One Time Spending Key (osk):
H(rbG) + a

One Time Public Key (opk):
(H(rbG) + a) G

Coin

Master SK: (a, b)

Viewing Key (vk): (aG, b)

Shielded Address (pk): (aG, bG)

Transaction: void_number || utxo || Enc(rbG, asset_info) || rG