Studio comparativo dei sistemi di e-voting

Alessandro Fraticelli[1]
alessandr.fraticelli@studenti.unicam.it

Computer Science @ Unicam

Studio comparativo dei sistemi di e-voting:

- Professore e relatore: F. Marcantoni
  https://computerscience.unicam.it/marcantoni/
- Studente: Alessandro Fraticelli
  alessandr.fraticelli@studenti.unicam.it - 097988

Indice

Introduzione

Questa tesi si propone di esplorare lo stato attuale dei sistemi di voto elettronico, riassumere un elenco di requisiti e principi di progettazione che ne garantiscano l'integrità offrendo una rassegna dei protocolli più conosciuti e, infine, fornendo una descrizione dell'implementazione di uno di questi.

Definizione

Per voto elettronico, o *e-voting* (dall'inglese *electronic voting*), si intende qualsiasi forma di elezione in cui, almeno in un momento, una copia elettronica del voto è memorizzata elettronicamente e il risultato elettorale è calcolato sulla base dei voti elettronici memorizzati. Esistono diverse forme di voto elettronico, tra cui il voto via Internet, il voto tramite terminale elettronico in seggio, o tramite sistemi a scansione ottica.

TIPI DI VOTO ELETTRONICO

Le tre dimensioni fondamentali che caratterizzano le categorie di forme elettorali sono:

- **Supporto**
- **Ambiente**
- **Momento**

CATEGORIE DI SISTEMI DI VOTO ELETTRONICO

<table>
<tr><th></th><th>Ambiente supervisionato</th><th>Ambiente non supervisionato</th></tr>
<tr><td rowspan="2">Supporto cartaceo</td><td colspan="2">Sistemi a schede perforate</td></tr>
<tr><td colspan="2">Sistemi a scansione ottica</td></tr>
<tr><td rowspan="4">Supporto elettronico</td><td>Macchine per il voto elettronico in rete nei seggi elettorali</td><td></td></tr>
<tr><td>Macchine per il voto elettronico stand-alone nei seggi elettorali</td><td></td></tr>
<tr><td></td><td>Macchine per il voto elettronico a chiosco</td></tr>
<tr><td></td><td>Voto elettronico a distanza</td></tr>
</table>

Requisiti costituzionali e principi di progettazione proposti da D. Gritzalis

Requisiti costituzionali	**Principi di progettazione dei sistemi di voto**
Generalità	Isomorfo al tradizionale
	Idoneità
Libertà	Incoercibilità
	Nessuna propaganda nel sito di voto elettronico
	Possibilità di voto non valido
Uguaglianza	Uguaglianza dei candidati
	Uguaglianza degli elettori
	Un elettore - un voto
Segretezza	Segretezza
	Equilibrio tra sicurezza e trasparenza
Immediatezza	Registrazione e conteggio delle schede non monitorati
Democrazia	Affidabilità e trasparenza
	Verificabilità e responsabilità
	Affidabilità e sicurezza
	Semplicità

Principi di sicurezza

- **Correttezza**: Il sistema di voto elettronico deve produrre il conteggio corretto, che è la somma di tutti i voti espressi, in maniera verificabile. È tollerabile il conteggio venga manipolato leggermente, a patto che la possibilità di essere scoperti sia elevata per manipolazioni consistenti che cambiano il risultato delle elezioni.
- **Indipendenza del software**: "Un sistema di voto è indipendente dal software se una modifica o un errore non individuato nel suo software non può causare una modifica o un errore non individuabile nel risultato delle elezioni." R. Rivest, *On the notion of 'software independence' in voting systems.*

Sicurezza end-to-end

- **Verifica *individuale***: Possibilità dell'elettore di verificare che la scheda inserita sia stata correttamente inclusa nel conteggio finale.
- **Verifica *universale***: Possibilità per le autorità di voto di pubblicare delle prove che convincano del corretto conteggio delle schede ricevute.

