

기업혁신, 블록체인을 어떻게 활용할 것인가

1. 블록체인 개요
2. 블록체인 적용 사례
3. 블록체인 적용 방안



안필용 책임

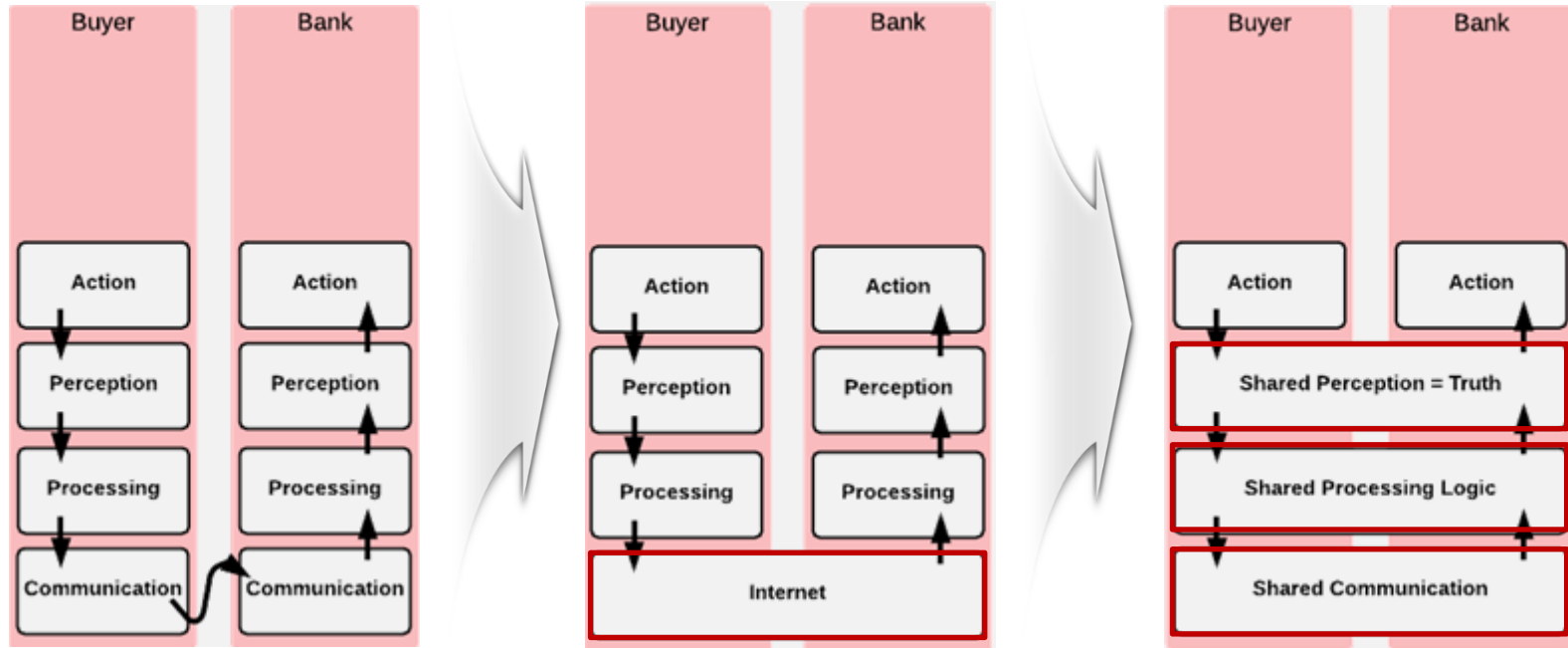
Copyright © LG CNS

LG CNS의 사전 승인 없이 본 내용의 전부 또는 일부에 대한 복사, 전재, 배포, 사용 등을 금합니다.

