

하이퍼레저 패브릭 구조 및 주요 구축사례

February 27th, 2018

Contents

1. 하이퍼레저 패브릭 소개

2. 주요 구축사례 및 시사점

하이퍼레저 프로젝트 현황



Infrastructure Technical, Legal, Marketing, Organizational



Ecosystems that accelerate open development and commercial adoption



Frameworks

Meaningfully differentiated approaches to business blockchain frameworks developed by a growing community of communities from the entire industry



Modules

Typically built for one framework, and through common license and community of communities approach, ported to other frameworks



비즈니스를 위한 블록체인의 4가지 기술요소

1

비즈니스
네트워크내에 모든
거래가 기록되고
공유됨

Shared
ledger
(공유 원장)



2

비즈니스 규칙 및
로직은 계약에
함축되어 트랜잭션
수행시 실행됨

Smart
contract
(스마트계약)



원장은 공유되지만,
참여자의 개인정보는
암호화 기술을
통해서 보호되어야
함

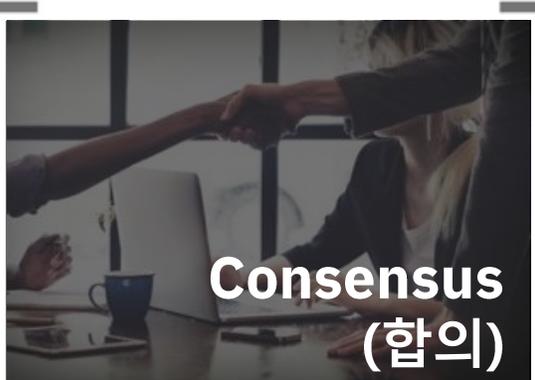
Privacy & Security
(프라이버시 및 보안)



4

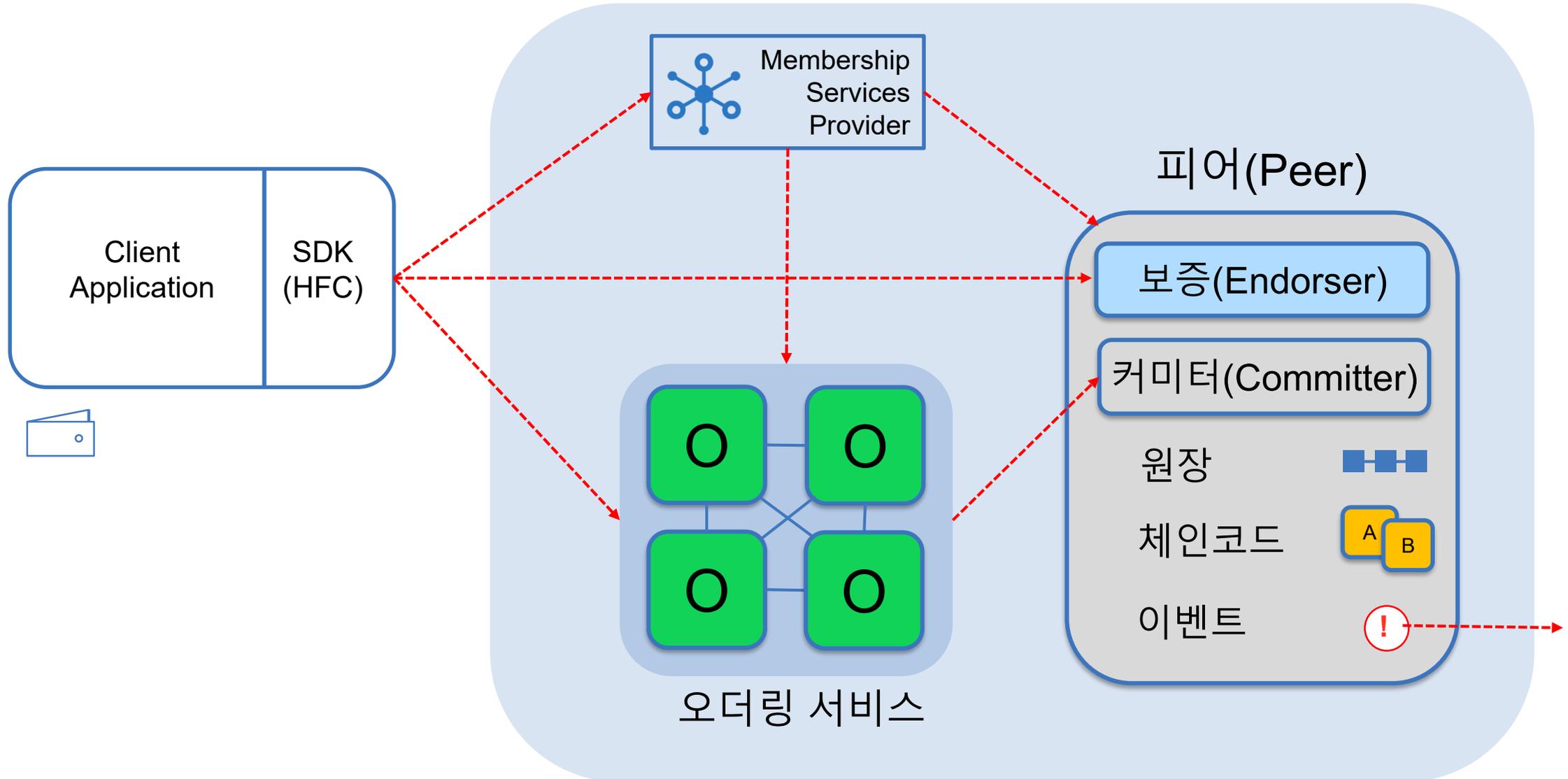
검증된 트랜잭션에
대한 네트워크에
참여한 참여자의
동의를 필요함

Consensus
(합의)

