환의 매개,
- 셋째, 계산의 척도,
- 넷째, 가치저장의 기능

화폐의 진화

상품화폐(commodity money)

->금속화폐(metallic money)

->불환지폐(fiat money, legal tender)

->예금화폐(deposit money)

->전자화폐(electronic money)의 순으로 진화

-> 암호화폐 등장

거래의 효율성을 높이는 방향으로 발전해 옴

화폐의 정의
화폐의 기능을 하는 금융자산

- 통화(M1): 화폐의 지급결제수단으로서의 기능을 중시
  - 민간 보유 현금과 당좌예금, 보통예금 등 은행 요구불예금의 합계. 수표도 포함
- 총통화(M2): 통화(M1)에 정기예금, 정기적금 등 은행의 저축성예금과 거주자외화예금을 포함
- 총유동성(M3): 가장 넓은 의미의 통화지표
  - 총통화(M2)에 종합금융회사, 투자신탁회사, 상호신용금고, 새마을금고, 신용협동조합, 생명보험회사 등 비은행금융기관의 각종 예수금과 은행 및 비은행금융기관이 발행하는 금융채, 양도성예금증서(CD), 표지어음 및 상업어음매출 그리고 환매조건부채권매도(RP) 등을 포함

암호화폐의 성격, 지급형, 기능형, 증권형에 따라 적절한 통화지표에 포함 가능할 것으로 보임

암호화폐와 통화정책

- 국제결제은행(BIS)는 최근 보고서에서 DLT와 결합된 중앙은행 CBDC는 지급결제의 효율성을 높이고 특히 현금이 사라지는 국가에서는 CBDC가 안정적이고 편리한 결제수단으로 활용될 수 있을 것으로 전망
- CBDC는 중앙은행 통화정책 수단의 선택폭을 넓혀 주어 통화정책의 구조를 근본적으로 바꾸지는 않을 것이라고 전망

블록체인과 통화제도 통화정책

- 법정화폐와 민간화폐의 공존
- 중앙은행제도 vs 자유은행제도
- 기술혁신 vs 통화제도의 안정성
  - 거시경제 단기 안정화 위한 통화정책의 운용방식

암호화폐 전문 상업은행 등장

- 암호화폐계의 거물 노보그라츠는 2월 2억 5000만달러를 모금해 "갤럭시 캐피털"이라는 암호화폐 전문 상업은행을 설립할 계획이라고 발표.
- 암호화폐만 취급. 암호화폐 자산관리, 거래, ICO, 시장 조사 등 암호화폐와 관련한 업무를 전문적으로 처리할 계획이라고 발표.

암호화폐 전문 투자펀드도 속속 등장

- 2017년 월가를 떠난 매트 괴츠는 암호화폐 투자회사 블록타워 캐피탈을 설립
- 코인베이스도 본업인 암호화폐 거래소를 넘어 암호화폐 스타트업 육성을 위한 투자기업 '코인베이스 벤처' 설립을 공식 발표.

암호자산 시대 도래

- 모든 자산거래를 암호화한 암호자산으로 분산거래
- 스위스 독일 증권거래소에서 암호자산을 상장 검토

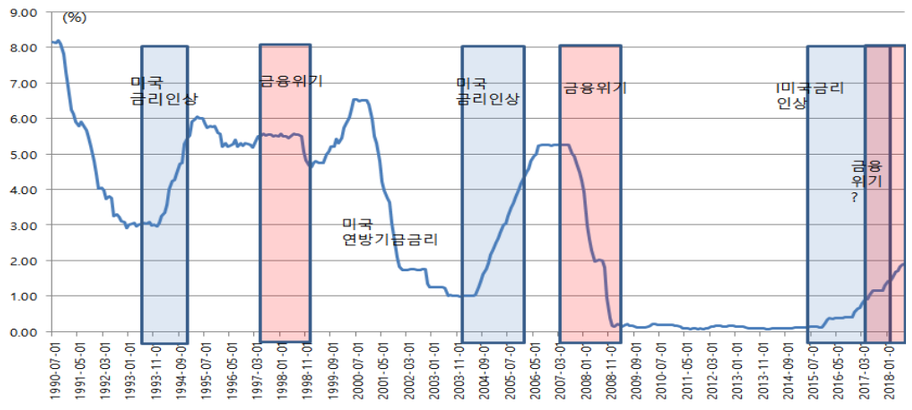
블록체인 기반거래 국제규범도 추진

- 최근 EU집행위원회는 영국을 포함한 22개 EU 회원국이 '유럽 블록체인 파트너십' 출범에 공동서명했다고 발표.
- EU를 블록체인 기반 단일 금융시장으로 발전시키자는 원대한 계획 추진

암호화폐와 국제금융제도

- 1945년 달러 기축통화제도 정립 (영국 케인즈와 미국 화이트 논쟁)
  - 트리핀 딜레마. "미국이 경상적자를 허용하지 않고 국제 유동성 공급을 중단하면 세계 경제는 크게 위축될 것"이며 "그러나 적자 상태가 지속돼 미 달러화가 과잉 공급되면 달러화 가치가 하락해 준비자산으로서 신뢰도가 저하하는 딜레마
- 1997년 동아시아금융위기 발생
  - 근본적으로는 동아시아에서 글로벌유동성이 부족한 점이 원인이라는 진단 하에 아시아통화기금(AMF) 도입이 논의. 미국의 반대로 중단
- 2008년 미국발 글로벌 금융위기가 발생
  - 프랑스 사르코지 대통령과 중국을 중심으로 미국 달러, 유로에 이어 제3의 기축통화가 필요하다는 주장이 제기되었으나 2011년 유로존 위기 발생과 사르코지 대통령의 퇴임으로 유야무야
- 2009년 비트코인 출시
  - 2019년 다시 비트코인 가격 재반등

미국 금리변동과 금융위기



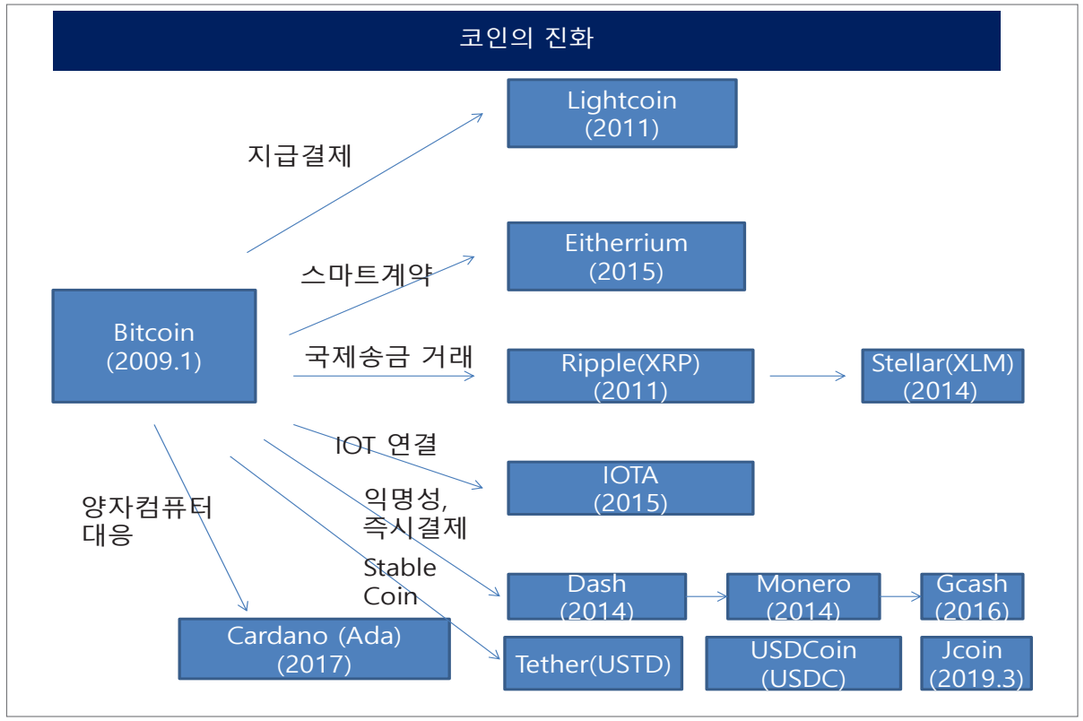
근년에 Stable Coin 등장 주목

국제기축통화제도에 미칠 영향

- 현재: 달러 유로 엔 파운드
- 미래: 달러 유로 엔 파운드 + 암호화폐
- 암호화폐 많이 보유=외환보유액 많이 보유 기능하게 되는 시대 도래 전망

코인의 진화

- 코인 1.0: 비트코인과 같은 범용 지급결제용 코인
- 코인 2.0: 이더륨과 같은 스마트계약 플랫트폼 기능을 하는 코인
- 코인 3.0: 코인을 이용한 블록체인 기반 거래에 사용되는 토큰으로 모든 거래가 블록체인 기반화 하면서 사용될 토큰의 폭발적 급증



블록체인 이용 다방면 폭발적 증가

- 금융권
  - 한국증권업계: 공인인증서 대신 블록체인 공동인증제 도입 (2017년 말)
  - 한국은행업계: 블록체인 공동인증제 BankSign 2018년 7월 도입
  - 삼성 SDS: 인공지능 블록체인 기반 금융플랫폼 “넥스파이낸스” 공개
  - SKT: 블록체인 기반 지급결제시스템 연내 출시
- 의료
  - 메디블록, 직토, 엑스블록시시템즈, 휴면스케에프 등
- 지역화폐
  - 글로스퍼 노원화폐 등
- 게임
  - 플레이코인, 서브드림스튜디오 등
- 한류콘텐츠
  - ENT캐시, Kstar코인, 코펀 등
- 스마트컨트랙트: Xtock 등
- 물류: 삼성SDS 블록체인 기반 항만 해운 물류
- 환경: Cyclean 등

블록체인 기반 글로벌 송금결제 컨소시엄

글로벌 금융서비스 개발 스타트업 R3는 ‘R3CEV(Crypto, Exchanges and Venture practice)’라는 블록체인 컨소시엄을 운영

R3CEV는 지난2016년 9월 결성돼 씨티그룹, 뱅크오브아메리카(BoA), JP모건체이스, 모건스탠리, 골드만삭스, UBS 등 100여개 금융회사 회원사 (연간 25만 달러(약 3억원).

R3는 기본적인 시스템 설계 및 기술개발을 담당하고, 회원사는 자사 응용 프로그램 프로그래밍 인터페이스(API)에 연결해 시스템을 테스트. 우선 블록체인 기반의 해외송금시스템을 개발해 해외송금 수수료를 기존의 1/10 수준으로 낮출 계획.

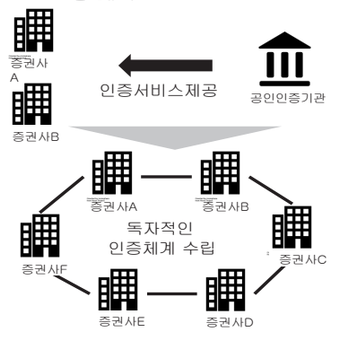
R3CEV는 송금을 넘어 결제, 회사채, 보험, 주식, 부동산 등 8개 영역에 블록체인 기술을 적용해 거래 안정성을 강화

금융권 블록체인 컨소시엄 사업 본격화

증권, 은행, 보험 각 분야별 블록체인 컨소시엄이 출범되어 사업 착수, 우선 고객 편의성을 높일 수 있는 인증서비스 분야 개발

금투업권 컨소시엄

- 금융투자협회 주관, 25개 증권사와 5개 블록체인업체 참여 (16년 12월)
- 블록체인 기반 공동사설인증 시범서비스 (17년 7월)
- 공인인증에 투입되는 자원과 비용을 절감하고, 향후 금융투자상품 거래 적용 계획



은행권 컨소시엄

- 전국은행연합회 주관, 18개 은행이 참여 (16년 11월)
- 은행권 공동 인증 서비스, 외국환 지정 거래 변경 사업 추진

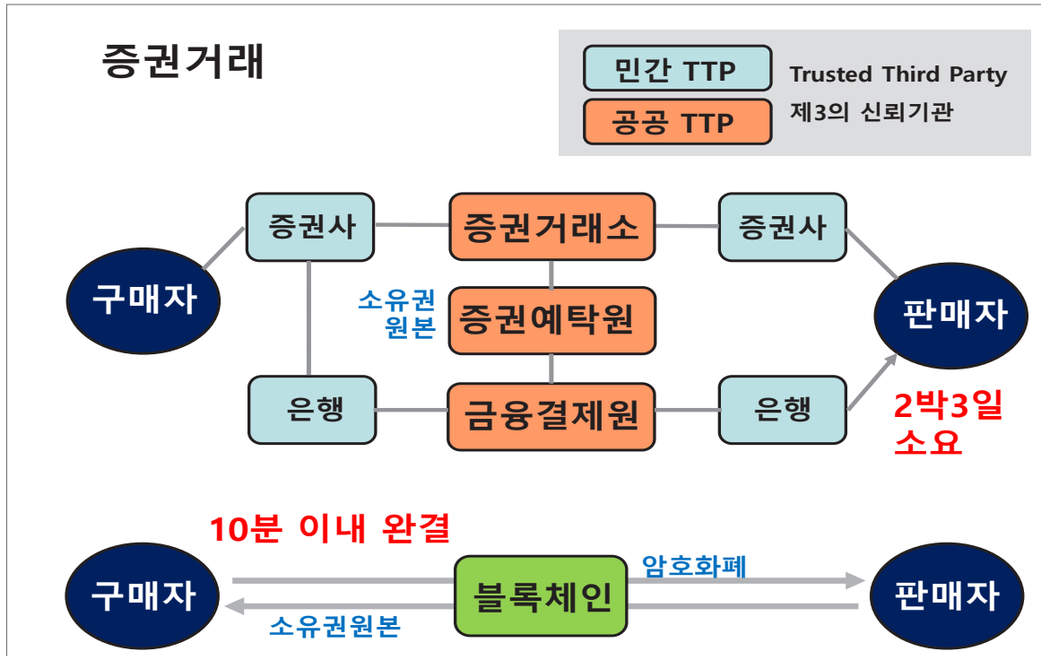
보험업계 컨소시엄

- 생명보험협회와 손해보험협회가 각각 블록체인 컨소시엄 TF 구성 (17년 6월)
- 스마트계약을 통한 보험금 자동지급 기술 검토

카드업계

- 각 카드사별로 블록체인을 인증 기술에 적용
- 간편인증, 포인트관리, 간편송금으로 적용 확대

38



보험업계

- AIG와 IBM 블록체인 기반 스마트 보험계약 시스템 구축

- Aegon, Allianz, Munich Re, Swiss Re 및 Zurich는 2016년 10월 블록체인 컨소시엄인 B3i (Blockchain Insurance Industry Initiative)를 출범함
  - 이후 10개의 (재)보험사들이 합류하여, 현재는 15개의 (재)보험회사들로 구성된 최대의 보험산 업 블록체인 컨소시엄임. 2017년 12월까지 상용화하는 것을 목표로 하고 있음
  - 재보험 계약의 체결, 보험료 납입, 보험사고 보고 및 보험금 정산이라는 일련의 과정을 블록체인으로 처리 가능하도록 시스템 구축

지역발전을 위한 화폐 발행

- 지역기업이 이점을 가지는 인센티브 부여를 통해 지역 발전에 기여할 수 있도록 프로그램화된 지역화폐 발행
  - 특정지역의 숙박시설, 가게 등에만 사용할 수 있는 지역화폐를 발행해 해당지역에서만 사용할 수 있도록 하여 지역 경제 발전에 기여

- 법정화폐를 보완하는 수단으로 도입된 **지역화폐**는 **지역경제 발전의 원동력**을 지역 내부에서 찾아 활용되는 특징을 가지고 **지역경제 자립과 활성화**의 **선순환** 을 만들어내는데 의의

지역화폐 현황 02

지역경제 활성화	지역공동체 유대 강화	소외계층 지원	관광 활성화
마포구 지역화폐 '모아'	대전의 '두루'	성남의 '성남사랑상품권'	'화천사랑상품권'
- 2016년 발행 - 가맹점 180여곳 - 누적된 유통규모 2억여원	- 2000년 발행 - 회원수 651가구 - 매년 1만~15000건 거래 - 약 3억원 가량중 50%이상을 지역화폐 두루로 거래 - 주민 주체 발행	- 2006년 발행 - 청년배당 명목 - 7000여개 가맹점 - 소외계층 지원	- 축제장 입장료 일부를 지역화폐로 반환 - 입장료 부담을 줄여 더 많은 관광객 유치 - 지역 내 소비 유도

노원 지역화폐

사회적 가치를 경제적 가치로의 전환

봉사활동 · 기부

↓

지역화폐 지급
(봉사활동 1시간에 700NW 지급)

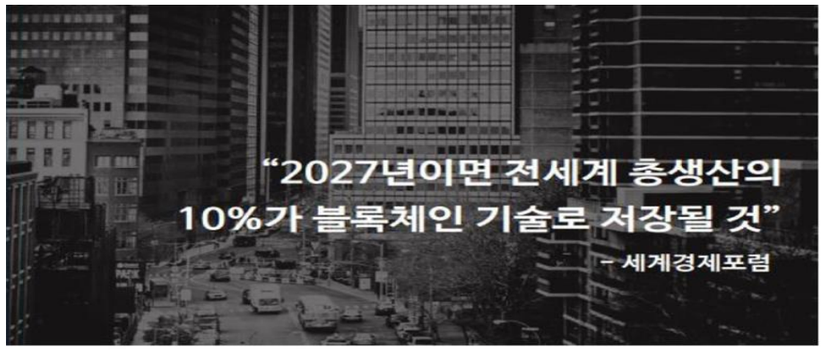
↓

가맹점에서 사용
(애플리케이션 · 회원카드)

4차 산업혁명과 기하급수적 코인탄생

- 4차 산업혁명의 진전으로 산업별 부문별 블록체인기반 거래가 확산될 수록
- 획기적인 거래의 효율성, 비용절감, 투명성, 보안성으로 인해 매년 수 백 개의 코인 탄생 전망.

기술의 폭발점(tipping point)과 인류문명의 거대한 전환(Deep Shift)



각국은 건전한 규제로 블록체인 암호화폐 발전 도모

	정의	규제	과세	ICO
미국	자산/ 화폐	거래소 등록	자본이득세 / 소득세 부과	적격투자자제도
일본	화폐	거래소 등록	소비세 면제. 거래차익 잡소득으로 과세	허용.
영국	민간화폐	거래소 등록	부가가치세 폐지 거래수익 비과세 법인세 부과	허용
독일	금융상품	거래소 등록	투지거래 소득세 25% 부과 채굴, 개인거래 비과세	허용
스위스	지방정부화폐 지방결제수단. 물건 등 자산	스위스 금융시장감독위원회(FINMA) 라이선스	부가가치세 없음 법인세 14.6%(Zug) 개인자본소득 비과세	허용. 크립토밸리 육성

규제 동향 요약

- 암호화폐를 자산, 금융자산 또는 민간화폐로 인정하는 추세 확산
- 투자자보호를 위해 거래소는 등록제를 도입하는 추세
- 과세는 부가가치세 면세, 거래소득 비과세 추세 (화폐로 간주) 속 미국 일본은 소득세 과세
- ICO는 증권형토큰은 증권으로 간주 증권거래법 규제, 지불형코인/토큰은 자금세탁방지시스템(AML) 고객신원확인(KYC) 구축 요구. 반면 유틸리티토큰은 비규제 추세
- 점차 제도 구축되면서 암호화폐 사용 확산 전망

한국, 블록체인은 육성

- 정부: 블록체인을 신성장 동력 산업으로 선정 육성
  - 한국인터넷진흥원(KISA): 블록체인 시범사업 프로젝트: 기존 6개-> 12개로 확대.
  - 과학기술정보통신부: 4개 시범사업 추진
  - 중앙선거관리위원회(온라인투표), 국토교통부(부동산거래)) 농림축산식품부(축산물이력관리) 외교부(국가간 전자문서 유통) 해양수산부(해양물류)
- 지자체: 제주: 블록체인특구 추진. 서울: 블록체인 5년계획 발표: 마포와 개포에 블록체인단지 조성, 1223억 투입, 충북: 블록체인센터 설립 등
- 국회: 관련 법안 논의 중 (현재 20여 개 법안 제출 중)
  - 최근 "국회블록체인포럼" 출범

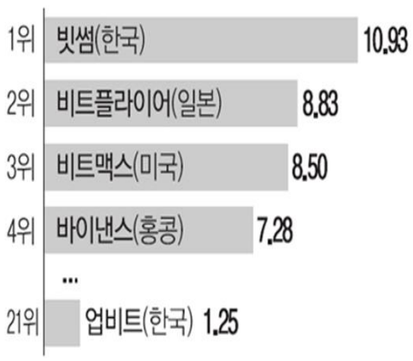
한국, 암호화폐는 과도한 '무법'규제

- 암호화폐 실체를 불인정
- **암호화폐공개 (**ICO) 금지
- 암호화폐거래를 유사수신행위로 간주
- 암호화폐거래소를 단순 통신판매업자로 간주
  - 필요한 건전한 규제도 하지 않아서 영세한 거래소 난립으로 투자자 피해 속출

한국의 블록체인 암호화폐 회사

- 한국은 세계적으로 블록체인 암호화폐 산업 열기가 뜨거운 국가임
  - 세계 최고 수준의 반도체 모바일폰 초고속통신망 등 관련 정보기술(IT) 하드웨어 산업발달 (IT 강국)이 중요한 배경
  - 대학교 진학률 80%의 고학력도 청년들의 창업열기
- **암호화폐공개(ICO)를 한 회사: 124개**
- **코인을 거래소에 상장한 회사: 81개**
- **ICO를 준비 중인 회사: 38개**
- **암호화폐 거래소: 56개**
- 이외에도 대략 200여 개의 많은 스타트업들이 창업을 준비 중임

세계적인 수준의 거래소 추락



2018

30위권 밖으로 밀린 국내 가상화폐거래소

(단위:억원)

거래소명	세계 순위	하루 거래량
빗썸	35위	5328
업비트	48위	1726
후오비코리아	53위	1357
코인빗	67위	560
코인원	86위	208

*5월 5일 오후 3시 기준 자료:코인마켓캡

2019. 5

국내 규제로 거래소 해외진출 러시

- 네이버: 싱가포르에 거래소 "비트박스" 설립하고 암호화폐 "링크" 발행 (2018. 7)
- 카카오: 일본에 블록체인자회사 "그라운드x" 설립, 암호화폐 "클레이" 공개(2018.10)
- 빗썸: 홍콩에 거래소 빗썸덱스 설립(2018.10) 등 아시아 10개국에 진출 계획
- 업비트: 싱가포르에 거래소 설립(2018.10)
- 넥슨: 유럽 거래소 "비트스탬프" 인수(2018.10)
- 코인원: 인도네시아에 거래소

중국 암호화폐 거래소는 한국진출

구분	거래소 명	진출 국가	해외 법인명	진출 시기	비고
중화권 최대	Binance	한국		준비중	원래 홍콩에 있었으나 몰타로 이전 예정, 한국어 지원
		일본		2018.7 철수	일본 금융청 규제로 현지 철수
중국 Big 3	Huobi	한국	후오비코리아	2018.3	
		미국	HBUS	2018.6	
		일본		2018.7 철수	일본 금융청 규제로 현지 철수
	Okcoin	한국	오케이코인코리아	2018.4	NHN엔터테인먼트과 제휴
		홍콩	OKEx	2017.1	홍콩으로 이전하여 자회사 형태로 운영
	BTCC	한국	BTCC 코리아	2018.3분기 예정	
		홍콩, 런던		2018.1	2018.1 홍콩 블록체인 투자사에 피인수
그 외	Zeniex	한국	지닉스	2018.5	한·중 합작
	비트제트	한국		2018.5	한국블록체인협회 가입 타진 중
	Gate.io	한국	게이트코리아	2018.5	

한국 블록체인 암호화폐 기업들의 탈한국러시

— BOSCOIN(2017.6), ICON (1000억원, 2017. 8) Hdacs(3000억원, 2017. 12): 스위스에 재단 설립하고 ICO

— 메디블록(2017.12): 지브롤터에 재단 설립하고 ICO

— 글로스퍼: 홍콩에 재단, 조만간 글로스퍼 재팬 오픈 예정

— 블록체인 기반의 보험플랫폼 구축을 추진하고 있는 직토(Zikto): 싱가포르에 재단 설립하고 ICO 설립하고 ICO

— 카카오: 블록체인개발 자회사 '그라운드X' 일본에 설립, 연내 블록체인개발 위한 '카카오 3.0시대' 전략 발표(2018. 3. 27)

— 네이버: 자회사 '라인파이낸셜' 일본에 설립(2018. 1월). 일본정부에 암호화폐 거래 허가 신청

한국 블록체인 암호화폐 생태계 붕괴 우려

- 벤처기업자금조달 어려움 증대로 창업생태계 붕괴 우려
- 법률자문 회계자문 컨설팅 등 관련 사업서비업 발전 저해
- 관련 인력양성 지체

국부유출

- 높은 해외 재단 유지비용으로 인해 1~200억원 규모의 ICO로는 한국에 가져와서 사업할 자금 마련이 쉽지 않은 실정 (현재 약 100여 개 기업 해외ICO 추정)

— 법인세: 쥬크 14.6%. 싱가포르 15%

— 인건비: 스위스; 스위스인 고액연봉의 대표와 임원 3명 등 한국인과 현지인 5:5 채용의무

— 급등하고 있는 사무실임대료 등

— 송금도 현지 법인의 판단에 따라 가부 결정하는 등 ICO 조성된 자금을 가져오는데도 어려움

기술유출

- 명목상으로는 현지 법인(비영리)이 ICO의 주체
  - 코인발행 비지니스모델과 기술내역 관장해 과도하게 세밀한 기술내역까지 제출할 것으로 요구하는 사례

4차 산업혁명 지연

- 블록체인과 암호화폐 산업의 미발달은 블록체인을 기반으로 하는 각종 4차 산업혁명을 지연시켜 한국이 4차 산업혁명에서 낙오되게 할 수도 있을 우려

- 산업혁명에서 뒤진 국가가 그 후 후진국의 신세를 면치 못했듯이 4차 산업혁명의 낙오는 한국을 다시 도래하는 새로운 문명의 시대에 후진국으로 주저앉게 할 우려

특구지정 필요성

- 한국은 규제가 많은 국가로 한꺼번에 모든 규제를 개혁하는데 한계

○ 규제친화적 top-down 국가시스템을 비즈니스친화적(business friendly)인 bottom-up 국가시스템으로 개조하는 데는 엄청난 노력과 시간이 소요

.

