



하이퍼레저 패브릭 HandOn Overview

KLAB Software Engineer
김형석

Contents

01 Lab Overview

02 블록체인을 이용한 통합인증 UseCase 소개

03 Lab 기능설명



01. Lab Overview

- Lab 목표/주제 소개
- Lab 필요한 Tools/Software
- Lab 사전 준비 사항



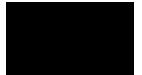
- Lab 목표/주제 소개

- Hyperledger Fabric v1.4를 이용한 네트워크 구축
- IBM Blockchain Platform을 이용한 개발 속도 향상
- Chaincode(SmartContract) 개발/테스트 가이드(golang)
- 그룹통합인증 실습(DB / Blockchain)

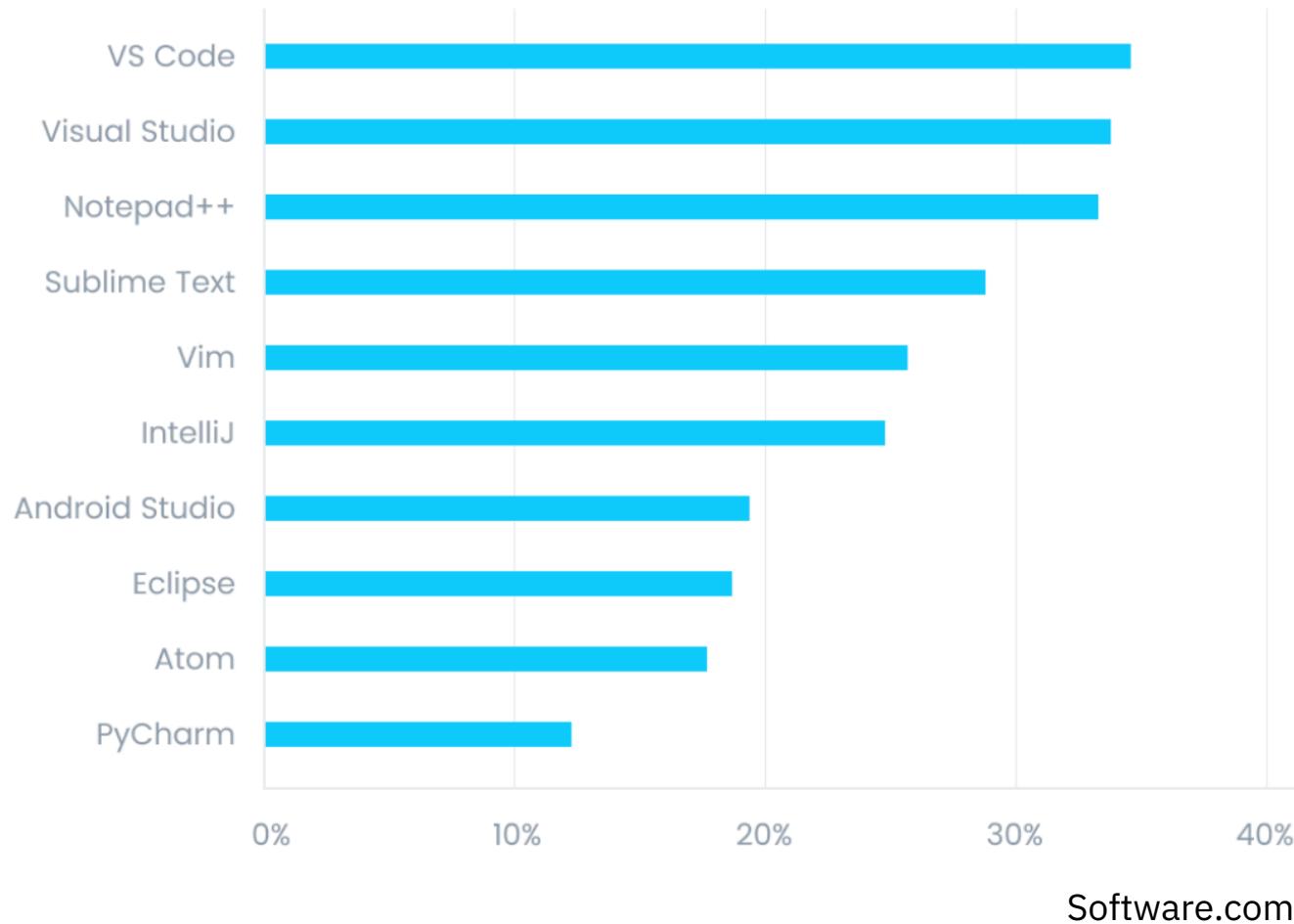


- Lab 필요한 Tools/Software

- IDE - Vscode(Required), IntelliJ(Optional), Eclipse(Optional)
- Git – SourceTree(Optional)
- VirtualBox(ubuntu), Docker, maven
- Golang , JavaSDK v1.8, SpringBoot, MySQL
- SSH Program : putty, iterm2



[별첨] 2019 Most Popular Developer Environments

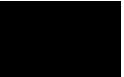


Software.com



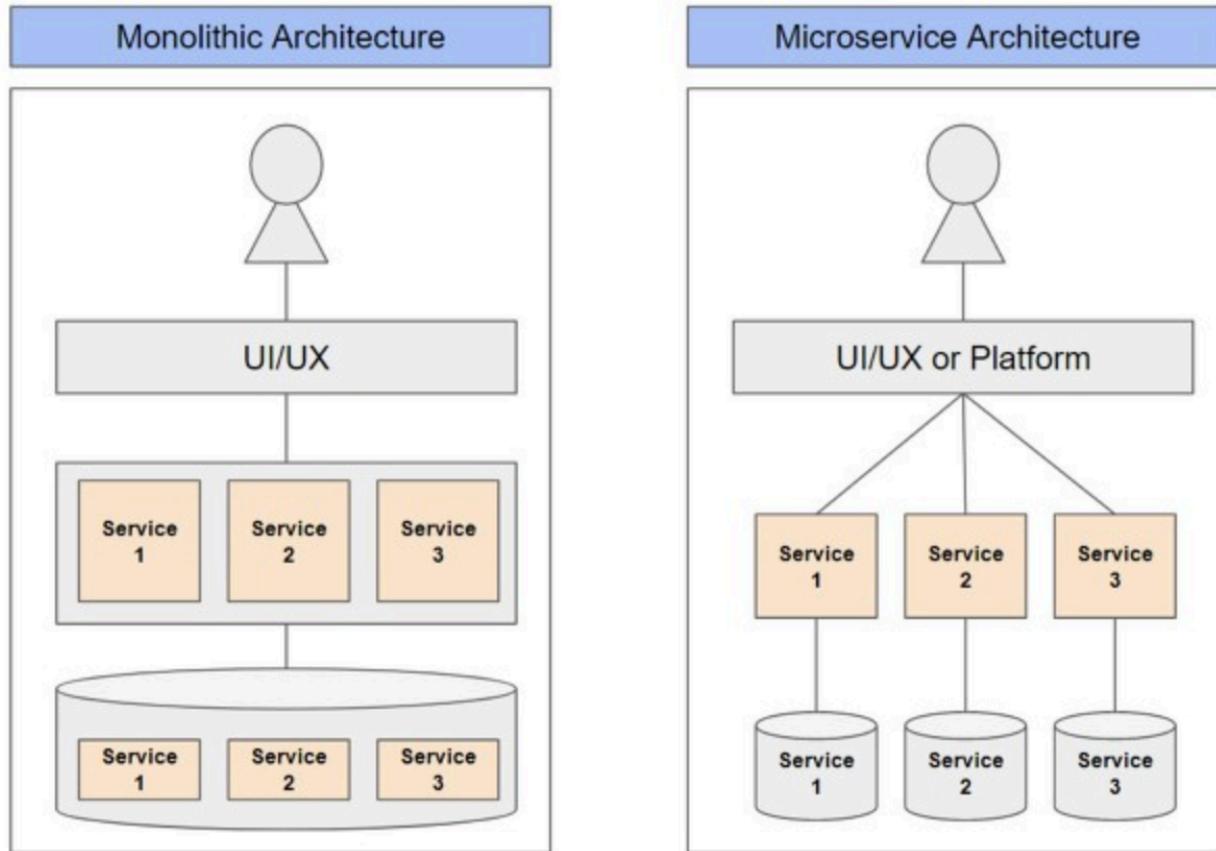
[별첨] Why SpringBoot?

- 기존 Java 환경에 대한 고려
- 코드 재사용으로 MSA 구현 가능
- Low Learning Curve
- Tomcat 내장 별도 Deploy과정 필요 없음
- Etc...



[별첨] MSA(Microservice Architecture)

<https://yjc.tistory.com/309>



〈Monolithic 방식과 MSA 방식 비교〉



- Lab 사전 준비 사항

- 개별 노트북 준비
- GitHub 계정 생성
(<https://github.com/>)



02. 블록체인을 이용한 통합인증 UseCase 소개

- Why 인증?
- 은행연합회(BankSign)
- 금융투자협회(Chain ID)
- Kakao(인증서)
- SKT(블록체인 기반 모바일 신분증)



Why 인증?

