The Myth of "Secure" Blockchain Voting

David Jefferson, Verified Voting[1]

In the last couple of years several startup companies have begun to promote Internet voting systems, this time with a new twist – using a *blockchain* as the container for voted ballots transmitted from voters' private devices. Blockchains are a relatively new system category somewhat akin to a distributed database. Proponents promote them as a revolutionary innovation providing strong security guarantees that can render online elections safe from cyberattack.

Unfortunately, such claims are false. Although the subject of considerable hype, blockchains do not offer any real security from cyberattacks. Like other online elections architectures, a blockchain election is vulnerable to a long list of threats that would leave it exposed to hacking and manipulation by anyone on the Internet, and the attack might never be detected or corrected.

In its recent report[2], "Securing the Vote – Protecting American Democracy" the National Academy of Sciences summarized its findings:

> Conducting secure and credible Internet elections will require substantial scientific advances.
>
> The use of blockchains in an election scenario would do little to address the major security requirements of voting, such as voter verifiability. The security contributions offered by blockchains are better obtained by other means. In the particular case of Internet voting, blockchain methods do not redress the security issues associated with Internet voting.

In this short paper we attempt to explain why blockchains cannot deliver the security guarantees required for safe online elections. But the summary is simple: *Most of the serious vulnerabilities threaten the integrity and secrecy of voting before the ballots ever reach the blockchain*.

What is a blockchain election?

A blockchain is a type of distributed data container that is usually, but not always, intended to be collectively owned and operated by a group of independent and mutually distrusting organizations acting as peers, without any leader or central authority. In a blockchain-based election the blockchain serves as a distributed ballot box holding the voted ballots, though it is sometimes used to hold other information as well.

There are at least two distinct ways to deploy blockchains for voting, the *multi-owner chain* and the *single-owner chain*.

With the multi-owner chain the intent is that the public should not have to blindly trust that everything will go perfectly at the local Election Agency that is charged by law with the collection and counting of ballots. Instead, the public would trust the collective behavior and

---

[1] https://www.verifiedvoting.org/board-of-directors

[2] National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. doi: https://doi.org/10.17226/25120, p. 105

agreement of a group of independent participating organizations (co-owners) that check-and-balance one another as they collect voted ballots submitted through the Internet and store them in the blockchain. The local Election Agency may be one of the peer co-owners, while others might be local political parties or civic organizations. This approach represents a fundamental change in election administration since the Election Agency is effectively outsourcing the collection of voted ballots to the co-owners and no longer has full control over determining what ballots have been cast.

The single-owner chain is a special, simplified form of the multi-owner chain in which all of the co-owners are the same organization, either the Election Agency itself or a vendor or contractor. Since the blockchain is owned and run by that single organization, there is no independence among the participants, no real check-and-balance effect, and no essential security improvement over an ordinary centralized database. The single-owner strategy sacrifices whatever virtues there might be of a multi-owner blockchain. Nonetheless, some companies are marketing exactly this kind of blockchain election, and even claiming it is an advantage.

Blockchain vulnerability to collusion

In a multi-owner blockchain, a critical fraction of the co-owning organizations must agree on what blocks or data are added to the blockchain. For example, in Bitcoin if a subset of co-owners (known as "miners") commanding a majority of the aggregate computing power should collude with one another, they can arbitrarily decide what transactions are added the chain, potentially resulting in large scale theft if, for example, the colluders decide to record false transactions to transfer other people's bitcoins to themselves. Such transactions could not be reversed because there is no central authority — no enforcement power except the agreement of the colluding co-owners.

A similar type of threat is present when a blockchain is used in elections. The co-owning organizations must reach consensus on each ballot to be stored in the blockchain, and the final set of ballots in the blockchain will be the basis for the final vote counts. But a majority of co-owners might agree on a fraudulent set of ballots leading to declaring the wrong winners. Alternatively, outsider attackers such as other nation states or foreign criminal organizations might penetrate the servers, injecting malicious software to create the same effect as collusion to rig the election remotely. The local Election Agency may be unable even to detect such a penetration attack, let alone correct it.

