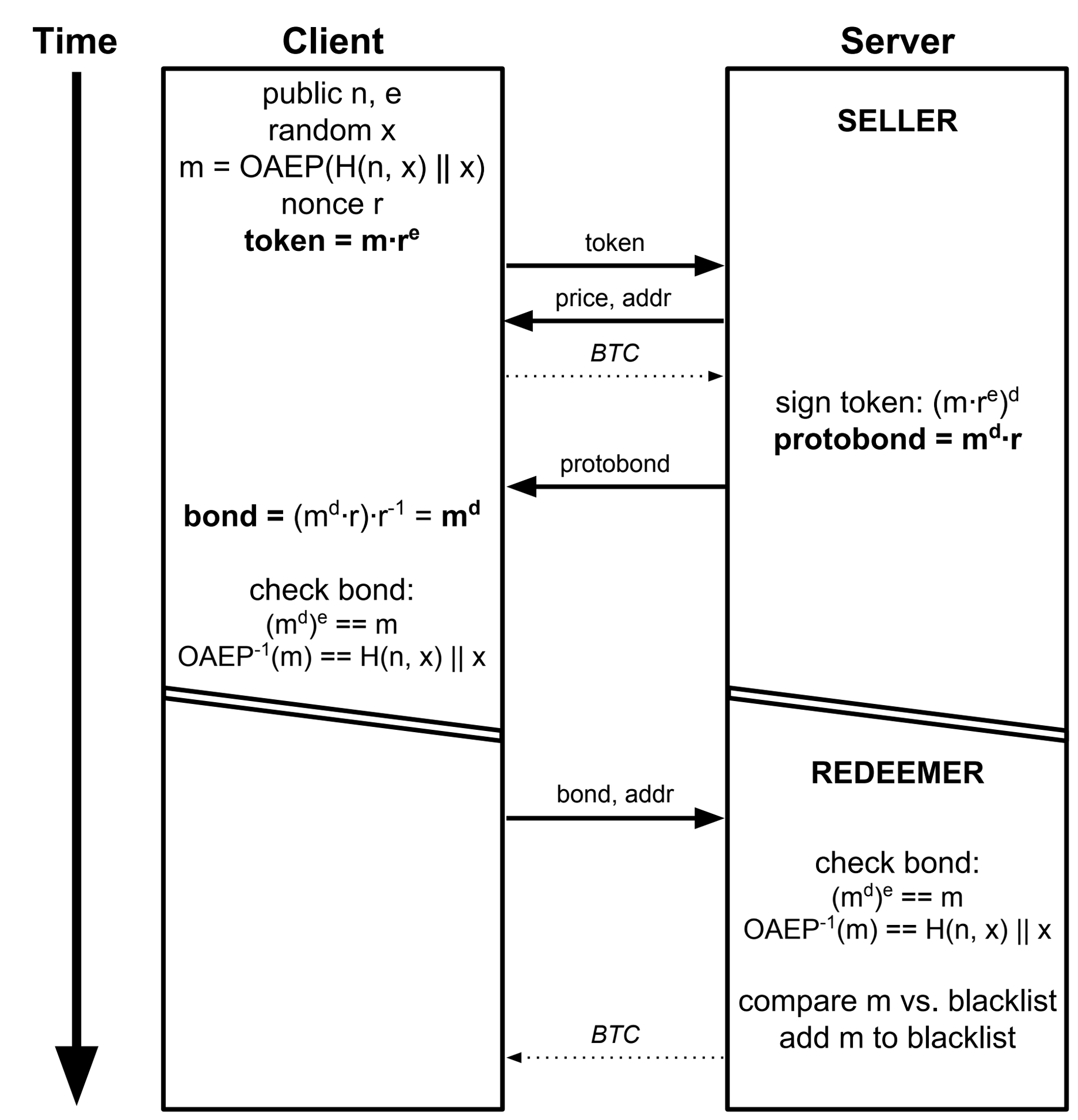
Time
Client
Server
public n, e
random x
m = OAEP(H(n, x) || x)
nonce r
token = m·r^e
SELLER
token
price, addr
BTC
sign token: (m·r^e)^d
protobond = m^d·r
protobond
bond = (m^d·r)·r^-1 = m^d
check bond:
(m^d)^e == m
OAEP^-1(m) == H(n, x) || x
REDEEMER
bond, addr
check bond:
(m^d)^e == m
OAEP^-1(m) == H(n, x) || x
compare m vs. blacklist
add m to blacklist
BTC