

THE RESEARCH UNIVERSITY PRESS

International
Computational Law Journal

VOLUME 2 / ISSUE 4 / CURATED SOURCE EDITION

Remote Voting in the Age of Cryptography

Nathaniel Williams

MIT Computational Law Report · Originally published 2022-12-05

Independent reader edition under CC BY 4.0. This attribution cover was added; original source PDF pages follow unchanged. Original authorship and source identity are retained. MIT, Stanford University, Stanford Law School and CodeX have not sponsored or endorsed this republication.

Source, license and version evidence accompany the online article.

MIT Computational Law Report

Remote Voting in the Age of Cryptography

Nathaniel Williams

License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)

ABSTRACT

Despite the massive shift towards digital communication throughout the COVID-19 pandemic, voting technology lags behind. Moreover, many historical challenges to democracy, such as voter suppression, low turnout, and a newfound health risk, are tied to the use of in-person-first, paper voting systems. So why has there not yet been a shift away from traditional voting systems, and what might such a shift look like?

This paper identifies some properties with which to analyze the pros and cons of various voting systems. First, we present an overview of the technological, social, and legal barriers to the mass adoption of Remote Electronic Voting (REV) technology in mainstream democratic practice. With this framework in mind, we then explore our technological experiments in REV. The designs we present offer an opportunity to combine voting system properties that have, up until now, been deemed incompatible. We then broaden the scope and imagine how the adoption of such a REV system might affect our society's practice of democracy.

Introduction

The impact of information and communication technologies (ICT) on society as a whole is undeniable. The SARS-CoV-2 pandemic especially marked this trend. ICT adoption by the population has profoundly affected our ability to respond to this global emergency. Furthermore, there is no doubt that many of these changes will persist. Nevertheless, some human activities remain seemingly impervious to the widespread transformative power of ICTs. Among these, the case of voting is especially paradigmatic.

Electoral processes play a fundamental role in legitimizing power and decision-making in democratic societies. In many cases, however, residents have had to assume a high level of personal risk when exercising their right to vote in person during the pandemic. In the rare cases where populations have adopted ICTs to increase the accessibility of voting, this adoption has been hasty and inadequate. Moreover, this immediacy has often resulted in the significant erosion of privacy guarantees or the integrity of voting processes.

Problems Facing Voting

Paper voting, having faced decades of disasters and successes, is undoubtedly a battle-tested system. This method is also the most familiar; the image of a paper ballot is

integral to our understanding of voting. Nevertheless, paper ballots are enmeshed with many of the core problems facing democracy.

One of the most insidious barriers to democracy throughout history has been voter disenfranchisement and suppression. Researchers note that the practice is common in democracies in which "competing elites believe that the benefits of reducing voting by opponents outweigh the costs of voter suppression."[1] In the case of the United States, in particular, the practice "has haunted America since it was founded."[2] Legal and explicit voter disenfranchisement against women, Black citizens, and non-citizen nationals has shaped most of U.S. history. Supplemental to formal, institutional measures is a historic set of indirect institutional laws (poll-taxes, voter I.D. requirements, etc.) and "ad-hoc, extra-legal, and decentralized" practices such as outright violence against Black voters in the Jim Crow era.[3] Most institutional measures are endemic to a society's legal system, regardless of the voting methods employed within that system. Typical methods of informal disenfranchisement through physical coercion, however, is directly tied to in-person, paper voting.

The COVID-19 pandemic has introduced a whole new set of issues with paper voting. Most straightforward is the epidemiological risk associated with voting in-person during a pandemic. This risk has been significant enough to spur a massive adoption of ICTs in other sectors of business in civil society.[4] Such a shift, however, has not extended to the case of voting systems. The remote alternative of mail-in voting has alleviated this concern for election processes, but it has also become highly politicized and distrusted (despite being as secure as in-person voting).[5] In addition, minor disruptions can place ballots at risk of arriving late, and postal services (especially those that are already stretched thin) may be overwhelmed attempting to deliver ballots on time.[6]

Even under opportune conditions, a high-cost and low-frequency limits paper voting. Research estimates that the administration of national elections usually costs somewhere between $1 and $13.50 per elector,[7] with postal voting costing more than poll-station voting.[8] Even if a population desires to experiment with a more frequent and interactive form of democracy, this high cost limits most governments to infrequent elections. Beyond the administrative cost is the cost to individual voters. The time spent in transportation to polling sites and away from work or personal activities, as well as the possibly unpleasant experience of waiting in a long queue to mark a ballot, increases voters' perception of the cost incurred by voting. This perceived cost, real or not, has been shown to dramatically affect voter participation

levels.[9] The cost of the time spent counting paper ballots (by hand or by physical machine) is non-negligible, either. As evidenced by the 2020 US general election, any delay in the tabulation of election results can open sites of confusion for malicious actors to latch onto, dramatically decreasing trust and faith in public cooperation. A survey conducted by Politico and Morning Consult in the aftermath of the U.S. 2020 General Election found that only 57 percent of voters trusted the election system's integrity.[10] The study notes that no political party's members had greater than around 80 percent confidence in the election system, suggesting that the low confidence level was only partly caused by the partisan use of election mistrust as a rhetorical tool.

