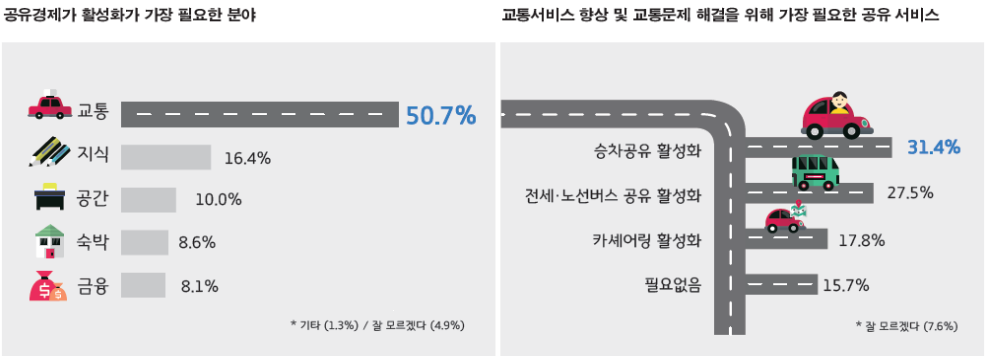
목차

1. 과제 배경 및 목표

1.1. 과제 배경

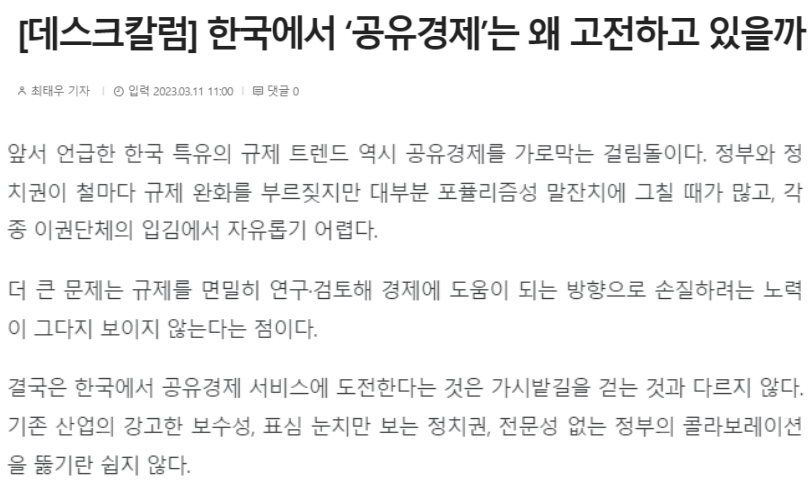
- **국내 공유 교통 활성화의 필요성**

최근 전 세계적으로 공유 경제가 미래를 대표하는 새로운 경제 모델이라는 인식이 확산됨에 따라, 국내에서도 이에 대한 관심과 수요가 증가하고 있다. 공유 경제는 차량, 숙소, 공간, 물건 등의 개인이 보유한 자원을 다른 사람과 공유하는 경제 모델로, 개인이 모든 자원을 소유할 필요 없이 필요에 따라 공유하거나 대여함으로써 자원을 효율적으로 활용하고 소유의 유연성을 제공한다.



[그림1] 공유경제 활성화 방안에 대한 국민의견조사

KDI 여론분석팀의 설문조사에 따르면, 공유 경제가 가장 필요한 분야로 교통 분야로 꼽혔다. 에어비앤비, 사무실 공유 등 공유 경제가 잘 활성화되어 있어 비교적 수요가 적은 다른 분야에 비해 수요가 가장 많은 교통 분야에서는 국내 시장에 진입했지만 운수사업법의 규제에 가로막혀 물거품이 된 서비스들이 많다. 또한 '공유도시, 서울' 정책의 일환으로 시작된 서울시의 '나눔카' 사업도 올해부터 종료되면서, 공유 교통의 실현은 점점 더 멀어져 가는 실정이다.



[데스크칼럼] 한국에서 '공유경제'는 왜 고전하고 있을까

최태우 기자 | 입력 2023.03.11 11:00 | 댓글 0

앞서 언급한 한국 특유의 규제 트렌드 역시 공유경제를 가로막는 걸림돌이다. 정부와 정치권이 철마다 규제 완화를 부르짖지만 대부분 포퓰리즘성 말잔치에 그칠 때가 많고, 각종 이권단체의 입김에서 자유롭기 어렵다.

더 큰 문제는 규제를 면밀히 연구·검토해 경제에 도움이 되는 방향으로 손질하려는 노력이 그다지 보이지 않는다는 점이다.

결국은 한국에서 공유경제 서비스에 도전한다는 것은 가시밭길을 걷는 것과 다르지 않다. 기존 산업의 강고한 보수성, 표심 눈치만 보는 정치권, 전문성 없는 정부의 콜라보레이션을 뚫기란 쉽지 않다.