— 한 국가사회의 문화를 바꾸는 문제이므로 쉽지 않을 수도 있음

○ 각종 기득권 그룹 세력들의 막강한 반규제 파워

- 복지국가 지향에 따른 높은 재정수요를 감안할 때 동아시아 외국의 블록체인기업들이 한국으로 들어올 정도로 법인세를 낮추는데도 한계

규제프리 특구 혜택

□ 결국 한국의 제반 여건을 고려할 때 현 단계에서는 크립토산업에 대해서는 사전허가 사후규제(문제가 발생시 사후에 규제하는 샌드박스식 규제) 하는 규제프리 특구 조성 필요

○ 특구 내에서는 획기적인 규제개혁으로 Bottom-up 기업투자 환경 조성

○ 특구 내에서는 동아시아지역 기업들도 들어올 정도로 매력적인 수준의 법인세 인하

— 법인세 쥬크 14.6%(외국법인 9~10%, 2020년 12%로 인하), 싱가포르 15%인 점을 고려해 15% 수준까지 인하

○ Crypto labs, 인큐베이터 등 창업공간을 제공하는 민간기업에 대한 세제, 금융 혜택 등 유인제도 도입

크립토특구 조성 효과

□ 한국 블록체인 암호화폐 산업 발달로 디지털금융생태계 조성

○ 한국은 디지털금융에 필요한 하드웨어, 즉 △5G 초고속통신망, △ 모바일, △ 반도체가 세계 1위
○ 청년들의 창업열기도 높은 편임
○ 소프트웨어 발달에 필요한 규제만 혁파되면 디지털금융시대 세계의 금융중심이 될 수 있음
— 쥬크와 싱가포르는 글로벌 디지털금융허브를 두고 쟁패하는 모습

□ 블록체인 암호화폐 산업 발달은 4차 산업혁명의 기반이 되어 4차 산업혁명 시대 한국이 선진국으로 도약할 수 있는 토대가 될 것임

□ ICO통한 자금조달 활성화로 창업생태계 활성화

규제프리 특구 효과

□ 국부유출도 방지

○ 법인세 한국납부
○ 인건비 사무실 운영비 등 한국지출

□ 기술유출도 방지

○한국에 ICO 법인 설립 운영

□ 관련 연관산업 발달로 디지털금융 허브 조성, 아시아디지털금융중심지로 발전

○ 각종 미트업 컨퍼런스 등 MICE산업 발달
○ 법률 회계 컨설팅 등 사업서비업 발달
○ 관련 우수인력 양성 위한 대학 활성화 등 교육산업 발달
— 대학에 관련 학과 증설, 경영대학원, 기술경영대학원 등 확충 활성화

□ 자연스럽게 금융 MICE 사업서비스 교육의 허브로 발전하며 고부가가치 고임금의 양질 일자리 창출

□ 기존의 관광문화휴양도시+ 블록체인 암호화폐산업 (동아시아지역 블록체인 암호화폐기업, 암호화폐 재단 200개 이상)+금융+법률+회계+세무+교육+MICE산업+숙박 음식업 등 관련산업이 집적된 종합 크립토밸리나 비치, 마운틴, 아일랜드로 발전

외국의 혁신 사례

- 영국: 2014년 "핀테크 수도(Capital of Fintch)" 선언, 런던테크시티 구축 (Level 39), Teck UK로 발전
  - 23개 클러스트 150만 개 일자리창출) 2015년 규제샌드박스 도입
  - 금융당국 핀테크 전담부서 "Innovation Hub", 금융당국의 목표는 **"금융회사의 혁신을 고취하는 데 있다"**

- 싱가포르: 2016년 규제샌드박스 도입, 획기적인 규제 환경, 법인세 15%로 동남아 핀테크 성지로 부상

외국의 혁신 사례

- 스위스 쥬크: **"암호화폐 수도(capital of crypto nation) "** 를 목표로 조세 혜택 (법인세 14.6%, -> 2020: 12%), 친기업 환경, 법제도 등 각종 **인프라 개선에 필요한 환경 조성 등에 정책 역량 집중**
  - **300여 개 블록체인 암호화폐 회사 운집해 세계적인 "크립토밸리"로 발전**

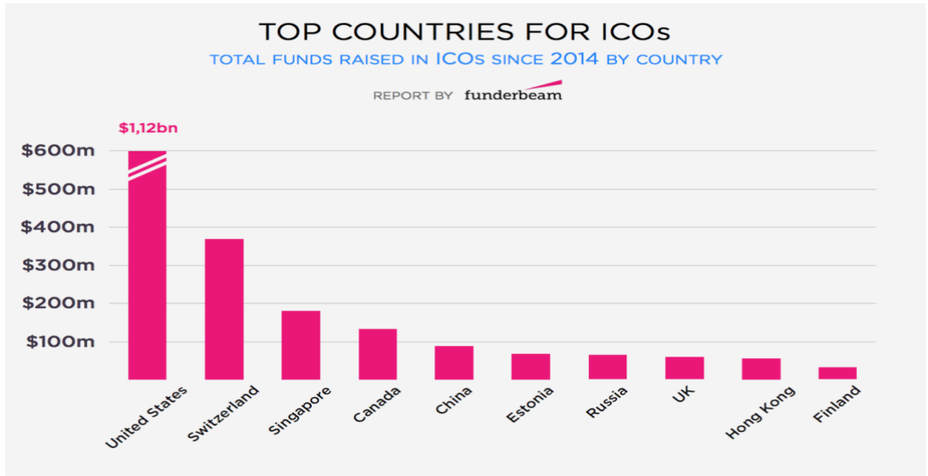
- 중국: 사전허가 사후규제 도입, 핀테크 비약적 발전, 상하이 국제금융센터로 발전
  - 약 2억 명에게 포용금융제공

스위스 크립토밸리 쥬크 전경

스위스 크립토밸리

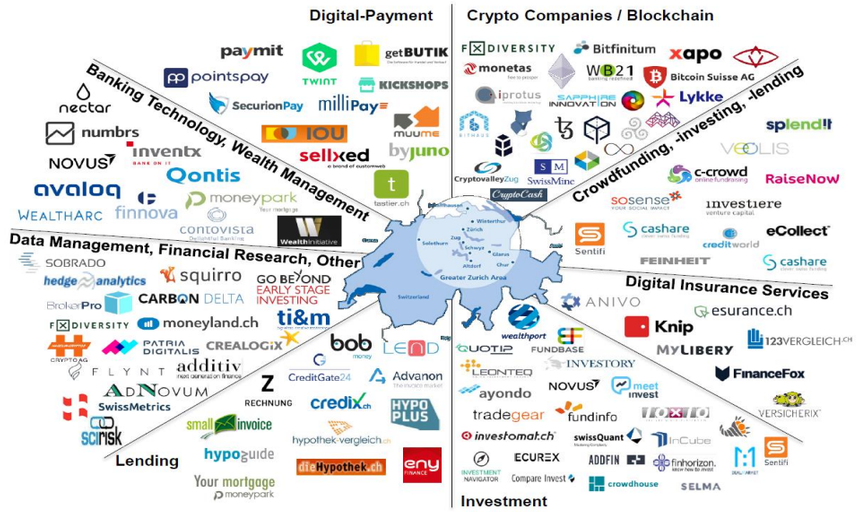
2017년 ICO를 통한 글로벌 자금 조달 1/4이 스위스에서 이루어졌으며 특히 글로벌 최대 10대 ICO 중 4 개가 스위스 Zug에서 시행

국가별 ICO 현황



자료: KPMG

반면 Zug 크립토밸리에서는..
글로벌 볼록체인기업들 유입 (약 250여 개)



2017년 주요 ICO 국가별 분포

		TOTAL RAISED	END OF ICO	DURATION (DAYS)	CATEGORY	COUNTRY
1	Filecoin	$257m	07.09.2017	28	Data storage network	USA
2	Tezos	$238m	13.07.2017	14	Smart contract platform	Switzerland
3	EOS	$159m	01.07.2017	5	IT Infrastructure	USA
5	Bancor	$157m	12.06.2017	<1	Cryptocurrency	Switzerland
4	Polkadot	$145m	27.10.2017	12	Technology	Germany
5	The DAO	$142m	28.05.2017	28	Venture capital platform	Switzerland
6	Qash	$106m	08.11.2017	2	Fintech	Singapore
7	Kin Kik	$98m	26.09.2017	14	Social Media	Canada
8	Comsa	$95m	06.11.2017	35	Fintech	Japan
9	Status	$95m	20.06.2017	<1	Messaging platform	Switzerland
10	TenX	$83m	24.06.2017	<1	Digital-only bank	Singapore

자료: PwC Strategy& analysis

Fintech 허브 랭킹 2018

Rank	YOY	City / Country	Scores
1	-	Singapore	
2	-	Zurich / Switzerland	
3	-	Geneva / Switzerland	
4	+4	London / UK	
5	+2	Amsterdam / Netherlands	
6	-2	Toronto / Canada	
7	+3	Stockholm / Sweden	
8	-3	New York City / US	
9	-3	San Francisco / US	
10	-1	Hong Kong (China)	
11	+2	Frankfurt / Germany	
12	+2	Berlin / Germany	

정치/법 경제 사회 기술

IFZ, Tintch Study 2018

암호화폐와 부패방지, 포용금융

가상화폐와 부패방지

- 중세 르네상스시대 글로벌 무역에서 막대한 금은보화를 축적한 이태리I 베네치아 피렌체 상인들이 금은보관증서를 유통시키며 시작된 은행업은 엄청난 부를 축적하는 과정에서 정경유착의 부패고리가 형성. 이러한 부의 축적과정은 현대의 금융그룹도 예외가 아닌 실정
- 특히 관치금융이 심한 나라일수록 언제나 정경유착의 부패문제가 심각. 특히 거대금융그룹의 과도한 탐욕은 2008년 글로벌금융위기와 같은 금융위기를 초래해 세계경제를 강타
- 가상화폐는 이러한 관치금융과 정경유착 부패의 고리인 금융업의 중개를 필요 없이 블록체인이라는 신뢰 시스템을 기반으로 한 쌍방거래이어서 관치금융과 정경유착 부패 문제를 획기적으로 감소시킬 전망 (하바드대 로고프 교수의 근간『현금의 저주』).

가상화폐와 부패방지(계속)

- 암호화폐의 출현이 경제의 효율을 획기적으로 증진시켜 새로운 부를 창출함은 물론 많은 사람들을 중앙화된 엘리트중심의 금융권력으로부터 자유롭게 할 전망
- 암호화폐가 범죄에 악용될 것이라는 우려도 있으나 이는 현재 세계적으로 논의되고 있는 고객신원확인(KYC) 자금세탁방지(AML) 강화로 상당부분 해결될 수 있을 것으로 전망

가상화폐와 포용적 금융

- 중국 서남아시아 중동 아프리카 등 25억 명 정도의 인류는 아직도 은행계정을 갖지 못하고 있지만 상당수는 모바일폰은 가지고 있음
- 스마트폰의 등장과 이로 인해 가능해진 쌍방(P2P)거래를 근간으로 하는 P2P대출 크라우드펀딩 인터넷전문은행 등 모바일금융은 이들에게 생애 처음으로 금융이라는 것을 이용할 수 있는 기회를 제공. 금융포용이 확산. 빈곤탈출의 기회 제공
- 가상화폐의 출현은 금융소외 계층에 금융포용의 새로운 기회를 제공. 모바일폰을 통해 비트코인을 전송해 새로운 삶의 기회를 제공 (폴 비냐, 마이클 케이시 공저인『암호화폐 시대』(The Age of Cryptocurrency)(2016))

투자자보호

투자자 보호 1: 건전한 거래소 정비

- 건전한 가상화폐 거래소 등록/인가 등 거래 생태계 구축
  - 일본 최대 거래소 해킹 사건의 교훈

코인체크는 2017년 일본 금융청(FSA)에 등록한 15개의 거래소가 아니었음

대부분의 코인을 외부인터넷과 연결된 전자지갑인 핫월렛에 저장하고 있었음. . 미국 거래소 코인베이스가 전체 암호화폐의 97%를 외부인터넷과 연결되지 않는 콜드월렛에 저장

주요 거래소에서는 비밀키를 여러 개 사용하는 다중증명기능을 사용하고 있는데 이 거래소는 비밀키를 하나만 사용하는 단독서명기능에 의존. 이 경우 하나뿐인 비밀키가 해커 손에 넘어가면 탈취당한 암호화폐를 바로 꺼내갈 수 있음

이런 점들을 볼 때 코인체크 사고는 예고된 사고이라고 해도 과언이 아님.

투자자 보호: 건전한 거래소 정비

- 한국도 조속히 투자자보호를 위한 가이드라인을 정하고 법제화해 등록제나 인가제/등록제를 시행
- 요건에 미달하는 거래소는 즉각 거래를 중지하도록 해야 투자자 손실을 막을 수 있음
- 해킹 파산 등으로 투자자가 입을 손실에 대비한 보험제도, 거래소 전용 이상징후탐지시스템(FDS), 국제공조체제도 구축하는 등 다각적인 투자자보호대책을 강구해야 함
- 문제가 발생하면 무조건 거래소 폐쇄는 올바른 대책이 아님.

투자자 보호 2: 가상화폐 신용평가제도 구축

- 건전한 가상화폐 거래 생태계를 구축하기 위해서는 가상화폐 신용평가제도 구축 필요
  - 미국의 한 신용평가회사가 세계 최초로 74종의 암호화폐에 대한 신용등급을 발표
  - 한국: 글로벌코인평가 설립. 코인평가 착수

세계 디지털금융중심지 한국의 꿈

세계 1위 하드웨어: 초고속통신망, 모바일, 반도체

갖추어야 할 소프트웨어:

규제혁파 (사전허가 사후규제)
창의인재 양성
모험금융산업 육성

블록체인과 금융정책의 미래

김양우 교수
(수원대학교)
(전)금융경제 연구원장

2

4차 산업혁명과 블록체인

4차 산업혁명이란?

다통령직속 4차산업혁명위원회

인공지능, 빅데이터, 초연결 등으로 촉발되는 지능화 혁명, 그리고 그 이상

4차 산업혁명과 블록체인

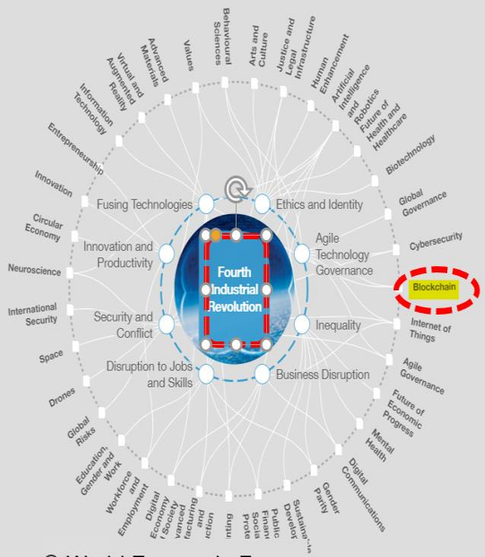
4차 산업혁명의 인문사회학적 의미

1차 산업혁명	2차 산업혁명	3차 산업혁명	4차 산업혁명
증기기관	전기	퍼스널 컴퓨터	통신
개인의 노동	인류의 노동	개인의 사고	인류의 사고
기계가 대신	대량 생산이 대신	컴퓨터가 대신	인공지능이 대신

https://bsalary.tistory.com/53?category=586007

4차 산업혁명

" 통신을 통하여 모든 것이 연결되고,
연결을 통하여 다양한 기술이 융합되어 나타나는 혁신적인 진보" https://bsalary.tistory.com/53?category=586007



© World Economic Forum

◆ 4차 산업 혁명 :
-인간이 살고 일하며 서로 연결시키는 근본적 변화 의미

-인류 발전의 새로운 장으로서, 기술 진보에 의해 가능

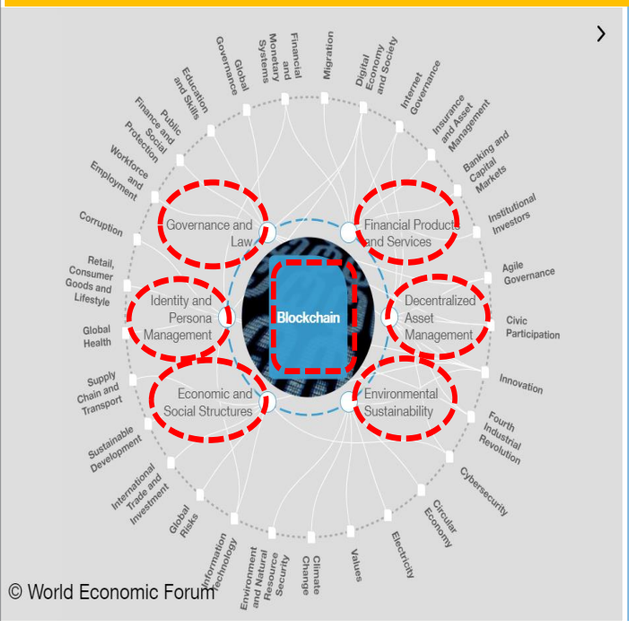
❖ 기술진보

- 1~3차 산업혁명 파급력에 어울리는 기술진보
- 약속, 위험 동시 제공
- 물리, 디지털 및 생물계 통합

❖ 이 혁명의 속도, 넓이 및 깊이는 국가가 어떻게 발전해야 하는지, 조직이 어떻게 가치를 창출하는지, 인간이 되는 것이 무엇을 의미하는지 다시 생각

◆ Blockchain은 4차산업혁명 견인하는 7대 기반기술의 하나

Blockchain



© World Economic Forum

A blockchain provides an **immutable record of transactions** performed across a network **without** the need to rely on an **intermediary**, such as a central bank.

거래 수정불가 + 중개인 불필요

It is a concept that brings together **economics and digital technologies** in a way that was never before conceived.

경제학+디지털기술

Blockchain enables not just new means by which to deliver **financial services** and support **cryptocurrencies**, but can also reshape and redefine **government**, **legal services, accounting**, **insurance**, **supply chains**, and **energy distribution**.

