



UNIVERSITÀ  
DEGLI STUDI DI BARI  
ALDO MORO

## National Evoting System Smart contract based

### **Lambrusco Team:**

Andrea Di Chicco

Federico Casarano

Roberta Gnisci

Nicola Lopez

Massimiliano Ambruoso

Domenico Ciriello

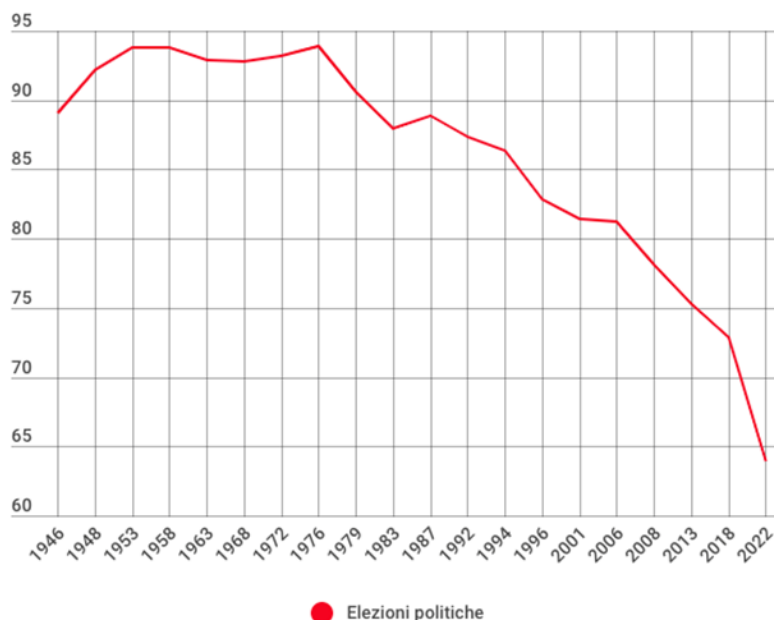
# Contents

<b>1</b>	<b>Introduzione</b>	<b>1</b>
<b>2</b>	<b>L'attuale sistema di votazione</b>	<b>3</b>
2.1	Il voto maggioritario . . . . .	4
2.2	Come eleggiamo i parlamentari . . . . .	4
2.3	I seggi Elettorali . . . . .	6
2.4	Il voto . . . . .	7
2.5	Il flusso di dati nel sistema elettorale . . . . .	15
2.6	Il sistema informatico . . . . .	16
2.7	Scomposizione processo . . . . .	20
<b>3</b>	<b>Il BPR</b>	<b>22</b>
3.1	SELF-SOVEREIGN IDENTITY(SSi) . . . . .	22
3.2	La blockchain . . . . .	26
3.3	Gli smart contract . . . . .	30
3.4	Il nuovo processo . . . . .	33
3.5	La sicurezza . . . . .	42
<b>4</b>	<b>Analisi dei rischi e di realizzazione</b>	<b>45</b>
4.1	Implementazione e-voting da parte di altri stati . . . . .	45
4.2	Formazione e sicurezza . . . . .	47
4.3	Realizzazione e preventivo . . . . .	50
<b>5</b>	<b>Confronto e conclusioni</b>	<b>52</b>

# 1. Introduzione

---

Il nostro progetto nasce a seguito di alcune considerazioni effettuate in merito alle recenti **elezioni** avvenute in Italia. Come è emerso, una gran parte della popolazione è risultata impossibilitata a poter esprimere la propria preferenza, a causa di fattori esterni alla sua volontà. Secondo l'ISTAT le persone a cui viene preclusa la possibilità di esercitare il proprio **diritto di voto** sono circa 4,9 milioni all'anno. Tra questi, la maggior parte sono giovani tra i **18 e i 35 anni**. Che siano studenti o lavoratori, i ragazzi e le ragazze che sono lontani e lontane da casa sono obbligati a pagare per poter recarsi alle urne. Quest'anno, inoltre, la data del 25 settembre ha coinciso con il periodo degli esami universitari di settembre, rendendo l'esercizio del voto ancora più difficile. Italia, Cipro e Malta sono gli unici paesi membri dell'Unione Europea a non garantire il voto per i fuori sede. Alcune categorie di lavoratori, come ad esempio i corpi militari, possono già votare al di fuori del loro comune di residenza. Per gli studenti esistono solamente agevolazioni su treni e aerei, ma presentano una serie di problemi: sono poco pubblicizzati, è difficile accedervi, gli sconti sui treni si applicano solamente a lunghe tratte mentre quelli sui voli solo sulla compagnia di bandiera, per cui il prezzo di base è già molto alto rispetto alle low cost. Un'alternativa a questi due metodi di spostamenti l'ha fornita FlixBus, la nota compagnia di trasporto su gomma. Inviando una mail con la foto della propria tessera elettorale e quella del biglietto acquistato verso il proprio comune di residenza, la compagnia si impegna a rimborsare tutti i suoi viaggiatori con un voucher spendibile per un altro viaggio entro il 31 marzo (escluse le festività natalizie).



L'affluenza alle elezioni politiche del 25 settembre 2022 è stata del **63,9%**, la **più bassa** mai registrata nella storia del nostro Paese. Rispetto all'ultima volta che gli

italiani sono stati chiamati al voto, durante le politiche del 2018, l'affluenza è calata del 9%. Con picchi nelle regioni del Sud, prima di tutte la Calabria dove il 49,2% degli aventi diritto ha scelto di non andare a votare. Nel grafico sopra riportato la percentuale di affluenza al voto per tutte le elezioni per il rinnovo delle Camere dal 1946 a oggi. Lo scarto di 9 punti percentuali registrato all'indomani del 25 settembre 2022 è il più alto tra due tornate elettorali, tra il 2013 e il 2018 era stato infatti del 5%. Dopo la Calabria dove ha votato solo il 50,8% degli aventi diritto, troviamo volumi lievemente più alti in Sardegna con il 53,1% e in Campania dove i votanti sono stati il 53,2%. Rispetto alla tornata elettorale del 2018 in Calabria si registra un calo dell'affluenza del 12,9%. In Sardegna il calo è stato del 12,4%. In Campania la perdita di flusso verso i seggi, rispetto a quattro anni fa, è stata molto più rilevante arrivando a scendere del 14,9%, anche in ragione del nubifragio che ha colpito Napoli e provincia. Nei dati sopra riportati, emergono dei fattori accomunanti:

- essere **residenti** al di fuori del proprio comune di nascita;
- **vincoli reddituali** relativi allo spostamento.

Di certo possiamo anche ricercare fattori socioculturali alla base dei motivi per cui alcune di queste persone non hanno espresso il loro voto. Tuttavia, questo non concerne l'oggetto di questo progetto, il quale vuole proporre una soluzione che in molti ambiti è stata già applicata per risolvere problemi risultanti dei fattori sopra citati. Per quanto riguarda il secondo fattore in particolare, dalle maggiori compagnie di trasporti, sono state proposte delle iniziative per permettere, alle persone residenti all'infuori del comune di nascita, uno spostamento più agevole dal punto di vista economico. Queste iniziative tuttavia hanno avuto un successo limitato, perchè non sono state in grado di offrire un incentivo sufficiente ad effettuare lo spostamento necessario al fine della votazione. La proposta che perciò ci appare scontata fare è quella di un **sistema di voto elettronico**; così facendo non vi sarebbe alcun ostacolo all'esercizio di questo nostro diritto e dovere. Ogni cittadino, con un tale sistema di voto, potrà perciò esprimere le proprie preferenze relative al proprio rappresentate politico, condizione essenziale per uno stato che voglia definirsi come **democratico**.

## 2. L'attuale sistema di votazione

---

Le elezioni politiche a livello nazionale, previste dalla nostra Costituzione ogni cinque anni, servono per eleggere i **membri del Parlamento**, che è composto da due assemblee o camere: la **Camera dei deputati** (con sede a Palazzo Montecitorio) e il **Senato della Repubblica** (con sede a Palazzo Madama). La legge 3 novembre 2017, n. 165, cosiddetto “Rosatellum” (dal nome del deputato Ettore Rosato, che l’ha proposta), attraverso una serie di modifiche ai testi unici per l’elezione della Camera dei deputati e del Senato della Repubblica, rispettivamente, il d.P.R. 30 marzo 1957, n. 361, e il d.l.gs. 20 dicembre 1993, n. 533, ha trasformato il sistema di elezione di entrambe le Camere, delineando un sistema elettorale misto: deputati e senatori sono eletti in parte con un sistema “maggioritario uninominale” e in parte con un sistema proporzionale (o plurinominale). La legge costituzionale 19 ottobre 2020, numero 1 ha modificato gli articoli 56 e 57 della Costituzione prevedendo rispettivamente per la Camera un numero di deputati pari a 400, otto dei quali eletti nella circoscrizione Estero, e 200 senatori, 4 dei quali eletti nella circoscrizione Estero, stabilito in seguito al referendum costituzionale del 2020, che ha “tagliato” di fatto i parlamentari. In precedenza, vi erano 630 deputati e 315 senatori. Deputati e senatori sono eletti dai cittadini, con l’eccezione dei senatori a vita, nominati dal Presidente della Repubblica per particolari meriti, e dei senatori di diritto, cioè gli ex Presidenti della Repubblica (anch’essi in carica a vita). Per essere eletti alla Camera bisogna aver compiuto **25 anni**, mentre per essere eletti al Senato bisogna averne **almeno 40**. Contemporaneamente detiene il diritto di voto alle elezioni politiche qualsiasi cittadino italiano che abbia compiuto **18 anni** (prima del 2021 il voto per il Senato richiedeva di aver compiuto **25 anni d’età**).

## 2.1 Il voto maggioritario

### Sistema maggioritario uninominale

Considerando il sistema maggioritario uninominale, i collegi sono **147 per la Camera** e **74 per il Senato**. In ogni collegio è eletto in Parlamento un solo **rappresentante** e ogni partito o coalizione di partiti candida una sola persona a sua scelta. Viene eletto il candidato che ottiene il maggior numero di voti. È per questo motivo che il sistema si chiama maggioritario uninominale. Quindi, grazie a questo primo sistema, vengono eletti 147 deputati e 74 senatori.

### Sistema proporzionale plurinominale

Considerando il sistema proporzionale, il territorio italiano è suddiviso in collegi "plurinomiali": sono 49 per la Camera e 26 per il Senato. In ognuno di questi collegi si elegge **più di un rappresentante** (motivo per cui il sistema si dice "plurinominale") : a seconda di quanto è grande la popolazione del collegio considerato, sono eletti da uno a otto parlamentari, con alcune eccezioni. In ogni collegio plurinominale possono presentarsi sia liste singole, composte da un solo partito non alleato con altri, sia coalizioni composte da più partiti, che presentano tante liste di candidati quanti sono i partiti che la compongono. Ogni lista deve contenere da due a quattro candidati al massimo. I seggi sono assegnati ai partiti proporzionalmente ai voti ricevuti. Gli elettori **non esprimono preferenze per i candidati**, ma, votando per un partito, approvano potenzialmente in blocco la **lista dei candidati**. Questi ultimi sono eletti in base all'ordine con il quale sono presentati. Se, per esempio, la lista X ha ottenuto due seggi, andranno in Parlamento i primi due candidati dell'elenco.

## 2.2 Come eleggiamo i parlamentari

I membri del Parlamento sono eletti nel modo seguente:












- **il 37%** (147 deputati e 74 senatori) con il sistema maggioritario uninominale;
- **il 61%** (245 deputati e 122 senatori) con il sistema proporzionale (o plurinominale);
- **il 2%** (8 deputati e 4 senatori) tra gli italiani all'estero, che votano con il proporzionale e possono esprimere le preferenze sui parlamentari da scegliere, all'interno della lista del partito che votano.

Al seggio, ogni cittadino vota esprimendo **una sola preferenza** per ciascuna delle due Camere. I candidati all'uninominale, infatti, sono automaticamente collegati a una lista proporzionale. Se si vota per un candidato all'uninominale, perciò, il voto vale automaticamente anche per la lista proporzionale collegata e viceversa. Il nostro sistema proporzionale prevede anche una **soglia di sbarramento**, cioè una percentuale minima di voti che partiti e coalizioni devono raggiungere a livello nazionale per far entrare i loro candidati in Parlamento. Chi non la raggiunge non elegge nessun deputato o senatore.

Le soglie sono le seguenti:

- **3%** del totale dei voti per le liste singole, con eccezioni per le liste che rappresentano minoranze linguistiche e, solo al Senato, per quelle che superano il 20% in una qualunque Regione;
- **10%** del totale dei voti per le coalizioni.

