

[실습] 블록체인 핵심기술

→ 거래 검증 기술

## 블록체인 (Blockchain)

### 06. 거래 (Transaction) 기능 구현

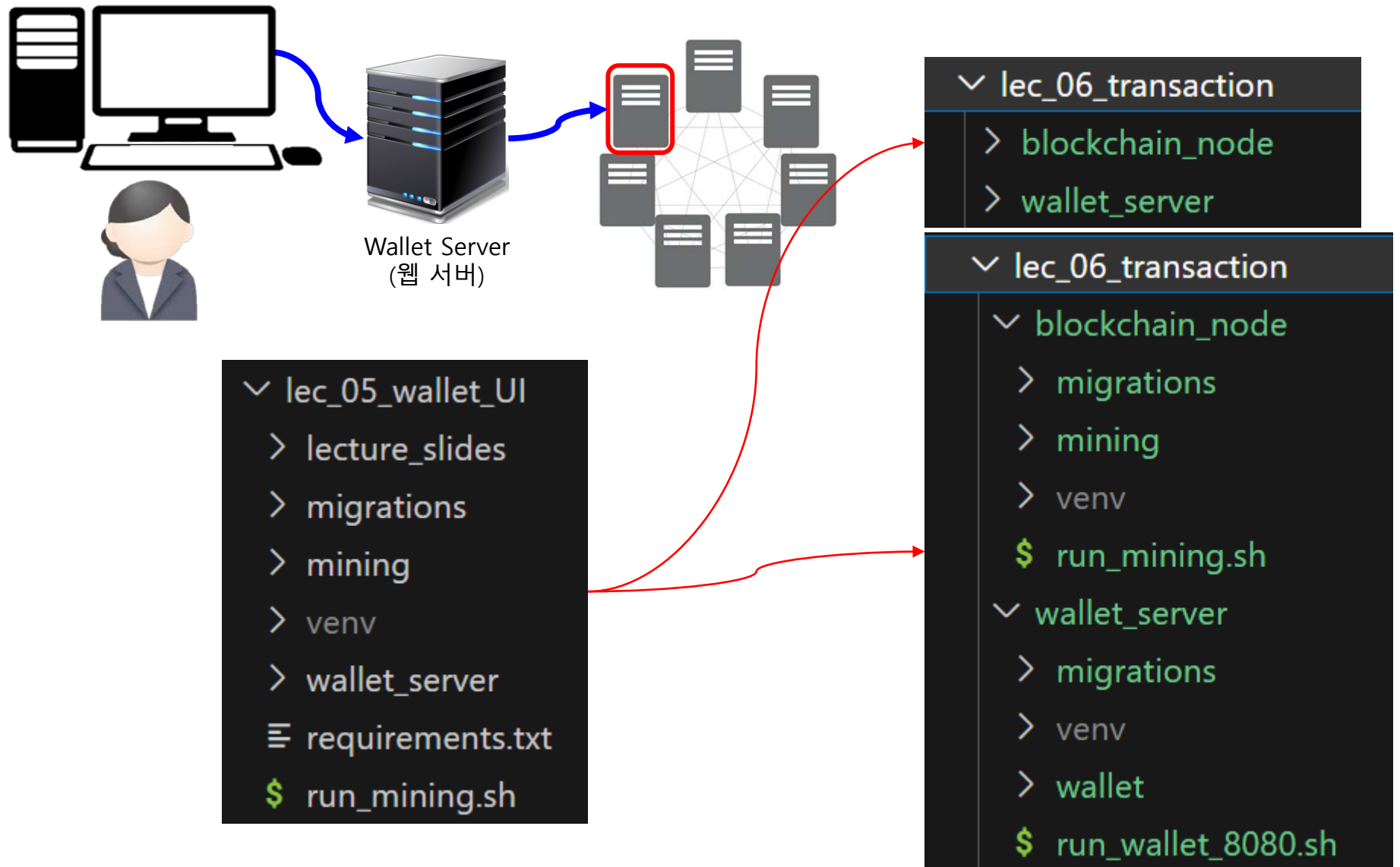
소프트웨어 끝대 강의

노기섭 교수

([kafa46@cju.ac.kr](mailto:kafa46@cju.ac.kr))