I sistemi di voto che forniscono una verifica sia individuale che universale si dicono sicuri *end-to-end*.
La sicurezza E2E nei sistemi di voto può anche essere divisa in termini di tre fasi fondamentali:

- *Cast-as-intended*
- *Recorded-as-cast*
- *Tallied-as-recorded*

Segretezza del voto

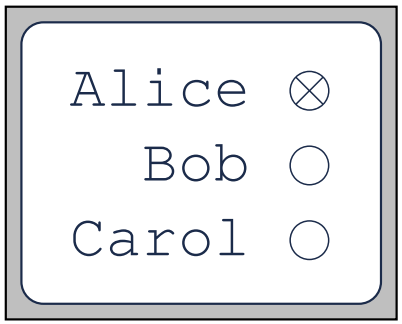
- **Assenza di ricevute**: L'elettore non riceve alcuna prova che possa essere utilizzata per dimostrare a terzi come ha votato.
- **Resistenza alla coercizione**: Un sistema di voto che non fornisce alcuna informazione sulla scelta dell'elettore anche se quest'ultimo devia dal processo di voto previsto è detto resistente alla coercizione.

Bingo Voting

Sistema stand-alone proposto nel 2007, chiamato così per via dell'utilizzo in esso di un generatore di numeri casuali, paragonabile all'estrazione di numeri per il gioco del bingo. Per un'elezione con n candidati e m elettori idonei, vengono generate $m \cdot n$ stringhe di numeri casuali, raggruppati in modo che a ogni candidato sia assegnata una serie di n numeri casuali. Questi sono detti "Voti fittizi".

Bingo Voting

In cabina elettorale, l'elettore preme il pulsante del candidato scelto sulla macchina per votare. Un numero casuale R viene generato e mostrato all'elettore, viene poi stampata una ricevuta con l'elenco dei candidati associati a dei numeri. Solo il candidato scelto dall'elettore viene associato al numero R, gli altri ottengono un voto fittizio casuale generato precedentemente. L'elettore deve verificare che il numero casuale sia assegnato al candidato desiderato e contestare il voto se non lo è.



Bingo Voting

Dopo l'elezione, viene pubblicato su una bacheca:

- il risultato finale dello scrutinio calcolato dalla macchina per il voto;
- un elenco di tutte le ricevute emesse;
- gli elenchi di tutti i voti fittizi non utilizzati per ogni candidato;
- prove che ogni scheda votata contenga esattamente un voto non fittizio.

Gli elettori possono verificare la propria ricevuta nell'elenco per confermare che è stata inclusa nel conteggio. Il numero per ciascun candidato di voti fittizi non utilizzati corrisponde al numero di voti ricevuti.

Prêt à Voter

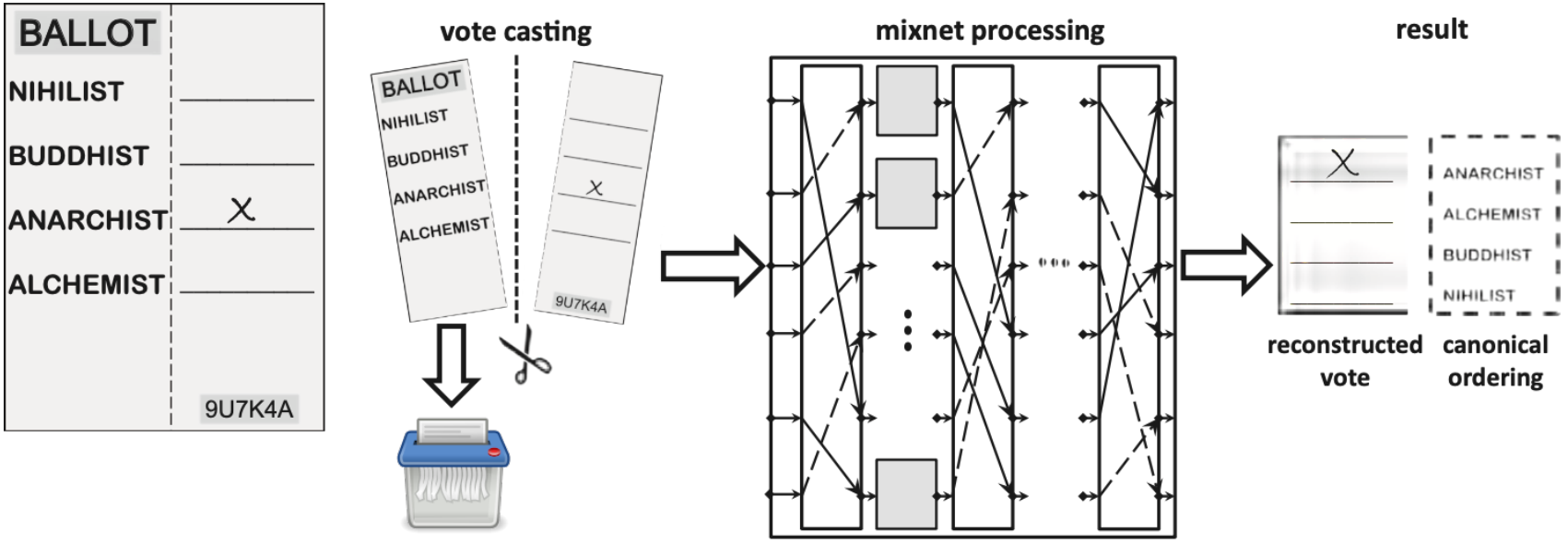
Prêt à Voter è un sistema di voto a scansione ottica supervisionato verificabile end-to-end.