2010년 7월19일부터 2017년 12월11일까지 비트코인 가격

자료: 빗썸 그래프

15,000달러

10,000달러

5000달러

0달러

2013년 11월25일
979.45달러

2010년 7월19일
0.06달러

2017년 12월11일
1만5823.68달러

2017년 10월9일
5277.83달러

2017년 2월6일
1017.58달러

2012년

2014년

2016년



Why 인증?



Why 인증?

◇ 공인인증서 우월 지위 폐지…인증수단 다양화

과기정통부는 획일화된 인증시장을 혁신하고, 신기술 도입을 활성화하기 위해 공인인증서 제도를 폐지하기로 했다.

관련 법에 명시된 공인인증서의 우월적 지위를 폐지해 사설인증서와 마찬가지로 다양한 인증수단의 하나로 활용하게 한다는 계획이다.

이를 위해 전자상거래법과 전자서명법 등 공인인증서 사용을 의무화한 법령 개정을 순차적으로 추진할 방침이다. 관계 부처와 협의를 마친 10개 법령은 상반기 중 국회에 개정안을 제출하고, 하반기에는 전자상거래법과 나머지 20개 법령을 제출할 예정이다.

공인인증서의 법적 효력이 사라지더라도 본인 확인이 필요한 영역에서는 대안으로 전자서명을 활용하도록 할 방침이다. 이와 관련해 3월 중 전자서명의 안전한 관리와 평가 체계에 관한 세부 방침을 마련한다.

- 2018년 1월 / 한겨레



Why 인증?

영국은행 수석 경제학자 “비트코인, 20~30년 후 현금 대체 충분히 가능 ...

<https://blockinpress.com/archives/17232> ▼

7일 전 - 영국 중앙은행의 앤디 G 헐데인(Andrew G Haldane) 수석 이코노미스트가 “비트코인은 현금을 대체할 가능성 있다”고 언급했다. 18일(현지시간) ...

한은 “암호자산, 화폐 대체할 가능성 극히 낮다” - 매일경제

<https://www.mk.co.kr/news/economy/view/2018/07/426488/> ▼

2018. 7. 6. - 국내법상 상품으로 해석 한국은행은 암호자산이 법정화폐와 경쟁하며 ... 지급수단으로서 기능을 강조하는 비트코인 등 1세대 암호자산의 지속 ...

미국 연방 준비 제도 이사회는 암호화폐를 준비하고 있을까 - 코인투데이

cointoday.co.kr › INSIGHT ▼

2018. 12. 31. - 세인트루이스 연방 준비은행의 연구원인 알렉산더 베렌센(Aleksander Berentsen)과 그의 동료 파비안 쉬어(Fabian Schar)는 중앙은행이 자신의 ...



1. 은행연합회(BankSign)



뱅크사인(BankSign)이란?

뱅크사인이란 은행권이 공동으로 도입한 새로운 인증서비스입니다.

뱅크사인은 공개키(PKI) 기반의 인증 기술, 블록체인 기술, 스마트폰 기술 등 첨단기술의 융합을 통해 전자금융거래를 더 안전하고 편리하게 해 줄 것입니다.



1. 은행연합회(BankSign)

금융기관	PC	앱	비고
국민	○	△	모바일(앱)은 KB스타뱅크 미니만 이용 가능. PC뱅킹에서 사용하려면 스타뱅크 미니에서 등록을 해야한다.
신한		○	2019년 상반기 PC 예정
우리	○	○	
하나	○	○	
SC제일	○	○	
우체국		X	
기업	○	○	
농협		○	2019년 상반기 PC 예정
수협	○		
대구			2019년 상반기 PC 예정
부산			2019년 상반기 PC 예정
제주			2019년 상반기 PC 예정
전북	○		
광주			2019년 상반기 PC 예정
경남	○		
케이	○	○	
산업			2019년 상반기 PC/앱 동시 예정
씨티	X	X	추후 참여를 검토한다고 한다.
카카오	X	X	초기에 지원 예정이였으나, 자체 인증서가 있기에 도입이 불필요하다고 간주하여 아직은 검토중이라고 한다.



2. 금융투자협회(ChainID)

App Store Preview

This app is only available on the App Store for iOS devices.

CHAIN ID - 금융투자업권 블록체인 공동인증 [4+]
ICONLOOP Inc.