## 06. 05 디렉토리 재구조화

# 현재까지 개발한 디렉토리 구조



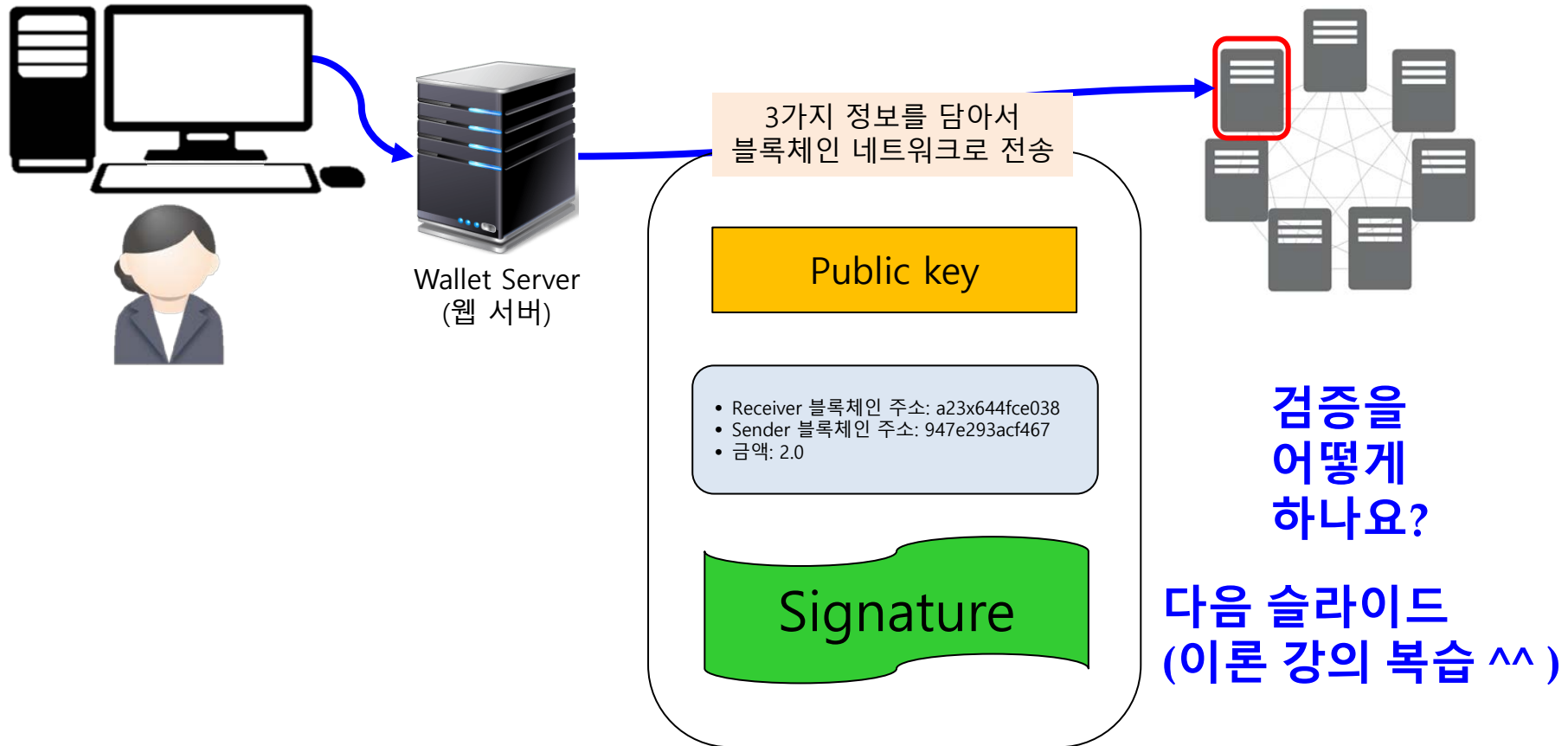
## 06. 06 Wallet 클래스 코딩(구현)

# 지갑(wallet)이 가져야 하는 기능

- 1. Private / Public Key
  - 2. Blockchain Address
  - 3. Signature Generation
  - 4. Total Amount (코인 보유 조회) → Javascript로 Blockchain 서버 요청
  - 5. Verify Transaction
- 회원가입 할 때  
생성하여 제공
- 거래 내역을 Blockchain Node에게  
전송할 때
- 지갑(wallet)에  
있어야 할 기능
- Blockchain Node가 거래내역을  
전달 받았을 때 필요한 기능
- Blockchain 노드에  
있어야 할 기능

