KSD 한국예탁결제원

최종보고

채권장외결제시스템 블록체인기술 적용 타당성 검토를 위한 컨설팅

2018.09.18

unipoint

KSD 한국예탁결제원

Contents

uniPoint

1. 사업개요

본사업의 개요는 다음과 같습니다.

사업명칭	『 채권장외결제시스템 블록체인기술 적용 타당성 검토를 위한 컨설팅 』 사업
발주기관	한국예탁결제원
사업수행	㈜유니포인트
사업기간	2018년 6월 20일 ~ 2018년 9월 19일 (3개월)
계약금액	******(원, VAT별도)
사업범위	채권장외결제시스템에 적합한 블록체인기술 확인 및 적용가능 모델 수립
	블록체인 모델의 타당성 및 가능성 확인
	모의테스트 결과 시연 및 블록체인 적용 보고서 작성

2. 블록체인 외부 환경 및 동향

1. 화폐 및 증권 등 자산의 디지털화 가속

- 현행 지폐·증권을 보완 및 대체하려는 암호화폐·토큰화증권 등 **블록체인 기반 자산 출현**

⇨ 블록체인상 **비트코인·채권(Bond-i)** 등 발행, 블록체인상 주식 보유자의 권리 인정(델러웨어주 등)

2. 일부 블록체인을 통한 CSD산업 재편 논의

- **일부 지주사 형태 증권거래소**는 블록체인 기반 예탁결제제도 변혁 가능성을 타진 (**호주, 싱가폴 등**)
- **신규 플랫폼 사업자는** 중앙집중형을 대체하는 분산형 CSD시스템 구축을 시도 중 (**호주 SETL**, 미국 T Zero 등)

3. 정부의 블록체인을 통한 금융혁신 추진

- **금융위**는 블록체인 공동인증 추진을 위하여 '금융권 **블록체인 공동컨소시엄 운영계획'('16.11월)**을 수립
- **과기부**는 국가차원의 블록체인 기술 조기 경쟁력 확보를 위하여 최근 '**블록체인 기술 발전전략'('18.6월)**을 수립

4. 블록체인 기술의 진화

- 지급수단 기능에서 다양한 거래분야로 적용되어 향후 **공공서비스·계약·증명 등 분야로 확장 예상**

⇨ 1세대(가상통화) ⇒ 2세대(스마트계약 , 분산앱) ⇒ 3세대(확장성, 상호운용성)

3. 사업목적

채권장외결제업무를 대상으로 **블록체인 기술 적용 타당성 검증**을 수행하였습니다.

자본시장의 다양한 부문에 변혁을 가져올 것으로 기대되는 블록체인 기술을 우리원 고유업무에 적용(PoC)해 보는 것이 어떨까?

채권장외결제

채권장외결제의 최종성 확보

한국예탁결제원의 채권장외결제시스템에 적합한 **블록체인기술** 및 **적용가능모델 확인**

적용가능성

블록체인 모델의 기술적 가능성 평가

시뮬레이션 실시를 통한 **블록체인 모델의 기술적 적용가능성** (안정성과 효율성 등) 평가

향후 발전 방안에 대한 비즈니스 모델링

향후 블록체인 환경에 **업무적용**

블록체인 기반 기술 적용 타당성 검토 컨설팅

향후 블록체인 적용 모델 수립

블록체인 실증환경 구축을 통한 기능성,안정성,보안성,효율성 등 적용가능성 확인

4. 사업범위

본 사업의 **범위**는 다음과 같습니다.

01

- 현행 업무절차와 원장 구성을 기반으로 블록체인 사상에 적합한 비즈니스 모델 수립
  - 대상업무: 채권장외결제 (**매매자료제출~결제처리 전 과정**)
- 블록체인 플랫폼 기술적인 특징 및 채권기관투자자결제 업무 특성을 고려하여 블록체인 적용 모델 수립

02

- 오픈소스 기반의 **폐쇄형 블록체인 플랫폼 환경**으로 기술검증 시스템 구축
- 수립된 모델을 수행사 내부에 블록체인 가상네트워크 구성
- 블록체인 노드 관리, 멤버쉽 관리, 모니터링 등 관리기능 구성

03

- 실제 데이터를 이용하여 실무처리상 발생될 수 있는 **다양한 시나리오를 고려한 시뮬레이션 수행**
- 최종 기술검증 결과에 대한 시연
- 블록체인 적용 보고서 작성

04

- 블록체인 기술 내재화를 위한 최적의 전략과 수행방안을 제시하고 관련 기술지원
- 프로젝트 수행 단계 별 담당 직원에게 교육 실시

5. 프로젝트 방법론

업무분석,모델수립,환경구성 및 시뮬레이션을 통한 타당성 검증을 약 3개월(13주)간 진행하였습니다

	Phase.1	Phase.2	Phase.3
	착수 및 모델수립 (1.0M)	블록체인 환경구성 및 타당성 검증 (1.8M)	결과보고 시연(0.2M)
주요 Task 및 Activity	**Task** 1 블록체인 이해 • 블록체인 개념 정립을 위한 교육 진행 2 분석 및 모델수립 • 채권장외결제 업무분석 • 비즈니스 검토 및 심화토론 • 비즈니스 모델 구체화 • 구축범위 구체화	**Task** 3 솔루션 디자인 4 블록체인 환경 구성 5 블록체인 솔루션 개발 6 시뮬레이션 수행	**Activity** • 솔루션 다이어그램 • 키-밸류 스토어 디자인 • 아키텍처 다이어그램 • 어플리케이션 화면 디자인 • 소스코드 및 환경 파일 • 체인 코드 전개 • 블록체인 환경 설정 • 암호화 환경 구성 • 하이퍼레저 패브릭 V1.1 설치 • 체인코드(Chaincode) 및 키-밸류 스토어 개발 • 프로토타입 • 어플리케이션 화면 및 웹 어플리케이션 서버 • 시뮬레이션 시나리오 작성 • 시나리오별 실제데이터 수집(필요시 변환) • 시뮬레이션 결과 작성	7 모의테스트 및 결과보고
주요 역할	• 프로젝트 관리자(PM) • 블록체인 아키텍트	• 프로젝트 관리자(PM) • 블록체인 아키텍트	• 관리 화면 어플리케이션 및 API 개발 • 체인코드(Chaincode)/키-밸류 스토어 개발 • 블록체인 인프라환경 구축	

6. 수행조직

발주사 비즈니스/ IT 등 협업 조직의 지원을 통하여 사업을 원활히 수행하였습니다.

