TH 1ESTATE

Grassroots Democracy

Anyone can now prove that a majority of the country agrees with a particular petition statement.

Abstract:

A new technique offers the best of surveys, initiatives, juries, protests, and petitions—while overcoming their shortcomings in demonstrating the public will. With it, anyone can now for the first time irrefutably prove that a majority would sign on to particular petition language. All that's needed is about $1,000 worth of supplies and a postal mailing list for the country or region.

The list is sampled in a way that is irrefutably random and un-manipulatable. Those receiving ballots are given time to research and submit their decision securely online. They know that their input is significant because of the limited sample size. They also know that it will be counted correctly, because the security is

superior to that of conventional automated election systems. In fact, anyone online can verify that those creating and mailing the paper ballots cannot influence selection, manipulate outcome, or link responses to addresses. Vote-buying, an unsolved problem in all other current non-polling-place balloting, is effectively solved by decoy ballots. Economic incentives can be provided to those casting ballots without any possible linkage to their response.

The needed supplies are readily available and have already been tested, the server backend can be part of any blockchain, and the poll can be announced only after the ballots are mailed, making interference all but impossible.

Introduction

The novel technique introduced here offers the central advantages, but avoids the limitations and failings, of established techniques such as surveys, initiatives, juries, protests, and petitions:

- **Surveys have the advantage of timeliness, but they don't allow deliberation, they are restricted in many countries, and they are widely distrusted, typically because of potential bias, recent damaging failures, or lack of both privacy and transparency.**

- **Ballot initiatives have the advantage of providing agreed-upon language for subsequent legislation, but are available at the national level only in Switzerland, involve significant signature collection cost and delays, are often multi-issue bundles, and are known to be influenceable by all manner of targeted messaging.**

- **Juries have the advantage of evoking dedication from jurors and being able to compensate them at least modestly, but by law they do not set public policy and are known to be easily manipulated through culling, through what is told jurors, and through communication among jurors.**

- **Protests and similar expressions of public sentiment have the advantage that they can be initiated by grassroots efforts, but are increasingly subject to escalation/retaliation, can negatively impact public opinion, and are ineffective at convincing governments unless near-majority support is evidenced.**

- **Petitions have the advantage of irrefutability, but they have no privacy, they are costly, and sign-on by a majority is needed for them to be convincing—yet evidencing this level of support has never been achievable at scale until now.**

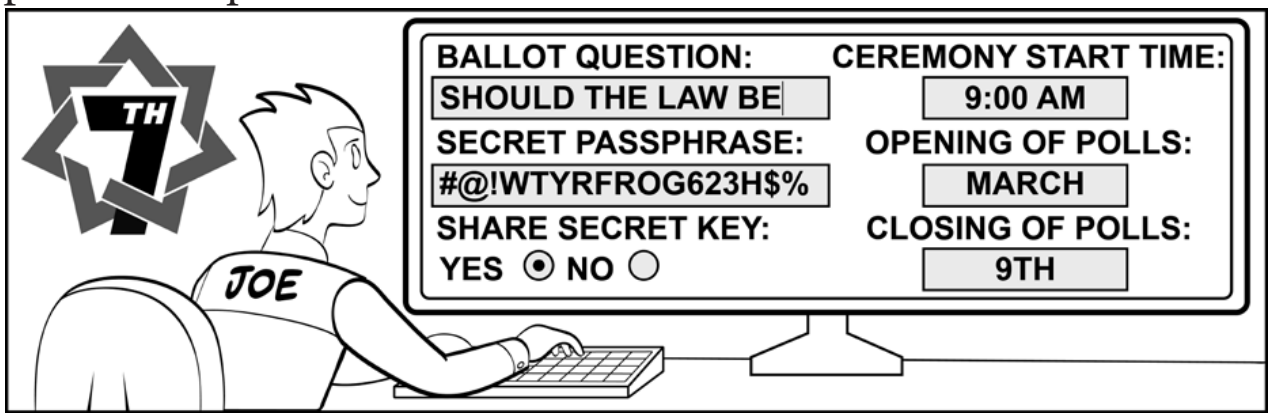
The technique introduced combines the timeliness of surveys, the independent deliberation and precise language of ballot initiatives, the dedication of jurors (with options for enhanced compensation), greater ease of grassroots initiation than protests, and irrefutability and privacy rivaling those of elections. It is the first practical means for establishing the true public will.

