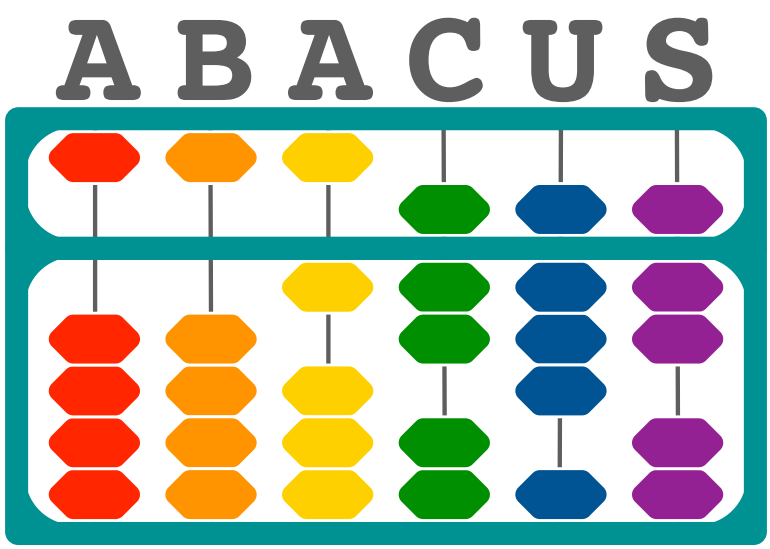
A RECIPE FOR TRUSTWORTHY ELECTIONS

ABACUS VOTING



OVERVIEW

Abacus is an open-source, paper-backed voting system. It combines ballot creation, accessible voting interfaces, ballot scanning, tabulation, and transparent publishing of election results. A code system lets each voter anonymously confirm that their ballot was counted accurately.

DEMOCRACY UNDER ATTACK

Tyrants and anarchists are plotting to undermine democratic systems.

Their prime tactic is to sow distrust in election results.

If that weren't enough, nature itself may threaten democracy. In 2003, cosmic rays bit-flipped a Belgian voting machine, causing a candidate to receive 4096 extra votes, according to an official report.

How can we redesign voting systems to build trust in the face of real and imagined threats on the ballot box?

Certainly, trust requires accuracy.

But accuracy by itself isn't enough.

ACCURATE & OPAQUE

BLACK HOLE
(Messier 87)

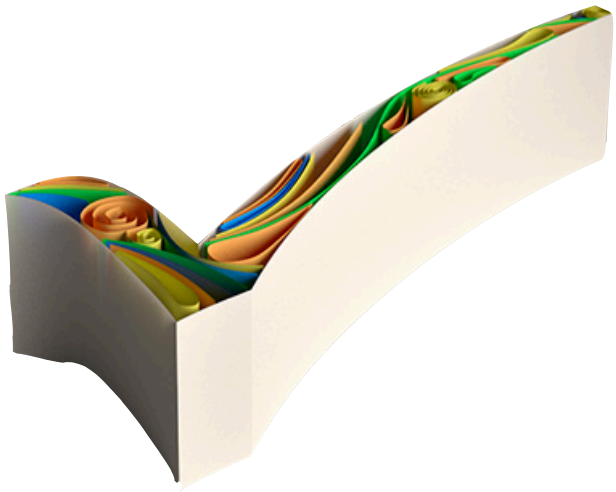
Even if they are accurate, opaque voting systems inspire about as much trust as a black hole. Unless citizens can confirm that their votes were counted correctly, they're unlikely to feel safe in the face of real or imagined threats to these systems.

PAPER: THE GOLD STANDARD

Paper is an ancient, well-understood technology — ideal for building trust.

MACHINES	PAPER
readable and writeable through opaque hardware only	directly readable and writeable by humans
behaves unpredictably	behaves predictably
volatile data storage	durable data storage
hundreds or thousand of dollars to produce per unit	pennies to produce per unit
nearly free to send data -> denial-of-service attacks are cost effective	~$1 to mail per ballot -> denial-of-service attacks are uneconomical
can be corrupted and restored silently and remotely	harder to scale paper-based attacks

Paper trails are therefore essential for reliable audits and should be at the core of any trustworthy voting system.



