1 Abstract

An electronic voting protocol provides end-to-end verifiability if the voter can verify that their vote was correctly counted and any party can verify the results of the election. There have been several proposals outlining potential systems, however these have all been built on top of protocols primarily designed as transaction ledgers. In this paper I propose a voting solution, built on the Ethereum protocol, that uses the properties of smart contracts to enforce strict rules surrounding the ballots of an election. These ballots are both independently and universally verifiable and maintain all of the desirable properties of the blockchain (such as immutability). All of this is achieved without sacrificing voter privacy or ballot integrity. The resulting system shows clear potential for Blockchain technology to become a central part of applications wishing to provide transparency and security in public scenarios.