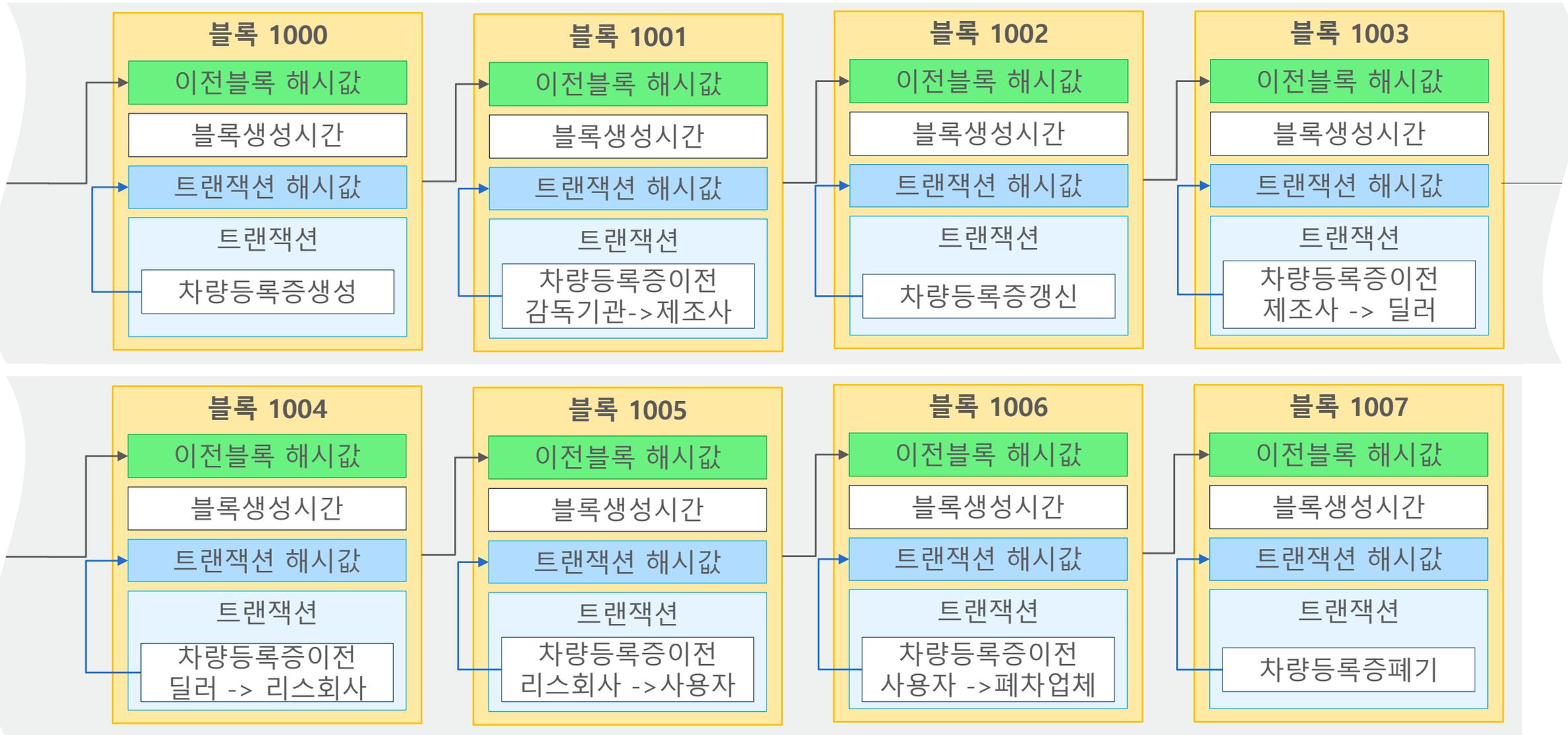


3

Fabric V1.0 아키텍처

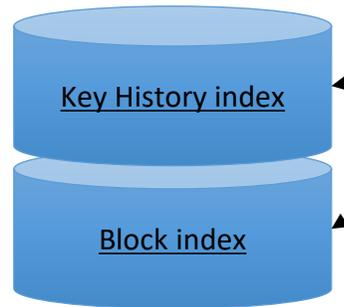


1 분산원장 > 블록체인 구조



블록 데이터 관리 (파일 시스템)

- 트랜잭션 및 RW 세트의 기록 (인증 정보 등록)
- 파일에 추가되어 저장되는 구조
- 인덱스에 의한 쿼리 지원
 - ✓ 블록 번호나 블록 해시 값에 의한 블록 검색
 - ✓ 블록 번호의 범위 지정에 의한 쿼리 (시작 블록 No ~ 종료 블록 No.)
 - ✓ txId 트랜잭션 조회



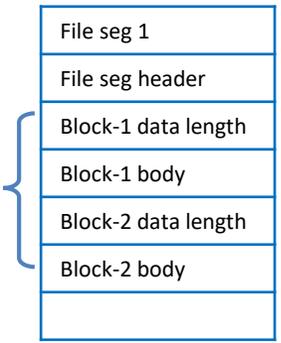
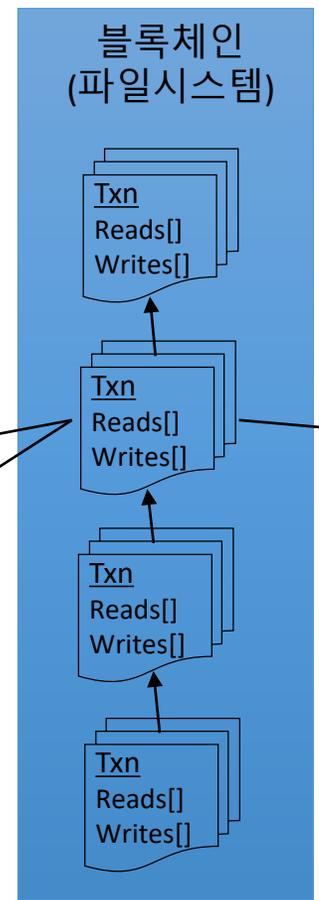
Indexes point to block storage location

blockNum → block file + offset

blockHash → block file + offset

txId → block file + offset

blockNum:txNum → block file + offset



스테이트 데이터베이스(State DB)

- 트랜잭션 실행 결과의 스냅 샷을 기록 (해시된 퍼블릭키, 해시된 주민등록번호)
- 기본적으로 Key-Value Store (LevelDB)
- 기본 동작 : PutState, DeleteState, GetState
- 플러거블(pluggable) 형태로 CouchDB 지원

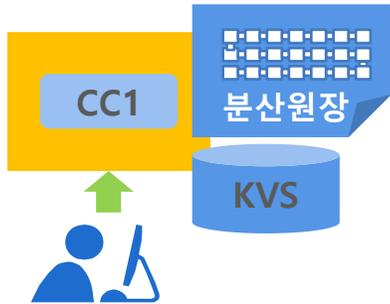


◆ 주요 체인코드 관련 처리 (가상머신에서 수행)



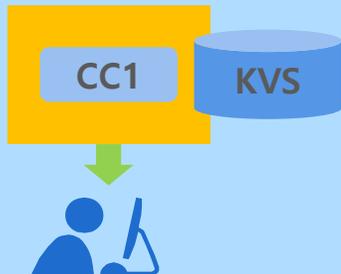
배포(Deploy)

- ✓소스코드에 따라 체인코드를 등록
- ✓원장에 기록됨(새로 배치했다는 정보가 기록됨)



호출(Invoke)