1. 블록체인 개요

- 블록체인과 신뢰
- 블록체인의 이해
- 블록체인의 주요 기능 및 활용
- 블록체인 유스케이스

Depth of Trust



Internet 이전
정보의 생산과 소유

Internet 등장
정보의 공유

Blockchain 등장
정보의 신뢰성 확보

블록체인의 시작

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing

P2P Network

Encryption

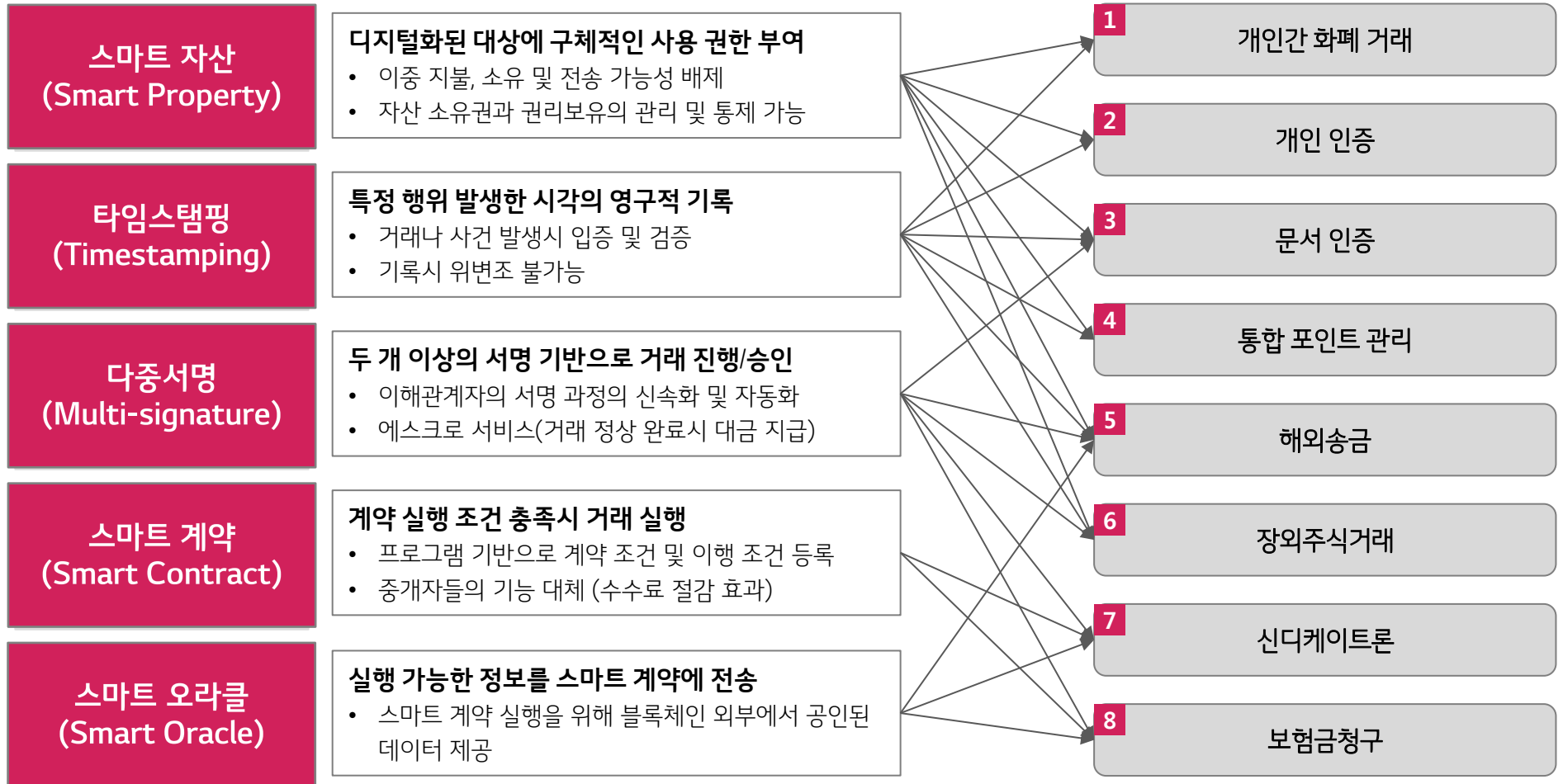
Consensus Algorithm

Block + Chain

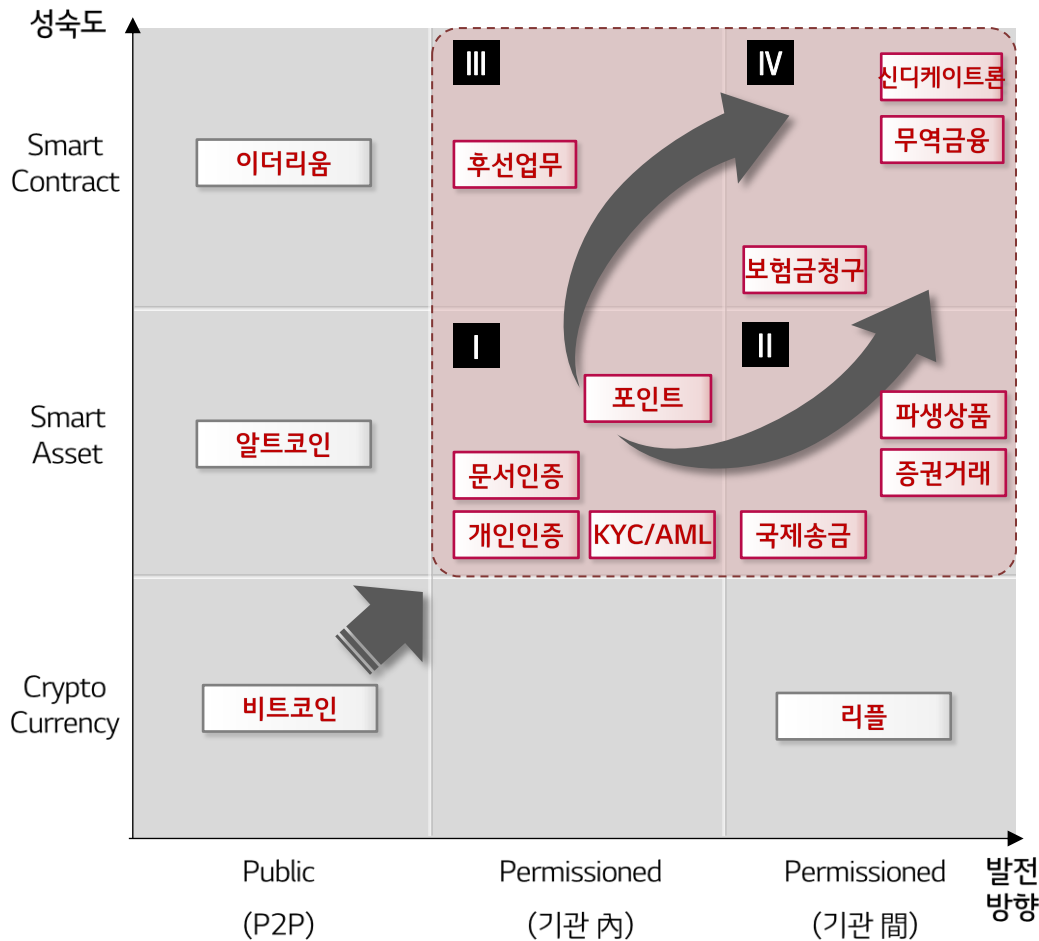
Smart Contract

블록체인의 주요 기능 및 활용

블록체인은 스마트 자산, 타임스탬핑, 다중서명, 스마트 계약, 스마트 오라클 등의 기능을 통해 다양한 서비스에 활용될 예정임



블록체인의 금융 유스케이스의 도입은 기관 內 인증업무 중심으로 우선 적용되고 있으며, 점차 기관 間의 Smart Contract 기반의 다양한 업무로 확대되고 있음



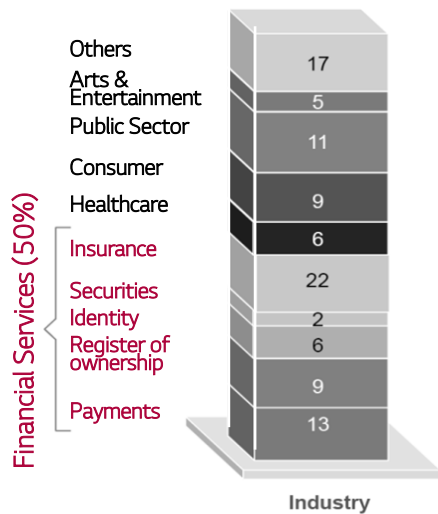
- I 기관 內 Asset**
 하나의 기관이 내부/외부 사용자를 대상으로 Asset을 관리하기 위함
 예) 인증, KYC/AML, 포인트 등
- II 기관 間 Asset**
 복수의 기관이 내부/외부 사용자를 대상으로 Asset을 교환 및 결제하기 위함
 예) 자산거래(국제송금, 증권 등)
- III 기관 內 Contract**
 하나의 기관의 내부/외부 사용자를 대상으로 조직간의 연계 업무 Process Innovation
 예) 후선업무 (담보 평가 등)
- IV 기관 間 Contract**
 복수의 기관이 내부/외부 사용자를 대상으로 교환/결제 등의 업무 Process Innovation
 예) 신디케이트론, 무역금융, 보험금 청구 등

2. 블록체인 적용 사례

- 블록체인 시장동향
- 블록체인 적용 사례 > 성숙모델
- 비금융권 블록체인 적용 사례

블록 체인 기술을 적용할 수 있는 유스케이스 중 약 50%가 금융 산업에 집중됨

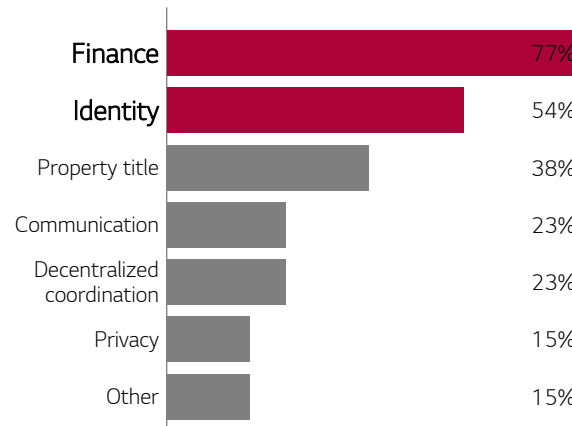
Blockchain Use case



McKinsey Panorama, web search

Will impact Financial Services

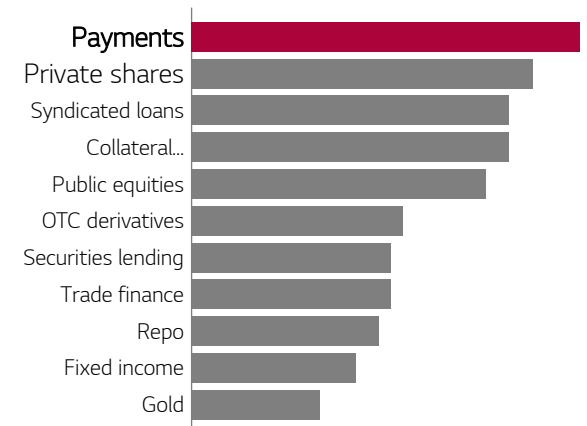
“블록체인 기술이 어느 부분에서 가장 큰 영향을 줄 것이라고 생각하십니까?”



Credit Suisse research

Financial Service 중에서는

“금융 서비스의 변화를 가져올 유망한 유스케이스”



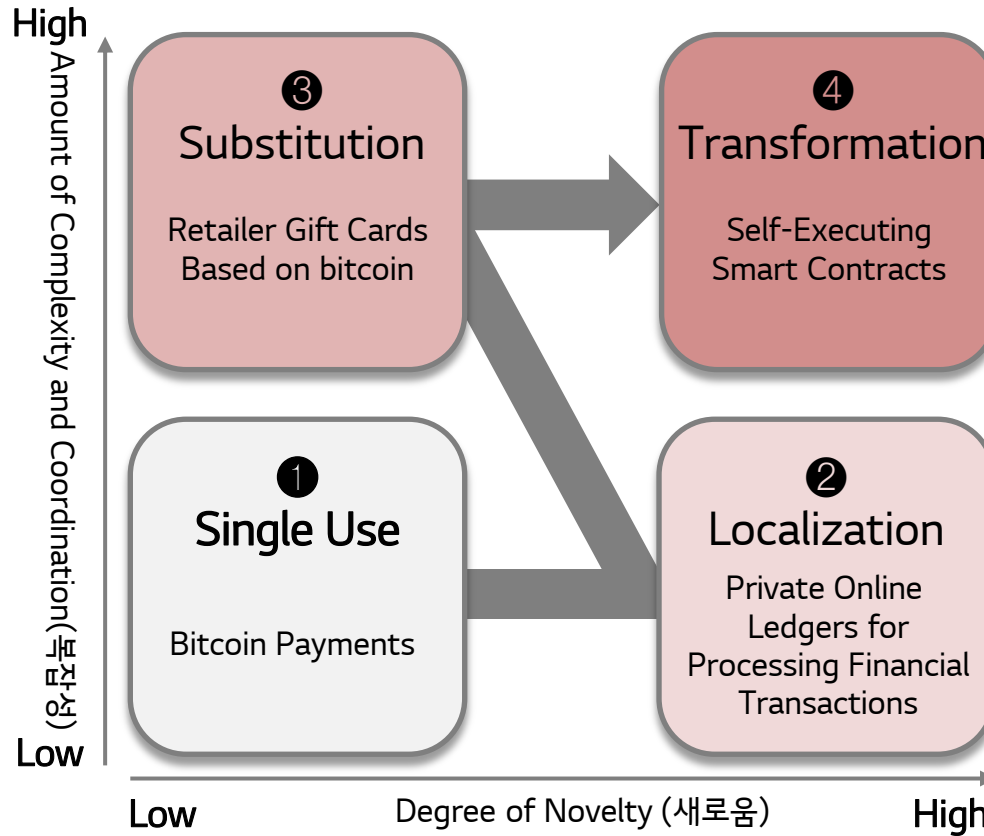
Greenwich Associates 2016, Credit Suisse research

