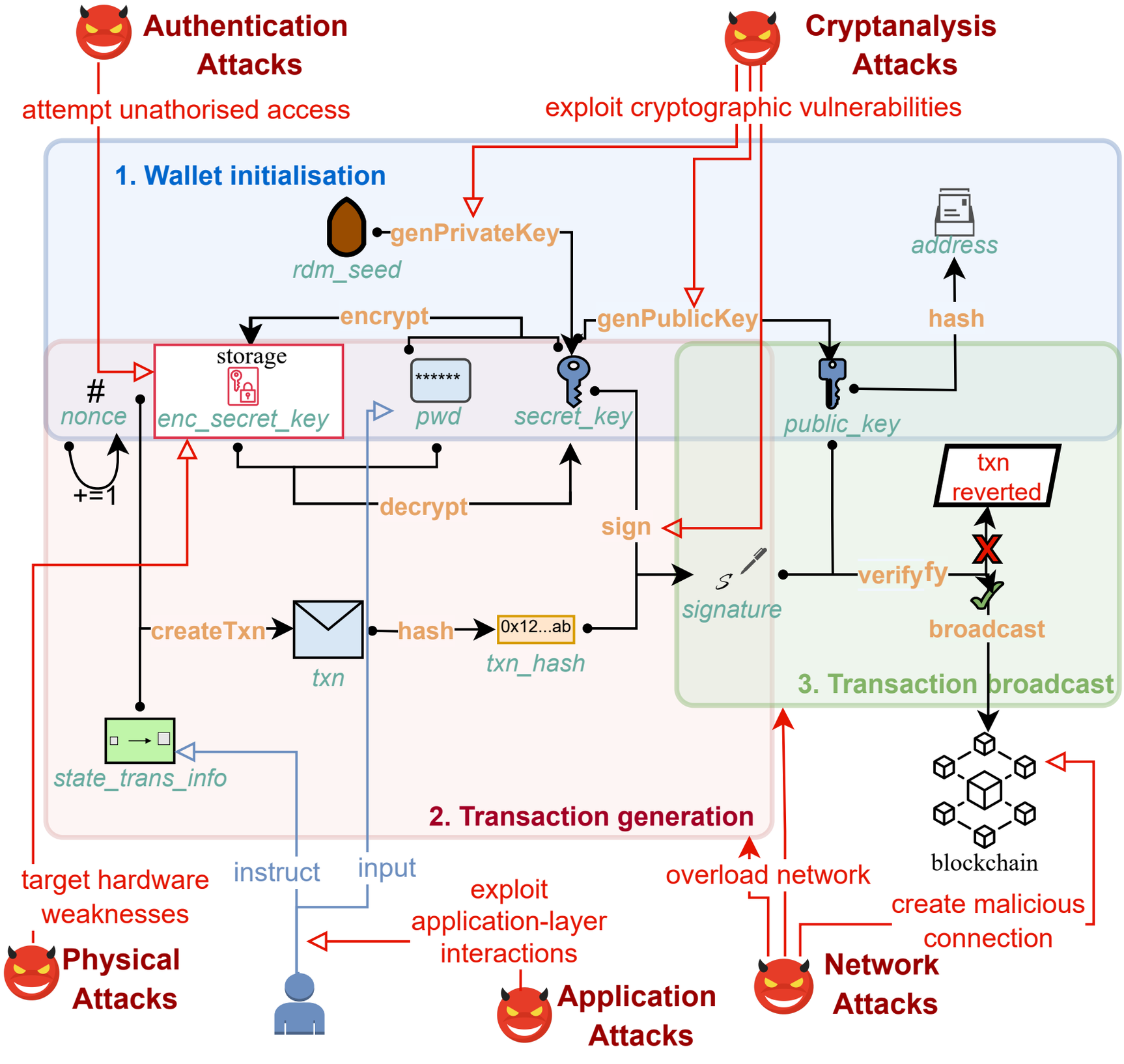
Authentication Attacks
attempt unathorised access
Cryptanalysis Attacks
exploit cryptographic vulnerabilities
1. Wallet initialisation
rdm_seed
genPrivateKey
address
encrypt
genPublicKey
hash
storage
#
nonce
enc_secret_key
******
pwd
secret_key
public_key
+=1
decrypt
sign
txn reverted
verify
signature
broadcast
createTxn
hash
0x12...ab
txn
txn_hash
3. Transaction broadcast
state_trans_info
2. Transaction generation
blockchain
target hardware weaknesses
instruct
input
exploit application-layer interactions
overload network
create malicious connection
Physical Attacks
Application Attacks
Network Attacks