FEATURE

Why blockchain-based voting could threaten democracy

As the desire to increase voter turnout remains strong and the number of online voting pilot projects rises in the U.S. and abroad, some security experts warn any internet-based election system is wide open to attack, regardless of the underlying infrastructure.

By Lucas Mearian
Senior Reporter, Computerworld | AUG 12, 2019 3:00 AM PST

Public tests of blockchain-based mobile voting are growing.

Even as there's been an uptick in pilot projects, security experts warn that blockchain-based mobile voting technology is innately insecure and potentially a danger to democracy through "wholesale fraud" or "manipulation tactics."

The topic of election security has been in the spotlight recently after Congress held classified briefings on U.S. cyber infrastructure to identify and defend against threats to the election system, especially after Russian interference was uncovered in the 2016 Presidential election.

Thirty-two states permit various kinds of online voting — such as via email — for some subset of voters. In the 2016 general election, more 100,000 ballots were cast online, according to data collected by the U.S. Election Assistance Commission. The actual number is likely much higher, according to some experts.

One method of enabling online voting has been to use applications based on blockchain, the peer-to-peer technology that employs encryption and a write-once, append-many electronic ledger to allow private and secure registration information and ballots to be transmitted over the internet. Over the past two years, West Virginia, Denver and Utah County, Utah, have all used blockchain-based mobile apps to allow military members and their families living overseas to cast absentee ballots using an iPhone.

Mike Queen, deputy chief of staff for West Virginia Secretary of State Mac Warner, said that while the state currently has no plans to expand the use of the mobile voting beyond military absentee voters, his office did "a ton of due diligence" on the technology before and after using it.

"Not only does blockchain make it secure, but [the blockchain-based mobile app] has a really unique biometric safeguard system in place as well as facial recognition and thumb prints," Queen said via email after 2018 General Election.

[IT has a new 'It Crowd': Join the CIO Tech Talk Community]

Voatz iPhone mobile voting application.

Security experts disagree. The issues around online voting include server penetration attacks, client-device malware, denial-of-service attacks and other disruptions, all associated with infecting voters' computers with malware or infecting the computers in the elections office that handle and count ballots.

"If I were running for office and they decided to use blockchain for that election, I'd be scared," said Jeremy Epstein, vice chairman of the Association for Computing Machinery's U.S. Technology Policy Committee.

Epstein co-authored an election security report with Common Cause, the National Election Defense Council, and the R Street Institute, "Email and Internet Voting: The Overlooked Threat to Election Security," in it, he criticized blockchain and internet voting as a ready target for online attacks by foreign intelligence and said transmission of ballots over the internet, including by email, fax and blockchain systems, are seriously vulnerable.

"Military voters undoubtedly face greater obstacles in casting their ballots. They deserve any help the government can give them to participate in democracy equally with all other citizens," Epstein wrote. "However, in this threat-filled environment, online voting endangers the very democracy the U.S. military is charged with protecting."

There are many reasons blockchain is not good for voting, Epstein said. For one, it assumes there's no malware in the voter's computer. It also assumes you want all the votes to be perennially public, because if someone finds a way to hack into the blockchain, everyone's vote becomes public. And, while blockchain networks may be able to handle small absentee voter populations, the technology could not stand up to use by the general voter populace and its volumes.

Until there is a major technological breakthrough in or fundamental change to the nature of the internet, the best method for securing elections is a tried-and-true one: mailed paper ballots, according to Epstein.

While paper ballots are not tamper-proof, they are not vulnerable to the same wholesale fraud or manipulation associated with internet voting, Epstein said.

"Tampering with mailed paper ballots is a one-at-a-time attack. Infecting voters' computers with malware or infecting the computers in the elections office that handle and count ballots are both effective methods for large-scale corruption," Epstein said.

West Virginia, the first state to use a blockchain-based mobile voting system, was also criticized by Epstein who said the state was willing to go out on a limb "pretty much more than anyone else" and "never shared publicly how they decided these systems were secure.

"They're taking word of the vendor," Epstein said.

What we don't know about internet voting

In a research paper written by computer scientists from Lawrence Livermore National Laboratory and the University of South Carolina, along with election-oversight groups, internet voting startup Voatz was called out for not releasing any "detailed technical description" of its technology.

Voatz's blockchain-based voting service was the one used West Virginia, Denver and Utah County to enable military absentee voting.

"Most of the details of the architecture and procedure are apparently confidential, though it is not clear why," the research paper said. "The system has not gone through federal certification, or any public certification to our knowledge. The company has not disclosed its source code nor allowed its system to be examined open by third parties."

Voatz has contracted with Palo Alto-based authentication company Jumio to perform remote voter authentication. The authentication procedure requires a voter using the Voatz iPhone app to send to Jumio a photo of their driver's license or passport photo page along with a short, live selfie video of their face. Jumio uses machine learning facial comparison software to determine whether the face on the ID matches the one in the video. If it does, the voter is authenticated.

The researchers questioned the efficacy of using a tiny driver's license or passport photo for authentication purposes and noted those photos can be up to 10 years old. Among other problems, they also noted facial comparison systems have been discovered to have high error rates, especially for minorities.

One of the groups that contributed to the report was the non-profit Verified Voting Foundation, whose says its purpose is to preserve the democratic process with modern voting technology. Marian Schneider, president of the Verified Voting Foundation, said online voting can't be made safe and blockchain is an unnecessary complexity.

