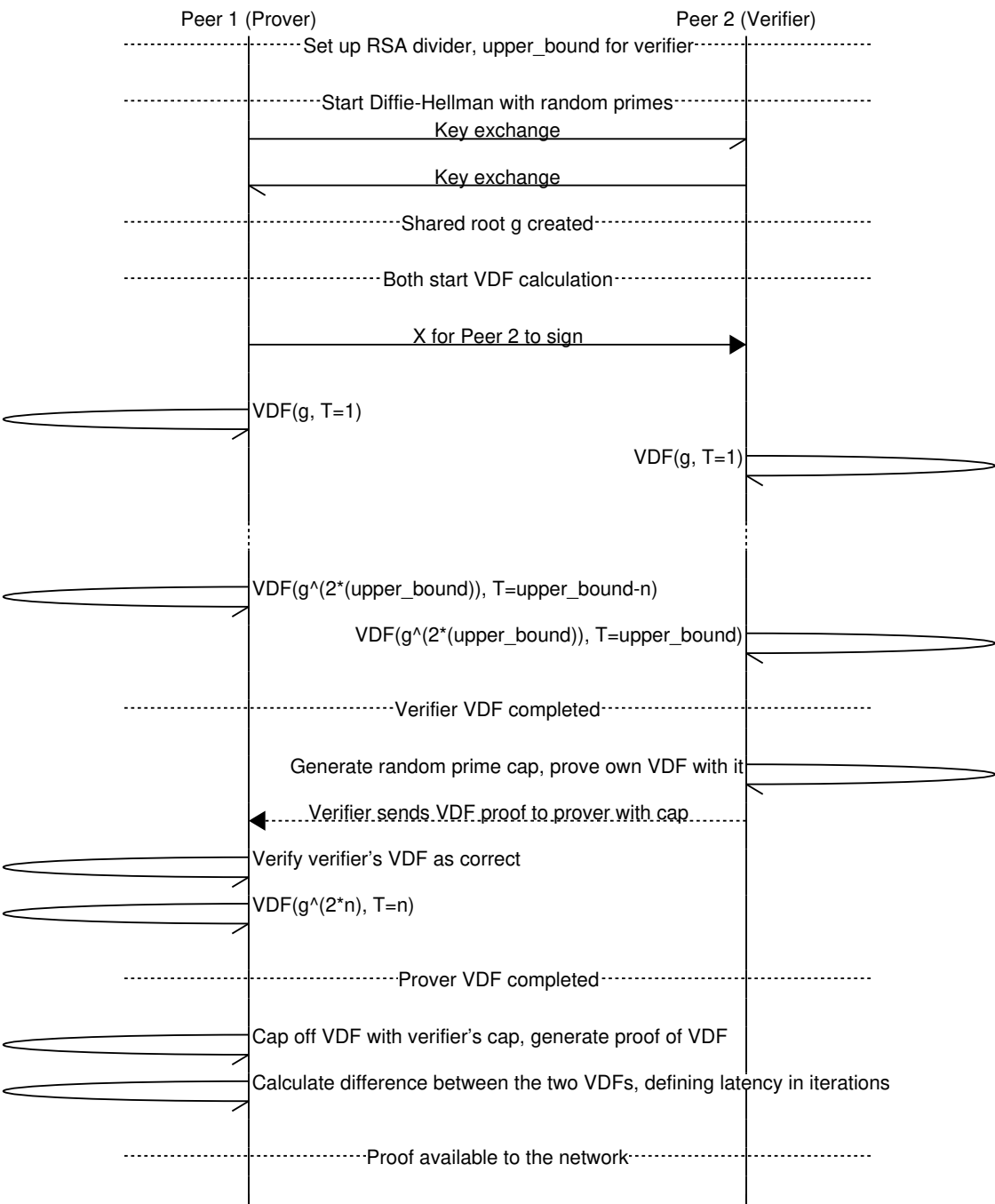
Peer 1 (Prover)
Peer 2 (Verifier)
Set up RSA divider, upper_bound for verifier
Start Diffie-Hellman with random primes
Key exchange
Key exchange
Shared root g created
Both start VDF calculation
X for Peer 2 to sign
VDF(g, T=1)
VDF(g, T=1)
VDF(g^(2*(upper_bound)), T=upper_bound-n)
VDF(g^(2*(upper_bound)), T=upper_bound)
Verifier VDF completed
Generate random prime cap, prove own VDF with it
Verifier sends VDF proof to prover with cap
Verify verifier's VDF as correct
VDF(g^(2*n), T=n)
Prover VDF completed
Cap off VDF with verifier's cap, generate proof of VDF
Calculate difference between the two VDFs, defining latency in iterations
Proof available to the network