La scheda di sintesi:

		 Camera dei Deputati	 Senato della Repubblica
	Circoscrizioni	28	20
	Collegi uninominali (seggi)	147	74
	Collegi plurinominali	49	26
	Numero seggi nei collegi plurinominali	245	122
	Eletti con maggioritario (collegi uninominali)	37%	
	Eletti con proporzionale (collegi plurinominali e circoscrizione Estero)	63%	
	Candidati uninominali e listini "bloccati"	1 candidato per lista/coalizione nel collegio uninominale da 2 a 4 candidati nel collegio plurinominale	
	Pluricandidature	Lo stesso candidato può candidarsi al massimo in 5 collegi plurinominali e in un collegio uninominale. Il candidato nella circoscrizione Estero non si può candidare in nessun collegio plurinominale o uninominale.	
	Parità di genere	Massimo 60% uomini e 40% donne, o viceversa.	
	Voto disgiunto	NO	
	Preferenze	NO	
	Soglie di sbarramento (partecipano al riparto dei seggi)	Le liste singole che ottengono almeno il 3% dei voti validi a livello nazionale ovvero, per il Senato, le liste singole che hanno ottenuto almeno il 20% regionale. Le coalizioni di liste che ottengono sul piano nazionale almeno il 10% dei voti validi e che contengono almeno una lista collegata che ha ottenuto almeno il 3% dei voti, ovvero, per il Senato, una lista collegata che abbia raggiunto almeno il 20% a livello regionale.	
	Premio di maggioranza	NO	
	Ballottaggio (2° turno di votazione)	NO	

## 2.3 I seggi Elettorali

Ai fini delle operazioni di voto e scrutinio, per ogni sezione è istituito un **Ufficio elettorale di sezione**, così composto (articolo 34 del testo unico di cui al d.P.R. n. 361/1957):

Ruolo	Nominato	Requisiti essenziali per la nomina	Data nomina in generale	Seggio ordinario e sezione ospedaliera	Seggio speciale	Seggio volante
				numero componenti		
Presidente	dal Presidente della Corte di Appello	Iscrizione all'Albo dei presidenti di seggio	entro il 30° giorno antecedente la votazione	1	1	1 (del seggio ordinario)
Vice presidente	tra gli scrutatori	di legge	all'atto dell'insediamento del seggio	1 (tra gli scrutatori)	-	-
Scrutatore	dalla Commissione elettorale comunale	Iscrizione all'Albo degli scrutatori di seggio	mediante nomina tra il 25° ed il 20° giorno antecedente la votazione	4	2	1 (del seggio ordinario)
Segretario	dal Presidente	di legge	prima della costituzione dell'Ufficio elettorale di sezione	1	1 (tra i 2 scrutatori)	1 (del seggio ordinario)

## La tessera elettorale

La tessera elettorale personale, prevista dall'articolo 13 della legge 30 aprile 1999, n. 120, ed istituita con d.P.R. 8 settembre 2000, n. 299, attesta la **regolare iscrizione** dell'elettore nelle liste elettorali del comune in cui risiede. E' un documento ufficiale a **carattere permanente**, che permette di esercitare il diritto di voto, unitamente ad un documento di identificazione, in occasione di ogni elezione o referendum [articolo 1, d.P.R. 299/2000 ]; essa è utilizzabile fino ad un massimo di **18 consultazioni**, corrispondenti agli spazi utili al suo interno per l'apposizione del bollo della sezione elettorale al momento del voto [articolo 2, comma 3, d.P.R. n. 299/2000 ]. La tessera elettorale:

- contiene il cognome e nome dell'elettore, e, il luogo e la data di nascita, la data e l'Autorità che l'ha rilasciata, l'indirizzo dell'elettore, il numero e l'indirizzo della sezione alla quale l'elettore è iscritto e assegnato, il collegio o la circoscrizione o la regione nelle quali può esprimere il diritto di voto in ciascun tipo di elezione, le note e avvertenze e l'eventuale data di aggiornamento della tessera;
- è idonea a certificare l'avvenuta partecipazione al voto nelle singole consultazioni elettorali (politiche, europee, regionali, comunali e circoscrizionali) e referendarie;
- è valida fino all'esaurimento degli appositi spazi per la certificazione dell'avvenuta



partecipazione alla votazione.

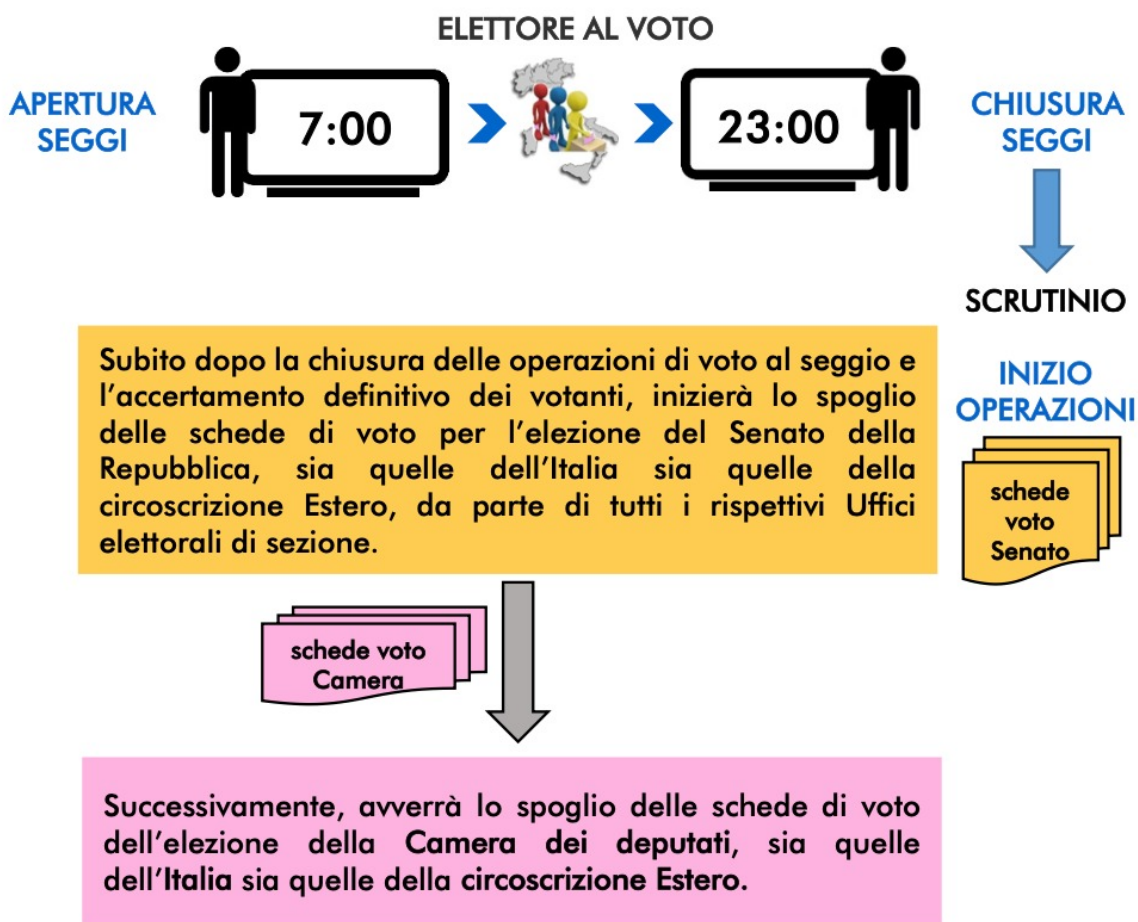
## 2.4 Il voto

Ciascun elettore dispone di un voto da esprimere su **un'unica scheda per consultazione** (una per la Camera e una per il Senato), recante il nome del candidato nel collegio uninominale e il contrassegno di ciascuna lista o, nel caso di liste in coalizione, i contrassegni di tali liste, con a fianco i nominativi dei candidati, da 2 a 4 (cosiddetto “listino bloccato”), nel collegio plurinominale (articoli 31 e 58 del testo unico Camera di cui al *d.P.R. n. 361/1957*, e articoli 11 e 14 del testo unico Senato di cui al *d.lgs. n. 533/1993*, modificati dalla *legge n. 165/2017*). L'elettore, **a seguito dell'identificazione**, riceve le schede di voto e la matita copiativa ed esprime il proprio voto, in segreto, nella cabina indicata da uno dei componenti del seggio. Per poter votare occorre presentarsi con:

- la tessera elettorale con almeno uno spazio vuoto dei diciotto previsti per la certificazione del voto, o l'attestato del sindaco sostitutivo della tessera;
- un documento di riconoscimento per l'identificazione. I documenti di riconoscimento ammessi al seggio sono compresi in tre categorie [*articolo 57, secondo comma, testo unico di cui al d.P.R. n. 361/1957*].

### Obblighi dell'elettore

- Se l'elettore non vota nella cabina, le schede consegnategli sono annullate.
- Se l'elettore, dopo avere ritirato le schede, prima ancora di entrare in cabina, le riconsegna al presidente senza alcuna espressione di voto, le schede sono annullate.
- Se una scheda votata viene riconsegnata non ripiegata, il presidente invita l'elettore a ripiegarla facendolo rientrare nella cabina.
- L'elettore non deve sovrapporre le schede una sull'altra al momento dell'espressione del voto, per evitare che il segno di voto tracciato su una scheda sia visibile anche su quella sottostante.
- L'elettore non può esprimere preferenze (scrivendo il cognome e nome di un candidato) nè votare per una lista non collegata al candidato nel collegio uninominale (cosiddetto “voto disgiunto”).



È stato illustrato il modo in cui l'elettore esprime il voto nel luogo di residenza. Il nostro progetto ha come obiettivo quello di presentare una valida alternativa alle operazioni di voto, volta a semplificare il processo per chi è impossibilitato a recarsi nel seggio di residenza. Di seguito, riportiamo alcune casistiche inerenti alle categorie di individui, soggetti a complicazioni sanitarie, burocratiche e logistiche, che esprimono il proprio diritto al voto in maniera differente.

La legge prevede che possano votare in Italia fuori del comune di residenza solo alcune categorie di elettori:

#### **1. Il voto domiciliare per gli elettori affetti da infermità che ne rendano impossibile l'allontanamento dall'abitazione**

Sono ammessi al voto domiciliare, in un qualsiasi comune, gli elettori affetti da **gravissime infermità**, tali che l'allontanamento dall'abitazione in cui dimorano risulti impossibile, anche con l'ausilio dei servizi di trasporto e accompagnamento, e gli elettori affetti da gravi infermità che si trovino in condizioni di dipendenza continuativa e vitale da apparecchiature elettromedicali tali da impedirne l'allontanamento dall'abitazione in cui dimorano [articolo 1 del decreto-legge n. 1/2006, come modificato dalla legge n. 46/2009]. L'elettore interessato deve far pervenire al sindaco del comune nelle cui liste elettorali è iscritto, in un periodo compreso fra il 40° e il 20° giorno antecedente la data

di votazione, quanto segue:

- un'espressa dichiarazione in carta libera attestante la propria volontà di esprimere il voto presso l'abitazione in cui dimora e recante la indicazione dell'indirizzo completo di questa, possibilmente, con un recapito telefonico;
- un certificato, rilasciato dal funzionario medico, designato dai competenti organi dell'azienda sanitaria locale, in data non anteriore al 45° giorno antecedente la data della votazione, che attesti l'esistenza delle condizioni di infermità di cui all'articolo 1, comma 1, del *decreto-legge 3 gennaio 2006, n. 1*, convertito con modificazioni dalla *legge 27 gennaio 2006, n. 22*, come modificato dalla *legge n. 46/09*;
- una copia della tessera elettorale.

La raccolta del voto avviene a cura dell'**Ufficio distaccato di sezione** o "**seggio volante**" durante le ore in cui è aperta la votazione, assicurando, con ogni mezzo idoneo, la libertà e la segretezza del voto nel rispetto delle esigenze connesse alle condizioni di salute dell'elettore.

## **2. L'esercizio domiciliare del voto per gli elettori sottoposti a trattamento domiciliare o in condizioni di isolamento per Covid-19**

Gli elettori sottoposti a trattamento domiciliare o in condizioni di isolamento per Covid-19 sono ammessi ad esprimere il voto presso il proprio domicilio nel comune di residenza [articolo 4, comma 1, *D.L. 4 maggio 2022, n. 41*]. Tali elettori devono far pervenire al sindaco del comune nelle cui liste sono iscritti:

- una dichiarazione attestante la volontà di esprimere il voto presso il proprio domicilio e recante l'indirizzo completo di questo;
- un certificato, rilasciato dal funzionario medico designato dai competenti organi dell'azienda sanitaria locale, in data non anteriore al quattordicesimo giorno antecedente la data della votazione, che attesti l'esistenza delle suddette condizioni sanitarie per Covid-19.

La raccolta del voto avviene a cura dell'**Ufficio distaccato di sezione** o "**seggio volante**" durante le ore in cui è aperta la votazione.

## **3. Il voto degli elettori degenti in ospedali e case di cura, dei ricoverati in case di riposo e i tossicodipendenti degenti presso comunità**

*Sono ammessi a votare nel luogo di ricovero, se iscritti nelle liste elettorali dello stesso comune o di altro comune del territorio nazionale, previa esibizione della tessera elettorale [articoli 51, 52 e 53, testo unico di cui al d.P.R. n. 361/1957].*

Gli interessati devono fare pervenire, non oltre il terzo giorno antecedente la data della votazione, al sindaco del comune nelle cui liste elettorali sono iscritti, una dichiarazione attestante la volontà di esprimere il voto nel luogo di cura.

La dichiarazione deve espressamente riportare:

- il numero della sezione elettorale alla quale l'elettore è assegnato;
- il numero di iscrizione dell'elettore nella lista elettorale di sezione, risultante dalla tessera elettorale;
- l'attestazione in calce del direttore sanitario del luogo di cura, comprovante il ricovero dell'elettore nell'istituto e deve essere inoltrata al comune di destinazione per il tramite del direttore amministrativo o del segretario dell'istituto stesso.