- 산업별 블록체인 Use case 현황
 - 약50%가 금융영역의 Use case
 - 특히 보험영역이 전체 22% 차지하며 다양한 Use case가 도출

- Transaction 비율이 높은 Finance와 Identity 영역에서의 블록체인 적용 가능성과 효과가 높을 것으로 전망

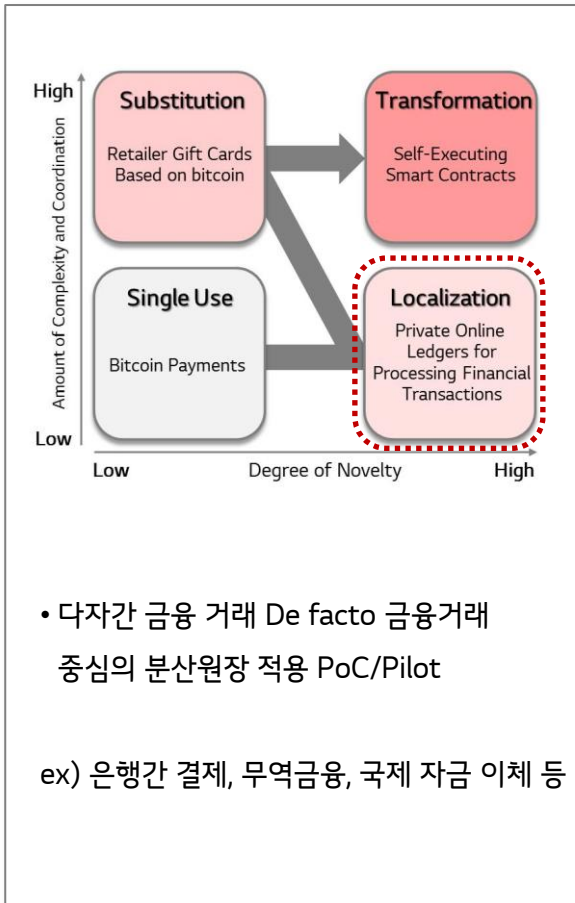
- 결제와 자금시장에서의 블록체인 도입 효과가 클 것임

블록체인은 활용 범위 확대, 적용 업무의 복잡성에 의해 순차적으로 성숙/발전되고 있으며, 금융권의 경우 1) Single Use, 2) Localization, 3) Substitution, 4) Transformation 단계로 발전하고 있음



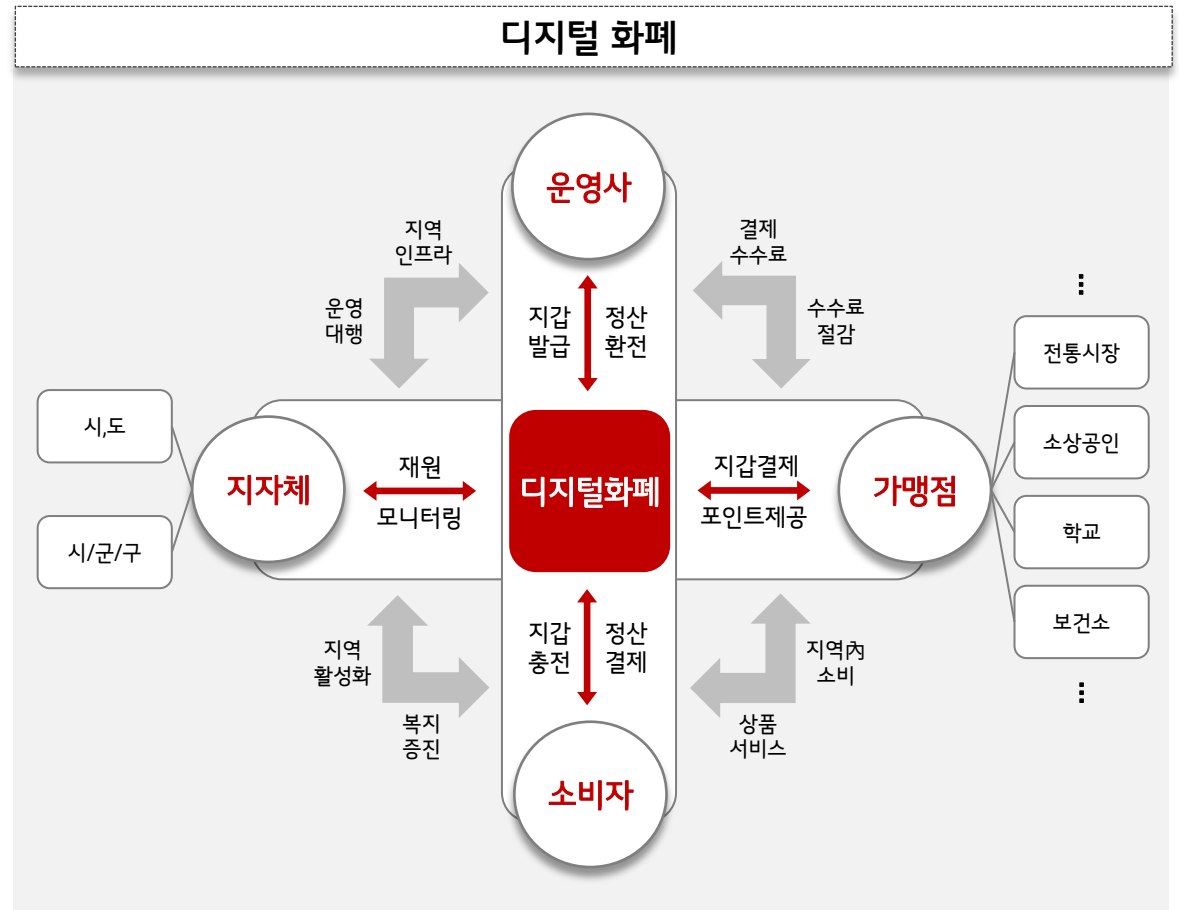
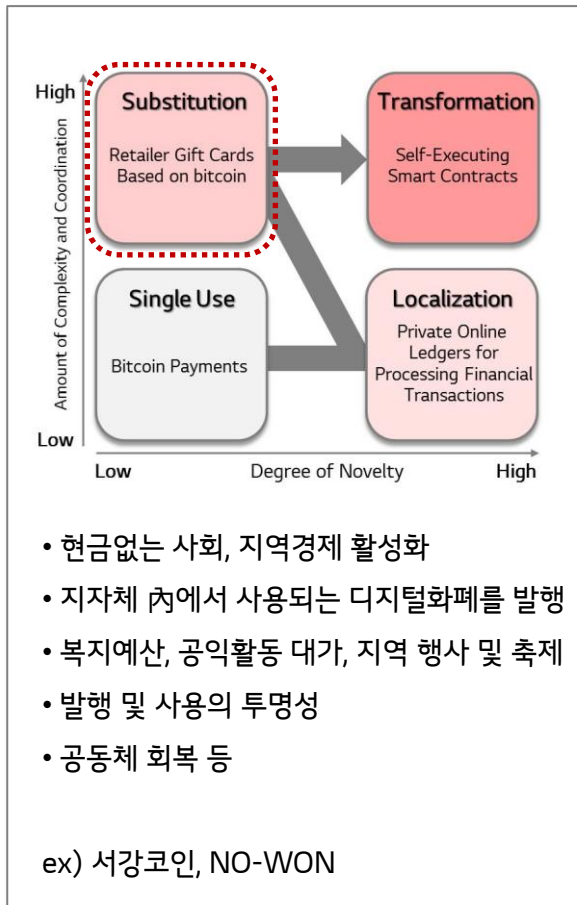
* Source : 'The truth about Blockchain', (HBR), 2017.01

