Oracle-integrated Multisig wallet

**Project:** Oracle-integrated Multisig wallet

**Author:** Vinh Le

**Date:** 2 September 2022

**Overview:**

A multisig factory web3 dapp allowing user to create multisig wallet with off-chain signature to save gas, pre-compute multisig wallet for fund deposit, add or remove signers/owners based on needs. This multisig wallet also integrate an oracle which supports adding signers when a certain threshold on BTC reserves/ ETH price is reached (too low/high), hence give owners additional method to escape funds when losing the private key/ access to the wallet.

**Deliverables:**

1. Web App: A user-friendly multisig factory web application that allows users to:
   1. Connect their wallets
   2. Create multisig wallet by specifying wallet name, owners, quantity of signature required on the desired networks
   3. Sign off-chain to save gas fee
   4. Add signers, remove signers, owners
   5. Change the number of signatures required
   6. Receive pre-computed multisig wallet address so user can deposit funds to wallet
   7. Allow oracle options (check BTC reserves/ ETH price) which allows for additional signatures provided when price/reserves thresholds are triggered facilitating fund sell/trade
   8. Distribute funds equally or according to predefined allocation to owners’ wallets
2. Smart Contract(s): A set of smart-contracts to perform off-chain sign activities to on-chain transactions to maintain transparency.
   1. MultisigFactory
      1. A mapping to list to keep track of every multisig wallet created.
      2. Creating a new multisig wallets with list of owners, number of signatures required, chainId parameters
      3. Use create2 from OpenZeppelin to pre-compute multisig-wallet based on user-defined wallet name (hash function)
   2. MultisigWallet
      1. Contracts defining constructor, init and other functions of a multisig wallet instance including add, remove signers, change number of signatures, make transactions, etc.
      2. Support recovering the original signer of the message
      3. Sign 1 signature given the threshold of price feed/reserve is triggerd
   3. Oracle
      1. Integrate WBTC reserves and WBTC contract to check supply against reserves through data feeds
      2. Integrate ETH price feed to check for price against threshold
      3. Return boolean for comparisons to aid in signing conditional logics of Multisig wallet

**Workflow Visual:**

Chart, diagram, funnel chart

Description automatically generated