Blockchains won't fix internet voting security – and could make it worse

October 18 2018, by Ari Juels, Ittay Eyal And Oded Naor

Credit: Jorge Jesus from Pexels

Looking to modernize voting practices, speed waiting times at the polls,

increase voter turnout and generally make voting more convenient, many government officials – and some companies hawking voting systems – are looking to an emerging technology called a "blockchain." That's what's behind a West Virginia program in which some voters serving abroad in the military will be able to cast their votes from their mobile devices. Similar voting schemes have been tried elsewhere in various places around the world.

As researchers in the Initiative for CryptoCurrencies and Contracts, we believe in the transformative potential of blockchain systems in a number of industries. Best known as the technology behind bitcoin and other cryptocurrencies, blockchains can do much more than allow anonymous strangers to send each other money without fear of fraud or tampering. They have created new ways for people to invest in technology ventures that have attracted billions of dollars, and may someday store records that make educational credentials, land ownership and food origins more transparent and harder to forge.

Blockchains might sound like an ideal remedy for the trust problems caused by internet voting. Data can only be added to a blockchain – not deleted or changed – because multiple copies are stored on computers owned by different people or organizations and perhaps spread across different countries. Strict controls can be placed on a blockchain's contents, preventing unauthorized data from being added. And blockchains are designed to be transparent – with their contents often readable by anyone's computing device anywhere in the world.

Yet as scholars who have studied traditional and blockchain-based voting, we believe that while blockchains may help with some specific issues, they can't fix the basic problems with internet voting. In fact, they could make things worse.

Computers can break, or be broken

For years, experts on election security have warned that the internet is too dangerous for such socially crucial and time-sensitive functions as voting. Renowned cryptographer Ronald Rivest, for instance, has remarked that "Best practices for internet voting are like best practices for drunk driving" – there's no safe way to do either one.

The stakes are enormous. Democracy requires widespread public trust – not just that a declared winner actually received the largest number of votes, but in the integrity of the system as a whole. People need to trust that the votes they cast are the ones that are counted, that their neighbors' votes are totaled accurately and not the result of bribery or coercion and that local tallies are communicated safely to state election officials.

Even advanced computing devices today cannot provide such assurances. Most hardware and software are rife with hidden security flaws, and are not regularly updated. Devices are vulnerable, and so are networks. Internet outages – even caused by trivialities like gamers trying to get a leg up on their competitors – could prevent people from voting. Intentional, targeted attacks against internet traffic could cause major disruptions to democratic institutions on a national scale.

The stability and integrity of democratic society itself are too important to be relegated to flawed computer systems.

Adversaries are looking for opportunities

Hackers – backed by foreign governments or not – are always looking for new targets and fresh ways to sow social discord. They'll find – and fully exploit – any technical weaknesses available to them. Without a paper trail, the very possibility that someone could have secretly changed votes will further erode public trust in democratic elections.

Blockchains depend on computing devices

A key method by which blockchain voting could worsen election integrity is by claiming to increase trustworthiness without actually doing so.

It's easy to imagine a voting system in which only authorized voters could cast ballots, with those ballots indelibly recorded on a blockchain. The blockchain would act as a single authoritative election record that could not be erased or tampered with. For all intents and purposes, the record would be hack-proof.

However, tallying votes on a blockchain doesn't magically make a voter's phone or computer secure. A vote may be securely recorded, but that means nothing if the vote was cast incorrectly to begin with. If your phone is infected with malware that switches your vote from Candidate R to Candidate D, it doesn't matter how secure the rest of the voting system is – the election has still been hacked. In some cases, blockchains may be able to help voters detect that sort of tampering – but only if the hack-detection software itself hasn't been hacked.

In addition, some companies' business practices undermine the potential to trust their blockchain systems. The manufacturer of the system West Virginia will use in November – like many companies manufacturing physical voting machines – is refusing to embrace the transparency that is central to the security industry, the blockchain community, and democracy itself. They are not providing public access to the cryptographic protocols at the heart of their systems, leaving the public instead to rely on the manufacturer's promises of security. There's no way for an independent auditor to be truly certain that the systems are free of subtle bugs or security flaws – or even massive holes that would be obvious to experts.

Vote buying becomes newly possible

Another way blockchain voting could worsen existing voting problems is by increasing the likelihood of vote buying. Sometimes a glass of beer is all that's needed to bribe a voter. Vote buying is happily rare in large-scale U.S. elections, in part because the secret ballot makes verifying a bought vote very difficult and because there are serious criminal penalties.

Internet voting could completely negate both of these protections. Putting votes on blockchains eliminates the secrecy of the voting booth. Encryption doesn't help: Software can prove mathematically to a vote buyer that a voter's device encrypted the name of a particular candidate. In addition, foreigners who might try to influence people's votes are very hard to prosecute.

Some voting companies contend that their systems publicly identify voters only by random numerical identifiers, so they aren't subject to vote-buying or intimidation. But in many of these systems, voting identities can be linked to accounts in cryptocurrency systems – where a voter could receive a bribe, potentially without revealing who was paid, how much or by whom.

Officials and companies who promote online voting are creating a false sense of security – and putting the integrity of the election process at risk. In seeking to use blockchains as a protective element, they may in fact be introducing new threats into the crucial mechanics of democracy.

Provided by The Conversation