In the middle of a pandemic, it’s not surprising that there have been increasing calls to explore the possibility of conducting elections online. A growing number of tech start-ups have even advocated for using blockchain technology, which they say would [boost voter turn-out and improve public trust](https://www.fastcompany.com/90419485/i-study-blockchain-it-shouldnt-be-used-to-secure-our-elections).

**But in**[**a new paper**](http://people.csail.mit.edu/rivest/pubs/PSNR20.pdf)**looking at a range of examples, a team of MIT cybersecurity experts have come out strongly against using any form of blockchain-based voting, and said that online voting in general is much more vulnerable to being hacked than in-person or mail-in voting. They say that the physical nature of mail-in ballots make them much less susceptible to large-scale attacks compared to online voting, where exploiting a single vulnerability could impact every ballot at once.**

The team says that blockchain-based approaches are ripe for what they call “serious failures” - situations where election results have been changed in ways that are undetectable, or, even if detected, would be irreparable without running a whole new election.

“While current election systems are far from perfect, blockchain would greatly increase the risk of undetectable, nation-scale election failures,” says MIT professor Ron Rivest, co-creator of RSA public-key encryption and senior author of the new paper. “Any turnout increase would come at the cost of losing meaningful assurance that votes have been counted as they were cast.”

**Though blockchain-based apps like Voatz have been deployed in state and county elections, researchers like paper co-author Mike Specter have previously shown that such systems suffer from**[**serious security vulnerabilities**](https://news.mit.edu/2020/voting-voatz-app-hack-issues-0213)**enabling attackers to monitor votes being cast and even change or block ballots.**

Lead author Sunoo Park says that an essential quality lacking in blockchain systems is “software independence” - that is, the assurance that an undetected change or error in a system’s software cannot cause an undetectable change in the election outcome. Blockchain-based approaches require voters to use software for which a single bug could undetectably change what they see (e.g., showing them that their vote was cast for a certain candidate when it actually wasn’t).

The researchers argue that, at this point in time, only paper ballots allow voters to directly verify that their ballot accurately represents their intended vote.

“If vote-casting is entirely software-based, a malicious system could fool the voter about how the vote was actually recorded,” says Rivest, whose team’s paper was published online this week. “Democracy — and the consent of the governed — cannot be made contingent on whether some software correctly recorded voters’ choices.”

Many proponents of online voting cite the fact that industries like retail and banking have had relative success with online security for decades. But the team expresses two major objections to those parallels.

For one, they say that those systems have higher tolerances for failure that can be more readily accommodated in the case of scenarios like credit card fraud.

“For elections there is no insurance or recourse against a failure of democracy,” Rivest says. “There is no means to ‘make voters whole again’ after a compromised election.”

Secondly, with voting there are important differences in anonymity. With banking you can look at receipts to detect and fix fraudulent purchases. With voting, it's vital that we \*not\* be able to prove the way we voted, so that votes cannot be sold or coerced in any way.

Park, Rivest and Specter co-wrote the paper with Neha Narula, director of MIT’s [Digital Currency Initiative](https://dci.mit.edu/) (DCI). This project was supported in part by the DCI, the National Science Foundation, the MIT Internet Policy Research Initiative and a Google fellowship.

**“Electronic voting is more vulnerable [than paper-based alternatives] to 'serious failures': situations where election results have been changed and the change may be undetectable, or even if detected, be irreparable without running a whole new election.”**

In the current scenario, most of the countries of the world hold their elections using Electronic Voting Machines, where your vote gets registered electronically with the help of an Electronic Machine without using and wasting ballot paper to vote for elections. As security is a major concern nowadays, ensuring that no person exercises the right to vote twice is the main aspect. We can resolve this issue by introducing Finger Print Based Voting, where a person can be authorized based on his Finger Print. This will put an end to fake voting. The domain of the project is the Internet of Things where we are building Fingerprint Based Biometric Voting Machine using Arduino. We know that IoT is the system of interrelated computing devices, mechanical and digital machines, objects, and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Thus our Fingerprint online module is an application where the user is recognized by his finger pattern. As we know that the minutiae features on a finger of each human being are different, the voter can be easily authenticated. The online system allows the voter to vote through his fingerprint. The fingerprint of the voter is used to uniquely and distinctively identify him/her using the fingerprint module. Also, the system promises the right to vote a candidate only once, thus not allowing the voter to vote for the second time. An admin is assigned to add all the candidates standing for the election. Only the admin has the right to add a candidate name and photo who are nominated. The Admin will also register the voter's name by verifying voter's details. Admin will authenticate the voter by verifying the voter's identity and then admin will register the voter. Once the user has got the voters id and password from the admin the user can log in and vote for the candidates who were nominated. The system will allow the user to vote for only one candidate. In the end, the election result is published by using the election id. Even users can view the election result.