Haveno Multisig Trade Protocol

Roles

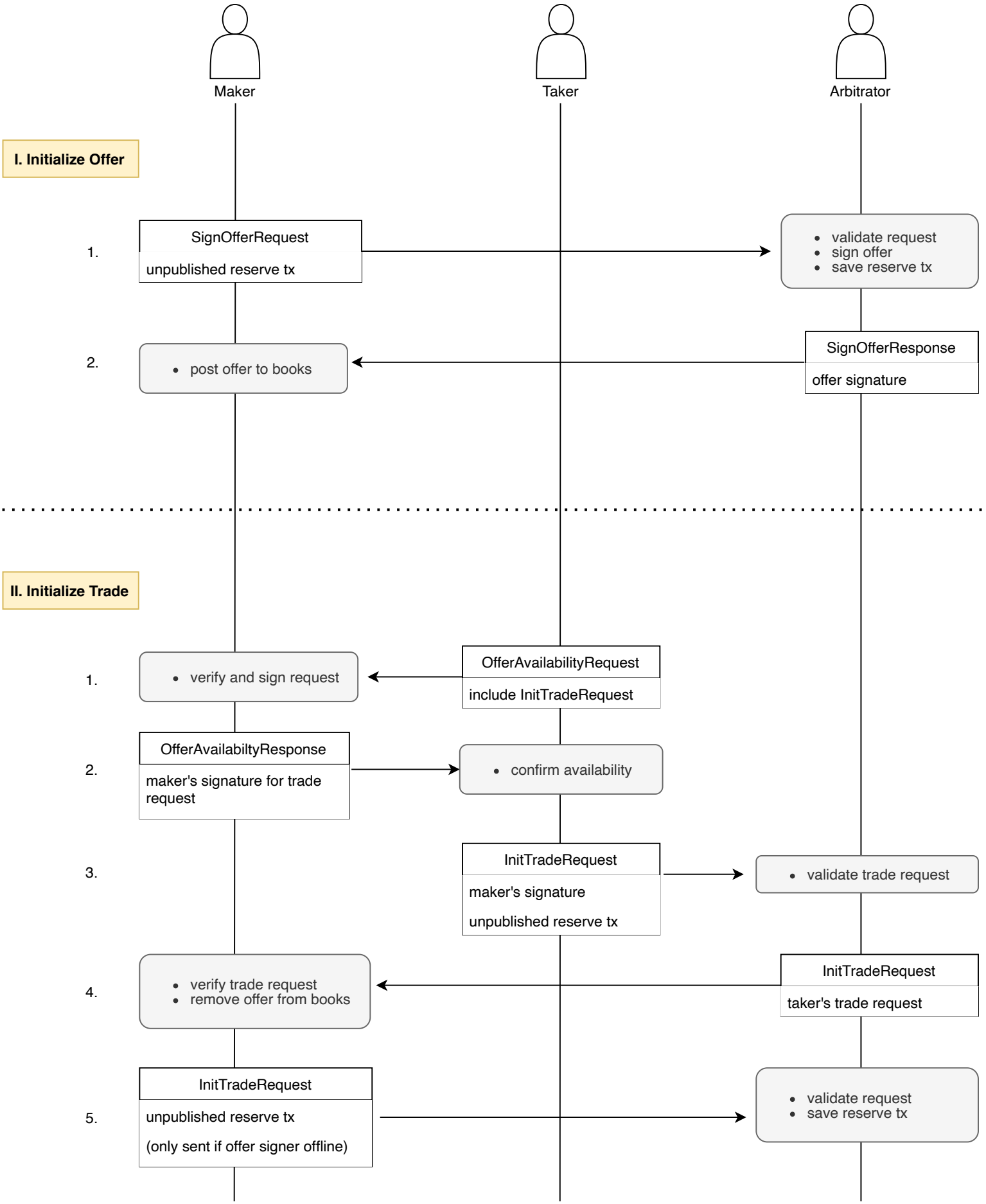
- **Buyer** - person buying XMR
- **Seller** - person selling XMR
- **Maker** - person making offer
- **Taker** - person taking offer
- **Arbitrator** - entity resolving possible disputes