From a technical security perspective, the system is also the first (apart from those limited to use in a single room) capable of proving majority support, by providing both public verifiability of the outcome and ballot secrecy, all without relying on unproven mathematical assumptions. The techniques introduced to inhibit vote selling and incentivise voters are also novel.

The Fourth Estate has long been synonymous with media such as newspapers and television. Various Internet-based media have more recently been dubbed the Fifth and Sixth Estate, but the seventh has been left unassigned. Here, the 7th Estate is laid claim to on behalf of the new possibility introduced here—publicly verifiable proof of the public will.

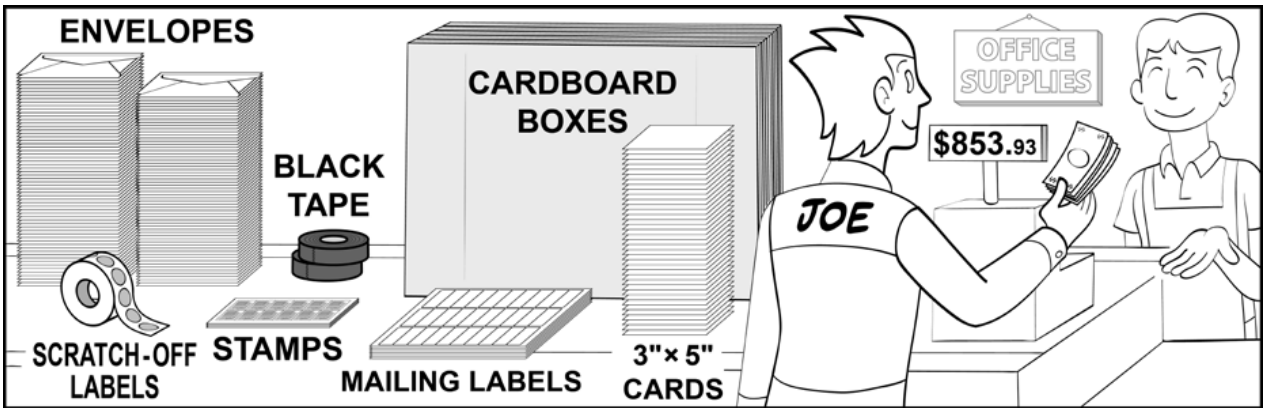
Getting Started

In order to prepare a proof of majority support, “Joe” obtains the needed open-source software **(https://github.com/xx-labs/7th_estate)**, installs it, and runs it. He then enters the language he wants decided on along with three dates and times: opening of polls; close of polls, allowing adequate time for deliberation; and the start time for a pre-poll “ceremony' (described below). The software also obtains a secret passphrase from Joe, which it uses to create and encrypt parts of the poll data.

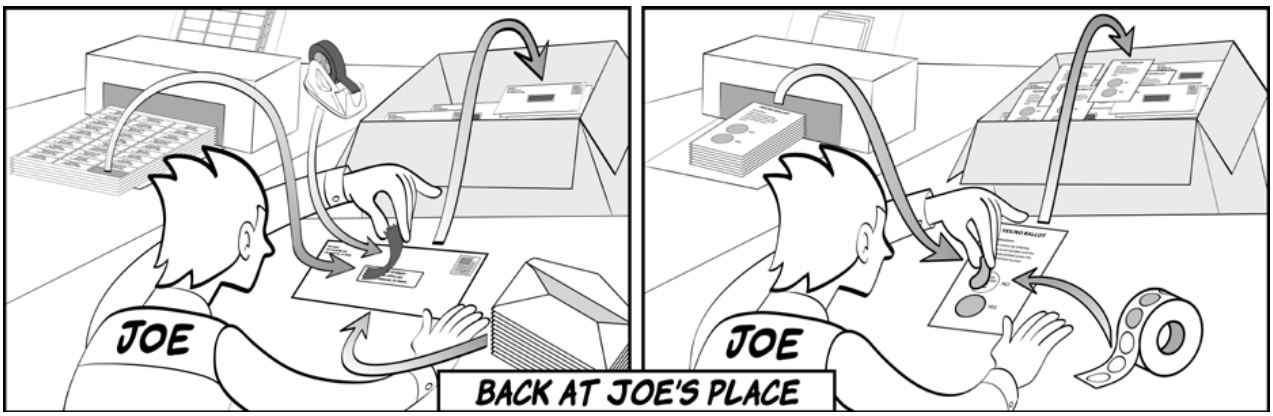


The software then commits all the data as a hash to one or more blockchains. Even though the fact that something has been committed to in this way is public, nothing more need become public at this time, neither any details of the values committed nor even that the commitment relates to a poll.

