How Blockchain Could Secure Elections

CB INSIGHTS

Elections are under threat from malicious actors that can infiltrate voting machines, alter voter registration databases, coordinate disinformation campaigns, and more. Blockchain technology could help.

In early 2017, US Secretary of Homeland Security Jeh Johnson designated elections as part of the nation's critical infrastructure.

This means elections are eligible to receive prioritized cybersecurity assistance and other federal protections from the Department of Homeland Security, alongside nuclear reactors, federal transportation systems, and more.

Election security is especially important as midterm elections approach.

US intelligence officials warn that Russia and other hostile governments could interfere in the US congressional midterms on November 6th.

> *It's "too late to protect the 2018 elections."*
>
> — ALEX STAMOS, FORMER CHIEF SECURITY OFFICER AT FACEBOOK

This summer, Facebook announced it was investigating malicious activity on its social platform, similar to the election meddling seen during the 2016 presidential election.

While November 6th is likely too soon to effectively secure every aspect of midterms election, there is still time to more effectively protect systems ahead of the 2020 presidential election.

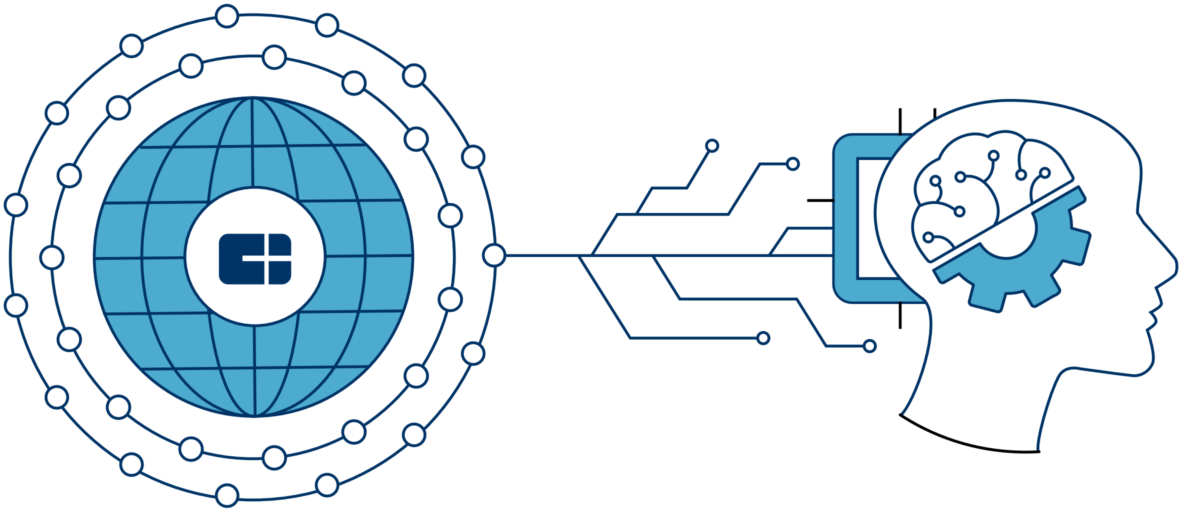
Election security involves the protection of election processes and critical voting infrastructure from cyber attacks. Elements in need of protection include: registration databases, voting machines, other systems to manage the election, and systems that report & display results.

Some election security methods rely on time-consuming manual processes. This year, France and the Netherlands counted election ballots by hand to prevent hackers from interfering with results.

But now, blockchain is being touted as a new way to make elections more secure. Some states are already adopting the technology: West Virginia will make mobile blockchain voting available to overseas voters for the November midterm election.

Below, we detail the vulnerabilities in today's elections, and the viability of blockchain technology to secure the future of voting.

Table of Contents



At CB Insights, we believe the most complex strategic business questions are best answered with facts.

We are a machine intelligence company that synthesizes, analyzes and visualizes millions of documents to give our clients fast, fact-based insights.

From Cisco to Citi to Castrol to IBM and hundreds of others, we give companies the power to make better decisions, take control of their own future, and capitalize on change.

WHERE IS ALL THIS DATA FROM?

The CB Insights platform has the underlying data included in this report

CLICK HERE TO SIGN UP FOR FREE

> "We use CB Insights to find emerging trends and interesting companies that might signal a shift in technology or require us to reallocate resources."

