As we passed the 100-day mark in the new Trump administration, many questions are still being asked about how to best address voting in the future. Back in January of this year, I described how the 2016 U.S. presidential election shined a light on outdated election technology.

Over three months later, time is running out in order to put new voting technology and processes in place for upcoming elections in 2018 and beyond.

So what election solutions hold the most promise? Many experts believe that blockchain technology offers new hope for electronic voting and even mobile (or online) voting. What actions are being taken now?

This TEDx video describes the history of blockchain, as well as a high-level overview with examples beyond just financial services.

In order to do a deeper dive into this topic, I turned to Pete Martin, the CEO of Votem, to answer my questions on blockchain, online voting, global election activities and related topics. On LinkedIn, Pete describes himself as a “Serial entrepreneur, mobile voting revolutionary, classic rock drummer.”

Pete thinks that our voting system is ripe for disruption. He says that Votem’s mission is to have 1 billion people globally vote using their mobile phone by 2025.
Interview with Votem CEO Pete Martin

Dan Lohrmannn (DL): What is blockchain technology and why is it more secure?

Pete Martin (PM): Blockchain is a permanent cryptographic record, or ledger, of digital events that’s “distributed,” or shared among many different parties. It can only be updated by consensus of the participants in the system. Once entered onto the ledger, information can never be erased and it contains a cryptographically verifiable record of every single transaction (vote) ever made. Because “independent authorities” who may not trust each other need to attest to the accuracy of every transaction and “agree” on whether to make it a permanent record or not, it provides a level of transparency and permanence not possible with current technology. This technology is immune to even “insider threats,” which is one of the largest vulnerabilities to current systems.

DL: How can voting benefit from blockchain technology?

PM: Blockchain technology provides all of the characteristics you would want in a platform that is arguably the most important part of a democratic society; it’s fault-tolerant, you cannot change the past, you cannot hack the present, you cannot alter the access to the system, every node with access can see the exact same results, and every vote can be irrefutably traced to its source without sacrificing a voter’s vote anonymity. End to end verifiable voting systems will give the voter the ability to verify if their vote is correctly recorded and correctly counted, for instance, if a ballot is missing, in transit or modified, it can even be detected by the voter and caught before the election is over.

DL: What are the biggest issues with the current processes that blockchain technology is trying to solve?

PM: Transparency, accessibility, security, and auditability. Many experts believe that in-person voting using paper ballots is the only truly secure and guaranteed way to cast a ballot. Although the process is generally run without incident by dedicated elections officials, any manual human-based process is bound to be prone to errors and mistakes. Moreover, there are millions of ballots cast absentee by mail, which introduces a whole new set of issues.

The current voting process is relatively transparent to elections professionals, but how does the average citizen know their vote was cast as intended and counted as cast? Recent surveys suggest that most people actually don’t trust “the system.” We’ve become accustomed to ordering a product online, tracking the status of our order; we know exactly when it’s been shipped and when it arrives; this is the sort of transparency
that voters are entitled to, and we can accomplish that with blockchain in a highly secure manner. With blockchain, we have the ability to “audit” every single vote in real time, which is something very difficult, if not impossible, to do in today’s process.

**DL: What is the state of electronic or online voting in the U.S. and beyond?**

PM: Online voting has been used in 23 countries around the world and in limited uses in the U.S. The security that underpins most of the legacy electronic and online voting platforms was developed 10 years ago and has recently been proven to be vulnerable to tampering. We solve these intrinsic vulnerabilities. Blockchain was architected from the ground-up to be mass hack-proof with the highest levels of security, which makes it an ideal platform for voting. With the threat of nation states’ attacking democracy around the world, we are confident that it’s the right technology to stave off known potential threats.

**DL: Online voting has been happening around the world for a while; what alternate technologies have been used and how does blockchain compare to this?**

PM: The predominant technology used previously for online elections is called Mix Networks, commonly referred to as Mix-Nets. Mix-Nets, introduced in 1981, create hard-to-trace communications taking messages from multiple senders, shuffling them, and then sending them back out in random order to the next destination (possibly another server). Sophisticated adversaries can provide long-term correlation attacks and track the sender and receiver of the packets. With blockchain, every vote is cryptographically validated by each independent “node” and written permanently to the ballot box, making the system inherently immune to malicious tampering attacks, rendering the hackers’ mission virtually impossible.

