Question: does the withdrawal key have

to be a public/private key pair? Does it need to sign anything?

I am thinking if we make this into a contract address, that would allow staking pools to use smart contracts to manage their pools, at least on withdrawal. (Deposit could be a proof of deposit that issues a pool share token)

Similar point for the deposit: is there a way this could be designed where it doesn't need a signature? For the deposit, we don't really care where the money comes from for a validator as long as it exists in the Beacon Chain.

I understand that the Validators themselves definitely need to be keypairs to sign protocol messages, but if smart contracts can use the on-/off-ramps for Validator funds, that enables interesting things (maybe bad

things)