# 목표

* ChatGPT 를 활용하여

P2p 기반 가치 이전(value transfer) PoC, 기술보고서, 실습 교제 작성

데이터 암복호화, P2P, Blockchain 분야 역량 강화

# 활용 기술

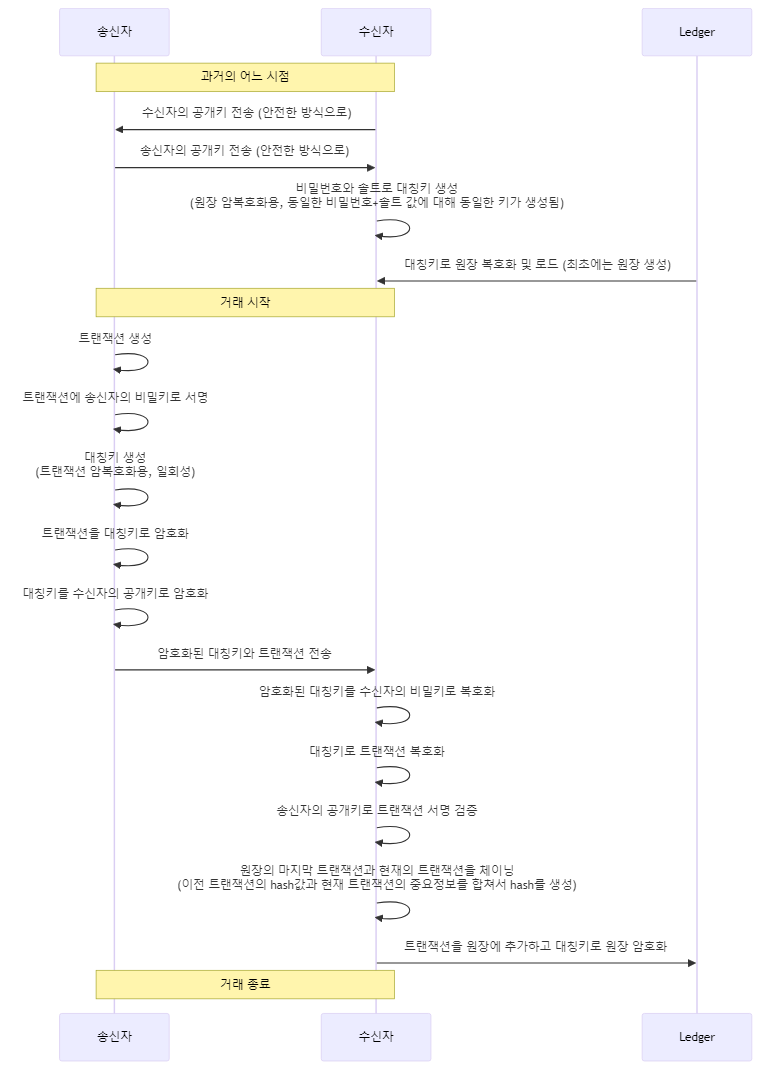
* Blockchain, DHT(Distributed Hash Table), Kademlia, WebRTC, 각종 암복호화 기술

# 과제 요약

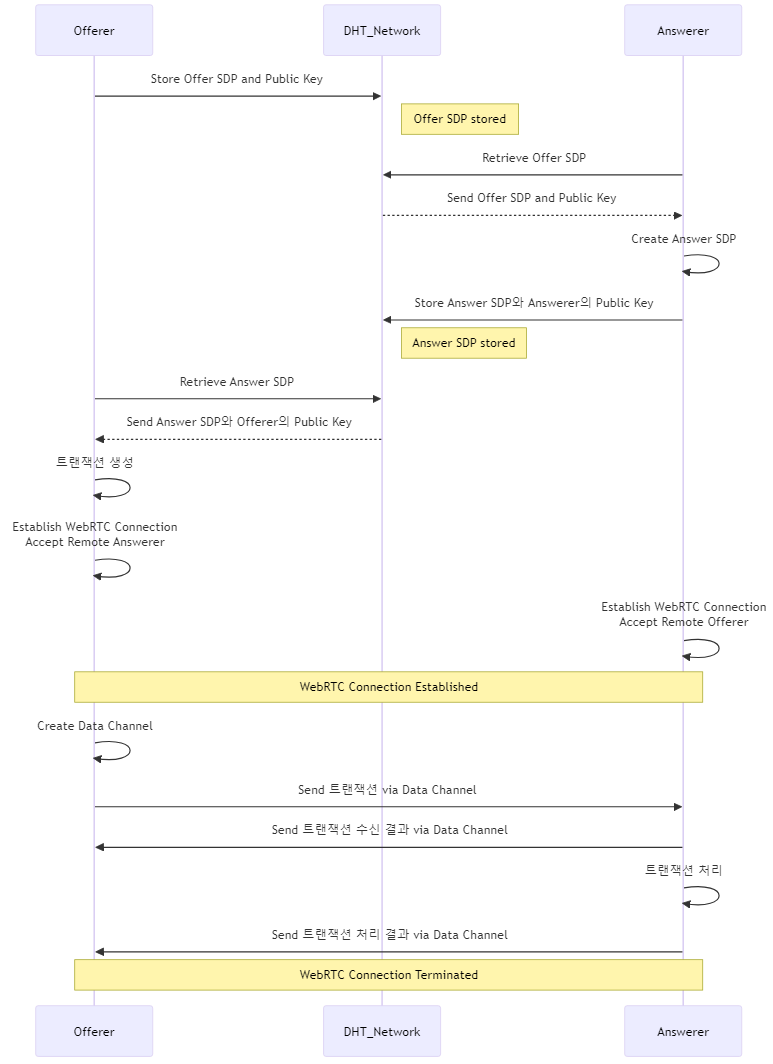
* “식권대장 시스템을 탈 중앙화할 경우 설계를 어떻게 할 것인가”
* A (offerer)가 B (answere) 에게 어떤 가치를 이전할 때 서버를 거치지 않고 신뢰할 수 있는 방법으로 이전하는 가장 단순한 시스템을 설계하고 개발하는 PoC를 수행함

