Strictly Private and Confidential

theloop

오픈소스 보안 블록체인 기술 소개와 적용 사례

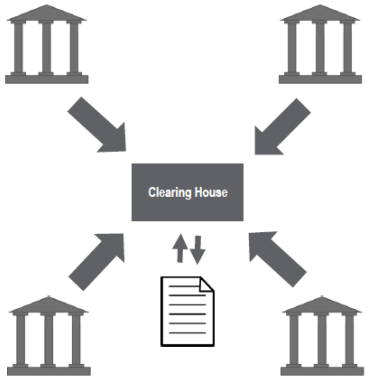
Open Source Blockchain

- 블록체인 개요 및 오픈 소스 동향

블록체인

블록체인 기술의 등장으로 거래 모델이 기존 중앙집중형에서 분산형으로 패러다임 전환이 이루어지고 있음

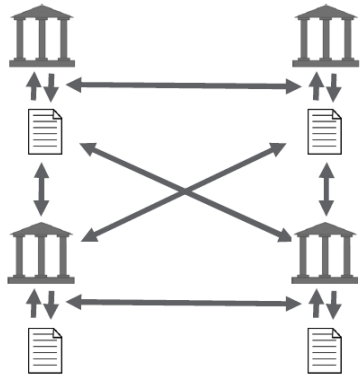
기존 거래 (Centralized Ledger)



Source: Oliver Wyman. For illustrative purposes only.

- 중앙 집중형 구조
- 개인과 제 3자 기관(은행, 정부 등) 간의 거래
- 중앙 서버가 거래 공증 및 관리

블록체인 기반 거래 (Distributed Ledger)



Source: Oliver Wyman. For illustrative purposes only.

- 분산형 구조
- 거래내역이 모든 네트워크 참여자에게 공유 및 보관
- 모든 거래 참여자가 거래내역을 확인(작업증명, Proof-of-work)하는 공증 및 관리

Secure
보안성

Transparent
투명성

Cost Efficiency
경제성

Fraud Reduction
사기방지

Instantaneous
즉시성

블록체인 종류

PUBLIC BLOCKCHAIN (Open Platform)

ethereum

bitcoin

- **Description:**
  - 비트코인 등의 가상화폐가 작동하는 방식으로, 누구나 해당 블록체인 네트워크에 접근 가능
- **퍼블릭 블록체인 이슈:**
  - 거래가 모든 노드들에게 공개되어 있어 보안이 필요한 다양한 거래에 활용할 수 없음
  - PoW, PoS 등의 프로세스를 통해 블록생성 및 거래확정 → 거래 확정의 주체가 불분명
  - 관련규제 및 컴플라이언스 요소를 만족시키기 어려움
  - 블록생성(거래확정) 주기가 길어 빠른 속도가 필요한 거래에 활용하기 어려움

VS.

PRIVATE BLOCKCHAIN (Permissioned Platform)

HYPERLEDGER

theloop

R

ripple

- **Description:**
  - 퍼블릭 블록체인과 달리 허가된 사용자만이 네트워크에 접근하여 정해진 권한만을 이용하기 때문에 금융권 인프라에 적합
- **주요 특징:**
  - 금융기관간 거래에 적합한 거래방식 지원
  - 허가된 사용자들의 합의과정을 통해 거래가 확정되므로 거래 확정의 주체가 명확
  - 규제 및 컴플라이언스 요소들을 만족시킬 수 있도록 커스터마이징 가능하게 설계
  - 거래의 성격에 따라 합의 알고리즘, 블록생성 주기 등을 최적화 하여 빠른 속도가 필요한 거래에도 활용 가능

컨소시엄 동향

블록체인 기술은 단일기관보다는 다자간 거래에서 본질적 가치를 실현할 수 있어, 미국, 중국, 일본 등 해외에서는 금융기관을 중심으로 컨소시엄이 빠르게 구성되고 있는 추세

Global

R3CEV

DBS J.P.Morgan UBS HSBC + 70개 금융기관

- **Founded:** 2015년 9월
- **Description:**
  - 분산장부기술 기반의 해외송금 및 트레이딩 시스템 구현
  - 블록체인 기반 디지털 화폐 개발

China

The Financial Blockchain Shenzhen Consortium

平安银行 PING AN BANK 腾讯 Tencent + 30개 기술사 및 금융기관

- **Founded:** 2016년 5월
- **Description:**
  - 보험 및 트레이딩 플랫폼 적용
  - 블록체인 기술이 적용 가능한 금융분야에 블록체인 적용 예정

Japan

The Japan Bank Consortium

MIZUHO 住信SBIネット銀行 SBI Sumishin Net Bank SMFG MUFG + 30개 은행

- **Founded:** 2016년 10월
- **Description:**
  - 24시간 운영되는 실시간 국내외 송금 인프라 구현 목표
  - 2017년 봄 PoC 거쳐 서비스 출시 예정

Korea

Financial Investment Blockchain Consortium

신한금융투자 금융투자협회 Korea Financial Investment Association true friend 한국투자증권 NH투자증권 MIRAE ASSET 미래에셋대우 + 25개 증권사

- **Founded:** 2016년 12월
- **Description:**
  - 증권사 간 인증 공동 플랫폼 구축
  - 청산결제 자동화와 장외거래 등 단계적으로 연구 및 추진

Hyperledger Project

Linux Foundation에서 진행하고 있는 오픈소스 블록체인 프로젝트로 비지니스 거래에 적용할 수 있는 블록체인 플랫폼 개발을 목표로 하고 있음

Hyperledger Burrow

Hyperledger Burrow provides a modular blockchain client with a permissioned smart contract interpreter partially developed to the specification of the Ethereum Virtual Machine (EVM).

Hyperledger Fabric

Hyperledger Fabric is an implementation of blockchain technology that is intended as a foundation for developing blockchain applications or solutions.

Hyperledger Iroha

Hyperledger Iroha is a distributed ledger project that was designed to be simple and easy to incorporate into infrastructural projects requiring distributed ledger technology.

Hyperledger Sawtooth

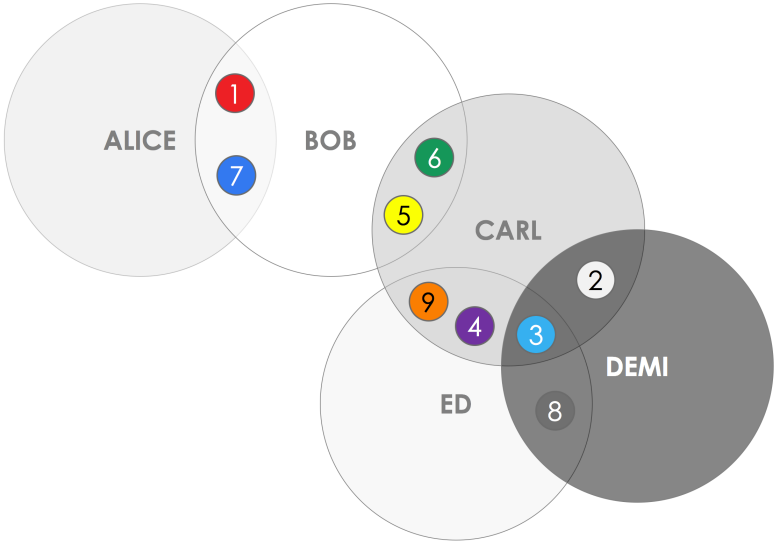
Hyperledger Sawtooth is a modular blockchain suite designed for versatility and scalability.