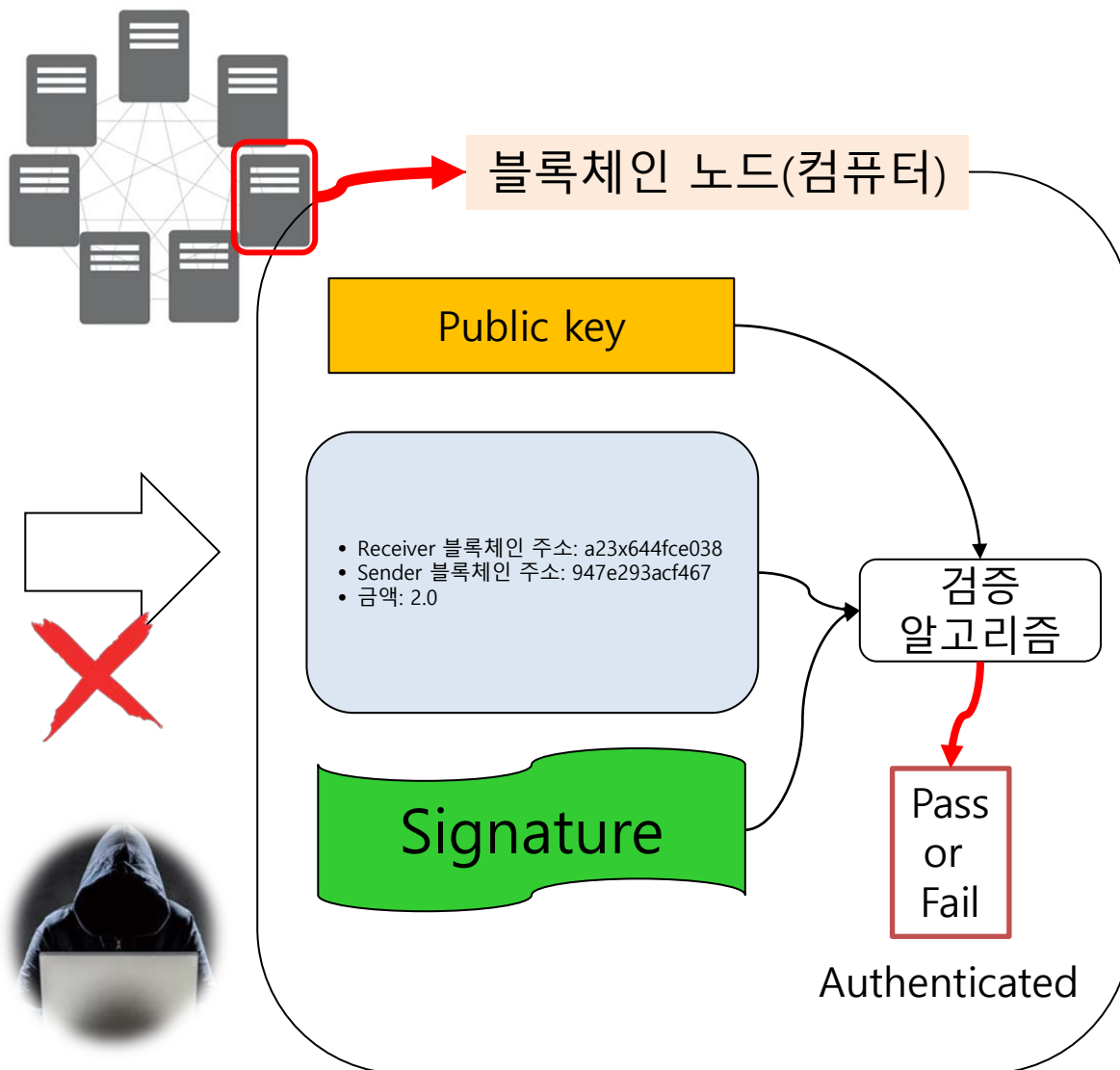
# Blockchain 노드에서 transaction 검증

# 거래 내역에 대한 검증을 구현해야 하는 상황



# 블록체인 검증 메커니즘

넘겨 받은  
정보가  
올바른 지  
검증하는 과정





# 작업할 내용

## ■ transfer.py

- verify\_transaction\_signature 메서드 추가
- add\_transaction 메서드 수정

## ■ utils/blockchain\_utils.py

- valid\_transaction\_params 함수 추가
  - 검증에 필요한 정보가 모두 전송되었는지 확인

Wallet 서버에서 private key, public key, wallet  
address 생성하여 저장

[Home](#)   [회원가입](#)   [로그인](#)