금융서비스, 가상화폐, 정부, 법률서비스, 회계, 보험, 공급체인 등 활용 다양

4차 산업혁명과 블록체인

지능정보기술과 블록체인

◆ 4차 산업혁명 핵심 기반기술 = 지능정보기술 (ICBM)

- IoT, 클라우드, 빅데이타, 인공지능 등 데이터 기반으로 기계에 인간의 인지 학습 추론 능력을 구현하는 기술군
- 다양한 분야에 활용될 수 있는 기반기술 성격의 "범용기술"
- New IT 시대 = 초연결, 초지능, 초융합시대 지향

  다양한 지능정보기술과 서비스가 융합되어 새로운 가치창출

  → 지능정보사회의 연결/ 융복합에는 완벽한 신뢰 프로토콜 필수적

◆ 블록체인 기술

- 디지털 환경에서 참여자간 신뢰 프로세스를 분산구조로 재설계하여 신뢰 극대화
- 단독으로는 만병통치가 아니며 타 기술과 융복합 될 때 시너지 극대
- 금융산업 뿐만 아니라 다양한 산업으로 급속도 확산되는 범용기술

4차 산업혁명과 블록체인

"2027년 까지 전 세계 GDP의 10%가 블록체인 기술로 저장될 것"

"2023년에는 국가가 세금을 블록체인에서 징수하기 시작할 것"이라고 예측

WORLD ECONOMIC FORUM

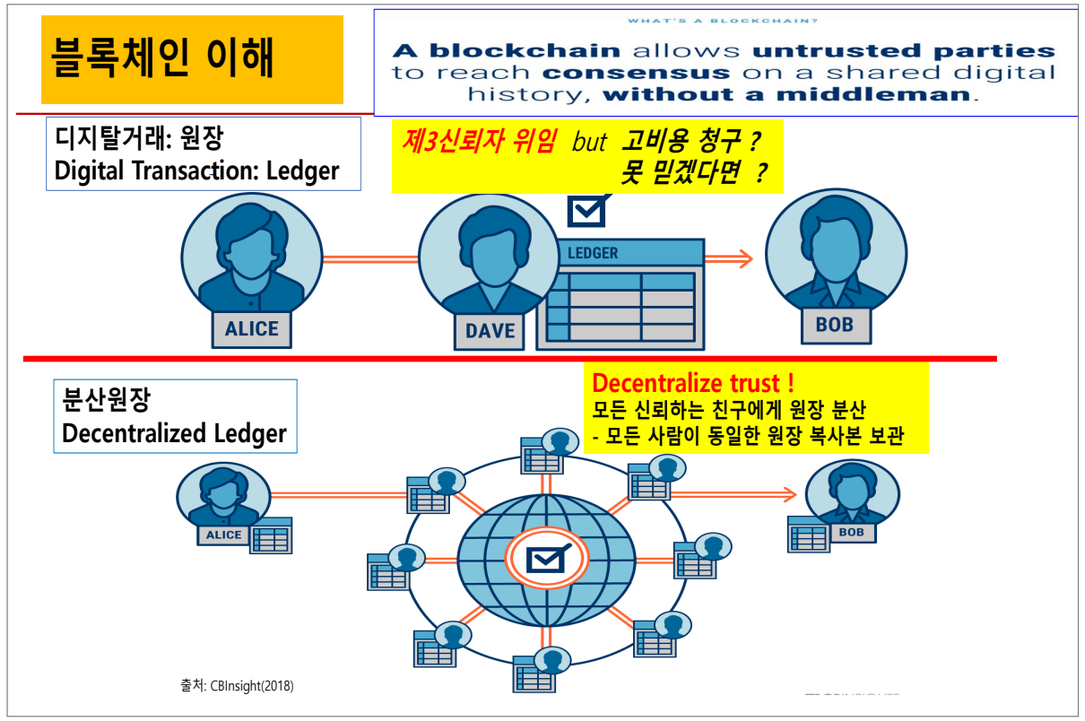
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Global Agenda Council on the Future of Software & Society

Deep Shift

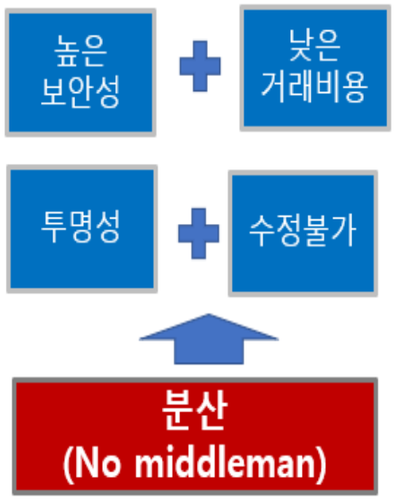
Technology Tipping Points and Societal Impact

블록체인 이해



블록체인 이해

블록체인의 특징



- 위조/해킹이 거의 불가능해 **보안성이 높고, 수정 불가**
- 거래 정보의 **투명성이 보장**
- 공인된 3자가 필요하지 않으므로 **불필요한 비용의 절감과 효율성**을 확보
- 금융업에서 블록체인을 활용할 경우
  데이터 관리비용 절감효과가 클 것으로 기대
  - 비용이 줄어들면 은행의 이익이 늘어나게 되고, 은행은 자사 고객들에게 수수료 등 거래비용을 저렴한 가격에 제공할 수 있음.
- 소비자 입장에서도 **낮은 수수료비용** 뿐 아니라 금융서비스 이용 시 훨씬 **편리해진 서비스, 거래 속도 향상** 등 다양한 혜택을 누릴 수 있음.

블록체인 이해

Different Types of Blockchains

Property	Public	Consensus	Private
Consensus Determination	All	Selected Set	One Organization
Read Permission	Public	Public or Restricted	Public or Restricted
Immutability	Nearly Impossible to Tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus Process	Permisionless	Permissioned	Permissioned

블록체인 이해

Public Blockchain

Consensus
Each node can take part in the consensus process

Efficiency
Time-intensive to propagate transaction and blocks because of the large amount of nodes.

Read Permission
Transactions in the public blockchain are visible to the public

Decentralized
Public blockchain is completely decentralized

Immutability
Record are stored on a large number of participants, making it nearly impossible to tamper transactions

Consensus Process
Everyone can join the consensus process

블록체인 이해

□ 블록체인 장점과 단점

장 점		단 점	
비용절감	o 수수료절감(제3자 공증 없음) o 보안투자비용 절감 o 시스템구축 비용절감(공개 소스로 쉽게 연결 및 확장)	미완성 기술	o 아직까지 완성되지 않은 기술 o 은행, 증권 등의 구조에 맞춰 다시 짜야 함
신속성	o 거래승인, 기록이 다소 참여자에 의해 자동 실행(T+0)	시스템 교체 이슈	o 현 전산시스템은 중앙 집중시스템(전용선과 폐쇄망에 의해 보안확보) o 시스템변경 -> 시간 및 비용
보안능력	o 분산시스템으로 해킹, 디도스 공격에 방어능력	속도와 처리용량	o 개발단계로 현 시스템 대비 속도가 느리고 대용량 커버이슈
감사기능	o 제3자 누구든 장부의 무결성 확인가능	법, 제도 개정	o 현 금융법규는 중앙 집중시스템에 의거함

블록체인 혁명

"We have come to the conclusion, unequivocally, that blockchain is the most important invention in computer science in a generation."

-Alex Tapscott, co-author with Don Tapscott of "The Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World"

블록체인 혁명

"블록체인 혁명은 제2의 인터넷 혁명"

3차산업 근간	4차산업 근간
인터넷 (1세대 인터넷)	블록체인 (2세대인터넷)
정보의 인터넷 (가치 이전 X)	**가치의 인터넷** (가치 이전) → 경제/정부 업무 향상 등 무한 가능성
Internet transformed and commoditized how society **communicates**	**Blockchain** will transform and commoditize **how** society **agrees, trusts, and transacts.**

블록체인 과 "신뢰 프로토콜"

인터넷에서 간과되던 요소는 "신뢰 프로토콜"
블록체인은 이러한 수단의 근간 제공하는 혁명적 아이디어

인터넷

정보의 전송 가능하지만
가치 (돈) 전송 불가 !!

신용확인 필요
– **강력 중개기관 필수**
거래/ 정산 기록 → 가치 이전 가능
- 불투명 / 해킹/ 불성실 인력 등

블록체인 = 신뢰 프로토콜

가치의 이전 가능

중간기관 불필요

- 암호기술(이중지불방지)
- 협업
- 정교/세련된 코드

블록체인 혁명

◆블록체인은 사회 / 경제적 혁명 일까?

로랑 를루
La Blockchain (2017)

블록체인 : 비파괴적 신뢰혁명기술
탈중앙화와 분산화를 통해
신뢰, 공유, 투명성을 보장하는 기술

1. 인터넷 가치 남용에 따른 소수특권 등장

- GAFA는 **인터넷** 기반 성장 자율 운영 시스템 정립
- But Happy Few를 탄생

→ "혁명의 불씨" 기대 불구,
통제, 불투명, 패권 방향

2. 블록체인, 신뢰 회복

- **3대 메커니즘**
  - 비대칭형 **암호화** 알고리즘
  - **탈중앙화** 시스템
  - **제3 신뢰기관 없이** 분산 방식으로 **합의** 도출하는 P2P 모델
- 네트워크 기반, 신뢰와 상호협력으로 가치창출/공유

→ 공평/투명/보안/ 위변조 불가능
→ **혁명의 싹을 틔울 역량 보유**
→ **경제 사회적 무한 잠재력**

3. 블록체인은 민주주의적 기술

- 오픈소스 기반 기술 → 분산 거버넌스 이므로 합의가 중요
- 연산작업권한 가진 소수 이용자의 힘
- 51% 룰

◆블록체인이 혁명이라면 어떤 혁명 일까? 접근 바꿔야...

로랑 를루
La Blockchain (2017)

◆ 블록체인, 기능적 관점

1. 경제
-금융거래 탈중앙화, 간소화, 중개자 배제

2. 기업 4.0
-분산자율조직 DAO모델화

3. 앱
-거래정보 및 데이터 보안

4. 거버넌스
-분권화, 합의

VS

◆ 블록체인, 역사적/이론적 관점

1. 가치
본질적 가치 보유 여부

2. 화폐
- 용도, 값어치, 발행자

3. 노동
- 무엇을 생산

4. 개인
- 자신의 존재 정의

5. 정치시회적 조직
- 운영 거버넌스

블록체인은 세상에 혁명을 가져올 도구

1. **블록체인은 혁명자체는 아니지만 – 단순 전문기술로만 보면 잘못**
2. **인류문명 발달에 기여하는 인공적 산물 → 시대 변화 가져올 잠재력**

블록체인 혁명과 문명

"블록체인으로 무엇을 할 수 있는가? (김용태, 2018)

1차산업혁명 융합
= 증기기관 + 복식부기 (장부2.0)

4차산업혁명 융합
= AI + 블록체인(분산장부/ (장부3.0)

"블록체인은 문명의 이동의 축"

1%가 쥐고 있던 권력을

99% 피어들에게 분산 이동시켜서
99%가 주인이 되는 동굴건설체 건설하는 알고리즘

"소유의 종말" : 디지털 노마드 시대

산업문명 양식 : 생산과 소유 문명

블록체인 양식 : 연결과 공유 문명
비움/ 깨뜨림 / 버림의 철학

유목민의 질문 : "집 " 이 아닌 "길 "

영국정부
"블록체인은 권리장전을 새로 창조하는 것만큼이나 중차대한 사건으로 기록될 만큼 그 영향력이 지대"

블록체인을 통한
초신뢰사회 :

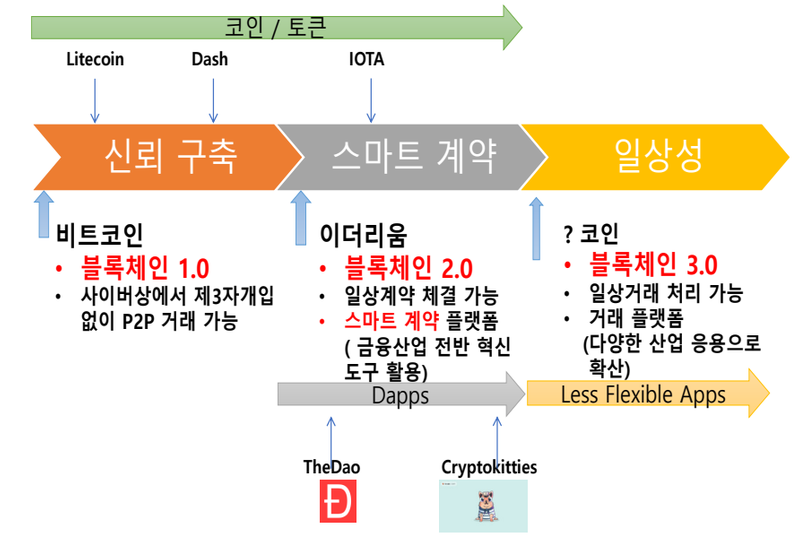
-금융/유통/정부/정치/보안 혁명

*https://www.youtube.com/watch?v=_a2x_D8p5KQ&t=267s

4차산업혁명시대
전 분야의 근본적
재정립을 추동할
파괴적 혁신 기술

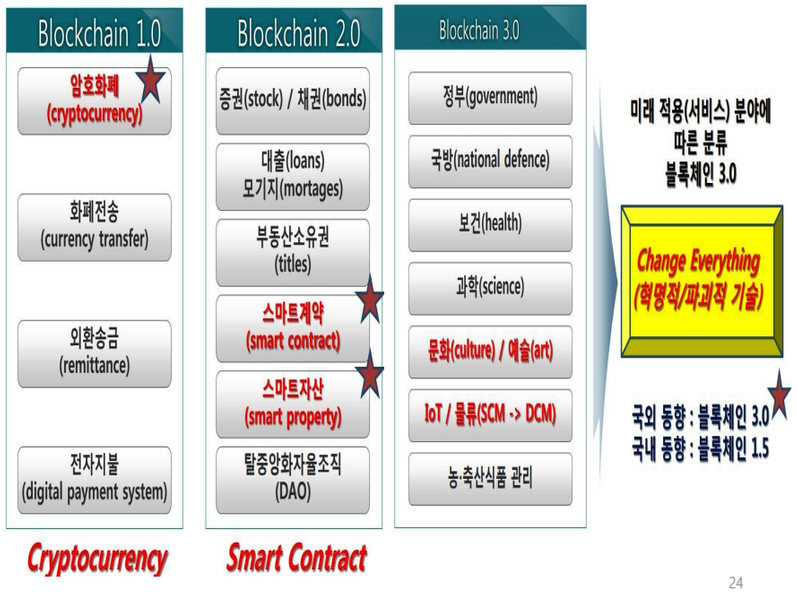
- KT경제경영연구소 (2019)

블록체인 패러다임 변화



멜라니 스완 ("Blockchain : Blueprint for a New economy" 2015), 이영환 (2017)

블록체인 생태계

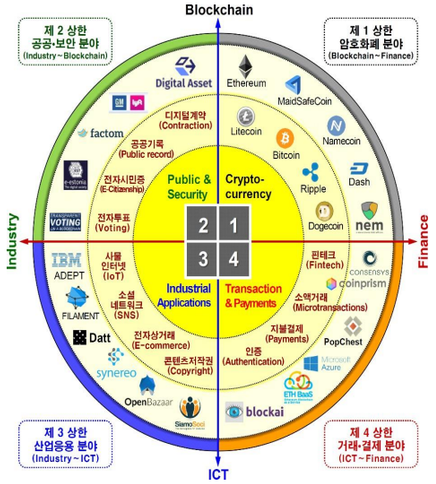


자료: 박성준(2017), 블록체인 기술과 디지털 경제의 전망

블록체인 활용

블록체인 활용

□ 블록체인 활용분야



탈중앙화, 탈중개화를 기반으로, 기존의 경제적 가치와 정보(화폐, 자산, 재산 혹은 신분)에 대한 새로운 사업기회 창출

5 ways blockchain technology is changing the world

1. Banking

2. Raising capital
ICO → IEO

3. Agriculture
Farmers 적정가격 보장 / consumers 원산지 파악 / retailers 구매 적법성 보장

4. Supply chain management
공급체인관리 - 추적 가능성 및 투명성
IBM partnership with Maersk : "digitised global trade"

5. Artificial intelligence
AI 에 정확한 데이터 제공
smart contract technology 로 AI 특정 행동 수행 지시 (재난 발생 방지 행동 요령 등)

https://www.information-age.com/5-ways-blockchain-technology-changing-world-123470689/

블록체인과 IoT / 빅 데이터 / AI 융합

◆IoT 기술 :

핵심 기술: 센싱 / 케넥티비티 / 플랫폼

이슈 :
1. 사물인터넷 기기 폭증 전망

2. 기기센서 데이터의 수집, 통합, 분석 과정에서의 인증, 보안, 운용 효율성 등이 필수적
→ 보안 / 개인정보보호 중요

◆블록체인 융합

1. 보안성 제공 및 부정 조작 불가능

2. 운용비 절감
불필요한 중복적 중개자 제거

3. 내부 암호화폐 활용
스마트머신 간 안전한 자율거래

◆빅데이터 분석 :

인터넷/모바일/센서 등 방대한 데이터 분석해서 새로운 가치 창출하는 기술

이슈 :
1. 개인정보 비식별조치 가이드라인
*기준 강화(완화)시 데이터 가치하락(상승)

2. 중앙집중 관리-불투명/ 위변조 우려
3. 데이터 수집 시간 / 보관 비용

◆블록체인 융합

1. 데이터 안전, 신뢰 보관
2. 데이터 무결성과 개인정보보호→
데이터 융복합 시장 창출

예: 차량기반 IoT +빅데이터 +블록체인
→ 보험상품 설계 / 숙박예약/ 차량 타겟마케팅 서비스 등

예: 신용보강으로 신용평가 개선 →
투자리스크 하락으로 신규고객 발굴

◆인공지능 (AI)

기계가 알고리즘을 통해 인간처럼 사고, 학습,판단할 수 있게 하는 인공적 지능

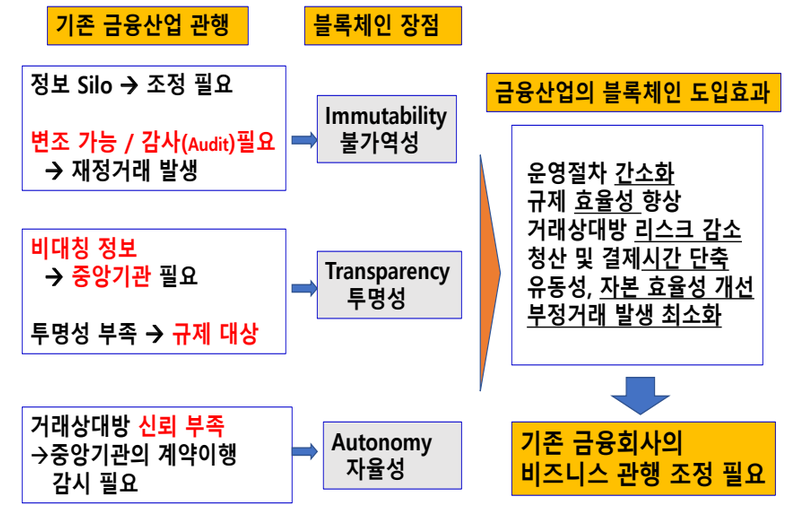
이슈 :
1. 다양한 더 많은 데이터가 주어질수록 AI의 가치가 풍부
2. 블록체인이 제공한 가치 정보를 활용하여 지속적으로 증강된 정보 생산

◆블록체인 융합 (상호 보완)

1. 개인이 데이터를 소유, 활용, 거래 가능한 최적 플랫폼 제공
2. AI가 학습 가능한 고품질 데이터 제공 → 양적/질적/가치있는 데이터 제공 및 지적자산화

◆ AI 는 블록체인을 더 똑똑한 구조로 지능화 – 상호 한계 보완 (Dynamic Smart Contract)

금융산업과 블록체인 활용



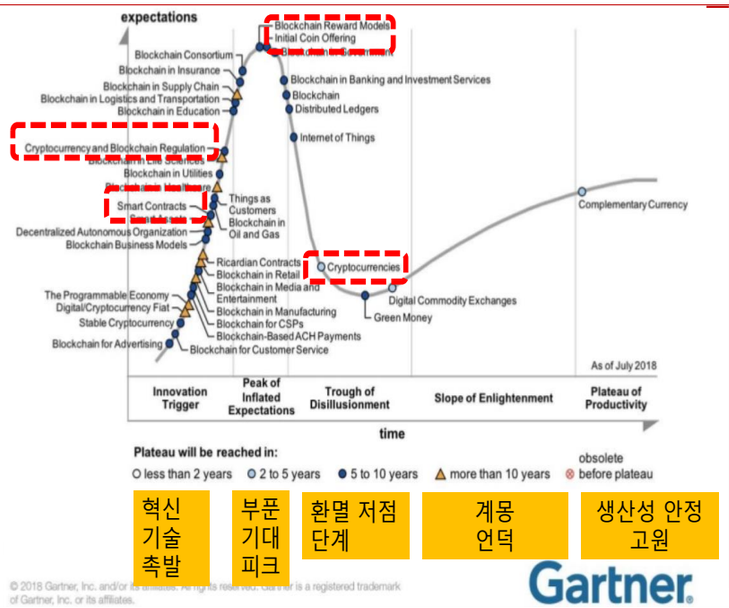
https://media.consensys.net/welcome-to-the-fourth-industrial-revolution-19-blockchain-predictions-for-2019-8b2e542bf86a

Welcome to the Fourth Industrial Revolution — 19 Blockchain Predictions for 2019

Andrew Keys Follow

Jan 13 · 16 min read

Hype Cycle for Blockchain Business, 2018



혁신 기술 촉발 | 부푼 기대 피크 | 환멸 저점 단계 | 계몽 언덕 | 생산성 안정 고원

Gartner

In 2017 cryptocurrencies took the world by a storm.

The price of Bitcoin shot up to over $20,000 → $ 4,000 → $8,000

The average ICO returned well over 10x.

ICO funding surpassed traditional VC funding.

Blockchain technology emerged as the new buzzword of choice by executives.

Is this all just hype?

https://www.blockchain-expo.com/2018/10/blockchain/future-of-blockchain-technology/

THE FUTURE OF BLOCKCHAIN TECHNOLOGY: TOP FIVE PREDICTIONS FOR 2030

By: Kate Mitselmakher
11, October, 2018
Categories: Blockchain -

Prediction # 1: Government Crypto

By 2030, most governments around the world will create or adopt some form of virtual currency.

Prediction #2: Trillion-Dollar Protocols

By 2030, there will be more trillion-dollar tokens than there will be trillion-dollar companies

Prediction #3: Blockchain Identity for All

By 2030, a cross-border, blockchain-based, self-sovereign identity standard will emerge for individuals, as well as physical and virtual assets.

Prediction #4: World Trade on a Blockchain

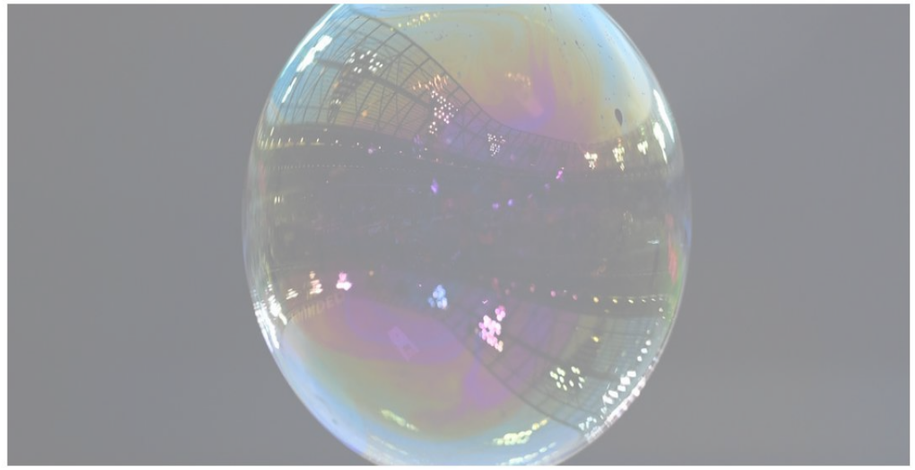
By 2030, most of world trade will be conducted leveraging blockchain technology.

Prediction #5: Blockchain4Good

By 2030, significant improvements in the world's standard of living will be attributable to the development of blockchain technology.

https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business/

These 11 questions will help you decide if blockchain is right for your business



Blockchain is not meant to be a workaround Image: Reuters

블록체인 경제

홍기훈 교수
(홍익대학교)

블록체인 경제

홍기훈, Ph.D, CFA, FRM
홍익대학교 경영대학

06. 18, 2019
대한전자공학회

블록체인 경제?

- 가상화폐 → 여기에 왜 (화폐)경제학이 필요한지?
- 플랫폼 경제 → 정확히 블록체인 specific 은 아님
- 공유경제, 분산경제 → ?? 경제라는 단어만 들어갔지 개념 자체도 애매하고 경제학에서의 '경제'의 개념과는 거리가 있음
- 코이노믹스 → 행동경제학을 잘못 적용
- 나머지 → 수요, 공급, 탄력성, 안전자산, capital flight 등 다양한 경제학의 개념들을 적용하지만 잘못 된 또는 왜곡 된 사용

Yap Island

The Island of Stone Money (1910)

금속물질 생산되지 않아 돌을 돈으로 사용
다듬는 수고와 공을 들인 돌은 노동의 상징

Fei - 크고 두꺼운 돌바퀴
약 600km 떨어진 섬에 있는 석회 이용
채석, 가공 후 카누와 뗏목으로 운송

화폐거래 시 운반하기 어려운 페이를 지불해야 할 경우 새 주인은 그 돌이 자신의 것이라 인정을 얻고 원 주인 집안에 그대로 남겨둠

매우 큰 돈을 가졌지만 페이를 가지고 있지 않은 집안 예

독일이 식민지 시절 도로 보수명령을 이행하지 않은 집의 페이에 검은 십자표시

우리도 은행에 돈을 넣어놓고 거래에 이용함 → 화폐의 근간은 신뢰!

