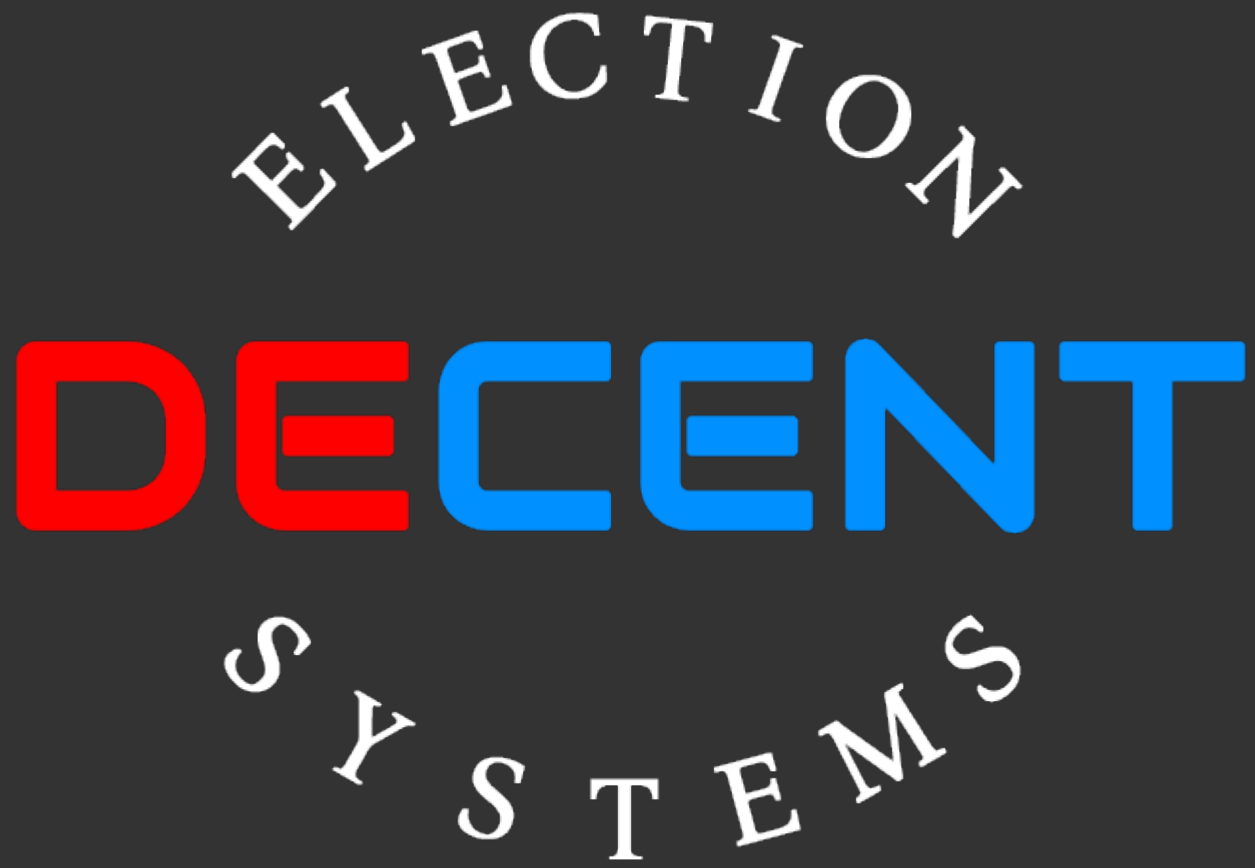
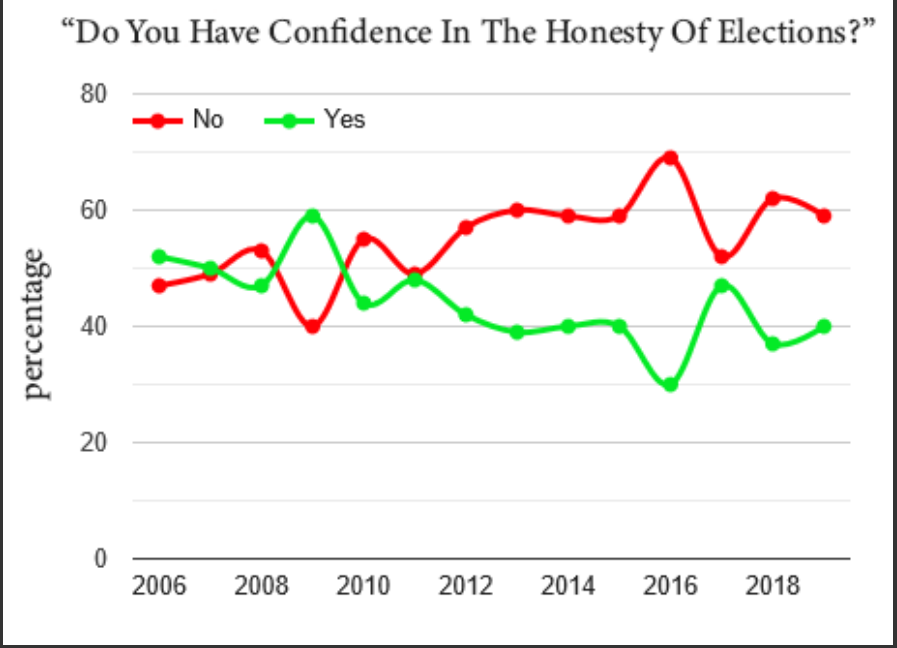