KSD 수행 조직

수행총괄
연구개발부
(신사업개발팀)

협업그룹
청산결제부
(채권결제팀)
IT서비스부
(결제서비스팀)

자문그룹
IT전략부
(IT혁신기술팀)
연구개발부
(조사연구센터)

- 블록체인 적용 업무 검토 및 모델수립(분석단계)
- 블록체인 적용 아키텍처 수립을 위한 협의(설계단계)
- 블록체인 적용 시뮬레이션 시연 검토(구현단계)
- 향후 우리원 블록체인 사업 추진 전략 방향 검토

유니포인트 수행 조직

P M
이** 부장

블록체인 개발
김** 부장

화면(웹) 개발
이** 차장

기획/디자인
김** 과장

- 블록체인 적용 업무 분석 및 설계
- 블록체인 개발, 응용기능 개발
- 블록체인 적용 타당성 컨설팅

KSD 한국예탁결제원

Contents

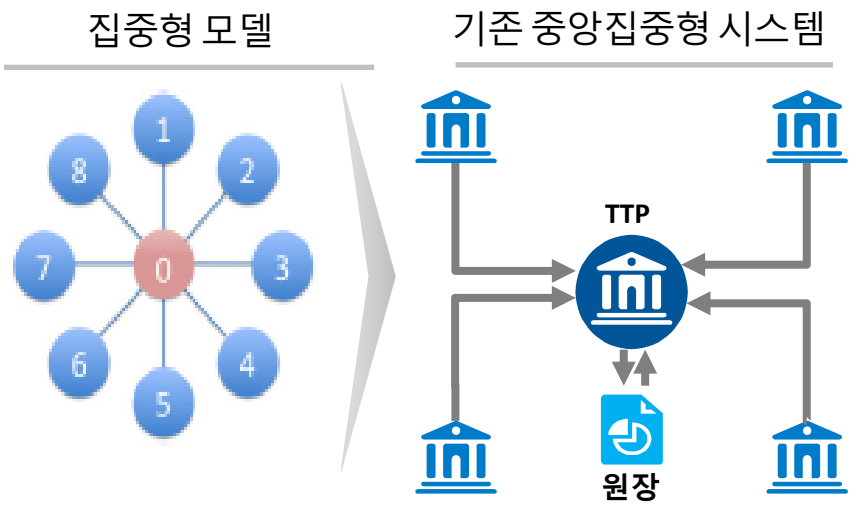
uniPoint

1. 블록체인 이해(1/2)

분산환경 네트워크 모델이 적용된 **공유원장** 기술입니다.

집중형(클라이언트-서버) 시스템

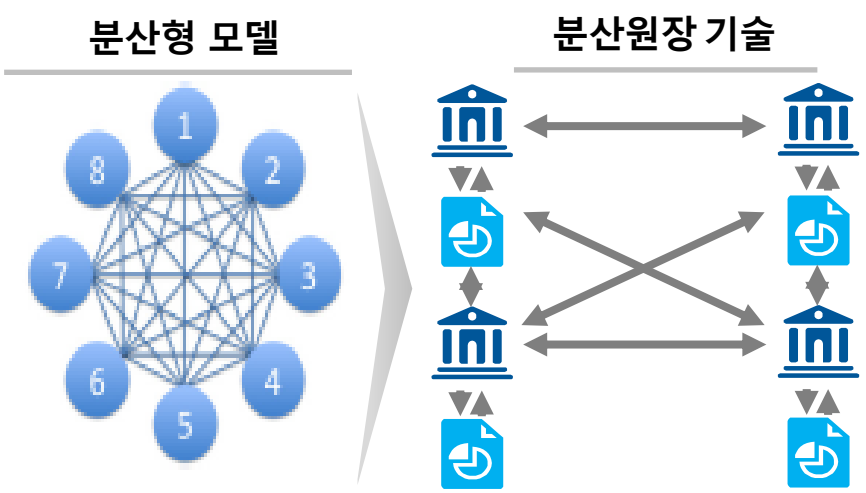
- 거래 장부를 **신뢰할 수 있는 제3의 기관(TTP-Trusted Third Party)**을 설립하고 해당 기관에 대한 신뢰를 바탕으로 **중앙집중형으로 관리**



- 기록 관리 권한과 책임이 특정 기관에 집중
- IT인프라 및 보안관련 대규모 인력·설비투자 필요
- 해당 기관의 신뢰 확보를 위한 규제·감독 강화