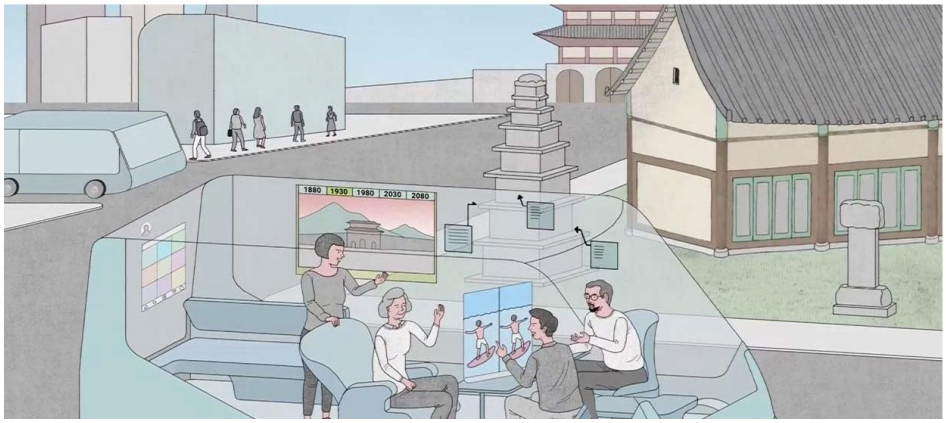
[그림2] 미성숙한 단계에 있는 한국의 공유 경제

- **스마트 시티 속 공유 모빌리티**

현재 우리나라에서는 부산, 세종, 부천 등 많은 지자체들이 공유 경제를 기반으로 지속가능한 도시를 구축하기 위해 스마트 시티 프로젝트를 추진 중에 있다. 스마트 시티는 기존 도시 인프라를 더욱 지능적이고 효율적으로 운영함으로써 도시의 지속 가능성과 삶의 질을 향상시키기 위해 도입된 개념으로, 혁신적인 4차 산업혁명 기술을 교통, 환경, 에너지, 행정 등 다양한 분야에 적용하여 스마트 시티를 조성하는 것을 목표로 삼고 있다.

리빙시티 - 자급자족이 가능한 주변 도시

대도시 규모인 스마트시티 주변에 자리한 리빙시티에는 개인 모빌리티를 공유할 수 있는 P2P(Peer to Peer) 형태의 공유 모빌리티가 주를 이룰 것으로 예상됩니다. 이를 통해 리빙시티 거주자는 물론, 관광 등의 목적을 가진 방문객도 자유롭게 메가시티를 오갈 수 있습니다. 메가시티로의 이동은 도시 고속망을 통한 초고속 교통 수단을 이용합니다.



[그림3] 현대자동차그룹에서 구상한 리빙시티 속 공유 모빌리티 모습

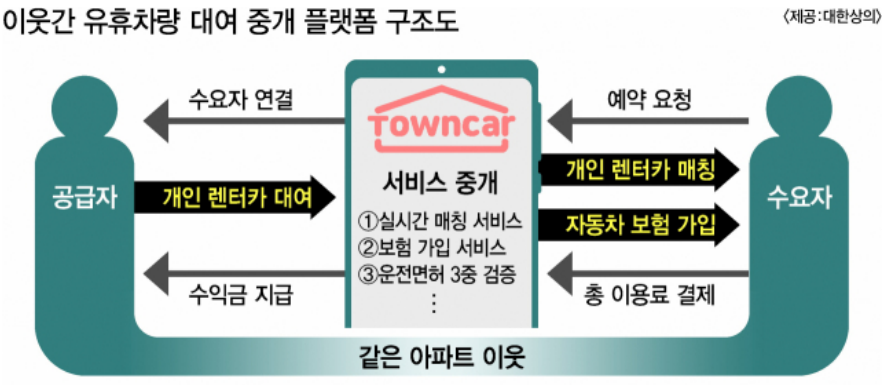
지속가능한 도시에서는 [그림3]의 모습과 같이 '활용되지 않는 유휴 자원을 타인과 공유하여 불필요한 소비 자원을 줄이고, 사회 공동의 이익 증가에 기여' 라는 진정한 의미의 공유 경제를 달성할 수 있어야 한다. 그러나 현재 상용 중인 대부분의 차량 공유 서비스는 B2C 방식으로 '진짜' 공유 경제라고는 볼 수 없다. 차량을 플랫폼 운영자(렌터카 회사)가 소유하고 있어 중개 수수료가 발생하며, 렌터카를 계속해서 생산하므로 자원을 불필요하게 낭비하게 되기 때문이다.

- **P2P 방식의 공유 모빌리티 서비스**

이렇게 혁신 기술을 이용해 스마트 시티를 구현하는 과정에서 기존의 전통적 규제 체계와 충돌이 발생하자, 최근 정부에서는 스마트 시티 확산 사업 중 하나로 '규제 샌드박스' 제도를 활성화하고 있다. 규제의 제약으로 구현되지 못하는 혁신 기술 서비스에 특례를 부여하고 실증비를 지원하는 사업이다. 운수사업법의 규제로 P2P 방식의 차량 공유 서비스는 지금까지 존재하지 않았지만, 규제 샌드박스 도입 이후 '타운카'라는 국내 최초 개인 차량 공유 플랫폼이 등장하게 되었다.

