싱가포르 통화청의 블록체인 프로젝트 주요내용 및 시사점

(보안기술연구팀, 2018.1.22.)

1 개요

□ 싱가포르 통화청(MAS)은 블록체인 기반의 은행 간 실시간 총액결제 시스템[1]을 구축하기 위해 'Project Ubin'을 추진 중이며,

○ '17년 10월, **Project Ubin의 2단계 실험을 완료**하여 실험 내용과 이를 통해 도출한 **다양한 추가 고려사항을 공개**[2]

○ 또한, 금융권 블록체인 시스템에서 **중앙기관의 필요성과 중앙기관의 역할 재정의**의 중요성을 강조

□ 본 보고서에서는 Project Ubin 2단계(이하 'Ubin 2')의 **주요 추진사항을 소개**하고 **금융권 블록체인 시스템 구축 시 고려사항을 제시**

< Project Ubin 개요 >

○ **(목적)** 싱가포르의 은행 간 실시간 총액결제 시스템(MEPS+)을 블록체인 기반 시스템으로 대체하고자, 블록체인 기술의 적용 가능성을 검증

○ **(방식)** 실시간 총액결제 시스템에 필요한 기능 및 고려사항에 따라 단계별로 추진 중이며 **현재 2단계까지 완료**(`16년 12월 1단계 완료)

<Project Ubin 단계별 비교>

기준	1단계(`16년 하반기)	2단계(`17년 하반기)	향후 계획
목표	**중앙은행(MAS)이 발행한 디지털 통화**를 활용 가능성 검토	**결제유동성 절약기능, 개인정보보호 기능** 적용 검토	**증권대금 동시결제, 외환 동시결제 기능** 등 적용 검토
참여기관	금융회사 : 9개 기술업체 : 2개	금융회사 : 12개 기술업체 : 4개	-
블록체인 플랫폼	Ethereum	Corda, Hyperledger Fabric, Quorum	-

※ Project Ubin 1단계의 세부내용은 '금융보안원, 싱가포르의 분산원장기술 기반 자금 교환 시스템 구축 프로젝트(Project Ubin) 소개, 2017.7.' 참고

1) 실시간 총액결제 시스템 - 금융회사 간의 자금이체, 증권이체 등을 중앙은행의 계정을 통해 건별로 즉시 처리하는 시스템
2) MAS(Monetary Authority of Singapore), Project Ubin Phase 2, Nov. 2017.

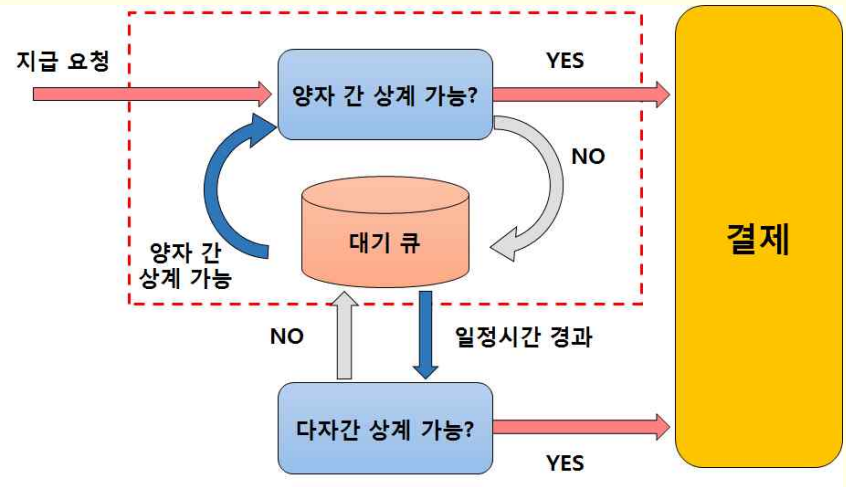
2 Ubin 2의 주요 내용

(가) 추진 목적 및 시스템 구성

□ **(목적)** 블록체인 기반 실시간 총액결제 시범 시스템에서 **개인정보 보호**와 **결제유동성 절약기능의 적용 가능성**을 검토

결제유동성 절약기능(LSM, Liquidity Saving Mechanism) - 금융회사 간의 실시간 총액결제 시스템에서 결제계좌에 잔액이 부족하면 **지급요청을 대기 큐(queue)에 추가**하여 **결제계좌 잔액이 일정수준 이상이 되면 처리**하거나, **상계(netting)[3]를 통해 처리**하는 방식

