| 1: Init transaction: account info, TsxData |
|---|
| 1.1: options, out hmacs |
| 2: Set inputs: input[i] |
| 2.1: vin[i], hmacs, pseudo_out, alpha |
| 3: Set Inputs permutation |
| 4: Set inputs: input[i], tx.vin[i], pseudo_out[i], hmacs |
| 5: All inputs set, options rsig data |
| 5.1: options, rsig data |
| 6: Set outputs: out[i], hmac |
| 6.1: vout[i], rsig, out_pk, ecdh_info, hmacs |
| 7: All out set |
| 7.1: tx_prefix_hash, tx_extra, rtcsig_base, full_message_hash |
| 8: Sign: input[i], pseudo_out[i], alpha[i], spend_key[i], hmacs |
| 8.1: Signature for input i, cout |
| 9: FinalRequest |
| 9.1: FinalAck: cout keys, enc tx keys |