Transaction Message Format

Transactions in this system have a format that varies based on their **length, which dictate the transaction type** and the data it carries.

General Transaction Message Structure

- **Signature (variable length)**: A digital signature to verify the authenticity of the transaction, typically generated using the sender's private key.
- **Source Address (4 bytes)**: The identifier of the account initiating the transaction.
- **Transaction Type (variable, determined by length and content)**:
    - **Update State Transaction (100 bytes)**:
        - Contains new state information for the source account.
    - **Release from Staking Transaction (68 bytes)**:
        - Initiates the release of funds staked.
    - **Stake Transaction (72 bytes)**:
        - Commits funds for staking.
    - **Delegate Transaction (74 bytes)**:
        - Delegates staking power.
    - **Simple Transfer Transaction (76 bytes)**:
        - Transfers funds to a target account.
    - **Transfer with State Update Transaction (108 bytes)**:
        - Transfers funds and updates state.
    - **Account Key Change Transaction (244 bytes)**:
        - Updates account's public keys.
    - **Create Account Transaction (248 bytes)**:
        - Establishes a new account.

Detailed Breakdown for Transaction Types

- **Update State (100 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)
    - State Hash (32 bytes): The hash representing the new state of off-chain accounts.
- **Release from Staking (68 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)
- **Stake (72 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)
    - Amount (4 bytes): How much is staked.
- **Delegate (74 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)

    - Target Address (4 bytes)
    - Amount (2 bytes): Size of the delegation.
- **Transfer Simple (76 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)
    - Target Address (4 bytes)
    - Amount (4 bytes): How much to transfer.
- **Transfer with State Update (108 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)
    - Target Address (4 bytes)
    - Amount (4 bytes)
    - State Hash (32 bytes): Hash of the state post-transaction.
- **Change Account Keys (244 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)
    - New Public Keys Data (176 bytes): The public keys replacing the old ones in the account:

      Schnorr Public Key: 32 bytes

      BLS Public Key: 48 bytes
      Proof of Possession (BLS Signature): 96 bytes
- **Create Account (248 bytes total)**
    - Signature (64 bytes)
    - Source Address (4 bytes)
    - Initial Amount (4 bytes)
    - Public Keys Data (176 bytes): Establishing the credentials for the new account:

      Schnorr Public Key: 32 bytes

      BLS Public Key: 48 bytes
      Proof of Possession (BLS Signature): 96 bytes

Batch or Contract Transactions (Variable size)

- Signature (64 bytes)
- Source Address (4 bytes)
- Variable payload depending on the batch or contract specifics, which could include:
    - For batch transactions: Aggregated transactions data.
    - For contract transactions: Contract invocation data such as function identifiers, arguments, etc.

General Structure for Variable Size Transactions

- **Signature (64 bytes):** Digital signature to verify the authenticity and integrity of the transaction.

- **Source Address (4 bytes):** The identifier for the account initiating the transaction.
- **Amount (4 bytes):** Defines the amount involved in the transaction. For batch transactions, it may represent the aggregated total fee paid by the batcher. The batcher is paid off-chain through the changes in tx hashes.
- **Pad (1 byte):** Determines the transaction type; values greater than 1 define a batch transaction, otherwise, it's a contract transaction. The exact value of this byte defines the padding with zero data to avoid matching the length of the previous transactions.
- **State (40 bytes: 32 bytes state hash with 8 byte blockHeight):** Contains state-related hash, with the block height encoded in the last 8 bytes of the state field.
- **Addresses (Variable size, batch-specific):** For batch transactions, contains multiple 4-byte length indexes representing the participating account addresses.

Batch Transactions

- **Addresses (Variable size):** A list of 4-byte indexes representing the participating accounts, used in batch transactions to aggregate multiple operations.

The transaction structure is designed to be flexible, accommodating different types of operations within the same framework. In batch transactions, the `addresses` field is crucial for identifying all participating accounts, and the `state` field contains necessary state data along with the block height information encoded in its last 8 bytes, which is crucial for maintaining the integrity and order of transactions within the blockchain.

Contract Transactions

- **Payload (Variable size):** Specific to contract transactions, contains the data necessary for contract interaction, like function calls and arguments. The start of the payload is after the `pad` and `amount` for contract-specific data.

Execution and Verification Logic

- In `verifyBatch`, the function checks the block height against the recorded state to ensure the transaction's validity within the current blockchain context.
- In `execBatch`, the batch transaction execution involves iterating over the addresses, modifying state and balances as per the transaction logic defined.

Execution and Verification Data

- **Public Keys associated with Addresses**: For all accounts, public keys are **associated with 4 byte** addresses, ensuring the link to the correct account entities within the blockchain.
- **Counters (or Nonces)**: Used to maintain the sequence and prevent transaction replay attacks. The transaction is hashed with a counter, and the signature signs this hash.
- **State Hash**: Each transaction alters the off-chain state of the account, represented by a hash that encapsulates the chain of all previous account states.