

the loop

loopchain-블록체인으로 진짜 서비스
만들어보기



말은 많은 Blockchain

● Blockchain
검색어

+ 비교

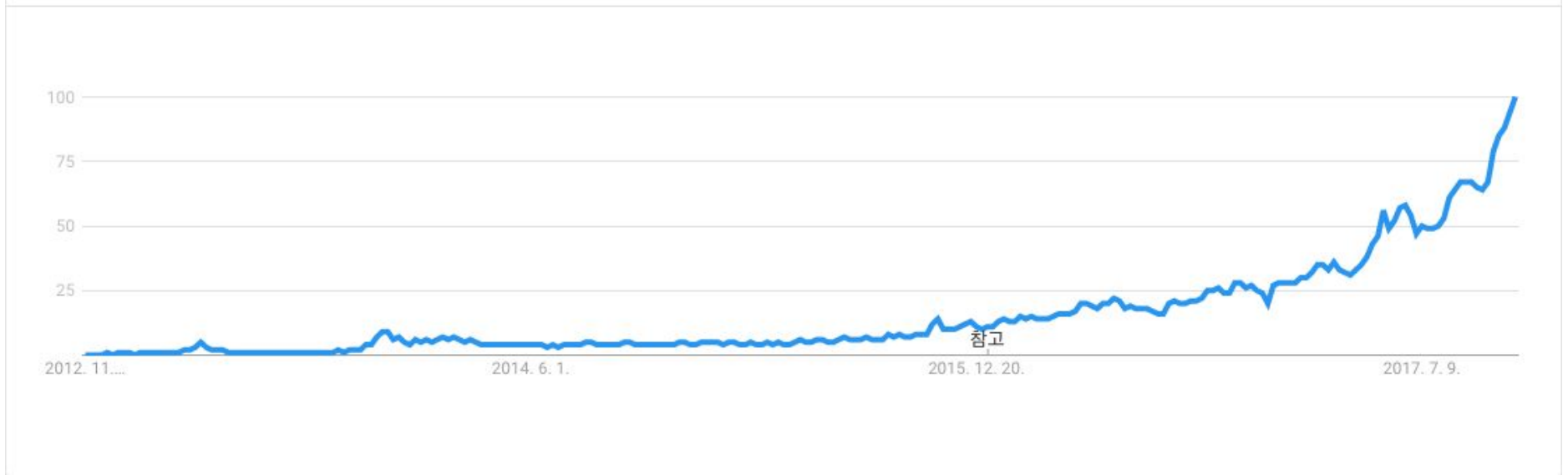
전 세계 ▼

지난 5년 ▼

모든 카테고리 ▼

웹 검색 ▼

시간 흐름에 따른 관심도 변화 ?



진짜 만든 것은 있나?

뭐가 많이 있기는 한데..... 우리가 써먹어 볼건 있나요?

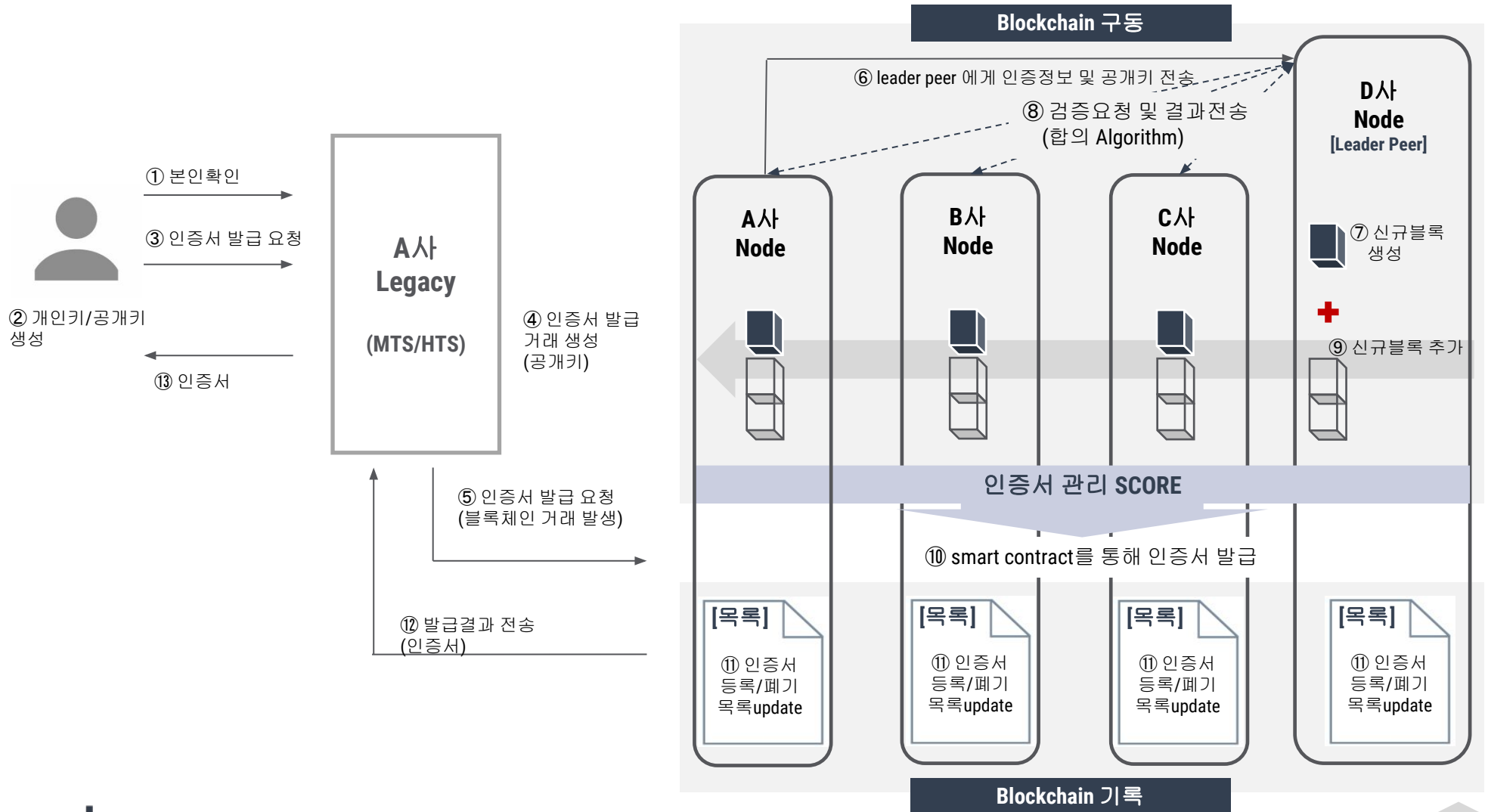


그런데 이런 일이 일어났습니다.