## 5. Il voto dei detenuti

I detenuti in possesso del diritto di elettorato attivo sono ammessi a votare all'interno del **luogo di reclusione** o custodia preventiva [*articolo 8, legge n. 136/1976, modificato dall'articolo 13, comma 1, d.P.R. n. 299/2000*]. Il detenuto elettore deve far pervenire, non oltre il terzo giorno antecedente la data della votazione, per il tramite del direttore dell'Istituto di prevenzione e pena, al sindaco del comune nelle cui liste elettorali è iscritto, una dichiarazione attestante la volontà di esprimere il voto nel luogo in cui si trova. La dichiarazione deve espressamente riportare:

- il numero della sezione alla quale l'elettore è assegnato;
- il numero di iscrizione nella lista elettorale di sezione, risultante dalla tessera elettorale;
- l'attestazione del direttore dell'istituto comprovante la detenzione dell'elettore.

## 6. Il voto assistito

Gli elettori affetti da grave **infermità fisica**, che non possono esercitare autonomamente il diritto di voto e hanno bisogno dell'assistenza di un altro elettore per esprimere il proprio voto al seggio, possono richiedere al comune di iscrizione elettorale l'annotazione permanente del diritto al voto assistito, mediante apposizione di un corrispondente simbolo o codice nella tessera elettorale personale, nel rispetto delle disposizioni vigenti in materia di riservatezza personale [*articolo 1, comma 2, legge 5 febbraio 2003, n. 17*]. Tale annotazione evita all'elettore, fisicamente impedito, di doversi munire di volta in volta, in occasione di ogni consultazione elettorale, dell'apposito certificato medico. Possono usufruire del voto assistito con un accompagnatore in cabina gli elettori [*articolo 55, secondo comma, T.U. n. 361/1957, modificato dall'articolo 1, comma 1, legge n. 17/2003*]:

- non vedenti;
- amputati delle mani;
- affetti da paralisi;
- con gravi impedimenti fisici, che rendono impossibile l'esercizio autonomo del voto.

Gli elettori esprimono il voto con l'assistenza di un accompagnatore di fiducia nella cabina elettorale, che può essere un elettore della propria famiglia o, in mancanza di esso, di un altro elettore liberamente scelto, purché l'uno o l'altro sia iscritto nelle liste

elettorali in un qualsiasi comune della Repubblica Italiana [articolo 29, comma 3, *legge n. 104/1992*, e articolo 55, comma 2, testo unico di cui al *d.P.R. n. 361/1957*].

## 7. Il voto all'Estero

Il voto degli elettori italiani residenti all'estero iscritti all'**AIRE**: la circoscrizione Estero. La circoscrizione Estera è prevista *dall'articolo 48 della Costituzione e l'articolo 6, comma 1, della legge n. 459/2001* individua nel suo interno le seguenti **quattro ripartizioni** comprendenti Stati e territori afferenti a:

1. Europa, compresi i territori asiatici della Federazione russa e della Turchia;
2. America meridionale;
3. America settentrionale e centrale;
4. Africa, Asia, Oceania e Antartide.

Sono ammessi al voto per corrispondenza gli elettori iscritti all'AIRE e gli elettori italiani che si **trovano temporaneamente all'estero** per almeno tre mesi, per motivi di lavoro, studio o cure mediche, nonché i familiari conviventi all'estero che hanno presentato domanda di voto per corrispondenza all'estero al proprio comune. Il Ministero dell'interno consegna al Ministero degli Affari Esteri e della Cooperazione Internazionale i modelli delle schede elettorali, per l'elezione della Camera dei deputati e per il Senato della Repubblica, non più tardi del 26° giorno antecedente la data della consultazione. Gli Uffici consolari, ai sensi dell'articolo 12, terzo comma, della legge n. 459/2001, spediscono “...con il sistema postale più affidabile e, ove possibile, con posta raccomandata, o con altro mezzo di analoga affidabilità...”, alla residenza di tutti gli elettori, non oltre 18 giorni prima della data stabilita per le votazioni in Italia, il plico elettorale. Il plico elettorale contiene:

- foglio informativo;
- due schede elettorali, una per l'elezione della Camera dei deputati, una per il Senato della Repubblica;
- busta piccola di colore bianco per contenere le schede votate dall'elettore;
- liste dei candidati nella circoscrizione Estero, suddivise per le 4 ripartizioni, sia per la Camera, sia per il Senato;
- certificato elettorale;
- busta preaffrancata per la restituzione al Consolato.

*Gli Stati in cui non si vota per corrispondenza*

**Ripartizioni della circoscrizione Estero:**

<b>a)</b>	<b>EUROPA</b>
<b>b)</b>	<b>AMERICA MERIDIONALE</b>
<b>c)</b>	<b>AMERICA SETTENTRIONALE E CENTRALE</b>
<b>d)</b>	<b>AFRICA, ASIA, OCEANIA E ANTARTIDE</b>

STATO	RIPARTIZIONE AFFERENTE
AFGHANISTAN	d)
BHUTAN	d)
BURKINA FASO	d)
CIAD	d)
COSTA D'AVORIO	d)
CUBA	c)
ERITREA	d)
IRAQ	d)
LIBERIA	d)
LIBIA	d)
NIGER	d)
REPUBBLICA CENTRAFRICANA	d)
REPUBBLICA DEL SUD SUDAN	d)
REPUBBLICA POPOLARE DEMOCRATICA DI COREA	d)
SIERRA LEONE	d)
SIRIA	d)
UCRAINA	a)
YEMEN	d)
ZIMBABWE	d)

Inoltre, i rappresentanti di lista, designati dai partiti, possono esprimere il diritto di voto presso il seggio in cui svolgono tali funzioni qualora siano elettori dello stesso collegio plurinominale alla Camera e della stessa regione al Senato. Per gli elettori che, non rientrando in tali categorie, per esercitare il diritto di voto devono obbligatoriamente raggiungere il comune di residenza recandosi presso il proprio seggio di iscrizione elettorale.

## LO SCRUTINIO DEL VOTO ESPRESSO IN ITALIA

I dati ufficiosi sul voto affluiranno al Ministero dell'interno attraverso la rete dipartimentale con le **Prefetture-UTG** e/o direttamente dai comuni tramite il Sistema Informativo Elettorale (**S.I.EL.**).

### Votanti

Ogni comune dovrà comunicare i dati sull'affluenza alle urne, sia nel corso della votazione sia alla chiusura delle operazioni di voto:

- notizie sul dato assoluto dei votanti (solo totale) alle ore 12:00;
- notizie sul dato assoluto dei votanti (solo totale) alle ore 19:00;
- notizie sul dato assoluto dei votanti alle ore 23:00, ovvero alla chiusura delle operazioni di votazione, distinti in uomini, donne e totale.

### Scrutini

Terminate le operazioni di voto, alle ore 23, dopo aver accertato il numero dei votanti definitivo, iniziano le **operazioni di scrutinio** da parte di tutti gli Uffici elettorali di sezione. Prima viene eseguito lo spoglio delle schede per l'elezione del Senato della Repubblica, successivamente, al termine, quelle per l'elezione della Camera dei deputati. Lo scrutinio deve svolgersi senza alcuna interruzione e deve essere ultimato entro le ore 14 del giorno seguente (articolo 73, primo comma, testo unico di cui al *d.P.R. n. 361/1957*). Solo se, per causa di forza maggiore, le operazioni di scrutinio non possono essere ultimate entro il termine prescritto, il presidente dell'Ufficio elettorale di sezione le deve sospendere (articolo 73, secondo comma, testo unico di cui al *d.P.R. n. 361/1957*). Le operazioni di scrutinio saranno completate, utilizzando le stesse tabelle di scrutinio usate dai seggi, dall'Ufficio elettorale regionale, per l'elezione del Senato, o dall'Ufficio elettorale circoscrizionale, per l'elezione della Camera.

VOTI NULLI					VOTI VALIDI																																																												VOTI CONTESTATI E PROVVISORIAMENTE ASSEGNA TI																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																								
COMPRESI I VOTI CONTESTATI E PROVVISORIAMENTE ASSEGNA TI																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									
1	2	3	4	5	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9

Dalle ore 23:00 del giorno di votazione verranno diffuse progressivamente, sulla base dei dati che affluiranno a chiusura delle varie sezioni, le seguenti comunicazioni:

- il numero delle sezioni scrutinate;
- il totale dei voti ottenuti da tutti i candidati uninominali;

- il numero dei voti validi ottenuti da ciascun candidato uninominale;
- il numero dei voti espressi solo in favore di ciascun candidato uninominale;
- il totale dei voti ottenuti da tutte le liste;
- il numero dei voti validi ottenuti da ciascuna lista.

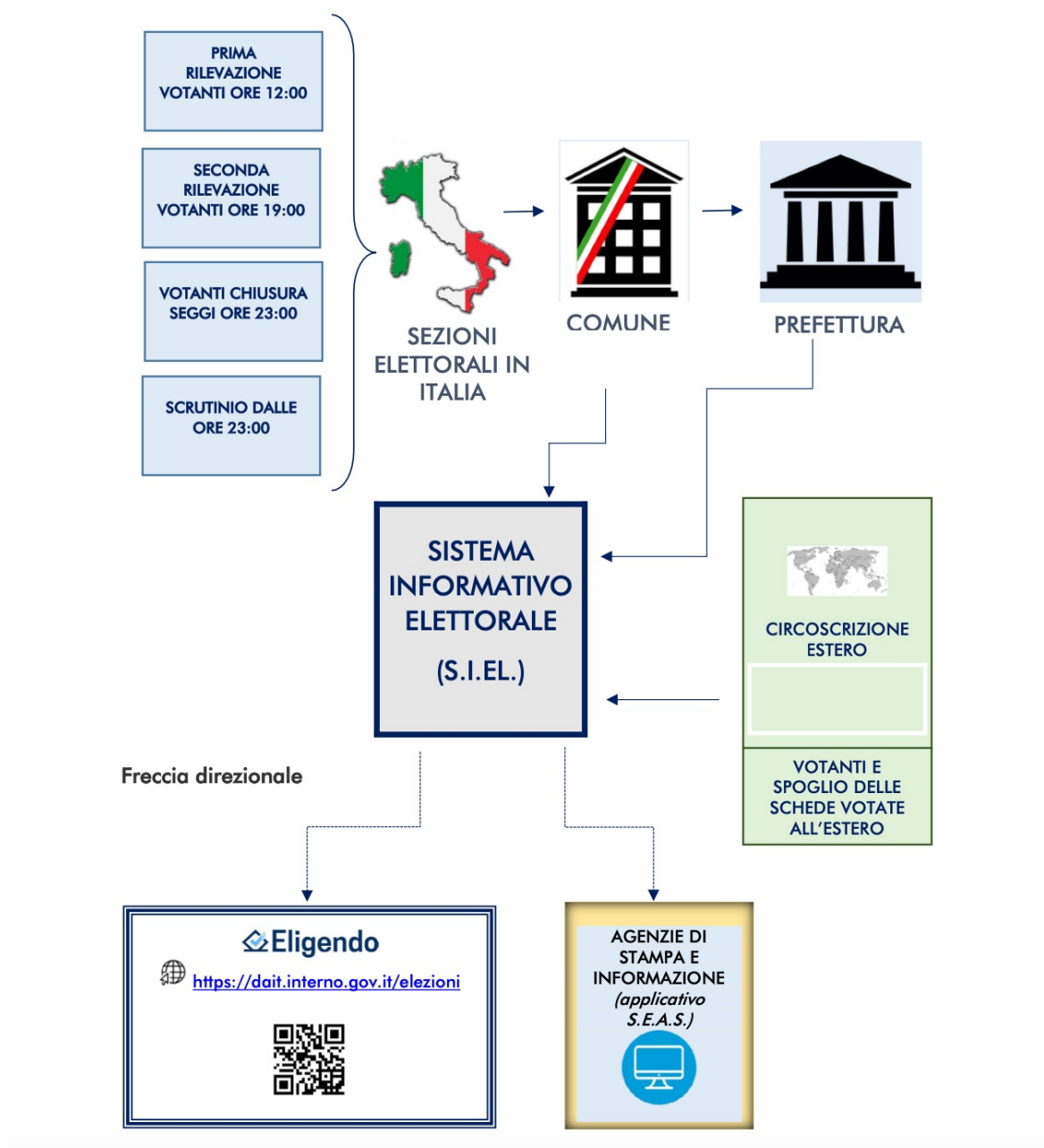
Il ruolo della Prefettura-UTG è fondamentale nell'organizzazione della **raccolta e della diffusione degli esiti** di ogni consultazione elettorale e referendaria, nella supervisione e monitoraggio delle attività sia nelle fasi pre-elettorali sia nella fase di scrutinio. I risultati elettorali ufficiali che vengono trasmessi dai comuni devono, infatti, essere validati dagli Uffici elettorali della Prefettura- UTG prima della loro diffusione da parte del **Ministero dell'interno**. La comunicazione dei risultati complessivi di tutte le sezioni di ogni comune dovrà comprendere anche il numero delle schede bianche, nulle nonché di quelle contestate e non assegnate. I risultati ufficiali saranno diffusi sul sito internet dal Ministero dell'interno:

- ITALIA, a livello comune, collegio uninominale, collegio plurinominale, circoscrizione/regione e nazione;
- ESTERO, a livello Stato, ripartizione della circoscrizione Estero e in complesso.