- La scheda elettorale cartacea contiene un elenco rimovibile di nomi dei candidati in ordine casuale
- Metà destra: aree di marcatura per ogni candidato e una stringa chiamata *onion*
- Lato sinistro staccato e distrutto prima della scansione del voto
- Voto acquisito tramite lettura digitale del lato destro della scheda, che l'elettore conserva come ricevuta
- Voto criptato (parte destra) pubblicato in bacheca per verificare l'integrità del voto.

Solo l'elettore conosce l'ordine dei candidati $\rightarrow$ Nessuno, compreso lo scanner, può conoscere il voto.

Prêt à Voter

L'idea dell'elaborazione del voto di Prêt à Voter è quella di trasformare l'insieme dei voti criptati in un insieme di voti non criptati, senza che possano essere ricollegati agli elettori.
Tutte le ricevute sulla bacheca vengono passate attraverso una *mixnet* per ricostruire la scelta dell'elettore nell'ordine canonico dei candidati. I voti ricostruiti vengono conteggiati normalmente.



Prêt à Voter

I voti espressi vengono pubblicati su una bacheca dove gli elettori possono verificare che siano riportate le informazioni sulla loro ricevuta (il voto e l'*onion*). Se il voto non compare nella bacheca, o compare in modo errato, l'elettore può utilizzare la ricevuta per contestare il buon andamento dell'elezione, poiché fornisce la prova di un voto che non è stato incluso nel conteggio.

Helios

Helios è un sistema di voto elettronico *open source* appartenente alla categoria dei sistemi di voto a distanza.
Pensato come strumento per elezioni con un basso rischio di coercizione che tuttavia necessitano della segretezza del voto e di risultati elettorali affidabili.

Per creare e amministrare un'elezione, è necessario effettuare il login utilizzando l'autenticazione di terze parti come Google o GitHub.
Come amministratore dell'elezione, si ha il potere di designare chi può votare, quando l'elezione inizia, quando l'elezione termina e quando i risultati vengono pubblicati.
Oltre a questo, l'amministratore non ha alcun potere al di là di quello degli elettori.

Dopo aver effettuato il login, è possibile per un utente creare un'elezione compilando un modulo che definisce le caratteristiche principali dell'elezione.

