1 Conclusion

1.1 Overview

Although this system has been designed and developed with the idea of a national general election in mind, the protocols and ideas involved could be applied to smaller scale ballots which wish to provide transparency in their audit. Although we wish to minimize trust in a central authority, due to the nature of these type of elections (where there needs to be some degree of voter eligibility verification), we cannot fully decentralize this system as we need to only allow those eligible the rights to vote. Despite needing to verify an individual we still need to ensure that their votes are publicly anonymous, especially given the public transactions underpinning the blockchain concept while providing the ability for an individual to verify that their vote was correctly counted.

I do not see this system as a direct "replace all" for national election voting. I believe there will still be a need for traditional voting implementations in certain situations; for example, maintaining postal vote for the elderly who may not have the technical capability or equipment for online voting. However I do think that this could be phased in along side traditional voting, eventually replacing the pre-existing e-voting systems and ultimately becoming the main way for the majority of people to choose their government.

I started this project with the goal of producing an 'end-to-end' verifiable voting platform. This project succeeds in presenting the protocol for such a system through use of Blockchain technology.

The system provides *individually verifiability*. When voters submit their vote they receive a transaction hash which they can use to check that their vote was successfully included in the Blockchain. This 'cast-as-intender verification' can only be done by the voter, as they are the only one who knows which specific transaction relates to them. While some level of voter education would be necessary for the average voter to desire & be able to check their vote was counted (as the onus of this does still rest with the voter), at worst this is no different from the currently employed systems where uses must trust their vote was submitted & counted correctly while providing benefit to those who engage in it.

The system also provides *universally verifiability* as anyone, whether they are participating in the election or not, can verify the results of the election through querying the ballot contracts. These results hold all of the desirable properties of the Blockchain such as being immutable & instantly globally distributed. Due to the underlying contract design, be assured that each Ethereum address voted at most once per ballot.

The system also manages to protect voter privacy through the use of blinded tokens. This is how the system is able to register an Ethereum address to a

ballot contract, without being able to link it to an individual, but they can be assured that it belongs to *some* verified voter. Voter privacy after the election is tied to the voter, as only they know the resulting transaction hash (voting receipt) for each vote cast it is kept private at their discretion.

While the proposed system does not solve all the issues associated with electronic voting, it does provide a valuable alternative to current proprietary electronic systems & has potential use in both governmental and private organizations wishing to conduct transparent ballots.