

# 블록체인기술 활용사례

자본시장을 중심으로

2016. 06. 01.

코스콤



# INDEX

I 개요

II 활용사례 소개 - PoC

III PoC Demo

IV 에필로그



# I 개요

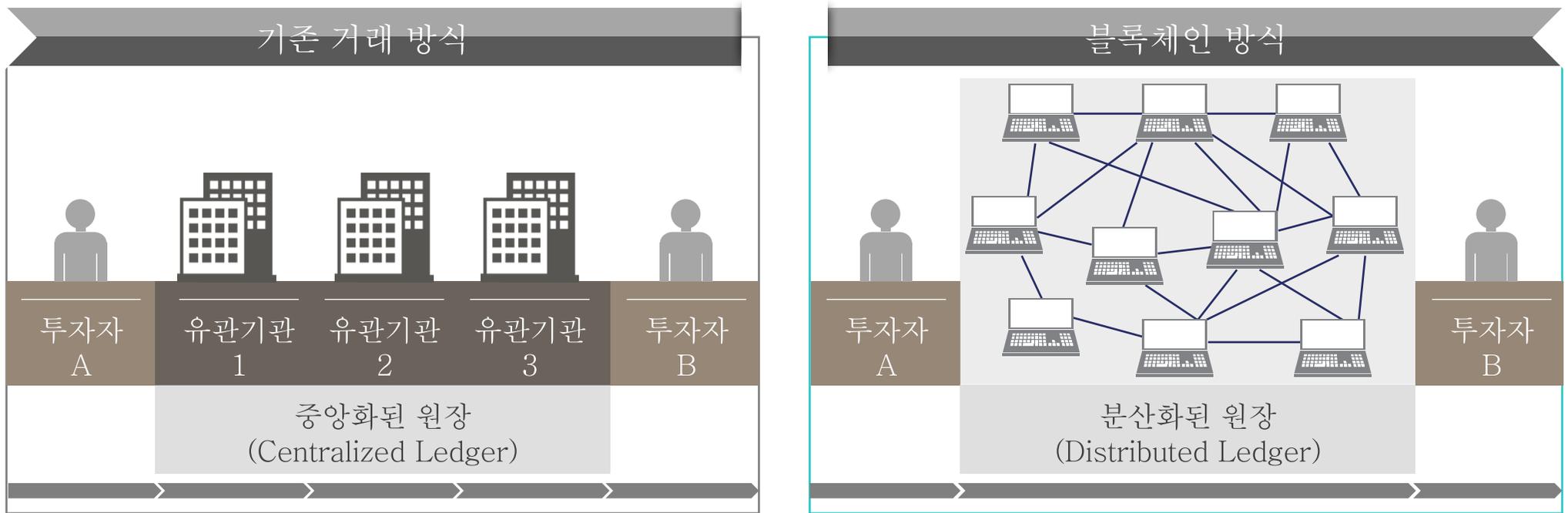
---



# 01 블록체인 개념

블록체인 : 비트코인의 핵심기술인 ‘공개 분산 장부 (Open Distributed Ledger)’

비트코인 : 글로벌 통용 ‘암호화 가상 화폐 (Crypto Currency)’



거래 내역 정보를 중앙 서버(Centralized Ledger) 기록하지 않음

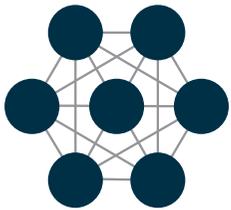


네트워크 참여자가 ‘공동’으로 거래정보를 검증·기록·보관



‘공인된 제3자’ 없이 거래 기록의 신뢰성을 확보할 수 있는 기술 구현 가능

분산성, 투명성, 보안성, 확장성 등 다양한 특징을 지님



분산성  
(Distributed, P2P-based)

- 공인된 제3자의 중개 없이 개인간 거래 가능
- 지급·결제 처리 등 소요 시간 단축 가능



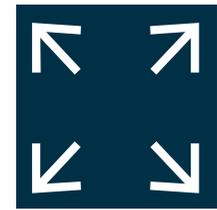
투명성  
(Transparent)

- 모든 거래 기록에 공개적 접근 가능
- 거래 양성화 및 규제 비용 절감



보안성  
(Secure)

