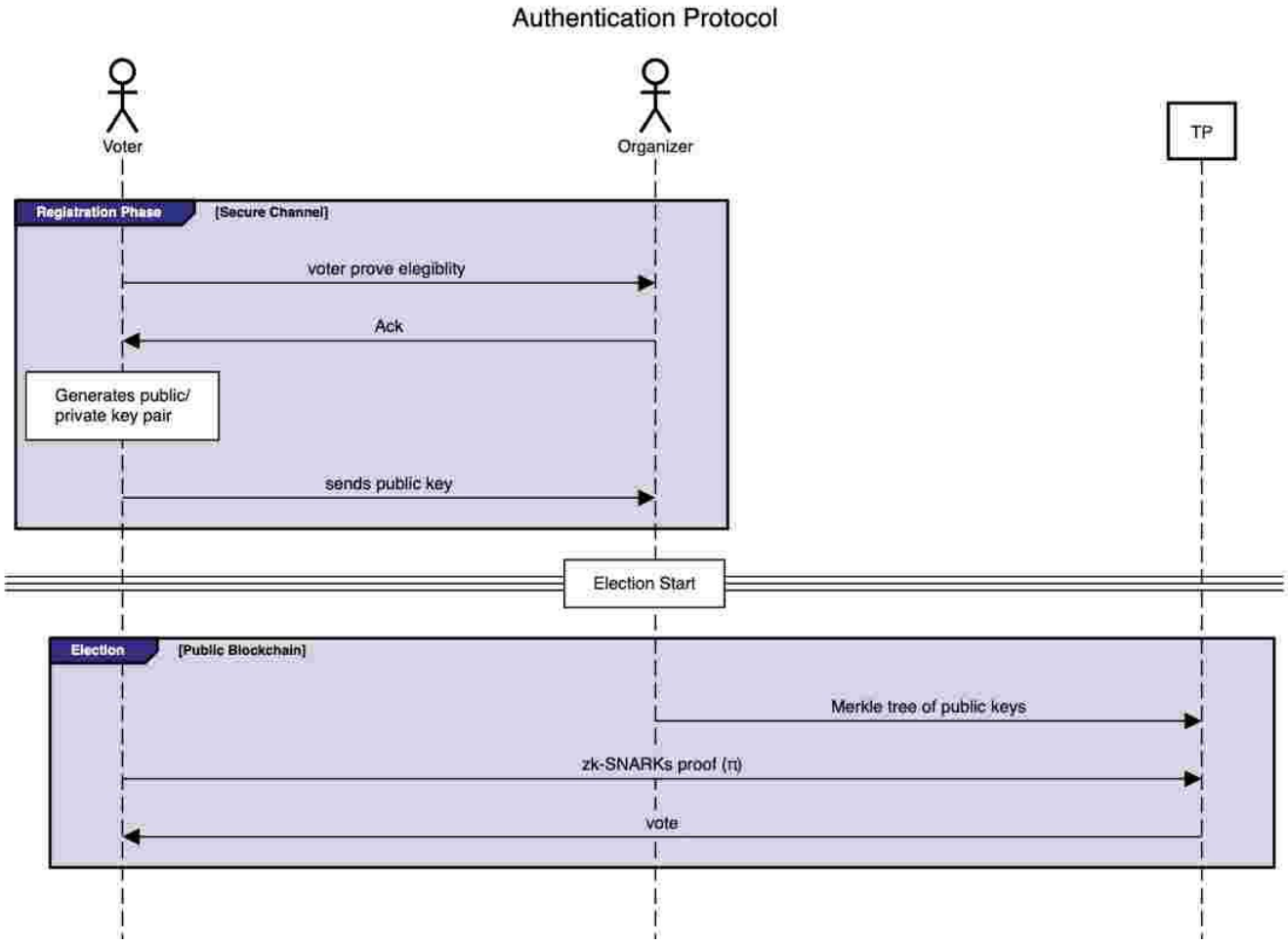
Authentication process of the TP

Following the protocol of Z-cash[1] and the following proposal[2], the authentication protocol of the TP will be as follow:

1. The voter would identify to the organization to prove elegibility of the vote.
2. Once verification acknowledged, voter generate a pair of public / private key (p_b, p_v) and gives the p_b to the organization
3. The organization deploys the TP, with a Merkle tree of the p_bs of verified users as input parameter
4. In order to receive the vote from the TP, the voter has to construct a zk-proof, π s.t:
    1. π proves that the voter has knowledge of a p_b in the Merkle tree
    2. π proves that the voter has knowledge of a p_v that construct p_b

Sequence Diagram



References

1. https://www.youtube.com/watch?v=84Vbj7-i9CI
2. https://ethresear.ch/t/zero-knowledge-proof-of-membership/3084