TRUST, BUT VERIFY

What are solutions to increase confidence in election results?

Minimum: Voters should be able to check an auditable paper record of their vote before submitting it.

But how can they know those records won't be destroyed, altered, or miscounted?

Better: The administrator publishes scans of all the ballots.

Best: Each voter can identify which published ballot is theirs (while preserving anonymity).

This is the Abacus process: true *end-to-end-voter-verifiable* elections. Under this process, each ballot includes a paper receipt with two codes:

- **a ballot code**

  This unique random code is also printed on each page of the ballot, e.g.: EPTG - DLEN - CYYM - PNUH - IZID

  Voters can enter their ballot code online to view the image of their scanned ballot and confirm that it was recorded and counted accurately.

  For increased security, the ballot codes are redacted from the public images, while the association is privately maintained on the back end.

  (The chance of guessing a valid 20 letter code like this among a pool of 1 billion ballots is ~1 in 20 quintillion.)

- **an ownership code**

  A voter may use an ownership code to prove that they are the rightful owner of a particular ballot code.

  If a ballot code is somehow stolen, a voter can submit the ownership code to receive a new pair of codes as replacement.

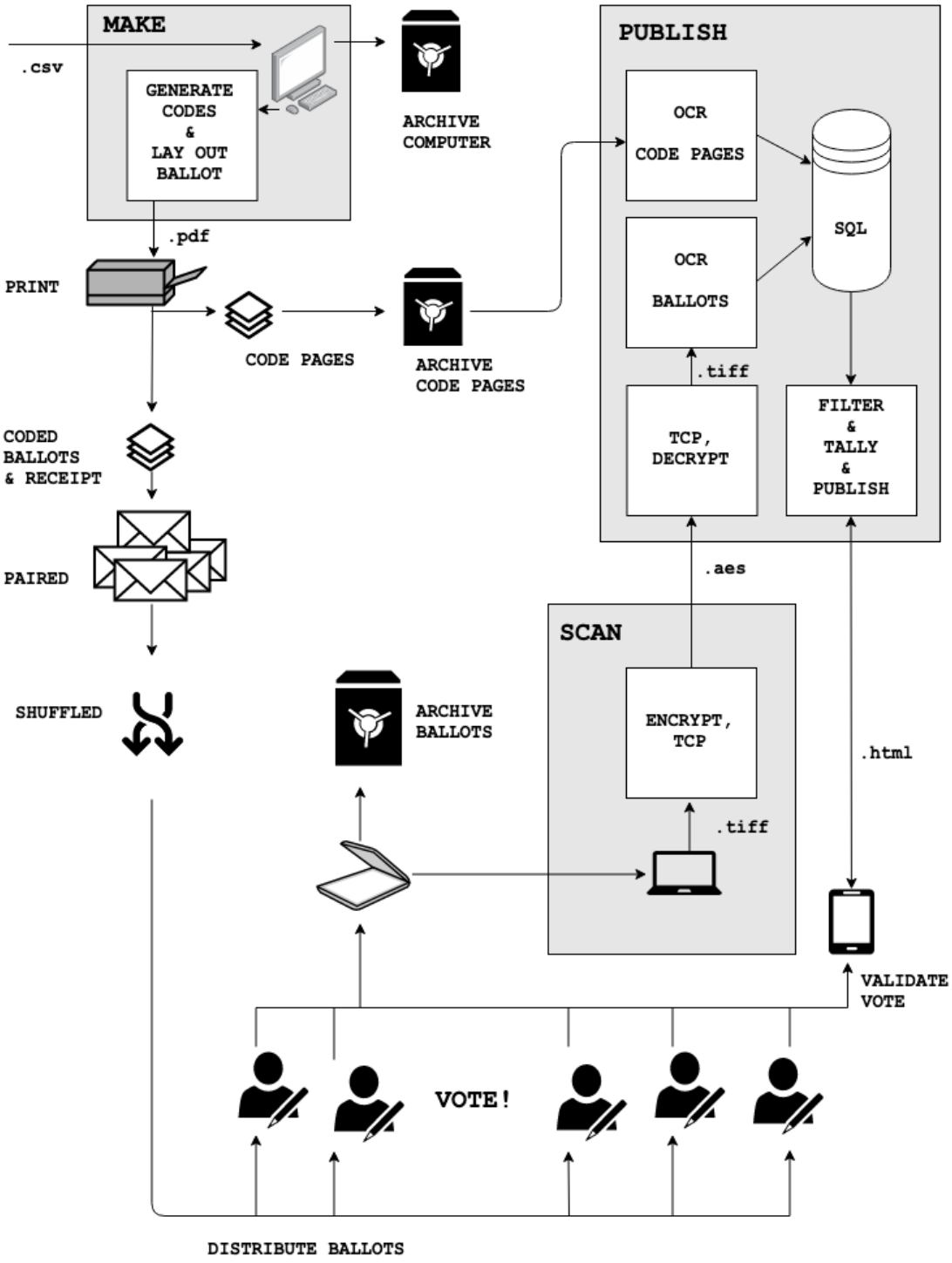
VOTING METHODS

Ranked-choice-voting and score-voting are gaining interest as alternative voting methods, with proponents arguing that they can promote a shift from scorched-earth politics to governance from common ground. Abacus software supports alternative and conventional voting methods with equal vigor.

	CONVENTIONAL	RANKED-CHOICE	SCORE
INSTRUCTIONS	**Vote for exactly one candidate.**	**Rank the candidates from 1st to nth.**	**Give each candidate a score.**
HOW WINNER IS DETERMINED	first candidate with more than half of the vote	instant runoff (or a similar procedure)	candidate with the highest average score

The corresponding ballots are below. Note that the conventional ballot uses a higher density layout. Also note the ballot codes on the bottom of the header.

FLOW CHART


MAKE
.csv
GENERATE CODES & LAY OUT BALLOT
ARCHIVE COMPUTER
.pdf
PRINT
CODE PAGES
ARCHIVE CODE PAGES
CODED BALLOTS & RECEIPT
PAIRED
SHUFFLED
ARCHIVE BALLOTS
PUBLISH
OCR CODE PAGES
OCR BALLOTS
SQL
.tiff
TCP, DECRYPT
FILTER & TALLY & PUBLISH