Voting System Properties

Remote e-voting (REV)[11] researchers typically refer to a set of privacy, verifiability, and integrity properties with which to judge a system:

Ballot Privacy (BP)	No outside observer can determine the contents of a specific vote.
Receipt-Freeness (RF)	After an election, a voter cannot prove how they voted.
Coercion Resistance (CR)	During an election, a voter cannot prove their vote to a coercer.

Table 1. Security properties.[12]

Individual Verifiability (IV)	A voter can verify that their ballot was correctly contained in the set of published results.
Universal Verifiability (UV)	Anyone can verify that the published results correspond with the set of published votes.
Eligibility Verifiability (EV)	Anyone can verify that each vote included in the results was cast by an eligible voter, and that each voter cast no more than one vote.
End-to-end verifiability (E2E)	The combination of IV, UV, and EV. The standard of a fully verifiable election.

Table 2. Verifiability Properties.[13]

Censorship-Resistance	No party, even the administrator of an election, can censor a valid vote.
Non-Repudiation	No party can modify or erase a vote that has been cast, with the exception of a valid voter nullifying their vote.
Correct Execution	No party can forge a false tally of votes.

Table 3. Integrity Properties.[14]

Paper voting typically performs well, at least theoretically, concerning privacy properties. Any attacks to BP, RF, or CR must include physical control of a polling location (or a voter's home, if voting by mail). Vote buying in a traditional system, for example, must be simple and in-person- the buyer is in attendance and observes the voter cast their ballot. Automated vote buying, on the other hand, is harder to accomplish with traditional voting systems, as it requires some form of digital proof of a vote which can then be automatically rewarded.

Verifiability, on the other hand, is severely lacking in traditional voting systems, whose designs have stagnated. Individuals usually cannot verify, without trusting some authority, that their paper ballot was counted correctly. Systems that do offer in-person IV tend to include a more significant time investment from voters. Some systems offer attempts at UV, but these include trusted components and stop short of meeting our definition of verifiability. The technological barrier here is so great that some privacy researchers believe traditional systems may be unable to combine both privacy and verifiability.[15] It is worth noting that some declare the same about digital voting.[16] However, given the immaturity of research into this question and the rapidity of technological advancement, the potential of REV remains an open research question.

This is not to say that traditional voting is usually insecure or fraudulent. Rather, it is to say that the source of integrity of paper voting systems stems from trust in the authority administering the vote. In high-stakes democratic processes, we might strive for a level of verifiability that places no trust in the parties administering the election. Aside from the security of voting itself, the "capacity to ensure the effective administration of the electoral process is crucial to maintain[ing] public confidence"[17] in democracy. In a time when only 44% of people globally are satisfied with democracy, increasing public confidence in democratic processes themselves is critical.[18] Thus, a

lack of IV, UV, or E2E verifiability should be seen as a major weakness in any voting system.

As we've noted with the case of voter suppression, traditional voting systems are typically vulnerable to small-scale censorship. Malicious third-parties and election officials alike can target individuals with violence, threats, or discouragement. In addition, inaccessible polling stations can lead to a soft-censorship of voters who live far away, have mobility issues, are unable to leave work to vote during the allotted time, et cetera. REV systems drastically reduce the attack surface for individual censorship and discouragement, but they can be vulnerable to wide-scale censorship if not specifically designed with network-level censorship in mind.

Non-repudiation is similarly missing from any traditional voting system that allows an individual to miscount or discard a ballot while tallying. If a system has implemented E2E verifiability, however, voters can ensure that their ballot has not been altered or erased. Systems can ensure non-repudiation by allowing voters to verify the receipt of their ballot in real-time and re-submit a vote if it has not been correctly counted. Correct execution is difficult to ensure in large-scale traditional systems and may not be possible without some trusted components. Smaller-scale elections can ensure correct execution with a "public square" method in which each ballot is examined and counted by all community members in a public setting. REV systems can scale this approach with a public and distributed computation of vote results.

Moving Forward

Those of us working on Vocdoni, an open-source REV infrastructure, believe we have developed a way to address each of these problems inherent to traditional voting systems. We claim our design enables end-to-end verifiability, alongside levels of anonymity, privacy, and censorship-resistance that, to the best of our knowledge, rival the best of paper voting systems. Perhaps more inspiring to us, however, is a vision of voting models that leave society better equipped to transform our democratic practices. *What if we had a system in which everyone could vote from their mobile phone and open a browser to verify the results of an election, all without having to place trust in any central authority?* In addition to solving some of our current problems, this system would enable civic participation to fundamentally shift as trust in collective decision-making grows and the barriers to direct democracy shrink.