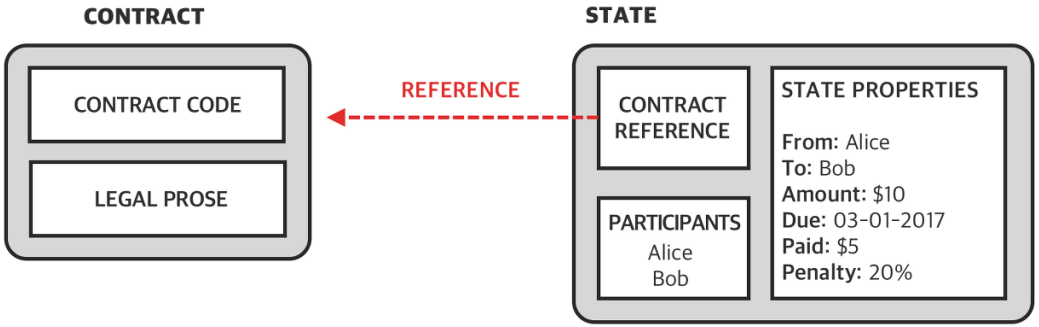
Hyperledger Indy

Hyperledger Indy provides tools, libraries, and reusable components for interoperable digital identities rooted on blockchains or other distributed ledgers.

R3 Corda

R3는 전세계 80여개 은행들이 블록체인 컨소시엄으로 2016년 12월 자체 블록체인 플랫폼인 Corda 공개하였고 Hyperledger 프로젝트에도 참여중임





- 이해당사자만 거래 데이터를 공유
- 모든 노드들이 데이터를 공유하는 블록체인 구조 아님
- 블록체인이 아닌 분산 원장 플랫폼

- Corda 스마트 컨트랙트
- 계약 코드(Contract Code)와 계약의 상태인 볼트(Voult), 실제 제도권을 지원하기 위한 법률언어(Legal Prose)로 구성

loopchain Introduction

- loopchain 소개 및 오픈소스 프로젝트

theloop

loopchain 개요

공개된 블록체인 기술은 실제 엔터프라이즈 서비스에 적용하는데 한계가 있었으며 적용 거래에 따라 모든 부분에서 최적화가 가능한 블록체인 엔진이 필요

Distributed Ledger | Smart Contract | Attempt for Enterprise | Optimized for Enterprise

loopchain 주요 특징

엔터프라이즈 환경에 적용할 수 있고 엔진부터 응용까지 전 스택에서 커스트마이징이 가능한 Enterprise Blockchain

SCORE (Smart Contract On Reliable Environment)
자체 개발한 생산성 높은 스마트 계약 플랫폼으로 다양한 서비스 구현 가능

LFT Algorithm
BFT를 지원하는 고성능 합의 알고리즘을 기반으로 실시간 거래 지원

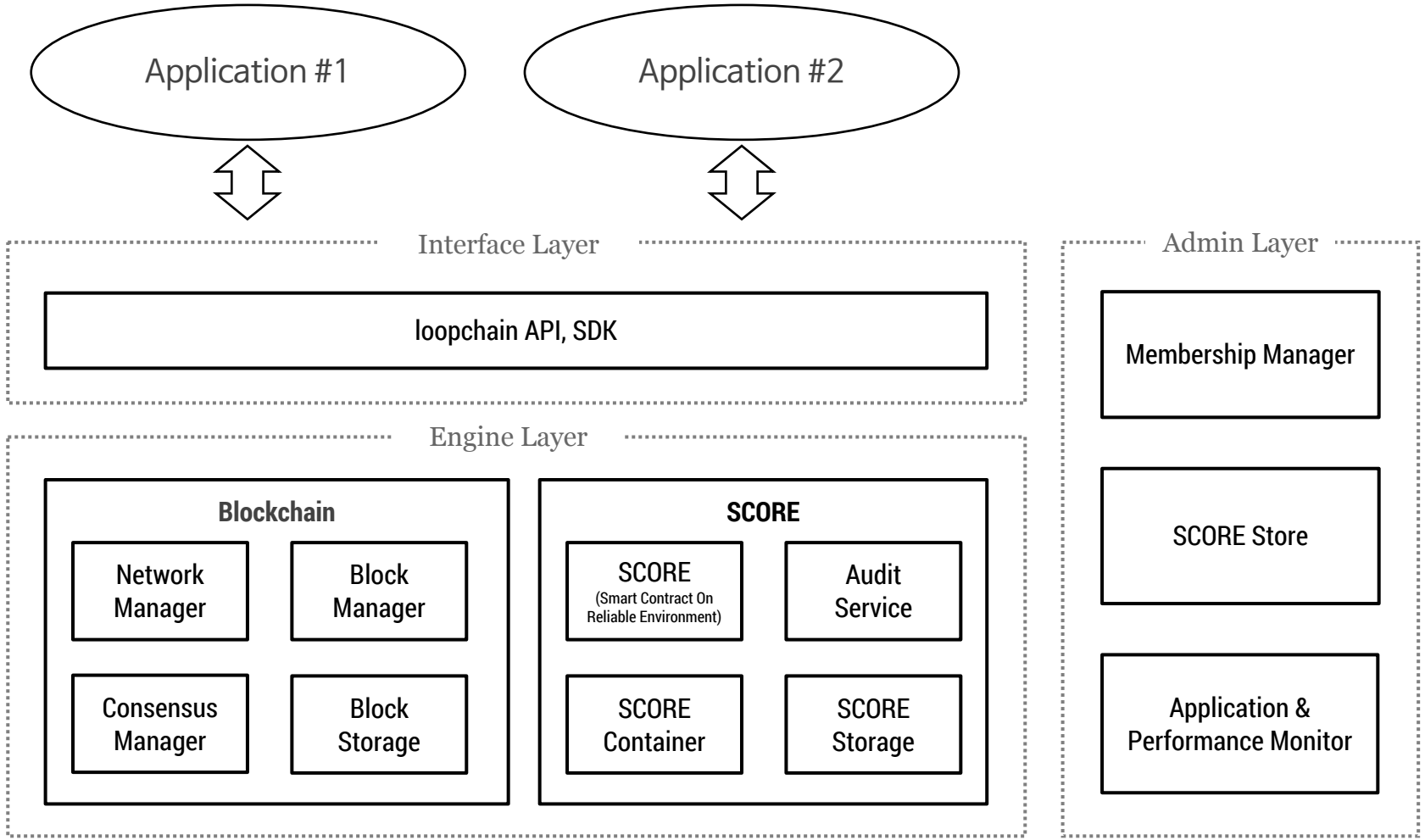
Multi Channel
하나의 독립적인 블록체인 네트워크내에서 업무별로 가상의 네트워크를 구성하여 채널별로 거래 요청, 합의 및 스마트컨트랙트 수행