Campo	Descrizione
Nome breve	Non può contenere spazi, farà parte dell'URL dell'elezione, ad esempio my-club-2010
Nome	Il nome dell'elezione
Descrizione	Appare sulla pagina principale per questa elezione / referendum
Tipo	Elezione / referendum;
Uso di alias per gli elettori	Se selezionato, le identità degli elettori saranno sostituite con alias, ad esempio "V12", nel centro di monitoraggio dei voti
Randomizza l'ordine delle risposte	Abilitare questa opzione se si desidera che le risposte alle domande appaiano in ordine casuale per ogni elettore
Privato?	Un'elezione privata è visibile solo agli elettori registrati.
Indirizzo email di supporto	Un indirizzo email a cui gli elettori possono rivolgersi in caso di problemi, di default è l'indirizzo associato all'email dell'admin.
Inizio Voto	Data e ora dell'inizio della votazione
Termine Voto	Data e ora della fine della votazione

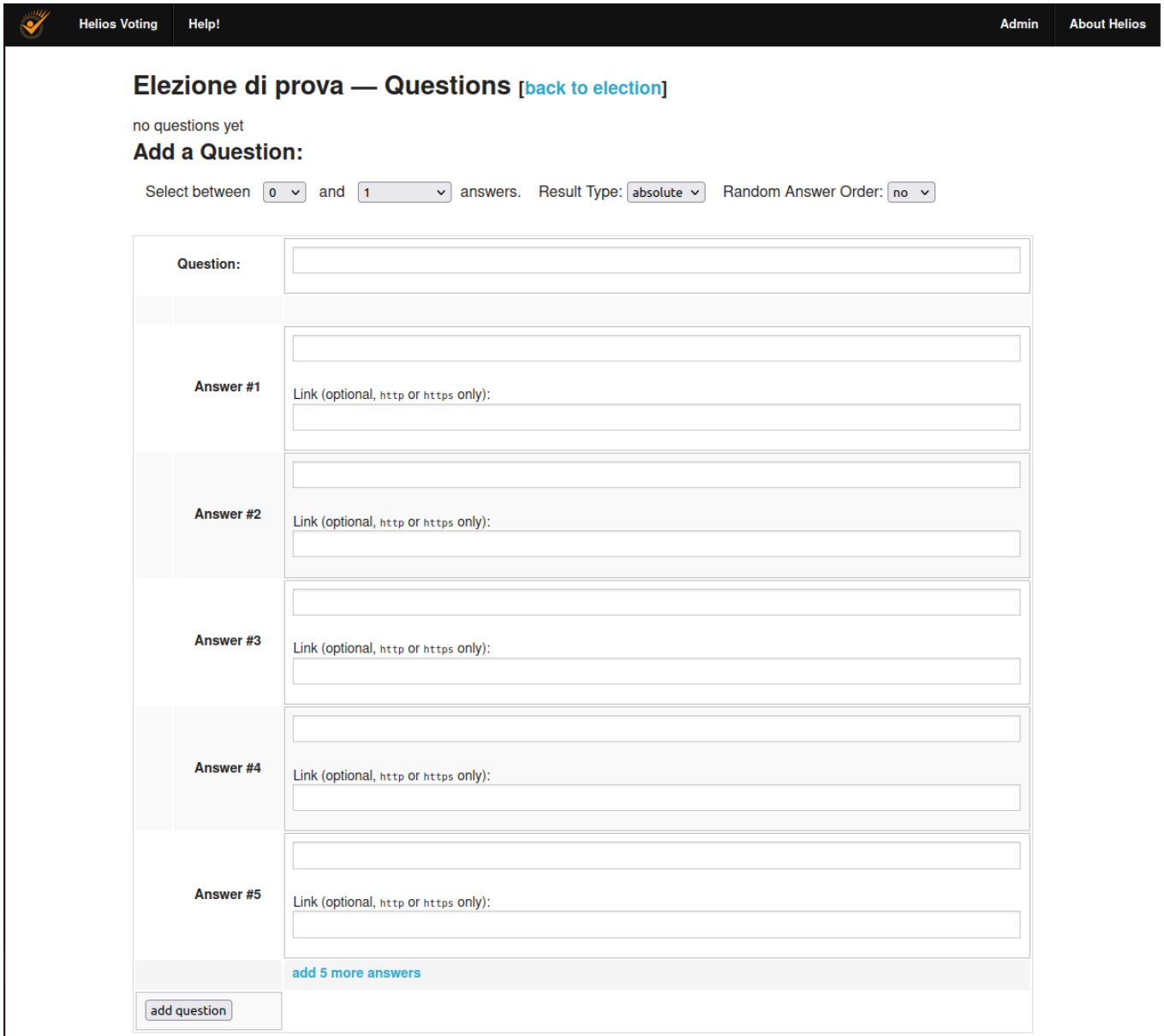
Queste caratteristiche possono essere modificate fino all'inizio dell'elezione.