In order to function well, a democracy must expand far beyond sparse representative elections. Democracy can include more frequent and local elections, voting directly on

issues, participatory budgeting, petitions, even union participation and social movement organizing. However, the prevailing image of democracy is stymied in part by a participation system that limits most citizens to a small subset of these activities. In part, this is because of the high-cost, low-frequency model discussed above. It would be prohibitively expensive to administer a paper election once a month, not to mention turning out residents to vote on lower-stakes, local issues. Voting that is cheaper, both to administrators and end-users, and that assures equal or greater security to existing ones, could flip the low-participation paradigm on its head. There would certainly still be social and political barriers to overcome. However, such technology at least opens the door to a whole new set of direct, fluid, participatory, and equitable forms of decision-making.

Even the way we tally votes has substantial implications on elections. Excitement has grown around alternative voting schemes such as ranked-choice voting (RCV), proportional representation, Condorcet-type, approval, quadratic voting, and more.[19] According to FairVote, 22 jurisdictions in the US used RCV in their most recent election.[20] But this adoption is limited by a high technological cost to both administrators and voters. Leveraging the benefits of a system like RCV, along with an intuitive user interface, is technologically infeasible on top of antiquated paper tabulation systems.[21] Furthermore, each of these methods has its strengths and weaknesses, and it is clear that no one of them is the best for every situation. Rather than investing in a rigid system that supports one of these models, we might imagine a voting system with sufficient flexibility to support the addition of novel election types at a low cost.

Our philosophy for the Vocdoni project goes beyond new democratic tools; we envision a new set of fundamental rights, namely *privacy* and *information.* In the context of voting, these rights might correspond to anonymous voting and E2E verifiability, respectively. If we take these rights for granted, it is not enough to trust an authority to preserve ballot anonymity or ensure election integrity manually. The right to information, furthermore, could be extended to the right to communicate and make decisions free from state censorship. This right is clearly threatened in any country where a central state authority must host the only legally valid decision-making processes.

One such situation might be a direct-democracy referendum for independence for a subset of a nation’s territory. Referenda of this sort have increased in prevalence dramatically since the 1990s, corresponding to a decrease in armed independence

movements, but are "not usually politically or legally granted by states."[22] One might look to the case of the 2017 Catalonian referendum as a recent example of this, in which a regional independence vote organized by local officials was declared illegal and met with violent police force at polling sites.[23] Regardless of one's view of any particular conflict, it is evident that in-person voting, in this case, was unable to provide a baseline of censorship resistance. The rights of a regional population to express their collective will could be easily undermined, partly due to the in-person and centralized nature of the voting infrastructure.

Censorship-resistant voting in the form of a digital poll certainly would not remove all barriers to collective decision-making in high-stakes situations such as independence referenda. But such technology could restrict the ease with which a dominating force can censor polling and increase public trust both internal to a territory and globally. REV might act as a tool that can help ensure the rights to voting and information and free-up resources to be used in other sites of political struggle.

Barriers to Remote Electronic Voting

The barriers to the mass adoption of REV technology are three-fold: technological, social, and political.

Technological Barriers

None of the theoretical benefits of a philosophy of anonymous and universally verifiable voting system can be realized until such a system has been implemented and tested. These two properties, in fact, may be the most significant hurdles to building such a system. Some cryptographers believe E2E verifiability to be "at odds with" ballot secrecy altogether.[24] This concern makes sense- it seems impossible to both verify that each ballot is valid and counted correctly and provide absolute anonymity between a voter, their ballot, and the contents of that ballot. As we will explore, however, recent innovations in the field of cryptography may provide an elegant solution to this apparent contradiction.

Bundled with ballot secrecy is the challenge of vote-buying and coercion, in which a group sways the results of an election by threatening or bribing voters to vote for a specific candidate. The primary defense against this type of attack is usually assumed to be Receipt-Freeness (RF). If a voter cannot prove the contents of their ballot to an outsider once an election has ended, how could they possibly be bribed to vote a certain way? Unless the malicious actor is peering over their shoulder at the time of voting, they could accept the bribe (or threat) and vote however they want. REV may

add security by enabling users to override their vote until an election ends, so they can vote one way in front of a threatening party and then change their vote later. Unfortunately, there are still limits to this theory; vote-buying has been shown to be effective even in environments that guarantee RF, possibly due to social or psychological factors.[25] Digital voting differs from traditional voting with respect to vote-buying in its vulnerability of scale. The cost to influence voters may be much lower if it can be done primarily digitally and in an automated manner, although this tactic could also reduce the social effect noted above.

REV is much more resistant to local police-level or "mob" censorship, especially that against individual voters. However, it introduces the possibility of non-state censorship in the form of network attacks. Therefore, online voting infrastructure should be secured and protected against Denial-Of-Service (DOS) and other common attacks. Beyond standard measures, however, censorship-resistant infrastructure must also be protected from Internet Service Providers (ISPs) and state-level actors. This defense can be achieved partly through the use of decentralized technologies such as blockchains and peer-to-peer networks. One might turn to InterPlanetary File System (IPFS), for example, which grew in prominence as a distributed source of Wikipedia.com that evaded censorship after Turkey banned the website.[26] Decentralized technologies can leverage several properties[27] unavailable to traditional web infrastructure, making them incredibly resistant to censorship but also uniquely suited for privacy-oriented systems.