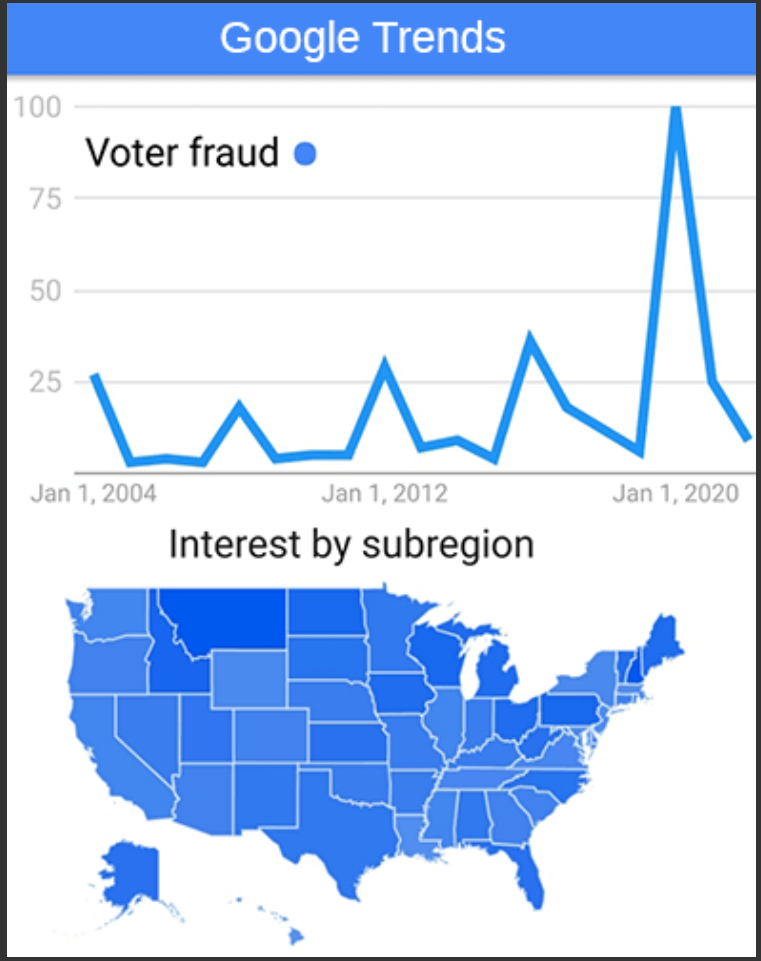
PROBLEM 1

Six in 10 Americans Do Not Have Confidence In The Honesty Of U.S. Elections

"Americans' current level of confidence in their elections is far from the lowest it has been at times in the past decade, but it is notably one of the worst ratings across the world's wealthiest democracies. Ratings were statistically lower last year only in Chile (31%) and Mexico (30%)."