<결제유동성 절약기능 예시>



□ **(시스템 구성)** 블록체인 적용 가능성을 다각적으로 검토하고자, 다양한 **블록체인 플랫폼(이하 '플랫폼')으로 시스템을 구성**

○ **(플랫폼)** 금융권의 다양한 시범 시스템에서 활용 중인 R3의 **Corda**, Hyperledger **Fabric**, J.P. Morgan의 **Quorum**을 사용

– 사용된 플랫폼은 금융권에서 요구하는 **개인정보 보호, 참여자 식별** 등의 기능을 제공

3) 금융회사 상호 간에 발생하는 채권/채무를 개별적으로 결제하지 않고 일정기간이 경과 한 후에 차액만을 결제하는 방식

○ **(구성 환경)** 플랫폼별로 블록체인 시스템(총 3개)을 마이크로소프트의 Azure 클라우드 환경에 구성[4]

<Corda 기반의 실시간 총액결제 시범 시스템 구성>

□ Corda 기반의 시범 시스템의 노드 구성

○ **(Bank)** 실시간 총액결제를 위한 지급지시 트랜잭션을 요청하는 주체

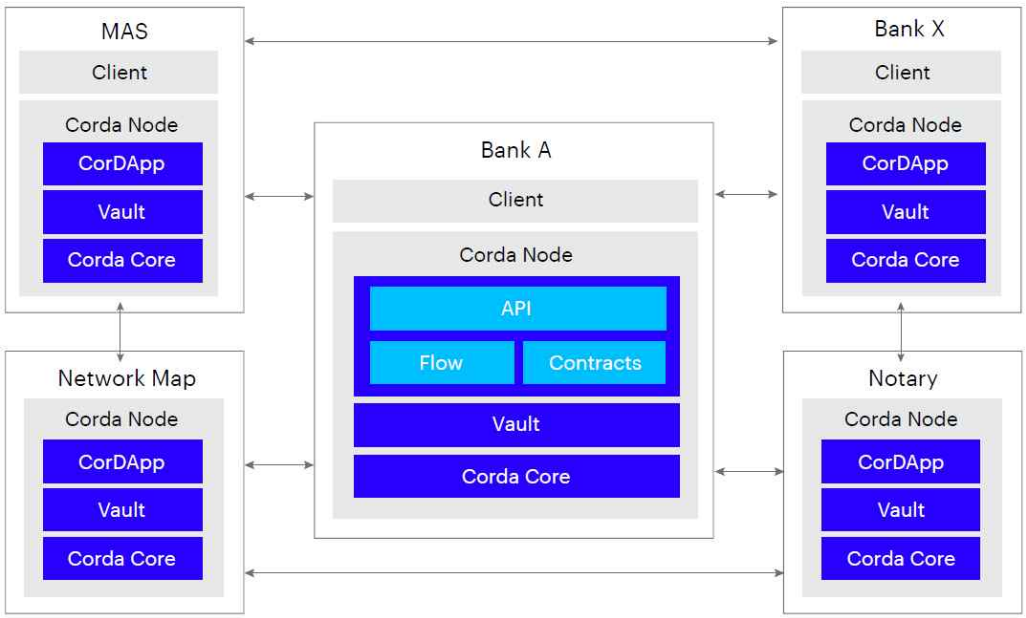
○ **(Notary)** 트랜잭션의 유효성을 확인하고 공증해주는 주체

○ **(Network Map)** 참여자 식별과 참여자 간에 거래 및 통신에 필요한 참여자의 공개 키와 IP 주소, 기타 정보를 관리 및 제공

○ **(MAS)** 디지털 화폐 발행, 거래 모니터링, 시스템 운영 등을 위해 싱가포르 통화청(MAS)이 노드로 참여

<Corda 노드의 구성>

모듈		역할 및 기능
Client		트랜잭션을 생성 및 타 노드와 송·수신
Corda Node	CorDApp	트랜잭션을 실행 및 처리
	Vault	CorDApp을 실행 및 관리
	Corda Core	블록체인 노드의 기본 모듈



