Corda Interoperability: Cross-chain swaps

A worked example

Cross-chain swaps in Corda

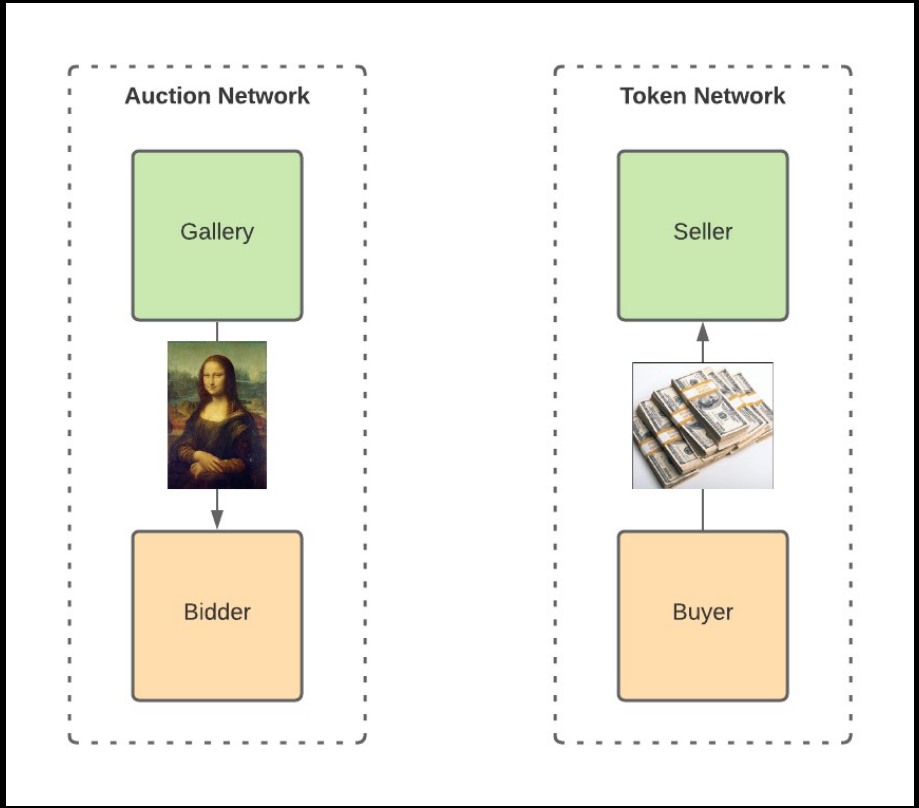
- The Corda 5 network model separates *applications* into distinct *networks*.
- This creates a need for mechanisms for reliable interoperation between applications/networks.
- Cross-chain swaps are one of the primary mechanisms for two-way exchange of state:
  - An **asset** on one network is exchanged for
  - **consideration** (e.g. tokens) on another
  - Either *both* receiving parties obtain the transferred state, or *neither* does.

A Tale of Two Networks

An *Auction* network enables participants to track ownership of digital art works.

A *Token* network enables fungible tokens representing digital currency to be sent from one party to another.

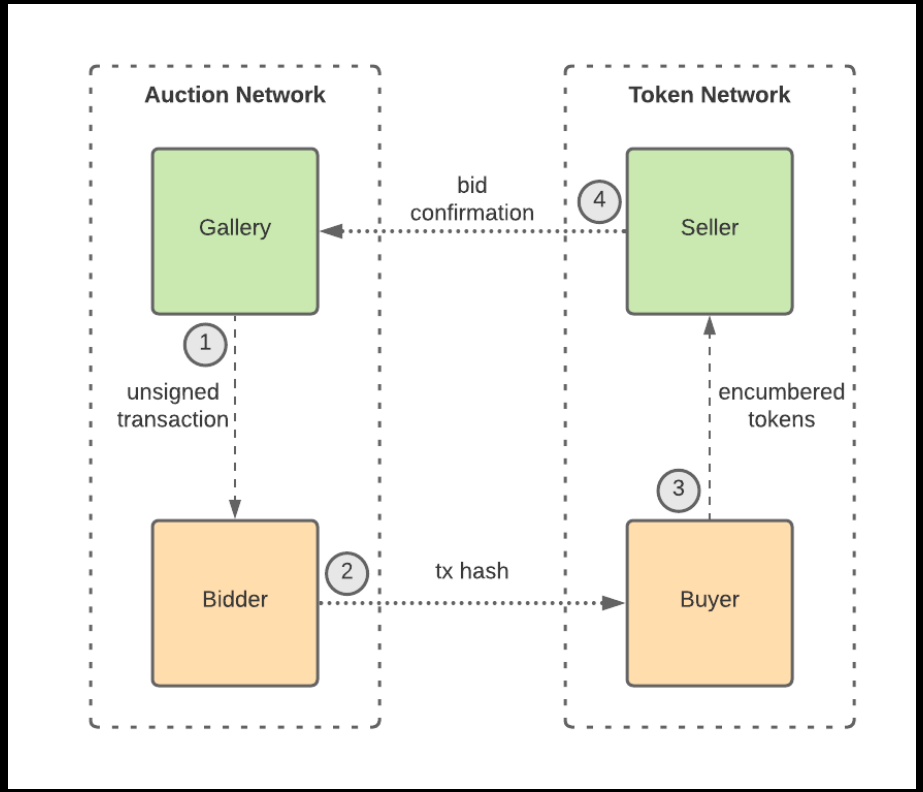
We would like to use tokens on the token network to pay for the purchase of art works on the art network.



