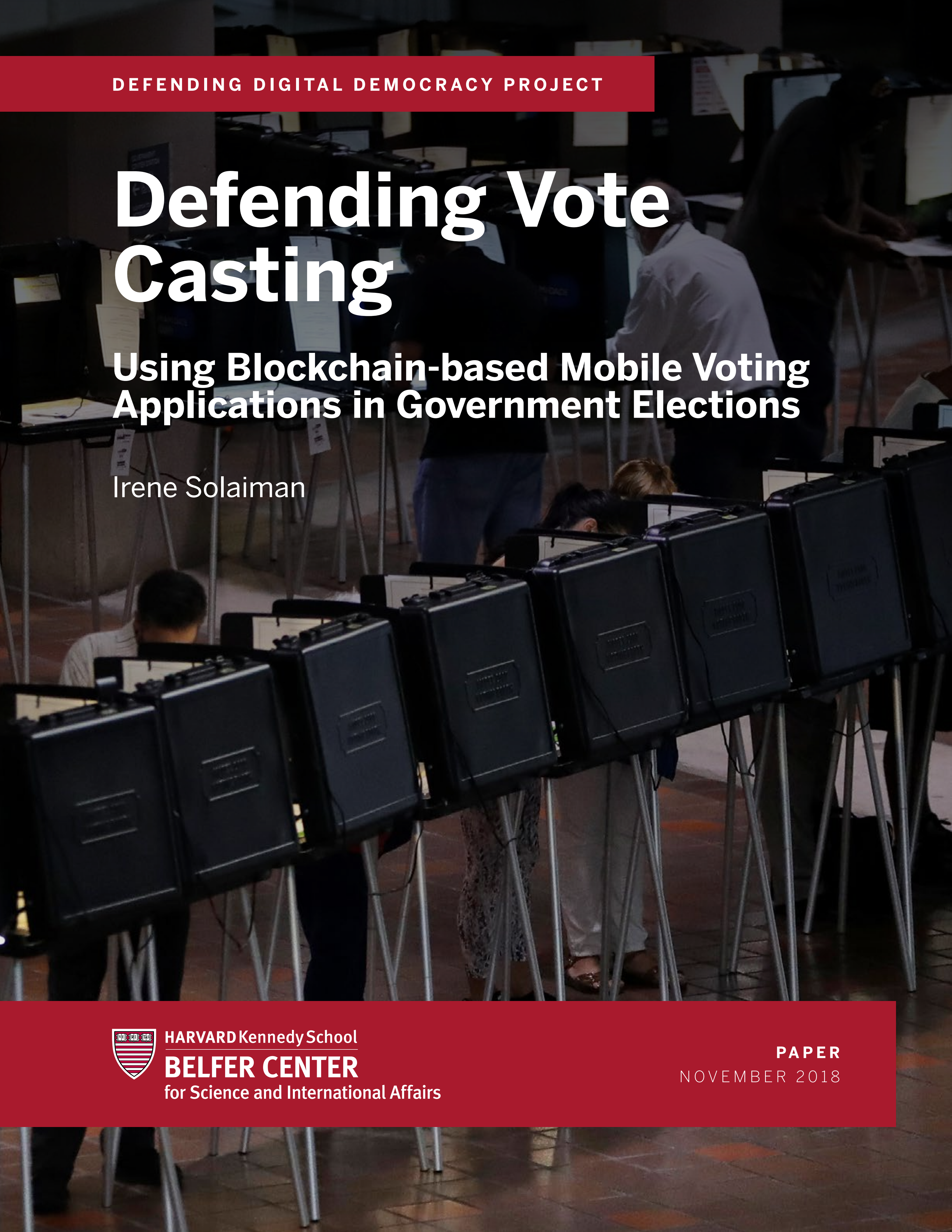

DEFENDING DIGITAL DEMOCRACY PROJECT

Defending Vote Casting

Using Blockchain-based Mobile Voting Applications in Government Elections

Irene Solaiman

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
NOVEMBER 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/d3p

Statements and views expressed in this report are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Layout by Mari Dugas

People vote on the first day of early voting in Miami-Dade County, Monday, Oct. 22, 2018, in Miami. (AP Photo/Lynne Sladky)

DEFENDING DIGITAL DEMOCRACY PROJECT

Defending Vote Casting

Using Blockchain-based Mobile Voting Applications in Government Elections

Irene Solaiman

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
NOVEMBER 2018

About the Author

Irene Solaiman is a second-year Master in Public Policy candidate at the Harvard Kennedy School. She is a researcher for the Defending Digital Democracy Project. She served in the U.S. Department of State's Server Operations Center before working on foreign policy with the U.S. Foreign Service in the Bureau of Near Eastern Affairs and the U.S. Embassy Tanzania. Her current research studies blockchain applications to cybersecurity.

