

Native AA

1. Why AA?

Validate txs on smart contracts

Allows -

- a) session keys
- b) multisig
- c) different signing algos
- d) Paymasters - gas sponsorship, alt fee token, enabling privacy protocols

Execution is also defined by smart contracts

2. Lessons learned from 4337

85% userOps used paymaster

Gas sponsorship major use case

(Simplified user onboarding)

Some wallets adopted 4337 (safe, oks, trust wallet, coinable etc)

Private relay service is cheaper

Pimlico, biconomy, alchemy some of the most used paymaster service providers

3. Why native AA?

- a) remove EOAs completely
- b) remove factory contract for smart account deployment
- c) enable alt fee token gas payments
- d) EIP 7870 hardware reqmts preserved

4. Advantages

- a) extra gas costs are not required (30k gas overhead basic + 40k per operation) while with 7701 5k overhead
- b) FOCIL can support - no Censorship resistance + no centralized bundler. Because this new tx type goes straight to the chain.
- c) alt signature validation crypto techniques - quantum protected

5. Specs of 7701

i) Sender Account

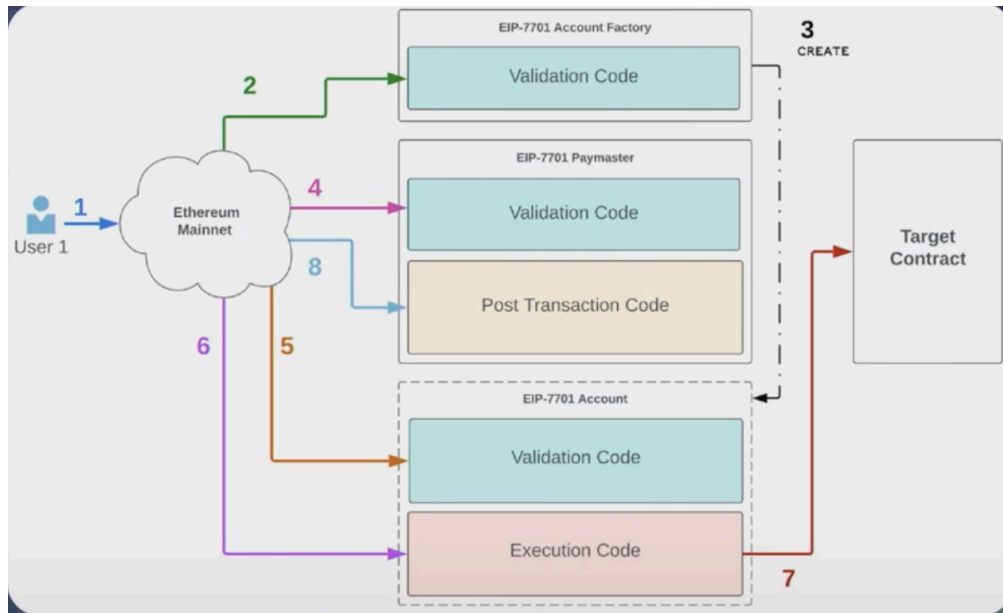
Validates, pays gas, execute call

ii) Deployer

Deploys the SA

iii) Paymaster

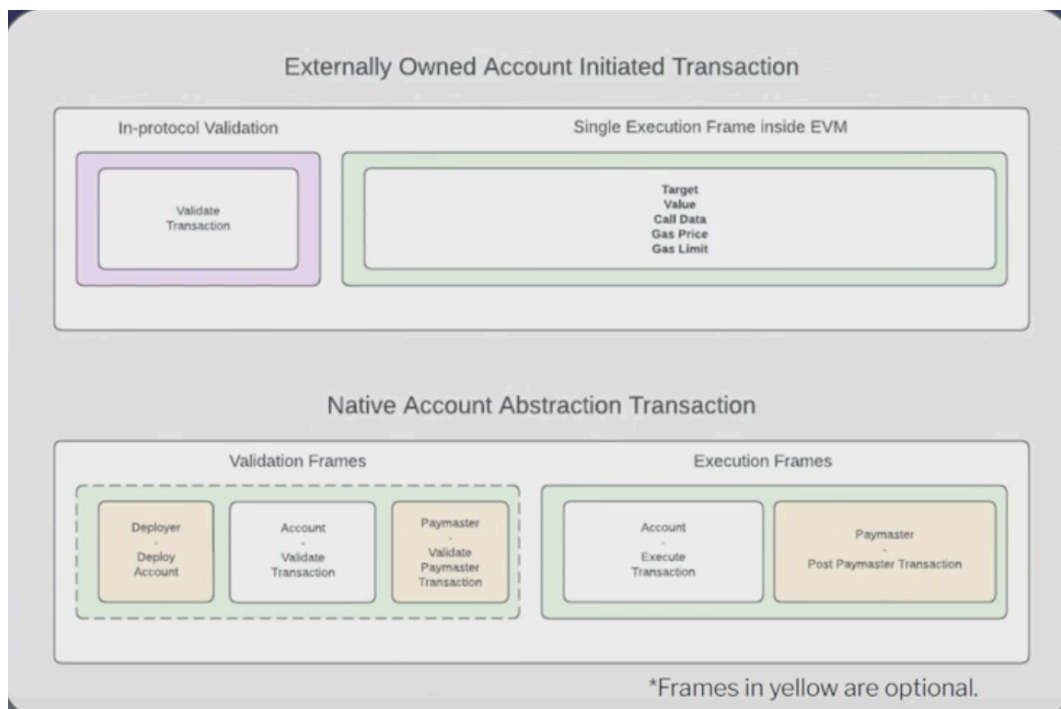
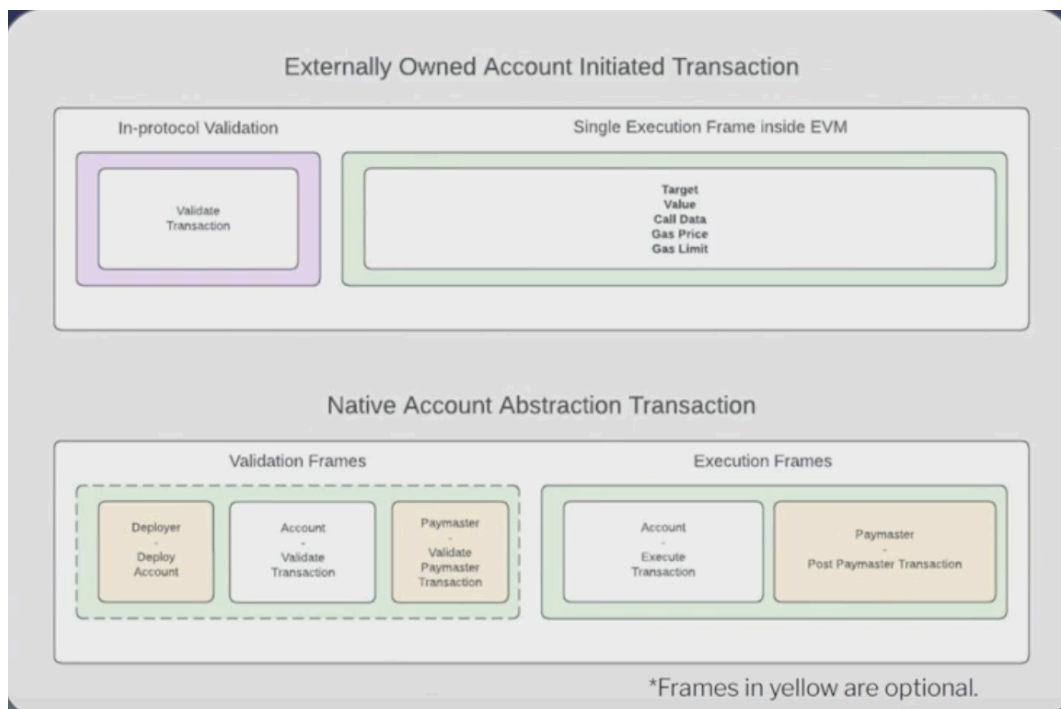
Pays gas



6. Flow of userOp-

Validation steps at account factory, then paymaster validation, and then SA validation, SA execution then post paymaster execution

DoS attacks are protected from by limiting validation gas (because in 7701 validation happens on nodes side (so users do not have to pay gas for invalid txs))



7. Tx type structure

```
AA_TX_TYPE || rlp([
  chain_id,
  nonce,
  sender, sender_validation_data,
  deployer, deployer_data,
  paymaster, paymaster_data,
  sender_execution_data,
  max_priority_fee_per_gas, max_fee_per_gas,
  sender_validation_gas, paymaster_validation_gas,
  sender_execution_gas, paymaster_post_op_gas,
  access_list,
  authorization_list
])
```

New opcodes introduced
TXPARAMDLOAD, TXPARAMSIZE, TXPARAMCOPY

Q/A: Why are blobs not part of the tx type

- Future of blobs uncertain
- Usual people do not use blobs
- First iteration might not need, adds more complexity