In the single-owner chain the "agreement" on what ballots are stored in the blockchain is among different parts of the same system, parts that are not independent but are all run by the same organization and probably running the same software. Blockchain contents could be manipulated either by the malicious action of an insider in the controlling organization, or by an external attack in which a single penetration may give the attacker access to all the blockchain servers. The single-owner strategy is thus arguably more vulnerable to both insider and outsider cyberattacks than the multi-owner chain, while offering little if any advantage over a conventional database.

The dangers of Internet voting in general

Computer security and election experts have studied the feasibility of Internet voting for over twenty years. There is a nearly universal consensus that no technology available today or in the reasonably foreseeable future, including blockchains, can adequately secure an online public election against all the potential threats it must be defended against. Public elections have unique security and privacy requirements much more stringent than those in other applications such as

e-commerce because election officials must always know exactly who is voting to verify eligibility and prevent double voting, but they must *not* be able to trace particular ballots to the individual voters that cast them. These requirements are easily met with paper ballots at a polling place, but they cannot be met reliably and securely with any online system, with or without blockchains.

Cyberthreats common to all Internet voting systems, including blockchain systems

Online elections are especially vulnerable to cyberthreats because anyone on the Internet can attack the elections remotely. A successful attack may never be detected, resulting in the wrong people being elected, but with no evidence, even forensic evidence, that anything was amiss. Many foundational computer security problems must be solved before we can safely conduct elections online, and no one is close to solving any of them in a way that is practical for ordinary voters.

The use of blockchains does nothing to ameliorate any of the following cybersecurity problems inherent in all forms of Internet voting.

- *No reliable voter identification (authentication):* Without strong cryptographic infrastructure that does not currently exist in the U.S. there is no foolproof way to determine exactly who is trying to vote remotely over the Internet. All known and proposed identification methods have grave weaknesses. Passwords are notoriously unreliable for many reasons. Birthdates, SSNs, driver's license numbers and other personal information cannot be used because they have been stolen for tens of millions of voters many times in major data breaches such as those at OPM[3], Equifax[4], Heartland[5], and Yahoo[6]. Biometric identification does not work through the Internet because election officials do not have databases of voter biometric information to match against. Facial photo-based methods are not standardized, are forgeable, and have high error rates even when there is no deliberate attempt to fool them, especially for minority ethnicities.

  Voter identification and authorization has to be complete *before* there is any consideration of adding the voter's ballot to the blockchain. The blockchain does not help with this step.

- *Malware:* In online voting systems voters fill out and cast ballots from their own personal devices. Those devices may be infected by low-level malware or a malicious counterfeit voting app. It is well within the capability of a foreign state to spread malware to millions of devices, but there is no reliable way to tell whether or not a device is infected. All malware detection systems are fundamentally imperfect and limited.

  Malware could change votes invisibly inside the voting device even before they are transmitted. Or it might silently discard the ballot, or send the voter's name and vote choices to a third party, enabling coercion, retaliation, vote buying and selling, or pre-counting of votes. Blockchains cannot address the many threats that malware poses because the harm is done long before the ballot gets to any of the blockchain co-owners.

- *Denial of service (DoS) attacks:* A server can be overwhelmed with fake traffic from a botnet (a large number of Internet-connected devices remotely controlled without the

[3] https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach
[4] https://www.ftc.gov/equifax-data-breach
[5] https://www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach/#de9afb9744ad
[6] https://en.wikipedia.org/wiki/Yahoo!_data_breaches

owners' consent) so that real ballots cannot get through. Such attacks have occurred in real elections in Arizona (2000)[7], Ontario (2003, 2012[8]) and Hong Kong (2012)[9][10]. Much of the online infrastructure of Estonia was brought to a halt for days in 2007 by DoS attacks from Russia[11]. And on Oct. 21, 2016, the Mirai botnet attacked Dyn (a major Domain Name System (DNS) provider), making dozens of the world's most highly trafficked web sites inaccessible[12]. DoS attacks happen every day to smaller targets and are among the easiest of all cyberattacks to perpetrate.

There is no ironclad defense against DoS attacks, and nothing prevents such an attack from disrupting a blockchain voting system. Although blockchains use multiple redundant servers they offer no additional protection against DoS attacks beyond what is achievable for a conventional server with the same aggregate communication capacity.