Acknowledgments

Thank you to Eric Rosenbach, Mari Dugas, and the Defending Digital Democracy Project; Chuck Flannery, Deak Kersey, and the Office of the West Virginia Secretary of State; and the Voatz team for their support and insights.

Table of Contents

People vote on the first day of early voting in Miami-Dade County, Monday, Oct. 22, 2018, in Miami. (AP Photo/Lynne Sladky)

Executive Summary

- Threats to U.S. elections, including undermined trust in election infrastructure and vote casting accessibility, necessitate innovation in voting security and accessibility.
- The decentralized U.S. election system's use of mail-in absentee ballot voting disadvantages voting populations such as overseas voters.
- Blockchain-based mobile voting applications provide an accessible vote casting method that addresses key overseas disadvantages like timely vote tallying and ease of use.
- Blockchain vote records are secure and immutable, but internet architecture surrounding existing applications raise cybersecurity concerns. Safeguards like connected voter verified audit trails can improve security.
- Implementing blockchain-based mobile voting impacts voter accessibility, security, speed and accuracy, privacy, user perception, and election officials.
- Existing application software is not currently sustainable at a large scale, but is best applied to small voting populations, like overseas voters, for better monitoring and administrative costs.

1. Introduction

The U.S. election system is part of the critical infrastructure upholding democracy. Election officials are responsible for ensuring fair elections in which vote casting is secure and accessible to the 200 million registered voters,[1] including an estimated 3 million eligible voters overseas.[2] U.S. election officials must be able to address election security concerns while encouraging voter registration and turnout and being conscious of voter needs. Election security in the U.S. has been challenged in every vote casting method used, from filling out paper ballots to tapping touchscreens. To combat threats to elections, different methods to cast ballots have been developed.

Blockchain-based mobile voting has been and is being piloted as an alternative voting method. The underlying blockchain technology differentiates it from previously attempted networked vote casting methods. Previously used for economic transactions, blockchain is an emerging technology that uses a distributed system to create an immutable and incorruptible peer-to-peer network. The distributed system means information is not centralized, ensuring all data has copies, information cannot be lost, and there are no central points for cyberattack. Data inputted into blocks are timestamped, encrypted, and "locked" to prevent tampering. The peer-to-peer network provides a validation mechanism to protect the integrity of the data being locked into each block.

Blockchain-based mobile voting applications strive to provide a secure, accessible means for voters to cast their ballots. Its use cases span small, privately held elections to its introduction in the 2018 midterm elections for overseas voters.

2. Vote Casting in the U.S. Election System

The U.S. election administration system is decentralized. Elections are often run at the county level, if not township or city, and every polling location may function differently.

Paper ballot voting is the most common form of voting worldwide. It is the least susceptible to cyberattacks. However, human error in paper ballot use is common, from filling out the ballot to vote tallying. Inadvertent stray marks, incorrect ink, or filling out multiple options may invalidate a ballot. Paper ballots are also susceptible to fraud through theft, destruction, or substitution. They also present logistical challenges in tallying. Issues like invalidated ballots affected the U.S.'s 2000 presidential election and led to the 2002 Help America Vote Act (HAVA). States were required to update their voting equipment and make vote casting more accessible. The Act gave states funding for new equipment and mandated that all voting equipment be tested and certified. It also required voting machines to have a manual audit capacity.[3]

In the 2016 election, the majority of U.S. voters used electronic vote casting machines, either in the form of a Direct Recording Electronic device that records votes electronically, or an optical scanner that scans their paper ballot.[4] Electronic systems are vulnerable to cyberattacks and the vendors that produce the machines are entrusted with ensuring machine security and vote integrity. Properly programmed and streamlined vote casting and tallying systems may reduce human error and logistical challenges but present cybersecurity concerns, especially without a voter verified paper audit trail (VVPAT) in case of a system malfunction.

