I. Introduction

One of the modern advancements that has gained use during elections is electronic voting or e-voting. E-voting's main objective is to improve the effectiveness and minimize the expenses associated with convention voting [1]. However, these e-voting systems are often concerned with security issues such as voter privacy or data relevance. Traditional voting techniques also incur significant costs, including time for registering voters and counting their votes. Based on these factors, implementing electronic voting systems presents a logical step forward [2].

Blockchain technology assists us in getting rid of these issues as it is decentralized, secure, and ledger-like for storage and transaction verification [3] [4]. For instance, all blockchain transactions are encrypted and authenticated in a peer-to-peer network [5], making changes nearly impossible. This work enhances the blockchain-based electronic voting system by applying Zero Knowledge Proof (ZKP). ZKP is a cryptographic method that verifies supporting evidence without revealing protected information [6]. This research develops smart contracts that facilitate the self-execution and validation of transactions using digital signatures [7]. These eliminate third-party intermediaries to ensure greater transparency and security [8].

Several previous studies have focused on introducing blockchain technology into e-voting systems. Hjalmarsson et al. [9] proposed a cost-efficient and anonymous voting system by incorporating blockchain technology into electronic voting based on smart contracts. Tso et al. [10] utilized smart contracts in their vision of e-voting systems to remove the need to operate through a third party, enhancing the security features of users and the system, thus making it more reliable. Bhawiyuga et al. [11] designed an application that runs on the decentralized Ethereum platform and is intended to maintain the authenticity of stored e-voting data. Rathee et al. [12] combined IoT devices with Blockchain technology to create a quick and cost-effective e-voting system. Therefore, we apply ZKP to maintain voter privacy and anonymity in this case. We rely on the Polygon network to achieve lower costs and quicker transactions.

We implement an e-voting system as a decentralized application (DApp) built on Polygon's layer 2 networks. The application systems implement a role-based access control system and integrate three user classifications. First, a Superadmin's role is to control the registration of candidates and supervisors' accounts. Second, a Supervisor's role is to register voters and supervise elections. Lastly, the voters vote securely. The ZKP guarantees voter privacy by allowing for voter verification, anonymous voting with the possibility of verification, and not disclosing identity while verifying voting eligibility. These mechanisms can address the most significant difficulties in achieving a safe, private, and effective voting procedure.