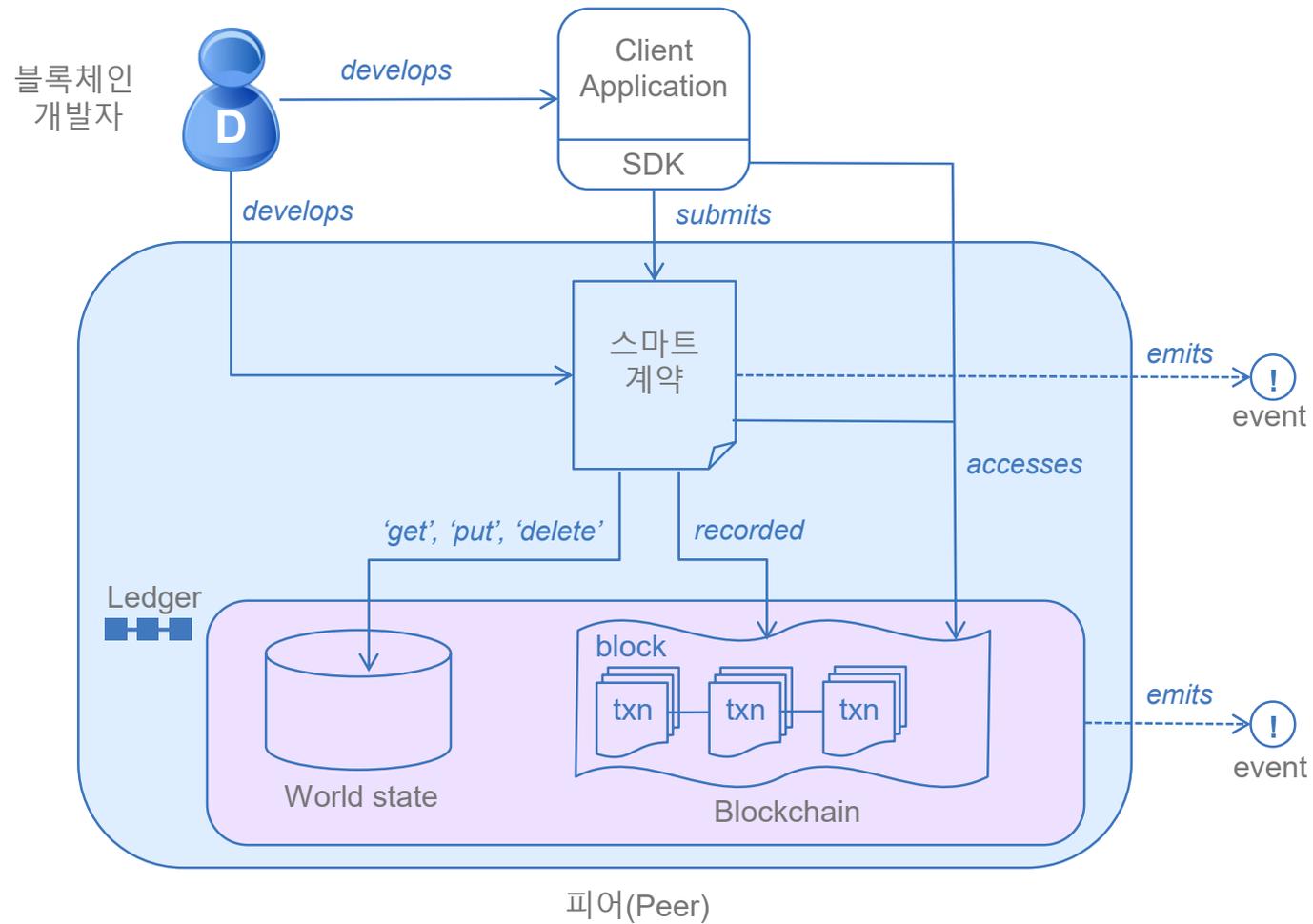
- ✓체인코드를 실행함
- ✓KVS에 데이터를 읽고 저장함
- ✓원장에 기록됨



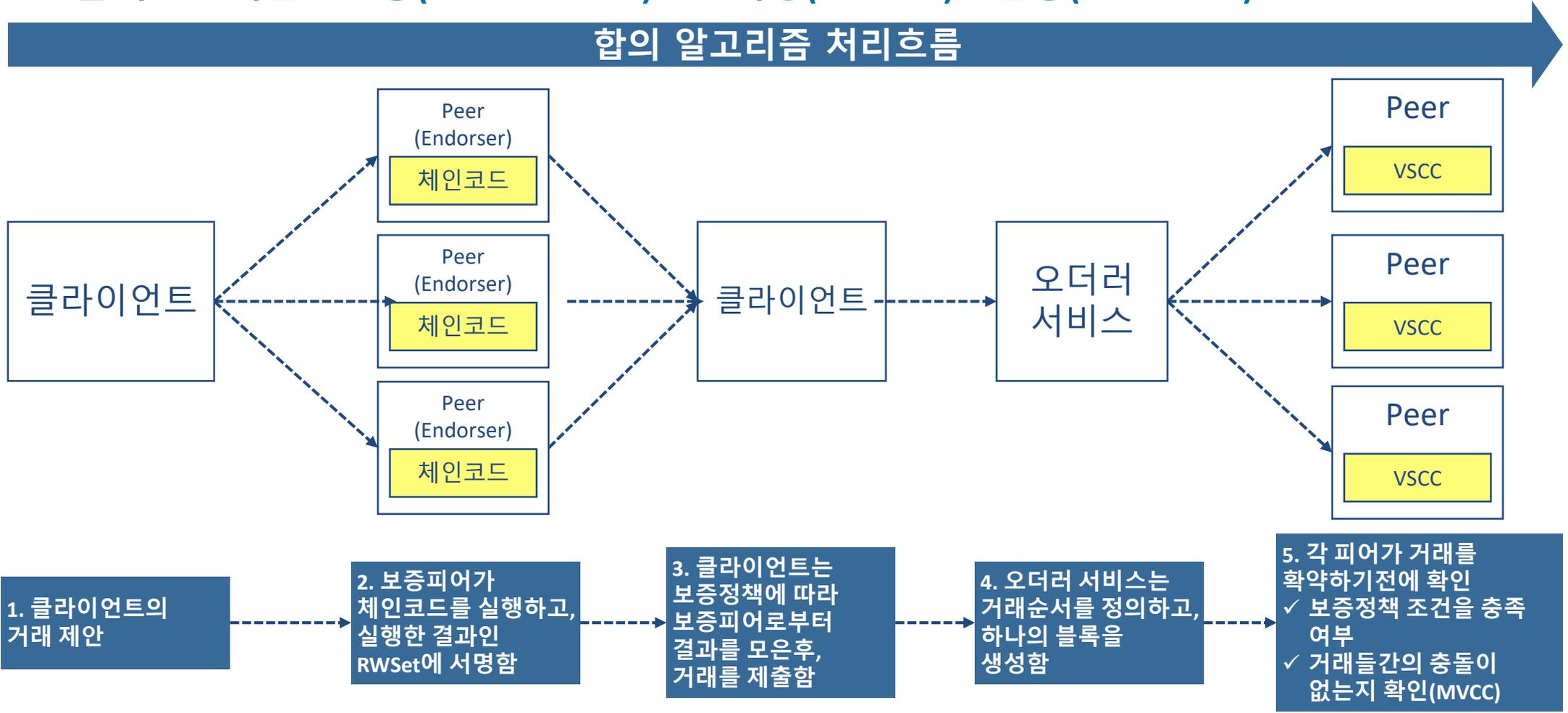
조회(Query)

- ✓체인코드에 데이터 조회함
- ✓KVS에서 데이터 읽기만 수행함
- ✓원장에 기록하지 않음

2 스마트계약 > 어플리케이션과 원장과의 구조



합의알고리즘 = 보증(Endorsement) + 오더링(Orderer) + 검증(Validation)