Absentee voting, where voters submit ballots by mail, is encouraged for voters who will be outside their physical jurisdiction on Election Day. This vote casting method has a wide range of users, from overseas military voters to out-of-state college students. This system relies heavily on the U.S. postal service, which may have disparate levels of service from metropolitan to rural areas and could delay deliveries past deadlines.[5] Concerns include voter coercion if the ballot is completed without privacy, and stolen or intercepted ballots. Mail-in absentee ballots are at greatest risk of fraud and forgery among paper ballot vote casting methods.[6]

3. Threats to U.S. Elections

The threat landscape to U.S. elections highlights three key concerns: foreign interference, cybersecurity vulnerabilities, and voter accessibility.

Foreign interference

Foreign interference in U.S. elections, whether from a state or non-state actor, is a long-standing threat to election systems and democracy. After the 2016 U.S. presidential election, the CIA, FBI, and NSA stated with "high confidence" that the Russian government conducted information operations to influence the election. In addition to influence campaigns through traditional and social media outlets, illicit cyber activities compromised election-related documents.[7] Any perceived foreign interference affects voter trust in existing election systems and risks deterring voters from going to the polls.

Cybersecurity vulnerabilities

In 2017, the U.S. Department of Homeland Security stated Russian hackers probed election-related computer systems in 21 states during the 2016 election. Despite claims that systems were compromised, U.S. officials assert there is no evidence that votes were altered.[8] Outdated vote casting machines without paper audit trails are a vulnerability if vote casting machines are thought to be compromised. However, many states have been unable to update voting machines due to logistics, such as limited time and resources before an upcoming election.[9] Election systems with internet connectivity are especially vulnerable. Votes, if compromised, are subject to manipulation or deletion, and compromised systems may produce inaccurate results. The U.S.'s decentralized system prevents centralized hacks, but disperses resources and cybersecurity expertise. Aging systems with out of date software pose an additional threat if not updated. Even if a cyberattack attempt fails, the attempt could foster distrust in the system.

Voter Accessibility

Threats to democracy already exist within the election system; logistic barriers and other obstacles keep eligible voters away from polls. 10% of eligible voters do not have the proper form of identification that satisfy voter identification laws.[10] Many voters are unable to take time off from work or personal duties to cast a ballot. Among those disadvantaged are overseas civilian voters. The 1986 Overseas Citizens Absentee Voting Act (UOCAVA) and 2009 Military and Overseas Voter Empowerment Act (MOVE) sought to address legal and time considerations respectively, the latter implementing electronically delivered ballots, but low turnout remains with a turnout rate of approximately 7%. This turnout rate is attributed largely to infrastructural barriers such as mail speed and the ability to transmit and receive election-related materials. In the 2016 elections, approximately 19,000 absentee ballots were rejected,[11] with missed deadlines being the most common reason for their invalidation.[12] Overseas military voters face similar obstacles and may not have access to secure mailing systems in certain regions.

4. Blockchain-based Mobile Voting in Practice

Several startups have developed blockchain-based mobile vote casting systems that have been used in private or small-scale elections. The non-profit Democracy Earth Foundation founded Sovereign, which utilizes "liquid democracy". In this system, which was used during a referendum for an unofficial agreement between the Colombian government and the Revolutionary Armed Forces of Colombia (FARC) rebel group, voters distribute a finite number of vote tokens.[13] The startup Votem has been used to cast over 8 million votes in private elections, including for the Rock & Roll Hall of Fame.[14] Other startups include VoteWatcher, Boulé, Follow My Vote, and Voatz.

Building on blockchain's popularity in the finance sector, Nasdaq tested blockchain voting in 2017 with a web-based blockchain voting program. The vote took place in Estonia, a country with nationwide internet voting known as i-Voting.[15] The voters, shareholders who have invested in companies on the Tallinn Stock Exchange, complimented the user interface and security in a post-use survey.[16] Nasdaq publicly stated interest in continuing using this vote casting method in Annual Meeting shareholder voting processes for greater efficiency and integrity.[17]

Blockchain-based mobile voting has also been used for small-scale government elections. The Swiss city of Zug tested mobile blockchain-based voting in a consultative vote mid-2018 for voters with digital IDs. The pilot intended to host an election that protected voter privacy and secrecy and was verifiable, unchangeable, and comprehensible. Although a small-scale election with 72 voters, participants found the process easy and the city's head of communications called it a success.[18]

Most notably, a similar application using the Voatz platform will be used in the 2018 U.S. midterm elections for eligible overseas voters registered with participating West Virginia counties.