규제가 없는 해외에서는 'Turo', 'Getaround'와 같은 서비스가 이미 몇 년째 활발하게 운영되고

있다. 규제가 없는 대신 기본으로 차주에게 지불하는 대여 비용 외에도 사회적 기여금, 예약 수수료, 25세 미만 수수료, 보증금, 흡연 수수료, 통행료, 연료교체비 등 많은 비용을 지불해야 한다.



[그림4] 국내 최초 개인 차량 공유 플랫폼 '타운카'

'타운카'는 비교적 최근에 규제 샌드박스를 통과하였기 때문에 상용화가 잘 되어있는 해외 서비스에 비해 아직 부족한 점이 많다. 차량을 관리하는 키퍼와 대여자가 직접 만나서 차 키를 교환하는 과정이 필수적이라 번거롭다는 단점이 가장 크다. 'Turo', 'Getaround'에서는 GPS로 자동차 위치를 확인하고, 스마트폰으로 문을 열고, 잠그고, 시동을 걸 수 있다. 차량 위치와 주행거리를 스마트폰으로 알 수 있으며, 대여, 반납 시 상태는 사진으로 찍어 공유하는 방식이다.

- **공유 모빌리티 서비스의 발전 방향**

'타운카'는 공유 경제를 달성하기 위한 새로운 방식을 도입해 규제 샌드박스를 통과했다는 데 큰 의의가 있지만, 아직은 번거로운 과정을 거쳐야 하며 스마트 시티의 핵심인 혁신 기술을 사용했다고 보기는 어렵다. 또한 다양한 사람들이 서로의 자산을 공유하며 상호 작용을 하게 되는데, 기존의 시스템만으로는 버그나 해킹으로 인한 정보 유실 및 유출과 같은 위험이 여전히 존재한다.

이에 따라 스마트 시티에서 안전하게 사용할 수 있는 공유 모빌리티 서비스가 필요한데, 본 과제에서는 블록체인의 분산화된 시스템 구조와 암호화 기술을 통한 데이터 관리와 거래로 이를 해결하고자 한다.

기술적인 측면에서 높은 수준의 암호화와 정보의 분산 저장 및 처리를 기반으로 하는 블록체인은 스마트 시티의 정보 통신 인프라에서 중요한 역할을 수행할 것이다. 사회경제적으로는 블록체인의 분권화를 기반으로 시민들이 개인정보 데이터 주권을 스스로 관리할 수 있도록 함으로써 시민 각각이 사회경제적으로 독립하고 함께 성장할 수 있는 기회를 제공한다. 전문가들은 블록체인으로 기존 공유 경제의 취약한 부분인 중앙집중형 통제와 해킹에 취약한 보안기술, 큐레이션의 실패 등을 개선하고, 한 단계 업그레이드된 공유 경제 시대를 맞이할 것으로 예상하고 있다. 아직 국내 블록체인 기술은 초기 단계이며, 광범위하게 적용되는 단계에 도달하지 못한 상태이다. 따라서 본 과제에서는 블록체인의 기술적 측면과 사회적 특성을 함께 고려하여 스마트 시티에 공유 모빌리티 서비스를 도입하기 위한 아이디어를 제안한다.

1.2. 과제 목표

- 본 과제에서는 스마트 시티에서 시민들 간에 개인 모빌리티를 공유할 수 있는 **P2P 방식의 공유 모빌리티 서비스**를 개발하고자 한다. **DID를 통한 차량 검증**으로 개인이 차량의 정보를 관리하는 주체가 되도록 하고, **허가형 블록체인으로 검증된 차량만 거래에 참여**할 수 있으며 내부에서만 모든 거래 정보가 투명하게 공개되는 안전한 거래 시스템을 설계한다.
- 기존 렌터카 서비스는 플랫폼 운영자(렌터카 회사)가 차량을 보유하고 이를 대여하는 방식이다. 이러한 방식은 차량 정보 제공에 불균형이 발생하여 사용자들은 차량 이용에 불편함을 겪었다. 따라서 본 과제에서는 P2P 기반 차량 공유 시스템을 통해 자원의 중앙화를 개선하고자 한다.
- P2P 거래 시스템에서 개인 차량의 신뢰성을 확보할 수 있는지에 대한 의문이 생기는데, 이는 DID(Decentralized Identifier) 기술을 도입하여 해결할 수 있다. DID는 탈중앙화 신원 증명 시스템으로, 기존의 신원 인증 방식과 달리 개인이 직접 자기 신원을 인증하는 SSI(Self Sovereignty Identity)를 가능하게 하는 기술이다. 개인 차량에 사물 DID를 등록하고 이를 검증함으로써 사용자에게 신뢰성 있는 차량 정보를 제공할 수 있다. 동시에 개인이 차량의 정보를 관리하는 주체가 되어 개인 차량 정보에 대한 과대한 노출을 방지할 수 있다.

1.3. 기대 효과

- 본 과제를 통한 기대효과는 다음과 같다.