신원 관리(Identity)

- 업무 사용을 위해서는 참가자의 신원 확인이 필요
 - ✓ 책임 스푸핑(Spoofing) 방지
- 참가자의 신원인증 (참가자의 정체성과 특성의 확인)

트랜잭션의 기밀성(Confidentiality)

- 트랜잭션이 암호화되어 일반 사용자에게 보이지 않도록 함

재생(Replay) 공격 대책

- 과거의 트랜잭션을 복사하여 재전송하는 공격을 방지함

개인정보 보호

- 트랜잭션의 발행자의 익명화
- 동일한 사용자가 발행한 여러 트랜잭션들은 연관성이 없도록 함

액세스 제어

- 스마트계약을 실행할 수 있는 사람을 제한 (초기화, 함수 실행, 데이터 참조 등)

PKI 인증서와 전자서명

- 사용자의 신원을 확인함
- 개별 트랜잭션은 익명의 인증서를 통해 신원을 숨긴 채 인증 할 수 있음

IBM의 연구보고에 따르면, 기업용 블록체인은 허가형 블록체인 (Permissioned Blockchain)이 유일한 방법이라는 결론

Contents

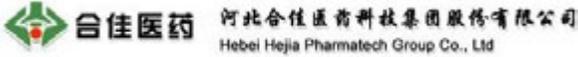
1. 하이퍼레저 패브릭 소개

2. 주요 구축사례 및 시사점

패브릭 기반의 구축사례(1/3)

<p>FX Netting</p> 	<p>Settlements through digital currency</p> 	<p>Diamond Provenance</p> 	<p>Identity management</p> 
<p>Credit Defaults Swaps</p> 	<p>Trade Finance</p> 	<p>Channel Financing</p> 	<p>Low liquidity securities trading and settlement</p> 
<p>Bike blockchain</p> 	<p>Reward points management</p> 	<p>Food Safety</p> 	<p>Contract Management</p> 
<p>Global Trade Digitization</p> 	<p>Trade Logistics</p> 	<p>Health Data Exchange</p> 	<p>환율고시 및 외화송금</p> 

패브릭 기반의 구축사례(2/3)

<p>Private Equity</p> 	<p>Supply chain finance</p> 	<p>Bond Trading</p> 	<p>Asset custody system</p> 
<p>Finance, real estate and asset custody</p> 	<p>Managing customer's digital identities</p> 	<p>Commodity trade finance for US crude oil transactions</p> 	<p>Supply chain financial services for pharmaceutical procurement</p> 
<p>Corporation identity management</p> 	<p>Cotton trading consortium</p> 	<p>Property portfolio revaluation</p> 	<p>Logistics / Supply chain</p> 
<p>Digital trade finance instrument</p> 	<p>Know Your Customer</p> 	<p>Blockchain experiment</p> 	<p>Loyalty and Rewards Platform</p> 

패브릭 기반의 구축사례(3/3)

<p>Truck-Tracking Solution</p> <p>AOS</p>	<p>Smart Insurance Contract</p> 	<p>Securities Lending</p> <p>Santiago Exchange</p>	<p>Customer Identification with Watson</p> <p>Signzy Technologies</p>
<p>Flexible Power Grid management in Netherlands & Germany</p> 	<p>Carbon Credit Management Platform</p> 	<p>Order, Logistic & Payment (OLP) platform</p> <p>INVICTUS (Singapore Start-up)</p>	<p>Trade Finance Platform</p> <p>Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Societe Generale, Unicredit</p>
<p>Financial Platform for Asian Market</p> <p>AEON Financial Services</p>	<p>Bank guarantees</p> <p>ANZ, Westpac & Scentre</p>	<p>Trade finance with Watson AI</p> 	<p>Letter of guarantee service</p> <p>KBank (Kasikornbank)</p>
<p>Store Academic Records</p> <p>SONY</p>	<p>Car Secure Payments "On The Go"</p> 	<p>Bancassurannce</p> 	

스마트계약을 활용한 채널파인낸싱 업무 혁신

IGF(IBM Global Financing) 업무는 연간 25,000 여건의 분쟁을 해결하기 위해 블록체인 기반으로 구축하여 분쟁시간 단축 및 분쟁건수 감소

TODAY



전세계 IGF 상태			
4000+ 파트너사와 공급사	2.9M 년간 청구서(Invoices)	\$44B 년간 운영 재정	
\$100M 언제나 묶여있는 자본	25,000 년간 분쟁	\$31K 분쟁이 생긴 청구서의 평균값	44 days 분쟁을 해결하는데 걸린 시간의 평균

분쟁원인

- 부품 수량 혹은 박스 수량 부족
- 배송 증명
- 가격/할인 금액 부정확
- 세금 부정확
- PO number 부재/기일초과/취소

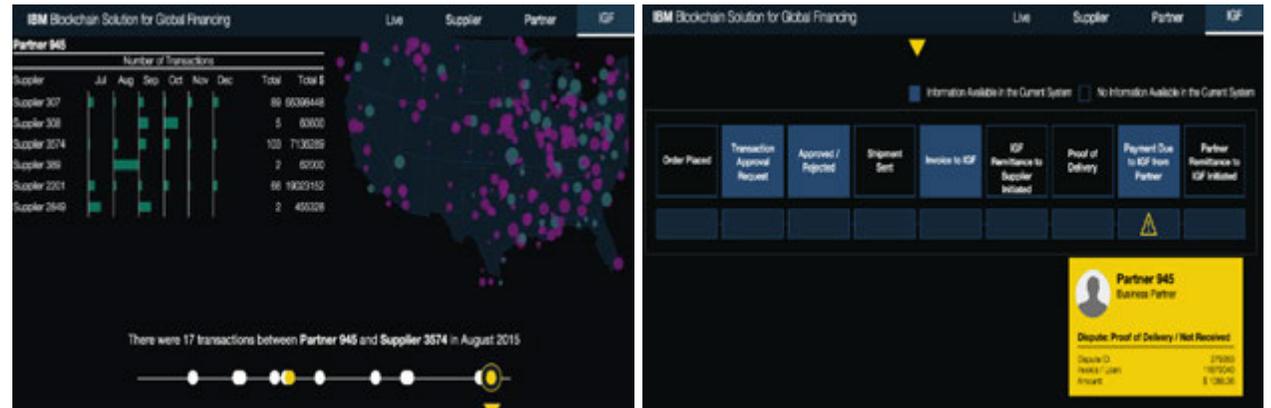
TOMORROW

What

- Blockchain을 통하여 안전하고 투명한 방식으로 데이터를 공유함으로써 상업 금융 비즈니스의 효율성을 향상시킴.

