

1. Team Info

1.1 과제명

암표 근절을 위한 DID 및 NFT 기반 티켓팅 시스템, WE-Ticket

1.2 팀 정보

팀 번호-이름 : 04 -Typha (타이파)

1.3 팀 구성원

- 황지은(2376329): 리더, 백엔드(인증·티켓팅 시스템) 및 블록체인(티켓팅 시스템) 설계·구현, 티켓 예매 (예매 동시성 처리 및 좌석 점유 타임아웃 처리) 검증
- 정혜교(2176355): 팀원, 기획, 프론트엔드 및 블록체인(티켓팅·입장 시스템) 설계·구현, 사용자 시나리오 검증
- 이원주(2176278): 팀원, DB 및 백엔드(양도·기반 시스템) 설계·구현, 트랜잭션 원자성 (티켓 예매 데이터 생성 및 양도 소유권 이전) 검증

2. Project-Summary (과제 요약)

2.1 문제 정의

K-POP 공연에서는 암표 거래, 즉 허가된 시스템 외 거래로 공정한 입장권 구매를 방해하는 문제가 심각하다. 팬들은 절박한 마음으로 위험을 감수하고 암표를 구매하려다 사기 피해에 노출된다. 암표 문제 해결을 위해 공연 기획사는 많은 비용과 인력을 투입하지만, 과도한 본인 확인으로 성과 없이 팬들의 인권만 침해되는 실정이다. 이는 기획사의 브랜드 손상으로 돌아오며, 이러한 악순환이 계속되고 있다.

따라서 기존의 티켓팅 및 입장 관리 시스템은 암표 방지 실효성 부족, 기획사의 현장 운영 비용 낭비, 실소비자의 개인정보 주권 침해라는 구조적 한계를 가지고 있으며, 이를 해결하기 위한 새로운 기술적 접근이 절실히 요구된다. WE-Ticket 은 K-POP 공연 기획사를 타겟 고객으로 하여, 티켓 소유권을 기술적으로 완벽하게 보장하여 암표를 근절하면서도 현장 운영 효율성과 개인정보 보호를 동시에 실현하는 것을 핵심 과제로 삼는다.

2.2 기존 연구와의 비교

Yes24 등 전통적 티켓팅 플랫폼과 ticket N 등 기존 전자 티켓 플랫폼은 사용자에게 익숙한 플랫폼이지만, 검표 시 티켓 소유권을 확실히 검증하기 어렵다. QR 코드는 캡처를 통한 불법 양도가 가능하며, 휴대전화 인증 역시 타인 명의 도용이 가능하다. 반면 WE-Ticket 은 소유자 외 타인의 사용을 원천적으로 차단하는 완전한 소유권 증명 체계를 구축한다.

모던라이언 등 일반 NFT 티켓 플랫폼은 압표 해결을 위해 블록체인 기술을 도입했다는 점에서 의의가 있으나 입장 지연 문제가 여전하다. 실물 신분증 대조를 병행하거나, NFT 티켓 인식 시스템이 미비했기 때문이다. 그러나 WE-Ticket 은 1 초 간편 입장이 가능하다.

2.3 제안 내용

WE-Ticket 은 DID(분산 신원 증명)과 NFT 로 티켓 전 과정(예매, 발급, 소유권 관리, 양도, 입장)을 재설계한, 새로운 티켓팅 시스템이다.

첫째, 가장 핵심인 입장 시스템이다. 공연 입장 시 DID 와 생체 인증을 결합해 신원 및 티켓 소유권을 검증한다. 이를 통해 실물 신분증 대조나 개인정보 노출 없이, 휴대폰 NFC 탭만으로 1 초 간편 입장을 제공한다.

둘째, 인증 시스템에서는 본인 인증으로 신원을 확인하고 DID 를 생성한다.

셋째, 티켓팅 시스템에서는 위변조 불가능한 NFT 티켓을 발행하여, 티켓의 명확한 소유권을 보장한다.