- *Penetration attacks:* No servers, including blockchain servers, are immune to remote penetration and surreptitious takeover by determined sophisticated attackers. A penetration attack on vote servers was famously demonstrated in 2010 by University of Michigan professor Alex Halderman, who gained total remote control of the election servers during a test of a Washington, DC Internet voting system[13]. The attack went undetected for days. Foreign adversaries have gained control of various other servers in the U.S. many times, including the Illinois State voter registration database[14].

  In both the multiple- and single-owner cases blockchains use multiple servers. But if attackers can disable or gain control of a large enough fraction of those servers they can disrupt or control the outcome of the election, perhaps undetectably and most likely uncorrectably. The single-owner blockchain strategy is especially vulnerable to penetration because an attack that works on one server will probably work on all.

- *Nonauditability:* Paper ballots and hand auditing of machine counts are by far the best cyber defense we have for elections.[15] But online voting systems, including blockchain systems, do not allow for true, voter-verified paper ballots that are essential for meaningful recounts, audits, and statistical spot checks. Thus, the most powerful and common-sense tools we have for protecting elections against cyberattacks of all kinds are unavailable in blockchain elections.

Threat to national security

Election security is a matter of national security. Blockchains, despite the hype surrounding them, offer no defense against the well-known threats to which all online elections are vulnerable. Nation-state rivals like Russia have demonstrated a capacity and willingness to interfere with our electoral processes and would have no difficulty disrupting or undermining a blockchain election.

---

[7] Kurt Hyde and Steve Bonta, "Voting on the Web", The New American, October 9, 2000, p.28

[8] Meagan Fitzpatrick, CBC News, Aug. 8, 2012, https://www.cbc.ca/news/politics/ndp-gives-up-convention-cyber-attacker-remains-a-mystery-1.1158440

[9] https://blogs.wsj.com/chinarealtime/2012/03/23/cyber-attack-targets-hong-kong-mock-vote

[10] https://en.wikipedia.org/wiki/Hong_Kong_Chief_Executive_election,_2012#Mock_polls

[11] https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[12] https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

[13] https://www.nytimes.com/2010/10/09/us/politics/09vote.html

[14] https://abc7chicago.com/politics/12-russians-indicted-for-hacking-in-2016-election/3758586

[15] https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

In this era of ubiquitous cyber threats, it is dangerous and irresponsible to introduce online voting in the U.S. — or in any other democratic nation — with or without blockchains. Online voting includes email, fax, and web-based voting, as well a voting via apps from mobile devices. Any kind of Internet voting, with or without blockchains, serves as an invitation to hackers, political partisans, and international rivals to attempt to remotely and silently suppress or change votes, putting a thumb on the political scale in favor of their goals instead of those of the electorate.

Better alternatives to Internet voting

Internet voting has been discussed in the U.S. for 20 years and piloted several times, primarily in an effort to reduce barriers for overseas and military voters. Historically it was difficult for them to vote because they had to mail in a request for an absentee ballot, wait to receive it by mail, and mail the voted ballot back, incurring at least three postal delays. Often the blank absentee ballots were not available in time for overseas and military voters to meet the Election Day deadline. It used to be widely believed that Internet voting would be the best way to resolve these problems.

But today overseas and military voters face far fewer such obstacles. By law absentee ballots must now be made available 45 days in advance of Election Day, and in some states voted ballots can be received after Election Day and still be counted. Furthermore, ballots must be made available electronically, so most voters can download blank ballots and print them instead of waiting to request and receive them by mail. Postage paid express return of voted ballots is available, getting marked ballots back to election officials in most cases in just a few days.

What should we do instead?

Instead of deploying inherently vulnerable Internet voting systems, including blockchain systems, all jurisdictions should move to paper ballots (if they don't already use them) and should implement routine, statistically valid manual post-election audits (or strengthen the ones they have).

Paper ballots plus routine manual audits provide the trustworthy records and procedures needed to verify and demonstrate that the declared election outcomes are correct. Strong audits provide better security than any all-electronic voting system can, especially Internet voting systems.

Jurisdictions should invest further in improving the process of mail-in voting, ensuring that all military and overseas voters know when to start the voting process and how to obtain their ballots, expanding the availability of postage-free express mail for ballots, and offering improved voting options for deployed military. We have much more work to do to assure that all Americans can vote easily and safely while maintaining justified confidence in the security of elections. At a minimum, however, we must avoid the built-in structural risks common to all forms of online voting.