Formal Description of Transaction Validation Logic

Definitions:

Let S be the set of struct data passed by the tx builder
Let T be the set of actual transaction inputs and outputs
Let I be the intent struct signed by the owner
Let H be the hash function
Let Sig be the signature provided

Validation Process:

Step 1: Struct Data Matching

$$\forall s \in S, \exists t \in T : s \equiv t$$

Step 2: Transaction Details Validation

$$\begin{aligned} H(T) &\equiv H(I) \\ Verify(Sig, H(T)) &= true \end{aligned}$$

Conclusion:

The transaction is valid if and only if:

$$(\text{Step 1 is true}) \wedge (\text{Step 2 is true})$$

Interpretation:

- The tx builder has created a transaction T that satisfies the intent struct I signed by the owner.
- The struct data S provided by the tx builder matches the actual transaction details T.
- The hashed transaction details can be verified using the provided signature, ensuring the owner's authorization.

This formal description ensures that:

1. The transaction builder has correctly interpreted and implemented the owner's intent.
2. The actual transaction on the blockchain matches this intent.
3. The owner has cryptographically approved this specific transaction structure.