## 2.5 Il flusso di dati nel sistema elettorale

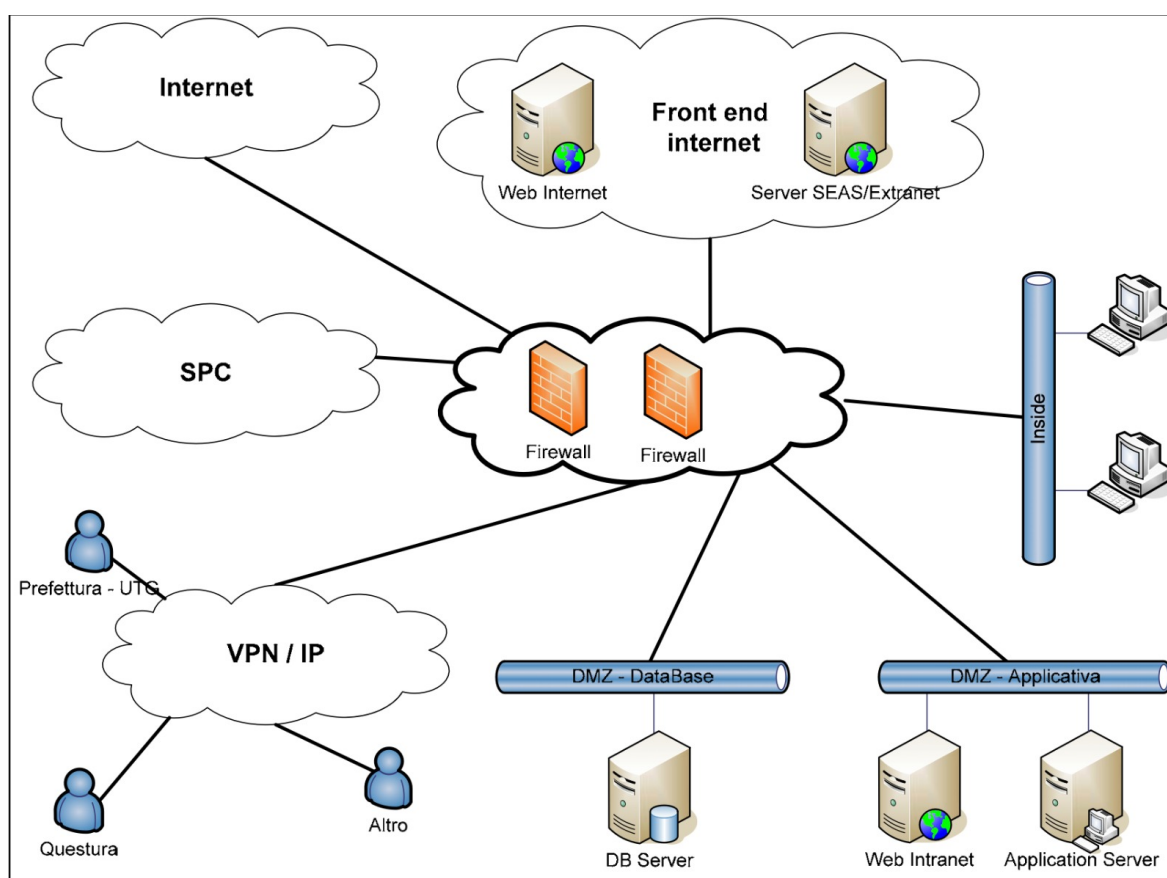
In definitiva, il dato attestante la preferenza di ogni singolo individuo votante viene trasmesso da ogni **Comune italiano** direttamente alla **Prefettura** qualora quest'ultimo non sia adeguatamente informatizzato, attraverso canali tradizionali e supporti cartacei. Per grandi Comuni, per Comuni informatizzati e per la Circoscrizione Estero, il dato viene direttamente inserito nel **archivio centrale** del S.I.EL (Sistema Informativo Elettorale) e successivamente pubblicato a cura di **Eligendo** e dalle agenzie di stampa e informazione autorizzate. La condivisione del dato avviene seguendo le modalità previste dalle Prefetture-UTG, definite in precedenza.



## 2.6 Il sistema informatico

Il Sistema Informativo Elettorale (S.I.E.L.) si compone di risorse, processi e metodi volti alla gestione e analisi dei dati in tempo reale e rappresenta la via principale con la quale lo Stato gestisce le informazioni ricavate dalle elezioni politiche nazionali. Per quanto riguarda la gestione automatizzata delle informazioni, lo Stato, in particolare il Ministero Degli Interni, utilizza il **Sistema Informatico Elettorale (SIE)**. SIE gestisce una **LAN** divisa in tre zone principali:

- una dmz per i DB su cui risiedono i server sui quali girano i motori degli RDBMS (sistema di gestione di database relazionali) di SIE;
- una dmz per gli application server;
- una LAN di client su cui sono attestati i pc client di SIE stesso.



Esistono poi, collegate alla LAN di SIEL, **ulteriori LAN** su cui sono attestati anche i web server di SIEL con visibilità su Internet, nonché i web server per la extranet (agenzie + sala Procedura Elettorale stampa) e i server che gestiscono il SEAS (Servizio Elettorale per le Agenzie di Stampa).

La LAN di SIEL si attesta anche sulla **VPN/IP del Ministero dell'Interno** che permette lo scambio di informazione tra gli Uffici centrali e gli Uffici periferici (Prefetture – UTG per esempio) del Ministero dell'Interno. Le funzionalità ed i servizi dell'Applicazione Elettorale gestiscono l'acquisizione e la diffusione dei dati relativi alle

varie fasi di ciascun evento elettorale in corso. L'attuale sistema è stato realizzato con l'utilizzo di tecnologie di nuova generazione.

## **APPLICAZIONE ELETTORALE**

Finalizzata alla gestione di tutte le informazioni relative alle fasi: pre-elettorale (dati retrospettivi, seggi, sezioni, comunicazioni, elettori, liste, candidature, anagrafica candidati, contrassegni) ed elettorale (insediamento sezioni, votanti, scrutini liste e candidati, preferenze).

-DDE Consente di diffondere le informazioni prodotte e/o utilizzate nell'arco delle fasi successive di ogni evento elettorale.

-SEAS Gestisce la diffusione dei dati elettorali alle Agenzie di stampa e ad altri organi quali partiti politici ed Enti di ricerca accreditati presso il Ministero dell'Interno.

-Query a richiesta Permette la visualizzazione e la stampa dei dati pre-elettorali ed elettorali. A tal fine l'utente può utilizzare interrogazioni già predisposte da SIE del Ministero.

## **PRINCIPALI FUNZIONALITA'**

Il ciclo di vita di ogni evento elettorale comincia con l'effettiva **preparazione dell'ambiente**, che si basa sulla tipologia di elezione e sugli enti partecipanti, e termina con la storicizzazione dei dati acquisiti prevedendo come fasi intermedie un pre-elettorale (raccolta di informazioni sul numero delle sezioni elettorali, degli iscritti nelle liste elettorali di ciascun Comune e delle informazioni relative alle liste presentate), un elettorale (acquisizione affluenze alle urne, insediamento seggi e informazioni relative allo scrutinio) e un post-elettorale (storicizzazione dei dati ufficiosi). La maggior parte di queste fasi richiede l'invio di informazioni da parte dei Comuni verso la **Prefettura-UTG** di competenza, che a loro volta le tramettono a SIE. Le criticità rappresentate dalla soluzione attuale comportano:

Ritardo nelle comunicazioni

Il dato relativo ai votanti ed agli scrutini è disponibile presso la Prefettura - UTG in tempi relativamente rapidi, mentre l'acquisizione dello stesso dato sui sistemi di SIE avviene solo in un momento successivo.

Possibilità di errore

Per consentire la comunicazione a SIE dei dati, eventualmente, archiviati sui sistemi informatici della Prefettura - UTG è necessario che l'operatore inserisca a mano gli stessi dati utilizzando l'interfaccia web del sistema elettorale. La possibilità di errore legata all'attività di reinserimento manuale delle informazioni potrebbe causare il mancato allineamento tra i dati registrati in Prefettura - UTG e quelli trasmessi a SIE. Allo stato attuale non esiste procedura informatizzata che, consentendo la comunicazione informatica diretta tra i Comuni e SIE, possa garantire il superamento delle criticità descritte.

## PRINCIPALI FUNZIONALITA' APPLICAZIONE DDE

Attualmente SIE realizza la diffusione dei dati elettorali ufficiosi tramite i seguenti canali:

1) **Siti web** La componente DDE del Sistema Elettorale genera tre siti web per la **visualizzazione dei dati elettorali**. Il primo (<http://elezioni.interno.it>, "Eligendo") è un sito web accessibile su Internet i cui contenuti sono rivolti a tutti i cittadini;

Il secondo è un sito web accessibile sulla rete Intranet del Ministero dell'Interno i cui contenuti sono rivolti, principalmente, agli operatori della sala stampa istituita presso la sede del Viminale del Ministero dell'Interno;

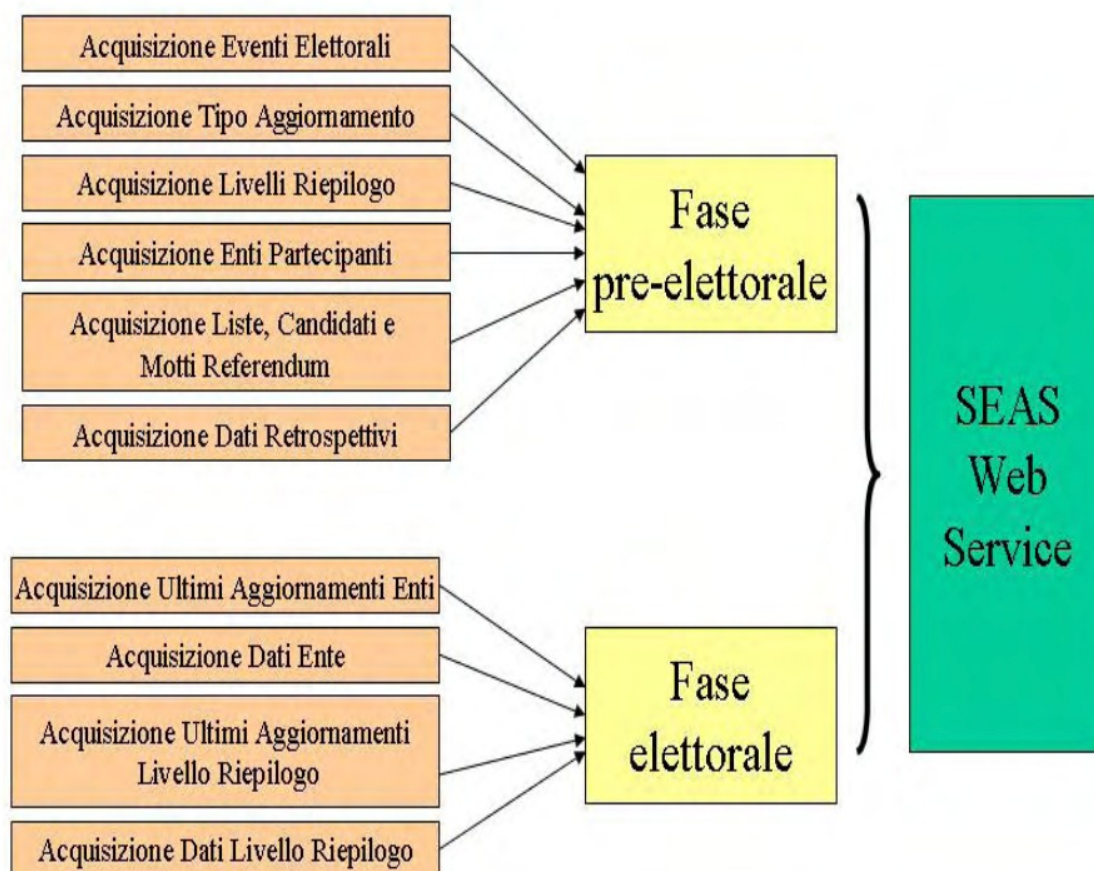
Il terzo è un sito web detto "extranet" ovvero una rete intranet rivolta agli Uffici della Presidenza della Repubblica, Senato della Repubblica, Camera dei Deputati e Presidenza del Consiglio dei Ministri e, su richiesta, alle agenzie di stampa e ai partiti politici.

2) **Stampe a richiesta** La componente DDE del Sistema Elettorale consente di generare un insieme di stampe in formato .pdf con i dati elettorali. La generazione delle stampe può essere richiesta dagli operatori del Ministero dell'Interno e delle Prefetture - UTG che dispongono dell'applicazione "Stampe a richiesta" e di un profilo di autenticazione per l'accesso.

3) **Agenzie di Stampa** La componente DDE del Sistema Elettorale genera un export dei dati elettorali ad uso delle agenzie di stampa. L'export dei dati è realizzato in formato XML e può essere consultato solo dalle agenzie accreditate tramite l'accesso a servizi web.

