Internet Voting Using Zcash.

By Pavel Tarasov

Voting systems have been around for hundreds of years and despite different views on their integrity, have always been deemed secure systems with some fundamental security and anonymity principles. Numerous electronic systems have been proposed and implemented, however many of these systems have been rejected, while creating further suspicion about the integrity of elections due to detected security vulnerabilities within these systems. Electronic voting, to be successful, requires a more transparent and secure approach, than the approach that is offered by current electronic voting protocols. The approach presented in this paper involves a protocol developed on blockchain technology. The particular technology that is used as basis for the voting system is a new electronic currency protocol and offers a factor of anonymity in transactions, which has not been observed in blockchain technologies to date. The proposed voting protocol offers anonymity of voter transactions, while keeping the transactions private and the election transparent and secure. The underlying blockchain protocol has not been modified in any way, the voting scheme proposed merely offers and alternative use case of the protocol at hand, which could be presented as the basis for voting systems on blockchains with further development of underlying blockchain protocols.