- 참여자 간 정보 공동 소유로 해킹 가능성 차단
- 보안성이 탁월한 시스템 구축 가능

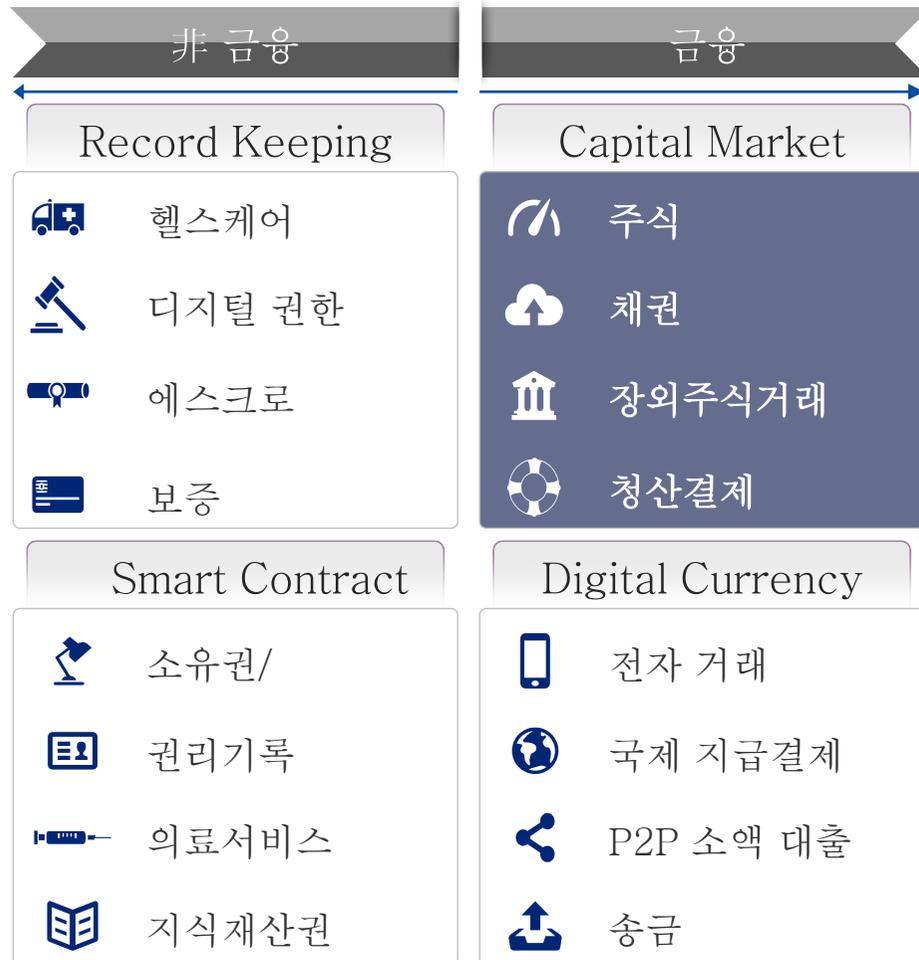


확장성  
(Scalable)

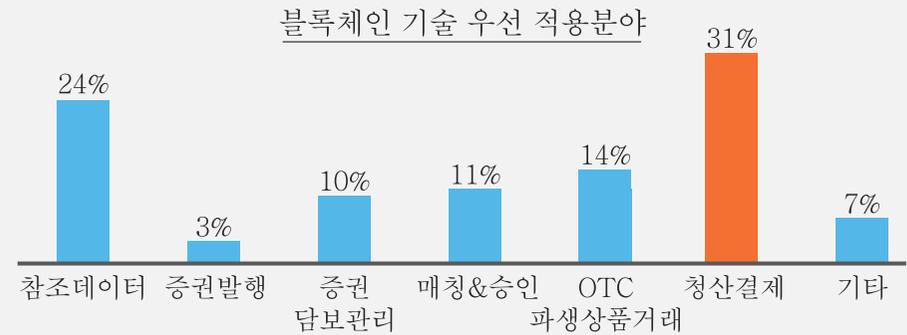
- 공개된 소스에 의해 쉽게 구축·연결·확장 가능
- 시스템 구축 시 유연성

# 03 블록체인 특징

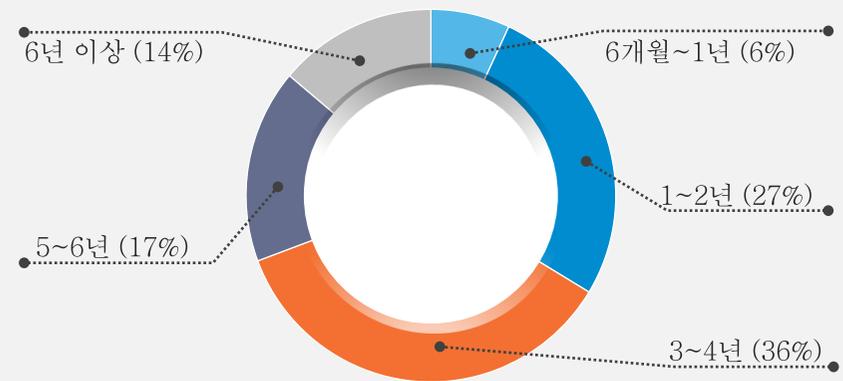
주식·채권 발행, 유통, 청산결제 등 적용 가능 → 위험·시간·비용 감소 예상