4) 마이크로소프트는 Azure를 기반으로 BaaS(Blockchain as a Service)을 통해 상기 블록체인 플랫폼을 포함한 다양한 블록체인 플랫폼을 제공 중이며, 이용자는 이를 통해 블록체인 시스템을 효율적으로 구성 가능

(나) 추진 내용

□ **(결제유동성 절약기능)** 결제 **대기 큐(Queue)** 기능, **상계(Netting)** 기능을 스마트 컨트랙트 기반으로 개발 및 적용

○ **(대기 큐)** 은행의 지급요청을 결제계좌의 잔액부족으로 처리(결제)할 수 없는 경우 해당 지급요청을 대기 큐에 추가하고,

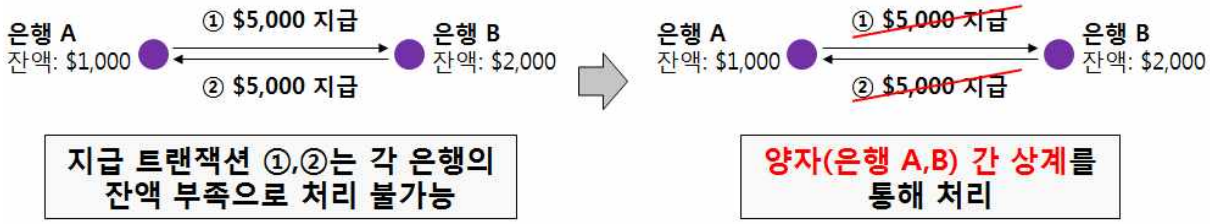
– 향후 결제계좌의 잔액이 충분해지면 처리하거나, 양자 또는 다자간 상계를 통해 처리

– 대기 큐 내의 지급요청은 큐에 추가된 순서대로 처리되며, 우선순위 설정/변경, 취소에 의해 처리순서가 변경 가능

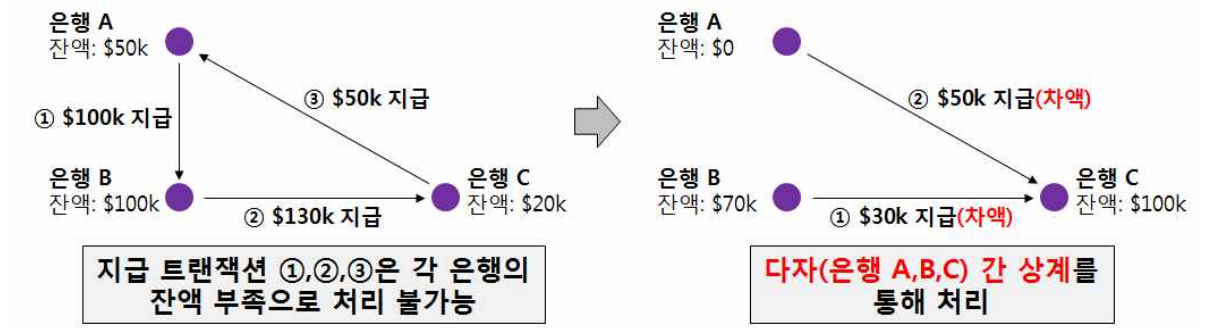
○ **(상계)** 상호 간 결제계좌의 잔액 부족으로 결제가 불가능한 경우(교착상태), 양자 또는 다자간 상계를 실행하여 처리

<양자 간 상계, 다자간 상계 예시>

양자 간 상계



다자간 상계



□ **(개인정보 보호)** 다자간 상계 처리 시 거래내역, 거래당사자의 신원 등 개인정보의 기밀성을 보장 가능한지 여부를 검토

○ 사용된 플랫폼에서는 최소한의 거래정보 공유, 익명화된 서명키 사용 등의 방식으로 개인정보 보호가 가능하나,

○ 다자간 상계 시에는 은행 간 거래내역 등이 거래 당사자가 아닌 타 은행에도 공유되어 개인정보 침해가 발생 가능

<사용된 플랫폼별 개인정보 보호 방식>

<table>
<tr><th>플랫폼</th><th>거래내역 보호</th><th>거래 당사자 신원 보호</th></tr>
<tr><td>Corda</td><td rowspan="2">최소한의 참여자(need to know)에게만 거래내역을 공유
- Corda : 거래당사자 및 공증인에만 공유
- Fabric : 채널(Channel) 참여자에만 공유</td><td rowspan="2">거래마다 익명화된 공개키 쌍을 생성 및 사용</td></tr>
<tr><td>Fabric</td></tr>
<tr><td>Quorum</td><td colspan="2">거래내역 및 거래 당사자의 신원정보 없이 거래 유효성을 확인할 수 있는 Zero Knowledge Proof 방식을 적용</td></tr>
</table>