## ARCHITETTURA E PRINCIPALI FUNZIONALITA' SISTEMA SEAS

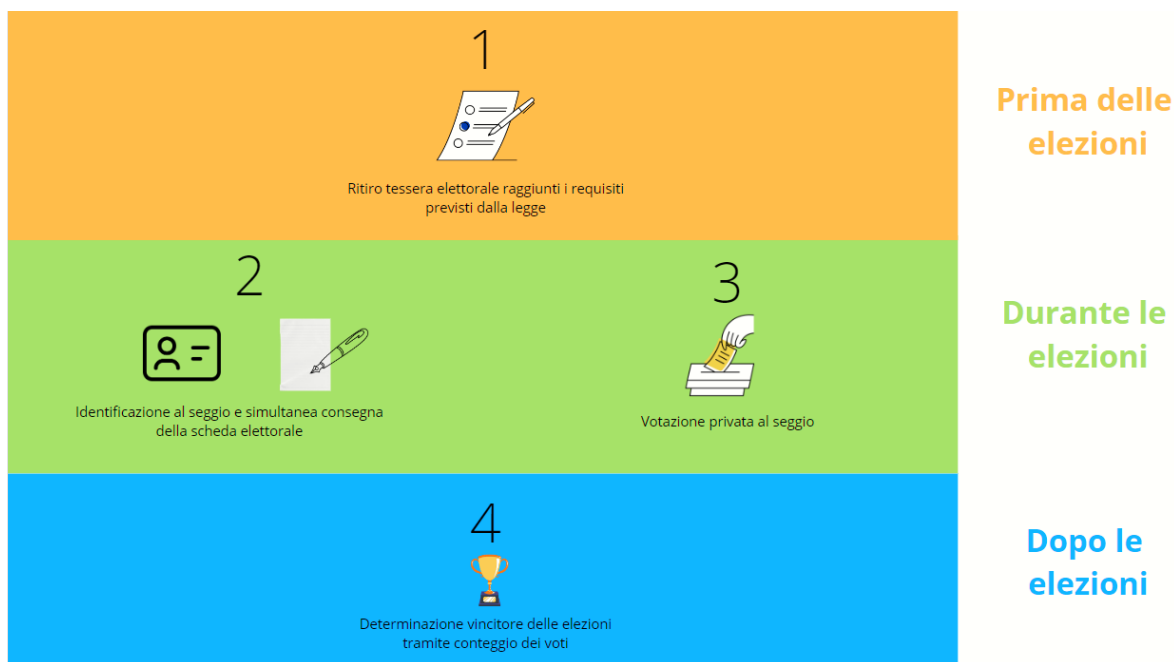
L'applicazione SEAS (Servizi Elettorali per le Agenzie di Stampa) gestisce la diffusione dei dati elettorali verso le **Agenzie di Stampa** e verso eventuali altri organi accreditati presso il Ministero dell'Interno. Il Web Service SEAS, che comunica attraverso il Web, mediante protocollo SOAP, fornisce un sistema standard per i messaggi di richiesta e di risposta dei servizi disponibili, ed è accessibile solo ad utenti certificati. I diversi servizi che vengono messi a disposizione degli utenti sono raggruppati in due fasi distinte della gestione degli eventi elettorali: una fase pre-elettorale e una fase elettorale



## 2.7 Scomposizione processo

Il macro processo di votazione nazionale può essere scomposto in diversi micro processi. Cerchiamo di analizzarli prima dal punto di vista del cittadino e successivamente per l'organizzazione.

### PER IL CITTADINO:



### PER L'ORGANIZZAZIONE:



**Tecnologie e strumenti:**

- DataBase;
- VPN / IP;
- LAN;
- Carta e penna.

**Vantaggi:**

- Privacy e segretezza del voto molto elevati;
- Sicurezza nel sistema percepita molto elevata.

**Svantaggi:**

- Costi molto elevati;
- Problemi legati all'errore umano (sicurezza effettiva bassa);
- Necessità di essere fisicamente al seggio.

## 3. II BPR

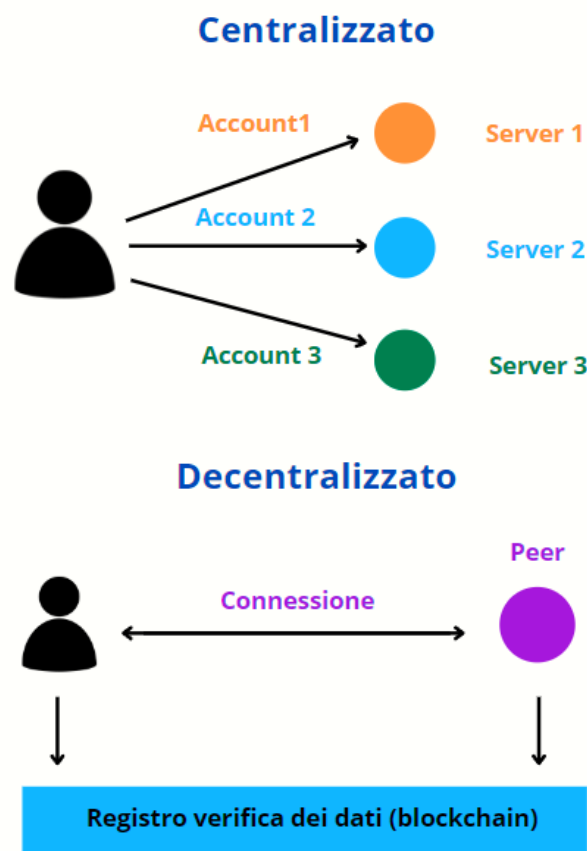
---

Nel capitolo precedente abbiamo analizzato l'attuale processo di votazione in vigore in Italia. Il processo nel suo complesso è efficace, ma non efficiente. Parte della popolazione è indirettamente tagliata fuori dalle votazioni, i costi sono eccessivamente elevati, la sicurezza percepita è elevata, diversamente da quella effettiva (principalmente legata all'errore umano). In questo capitolo andremo ad introdurre le tecnologie che riteniamo funzionali per il nostro processo di e-voting.

### 3.1 SELF-SOVEREIGN IDENTITY (SSI)

La Self-Sovereign Identity (SSI) è un modello di identità digitale decentralizzato basato sulla tecnologia Blockchain. Si fonda sulla restituzione all'utente del controllo sulle proprie informazioni personali e consentirebbe di risolvere i limiti dei sistemi di identificazione digitale ad oggi prevalenti, quelli cioè basati sulla presenza di Identity Provider (come ad esempio il caso SPID). L'SSI propone un nuovo paradigma di gestione dell'identità riassunta nella seguente figura:

#### Modelli di identità





Come è facile intuire, il concetto di SSI ha una portata tanto innovativa quanto rivoluzionaria ed è per questo al centro di un importante dibattito circa i potenziali benefici e le possibilità di impiego. Nel delineare le caratteristiche fondamentali della Self-Sovereign Identity, sono stati definiti i dieci principi alla base di questo modello.

Secondo la definizione dell'Osservatorio Blockchain Distributed Ledger, il concetto di SSI consente all'utente di non delegare la custodia ed il controllo delle informazioni personali ad un attore terzo. Il cuore di questo modello è la possibilità, da parte dell'utente, di generare automaticamente un identificativo che può dimostrare di controllare. Questi meccanismi crittografici presentano 3 diversi livelli di sicurezza (LoA) di cui ci occuperemo meglio nella sezione della sicurezza.

Nel delineare le caratteristiche fondamentali della Self-Sovereign Identity, sono stati definiti i dieci principi alla base di questo modello.

1. **Esistenza**

Avendo lo scopo di rendere accessibili nel mondo digitale attributi e informazioni sull'utente, l'identità SSI non potrà mai essere "disaccoppiata" dalla sua entità fisica e non potrà quindi esistere esclusivamente nel mondo digitale.

2. **Controllo**

L'autorità/proprietà sul profilo dell'identità SSI è in mano all'utente stesso, che può disporre della sua condivisione in autonomia. Questo non preclude ad altre entità, come utenti, aziende o istituzioni, di fare asserzioni sull'utente e definirne alcune caratteristiche o proprietà.

3. **Accesso**

L'utente deve essere in grado in qualsiasi momento di recuperare agilmente i propri dati, senza che alcun dato venga nascosto.

4. **Trasparenza**

Gli algoritmi alla base del sistema tecnologico dell'identità SSI devono essere gratuiti, open source, ben noti e indipendenti, così da avere sempre piena trasparenza sul loro funzionamento e aggiornamento.

5. **Persistenza**

Idealmente, l'identità dovrebbe durare per sempre o comunque fino a che l'utente desidera. Questo non implica che i dati e gli attributi associati a questa identità debbano rimanere immutati, quanto piuttosto che il profilo generale deve essere persistente.

6. **Portabilità**

Le informazioni sull'utente e sulla sua identità devono essere "trasportabili", ovvero non vincolate a un'entità digitale, per esempio a un social network, né a una specifica giurisdizione, come uno Stato.

7. **Interoperabilità**

Le identità dovrebbero essere utilizzabili il più ampiamente possibile, un'identità SSI è utilizzabile a livello globale e non si limita a determinate attività o settori.

## 8. **Consenso**

La condivisione dei dati identificativi con altri attori all'interno dell'eco - sistema deve avvenire esclusivamente con il consenso dell'utente.

## 9. **Minimizzazione**

Quando i dati vengono scambiati tra i vari attori previo consenso dell'utente, questa condivisione deve coinvolgere il minimo set di dati necessario per la fruizione del servizio a cui si sta accedendo.

## 10. **Protezione**

I diritti e le libertà delle persone hanno la priorità sulle esigenze della rete a supporto del modello SSI.

### *SSI su Blockchain: i vantaggi per l'identità digitale*

Le tecnologie Blockchain e Distributed Ledger stanno dunque favorendo e accelerando lo sviluppo di nuovi modelli decentralizzati per la Digital Identity. La massima decentralizzazione, come visto, si trova nei modelli Self Sovereign Identity: i punti di contatto tra questi modelli e la Blockchain sono molteplici e una loro combinazione potrebbe risultare vincente.

Le Distributed Ledger Technologies consentono di risolvere alcuni limiti dei modelli vigenti di identità digitale, tra cui lo scarso controllo dell'utente sulle informazioni condivise e sulla privacy dei propri dati, la limitata flessibilità nella creazione di soggetti in grado di emettere certificati, il rischio di frodi e duplicazioni dei documenti, nonché gli elevati costi infrastrutturali. La Self Sovereign Identity su Blockchain aprirebbe infatti le porte all'utilizzo di moderni strumenti crittografici in grado di raggiungere livelli di privacy ad oggi inediti nell'ambito dell'identità digitale, anche in caso di revoca dei certificati. È il caso, per esempio, delle Zero Knowledge Proof ovvero, un metodo interattivo utilizzato da un soggetto per dimostrare ad un altro soggetto che una affermazione/attributo è vero senza rivelare nessun' altra informazione oltre alla veridicità dell'informazione richiesta; ad esempio, potrebbe essere utilizzato per dimostrare di essere maggiorenne senza svelare la data di nascita.

### *Funzionamento del modello SSI*

Il sistema SSI si basa su 3 elementi:

- **Decentralized Identifier (DID)**

Una stringa alfanumerica che identifica univocamente un'entità: codici alfanumerici basati su un sistema a doppia chiave crittografica, memorizzato su una Blockchain, che consentono di identificare univocamente un'entità online;

- **Verifiable Credential (VC)**

Un qualsiasi tipo di attributo collegato ad un'entità. Gli equivalenti fisici di una VC sono per esempio la patente di guida o il diploma di laurea. Nel modello SSI, però, le VC sono digitali, imm modificabili e verificabili in maniera indipendente in ciascuna interazione per cui è richiesto quello specifico attributo;

- **DID Document**

Essendo il DID un elemento atomico (solo un codice alfanumerico), ha necessità di un elemento aggiuntivo contenente ulteriori informazioni sull'entità identi-

cata. Per esempio, un individuo in possesso di un DID potrebbe inserire nel suo DID Document la lista dei DID “fidati” nel caso la sua chiave crittografica fosse compromessa, oppure potrebbe voler indicare dei delegati a firmare dei documenti in sua vece.

### *La revisione eIDAS ed il wallet europeo*

Essendo a conoscenza delle potenzialità di questa tecnologia, l’unione europea ha già da tempo emanato, e continua ad emanare, direttive volte a regolamentarne l’utilizzo: il **Regolamento eIDAS** (electronic IDentification Authentication and Signature – n. 910/2014). Il 3 giugno 2021 infatti la Commissione europea ha reso nota una *proposta di revisione al Regolamento eIDAS*, insieme a un documento di raccomandazioni per lo *sviluppo di un digital wallet europeo*. Il piano della Commissione è quello di permettere a tutti i cittadini e a tutte le imprese all’interno del territorio europeo di accedere a un sistema di riconoscimento interoperabile, che dia la possibilità di archiviare e utilizzare i dati legati all’identità digitale per l’accesso a un set di servizi ampio e diversificato. Gli scenari che si aprono sembrano andare sempre più nella direzione del paradigma SSI: all’interno del documento si fa riferimento a dei “registri elettronici”, che fornirebbero agli utenti una prova e una traccia di controllo immutabile delle transazioni e dei dati identificativi.

### *Applicazioni delle SSI*

Grazie a questo modello è quindi possibile avere un’identità digitale con la quale poter accedere a informazioni personali, banche o servizi pubblici senza doversi ricordare diverse credenziali. Nell’ambito del nostro progetto la SSI ha un ruolo fondamentale in quanto rappresenta la modalità di identificazione dei soggetti che accederanno alla nostra piattaforma.