싱가폴 중앙은행 디지털화폐 프로젝트를 통해 다자간 금융거래 중심의 분산원장 적용을 시도하여, 싱가포르의 총액결제시스템을 은행간 결제가 P2P로 24시간 7일 자유롭게 이루어질 수 있게 구축함

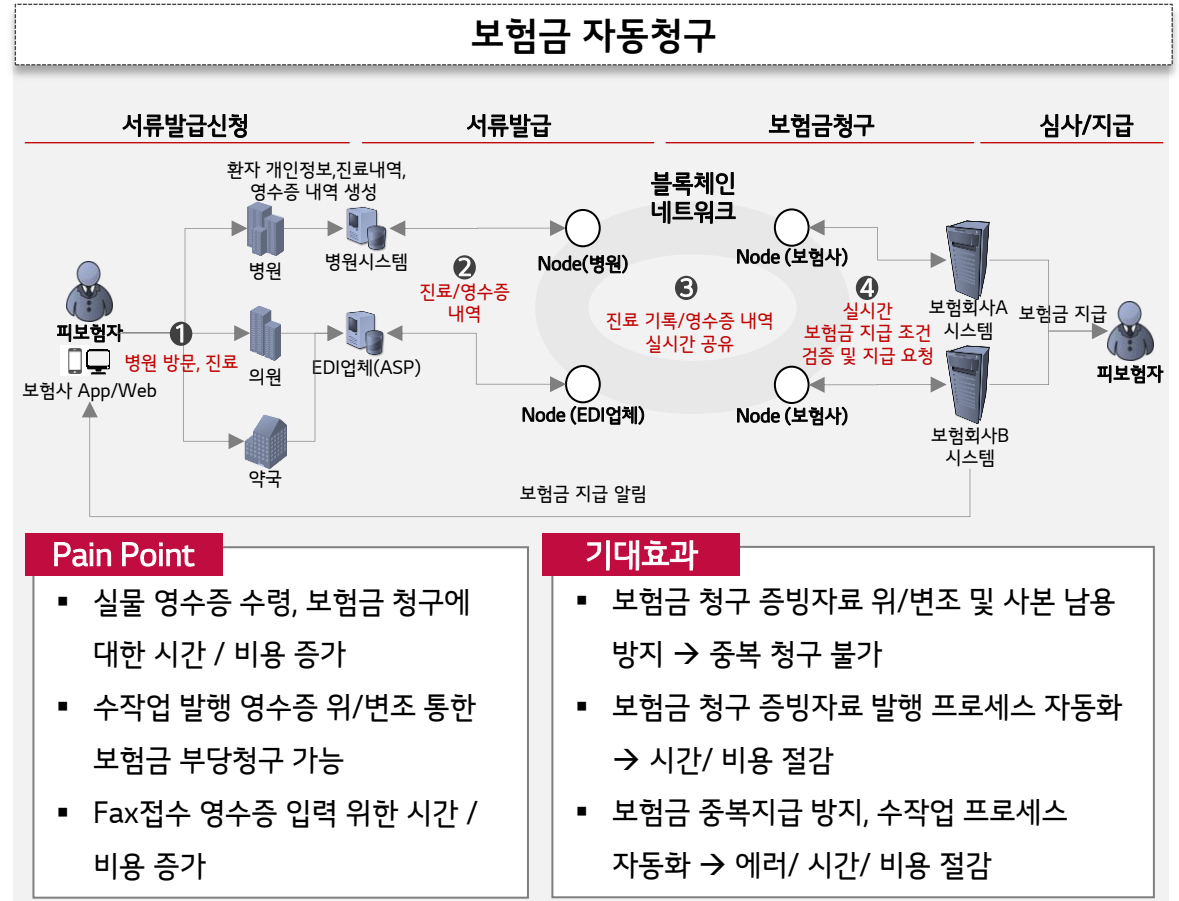
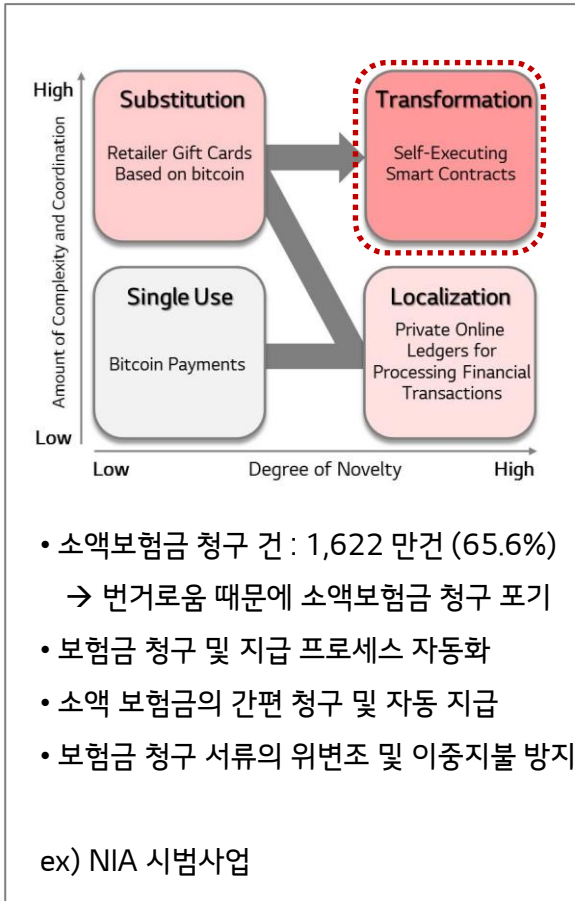


| Financial Transactions | |
|---------------------------|--|
| Project Ubin | <p><u>Cross-border Payments/Securities - PoC Accelerator - Cash & payment</u></p> <p>싱가폴 통화청과 은행 5곳이 참여한 중앙은행 디지털화폐 프로젝트로서 싱가포르의 총액결제시스템을 Corda 기반으로 구현하여 은행간 결제가 P2P로 24시간 7일 자유롭게 이루어질 수 있게 구축</p> |
| Project Marco Polo | <p><u>Tracking goods and trade documents - PoC Incubator - Trade Finance</u></p> <p>15개 글로벌 금융기관이 참여하여 무역거래를 보다 안전하고 효율적으로 하기 위하여 분산원장기반 플랫폼 위에 상품과 무역서류를 공유하고 추적</p> |
| Project Argent | <p><u>Cross Border Payment - Pilot Accelerator - Cash & Payment</u></p> <p>LG CNS를 포함한 20 여개 글로벌 금융사 및 파트너사들은 분산원장 기술을 활용하여 빠르고 효율적이며 저비용의 국제 자금 이체를 가능하게 하는 솔루션 개발 중</p> |

블록체인은 디지털화폐의 발행 및 관리를 가능케 하는데, 이는 현금없는 사회, 지역 경제 활성화, 발행 및 사용의 투명성 확보 및 공동체 회복 등의 효과를 생성할 것으로 기대하고 있음



블록체인 네트워크 및 스마트계약은 질병상해 진료비 청구 및 심사 프로세스를 자동화하고, 소액보험금의 간편 청구 및 자동 지급을 가능케 하며, 보험금 청구 서류의 위변조 및 이중지불을 방지할 수 있음



3. 블록체인 적용 방안

- LG CNS 블록체인 오픈링
- LG CNS 블록체인 플랫폼
- Why R3 Corda?
- LG CNS의 블록체인 구현 사례
- 블록체인 단계별 적용 Approach
- 블록체인 기술을 어떻게 적용할 것인가?