(다) 추진 결과 및 향후 계획

□ **(결과)** 3개의 플랫폼별 블록체인 시스템에서 **개인정보 보호기능과 결제유동성 절약기능을 동시에 제공 가능함을 확인**하였으며,

○ 플랫폼별 성능을 **개인정보 보호, 확장성, 처리성능, 시스템 복원력, 결제 최종성** 측면에서 분석한 결과, 모두 동등한 수준의 성능을 보임

□ **(향후 계획)** Project Ubin의 다음 단계에서는 증권대금 동시결제, 외환 동시결제 기능 등의 적용 가능성과 **서비스 가용성, 시스템 관리 측면의 다양한 고려사항을 함께 검토할 계획**

3 블록체인 기반 금융시스템 구축 시 고려사항

▸ 싱가포르 MAS는 Ubin 2의 경험을 기반으로 **블록체인 기반 금융시스템 구축 시 고려해야할 사항을 (가) 시스템 관리 (나) 서비스 가용성** 측면에서 도출

(가) 시스템 관리

□ 블록체인 시스템의 **효율적 관리와 안전성 보장을 위해** 시스템의 **탈중앙화 수준, 노드 관리, 중앙기관의 역할에 대한 고려할 필요**

1) 탈중앙화 수준

○ **탈중앙화 수준**은 해당 시스템에 참여한 주체의 권한, 의무, 기여도 등이 평등한 수준을 의미

○ 모든 참여자가 평등한 경우 **탈중앙화 수준이 높고**, 참여자가 평등하지 않거나 특정 참여자가 일부 역할을 담당할 경우 **탈중앙화 수준이 낮음**

□ 블록체인 시스템 구축 시 탈중앙화 수준을 고려해야할 사항으로 **금융회사의 참여 형태, 블록체인 간 상호연동 방식** 등이 존재

○ **(금융회사 참여 형태)** 금융회사등은 블록체인 네트워크에 **직·간접형태로 참여하는 준(semi) 탈중화** 네트워크으로 구성 가능

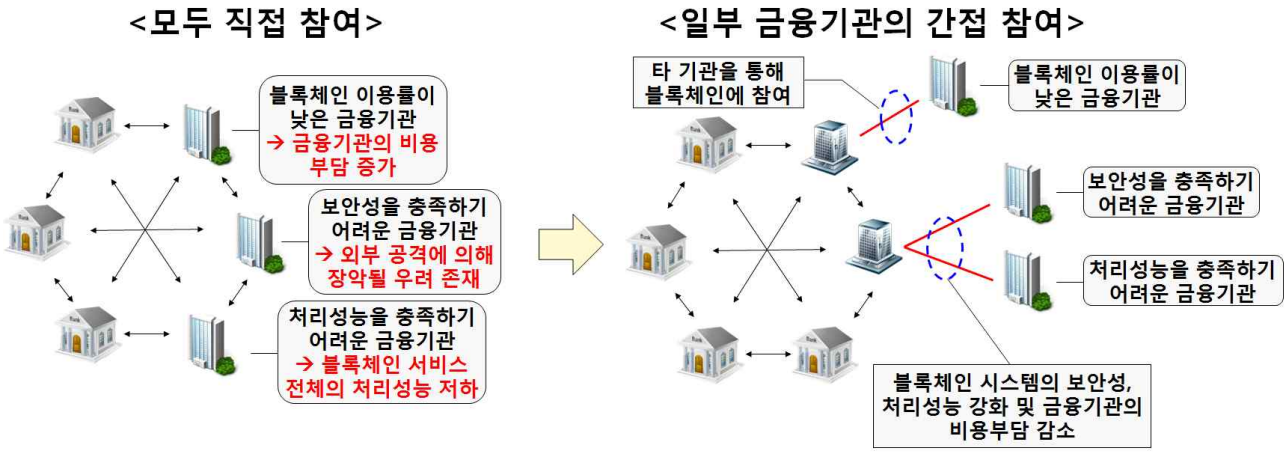
– 블록체인 이용률이 낮은 금융회사*는 시스템 유지 및 보안에 필요한 비용을 절감하고자 직접 참여기관을 통해 간접적으로 참여 가능