Set-up phase

We begin with the exchange of two *partial legs*:

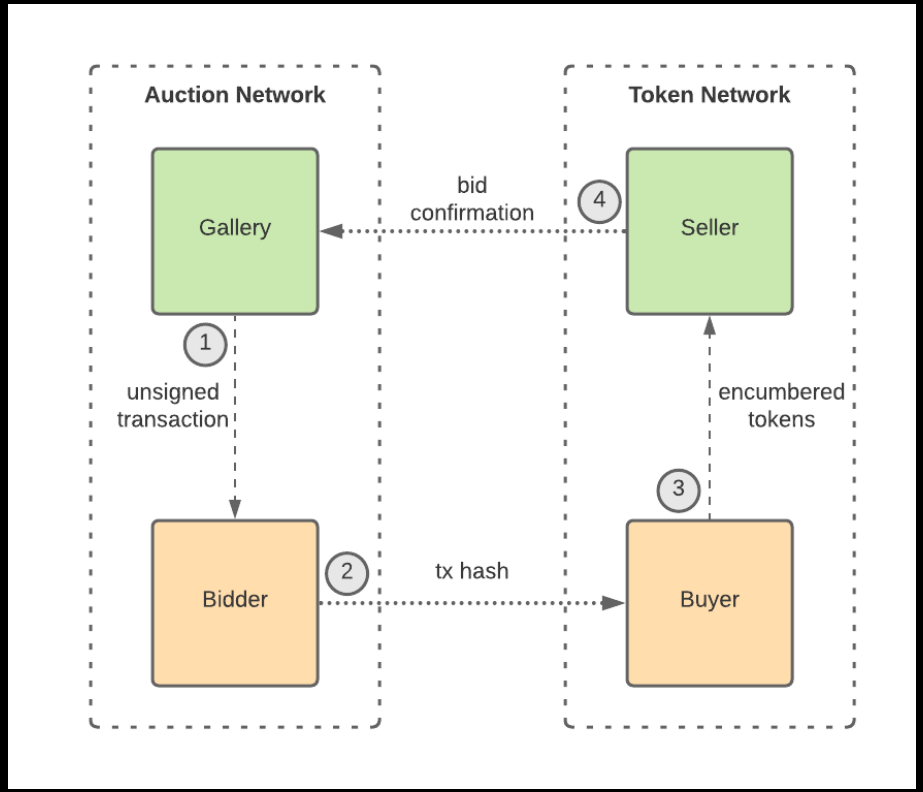
- (1) The bidder requests an *unsigned transaction* from the gallery, and verifies that it would transfer ownership of the artwork from the gallery to the bidder.
- The gallery constructs a transaction, which includes a timestamp for completion of the swap.