LG CNS 블록체인 서비스 오퍼링은 고객의 비즈니스 및 IT환경에 맞는 컨설팅 & PoC Service, Solution & Cloud Service 및 SI 구축 Service로 구성되어 있음

LG CNS 블록체인 오퍼링

블록체인 컨설팅 & PoC

Design Thinking 방법론 기반

| 수행 단계 | Phase1 시범 과제 및 분석 | Phase2 과제 및 요구사항 | Phase3 PoC 개발 도출 | Phase4 PoC |
|-----------------|---|---|--|--|
| 수행 단계 | Tech. Feasibility Use case Long List 분석 ↓ 기술 성숙도 및 실현화 수준 | 경제적인 과제 • Simple Use case 소개 • Design Thinking 방법론 | 적용 대상 요구사항 평가 • 평가 기준 수립 • 도입효과 및 실현 가능성 • 타(타)사 및 2차(차)조사 | 개발 수립 필요성 • PoC 실행계획 수립 • Scope, 요구사항, 로드맵 • 타사 역량 Assess 분석 |
| 단계별 수행 Activity | Business Feasibility • Digital Transformation • Industry Trend ↓ 신기술 도입 필요성 및 타사(사)비 | 업무 전문가 인터뷰 • As-is, To-be Pain Point, SWA • 기존/신 기술/과제/질문 • 제안서 및 개발 방안 | 개발 도출 • 적용 PoC, 개발 전략 • PoC 개발 조건 및 과제 수준 상세화 | 개발 • 컨소시엄(이)형태 설계 • 금융기관 기반 설계 • SI 및 운영 설계 |
| Output | 개발비 지원 방안 | 개발 대상 요구사항 | PoC 개발 업무 | PoC 시스템 |



- 유스케이스 도출, 적용 업무 선정 및 PoC


금융 특화 플랫폼 및 다양한 서비스 제공

자금이체 & 지급결제 솔루션

디지털지역화폐 솔루션

Cloud 기반 블록체인 서비스

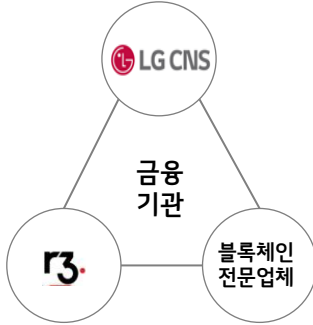





- 기관간 자금 이체/ 지급결제 서비스 제공
- 모바일 앱기반(M2M) 지역화폐 서비스 제공
- LG CNS Cloud 기반 블록체인 서비스 제공

최고의 SI Partnership

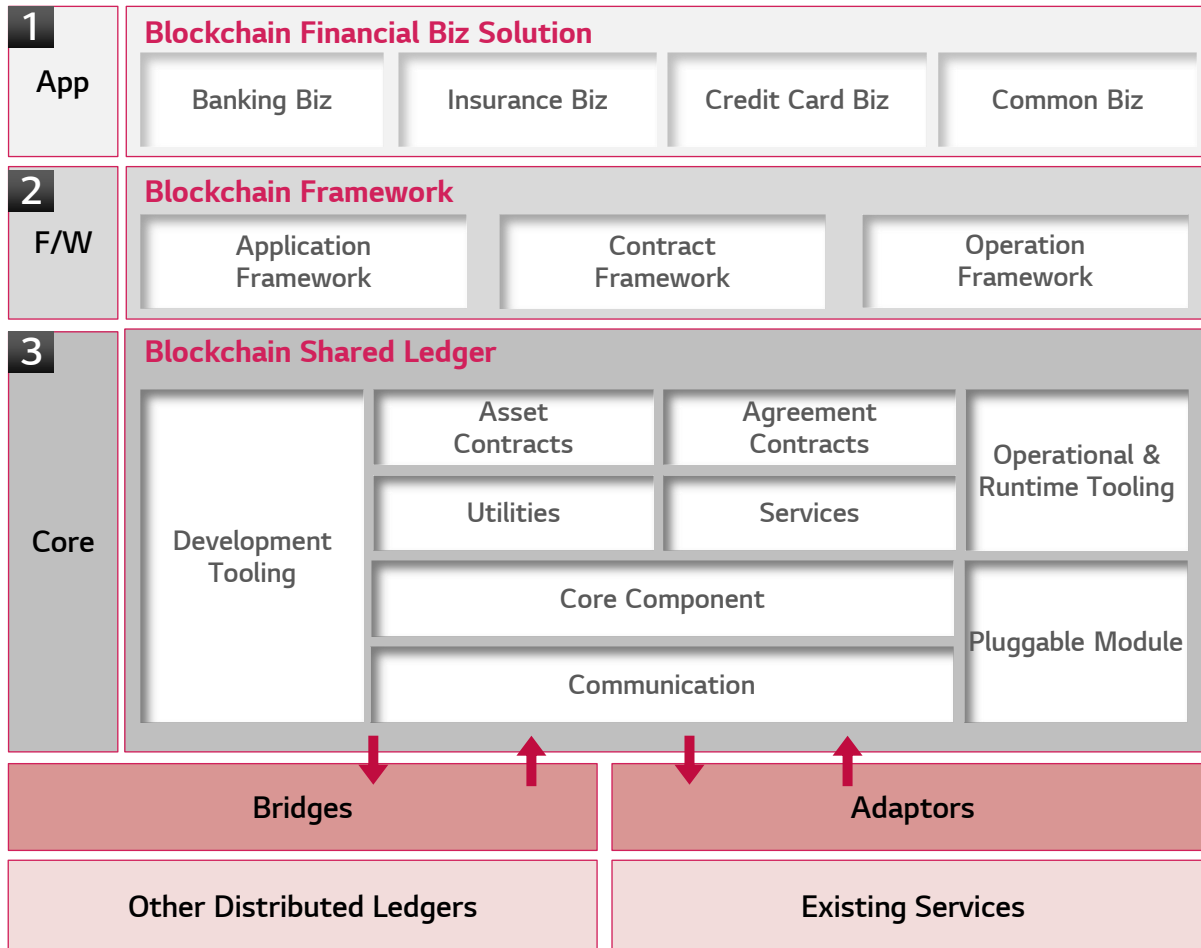
국내 최고의 블록체인 협의체



- 글로벌 최대 금융블록체인 컨소시엄 + 국내 블록체인 전문업체 협업

금융 거래에 최적화된 R3 Corda 분산원장 기술과 LG CNS의 보유한 풍부한 금융지식과 이행경험이 결합하여 안정적인 블록체인 플랫폼을 제공함

Corda 기반 LG CNS 블록체인 플랫폼



주요 특징

1 금융특화 Biz 솔루션 제공

- 금융 산업별(은행, 보험, 카드) 특화된 Biz 솔루션 기반 사업 제공
- 선진 금융의 Asset을 지속적으로 확보함에 따라 선제적으로 블록체인 금융업무 적용 및 확산

2 블록체인 프레임워크 제공

- 블록체인 개발 생산성 제고
 - 공통 또는 범용 모듈에 대한 Application, Contract 및 Operation 프레임워크
 - Smart Contract Template 제공
- 블록체인 서비스 안정성 제고
 - 한국 금융환경에 맞는 Pluggable Module 제공
 - . Operation Tool 등

3 R3 Corda 기반 환경 구축

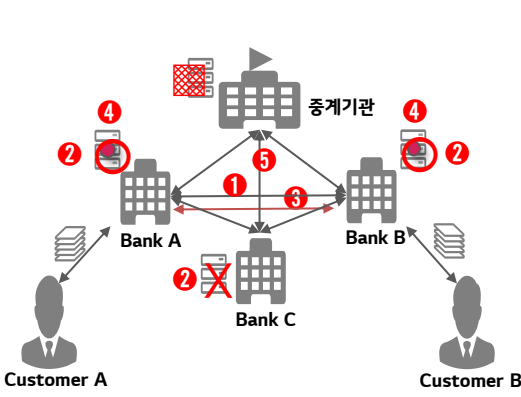
- 금융에 특화된 블록체인 플랫폼 R3 Corda 기반으로 지속적인 기반기술 고도화 제공
- 기존 금융망 및 타 블록체인 기반기술과의 유연한 연계 기능 제공

기존 블록체인은 Bitcoin/Ethereum 기반의 컨셉을 활용하여 만든 플랫폼이나, R3 Corda는 글로벌 금융기관의 Needs를 바탕으로 새롭게 구현한 아키텍처 기반의 “금융 거래 최적화 블록체인 플랫폼”임

Why R3 Corda?

| | 비트코인 | 이더리움 | Cord |
|----|---|---|--|
| 배경 | <ul style="list-style-type: none"> • 중개자 없이 • 신뢰할 수 없는 개인 간에 • 금전적 가치를 • 이전할 수 있을까? | <ul style="list-style-type: none"> • 전세계에 있는 컴퓨터들이 • 서버 역할을 해서 • 응용프로그램을 • 실행할 수 있을까? | <ul style="list-style-type: none"> • 중개자 없이 • 중복과 대사 작업이 없이 • 금융기관 간의 거래를 • 처리할 수 있을까? |
| 지향 | Censorship-resistant P2P Cash System | Unstoppable Applications | Shared control of financial agreements |