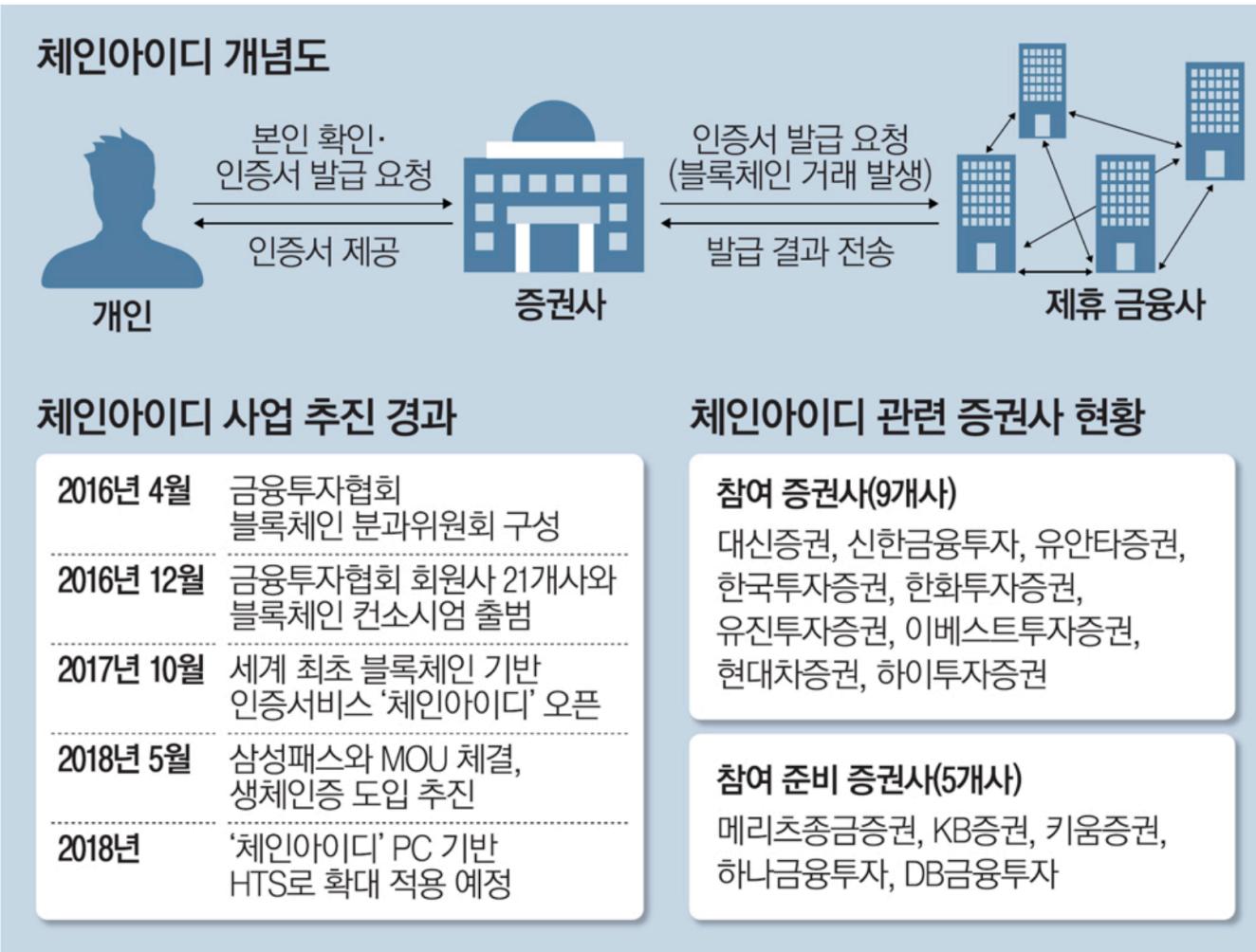
Free

iPhone Screenshots

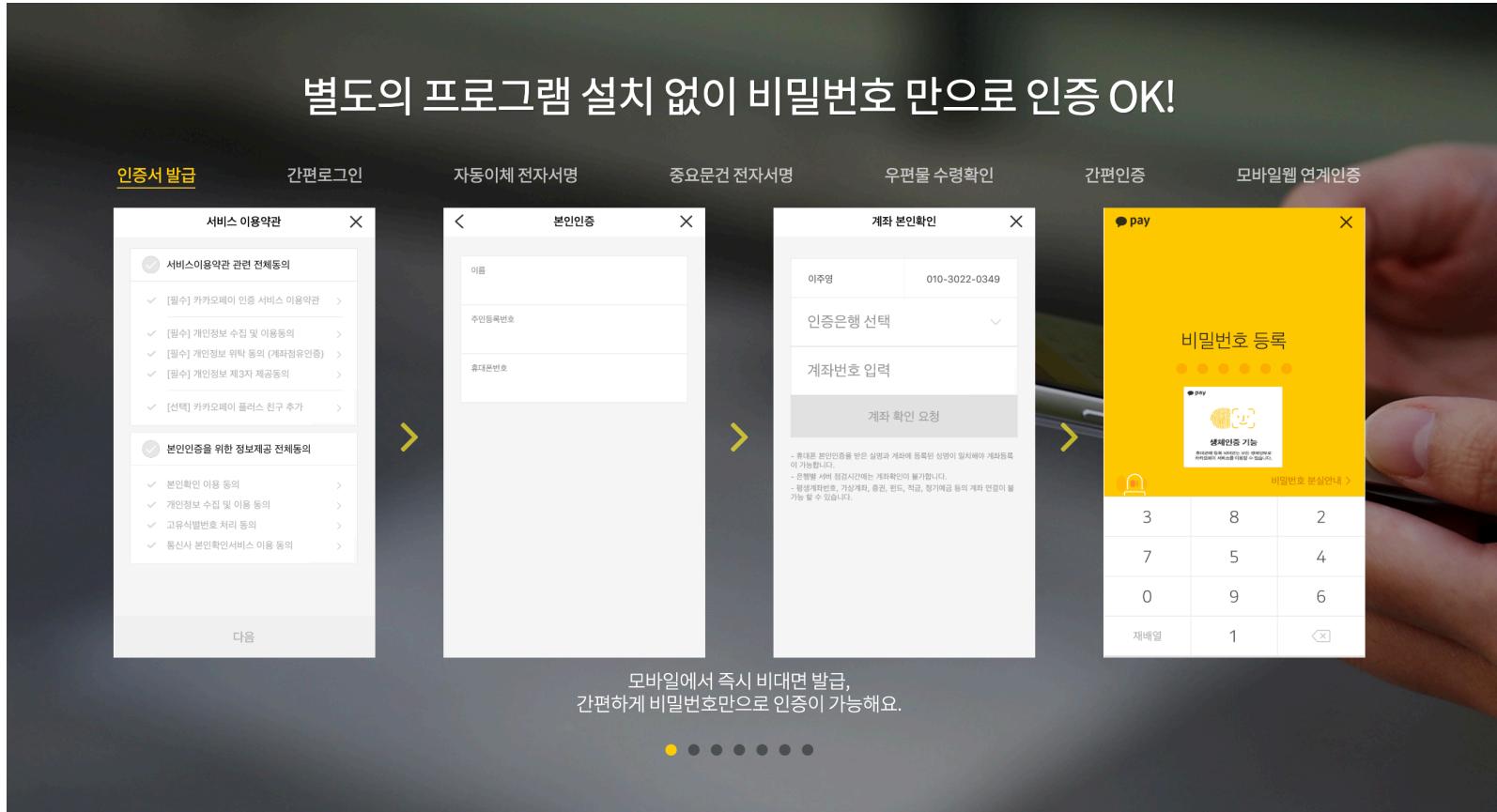
Copyright © theloop All rights reserved



2. 금융투자협회(ChainID)



3. Kakao(사설인증서)



3. Kakao(사설인증서)

이제 카카오페이지로 편리하고 안전하게 인증하세요

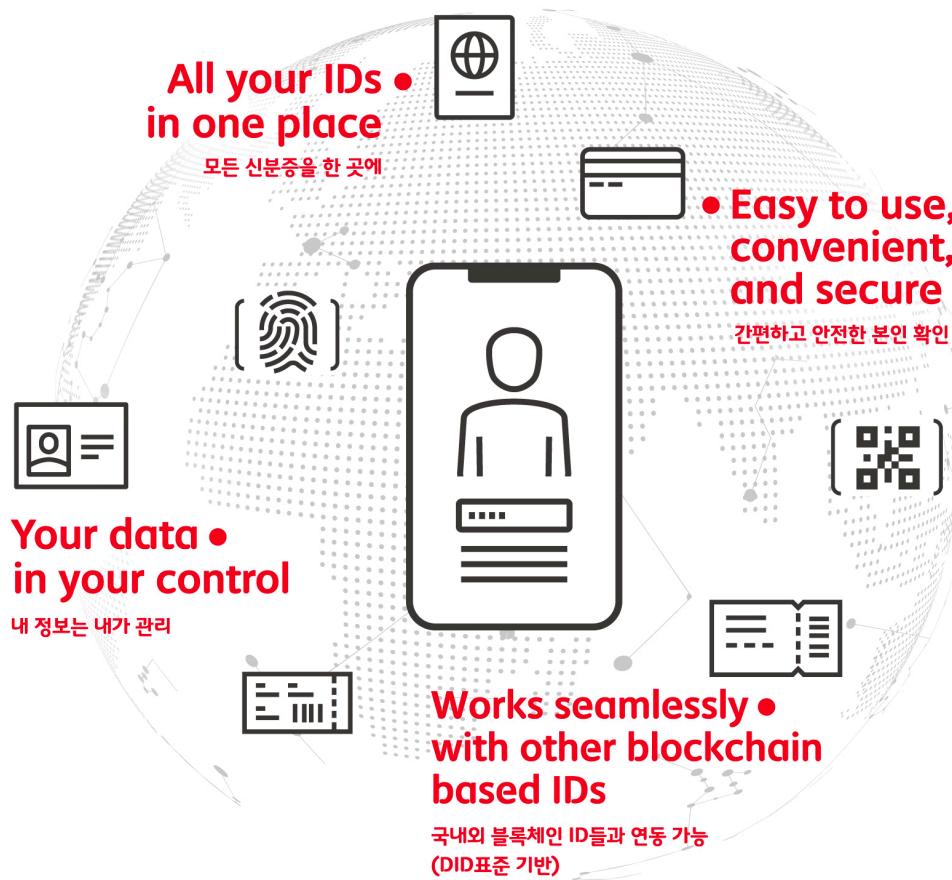
The infographic consists of six white rectangular boxes arranged in two rows of three. Each box contains a yellow icon and Korean text describing a benefit. The top row includes a speech bubble icon, a hand icon with a '2' and a sunburst, and a screen icon with Korean won symbols. The bottom row includes a fingerprint and lock icon, a document and pen icon, and a 24-hour clock icon.

- 별도의 설치없이,
카카오페이지로 인증서 발급
- 한 번 발급으로
2년 동안 이용 가능
- 국내 유일의
블록체인 기반 사설 인증

- 지문, 안면인식을 통한
간편 인증
- 카카오페이지 인증으로
