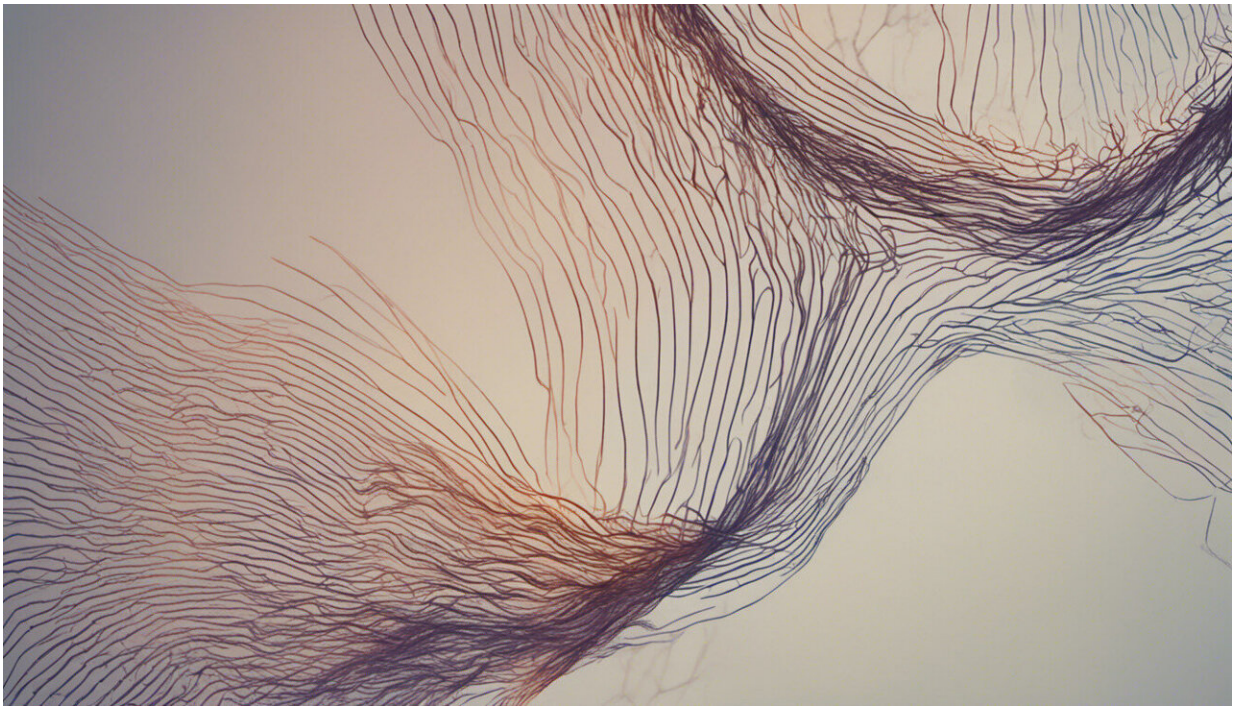
Blockchain voting: Vulnerable to hackers, software glitches, bad ID photos, and more

October 18 2019, by Nir Kshetri



Credit: AI-generated image (disclaimer)

A developing technology called "blockchain" has gotten attention from election officials, startups and even Democratic presidential candidate Andrew Yang as a potential way to boost voter turnout and public trust in election results.

I study blockchain technology and its potential use in fighting fraud, strengthening cybersecurity and securing voting.

I see promising signs that blockchain-based voting could make it more convenient for people to vote, thereby boosting voter turnout. And blockchain systems can be effective at strengthening the security of devices, networks and critical systems like electricity grids, as well as protecting personal privacy.

The few small-scale tests run so far have identified problems and vulnerabilities in the digital systems and government administrative procedures that must be resolved before blockchain-based voting can be considered safe and trustworthy. Therefore I don't see clear evidence that it can prevent, or even detect, election fraud.

How it works

There are a few steps in a blockchain-based voting system, which uses technology to mirror the process of in-person voting.

First, the system needs to verify a voter's identity—often by having the user upload a photo of a government-issued ID and then a photo or video self-portrait. The system confirms the ID's validity, and facial recognition software makes sure the person in the self-portrait is the person on the ID. Then the user is authenticated as eligible to cast a vote.

Only at that point does blockchain technology actually enter the process. The system gives each authenticated voter a digital token that represents the person's vote and a list of the digital addresses to which he or she can send that token. Each address indicates a vote for a particular candidate or an answer to a ballot question.

The tokens don't indicate who cast them, so votes remain anonymous.

When a voter sends a token, a record of that act is stored simultaneously on several different computers, making it much harder for hackers to alter the vote records. After casting the ballot by sending the token, the user receives a unique code that they can use to look at the anonymized online vote tally to confirm their vote was counted as they intended.

