Unified Rigidity Coin (URC): Protocol Contract and Security Model

Inacio F. Vasquez

January 26, 2026

Protocol Contract (Normative)

URC is defined by the following invariants.

(I1) Cryptographic ownership. A spend of UTXO u is valid only if the input public key equals the stored UTXO public key.

(I2) Ed25519 authentication. For every non-coinbase transaction tx with input (pk, sig),

$$\text{Verify}\big(pk,\ \text{canon}(tx \setminus sig),\ sig\big) = \top.$$

(I3) No inflation. For every non-coinbase transaction tx,

$$\sum \text{in}(tx) \geq \sum \text{out}(tx).$$

(I4) No double-spend. Every UTXO key may appear in inputs at most once (block-local and mempool-global).

(I5) Checkpoint safety. If $h \in \text{dom}(\text{CHECKPOINTS})$, then

$$\text{hash}(B_h) = \text{CHECKPOINTS}[h].$$

(I6) Proof-of-Work validity.

$$\text{int}(\text{SHA256}(\text{canon}(\text{header})), 16) < T_0.$$

(I7) Fee-based mempool ordering. Transactions are ordered by fee-per-byte:

$$tx_1 \prec tx_2 \iff \frac{\text{fee}(tx_1)}{|\text{canon}(tx_1)|} > \frac{\text{fee}(tx_2)}{|\text{canon}(tx_2)|}.$$

Threat Model and Non-Claim

The adversary may control:

- the network,
- message ordering,
- and arbitrary computational resources.

URC explicitly does **not** claim asymptotic security accumulation. Security is structural, not economic.