간단하게 전자서명 가능
- 은행 방문없이
24시간 언제든 발급 가능



4. SKT(사설인증서)



4. SKT(사설인증서)

< 민간 주도 국민프로젝트 과제 및 참여기관 >

과제명	참여기관(<u>주관사</u> , 참여사)
① 탈중앙화 기부 플랫폼	(주)이포넷, (주)두나무, 어린이재단, 이노블록
② 블록체인 기반 중고차 서비스 플랫폼 개발	현대오토에버, (주)블로코, 에이비씨솔루션, 현대글로비스
③ 블록체인 ID인증 네트워크 기반 금융, 통신 교육 분야 서비스 개발 및 응용 확산	SK텔레콤, 코스콤, 코인플러그, LGU+, 하나은행, 해치랩스, 우리은행, SK플래닛



03. Lab 기능설명

- 블록체인에 저장할 정보
- 회원가입(Create)
- 회원탈퇴(Delete)
- 로그인/SSO(Update/Read)



[별첨] Fabric에 저장할 정보

- HyperLedger의 stateDB는 Key/Value로 저장됨

```
type User struct {
    ObjectType      string `json:"docType"`
    UserId          string `json:"userId"`
    UserName        string `json:"userName"`
    UserPassword    string `json:"userPassword"`
    LastLoginTime   string `json:"lastLoginTime"`
    LimitLoginTime  string `json:"limitLoginTime"`
}
```