"Current commercial systems with blockchain components are using the blockchain as an encrypted ballot box. Votes go there after they are susceptible to all of the attacks [already mentioned]," Schneider said. "If something happens, it might not be detected, and incorrect data would be in the blockchain.

"I don't think online voting can resolve any issues because the issues it purports to resolve create other issues that are worse," she continued. "The ability to track back to a voter's vote makes current systems not secret so they do not preserve the right to a secret ballot."

The need is real

Blockchain andinternet-based voting platforms, however, have been viewed as one way to boost voter participation by making the process easier through mobile apps that allow both registration and ballot casting to occur from anywhere in the world. Voters in those systems pre-register and then can use their smartphone's biometric finger print readers or facial recognition technology to sign in to cast their votes.

The number of pilots, while growing, remains relatively small - a few dozen, mainly for shareholder proxy voting and university student government elections. But state and municipal governments have been testing blockchain-based mobile voting over the past year.

In the 2018 election, 144 registered West Virginia voters from 21 counties cast ballots from 31 different countries using an app from Voatz.

New research from the University of Chicago found that allowing military members overseas to vote using a mobile device increased turnout by 3% to 5% among those eligible to use the system in the 2018 federal election in West Virginia.

Anthony Fowler, lead study author and associate professor at the University of Chicago, said that being able to cast ballots online using only smartphones or other mobile devices can dramatically reduce the costs of voting, particularly for under-represented groups, and has significant effects on the size and composition of the voting population.

"We are likely to see more trials soon, so this is a good time to study the consequences of this reform," Fowler wrote. "New survey data shows that many Americans are understandably wary of online voting."

A third-party audit conducted by the National Cybersecurity Center (NCC) and Denver Election Division showed that votes cast over the blockchain application were recorded and tabulated accurately. The final numbers showed that voter turnout doubled from the 2015 election and a post-election survey from the Denver Elections Division found that 100% of respondents said they favored secure mobile voting over all methods available to them.

"We are very excited about the promise of this technology," Jocelyn Bucaro, Denver's Deputy Director of Elections, said in a statement. "Our goal was to offer a more convenient and secure method for military and overseas citizen voters to cast their ballots, and this pilot proved to be successful. More voters participated in this cycle, in part thanks to this convenient method, and those voters who voted using the application prefer to vote by this method in all elections in the future."

Jonathan Johnson, an Overstock.com board member and the president of Medici Ventures, Overstock's subsidiary responsible for advancing blockchain technology, believes remote voting via electronic devices will be more widely adopted.

"After a successful pilot program in West Virginia of the Voatz digital remote voting application ... more states will look to re-enfranchise their overseas voters," Johnson said in an earlier interview. "Other states may use it to make accommodations for disabled voters. But, as people get comfortable with it, there will be an outcry for it from the voting citizenry. If I can vote overseas using it, then why can't I use it when I'm here [in country]?"

Medici Ventures-backed Voatz is among a small community of mobile voting platforms worldwide using blockchain as the basis for a distributed voting system. Other companies include Barcelona-based Scytl, Australia-based Securitas, London-based Smartmatic Corp., and Cleveland-based Votem Corp. Though Votem reportedly shuttered its operations after layoffs, Votem CEO Peter Martin said via email the company continues to support its customers 'and in fact have signed up some new customers."

Even so, several European countries abandoned internet voting after seeing that the increases in turnout were not as large as expected, the University of Chicago study pointed out; those lower-than-expected increases, however, could have been affected by already waning voter turnout in those European nations.

Estonia a model for online voting

Estonia, however, has embraced internet-based voting and created the world's first national online voting system. In 2005, the Baltic nation of 1.3 million people introduced online voting via Smartmatic Corp.'s technology and used it for local government elections; four years later, Estonia used internet voting for parliamentary elections in which more than 30,000 people voted online.

The Estonian internet voting system has now been used in eight major elections over 12 years. Today, online voting participation in the Balkan state has reached 44.4% of the population.

The Parliamentary elections held earlier this year saw an increase of 40% in online participation over the same elections in 2015. Online voting, or i-voting as it's called in Estonia, takes place in advance of election day and runs until the fourth day before the election. Citizens download a voting application via a national election site, then register through a national ID card or mobile PIN assigned through a registration process.

Estonian citizens and permanent residents can request two forms of digital identification: digi-ID and mobil-ID. Digi-ID is a card similar to the national ID card that is designed only for online use. The digi-ID card does not have a printed photo of the citizen, and contains less personal data then the national ID card, while still providing authentication and digital signature functions. Mobil-ID provides similar functionality to digi-ID, but is built into a mobile phone SIM card rather than a chip-and-PIN card. This enables the citizen to perform digital signatures and sign using their mobile phone with no extra hardware.

Smartmatic's online voting system was also used in the 2016 Utah Republican Party Caucus and voters from more 45 countries, including places as far away as French Polynesia, South Africa and Japan, cast ballots online. Eighty-nine percent of 24,486 registered Utah Republican Party members registered to vote online and participate in the caucus process, according to Smartmatic.

Related: Security | Government IT | Cloud Computing | Blockchain | Emerging Technology | Mobile | iPhone

1 2 NEXT >

7 inconvenient truths about the hybrid work trend