**DL: It seems that your focus is on “mobile voting” specifically, explain your thoughts here?**

PM: Mobile, as a computing platform, is clearly the present and future of how humans will interact with their world. Today, we do practically everything on our phones and this is even more prevalent outside the U.S., citizens in countries like Kenya, China and Australia do practically everything on their mobile devices. Smart phone penetration across the world is expected to exceed 80% or even higher within a few years. The technological and human factor challenges are greater on a mobile device but the time is ripe for this intersection. We define “mobile voting” as remote voting, and understand that the form factors of “mobile” will vary widely on different devices around the world from phones to tablets etc.

**DL: As a former CISO for the state of Michigan, I can tell you that the world is filled with known and unknown threats to all systems connected to a network. How will you ever convince an elections official whose job is to ensure their election is executed without incident that you can eliminate any potential issues?**

PM: This is probably our toughest challenge after we solve the technological challenges. We understand that this is a “trust” business and that citizens need to trust
their election management bodies (EMB), and EMBs need to trust their technology partners. We’ll earn this trust by having the industry skeptics help us architect a forensically auditable trust-centric solution. Further to that, we are securing certification from the U.S. Elections Assistance Commission (EAC) and partnering with many organizations that make it their job to oversee and audit elections by giving them an independent auditing node to observe our platform to oversee and audit the election in real time.

**DL: It’s now known that the Russians (and possibly other hackers as well) attacked our voter registration systems; how could blockchain have prevented that?**

**PM:** We take it as a given that our system will be a target. The reason we selected blockchain is that it is a permanent record, or ledger, of digital events that’s “distributed,” or shared among many different parties. It can only be updated by consensus of the participants in the system. Having systems like a state’s voter registration records on a blockchain system would detect and therefore prevent potential alterations by hackers. By requiring consensus between all auditing “nodes” on the network, you can prevent compromised computers from making undetectable changes to these records.

**DL: What can be done to make new election technology more secure?**

**PM:** Technology experts and ethical hackers are working feverishly to create technologies that detect, resist and eliminate attacks on a system, from new end-to-end encryption standards to detection methods and zero-day attack prevention. We started our development and architecture with a laundry list of all of the potential issues with mobile and online voting, technological and human, and built a solution to effectively meet every potential threat to fair and free elections. This is an evergreen effort that we are dedicated to sustaining as vulnerabilities are identified to be mitigated.

**DL: How about the people and process part of voting online? What is hindering progress?**

**DL: How about the people and process part of voting online? What is hindering progress?**

**DL: Who is working on improving the voting process. Can online voting be a reality? How soon?**

**PM:** There are a few progressive companies in addition to ours that are paving the way to online voting. We are all working with forward-thinking secretaries of state and other elections officials to pilot the technology in "lower risk" elections. For instance in this past election, the Iowa Caucus cast their votes online and on mobile devices using a voting app created in conjunction with Microsoft. The Utah Republicans conducted their state’s caucus using online voting technology. In the proxy voting space, Nasdaq completed a successful project with Estonia using blockchains for proxy voting as did Broadridge for shareholders. We think we’re two years away from major online elections running on blockchain in the U.S., and we expect we’ll see acceleration in the private elections market before that.
**DL:** Are there some new and unique ways that your team is tackling this blockchain voting issue? Do you have any case studies to share?

PM: We are demonstrating the power of blockchain voting technology in private elections such as the Rock and Roll Hall of Fame Fan Vote where almost 2 million votes were cast without incident on the Votem platform. You can find our case studies here https://votem.com/case-studies/

**DL:** Where can people turn for more information on blockchain voting? Are there nonprofits or vendor-agnostic sources that can help?

PM: Here are some inks to great articles and resources to help: https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business
http://www.nasdaq.com/article/don-tapscott-announces-international-blockchain-research-institute-cm762234#ixzz4fN5wGQhT

**DL:** My thanks to Pete Martin for taking the time to answer my questions on blockchain, voting and the future of elections around the world.

I also encourage readers to keep an eye out for the National Association of State CIOs (NASCIO’s) upcoming white paper on blockchain, which will describe the many ways that governments are (and plan to) use blockchain technology in diverse ways.

As announced at the NASCIO Midyear Conference last week, the blockchain report will be coming out in the next month or so at this NASCIO publications website.

http://www.govtech.com/blogs/lohrmann-on-cybersecurity/can-blockchain-technology-secure-your-vote.html