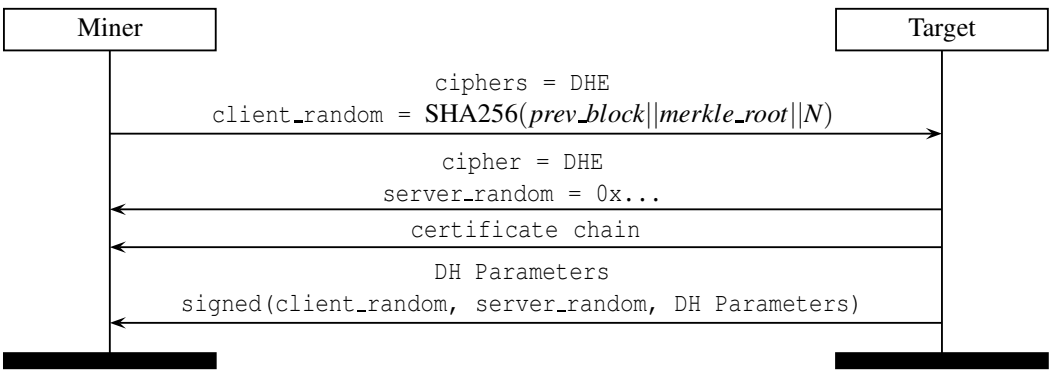
Miner
Target
ciphers = DHE
client_random = SHA256(prev_block||merkle_root||N)
cipher = DHE
server_random = 0x...
certificate chain
DH Parameters
signed(client_random, server_random, DH Parameters)