The feasibility of any voting system to meet all technical requirements is still an open research question. Especially considering this fact, any design that seems to solve the challenges listed above must be thoroughly vetted and audited by outside parties. This need is made particularly clear by the case of Voatz. This proprietary voting technology became the first internet-only voting app to be used in "high-stakes U.S. federal elections" and used a blockchain to secure & tally votes.[28] Voatz came under fire, however, when a 2020 study by MIT security researchers found that their system was susceptible to vulnerabilities that could allow remote attackers to suppress, de-anonymize, read, or alter ballots.[29] On the one hand, open-source technology assuages fears of unknown exploits. A publicly available and sufficiently community-oriented codebase might receive audits from programmers and users, a practice that is likely to catch security bugs much faster than maintainers of a proprietary codebase might.[30] On the other hand, regular third-party audits from respected security firms are still necessary before a system can be used in high-stakes scenarios.[31]

On top of network- and protocol-level challenges, the client application itself needs to be secure. Mobile, web, and desktop applications each have their own sets of security concerns that need to be addressed. The core issue at hand, however, is that a compromised device could compromise a voter's ballot that they submit. Device security is an uphill battle, and one can never be absolutely certain—but applications can use techniques to scan a device for malware, block key-logging of passcodes, and block screen-recording. In high-stakes environments, any e-voting system must be developed under the assumption of insecure end-user devices.[32] Thus, these technical defenses become indispensable, but should be supplemented with individual verifiability of the system as a whole; the voting application can encourage users to verify, from a separate device, that their vote has been cast as intended.

On top of these primary technological challenges, REV must also include a widely accessible and intuitive interface. User testing akin to successful online platforms is necessary to confirm that the least technically gifted members of society and those with disabilities that affect the usability of a platform can vote easily. Other measures such as in-person voting, vote delegation, and extensive voter support can supplement platform usability.

Social Barriers

The social challenges to the adoption of REV may be even more significant than the technical ones. Alongside the issue of accessibility is one of technical education and availability. Technological literacy might be thought of as the widespread ability to use devices and learn new software. This form of literacy is crucial to e-voting, as a society with low levels of device literacy would not have the resources to provide support to all voters who need help using the technology. Technological literacy, however, might also refer to knowledge of how to "overcome the inadequacies of interrupted internet access" in environments where access to devices and connectivity is not guaranteed.[33] However, this type of literacy is unable to allow users to overcome structural internet access problems such as "pricing and data allowances of inferior rural services."[34] Accessibility and technical education, therefore, necessarily include high-quality broadband availability and free device access for those who need it. As mentioned above, alternative options to interfacing directly with a device must be available, but only as a backup measure. A government that implements digital voting before ensuring this form of technological literacy and availability would likely introduce greater disparities to voting access.

In order for a governance model to be successful, it should garner high levels of public trust. We have identified that public confidence in elections is already lacking. While REV technology has the opportunity to build trust, it also risks compounding election distrust with technology distrust. Distrust here is two-pronged; a REV system could gain trust among security experts and election administrators, but the vast majority of voters will never lay eyes on the code or design. Technologies that increase the efficiency of civic processes by replacing older (and less digital) ones can often risk diminishing community trust and engagement.[35] Researchers note that, when attempting civic engagement with new technology, it is vital for leaders to understand the "logic of Trust" used by a community and to work with community members to build reputation.[36] In the context of REV, this would be an immense task. The "community" targets would include the general public, media, local and regional elected officials, community organizations, and more. Rather than presenting REV as perfect, a trust-building process should engage with the current problems with voting technology and educate the public about the issues that will, and will not, be solved with a voting system.

Political leaders and administrators of public elections have an additional responsibility beyond building trust. Officials should understand which properties are desirable, and why some solutions might be better than others. For example, those choosing a voting system on behalf of the public should be able to identify the tradeoffs between Free and Libre Open Source Software (FLOSS) versus proprietary software. This responsibility, however, will not be fulfilled or widely accepted unless it is strongly advocated for.

Even using strategies that have been researched and tested in the field of trust-building in civic technologies, a smooth transition to REV would have to be gradual.[37] Ideally, the technology would first be deployed at lower-stakes and smaller scales. Voters could have a chance to become acclimated to the experience of voting digitally while receiving education and support from local leaders, years before this voting grows to a national scale.

Legal Barriers

REV will likely have to adapt to local regulations in each jurisdiction in which it is employed. The U.S. Election Assistance Commission (EAC), for example, recommends a set of guidelines any voting system should follow, from the method and conditions necessary for printing ballots to the text size and font required of a digital voting system.[38] The EAC, additionally, indexes dozens of recommendations, testing

procedures, and requirement checklists for voting systems published by individual states and municipalities.[39] One can imagine the complexity of the task of ensuring compliance with all local election regulations in the U.S. alone, not to mention the rest of the world. Mass adoption requires a localized approach that works with regulators to adapt to their specificities and advocates for standardized election protocol regulations.