데이터 주권 실현	플랫폼 운영 주체가 모든 데이터를 소유하고 통제하는 중앙집권형 방식에서 벗어날 수 있다.
중개 수수료 절감	중개업체 없이 차량 소유자와 이용자 간의 직접적인 거래가 이루어지므로 중개수수료를 절감할 수 있고, 다양한 차종을 이용할 수 있다
신뢰성, 투명성 제공	차량의 이용 기록이나 거래 내역 등을 블록체인에 기록함으로써 안전하게 관리하고 검증할 수 있다.
유휴 자원의 활용	차량 소유자는 사용하지 않는 시간 동안 차량을 공유함으로써 경제적인 이익을 얻을 수 있고, 효율적인 자원 활용으로 불필요한 차량 구매와 생산을 줄일 수 있다.

1.4. 현실적 제약 사항 분석 결과 및 대책

국내에서는 50대 미만의 소규모 사업의 경우 자동차 대여사업 운영이 불가능하다는 정부 규제 '여객 자동차 운수사업법'이 있어 카셰어링 서비스가 활성화되지 못한다. 해당 법이 버티고 있는 한 서비스가 아예 불가능하다. '타운카' 서비스의 경우 2년 가까이 '규제 샌드박스'에 매달려 국내 최초로 승인을 받을 수 있었다. 이러한 현실적 한계로 본 과제에서 실제 서비스를 구현하기는 불가능하지만, '타운카'와 같은 기존 서비스에 차량용 DID와 블록체인을 도입하여 향후 발전시킬 수 있는 부분을 아이디어로 제시하는 데 초점을 맞추고자 한다.

2. 요구사항 분석

2.1. 기능 요구사항

번호	비즈니스 요구 사항	상세 요구사항
A1	회원가입 기능	- 가입정보(아이디, 비밀번호, 이메일등)와 인적사항 등록(이름, 주소지, 전화번호등)을 통한 회원가입 기능 구현 - 인증서를 통해 면허와 본인인증을 수행 (구현상 생략)
A2	로그인 기능	- 사용자가 입력한 값과 DB에 있는 값을 비교해 로그인 승인 여부 결정 - 로그인 승인 시 JWT 토큰을 부여하여 메인 페이지로 이동 및 주요 기능 사용 가능하도록 허용
B1	메인페이지 기능	- 로그인 시 제일 처음 나오는 화면으로 유저들은 차량 등록, 차량 검색, 차량 대여 서비스 이용 가능
B2	마이페이지 기능	- 해당 유저가 등록한 차량들 제공 - 해당 유저가 대여 예약한 차량에 대한 정보 제공 - 해당 유저의 거래 기록 제공 (차량 제공 기록, 차량 대여 기록)
C1	차량 등록 기능	- 차주의 차량에 대한 DID 등록을 하면 시스템에서 VC 발급하여 차주에게 제공 - 차주는 차량에 대한 VP(차량 번호, 출차일, 주행거리, 대여기록, 소유자 ID)와 차량 사진, 주차지, 대여가능일시, 금액 등을 제출하여 차량 등록 가능
C2	차량 검색 기능	- 대여자의 주소지를 기반으로 인근에 등록되어 있는 모든 차량 목록 제공 - 대여자가 사용하고자 하는 날짜를 입력하면 필터링하여 이용가능한 차량 목록 제공

D1	대여 신청 기능	- 대여자가 이용하려는 차량의 차주에게 대여 신청을 하고 차주가 승인하면 거래 시작
D2	채팅 기능	- 거래가 시작되면 차주와 대여자 간 채팅 기능 활성화
D3	결제 기능	- 차주와 대여자 간의 의견 조율 후, 대여자가 등록된 금액을 해당 기능을 통해 차주에게 지불

2.2. 사용자 요구사항

번호	사용자	상세 요구사항
A1	차주	- 서비스 이용을 위해서 회원가입이 필요 - 대여 원하는 차량에 대해서 VC를 발급하고 VP를 사용하여 등록이 가능 - 대여자와의 채팅을 통해 의견을 조율 - 마이페이지에서 등록한 차량이나 차량 제공 기록등 내역 조회
A2	대여자	- 서비스 이용을 위해서 회원가입이 필요 - 대여를 위해 차량 검색 - 대여하고 싶은 차량에 대해서 대여 신청 - 차주와의 의견조율을 위해 채팅 기능을 사용 - 대여 신청을 하고 결제를 진행 - 마이페이지에서 대여 예약한 차량이나 차량 대여 기록등 내역 조회

