1 Abstract

Existing electronic voting systems all suffer from a serious design flaw: They are centralized by design, meaning there is a single supplier that controls the code base, the database and the system outputs while also supplying the monitoring tools to verify the result. The lack of an independently verifiable system means that, once voters mark their ballot choice, they must place their trust in the organization that their vote is recorded and counted as intended. The lack of an independently verifiable output makes it difficult for these centralized systems to acquire the trustworthiness required by voters, thus potentially limiting voter participation, or cast doubt upon the published output of an election.

To provide an immutable, verifiable and secure online voting system I intend to leverage the availability of the Bitcoin Blockchain as a secure transaction database. From this public ledger, voters will be able to independently audit the inclusion of their vote, and the outcome of the election as a whole, while being sure that the results cannot be changed due to the immutability of the Blockchain.