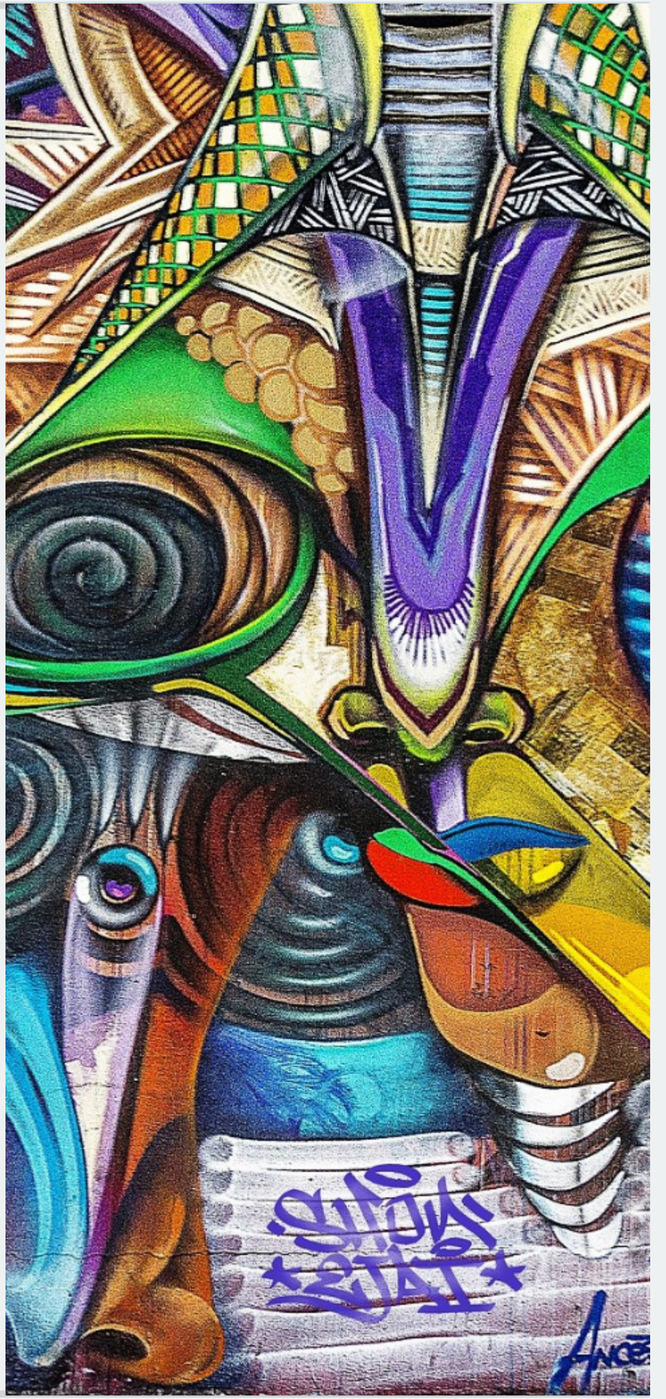
하나Art

보안을 강화한,

소액투자를 위한 미술품 공동구매 플랫폼

하나금융티아이 교육생

광명융합기술교육원 조세진



1. 미술품 공동구매 플랫폼 하나아트란?

아트테크의 관심 증가

금융
생활밀착형 플랫폼

01

미술품
공동구매 플랫폼

데이터 유실,
조작 위험성

02

블록체인의 형태로
구매내역 저장

번거로운
예치금 이체 절차

03

예치금
자동이체 서비스

2. 하나아트의 서비스 기능

사용자

계좌	공동구매	아트스캔	회원정보
자동이체 설정	공동구매 작품 조회	전체 블록 조회	구매 내역 확인
예치금 입금	구매	전체 트랜잭션 조회	매각 상품 수익률 확인
계좌 조회	소유자 현황	My Wallet 검색	온라인 권리증 확인
예치금 조회	매각 진행현황		회원정보 조회
	공지 확인		

관리자

작품 및 작가 관리	데이터 조회
공동구매 작품 등록	로그 데이터
매각 투표 진행	사용자 현황 데이터
공동구매 작품 등록	
수익 분배	
작가 등록	
공지 등록	