넷째, 양도 시스템에서는 통제된 환경에서 합법적인 ‘소유권 이전’을 기술적으로 구현한다.

본 솔루션은 사용자 인증 수준에 따라 차별화된 서비스를 제공한다. 간편 인증을 통한 일반 사용자는 티켓팅 및 입장이 가능하며, 모바일 신분증을 통한 추가 본인 확인을 완료한 사용자는 양도까지 이용할 수 있다.

2.4 기대 효과 및 의의

본 프로젝트로 공연 티켓팅 혁신을 넘어, 산업 전반에 걸친 파급 효과를 기대할 수 있다. 첫째, 사회적 가치 측면에서 암표를 80% 근절하여 소비자 피해를 근본적으로 줄인다. 둘째, 경제적 가치 측면에서 공연 기획사의 운영비를 30% 절감하고, 합법 양도 수수료 및 NFT 기반 부가 서비스로 신규 수익원을 기존 매출 대비 10% 더 창출한다. 셋째, 산업 확장성 측면에서 장기적으로 스포츠, 컨퍼런스 등 다양한 이벤트 시장으로 확장 가능하며, DID 기반의 자기주권 신원 체계는 글로벌 디지털 신원 관리 인프라와도 연결될 수 있다. 넷째, 기술적 가치 측면에서 DID·VC·NFT 를 결합한 새로운 형태의 신원 및 소유권 관리 구조를 제시하여, 글로벌 블록체인 및 Web3 생태계와도 연동될 수 있다.

2.5 주요 기능 리스트

2.5.1 인증 시스템

- ① 내 인증 레벨 조회: DB 에서 사용자의 인증 레벨을 조회한다.
- ② 본인인증 시행 및 정보 저장: OmniOne CX 로 본인인증을 한 후 개인정보와 인증 레벨을 DB 에 저장한다.
- ③ DID Document 등록: 사용자 기기에서 DID Document 를 생성하고 블록체인에 등록한다.
- ④ 추가 본인 확인 약관 동의 수집: 양도 시스템 이용을 위한 추가 본인 확인 관련 동의 제출을 처리한다.

2.5.2 입장 시스템

- ① 일회성 인증값(Nonce) 발행: 사용자가 특정 게이트를 통해 공연장 입장을 요청할 때, 해당 요청의 유효성을 검증하고 임시 nonce 값을 발행한다.
- ② DID 기반 입장 인증: 인증된 사용자가 제출한 DID 인증 문서를 기반으로 공연 입장을 승인/거부한다.

2.5.3 티켓팅 시스템

- 1) 공연 조회
 - ① 전체 공연 목록 조회: 전체 공연 목록을 조회하며, genre 파라미터로 특정 장르의 공연만 필터링할 수 있다.
 - ② 인기 공연 목록 조회: 가장 인기있는 공연 3 개 목록을 조회하여 제공한다.
 - ③ 예매 가능 공연 목록 조회: 현재 예매 가능한 공연 목록을 조회하여 제공한다.
 - ④ 공연 세부 정보 조회: 특정 공연의 세부 정보(티켓 오픈 일시, 매진 여부 등)를 조회한다.
- 2) 티켓 예매
 - ① 공연 회차 및 좌석 정보 조회: 특정 공연의 회차 정보와 좌석 상세 정보를 조회한다.
 - ② 티켓 예매 및 NFT 발행: 티켓 결제 및 예매를 진행하며, 해당 티켓을 블록체인 기반의 NFT 로 등록한다.
 - ③ 티켓 예매 취소: 티켓 예매 취소 및 환불을 처리한다.