Beti Cung,

CORPORATE STRATEGY, MICROSOFT

Microsoft

TRUSTED BY THE WORLD'S LEADING COMPANIES

citi IBM GE BARRICK Castrol

SEQUOIA DASSAULT SYSTEMES CISCO salesforce

1

Election security vulnerabilities

Identifying vulnerabilities in election hardware and processes is vital to preventing future attacks.

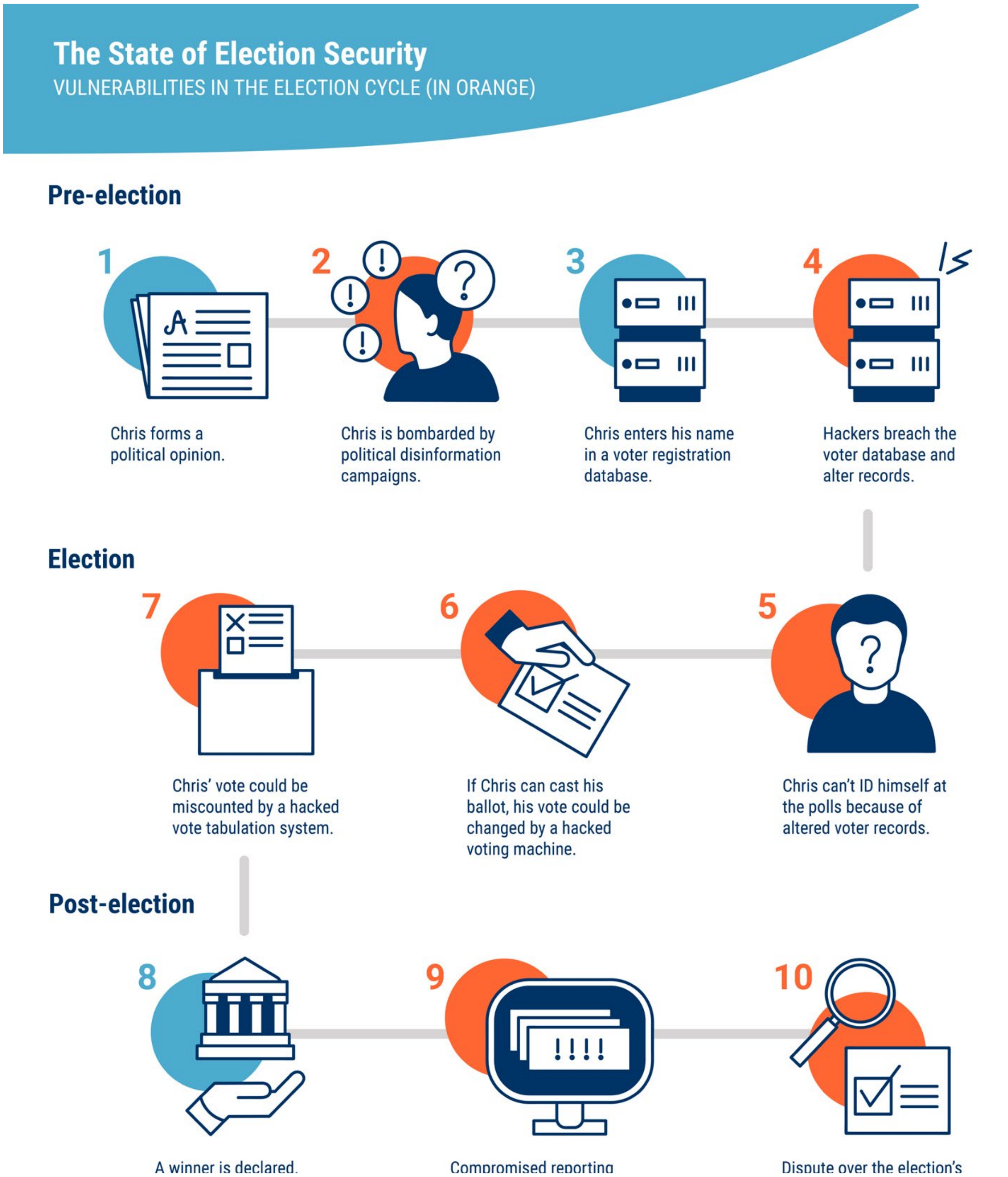
For election cybersecurity, the focus is often on hacking voting machines. However, vulnerable machines are only one part of a complex, interconnected system with multiple weak points for bad actors to exploit.

