# The Myth of "Secure" Blockchain Voting

**David Jefferson, Verified Voting***

Several startup companies have recently begun to promote Internet voting systems, but with a new twist – using a *blockchain* as the container for voted ballots transmitted over the Internet from the voter's private device. Blockchains are a relatively new system category a little akin to a distributed database. Proponents of blockchain voting promote it as a revolutionary innovation providing strong security guarantees that enable truly secure online elections. *Unfortunately, these claims are false. Blockchains do not offer any real election security at all.*

Internet voting has been studied by computer security researchers for over twenty years. Cyber security experts universally agree that no technology, including blockchains, can adequately secure an online public election. Elections have unique security and privacy requirements fundamentally different from and much more stringent than those in other applications, such as e-commerce. They are uniquely vulnerable because anyone on Earth can attack them, and a successful cyberattack might go completely undetected, resulting in the wrong people elected with no evidence that anything was amiss.

There are many foundational computer security problems that must be solved before we can safely conduct elections online, and we are not close to solving any of them. The use of blockchains does not even address these problems. Here are just a few:

- *No reliable voter identification:* There is no foolproof way of determining exactly who is trying to vote remotely through the Internet. All known and proposed methods have grave weaknesses, and blockchains do not address the issue at all.
- *Malware:* The voter's device may be infected by a virus or counterfeit app that could change votes even before they are even transmitted, or it may silently discard the ballot, or send the voter's name and vote choices to a third party, thereby enabling coercion, retaliation, vote buying and selling, or pre-counting of votes, all undetectably. Blockchains cannot address malware.
- *Denial of service attacks:* A server can be overwhelmed with fake traffic from a botnet so that real ballots cannot get through. Blockchains as proposed for elections use multiple redundant servers, but they offer no additional protection against denial of service attacks beyond what is achievable with a conventional system having the same aggregate communication capacity.
- *Penetration attacks:* No servers, including blockchain servers, are immune to remote penetration and surreptitious takeover by determined sophisticated attackers. Even though blockchains use multiple servers, if attackers can disable or gain control of a little more than 1/3 of them they can totally disrupt or control the outcome of the election.
- *Nonauditability:* Online voting systems, including blockchain systems, do not allow for the kind of true, voter-verified paper ballot backup that is necessary for a meaningful recount, audit, or statistical spot check. Thus, the most powerful and common-sense tools we have for protection against cyberattack are unavailable.

Election security is a matter of national security. Blockchains, despite all the hype surrounding them, offer no defense against any of these well-known threats to which all online elections are vulnerable. National rivals like Russia have demonstrated a capacity and willingness to interfere with our electoral processes and would have no difficulty disrupting or undermining a blockchain election. In this era of ubiquitous cyber threats, it is reckless and irresponsible to introduce any kind of online voting in the U.S.

---

* https://www.verifiedvoting.org/board-of-directors/