--Gallup[1], February 13, 2020





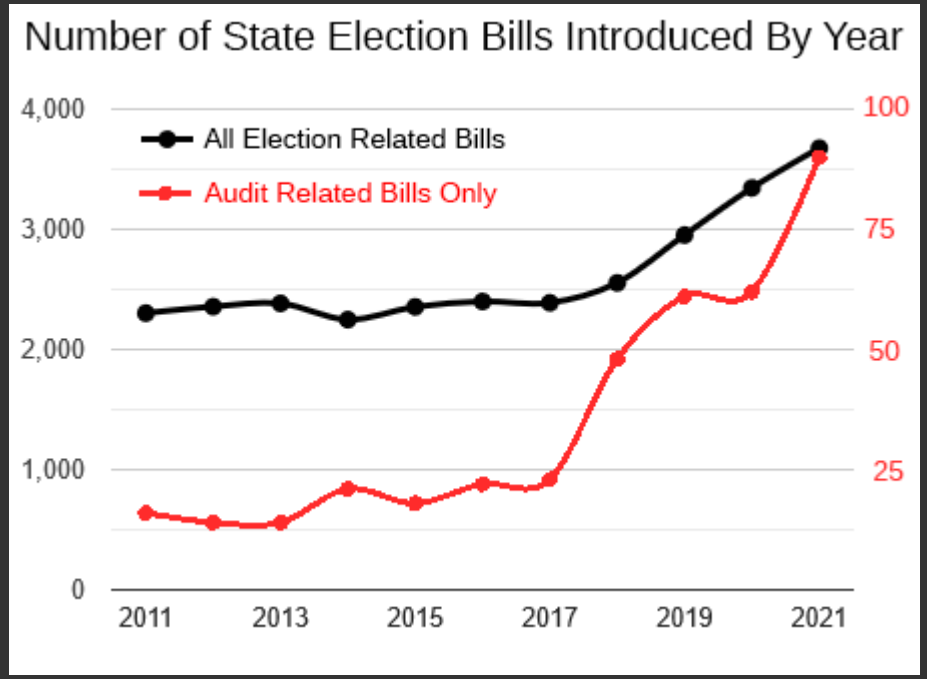
PROBLEM 2

When a box of uncounted ballots is found without a chain of custody, how would one determine if said ballots were illegally discarded and must be added to the count, or illegally created and must be ignored?

Absent a paradigm shift in the way votes are counted, election laws are no more than paper tigers - incapable of proving or disproving that:

- Illegal ballots were added
- Legal ballots were deleted
- Legal ballots were altered

Laws alone cannot solve these problems.



Source: National Conference of State Legislatures[2]

MISSION

Use cryptography to revolutionize voting systems.

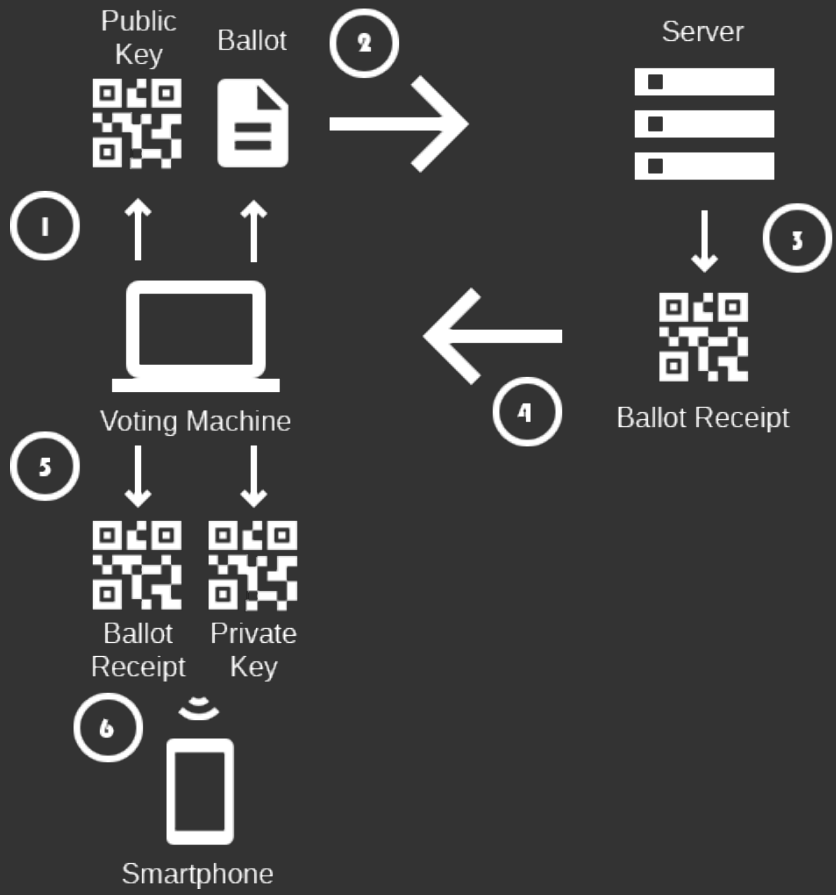
Restore faith in elections by making fraud impossible.

Decentralize the auditing process rendering it accessible to anyone.