아이디

최소 4글자 이상

비밀번호

대소문자, 특수기호, 숫자 포함해야 하며, 7글자 이상

비밀번호 확인

비밀번호 확인을 위해 다시 한번 입력해 주세요

이름

(예) 홍길동

휴대전화번호

010-1234-5678

이메일

email@example.com

제출하기

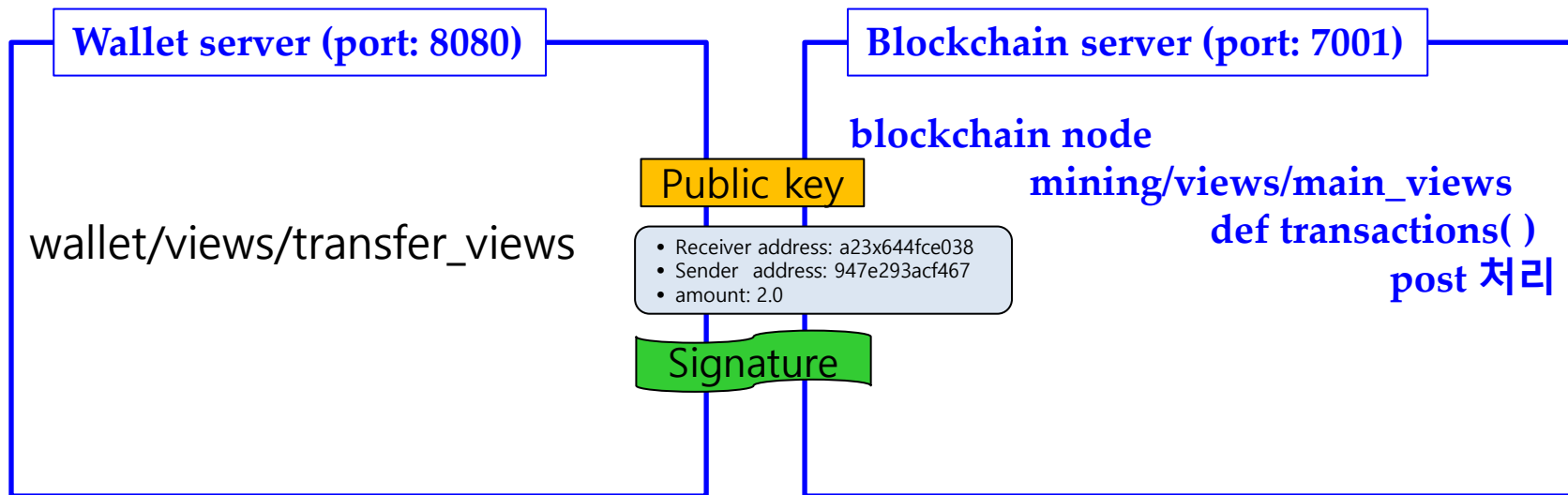
취소

- `wallet_server/views/auth_views.py`

wallet server → blockchain node  
이체 요청 기능 구현

# Transaction 추가 요청 기능

- wallet/templates/transfer.html
- wallet/static/js/transfer.js
- Transaction 추가 요청: controller (views) 코딩



데이터 전송: requests 패키지 활용

[실습] 블록체인 기반 코인(보조 기술)