Joe also needs some commonly available supplies. He purchases 1,000 each: postage stamps, cards to print ballots on (3"×5"/A6 or 4"×6"/A5), envelopes to mail ballots in (#7/C6 or #10/C5), and printable mailing labels (e.g., Avery 5520). He also needs 2,000 scratch-off labels (e.g., “ScratchTix” 1" circles), two rolls of opaque black tape (e.g., 1" Scotch 235), one roll of 3" packing tape, and two corrugated cardboard boxes (double wall 24" cubes).



The software generates the ballots and address labels, which Joe prints using the supplies. Next, Joe affixes the labels and stamps on the envelopes and hides each address with a piece of the opaque black tape. He also prints the ballots on the cards and covers the two printed "vote-codes" on each ballot card with separate scratch-off dots.



Joe avoids maintaining any record of the addresses or codes printed. If this data were to fall into the wrong hands, those limited misuses that are not blocked would likely be detected and discredit him and the poll. Even if Joe were, for instance, to record the addresses printed, he would still not know which ballot was sent to which address. But if he were to try to use

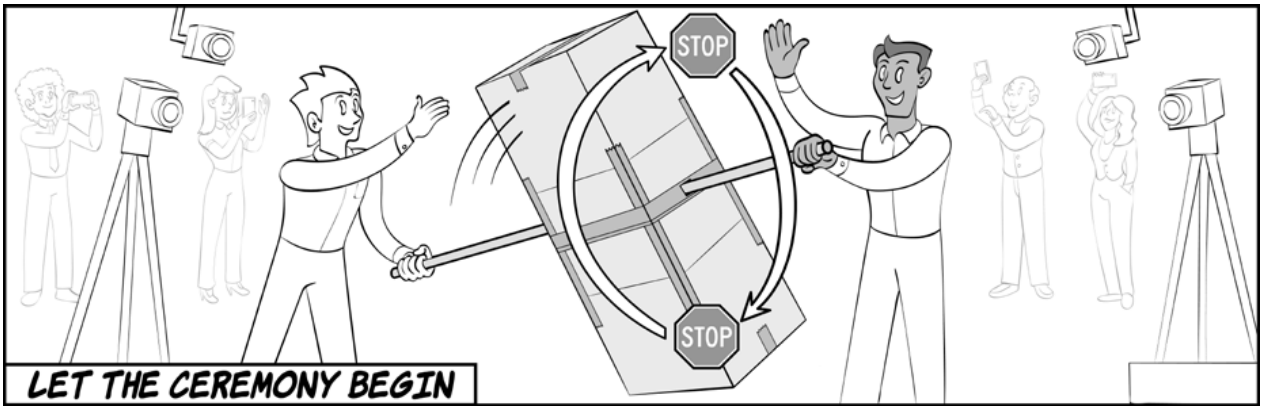
the addresses before they become public, in an attempt to influence ballot recipients, this could be reported by the ballot recipients, as detailed below. If Joe were to record and use the vote-codes, irrefutable evidence of such abuse would become available to auditors and to ballot holders, as also detailed further below.

Joe can optionally arrange that some friends would be capable of carrying out the poll without him. For this, the software can divide the passphrase that Joe entered into "shares," so that any majority of such shares is both necessary and sufficient to complete the poll. Joe can even divide and distribute the physical polling materials before the ceremony.

Ceremony

Joe committed to the ceremony date in the setup and may have shared keys with some of those he has invited to attend. Ideally, those attending the ceremony include different stakeholders related to the question on the ballots. The ceremony attendees should be encouraged to at least record videos of the proceedings from varied angles (a technique used in international arms verification) and post hashes of them to the blockchain. Possibly better also in terms of publicity, but with increased danger that the poll could be stopped, the ceremony could be announced in advance or even live-streamed.