블록체인(분산형) 기반 시스템

- **모든 참여자가 거래내역이 기록된 장부 전체를 각각 보관하고 새로운 거래를 반영**하여 갱신(Update)하는 작업도 공동으로 수행

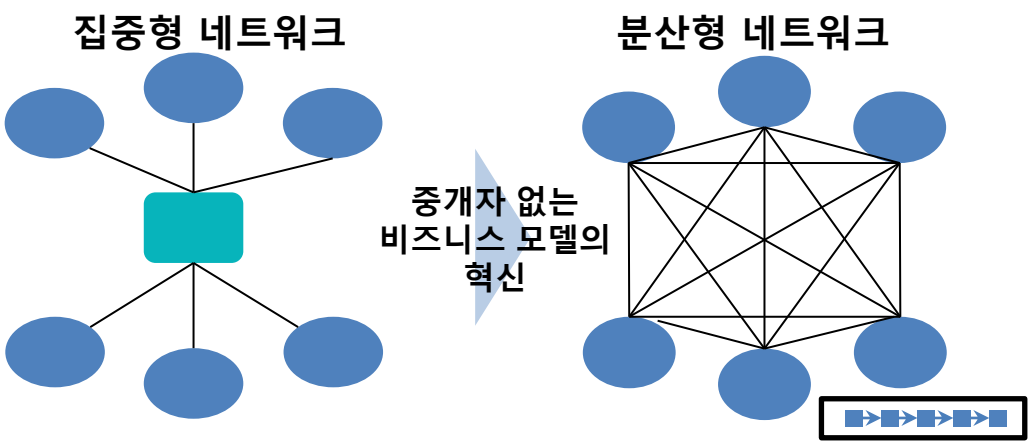


- 중앙집중적 생태계 및 서버 구축 불필요
- 거래기록 및 증명 방식의 근원적인 변화 필요
- 제3의 기관 없이 신뢰성 및 보안성 확보 가능

1. 블록체인 이해(2/2)

블록체인을 요약하면 다음과 같습니다.

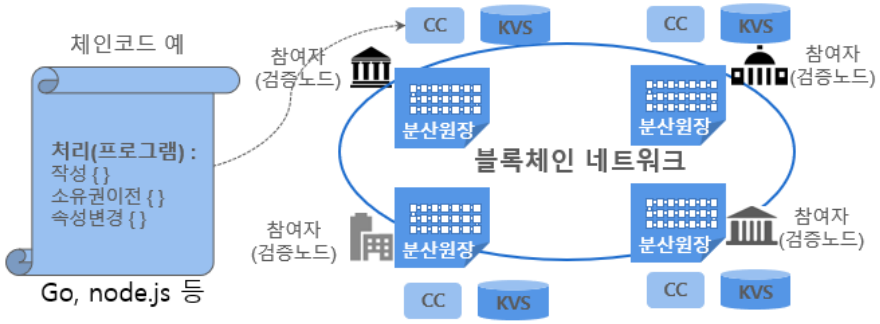
1.블록체인 : 비즈니스 모델의 혁신



2.합의(Consensus)알고리즘

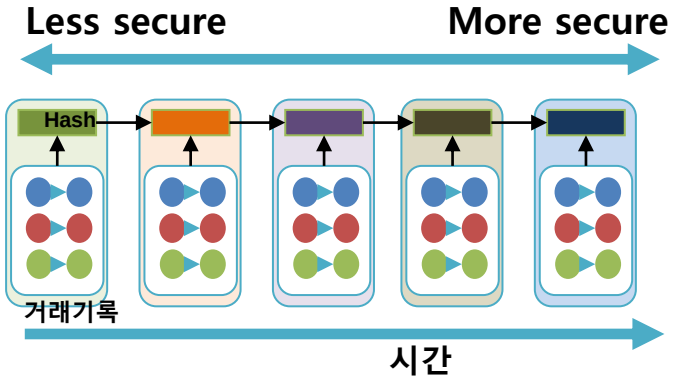
다양한 합의알고리즘을 통해서 **참여자들의 거래정보를 일관성있게 유지**함으로써 신뢰된 네트워크 제공