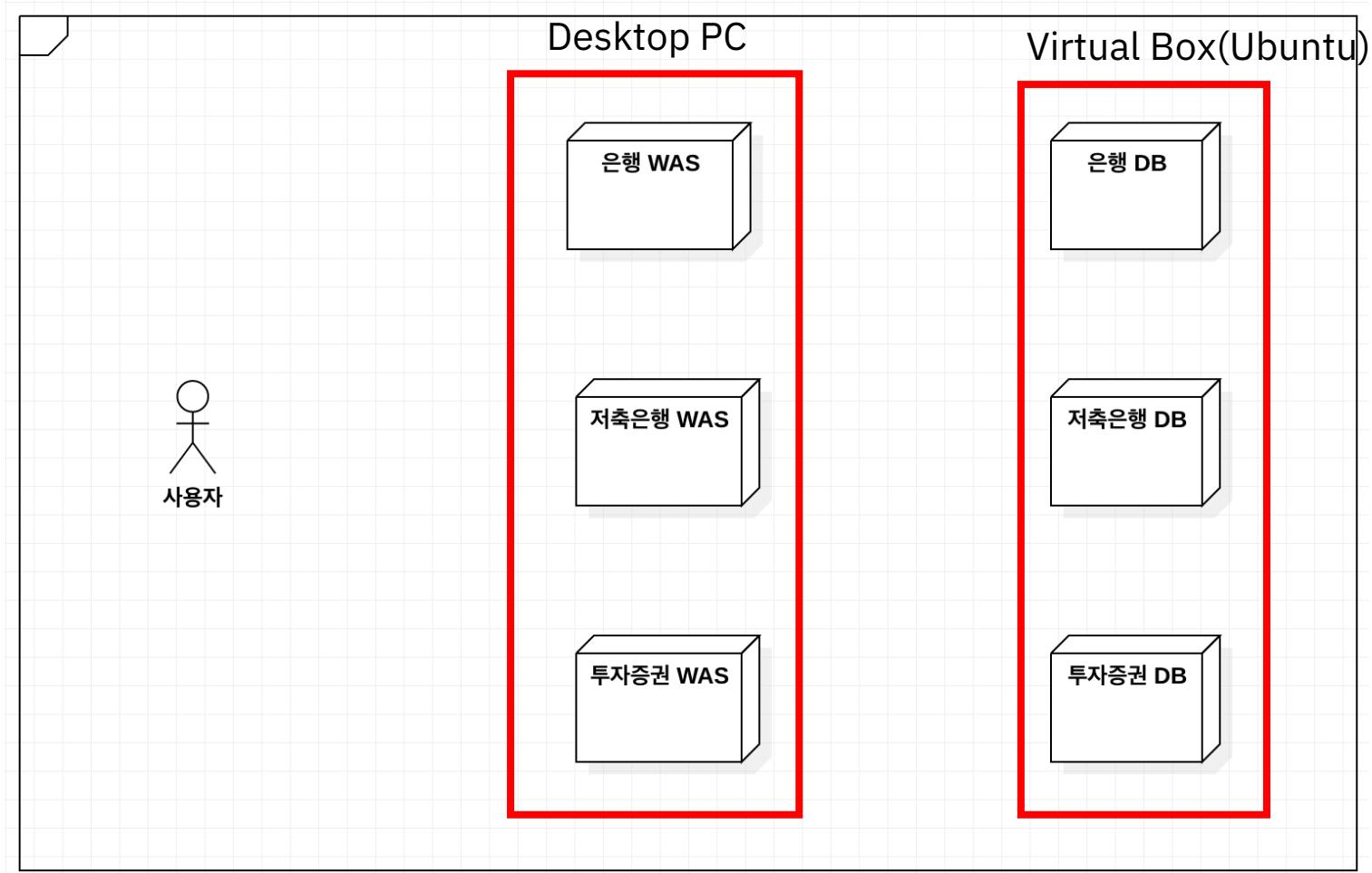
Couch DB Only
key

단방향 암호화(sha256)

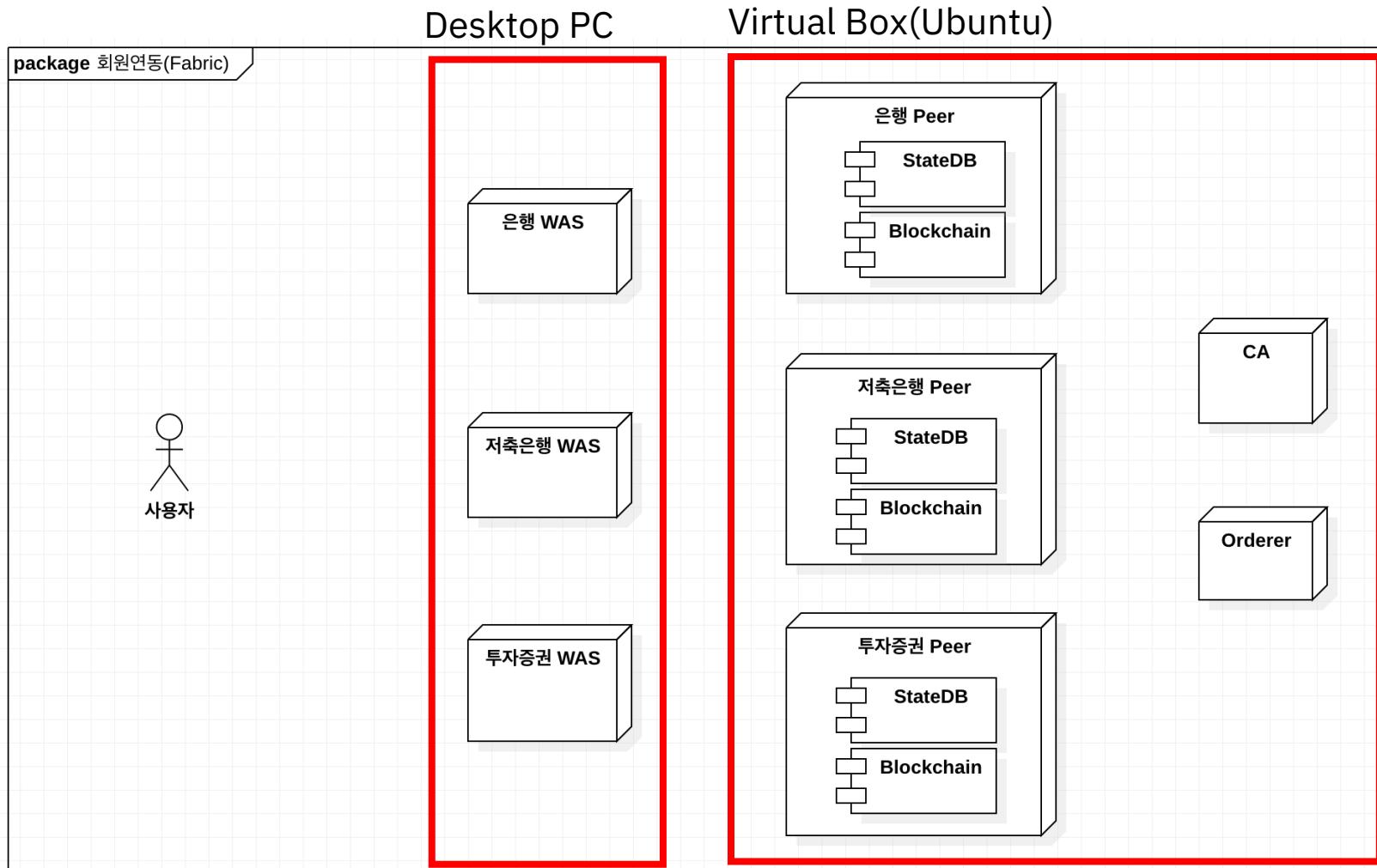
- 등록 그룹사
- 등록 일자
- 패스워드 만료일자



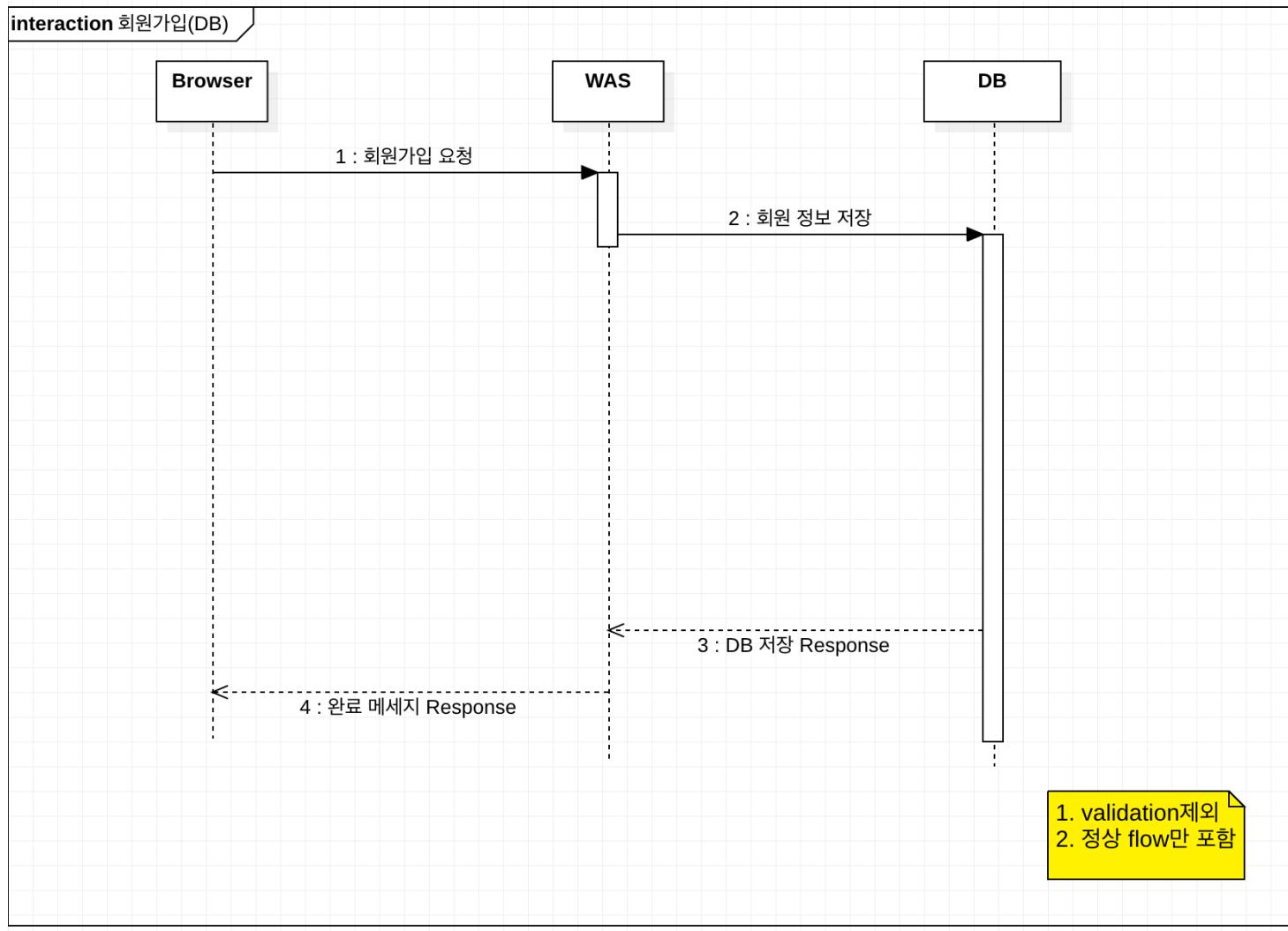
[별첨] Lab Architecture(DB)