화폐경제학 101

자급자족 > 물물교환 > 실물화폐 > 금속화폐 > 지폐 > 예금화폐

화폐: 통용되는 지불 수단인 통화로 정의되다가 화폐의 범위가 확대되면서 총통화나 총유동성으로 정의되고 있다. 인류 생활과 함께 화폐가 발달하면서 화폐의 기능은 **가치척도와 교환 수단**에서 **지불 수단과 가치저장 기능**으로 변화하였다.

화폐공급: 화폐를 본원통화와 파생통화로 구분할 때 본원통화의 공급은 중앙은행에 의해 이루어지고 파생통화의 공급은 시중은행에 의해 이루어진다.
→ 중앙은행은 발행을 독점, 공급을 독점하지 않음

핵심연구주제: 화폐공급의 외생성 (통화학파) 과 내생성 (은행학파)
화폐량 (공급) 의 변화가 경제활동 수준의 변화를 일으키는 '원인' 인가 혹은 그 '결과' 인가에 대한 논쟁

통화학파 vs. 은행학파

통화학파	은행학파
David Ricardo, Alfred Marshall, Arthur Cecil Pigou, Friedrich August von Hayek, Milton Friedman	Henry Thornton, John Fullarton, Thomas Tooke
경제에 있어 화폐의 역할은 외생적이기 때문에 화폐공급은 경제활동에 영향을 받지 않고 경제 외적 요인 (예를 들어 중앙은행)에 의해 결정되며 경제활동에 영향을 미치는 지배적 요인이라고 주장	화폐를 경제활동의 결과로 간주하고 화폐의 공급은 화폐수요에 의해 이루어진다고 주장 → 시장논리에 더 가까움
중앙은행이 통화정책을 이용하여 통화량 조절을 통한 완전고용, 물가안정, 국제수지항상, 경제성장촉진 등을 추구	전 세계적으로 통용될 수 있는 암호화폐의 수요가 실제 그러한 화폐를 탄생시키는 현상
2008년 금융위기가 통화학파가 주도하는 통화정책의 결과였고 그렇기 때문에 통화학파의 몰락이라고 보는 경제학자들이 있음 (물론 실제로 몰락하지는 않음)	2008년 금융위기의 반동으로 중앙은행의 통제를 벗어난 비트코인이 관심을 받게 되었고 필자는 이러한 현상이 기존의 중앙은행 통화정책 중심의 경제정책을 주도해온 통화학파에서 은행학파로 패러다임을 움직이고자 하는 수요가 존재하기 때문이라 생각

통화정책

기준금리를 이용한 통화량 조절을 통한 경제 영향력 감소 예상

예를 들어 중앙은행이 기준금리를 내리면

전반적 이자율 하락 → 저축이 덜 매력적이 되어 저축이 감소

낮은 이자율을 통해 더 많은 부채를 감당가능

화폐공급 증가 → 투자가 활성화를 통해 경제가 더 빠르게 성장

전 세계적으로 통용되고 공급량이 고정되어 있는 암호화폐가 존재하면 한 국가에서 기준금리를 낮춘다면 사람들은 자신들의 저축을 암호화폐로 바꿀 것 → 통화정책의 영향력 감소

세계적으로 통용되는 암호화폐가 정착한다면 우리들은 중앙은행의 기준금리 발표에 지금 보다는 덜 관심을 가지게 될 것

시뇨리지

흔히 중앙은행의 통제에서 벗어난 화폐의 등장은 시뇨리지 감소를 가져와 추가 세금을 발생 시킬 것 이라 말함 → 일단 '추가' 라는 말이 맞지 않음

중앙은행이 기준금리를 낮추어 통화공급을 늘려 인플레이션이 발생하면 기존 통화에서 실질가치가 줄어들고 그만큼의 부가 중앙은행으로 가기 때문에 인플레이션은 시뇨리지를 통한 세금의 한 종류

비트코인이나 이더리움이 화폐로 정착한다면 위에서 말한대로 기준금리를 통한 통화정책이 어려워지기 때문에 시뇨리지를 통한 인플레이션 세금의 규모는 감소할 것 → 시뇨리지 감소

그러나 (암호화폐를 포함한) 가상화폐 활성화를 통해 작은 단위, 특히 발행비용이 높지만 화폐의 가치가 낮아 역(逆)시뇨리지(화폐발행을 통한 손실)의 주요 원인인 동전의 이용 감소 예상 → 시뇨리지 증가

암호화폐의 정착이 시뇨리지를 증가시킬 지 감소시킬 지는 정확히 알 수 없음 → 시뇨리지 감소의 가능성은 반만 맞는 이야기

그레샴의 법칙

[기자수첩] 그레샴의 법칙

홍기원 기자 | 입력 2017.03.05 12:56 | 댓글 0

[한국농정신문 홍기원 기자]

좋은 품질의 물건과 그렇지 않은 물건이 시장에서 경쟁하면 좋은 품질이 살아남는다는 게 일반적인 상식이다. 하지만 중증 현실에선 정반대인 현상이 일어난다. 박근혜·최순실 게이트가 보여준 현실은 '악화가 양화를 구축한다는 말로 집약되는 그레샴의 법칙을 다시 곱씹어 보게 한다.

그런데 우리나라 축산의 오늘날은 어떠한가. 악화가 양화를 구축하고 있지는 않은가.

AI와 구제역 사태에서 정부는 축산농가에게 방역의 책임을 돌렸다. 동시에 계란가격이 뛰자 앞뒤 가리지 않고 수입 계란을 들였다. 정부가 선택한 두 조치는 서로 모순된다.

인쇄 스크랩 글꼴 + −

한경BUSINESS

삼성전자, '일등'에 도취해선 안 돼 본문듣기 설정

기사입력 2017-07-31 17:21 기사원문

공감 댓글

[한상춘의 국제경제 심층 분석]
초불확실성 시대 진입…얘를 제쳤지만 '승자의 저주' 우려해야

[한상춘 한국경제 객원논설위원 경 한국경제TV 해설위원] 혼히 요즘을 '규범의 혼돈(chaos of norm)' 시대라고 부른다. 특히 도널드 트럼프 정부 출범 이후 그렇다.

각국의 이기주의와 보호주의로 제2차 세계대전 이후 '자유무역'을 목표로 지향해 왔던 '관세와 무역에 관한 일반협정(GATT)'과 '세계무역기구(WTO) 체제'가 근본적으로 흔들리고 있기 때문이다. GATT·WTO 체제를 주도했던 미국이 이탈한다면 다른 국가가 지키기는 더 어렵다.
환태평양경제동반자협정(TPP)·파리기후협약 등이 미국을 배제한 차선책이 논의되고 있지만 얼마나 성과를 거둘 수 있을지는 미지수다. 경제적 실리에 의해 좌우되는 국제 관계에서는 철저하게 '그레샴의 법칙(악화가 양화를 구축한다)'이 적용되기 때문이다.

Home > 다시보기 > 뉴스M

[여의도는 지금] '신선한 파격' 문재인의 리더십, 평가는?

기사입력 2017-05-11 16:27 | 최종수정 2017-05-11 16:46

그런 모습을 볼 수 있었던 게 커뮤니케이션을 관리하는 팀이 그만큼 많았기 때문입니다.

그래서 국민과 어떻게 소통하는지에 대한 것을 행동으로 보여주시고 또한 시스템적으로도 국민과 다가설 수 있도록 해 주는 것.

왜냐하면 이제 6개월 정도의 허니문(=> 곧나면 그레샴의 법칙이라고 하지 않습니까?

분명히 가짜 뉴스, 또 악화 뉴스가 아주 나쁜 이미지를 자꾸 주게 될 수 있습니다.

그러한 것들이 벗어나려면 지금 좋을 때 더 많이 다가서는 이미지 전략을 하신다면 말씀하셨던 패권, 친문 패권주의 그런 부분에 대한 것들을 많이 해결하시지 않나 싶습니다.

오피니언 [탐정칼럼] 강봉균發 한국판 양적완화, 악화가 양화 구축하나

칼럼

세종=정원석 기자

기사 100자평(1)

입력 : 2016.04.01 04:00

영국 풍자 만화가 제임스 길레이의 1797년작(作) '위기에 빠진 영란은행(the Old Lady of Threadneedle Street in Danger)'이라는 그림은 중앙은행과 정부의 관계를 신랄하게 보여준다.

여기는 영란은행(Bank of England)이라는 자물통을 지키고 있고, 신사는 구애하는 척하면서 은근슬쩍 여기의 호주머니를 탐한다. 신사는 당시 영국 수상 윌리엄 피트, 여기는 영란은행이다. 여기는 이렇게 외친다.

"그토록 오랫동안 절절을 지키라고 해 놓고서, 그것을 당신이 한꺼번에 탕할 수 있도록 해 달라고 하다니요(What I have kept Honor untainted so long, to have it broke up by you at last)"

그림을 통해 길레이는 나폴레옹과의 전쟁 비용을 마련하기 위해 영란은행의 금태환 의무를 포기시킨 영국 정부를 비판했다. 금태환 의무를 없애를 테니 무한정 돈을 찍어서 정부에 대출하라는 게 피트 수상의 요구였다.

그레샴의 법칙

"악화가 양화를 구축한다" (bad money drives out good)

나쁜화폐 vs. 좋은화폐

일반적인 질문: 가상통화가 명목화폐를 구축할 것인가?

좋은화폐: 명목화폐 vs. 나쁜화폐: 가상통화 → 가상통화가 명목화폐를 구축
??????????????
그럴 수도 있지, 대충대충

흔히 '나쁜 것이 좋은 것의 자리를 빼앗는다' 라는 말을 하고 싶을 때 자주 쓰여지는 잘못 된 적용 → 가치평가의 맥락이 아님을 잘못 이해

그레샴의 법칙을 현재의 가상통화 현상에 대입하기 위해서는 악화와 양화에 대한 정확한 정의와 이 법칙을 이야기 하게 된 상황적 이해가 필요

1525년 프로이센 공국

여러 제후국으로 나뉘어져 여러 종류의 화폐를 사용하던 독일

튜튼기사단의 리투아니아 압박 → 폴란드 – 리투아니아 연합 → 1410년 탄넨베르크 전투 → 1453~1466년 13년 전쟁 → 폴란드의 봉신

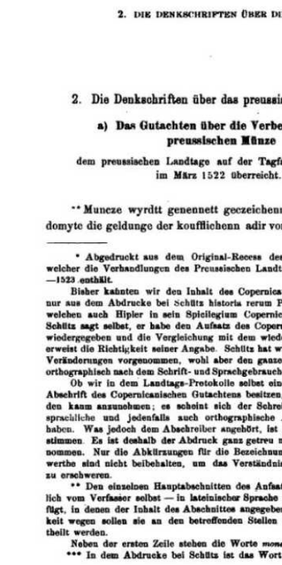
16세기 초 알브레히트 폰 호엔촐레른의 반란 → 전황이 어려움
→ 신성로마제국에 도움 요청, 카를 5세가 거절
→ 루터의 설득에 의해 신교개종, 튜튼기사단 해체 (최초의 신교국가)

1525년: 폴란드 왕 지그문트 1세가 프로이센공작 작위를 수여

지속적인 폴란드와의 전쟁자금을 조달하기 위해 발행한 채권의 가치를 낮추기 위해 1517, 1519, 1526년에 은화내 은 함유량을 감소시킴

폴란드 왕과 프로이센 공은 화폐개혁을 추진하고자 함
니콜라스 코페르니쿠스: Monetæ cudendæ ratio (주조국에 관하여)

Monetæ cudendæ ratio



2. DIE DENKSCHRIFTEN ÜBER DIE MÜNZE. 21

2. Die Denkschriften über das preussische Münswesen.

a) Das Gutachten über die Verbesserung der preussischen Münze

dem preussischen Landtage auf der Tagfahrt zu Graudenz im März 1522 überreicht.*

** Munecze wyrdit genennett geczeichennt Goldt, adir Sylber, domyte die geldunge der koufflichenn adir vorkoufflichenn dinge***

* Abgedruckt aus dem Original-Recess des Danziger Stadtarchivs, welcher die Verhandlungen des Preussischen Landtags aus den Jahren 1515—1523 enthält.

Bisher kannten wir den Inhalt des Copernicanischen Münz-Gutachtens nur aus dem Abdrucke bei Schütz historia rerum Prussicarum (S. 480—482), welchen auch Hipler in sein Spicilegium Copernicanum aufgenommen hat. Schütz sagt selbst, er habe den Aufsatz des Copernicus „von Wort zu Wort" wiedergegeben und die Vergleichung mit dem wiederaufgefundenen Originale erweist die Richtigkeit seiner Angabe. Schütz hat wirklich keine wesentlichen Veränderungen vorgenommen, wohl aber den ganzen Aufsatz sprachlich und orthographisch nach dem Schrift- und Sprachgebrauche seiner Zeit umgewandelt.

Ob wir in dem Landtags-Protokolle selbst eine diplomatisch treue Abschrift des Copernicanischen Gutachtens besitzen, ist aus mehreren Gründen kaum anzunehmen; es scheint sich der Schreiber vielmehr mancherlei sprachliche und jedenfalls auch orthographische Aenderungen erlaubt zu haben. Was jedoch dem Abschreiber angehört, ist gegenwärtig nicht zu bestimmen. Es ist deshalb der Abdruck ganz getreu nach dem Manuskripte genommen. Nur die Abkürzungen für die Bezeichnung der Münzen und Münzwerthe sind nicht beibehalten, um das Verständniss nicht unnöthigerweise zu erschweren.

** Den einzelnen Hauptabschnitten des Aufsatzes sind — wohl schwerlich vom Verfasser selbst — in lateinischer Sprache Randbemerkungen beigefügt, in denen der Inhalt des Abschnittes angegeben wird. Der Vollständigkeit wegen sollen sie an den betreffenden Stellen unter dem Texte mitgetheilt werden.

Neben der ersten Zeile stehen die Worte *moneta quid sit definitur*.

*** In dem Abdrucke bei Schütz ist das Wort *dinge* ausgefallen.

Die denkschriften über das preussische münzwesen
(프러시아 주화에 관하여)

전쟁자금 조달을 위해 돈을 빌린 도시들이 대부분의 채무자

1517, 1519년 은 함유량 감소는 채권자들에게 불리

프로이센의 금융안정성을 위협
도시들은 은 함유량을 지속적으로 낮춤

Debased coinage drives undebased coinage out of circulation

세가지 화폐 정책제안: 1) 폴란드와의 고정환율제, 2) 1418년 수준으로 은 함유량 복귀, 3) 화폐개혁 → 실패, 1526년에 다시 은 함유량 낮춤

그레샴의 법칙

엘리자베스 1세에게 실링 (영국 은화) 을 만들어 내는데 필요한 은의 부족 현상이 왜 일어나고 있는지 설명하기 위해 쓴 편지

헨리 8세는 전쟁자금을 충당하기 위해 92.5% 였던 기존 은화의 은 함량을 33%까지 낮추어 발행 → 시뇨리지의 한 형태, 결국 증세

1525년 프로이센, 1550년 잉글랜드의 공통점:
직접 증세가 아닌 지나친 시뇨리지로 정부지출 (특히 전쟁자금) 을 충당

은 함량이 높은 은화를 사용하지 않고 은 함량이 낮은 은화만을 사용
→ 은 함량이 높은 은화는 녹여서 더 많은 은화로 만들 수 있었기 때문
→ 화폐 공급대비 은 부족: 결국 인플레이션

그레샴의 법칙의 두 화폐는 경제 내에서 같은 명목가치를 지니지만 다른 내재가치를 가져야 함 → 1) 거래가치는 같은데 2) 실제가치가 달라야 함

가상화폐와 명목화폐는 쓰임이 다를 확률이 높음 (선호 경제주체 다름)
두 화폐 모두 내재가치가 0, 실제가치에 대한 판단은 어려움

헨리 8세 (1509 – 1547 통치)

헨리 7세는 가혹한 징세로 인기가 없었음
징세관 Edmund Dudley 를 처형하여 인기몰이

6번의 결혼, 2명의 왕비 처형, 종교개혁

1511 – 16: 프랑스, 스코틀랜드 (캉브레동맹전쟁)
1521 – 26: 프랑스 (이탈리아전쟁)
1526 – 30: 신성로마제국 (코냑동맹전쟁)
1544 – 50: 스코틀랜드, 프랑스
→ 재위 39년: 20년 전쟁, 19년 ~~여자~~ 후계자 문제

1527: 캐서린과 이혼 시도 → 실패
1531: 캐서린 추방, 1533: 앤 불린과 결혼
1534: 수장령 선포, 종교개혁
1536: 앤 불린 처형, 제인 시무어와 결혼
1537: 에드워드 6세 탄생
1540: 앤 결혼이혼, 캐서린 하워드 결혼
1542: 캐서린 하워드 처형
1543: 캐서린 파와 결혼

지속된 전쟁
+ 종교개혁
+ 6번의 결혼

돈돈돈돈!

가상통화 vs. 명목화폐

가상통화가 명목화폐를 구축한다

1) 가상통화와 명목화폐는 쓰임이 다를 확률이 높음

2) 실질가치가 서로 다를 것은 어떻게 알지??

교훈:

비슷해 보인다고 막 가져다 적용하지는 말자!

고정환율제 vs. 다중화폐제

고정환율제	다중화폐제
금본위제, 브레튼 우드 체제, EU, 현재 중국, 대부분의 개발도상국	민간화폐제도 (북송, 근대유럽, 미국의 자유은행시대 등), 스위스, 남미 (달러)
장점: 편리함, 단순함 단점: 금융위기라고 불리우는 조정과정, 비대칭적인 GDP 배분	장점: 효율성, 유연성, 자율성, 안정성 단점: 정보비대칭 또는 화폐발행력 상실로 인한 화폐정책 포기
비트코인을 비롯한 암호화폐들이 새로운 고정환율제의 기폭제가 될 것이라는 주장의 가장 중요한 가정은 명목화폐의 Crowding Out → 이론적, 직관적, 실증적으로 분석해 보았을 때 사실이 아닐 확률이 높음	전 세계적으로 통용되는 암호화폐의 등장은 국제화폐 + 로컬화폐 라는 다중화폐제를 촉진시킬 확률이 높음 → 민간화폐제도와 비슷하나 레버리지와 화폐공급량이 조작(?) 불가라는 점에서 차이 있음

고정환율제: 브레튼 우즈 체제

비트코인을 기준으로 나머지 알트코인을 거래: 브레튼 우즈 체제 처럼..
비트코인이 미국 달러의 역할?
역시나 브레튼 우즈 체제의 배경에 대한 정확한 이해가 선행 되어야 함

세계 2차대전으로 인해 대부분의 유럽경제는 파탄
전후 주요 국가에서 초인플레이션 발생, 화폐가치 급락

전간기에 포기한 금본위제로의 부분적 복귀 현상 → 화폐가치의 안정화
압도적으로 많은 금을 보유한 미국 달러는 우위를 차지

화이트: 채권국 (미국)의 환율안정 중시
케인즈: 채무국 (영국)의 국제신용요건 완화

미국 승리

완전고용과 물가안정을 촉진하는 동시에 국제무역을 제한하지 않으면서도 대외균형을 달성할 수 있게 하는 국제통화제도를 설계

모순적: 고정환율제는 무역을 원활하게 해주지만 국내 정책목표를 달성하려면 무역 불균형을 해소할 수단이 없어 양자택일을 해야만 함

고정환율제: 브레튼 우즈 체제

1개의 기준통화와 N-1 개의 통화로 구성되는 금본위제
→ 국제공조의 금본위제, 이미 경험했음

브레튼 우즈를 정말 스페셜하게 만들어 주는 것은 IMF
고정환율제가 가져오는 경직성을 완화하려는 시도

회원국들은 국내 경제목표를 달성하기 위해 IMF 에서 대출 가능
→ IMF 펀드가 회원국들이 낸 것이기 때문에 결국 연대 보험

국제수지가 근본적인 불균형이라는 IMF의 동의가 있으면 달러 환율을 조정할 수 있음, 단 미달러에는 적용 못함
→ 상식적, 합리적, 50, 60년대 경제성장을 주도

유동성 딜레마: 금의 공급은 한정되어 있기 때문에 기축통화 국가의 무역수지가 국제 유동성 결정 → 미국은 중용을 지켜야 함, 문제가 생기면?

다른 통화는 능동적으로 평가가치 변경가능, 미달러는 안되기 때문에 미국의 국제수지 조정이 매우 어려움

유럽 경제의 빠른 성장과 미국의 국제수지 적자 누증, 통화위기 발발

비트코인 vs. 알트코인

비트코인을 기축통화로 알트코인을….

금? 고정? IMF? 잉????

교훈:

비슷해 보인다고 막 가져다 적용하지는 말자!

가상화폐는 안전자산인가?

- "지난주 미국과 북한의 군사적 긴장이 불거졌던 때 비트코인이 안전자산으로 인식된 것도 호재가 됐습니다." (YTN, 2017년 8월 16일)
- "'비트코인=안전자산' 인식… 한 달 만에 가격 두 배로 급등" (중앙SUNDAY, 2017년 8월 20일)
- "비트코인, 이더리움, 리플, 라이트코인 등 가상화폐가 안전자산인지 위험자산인지를 놓고 갑론을박이 벌어지고 있다" (뉴시스, 2017년 8월 22일)

가상화폐는 안전자산인가?

- 안전자산(risk-free asset)이란, 위험이 없는 금융자산을 의미하고 무위험 자산이라고도 함.
  - 금융적 투자에는 일반적으로 채무불이행위험과 시장가격변동위험이 수반되는 데, 안전자산은 채무불이행의 위험이 없는 자산이다.
  - 비트코인은 일단 안전자산은 아님.
- 안전자산이 아닌 자산피난처(safe haven)를 생각하고 글을 쓰면서 안전자산(risk-free asset)이라는 단어를 잘못 선택한 것이 아닐까 생각.
  - 자산피난처란, 전반적인 시장의 상황이 좋지 않을 때 가치를 유지하거나 가치 감소가 덜한 투자자산을 의미.
  - 자산피난처의 역할의 자산은 가치변동성이 높지 않고 다른 자산이나 시장과의 수익률 상관관계가 낮은 특성이 있음.
  - 금과 미 재무성 증권(Treasury Bill)이 대표적.

자산 피난처

- 환 시장의 변동성이 커지면 유로, 파운드, 레알, 위안 등 과 같은 통화자산의 가치가 하락 할 위험 또한 높아짐.
  - 딜러들이 생각하기에 자산의 가치가 하락할 위험이 상승할 가능성 보다 높다고 생각한다면 상대적으로 가치변동성이 작은 금을 대체자산으로 선택하여 통화에 투자한 자금을 회수하여 일시적으로 금을 피난처로 삼기 때문에 자산피난처라고 부르는 것.
- 즉 자산피난처는 시장상황이 나빠지면 (변동성 증가와 가치하락 확률 증가), 상대적으로 가치의 변동성의 낮은 자산 피난처에 자본이 집중됨.

비트코인!

- 비트코인 수익률과 거래 데이터를 이용하여 분석한 논문 (Baur, Hong and Lee, 2016)의 결과에 따르면 실제로 금과 같이 자산피난처로 쓰이는 듯한 현상이 일어 남.
  - 즉 시장에 악재가 연달아 일어나면 통화나, 주식 또는 다른 위험자산에 투자되어 있던 자금이 회수되어 비트코인에 투자되는 현상이 일어난다는 이야기.
- 자세히 데이터를 분석을 통해 분명 금과 같은 현상이 일어나기는 하지만 그 이유가 다름을 위 논문은 밝혀냄.
  - 금은 변동성이 작아 위험의 노출을 줄여 가치를 보존하고자 하는 투자자들이 피난처로 사용
  - 비트코인은 나빠진 시장상황으로 인해 낮아진 기대수익률을 높이기 위해 투기적인 성향을 가진 투자자들이 비트코인의 보유비중을 높이는 것을 알 수 있었음.
  - 즉 금과 비트코인은 시장 상황이 나빠질 때 자산이 몰리는 비슷한 현상을 보이지만 그 이유는 정 반대라는 의미.