A Hacker's Exploration

Vocdoni's voting protocol appears to be the first and only voting system that provides anonymity alongside E2E verifiability and advanced mechanisms for reducing coercion. No production-quality software fulfills all of these properties. Nevertheless, we have composed a set of cutting-edge cryptographic tools on top of a specialized voting-specific blockchain (Vochain) into a free and open-source proof-of-concept that seems to bridge the contradictions between anonymity and verifiability. The base of this modular implementation, the Vochain, is a distributed Byzantine fault tolerant ledger that validates and processes ballots.[40] Thanks to its decentralized design, the entire protocol can execute on machines owned by many different parties. More than two-thirds of these parties would need to coordinate to successfully block computation or censor specific voting transactions. This logic is the same as that which is used on some public blockchains to secure high-stakes financial transactions (Cosmos, Polkadot, xDAI). The technology allows us to trust the computation as a whole without placing trust in any individual machines on the network (correct execution). Combined with other decentralized technologies such as IPFS, this enables a high default level of censorship resistance to network-level attacks.[41]

Census

Also key to our implementation is the use of Merkle Trees to represent voter census. A *Merkle Tree* is a data structure that contains many elements- in this case, cryptographic keys associated with unique voters. These elements are hashed together several times to generate the Merkle Root, a single value representing the tree as a whole. Thus, a user can prove that their public key belongs in the census Merkle Tree without knowing any other public key included in the census.

An alternative to the Merkle Tree census is the use of a Credential Service Provider (CSP) to authenticate voters. Under this model, a CSP can authenticate each user throughout a voting process, based on some arbitrary criteria (e.g., a digital certificate issued by a Certificate Authority (CA)). After the authentication, the user sends the

CSP a new temporary random generated public key for the election, which the CSP computes a blind signature on.[42] Users can then unblind this signature and cast a vote with their unblinded CSP signature as proof. This allows voters to demonstrate their validity with anonymity. The tradeoff here is that a service must exist to authenticate users throughout the voting process. Additionally, the CSP administrator could time-correlate a voter's authentication request with their vote cast on the public blockchain, de-anonymizing this vote. A latency mixnet mechanism could be used to deter this attack.[43]

Anonymity

Our voting protocol's second piece of cutting-edge cryptography is a Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK). This powerful tool can generate a Zero-Knowledge Proof (ZKP), which is as counterintuitive as it sounds- a ZKP proves some property about a piece of information without revealing the contents of that information itself. We use zk-SNARKs to verify the Merkle Proofs generated by each voter when casting their vote. The Merkle Proof itself, therefore, can remain private. A user can deterministically prove that they belong in the census of eligible voters without revealing any information about their identity.

One limitation to our use of zk-SNARKS is their lack of quantum resistance. Our design as a whole has not yet been audited for quantum resistance, and it is possible that, in the future, quantum computing could evolve algorithms to crack the anonymity provided by a ZKP. Quantum-resistant analogs to the cryptography used in our design, such as a post-quantum zk-SNARK, remain an open (and promising) field of research. In the meantime, a private voting blockchain could be used for high-stakes processes where anonymity takes precedence over universal verifiability.

Verifiability

The voting protocol achieves both individual verifiability and eligibility verifiability with the use of a unique nullifier used as an input to each voter's ZKP. This nullifier is derived from the voter's secret key and the process ID. The nullifier allows voters to identify the transaction containing their ballot, whose contents anyone can examine. We designed the zk-SNARK circuit to ensure that only that voter's secret key can generate the nullifier and the ZKP associated with their vote package, so any user can be sure that their vote was counted as cast.

The use of a Merkle Census Tree enables Universal Verifiability, the third type of voting system verifiability. While the ZKP hides the identity of any one voter, it proves

without a doubt that that voter possesses a secret key that belongs in the official census of eligible voters. It also allows the Vochain to ensure that only one valid vote can be cast by each eligible voter. At the same time, however, non-repudiation can be achieved by enabling a voter with a valid proof to override their vote while a process is active, only counting the last valid vote for each nullifier (this feature is compatible with our design, but not yet implemented). When a voting process ends, therefore, any party can verify the set of ZKPs and be sure that each vote that was cast is a valid vote.

Proof-of-Concept: Absolute Anti-Coercion

The design presented above achieves complete anonymity and E2E verifiability, but it lacks anti-coercive properties. Under this scheme voters can provide a proof that demonstrates which vote envelope was cast by them both during and after an election, thereby eroding BP, RF, and CR. If a malicious third party is able to interact individually with voters, they can offer a reward in exchange for a valid proof that a voter has cast a certain ballot. Thus, automated vote-buying is a risk here.

In order to achieve complete anti-coercion while keeping our design principles, we designed a proof-of-concept using a second layer of zk-SNARKs. This second zk-SNARK is used to batch votes and verify their correctness without revealing the contents of any single vote envelope. The design functions as follows: first, voters submit their anonymized vote envelopes, along with their census ZKPs, to a Relayer through a private transport channel (such as HTTPs). The Relayer aggregates vote envelopes and then validates and computes them in batches (i.e 20 envelopes at a time) to produce a second ZKP. This proof can be verified given the list of nullifiers and vote packages from the batch, which are randomly ordered in order to detach a nullifier from its specific vote package. The new ZKP and the mixed input list will be stored on the public voting blockchain. The ZKP thus guarantees that it has correctly aggregated results on a set of votes that were uniquely cast by valid voters in the census. As the set of results combines many votes, no individual ballot contents can be revealed despite all votes being cryptographically verified.