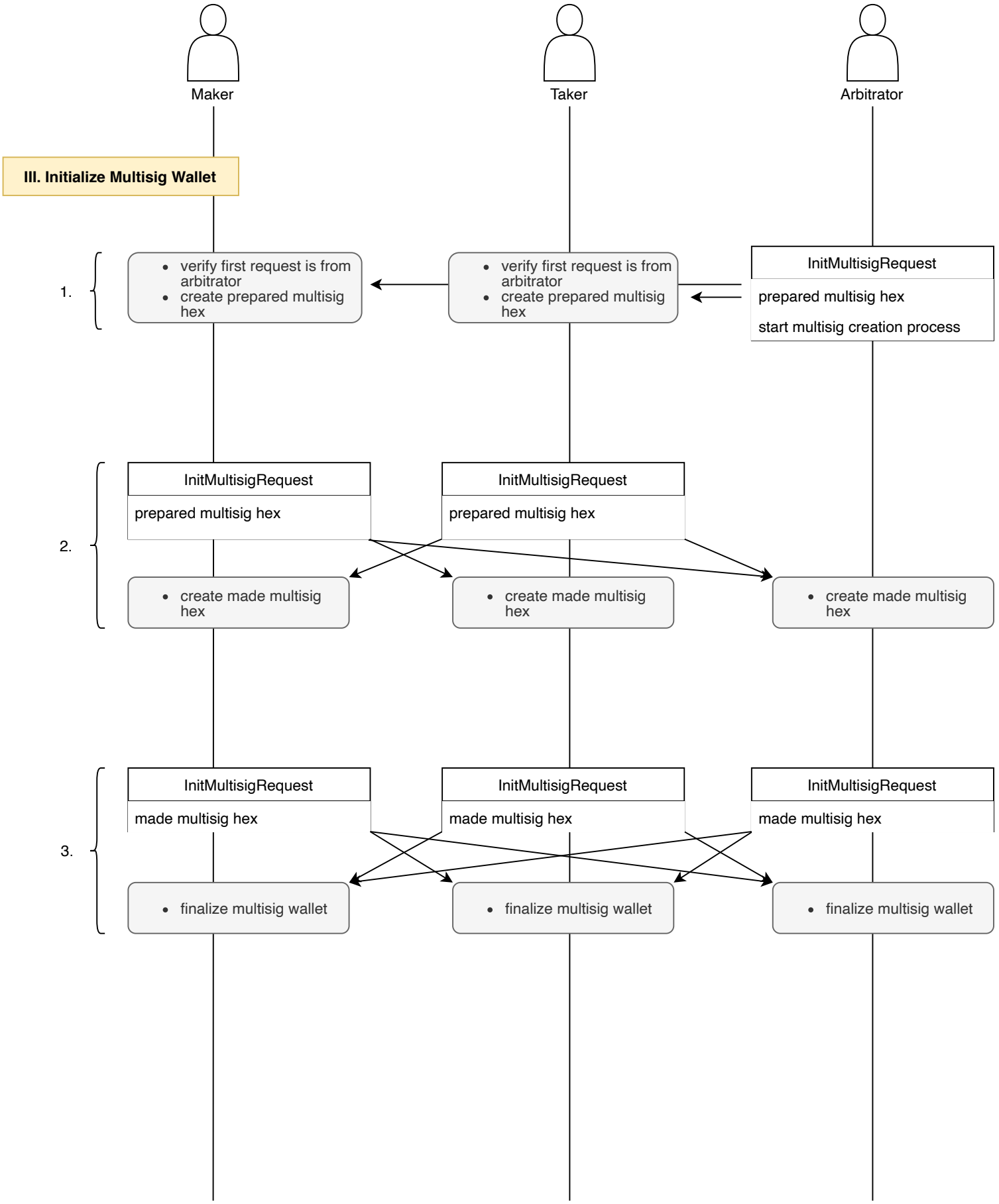
For each trade, a trader is a buyer or seller and a maker or taker.