민간화폐제도: 북송 (10, 11 세기)

민간화폐: 17C 영국, 18C 스코틀랜드, 19C 미국 → 하이에크 (통화학파)
국가가 향후 받을 세금을 담보로 레버리지를 이용 시장에 유동성 공급
가상화폐 현상과 모티베이션이 완전히 다름 → 역시나 잘못된 적용

사천성: 산세가 험하여 철전 휴대 어려움 → 수표의 일종인 교자 발행

11×19cm 의 크기, 발행일자, 발행순차, 일련번호, 태환가, 계, 관인
교자포호에서 발행, 교자를 제시하면 그에 상응하는 철전으로 교환
발행한 상인이 파산, 대량의 교자를 발행하여 철전을 모으고 도피

1004년: 인가제로 바꾸면서 16호의 부유한 상인들만 허가 → 공신력
1023년: 익주에 교자무 설치, 국가화폐로 발행 → 제도권 흡수
사인에 의한 교자 발행 금지

발행이 저렴한 화폐의 등장! → 국가 재정 확충의 유혹
요, 서하, 금과 전쟁 자금: 준비금 없이 교자발행 증가를 통해 조달
인플레이션 유발, 교자 교환 시 액면가의 20% 정도밖에 받지 못함
1105년: 기존 교자 단위의 1000배인 민을 이용하는 전인이라는 화폐 발행

신뢰, 신뢰, 신뢰, 신뢰

통화의 태환성

태환성: 자국통화의 보유자가 그 통화를 **일정교환비율**로 타국통화와 어떠한 목적에서든지 교환할 수 있는 권리 → 고정환율제와 유사

통화 태환성에 의하여 국제거래의 환 위험 감소: 국내에 없으면 외국에서 사면 되지, 외화를 받아도 항상 같은 자국통화 수령

외환보유고가 충분하지 못하면 통화 태환성 정지 → 익숙한 이야기!

화폐는 종이 조각: 신용과 합의
법정통화: 정부의 징세능력과 무관 (미래의 세금에 대한 권리 아님), 단지 금전채무에 있어 채권자가 받아들여야 하는 의무만 있음

결국 통화의 태환성은 신용과 합의 그리고 국가의 경제성에 기반
가상화폐가 진정한 의미의 화폐가 되려면 태환성에 대한 고민 필요

가상화폐는 그 자체로도 충분히 혁신적
투기, 포장, 호도, 과장, 여론몰이, 우기기 보다는
신뢰를 쌓는 과정이 통화역할 수행에 더 필요

블록체인 : 디지털자산혁명

인 호 교수
(고려대학교)

스마트컨트랙트 기술

인 호 교수

고려대 블록체인연구소 연구소장

1. 스마트컨트랙는 무엇인가?

2. 스마트 컨트랙트로 무엇을 할 수 있는가?

3. 스마트컨트랙트의 기술 이슈

4. 결언

오픈 플랫폼 기반 생태계 조성 및 시범사업으로 선도 필요

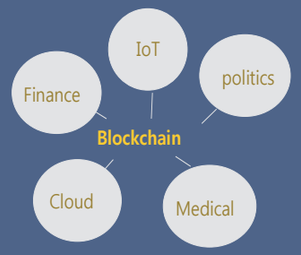
블록체인 SC R&D 투자 → 기술이전 및 시범사업 추진 → 글로벌 표준화/ 기술 선도 → 글로벌 시장 장악

블록체인 산업 육성 범학연산 협의체 구성 블록체인컨소시엄	블록체인 R&D 선도 블록체인 기업 발굴/투자/ 육성	블록체인 시범사업 글로벌 블록체인 표준화 - 혁신 블록체인 기술 수용	글로벌 블록체인 산업 선도 및 국제 경쟁력 강화

블록체인 기업 : 국내 시범사업을 통한 검증 → 해외 상장(NASDAQ) → 표준화 리드를 통해 지속 성장 체제 구축

글로벌 선도를 위한 규제완화 및 인력양성 필요

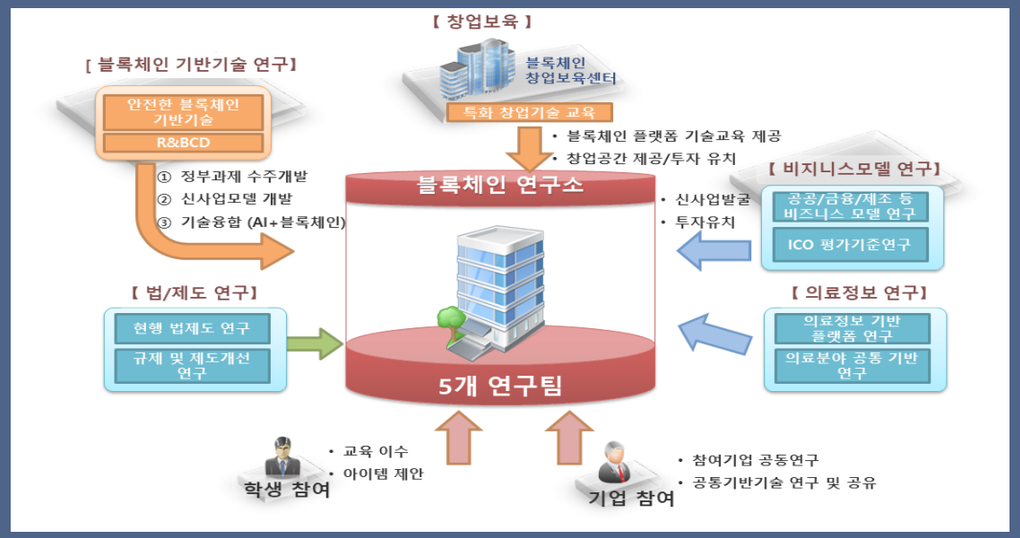
국가 미래기술 정책 Think Tank 필요



- 다양한 학문적 접근 및 융합의 장이 필요
- 산학연 공동 연구 및 토론의 장이 필요
- 국가의 미래 기술 정책 및 전략의 think tank가 필요

➔ 블록체인연구소 설립

고려대 블록체인 연구소 개요



공동연구 기업 참여 방안

Tier-1	연구원 파견 (연구공간 제공) 연구성과 공유 (기업 활용 가능)
Tier-2	블록체인 기술 공동 연구
Tier-3	블록체인 기술의 교육/세미나 및 훈련, 인턴 프로그램 운영 블록체인 창업센터 공동 운영
	블록체인 기반의 새로운 비즈니스 창출을 위한 사업전략, 컨설팅 (맞춤형 과제로 수행)

혁신은

새로운 시장을 만드는 것이 아니라

시장의 주체를 바꾸는 것이다.

Part Ⅳ

블록체인기술 및 전자정부 미래 전망

좌장 : 주일택 소장

AI와 블록체인

이영환 대표
(㈜딜라이트체인)

Blockchain and AI:
the pros and cons

Youngwhan Lee, Ph. D.
Project Leader EcoVerse™

nicklee@delightchain.io
https://ecoverseglobal.io

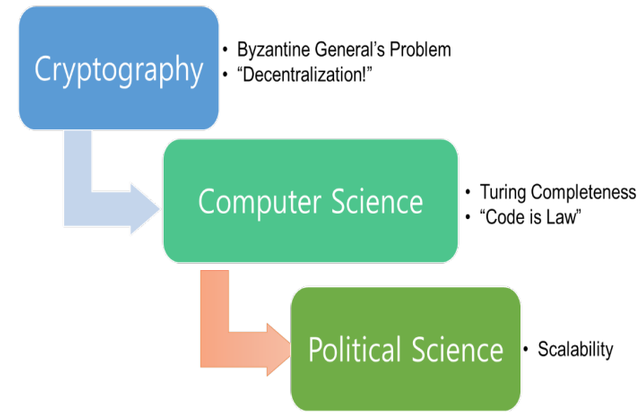
Do you trust these people?

Contents

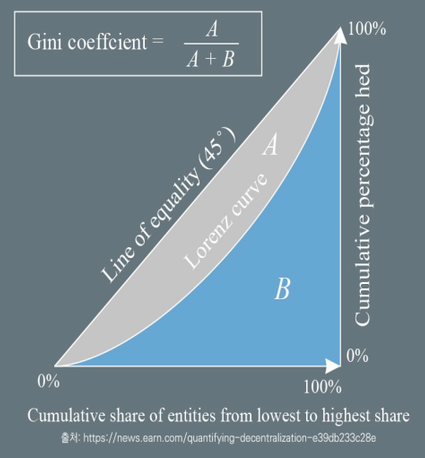
1. Introduction

1) Background: Why is AI needed (in Blockchain)?

- Birth of an electronic payment system as the result of financial crisis
- “Promises” for autonomous execution
- Scalability achieved after abandoning decentralization



Gini Coefficient

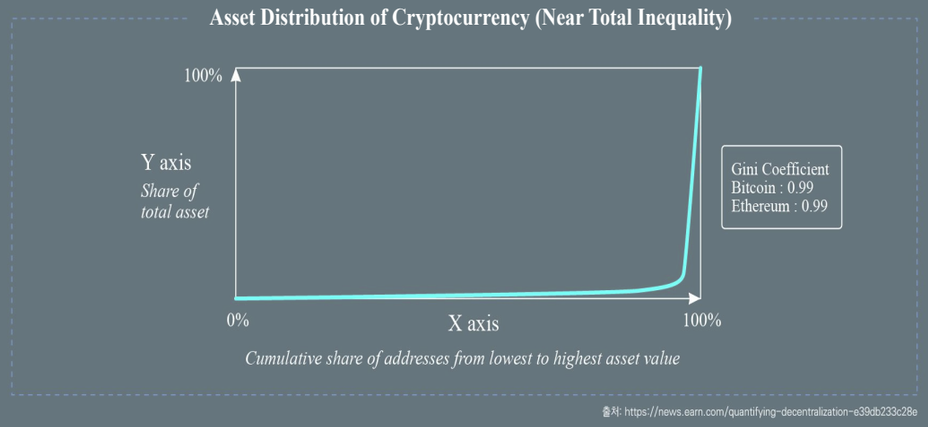


출처: https://news.earn.com/quantifying-decentralization-e39db233c28e

Youngwhan Lee, Ph. D.

EcoVerse

The Economic Issue in Consensus Algorithm



출처: https://news.earn.com/quantifying-decentralization-e39db233c28e

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

"Dr. Doom" Roubini

'Dr Doom' Nouriel Roubini attacks cryptocurrencies as 'the mother and father of all scams and bubbles, and labels blockchain 'the most overhyped technology ever'

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

If problems are left untreated

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

2) AI to Solve the Mediocrity of Blockchain Mainnet

Attributes Desired in AI

- Independent from humans
  - Any kinds of hacking, colluding, cheating and/or censorship become difficult. Any changes in their knowledge must be impossibly difficult. In the case of any changes in the knowledge and behavior of agents needed, they must be the subject of parliament authorization thru a special predefined communication protocol.
- Cooperating with each other among agents
  - Agents must communicate, cooperate, and coordinate with each other.
- Evolving from attempted attacks
  - While attacks and hackings are difficult and almost impossible, the hackers will be attempt to crack in to the network and steal. The agents must continue to learn their patterns and be able to incorporate the learnings and improve their knowledge.

2) AI to Solve the Mediocrity of Blockchain Mainnet

Advantages of Hiring AI Agents for Block Producers

- **No incentives to block producers (AI agents).**
  - This means that incentive distribution plan can be fair and equitable so that the ordinary people, not the BPs, will get the wealth distributed, created by seigniorage.
- **Arguably, no liars and no colluders exist among BPs.**
  - Many blockchain attacks, requiring helps from colluded block producers are impossible.
- **Many hackings and attacks becomes annihilated or trivial.**
  - Annihilated ones: selfish mining, blacklisting, 51% attack, time jacking, and so on.
  - Trivial ones: transaction confirmation, DoS attack, and so on.

2) AI to Solve the Mediocrity of Blockchain Mainnet

Disadvantages of Hiring AI Agents for Block Producers

- **Conflicting world views of two agents, similar to forking, may occur.**
  - In this case, conflict resolution mechanism must be implemented.
  - Examples: Forking, time jacking, and DoS attack

2. Problems that must be addressed

Challenging Problems

- Gini Coefficient

$$C_p = \sum_{d=1}^{l}\left(W_d \cdot M_d \cdot \sum_{a=1}^{m} W_{d,a} \cdot A_{p,d,a}\right) + \sum_{c=1}^{n} W_c \cdot B_{p,c}$$

Where, C_p: contribution of participant 'p'

W_d: dApp 'd's weight of contribution to the entire network

M_d: MAU (Monthly Active User) of dApp 'd'

$W_{d,a}$: participant's weight of activity a on dApp 'd'

$A_{p,d,a}$: participant p's amount of activity a on dApp 'd'

W_c: committee c's weight on all committees

$B_{p,c}$: participant p's amount of activity on committee c

Challenging Problems

- Scalability

Item	Bitcoin	Ethereum	EOS	EcoVerse™
Consensus model	PoW	PoW	DPoS	AI-DPoC
Block Generation Tiime	600 sec	15 sec	3 sec	0.5 sec
Transaction Finalize Time	3,600 sec	180 sec	45 sec	2 sec

Challenging Problems

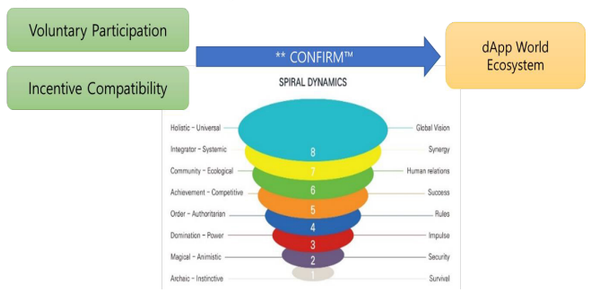
- Self-Sustainability

∀C ∀x ∀t ((incentive-paid x, t, C) > (incentive-wanted x, t, C)) → (incentive-compatible C)

where, the contribution is denoted with C, participant x, and time t.

- Applying spiral dynamics, a theory from socio psychology. The theory tells that people are different and get satisfied by different things.

Keys for Self-Sustainability

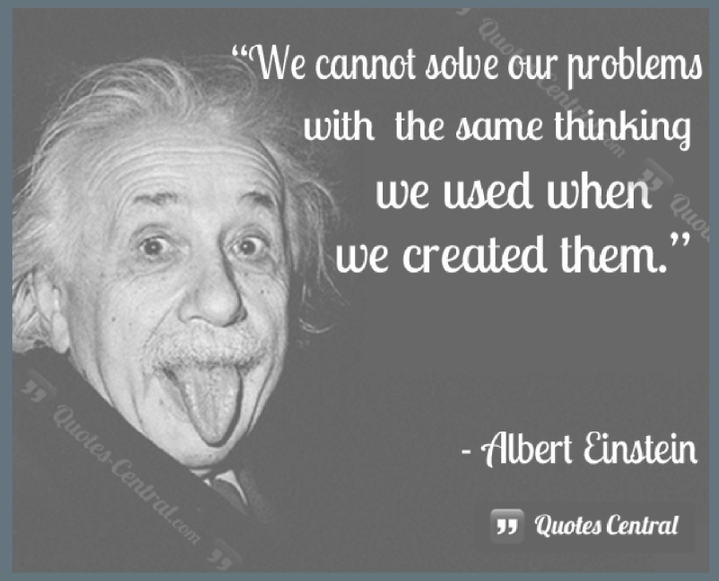


2. Products and Services

Competitive Edges of EcoVerse

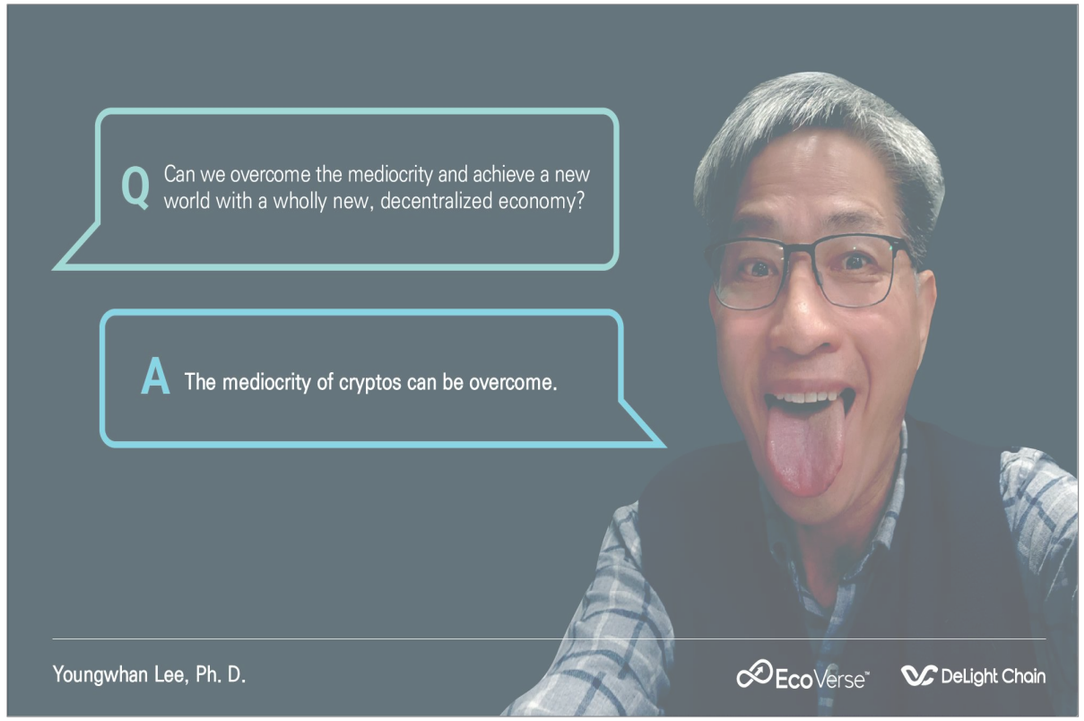
- **Competitive Edge 1: Commercial-Grade Serviceability for Retail Stores**
- Detecting and avoiding any possible collusions from happening is the primary obstacle for the scalability of the cryptocurrency. Since AI agents are employed, no intentional collusion will occur. Although the preventive measure will be implemented, we at EcoVerse is confident to provide better scalability than the most. Therefore, our platform has the competitive edge for commercial-grade serviceability for daily activities.
- **Competitive Edge 2: Self-Sustainability**
- We at EcoVerse™ have been striving for fair and equitable wealth distribution to the ordinary people in the platform. This can be seen that the incentives are given to the users, not block producers. Also the incentives will be defined by decentralized applications differently and therefore, diversified. With this, we believe that the ordinary people give efforts to get their own feeling of “satisficing,” the platform will be self-sustainable differing from most of other platforms that are self-destructive in the long run.
- **Competitive Edge 3: SSI-based Incentives to End Customers**
- The basic DApp(decentralized application) that EcoVerse platform offers is DBSONA™(DB for Persona) which is based on SSI. The SSI-based design ensures that no personal information will be released and opened without the approval of the user. On the other hand, with the consent from the users, DBSONA offers detailed information about people including various analyses, e.g. shopping patterns, favorite places, and so on. This will not only benefit DApp developers, but also be the source of incentives to the users as they get paid for their own information.
- Satisficing is a decision-making strategy that aims for a satisfactory or adequate result, rather than the optimal solution. (-from Investopedia) People tend to settle with “satisfying and sufficing” choices instead of the optimal and the most ideal one.
- SSI (Self-Sovereign Identity) means that people are the owners of his/her own information, on- and offline.

4. Conclusion



Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain



EcoVerse™ Platform is the first-ever
self-sustainable platform
embracing Ubuntu economy

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

References

1. EcoVerse Manifesto. https://bit.ly/2BncBY2
2. EcoVerse Whitepaper. https://ecoverseglobal.io/17.
3. To Integrate Blockchain and AI Part 1. https://link.medium.com/jQJtOhpssT
4. To Integrate Blockchain and AI Part 2. https://link.medium.com/j4Insn5rsT
5. To Integrate Blockchain and AI Part 3. https://bit.ly/2R8GGPy
6. To Integrate Blockchain and AI Part 4. https://bit.ly/2HwR703
7. Youngwhan Nick Lee. Replanning in Response to Conflicts. University of Illinois Press. Doctoral dissertation.
8. Requirements for Self-Sustainable Blockchain, Part 1. https://bit.ly/2KDiV0D
9. Requirements for Self-Sustainable Blockchain, Part 2. https://bit.ly/2RrkXne
10. Requirements for Self-Sustainable Blockchain, Part 3.https://bit.ly/2PPgZUy.
11. Requirements for Self-Sustainable Blockchain, Part 4. https://bit.ly/2PI6tIL.
12. Requirements for Self-Sustainable Blockchain, Part 5. https://bit.ly/2A75zVs
13. Requirements for Self-Sustainable Blockchain, Part 6. https://bit.ly/2TwxFlV
14. Answers to Roubini, "Dr. Doom." https://bit.ly/2PC7riX
15. Defending ICON's Empty Blocks and Other Issues. https://bit.ly/2F4L5lQ
16. Making a cryptocurrency mechanism to be incentive-compatible. https://bit.ly/2KnTksq
17. Buterin questions, EcoVerse(tm) answers! https://bit.ly/2Qeb7rc
18. Are Cryptocurrencies Self-Sustainable? https://bit.ly/2KsaDbS

외부 정보 접근을 위한 Smart Contract Oracle 기술 개발

주일택 소장

(㈜ IoTrust)

IoTrust
Delivering Trusted Connectivity

BlockChain

외부 정보 접근을 위한 스마트 컨트랙트 오라클 기술

주 일택

Contents

Oracle

ORACLE DATABASE

오라클은 귀중한 조언을 해주는 사람, 서비스, 시스템

1. (고대 그리스에서) 신탁을 받는 곳[신탁을 전하는 사제]

They consulted the **oracle** at Delphi.

그들은 델피 사원에서 (사제에게) 신탁을 구했다.

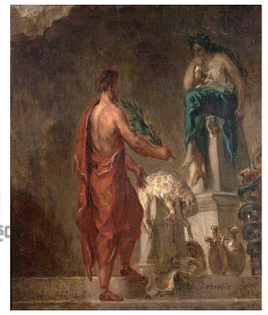
2. (고대 그리스에서) 신탁

3. [주로 단수로] **귀중한 조언[정보]을 주는 사람[책]**

My sister's the **oracle** on investment matters.