## 3.2 La blockchain

La blockchain è l'innovativa tecnologia di database che costituisce il punto di partenza di quasi tutte le criptovalute. Distribuendo all'interno di una rete copie identiche di un database, la blockchain rende molto difficile hackerare o aggirare il sistema. Sebbene le criptovalute rappresentino al momento l'utilizzo più diffuso della blockchain, questa tecnologia ha il potenziale per essere impiegata in un'ampia gamma di applicazioni.

### *Cos'è la blockchain?*

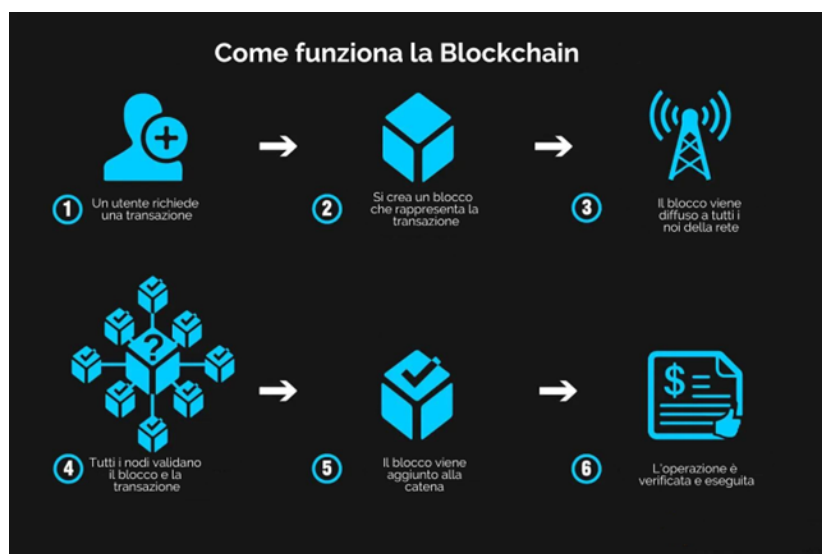
Essenzialmente, la blockchain è un registro digitale distribuito in grado di memorizzare dati di qualsiasi tipo. Una blockchain può registrare informazioni sulle transazioni in criptovalute e sulla proprietà degli NFT, ovvero i gettoni digitali non fungibili. Benché questo genere di informazioni possa essere memorizzato in qualsiasi database convenzionale, la blockchain è unica in quanto è decentralizzata. Invece di essere gestito in un'unica sede da un solo amministratore – si pensi a un foglio Excel o al database di una banca – il database di una blockchain è custodito in molte copie identiche distribuite su una rete di computer. I vari computer del network in questione vengono definiti nodi.

### *Come funziona la blockchain*

Quando si parla di blockchain, il registro digitale viene descritto come una “catena” composta da singoli “blocchi” di dati. Ogni volta che si aggiungono nuovi dati alla rete, viene creato un nuovo “blocco” che si unisce alla “catena”.

In questo modo, tutti i nodi aggiornano la propria versione del registro della blockchain in modo che rimanga identico. L'elemento chiave per cui la blockchain è considerata altamente sicura è proprio il modo in cui vengono creati i nuovi blocchi: la maggior parte dei nodi deve infatti verificare e confermare la legittimità dei dati inseriti prima che un nuovo blocco possa essere aggiunto al registro.

Si tratta di un sistema diverso da quello di un database autonomo o di un foglio di calcolo, dove un singolo individuo può apportare modifiche senza alcuna supervisione. “Una volta raggiunta l'unanimità, il blocco viene aggiunto alla catena e le transazioni corrispondenti vengono memorizzate nel registro distribuito”.



Generalmente le transazioni sono protette dalla crittografia, il che significa che i nodi devono risolvere complesse operazioni matematiche per elaborare ciascuna transazione. Esistono blockchain pubbliche e private. In una *blockchain pubblica*, chiunque può partecipare, il che significa che può leggere, scrivere o verificare i dati della blockchain. Risulta particolarmente difficile alterare le transazioni registrate in una blockchain pubblica, poiché non c'è un'unica autorità che controlla i nodi. Una *blockchain privata*, invece, è controllata da un'organizzazione o da un gruppo. Solo questo ente può decidere chi invitare ad accedere al sistema, oltre ad avere la facoltà di tornare indietro e modificare la blockchain. La blockchain privata è più simile a un sistema interno di archiviazione dati, ma è distribuita su più nodi per aumentarne la sicurezza.

- **Meno errori nelle transazioni**

Poiché le transazioni sulla blockchain devono essere verificate da più nodi, gli errori risultano notevolmente ridotti. Se un nodo ha un dato errato nel proprio database, tutti gli altri constateranno che è diverso e si accorgeranno dell'errore. Inoltre, ogni asset è identificato e tracciato individualmente sul registro della blockchain, quindi è impossibile che venga speso più volte;

- **Eliminazione degli intermediari**

Utilizzando la blockchain, le due parti coinvolte in una transazione possono confermare le operazioni e completarle senza passare attraverso terze parti riducendo in questo modo sia i costi di transazione sia i tempi delle transazioni;

- **Alto grado di sicurezza**

Dal punto di vista teorico, in una rete decentralizzata come la blockchain è quasi impossibile che qualcuno riesca a portare a termine transazioni fraudolente. Per immettere transazioni falsificate nel database, sarebbe necessario hackerare tutti i nodi e modificare tutti i registri. Inoltre molti sistemi blockchain si avvalgono di metodi di verifica delle transazioni di tipo “proof-of-stake” o “proof-of-work”, che rendono difficoltosa, oltre che contraria agli interessi dei partecipanti, l'aggiunta di transazioni fraudolente;

- **Operazioni più veloci**

Dal momento che funzionano 24 ore su 24, 7 giorni su 7, le blockchain permettono di effettuare qualsiasi tipo di operazione in modo più efficiente. Il loro utilizzo consente infatti di eliminare i tempi di attesa richiesti dalle banche o dalle agenzie pubbliche per confermare manualmente ogni operazione.

### *Svantaggi della blockchain*

- **Limite massimo di transazioni al secondo**

Dato che la blockchain dipende da una rete più ampia per approvare le transazioni, c'è un limite alla velocità con cui opera. Ad esempio, Bitcoin può elaborare solo 4,6 transazioni al secondo, contro le 1.700 al secondo di Visa. Inoltre, la crescita del numero di transazioni può creare problemi in termini di velocità della rete;

- **Costi energetici elevati**

Il lavoro di tutti i nodi per la verifica delle transazioni richiede una quantità di energia elettrica significativamente maggiore in confronto a un singolo database

o a un foglio di calcolo. Per questo motivo, le transazioni su blockchain non solo sono più costose, ma generano anche ingenti livelli di emissioni di anidride carbonica;

- **Rischio di perdita degli asset**

Alcuni asset digitali sono protetti da una chiave crittografica, come ad esempio le criptovalute conservate in un wallet basato sulla blockchain, custodire questo dato con attenzione è fondamentale. “Attualmente non c’è modo di recuperare la chiave crittografica privata che consente di accedere a un asset digitale: se il proprietario la smarrisce, pertanto, perderebbe definitivamente anche il proprio asset”. La blockchain è un sistema decentralizzato, quindi non è possibile rivolgersi a un’autorità centrale, come la propria banca, per richiedere l’accesso;

- **Rischio di attività illegali**

La decentralizzazione della blockchain garantisce maggiori livelli di privacy e riservatezza, cosa che purtroppo costituisce un’attrattiva per chi vuole compiere attività illecite. Tracciare una transazione irregolare su blockchain è più difficile che rintracciarla all’interno di transazioni bancarie cui è associato un nome.

### *Quali sono gli usi della blockchain?*

La blockchain viene utilizzata per molti scopi diversi, che spaziano dai servizi finanziari alla gestione dei sistemi della pubblica amministrazione.

#### **Criptovalute**

Attualmente la blockchain viene utilizzata principalmente come tecnologia che rende possibile l’esistenza delle criptovalute, come Bitcoin o Ethereum. Quando vengono acquistate, scambiate o spese criptovalute, le transazioni vengono registrate su una blockchain. Quanto più si utilizzeranno le criptovalute, tanto più la blockchain potrà diffondersi.

#### **Servizi bancari**

Oltre che per le criptovalute, la blockchain viene utilizzata per elaborare transazioni in valuta fiat, come l’euro, il dollaro e la sterlina. In questo modo l’invio di denaro può avvenire più rapidamente rispetto alla tradizionale in banca o tramite altri istituti finanziari, grazie a una maggiore velocità del processo di verifica delle operazioni e poiché le transazioni possono essere elaborate anche al di fuori dei normali orari di ufficio.

#### **Trasferimenti di asset**

La blockchain può essere utilizzata anche per registrare e trasferire le proprietà di una serie di beni. Al momento si utilizza molto per i beni digitali come gli NFT, come dimostrazione della loro proprietà nulla vieta però di utilizzare questa tecnologia per gestire la proprietà di beni fisici come case o automobili.

#### **Smart Contract**

Un’altra innovazione basata sulla blockchain consiste nei contratti ad esecuzione automatica noti come “smart contract”. Questi contratti digitali entrano in vigore automati-

camente quando sono soddisfatte determinate condizioni. Ad esempio, il pagamento di un acquisto può essere effettuato istantaneamente se l'acquirente e il venditore rispondono a tutti i parametri specificati per la transazione.

## **Sistemi di votazione**

Gli esperti del settore sono inoltre alla ricerca di soluzioni che consentano di utilizzare la tecnologia blockchain per contrastare le frodi nei sistemi di votazione. Teoricamente, infatti, la blockchain potrebbe consentire ai votanti di esprimere una preferenza non modificabile, eliminando al contempo la necessità di raccogliere e scrutinare manualmente le schede elettorali cartacee.

### 3.3 Gli smart contract

Esso è un protocollo informatico che su una blockchain facilita, verifica o fa rispettare la negoziazione o l'esecuzione di un contratto poiché programmato per rispondere alla funzione *if-then* (“se-allora”).

#### *Definizione*

Lo smart contract può essere definito come un codice digitale che offre una serie di garanzie a condizioni predefinite concordate tra le parti. In sostanza, le parti possono stabilire una condizione che può avviare un'azione o una serie di azioni quando non soddisfatte.

A differenza dei contratti tradizionali nei quali se una parte viola i termini di un accordo, l'altra può portarla in tribunale, gli smart contract rafforzano tali accordi, in modo che le regole vengano applicate automaticamente senza che tribunali o terze parti siano chiamati in causa.

#### *Come funzionano gli smart contract*

Gli smart contract funzionano seguendo semplici istruzioni “*se/allora*” scritte nel codice su una blockchain. Esso è depositato in una rete di computer ed esegue le azioni quando le condizioni predefinite sono state soddisfatte e verificate. Queste azioni potrebbero consistere nella registrazione di un veicolo, l'emissione di un biglietto, un pagamento, ecc. Al termine della transazione la blockchain viene aggiornata e la transazione non può essere modificata o manomessa.

All'interno di uno smart contract possono essere apposte tutte le clausole necessarie per verificare che l'attività sia stata completata in modo soddisfacente. Per stabilire i termini bisogna determinare come le transazioni e i loro dati sono rappresentati sulla blockchain, concordare le regole del “*se/allora*”, esplorare tutte le possibili eccezioni e definire un quadro per la risoluzione delle controversie.

Uno smart contract viene programmato da uno sviluppatore scrivendo una riga di codice e definendo le regole. Dopodiché verrà portato sulla blockchain (quella più largamente usata è quella di Ethereum) dove tutti i computer collegati alla rete hanno una copia di questo contratto intelligente.

Chiunque può utilizzare smart contract se in possesso di token ether, acquistabile sugli exchange di criptovalute, e di un wallet per inviare e conservare ether.

#### *Vantaggi degli smart contract*

Sono diversi i vantaggi che gli smart contract offrono alle parti coinvolte molti dei quali riprendono le caratteristiche principali della blockchain, piattaforma sulla quale questi si basano.

Ecco i 4 principali:

- **Trasparenza**

Non essendo coinvolte terze parti e dato che i dati crittografati delle transazioni sono condivisi dai partecipanti, si riduce al minimo la possibilità che vengano manipolate le clausole del contratto a proprio vantaggio;

- **Sicurezza**

Basandosi sulla blockchain, anche gli smart contract garantiscono l'immutabilità



dei dati consentendo di stipulare accordi senza il rischio di possibili violazioni o errori. Questa trasparenza fornisce alle parti sicurezza e fiducia;

- **Risparmio**

L'eliminazione degli intermediari si traduce naturalmente in una riduzione dei costi. Non avendo bisogno di una terza parte per verificare i termini di contratto e assicurarne la validità, le commissioni e i costi associati alla presenza di uno o più intermediari scompaiono;

- **Velocità**

Il risparmio non è solo economico, ma anche di tempo. Niente intermediari, scartoffie, burocrazia e perdite di tempo per riconciliare gli errori dovuti spesso a errori umani: lo smart contract è digitale e automatizzato e, una volta soddisfatte le condizioni prestabilite, viene eseguito immediatamente. Tutto ciò lo rende uno strumento che semplifica i processi e gli accordi tra le parti, riduce la burocrazia e i costi associati ai contratti tradizionali, ma senza compromettere autenticità e credibilità. Non è un caso che gli smart contract siano usati o trovino un'ideale applicazione in diversi ambiti, dall'identità digitale alla gestione della catena di approvvigionamento, passando per i servizi finanziari, mutui e prestiti, assicurazioni e sanità.