Tiered System
인증된 기관의 참여와 거래·감사 등 차등적 권한을 기반으로 엔터프라이즈 환경에 적합한 시스템 구현

Modular Architecture
합의 및 검증부터 블록체인 엔진까지 거래에 따라 풀스텍 커스터마이징 가능

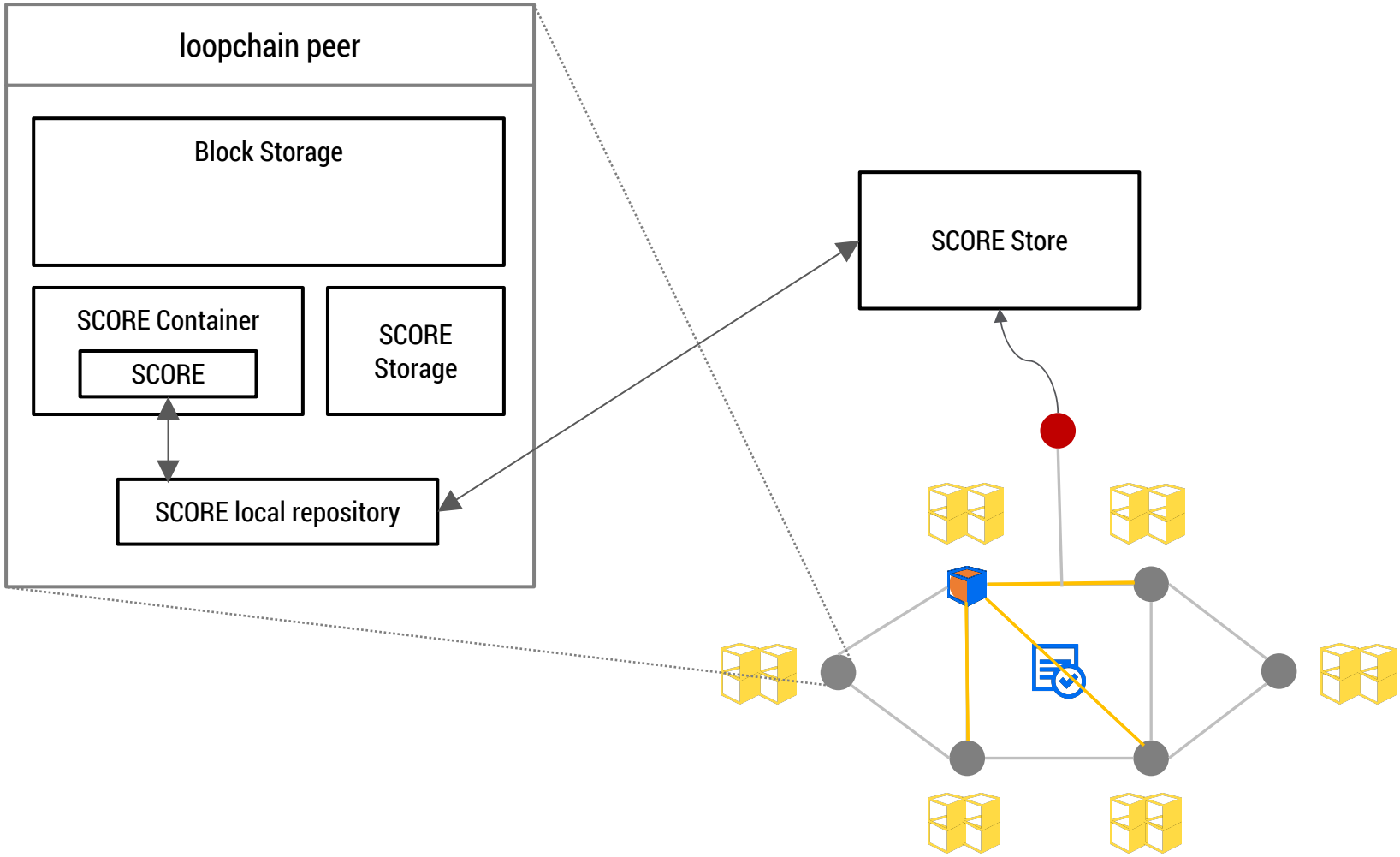
loopchain 구조도

모듈 방식 아키텍처를 채택하여 참여 노드 인증 및 합의 알고리즘, Smart Contract 모듈 등을 필요시마다 추가 및 커스트마이징 가능



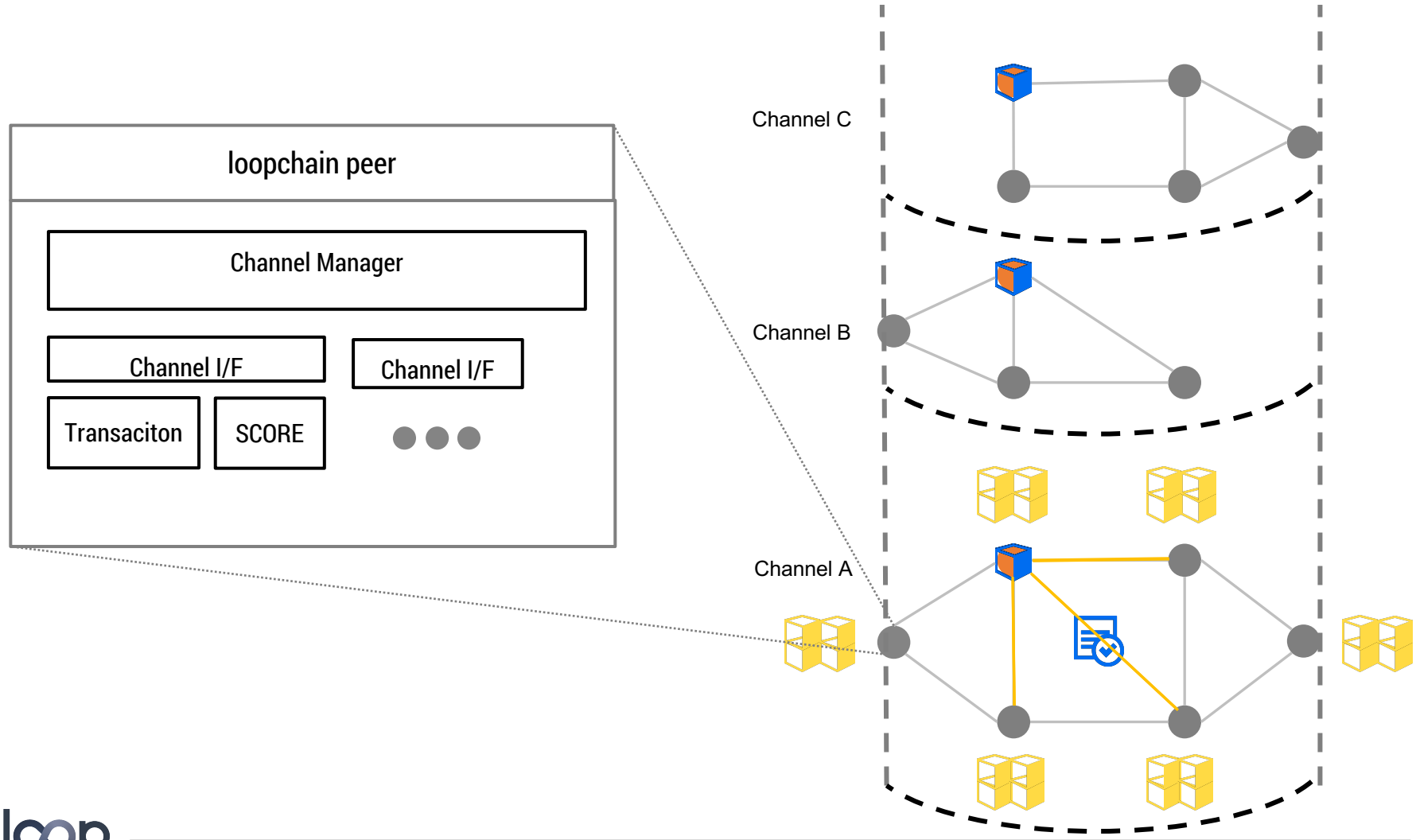
SCORE (Smart Contract on Reliable Environment)

loopchain 상에서 실행되는 Smart Contract로서 개발 생산성이 높고 SCORE Store를 통한 등록, 배포 및 버전 관리를 제공하여 다양한 업무 구현 가능



Multi Channel 지원

loopchain peer내에 채널별 거래 및 SCORE 분리를 제공하여 하나의 블록체인 네트워크에서 거래 당사자만 참여하는 업무별 채널 구성 가능



loopchain 오픈소스 프로젝트

오픈소스 프로젝트를 통한 신뢰성 확보 및 개발 생태계 구축을 통한 플랫폼 영향력 확대 필요

필요성	내용
블록체인 플랫폼 신뢰도 확보	▪ 블록체인 기술 특성상 신뢰가 중요하여 주요 블록체인 솔루션은 오픈소스화 통해 공개 검증이 이루어짐 ▪ 다양한 개발자를 통해 요구사항 소프트웨어 취약점 파악에 도움
오픈 소스를 통한 개발 생태계 구축	▪ Apache 2.0 라이선스를 통해 다양한 분야에서 무료로 사용 가능한 플랫폼 개발 ▪ 오픈 소스를 통해 개발자들이 다양한 서비스를 개발하고 수익을 창출할 수 있는 생태계를 구축하여 플랫폼 영향력 확대