투자 문제에 있어서는 내 누이[언니/여동생]가 조언을 다 해 준다

출처:Oxford Advanced Learner's English-Korean Dictionary



Pythia, Oracle of Delphi

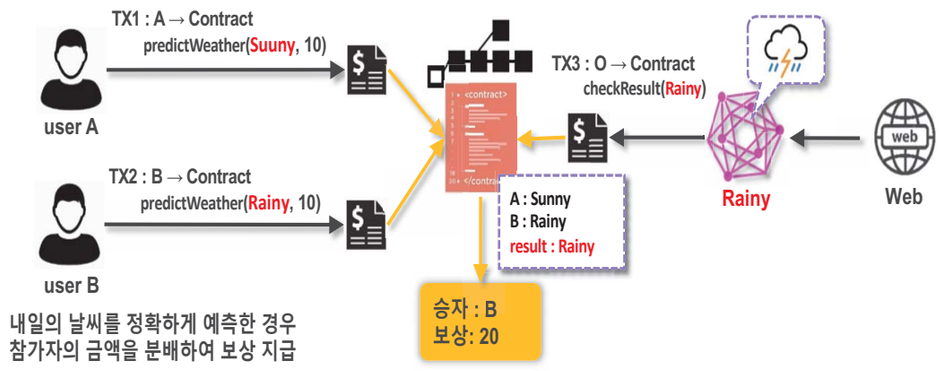
오라클

오라클은 시온의 사람들에게 예언자로 그려집니다. Oracle 이름 그대
하지만 오라클은 매트릭스가 리셋과 리로리드가 될 때 매트릭스가 좀
오라클은 직관적 사고로 그때그때의 상황을 판단합니다.
오라클은 모피어스와 동료들에게 큰 믿음을 주는 존재입니다.

Matrix Oralce

Smart Contract

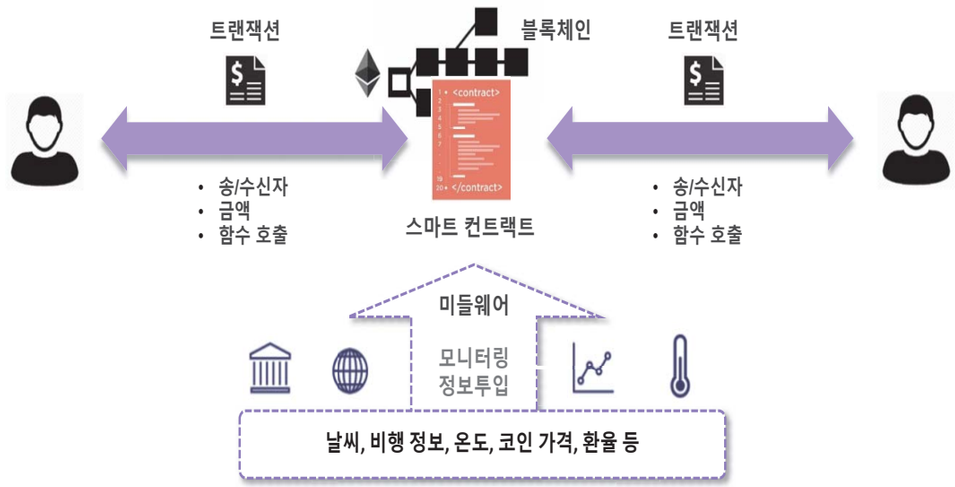
- 스마트 컨트랙트는 특정 조건을 만족할 때 블록체인상에서 실행되는 프로그램으로 정의
- 내일 날씨를 맞추는 사용자에게 이더(ether)를 보상하는 컨트랙트를 작성 가능
- 블록체인의 외부에 존재하는 날씨정보와 스마트 컨트랙트간의 연결성 이슈 발생



내일의 날씨를 정확하게 예측한 경우
참가자의 금액을 분배하여 보상 지급

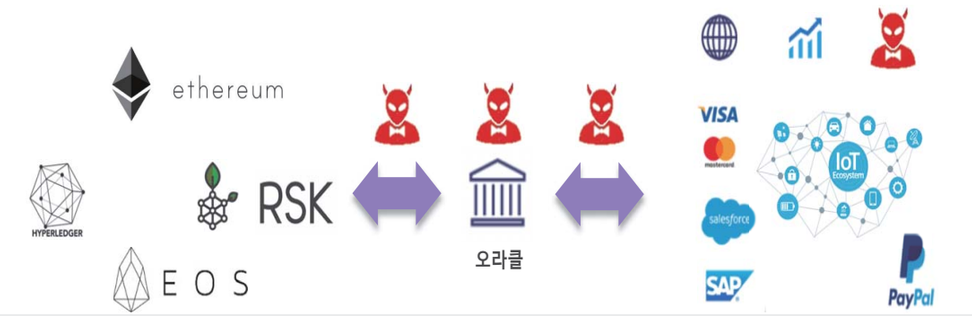
External Data Connectivity

외부 정보 연결성 이슈를 해결하기 위해, 정보 요청을 모니터링하고 정보를 투입하는 미들웨어 필요



Oracle Problem

외부 데이터가 블록체인 으로 들어오는 과정에서 위변조가 발생한다면, 데이터가 블록체인으로 관리 된다고 할지라도 신뢰하지 못함



데이터 전송 과정에서 위변조 ?

외부 데이터의 기밀성&무결성 문제

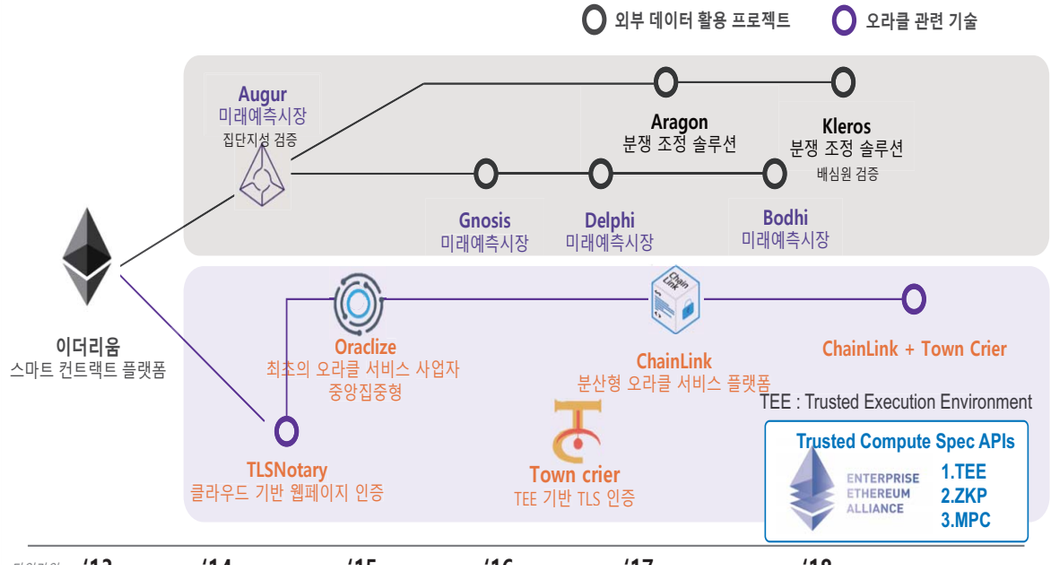
오라클 서버는 외부 데이터를 그대로 전송?

오라클 서버의 신뢰성 문제

오늘의 날씨가 Rainy가 맞는가?

외부 데이터의 신뢰성 문제

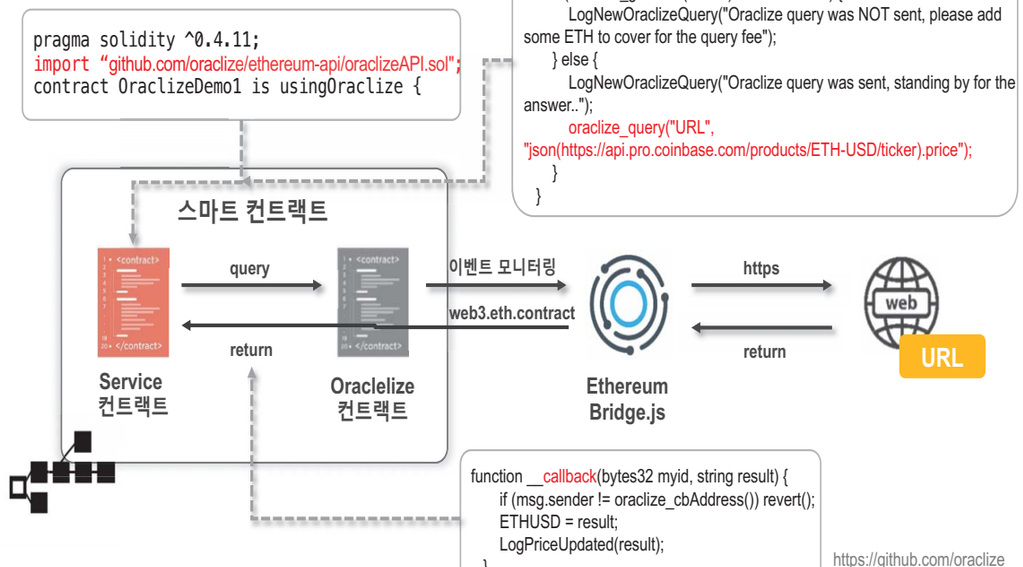
Oracle Technology



Smart Contract

```
pragma solidity ^0.4.11;
import "github.com/oraclize/ethereum-api/oraclizeAPI.sol";
contract OraclizeDemo1 is usingOraclize {
```

```
function updatePrice() payable {
    if (oraclize_getPrice("URL") > this.balance) {
        LogNewOraclizeQuery("Oraclize query was NOT sent, please add some ETH to cover for the query fee");
    } else {
        LogNewOraclizeQuery("Oraclize query was sent, standing by for the answer..");
        oraclize_query("URL", "json(https://api.pro.coinbase.com/products/ETH-USD/ticker).price");
    }
}
```

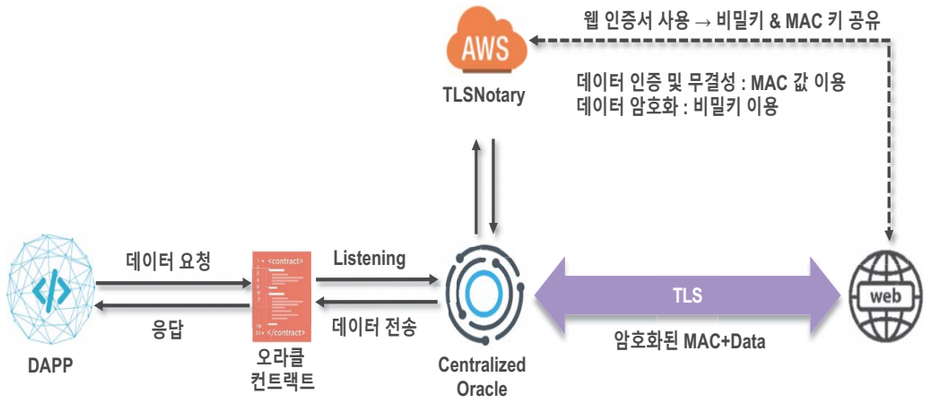



```
function __callback(bytes32 myid, string result) {
    if (msg.sender != oraclize_cbAddress()) revert();
    ETHUSD = result;
    LogPriceUpdated(result);
}
```

https://github.com/oraclize

Centralized Oracle

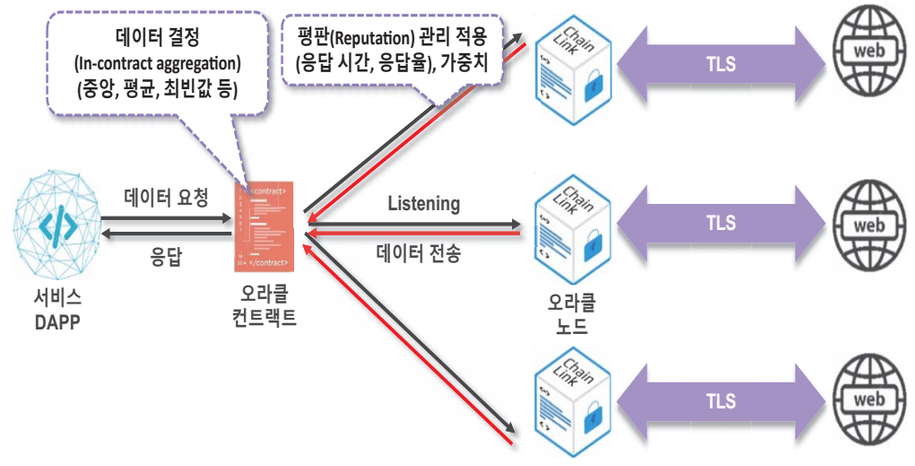
- 클라우드 기반의 TLSNotary (공증) 서비스를 이용하여, 외부 데이터 제공의 인증 문제를 해결
- 오라클 노드에서 데이터 변조 가능성 및 단일 장애 지점(Single Point Of Failure)발생 가능성 존재



TLS(Transport Layer Security) : 통신과정에서 전송 계층 종단간 보안과 데이터 무결성 확보를 위해 인증서를 활용하는 프로토콜 계층

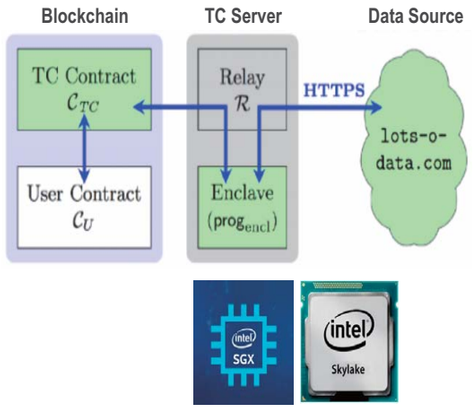
Decentralized Oracle in-contract aggregation

- 스마트 컨트랙트에서 오라클 응답 노드의 전체 데이터를 모아서 데이터를 결정
- In-contract aggregation 방식은 오라클 노드 비례하여 GAS 비용 발생



Town Crier : TEE Secured Oracles (2016)

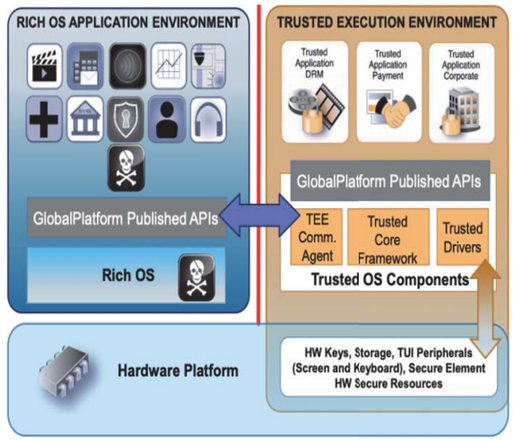
데이터 소스인 웹에서 데이터의 암/복호화 및 인증을 TEE 내에서 무결성 검증, Intel SGX TEE 이용



IC3 The Initiative For CryptoCurrencies & Contracts

https://www.town-crier.org/

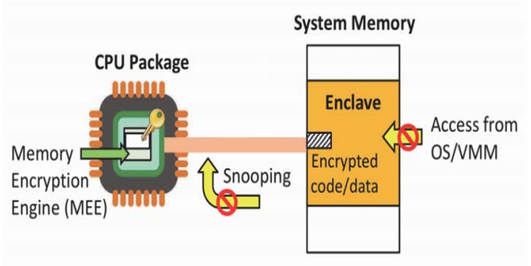
Trusted Execution Environment (TEE)



- TEE 국제 표준은 비영리 표준화 기구인 GlobalPlatform에서 2010년 제정
- 메인 프로세스내 별도로 독립된 보안 영역이 제공하는 신뢰있는 실행 환경
- 보안 소프트웨어 안전하게 실행
- 보안영역과 일반영역과의 정보교환 통제
- Intel SGX, Arm TrustZone

https://globalplatform.org

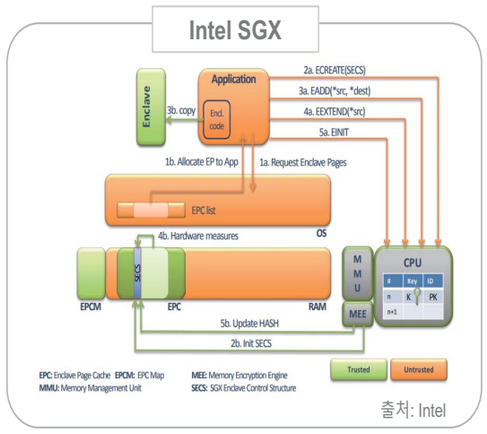
Intel SGX(Safe Guard Extension) Isolated Execution



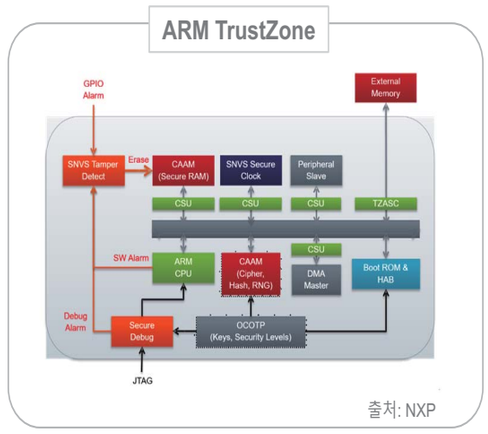
- CPU 패키징 (비밀키 랜덤 생성)
  - 비밀키로 인클레이브 생성
- 비밀 data의 안전한 보관
  - 메모리 상의 안전한 보관
  - 스토리지 상에 암호화하여 (sealing)보관
- 코드 암호화
- 코드 무결성 검사
  - 변조된 코드가 없음을 확인

Intel SGX vs. ARM TrustZone

TEE를 구축할 수 있는 대표적인 하드웨어 아키텍처로 Intel의 SGX와 ARM의 TrustZone이 있으며, 하드웨어 및 키 아키텍처 구성 방식 차이점이 있음