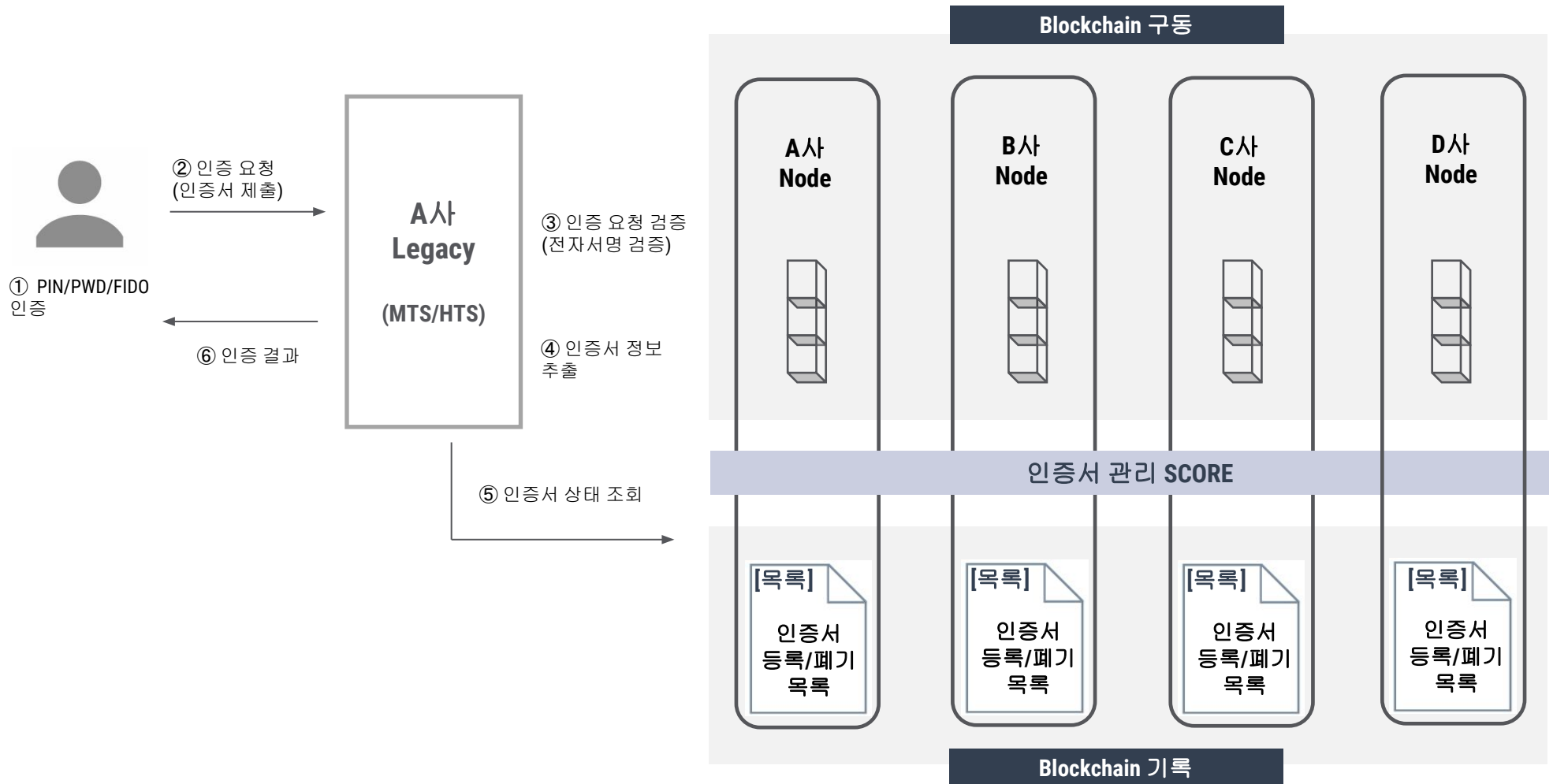
월 만든건가요?: 블록체인 기반 인증서 발급

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



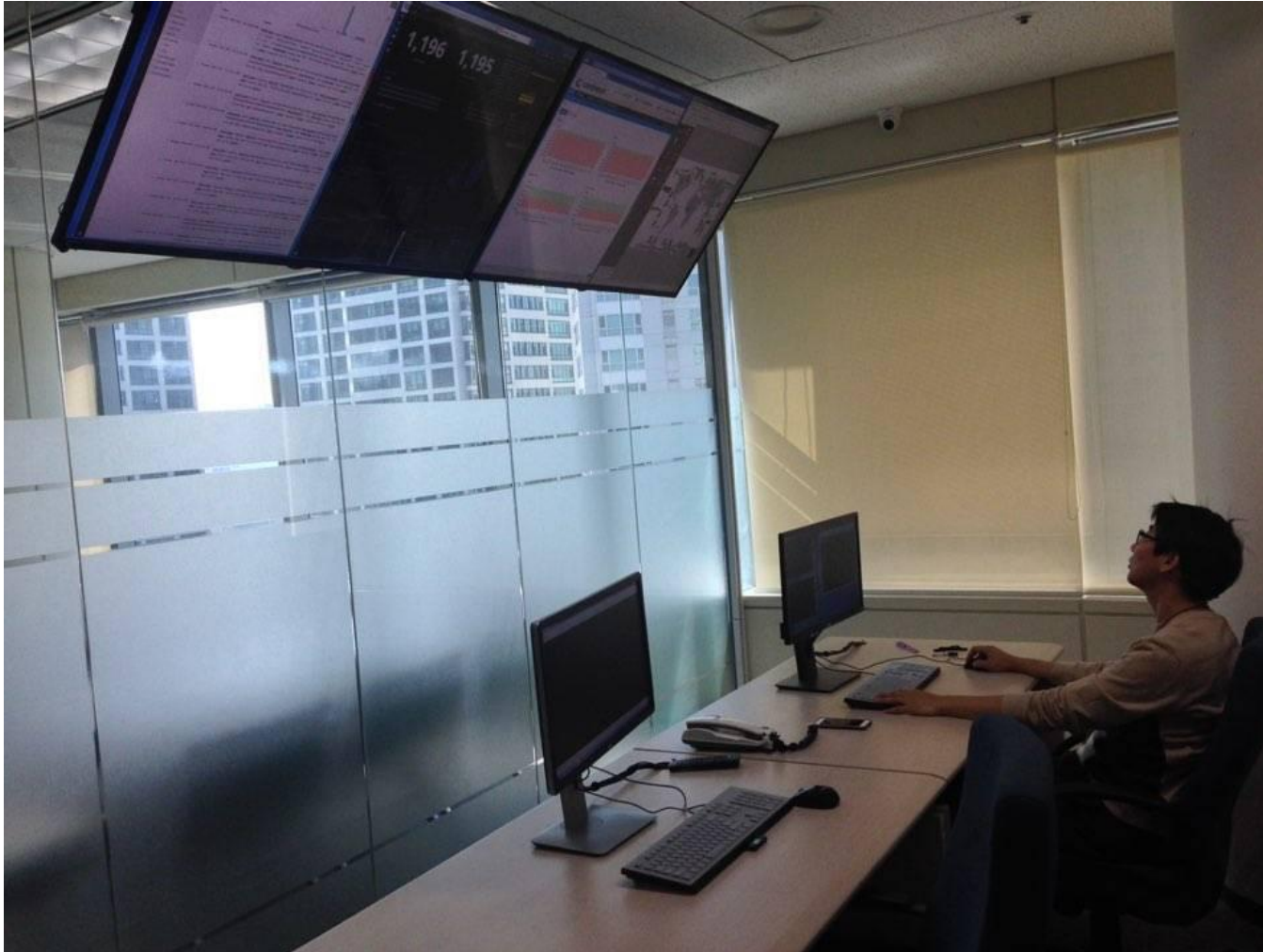
월 만든건가요?: 블록체인 기반 인증서 유효성 확인

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



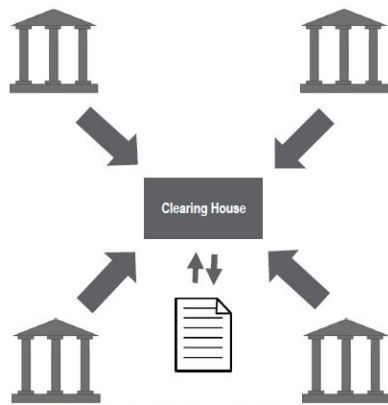
물론 그 뒤의 개발자들의 모습은.....

사실 저분은 서비스 관리자이십니다. (개발자들은 댄에서...)



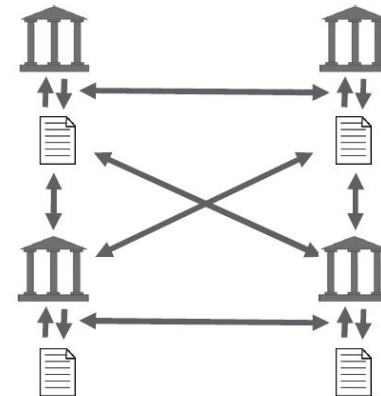
기술 개요 : 블록체인은 중개자 없이 신뢰할 수 있는 거래를 실현하는 기술

기존 전자 금융 거래



- 중앙 집중형 구조(Centralized Ledger)
- 개인과 제 3자 기관(TTP : Trusted Third Party) 간의 거래
 - 은행, 정부 등
- 중앙 서버가 거래 공증 및 관리

블록체인을 적용한 전자 금융 거래



- 분산형 구조(Distributed Ledger)