### *Svantaggi degli smart contract*

Ovviamente questa tecnologia presenta anche degli svantaggi che possono essere così riassunti:

- **Limiti tecnico-giuridici**

Il contratto intelligente, a differenza del contratto tradizionale, basa il suo meccanismo di vincolatività sulla tecnologia della blockchain che impedisce *ab initio* l'inadempimento delle parti. Infatti è tecnicamente impossibile violare volontariamente le condizioni prestabilite. Tutto questo pone in secondo piano le problematiche riguardanti la condotta del singolo ai fini dell'adempimento;

- **Difficoltà nella traduzione in linguaggio informatico**

La loro applicazione è profittabile solo quando è semplice tradurre le clausole contrattuali in linguaggio informatico, ed inoltre non è da escludere che si verifichi un errore da parte del programmatore che può compromettere l'esecuzione del contratto;

- **Irrevocabilità**

Questa scatta nel momento in cui gli stessi sono inseriti all'interno della blockchain, da cui segue l'automatica esecuzione delle prestazioni che rende inutilizzabile l'eccezione di inadempimento. La risoluzione di questa problematica potrebbe essere data dalla cosiddetta *funzione kill* o **funzione di autodistruzione** dello smart contract che punta a rimuovere i programmi non più impiegati, con la finalità di efficientare le *performance della blockchain*.

### *Smart contract: casi d'uso*

Oggi gli smart contract sono un elemento tecnologico fondamentale di molte applicazioni decentralizzate (dApp), ossia quelle applicazioni che operano su un sistema

computazionale distribuito, e l'uso e i potenziali vantaggi degli smart contract oltrepassano i confini della finanza, interessando settori e aziende di vario tipo.

## **Identità digitale**

Uno dei possibili casi d'uso degli smart contract è l'identità digitale. La blockchain, con gli smart contract, può aiutare il campo dell'identità digitale in termini di sicurezza e privacy, riducendo il rischio di frodi, violazioni e furti d'identità, e automatizzando il processo di creazione e condivisione dell'identità digitale, migliorando l'interoperabilità e la compliance.

### 3.4 Il nuovo processo

Il nuovo processo di e-voting è suddiviso in quattro fasi distinte:

- **Fase1:** Identificazione degli elettori aventi diritto, e attribuzione delle chiavi;
- **Fase 2:** Processo di votazione tramite smart contract;
- **Fase 3:** Congiungimento dei voti, decretazione del vincitore;
- **Fase 4:** Post elezione e gestione delle infrastrutture tecnologiche.

In questa sezione analizzeremo ogni fase, con l'obiettivo di avere sia una visione completa ma nel contempo semplice del progetto che proponiamo.

#### FASE 1

L'articolo 48 della costituzione italiana sancisce:

*“Sono elettori tutti i cittadini, uomini e donne, che hanno raggiunto la maggiore età”.*

Obiettivo del progetto è quello di estendere il voto ai fuori sede, questo vuol dire che in fase di autenticazione le condizioni che sarebbero oggetto di verifica sono tre:

- Maggior Età;
- Cittadinanza Italiana;
- Al momento della elezione il domicilio risulta essere al di fuori della regione di residenza.

La verifica di queste condizioni sarebbe gestita tramite un SSI per i vantaggi spiegati nel capitolo precedente. Ad oggi l'approccio non è molto diffuso, ma a livello europeo ne sono state viste le potenzialità. Il progetto su cui ci poggiamo è Dizme che garantisce e certifica l'identità digitale, il cui nome gioca sull'assonanza con “this is me”. Il progetto Dizme ha le seguenti finalità: portare l'identità digitale dentro un wallet che è sempre con noi, e integrare **il mondo SSI (Self Sovereign Identity)**, basato su tecnologia blockchain. Il motivo per cui abbiamo optato per il servizio di identità digitale Dizme è l'approvazione da parte del regolamento eIDAS(<https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>).

*Come funziona esattamente Dizme?*

InfoCert, in qualità di Governance Authority, definisce lo schema delle credenziali di identità gestite da Dizme e la mappatura dei tre livelli di garanzia (Level of Assurance, LoA), che cambiano in base alle modalità di accertamento dell'identità. Su proposta dei singoli emittenti (Issuer), sono definibili, infatti, schemi e tipi di credenziali differenti (Context Specific Credentials) che prendano in considerazione, ad esempio, le preferenze personali, le informazioni creditizie o reddituali, le certificazioni. La caratteristica di queste credenziali è l'accessibilità e la verificabilità in tempo reale. Inoltre, non sono soggette a logiche di integrazione o contratti commerciali.

La verifica di identità o di attributi context-specific (Proof Request) può essere:

- Full Disclosure, con la richiesta di condivisione di un set di credenziali, formulata dal Verifier, colui che ha bisogno di interrogare le credenziali per accedere a un servizio, al proprietario delle stesse (l'Owner), che deve esplicitare il consenso;
- Zero Knowledge, con il proprietario che garantisce al Verifier un determinato requisito senza svelare integralmente le credenziali.

Nel nostro caso specifico possiamo adottare due richieste:

- Il livello di sicurezza maggiore, identificato come LoA2;
- Zero knowledge, con l'obiettivo di evitare la diffusione di dati non strettamente necessari (Es. non serve sapere l'età precisa del cittadino, ma è sufficiente sapere che è maggiorenne).

I cittadini, dunque, come primo step si autenticano sulla piattaforma Dizme, con lo scopo di ottenere un'identità digitale. Quest'ultima permette ai cittadini di loggarsi sulla piattaforma “Lambrusco” (cuore pulsante del nostro progetto di cui parleremo ampiamente nella prossima fase) solo al sussistere delle tre condizioni espresse precedentemente. In questa maniera, potremmo garantire l'accesso all'evoting (e quindi alle chiavi private e pubbliche) solo ed esclusivamente agli aventi diritto.

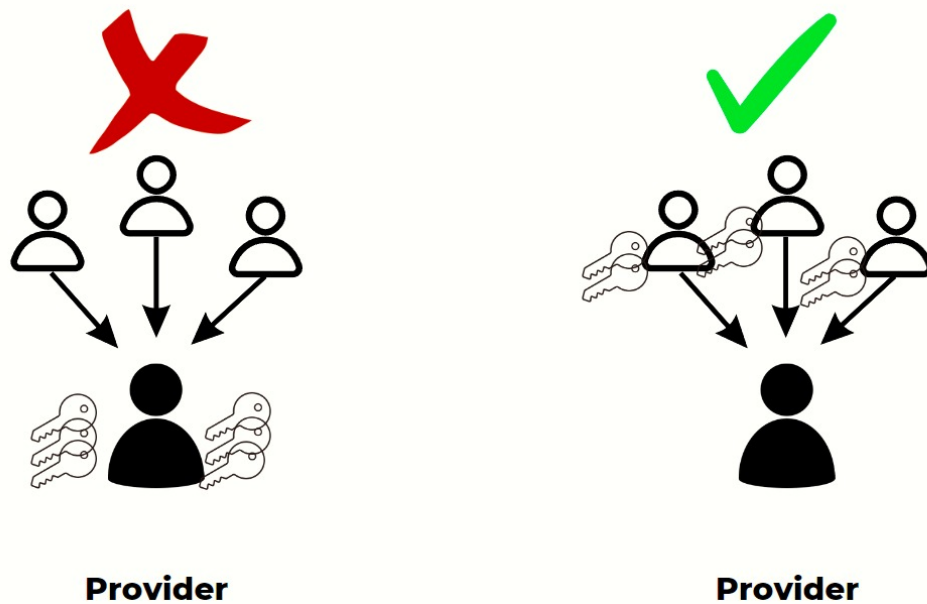
## FASE 2

La piattaforma “**Lambrusco**” (che chiameremo anche *Dapp*, ovvero decentralized application) viene sviluppata e gestita dal dipartimento della trasformazione digitale. Obiettivo di questa piattaforma è attribuire la coppia di chiavi agli iscritti, che, come abbiamo visto, rispettano i requisiti per il voto elettronico, e fornire una interfaccia user friendly tramite la quale è possibile indicare il nome del partito che si intende votare e attivare lo smart contact per la trasmissione del voto. Analizzeremo questa sezione delicata soffermandoci su tre punti:

1. La gestione delle chiavi;
2. La blockchain;
3. Lo smart contract.

## 1. La gestione delle chiavi

Al momento dell'autenticazione la Dapp genera automaticamente un wallet con le due corrispondenti chiavi, esattamente come se fosse un normale exchange come Coinbase, Binance ecc. La differenza sostanziale è che in quest'ultimo caso le chiavi pubbliche e private sono gestite interamente dal provider. Gli svantaggi nell'affidare le nostre chiavi (principalmente quella privata) ad un provider sono molteplici e legati ovviamente a problemi di sicurezza. Attacchi esterni al database centralizzato, dove sono contenute tutte le chiavi, potrebbero causare non pochi problemi.



Nel nostro progetto la sicurezza è fondamentale, motivo per cui ogni soggetto sarà pieno padrone delle sue chiavi (in gergo si dice “not you keys not your coins”). Come garantire all'utente che la chiave privata sia visualizzabile solo a lui e a lui soltanto? L'utente loggato nella Dapp, visualizzerà sia la chiave pubblica, questa verrà salvata nel sistema informativo pubblico (con scopo di verifica al termine delle elezioni) e sia la chiave privata solo un tempo limitato circa 30 min. In questo lasso di tempo l'utente dovrà salvare in modo idoneo e sicuro questo codice. Al termine di questo lasso di tempo, non sarà più possibile visualizzare la chiave privata e dunque non sarà più possibile esercitare il diritto di voto. È fondamentale che le chiavi private non siano salvate in nessun sistema informativo e che siano visibili solo all'utente. Neanche da parte della piattaforma stessa.

## 2. La blockchain

*Quale blockchain utilizzare per la validazione delle transazioni?*

Per rispondere all'esigenza di questo progetto è necessaria una blockchain con queste caratteristiche:

1. Pubblica;
2. Sicura (grande numero di nodi, e quindi difficilmente attaccabile);
3. Scalabile (in grado di validare blocchi in tempi ragionevoli);
4. Decentralizzata;
5. Che sia in grado di eseguire smart contract;
6. Capacità di gestire token fungibili (il voto).

Pur essendo un progetto nazionale creare una blockchain ad hoc potrebbe non essere la soluzione ideale, soprattutto nella prima fase in cui intendiamo estendere il diritto di voto solo ed esclusivamente ad i fuori sede. In questo caso infatti oltre a dover sostenere costi molto elevati potremmo avere problemi con il punto 2 e 4. Riteniamo invece che sia una scelta migliore affidarci, almeno inizialmente, ad una blockchain già consolidata che presenta tutti 5 punti prima citati: Ethereum.

## 3. Lo smart contract

Lo smart contract costituisce il programma vero e proprio che si occupa della gestione e della trasmissione dei voti. Lo sviluppo dello stesso compete agli sviluppatori blockchain più competenti a livello nazionale. Vediamo esattamente come funziona. Due giorni prima delle elezioni viene definito il numero preciso degli account creati sulla Dapp “ Lambrusco”. Questo dato viene passato come variabile in input allo smart contract , il quale creerà i token per egual numero. I token rispecchiano lo standard dei token fungibili ethereum (standard ERC-20). I token vengono identificati con un nome e un simbolo. Nel nostro il nome del token sarà “VOTE token” e il simbolo “EVT”. Lo smart contract presenta al suo interno alcune funzionalità che possono essere richiamate individualmente.

```

1  pragma solidity ^0.8.0;
2
3  // Importo lo standard ERC20 dei token fungibili
4  abstract contract ERC20Interface {
5
6      // funzioni dello smart contract richiamabili individualmente
7
8      function totalSupply() public virtual view returns (uint256);
9      function balanceOf(address _owner) public virtual view returns (uint256 balance);
10     function transfer(address _to, uint256 _value) internal virtual returns (bool success);
11     function transferFrom(address _from, address _to, uint256 _value) internal virtual returns (bool success);
12     event Transfer(address indexed _from, address indexed _to, uint256 _value);
13     event Approval(address indexed _owner, address indexed _spender, uint256 _value);
14 }
15
16 contract Token is ERC20Interface{
17
18     string public name = "VOTE";
19     string public symbol = "EVT";
20     // rendo la total supply pari al numero degli iscritti alla Dapp
21     uint public supply = 10000;
22
23     address payable public founder;
24     mapping(address => uint) public balances;
25     mapping(address => mapping(address => uint)) allowed;
26
27     event Transfer(address indexed _from, address indexed _to, uint256 _value);
28     event Approval(address indexed _owner, address indexed _spender, uint256 _value);
29
30     constructor() public {...}
31
32     function initializeAccount() public override view returns (uint256){
33         return supply;
34     }
35
36     function totalSupply() public override view returns (uint256){...}
37
38     function balanceOf(address _owner) public override view returns (uint256 balance){...}
39
40     function transfer(address _to, uint _value) internal override returns (bool success){...}
41
42     function transferFrom(address _from, address _to, uint256 _value) internal override returns (bool success){...}
43
44 }

```

Analizziamo quelle che ci interessano di più:

### 1. Inizializzazione degli account per il voto

Questa funzione verrà eseguita dagli esperti subito dopo la creazione dei token e consiste nell'inviare un solo ed unico token a tutti gli indirizzi pubblici che sono registrati (ricordiamo che gli indirizzi pubblici sono disponibili e presenti nel SI pubblico, diversamente da quelle private che sono segrete e a conoscenza solo ed esclusivamente dei singoli cittadini);

---

```

function initializeAccount() public override view returns
    (uint256){
    //L'ordine dei parametri: il mittente del token, il
        destinatario e la quantita'
    emit Transfer(founder,_to, 1);
    return true;
}

```

---

## 2. Trasmissione del voto

Ora che tutti i cittadini hanno nel proprio wallet il token per il voto, possono spenderlo. Per farlo viene richiamata la funzione Transfer che passa il voto dal votante all'elettore;

---

```
function transfer(address _to, uint _value) internal override
    returns (bool success){
    // funzione per la trasferire token da utenti ai candidati
    balances[_to] += _value;
    balances[founder] -= _value;
    emit Transfer(founder, _to, 1);
    return true;
}
```

---

## 3. Cancellazione del voto

Questa costituisce una forma di precauzione che può essere attuata nel caso in cui, a posteriori, ci si accorge che il voto di un singolo utente non è valido. In questo caso il funzionamento è inverso a quello della funzione precedente. Il voto passa dall'indirizzo dell'elettore a quello dell'utente;

## 4. Balance

Questa funzione verrà utilizzata al termine delle elezioni per stabilire quanti token hanno immagazzinato i singoli candidati nel loro indirizzo pubblico.