HELIOS

La pagina dell'elezione mostra, oltre al resto delle informazioni inserite dal creatore dell'elezione, l'indicazione contenente il passo successivo che l'amministratore deve eseguire per condurre l'elezione. Da questa pagina si possono quindi gestire:

- I quesiti per cui votare
- Gli elettori e le schede elettorali
- I fiduciari dell'elezione

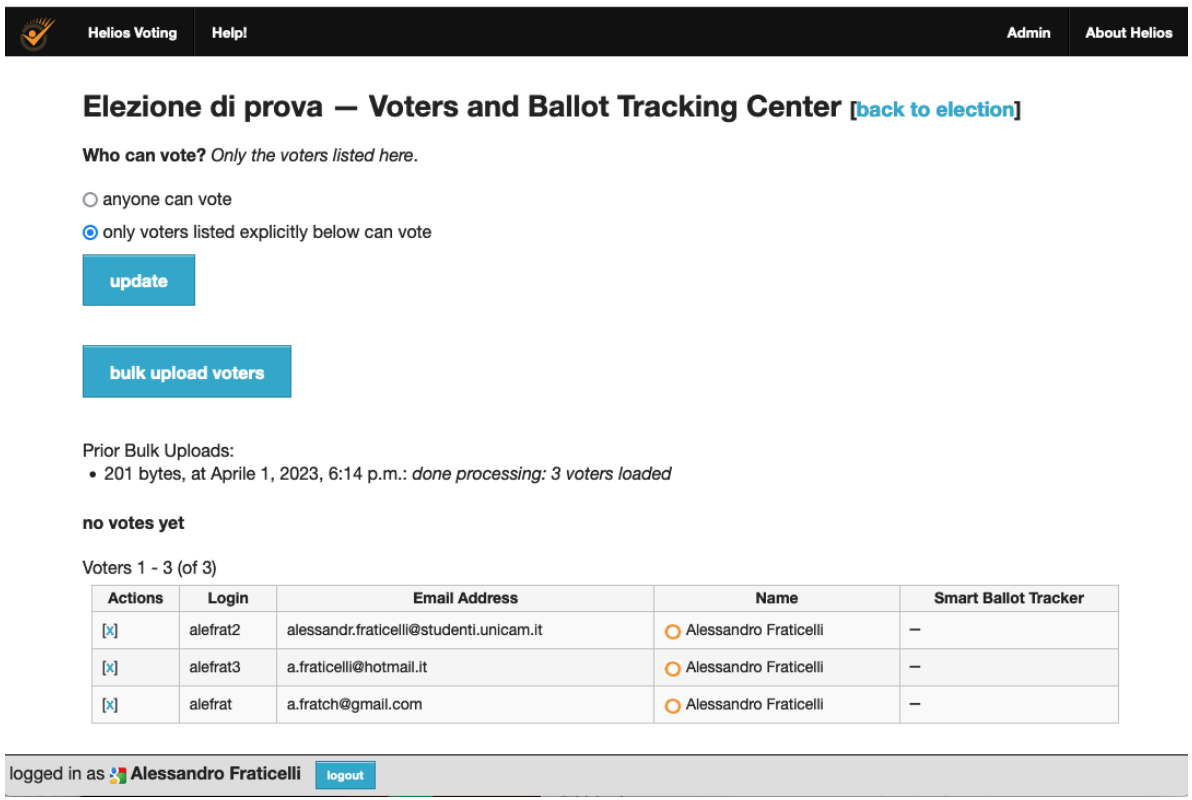
HELIOS - QUESITI



HELIOS - ELETTORI

Helios offre due opzioni principali per definire il gruppo elettorale:

- consentire il voto a chiunque possieda il link dell'elezione;
- caricare un elenco di elettori idonei.