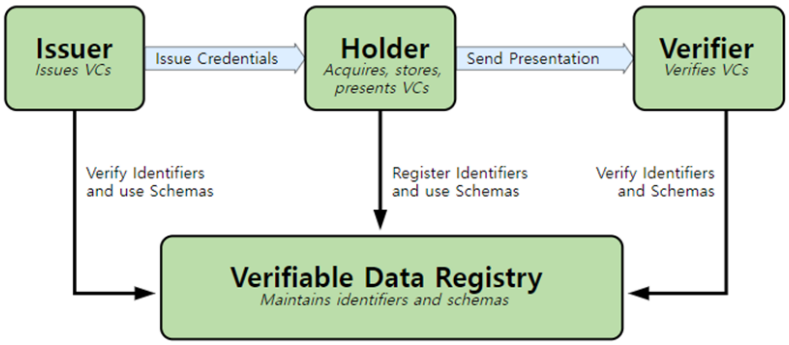
3. 설계 문서

3.1. 사용 기술

3.1.1. DID(Decentralized identity, 탈중앙화 신원 증명)

DID는 분산원장 기술을 기반으로 한 신원증명이며, 중앙시스템에 통제받지 않고 개인이 자신의 정보에 완전한 통제권을 갖도록 하는 디지털화된 신원관리 체계 기술이다. 즉, 개인 정보를 사용자의 단말기에 저장해, 개인 정보 인증 시 필요한 정보만 골라서 제출하여 사용자의 Privacy를 보장해주는 전자신원증명 기술이다. DID 서비스의 참여자는 사용자(Holder), 발행기관(Issuer), 검증인(Verifier)으로 구성된다. 사용자는 전자지갑 앱을 통해 개인정보를 직접 관리한다. 발행기관은

사용자가 신분증, 증명서 등의 발행을 요청할 경우 사용자를 검증한 후 VC를 발행한다. 검증인은 서비스를 제공하는 기업이나 기관이며, 사용자가 제출한 VP를 검증한 후 서비스를 제공한다.



[그림5] Verifiable Credentials Data Model에서의 역할과 데이터 흐름도

3.1.2. DID 구성요소

- DID

  DID는 DID document의 위치를 나타낼 수 있는 주소로 Scheme, Method, Method-Specific Identifier로 구성된다. Scheme는 DID 식별자임을 표시하는 것으로 어떠한 종류의 프로토콜을 사용하여 자원에 접근하는지 명시한다. Method는 DID document가 어느 저장소이고, 어디 저장되어 있는지 보여주며 CRUD를 수행하는 방법을 지정한다. Method-Specific Identifier는 저장소 내에 DID document가 저장된 위치를 검색하기 위한 주소이다.

[그림6] DID 모델 개요

- DID document

  DID Document는 DID 소유 인증에 사용되는 Public Key를 포함하고 있으며 DID를 설명하는 메타데이터가 포함된 구조화된 문서이다. 그리고 추가적으로 엔티티를 설명하는 다른 속성등을 추가할 수 있다. 일반적으로 분산저장소에 기록되는 DID docuemnet의 속성은 PublicKey, Authentication, Service가 있다.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

[그림7] DID Document 예시

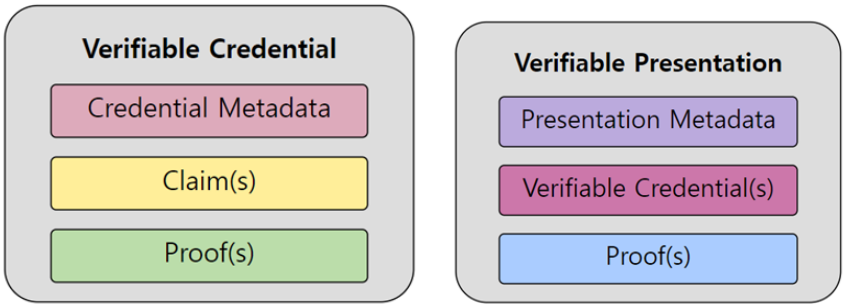
- VC (Verifiable Credential)

  VC는 신분증, 졸업증명서, 재직증명서 등 각종 증명서의 ID 속성이 포함되고 Credential Metadata, Claim, Proof로 구성된다.

  Credential Metadata는 VC를 발행한 기관, VC가 명시하는 객체, VC의 만료기간, VC의 폐기 방법 등이 정의된다. Claim에는 VC가 명시하는 객체의 ID 속성에 대한 정보로 Subject-Property-Value 방식으로 저장된다. Proof는 해당 VC에 대해 진위 여부 검증을 하기 위해 RSA. ECDSA 등 다양한 암호 기법이 사용된다.

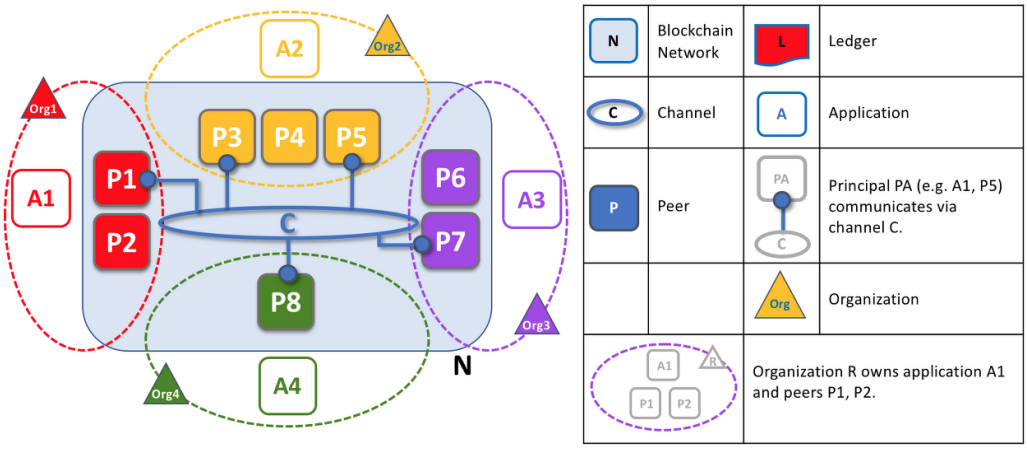
- VP (Verifiable Presentation)