Q. 블록체인 기술 적용에 가장 우선적 적용 사례는?



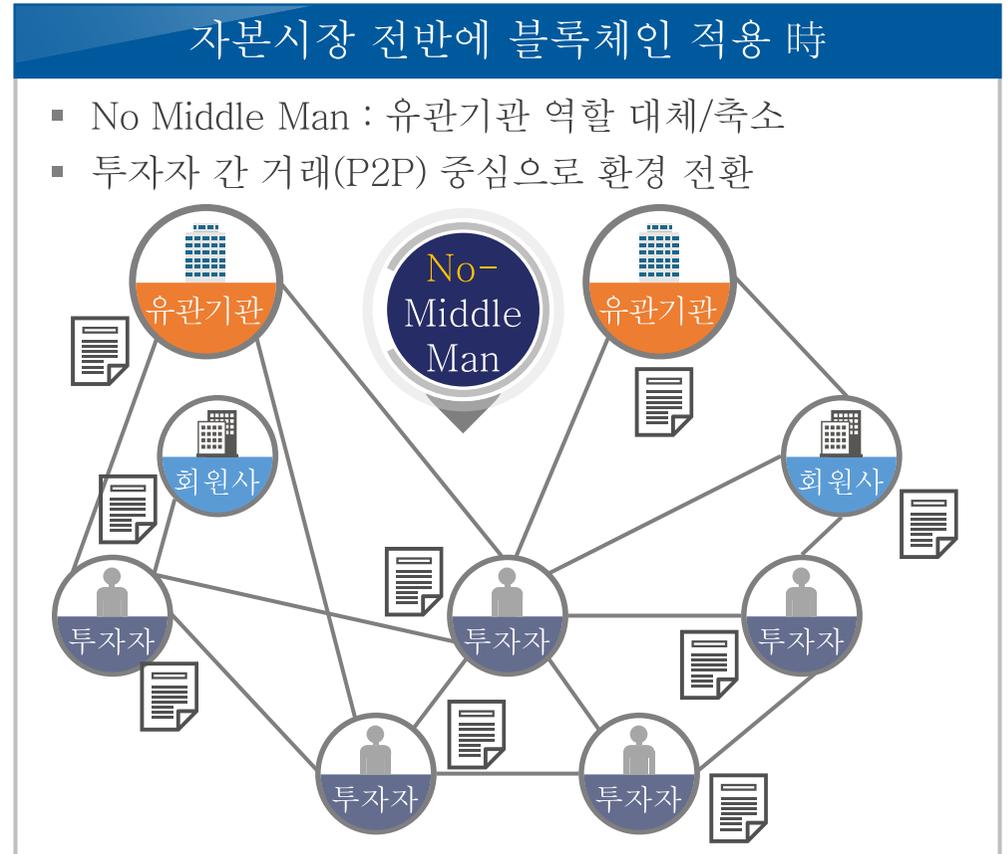
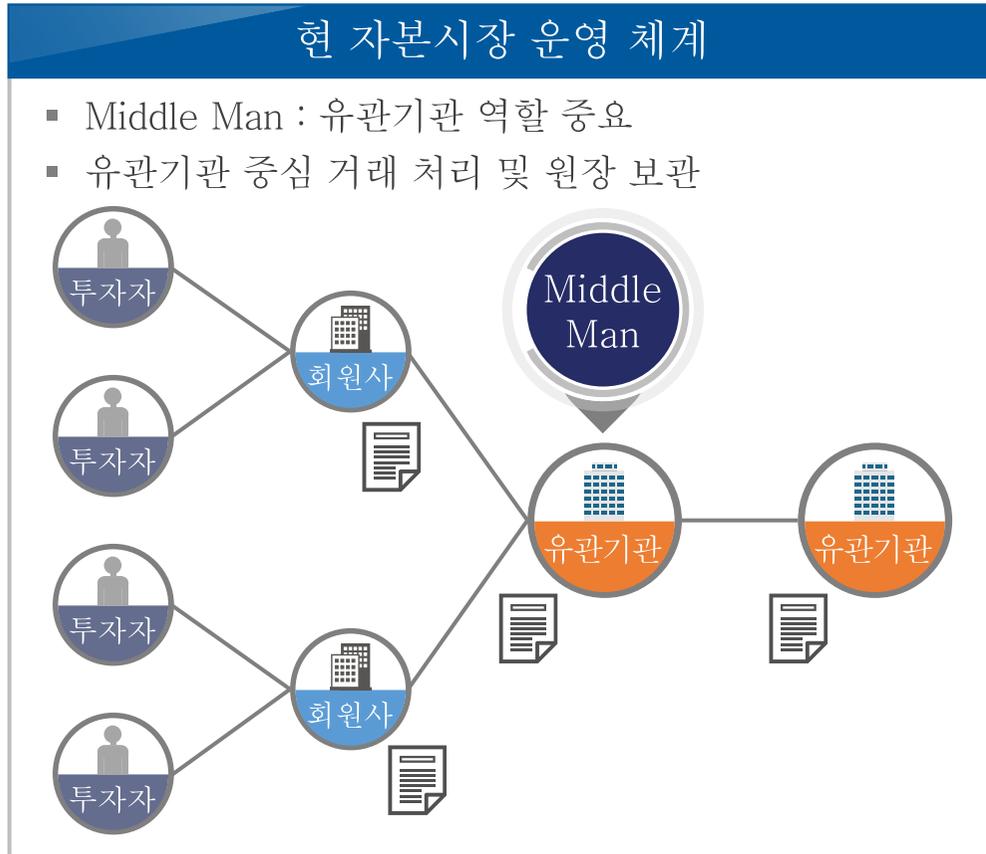
Q. 블록체인 기술이 실질적으로 적용되는 시점은?



■ <출처> 2016 블록체인 심포지엄 (2016.3, DTCC주관)  
 \* 거래소, 유관기관, 업체 대표 500명 대상 설문조사

# 04 블록체인 도입에 따른 자본시장 환경 변화(예상)

블록체인 본격 도입 시, 자본시장 전반(발행, 유통, 청산·결제 등)에 큰 변화 예상



적용 범위에 따라 제도·비즈니스·기술 전반에 걸친 변화 불가피 → 자본시장 내 유관기관의 역할 및 구도에도 큰 변화 예상 → 유관기관 및 정부/업계/학계 등 협업체계 마련 및 대응 필요  
 <출처> 자본시장 블록체인 협의체 (KRX)

## II 활용사례 소개 - PoC



자본시장에 적용할 수 있는 블록체인 기술을 검증하기 위한 PoC (Proof of Concept)

## ➔ 프로젝트 명

- 자본시장에 적용할 수 있는 블록체인 기술 검증 PoC

## ➔ 수행기간

- 2016년 4월 ~ 7월 (12주, 3개월), 스타트업(스케일체인)과 협력

## ➔ 프로젝트 목표

- 자본시장에 적용할 수 있는 블록체인 기술 검증
- 블록체인 활용 모델을 테스트 할 수 있는 개발·테스트 플랫폼 구축

## ➔ 수행범위

- 가상의 장외거래 시장(협외거래) 모델
- 블록체인 기술 검증을 위한 PoC (트랜잭션 처리건수 증가, 블록 생성 주기 단축 등)
- 블록체인 플랫폼 도입 및 개발환경 구축 (Permissioned Private Blockchain

Private Blockchain 플랫폼(비트코인 블록체인 기술 + OAP기반 자산발행)을 구축하고, 거래 대상 자산의 발행(등록) - 주문 - 협의 - 거래 - 거래확인 - 시장감시 순 과정을 테스트하고 검증함

## 1단계

### 비트코인 블록체인 기반

- 트랜잭션 전자서명 및 검증
- 비트코인 호환성
- Peer Discovery 및 메시지 교환
- 스크립트(P2PKH, P2PK, P2SH)
- 블록, 트랜잭션, 지갑 관리



## 2단계

### Open Assets Protocol 기반

- Multi-Asset, Multi-Sign
- OAP기반 자산발행, 이체
- 블록 크기 확장
- 블록 생성 주기 조정
- 자가치유 알고리즘
- 메시지 암호화



## 3단계

### 자본시장 모델 기반

- 트랜잭션 1000건/초
- 블록 생성 주기 1초 이내
- 데이터 분할 저장
- 다수결 블록 검증



## 자본시장 업무 특성을 고려한 다양한 테스트 시나리오 적용

### 성능 / 용량

- 초당 1건부터 1000건까지 거래 트랜잭션을 발생시켜 건별 처리시간 측정 (성능)
- 초당 1000건 처리를 지속하여 블록체인 용량 한계치 측정 (용량)