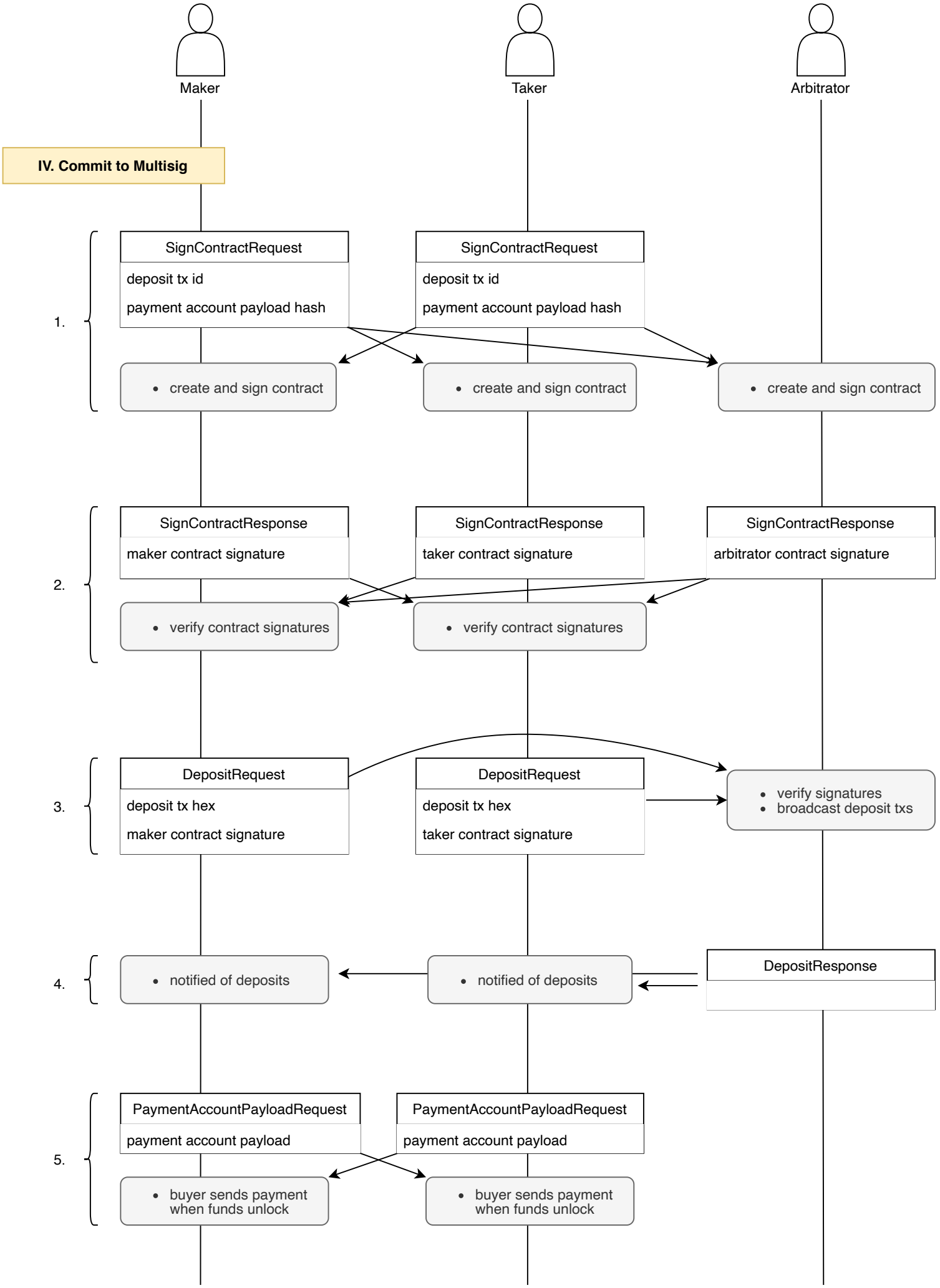
Protocol

1. Maker deposits funds to Haveno wallet and waits ~20 minutes. (optional)
2. Maker initiates offer. If maker does not have available or pending outputs to cover trade funds, prompt to first deposit to Haveno wallet and wait ~20 minutes.
3. Maker creates but does not relay "reserve transaction" which pays trade fee and returns multisig deposit amount to maker. Maker freezes input funds and submits offer to arbitrator to sign.
4. Arbitrator verifies maker reserve transaction and signs offer. If maker breaks protocol, arbitrator can punish maker by relaying reserve transaction to pay trade fee (unless maker spends reserved inputs which incurs mining fee).
5. Offer is posted and available to be taken immediately.
6. Taker deposits funds to Haveno wallet and waits ~20 minutes. (optional)
7. Taker verifies offer's arbitrator signature and initiates taking offer. If taker does not have available or pending outputs to cover trade funds, prompt to first deposit to Haveno wallet and wait ~20 minutes.
8. Taker creates but does not relay "reserve transaction" which pays trade fee and returns multisig deposit amount to taker. Taker freezes input funds and submits request to take offer to arbitrator.
9. Arbitrator verifies taker reserve transaction. If taker breaks protocol, arbitrator can punish taker by relaying reserve transaction to pay trade fee (unless taker spends reserved inputs which incurs mining fee).
10. Maker, taker, and arbitrator create 2/3 multisig wallet.
11. Maker and taker create but do not relay "deposit transactions" to pay trade fees and send deposit amounts to multisig. Buyer deposits trade amount + security deposit whereas seller only deposits security deposit.
12. Maker and taker sign contract with trade terms and ids of deposit trasactions.
13. Maker and taker submit signed contract and deposit transactions to arbitrator.
14. Arbitrator verifies contract and deposit transactions then relays deposit transactions to commit funds to multisig.
15. Buyer pays seller (e.g. sends ETH) outside of Haveno after at least a few confirmations.
16. When the multisig deposits are available (after ~20 minutes) and payment is acknowledged, maker and taker sign to release funds from multisig to payout addresses, or one trader opens a dispute with the arbitrator.