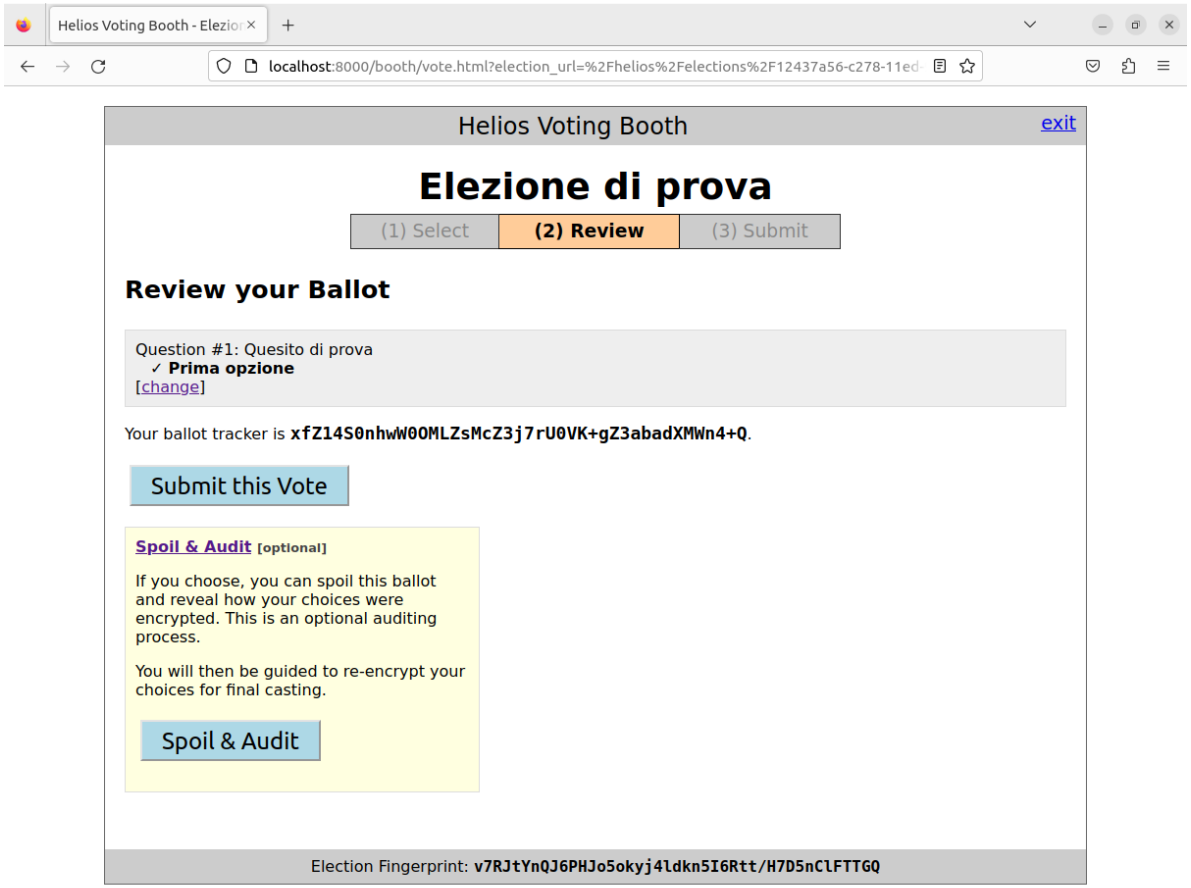


HELIOS - FIDUCIARI

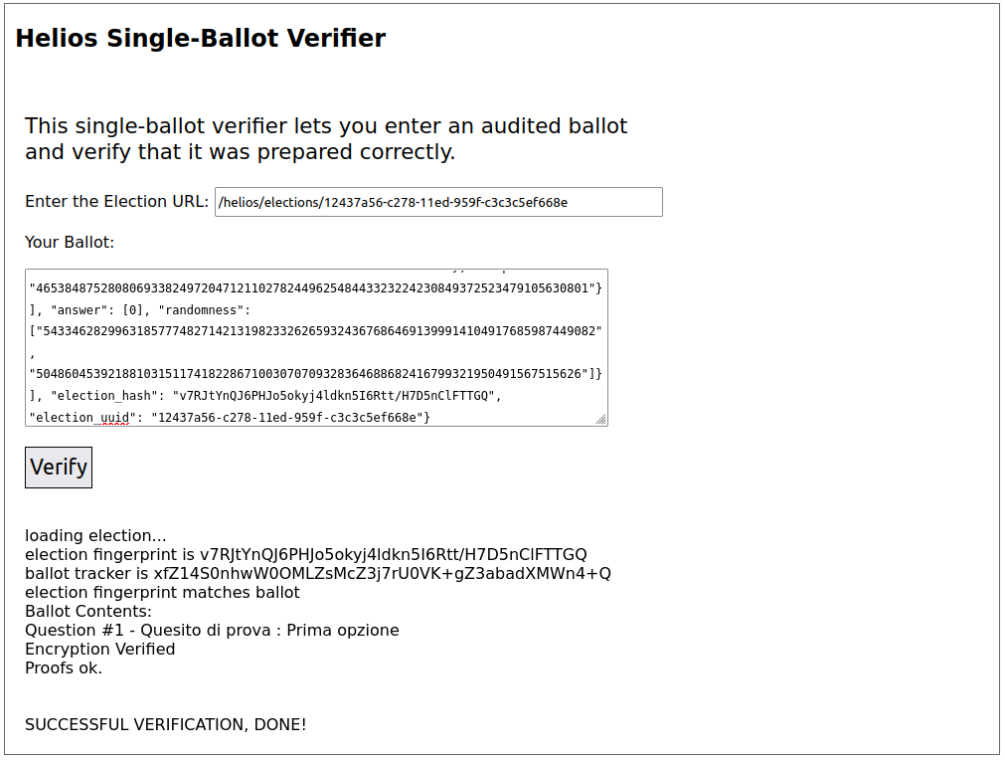
I fiduciari dell'elezione sono le figure alle quali ci si affida per la decrittazione del risultato elettorale. Ognuno di loro genera una coppia di chiavi, (pubblica e una privata) e carica la chiave pubblica sul server Helios. Al momento dello scrutinio, tutti i fiduciari devono partecipare alla decodifica dei risultati elettorali, utilizzando la propria chiave segreta.

HELIOS - VERIFICA DEL VOTO

Se un elettore vuole verificare che il suo voto sia stato espresso correttamente, può decriptare la scheda. Così facendo riceve un testo JSON con tutti i dati della scheda criptata, da inserire nel Single-Ballot Verifier.



HELIOS - VERIFICA DEL VOTO