블록체인이 금융에 적용되기 위한 필수 조건

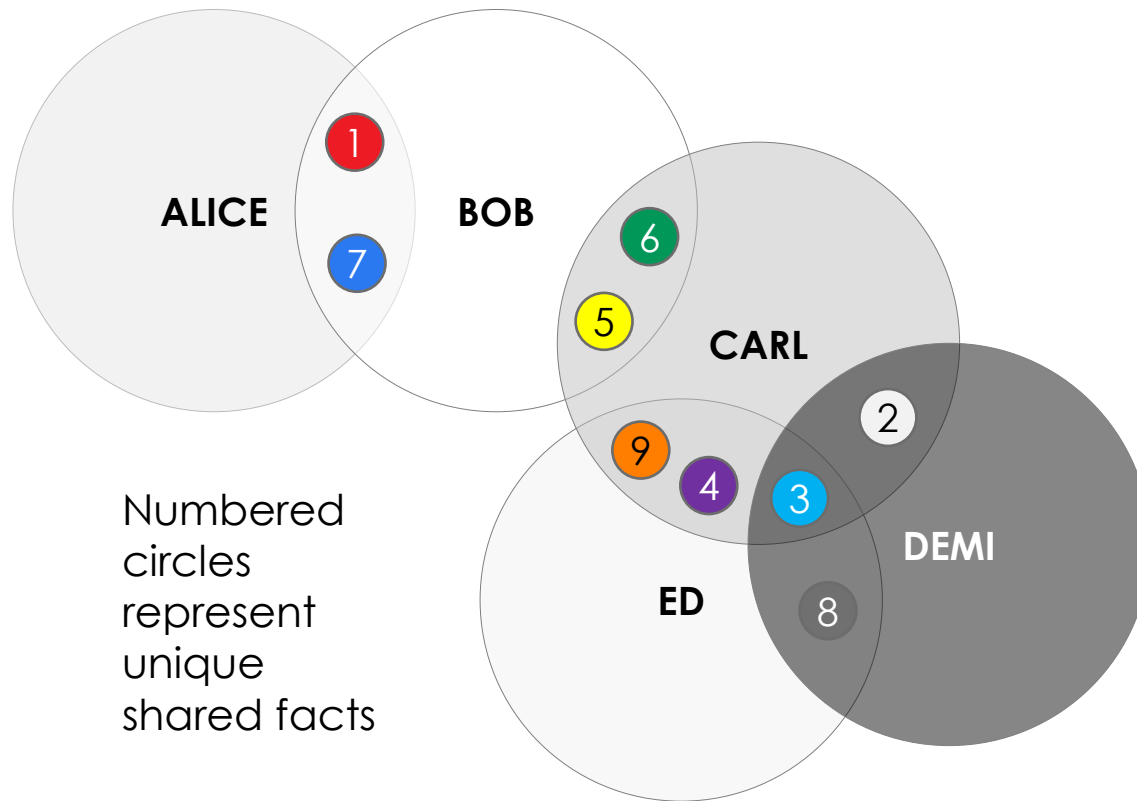


- ① 금융거래의 특성과 동일하게 당사자간의 합의만 요구
- ② 거래 당사자만 해당 금융 거래의 정보를 기록하고, 다른 참여자는 정보를 기록해서는 안됨
- ③ 빠른 처리 속도를 위한 아키텍처 구조 (Transaction as a BLOCK)
- ④ 금융거래의 법적 사항을 내재적으로 포함하는 구조
- ⑤ 감독기관이 실시간 감리/감독할 수 있어야 함
- ⑥ 금융의 자산/계약을 모델링할 수 있는 원장 구조여야 함

| | | |
|----------------------|-------|---|
| Privacy | 기존 | 모든 노드(참여자)에게 모든 거래 정보 전달 |
| | Corda | 거래 당사자에게만 해당 거래 정보 전달 → 거래 정보의 기밀성 확보 |
| Performance | 기존 | 참여자 합의, 블록생성 및 전파에 시간이 소요 |
| | Corda | 거래 당사자간 합의 및 기록 (다른 참여자 전파X) → 상대적으로 빠른 거래 처리 |
| Asset Modeling | 기존 | 금융 거래를 고려하지 않은 범용 원장 구조 |
| | Corda | 금융의 자산 및 계약을 모델링하는 원장 구조 → 검증된 자산 및 계약 모델링을 지원 |
| Inter-operability | 기존 | 금융에서 사용하지 않는 언어를 사용 (GO 등) |
| | Corda | 금융산업의 Library가 풍부한 JVM 기반 → 인프라, 인력의 활용이 용이 |
| legal enforceability | 기존 | 법률 사항을 첨부 형태로 관리 지원 |
| | Corda | 비즈니스 로직 구현 시 강제 실행할 법률 포함 → 금융 거래의 법률 이슈 헤지 |

기존 블록체인은 Bitcoin/Ethereum 기반의 컨셉을 활용하여 만든 플랫폼이나, R3 Corda는 글로벌 금융기관의 Needs를 바탕으로 새롭게 구현한 아키텍처 기반의 "금융 거래 최적화 블록체인 플랫폼"임

Privacy



$$ALICE = \{ 1, 7 \}$$

$$BOB = \{ 1, 7, 6, 5 \}$$

$$CARL = \{ 9, 4, 6, 5, 2, 3 \}$$

$$DEMI = \{ 2, 3, 8 \}$$

$$ED = \{ 9, 4, 8, 3 \}$$

목적

- 한은 금융망에서 이루어지는 업무 중 은행간 자금이체 업무를 분산원장 환경에서 설계하고 운영
- 분산원장기술 기반 은행간 자금이체시스템의 효율성, 회복성, 보안성, 확장성 평가

일정

- 시작 : 2017. 09. 21
- 종료 : 2018. 01. 12 (총 3.5개월)