Case Study: West Virginia

In early 2018, the office of the Secretary of State of West Virginia announced it would be piloting Voatz's blockchain-based mobile voting application for eligible overseas voters. This will be the first use of this kind of application in a U.S. federal election. Inspired by Secretary of State Mac Warner's military service abroad where secure ballot casting proved difficult, and by the 2016 election's low military and overseas voter turnout, the program aims to serve overseas citizens and active duty military personnel. The program has been fitted to comply with West Virginia laws, covering voters under UOCAVA.[19]

Tusk Montgomery Philanthropies, the organization funding the pilot, selected the Voatz platform for its security and transparency. The application relies on blockchain to create an immutable record of the votes cast, cybersecurity software to detect malware on smartphones, and biometrics for identification and authentication. The application only functions on pre-determined smartphones that meet security standards and have the latest software updates; should the malware detection software find any potential threat, then the application will prevent users from opening it. Any suspicious activity is flagged for human review. Tusk Montgomery Philanthropies, West Virginia Secretary of State's Office, and the Voatz team have conducted numerous third-party penetration testing and source code audits and have reported no issues. Voatz has also tested this platform in private elections, recording over 75,000 votes since its launch in 2015.

To prevent voter fraud, the platform utilizes biometric identification methods in addition to traditional voter identification by government-issued ID. Voters first take a photo of their government-issued ID with their mobile device's camera. They then record a video of their face in real-time, which is compared to their photo ID to verify their identity using facial recognition software. Once their identity is verified, voters may access their ballot on their smartphone. After making their desired choices, voters use their smartphone's fingerprint scanner to cast their ballot. Voter privacy concerns that votes are linked to identity, usually resulting in voters waiving their right to a secret ballot,[20] are mitigated; blockchain provides pseudonymity and all personally identifiable information (PII) is deleted once the vote is secured. West Virginia's system also creates an anonymous ID for the data that is inputted to public blockchain and does not publicly display any selections made by the voter. A "VVPAT" in the form of a certified email receipt is sent to both the designated election office and voters' email account when the voter casts their ballot. This acts as an audit mechanism and paper backup. Voters may view and verify that receipt and notify officials if there are any discrepancies.

The pilot was tested originally in two counties during the 2018 primary election and expanded to eligible overseas voters from 24 of West Virginia's 55 counties for the 2018 midterm elections.[21] This pilot is an option to those eligible, who may still choose to vote by existing traditional methods as applicable. The program is not slated to expand past overseas voters.

5. Application Architecture

Blockchain-based mobile voting applications must ensure votes are securely recorded, transmitted, and verified. Central to these applications' security is blockchain technology. Developed originally as the infrastructure for the cryptocurrency Bitcoin, blockchain allows users to share data securely and in a tamper-proof manner. Each block stores assigned data and is labeled with a "hash" that functions like a fingerprint. That data is time stamped and linked to a subsequent block, forming a chain. Records are also encrypted to prevent unauthorized viewing.

The blockchain is hosted on a distributed network, where multiple hosts, or nodes, each contain a copy of the blockchain. Hosting a blockchain, especially on a large scale, requires substantial energy resources to sustain computing power for its authentication and validation requirements. The distributed system means there is no central server susceptible to database deletion or denial of service attacks. In the cases of these voting applications, the network is private and only accessible by cryptographic key. Users with access to the blockchain can view the inputted data but cannot alter it once locked.

Blockchain provides a pseudonymous identity, which cannot be easily directly traced to the user. To prevent voter fraud, a voting application may employ several identification and authentication methods before votes are cast. Digital identification cards for constituents, used in states like Estonia, are a possible means of identification. Biometric identification, like facial recognition software, is another form that uses physical characteristics to authenticate users.

6. Impact on U.S. Elections

Blockchain-based mobile voting addresses threats to vote casting and elections and implementation would have a wide range of impacts.