# PoC 기능 요약

1. 가치를 안전하게 전송하고 안전하게 저장:
   * 데이터 전달 시 은닉(기밀성), 부인방지, 변조방지(무결성) 보장
   * 원장 관리
     1. 원장을 JSON으로 직렬화하고 AES-Fernet을 사용하여 암호화된 상태로 파일에 저장
     2. 트랜잭션의 이전 해시와 현재 해시를 검증한 후 원장에 추가



1. 탈중앙화 네트워킹 설계:
   * **DHT, Kademlia 기술 기반의 Peer 찾기**
   * WebRTC  기술 기반의 P2P 네트워킹



# PoC 수행 결과

1. 목표 시스템 설계

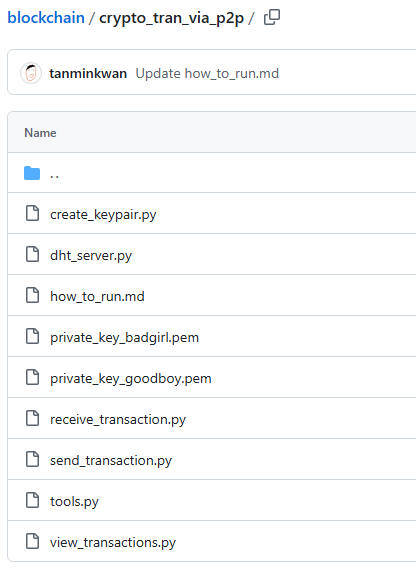
“4. PoC 기능 요약” 참고

o1-preview, o1-mini 모델과 대화식으로 최종 mermaid sequence diagram 결과물 생성

1. 소스 코드 생성 및 실행

설계에 맞게 o1-preview 모델에 의한 소스 코드 생성

기능 보완, 문제 발생 시 해결하는 방식으로 목표에 도달할 때까지 iteration 수행



1. 매뉴얼 및 기술보고서 작성

