













































## 9. APPENDIX

### Spot XBT validation construct

To submit a Spot XBT order, the Participant must have a valid Authentication Address. The Authentication Address is used to verify a Blockchain address and have this validation publicly available on the Bitcoin Blockchain.

The Settlement model offers a secure, mutual-acceptance, Settlement method whereby authenticated Participants can settle Spot XBT trades in a trust-less manner while maintaining their anonymity towards each other.

#### (a) Participant ID

Participants are designated a Participant ID which is fixed over the lifetime of the Account. The Participant ID is a unique 256-bit number, and can be viewed in the BlockSettle Terminal when logged in to the service.

#### (b) Validation Address

Validation Addresses are public and known BlockSettle addresses from which BlockSettle funds and revokes Authentication Addresses.

#### (c) Participant Public Key

Participants are required to deliver a Public Key to BlockSettle.

#### (d) Authentication Address

Authentication Addresses are created by applying the Elliptic-Curve-Diffie-Hellman (ECDH) function to the Participant ID together with the Public Key submitted by the Participant to generate an Authentication Address.

#### (e) Authentication Address Validation

Upon receipt of a new Participant Public Key, BlockSettle will execute a Bitcoin payment (within 24h) of a small balance of Satoshis from a Validation Address to the Participant's Authentication Address.

Provided the UTXO residing on the Authentication Address has not been spent nor funded a second and subsequent time by BlockSettle from its Validation Address (revocation), the Authentication Address is considered valid.

#### (f) Settlement ID

Each Spot XBT order is issued a unique Settlement ID. The Settlement ID is a 256-bit number.

(g) Settlement Address

Once a Spot XBT trade is matched, both Participants will have the following details (i) their own Authentication Address, (ii) the counterparty's Authentication Address, and (iii) the Settlement ID. Using these inputs, the ECDH function is used to add the Settlement ID to the respective Authentication Addresses, whereafter a unique 1-of-2 Settlement Address is constructed.

(h) Pay-In / Pay-Out

After validating the integrity of the construct, the XBT Buyer signs the Pay-Out, after which the XBT Seller signs the Pay-In. At this point, both Participants have conducted Settlement Executions based on the Private Key they control, signaling a mutual acceptance of the terms of the trade.

## 9.2. Private Market Validation Construct

For Private Market products, each Private Limited Company has its own Genesis Address from where all Equity Account Tokens are issued. Any UTXO offered for sale as an Equity Account Token can be traced back to its public and known Genesis Address.

(a) Genesis Address

A Genesis Address is the address from where all Equity Account Tokens relating to a specific Equity Position Account are issued. All Equity Account Tokens can be traced back to this address.