On Voter Accessibility

The current use of blockchain-based voting by smartphone makes voting more accessible to voters who do not have a secure or affordable means of mailing ballots or who are unable to access equipment like printers sometimes necessary to mail ballots. The application could also ease accessibility for voters with disabilities and special needs whose conditions may limit their ability to cast a mail-in ballot or visit a polling location. Voters with time restrictions (i.e. unable to leave work on Election Day) who are unable to cast a ballot in person would have a more convenient means for ballot casting. A 2016 survey of 3,649 U.S. citizens of voting age reported 33% would be more likely to vote if able to do so over the Internet from any location.[22] Moreover, the Federal Voting Assistance Program's international overseas voter analysis found that voters who received their ballot electronically were nearly 50% more likely to vote successfully.[23] Actual impact on voter turnout remain contested, as individuals must decide to vote and register before Election Day. Mobile application voting would largely be a tool of convenience.[24]

On Cybersecurity

The election cybersecurity threat landscape changes as election systems change. While the blockchain itself is immutable, technical vulnerabilities lie in vote casting and tallying. Further challenges lie in the architecture surrounding the blockchain and its effect on users, but including some form of a voter verified ballot image or "VVPAT" provides a means to conduct a more traditional post-election audit to confirm the results.

Blockchain provides a secure system if the vote is properly inputted.[25] On a blockchain, a vote may not be altered or lost. However, if there is malware on a voter's device that goes undetected before casting a vote, the vote can be compromised before it is locked in the blockchain. Threats to smartphones include phishing scams. Detecting malware is not foolproof, even with appropriate software security on a personal device. Compromised votes are usually not immediately apparent, if apparent at all, which further necessitates a VVPAT.

If voters are given a cryptographic key, hackers may focus on compromising that key to alter the vote before it is locked or view the vote tied to a voter's identity, raising privacy concerns. Cryptographic keys have been compromised in the past and the current proposed blockchain-based voting system uses voter's personal devices that are used for other functions and are not guaranteed to be secure.

On the receiving end, reporting software in any digital tallying system can be susceptible to hacking and manipulation. Although this may vary by the application used, vote tallying security depends on whether election offices host a copy of the blockchain or if vote tallies are transmitted by internet. Vote transmission over the internet is more vulnerable to interception and manipulation. In both cases, a VVPAT is needed to ensure vote integrity.

On Vendor Security

Just as the current security of vote casting machines is dependent on private vendors and providers, the company hosting the blockchain and the architecture around it is trusted not only to prevent manipulation, but also to not manipulate results themselves. The hosting service that controls the majority of nodes on the blockchain also controls what is added and therefore must be trusted to maintain vote integrity and prevent user discrimination.

The vendor also hosts all software and is responsible for preventing software corruption. Since ballots on a blockchain are presented electronically, they must be clearly verifiable and not disrupted upon viewing.[26] Vendors must also be able to accommodate expanding energy consumption to host the blockchain, especially if it expands. However, this is not a novel concern; software security autonomy is the norm for current election systems vendors.

On Vote Speed and Accuracy

Electronic transmission without interference ensures all votes submitted on time are counted by the deadline. A predetermined ballot structure with software that prevents voter error when filling out a ballot (i.e. voting for multiple candidates) will decrease chances of ballot invalidation. The tallying speed will also be faster than for paper mail-in ballots.

Additional audit systems that resemble a VVPAT must be added to the application, but electronic vote tallying on a blockchain will be streamlined and resistant to denial of service attacks.

On Voter Confidence

Current threats to U.S. elections seek to undermine trust in democratic systems. Blockchain records could provide a sense of security and mitigate fears of vote manipulation from foreign interference. However, a lack of understanding of the technology or its association with cryptocurrency and existing applications' surrounding internet architecture could negatively impact voter perception.

On Voter Privacy

A secret ballot cast in privacy is necessary to reduce the threat of voter coercion, vote buying, and vote tampering in addition to voter harassment. Casting a ballot from a personal device raises a general concern for absentee voting; voter coercion may occur in any environment that is not entirely private. Blockchain generally does not provide anonymity, especially when the inputted vote is tied to a voter identity. Some providers use biometric security to prove voter identity, a form of identification that is permanently tied to the user. PII like biometrics may be deleted after authentication, but recovery and de-identification is possible and dependent on vendor security. Additionally, votes are difficult to delete from the blockchain and could provide a permanent record of that vote.