피드백을 통한 플랫폼 진화	▪ 블록체인은 새로 시작하는 기술로 급격하게 진화하는 중 ▪ 소스 및 백서 등 문서 공개를 통해 다양한 외부 피드백 수용하여 플랫폼 반영

2017년 미래창조과학부 정보통신산업진흥원 지원 유망 공개SW 기술개발 지원 사업자로 선정

loopchain 오픈소스 프로젝트 일정

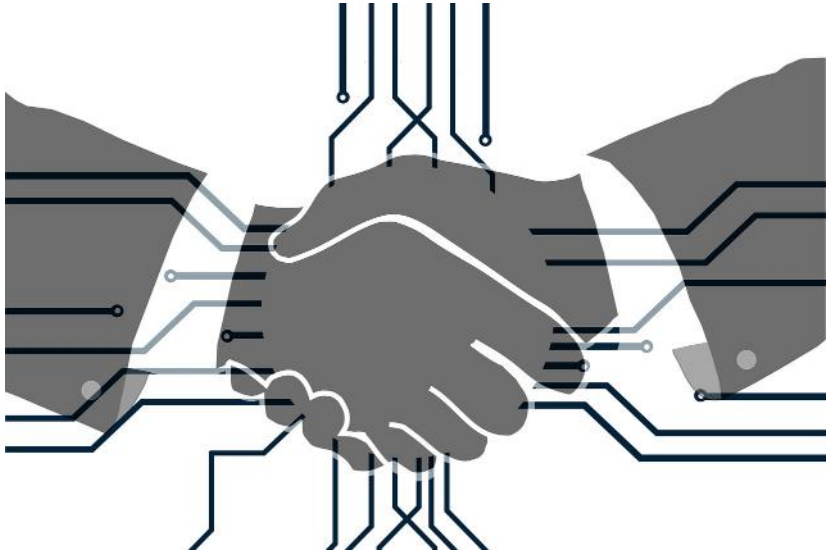
오픈소스 커뮤니티 구성 및 개발을 통한 오픈소스 프로젝트 정착

Smart Contract

- 블록체인 기반 스마트 컨트랙트

Smart Contract

- Nick Szabo가 1994년 최초 제안
- 계약 조건을 실행하는 컴퓨터 트랜잭션 프로토콜
- 지불 조건, 유치권, 기밀 유지 및 시행과 같은 일반적인 계약 조건 충족하고 악의적이거나 우발적인 예외 사항을 최소화
- 신뢰할 수있는 중개자의 필요성을 최소화



Smart Contract on Blockchain

블록체인을 단순한 분산 원장이 아닌 어플리케이션 서버로 확장하여 다양한 거래 서비스를 가능하게함

- Bitcoin Contract Code
  - 거래 정보에 누가(input) 누구에게(output) 얼마를(output value) 지불하며, 어떻게 검증할지(script) 기록됨
  - script는 OPCODE로 구성하여 script가 정상이면 거래를 정상으로 인정한다는 계약 조건을 명시한 것과 같은 효과 → Contract Code
  - OPCODE 는 Constants, Flow Control, Stack, String 의 Splice, Bitwise, Arithmetic, Crypto, Locktime, Pseudo-Words 의 카테고리에 해당하는 85개 정도의 명령어를 제공