- 제3자 기관 없이 **Peer-to-Peer** 네트워크 기반 신뢰 비즈니스 네트워크 구성 가능
- 위변조가 거의 불가능하고, 거래 시간과 운용비용 획기적 절감

기술 개요 : 공개 블록체인의 한계로 프라이빗 블록체인 대두

구분	퍼블릭 블록체인	프라이빗 블록체인
읽기 권한	누구나 열람 가능	허가된 기관만 열람 가능
트랜잭션 검증 및 승인	누구나 네트워크에 참여하면 거래 검증 및 승인 가능	승인된 기관만 가능
트랜잭션 생성	누구나 거래 생성 가능	거래 생성 권한이 있는 기관만 가능
합의 알고리즘	부분 분기를 허용하는 작업증명이나 지분증명 알고리즘	부분분기를 허용하지 않는 BFT 계열 의 합의 알고리즘
속도	7 ~ 20 TPS	1000 TPS 이상의 고성능
권한 관리	누구나 같은 권한을 가짐	Private Channel, Tiered System 등을 통하여 읽기, 쓰기 권한 관리가 가능
예시	비트코인, 이더리움	Loopchain, IBM Fabric, R3 Corda

- 비트코인, 이더리움 등 공개 블록체인은 낮은 성능 및 데이터 공개 이슈 존재
- 모든 노드가 같은 권한을 가져 금융 거래 등 규제가 필요한 영역 적용에 한계가 있음
- R3 CEV, IBM 등의 국제 기업들이 공개블록체인의 한계를 극복하기 위한 프라이빗 블록체인 개발 연구 중