3.스마트 컨트랙트



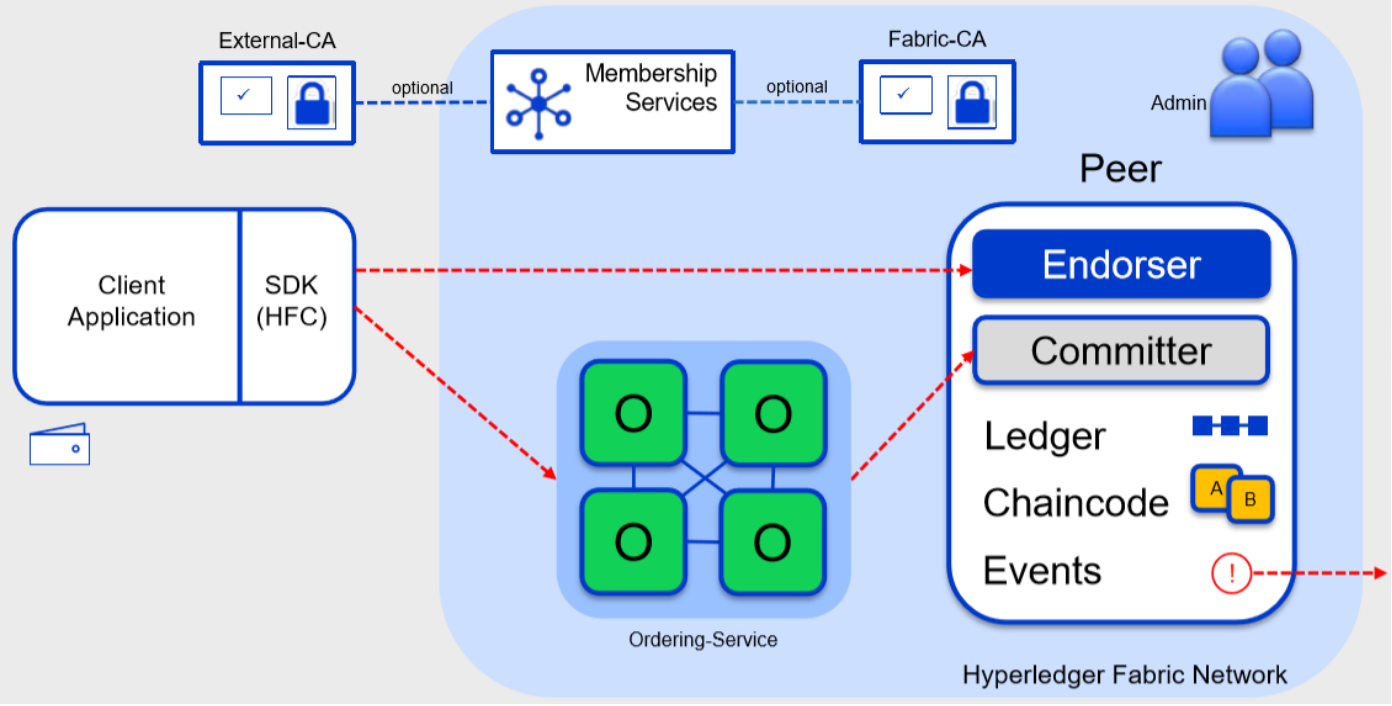
4.블록체인 거래원장 구조

시간순서상으로 기록된 암호화된 거래원장으로 하나의 블록은 하나 이상의 거래기록들로 구성되어 있음



2. 하이퍼레저 패브릭>개념아키텍처

블록체인플랫폼인 하이퍼레저 패브릭은 다음과 같은 아키텍처로 구성되어 있고, 피어(노드)의 역할은 다음과 같습니다.



* **인증서비스**는 인증서를 통해 네트워크의 참여자들에게 역할에 따른 **고유의 권한을 제공**

* **체인코드**는 피어네트워크에서 수행되어질 트랜잭션 로직을 가진 **스마트콘트렉트**

* **합의**는 피어네트워크상에서 각각의 **피어로부터 동의를 얻는 과정**

* **Peer**
- **Endorsing Peer :** 보증을 위한 특화된 피어로 일반적으로 스마트컨트랙트(체인코드)를 실행하고 트랜잭션 제안을 검증하여 수용 및 거부를 결정
- **Committer Peer** : 원장(블록)과 state관리, 트랜잭션 커밋 등 원장 보관의 역할

* **Ordering 서비스** : 원장에 트랜잭션 블록을 포함시키기 위해 Committer피어와 Endorsing피어들과 통신함
스마트 컨트랙트나 원장을 가지고 있지 않음

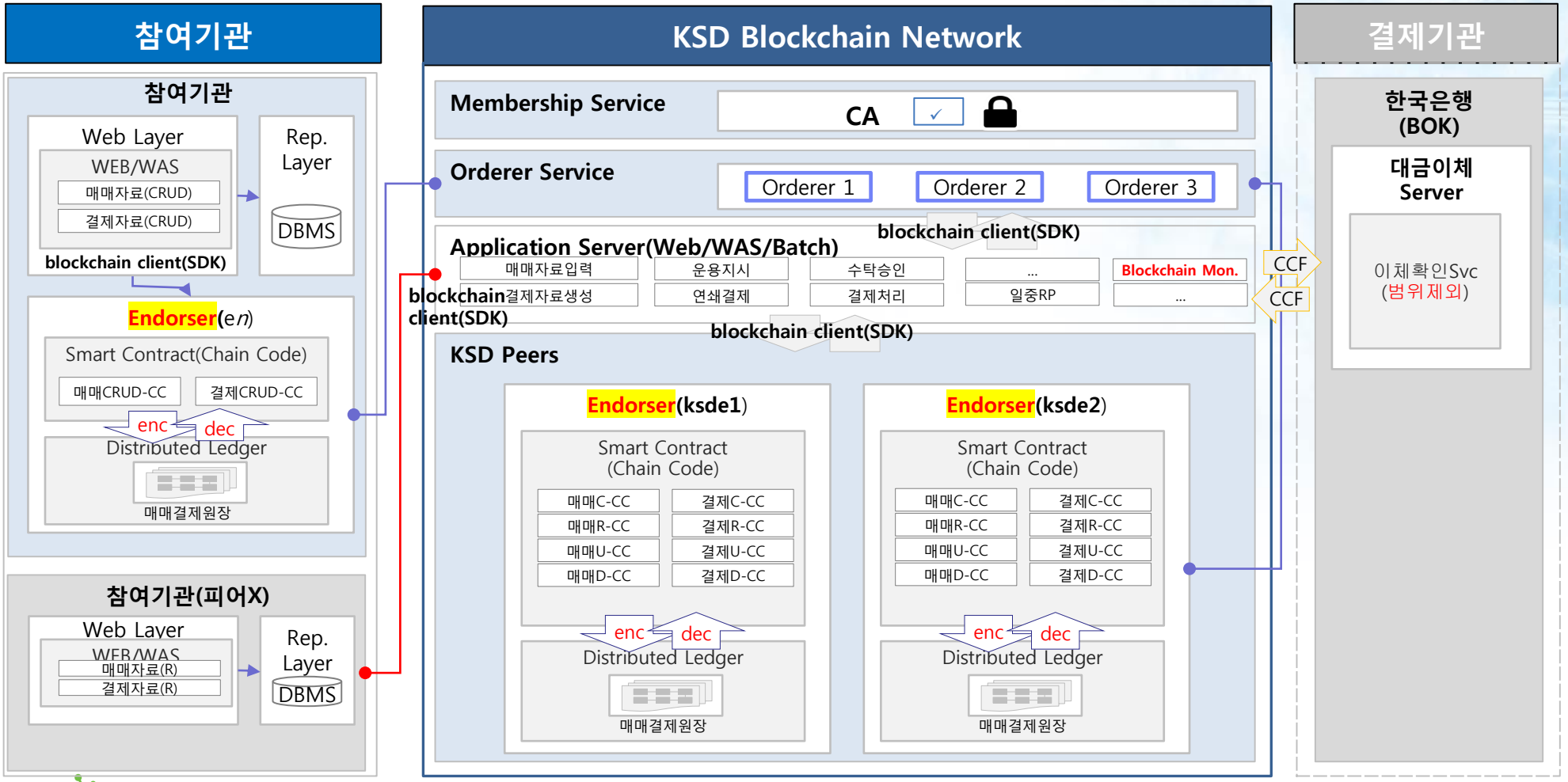
3. 적용 아키텍처 구성>Key-Point

채권장외결제시스템 블록체인 타당성 검토를 위한 아키텍처 구성의 이슈사항은 다음과 같습니다.