Securing elections requires securing the entire process.

The five most vulnerable parts of the electoral process, outlined by Ben Buchanan and Michael Sulmeyer of Harvard's Belfer Center Cybersecurity Project, are:

1. Information warfare
2. Electronic voter registration databases
3. Voting machinery and tabulation systems
4. Election reporting systems
5. Post-election audits

Below, we detail a voter's journey through the election process and highlight security vulnerabilities (in orange) along the way.



The State of Election Security

VULNERABILITIES IN THE ELECTION CYCLE (IN ORANGE)

Pre-election

1 Chris forms a political opinion.

2 Chris is bombarded by political disinformation campaigns.

3 Chris enters his name in a voter registration database.

4 Hackers breach the voter database and alter records.

Election

5 Chris can't ID himself at the polls because of altered voter records.

6 If Chris can cast his ballot, his vote could be changed by a hacked voting machine.

7 Chris' vote could be miscounted by a hacked vote tabulation system.

Post-election

8 A winner is declared.

9 Compromised reporting

10 Dispute over the election's

Here's a more detailed breakdown of these potential election vulnerabilities.

PRE-ELECTION

Fake news & information warfare

Before an election, the media voters consume helps shape their political opinions. But due to targeted disinformation campaigns, voters can have trouble determining fact-based sources to accurately inform their vote.

Digital deceptions distributed in the pre-election stages have a profound effect on election outcomes. Computational propaganda, digitally doctored photos and videos, weaponized social media, and more all can derail the democratic process.

In the run up to US midterm elections, experts are saying that homegrown disinformation operations in the US are starting to look like the foreign influence playbook deployed by Russia leading up to the 2016 election. Facebook has reportedly identified 559 pages and 251 accounts run by Americans designed to amplify misleading content and manufacture false consensus online.

Meanwhile, foreign influence operations are not going away. In August, Facebook announced it had identified and eliminated a new Russian network aimed at influencing Americans before the midterms.

For more on the effects of disinformation and digital deceptions, check out the CB Insights deep dive on **the future of information warfare.**

Hacked voter registration databases

Attacks on voter registration databases can also threaten people's ability to vote.

Removing sections of voters likely to support one candidate could effectively swing a close election.

If a person's identity has been removed from the voter registration database, they can't check in at polls. An attack that deletes an entire state's registration database could delay or even stop an election from taking place altogether.

According to indictments released by Special Counsel Robert Mueller, Russian intelligence officers successfully breached voter registration databases during the 2016 US presidential election. The indictments do not say whether Russia's meddling had an effect on the election's outcome.

The indictments echo a US Senate Intelligence Committee finding, which stated that Russia was in a position to, at a minimum, alter or delete voter registration data for a small number of states.

A cyber attack on voter registration databases is also in part an attack on privacy.

These databases often contain personally identifiable information (PII) such as names, addresses, phone numbers, and more. Hackers can exploit PII by selling it online in illicit dark web markets and use it to target potential voters with disinformation and propaganda.

DURING AN ELECTION

Hacked voting hardware

Votes and election results can be tampered with by hackers that exploit vulnerabilities in voting machinery and tabulation systems.

From a cybersecurity perspective, every part of the election process that involves some type of electronic device or software (especially if connected to the internet) is vulnerable to hacking.

However, security experts agree that internet-connected voting machines, tabulation systems, and their networks are particularly vulnerable.

This year, for the first time, DEF CON (one of the world's largest hacker conferences) featured a voting machine village (**Voting Village**) that let hackers hunt and exploit cyber vulnerabilities in election infrastructure — including voting machines, voter registration databases, and election office networks.

According to event organizers:

> *"By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems."*

One of the biggest worries when it comes to hacked voting machines is that these devices are subject to class breaks — security vulnerabilities that break not just one system, but an entire class of systems.

For example, stealing data through a software vulnerability at one company is a breach, but finding a common software vulnerability that exposes hundreds or thousands of companies at once is a class break.

Vulnerable supply chains create openings for large-scale election security class breaks.

Hackers at DEF CON reported multiple cases of voting machines with parts manufactured outside of the US (including hardware developed in China), highlighting the possibility of foreign entities exploiting vulnerable election supply chains.

A vulnerability in the election infrastructure supply chain means that hackers only have to find one point of entry to disrupt an entire make or model of voting machine.