loopchain 주요 목표

금융 서비스에 적용할 수 있고 엔진부터 응용까지 전 스택에서 커스트마이징이 가능한 Private Blockchain



Private Channel

인증된 기관만 참여하고 거래 기록 보호



Tiered System

거래/감사 등 차등적 권한을 기반으로
금융업무에 적합한 시스템 구현



Performance

빠른 합의를 기반으로 거래 시간 단축



Customization

합의 및 검증 등 다양한 커스트마이징이 가능

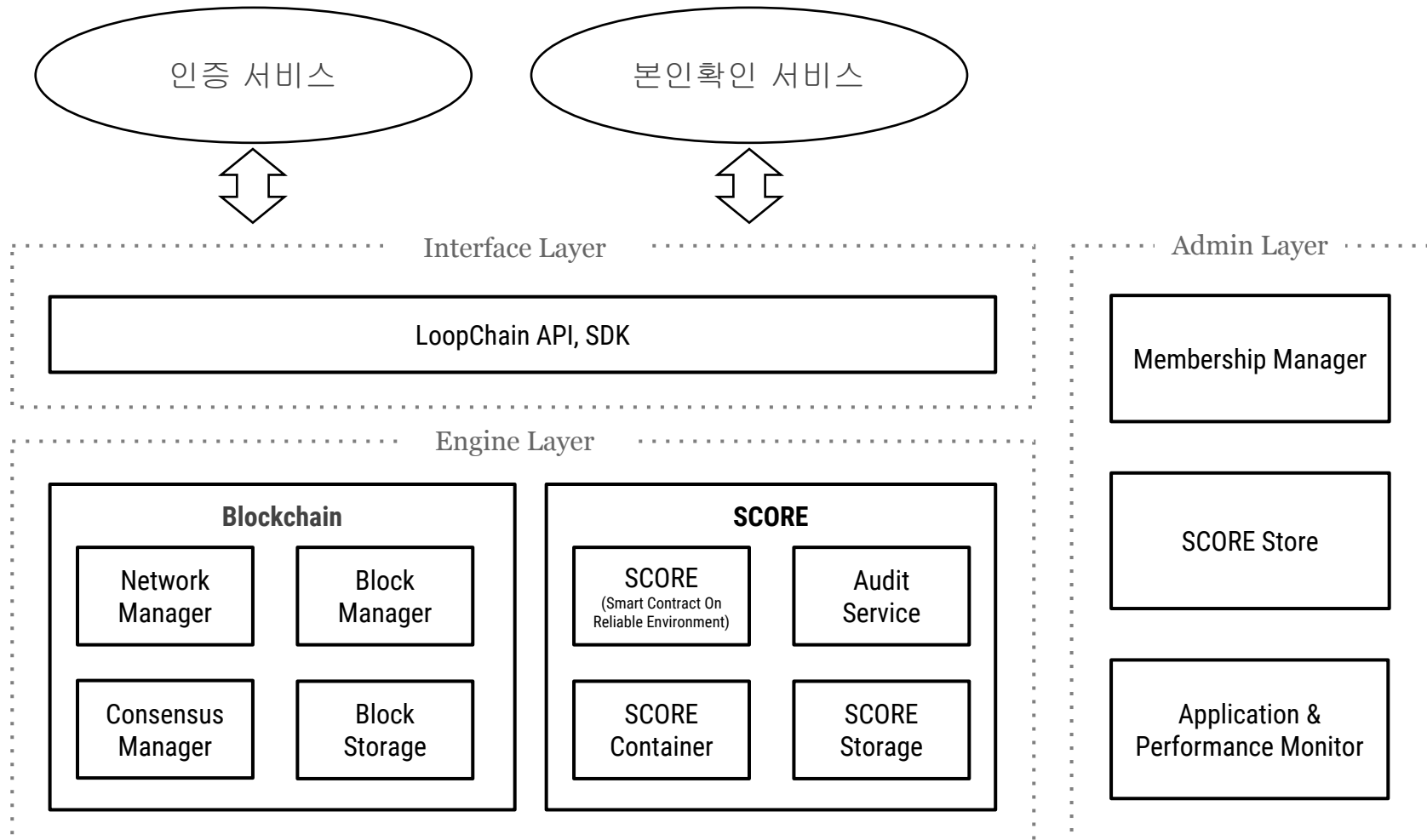


Scalability

대규모 거래 대응 및 외부 블록체인과 연동 지원