3. 프로젝트 일정

☑ 아이디어 및 설계 2021.09.06 ~ 09.12

- 메뉴 체계 및 요구사항 명세서
- ERD, Class Diagram, Flow Chart

☑ 개발 진행 2021.09.13 ~ 09.30

- 개발 환경 세팅 및 개발 진행

☑ 테스트 및 수정 2021.09.29 ~ 10.02

Monthly planning

4. 개발환경 및 시스템 아키텍처

언어

Java JSP JavaScript R SQL PL/SQL

프레임워크

spring spring boot MyBatis Bootstrap

DB

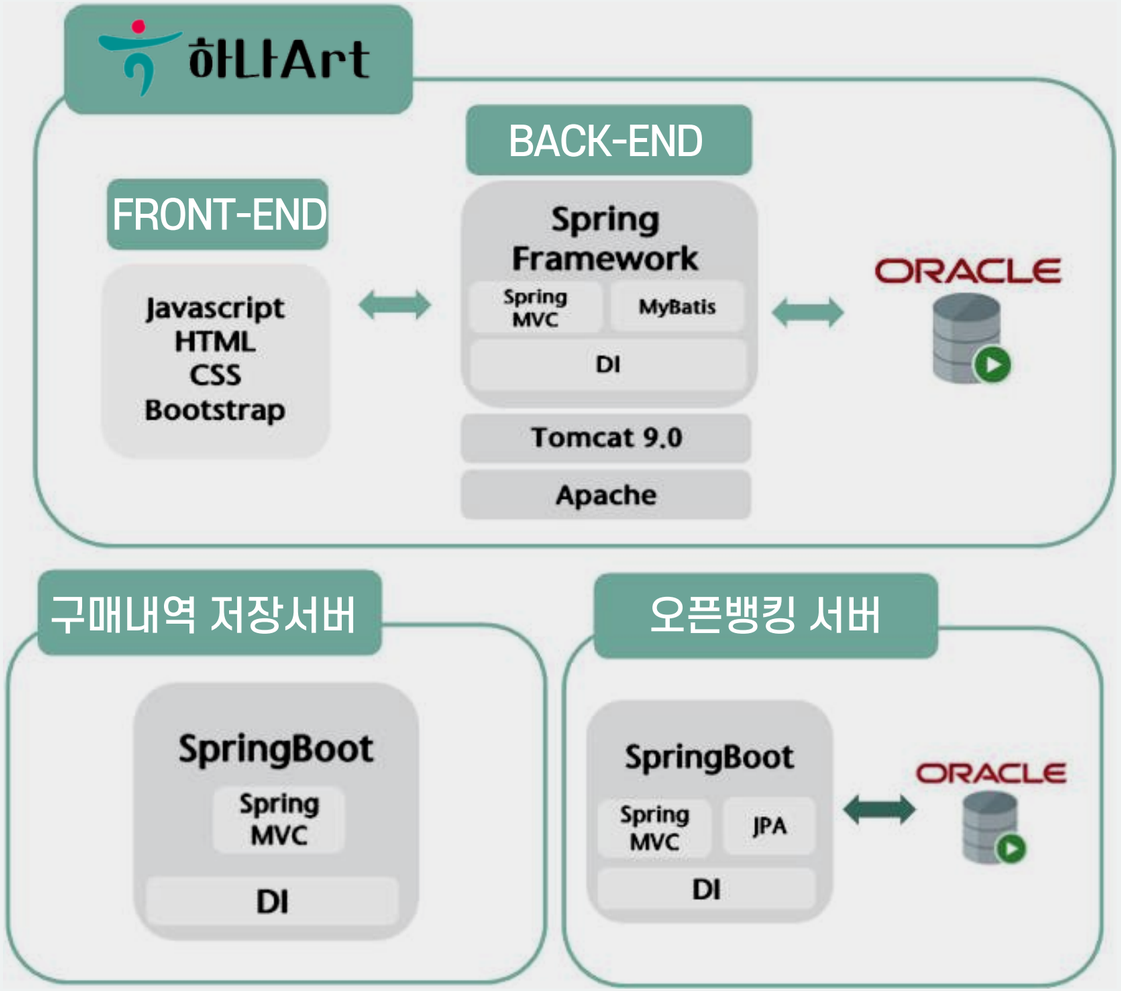
ORACLE DATABASE

형상관리

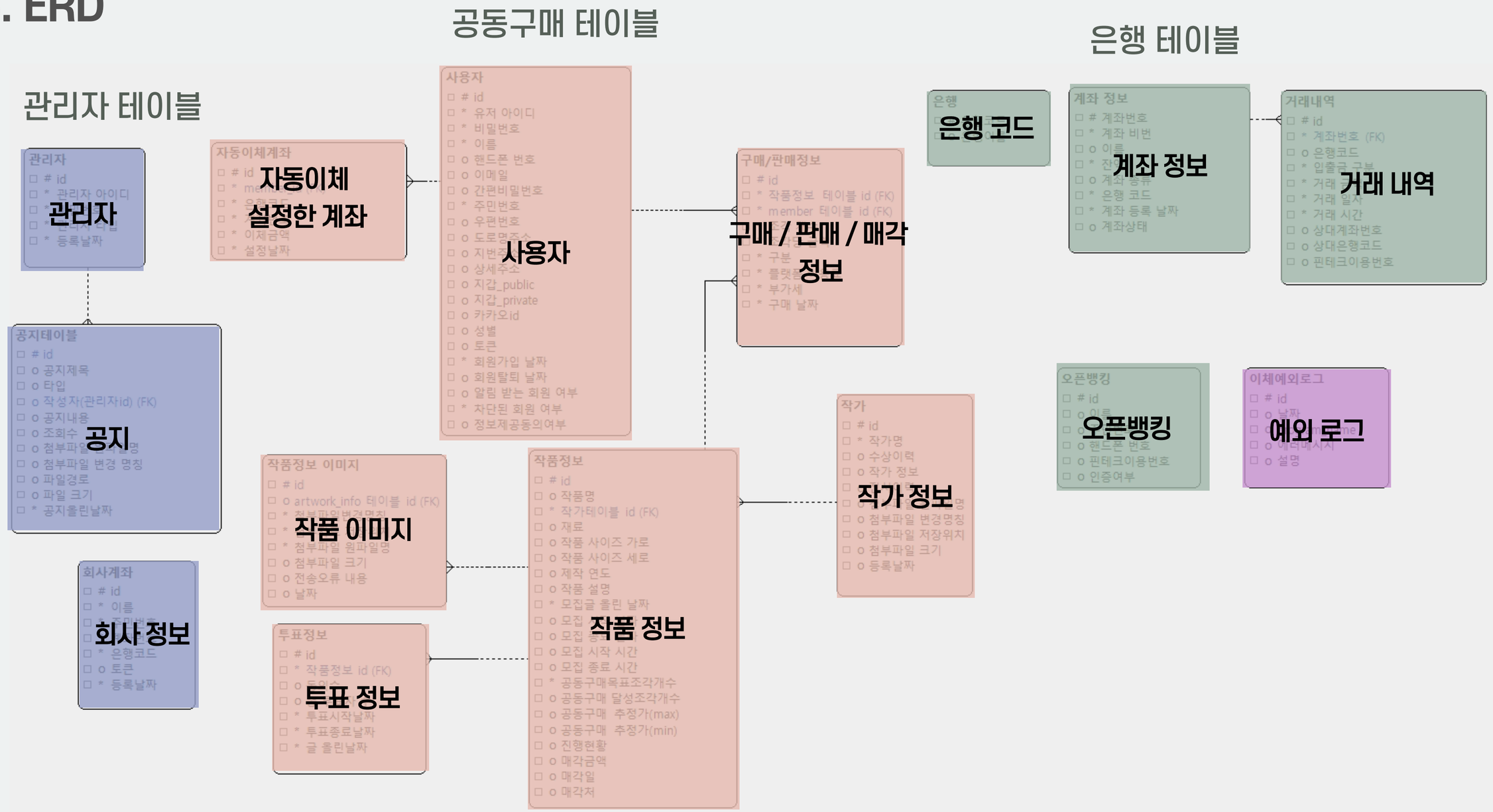
GitHub SourceTree

서버

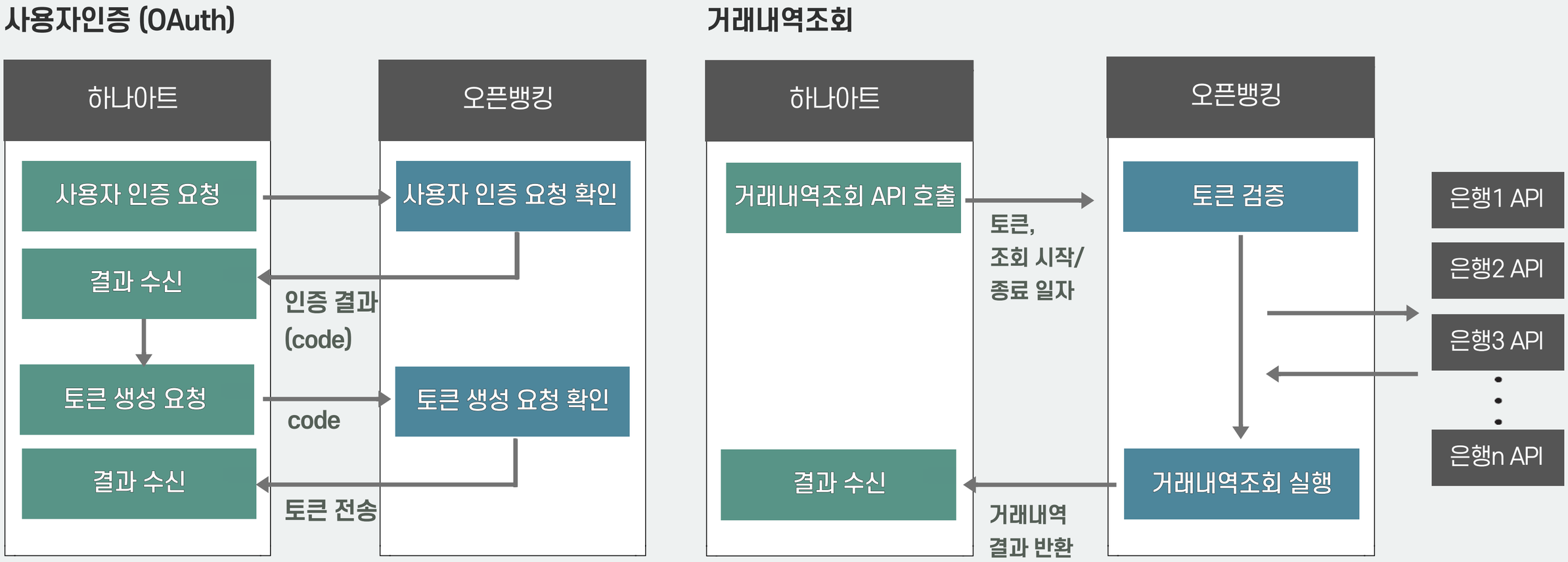
Apache Tomcat



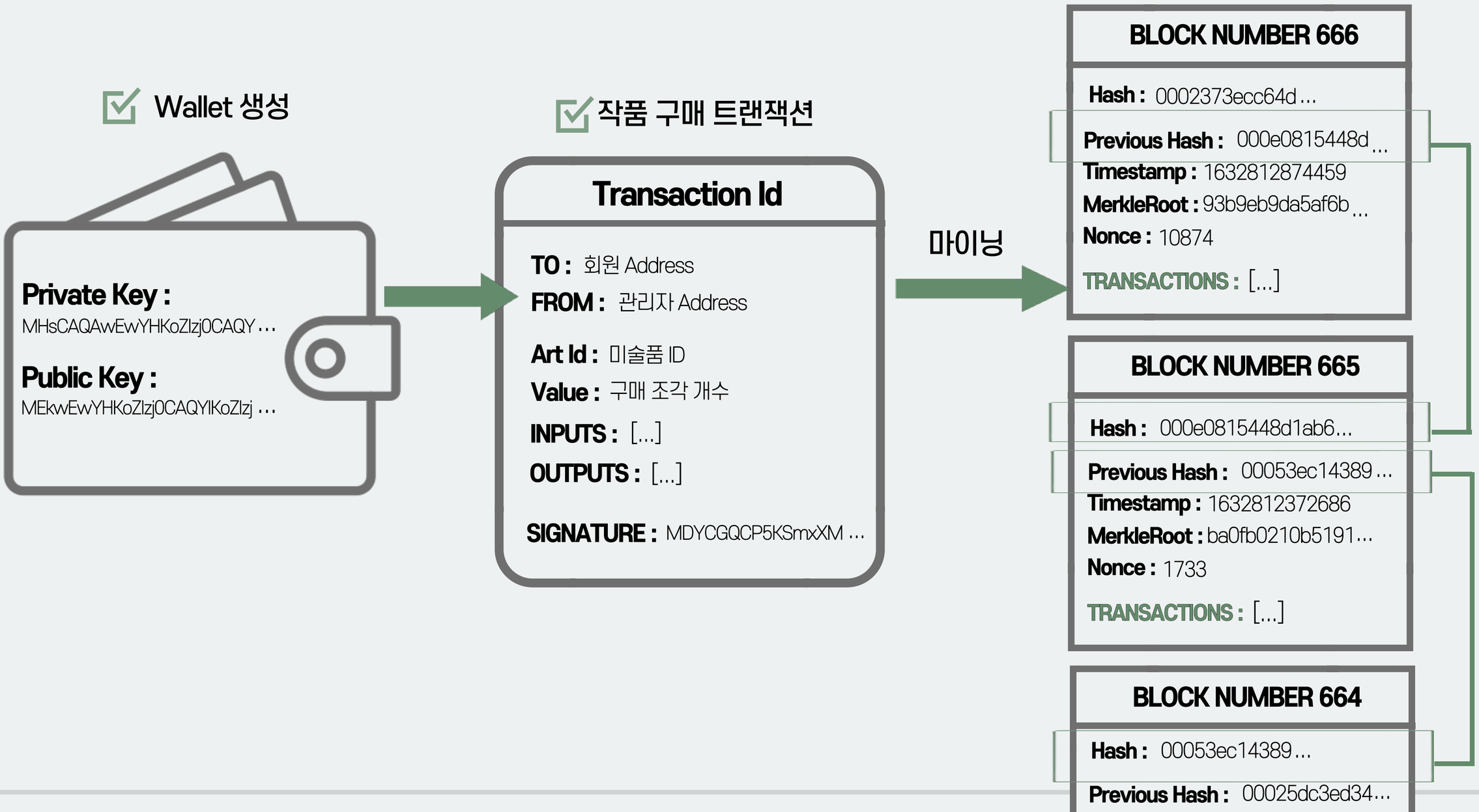
5. ERD


공동구매 테이블
은행 테이블
관리자 테이블
관리자
□ # id
□ * 관리자 아이디
□ * 등록날짜
관리자
자동이체계좌
□ # id
□ * 이체금액
□ * 설정날짜
자동이체
설정한 계좌
사용자
□ # id
□ * 유저 아이디
□ * 비밀번호
□ * 이름