In this scenario, voters are still able to verify that their vote has been processed, with cryptographic proof that their ballot has been counted exactly as it was created. No outsider, however, can determine what choices were selected by a specific voter. At the same time, the election's traceability and transparency properties are preserved. The tradeoff here is that, although users can verify that the ballot they created was counted correctly, they cannot inspect the contents of their ballot once it has been submitted. The only weak point, therefore, is in the actual creation of the vote

package. If a user has a compromised device, and performs no checks on the submission of their ballot, they would have no guarantee that the ballot they intended to cast matches the ballot submitted to the relay. Users could, however, inspect the network packets sent to the relay from their device and ensure that the ballot was submitted with integrity (tooling can be provided to assist with this verification step). From this point on, they can be sure that their ballot is not altered. This design therefore maintains E2E verifiability, thus reducing the assumed incompatibility between anonymity and verifiability into merely a question of optimizing for usability.

Conclusion

There is no doubt that the mass adoption of remote electronic voting systems will be lengthy and iterative. From infrastructural and application-level challenges to social and political ones, innovative solutions must be discovered and presented clearly and openly to stakeholders (all voters). The designs we have presented are intended to serve as a starting point for this process. We have shown that it is indeed possible to combine verifiability with privacy in a REV system that tackles many of the problems endemic to our current voting systems.

Technology alone cannot solve the problems democracy faces today, whether or not a "solution" exists in the first place. Legal and social barriers to active and fair civic participation begin and end far from the ballot box, and a new voting system will not simply upending existing power structures. What an innovation such as universally verifiable remote voting can do, however, is to substantially contribute to the democratization of many forms of governance by providing everyday people with a tool to express their collective will. The ability of a population to self-organize in a democratic and participatory manner is necessary, but not sufficient, to the task of undoing unjust hierarchies. And as we move forward into a (hopefully) post-pandemic era, cutting-edge digital technology presents the best opportunity to achieve direct governance at a population scale.

References

Blais, André, Jean-François Daoust, Ruth Dassonneville, and Gabrielle Péloquin-Skulski. "What Is the Cost of Voting?" *Electoral Studies* 59 (June 1, 2019): 145–57. *https://doi.org/10.1016/j.electstud.2019.02.011*.

Burnett, Craig M., and Vladimir Kogan. "Ballot (and Voter) 'Exhaustion' under Instant Runoff Voting: An Examination of Four Ranked-Choice Elections." *Electoral Studies* 37

(March 1, 2015): 41–49. https://doi.org/10.1016/j.electstud.2014.11.006.

Clark, Alistair. "The Cost of Democracy: The Determinants of Spending on the Public Administration of Elections." *International Political Science Review* 40, no. 3 (June 1, 2019): 354–69. https://doi.org/10.1177/0192512118824787.

Corbett, Eric, and Christopher A. Le Dantec. "'Removing Barriers' and 'Creating Distance': Exploring the Logics of Efficiency and Trust in Civic Technology." *Media and Communication* 7, no. 3 (August 6, 2019): 104–13. https://doi.org/10.17645/mac.v7i3.2154.

Damnjanović, Ivana. "Democratic Innovations in Serbia: A Misplaced Trust in Technology." *Contemporary Politics* 25, no. 1 (January 1, 2019): 111–27. https://doi.org/10.1080/13569775.2018.1544028.

De', Rahul, Neena Pandey, and Abhipsa Pal. "Impact of Digital Surge during Covid-19 Pandemic: A Viewpoint on Research and Practice." *International Journal of Information Management* 55 (December 2020): 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171.

Epperly, Brad, Christopher Witko, Ryan Strickler, and Paul White. "Rule by Violence, Rule by Law: Lynching, Jim Crow, and the Continuing Evolution of Voter Suppression in the U.S." *Perspectives on Politics* 18, no. 3 (September 2020): 756–69. https://doi.org/10.1017/S1537592718003584.

FairVote.org. "Alternatives to RCV." FairVote. Accessed August 24, 2021. https://www.fairvote.org/alternatives.

FairVote.org. "Ranked Choice Voting / Instant Runoff." FairVote. Accessed August 24, 2021. https://www.fairvote.org/rcv.

Fischer-Hbner, Simone, and Stefan Berthold. "Chapter 53 - Privacy-Enhancing Technologies." In *Computer and Information Security Handbook (Third Edition)*, edited by John R. Vacca, 759–78. Boston: Morgan Kaufmann, 2017. https://doi.org/10.1016/B978-0-12-803843-7.00053-3.

Freeman, Julie, Sora Park, and Catherine Middleton. "Technological Literacy and Interrupted Internet Access." *Information, Communication & Society* 23, no. 13 (November 9, 2020): 1947–64. https://doi.org/10.1080/1369118X.2019.1623901.