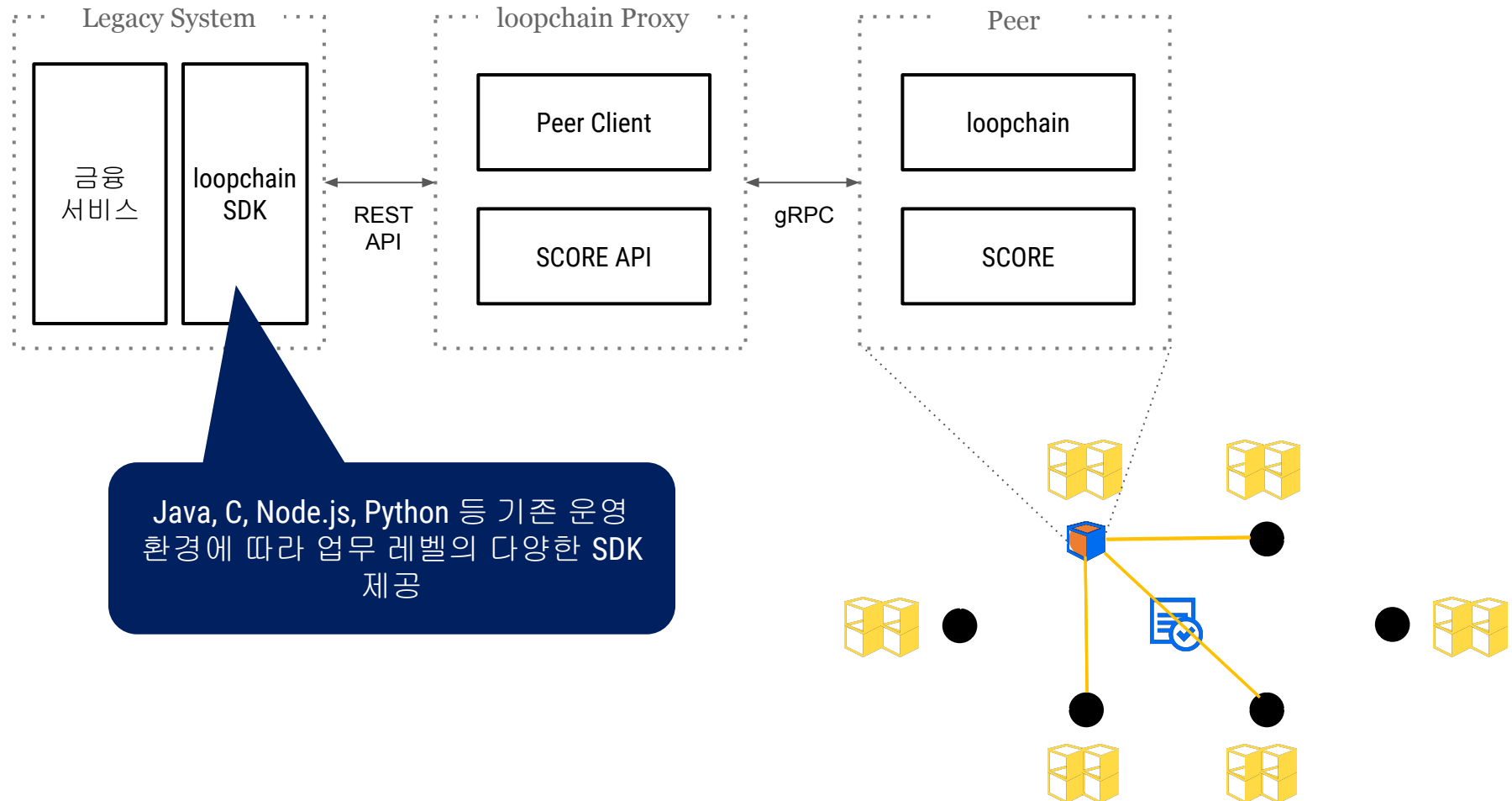
loopchain 구조도

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



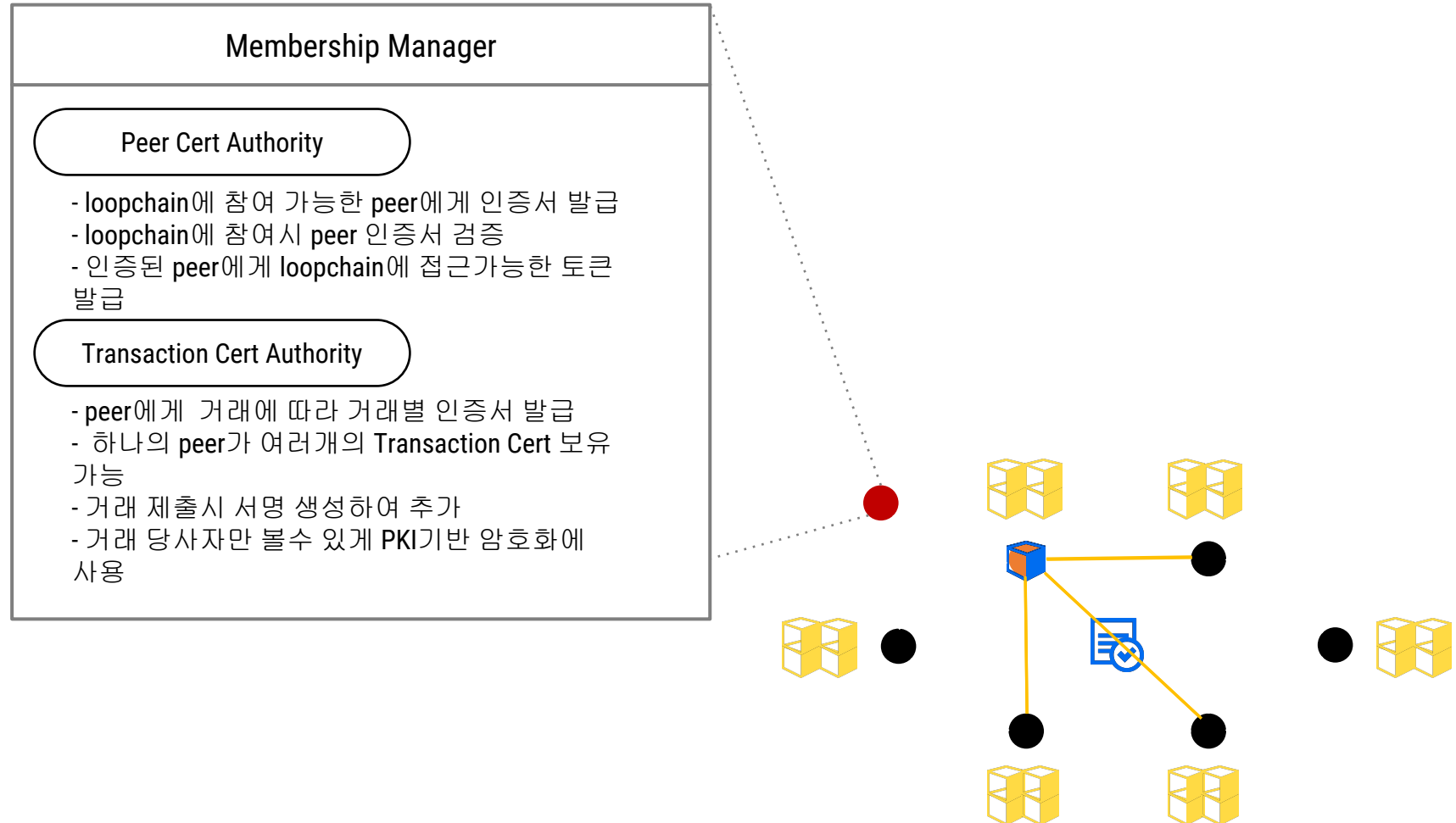
loopchain과 legacy 연동

loopchain proxy를 제공하여 블록체인 peer에 REST API로 접근이 가능하며 이를 legacy 환경 및 업무에 따라 간편하게 사용할 수 있도록 wrapping한 loopchain SDK를 함께 제공하여 API 호출만으로 업무 개발 가능