* 또는 거래에 직접 관여하지 않거나 일부 기능만 이용하는 非금융회사도 포함

– 이를 위해서는 시스템의 거버넌스 및 정책 수립·통제를 강화하고, 특히 **간접 참여기관을 대행하는 기관에는 높은 보안 수준 및 처리성능을 충족**하도록 요구

> ※ 간접 참여기관을 대행하기 위해 요구되는 보안수준 및 처리성능을 충족시키기 위해, **대표 금융회사(직접 참여기관) 또는 중앙기관이 대행 역할을 담당하는 방안**을 고려

<직·간접 참여 예시>



○ **(블록체인 간 상호연동)** 블록체인 시스템 간 상호연동 시* 업무·운영 관리 측면에서 탈중앙화 수준을 고려

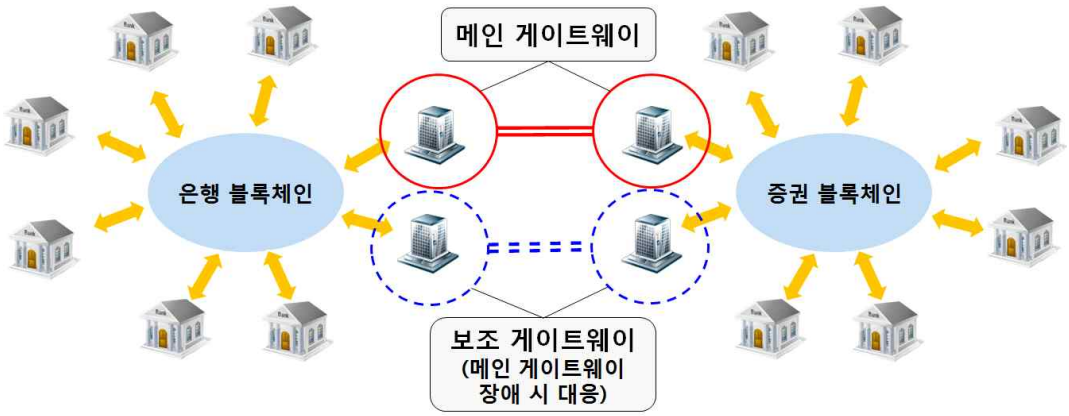
* 예: 은행 및 증권업권 블록체인의 연계를 통한 증권대금 동시결제 등

– 상호연동 시 모든 참여기관이 스마트 컨트랙트 등 블록체인 기능을 통해 연계하는 방식은 **탈중앙화 수준이 높으나 운영·관리의 효율성이 낮음**

– 블록체인 시스템을 **게이트웨이**(대표 금융회사 등이 운영)를 통해 연계하는 방식은 탈중앙화 수준은 낮지만 **다양한 보안 기능*을 효과적으로 제공 가능하며 운영·관리의 효율성이 높음**

* 안전한 통신, 침입탐지·차단, 사후 모니터링 등

<게이트웨이 기반의 블록체인 간 상호연동>



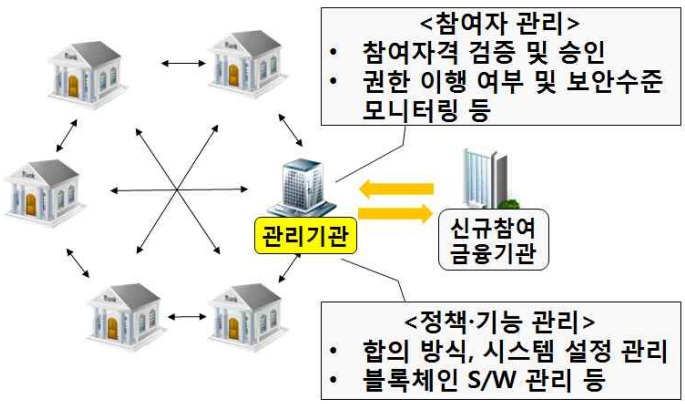
2) 노드 관리

□ 블록체인 시스템을 안전하게 운영하기 위해서는 **참여자 관리, 정책·기능 관리** 등의 기능이 필요하며 모든 노드에 일관성 있게 적용되도록 **담당 관리기관을 지정하는 방안을 고려**