  사용자는 검증인(Verifier)에게 자신을 증명하기 위해 VC를 직접 제출하지 않고 자신이 발급받은 VC로 VP를 생성하여 제출하고, 이 VC는 Presentation Metadata, Verifiable Credential, Proof로 구성된다. Presentation Metadata는 해당 데이터가 VP라는 것을 명시한 타입, 이용약관등 VP 검증에 참고할만한 데이터가 포함된다. Verifiable Credential에는 발급받은 VC 중 검증인이 요구하는 Claim만 선택하여 포함시켜 사용자의 Privacy를 보호할 수 있다. VP를 수신한 검증인은 VC의 Proof에는 발행기관(Issuer)의 서명이 들어가고 VP의 Proof에는 사용자의 서명이 들어가 있어 이것을 통해 검증을 한다.



[그림8] VC와 VP 구성요소

3.1.3. Hyperledger Fabric



[그림9] Hyperledger Fabric Architecture

- Ledger

  블록에 거래 정보가 저장되는 공간으로, 하이퍼레저 패브릭은 World State라는 저장소에 원장을 저장한다. 한 채널이 한 원장을 가지고, 한 채널 안의 노드들은 동일한 원장의 복사본을 가진다.

- Smart Contract and Chaincode

  Chaincode는 하이퍼레저 패브릭 네트워크에서 Smart Contract를 구현하는 코드로, 네트워크에서 발생하는 거래를 처리하고 결과를 반환하는 역할을 한다. 분산원장에 저장되어 있는 데이터를 읽고 쓰는 등의 작업을 수행하여 네트워크 참여자들 간에 합의되어 있는 비즈니스 규칙을 자동으로 실행한다.

- Peer

  오더러가 만든 블록을 검증하고 그 블록을 바탕으로 원장을 저장하고 유지하는 노드이다. 클라이언트의 요청에 의해 발생하는 체인코드의 실행을 담당하며, 체인코드 실행 결과를 트랜잭션으로 만들어 오더러에게 전달한다.

- Channel

  하이퍼레저 패브릭 컨소시엄 내 그룹 간의 커뮤니케이션 메커니즘으로, 데이터 분리를 가능하게 하며, 채널용 장부는 허가된 컨소시엄 멤버들만 접근이 가능하기 때문에 그룹들 간 프라이버시를 유지할 수 있다. 채널 설정을 통해 채널에 접근 가능한 피어의 권한을 부여할 수 있으며 이러한 채널 설정 정보는 블록에 담겨 장부에 기록된다. 한 네트워크 내부에는 여러 컨소시엄들이 사용하는 다수의 채널들이 존재할 수 있다. 해당 채널에 참여하는 노드들은 서로 다른 체인코드를 실행할 수 있는데, 이를 통해 하나의 블록체인 네트워크에서 여러 개의 응용 프로그램을 실행할 수 있다.

- Organization

  패브릭 네트워크를 구성하는 단위로, 하나 이상의 피어 노드를 가진다. 각 Organization은 독립적인 MSP(Membership Service Provider)를 통해 구성원을 인증하고 채널에 대한 접근 권한을 부여한다. 아래 그림에서 빗금 친 원형 구간이 Organization에 해당한다.

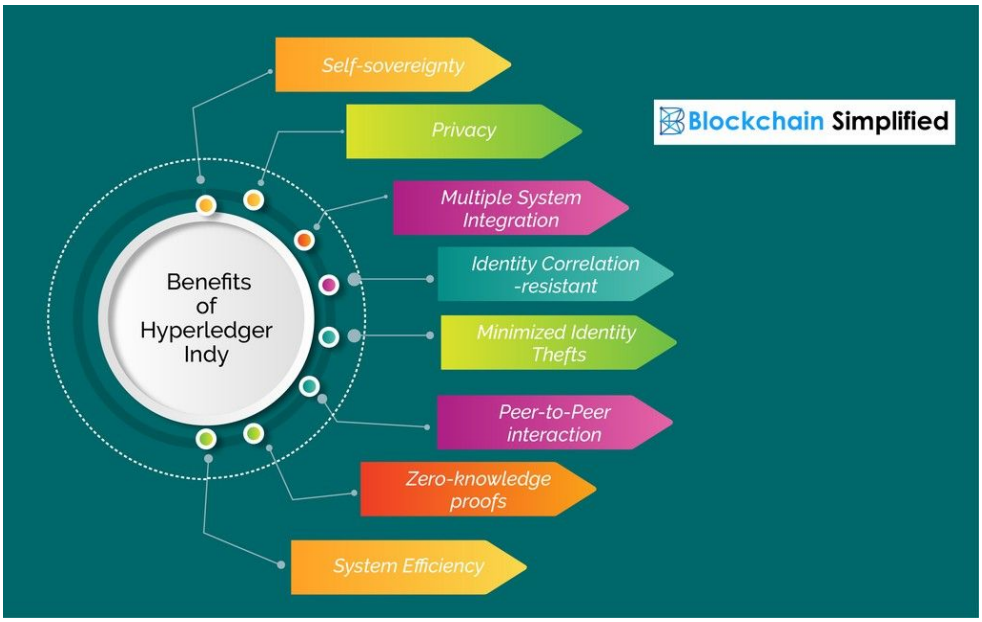
- Fabric CA(Fabric Certification Authority)