### 가용성

- 전체 노드의 50% 미만 장애 시 대책
- 전체 노드의 50% 이상 장애 시 대책
- 프로세스, 네트워크, 서버 장애



PoC  
테스트 항목

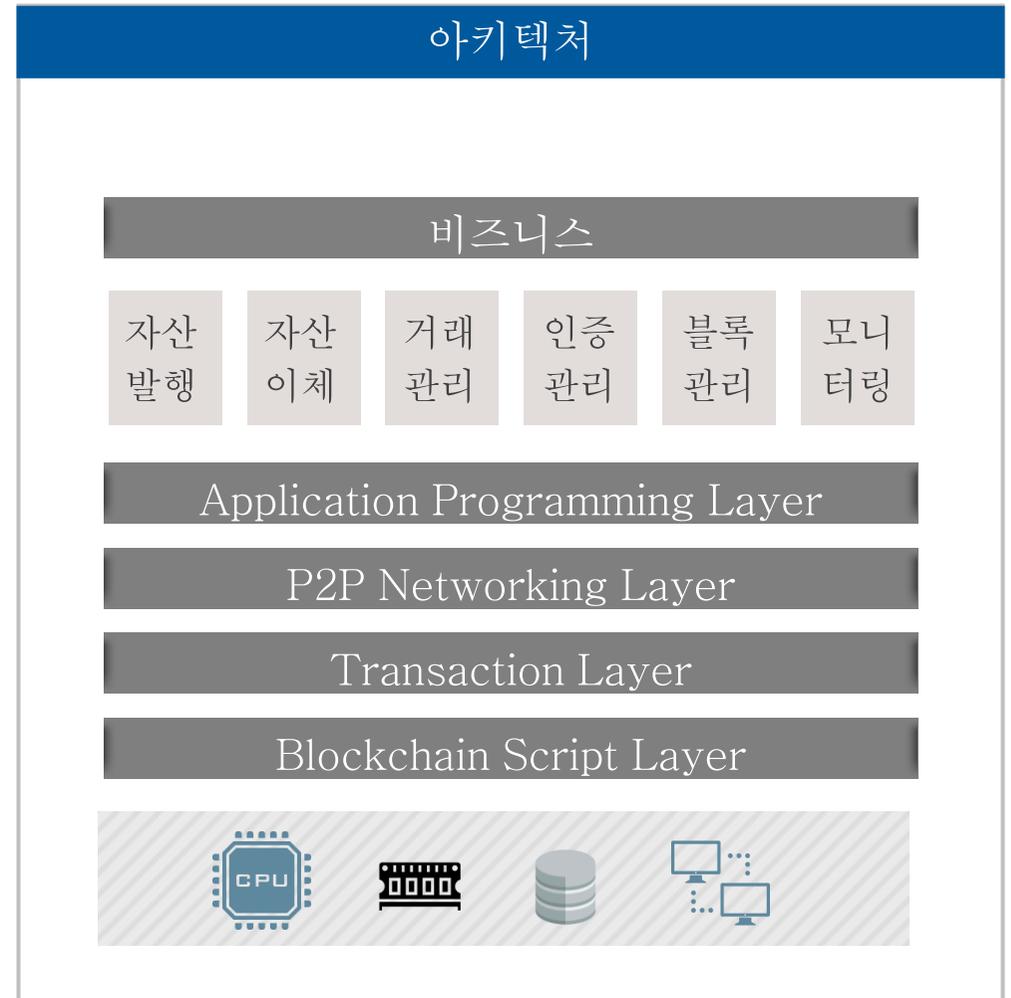
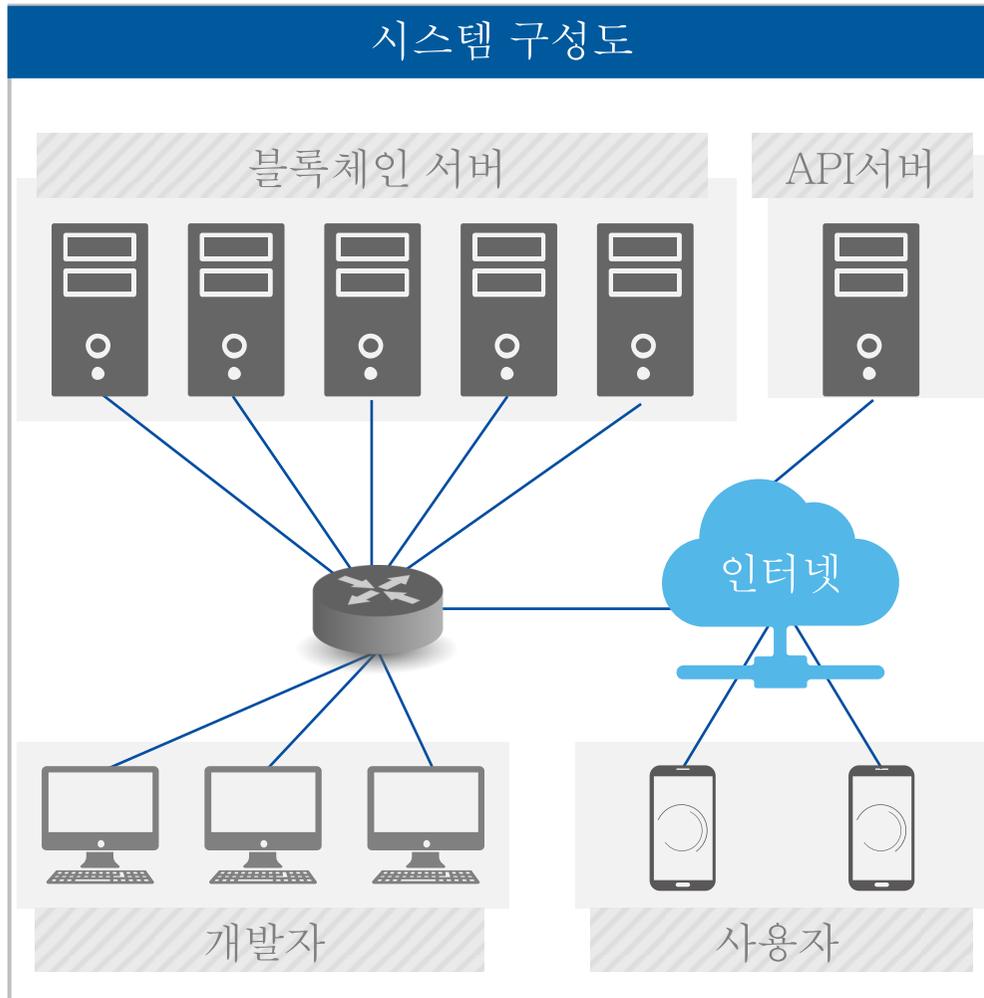
### 보안