범위

모의시스템 설계

- 결제흐름도 정의
- 노드 구성 설계
- 스마트계약 설계 등

모의시스템 구축

- R3 Corda를 이용한 은행간 자금이체 모의 시스템 구축

모의테스트 수행

- 총액결제 테스트
- 다자간결제 테스트
- 비기능 테스트

테스트평가 및 결과보고

- 평가항목별 평가
- 결과보고서 작성

CorDapp은

계약상태, 거래, 거래 절차를 정의하고 실행하는 분산원장 기반 어플리케이션

계약상태(State) 정의

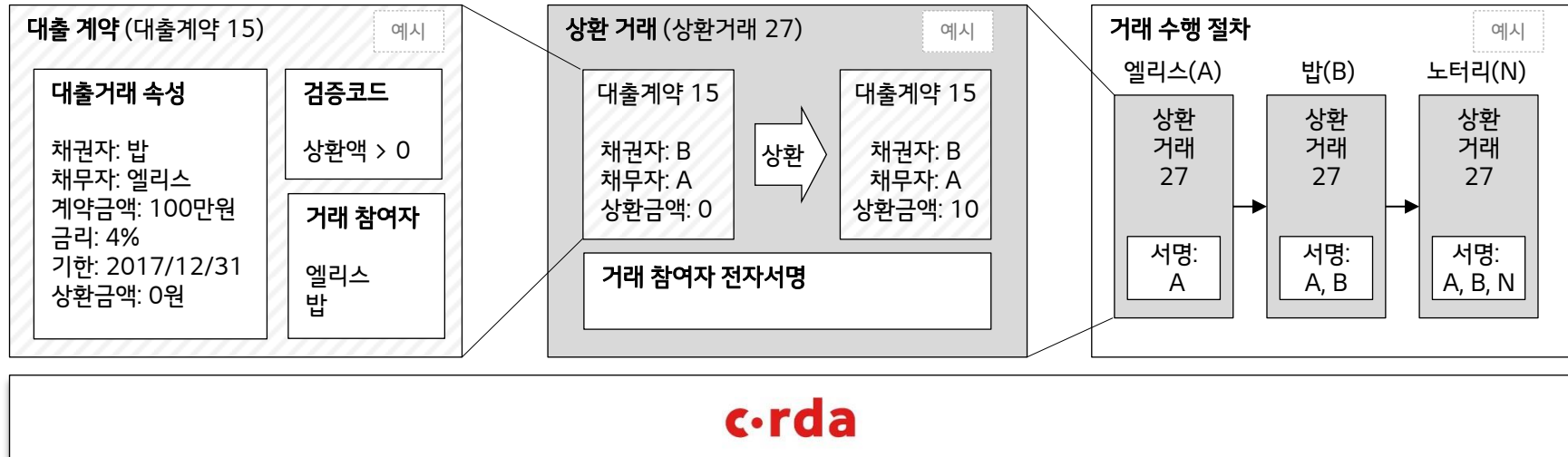
- 계약을 상태로 표현

거래(Transaction) 정의

- 계약상태의 변경을 거래로 정의

거래 절차(Flow) 정의

- 거래 처리를 위한 절차를 Flow로 정의



코다 네트워크는

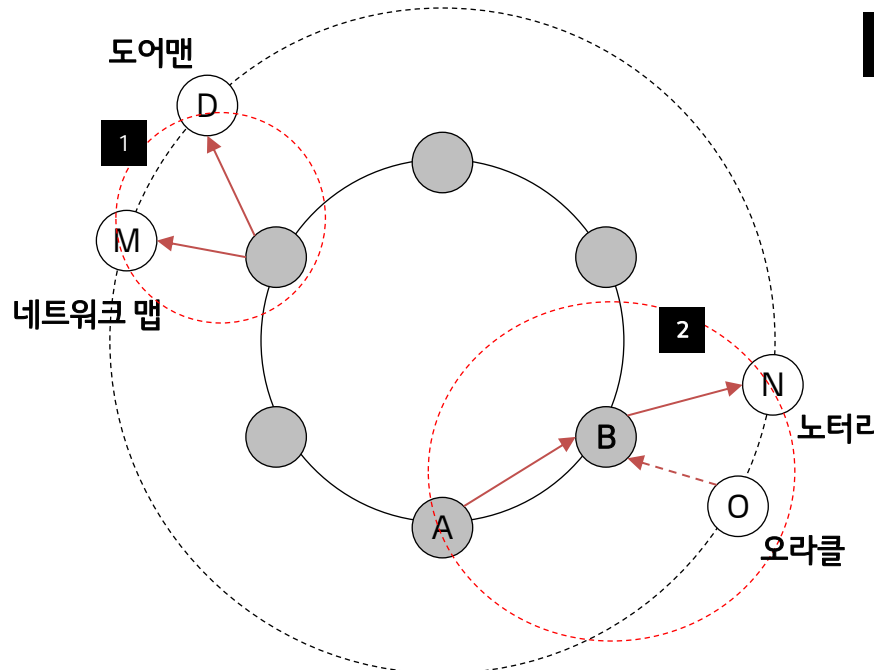
참여자 노드와 서비스 노드로 역할이 구분

등록 시 승인을 통해 네트워크에 참여한 이후 코덱(CorDapp)의 내용에 따라 거래를 처리

1 등록단계

허가를 통한 네트워크 참여

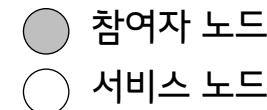
- 도어맨: 참여 허가 부여
- 네트워크 맵: 등록된 참여자 목록 보관



2 운영 단계

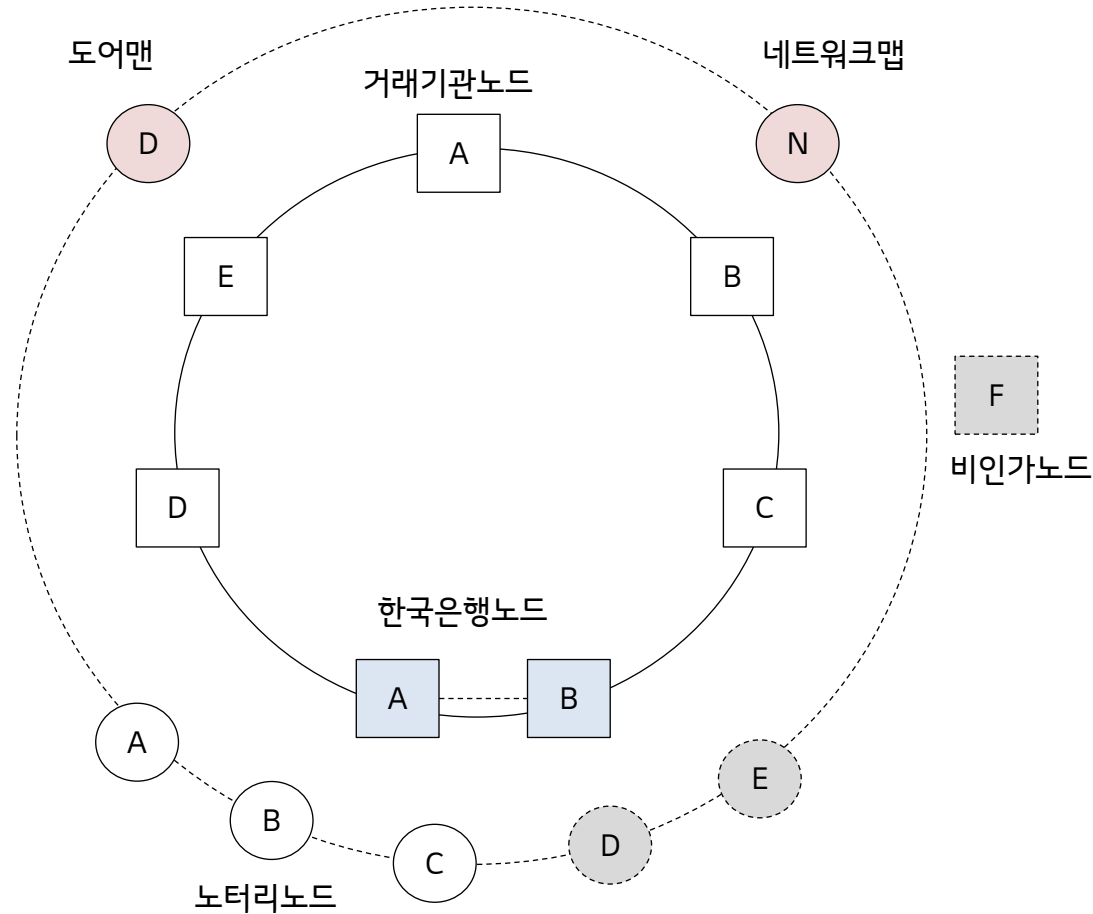
당사자간 거래 검증 후 노터리를 통해 확인, 필요 시 오라클을 통해 외부정보 활용

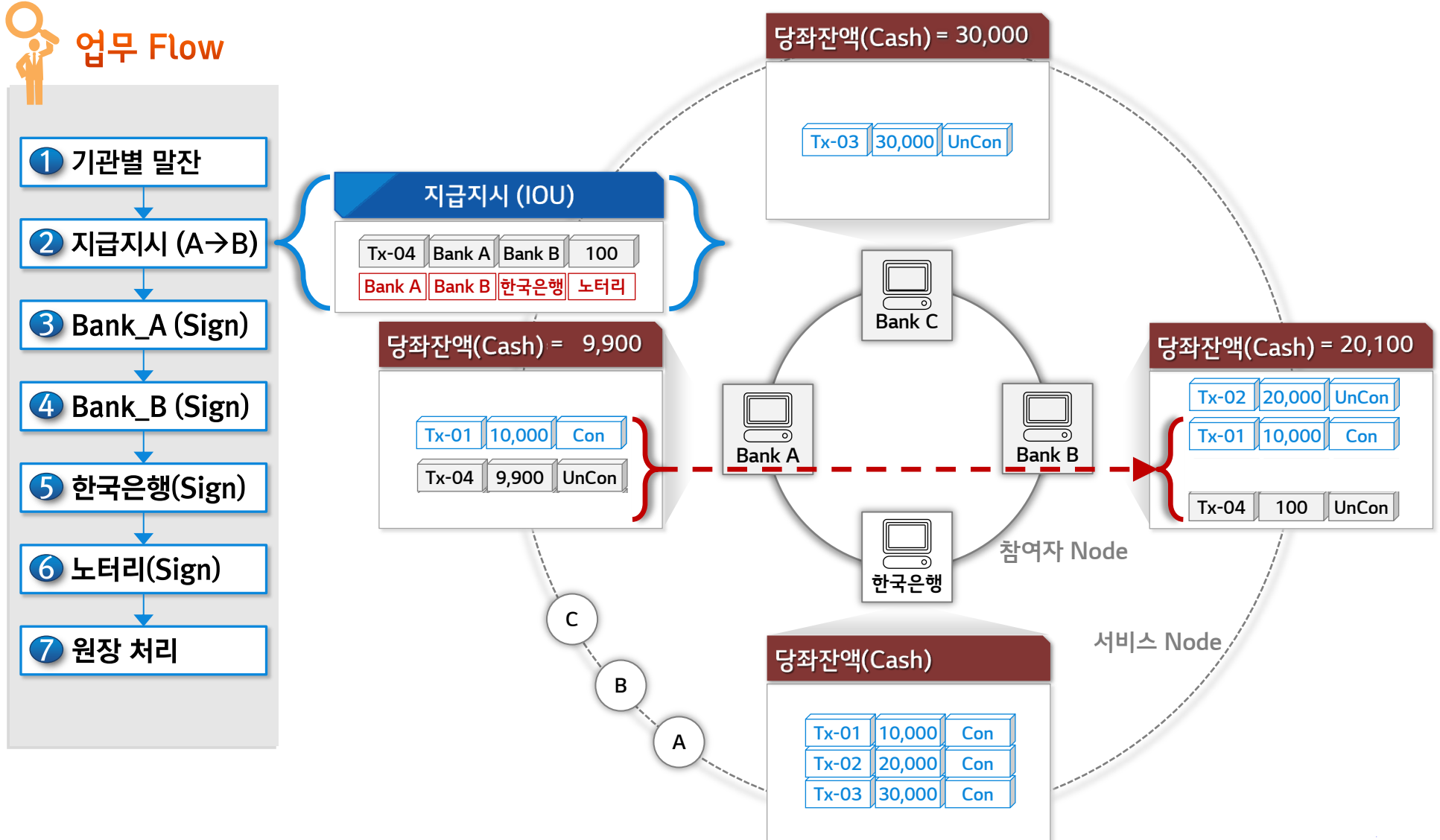
- 노터리: 거래 기록에 대한 확인
- 오라클: 신뢰할 수 있는 외부정보 제공