Furthermore, like all absentee ballot processes, a voter's identity could be discerned by a designated county election official prior to counting the ballot if necessary for audit or verification purposes. Thirty-two states allow some form of internet voting that links identity to ballot and require voters to waive their right to a secret ballot.[27] Blockchain-based mobile voting's pseudonymity would increase privacy for overseas voters who waive their secret ballot rights.

On User Bias

These vote casting applications may have user populations with age and party biases. Younger U.S. constituents are more likely to own a smartphone and are more likely to have updated devices. Only users with updated, compatible devices will be able to open the application in many cases. Confidence in and comfort with using electronic devices declines among older populations. Older constituents are also more likely to need help operating an electronic device or unfamiliar application, eliminating voter privacy.[28] Mobile and internet voting also tends to appeal most to independent and liberal-leaning voters.[29]

On Bureaucratic Costs

The high costs for any change in election architecture has long hindered election security. Implementing any new vote casting system requires political will and openness to not only change existing processes, but also update them. Any new electronic system should be accompanied by a paper audit trail, which is an additional expense. Maintaining a distributed system, usually through a third party, has high annual costs that would add to existing costs. Although Congress appropriated $380 million in March 2018 to be distributed among states' election security needs, it is the first funding since the 2016 election interference and further funding before the 2018 midterms has been blocked.[30] In the U.S.'s decentralized system, substantial funding may not trickle down to local jurisdictions.

7. The Future of Voting

Blockchain-based mobile voting

The current state of these applications, mainly considering cybersecurity and administration resources, makes this technology impractical for large-scale use. The need to protect votes from cyberattacks and interference as they are inputted and tallied requires monitoring and high vendor trust and security. Maintaining a blockchain depends on the blockchain's size, but expansion requires high computing power and storage capacity. A large-scale blockchain voting system would likely need more hosting nodes and would consume higher levels of energy. This would be the vendor's responsibility, but could lead to higher administrative costs.

However, this vote casting method presents a means for limited absentee ballot casting. Absentee voting was developed in the 1860s to allow military service members in the Civil War to cast ballots outside their physical polling locations;[31] it was designed to improve vote casting accessibility for a specific population. Blockchain-based mobile voting, as seen in the West Virginia pilot, replicates the original mission of absentee ballot voting.

Absentee voting today applies more broadly, now being encouraged in densely populated voting districts as an alternative to coming to poll sites. While this blockchain-based mobile voting is not sustainable as an overall alternative to absentee ballots, it can improve voter participation. Additionally, a smaller voting population using this application is more easily monitored for potential compromises. This is a potential solution for states with low overseas voter turnout.

Adaption and further adoption

The root technologies in these applications can instead be integrated in existing electronic vote casting machines that are used solely for vote casting purposes and have been vetted for malware. Startups like Voatz offer their voting application at poll sites using tablets.

A hybrid vote casting system that is end-to-end verifiable using blockchain but requires voters to cast ballots in-person on vetted devices improves security, but only for those able to vote in-person.[32] For overseas voters unable to return to their designated poll sites, U.S. embassies or consulates could provide vetted and secure vote casting systems that integrate similar technologies without the exacerbated risk of malware on a personal device.

With the U.S.'s decentralized election system, each state will approach new technologies differently and any uniform adoption is highly unlikely. Unfamiliarity with the underlying blockchain technology affects election officials' openness to adoption. Different states have different levels of openness to, familiarity with, and capacity to incorporate blockchain technology, although not in a voting capacity. State-level initiatives in Delaware and Illinois, as well as state bills in Colorado and Wyoming, promote researching government applications of blockchain technology.[33]

Global expansion

Other state governments are moving forward with integrating blockchain-based online voting into their national election systems in efforts to increase security and prevent voter fraud. In 2016, Ukrainian government officials signed a memorandum to use Ethereum blockchain in vote casting for political primaries, elections, and referenda. The E-vox platform used is being integrated into current election platforms in addition to online and mobile applications. The platform uses government and bank-issued digital signatures for voter authentication.[34]

8. Conclusion

No form of vote casting is entirely secure. Electronic voting methods, including blockchain-based systems, are most secure with a paper backup system like a VVPAT. As advances in election technology strive to combat threats to elections, blockchain-based mobile voting applications present a means to address voter accessibility, confidence in elections and security in preventing vote manipulation.