SOLUTION

Brief Description of Method

1. Create a ballot and asymmetric key pair. Hash the ballot, sign the hash with the private key, and sign that with the voting machine's Trusted Platform Module[3] (TPM).
2. Send the above (excluding the private key) to the authentication server.
3. Check the TPM signature, store the ballot, then sign the signed ballot hash with the election authority private key, resulting in the Ballot Receipt.
4. Return the Ballot Receipt to the Voting Machine and verify the receipt.
5. Present the Ballot Receipt and Elector's Private Key to the elector.
6. Elector reads the receipt with their smartphone or prints a physical copy.



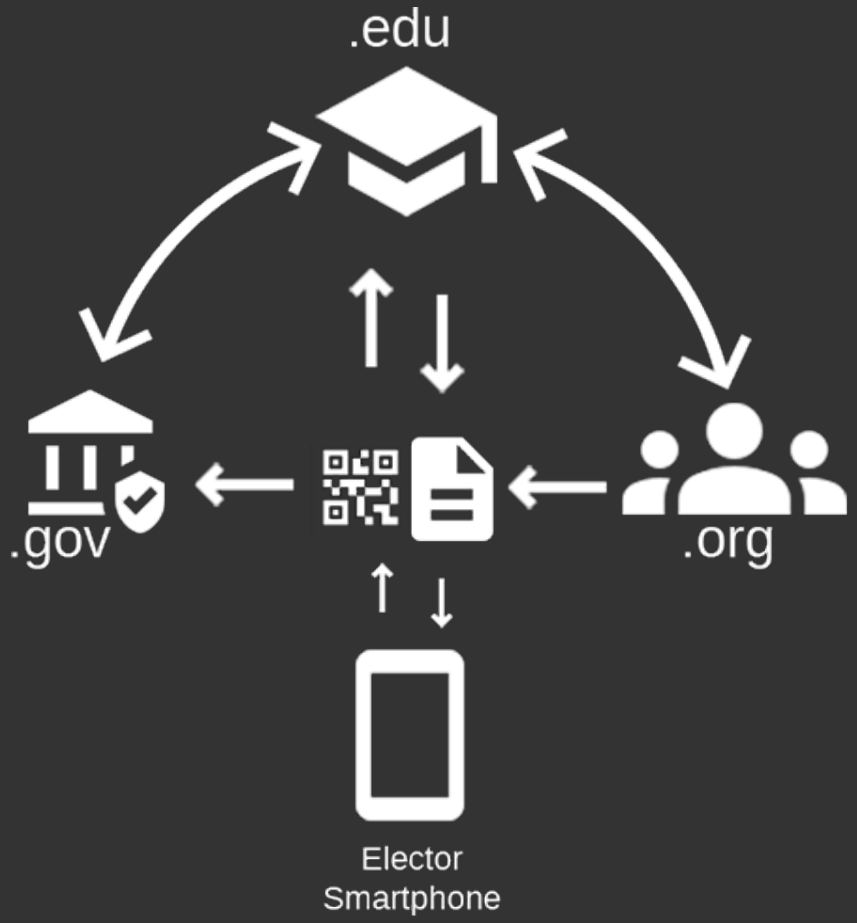
Full Method[4]

SOLUTION

Once the election concludes, the ballot database is published openly. The data can be downloaded by any interested party who can then use cryptographic checks to ensure the votes are unaltered and originated from a valid voting machine's Trusted Platform Module. This happens independent of elector participation in the counting/audit process.

The voting machines "unlock" allowing for read-only login and code/operating-system inspection.

Electors can use their smartphones to connect to the election oversight organization of their choice to validate their vote. Sending only the elector's public key preserves anonymity, and allows the chosen organization to identify the elector's ballot and return it to their phone. The elector's phone then performs the necessary cryptographic checks to prove vote integrity. The elector can inspect how their ballot counts toward the results and need not understand the cryptographic proof.



SOLUTION

The results of the cryptographic integrity checks are reported to the elector in their preferred format.

A basic interface is available to the layman showing a minimalistic VALID/INVALID color scheme, along with where the ballot was cast and the contents of said ballot.