□ o 핸드폰 번호
□ o 이메일
□ o 간편비밀번호
□ * 주민번호
□ o 우편번호
□ o 상세주소
□ o 지갑_public
□ o 지갑_private
□ o 카카오id
□ o 성별
□ o 토큰
□ * 회원가입 날짜
□ o 회원탈퇴 날짜
□ o 알림 받는 회원 여부
□ * 차단된 회원 여부
□ o 정보제공동의여부
사용자
구매/판매정보
□ # id
□ * 작품정보 테이블 id (FK)
□ * member 테이블 id (FK)
□ * 구분
□ * 플랫폼
□ * 부가세
□ * 구매 날짜
구매 / 판매 / 매각
정보
은행
은행코드
계좌 정보
□ # 계좌번호
□ * 계좌 비번
□ o 이름
□ * 잔액
□ o 계좌 종류
□ * 은행 코드
□ * 계좌 등록 날짜
□ o 계좌상태
계좌 정보
거래내역
□ # id
□ * 계좌번호 (FK)
□ o 은행코드
□ * 입출금 구분
□ * 거래 금액
□ * 거래 일자
□ * 거래 시간
□ o 상대계좌번호
□ o 상대은행코드
□ o 핀테크이용번호
거래 내역
공지테이블
□ # id
□ o 공지제목
□ o 타입
□ o 작성자(관리자id) (FK)
□ o 공지내용
□ o 조회수
□ o 첨부파일 원파일명
□ o 첨부파일 변경 명칭
□ o 파일경로
□ o 파일 크기
□ * 공지올린날짜
공지
작품정보 이미지
□ # id
□ o artwork_info 테이블 id (FK)