2.5.4 양도 시스템

- 1) 양수인
 - ① 양도 마켓 목록 조회: 양도 마켓 접속 시 공개 양도 티켓 목록을 조회한다.
 - ② 양도 티켓 세부 정보 조회: 특정 양도 티켓의 세부 정보(공연, 양도 가격 등)을 조회한다.
 - ③ 양도 이행: 양도 티켓 결제 및 양도 이행을 진행하여, DB 에서 티켓 소유권을 이전한다.
 - ④ 고유 식별코드로 비공개 양도 티켓 조회: 고유 식별코드를 통해 비공개 양도 티켓의 기본키를 조회한다.
- 2) 양도인
 - ① 비공개 양도 티켓의 고유 식별코드 조회: 비공개 양도 티켓의 최신 고유 식별코드와 식별코드 만료일시 정보를 조회한다.
 - ② 비공개 양도 티켓의 고유 식별코드 재발급: 비공개 양도 티켓의 고유 식별코드를 새로 발급한다.
 - ③ 양도 등록: 본인 소유 티켓을 양도 등록한다.

- ④ 양도 취소: 등록된 양도 티켓을 취소한다.
- ⑤ 양도 공개 여부 변경: 양도 방식을 공개 또는 비공개로 전환한다.
- ⑥ 양도 등록 완료한 내 티켓 목록 조회: 본인이 등록한 양도 티켓 목록을 조회한다.
- ⑦ 양도 등록 가능한 내 티켓 목록 조회: 양도 등록할 수 있는 본인 소유 티켓 목록을 조회한다.

2.5.5 기반 시스템

- 1) 회원 관리
 - ① 회원가입: 신규 회원가입을 처리한다.
 - ② 계정 탈퇴: 로그인된 사용자의 회원 탈퇴를 처리한다.
 - ③ 아이디 및 전화번호 중복 체크: 회원가입 시 데이터 중복 여부를 확인한다.
 - ④ 로그인/로그아웃: JWT 토큰을 이용하여 로그인, 로그아웃을 처리한다.
 - ⑤ ID/PW 찾기: 전화번호를 통한 ID 찾기, 전화번호와 ID 를 통한 PW 재설정을 제공한다.
- 2) 마이페이지
 - ① 내 티켓 세부 정보 조회: 본인 소유 티켓의 상세 정보를 조회한다.
 - ② 내 티켓 목록 조회: 본인이 현재 소유한 티켓 목록을 조회한다.
 - ③ 내 구매 이력 조회: 본인의 구매 이력을 조회한다. 티켓 취소 또는 양도 판매로 소유권을 잃은 티켓까지 보여준다.
 - ④ 마이페이지 정보 조회: 사용자의 마이페이지 정보(소유한 티켓 개수, 구매 이력 개수 등)을 조회한다.
 - ⑤ 1 대 1 문의 등록: 1:1 문의를 등록한다.

3. Project-Design (과제 설계)

3.1 요구사항 정의

WE-Ticket 은 DID 및 NFT 기술을 적용하여 공연 티켓 소유권 보장, 암표 거래 근절, 개인정보 보호를 목표로 한다.

3.1.1 기능별 상세 요구사항

1) 사용자 인증 및 신원 관리

- ① 사용자는 스마트폰을 통해 DID 를 발급받고, 단계별 인증 절차(간편 인증, 모바일 신분증 인증 등)를 수행해야 한다
- ② 본인 확인 과정은 생체 인증과 DID 결합을 통해 이루어져야 하며, 타인의 대리 사용을 원천적으로 차단해야 한다.

2) 티켓 발급 및 관리

- ① 공연 기획사가 설정한 회차·좌석 정보를 기반으로 NFT 티켓을 발급한다.
- ② 발급된 NFT 는 소유자 DID 와 매핑되며, 1 인 1 티켓 원칙이 시스템적으로 보장되어야 한다.

3) 양도 기능 제공

- ① 사용자 간 합법적이고 안전한 양도가 가능해야 한다.
- ② 공개 양도 (마켓 기반)과 비공개 양도 (고유 코드 기반)을 지원하며, 모든 양도 내역은 기록, 추적 가능해야 한다.