Benefits

- 분쟁 감소 및 신속한 결제
- 분쟁 해결 시간 단축 : 40일 이상에서 10일 미만으로
- 향상된 자본 효율성; 자유로운 자본 흐름



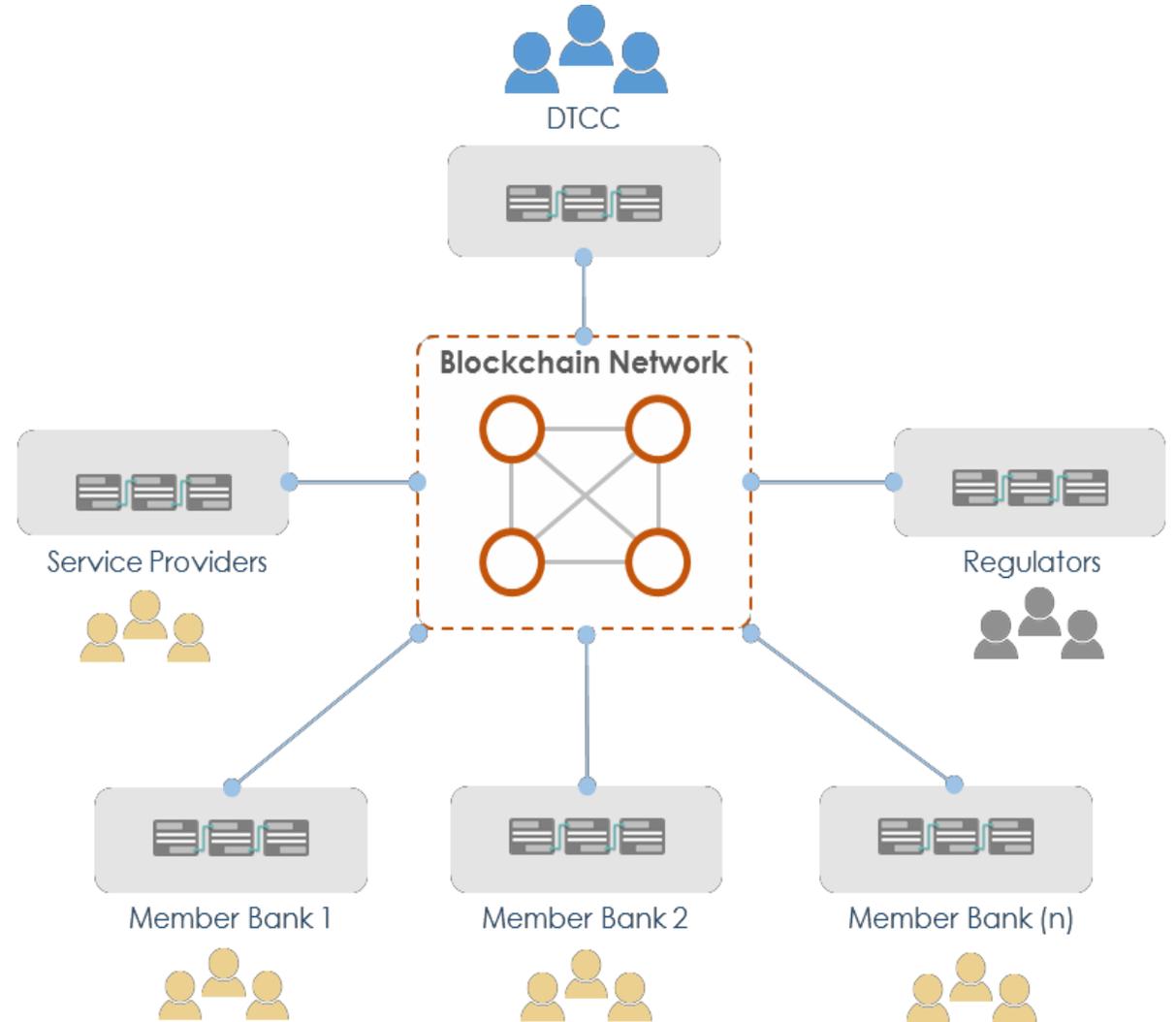
DTCC는

- 세계 자본시장의 후선업무(Post-Trade)시장 인프라를 지원
- 현재 11조 달러 이상의 **신용파생상품**에 대한 거래기록보관, 생명주기 이벤트 및 지불 관리를 자동화하는 TIW(Trade Information Warehouse)서비스를 제공
- 후선업무처리를 위한 **파생상품 분산원장(DDL)**을 지원하는 **TIW 서비스 재구축**

기대효과

분산원장 기술 적용을 통한 업계표준화 주도

업계 전반의 파생상품 처리비용을 더욱 간소화 및 자동화



중소기업을 위한 무역금융 플랫폼

DTC(Digital Trade Chain)이란?

- 유럽내 중소기업(SMEs)들을 위한 무역금융거래를 지원하기 위한 플랫폼

참여은행(현재 8개 은행)

- Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Societe Generale, Unicredit, Santander

기대효과

모바일폰을 통한 접근의 용이성

트랜잭션에 대한 통합된 뷰(View) 제공

거래에 대한 신뢰성을 높임

리스크 감소

The image shows the we.trade platform interface. At the top, a network diagram connects logos for Societe Generale, Natixis, UniCredit, HSBC, Rabobank, and KBC. Below this is the we.trade dashboard with a navigation bar (Dashboard, Trades, Create trade) and user profile. The dashboard features four key metrics: 14 New trade requests, 3 Amendments, 18 Awaiting shipment, and 5 Incoming payments. An 'Activities' section on the right lists recent transactions with timestamps and descriptions. A testimonial from Alenka H., Milano, is displayed on the left side of the dashboard.