○ **(참여자 관리)** 블록체인 시스템의 처리성능 및 보안수준을 일관성 있게 유지하기 위해 금융회사의 참가자격(보안수준 등)을 검증하고 권한을 부여하는 등의 참여자 관리가 필요

○ **(정책·기능 관리)** 합의 방식 및 시스템 설정, 블록체인 S/W에 대한 유지보수 및 패치 등이 전체 참여자에 동일하게 적용되어 일관성이 유지되도록 관련 정책·기능을 관리

<게이트웨이 기반의 블록체인 간 상호연동>



3) 중앙기관의 역할 재정의

□ 금융권 블록체인 시스템의 효율적 관리와 안전성 향상을 위해 **중앙기관이 참여하여 일부 역할*을 담당**하는 방안 고려

* 싱가포르 MAS는 지속적으로 중앙기관의 역할을 추가로 도출할 계획

○ **(주요 역할)** 중앙집중식 금융시스템에서 **중앙기관이 수행하던 감독, 거버넌스 등의 주요 역할은** 블록체인 시스템에도 안전성 및 효율성을 향상시키기 위해 **중앙기관이 담당 가능**

<중앙집중식 금융시스템에서 중앙기관의 주요 역할>

분야		주요 역할[5]
관리·감독	거래검증	금융거래 시 거래대상(예금, 증권 등)의 존재와 거래 유효성을 검증하여 거래의 신뢰성 보증
	감독	금융업무 수행 시 규제 이행여부, 금융거래의 적법성 등 관련 법규를 준수하는지 확인
	거버넌스	금융회사 인허가와 금융회사별 역할 및 권한 등을 부여하고 사업범위 등을 관리
사기방지		사기 거래를 차단 및 예방
분쟁해결		금융거래와 관련된 분쟁 발생 시 사실관계 확인 및 분석
보안강화		금융회사의 보안수준을 강화하고 침해사고를 예방하기 위해 보안성 평가 및 위협정보 공유 등 수행

○ **(기타)** 시스템 거버넌스, 참여자 관리, 간접 참여기관의 운영 대행, 블록체인 간 게이트웨이, SLA 거버넌스, 감사 등의 기능이 중앙기관의 역할로 적합

(나) 서비스 가용성

□ 블록체인 시스템의 가용성 향상을 위해 **시스템 복원 전략 수립과 금융서비스 상시 제공 방안** 마련의 필요성 제기

5) M. Mainelli and A. Milne, The Impact and Potential of Blockchain on the Securities Transaction Lifecycle, SWIFT Institute Working Paper, May 2016.

○ 일반적으로 블록체인이 적용된 시스템은 시스템 복원을 위해 **중앙집중식 시스템 방식**을 고려

○ 그러나 블록체인 시스템의 특성을 반영하여 효과적인 복원 시점, 백업 방식 등의 복원 전략을 마련할 필요

○ 또한, 블록체인 시스템을 기반으로 금융서비스를 **상시(24×7) 제공하기 위해서는 다양한 기준을 마련**

<상시 서비스 제공을 위해 고려해야할 기준(예시 : 실시간 총액결제 시스템)>

순번	기준
1	거래요청 처리와 관련된 기준 시간, 단위
2	금융회사 업무시간 이후의 거래요청 수수료 및 거래처리 인센티브
3	금융회사별로 상이한 업무처리 시간
4	금융회사별로 상이한 SLA(Service Level Agreement)
5	외환 거래 시 환율 결정 등

4 시사점

□ **(블록체인 시스템의 탈중앙화 수준 고려)** 블록체인 시스템에서 노드 관리, 상호연동 등의 기능을 특정 참여자가 담당하는 등, **블록체인 시스템의 효율적 관리, 보안성 제고를 위해 탈중앙화 수준을 적절히 조절**할 필요

□ **(중앙기관의 역할 도출)** 국내 금융환경과 국내·외 금융권의 블록체인 시스템 구축사례 등을 분석하여, **국내 금융권의 블록체인 시스템에 적합한 중앙기관의 역할을 도출 및 재정의**할 필요