4) 입장 시스템

- ① 공연장 입장 시 NFC 태깅과 DID 기반 생체 인증을 통해 소유권과 본인 여부를 1 초 이내에 검증해야 한다.
- ② 검증 과정은 블록체인 및 중앙 서버 이중 확인 구조를 갖추어야 하며, 복제, 위변조 가능성을 원천적으로 차단해야 한다.

5) 보안성

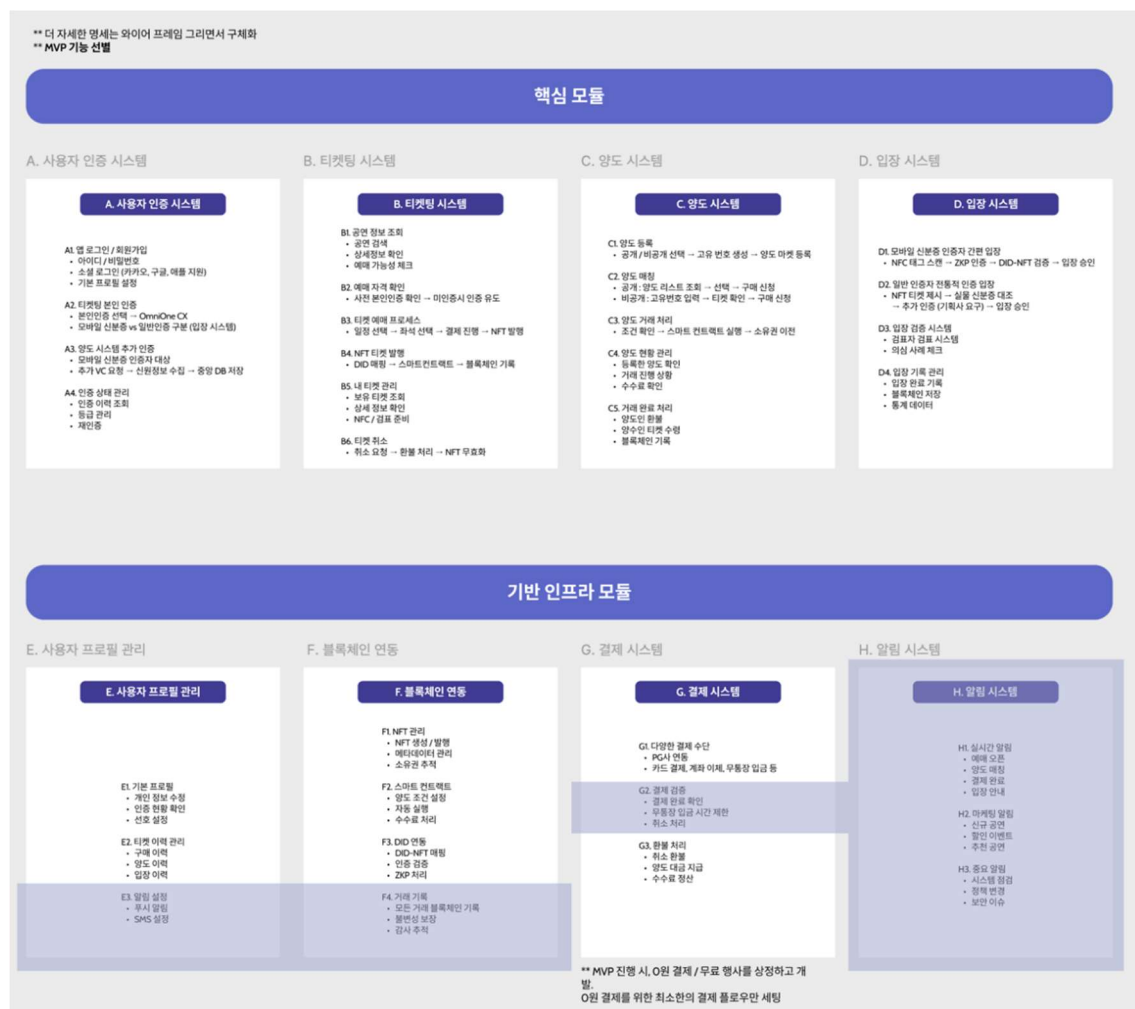
- ① 고유 CI 하나당 하나의 계정만 인증되어야 한다.
- ② 한 계정당 하나의 모바일 기기만 접속이 허용되어야 한다.