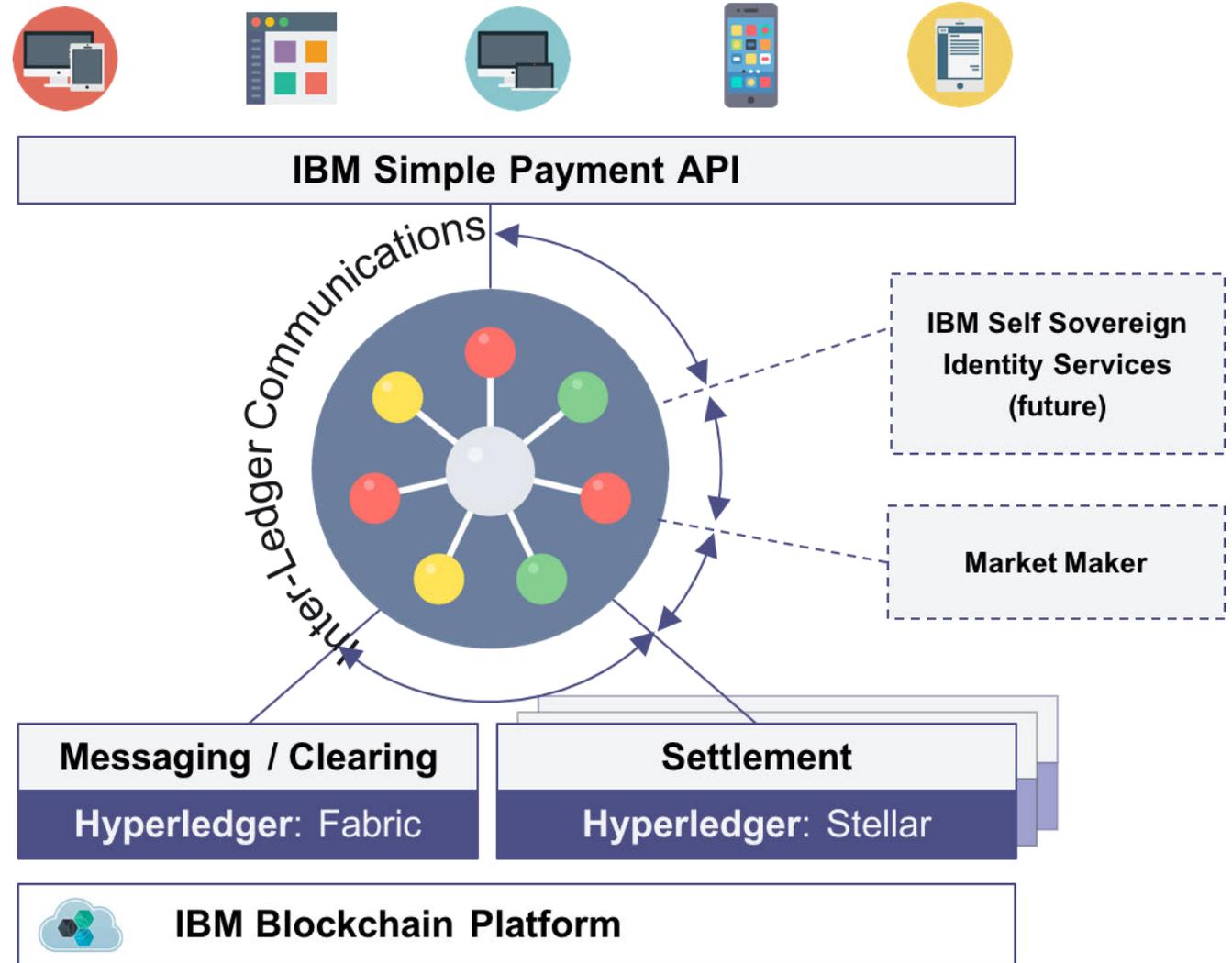
글로벌 페이먼트(Global Payment)

IUPS(IBM Universal Payment Solution)이란?

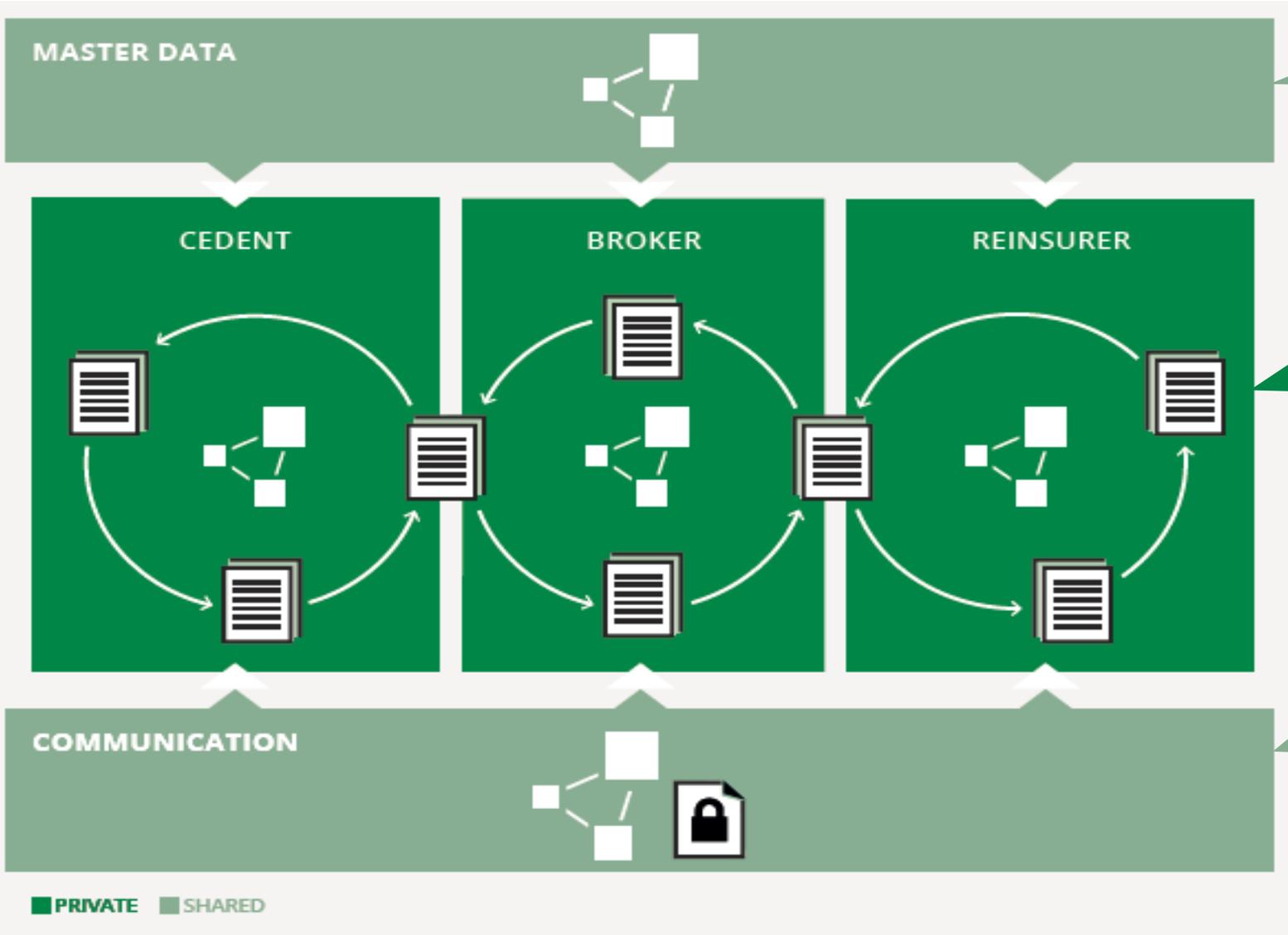
- ✓ 신흥국가간의 외환송금업무를 중계은행을 거치지 않고 중계 브릿지 역할로 디지털 자산을 활용한 청산/결제 네트워크
- ✓ 준실시간 청산/결제
- ✓ 2017년 4Q에 운영을 위한 파일럿 수행

참여 금융기관 및 솔루션 업체

- ✓ Banco Bilbao Vizcaya Argentaria,
- ✓ Bank Danamon Indonesia,
- ✓ Bank Mandiri,
- ✓ Bank Negara Indonesia,
- ✓ Bank Permata,
- ✓ Bank Rakyat Indonesia,
- ✓ Kasikornbank Thailand,
- ✓ Mizuho Financial Group,
- ✓ National Australia Bank,
- ✓ Rizal Commercial Banking Corp. (RCBC) Philippines,
- ✓ Sumitomo Mitsui Financial Group,
- ✓ TD Bank,
- ✓ Wizdraw (HK) of WorldCom Finance
- ✓ Stellar
- ✓ KlickEx Group