□ * 첨부파일변경명칭
□ * 첨부파일 경로
□ * 첨부파일 원파일명
□ o 첨부파일 크기
□ o 전송오류 내용
□ o 날짜
작품 이미지
작품정보
□ # id
□ o 작품명
□ * 작가테이블 id (FK)
□ o 재료
□ o 작품 사이즈 가로
□ o 작품 사이즈 세로
□ o 제작 연도
□ o 작품 설명
□ * 모집글 올린 날짜
□ o 모집 인원
□ o 모집 방식
□ o 모집 시작 시간
□ o 모집 종료 시간
□ * 공동구매목표조각개수
□ o 공동구매 달성조각개수
□ o 공동구매 추정가(max)
□ o 공동구매 추정가(min)
□ o 진행현황
□ o 매각금액
□ o 매각일
□ o 매각처
작품 정보
작가
□ # id
□ * 작가명
□ o 수상이력
□ o 작가 정보
□ o 첨부파일 변경명칭
□ o 첨부파일 저장위치
□ o 첨부파일 크기
□ o 등록날짜
작가 정보
회사계좌
□ # id
□ * 이름
□ * 은행코드
□ o 토큰
□ * 등록날짜
회사 정보
투표정보
□ # id
□ * 작품정보 id (FK)
□ * 투표시작날짜
□ * 투표종료날짜
□ * 글 올린날짜
투표 정보
오픈뱅킹
□ # id
□ o 이름
□ o 핸드폰 번호
□ o 핀테크이용번호
□ o 인증여부
오픈뱅킹
이체에외로그
□ # id
□ o 날짜
□ o 에러메시지
□ o 설명
예외 로그

6. 응용기술 - 오픈뱅킹(OAuth, JWT)