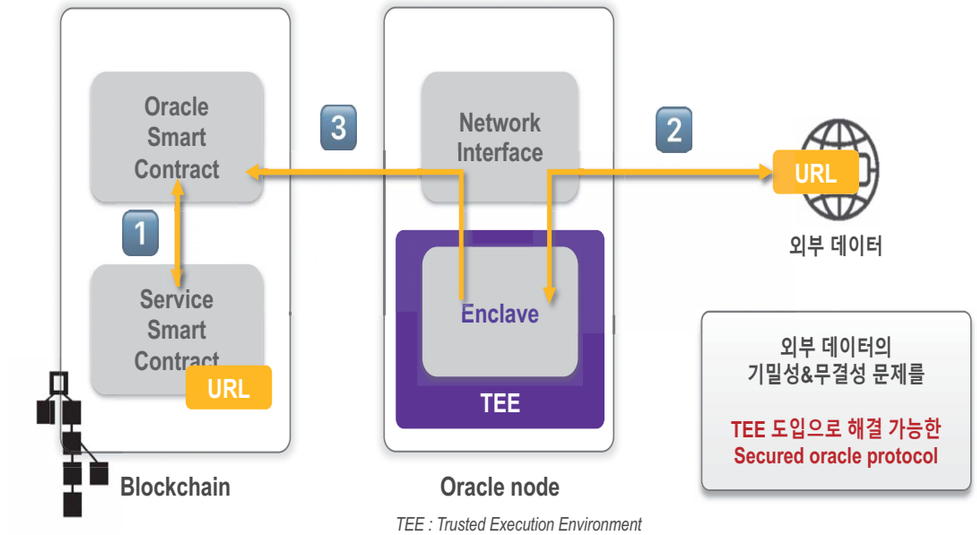


출처: Intel



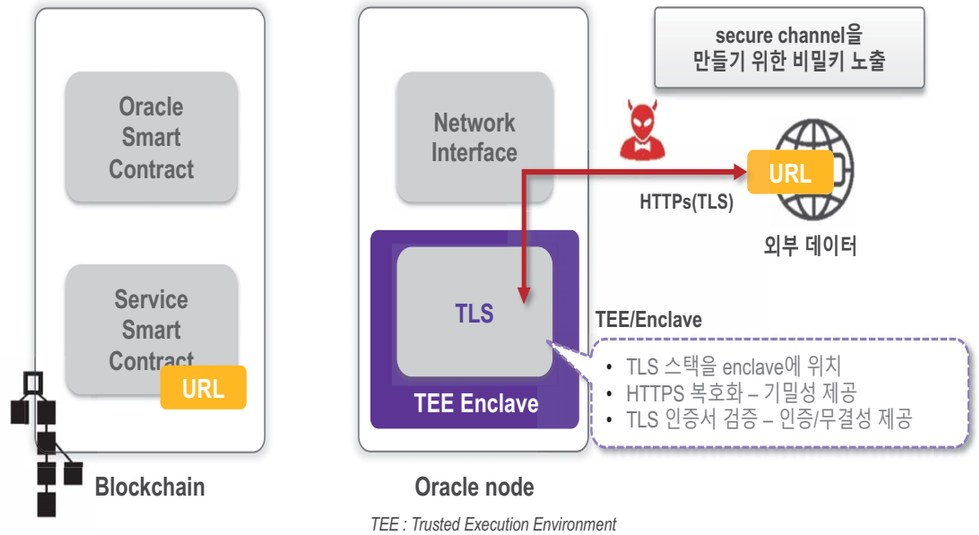
출처: NXP

Secured Oracle Protocol



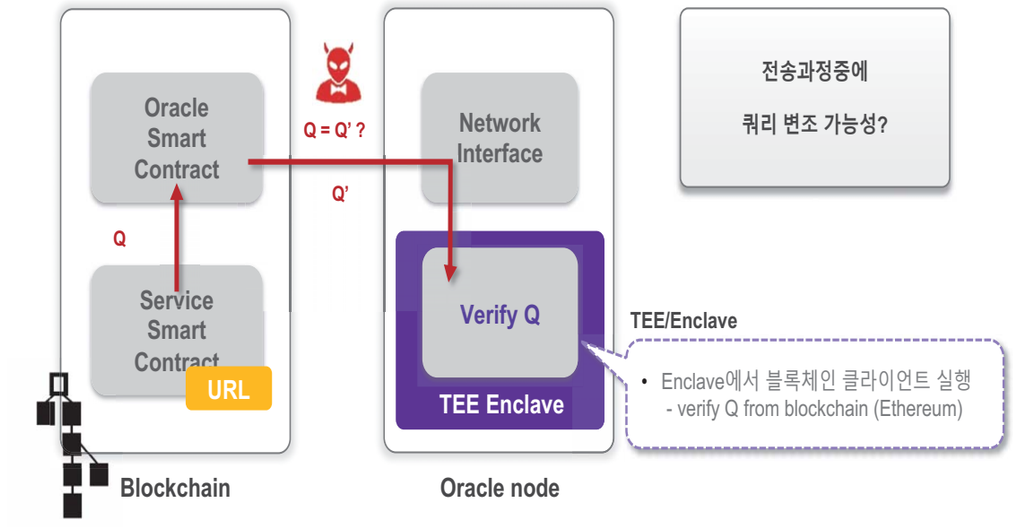
TEE : Trusted Execution Environment

2. External Secure Channel

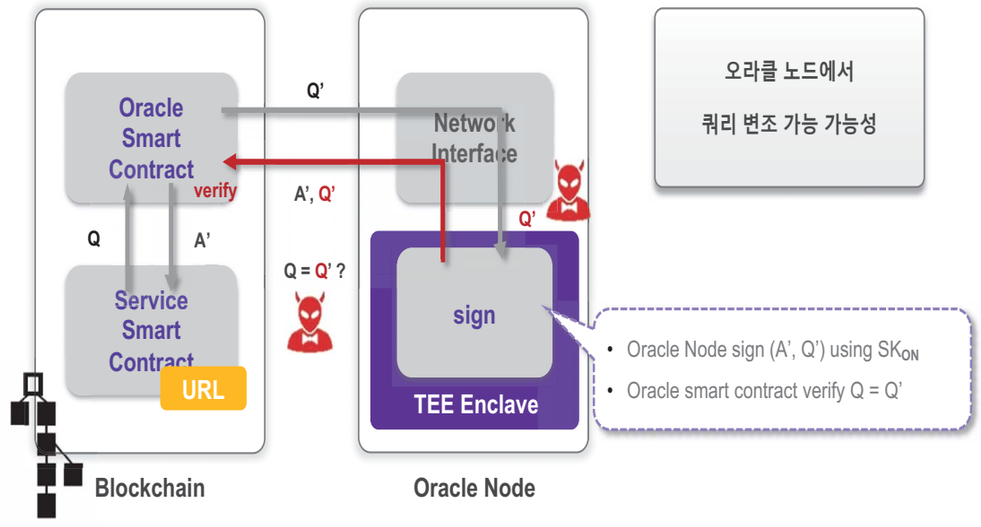


TEE : Trusted Execution Environment
TLS : Transport Layer Security

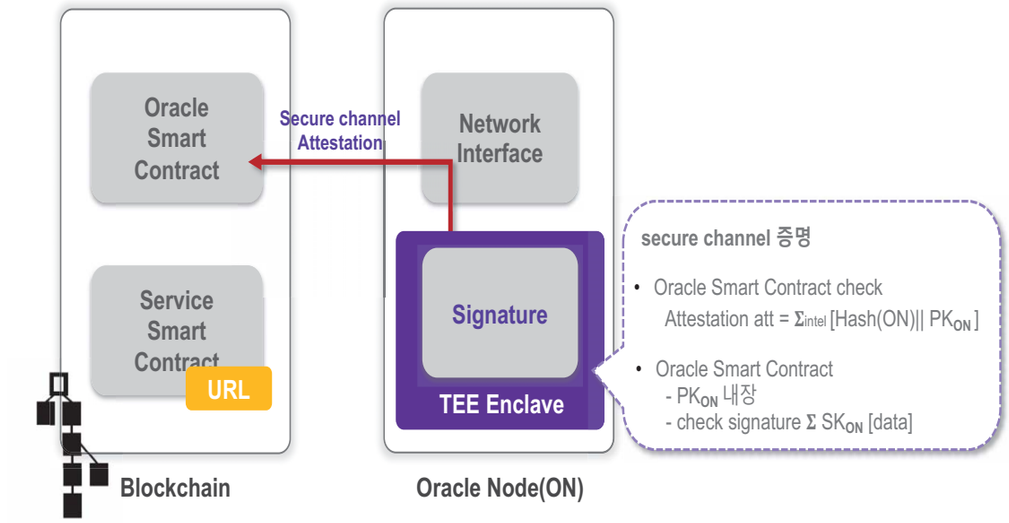
1. Request Query & Verify



3. Secure Channel attestation

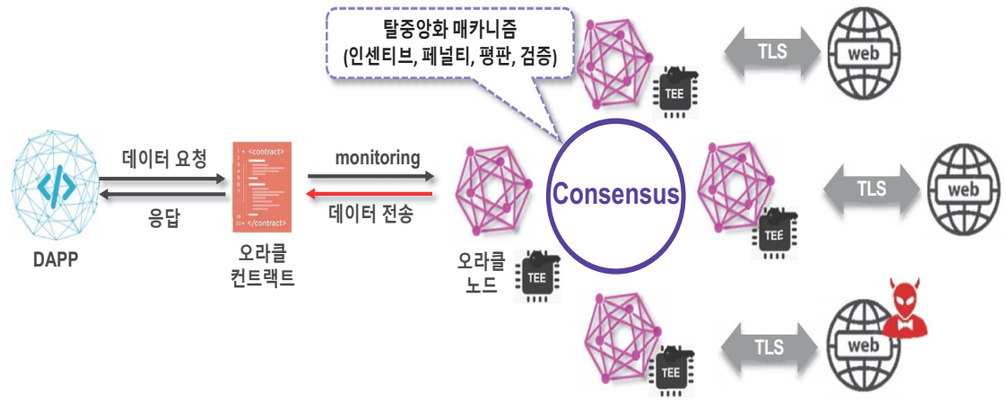


3. Secure Channel attestation



Secure Decentralized Oracle consensus

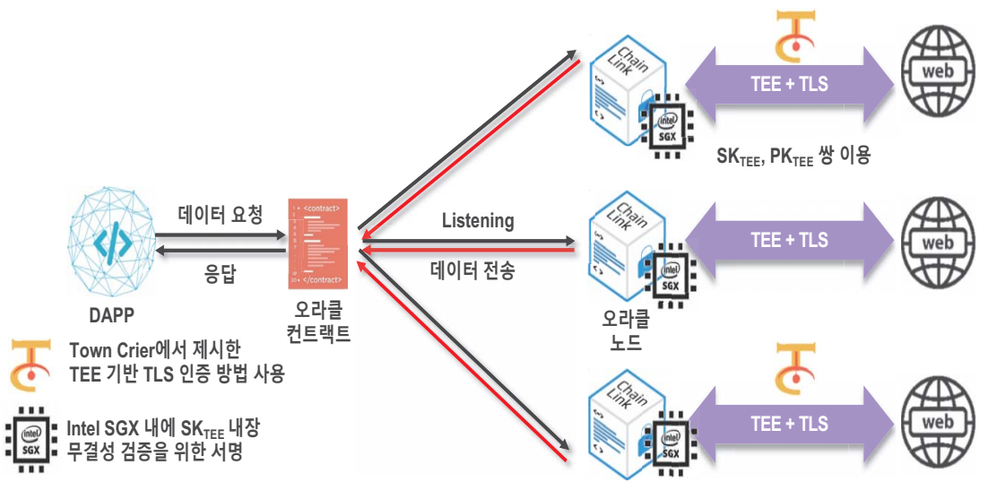
- TEE 기반의 오라클 노드들 합의로 신뢰하는 데이터를 결정하여 비잔틴 문제와 GAS 비용 문제 해결
- 보상, 페널티, 평판관리, 유효성 검증 구조가 잘 설계된 탈중앙화 메커니즘으로 외부 데이터 검증



Secure Decentralized Oracle in-contract aggregation

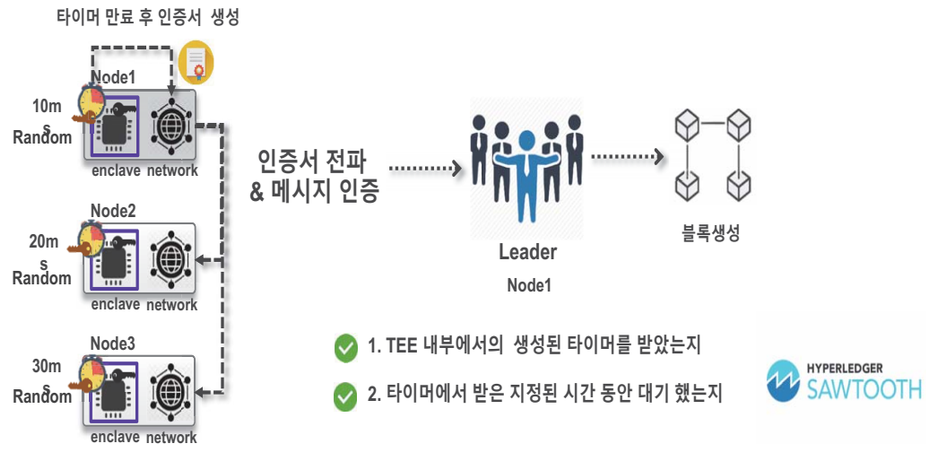
Town Crier에서 제한한 TEE기반 TLS 인증 방법을 분산화된 오라클 서비스 적용

Intel SGX TEE 안에 내장된 비밀키(SK_{TEE})를 이용하여 TLS 인증 및 암호화를 하여 무결성과 기밀성을 제공



PoET (Proof of Elapsed Time, 시간 경과 증명)

- 신뢰할 수 있는 보안 모듈(Intel SGX)을 기반으로 블록을 생성하는 리더를 랜덤하게 선정
- 가장 짧은 경과 시간을 가진 노드가 깨어나 새로운 블록을 투입하고, 필요한 정보를 전체 네트워크에 전파



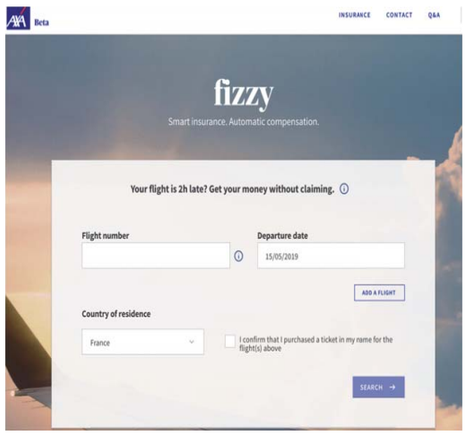
Requirement

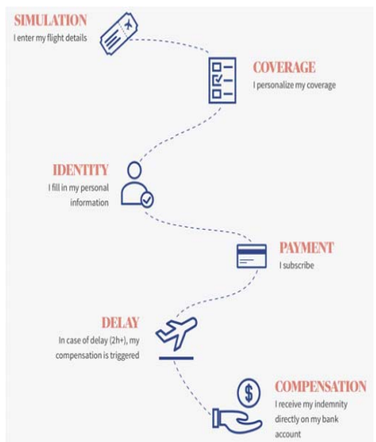
정보접근의 신뢰성 향상을 위한 TEE 기반 기술, 오라클의 탈중앙화 매카니즘 및 합의 방법

외부 데이터의 위.변조 불가 **데이터 인증 프로토콜**	단일 지점 장애 해결 **탈중앙화 오라클 노드**	In-contract aggregation 비용 축소 **데이터 결정 방법**
정보 기밀성 & 무결성 보호 **TEE 기반 오라클 노드**	외부 데이터의 신뢰성 향상 **탈중앙화 매카니즘**	오라클 노드의 탈중앙화 **합의 방법**

Oracle Application fizzy.axa

외부 데이터인 비행정보를 이용한 보험 스마트 컨트랙트 서비스





https://fizzy.axa (beta)

AXA flight Delay Insurance

- AXA Launches **Ethereum Smart Contract Insurance** Product for **Flight Delays**
- AXA is the first major insurance group to offer insurance using blockchain technology. Discover fizzy, a 100% automated, 100% secure platform for **parametric insurance** against delayed flights.
- When you buy flight delay insurance on the fizzy platform, we record the purchase in a tamperproof network, the **Ethereum blockchain**, making the insurance contract equally tamperproof.
- This smart contract is connected to global air traffic databases, so as soon as a **delay** of more than **two hours** is observed, compensation is triggered **automatically**.

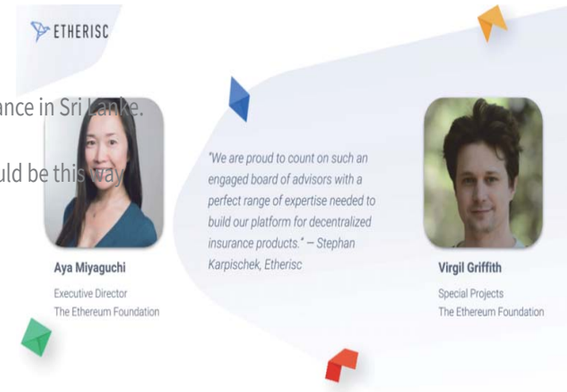
Parametric Insurance in Edcon 2019

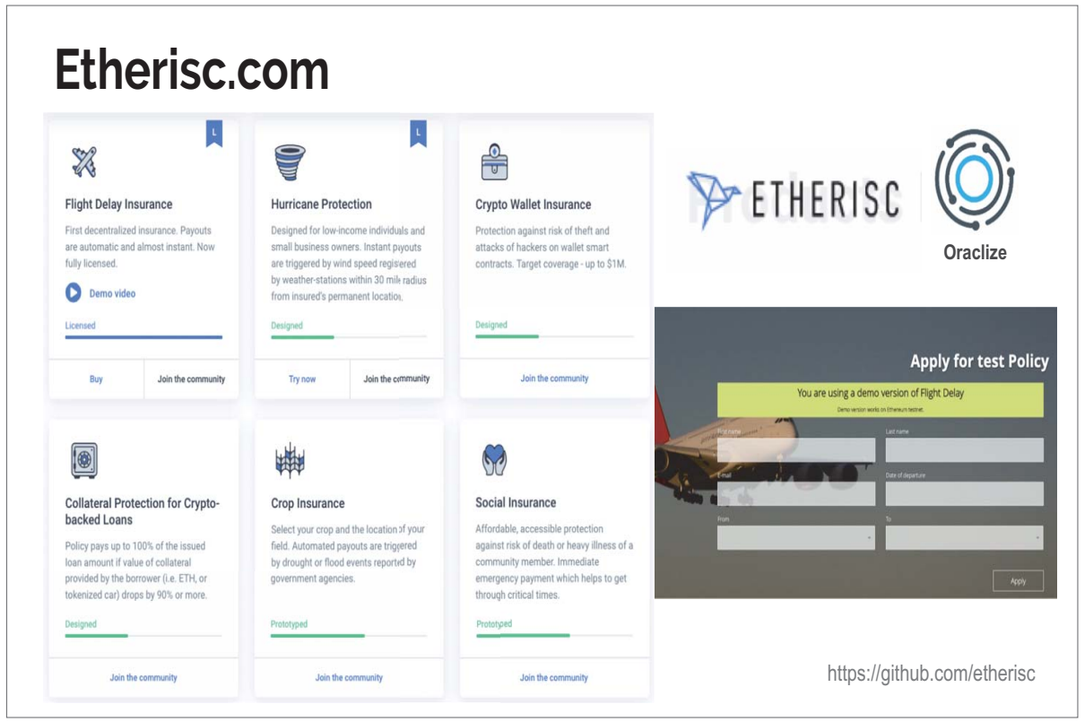
Next killer app : Parametric Insurance?

- First killer app : Money
- Second killer app : ICO
- Third killer app : Insurance?

  - Hurricane insurance in Puerto Rico. Crop Insurance in Sri Lanka.

- Probable all weather and disaster insurance should be this way





블록체인 하드웨어 가속기 및 지갑 개발 현황

현영권 대표
(㈜미디움)

미디움 블록체인

하드웨어 기반 블록체인 플랫폼

내용

- 미디움 블록체인
  - 일반
  - 트랜잭션 플로우
  - BPU
- 하드웨어 가속 성능 향상 포인트
  - 서명/서명 확인의 가속
  - Peer의 확장성을 위한 서명 알고리즘
  - Serialization
  - Key-value store
  - Smart Contract
  - Ethernet
- 보드 현황
- 테스트 결과

미디움 블록체인 - 일반

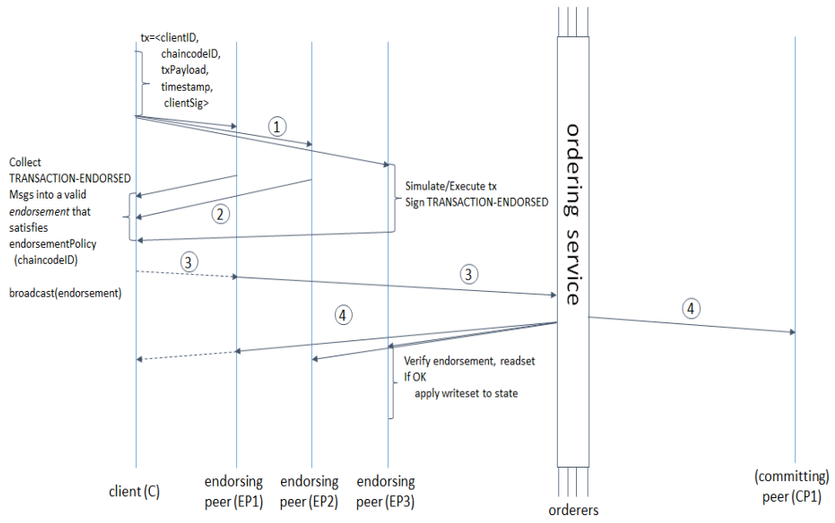
- 블록체인은 보안, 제 3인증 기관이 필요하지 않은 등 기존 시스템들에 없는 여러가지 새로운 특성을 가지고 있고, 이를 이용하여 다양한 산업분야에 사용될 수 있는 기술이다. 기술적 기반은 다양한 곳에 사용될 수 있지만 제한적인 트랜잭션 처리량을 제공함으로써 제한된 범위 내의 산업분야에만 적용되고 있다.

- 블록체인은 참여 노드 구성 형태에 따라 Permissioned 블록체인과 Permissionless 블록체인으로 나눌 수 있다. Permissioned 블록체인은 특정 회사 혹은 단체의 허가가 있는 경우에만 노드를 추가적으로 구축할 수 있는 형태를 의미하고, Permissionless 블록체인은 특정 회사/단체의 허가 없이도 블록체인의 구성 노드로 참여할 수 있는 형태를 의미한다. Permissioned 블록체인은 노드를 구성할 때 특정 요구조건에 따라 노드 참여를 제한할 수 있으므로 요구조건에 따른 시스템을 구축할 수 있다는 것을 의미한다. 따라서 성능 향상을 위해서 미디움 블록체인은 Permissioned 블록체인 형태로 네트웍을 구성하도록 한다.

- Permissioned 블록체인을 목표로 제일 많이 사용되는 것은 Hyperledger Fabric[1]이다. Hyperledger Fabric은 Linux Foundation의 프로젝트로 등록되어 있고, IBM에서 주로 개발에 참여하고 있다. Hyperledger Fabric은 Permissioned 이므로 노드의 스펙을 원하는 대로 정할 수 있지만, 노드의 스펙을 높인다고 해서 성능이 무한으로 늘어나는 것은 아니다. 여러가지 구현상, 정책적인 문제들로 인해 성능이 3,000 TPS 정도를 보여준다. 최근에 구현상의 문제들을 일부 해결함으로써 20,000 TPS 까지 높인 사례[2]도 있다.

- Hyperledger Fabric에서는 E-O-V (Execute-Order-Verify) 구조를 이용하여 전체 트랜잭션에 대한 검증과 블록생성을 진행한다. 트랜잭션 요청을 받게 되면 먼저 트랜잭션을 실행(Execute)하여 실행 결과를 추출하고, 블록을 생성하기 위한 순서를 정리(Order)한다. 마지막으로 생성된 블록에 있는 트랜잭션들을 검증(Verify)하는 과정을 거쳐 전체 트랜잭션이 블록으로 생성되도록 한다. 트랜잭션의 흐름은 아래의 그림 1 과 같다.

미디움 블록체인 – 트랜잭션 플로우



미디움 블록체인 - BPU

- 하드웨어 기반의 블록체인
  소프트웨어의 성능을 아무리 높인다고 할지라도, CPU의 처리속도보다 더 빨라질 수가 없다.
  CPU의 처리 속도 한계를 넘어가기 위해서 GPU가 탄생했고 사운드칩과 기타 주변의 칩들이 탄생했다.
  이와 같은 이유로 우리는 블록체인을 전문적으로 처리할 수 있는 전용 칩 ASIC을 개발하게 되었다.

- 백만 TPS를 처리할 수 있는 블록체인 기술
  일반적으로 시중에서 요구되는 처리 속도는 일반 은행의 경우에는 1만TPS이며 대형 인터넷마켓과 온라인 게임사의 경우에는 보통 10만 TPS 이상의 처리속도가 요구된다.
  이러한 성능의 구현을 위해서는 일반적인 블록체인 기술을 이용해서는 처리할 방법이 없다.
  처음부터 ASIC 제작을 전제한 완전히 새로운 반도체 칩에서의 최적화 요소가 결합된 블록체인의 설계가 필요했다.
  Signing과 Verifying의 속도를 칩 상에서 극한으로 끌어 올릴 경우 smartcontract와 LeverDB에서 병목인 발생한다.
  Smartcontract는 컴파일러는 Instruction set을 칩에 내재화 하면서 문제를 해결하였다.
  현재 DB로 사용하고 있는 Key-Value store는 E-O-V구조에서 workload의 부하를 몇 만 정도까지만 처리할 수 있다
  백만 트랜잭션을 처리하기 위한 Key-Value store의 하드웨어를 이용한 구조적 개선과 DB 인덱스 생성 및 탐색 알고리즘이 필요하다.

- E-O-V 아키텍쳐 기반의 Consortium 블록체인

하드웨어 가속 성능 향상 포인트

- 서명/서명 확인의 가속

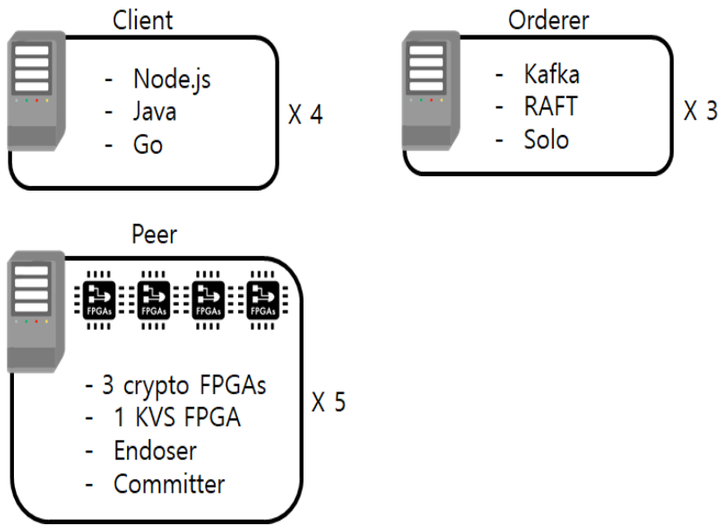
5 peer 3 orderer 시스템에서 valid tx가 필요한 sign & verification: 3개

sign/verify BMT (64 core CPU, 32GB RAM)

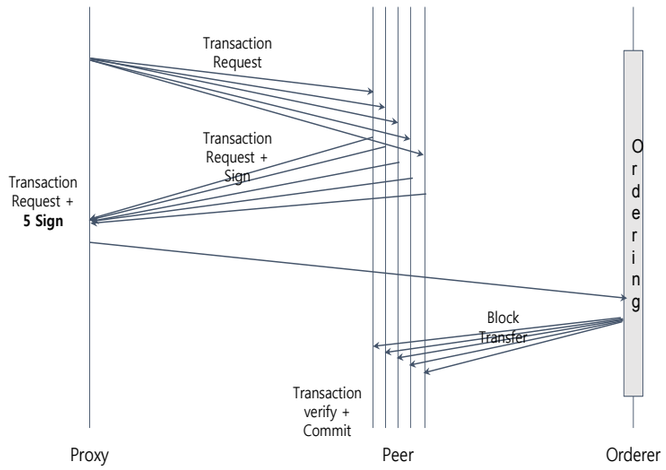
	Signing	**verification**
Threads	60	60
Avg elapsed time	0.7247	1.3382
Verify/sec	690,000	373,000

초당 30만 TPS (90만 verify/sec) 를 넘기 힘듬

hardware sign/verify
- 서명/서명 확인만을 위한 FPGA 보드 사용
- 보드당 30만 verify/sec * 3개 사용



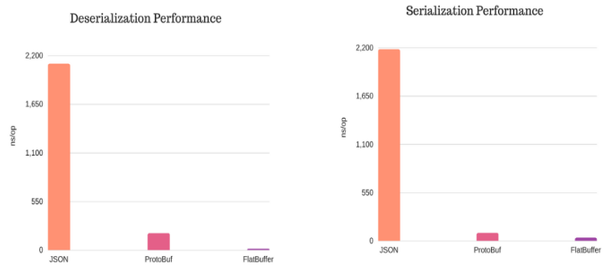
Peer의 확장성을 위한 서명 알고리즘



- Peer의 갯수가 많아지면 Transaction 당 Sign의 갯수가 많아져 Transaction verify에서 CPU 자원의 소모가 심함

Serialization

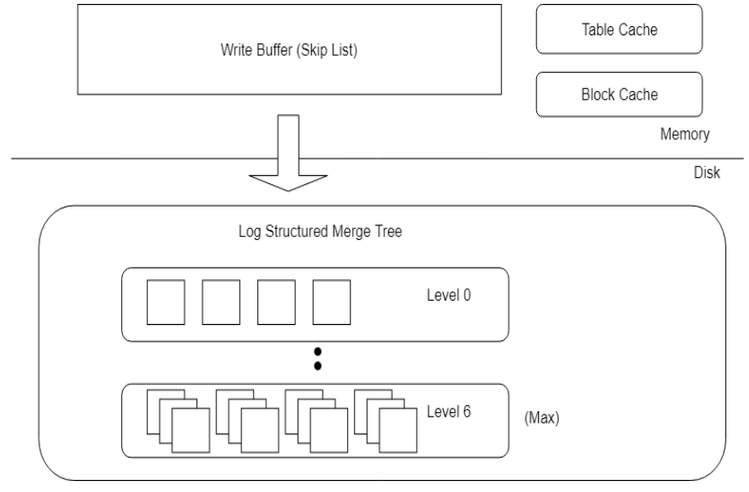
- Client <-> Peer , Peer <-> Peer 간 데이터 직렬화로 현재 Json/Protobuf 을 사용중
- FlatBuffers / SSZ 로 변경 고려중
- SSZ는 Ethereum RLP를 대체하는 serialization 방식으로 Ethreum 2.0 에서 사용 될 예정.
https://github.com/ethereum/eth2.0-specs/issues/2
- Flatbuffers 는 구글에서 만든 초고속 직렬화 라이브러리로 C++에서 protobuf에 비해 거의 3000배 빠른 성능을 보인다고 한다.
- 속도 비교



- 성능 향상이 있긴 하겠지만 1백만TPS 를 달성하려는 우리 미디움에서는 더욱 빠른 성능을 위해 장기적으로 FPGA상에서의 DATA LINK 에 대한 연구가 병행 될 것이기에 그것과 연계될 수 있는 직렬화 연구를 꾸준히 진행 할 것이다.