분류	아키텍처 구성 이슈사항	아키텍처 구성 Key-Point
참여기관	• 다양한 역할의 참여기관(증권기관/운용기관/수탁기관/증권금융/한국은행 등)으로 이루어진 환경	• **KSD보증, 참여기관보증 등 다양한 참여기관에 따른 피어 구성**
공유원장	• 참여기관은 해당기관이 속한 데이터만 참조해야 되고, 이외의 타기관 데이터는 공유되지 않아야 함	• **공유원장을 유지하면서 데이터 암복호화를 통한 거래데이터 기밀 유지 (검증환경에서는 단순화하여 적용)**
업무처리	• 매매자료입력>운용지시>수탁승인>연쇄결제>대리인 등 업무절차 및 처리 난이도 높음	• **중요업무처리는 포함하고 블록체인 검증을 위한 적용 업무Process를 간소화하여 진행**
업무테스트	• 다양한 업무처리에 따른 블록체인 검증을 위한 테스트 데이터 가공 및 환경 구성 어려움	• **시뮬레이션을 위한 업무Process를 선정하고 기준일 실거래데이터 기준 테스트 환경 구축**
기능테스트	• 블록체인 아키텍처에 대한 기능성, 안정성, 보안성, 효율성 등 관점에서 적용가능성 확인도 중요	• **실험환경 구축하여 기능점검항목을 정의하고 점검 후 내용 정리**

4. 블록체인 PoC 아키텍처

KSD 환경에는 Endorsing Peer 3개, Orderer Peer 3개로 구성하였고, 가상의 참여기관은 Endorsing Peer 1개씩 6개 기관을 구성하였습니다.



5. 개발영역> 1) 검증 대상업무

화면명	기능	기능설명	업무처리설명	업무적용 결과
매매>매매자료제출	조회	조회조건입력	매매자료 조회 조건 입력	현행 참여기관 Legacy시스템으로 자체 업무처리를 하기 위한 영역
		Legacy 시스템조회	조회버튼 클릭후 결과 확인	
	제출	매매자료제출	조회된 대상 중 선택 제출	1) 참여기관/KSD 사용자가 거래를 발생시키는 영역으로 로그인 유저(증권사/운용사/수탁사/KSD 등)에 따라서 접속하는 Peer를 구분 2) 접속된 Peer의 블록체인 원장을 조회하고 거래를 발생 3) 발생된 거래는 Endoser Peer에 의해 합의과정을 통하여 검증 4) 검증된 거래는 Ordering Service에 의하여 시간순서를 보장하여 Peer 들에게 전파하여 원장이 공유됨 단, 한국은행 등 대금이체 처리는 범위에서 제외
매매>매매자료확인	조회	매매자료확인 조회	매도자가 제출한 매매자료 조회하여 매수자가 확인	
	제출	매매자료확인	매수자가 매매자료를 확인하거나 또는 운용지시 진행	
매매>운용지시	조회	운용지시 대상 조회	매도자-매수자 자료 확인후 운용지시 대상을 조회	
	제출	운용지시 제출	운용지시 대상건에 대하여 운용지시 제출	
매매>수탁승인	조회	수탁승인 대상 조회	운용지시 제출된 매매자료 조회	
	제출	수탁승인 제출	수탁승인 대상건에 대하여 수탁승인 처리	
결제>연쇄거래	조회	연쇄거래 대상조회	결제자료중 연쇄거래 대상 조회	
	병합	연쇄거래-병합	결제준비 대상중 연쇄거래 대상을 선택하고 병합함	
	분할	연쇄거래-분할	결제준비 대상중 연쇄확정 대상을 선택하고 분할함	
결제>결제처리	조회	결제처리 대상 조회	결제처리 대상을 조회	
	처분제한	처분제한 처리	결제처리 대상건 선택하여 처분제한 처리	
	이체요청	이체요청 처리	처분제한 대상건 선택하여 이체요청 처리	
	이체확인	이체확인 처리	이체요청 대상건 선택하여 이체확인 처리	
	결제완료	이체요청 처리	이체확인 대상건 선택하여 결제완료 처리	

5. 개발영역>2)오픈소스 및 개발영역

PoC에 도입된 블록체인 플랫폼 및 응용App 소프트웨어는 오픈소스를 활용하여 구축하였습니다.

구분	오픈소스	사용용도	버전	개발영역
블록체인 네트워크	Hyperledger Fabric	블록체인 플랫폼	1.2	시스템구축
	Kafka	오더링서비스(분산 메시징)	0.9.0.1	
	Zookeeper	오더링서비스(분산 코디네이터)	3.4.9	
	CouchDB	State DB	2.0.0	
Application Server	Tomcat	테스트업무화면 및 블록체인모니터링을 위한 어플리케이션 서버	8.5.23	테스트업무App 블록체인모니터링
	MariaDB	어플리케이션용 DBMS	5.5.44	
	OpenJDK	Java 어플리케이션 개발도구	1.8.0	
	Go	체인코드 개발도구	1.7	체인코드

5. 개발영역>3)체인코드 및 응용App

블록체인기술을 활용한 개발은 스마트컨트랙트(체인코드)기능 6본와 업무화면 8본, 응용App 16본을 개발하였습니다.