- Ethereum Smart Contract
  - Vitalik Buterin
  - 함수를 공유한 상태에서 블록체인으로 함수 입력값을 공유하고 무결성을 보장하면 함수 결과값의 무결성도 보장할 수 있지 않을까?
  - Bitcoin의 Contract Code를 확장하여 완전한 업무 개발이 개발이 가능하도록 검증, 연산을 넘어 “상태”와 “함수”를 정의하고 “상태변이”와 “데이터 저장”이 가능한 Turing Complete 코드 개발을 가능하도록 함

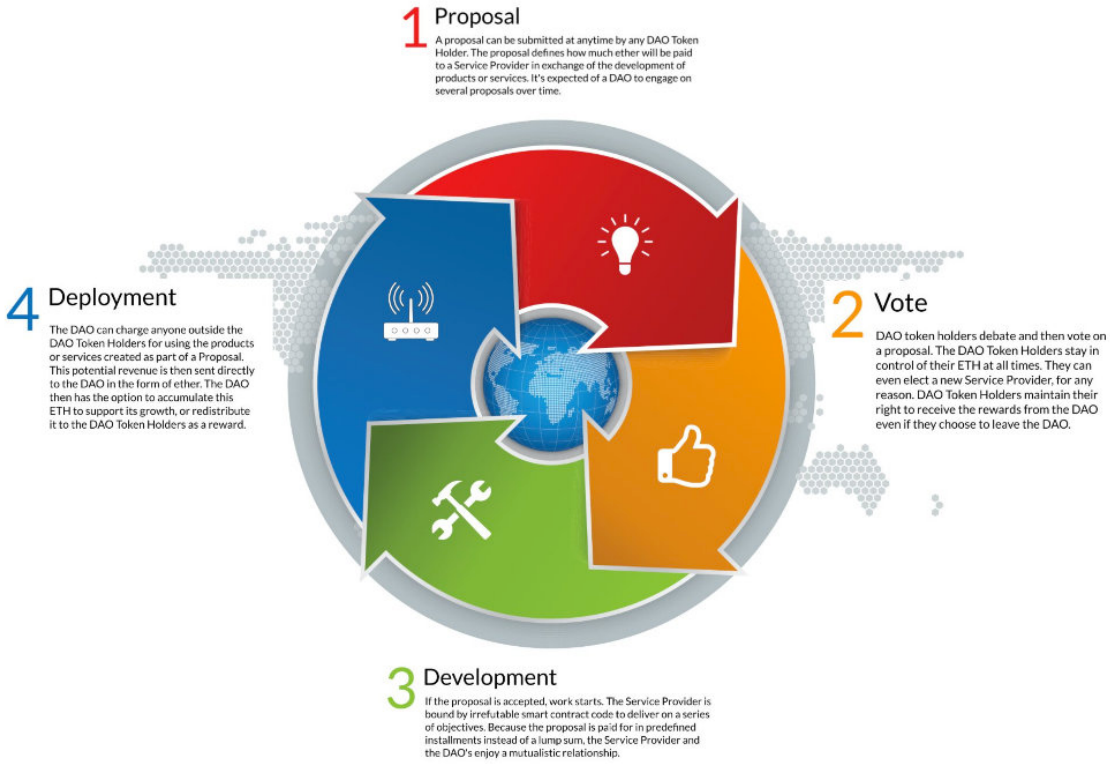
단순한 잔고가 아닌 일반적인 데이터가 블록체인을 통해 신뢰할 수 있게 변경 가능한 대상이 되어 금융, IoT, 분산컴퓨팅 등 다양한 곳에 블록체인을 적용할 수 있게 됨

DAO (Decentralized Autonomous Organization)

대표적인 이더리움 스마트 컨트랙트 중 하나로 탈 중앙화된 자율적인 벤쳐 캐피탈

- 펀딩
  - 회사의 의결권을 토큰(DAO Token)으로 행사할 수 있도록 함
  - 크라우드 펀딩을 통해 토큰을 이더로 구입할 수 있도록 판매
  - 약 2000억원 펀딩

- 운영 방식
  - 토큰을 보유한 누구라도 투자 제안서를 등록할 수 있음
  - 토큰을 통해 투자 제안서에 대해 투표
  - 제안이 통과되면 스마트 컨트랙트 기반으로 이더가 전송
  - 투자금 회수도 스마트 컨트랙트 기반으로 처리
  - 토큰 보유자는 언제던지 자신의 토큰을 이더로 환불 가능 (환불된 토큰은 다른 사람이 구매 가능)



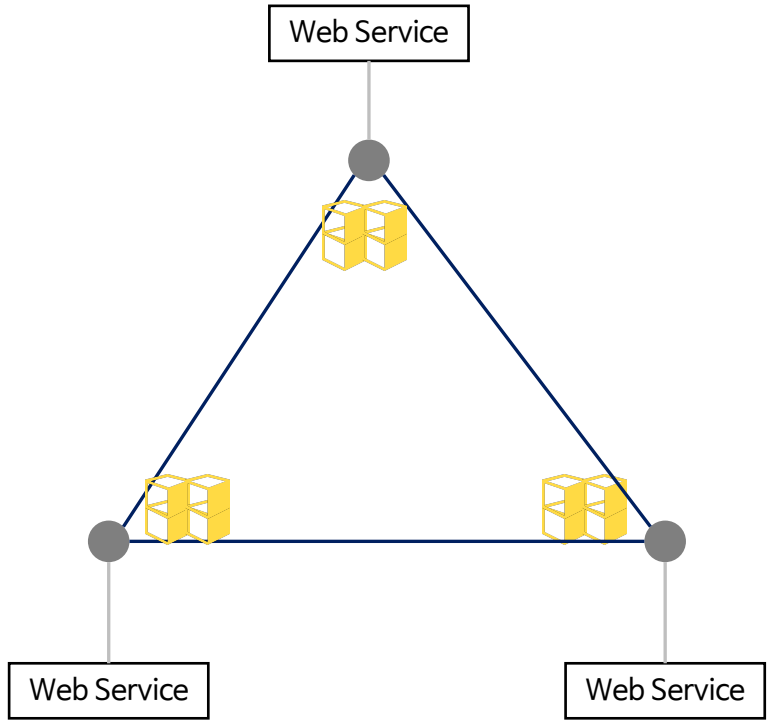
SCORE Demo (Chat Service)

Smart Contract기반 응용 서비스 Demo – SCORE로 작성된 채팅 서비스

- 채팅 서비스를 중앙화된 채팅 서버없이 블록체인 상에서의 Smart Contract로 구현

- 계약 내용
  - 계약으로 공유하는 데이터는 대화내역
  - 각 노드가 보내는 거래 내역에 메세지 내용 포함
  - 거래 내역에 포함된 노드의 전자서명이 정당하면 거래 내역에 포함된 메세지를 대화 내역에 추가함