A small number of election technology vendors and support contractors service the software systems used by many local governments.

Three companies dominate the American election industry: Dominion, Hart InterCivic, and, the largest, Election Systems and Software (ES&S). Ninety-two percent of US voters that voted in the last ten years did so on a machine made by one of these three companies.

Attackers targeting one or some of these companies could spread malware on election equipment across thousands of jurisdictions at once, affecting millions of voters.

POST-ELECTION

Compromised election reporting systems

Manipulated reporting systems could announce inaccurate voting results.

Researchers at Harvard's Belfer Center predict that if automated data streams are used to inform news organizations of an election's outcome, attackers could manipulate those data streams to try to trick the news into announcing the wrong winner.

Hackers could also take over an official social media account and disseminate false results directly.

We could also soon see the creation of spoofed videos of officials announcing bogus election winners. Highly realistic fake videos could be created using **generative adversarial networks** (GAN) — a type of AI used to carry out unsupervised machine learning. In a GAN, opposed neural networks work together to fabricate increasingly realistic audio, image, and video content.

Post-election audit

Dismay over an election can prompt calls for a post-election audit — comparing digital results to paper ballots.

However, post-election audits are vulnerable to inaccuracy without proper voting machinery in place.

Experts agree that reliable post-election audits are only possible with a paper trail. This means that voting machines that only record votes electronically (often via touchscreen) are not suitable for ensuring election integrity.

The safest voting machines use optical scan paper ballot systems. In these systems, voters mark their votes by filling in an oval on a paper ballot. Then the paper ballot is scanned by a machine at the polling place and digitized for electronic tabulation.

Today, there is no national mandate requiring paper ballot systems in the United States. States such as Georgia, New Jersey, Nevada, and **others** do not have a paper trail to follow post-election.

A new bill called the Protecting American Votes and Elections Act proposes that all state and local elections must ensure voter-verified paper ballots can be audited.

The bill also wants all federal elections to be subject to post-election audits.

The most reliable and cost-effective post-election audits are known as risk-limiting audits. Essentially, these test only the number of ballots needed to mathematically determine the accuracy of election outcomes.

Risk-limiting audits rely on hand-calculating the margin of victory to proportionally determine the number of ballots that need to be audited. Risk-limiting audits are new and adoption is not standard across election jurisdictions.

Currently, only 28 states require audits following elections.

2

Could blockchain technology be the solution?