분류	체인코드.오퍼레이션	주요기능	KVS
스마트 컨트렉트 (체인코드)	MasterLedgerCC.putTradeInfoList	블록체인 원장에 여러 개의 거래를 등록하기 위한 체인코드	매매결제자료
	MasterLedgerCC.putTradeInfo	블록체인 원장에 하나의 거래를 등록하기 위한 체인코드	
	MasterLedgerCC.queryTradeInfo	원장에 반영된 거래정보를 조회하기 위한 체인코드	
	MasterLedgerCC.queryAllTrades	원장에 반영된 모든 거래정보를 조회하기 위한 체인코드	
	MasterLedgerCC.queryTradeInfoByKey	원장에 반영된 특정 조건의 Key의 거래정보를 조회하기 위한 체인코드	
	MasterLedgerCC.getTradesByRange	원장에 반영된 특정 조건 범위의 거래정보를 조회하기 위한 체인코드	

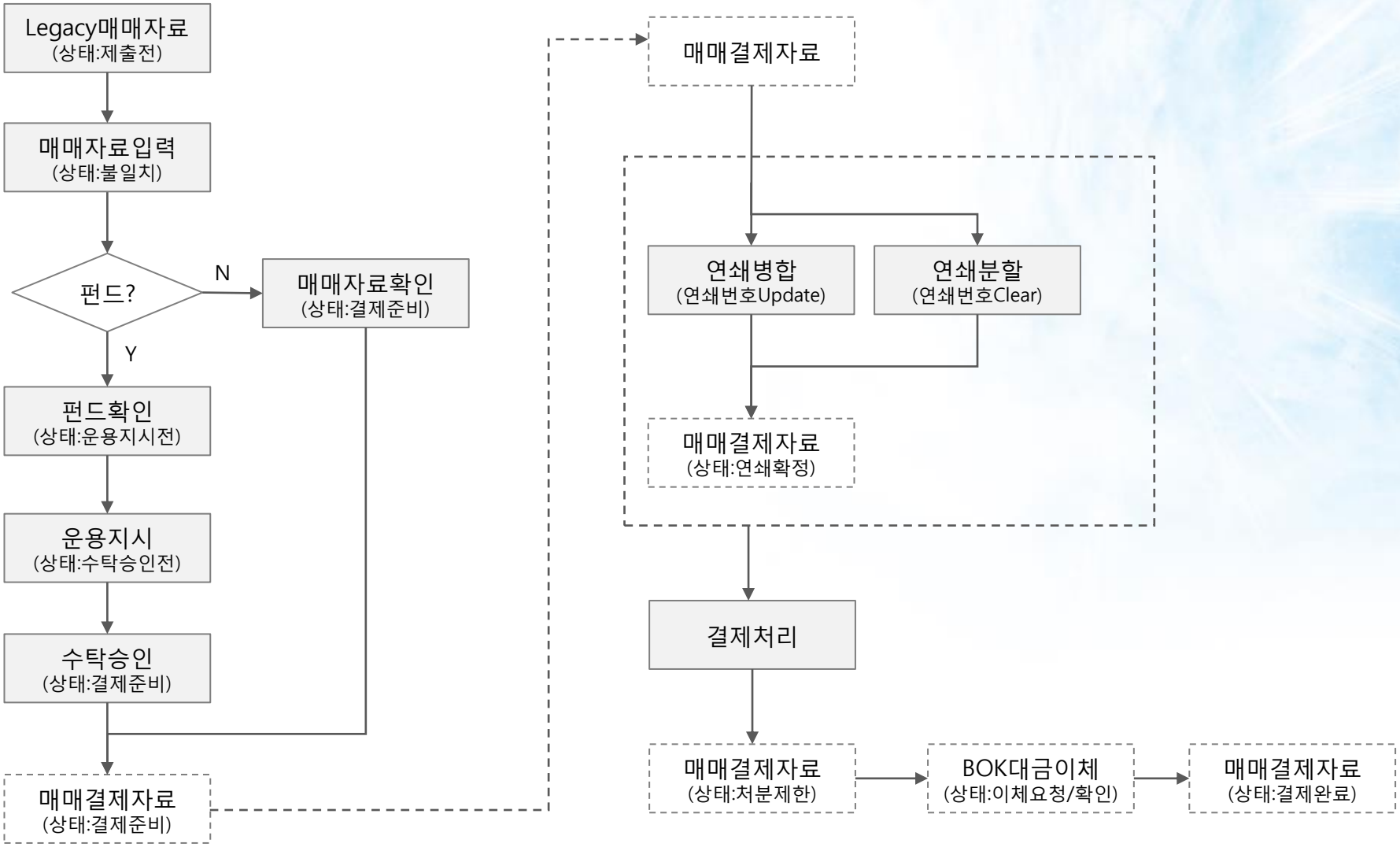
분류	주요기능	내역
응용 App	Legacy매매자료조회 매매자료입력 매수자료확인 운용지시요청 수탁승인요청 연쇄거래 결제처리-처분제한 결제처리-이체요청/이체확인 결제처리-결제완료 매매결제현황 등	매매결제자료 등록 및 조회용 화면 및 App프로그램(Java)