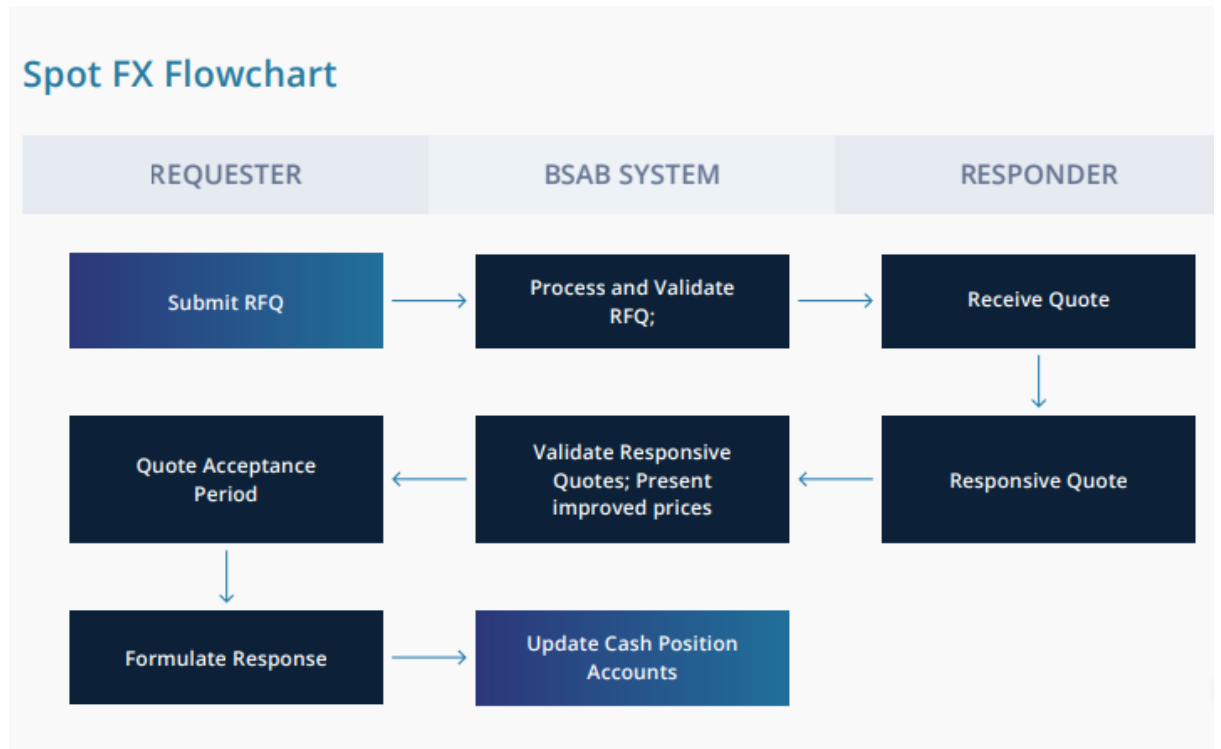
(b) Equity Account Tokens

Bitcoin Blockchain representations of the balance of Private Limited Company shares held by a Participant in an Equity Position Account. An Equity Account Token equals one share. Each Equity Account Token is represented by an amount of Satoshis.

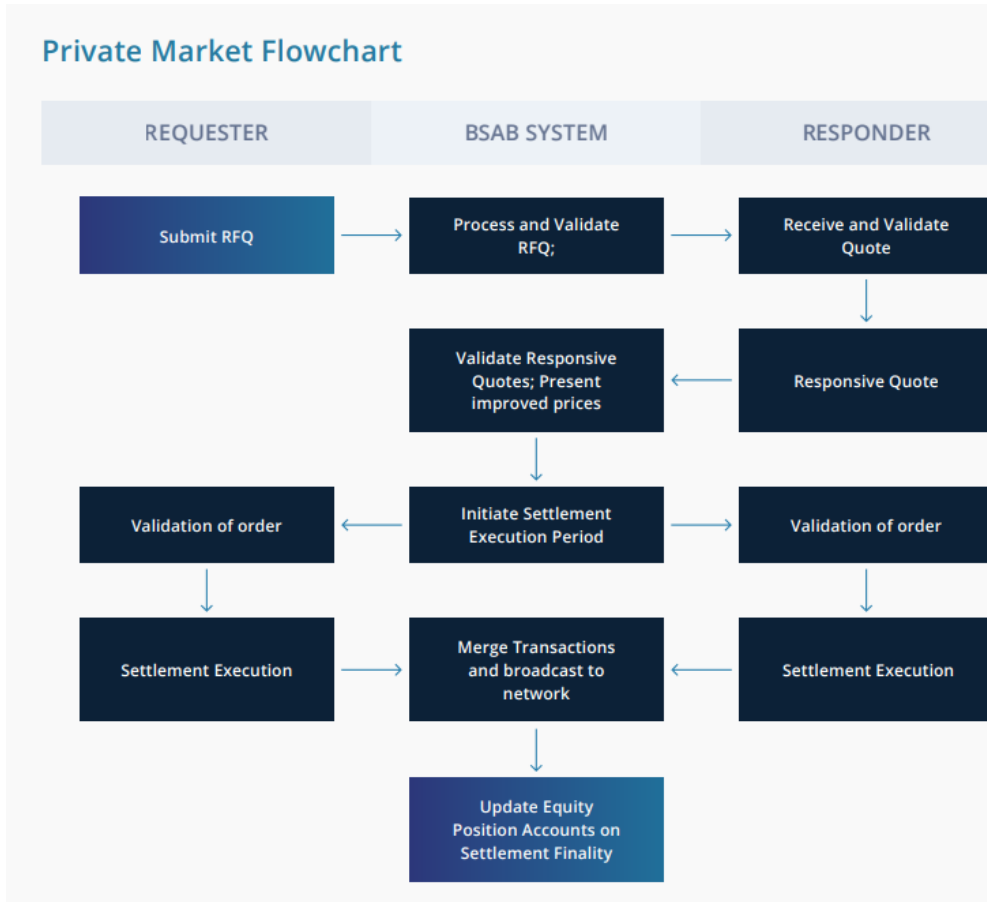
(c) Equity Wallet Leafs

Equity Account Tokens are maintained on deterministic derivation paths in the Participants Terminal. Each Equity Position Account has a deterministic path obtained by converting Equity Position Account instruments ticker to an integer (based on a hash of the human readable instrument denomination). All such wallets are grouped under a reserved coin type (as per BIP32 standardization procedure) representing Equity Account Tokens.