Gordon, Eric. “Civic Organizations and Digital Technologies in an Age of Distrust.” *Media and Communication* 7, no. 3 (2019): 54–56. http://dx.doi.org.grinnell.idm.oclc.org/10.17645/mac.v7i3.2385.

Gordon, Eric, and Rogelio Alejandro Lopez. “The Practice of Civic Tech: Tensions in the Adoption and Use of New Technologies in Community Based Organizations.” *Media and Communication* 7, no. 3 (August 6, 2019): 57–68. https://doi.org/10.17645/mac.v7i3.2180.

Herron, Michael C., and Daniel A. Smith. “Postal Delivery Disruptions and the Fragility of Voting by Mail: Lessons from Maine.” *Research & Politics* 8, no. 1 (January 2021). http://dx.doi.org.grinnell.idm.oclc.org/10.1177/2053168020981434.

Jie, Koh Wei. “Release Announcement: MACI 1.0.” *Privacy & Scaling Explorations* (blog), October 12, 2021. https://medium.com/privacy-scaling-explorations/release-announcement-maci-1-0-c032bddd2157.

Jonker, Hugo, Sjouke Mauw, and Jun Pang. “Privacy and Verifiability in Voting Systems: Methods, Developments and Trends.” *Computer Science Review* 10 (November 1, 2013): 1–30. https://doi.org/10.1016/j.cosrev.2013.08.002.

Laughlin, Nick, and Peyton Shelburne. “Tracking Voter Trust in the American Electoral System.” Morning Consult, January 27, 2021. https://morningconsult.com/form/tracking-voter-trust-in-elections/.

López, Jaume, and Marc Sanjaume-Calvet. “The Political Use of de Facto Referendums of Independence The Case of Catalonia.” *Representation* 56, no. 4 (October 1, 2020): 501–19. https://doi.org/10.1080/00344893.2020.1720790.

McKeever, Amy. “Voter Suppression Has Haunted America since It Was Founded.” *National Geographic*, August 21, 2020. https://www.nationalgeographic.com/history/article/voter-suppression-haunted-united-states-since-founded.

Medina, Manel. “Governmental Censorship of the Internet: Spanish vs. Catalans Case Study.” *Library Trends* 68, no. 4 (2020): 561–75. https://doi.org/10.1353/lib.2020.0011.

National Conference of State Legislatures. “Alternative Voting Systems,” June 25, 2020. https://www.ncsl.org/research/elections-and-campaigns/alternative-voting-systems.aspx.

National Security Agency. “Embracing A Zero-Trust Security Model,” February 2021.

Park, Sunoo, Michael Specter, Neha Narula, and Ronald L Rivest. “Going from Bad to Worse: From Internet Voting to Blockchain Voting.” *Journal of Cybersecurity* 7, no. 1 (January 1, 2021). https://doi.org/10.1093/cybsec/tyaa025.

Payne, Christian. “On the Security of Open Source Software.” *Information Systems Journal* 12, no. 1 (2002): 61–78. https://doi.org/10.1046/j.1365-2575.2002.00118.x.

Pew Research Center. “Globally, Many Are Dissatisfied with the Way Democracy Works and Frustrated with Elected Officials but Still Value Voting.” Pew Research Center, February 25, 2020. https://www.pewresearch.org/global/wp-content/uploads/sites/2/2020/02/PG_2020.02.27_global-democracy_00-4.png.

Pieters, Wolter. “What Proof Do We Prefer? Variants of Verifiability in Voting.” Accessed August 23, 2021. https://www.academia.edu/1059439/What_proof_do_we_prefer_Variants_of_verifiability_in_voting.

Porup, J. M. “Online Voting Is Impossible to Secure. So Why Are Some Governments Using It?” CSO Online, May 2, 2018. https://www.csoonline.com/article/3269297/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html.

Qiu, Linda. “Fact-Checking Falsehoods on Mail-In Voting.” *The New York Times*, January 5, 2021, sec. U.S. https://www.nytimes.com/article/fact-checking-mail-in-voting.html.

Smyth, Ben, Mark Ryan, Steve Kremer, and Mounira Kourjieh. “Towards Automatic Analysis of Election Verifiability Properties.” In *Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security*, edited by Alessandro Armando and Gavin Lowe, 6186:146–63. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-16074-5_11.

Specter, Michael A, James Koppel, and Daniel Weitzner. “The Ballot Is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections,” n.d., 20.

The IPFS Team. “Uncensorable Wikipedia on IPFS.” IPFS Blog & News, May 4, 2017. https://blog.ipfs.io/24-uncensorable-wikipedia/.

U.S. Election Assistance Commission. “Managing Election Technology.” Accessed September 1, 2021. *https://www.eac.gov/voting-equipment/managing-election-technology*.

U.S. Election Assistance Commission. “Voluntary Voting System Guidelines,” February 10, 2021. *https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines*.