KSD 한국예탁결제원

Contents

uniPoint

1. 시연 동영상

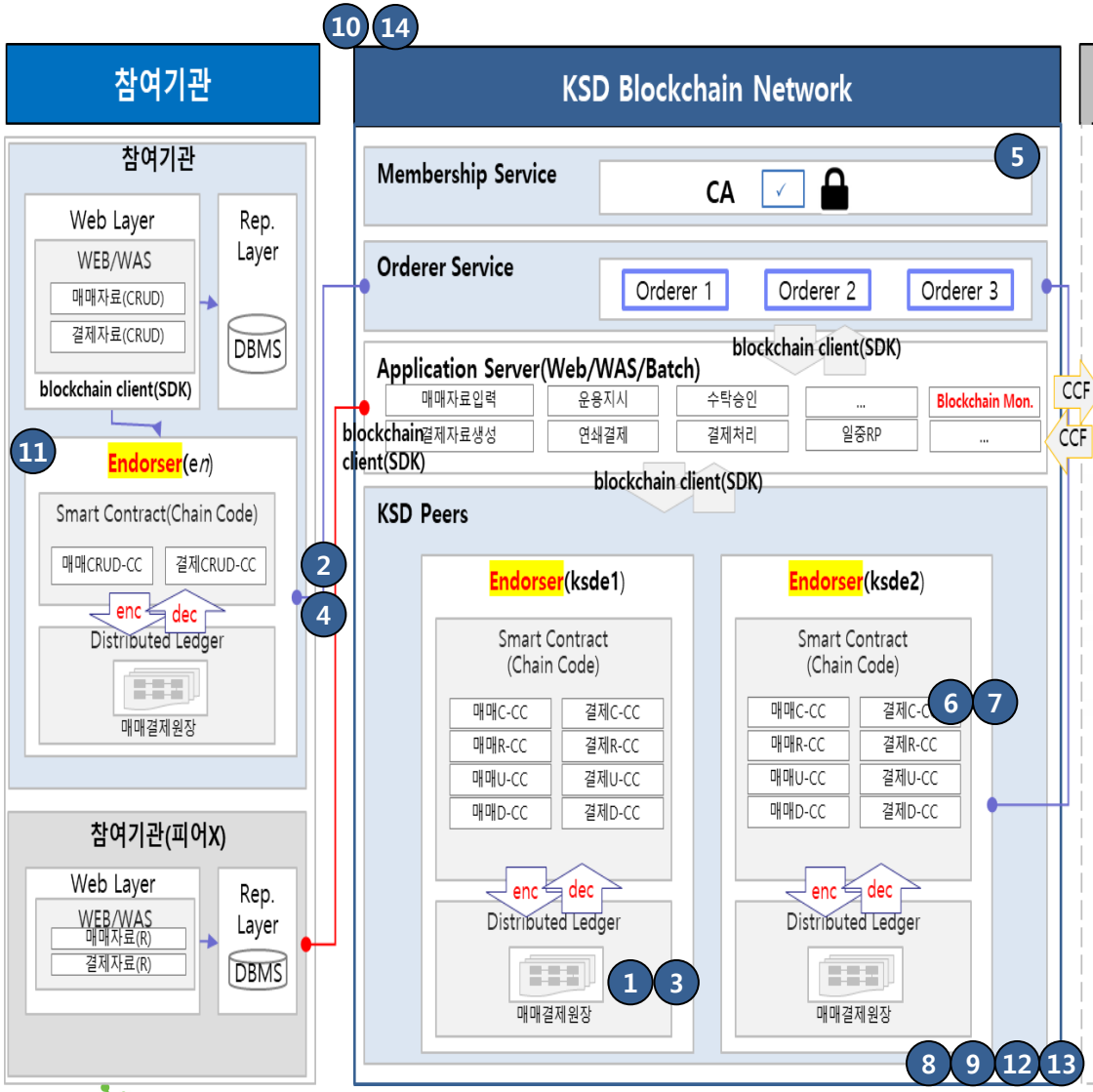

Legacy매매자료
(상태:제출전)
매매자료입력
(상태:불일치)
펀드?
N
매매자료확인
(상태:결제준비)
Y
펀드확인
(상태:운용지시전)
운용지시
(상태:수탁승인전)
수탁승인
(상태:결제준비)
매매결제자료
(상태:결제준비)
매매결제자료
연쇄병합
(연쇄번호Update)
연쇄분할
(연쇄번호Clear)
매매결제자료
(상태:연쇄확정)
결제처리
매매결제자료
(상태:처분제한)
BOK대금이체
(상태:이체요청/확인)
매매결제자료
(상태:결제완료)

KSD 한국예탁결제원

Contents

uniPoint

1. 블록체인 기술적용 결과>1)개요



구분	검증항목
기밀성 (Confidentiality)	[1]분산원장
	[2]전송구간
무결성 (Integrity)	[3]분산원장 무결성
	[4]전송구간 위변조
	[5]비인가된 접근
	[6]스마트컨트랙트
	[7]원장변경관리
가용성(Availability)	[8]블록체인 플랫폼
부인방지 (Non-Repudiation)	[9]거래부인방지
성능 (Performance)	[10]거래처리성능
확장성 (Extensibility)	[11]노드 확장성
유지보수 (Maintenance)	[12]개발 및 배포 용이성
	[13]모니터링 용이성
투자비용 (Investment Costs)	[14]도입/유지비용

2. 블록체인 기술적용 결과>2)상세 내용(1/2)