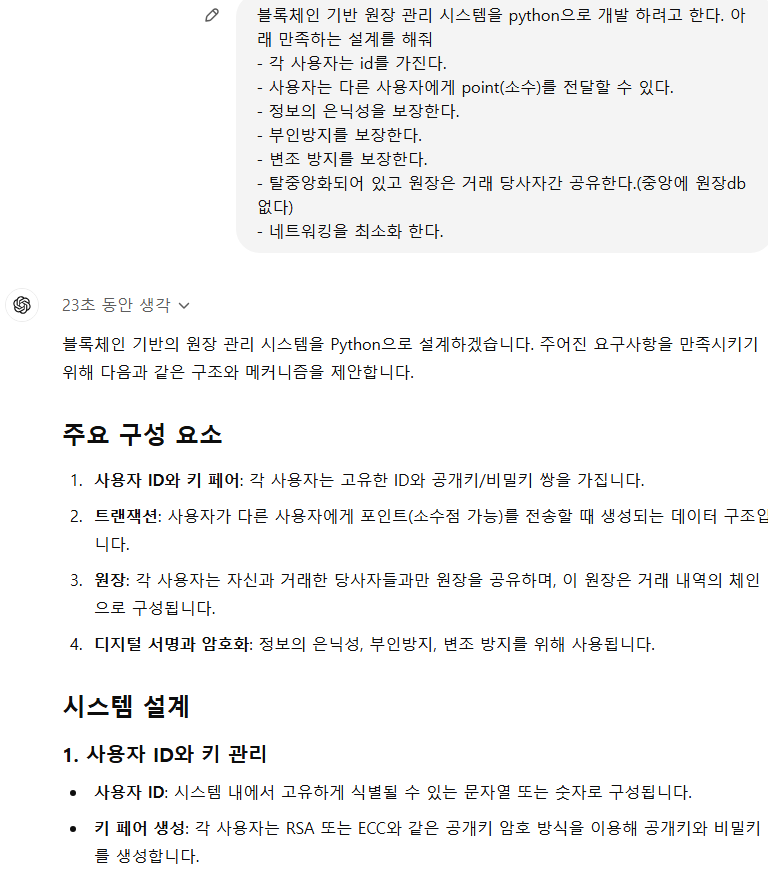
4o 모델에 의한 매뉴얼, 기술보고서 작성



* + - * 매뉴얼 발췌

# ChatGPT 활용 예시

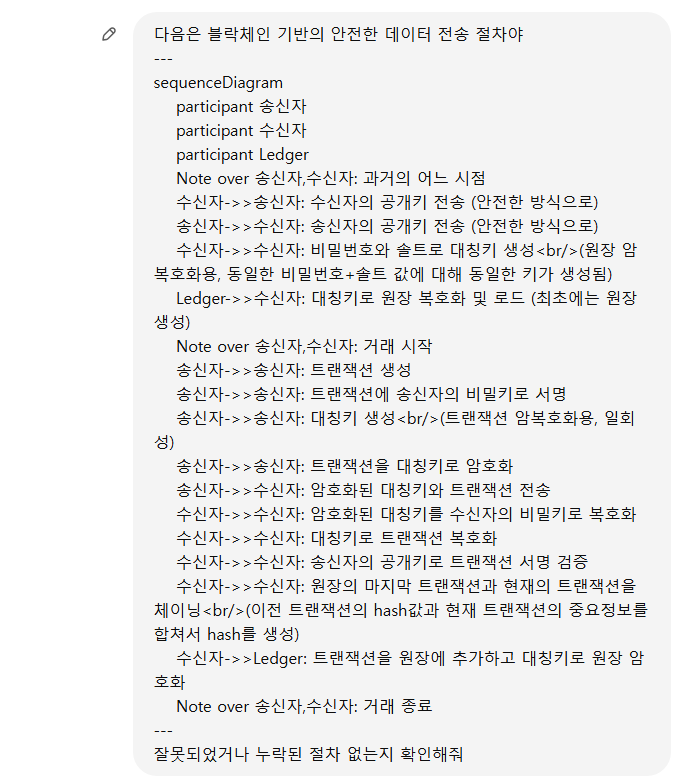
1. 시스템 설계, 기술요구사항 확인



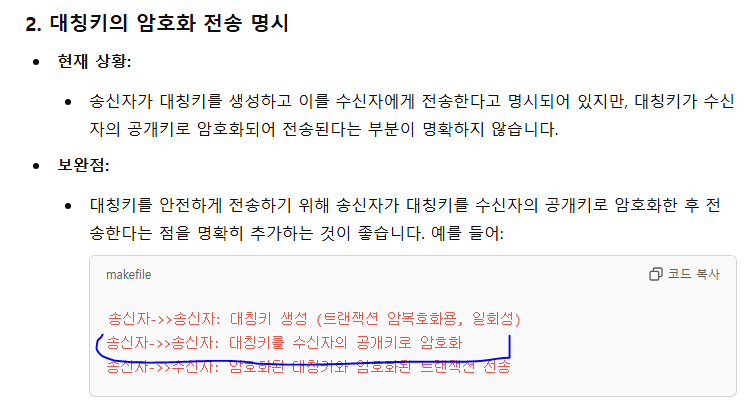
* + - * Chat 내용 발췌

1. 설계의 품질 확인
   * o1-preview 추론 능력을 활용, 복잡한 암복호화 절차에 문제가 없는지 확인
   * 특히, 완성된 Sequence Diagram 에서 일부 절차를 삭제하거나 잘못되게 수정을 한 후 문제를 찾으라고 시키는 방식으로 설계 검증

* 송신자->>송신자: 트랜잭션을 대칭키로 암호화
* **송신자->>송신자: 대칭키를 수신자의 공개키로 암호화**
* 송신자->>수신자: 암호화된 대칭키와 트랜잭션 전송
  + - * 정상적인 절차



* + - * 일부러 절차를 누락



* + - * o1-mini 답변 : 정확하게 누락된 절차를 찾아냄

1. Code Assistant 로 활용



1. 친절하고 똑똑한 구술 전문가로 활용