Small-scale trials, so far

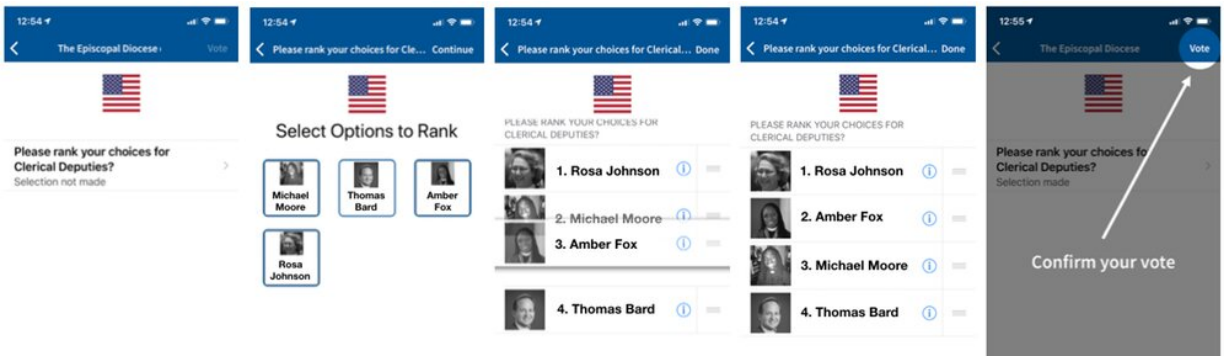
Early results show that blockchain systems may increase voter turnout, though it's not yet clear why. Many of the tests have been for informal ballots, like student government groups and community projects.

However, several election officials in the U.S. have held small-scale trials of blockchain voting, allowing members of the military who are stationed overseas to vote electronically, rather than by mail.

In the November 2018 congressional elections, West Virginia allowed 144 voters living overseas to cast ballots from 31 different countries using an app developed by a private company called Voatz, which is involved in many of these trials.

Another 200 voters overseas expressed interest in using the system, but their home counties in West Virginia weren't set up to do so. Based on the results, West Virginia says it plans to continue and expand the trial in the 2020 presidential election.

Denver, Colorado, had 119 voters who were overseas use a Voatz system to cast their ballots in municipal primary elections in May. In the city's June runoff election, 112 voters did so online through a blockchain system. In August, 24 voters cast their ballots from overseas using a Voatz app in a Utah County, Utah, election.



An example of a Voatz voting interface. Credit: Voatz

A big test in Moscow

The most recent—and largest—use of a blockchain-based voting system was in the city council election in Moscow, Russia, on Sept. 8. Because of concerns that the system was not set up securely, only three of the city's 20 electoral precincts allowed voters to use a blockchain-based mobile voting app to cast their ballot from anywhere with an internet connection.

Again, the evidence showed a boost in voter turnout: The city's overall turnout rate was around 17% of registered voters. That includes a 90% turnout among the voters who had registered to use the system.

However, technological complications barred some people from voting, which led at least one losing candidate to object that he would have won if everything had worked properly. That's the sort of problem that is most worrying for people who hope using mathematical principles and computerized encryption will help the public have trust in election outcomes.

Key challenges unsolved

There are several obstacles in the way of blockchain ever becoming useful for large-scale, legally binding voting.

One is that most people have little understanding of how blockchain systems work. Another, equally vital, is that even experts don't have a way to identify every possible irregularity in online voting. Voting on paper, by contrast, is well studied and easily verified and audited.

One crucial aspect of a blockchain voting system is the method by which the computer system verifies voters' identities. When a verified voter establishes an account on the system, that process creates a digital key that identifies them securely when casting a ballot. A more complex key is harder to hack, but also takes more computing resources to verify. It will be important to find a way to protect the integrity of the voting process, without exhausting government budgets buying advanced computing power. The computational power required may make blockchain systems inefficient for voting on a nationwide scale—or even statewide, in populous states like California and Texas.

The Moscow election system, for instance, initially assigned keys that were too easily hacked. That opened the possibility of voter impersonation, which is bad enough. But that weakness also violated the principle of a secret ballot by letting outsiders know how each person voted.

Outside the blockchain itself

Other problems with digital voting systems are separate from the underlying technologies. In some cases, government-issued IDs used to verify voters' identities are many years old.

Even when dealing with current images, facial recognition systems, including the one used by Voatz, have high error rates, especially for non-white voters. In addition, hackers may try to trick the system.

The phone or computer a voter uses to cast a ballot may not be secure, either – and it's not safe to assume that the computer networks they communicate over, and the servers the data is stored on, are safe from manipulation or even random errors.

Trust, but verify

Proprietary voting apps like Voatz offer the public no way to know whether voters' choices are accurately recorded, nor whether these apps truthfully deliver their ballots' encrypted copy to be counted by election officials.

Voatz has claimed that its system has been audited by third parties, but has made few details of that process or its findings available to the public. West Virginia officials who hired Voatz have also refused to reveal information about how its security was evaluated.

The company has said it would not release that information because it had a nondisclosure agreement with the auditors, and for fear its proprietary system design might be discovered by competitors.

It's possible that blockchain-based voting could boost voter participation rates, but there's no evidence yet that it is better at preventing election fraud. With plenty of potential trouble spots outside the system itself, and little public transparency within it, I have to conclude that blockchain voting is not yet safe or ready for service.

Provided by The Conversation