- Zero Knowledge setup params are generated/finalized by ceremony
- EA generates & deploys smart contracts

- Voters send identity commitments to EA
- Proposers send blockchain addresses to EA
- EA decides eligible voters/Proposers
- EA registers eligible proposer addresses to smart contract
- EA creates merkle tree from eligible voter identity commitments
- EA registers merkle tree root and identity commitments to smart contract

---

- Proposers propose a solution to the question (candidate)

- Voters decide voter secrets / preference list
- Voters generate zero knowledge proof for their vote commitments
- Voters send proof and vote commitments to smart contract
- Smart contract checks proof & stores commitment

- Voters send their vote secrets to smart contract to reveal their vote commitments
- Smart contract store revealed votes

- Everyone can issue a result query to smart contract to get the election result