Vasserman, Eugene Y. “Towards Freedom of Speech on the Internet: Censorship-Resistant Communication and Storage.” *ProQuest Dissertations and Theses*. Ph.D., University of Minnesota, 2010. *http://www.proquest.com/docview/635499381/abstract/850A3325DD284910PQ/1*.

Zhao, Wenbing, and Wenbing Zhao. *Building Dependable Distributed Systems*. Somerset, United States: John Wiley & Sons, Incorporated, 2014. *http://ebookcentral.proquest.com/lib/grinnell-ebooks/detail.action?docID=1650851*.

Footnotes

1. Epperly et al., “Rule by Violence, Rule by Law,” 756. ↩
2. McKeever, “Voter Suppression Has Haunted America since It Was Founded.” ↩
3. Epperly et al., 759. ↩
4. De’, Pandey, and Pal, “Impact of Digital Surge during Covid-19 Pandemic,” 1. ↩
5. Qiu, “Fact-Checking Falsehoods on Mail-In Voting.” ↩
6. Herron and Smith, “Postal Delivery Disruptions and the Fragility of Voting by Mail,” 9. ↩
7. Clark, “The Cost of Democracy,” 357. ↩
8. Clark, 364. ↩
9. Blais et al., “What Is the Cost of Voting?,” 150. ↩
10. Laughlin and Shelburne, “Tracking Voter Trust in the American Electoral System.” ↩

11. “Online voting” typically refers to a system that transmits votes over the internet. “Digital voting” or “e-voting” refers to systems in which votes are cast using a computer. We use the term “remote e-voting” (REV) to refer to a system that is both online and digital. ↩
12. Jonker, Mauw, and Pang, “Privacy and Verifiability in Voting Systems,” 4. ↩
13. Smyth et al., “Towards Automatic Analysis of Election Verifiability Properties,” 2. ↩
14. Jie, “Release Announcement: MACI 1.0.” Privacy & Scaling Explorations (blog), October 12, 2021. ↩
15. Jonker, Mauw, and Pang, 3. ↩
16. Porup, “Online Voting Is Impossible to Secure. So Why Are Some Governments Using It?” ↩
17. Clark, 355. ↩
18. Pew Research Center, “Globally, Many Are Dissatisfied with the Way Democracy Works and Frustrated with Elected Officials but Still Value Voting.” ↩
19. FairVote.org, “Alternatives to RCV”; National Conference of State Legislatures, “Alternative Voting Systems.” ↩
20. FairVote.org, “Ranked Choice Voting / Instant Runoff.” ↩
21. Burnett and Kogan, “Ballot (and Voter) ‘Exhaustion’ under Instant Runoff Voting,” 42. ↩
22. López and Sanjaume-Calvet, “The Political Use of de Facto Referendums of Independence: The Case of Catalonia,” 502. ↩
23. López and Sanjaume-Calvet, 505. ↩
24. Park et al., “Going from Bad to Worse,” 8. ↩
25. Pieters, “What Proof Do We Prefer?,” 2. ↩
26. The IPFS Team, “Uncensorable Wikipedia on IPFS.” ↩

27. “Uncensorable Wikipedia on IPFS”, for example, mentions that the distributed file-sharing system is able to evade censorship by enabling content to be served by any participant in the network. As long as any node is working, anyone connected to a gateway is able to download the content, which is cryptographically verified. This enables the use of IPFS in partitioned networks that may not be connected to the global web. It also allows for extremely flexible resistance to DOS attacks, as as soon as one gateway or node is blocked, users of the network can switch to another. No Domain Name-Service (DNS) or Certificate Authority System is required, cutting out two commonly used points of censorship by state and ISP actors in traditional (centralized) technologies. ↩
28. Specter, Koppel, and Weitzner, “The Ballot Is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections,” 1. ↩
29. Specter, Koppel, and Weitzner, 2. ↩
30. Payne, “On the Security of Open Source Software,” 12. ↩
31. U.S. Election Assistance Commission, “Voluntary Voting System Guidelines,” 6. ↩
32. National Security Agency, “Embracing A Zero-Trust Security Model.” ↩
33. Freeman, Park, and Middleton, “Technological Literacy and Interrupted Internet Access,” 1948. ↩
34. Freeman, Park, and Middleton, 1960. ↩
35. Gordon and Lopez, “The Practice of Civic Tech: Tensions in the Adoption and Use of New Technologies in Community Based Organizations.” 108. ↩
36. Gordon and Lopez, 108. ↩
37. Gordon and Lopez uncover three strategies for how public officials can build trust with community members. They recommend “Historicized Engagement”, “Focusing on Experience” (improving the human experience of interacting with government officials), and “Mediating Expectations.” ↩
38. U.S. Election Assistance Commission, “Voluntary Voting System Guidelines.” ↩
39. U.S. Election Assistance Commission, “Managing Election Technology.” ↩

40. Zhao, *Building Dependable Distributed Systems*. ↩

41. The IPFS Team, “Uncensorable Wikipedia on IPFS.” ↩

42. Fischer-Hbner and Berthold, “Chapter 53 - Privacy-Enhancing Technologies.” 769. ↩

43. Fischer-Hbner and Berthold. 765. ↩