  Fabric CA는 하이퍼레저 패브릭을 위한 인증기관이다. 네트워크 참가자를 등록하고 이들을 위한 디지털 인증서 및 공개 키를 발급하는 역할을 한다.

3.1.4. Hyperledger Indy

Hyperledger Indy는 개인 정보 보호, 보안 및 사용자 제어를 강화하는 데 사용할 수 있는 분산 ID 시스템을 구축하기 위한 플랫폼을 제공하고 다른 DID 플랫폼과의 주요 차이점은 빠르고 안전하며 내결함성이 있도록 설계된 Plenum 합의 프로토콜을 사용한다는 것이다.

이를 통해 노드 장애 또는 공격이 발생하는 경우에도 원장이 안정적으로 유지된다고 한다. 또한 Hyperledger Indy는 영지식 증명 사용을 지원하여 프라이버시를 손상시키지 않고 신원 속성을 선택적으로 공개할 수 있다.



[그림9] Hyperledger Indy 장점

3.2. 개발 환경 및 기술 스택

3.2.1. 개발 도구

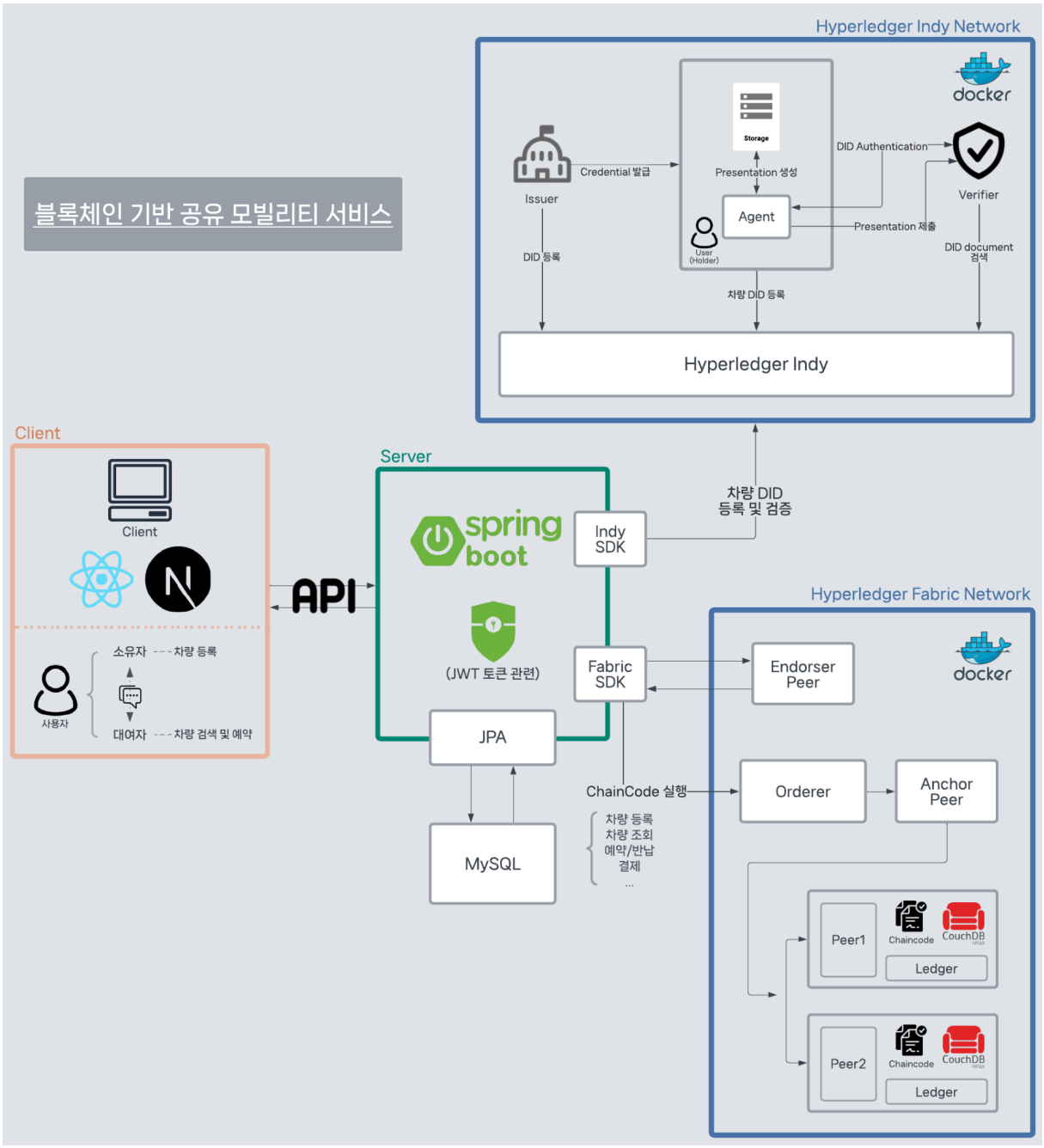
분류	단위	이름
블록체인 (신원식별)	플랫폼	Hyperledger Indy
블록체인	플랫폼/인프라	Hyperledger Fabric
Web Client	Front-end	React.js, Next.js
API Server	Back-end	Spring Boot
API Document Server	Document/Test	Swagger