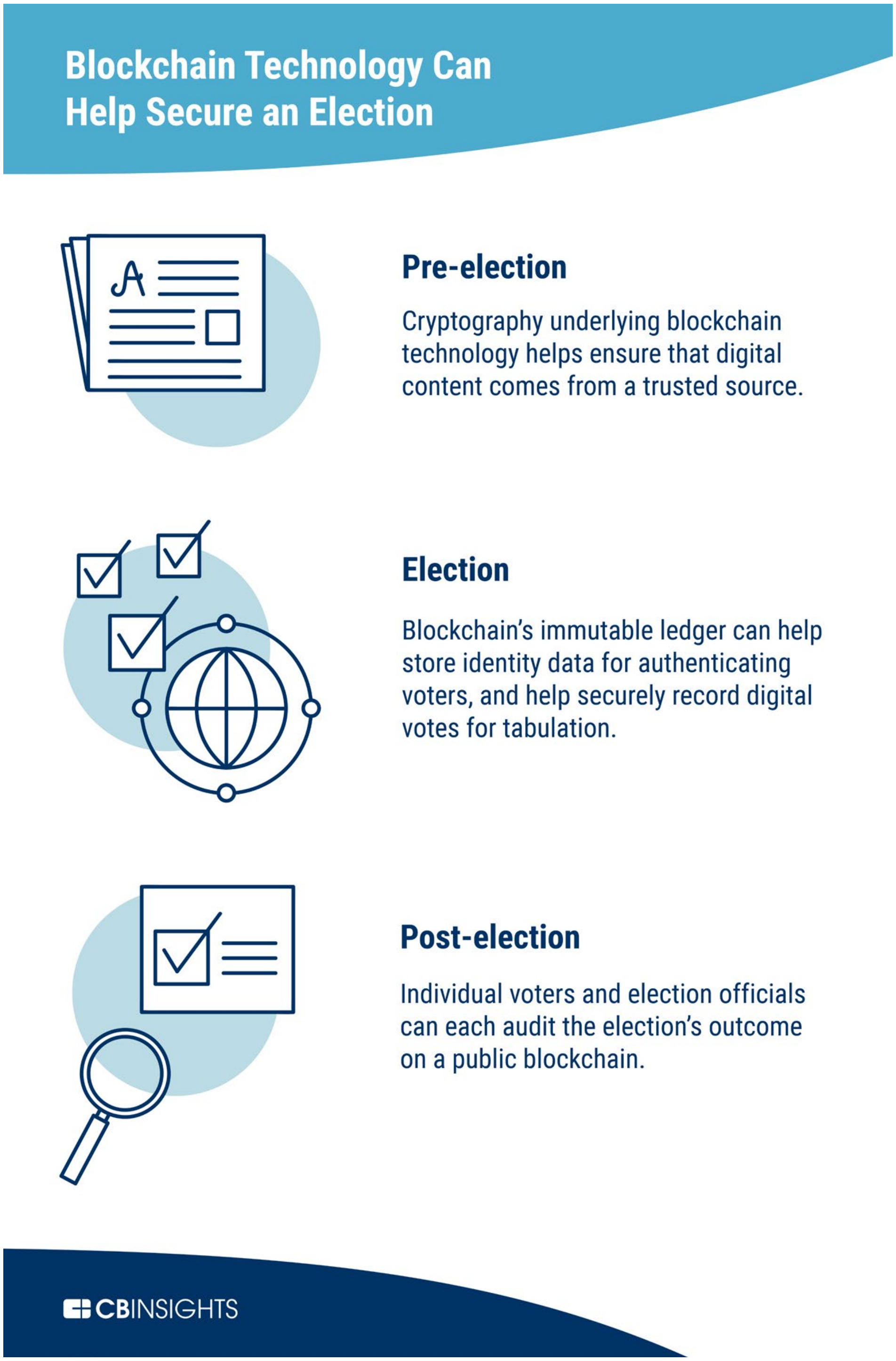
Blockchain's fundamental characteristics — transparency, immutability, and accountability — underscore the technology's potential for securing elections.

While blockchain's proponents argue that the technology could increase voter participation and improve security, some cybersecurity and election experts say blockchain makes election processes overly complicated and no more secure than other internet-connected election systems.

Despite this lack of consensus, several pilot projects around the world are starting to lay the foundations for blockchain-based voting.

Below, we highlight the technology behind a theoretically secure blockchain-based election.

To understand more about blockchain technology, check out the CB Insights primer: **What Is Blockchain Technology?**



Blockchain Technology Can Help Secure an Election

Pre-election

Cryptography underlying blockchain technology helps ensure that digital content comes from a trusted source.

Election

Blockchain’s immutable ledger can help store identity data for authenticating voters, and help securely record digital votes for tabulation.

Post-election

Individual voters and election officials can each audit the election’s outcome on a public blockchain.

CBINSIGHTS

Here's how blockchain technology could affect the voting process.

PRE-ELECTION

Cryptographic media verification

Cryptographic techniques that underpin the technology behind blockchain can also help ensure that digital content comes from a trusted, accountable source.

Essentially, voters would only consume media that is stamped with a unique cryptographic identifier, which — when cross-referenced with immutable records on a blockchain — can prove beyond a doubt where the media originated. Media without an identifier would be considered less trustworthy.

In this case, instituting a blockchain system for media verification would likely have to be undertaken at the media level, in coordination with the government and non-governmental institutions.

Mobile apps for blockchain voting

Skeptics note that any kind of voting over the internet is insecure, and that mobile adds layers of complexity that further erode security and transparency.

Proponents of mobile voting claim that making elections accessible via mobile devices can help increase voter participation — and that blockchain is the missing link in securing mobile internet voting.

West Virginia will make mobile blockchain voting available to overseas voters from all 55 counties for the November midterm election.

The program was funded with an initial $150K grant from venture capitalist and former Uber adviser Bradley Tusk. Tusk wants to increase voter participation, especially among active military personnel overseas.

After participating in West Virginia's pilot program, First Lieutenant Scott Warner said,

> *"In the same amount of time that I could've pulled up and watched a YouTube video, I actually got to go perform my civic duty."*

First Lt. Warner is considered one of the first voters in US history to record his ballot via blockchain in a federal election. Election officials had to copy Warner's vote by hand onto a paper ballot and scan it into a machine for it to count.

