October 19, 2021

The Honorable London Breed
Mayor
City and County of San Francisco
City Hall, Room 200
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102
via email

RE: The California Voter Foundation and Verified Voting Oppose Blockchain Voting

Dear Mayor Breed,

On behalf of the California Voter Foundation and Verified Voting, we are writing in opposition to ballot return via the internet, including San Francisco's proposed development of "blockchain voting" as was discussed at the August 13, 2021 Voting Accessibility and Advisory Committee meeting.[1] The California Voter Foundation (CVF) is a nonpartisan nonprofit organization working to improve the voting process to better serve voters. As a supporter of voter-verified paper ballots, post-election audits and robust election security, CVF is a longtime opponent of online voting. Verified Voting is a nonpartisan nonprofit organization with a mission to strengthen democracy for all voters by promoting the responsible use of technology in elections. Since our founding in 2004 by computer scientists, we have acted on the belief that the integrity and strength of our democracy rely on citizens' trust that each vote is counted as cast. With this in mind, we oppose allowing voted ballots to be returned electronically through

[1] Agenda from August 13, 2021 San Francisco VAAC meeting.
https://sfelections.sfgov.org/sites/default/files/Documents/GetInvolved/AgendasMinutes/130821_VAAC_Agenda.pdf

insecure means, and recommend more secure alternatives to ensure all voters are able to participate safely.

Multiple cybersecurity experts have concluded that internet voting is unsafe. The National Academies of Sciences, Engineering and Medicine released a report in 2018 stating that the technology to return marked ballots securely and anonymously over the internet does not exist.[2] Additionally, in the lead-up to the 2020 General Election, the Department of Homeland Security, the Election Assistance Commission, the Federal Bureau of Investigation, and the National Institute of Standards and Technology told states and election officials that electronic ballot return "creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system. We view electronic ballot return as high risk. **Securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time** [emphasis added]."[3] Nothing has changed; no new internet technology has been created to mitigate this risk.

Blockchain does not solve the security issues inherent to internet voting.

The National Academies report states that "blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities." Blockchain technology is designed to keep information secure once it is received. It cannot defend against the multitude of threats to that information before it is entered in the blockchain, and voters cannot verify their votes are entered into the blockchain correctly without compromising ballot secrecy. Recording ballots on a blockchain also risks ballot secrecy if encryption keys are not properly protected or software errors allow decryption of individual ballots.

We must point out that the actual device (e.g. smartphone, computer) that voters would cast their ballots on have security vulnerabilities. The voter's device may already be corrupted with malware or viruses that could interfere with ballot transmission or even spread that malware to the computer at the elections office on the receiving end of the online ballot. Unlike other internet transactions, voting must simultaneously maintain ballot secrecy while still providing a verifiable record of the voter's intent. Internet voting does not allow the voter to verify that the record received by the elections office in fact reflects the voter's choices, and thus those ballots are not auditable.

California has already studied this issue. In 2000, then Secretary of State Bill Jones convened the "California Internet Voting Task Force." The task force's final report states, "Technological threats to the security, integrity and secrecy of Internet ballots are significant. The possibility of 'Virus' and 'Trojan Horse' software attacks on home and office computers used for voting is very real and, although they are preventable, could result in a number of problems ranging from a denial of service to the submission of electronically altered ballots."[4] This is as true today as it was when written in 2000.

---

[2] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.
[3] DHS Memo. https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001
[4] California Internet Voting Task Force, 2000. https://elections.cdn.sos.ca.gov/ivote/final_report.pdf

We understand the profound challenges you face to assure every voter's ability to vote. CVF and Verified Voting strongly support interventions to assure voters' equal opportunity and access to cast their vote – securely and verifiably. Recognizing that no current solution is ideal for all voters, we support thoughtful consideration of other secure innovations, such as Remote Accessible Vote by Mail (RAVBM) which has been implemented by the State of California. This innovation allows for electronic delivery of a blank ballot to the voter so they may use their own equipment at home to mark their ballot, print it out and return the paper ballot to their elections office. Many were involved in helping California adopt RAVBM, including accessibility advocates and security experts. We believe there is always room to improve RAVBM and would be happy to participate in discussions about that topic. However, internet voting, with or without blockchain, is not the answer. The contested 2020 election underscores the importance of being able to examine voted paper ballots, not just digital artifacts. A recent report published in the Journal of Cybersecurity warns, "While current election systems are far from perfect, Internet- and blockchain-based voting would greatly increase the risk of undetectable, nation-scale election failures."[5]

California law has long protected against connecting voting systems to the internet. At a time when election security and public confidence are under attack, undermining those protections would result in unprovable election results. We urge San Francisco not to adopt, test or develop internet voting.

Respectfully submitted,

Kim Alexander
President & Founder
California Voter Foundation

Mark Lindeman, Ph.D.
Director
Verified Voting

Cc:
Nicole Bohn, Director, Mayor's Office on Disability
Deborah Kaplan, Deputy Director, Mayor's Office on Disability
Mary Ellen Carroll, Executive Director, Department of Emergency Management
John Arntz, Director, Department of Elections
Donna Johnston, President, California Association of Clerks and Election Officials
San Francisco Committee on Information Technology
San Francisco Elections Commission
San Francisco Board of Supervisors

[5] Sunoo Park, Michael Specter, Neha Narula, Ronald L Rivest, MIT, Going from bad to worse: from Internet voting to blockchain voting, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, https://doi.org/10.1093/cybsec/tyaa025