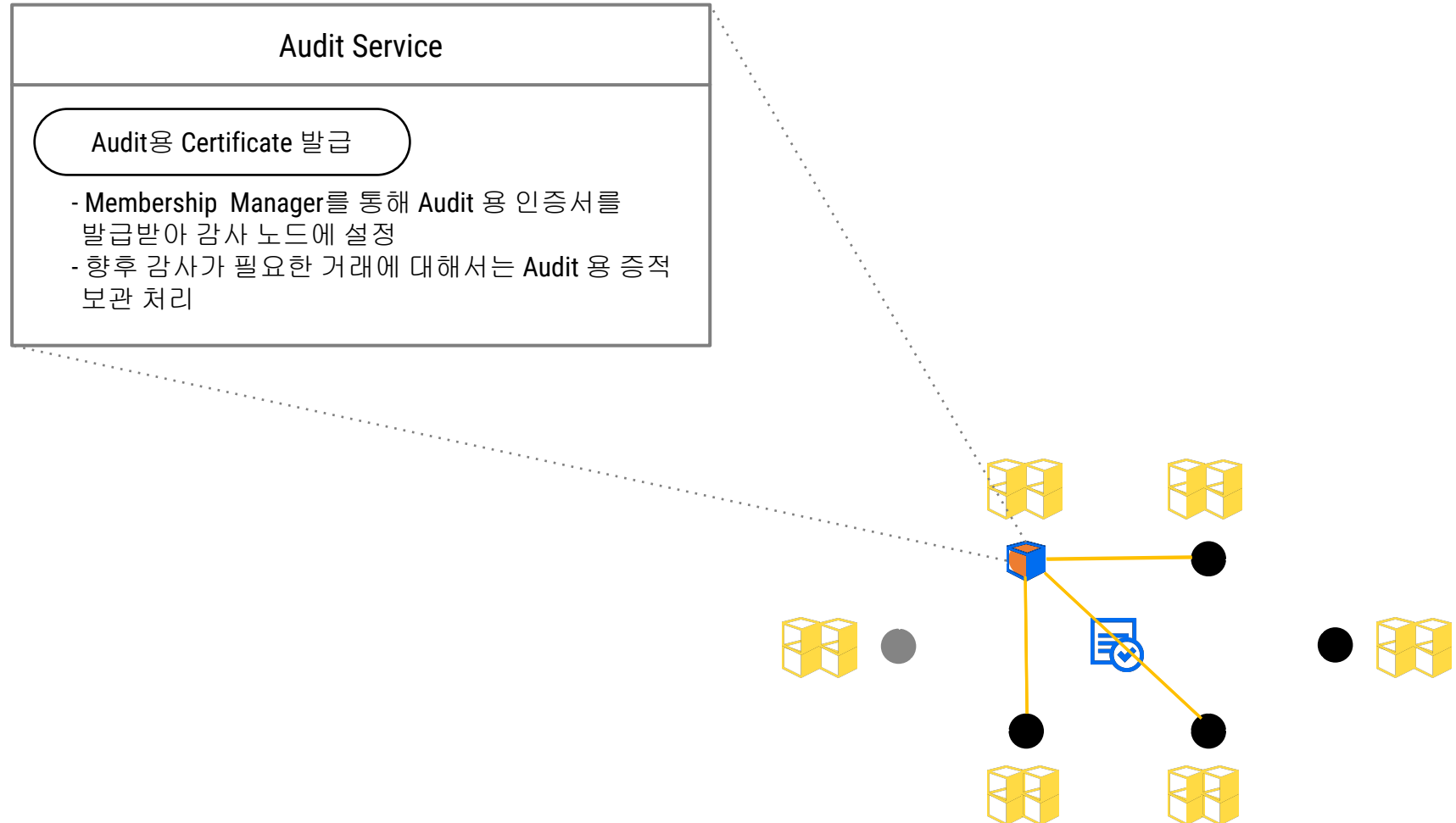
Private Channel

PKI 기반 참여 노드 및 거래 노드를 관리하여 인증된 노드만 블록체인에 참여할 수 있도록 하며 거래 내역에 대한 암호화를 제공하여 거래 내역을 보호



Tiered System

거래 노드 및 감사 노드를 분리하는 등 블록체인에 참여하는 노드에 차등 권한을 설정하여 다양한 업무 및 Compliance에 대응



Performance

PBFT를 개량하여 Private 블록체인에 최적화된 빠르고 효과적인 합의 알고리즘 구현

구현 목표

- 외부 공격에 의한 점령이나 시스템 일시 작동 정지의 가능성 고려
- 중앙기관 없이 참여기관끼리 합의(Consensus) 도출

PBFT

Practical Byzantine Fault Tolerance

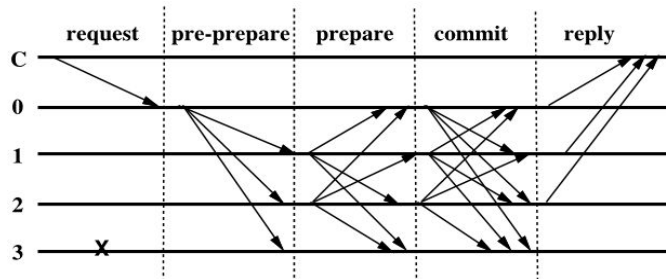
- 세 단계로 상태 구분
- 메시지 릴레이 프로세스를 통해
"Pre-Prepare", "Prepare", "Commit" 순으로
상태 변경

개선·최적
화

FBFT

Fast Byzantine Fault Tolerance

- Block Generator가 Broadcast하는 노드 수
제한
(다른 노드는 투표만 참여)
- 파이프라인 처리 기반 합의 단계 축소
- 노드 그룹핑 기반 투표권 관리