- 블록체인 위·변조 시도 및 상태 확인 (위·변조 방지)
- 블록체인 메시지 암호화 확인 (정보유출 방지)

### 추가 기능

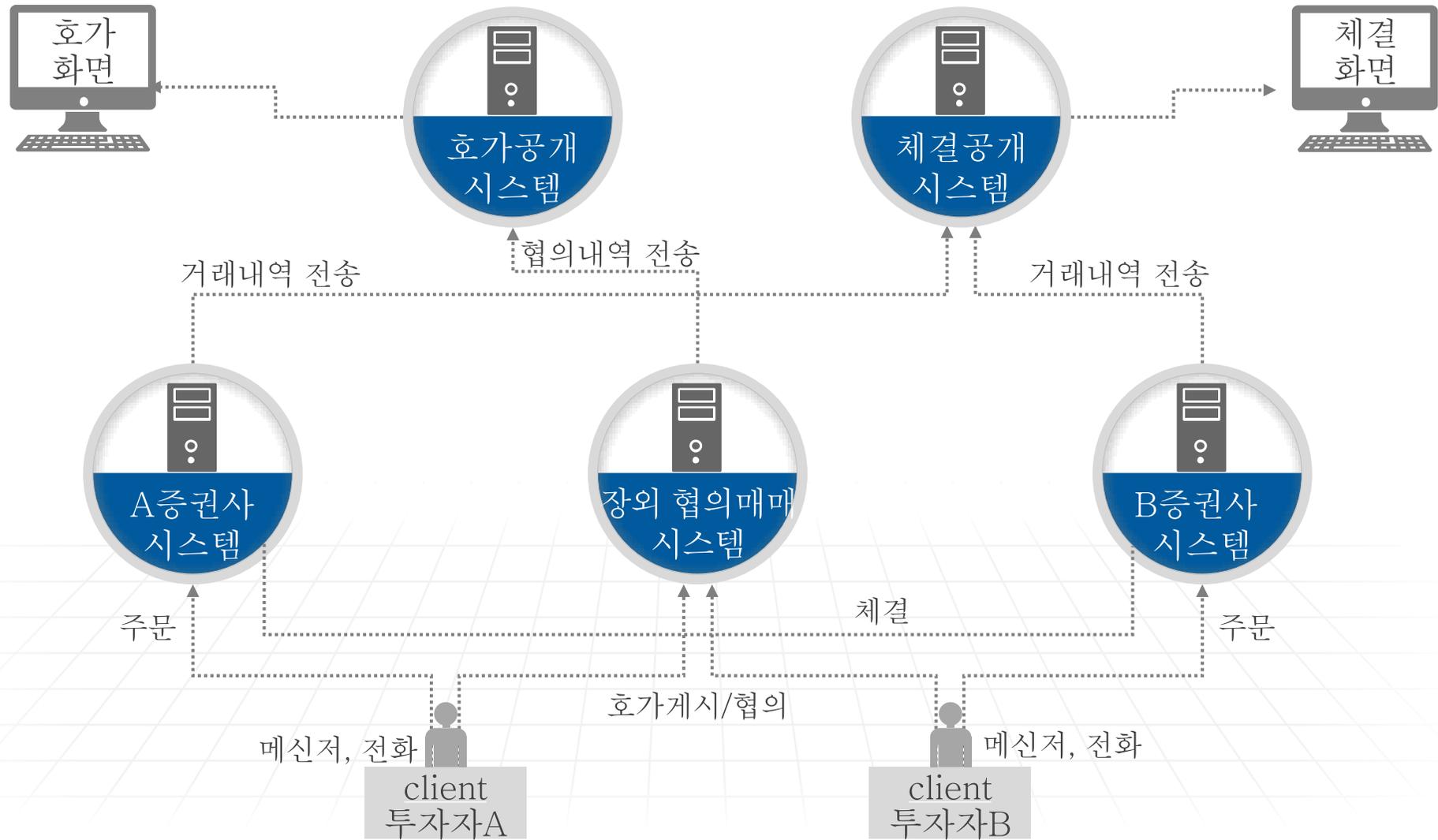
- 블록 사이즈 확대 (다양한 자산)
- 데이터 분할 분산 저장 (확장성)
- Legacy 시스템과 연계 (연계성)