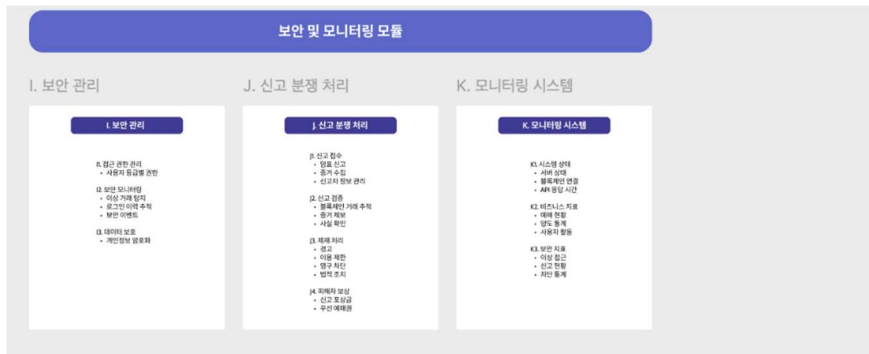
6) 사용자 경험

① 기존 티켓팅 앱과 유사한 인터페이스를 제공하여 사용자가 별도 학습 없이 직관적으로 사용할 수 있어야 한다.

② 예매, 결제, NFT 발행, 입장 인증까지의 전체 흐름이 끊김 없이 자연스럽게 이어져야 한다.

3.1.2 설계 모델 (모듈 명세서)