Set-up phase

(2) The bidder instructs the buyer, its counterpart on the token network, to offer tokens to the seller, passing across:

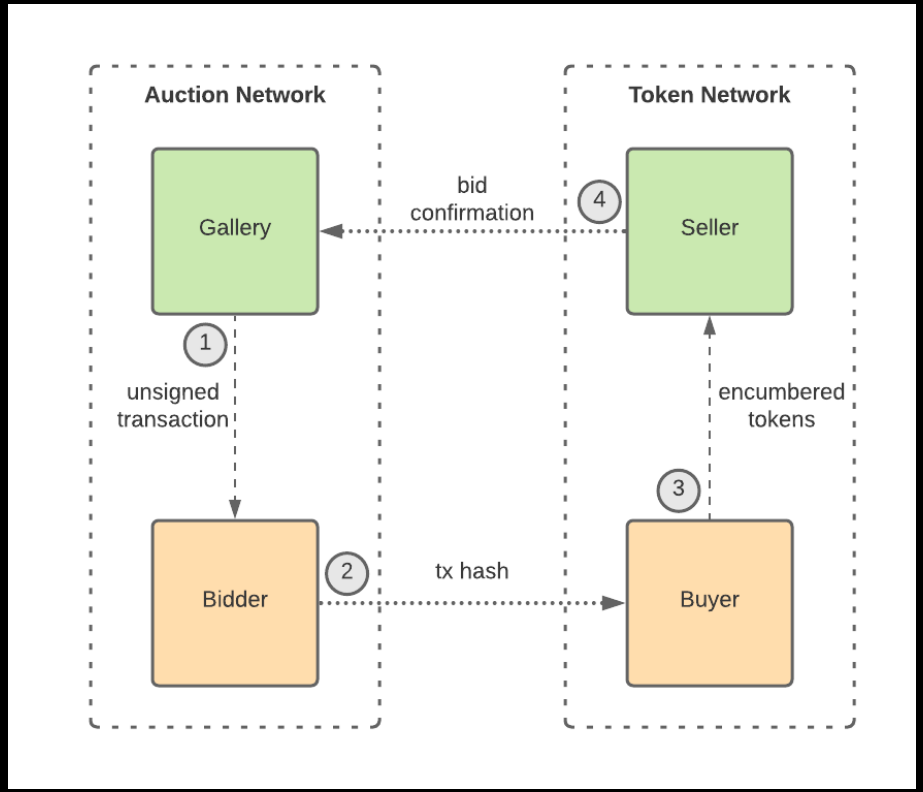
- the transaction hash
- the expiration timestamp
- details of the notary whose signature on the transaction hash is to be trusted as **proof of action** (i.e. that the transaction has been signed)



Set-up phase

(3) The buyer sends *encumbered tokens* to the seller:

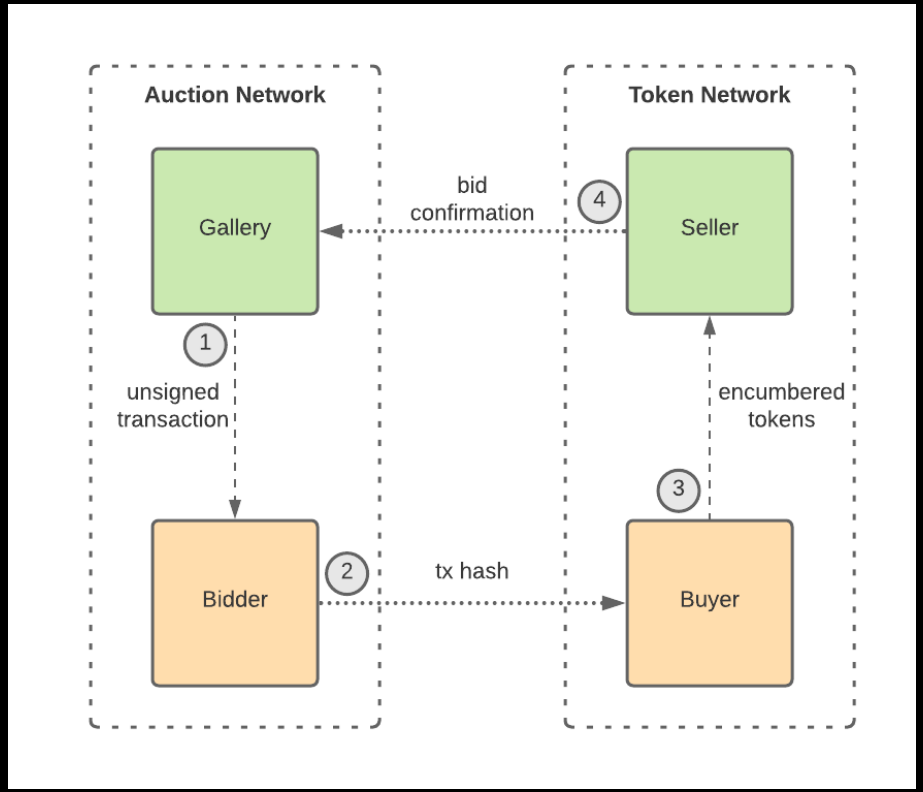
- Owned with a composite key (buyer and seller), cannot be used by either unless unlocked.
- Can be unlocked to the seller, given the auction network notary's signature against the hash of the transaction.
- Can be unlocked to the buyer after the timestamp has elapsed.