6. 응용기술 - 블록체인의 형태로 구매정보 저장



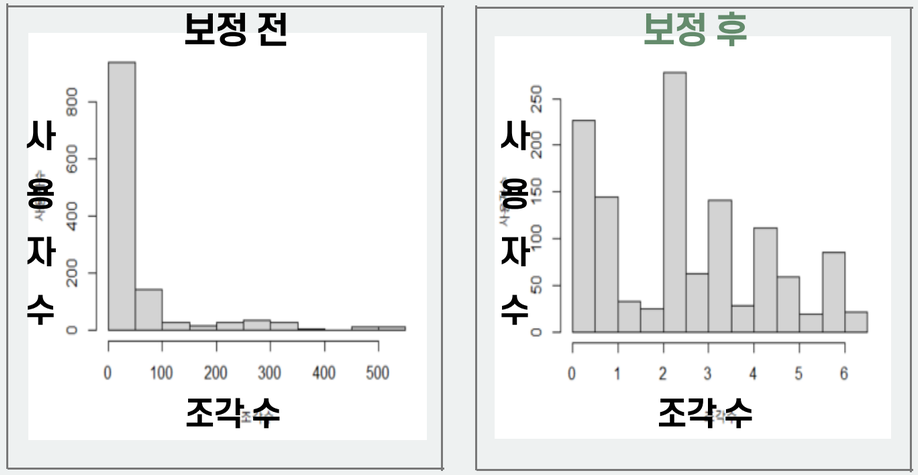
6. 응용기술 - 협업필터링을 사용한 추천서비스

☑ **사용 데이터 : 작품마다 구매한 조각 수**

- 5작품 이상 구매한 사용자의 데이터만 추출

데이터 보정

* 로그변환



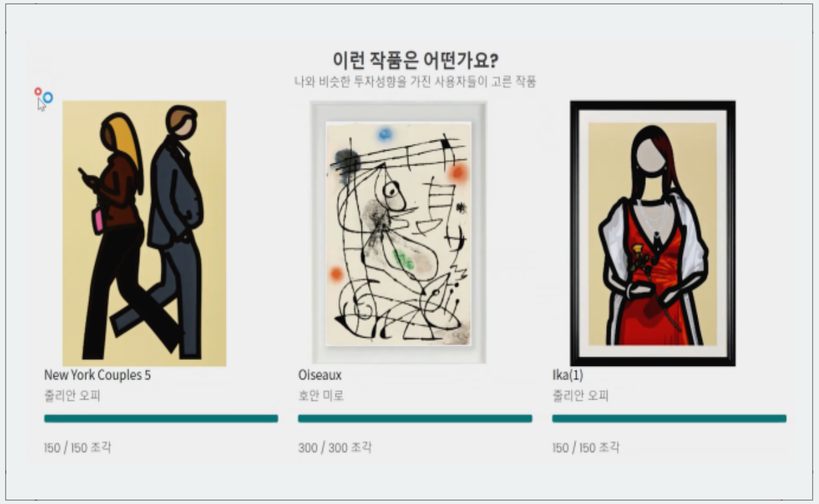
모델평가 및 최적모델 선택

* k-fold cross validation , F1 Score

- 스케줄러를 사용하여
하루마다 최적모델 선택하여 모델 저장

작품 추천

- 저장된 모델을 사용하여 작품추천 진행



6. 응용기술 - 그 외의 사용 기술

PL/SQL - 이체 함수

- 예외 정보를 담는 table에 로그 생성
- return 값으로 성공 실패 여부 판단
- 트랜잭션

크롤링 - 아트테크 기사

아트테크와 관련 기사 크롤링하여
메인 페이지에서 보여줌

웹소켓 - 실시간 알림

관리자가 작품을 등록 시
사용자 페이지에서 알림

log4j - 로그 데이터 관리

로그 데이터는 파일로 저장하고 매일 새로운 파일이 생성

스케줄러- 자동이체

사용자가 설정한 계좌와 금액에 따라서 자동 이체

카카오 메시지 API / 문자

자동이체 설정 내용, 매각진행현황 알림

7. 시나리오 요약

01 기존회원 작품구매

작품 구매 — 구매 확인 — <메인페이지> - 추천작품 확인 - 아트테크 기사 확인 — 관리자 작품 등록 — 친구에게 작품 추천

관리자

02 신규회원 예치금 자동이체

계좌 조회 — 예치금 자동이체 설정

03 작품 매각 진행

매각투표 — 매각 결정 — 매각 진행 현황 확인 — 수익률 확인

☑ 시연 영상

8. 느낀점 및 앞으로의 방향성

끊임없이 고찰하는 개발자가 되겠습니다.