Mobile and internet voting technologies are not presently secure enough for large-scale applications. Blockchain technology and its surrounding architecture, including threat of malware on personal devices, make this form of remote voting currently impractical for large-scale or nationwide practice. Malware detection on personal devices can lead to security vulnerabilities and energy consumption for vendors hosting the application is costly. A hybrid form of blockchain-based voting where the architecture is built into vote casting machines at poll places reduces risks from personal devices, but is not accessible for absentee voters and still faces energy obstacles. Other impacts on a large-scale election system, like user bias and bureaucratic costs further block current expansion.

Blockchain-based mobile voting applications are most applicable to small-scale absentee ballot voting. It has the potential to affect low turnout rates for overseas voters under UOCAVA. On a small-scale, security and energy concerns are more manageable and present a viable means to engage populations like overseas voters.

Endnotes

1 Goldmacher, S., Shepard, S., Kruse, M., Grunwald, M., & Shafer, J. (2016, October 19). America hits new landmark: 200 million registered voters. Retrieved from https://www.politico.com/story/2016/10/how-many-registered-voters-are-in-america-2016-229993

2 Overseas Citizen Population Analysis Report. (2018, September). Retrieved from https://www.fvap.gov/uploads/FVAP/Reports/FVAP-2016-OCPA-FINAL-Report.pdf

3 Tokaji, D. P. (2006, March 14). Voting Technology: Beyond HAVA, Beyond Paper. Retrieved from https://moritzlaw.osu.edu/electionlaw/comments/2006/060314.php

4 DeSilver, D. (2016, November 08). Most U.S. voters use electronic or optical-scan ballots. Retrieved from http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/

5 A Consensus Study Report of The National Academies of Sciences, Engineering, Medicine, Copyright National Academy of Sciences, 2018. ISBN 978-0-309-47647-8 | DOI 10.17226/25120

6 Wines, M. (2018, September 06). 6 Ways to Fight Election Hacking and Voter Fraud, According to an Expert Panel. Retrieved from https://www.nytimes.com/2018/09/06/us/election-security-expert-panel.html

7 Masters, J. (2018, February 26). Russia, Trump, and the 2016 U.S. Election. Retrieved from https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election

8 Bernstein, S. (2018, May 31). Ahead of November election, old voting machines stir concerns among... Retrieved from https://www.reuters.com/article/us-usa-election-votingmachines/ahead-of-november-election-old-voting-machines-stir-concerns-among-us-officials-idUSKCN1IW16Z

9 Bernstein, S. (2018, May 31). Ahead of November election, old voting machines stir concerns among... Retrieved from https://www.reuters.com/article/us-usa-election-votingmachines/ahead-of-november-election-old-voting-machines-stir-concerns-among-us-officials-idUSKCN1IW16Z

10 Austin-Hillery, C. C. (2017, June 30). The Threat to U.S. Elections You Don't Know About But Should. Retrieved from http://time.com/4837622/voter-suppression-democracy-senator-chris-coons/

11 Nguyen, T. (2018, August 10). West Virginia to offer mobile blockchain voting app for overseas voters in November election. Retrieved from https://www.washingtonpost.com/technology/2018/08/10/west-virginia-pilots-mobile-blockchain-voting-app-overseas-voters-november-election/?noredirect=on&utm_term=.83a30acaa8a0

12 Overseas Citizen Population Analysis Report. (2018, September). Retrieved from https://www.fvap.gov/uploads/FVAP/Reports/FVAP-2016-OCPA-FINAL-Report.pdf

13 Heilweil, R. (2017, December 04). Nine Companies That Want To Revolutionize Voting Technology. Retrieved from https://www.forbes.com/sites/rebeccaheilweil1/2017/12/02/eight-companies-that-want-to-revolutionize-voting-technology/

14 Yurieff, K. (2018, May 8). Can this technology modernize how we vote? Retrieved from https://money.cnn.com/2018/05/08/technology/blockchain-voting-elections-votem/index.html

15 Leetaru, K. (2017, June 08). How Estonia's E-Voting System Could Be The Future. Retrieved from https://www.forbes.com/sites/kalevleetaru/2017/06/07/how-estonias-e-voting-system-could-be-the-future/

