Blockchains and Elections

Joe Kiniry, Jeremy Epstein, David Jefferson, Barbara Simons, Daniel Zimmerman

October 2016

Blockchains are a 40+ year old cryptographic technology that has gained enormous attention due to the recent explosion of interest in Bitcoin.[1] Unfortunately, they have become the digital equivalent of a 19th century tonic that cures the flu, helps your hair grow back, and makes you lucky in love.

Bitcoin and its brethren are cryptographic currencies, or *cryptocurrencies*: the digital equivalent of cash and a banking network rolled into one. The way that cryptocurrencies work—and in particular, the way that they perform (geographically) distributed transactions between parties—is by putting a "blockchain" onto the public Internet.

A cryptocurrency blockchain is like a public, digital, tamper-evident ledger of transactions. The Bitcoin blockchain, and others like it, can be read by anyone and must contain entries having only a certain structure. Old entries cannot be removed or changed without raising red flags, and new entries can be added only under very specific circumstances. Moreover, there must be consensus among the majority of the parties working with the blockchain about the legitimacy of each new entry before it is added, so it is extremely difficult to scale blockchains to hundreds of millions of parties (aka voters) or tens of thousands of entries (aka votes) per second.

Blockchains are now being pitched as *the solution* for problems in many domains, including cybersecurity[2] and Internet voting.[3] Unfortunately, these promises cannot be fulfilled for Internet voting systems. The de facto standard requirements for a security of an Internet voting system can be found in the U.S. Vote Foundation's "The Future of Voting" report.[4]

Blockchains are a useful tool for some security issues. However, they do not help with most of the fundamental security and privacy requirements for Internet voting for public elections. Here is a list of specific threats common to all forms of Internet voting for which there are no good solutions today and none on the horizon, and that blockchains do not address. Blockchains do not:

---

[1] The first U.S. patent mentioning blockchains, #4078152, is from 1978.
[2] Guardtime's KSI — https://guardtime.com/
[3] Smartmatic's TIVI — https://tivi.io/tivi/
[4] The Future of Voting: End-to-End Verifiable Internet Voting — https://www.usvotefoundation.org/e2e-viv/summary

- ensure that only legitimate voters are authenticated and can vote;
- prevent distributed denial of service (DDoS) attacks on the elections infrastructure;
- prevent or mitigate the hacking of election officials' servers, or those of their vendors or contractors;
- prevent or mitigate malware on a voter's computer that can
    - change votes undetectably,
    - violate voter privacy undetectably,
    - block voting undetectably,
    - or enable large scale vote buying and selling undetectably;
- permit voters to verify that their votes were recorded correctly, or prove they were not, without having to reveal to anyone exactly how they voted;
- prevent or mitigate hacking of voter registration databases;
- keep every device used for voting up-to-date with the latest operating systems and security patches;
- ensure that voters' devices are using the correct voting software;
- facilitate observation to ensure that the election was free and fair;
- prevent voter coercion from abusive spouses or employers;
- prevent voters from accidentally providing their authentication information to fraudulent sites (e.g., phishing);
- prevent insider attacks on the voting system.

Experts in cryptography and election security do not see this long list of extremely challenging problems being solved in the next decade, and certainly not by blockchains. Until all of these problems are resolved, it is dangerous to national security to use any online voting system in public elections.

Vendors and other proponents of Internet voting are now trying to suggest that blockchains are *the breakthrough technology* that will finally enable secure Internet voting. Unfortunately, this is simply not true. The security issues with Internet voting are fundamental, and no single breakthrough will resolve them in the foreseeable future. It will take a complete overhaul of the architecture of our devices, their software stacks, and the Internet protocol suite, before an Internet voting system can be built to withstand the full range of attacks that might be directed against it.

Blockchains are useful, and can certainly be part of a secure voting solution. But they are only a small piece—they do an adequate job of solving an easy part of the security challenges in Internet voting, but nothing at all to solve the hard parts.