17. Arbitrator resolves dispute if applicable.

Note: all steps involving the arbitrator are automatic except resolving disputes.


Maker
Taker
Arbitrator
I. Initialize Offer
1.
SignOfferRequest
unpublished reserve tx
validate request
sign offer
save reserve tx
2.
post offer to books
SignOfferResponse
offer signature
II. Initialize Trade
1.
verify and sign request
OfferAvailabilityRequest
include InitTradeRequest
2.
OfferAvailabiltyResponse
maker's signature for trade request
confirm availability
3.
InitTradeRequest
maker's signature
unpublished reserve tx
validate trade request
4.
verify trade request
remove offer from books
InitTradeRequest
taker's trade request
5.
InitTradeRequest
unpublished reserve tx
(only sent if offer signer offline)
validate request
save reserve tx


Maker
Taker
Arbitrator
III. Initialize Multisig Wallet
1.
verify first request is from arbitrator
create prepared multisig hex
verify first request is from arbitrator
create prepared multisig hex
InitMultisigRequest
prepared multisig hex
start multisig creation process
2.
InitMultisigRequest
prepared multisig hex
InitMultisigRequest
prepared multisig hex
create made multisig hex
create made multisig hex
create made multisig hex
3.
InitMultisigRequest
made multisig hex
InitMultisigRequest
made multisig hex
InitMultisigRequest
made multisig hex
finalize multisig wallet
finalize multisig wallet
finalize multisig wallet


Maker
Taker
Arbitrator
IV. Commit to Multisig
1.
SignContractRequest
deposit tx id
payment account payload hash
SignContractRequest
deposit tx id
payment account payload hash
• create and sign contract
• create and sign contract
• create and sign contract
2.
SignContractResponse
maker contract signature
SignContractResponse
taker contract signature
SignContractResponse
arbitrator contract signature
• verify contract signatures
• verify contract signatures
3.
DepositRequest
deposit tx hex
maker contract signature
DepositRequest
deposit tx hex
taker contract signature
• verify signatures
• broadcast deposit txs
4.
• notified of deposits
• notified of deposits
DepositResponse
5.
PaymentAccountPayloadRequest
payment account payload
PaymentAccountPayloadRequest
payment account payload
• buyer sends payment when funds unlock
• buyer sends payment when funds unlock