모의테스트 노드 : 12 개

참여자노드 7개 (거래기관노드 5개, 한국은행노드 2개), 서비스노드 5개 (도어맨, 네트워크맵, 노터리노드 3개)





| 구분 | 평가항목 | 테스트 케이스 | 상세 |
|----------|-----------|--------------------------|---|
| 기능성 테스트 | 효율성 스마트계약 | 기관별 말잔등록 | 한국은행에서 각 기관으로 전일말 잔액 발행의 정상 처리 여부 |
| | | 지급지시건 자금이체 (이체금액 ≤ 계좌잔액) | 이체기관의 계좌잔액이 충분할 경우 자금이체의 정상 처리 여부 |
| | | 지급지시건 자금이체 (이체금액 > 잔액) | 이체기관의 계좌잔액이 부족할 경우 대기 처리되는지 여부 |
| | | 총액지급지시 처리 | 이체기관 대기원장에 저장된 대기거래에 대한 5분 단위 건별 결제 처리 여부 |
| | | 다자간 결제 처리 | 한국은행 대기원장에 저장된 대기거래에 대한 30분 단위 다자간 결제 처리 여부 |
| | | 1일치 지급지시건의 처리 | 하루치 지급지시 (9,301건)가 정상적으로 처리되는지 여부 |
| 비기능성 테스트 | 회복성 | 거래노드 일부 비정상 | 수취기관 중 하나가 비정상 작동 중일 경우 이체기관에서의 이체 처리 여부 |
| | | 검증노드 일부 비정상 | 3개의 노터리 노드 중 일부가 비정상 작동 중일 경우 합의 처리 여부 |
| | | 감사노드 일부 비정상 | 한국은행 듀얼 노드 중 하나가 비정상 작동 중일 경우 지급지시 처리 여부 |
| | 보안성 확장성 | 비허가 노드의 지급지시 | 허가받지 않은 노드가 자금이체를 시도할 경우 처리 여부 |
| | 확장성 | 검증노드 추가 | 노터리 노드를 3개에서 5개로 증가시켰을 경우 처리 속도 |

은행간 자금이체 거래를 안전하고 효율적으로 구현하는지를 주요국 중앙은행의 분산원장기술 테스트 결과 등을 참고하여 평가 항목 4 가지 기준을 정의하고 평가함

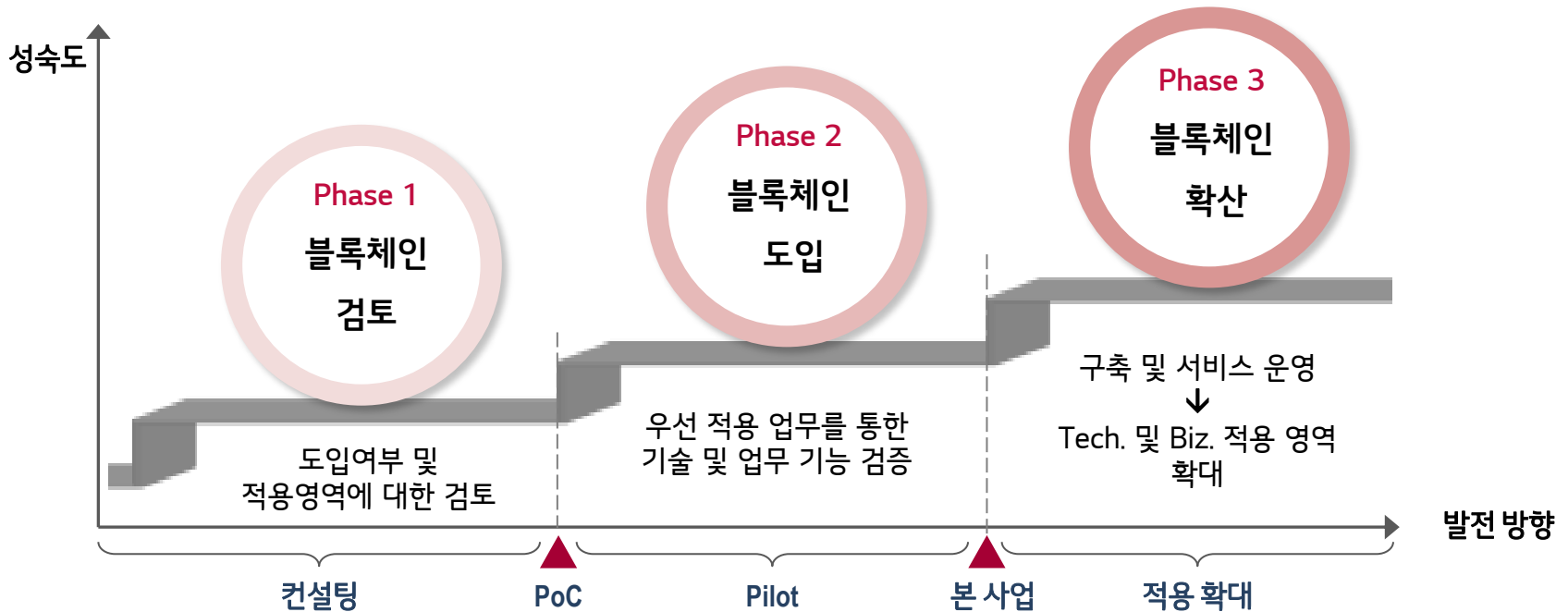
| 평가항목 | 평가 내용 | 평가 결과 |
|------|------------------------|--|
| 효율성 | 처리 속도 | 9,301건의 지급지시 처리에 현행(9시간)보다 2시간 33분이 추가로 소요 → 처리 속도는 현행 한은금융망이 우수 |
| 복원력 | 시스템 장애시 복구 가능성 여부 | 현 기술 수준에서 복원력 확인 불가 → 복원력은 한은금융망이 우수 |
| 보안성 | 권한이 없는 자의 시스템 접근 차단 여부 | 권한이 없는 자의 접근을 정상적으로 차단 → 모의시스템의 보안성은 상당히 양호 |
| 확장성 | 시스템 참가 금융기관의 확대 허용 | 참가 금융기관 확대에도 모의시스템 정상 작동 → 모의시스템의 확장성은 양호 |

평가 의견

1. 현재의 분산원장기술을 이용한 은행간 자금이체는 권한이 없는 자의 시스템 접근 차단, 참가기관의 확대 허용 등 보안성과 확장성 측면에서는 양호
2. 처리 속도가 지연 사유 : 기본적으로 다자간 결제의 경우, 분산원장기술의 거래기록 검증과정이 중앙 집중형 시스템에 비해 복잡
3. 장애 시 복구가 곤란한 사유 : 비밀유지를 위해 정보공유 범위를 제한한 데 주로 기인
4. OSS Corda의 한계로 처리 속도 지연, 장애시 복구 곤란 등 효율성과 복원력은 기존 방식에 못 미치는 것으로 나타났으나, '18년 하반기에 성능이 향상된 Corda Enterprise 버전 출시 예정

블록체인 도입을 위해서는 고객사의 상황에 맞는 “단계적이고 순차적인 접근 전략”이 필요함

단계별 적용 Approach



| | | | |
|-----------------------|---|---|--|
| <p>주요 TASK</p> | <ul style="list-style-type: none"> 적용 타당성 검토 우선 적용 영역 선정 적용 방안 및 로드맵 수립 | <ul style="list-style-type: none"> 블록체인 적용 및 기술 검증 업무 기능 구현에 대한 검증 확대 적용을 위한 표준 수립 | <ul style="list-style-type: none"> 블록체인 플랫폼 확대 적용 구축 및 서비스 운영 |
| | <p>고려사항</p> <ul style="list-style-type: none"> 비용대비 효율 요구사항, 업무 영향도, 실행가능성 | <ul style="list-style-type: none"> 속도, 성능, 안정성, 보안 기존 레가시 인프라와 연계 | <ul style="list-style-type: none"> 금융산업 규제 및 Compliance 다수 참여자 간 조율 및 합의 기술지원 체계 확보 |

감사합니다



안필용 책임
pyahn@lgcns.com