구분	검증항목	현행 시스템	vs	블록체인 시스템
기밀성	분산원장	암호화 후 DB 저장	=	암호화 후 원장 반영 (현행 시스템과 동일)
	전송구간	Web-WAS구간 SSL통신으로 구간암호화	<	통신채널 암호화로 기밀보장 (블록체인 기본구성)
무결성	분산원장 무결성	거래데이터는 예탁결제원 시스템에 존재 참여기관은 대사	<	블록체인에 거래 적합성 검증 프로세스 포함
	전송구간 위변조	참여기관과 전송구간 암호화 되지 않으면 위변조 가능	<	블록체인 네트워크 및 트랜잭션이 암호화되어 있어 위변조 어려움(블록체인 기본구성)
	비인가된 접근	중요 파일 위변조는 백업으로 대비 (접근관리 및 모니터링 가능)	<	사용자 인증(Ecert), 트랜잭션 인증(Tcert), 통신채널(TLS 인증서)를 통하여 비인가 접근 자체 불가능
	스마트컨트랙트	업무 프로그램 소스를 형상 및 변경관리 인가 사용자가 라이프사이클 (life-cycle)을 관리	=	노드/업무 별 체인코드가 분류 인가사용자가 라이프사이클(life-cycle)을 관리
	원장변경관리	메타시스템을 통하여 변경관리	=	원장 및 스마트컨트랙트에 대한 변경이력 및 버전 관리
가용성	블록체인 플랫폼	중요시스템 이중화 및 DR 장애 발생 후 복구 메커니즘 복잡	<	노드 복구 시 오더러를 통해 원장동기화 부분 오류 발생시에도 전체 기능은 작동 (장애 내성)
부인방지 (Non-Repudiation)	거래부인방지	시스템 로그 또는 대사파일로 이력 관리기능 필요	<	거래 부인방지가 성립되지 않는 것이 블록체인의 특징

2. 블록체인 기술적용 결과>2)상세 내용(2/2)

구분	검증항목	현행 시스템	vs	블록체인 시스템
성능	**거래처리성능**	이중화 및 부하분산 등 시스템 최적화	>	트랜잭션에 대한 Consensus(합의) 및 Peer간 원장동기화로 인하여 성능이 떨어짐 **(평균 50배 처리 시간이 소요)**
확장성	**Peer 확장성**	참여기관 추가에 따른 하드웨어,소프트웨어 설치 불필요	>	참여기관 추가 시 하드웨어/소프트웨어 설치 필요 블록크기에 따라서 상당한 동기화 시간 소요
유지보수	**개발/배포 용이성**	지원 솔루션 고도화	>	지원 솔루션 부족
	모니터링 용이성	다양한 모니터링 도구 지원	>	모니터링 도구 부족, 추가 개발 필요
투자비용	**도입/유지 비용**	초기투자비용 : 중앙운영기관 높음 운영유지비용 : 중앙운영기관 높음	>	초기투자비용 : 참여기관별 노드구성위한 비용 발생 운영유지비용 : 참여기관별 일정 수준의 유지비용 소요 • 현행 중앙집중시스템(레거시)에 일부업무(채권장외 결제업무 등)를 신규 블록체인으로 구성 및 유지할 경우 추가적 투자 및 유지비용 발생

3. 처리성능(참고)

측정조건: 현재 시장규모 하 처리능력 및 향후 시장성장 시 처리능력 예측을 위하여 통상적 1일 결제 건수(1548건)의 1/2/6/10배 상당 건수의 처리 완료에 소요되는 시간 비교

단위:초

동시처리 (묶음처리)	1배(1548건)			2배(3096건)			6배(9288건)			10배(15480건)		
	현행	블록체인	비교(배)	현행	블록체인	비교(배)	현행	블록체인	비교(배)	현행	블록체인	비교(배)
1	4.516	**220.537**	49	8.310	**349.511**	42	23.148	**1319.436**	57	49.676	**2448.922**	49
5	1.109	**51.226**	46	1.829	**101.652**	56	5.569	**307.900**	55	10.985	**575.0914**	52
10	0.739	**31.900**	43	1.507	**65.096**	43	5.389	**200.357**	37	9.512	**391.7076**	41
50	0.238	**13.729**	**58**	0.426	**30.125**	71	1.852	**93.773**	51	2.945	**175.7519**	60
100	0.218	**11.450**	53	0.385	**37.507**	**97**	1.411	**75.908**	54	2.283	**155.0469**	**68**
500	0.200	**8.948**	45	0.332	**21.446**	65	0.775	**57.829**	**75**	1.755	**107.6134**	61
1000	0.240	**6.024**	25	0.482	**16.579**	34	0.969	**55.034**	57	2.593	**100.5141**	39

처리성능 비교

- **블록체인 방식이 평균 50배 이상 처리시간 소요**
  - 블록체인은 트랜잭션에 대해 피어(Peer) 간의 합의(Consensus)가 필요하고, 각 피어 (혹은 노드)가 관리하는 원장을 동기화해야 하기 때문
  - 단, 거래가 특정시점에 집중되지 않는다면 성능체감은 낮음

4. 참여기관 필요사항 및 하드웨어 비용(참고)

구분	참여기관 필요사항	비고
컨소시엄 구성	- (만약) 구축 추진 시, 단독 추진 보다 컨소시엄 형태로 추진 필요. 이 경우 참여기관 동의 필요 - 비참여 기관에 대한 대안 필요	Peer 구성 없이 참여 지원
하드웨어	- 참여기관별 Peer 구성을 위한 서버 도입 필요	선택사항
소프트웨어	- 블록체인 플랫폼 구성은 오픈소스로 구성되어 있음	서버 접근권한/모니터링 등
네트워크	- 허가형(Permissioned) 블록체인으로 전용회선, VPN 등 네트워크 구성 필요	
응용개발	- 현행 SAFE+와 유사한 업무화면을 참여기관별로 개발 필요	개발표준 및 SDK(API) 제공
개발/운영인력	- 신규 도입 및 구축되는 하드웨어/소프트웨어/응용개발 등을 개발 및 운영 인력 필요	
기타	- 블록체인 적용에 따른 업무처리 프로세스 변화에 대한 협의 필요	

01 하드웨어

- **KSD : CA, 오더러 3, endorser 피어 3**
  - 약 4억 5천 소요
- **참여기관 : endorser 피어**
  - 기관별 약 7천 5백 소요

02 운영비용

- **현실적으로 전면 블록체인화는 불가능하므로 기존시스템(legacy)과 병존 필요**
- **과도한 추가 운영/유지보수 비용 발생 가능**

감사합니다

KSD 한국예탁결제원

uniPoint