Please create this COW-specific Smart Contract Wallet. I can't.

The idea is that it's managed by 2 keys: 1 for trading and 1 for withdrawing.

The "withdraw" key can (1) send/withdraw the funds to any external wallet, (2) add ERC20 tokens to a whitelist, (3) Update the "trade" key. — The "withdraw" key is kept in cold storage.

The "trade" key can trade any of those whitelisted ERC20 tokens into any other whitelisted ERC20 token. — The "trade" key can be a hot wallet. If it gets compromised the worst the attacker can do is initiate a bunch of trades.

There's probably some added complexity with "allowing to spend", but that's besides the point. Perhaps the allowance should be granted at the same time the "withdraw" key adds a token to the whitelist.