[별첨] Lab Architecture(Blockchain)

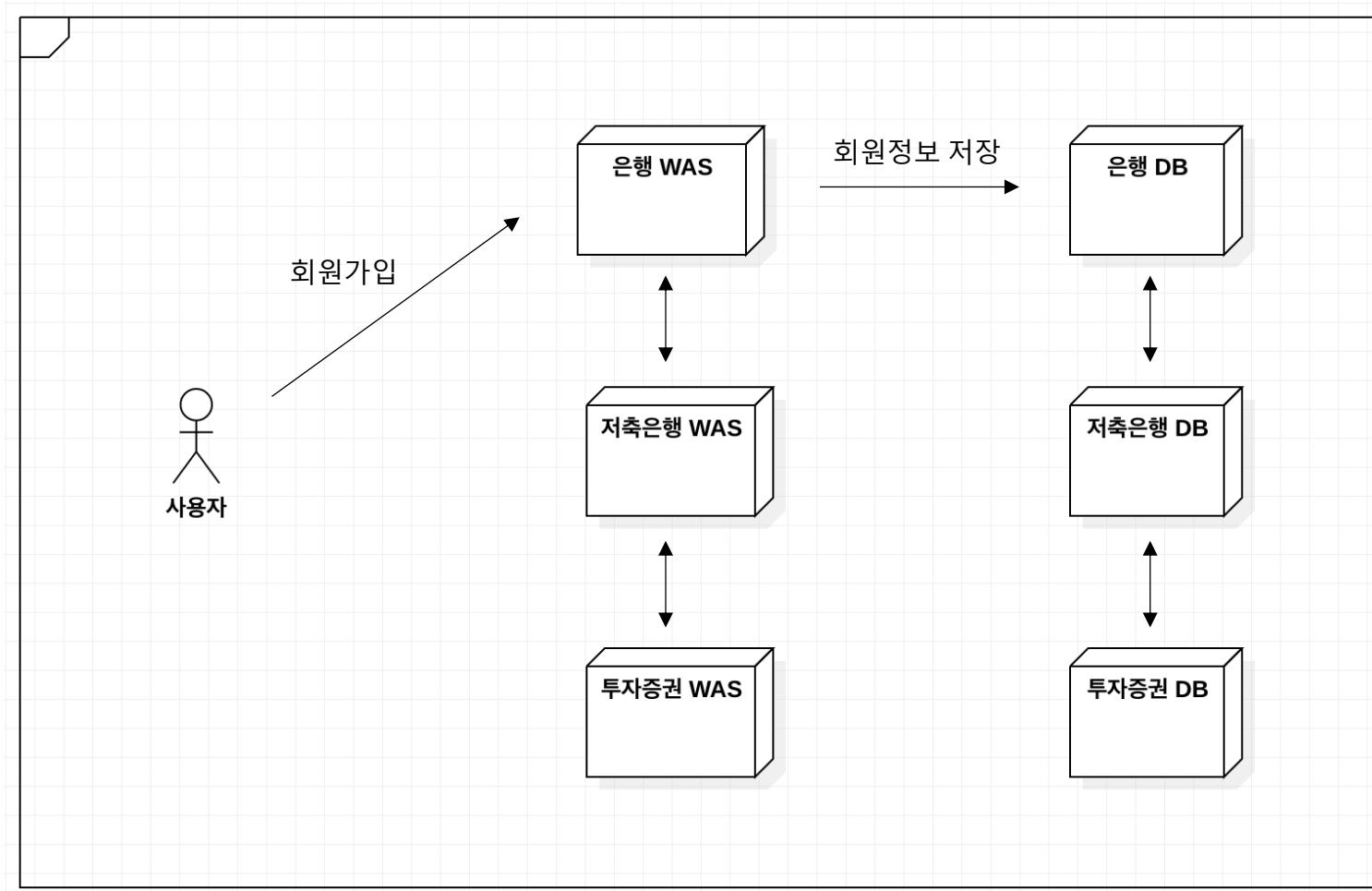


1. 회원가입(Create) / DataBase

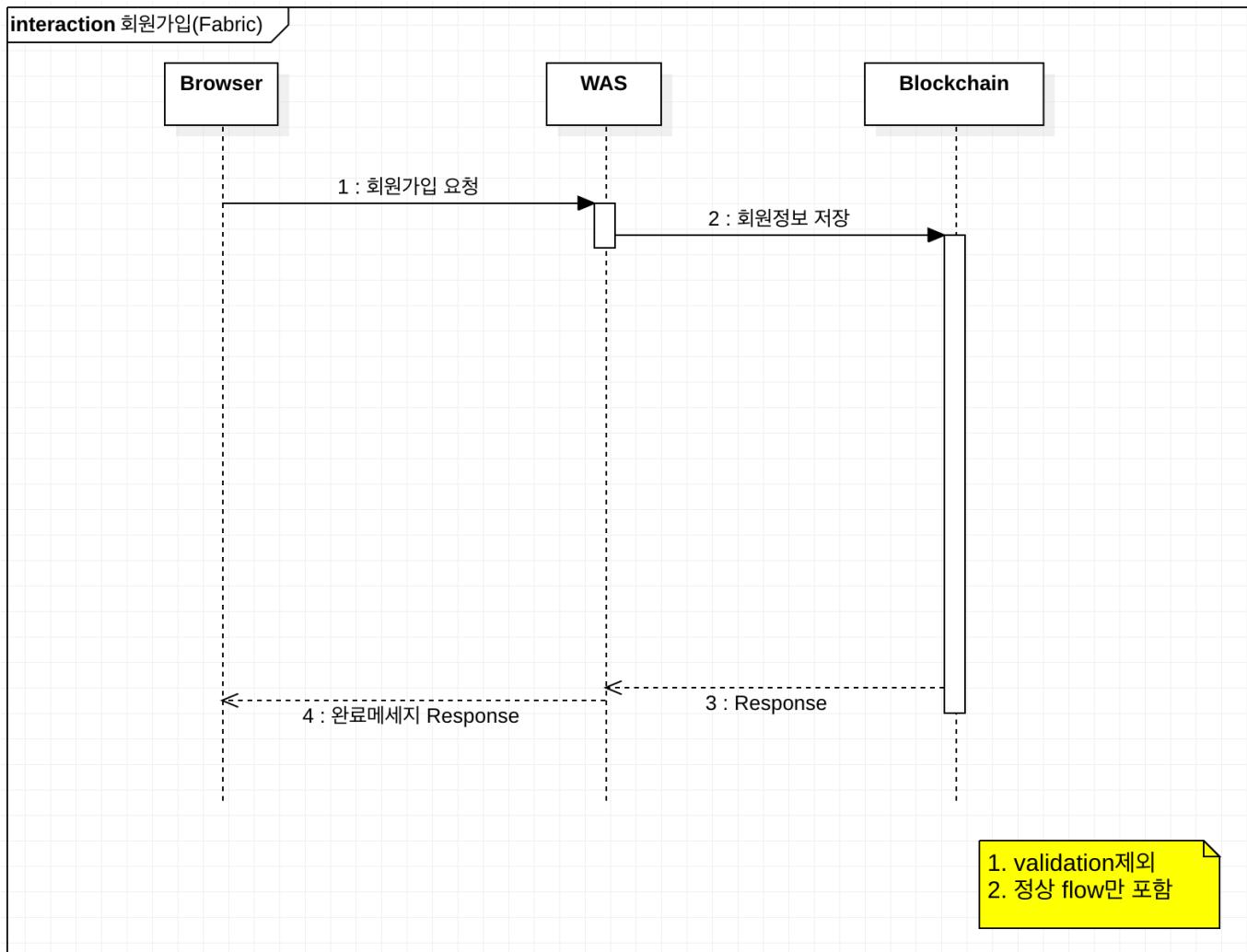


1. 회원가입(Create) / DataBase

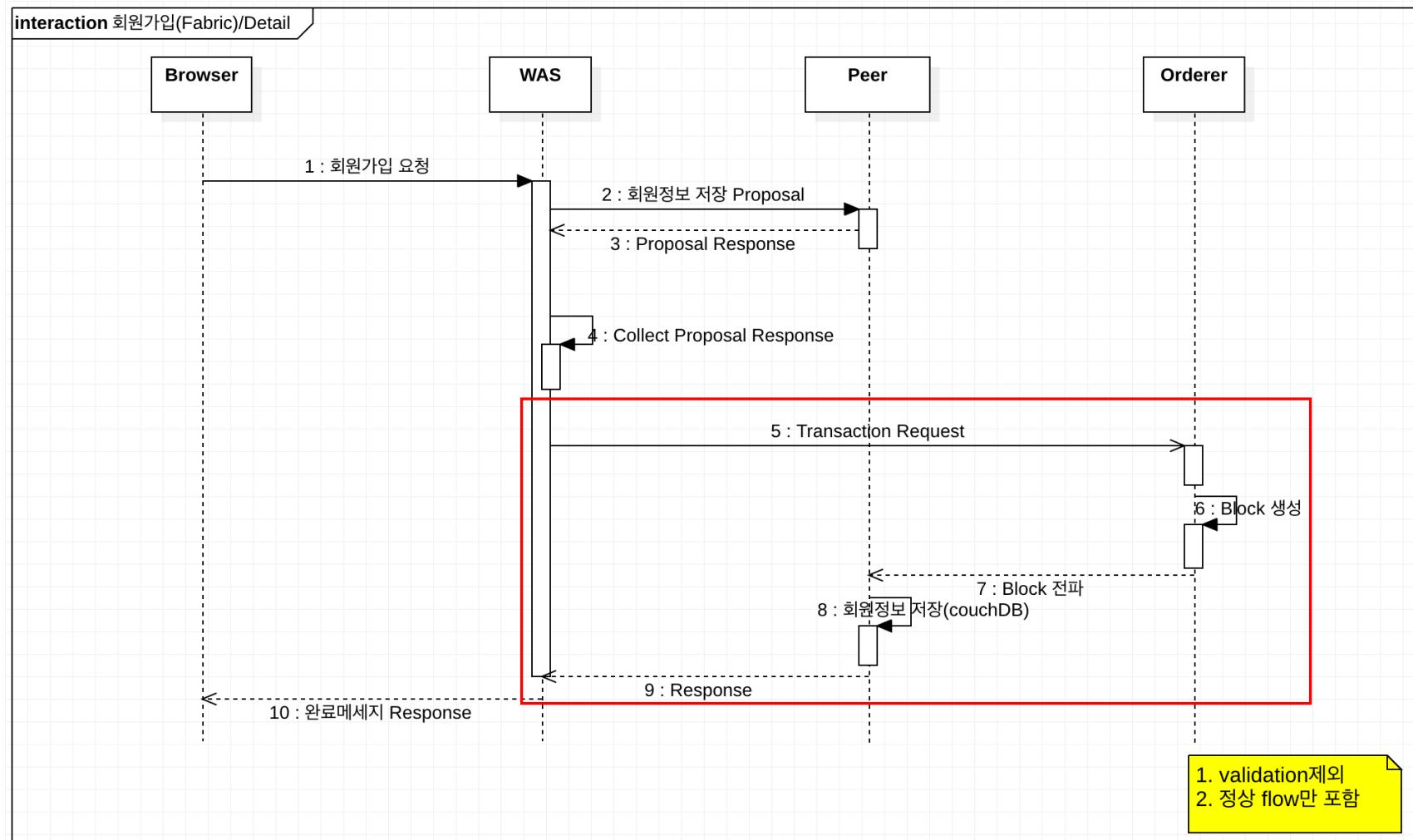
- 통합인증을 구현한다면?