- 데모 환경
  - 세개의 peer로 구성된 loopchain 구성
  - 각각의 peer에 loopchain API로 개발된 채팅 웹 서비스 노드 구현
  - 각 노드별 채팅 웹 서비스를 통해 브라우저로 접근하여 채팅 서비스 실행



Case Study - KOFIA

- 스마트컨트랙트 기반 금투협 공동인증 소개

theloop

블록체인 기반 공동인증서비스 구현 목표

블록체인을 통해 발급된 공동인증서 사용으로 효율적, 안정적인 전자서명 체계 구축

블록체인을 활용한

“인증기관 없는” 전자서명 체계 구축

인증 시스템 효율화

- 인증기관을 통한 인증서관리 및 유효성 검증에 소요되는 리소스 절감
- 정보의 중앙 집중으로 발생하는 Risk 및 타기관 의존요소 제거

고객의 인증서 사용편의 증대

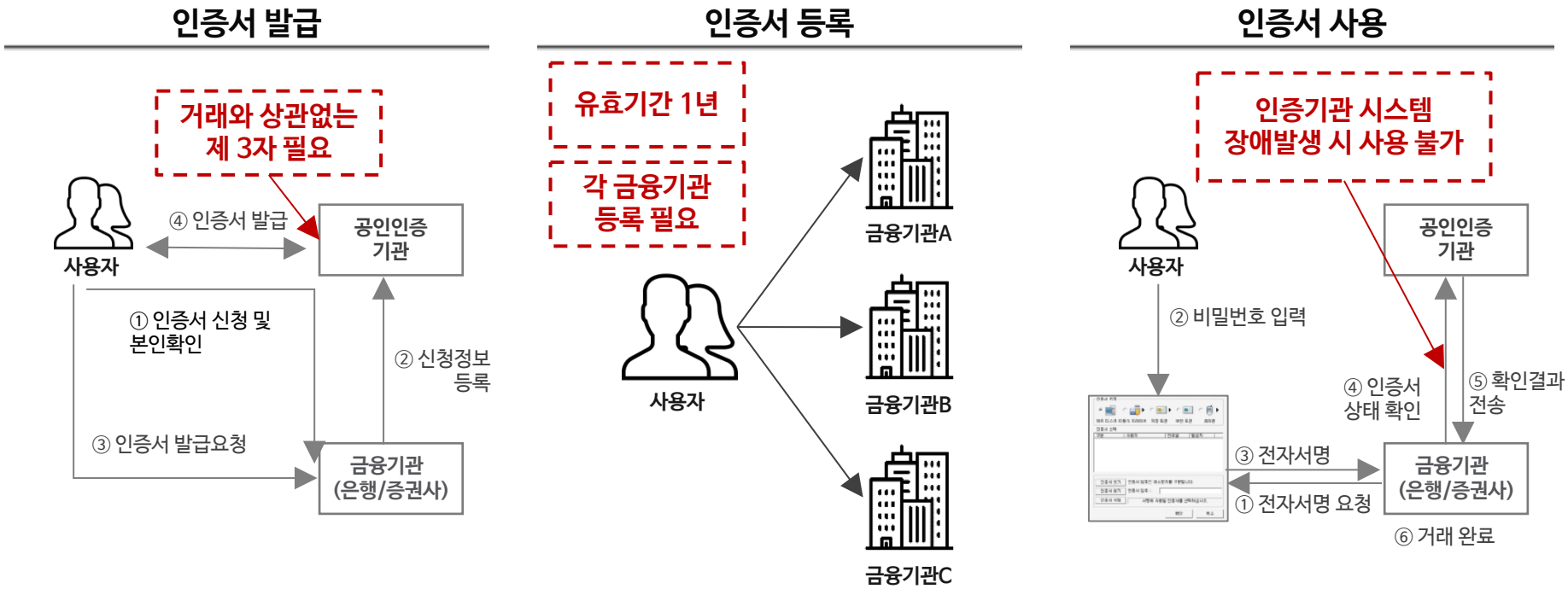
- 자체 인증정책 적용을 통한 다양한 편의요소 제공
- 참여기관 지속적 확장을 통한 사용성 확대

블록체인 네트워크 활용 사업영역 확대

- 향후, Trading 영역에 블록체인을 적용할 인프라 선구축 및 블록체인 기술 관련 사전학습효과 기대
- 본인확인 서비스제공 등 추가 사업기회 발굴

