1, Request

Bob

TTP

Alice

2,L

3,doc, EOO, L

4, L, EOO

5, L, EOR

6, L, doc

7 ,L, EOR

8, L

8,L

Explain of Coffry\_Saidha fair exchange protocol:

Notations:

L: Unique label to link all message of a given protocol run

EOO: SigA(H(doc))

EOR: SigB(sigA(H(doc)))

Step1: Alice sends a request to TTP that she wants a fair exchange;

Step2: After TTP receives the request from Alice, it sends a unique label to Alice;

Step3: After Alice receives the label, she will send the document which she wants to give Bob and EOO(SigA(H(doc))) and label to TTP;

Step4: After TTP receives the message from Alice, it stores the document and sends the EOO(SigA(H(doc))) and the label to Bob;

Step5: Bob sends the EOR(SigB(sigA(H(doc)))) and label to TTP after he receives EOO;

Step6: After receiving EOR from Bob, TTP would send the document and label to B which it store before;

Step7: TTP sends EOR and label to Alice which means Bob will receive the document which she wants to give.

Step8: Alice and Bob send the label to TTP which means this fair exchange finished.

Reference: Distributed Algorithms lecture notes.