B3i (The Blockchain Insurance Industry Initiatives)



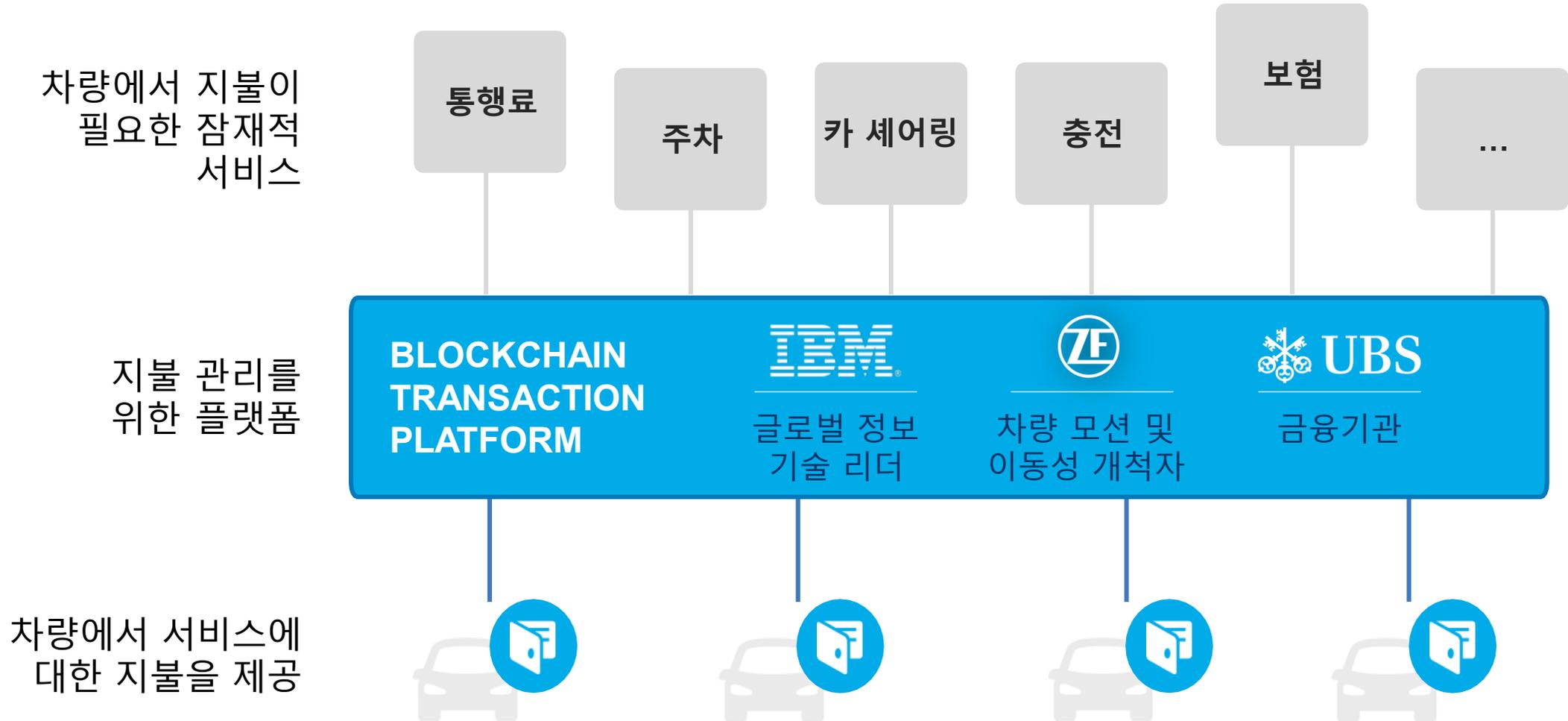
공개 회사 정보 및 공통 계약 조항을 포함하여 공통되고 합의된 마스터데이터

- ✓ 자체 계약 요소 및 데이터를 저장하는 사설원장(Privacy Ledger)
- ✓ 모든 조직은 또한 두 개의 공유 원장에 참여함

- ✓ 공유통신원장은 암호화되어 보호되며, 사설조직원장의 상태를 합의 하는데 사용된 통신정보를 저장함
- ✓ 거래당사자만이 통신내용과 대상을 볼수 있음

전기자동차의 전자결제 플랫폼

2017 프랑크푸르트쇼에서 ZF 와 UBS, IBM은 블록체인 기반의 전 세계 공용의 자동차 전자 결제 플랫폼 공동 개발하여 클라우드를 통해 제공



식품의 원산지 추적(미국)



복잡한 단계 (산지, 가공, 물류, 유통 등)

위생문제 추적 애로, 장기간 소요



Safety에 대한 소비자 신뢰 향상

(산지, 설비, 보관온도 등 이력 공유)

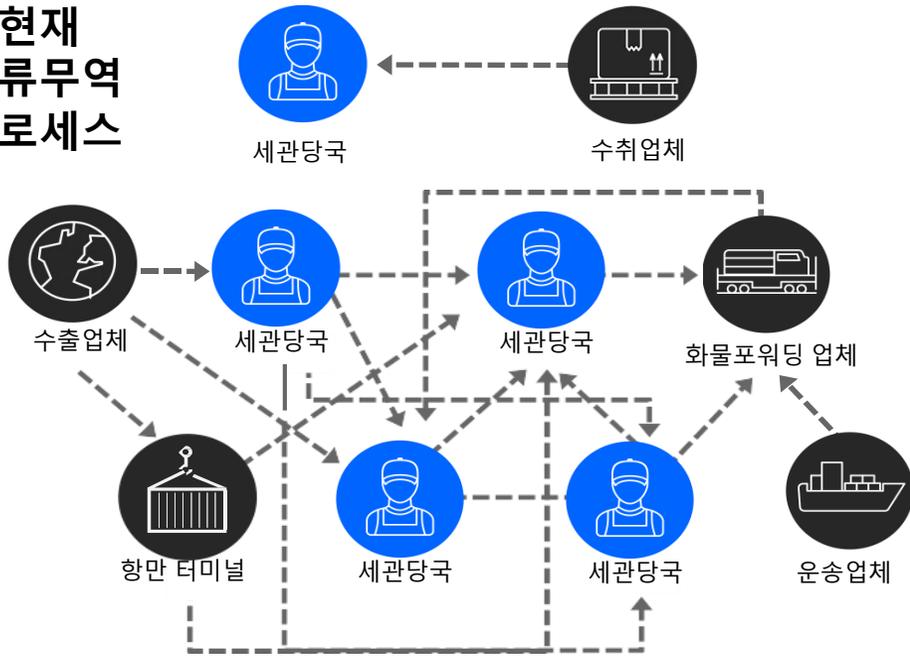
문제 발생시 즉시 추적

(2.3초 이내)