K/V Storage

LevelDB : Append Only DataBase with LSM Tree



K/V Storage

LevelDB Batch Write
(N Entries)

1. Dump Batch InTo Disk (for recovery)
2. Insert Batch Entries into Write Buffer (Skip List Data Structure)

LevelDB Random Read
(1 Entry)

1. Search Write Buffer (Skip List)
2. Search table # correspond to key range
3. Get Table if Cached or Read Disk
4. Search Block Offset correspond to key range
5. Get Block if Cached or Read Disk
6. Block Iteration

Additional Background Tasks

- Write Buffer
- Merge Tables

Smart Contract

현상황 및 문제점

- Smart Contract를 Peer 머신에 배포하면, 하나의 Smart Contract는 하나의 Process로서 실행됨.
- Smart Contract는 Peer와의 gRPC 통신으로 World State DB의 상태를 query 또는 update함.
- 배포된 Smart Contract가 수만개 이상일 경우, 잦은 Context Switching으로인한 시스템 전체 성능 저하 및 Peer에 상당한 부담이 될 수 있음.

미디움이 나아갈 방향

- Peer 머신의 PCI 버스에 Smart Contract 전용 ARM 보드 설치.
- 하나의 ARM 보드에 제한된 수의 Smart Contract 만을 실행함.
- ARM 보드 개수를 병렬적으로 확장함으로써 Smart Contract의 Scalability 문제를 해결함.
- Peer와 분리된 OS에서 실행되기 때문에 보안에도 유리

테스트 결과

4 Client / 5 Endorsor / 5 Commiter (블록 생성 TPS : 블록당 200,000 TX)

	CPU	FPGA (1)
Value Transfer	약 7만 TPS	약 4만 7천 TPS
Chain Code VT	약 4만 8천TPS	약 4만 6천 TPS

1 Client / 1 Endorsor / 1 Commiter (블록 생성 TPS : 블록당 200,000 TX)

	CPU	FPGA (1)	FPGA (3)
Value Transfer	약 90,000 TPS	약 67,000TPS	약 95,000 TPS
Chain Code VT	약 68,000 TPS	약 65,000 TPS	약 94,000 TPS

1 Client / 1 Endorsor / 1 Commiter (Verify BMT)

	CPU	FPGA (1)	FPGA (3)
48 Cores	약 200,000 TPS	약 180,000 TPS	약 480,000 TPS

* 상기 모든 테스트는 쓰레드 개수의 조절에 따라 달라 질 수 있다.

블록체인으로 여는 전자정부

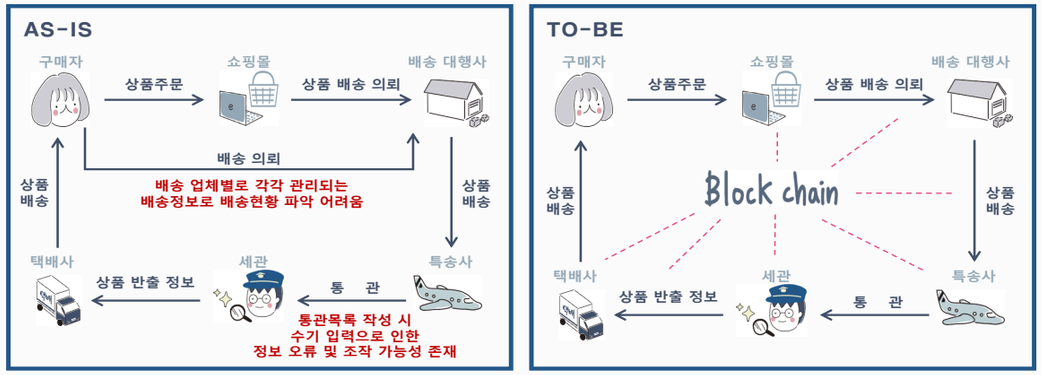
민경식 박사
(한국인터넷진흥원)


블록체인과 전자정부
-시범사업 추진현황을 중심으로-
CPU
민경식 (kyoungsik@kisa.or.kr)
한국인터넷진흥원
KISA


Contents
Ⅰ : ‘18년도 블록체인 사업 현황 및 성과
Ⅱ : ‘19년도 블록체인 사업 추진 현황
Ⅲ : 향후 추진방향
KISA
1

Ⅰ '18년도 블록체인 사업 현황 및 성과

지능형 개인통관 서비스 플랫폼 (관세청)



01 비효율적인 통관 정보 전달

02 정보 오류 발생 및 허위 신고 문제

03 어렵고 오래 걸리는 배송현황 파악

01 자동화된 업무처리를 통한 통관 효율성 향상

02 위조, 변조가 어려운 블록체인의 특성을 활용한 신뢰성 제고

03 블록체인 통관 정보를 온라인 포털을 통한 실시간 파악

Ⅰ '18년도 블록체인 사업 현황 및 성과

블록체인 공공선도 사업으로 모범사례 발굴 및 시장 활성화

- 6개 공공서비스 성과로 **기업 레퍼런스 확보**
- **우수 블록체인 활용 아이디어 발굴**을 위한 블록체인 진흥주간 개최(아이디어 192개/해커톤 40팀 접수)

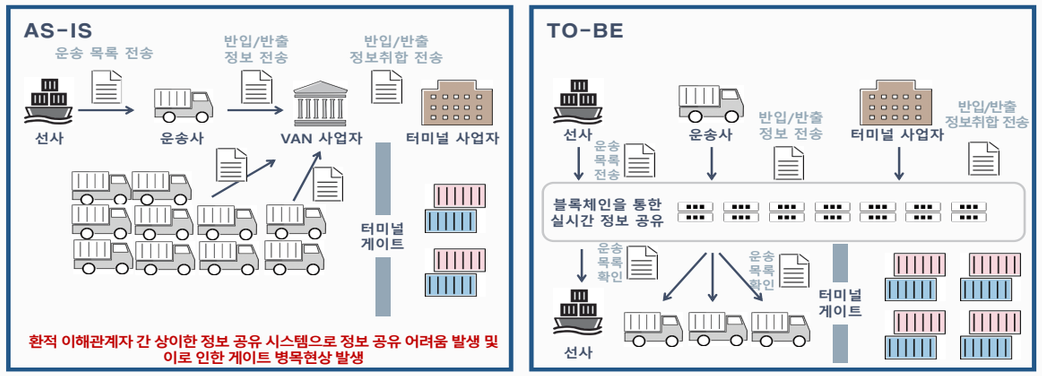
규제개선사항 발굴 및 대국민 인식제고

규제개선 연구반	TechBiz 컨퍼런스
5개 이슈 발굴 →'19년 개선 추진	6회 개최, 총 2,300명 참석

2018년도 6개 공공선도 시범사업 — 과제당 지원금 5.6억원(상호출자방식)

PAIN POINT 제거	이용자 편의 제공	기업 레퍼런스 확보
지능형 개인 통관 서비스 플랫폼	블록체인 기반의 컨테이너 부두간 반출입증 통합발급	Private 블록체인 기반 축산물 이력관리 시스템	블록체인 클라우드 기반 부동산 종합 공부 시스템	온라인 투표 시스템	e-App 서비스 플랫폼
관세청	해양수산부	농림축산식품부	국토교통부	중앙선관위	외교부

블록체인 기반의 컨테이너 부두 간 반출입증 통합발급 (해양수산부)



01 환적 이해관계자 간 정보 공유의 어려움

02 터미널 게이트의 병목현상 발생

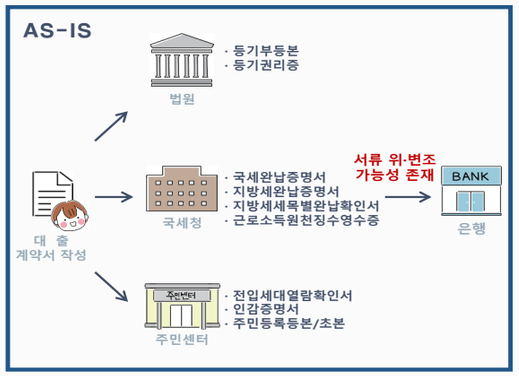
03 통일되지 않은 시스템으로 인한 혼란

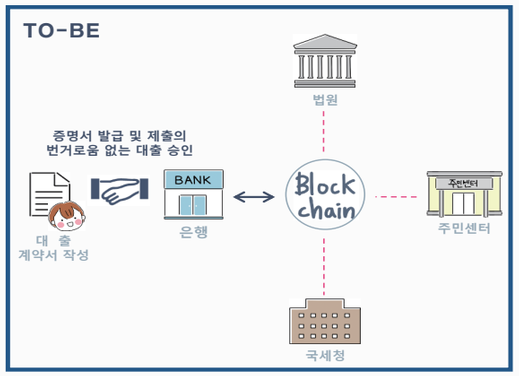
01 정보 공유를 통한 시간 및 비용 효율 증대

02 블록체인 특성에 기반한 항만물류 협력 생태계 조성

03 친환경 항만 구축 기여

블록체인 클라우드 기반 부동산 종합공부 시스템 (국토교통부)





01 과도한 시스템 운영비용과 정보공유의 어려움

02 힘들고 번거로운 토지 관련 증명서 발급

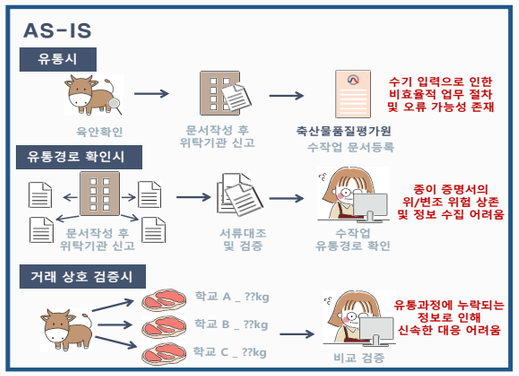
03 비정상 정보 검증의 어려움

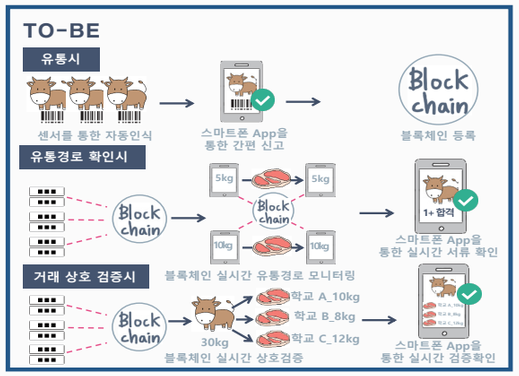
01 운영비용 감소 및 시스템 안정성 강화

02 편리하고 효율적인 부동산 거래

03 위변조 방지, 신뢰성 강화를 통한 국민 토지재산권 보호

프라이빗 블록체인 기반 축산물 이력관리시스템 (농림축산식품부)





01 비효율적인 축산물 신고 절차

02 축산물 관련 증명서 위변조 위험 및 신뢰성 문제

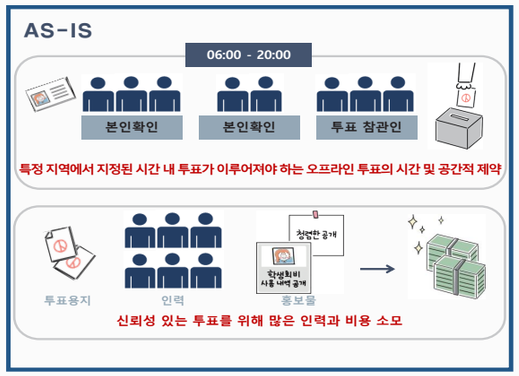
03 축산물 식품안전 문제에 대한 신속한 대응의 어려움

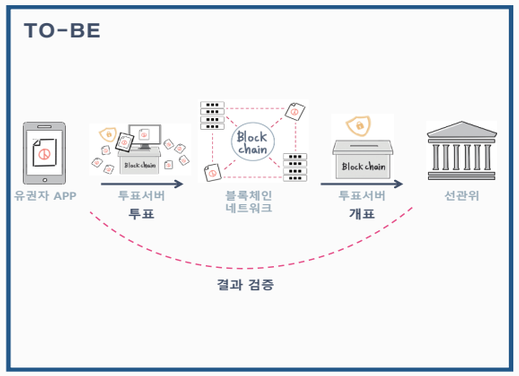
01 손쉬운 축산물 유통정보 확인

02 신속하고 신뢰할 수 있는 유통 체계 확립

03 신속한 이력 추적 및 실시간 문제 대응

블록체인 기반 온라인 투표 시스템 (중앙선거관리위원회)





01 오프라인 투표의 제약사항

02 기존 전자투표의 신뢰성 문제

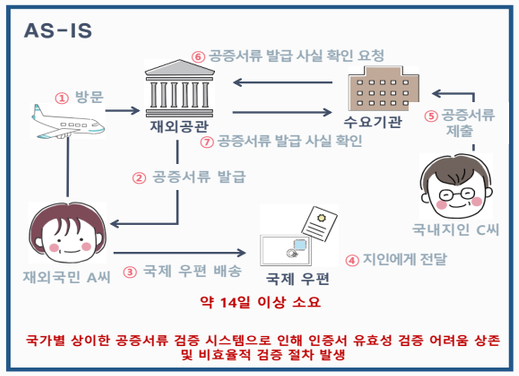
03 해킹 및 위변조 우려

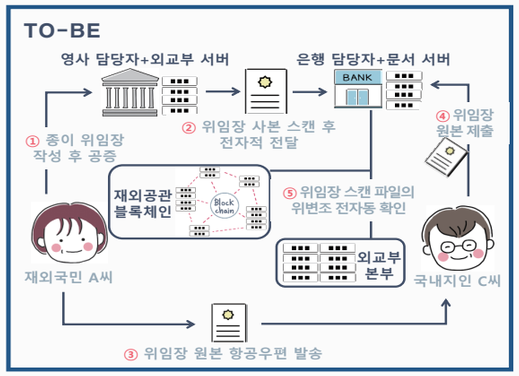
01 온라인 투표의 신뢰성 제고

02 신속 정확한 투표 및 개표 관리로 예산 절약

03 의사 결정의 효율성 증대 및 사회적 비용 감소

블록체인 기반 재외공관 공증 서비스 플랫폼 (외교부)





01 인증서 유효성 검증의 어려움

02 비효율적인 재외공관 공증 서비스 업무 절차

03 국가별 상이한 시스템으로 인한 불편함

01 국가간 인증 효율성 향상

02 안정적인 서비스 제공 가능

03 시스템 유지비용 감소

II '19년도 블록체인 사업 추진 현황

KISA

12대 공공선도 시범사업 과제 [1/2]

국가기록원

표준전자문서의 기록물 관리기관 간 실시간 공유로 **기록물의 진본성 및 무결성 검증**

식품의약품안전처

HACCP 운영 및 인증서 관련 정보 공유를 통해 **식품 위해사고 실시간 대응** 및 **원인 추적, 인증서 위·변조 방지**

방위사업청

방위사업 관련 제안서 및 평가정보를 공유하여 **방위사업의 투명성 제공**

서울의료원

전자처방전, 제증명서 공유로 **의료정보 무결성 보장 및 개인맞춤형 건강관리 정보 제공**

병무청

디지털 ID, 병역행정정보의 공유를 통해 **민원처리, 병무행정 효율화** 및 **대체복무요원 근태관리 신뢰성 제공**

한국남부발전

블록체인 기반 REC 거래시스템을 구축하여 공곱자 선정부터 대금지급까지 **신속하고 정확한 서비스 제공**

II '19년도 블록체인 사업 추진 현황

KISA

공공 · 민간 블록체인 산업 활성화를 위한
대규모 시범사업 및 인식제고 사업 추진

블록체인 시범사업 확대

- 12개 공공선도 시범사업 **32개 기업 참여**
  - **총 사업비 126억** (정부출연금 72억, 자부담금 54억)
- 3개 민간주도 국민프로젝트 **16개 기업 참여**
  - **총 사업비 85억** (정부출연금 45억, 자부담금 40억)

블록체인 산업 생태계 활성화

- TechBiz 컨퍼런스, 블록체인 진흥주간 등 **국민 체감도를 증진**시키고 **생태계 기반을 마련**할 수 있는 행사 추진(**'19년도 예산 2.5억**)
  - TechBiz 컨퍼런스(5,7,9月) / 진흥주간(12.16~18)

공공선도 시범사업 ▶ **과제당 6억원** (상호출자방식)

정부기관(6개)

- 국가기록원 — 신뢰 기반 기록관리 플랫폼
- 방위사업청 — 제안서 접수 및 평가 시스템
- 병무청 — 인증서 없는 민원서비스 제공 플랫폼
- 식품의약안전처 — 국민향 해썹(HACCP) 플랫폼
- 우정사업본부 — 전자우편 사서함
- 환경부 — 탄소배출권 거래 시스템

지방자치단체(4개)

- 부산광역시 — 재난재해 대응 서비스 구축
- 서울특별시 — 시간제 노동자 권익보호
- 전라북도 — 인공지능 맞춤형 관광 설계 시스템
- 제주특별자치도 — 폐배터리유통 이력 관리시스템 구축

민간주도 국민프로젝트 ▶ **과제당 15억원** (상호출자방식)

- 탈중앙화 기부 플랫폼
- 중고차 서비스 플랫폼
- 블록체인 ID/인증 네트워크

공공·산하기관(2개)

- 서울의료원 — 의료·금융 융합서비스 시스템
- 한국남부발전 — 신재생에너지 공급의무화제도 통합관리서비스

II '19년도 블록체인 사업 추진 현황

KISA

12대 공공선도 시범사업 과제 [2/2]

부산광역시

재난정보를 관할기관 간 정보 공유를 통해 **재난상황 대응의 신속성 제고**

제주특별자치도

폐배터리 수주기 정보를 공유하여 폐배터리의 **실시간 이력 검증** 및 **유통 안전성 확보** 가능

서울특별시

근로계약서 관련 정보를 공유 및 분산저장하여 **계약서 위변조 방지** 및 시간제 노동자 권익보호

우정사업본부

전자우편 수발신종추적 정보 통합관리로 온오프라인 **우편물 전달 정확도 증가** 및 **우편 내용의 일치성 제공**

전라북도

관광정보, All@전북(토큰) 사용정보를 활용하여 **수요자 맞춤형 관광서비스 제공**

환경부

탄소배출권 인증·거래 정보를 지속적으로 공유하여 **거래 안전성 및 시장 신뢰성 확보**

II '19년도 블록체인 사업 추진 현황

민간주도 국민프로젝트 3개 과제

탈중앙화 기부 플랫폼

기부자, 캠페인 운영자, 수혜자 간 **기부금 집행내역을 공유**하여 **사회적 불신 해소 및 투명성 확보**

블록체인 ID/인증 네트워크*

모바일 신분증, 스타트업 투자, 대학/협·단체 제증명 발행 등 블록체인 기반 **자기주권형 본인증명 서비스를** 통해 국민의 **개인정보 보호 강화**

* 블록체인 ID/인증 네트워크 기반 금융, 통신, 교육 분야 서비스 개발 및 응용 확산 사업

블록체인 기반 중고차 서비스 플랫폼

중고차 서비스의 각 **단계별 주요 이력을 공유**하여 **중고차 이력정보 위·변조 사전 방지**를 통한 신뢰성 확보

III 향후 추진방향 (1/2)

시범사업 추진 분야의 선택과 집중

블록체인 공공선도 시범사업 과제 선정에 있어 국가 주요 전략과제를 대상으로 수요 발굴 추진 검토

예) 빅데이터, AI, 스마트 시티 등

블록체인 기술지원허브 구축

블록체인 시범사업 참여기업 및 관련기업의 기술개발 및 성능향상을 도모하고 제품의 보안 수준 제고를 위한 개발환경, 보안 검증, 성능시험 서비스 제공

※ TTA와 협업 추진

II '19년도 블록체인 사업 추진 현황

국민참여 평가단 및 인식제고 활동

대국민 의견반영으로 서비스 개선

블록체인 국민참여 평가단

국민참여 평가단 대상 **정례회의 개최**

사전 서비스 체험·품평을 통해 **서비스 개선의견 도출**

대국민 인식제고를 통한 산업 활성화

블록체인 진흥주간

유관기업·기관, 협·단체와 관련 행사 매년 집중 개최

15대 시범사업 사업성과 공유

시범사업 참여사 중심의 **사업 성과 공유 및 발표**

시범사업 성과에 대해 **직접 체험**이 가능한 **전시 부스 운영**

※ 디오라마 존, 체험 서비스 등

블록체인 그랜드챌린지

시범사업 참여사의 플랫폼을 활용한 **블록체인 해커톤 개최**

블록체인을 통해 사회참여 촉진 및 이용자 중심 서비스 혁신이 가능한 **아이디어 공모전 추진**

III 향후 추진방향 (2/2)

우수사례 전파 및 해외시장 개척을 위한 국제화 추진

OECD, ITU 등 국제기구의 ICT 관련 회의 시 시범사업 우수사례를 소개 하고 국제협력활동 적극 추진

KISA 해외 거점(미국, 인도네시아, 오만, 코스타리카, 탄자니아)를 중심으로 국내 우수기업 해외진출 지원

블록체인 기술이 접목된 융복합 신규 사업 발굴

블록체인 시범사업에 KISA의 강점(위치정보, 개인정보, 정보보호)을 활용한 분야와 연계한 융복합 신규 사업 발굴 추진

블록체인으로 여는 미래사회 워크샵

■ **인쇄일** : 2019년 6월 17일
■ **발행일** : 2019년 6월 17일
■ **발행처** : **대한전자공학회**
(06130) 서울시 강남구 테헤란로 7길 22
(역삼동, 과학기술회관 신관 907호)
TEL : 02)553-0255
http://www.theieie.org
■ **인쇄처** : 경민기획 02)2269-1849
kmin1849@hanmail.net