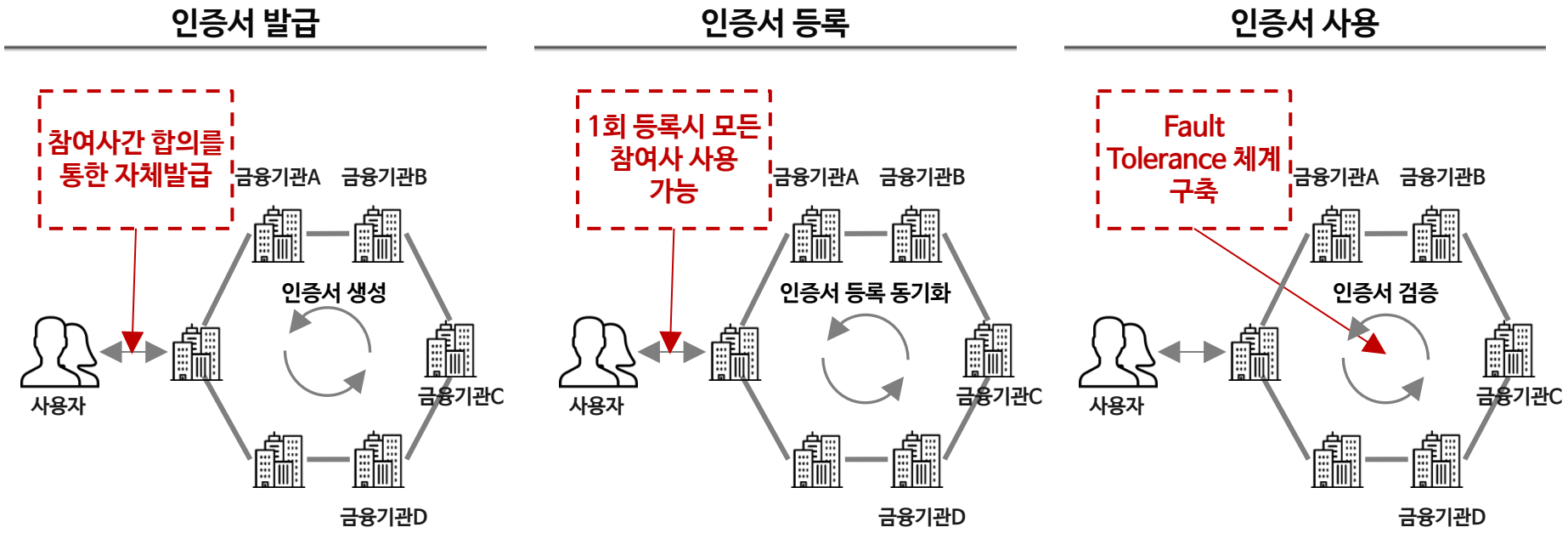
공인인증 운영 프로세스: As-Is

거래 당사자가 아닌 별도의 신뢰하는 제3자(공인인증기관)가 필요하며 이를 운영하기 위한 비용 발생 및 인증서 사용을 위한 번거로운 등록절차 존재



공동인증 운영 프로세스: To-Be

블록체인 기반의 인증서 발급/등록/사용이 가능하도록 구현하여 불필요한 프로세스 및 비용절감 효과 극대화



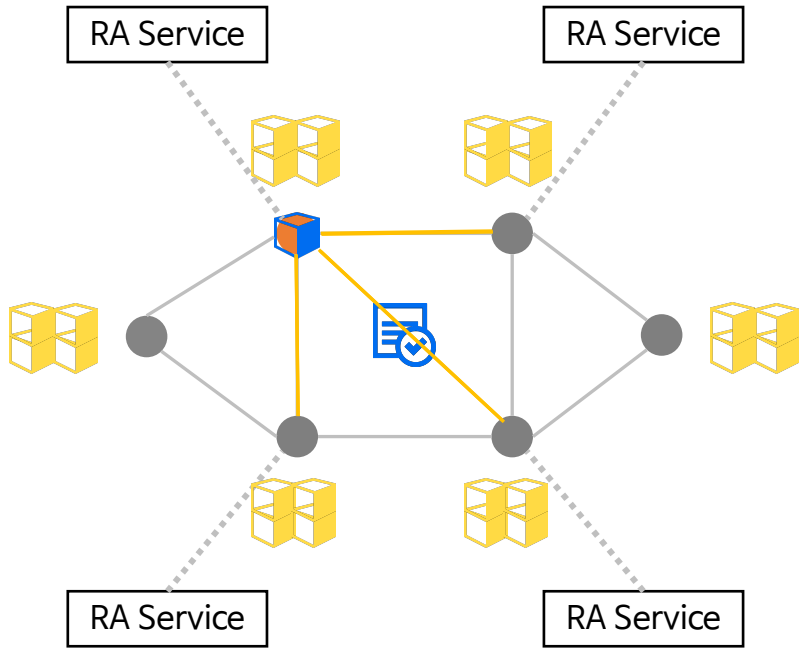
SCORE 기반 인증 서비스 개요

인증서 발급 및 상태 확인 기능을 별도의 인증기관 서비스를 만드는 것이 아닌 SCORE로 구현하여 loopchain에 등록하여 블록체인 자체가 참여 노드가 모두 신뢰할 수 있는 인증기관이 됨

- 인증서 발급 및 검증 서비스를 중앙화된 인증기관없이 블록체인 상에서의 Smart Contract로 구현

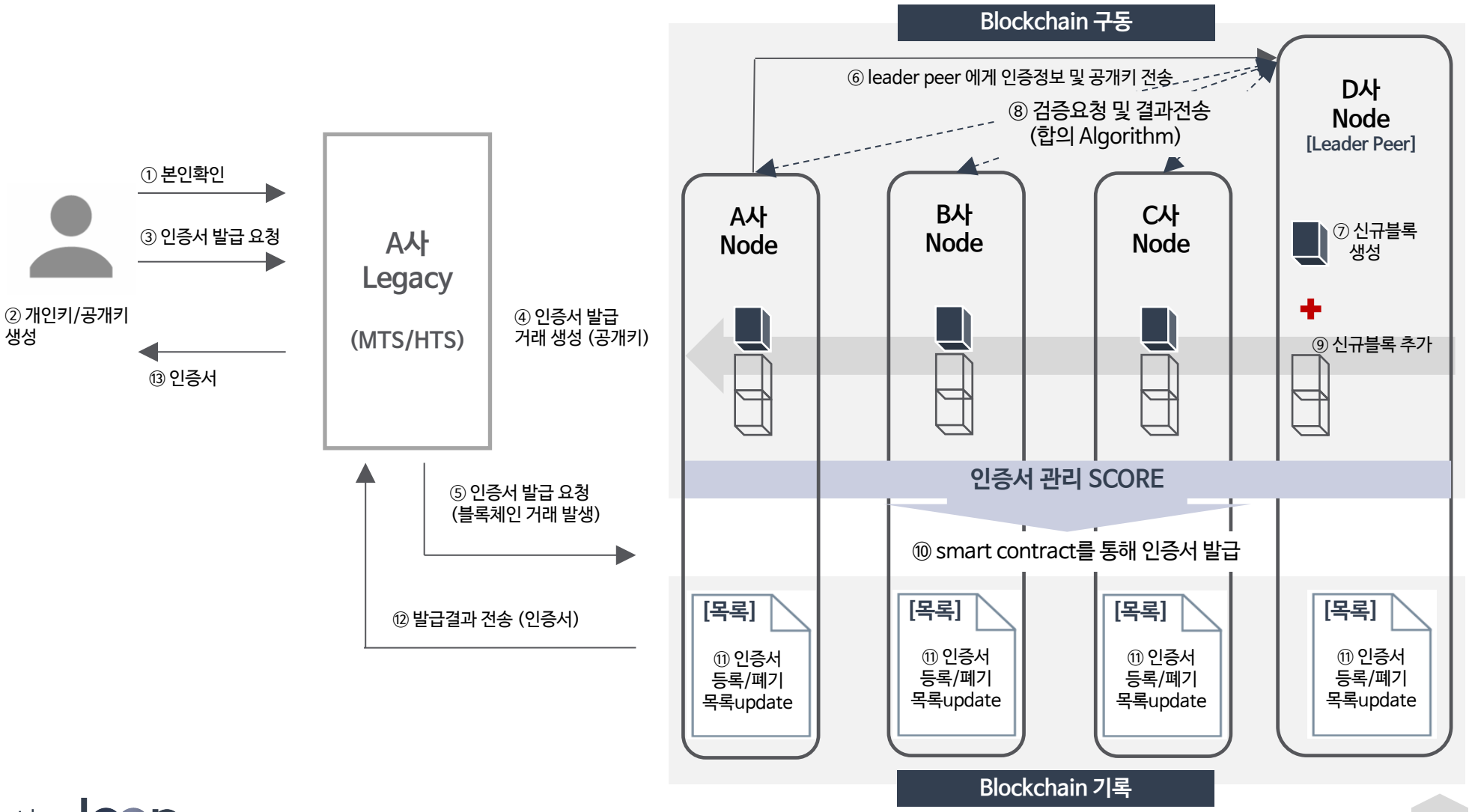
- 계약 내용
  - 계약으로 공유하는 데이터는 인증서 및 인증서 상태정보
  - 각 노드가 보내는 거래 내역에 인증서 발급에 필요한 정보(DN, 유효기간, 사용자 공개키 등) 포함
  - 거래 내역에 포함된 노드의 전자서명이 정당하면 거래 내역에 포함된 발급 요청 정보를 기반으로 인증서를 발급하여 계약 데이터에 포함함