5대의 블록체인 서버를 사용하여 Private Blockchain 플랫폼을 구성



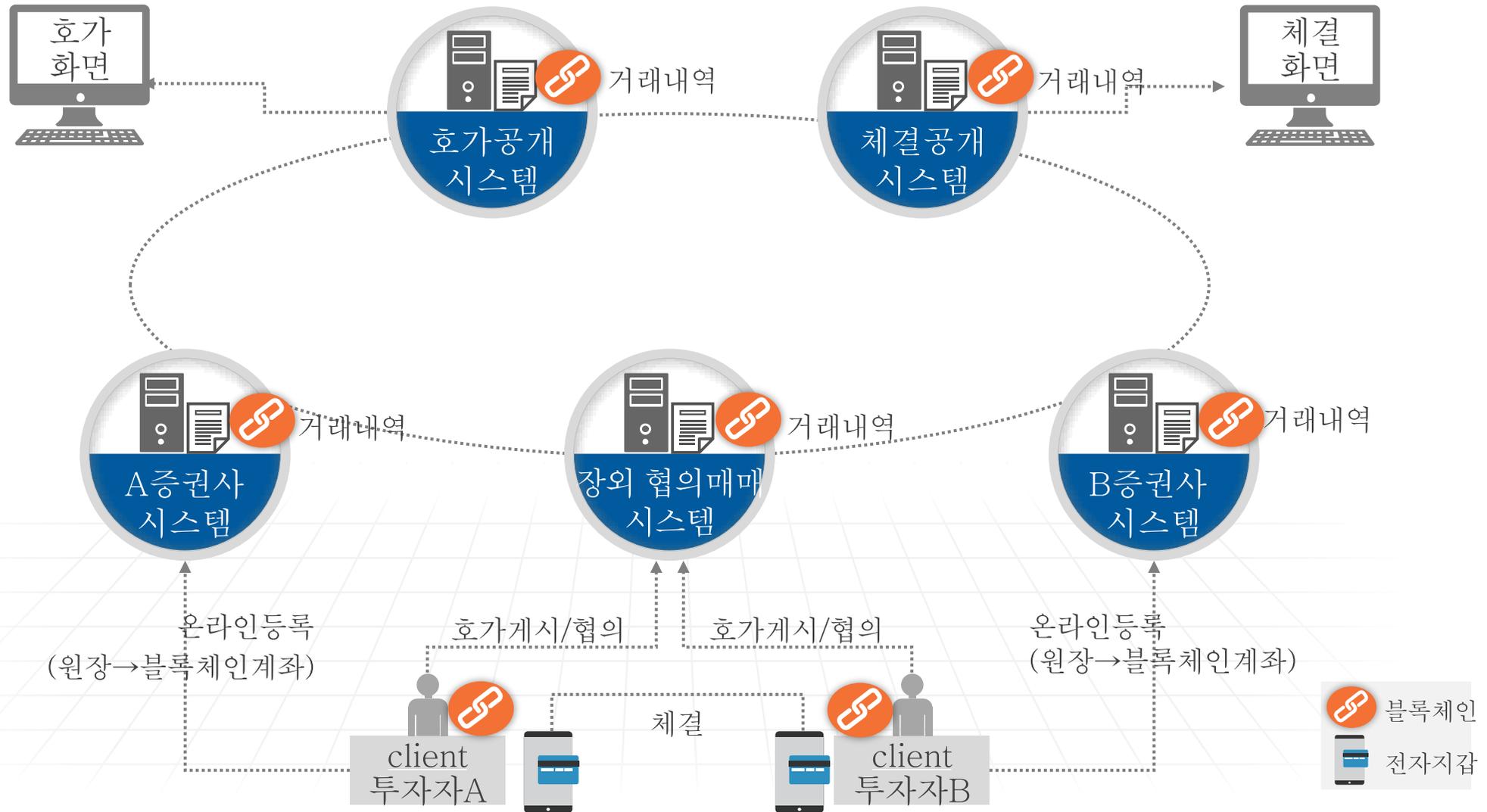
# 05 PoC 대상 업무 (As-is)