At the beginning of the ceremony, the ballots and empty envelopes are sealed into the two cardboard boxes that have been joined around a broomstick. The top flaps of each box are open and taped together edge to edge, forming a single hopper 6 feet high. (Inside, all edges are sealed with packing tape to prevent contents catching.) The hopper is then rotated through 180

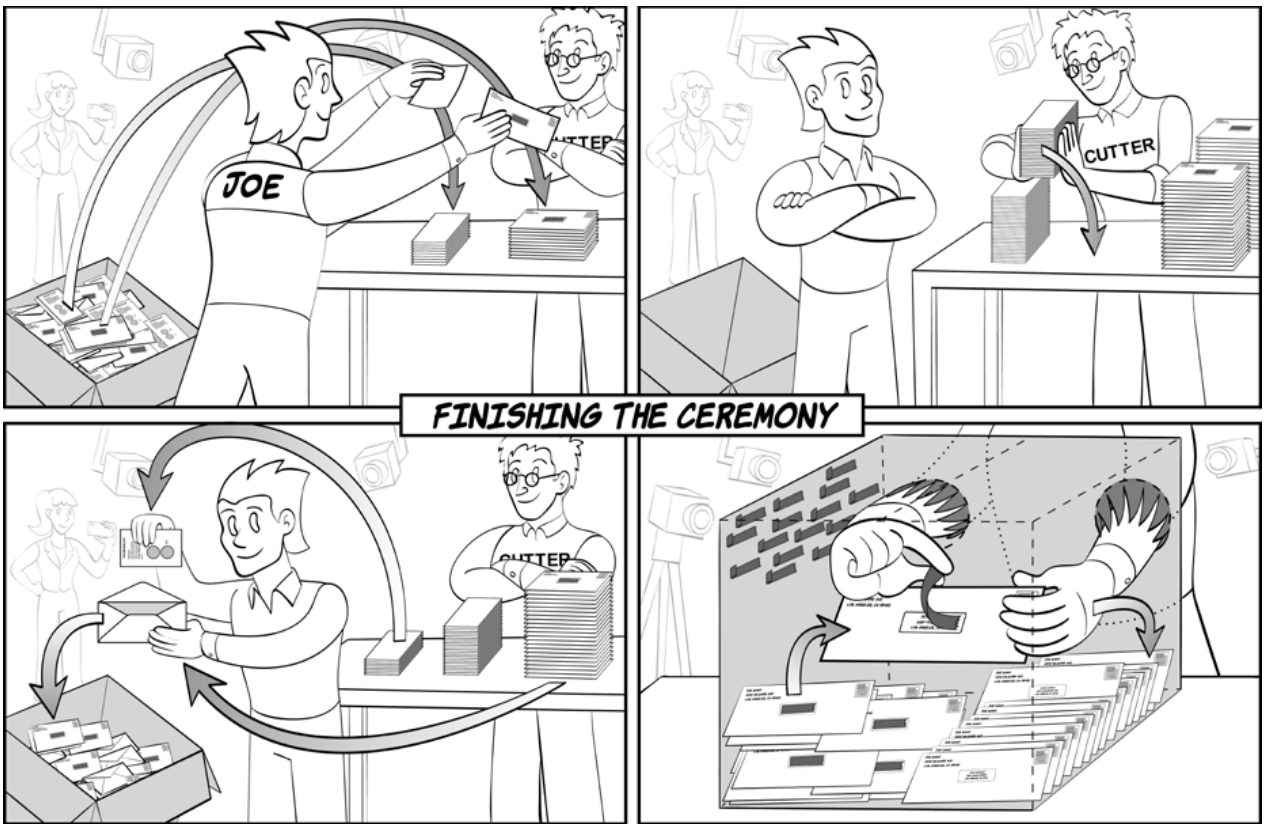


degrees around the horizontal broomstick, rapidly enough to hold the contents in place by centrifugal force, and then stopped when vertical. This is done 17 times, so the contents are thoroughly mixed by repeatedly falling the full six-foot height of the hopper.

There are various ways to ensure that which ballot is sent to which address is random and hidden from all. The ballots and envelopes inside the box can be removed and the stack of ballots can even be cut like a deck of cards, making the point that the order is random. Then the ballots, with the vote-codes still protected by scratch-off, can be individually stuffed into envelopes. Stuffing secure against cameras being used to recognize tiny differences in envelopes or ballots, such as tape or scratch-off alignment, could be accomplished without exposing the printed sides to view, or even by stuffing while ballots and envelopes remain in the box, though such blind stuffing takes about twice as long.