- 특징
  - 블록체인 자체가 인증기관이 되어 인증서를 발급하는 별도의 인증기관이 필요없음
  - 인증서 발급키를 SCORE 기반으로 블록마다 생성하여 사용하여 별도의 인증서 발급키 관리없이 X.509 형식의 인증서 발급
  - 금융기관은 공인인증체계와 같이 RA 역할을 수행



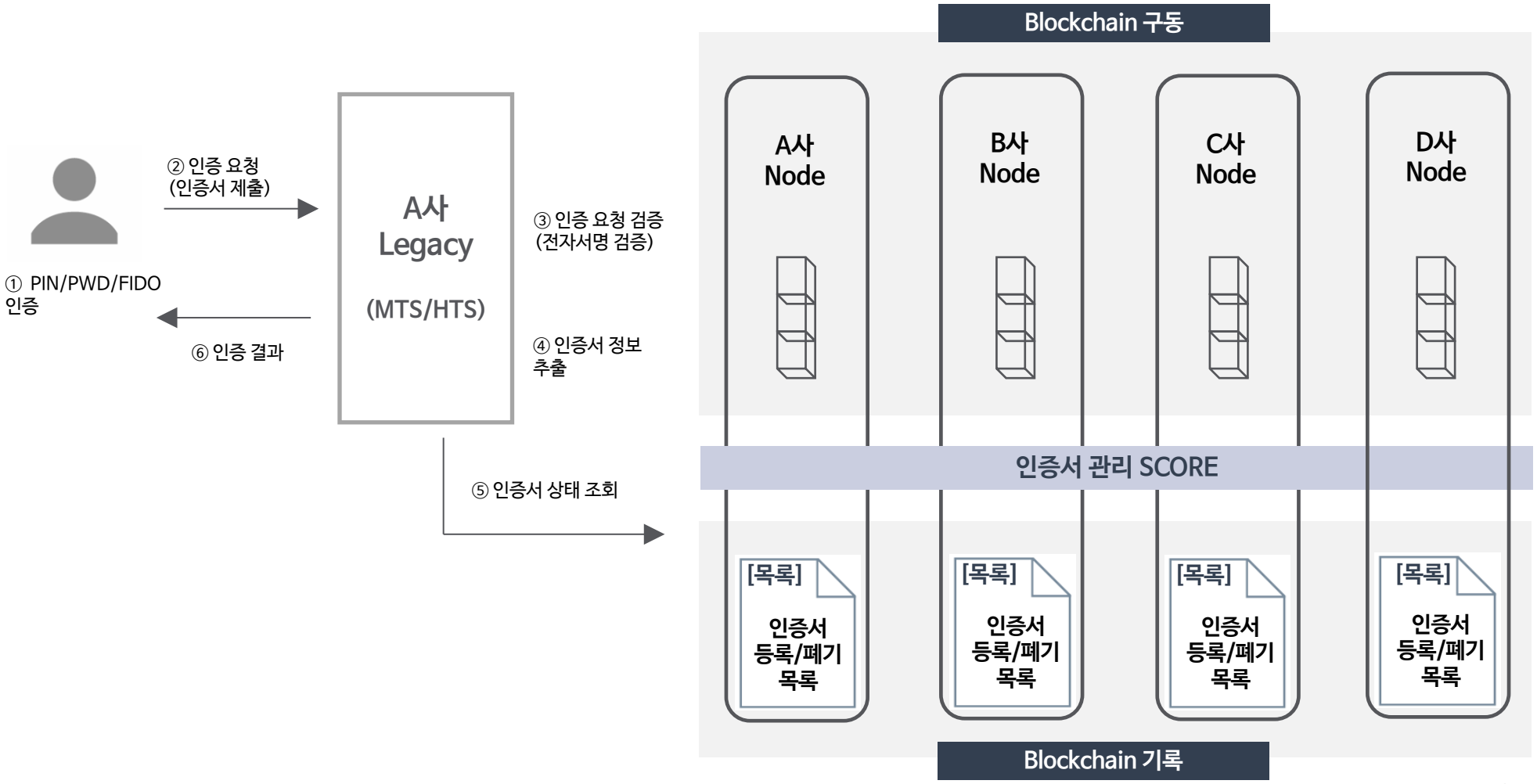
블록체인 기반 인증서 발급

각 증권사를 통해 인증서 발급 요청 후 인증서 발급에 필요한 정보를 기반으로 거래를 생성하고 이에 대한 Smart Contract를 실행하여 인증서 생성



블록체인 기반 인증서 유효성 확인

각 참여기관의 Smart Contract에 저장된 인증정보로 인증서 유효성 확인 : 기존 OCSP와 동일한 기능 제공



『금융투자업권 블록체인 컨소시엄』 로드맵

적용 예상업무	**블록체인 기반 공동 인증 및 정보 공유**	**금융투자상품의 청산결제**	**장외채권, OTC파생상품 등 금융투자상품의 거래**
내용	▪ 금투업권 공동 인증시스템 도입 ▪ 간편인증 및 생체인증 도입 ▪ 문서부인 방지 ▪ 의심/혐의거래 및 대포통장 등의 정보공유	▪ 청산결제 업무의 자동화 및 단순화 ▪ 블록체인을 이용한 보안 메시지 시스템 도입	▪ 금투융자상품 거래 시스템에 대한 블록체인 도입 ▪ 대체거래 시스템(ATS) 도입 ▪ 자금세탁방지(AML) 도입
효과	▪ 공인인증서 대체 등 인증 관련 비용 절감 ▪ 신뢰성과 실시간성을 확보한 정보 공유를 통한 고객 서비스 향상 및 업무 효율화	▪ 청산결제 등 Post-Trading 업무 효율성 향상 ▪ Post-Trading 시간 단축으로 인해 Liquidity Risk 감소	▪ 실시간 거래 매칭 및 즉시 체결 시스템 구축 가능 ▪ 실시간 소유권 확인을 통한 Counterparty Risk 제거

Thank you

theloop

theloop Inc. www.theloop.co.kr

L 서울시 영등포구 국제금융로 10 서울국제금융센터(Three IFC) 19층
T +82. 2 6105.8100
F +82. 2 6105.0121