현재 중앙 집중 방식으로 구현되어 있는 장외 협의매매 시장을 PoC 대상으로 함



# 05 PoC 대상 업무 (To-be)

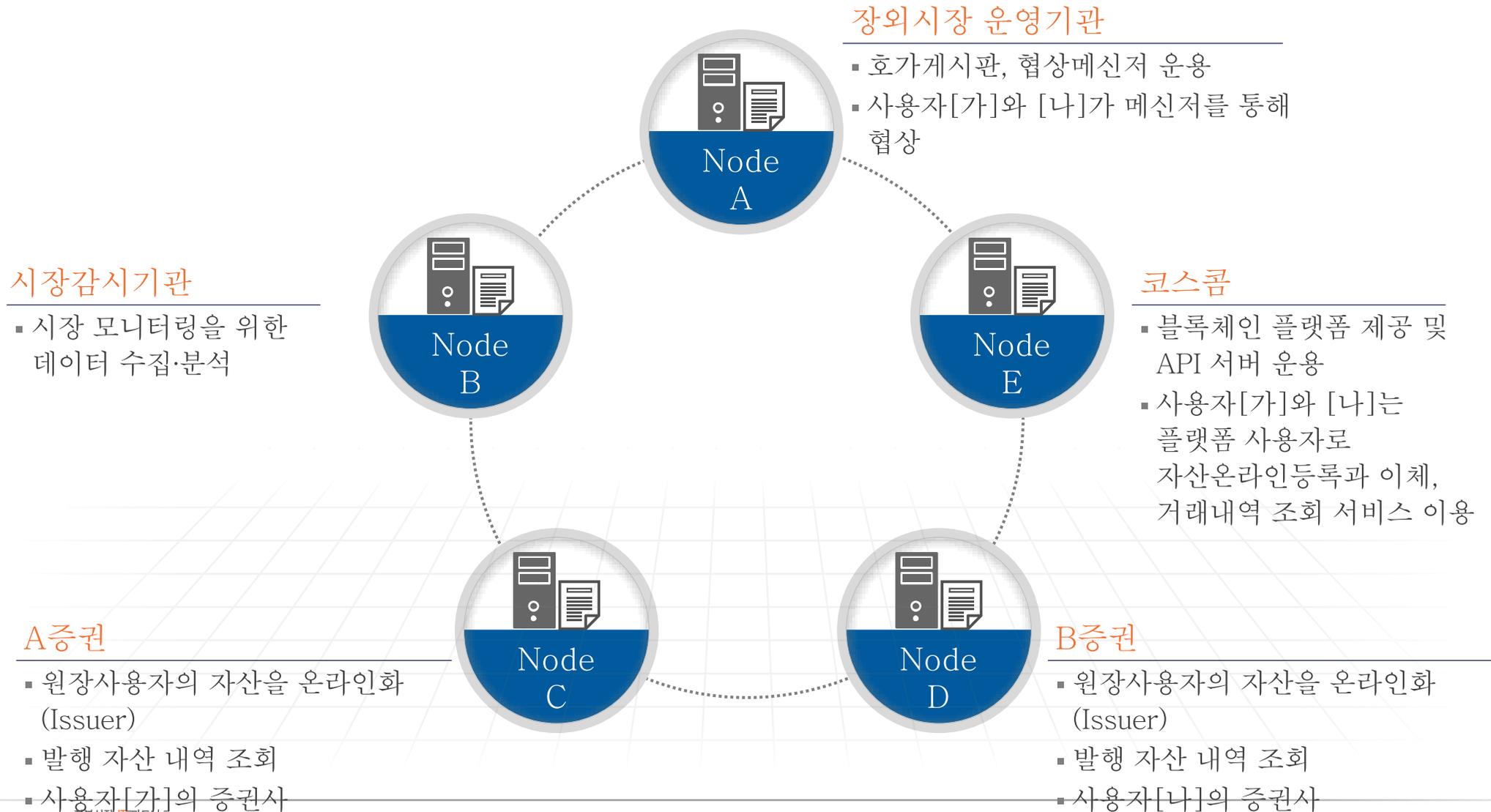
장외 협의매매 시장을 블록체인 기반 분산원장 방식으로 개발 중



# III PoC Demo



본 PoC에서는 블록체인 노드(서버)를 5대로 구성하고, 증권사를 포함한 자본시장 운영에 관련된 유관기관이 참여하는 과정을 검증함



### 장외시장 운영기관

- 호가계시판, 협상메신저 운용
- 사용자[가]와 [나]가 메신저를 통해 협상

### 시장감시기관

- 시장 모니터링을 위한 데이터 수집·분석

### 코스콤

- 블록체인 플랫폼 제공 및 API 서버 운용
- 사용자[가]와 [나]는 플랫폼 사용자로 자산온라인등록과 이체, 거래내역 조회 서비스 이용

### A증권

- 원장사용자의 자산을 온라인화 (Issuer)
- 발행 자산 내역 조회
- 사용자[가]의 증권사

### B증권

- 원장사용자의 자산을 온라인화 (Issuer)
- 발행 자산 내역 조회
- 사용자[나]의 증권사

# 02 상세 업무 처리 흐름도

등록·게시    거래참여    협의    거래    거래확인    시장감시

## ❖ 게시판

시간	종목명	만기일	구분	단가	수량	게시자	상태	거래참여
10:25	국민주택 2013-02	2018-02-28	매도	11578.50	100	홍길동	확정	거래참여
09:24	통안0146-1804-02	2018-04-02	매수	10016.69	150	박서방	대기	거래참여
09:17	국고02750-1709(12-4)	2017-09-10	매도	10179.33	20	정도전	대기	거래참여

**메신저**  
 게시자A : 반갑습니다.  
 참여자B : 네~ 이율 0.001만 내려주시면 바로 삽니다.  
 게시자A : ...

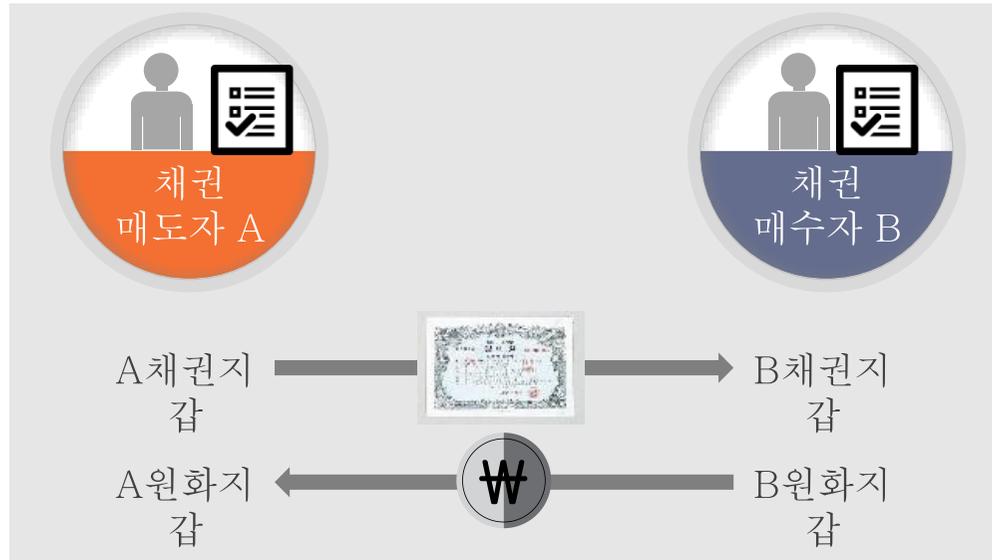
참여자정보  
게시자A  
참여자B

---

종목 **국민주택** 단가 **11578.49** 수량 **100** 협상확정

나의 잔고 **조회** 국민주택 2013-02 100주  
 월화 2,000,000원

**보내기**



**메신저**  
 게시자A : 반갑습니다.  
 참여자B : 네~ 이율 0.001만 내려주시면 바로 삽니다.  
 게시자A : ...

참여자정보  
게시자A  
참여자B

---

종목 **국민주택** 단가 **11578.49** 수량 **100** 협상확정

나의 잔고 **조회** 국민주택 2013-02 100주  
 월화 2,000,000원

**보내기**

# Demo (동영상)

# 04 PoC 의미 - 자본시장에 프라이빗 블록체인 검증



구분	비트코인의 경우	PoC의 경우
데이터(블록) 크기	블록 1MB 초당 7건 10분 블록 생성 주기	블록 1MB ~ 2MB 초당 1000건 1초 이내 블록 생성 주기
거래 참여자	모든 사람	Private 블록체인 참여 기관
거래 기록 열람자	모든 사람	허가된 열람자
거래 승인 권한	채굴자	허가된 참여 기관
블록 생성 권한	채굴자 경쟁	허가된 참여 기관
블록 생성 방식	PoW, 긴 체인 우위	룰 기반
보상	블록 내 수수료 + 25BTC(채굴)	수수료 없음
비용	사용된 컴퓨팅 파워 및 전력의 낭비	컴퓨팅 파워 최소한 사용
화폐/자산	비트코인(BTC)	다양한 금융 자산
컨센서스 방식	긴 체인 우위	긴 체인 우위 + 다수결 블록 검증
룰 개정 방식	커뮤니티의 동의	Private 블록체인 참여 기관의 동의