01

외부 API, 라이브러리 사용 시 공식문서의 중요성

02

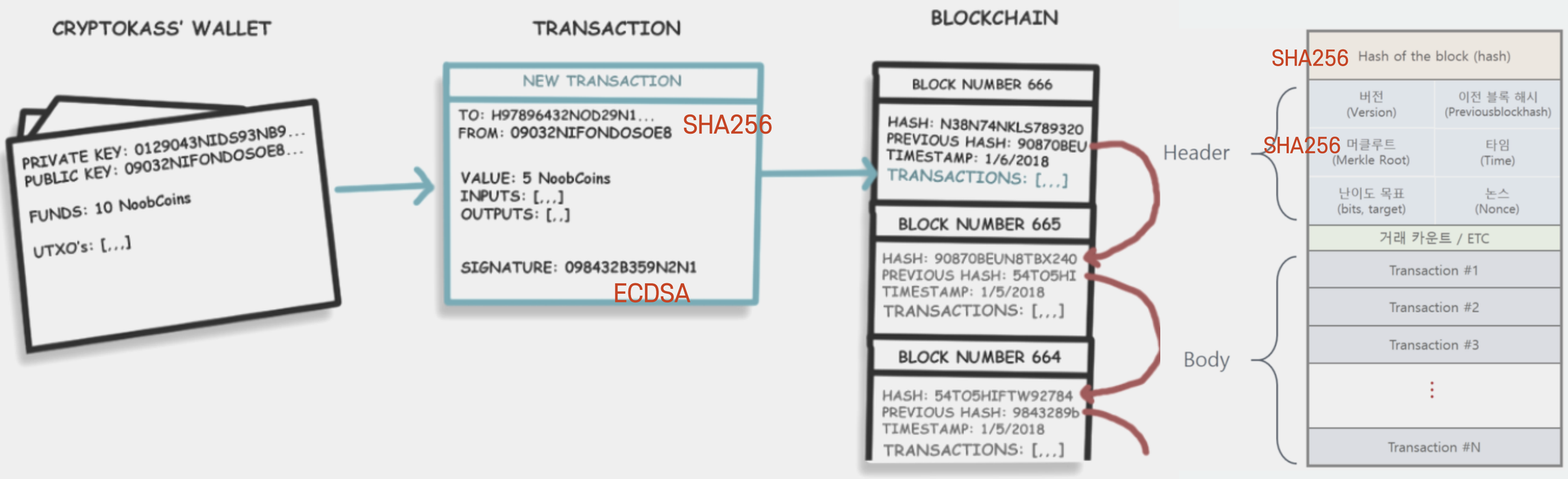
기술의 원리, 사용 목적의 명확한 이해

03

통계학과 개발자

Q & A

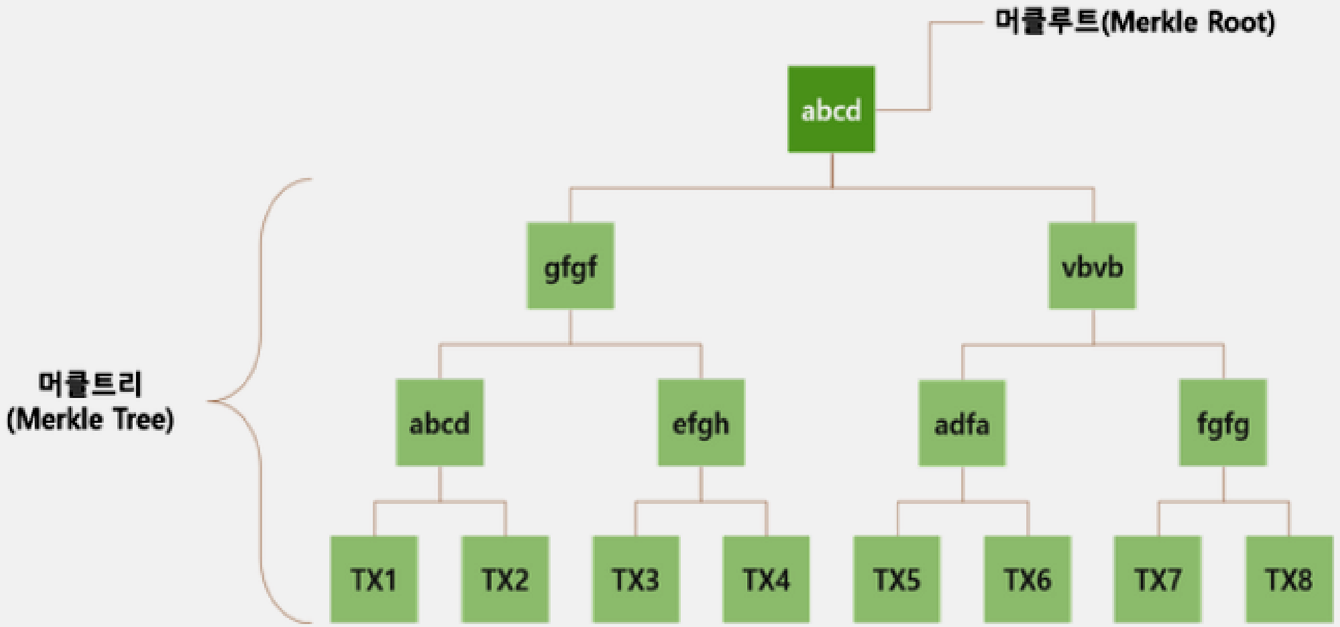
블록체인 추가 설명


CRYPTOKASS' WALLET
PRIVATE KEY: 0129043NIDS93NB9...
PUBLIC KEY: 09032NIFONDOSOE8...
FUNDS: 10 NoobCoins
UTXO's: [,,,]
TRANSACTION
NEW TRANSACTION
TO: H97896432NOD29N1...
FROM: 09032NIFONDOSOE8
SHA256
VALUE: 5 NoobCoins
INPUTS: [,,,]
OUTPUTS: [,,]
SIGNATURE: 098432B359N2N1
ECDSA
BLOCKCHAIN
BLOCK NUMBER 666
HASH: N38N74NKLS789320
PREVIOUS HASH: 90870BEU
TIMESTAMP: 1/6/2018
TRANSACTIONS: [,,,]
BLOCK NUMBER 665
HASH: 90870BEUN8TBX240
PREVIOUS HASH: 54TO5HI
TIMESTAMP: 1/5/2018
TRANSACTIONS: [,,,]
BLOCK NUMBER 664
HASH: 54TO5HIFTW92784
PREVIOUS HASH: 9843289b
TIMESTAMP: 1/5/2018
TRANSACTIONS: [,,,]
Header
Body
SHA256
Hash of the block (hash)
SHA256
버전
(Version)
이전 블록 해시
(Previousblockhash)
머클루트
(Merkle Root)
타임
(Time)
난이도 목표
(bits, target)
논스
(Nonce)
거래 카운트 / ETC
Transaction #1
Transaction #2
Transaction #3
Transaction #N

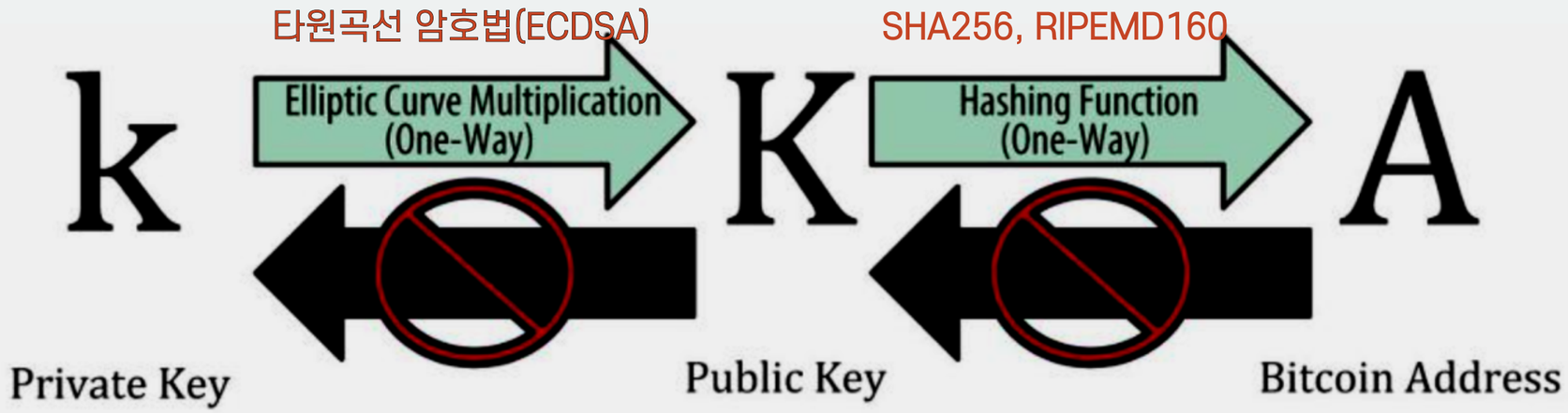
블록체인 추가 설명 - 머클루트

☑ 머클루트

- 트랜잭션들의 해시 트리
- 각 트랜잭션과 가까운 노드끼리 쌍을 지어서 해시 값을 구하여
최종적으로 구해진 해시 값이 머클루트 해시값이 된다.
- 각 거래정보가 변경 되었는지에 대한 유효성을 검사