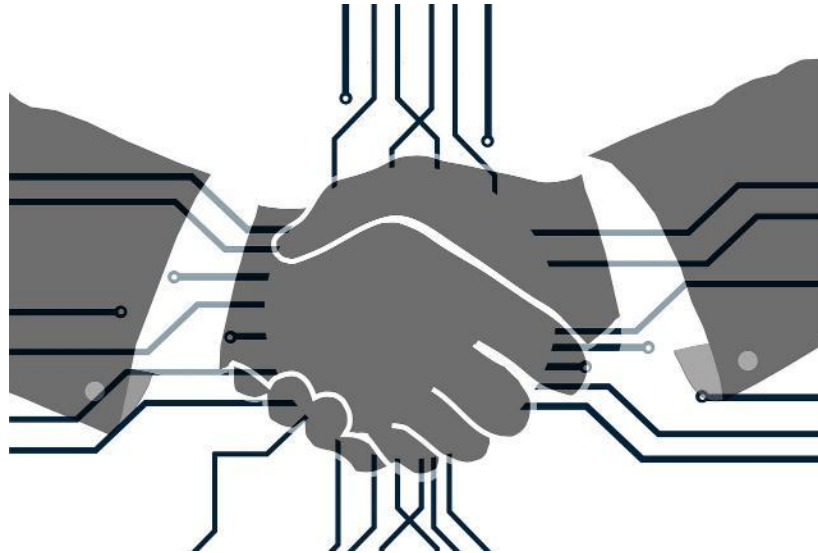


블록 생성주기 단축

1초 또는 더 짧은 주기로 블록 생성하며,
빠른 시간내에 모든 트랜잭션 전체 네트워크에 동기화

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 수 있는 중개자의 필요성을 최소화



Smart Contract on Blockchain

블록체인을 단순한 분산 원장이 아닌 어플리케이션 서버로 확장하여 다양한 거래 서비스를 가능하게 함

- 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

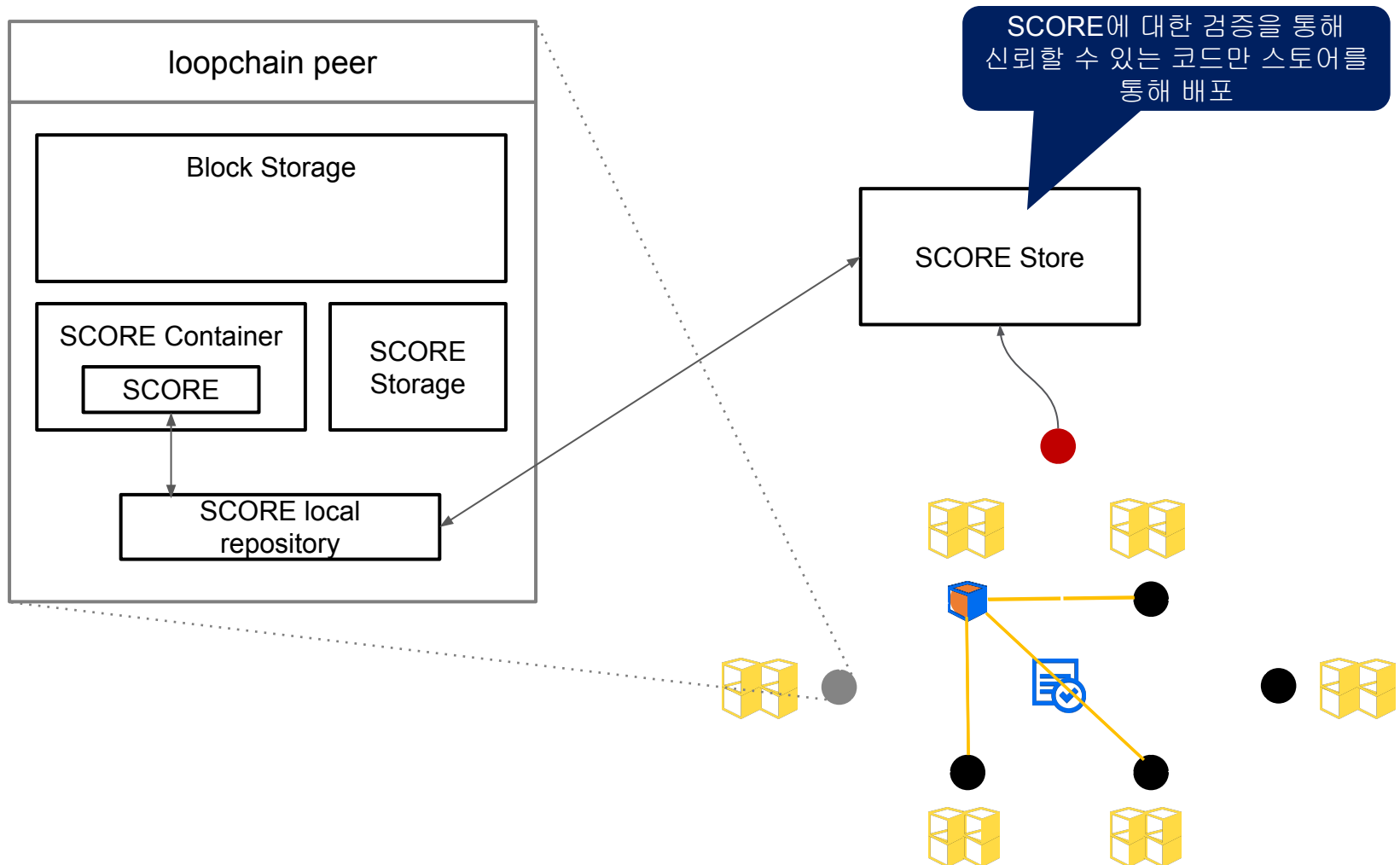
- Ethereum Smart Contract

- 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

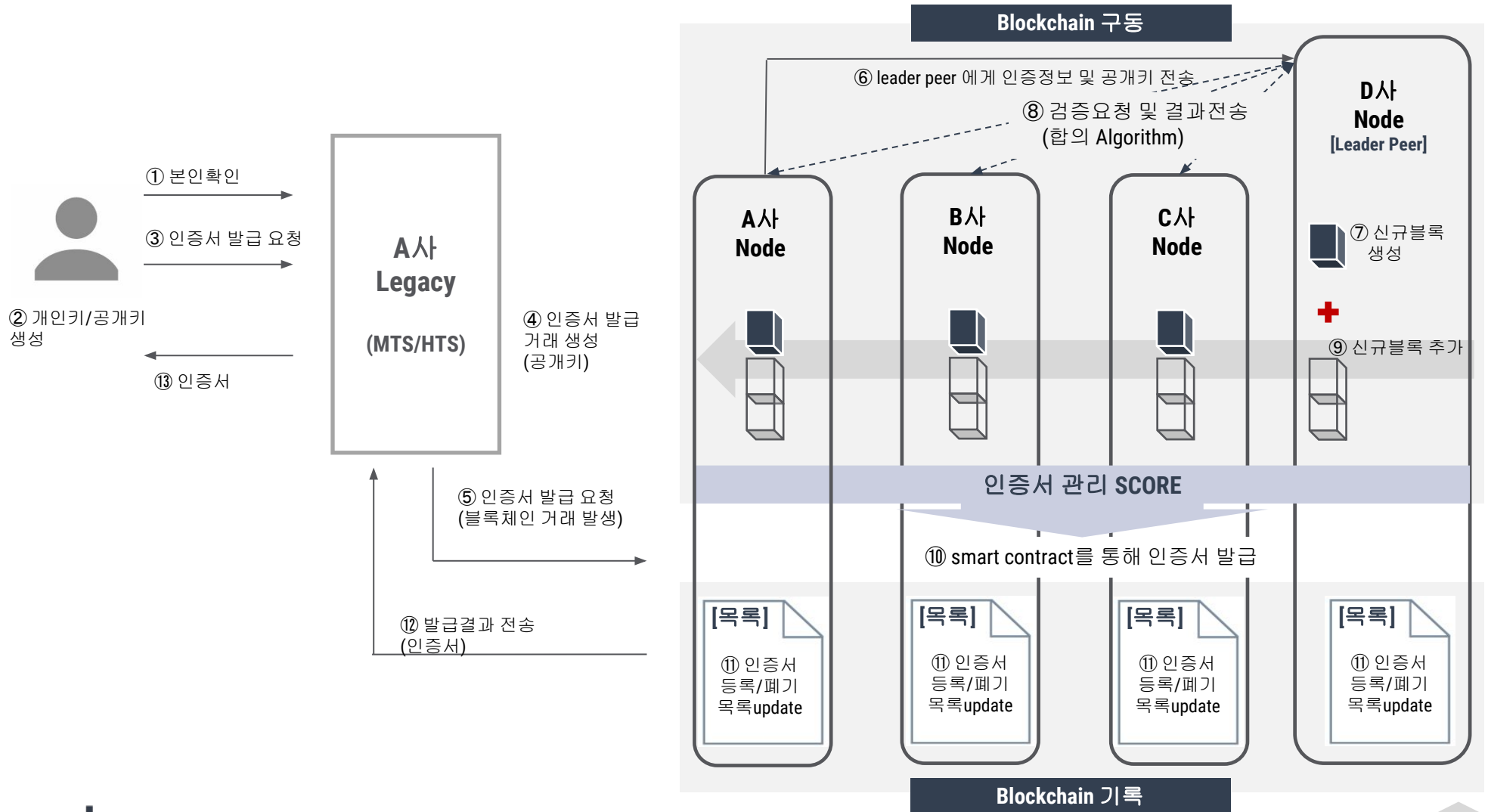
SCORE (Smart Contract on Reliable Environment)