GTD(Global Trade Digitization) 플랫폼

현재 물류무역 프로세스



물류무역 공급망 관리를 위한 높은 비용

운임송장 수수료 및 할증료에 대한 신뢰 부족으로 인해 비용이 들고, 시간이 많이 소비되고 오류검증 단계가 필요

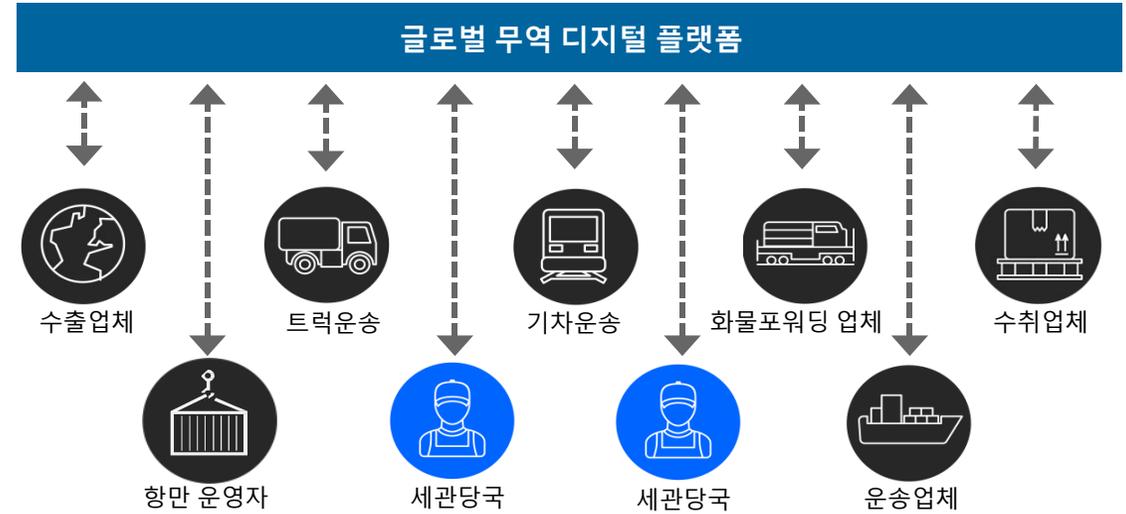
서비스 제공업체 및 물류업체의 통합을 위한 높은 IT 비용

국제무역을 위한 규제준수 비용이 높음

분실 및 잘못된 서류로 인한 국경간 지체

세관중개인 및 운송업체의 통관서비스의 높은 비용

블록체인 기술 적용



물류무역 공급망의 가시성 및 재고 예측가능성 확보

가시성 확보를 위한 수작업 프로세스 (여러 트랙 및 추적을 위한 대쉬보드 확인, 전화 및 이메일 제공업체) 를 제거함

화주는 효율적으로 수수료 및 할증료 확인

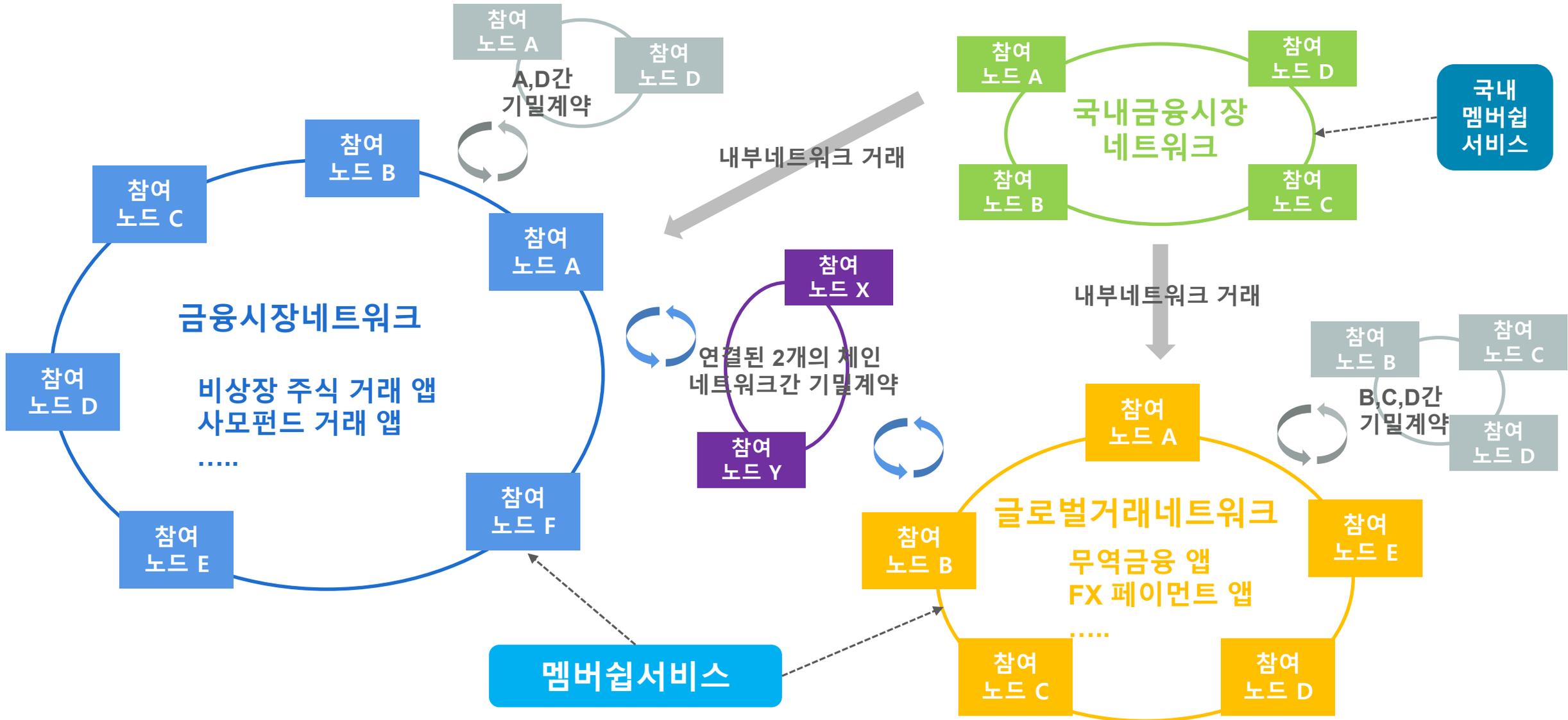
단일 및 표준 인터페이스 제공(운영비용 및 오류발생 줄임)

세관확인을 위한 물리적 서류양식 휴대 제거(문서처리비용 개선)

단순화된 프로세스 및 워크플로우 기반의 컴플라이언스 정책을 통해 비용감소

기
대
효
과

미래의 블록체인 네트워크





박 세 열
블록체인 기술리더/
금융총괄 아키텍트

Blockchain Technical Leader/
Client Technical Leader
S&D Architect Team
Technical Sales
Banking & Financial Markets



IBM Korea
Three IFC, 10 Gukjegeumyung-ro,
Yeongdeungpo-gu, Seoul, Korea

Mobile: +82-10-4995-7163
Phone: +82-2-3781-7163

E-mail: sypark@kr.ibm.com