블록체인 추가 설명 - key pair, Address



☑ Private Key

- 개인키는 256비트의 무작위로 생성된 숫자들로 구성
- 간단한 생성기가 아닌 완벽히 예측이 불가능한 도구를 이용하여 숫자 생성
- SecureRandom class에서 SHA1PRNG 알고리즘 사용

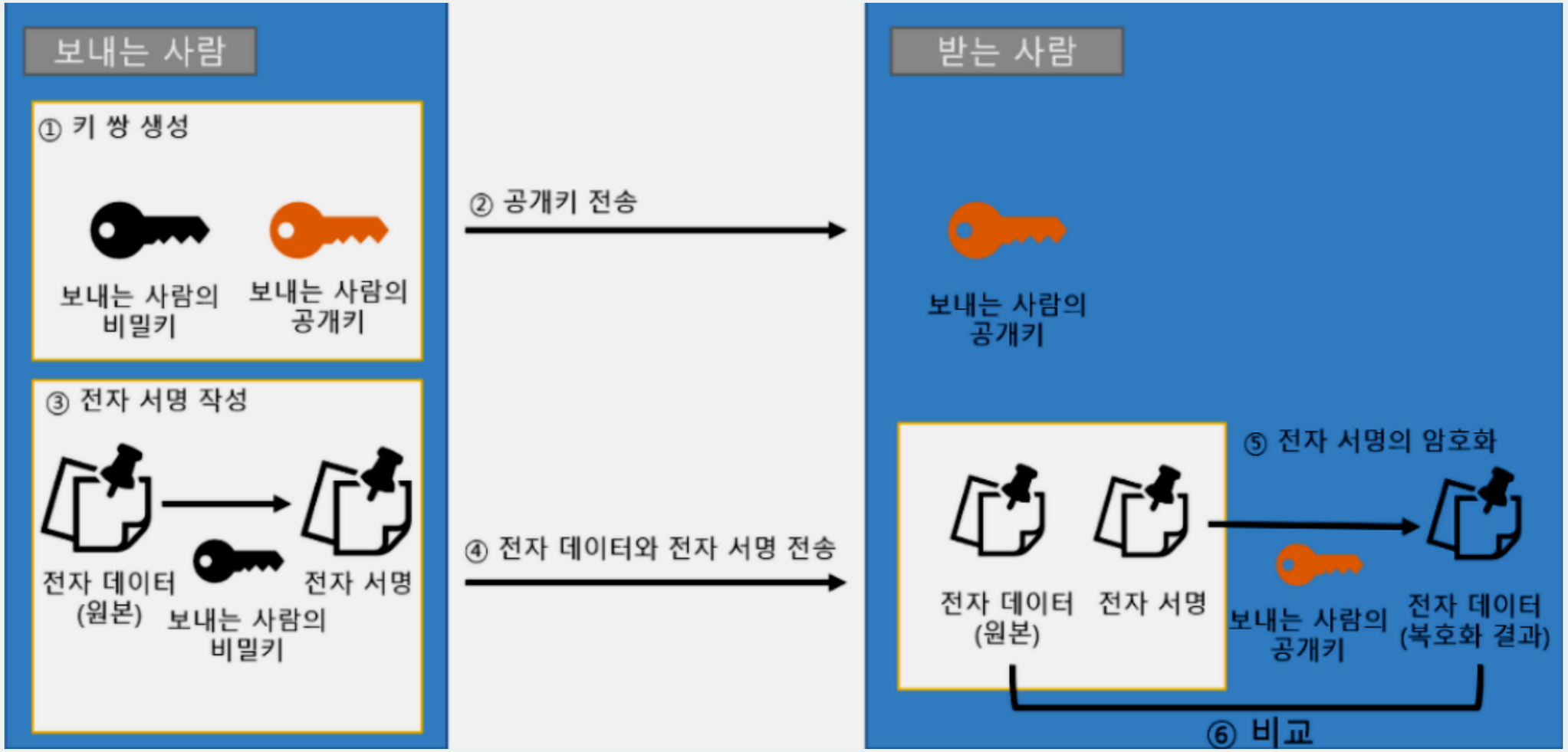
☑ Public Key

- 특정한 타원 곡선(secp256k1)과 수학적 상수를 사용
- 여기서 수학적 상수는 secp256k1이라는 곡선에서 정의되는 값
- ECDSA를 사용하여 생성

☑ Address

- SHA256과 RIPEMD160 해시 함수를 사용하여 공개키로부터 생성

블록체인 추가설명 - Signature



블록체인 추가설명 - 마이닝

☑ **채굴**은 작업증명(POW)을 통해 블록에 거래 내역을 정리해주고 보상을 받는 것

☑ Pow

Block

previousHash + timeStamp
+ merkleRoot + nonce

이 숫자가 블록 내에서 설정한
숫자보다 작으면 '작업완료'