After audits (described in a later section) the opaque black tape must be removed from the address labels, but without exposing any addresses to view. One way to do this is to return the envelopes to the box, in which armholes have been

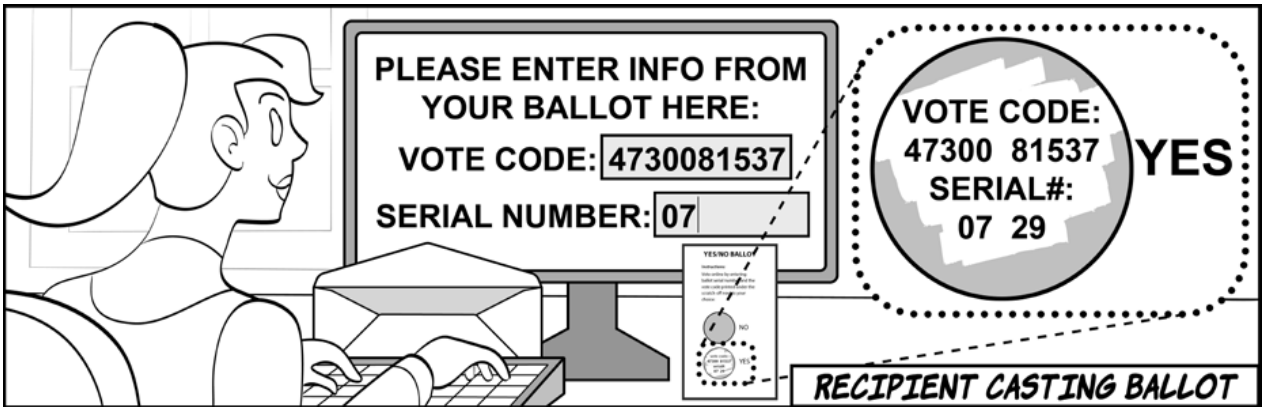
cut that let participants reach in and remove the opaque tape. (Armholes of 5" diameter circles or circumscribed octagons work, but are more comfortable and harder to see through when fitted with 6" squares of 1/8" or 3mm Shore 40a medium-soft silicone or neoprene rubber, with opening cuts like a 16-slice pie.)



Participants could then travel to post-office collection boxes and transfer the envelopes directly from the hopper to the postal system without ever exposing addresses to view. If envelopes are instead divided directly into mailbags, one per team of participants, no one team need know where all envelopes were mailed. The poll might be announced only after ballots are safely in the postal system, only after they are likely delivered, or even only after polling is closed.

Ballot Casting

Instructions printed on the ballots direct their recipients to one or more websites where they can enter their ballot serial number and a vote-code. To obtain the desired vote-code, a recipient scratches off the concealing layer next to their choice, for instance "Yes" or "No." The websites are not given enough information to create, modify, or even recognize choices cast. The sites can, however, verify check digits in the codes, corresponding for instance to sums or encryptions of the other code digits, in order to confirm the absence of input error. Ballot recipients can later verify, if they wish, that the vote-code they provided is posted on the blockchain.



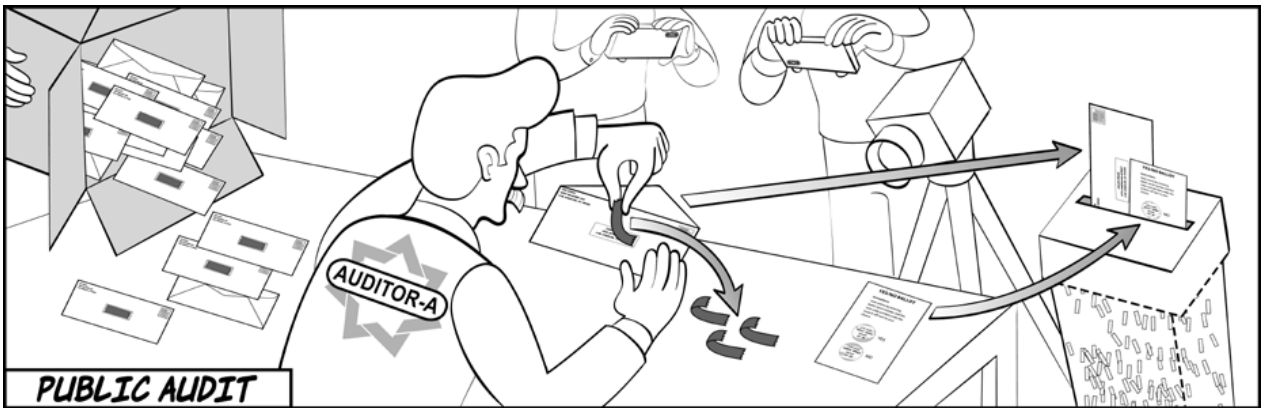
If what is posted is wrong (e.g., in case Joe were, as mentioned earlier, to cast ballot codes he secretly recorded), the printed ballot with at least one scratch-off intact serves as still-anonymous yet irrefutable evidence of malfeasance that could, for instance, be sent to any journalist.