1. 회원가입(Create) / Blockchain

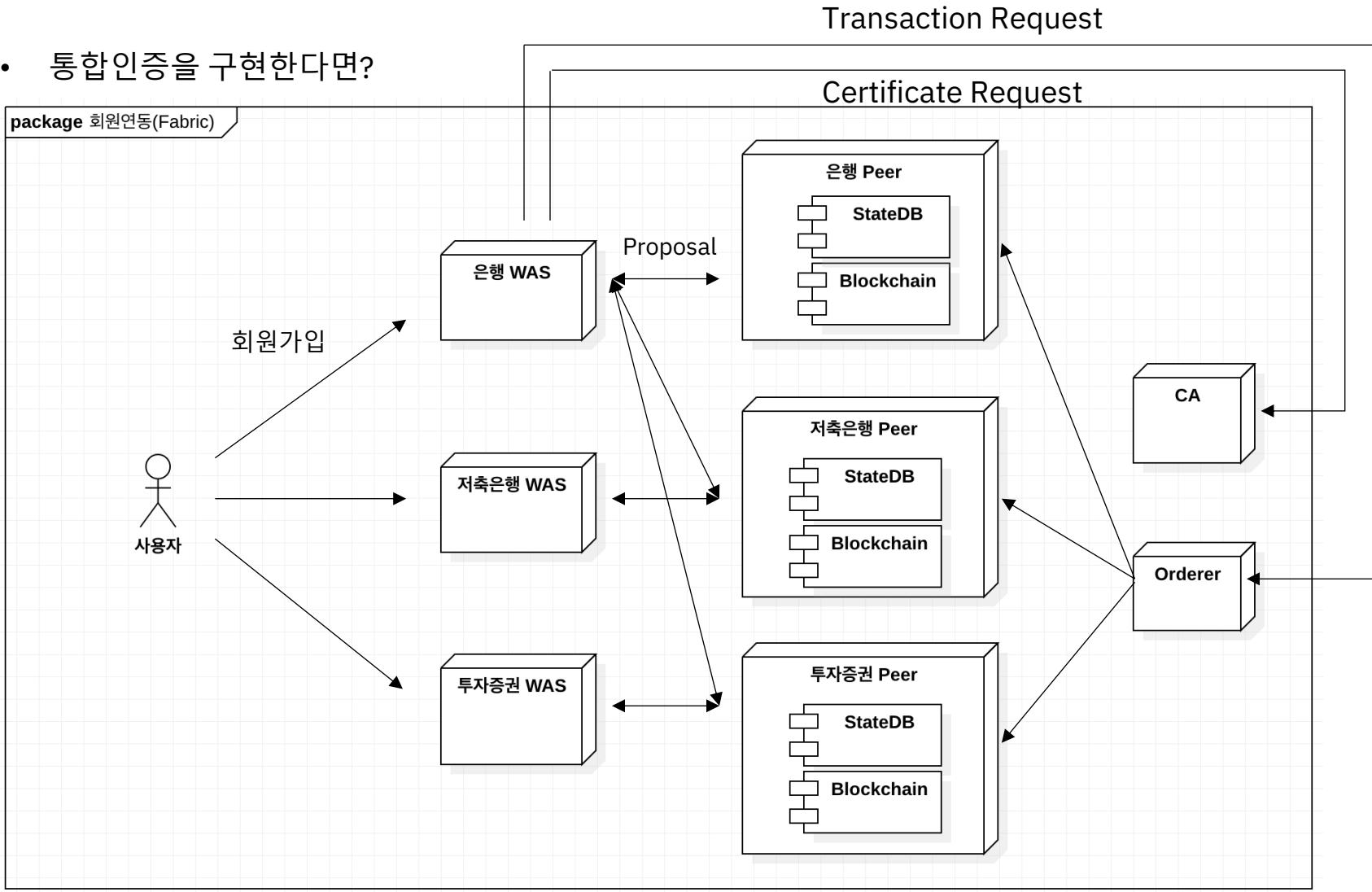


1. 회원가입(Create) / Fabric

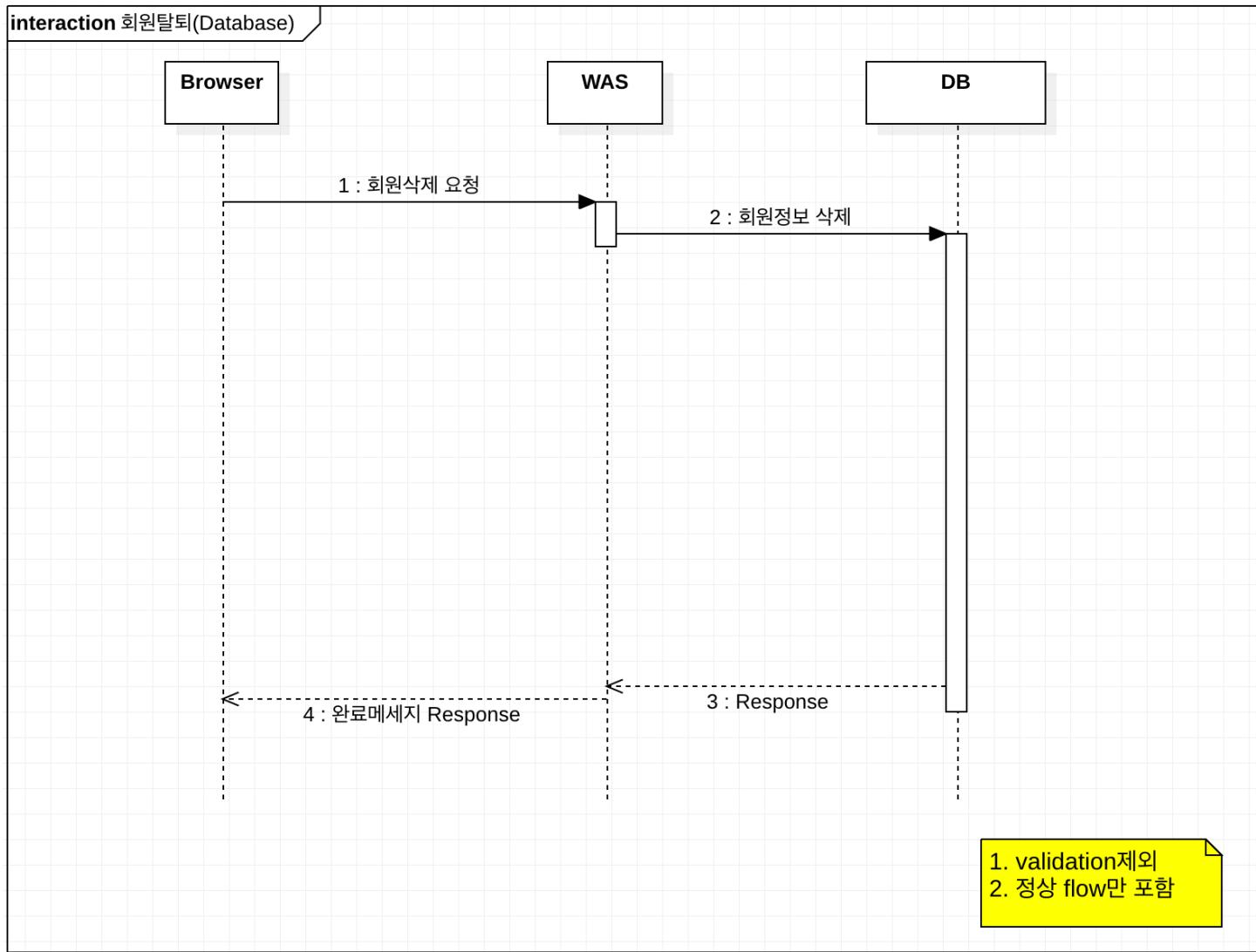


1. 회원가입(Create) / Fabric

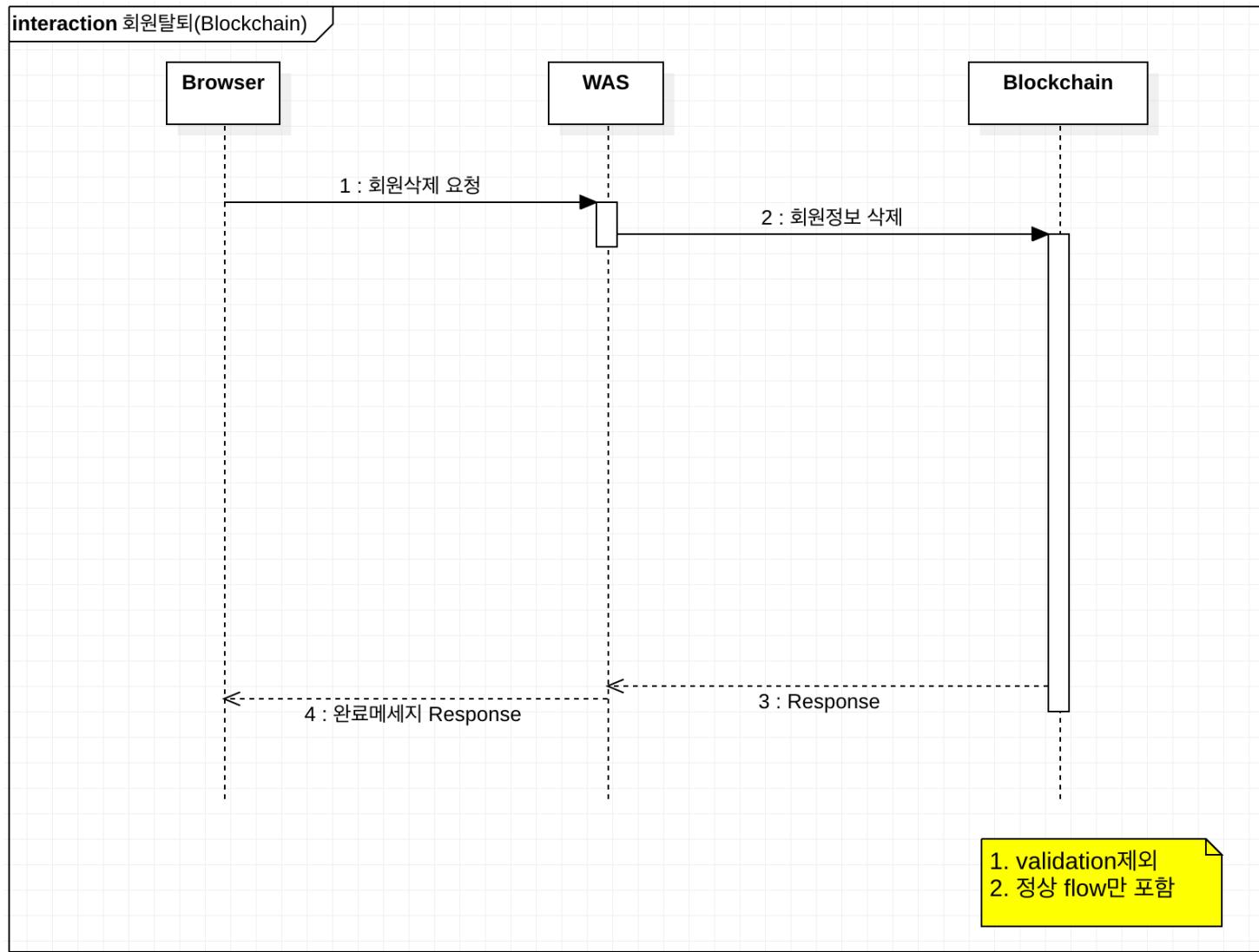
- 통합인증을 구현한다면?