Set-up phase

(4) The seller confirms to the gallery that the encumbered tokens have been received:

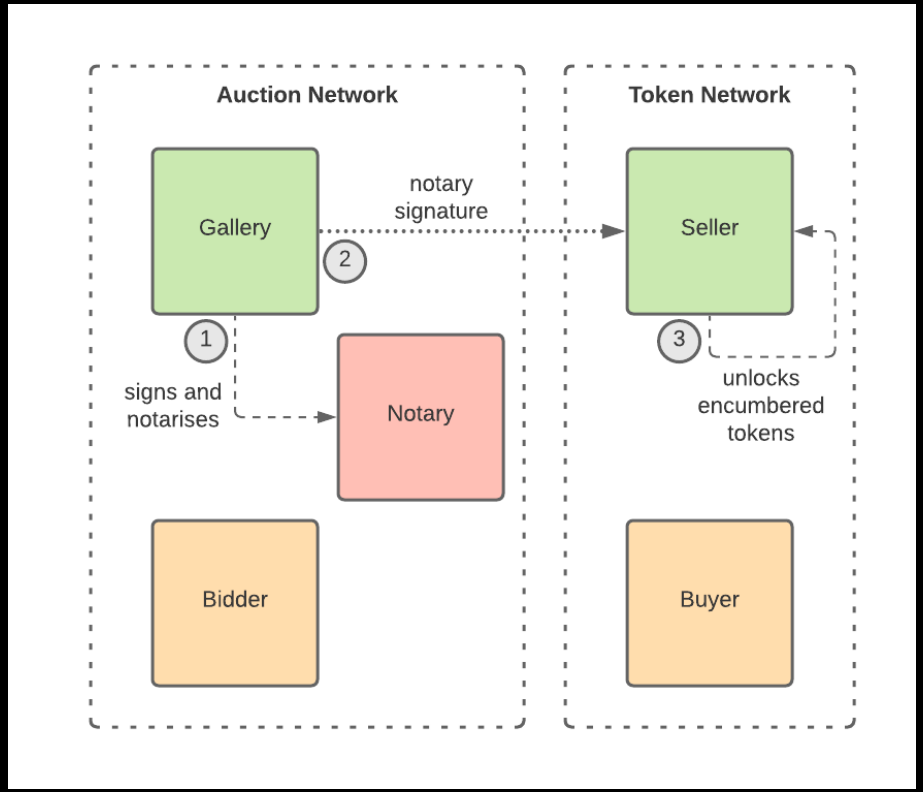
- The expiry timestamp must match that set by the gallery on the unsigned transaction.
- The gallery must have time, given observed clock drift between the two networks, to complete the next phase before the timeout occurs.



Proof of action phase

The legs are now completed using a notarized *proof of action*:

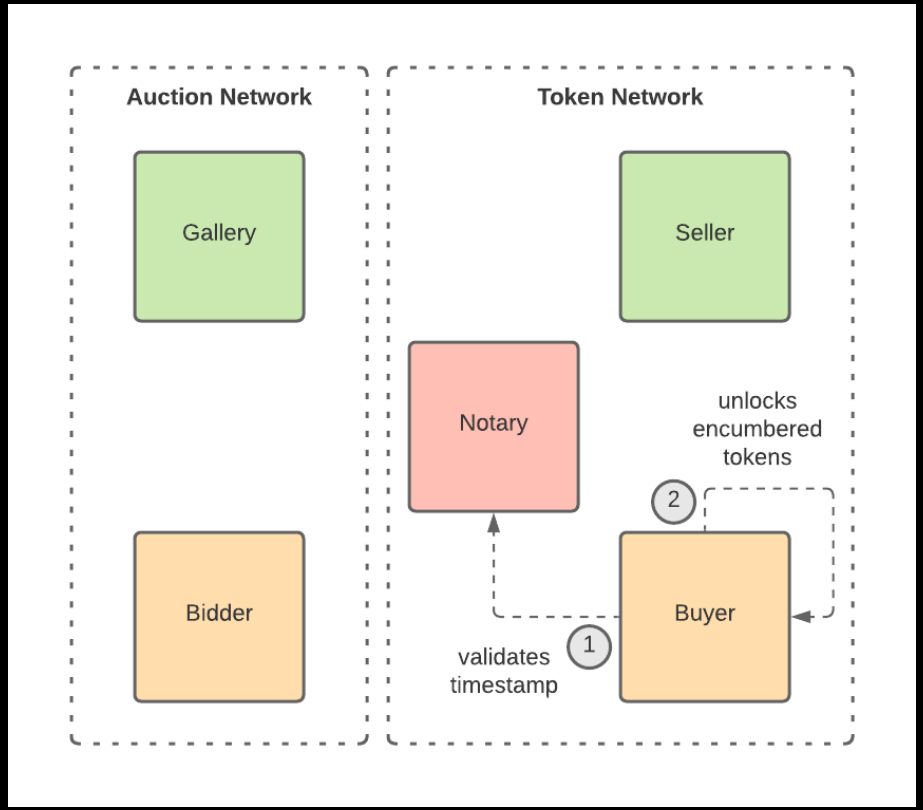
- (1) The gallery signs and notarizes the transaction transferring the artwork to the bidder. The notary validates that the gallery's signature is present.
- (2) The gallery passes the notary signature to the seller,
- (3) which uses it to unlock the tokens, according to the rules under which they were encumbered.



Rollback phase

If the gallery does not supply proof that the transaction has been signed within the given time frame, they revert to the buyer:

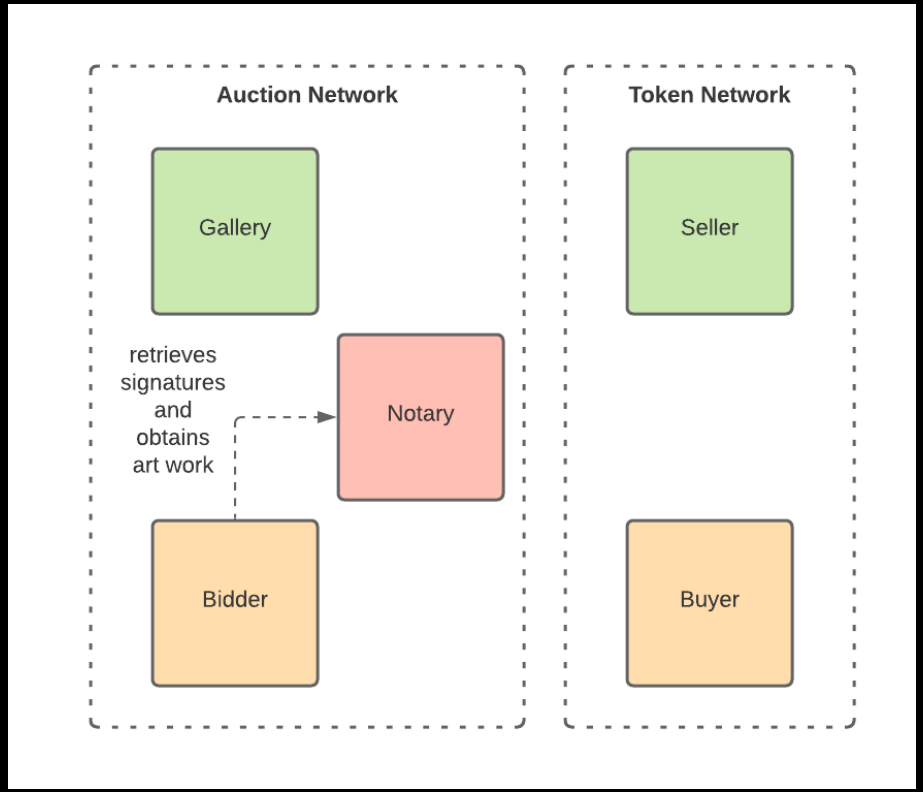
- The notary on the token network is the authority on when the transaction releasing the tokens to the buyer was notarized – it is only valid if this is after the time-out period has elapsed.



Denial of state remediation

If the gallery does not share the signed and notarized transaction with the bidder during finalization, the bidder can retrieve the signatures from the Art network Notary.