After the date and time Joe originally committed on the blockchain for the close of polls, Joe, or a quorum of those he shared keys with, runs the final software step. One thing this step does is post to the blockchain the list of choices cast, allowing anyone to tally and learn the result of the poll. The other thing it does is post certain keys to the blockchain. These keys decrypt just enough of the encryptions corresponding to each ballot to allow verification that the ballot correctly contributed to the tally—but not enough to allow the codes to be linked to any particular vote. Anyone can then use open-source software, or even write their own software, that uses the posted keys to verify the correctness of the tally.

Ballot counterfeiting might be attempted in order to discredit or corrupt the process. However, if a microphotograph of a few letters of the printed ballot instructions (using a digital 500x or 1000x microscope costing about $100) is included in the original blockchain commitment, it provides a nuclear-safeguards level of counterfeit resistance. This allows definitive resolution of any claim of a false ballot and prevents the alteration of ballots in transit to the postal collection boxes or even within the postal system.

Audits

Two types of audit are conducted, both during the ceremony. In the first, the "Public Audit," some participants at the ceremony draw some of the stuffed envelopes publicly at random from the box. These auditors then remove the opaque black tape from the envelopes and completely scratch off the contained ballots. All the information printed on these envelopes and ballots is thus revealed to all ceremony participants and the cameras.

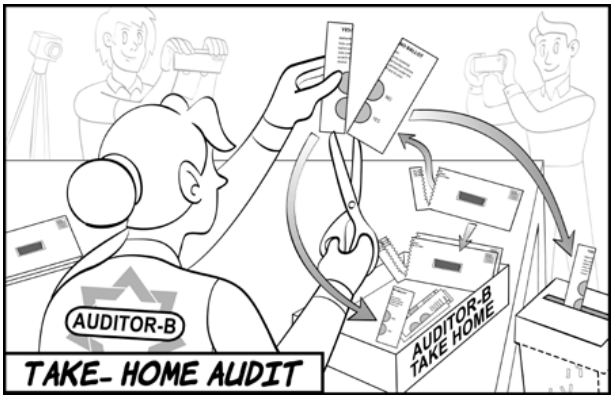


During or after the ceremony, Joe, or a quorum of those he has shared keys with, uses the software to post to the blockchain keys that decrypt just those encryptions related to the revealed addresses and vote-codes—leaving everything else safely encrypted. Since the ceremony videos are public, anyone anywhere can use these posted keys to decrypt and verify that what Joe originally committed to on the blockchain exactly matches the printing exposed at the ceremony.

(A variation, using multiple audits, makes influencing ballot recipients even more difficult: batches of tape-covered address labels, from multiple participants whose only role is to independently obtain and print them, are separately hopper-

tossed and publicly audited; the resulting labels are hopper-tossed together and blind-applied to pre-stuffed publicly-audited envelopes from Joe, with the many remaining labels then shredded.) Multiple participants could even independently perform the role of Joe here to divide knowledge of which ballots are decoys.

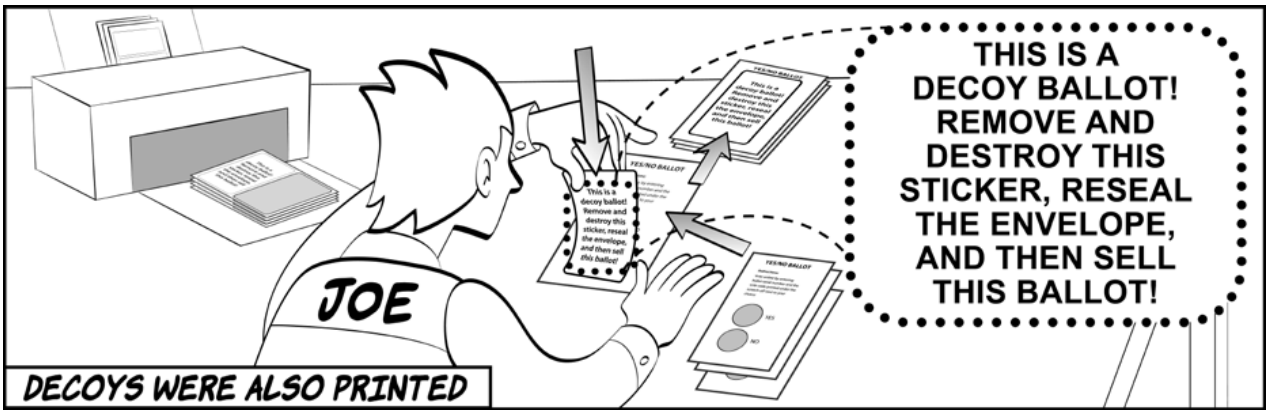
Some ceremony participants conduct "take-home audits." Each of these auditors publicly selects some envelopes from the box at random, removes the contained ballots, and cuts these with scissors vertically through the middle of both scratch-offs into two parts. Next, they publicly shred one of these ballot halves, randomly varying their choice of which half to shred. Each auditor takes their remaining ballot halves and the opened envelopes home.