Il "Single-Ballot Verifier" ottenendo la scheda criptata produce:

- l'hash dell'elezione, verificabile con quello nella "voting booth",
- l'hash del testo cifrato,
- il testo in chiaro della scheda.

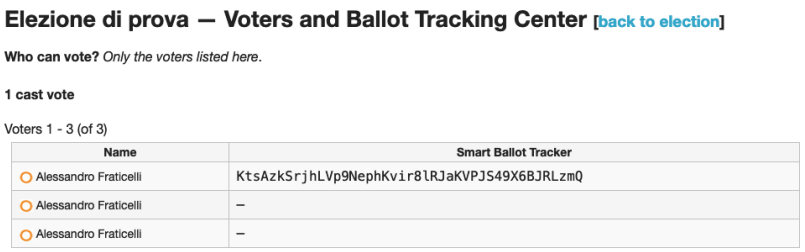
Scrutinio

Terminato il turno di votazione, il server Helios calcola una crittografia del conteggio elettorale, aggregando l'ultima scheda valida ricevuta da ciascun elettore.
Non è possibile ottenere informazioni sul conteggio finché ognuno dei fiduciari non ha inviato la sua decodifica parziale.
Fatto ciò, il server Helios combina le decodifiche parziali ottenendo il conteggio elettorale completo e lo rende disponibile insieme alle informazioni necessarie per la verifica delle elezioni.