.aes
SCAN
ENCRYPT, TCP
.tiff
.html
VALIDATE VOTE
VOTE!
DISTRIBUTE BALLOTS

MODULES

Abacus software runs as four independent modules:

PRINT

First, the election administrator(s) enters contests, candidates, instructions, and formatting options in a spreadsheet. Using the spreadsheet as input, this module prints coded ballots, collated with instruction and receipt pages. This module also creates a printable database of the codes generated.

VOTE

Voters can hand-mark blank ballots using pens or pencils. Alternatively, this module allows voting through a browser interface. Voters enter their ballot code, set their votes, and print out marked ballots. (Depending on election law, this may be done at precincts or at home.)

* Visually impaired voters are guided with audio feedback.
* Physically impaired voters can interface with the program using third-party hardware like joysticks or puff-and-sip devices.

SCAN

COTS hardware scans the marked ballots. This module then validates the ballots, encrypts the images, and uploads them to a central server. This module can be run across many independent computers connected to scanners in the field.

PUBLISH

As the images are transmitted from the field, this module: decrypts the images, interprets the images as votes, stores the images and votes in a database, filters the ballot codes against a scanned list of valid codes, and tabulates and publishes the filtered votes. This module also generates a website where voters can enter their codes to confirm their votes.

By dividing the system into distinct, focused modules, it is easier for security experts to vet the code base.

STEPS

1

The administrator(s) compiles the voter roll on a separate system.

2

The administrator uses an offline computer to generate pairs of ballot and ownership codes.

The administrator prints out the list of valid code pairs and archives the paper in a secure lockbox. (Keeping printed papers in a locked vault is more secure way than storing data on a computer.)

The administrator prints out coded ballots, collated with instructions and coded receipts.

The ballot-generating computer is placed in an offline safe. (Or it is destroyed.)

3

The ballots and receipts are paired and sealed in envelopes.

4

The envelopes are shuffled.

(This ensures that voter secrecy is maintained.)

5

The envelopes are distributed, either by mail or in person at polling stations.