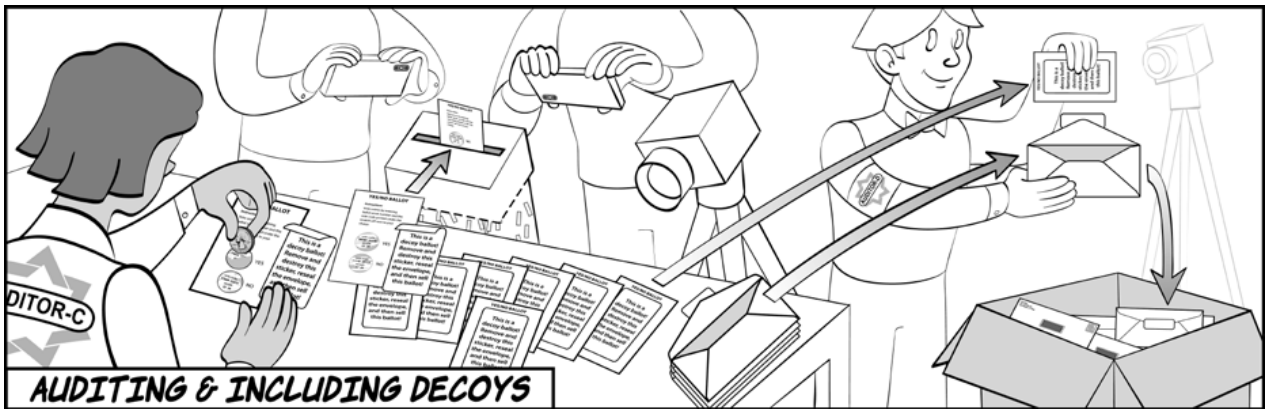
The half vote-codes taken home are not enough to cast a ballot but can serve as irrefutable evidence later. An auditor can even decide to commit to the blockchain a hash of the half vote-codes and addresses they kept, making when they were obtained indisputable. If anyone were to try to substitute ballots into envelopes after the ceremony (without opening all the envelopes and scratching off at least part of all the ballots) or to use Joe's key to cast ballots, the odds of such an attack or malfeasance being detected and proven by what was taken home are increased with each envelope or ballot attempted.

Decoys

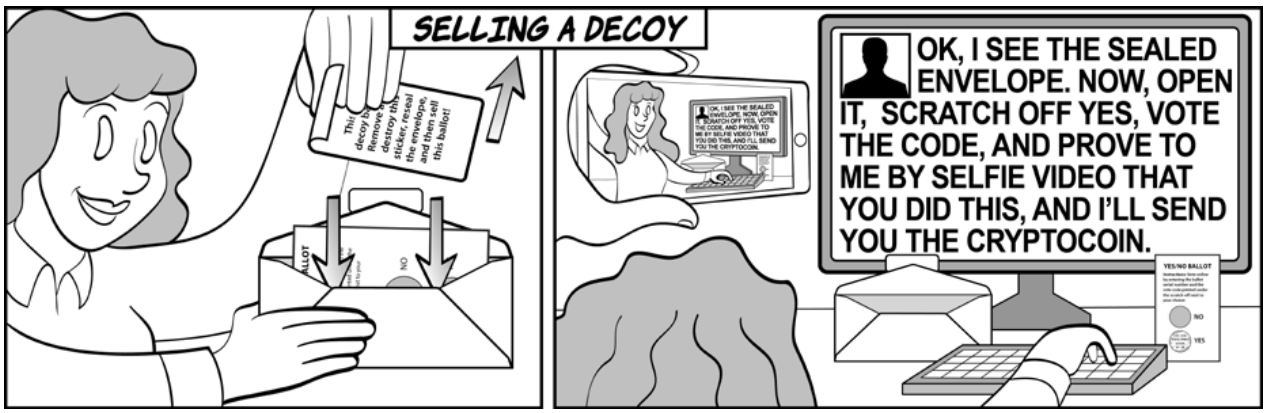
Joe decides to deploy "decoy ballots" to minimize the potential impact of vote buyers on the poll's outcome. Joe's software then commits to a set of decoy ballots that will secretly not be counted, even though otherwise they are completely indistinguishable from other ballots. Joe attaches a specially printed removable sticker (e.g., Avery 5422) to each such decoy ballot. Each sticker says "This is a decoy ballot! Remove and destroy this sticker, reseal the envelope, and then sell this ballot!"