AES 추가 설명

AES란

AES는 고급 암호화 표준이라는 의미이며,
암호화 및 복호화 시 동일한 키를 사용하는 대칭키 알고리즘

Secret Key

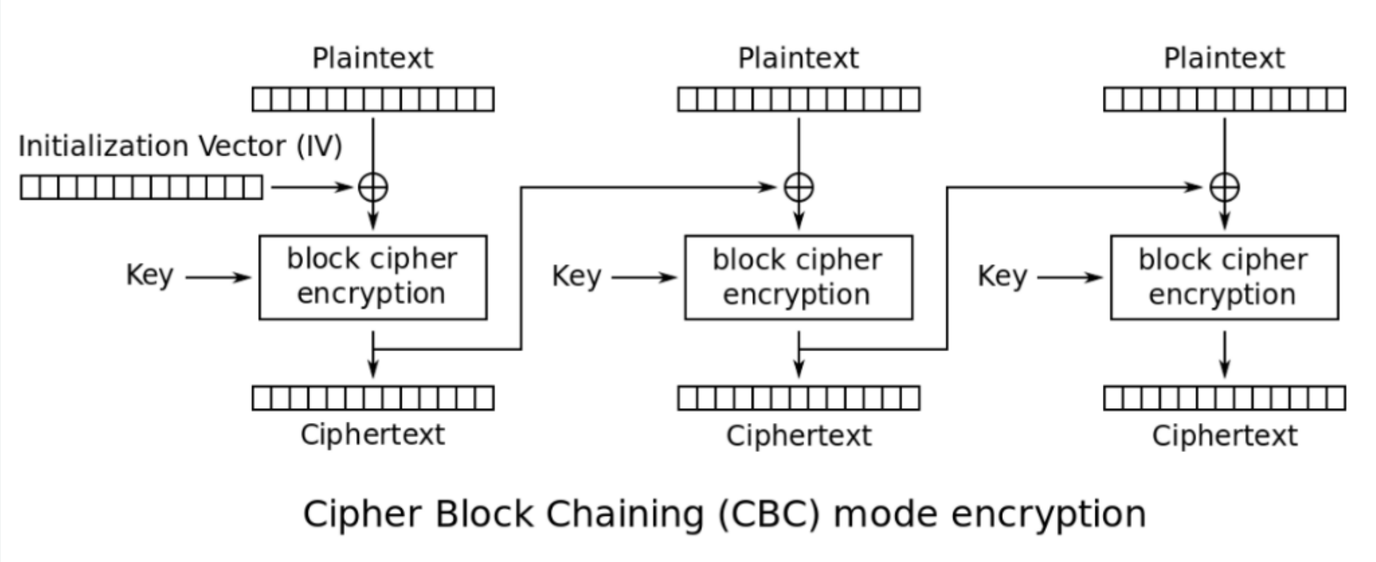
AES는 128비트(16바이트)의 고정된 블록 단위로 암호화를 수행

Block Cipher

AES는 128비트(16바이트)의 고정된 블록 단위로 암호화를 수행

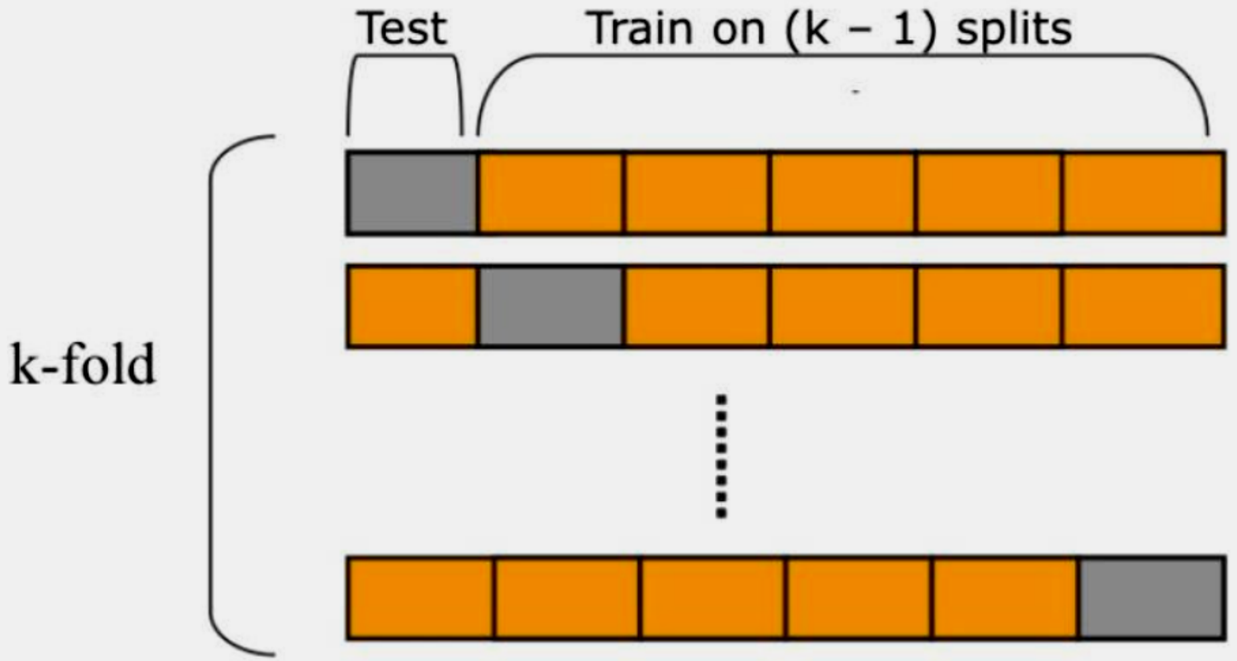
CBC (Ciper Block Chaning)

CBC는 블록을 그대로 암호화 하지않고 이전에 암호화했던 블록과 XOR 연산을 한 다음에 암호화를 수행



협업필터링 추가 설명 - K-Fold Cross Validation(교차검증)

- ☑ 총 데이터 개수가 적은 데이터 셋에 대하여 정확도를 향상
- ☑ Training, Validation, Test 세 개의 집단으로 분류하지 않고, Training, Test로만 분류
- ☑ 데이터 수가 적을 때 검증과 테스트에 데이터를 더 뺏기면 underfitting 등의 문제가 발생할 수 있음



오픈뱅킹 추가 설명 - OAuth 동작원리

7 access token

6 code, client Id, client secret

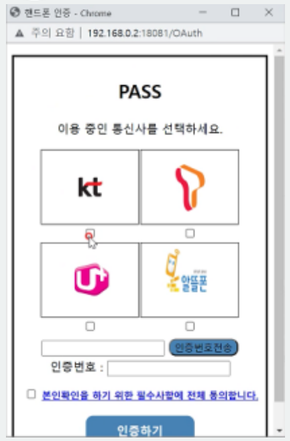
오픈뱅킹 서버

code 5

3

1 client Id, client secret

3 사용자에게 정보제공 동의 후 인증요청



2 오픈뱅킹 사용 요청