VERIFICA

VERIFICA *recorded-as-cast*

L'elettore può compierla controllando il Ballot Tracking Center dell'elezione, che mostra le stringhe identificative di tutte le schede destinate allo scrutinio, e verificando sia presente la propria con la stringa associata.



Conclusioni

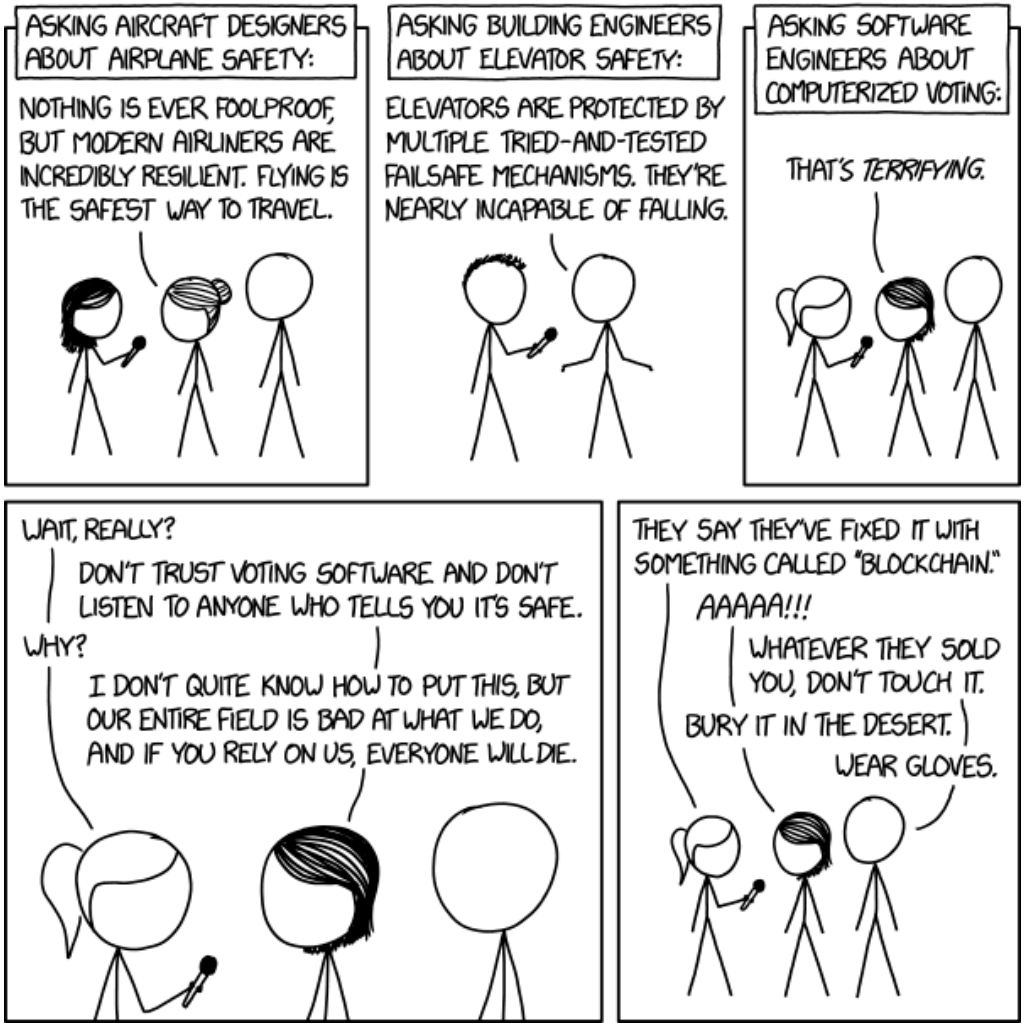


Figure: https://xkcd.com/2030/