

클라이언트(앱)

서버

1. 대칭키 교환 프로토콜을 통한 대칭키 교환

genesis_block_
create()

대칭키를 이용해 제네시스 블록생성

genesis_block_
create()

블록헤더 +
비식별 데이터

해시값을 확인하여 데이터의 무결성 확인

블록헤더 +
비식별 데이터

2. encrypt()를 통해 암호문 생성
후 데이터 송신

3. decrypt()를 통해 복호화 후 데
이터 수신

5. decrypt()를 통해 복호화 후 데이터 수신
보냈던 데이터와 비교한후 일치하면 데이터 정상전송 성공

4. encrypt()통해 암호문생성 후 데이터 송신.
받은 데이터를 되돌려보냄으로써 클라이언트가 제대로
데이터가 전송되었는지 해시값을 통해 확인한다.