3.2.2. SW

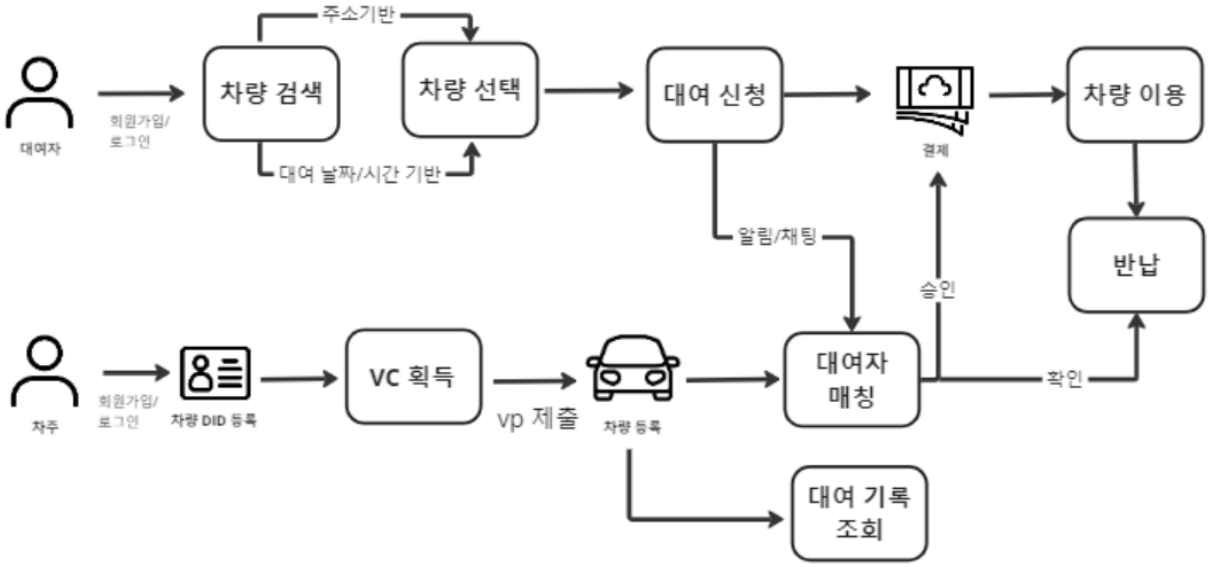
이름	내용
docker	블록체인 가상 환경
docker-compose	여러 docker container 정의 및 실행 도구
CouchDB	state database
npm / yarn	패키지 관리자
MySQL	사용자, 서비스 관련 database
git	버전 관리 시스템

3.3. 시스템 구성

- 시스템 구성도



- 서비스 흐름도 (클라이언트)



4. 개발 일정 및 역할 분담

4.1. 개발 일정

	5월					6월					7월				8월					9월			
업무	1주	2주	3주	4주	5주	1주	2주	3주	4주	5주	1주	2주	3주	4주	1주	2주	3주	4주	5주	1주	2주	3주	4주
사전 조사 및 블록체인 스터디																							
서비스 기획																							
착수 보고서 작성																							
요구사항 분석 및 개발범위 산정																							
블록체인 네트워크 구축																							
체인코드 개발																							
UI 디자인																							
서버 환경 구축																							
클라이언트 개발																							
중간 보고서 작성																							
API 연동																							
테스트 및 디버깅																							

결과 보고서 작성																					
발표 포스터 제작																					

4.2. 역할 분담

이름	역할
김돈우	- 블록체인 네트워크 구축(Indy) - 서버환경 구축(Spring)
이지현	- 클라이언트 UI 설계 및 기능 개발(React.js) - 블록체인 네트워크 구축(Fabric)
최세희	- 블록체인 네트워크 구축(Indy, Fabric) - 블록체인 체인코드 개발
공동	- 테스트 및 디버깅 - 보고서 작성