# IV 에필로그



# 01 블록체인과 관련된 고민거리(해결해 나가야 할 과제)

PoC를 통한 기술 검증과 더불어 블록체인의 다양한 걸림돌(이슈)이 해결되어야 함

## 01 경제적 측면

- 비용대비 효과 검증 사례 부족
- 위·변조 방지 외 정보유출 방지를 위해 비용은 계속 필요
- 블록체인 참여기관의 수익모델 발굴 필요

## 기술적 측면 02

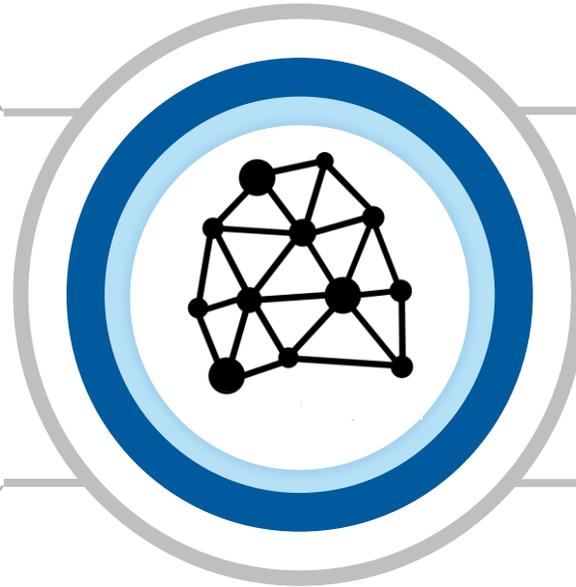
- 현 아키텍처로는 다양한 신종 파생상품 처리, 종목 정보 수용 한계
- 거래 유형별 적용 가능 범위의 한계(예: 협의매매 O, 경쟁매매 ?)
- 업무별 다양한 예외 케이스 대처방안 확보 필요 (예 : 취소/정정 주문)

## 03 금융회사 측면

- 분산 저장에 따른 거래 내역 노출 및 접근 권한 이슈
- 기존 Legacy 시스템과의 연계 방안
- 유지보수 용이성, 사용 편의성 확보 중요

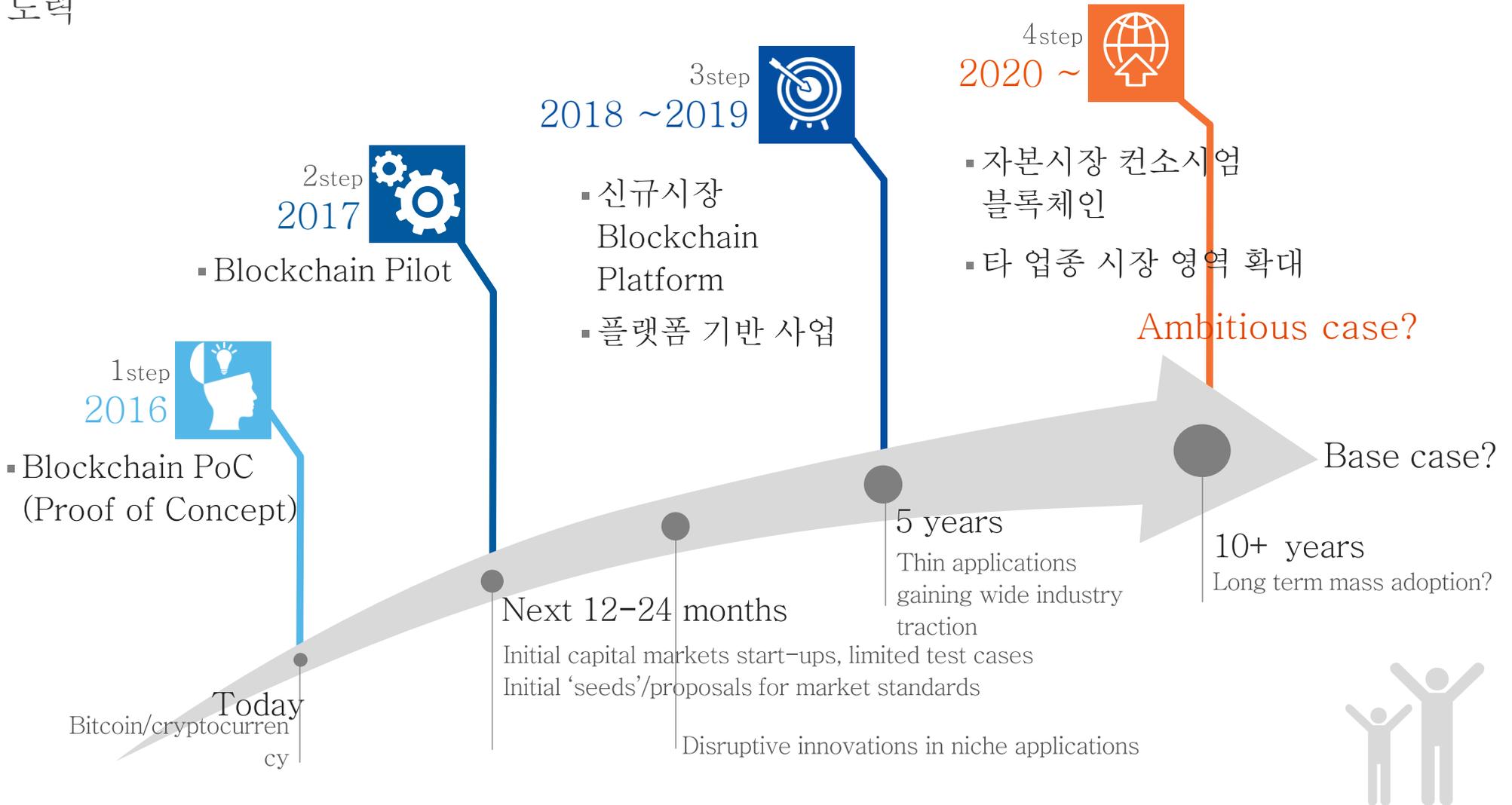
## 규제 관련 측면 04

- 분산 원장에 대한 금융 분야 규제 (개인정보보호법, 전자금융거래법, 신용정보법 등) 검토 필요
- 전자증권 발행, 유통, 거래 등 라이프사이클 관리에 관한 검토 필요
- T+2 결제일이 T+0로 될 것인가?  
(T+0 호용성)



# 02 코스콤 블록체인 Roadmap

자본시장 구성원이 모두 참여할 수 있는 컨소시엄 블록체인 기술 개발을 위하여 지속적으로 노력



<출처> Blockchain in Capital Market, Euroclear (2016)