### 9.3. Spot FX Flowchart



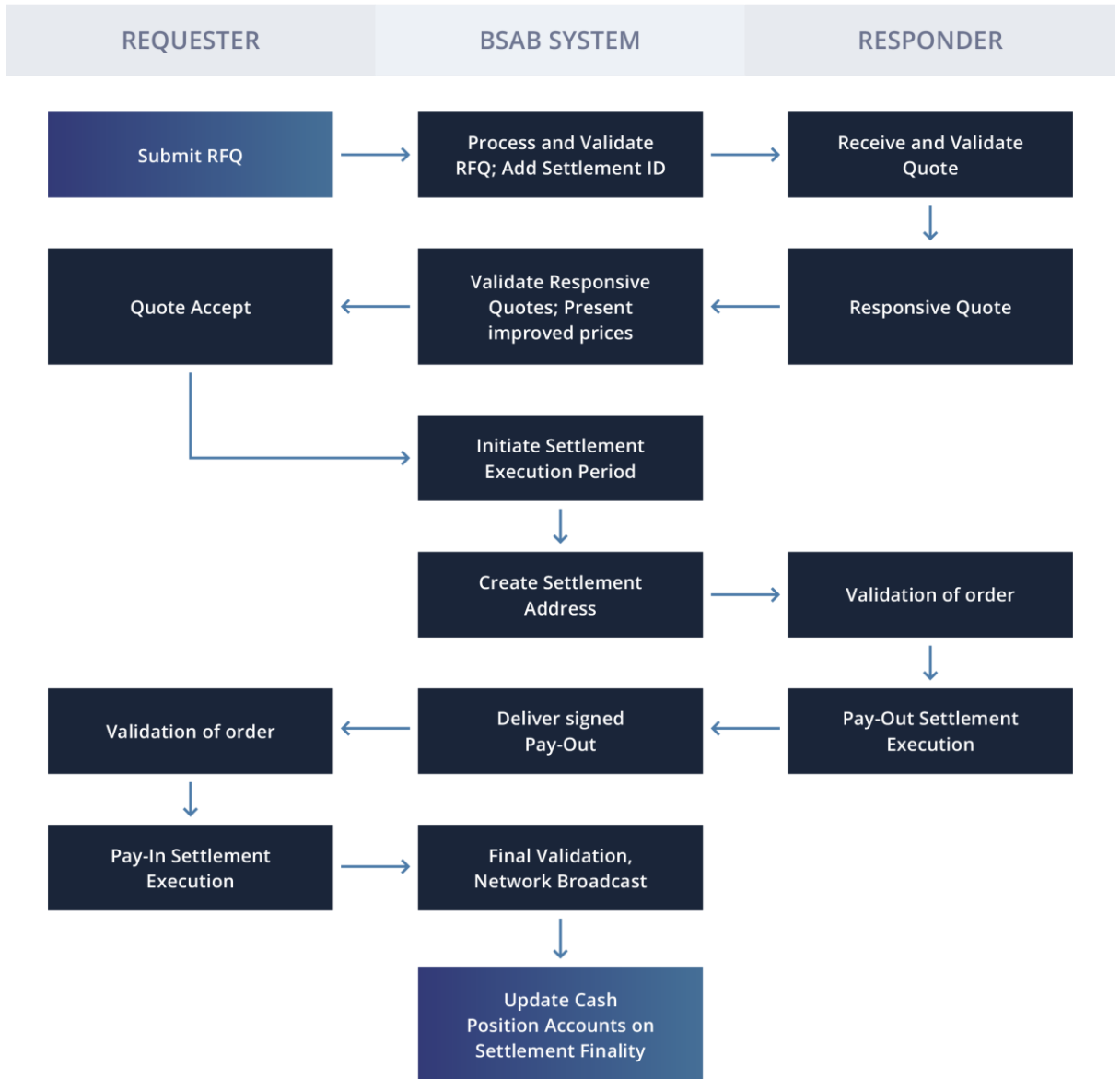
9.4. Private Market Flowchart





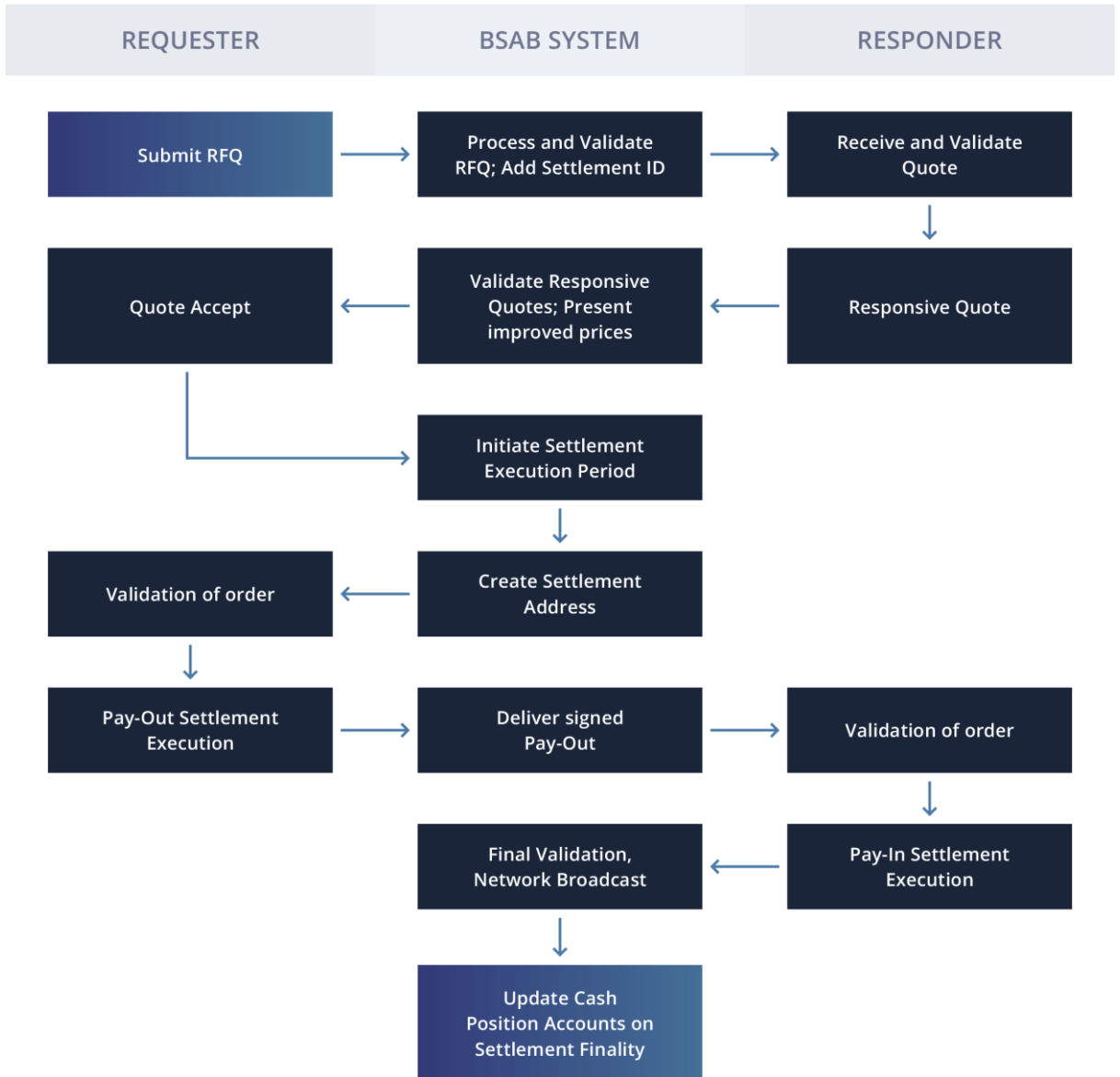
9.5. Spot XBT Sell Flowchart

### Spot XBT Sell Flowchart



9.6. Spot XBT Buy Flowchart

### Spot XBT Buy Flowchart



9.7. Authentication Address Creation Flowchart

## Authentication Address Creation