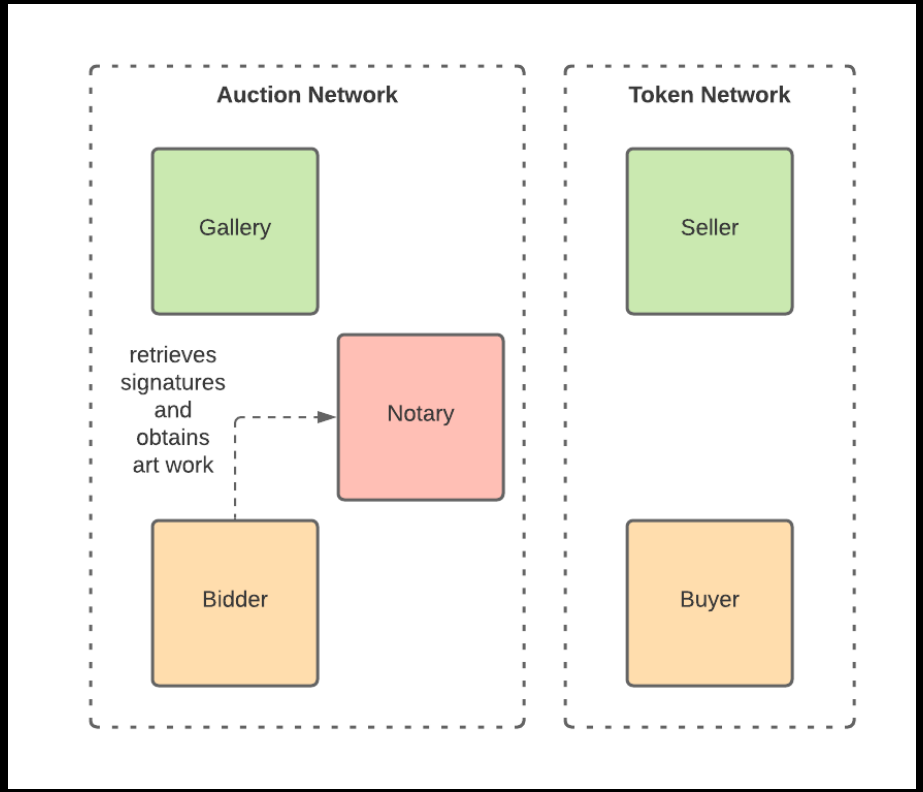
- The Corda 4 non-validating notary cannot do this.
- A fully-validating notary can, but is not a suitable solution in all cases.



Denial of state remediation

A signature-validating notary is being developed for Corda 5 that:

- Includes full signature data in the notarized Merkle tree (but tears off other transaction details).
- Validates the presence of required signatures.
- Enables future retrieval of signatures, by transaction hash, by interested parties.



Notaries as source of trust

This approach eliminates the need for additional trusted intermediaries to perform escrow or other services between networks:

- The bidder trusts the art network notary as a *finality authority*, and instructs the buyer to trust this notary's signature on the unsigned artwork transfer transaction as a condition for unlocking encumbered tokens.
- The seller trusts the token network notary as a *timestamp authority*, and accepts as valid the condition that encumbered tokens can be returned to the buyer if they have not been unlocked within the stated time frame.

Thank you

r3.com | corda.net | conclave.net

linkedin.com/company/
r3cev-llc

@inside_r3
@cordablockchain
@conclavecompute

New York
1155 Avenue of the
Americas,
34th Floor,
New York, NY 10036

Dublin
Lennox Building
50 Richmond St South
Saint Kevin's, Dublin,
D02FK02

San Francisco
655 Montgomery St., 6th
floor
San Francisco, CA 94111

Tokyo
Izumi Garden Tower 19F,
1–6-1 Roppongi, Minato-ku,
Tokyo 106-6019, JAPAN

London
2 London Wall
Place,
London, EC2Y 5AU

Hong Kong
Bonham Strand, 7F Office
18-121
Hong Kong

São Paulo
Av. Angélica, 2529
Bela Vista- 6th Floor
São Paulo - SP, 01227-200
Brazil

Mumbai
01A108, WeWork Enam
Samhav, C-20, G Block,
Bandra Kurla Complex,
Mumbai, 400051, India

Singapore
18 Robinson Road, Level
#14-02
Singapore, 048547