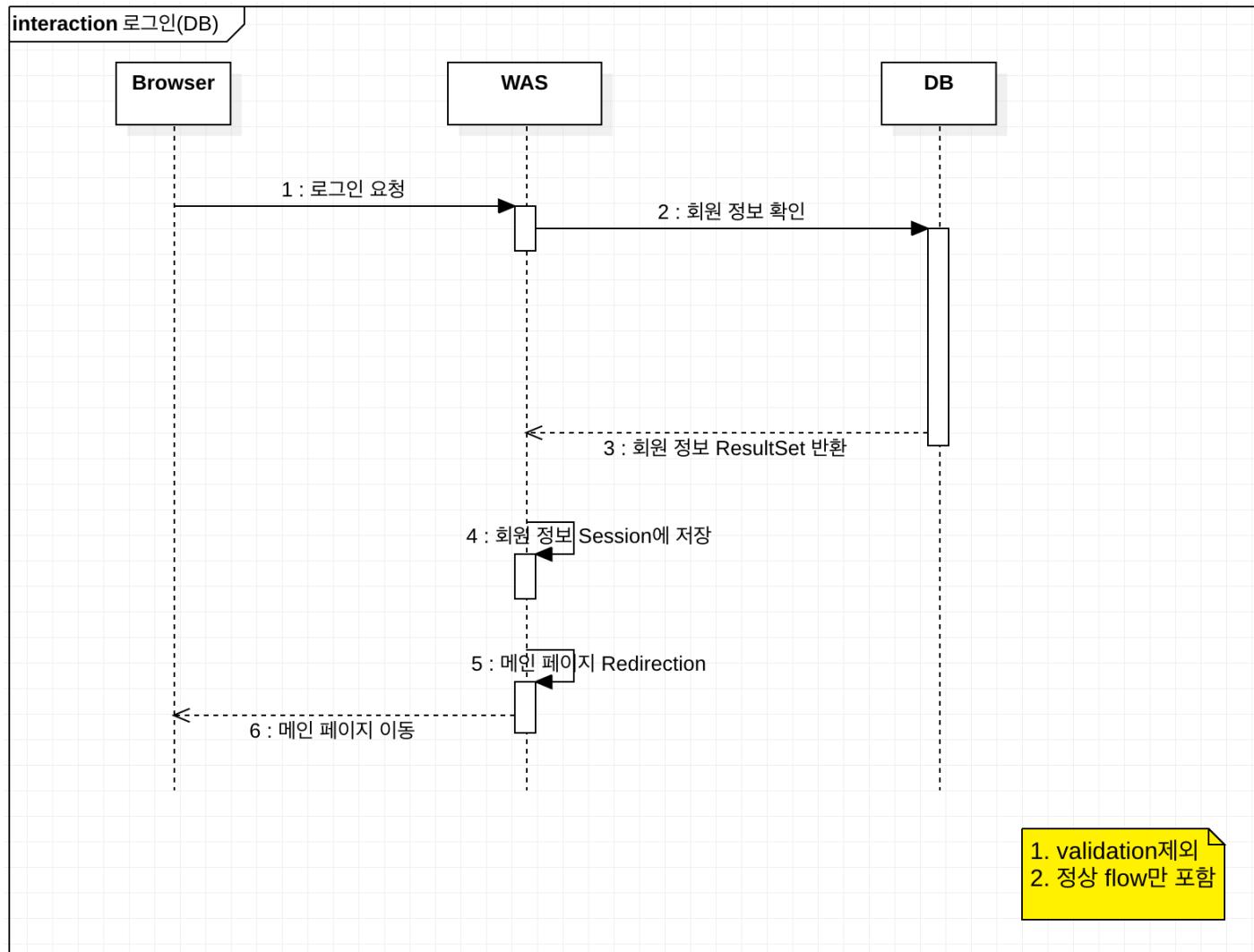
2. 회원탈퇴(Delete) / Database



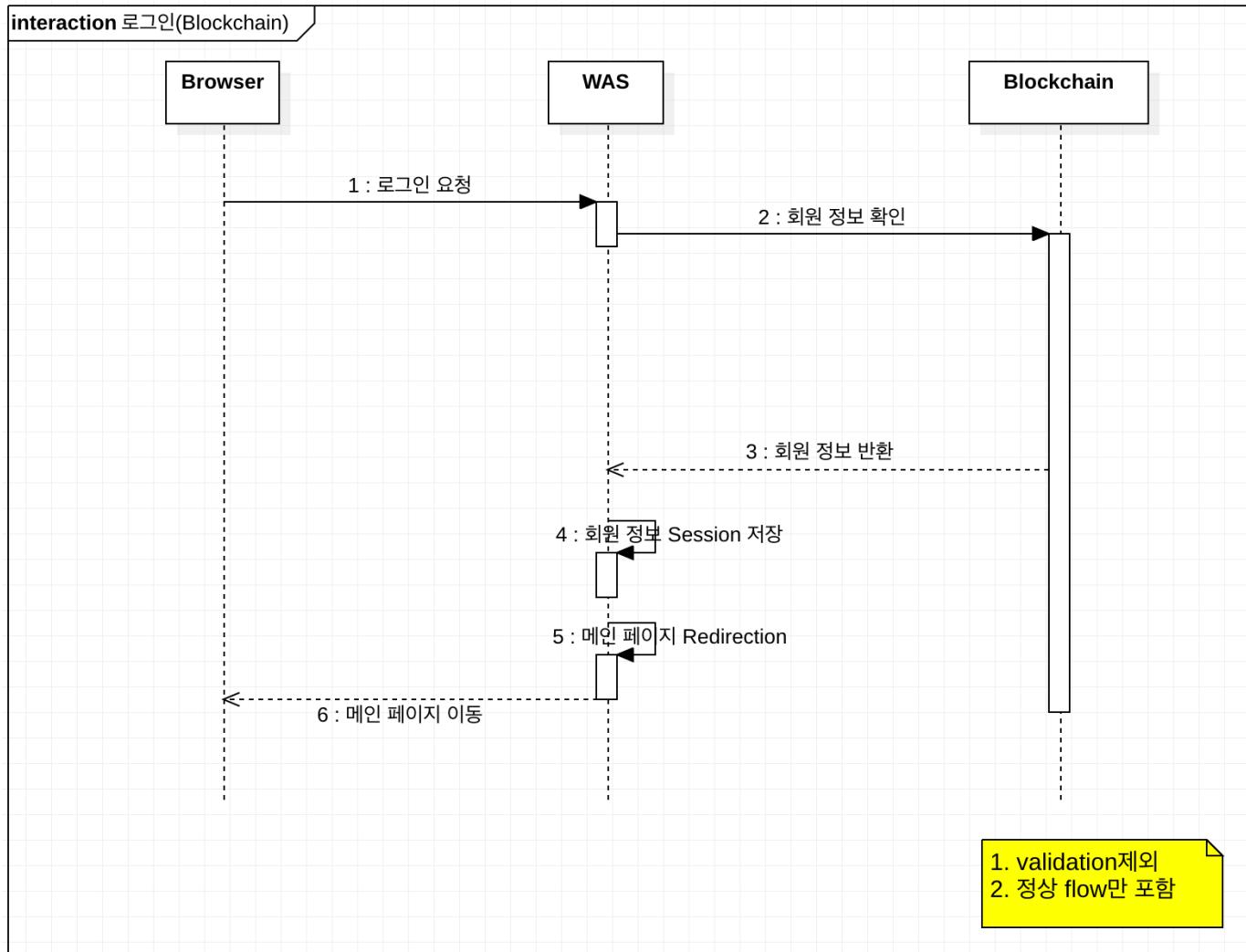
2. 회원탈퇴(Delete) / Blockchain



3. 로그인(Read) / Database

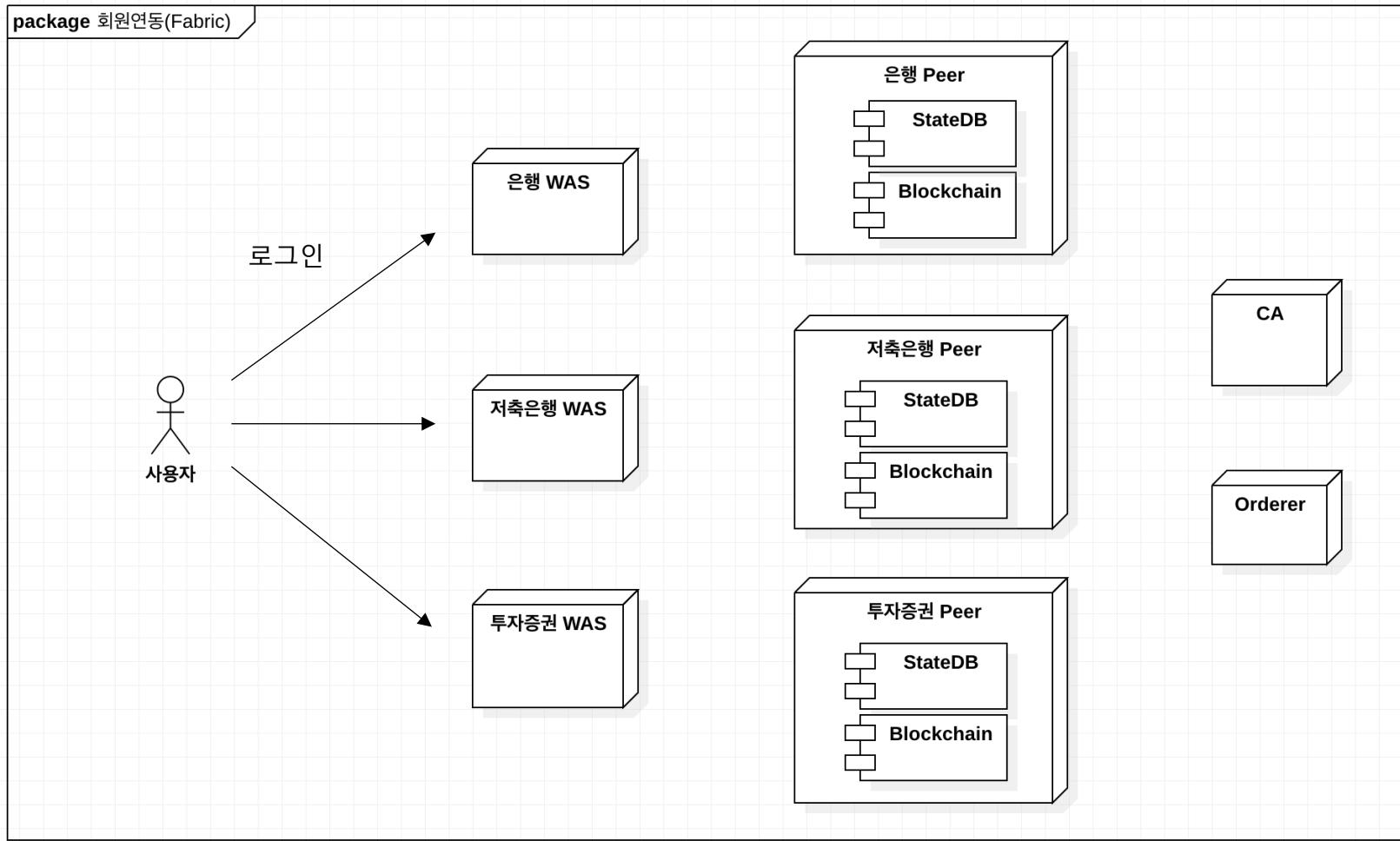


3. 로그인(Read) / Blockchain



4. SSO / Fabric

- SSO를 구현한다면?



[토론]블록체인 기능 정의

- SmartContract 기능 List

기능	기능명	비고
회원가입	CreateUser	
회원조회	SelectUserById	
회원수정	UpdateUser	
회원삭제	DeleteUserById	

- 블록체인에 저장할 데이터

변수	설명	비고
UserId	고객 식별 번호	Key
UserName	고객 조회	
UserPassword	고객 업데이트	
Regdate	등록 일자	

- DB <-> 블록체인 연동