Before being incorporated in with the rest of the ballots, a proportionate number of decoy ballots are picked for a separate public audit. Decoy ballots are included in the batch mailed, with the removable stickers on the ballots inside the envelopes. All envelopes should be easily resealable, such as by using removable self-adhesive stickers (e.g., Avery 6450) to seal the flap.



The decoy recipient should then accordingly seek out an advertisement from someone who wants to buy the ballot, say, among those on the side opposed by the recipient. To sell the decoy, the recipient can simply remove the sticker and livestream or otherwise video the complete voting act, even including reopening the envelope, in order to convince the buyer.



Vote buyers can verify that the vote-code was included in the posted data but can never learn that the vote they bought was a decoy—without Joe's key, which he should have destroyed (though some decoys without instructions can be incorporated during audit, to provide deniability). Sellers not only help with the integrity of the process by frustrating their dishonest opponents but are paid for doing so. Decoys should drive offers down below the price at which real ballot recipients would be willing to sell.

Incentives

Those casting ballots, via open-source software running on their smartphones, can obtain a reward. Essentially, their software forms a digital coin at random and "blinds" it by multiplying by a completely uncorrelated second random number. Some time after casting the ballot, the ballot-holder's smartphone software

receives what is called a "digital signature" on the blinded digital coin. The software can then remove the blinding factor while leaving the signature intact on the original random coin. This signature makes the coin valuable—but the original random coin, now signed, remains unlinkable in any way to its uncorrelated blinded counterpart shown during ballot casting.

Bad actors might attempt to insert their own blinded coins. To prevent this, the ballot-holder's smartphone software, during casting but before revealing the vote-code, commits an irreversible hash of the blinded coin and the vote-code to the blockchain. This software later opens the commitment to reveal the choice of vote-code and blinded coin. Lacking advance knowledge of the vote-code, a bad actor is thus unable to take priority. (If Joe were to try to use his advance knowledge of vote-codes to collect incentives, since he cannot know ballot-holder choices in advance, his malfeasance would likely be evidenced by intact scratch-offs that ballot holders could mail to journalists; even if he were to wait to learn a cast code, a similar process could resolve any dispute, with portions of the remaining code scratched off evidencing malfeasance with even higher probability.)

When the final tally-counting establishes that a given vote-code was correct, the validating signature on the corresponding blinded coin can safely be posted on behalf of incentive sponsors. Only the ballot-holder's smartphone software can then unblind this to obtain the signature on the original coin. That each cast vote-code receives the same signature is in this way transparently verifiable. Different compensation, still uncorrelated with ballot

choice, can nevertheless be given to different participants. One or more signed coins can, for instance, be selected to receive extra value by a fixed algorithm using a random value from the blockchain. This lets unmanipulatable lottery-like compensation provide powerful incentives.

Summary and Conclusion

The 7th Estate has been laid claim to here on behalf of publicly verifiable proofs of the public will. There has been no practical way to achieve such a proof until now. A solution has been detailed here, including all the supplies and the process steps, as a kind of kitchen-tested recipe ready for use by anyone interested in proving the public will. It overcomes the shortcomings of known techniques and offers the best features of each. It accomplishes this through a sampled public-choice system that is national-laboratory-level secure, ensures correctness of tally, allows verification of enfranchisement, thwarts vote-buying, and protects ballot secrecy even from those conducting and incentivizing the process. Yet it is low-cost, very difficult to stop or corrupt, and even fun to use.


TN
THE STATE