For the pilot, West Virginia used Boston-based blockchain voting startup **Voatz**.

The Voatz app uses facial recognition software to confirm voters' identities, compliant with West Virginia's laws. Votes are stored on the blockchain, inside what Voatz calls a "digital lockbox" in the cloud. The digital lockbox is essentially a secure cloud database that is made extra-tamper-proof via blockchain's immutable ledger technology. On primary day, county clerks unlock and collect the votes for tabulation.

Other startups developing blockchains for elections include: **Votem**, **Follow My Vote**, **Votebox**, and **XO.1**.

Notably, mobile internet elections could allow for a longer window for voting at digital polls. For example, Estonia's internet voting infrastructure allows voters to log on and vote as many times as they want during the pre-election period. Since each new vote cancels the last, a voter always has the option of changing their vote until the deadline.

DURING AN ELECTION

Digital identity and blockchain voting

Blockchain could help centralize the management of voter identities.

Blockchain elections require an assortment of identity data — such as government-issued IDs and biometric data collected during online registration — to match a voter with his or her digital identity in a government voter registration database. Increasingly, biometrics like iris and face data are being used to prove identity in conjunction with voting on blockchain.

The government or party organizing an election can designate a consortium of universities, nongovernmental organizations, and others whose consensus authenticates identity and determines which voters can vote. The concept is what's known as a permissioned ledger.

Blockchain purists say relying on a consortium runs counter to blockchain's fundamental idea — namely decentralization. Having voter identities dispensed and revoked by central authorities puts voters back at the mercy of a few administrators who get to decide which votes count.

On permissioned ledgers Josh Benaloh, a senior cryptographer at Microsoft said,

> *“Blockchains are a very interesting and useful technology for distributed consensus where there is no central authority. But elections just don’t fit that model.”*

Essentially, blockchain evangelists still have to contend with a number of technical issues that, if left unsolved, will limit the potential of the technology for transforming elections.

Blockchains could theoretically work well for securely storing votes in an immutable distributed ledger. However, beyond the secure database use-case, most blockchain election providers require additional layers of technology for effectively validating voters’ identity, keeping ballots secret, and letting voters track and verify votes.

POST-ELECTION

Post-election audits on the blockchain

With a public blockchain, each voter would be allowed to audit each ballot to confirm that reported vote totals are accurate, without revealing the identity or vote choice of each voter.

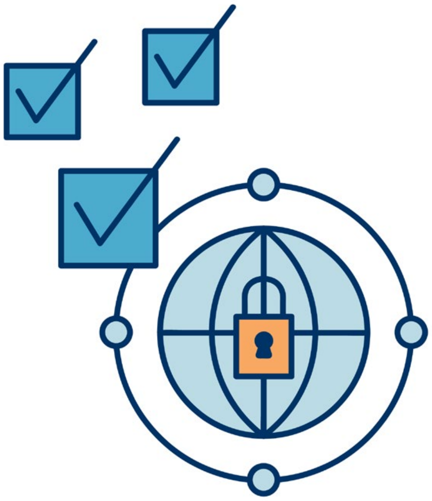
Today, the blockchain voting startups Votem and Voatz offer systems that enable voters to verify their own votes.

Voters cast ballots and receive QR codes tied to their vote. By scanning the QR code with another device, voters can reassure themselves that their vote was properly recorded. The system does not let voters know with certainty that their vote was part of the final election result, but no form of voting currently in use offers that level of assurance.

Opponents of blockchain voting claim that oversight and audits can be achieved more simply by other means, namely, risk-limiting audits designed to limit the amount of resources needed to prove an election's integrity.

3

What's next?



The gold standard for an election is one that is end-to-end (E2E) verifiable.

E2E verifiable elections have three primary components:

1. Voters are assured that their choices are properly recorded.
2. All voters can verify that their vote was counted in the official results.
3. The public can verify that the results of the election are accurate.

In the future, we could see security experts and election officials converge to develop election infrastructure and processes that reflect the need for an E2E verifiable election.

Experimenting with blockchain could be an important stepping stone toward the E2E verifiable goal.

At the same time, bedrock cybersecurity measures such as data security, network and endpoint monitoring, penetration testing, and more will continue to play a critical role in election security for the foreseeable future.