16 DeMarinis, R. (2017, January 23). Is Blockchain the Answer to E-voting? Nasdaq Believes So | Nasdaq MarketInsite. Retrieved from https://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html

17 Irrera, A. (2017, January 23). Nasdaq successfully completes blockchain test in Estonia. Retrieved from https://www.reuters.com/article/nasdaq-blockchain-idUSL1N1FA1XK

18 Switzerland's first municipal blockchain vote hailed a success. (2018, July 02). Retrieved from https://www.swissinfo.ch/eng/crypto-valley-_-switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928

19 Syeed, N. (2018, August 10). Is Blockchain Technology the Future of Voting? Retrieved from https://www.bloomberg.com/news/articles/2018-08-10/is-blockchain-technology-the-future-of-voting

20 W. Va. Code § 3-3-5(f)(2) provides, in part, "If the ballot was transmitted electronically [by an absent uniformed services voter or overseas voter, as defined by 42 U.S.C. §1973, et seq.], the voter shall return the ballot in the same manner the ballot was received, or the voter may return the ballot by United States mail, along with a signed privacy waiver form."

21 "West Virginia tests secure mobile voting app for military personnel" The Hill, March 28, 2018. http://thehill.com/policy/cybersecurity/380690-west-virginia-tests-secure-mobile-voting-app-for-military-personnel

22 Public Opinion toward Presidential Voting via the Internet (Rep.). (2016). Consumer Reports.

23 Federal Voting Assistance Program (2018, September 12). The Biennial Overseas Citizen Population Analysis, U.S. Citizens Abroad and their Voting Behaviors in 2016. Retrieved from https://www.fvap.gov/uploads/FVAP/Reports/FVAP-OCPABrief_FINAL.pdf

24 Archer, K., Beznosov, K., Crane, L., King, V., & Morfitt, G. (2014). Recommendations Report to the Legislative Assembly of British Columbia(Rep.). Independent Panel on Internet Voting.

25 "One Place Where Blockchain Could Really Help: Voting" Forbes, Feb 21, 2018. https://www.forbes.com/sites/mikemontgomery/2018/02/21/one-place-where-blockchain-could-really-help-voting/

26 A Consensus Study Report of The National Academies of Sciences, Engineering, Medicine. Copyright National Academy of Sciences, 2018. ISBN 978-0-309-47647-8 | DOI 10.17226/25120

27 Fitzgerald, C., Smith, P., & Goodman, S. (2016). The Secret Ballot At Risk: Recommendations for Protecting Democracy(Rep.). Electronic Privacy Information Center, Verified Voting, and Common Cause. Retrieved from http://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf

28 Anderson, M., & Perrin, A. (2017, May 17). Barriers to adoption and attitudes towards tech among older Americans. Retrieved from http://www.pewinternet.org/2017/05/17/barriers-to-adoption-and-attitudes-towards-technology/

29 Public Opinion toward Presidential Voting via the Internet(Rep.). (2016). Consumer Reports.

30 Hawkins, D. (2018, July 30). The Cybersecurity 202: The fight over election security comes to the Senate floor. Retrieved from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/07/30/the-cybersecurity-202-the-fight-over-election-security-comes-to-the-senate-floor/5b5dd0ad1b326b0207955e1b/?utm_term=.48e85fbb4049

31 Heidelbaugh, L. (2012, November). Absentee Voting in the Civil War: Ohio Cover. Retrieved from https://postalmuseum.si.edu/collections/object-spotlight/tally-sheet-cover.html

32 Koven, J. B. (2016, August 30). Block The Vote: Could Blockchain Technology Cybersecure Elections? Retrieved from https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/#793f995c2ab3

33 Blockchain and U.S. state governments: An initial assessment. Brookings, 2018. https://www.brookings.edu/blog/techtank/2018/04/17/blockchain-and-u-s-state-governments-an-initial-assessment/

34 Abouzeid, N. (2016, February 25). Ukraine Government Plans to Trial Ethereum Blockchain-Based Election Platform. Retrieved from https://www.nasdaq.com/article/ukraine-government-plans-to-trial-ethereum-blockchain-based-election-platform-cm585001

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/d3p

Printed in the United States of America