

# Stateless+CR+AA

Yoav Weiss

# AA transaction validity

- EOA transaction validity: ecrecover, nonce, balance
  - Only nonce or balance changes can invalidate
- AA transaction validity: EVM validation function
  - Arbitrary state dependency
  - No restrictions in protocol
  - Mempool DoS mitigated by the ERC-7562 rules

# Stateless mempool implications

- Stateless nodes may participate in the mempool
- For EOA they need balances and nonces
  - Partial statelessness could solve it
- For AA they need any code and slots accessed in validation
  - Can't use partial statelessness - no criteria

# Validity witnesses in mempool

- On eth\_sendRawTransaction RPC:
  - Validate
  - Generate witness for anything accessed in validation
  - Propagate {txn,witness} unless witness > MAX
- On p2p receiving:
  - Verify witness, drop if invalid
  - Verify txn validity, drop if invalid or not covered by witness
  - Propagate {txn,witness} unless witness > MAX

## Validity witnesses in mempool (cont'd)

- Witness may become invalid upon state changes while txn is pending
  - Seldom in account
  - Often in paymaster. Example: TokenPaymaster
- Stateful node needs to regenerate witness
  - DoS mitigation: ERC-7562 rules
  - Question: Should we even regenerate? Txn already propagated and builders are not stateless.

# Stateless+AA+FOCIL

- FOCIL allows excluding transaction if proven invalid
- Attesters need to execute account validation to verify invalidity
- Stateless attesters need missing code and slots for this
- Solution: Builder adds invalidity proofs sidecar
  - Witness for each failed validation
  - Attesters verify against current state

## Stateless+AA+FOCIL (cont'd)

- Must limit sidecar size
- Validation accesses few slots. Can be enforced.
- Require access list, at least a partial one for validation.
- FOCIL eligibility conditions:
  - Transaction has an access list
  - Access list contains up to MAX\_SLOTS
  - Anything accessed in validation appears in access list
- FOCIL satisfied if all excluded txns are proven in sidecar or ineligible

# Stateless+AA+FOCIL - Possible eligibility states

FOCIL satisfied for a transaction if:

- No access list - not eligible (no witness)
- Access list > MAX - not eligible (no witness)
- Validation accesses state not in access list - not eligible (witness)
- Access list sufficient, validation fails - eligible (witness)

Block invalid if:

- Eligible transaction doesn't fail validation
- Transaction excluded but not appearing in sidecar