

1 Introduction

Existing electronic voting systems all suffer from a serious design flaw; they are centralised 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 [1]. 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, which potentially limits voter participation, or cast doubt upon the published outcome of an election.

Despite the digitalisation of many aspects of modern life, elections are still being largely conducted offline, on paper [2], although the use of Electronic Voting Machines has been steadily growing over recent years. Paper ballots are still the traditional tool for voting and are typically marked by a human (voter) and then tallied by a machine. While costing less than most electronic systems to run, they rely on physical security and trust in polling stations to not manipulate and properly handle them [3]. Postal votes also utilize paper ballots and are used to allow voters to not have to physically attend a location in order to vote. These also suffer from the same flaws as traditional paper ballots while increasing the opportunities for attack during their passage through the postage system.

Voting systems comprise of five main components:

1. A registration service for verifying and registering legitimate voters.
2. Voter authentication stations with the task of determining a voters authorization to vote based on the completed work of the registration service.
3. Voting stations where the voter makes choices on a ballot.
4. A device called the ballot box where the ballot is collected.
5. A tallying service that counts the votes and announces the results.

Of the components listed above, only (2), (3) and (4) are used during an election, with (1) being required for an election to take place and (5) happening post election [4].

Current Electronic Voting (E-Voting) takes two forms; using a machine in a polling station, rather than a ballot paper and pencil, or casting a vote over the Internet. The former tends to refer to a Direct Recording Electronic system which typically displays ballot options on a screen that can be activated by the voter and then records that voting data in memory components to be processed later. However, as with many electronics, there is the inherent problem of the ability to modify software and potentially insert malicious code [3]. This has been an issue raised over several recent elections and a study from 2015 concluded that 43 American states would be using Electronic Voting Machines

that are at least 10 years old during the last presidential election [5]. Voting over the Internet, while having to deal with issues such as privacy, fraud, voting under duress, and corruption, does nothing to improve a voter's trust. The voter must still assume that once they have cast their vote it will be recorded and counted honestly.

In order for our proposed E-Voting system to be a tangible challenger to more traditional voting methods, it must be able to provide the current systems' services, at least at the same level but preferably with improvements, while also providing substantial benefits. There are several standard requirements that a voting system should adhere to, each holding equal weight: security, functionality, privacy, usability, and accessibility [6]. A "secure" voting system means one that cannot be tampered with or manipulated in any way, ensuring that votes are accurately recorded as cast. It also ensures that additional votes cannot be cast after the polls have closed or tampered with at any stage of the process. System functionality can be broad but should include; The correct registering and recording of all votes cast, permitting a voter to vote for any candidate they have the right to vote for, allowing only eligible registered voters to vote and only allowing each voter to vote once. Voters have the right to a secret ballot and to cast their vote in private [6]. This is essential to protect voters from being coerced or bribed into voting a certain way, this means that our system should not provide a receipt or any way for another person to determine the contents of a voter's ballot. On top of this the system should be easy for voters to use, meaning it's as intuitive as possible, and maintain universal vote access. It should avoid introducing bias by selecting platforms that are less available to some groups than to others as the choice of the language, ballot format, or devices may seem innocuous, but it may actually prevent small factions of the voters to cast their vote [7].

Whilst maintaining these essential foundations already provided in traditional voting systems, there are several improvements and additions which I intend to explore. The first benefit in using a blockchain to log votes is in its decentralised nature. This means there is less need for trust to be placed in a centralised organization where votes are hidden behind closed doors. It also has the benefit of being significantly harder to tamper with as, once a transaction has been verified, an attacker would need to possess at least 51% of the computing power of the network to attempt to forge transactions. Any attempts to otherwise use a forged block will be noticed by the rest of the network and ignored. This decentralized system also brings in more transparency as anyone can view, transactions in the blockchain leading to higher levels of trust in the elections outcome. This is further strengthened by the independent verifiability which could be performed by anyone, therefore removing the need to trust the election organizers' declaration of the outcome. Once a transaction (vote) has been confirmed in the blockchain (and has further blocks built upon it) this vote for a candidate becomes immutable, meaning that the entire outcome of an election will be stored indefinitely, and is able to be accessed at any time in the future.

Verifiability properties of electronic voting are divided in two categories. “Individual verifiability”, which involves auditing the processes of vote creation and vote storage by the voter; and “Universal verifiability”, which ensures that only votes from eligible voters are stored in the ballot box and that all stored votes are properly tallied, which can be performed by anyone [8]. Systems providing both types of verifiability are known as “end-to-end verifiable systems”.

One of the individually verifiable properties is cast-as-intended verification, which is focused on the audit of the vote creation process. Another property is recorded-as-cast verification, aimed at auditing the correct reception and storage of the vote in a remote voting server [8].

In this paper I outline the design of an “end-to-end verifiable system” built on the Ethereum Blockchain. In this system, a voter can register an Ethereum address which is then added to a list of *allowed addresses* inside a smart contract. Upon the ballot commencing, the voter will be able to modify the allocation of their vote inside this contract up to the point of the ballot ending. Due to the programmable nature of Ethereum contracts we can be sure that; no votes can be modified after the ballots end date, only the voter in control of the Ethereum address can change the vote associated with that address and only Ethereum addresses pre-registered to the contract are able to vote. Anyone can verify the number of votes for a candidate by querying the contract, and as they can be assured that only those addresses added to the contract are able to vote, we can be sure of the validity of each of these votes.