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



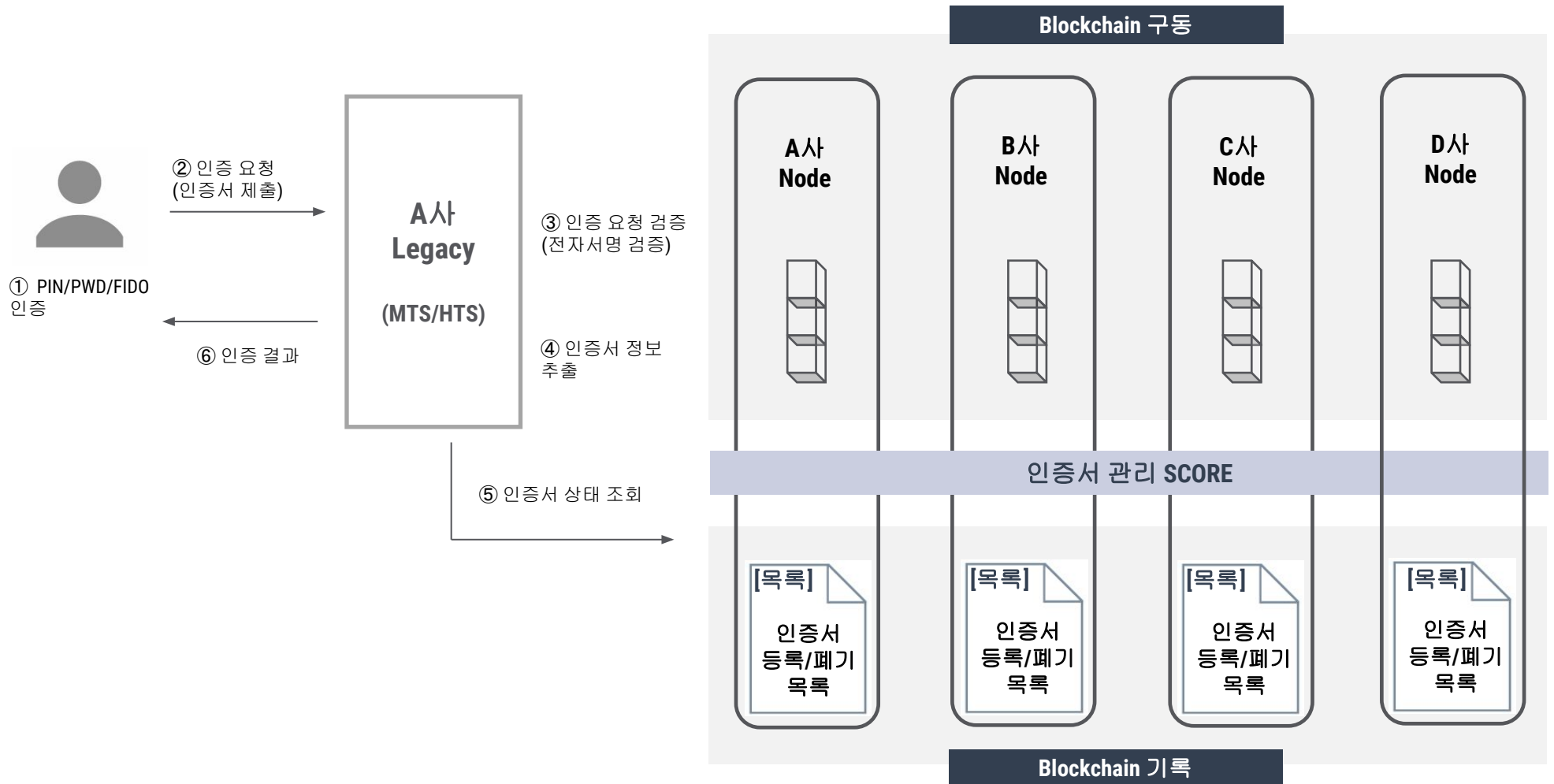
월 만든건가요?: 블록체인 기반 인증서 발급

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



월 만든건가요?: 블록체인 기반 인증서 유효성 확인

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



Github: <https://github.com/theloopkr/loopchain>

proxy_rest_api.md	Initial commit.	3 months a
pyvenv.cfg	Initial commit.	3 months a
radiostation.py	make more stable when load test.	23 days a
radiostation_proxy_restful_api.md	Initial commit.	3 months a
requirements.txt	make more stable when load test.	23 days a
rest_server.py	Initial commit.	3 months a
run_test.sh	Initial commit.	3 months a
setup.sh	Initial commit.	3 months a

README.md

loopchain

What is loopchain?

loopchain is a high-performance blockchain that can support real-time transactions based on efficient smart contract system.

loopChain

Features



01 / SCORE



02 / LFT Algorithm



03 / Tiered System



04 / Modular Architecture



Thank you

the**loop**

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