→ 씨쥬 코인 조회 ^^

## 코인 조회 기능



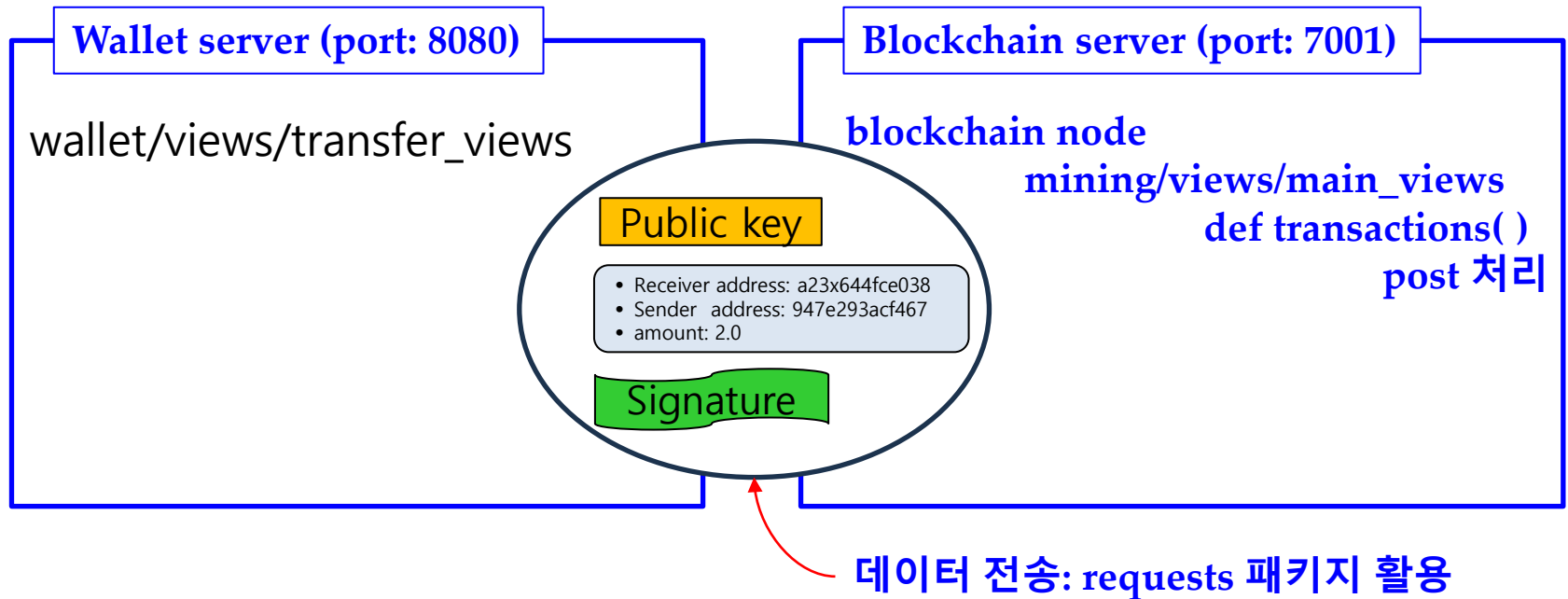
내 코인 현황?

이체 후 현황?



Wallet Server  
(웹 서버)