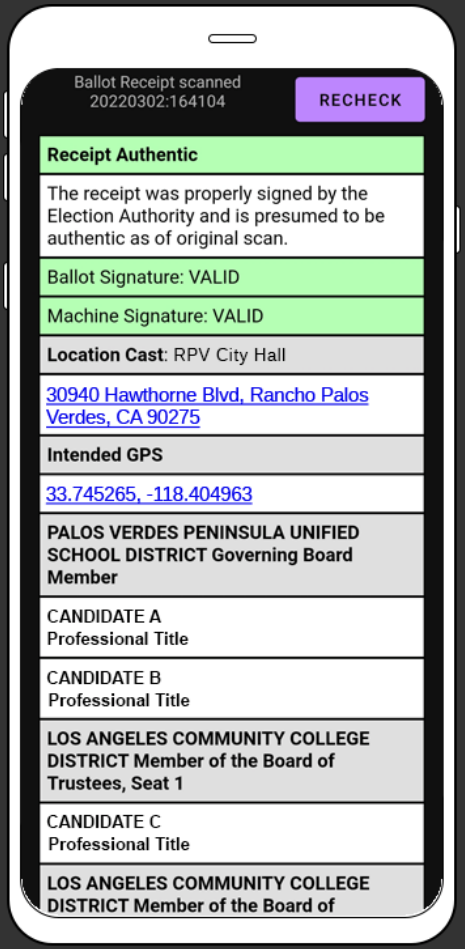
The advanced interface includes all of the necessary data (shown in hex) to allow a programmer to validate the ballot personally with their own code and computer.

If the ballot is altered, the signed hashes are proof.

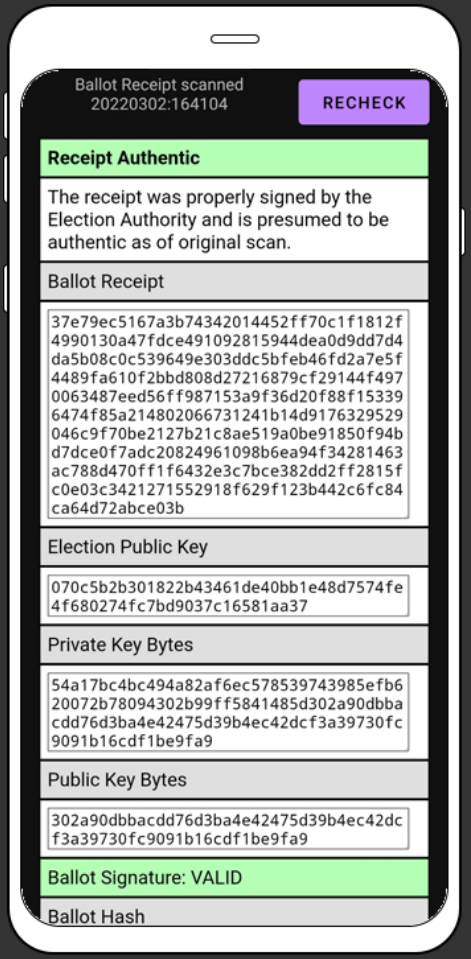
If the ballot cannot be found, the server-signed receipt proves deletion.

If the ballot is not signed by a whitelisted TPM, it is fraudulent.

Basic Interface



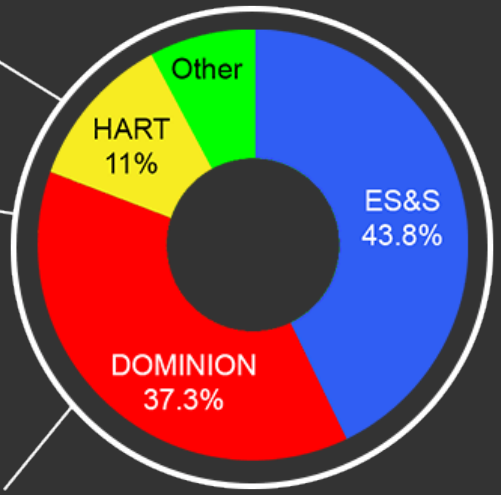
Advanced Interface



COMPETITION

Uses proprietary hardware and software.

Code and vote databases are hidden from the public.



Employs a “Just trust us” model to dictate election results with no way for you to double check.

DECENT

Uses modern hardware running Linux with current standards and secure boot.

Security experts and academics are invited to audit the software and hardware.

Publishes anonymized data openly enabling instant audits at zero cost which can be performed by anybody.

References

1. Gallup - Faith in Elections in Relatively Short Supply in U.S.
   https://news.gallup.com/poll/285608/faith-elections-relatively-short-supply.aspx

2. National Conference of State Legislatures Database
   https://www.ncsl.org/research/elections-and-campaigns/elections-legislation-database.aspx

3. Wikipedia - Trusted Platform Module
   https://en.wikipedia.org/wiki/Trusted_Platform_Module

4. Decent Elections – OSAKA Standard White Paper
   https://www.decentelections.com/OSAKA.pdf