6

Voters mark their ballots and return them, keeping their receipts if they wish to confirm their votes.

7

Ballots are scanned and archived.

For in-person voting stations, scanning is done on-site. For voting by mail, it may take place at a central facility.

8

At a predetermined date, the administrator opens the locked vault and scans the stored codes.

The software then decrypts, filters, interprets, tallies, and publishes the scanned votes.

Each published vote is indexed and includes a running total of the score based on all votes published before it (generated by the software), allowing observers to audit the tally in a decentralized manner.

9

When voters can enter their ballot codes online, they get a link to the corresponding published ballot and how the software interpreted it.

If election rules allow it, they may resubmit ballots to override their previous votes.

10

The administrator certifies the result.

FLEXIBLE ARCHITECTURE

The Abacus procedure supports many election scenarios.

BALLOT PRINTING: CENTRALIZED or DECENTRALIZED

Ballots may be printed at a single location or at multiple facilities. If election rules allow it, voters may print their own ballots at home.

VOTING: BY MAIL, IN PERSON, or REMOTE

Voters can receive and return their ballots by mail, in person, or a combination. Remote voting, e.g. for citizens overseas, can be enabled with an additional layer of codes.

SCANNING: CENTRALIZED or DECENTRALIZED

Scanning may be done centrally or at many locations.

CANDIDATE ORDER: FIXED or RANDOM

Candidates with a consistent top billing may have an unfair edge. Abacus allows for printing ballots with candidates in a fixed order or for varying the order randomly across ballots.

VOTING: REVISABLE or IMMUTABLE

If election rules allow it, Abacus can accommodate voters resubmitting their ballots using the same ballot code if they wish to change their votes within a designated voting period.

SINGLE or MULTIPLE ROUNDS

Abacus can support elections composed of party primaries followed by a general election.

It can also support multiple rounds of general voting. For example, election rules could lower the number of listed candidates each week:

```
50 → 20 → 10 → 5 → 2 → 1
```

Voters may automatically carry forward their ballots from the previous round.

OPEN-SOURCE SOFTWARE & COTS HARDWARE

We believe that sunlight cleanses code.

To maximize trust, our code base is fully open-source, free for anyone to prod and critique.

In addition, transparency increases voters' faith in the process. For example, the most subtle element of the Abacus software is the one that classifies scanned images as votes using optical character recognition (OCR). The element is highly nuanced in how it handles optical stray marks, write-in candidates, spoiled ballots, etc.

With conventional voting systems, this important function is executed as proprietary firmware tied to opaque scanning hardware. This means outside observers cannot inspect its reliability.

Under the Abacus framework, the software and hardware decouple. The ballot images and corresponding output are both published, so anyone can verify that the system is working as intended.

While this approach is primarily motivated by security and transparency, a side benefit is that commercial-off-the-shelf (COTS) hardware can be used. COTS scanning hardware is significantly less expensive than hardware manufactured specifically for elections.

Abacus software runs on open and proven data formats:

.csv, .pdf, .tiff, .aes, .sql, .html

OPEN-SOURCE SOFTWARE AS A BUSINESS

We're a public-benefit business,
dedicated to strengthening democracy.

Our mission clarifies our business:

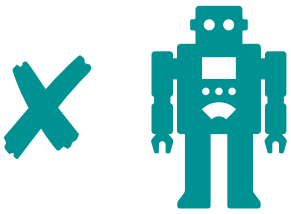
We don't sell opaque DRM software.

Security through obscurity is a false idol.

We don't sell cloud services.

Data centralization is a systemic risks.

We don’t think it’s wise for a single entity to host data for multiple elections. Call us old school, but we believe it's more secure for the system administrator to know exactly where their server is located. (Our software does run on third-party cloud services if desired.)



We don't (re)sell hardware.

We just don’t trust it.

We do offer a copyright removal license.

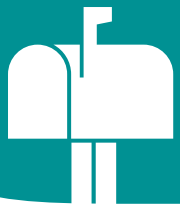
The license lets the user replace our copyright notice with their insignia.

DROP US A LINE . . .

1-510-859-8760

AbacusVoting.com

hello@AbacusVoting.com



Abacus Voting
340 S Lemon Ave #8490
Walnut, CA 91789