# 코인 조회



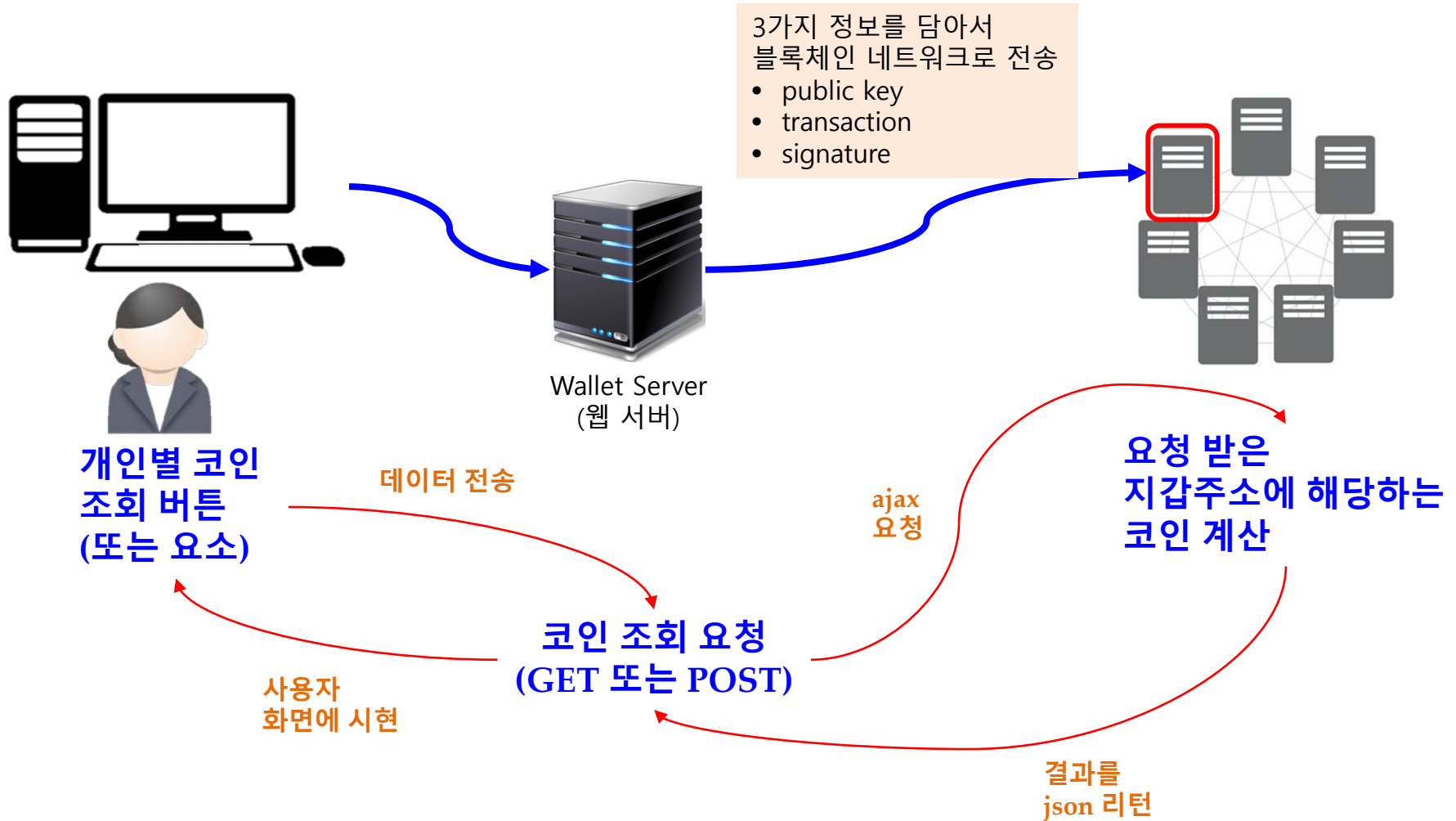
이미지 출처:  
<https://blog.naver.com/PostView.nhn?blogId=jaein999&logNo=221912328390>

어느 서버에 구현해야 하지???

도대체 어떻게 설계해야 하는 거야???



# 거래 내역에 대한 검증을 구현해야 하는 상황



# 시스템 기능 업그레이드 해야 할 곳

## ■ 작업해야 하는 부분

- blockchain\_node
  - mining/utils/blockchain\_utils
  - mining/main\_views.py
- wallet\_server
  - wallet/templates/transfer.html
  - wallet/static/js/transfer.js
  - wallet/views/transfer\_views.py

# 코인 자동 업데이트 기능 추가

Home   내 지갑   이체하기   test1 (로그아웃)

**'새로고침' 버튼을 클릭하면 업데이트**

test1 님의 전자지갑입니다.

**새로고침**

환산가치

씨주	
코인	원화(KWN)
10	공사중
지갑 주소	2UoFrQirwUcNAB7HtDw5qyC615nLiZrvbd1xuF57

Home   내 지갑   이체하기   test1 (로그아웃)

**화면 진입하면 자동으로 업데이트**

**내 코인 수량**

코인 이체하기

이체 수량   최소 0 초과 코인 수량을 입력하세요 (소수점 9자리까지 가능)

본인의 비밀키(private\_key)를 입력해 주세요

본인의 공개키(public\_key)를 입력해 주세요

받을사람 지갑 주소를 입력해 주세요

이체   취소



다음 강의  
이제부터는  
채굴(mining) 기능 구현  
합의(consensus) 알고리즘 구현

수고하셨습니다 ..^^..