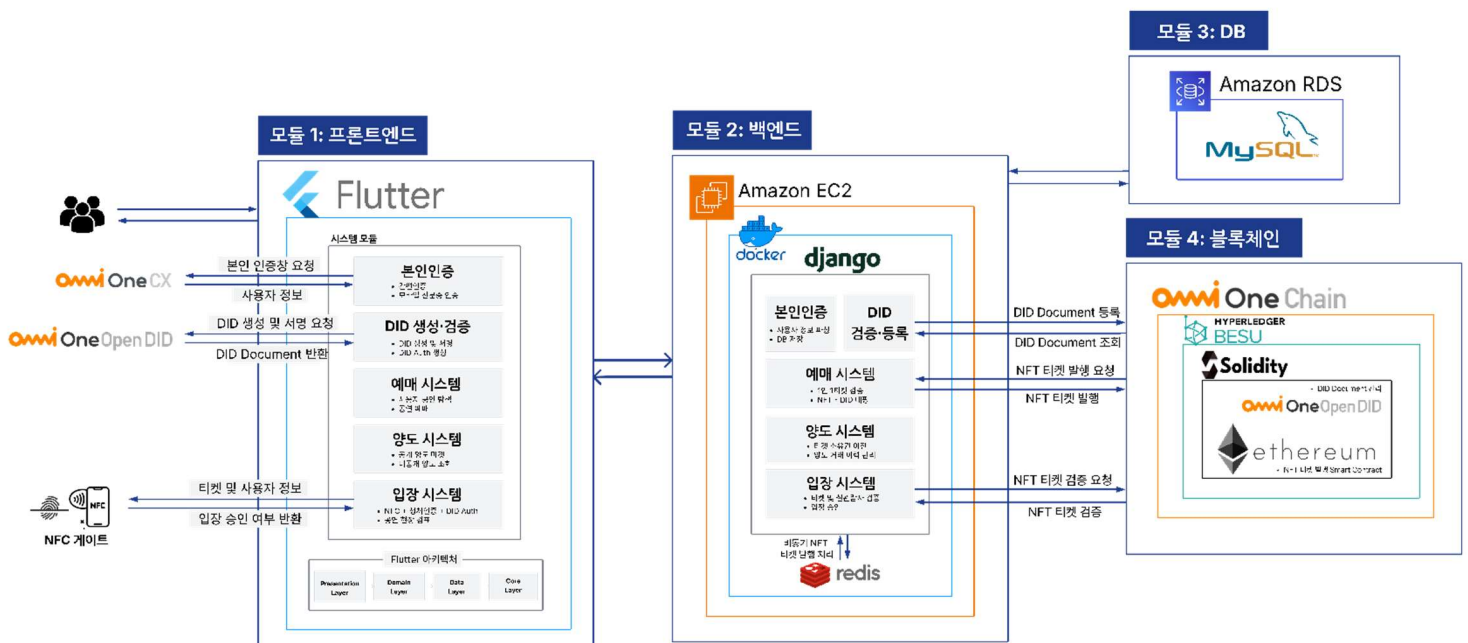
3.2 전체 시스템 구성

3.2.1 전체 시스템 아키텍처

클라이언트: Flutter 앱은 OmniOne Open DID 와 연동하여 분산 신원(DID) 발급 및 간편 입장을 제공하며, OmniOne CX 를 통해 사용자 인증을 수행한다.

서버: AWS EC2 의 Docker 환경에서 Django 가 구동되며, Redis 를 활용한 비동기 NFT 발행 처리와 MySQL 기반 RDS 를 통한 데이터 관리를 담당한다.

블록체인: OmniOne Chain 은 HyperLedger Besu 에서 Solidity 스마트 컨트랙트가 구동되어, Ethereum ERC-721 표준을 활용한 NFT 발행, OmniOne OpenDID 를 커스터마이징한 We-Ticket 자체 DID 관련 처리를 수행한다.



3.2.2 핵심 모듈 구성

WE-Ticket 은 인증, 티켓팅, 양도, 입장 시스템의 네 가지 핵심 모듈로 구성된다. 현재 인증 시스템, 티켓팅 시스템까지 구현된 상태이다.

1) 인증 시스템

서비스 접근 권한을 단계적으로 차등화한다. 미인증 사용자는 콘텐츠 조회만 가능하며, 일반 인증 사용자는 간편 인증 또는 모바일 신분증 인증을 통해 티켓 예매 및 입장이 가능하다. 안전 인증 단계에서는 모바일 신분증 인증을 통한 추가 본인확인을 거쳐 양도 기능을 이용할 수 있다. 인증 완료 시 사용자 스마트폰 내에서 DID 및 DID Document 와 Key Pair 가 생성되고, 서버 검증을 거쳐 블록체인에 등록된다.

2) 입장 시스템

본 프로젝트의 핵심 기술로, 사용자가 공연장 입구에서 스마트폰을 NFC 로 태그하면 생체 인증이 활성화된다. 생체 인증 통과 시 Auth DID 객체 생성 및 서명을 진행하여 서버에 전달한다. 서버는 클라이언트로부터 받은 Auth DID 를 기반으로 블록체인에서 DID 공개키를 조회하고 서명 검증을 수행한다. 동시에 해당 DID 의 사용자와 티켓 간의 관계를 확인하여 본인 소유 여부를 확정하고 입장을 승인한다.

3) 티켓팅 시스템

회차 및 좌석 선택 후 NFT 티켓을 발행하며, 해당 NFT 는 사용자의 변형된 CI 와 중앙 DB 에서 연결되어 관리된다. 이를 통해 실시간 소유권 검증과 1 인당 티켓 수 제한 정책을 기술적으로 구현한다.

4) 양도 시스템

안전 인증을 완료한 사용자만 이용할 수 있으며, 모든 양도 내역을 기록한다. 양도는 2 가지 방식을 지원한다. 공개 양도 시 마켓에 공개되고, 누구나 양도받을 수 있다. 비공개 양도 시 고유 식별코드(UUID, 24 시간 유효)가 발급되고, 해당 코드를 아는 사람만 양도받을 수 있다.