---

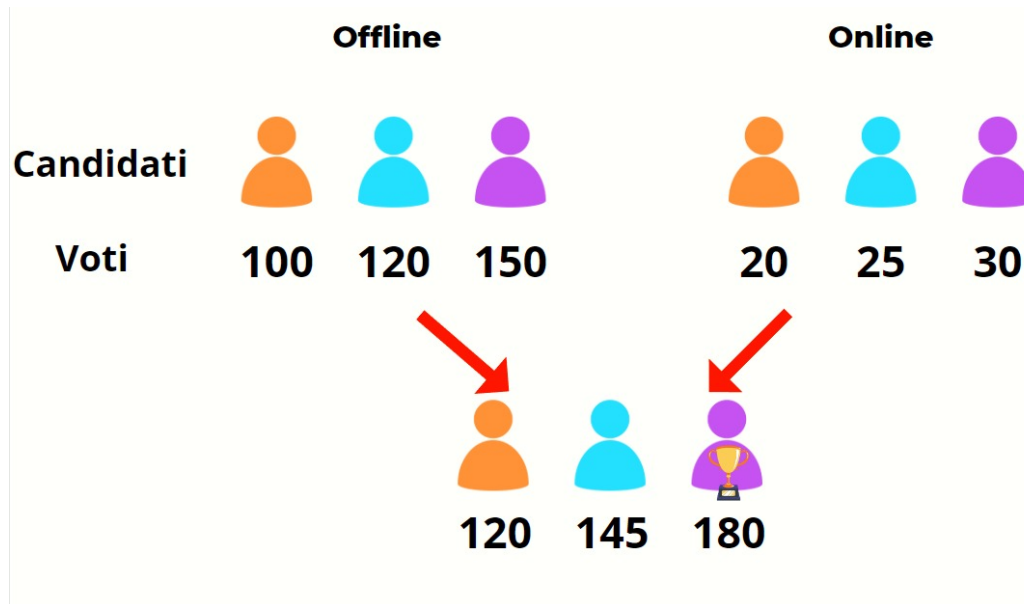
```
function balanceOf(address _owner) public override view returns
    (uint256 balance){
    // Restituisce il saldo di un account, puo' essere utile al
    // termine delle elezioni
    return balances[_owner];
}
```

---



### FASE 3

In questa fase le elezioni sono concluse. Ed è necessario riconciliare i risultati dei voti online e quelli offline. Questo avviene tramite una semplice sommatoria dei risultati.



Il nostro progetto prevede la coesistenza di queste due modalità di voto per il tempo necessario a far sensibilizzare la popolazione a queste tecnologie (circa 10-15 anni). Ovviamente se i riscontri dovessero essere positivi.

### FASE 4

Al seguito delle elezioni lo smart contract non avrebbe più utilità, sarebbe quindi opportuno rimuoverlo e cancellarlo, purtroppo le caratteristiche della tecnologia blockchain impediscono ciò. Lo smart contract sarà depositato all'interno della blockchain di ethereum per sempre in maniera immutabile. In caso di successive elezioni sarà possibile riutilizzarlo o in caso di modifiche sarà necessario crearne uno nuovo. La scelta di optare per una blockchain già solida come ethereum anziché una ad hoc ha risvolti anche in questa fase. Gestire una blockchain richiede parecchie risorse (sicurezza, i miner, i nodi) anche a seguito delle elezioni. Ben più importante, invece, risulta essere la gestione dell'account e delle chiavi a seguito delle elezioni. Le possibili soluzioni sono 2:

- Ad ogni elezione, ogni utente deve generare nuovamente delle chiavi pubbliche e private. Questo significa che gli account vengono creati appositamente per le elezioni per poi essere accantonati e non utilizzati mai più;
- Le chiavi della prima attivazione dovranno essere conservate anche per le prossime elezioni, e l'accesso alla Dapp, delle verifiche successive, continuerà a sottostare alle verifiche dell'identità digitale richiesta per quella determinata elezione (es.

all'inizio solo i fuori sede, poi i lavoratori che viaggiano tanto, poi i malati, poi gli studenti ecc).

Riteniamo, dunque, che la soluzione migliore sia la prima. Questo perché ad ogni elezione potrebbero cambiare i requisiti di accesso all'app e ovviamente per motivazioni di sicurezza.

quella di stabilire periodicamente un ricambio delle chiavi per la votazione.

### ***..Ricapitoliamo..***

Con questo schermo rivediamo la successione dei microprocessi previsti nel nostro nuovo sistema.

#### **PER IL CITTADINO:**



#### **PER L'ORGANIZZAZIONE:**



**Tecnologie:**

- SSI;
- blockchain;
- smart contract;
- crittografia.

**Vantaggi:**

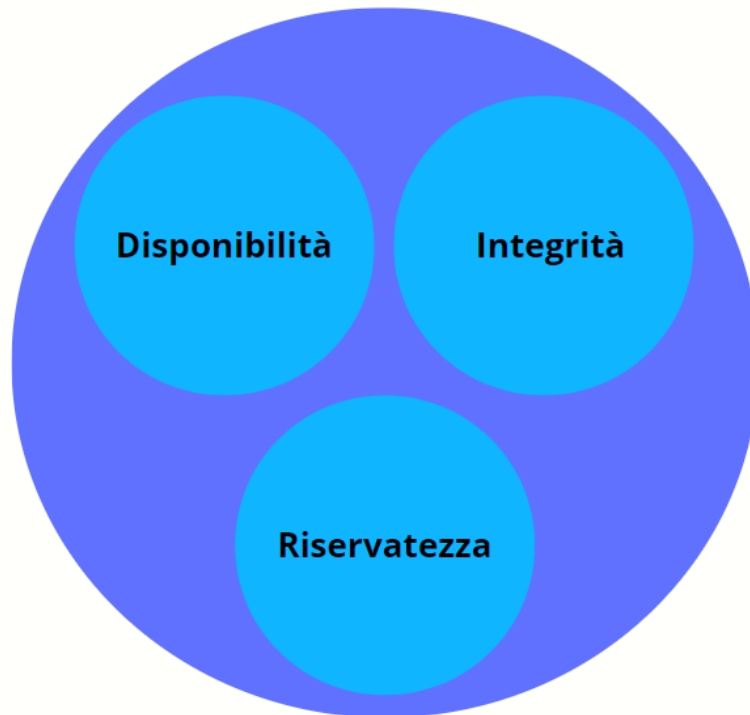
- Estensione diritto di voto ai fuorisede;
- privacy;
- gestione efficiente delle votazioni;
- abbattimento costi e dell'errore umano.

**Svantaggi:**

- Coesistenza di entrambi i processi nella fase iniziale;
- diffidenza verso le nuove tecnologie;
- problemi tecnici.

### 3.5 La sicurezza

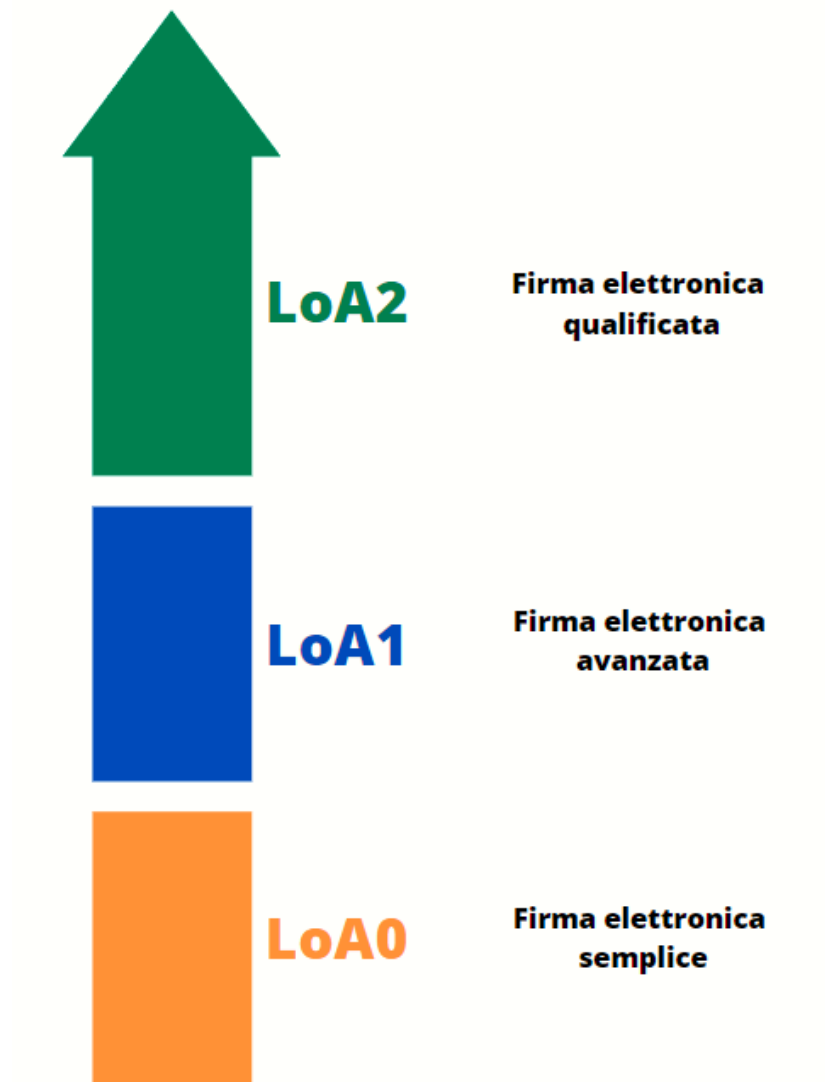
Lo standard di sicurezza del nostro progetto è garantito dalle caratteristiche stesse delle tecnologie utilizzate. Prendiamo in esame i tre obiettivi fondamentali della sicurezza informatica.



L'obiettivo della **riservatezza**, intesa come la capacità del sistema di interfacciarsi solo a soggetti autorizzati, viene garantita dalla SSI. Questa tecnologia infatti rispetta dei parametri di sicurezza: i LoA. Il termine “ livello di affidabilità ” si riferisce al grado di fiducia nell'identità rivendicata di una persona – quanto può essere certo un fornitore di servizi che sei tu quello usando il tuo eID per autenticarti al servizio, e non qualcun altro che finge di essere te. Secondo il Regolamento EIDAS (EU) 910/2014, gli schemi di identificazione elettronica ( eID ) sono classificati in base a tre livelli di affidabilità:

- Livello basso: ad esempio, l'iscrizione viene eseguita per auto-registrazione in una pagina Web, senza alcuna verifica dell'identità;
- Sostanziale: ad esempio, l'iscrizione viene eseguita fornendo e verificando le informazioni sull'identità e l'autenticazione utilizzando nome utente e password e password una tantum inviata al tuo cellulare;
- Alto: ad esempio, l'iscrizione viene eseguita registrandosi di persona in un ufficio e l'autenticazione utilizzando smartcard, come una carta d'identità nazionale.

## Livelli sicurezza SSI



I fornitori dei servizi che prevedono identificazione tramite eID richiederanno un certo LoA a seconda del servizio richiesto e delle informazioni che gestiscono. Grazie all'SSI è dunque possibile evitare che soggetti non autorizzati (es. i minorenni) accedano alla piattaforma per le votazioni.

L'obiettivo dell'**integrità**, inteso come la capacità di corretto inserimento e gestione dei dati, viene garantita invece dalla blockchain. L'Infrastruttura di Ethereum si occuperà dell'archiviazione nei blocchi dei dati relative alle votazioni. La perdita delle informazioni è pressoché impossibile grazie alle caratteristiche intrinseche della blockchain pubblica stessa. Nelle Blockchain i dati sono strutturati in blocchi e ogni blocco contiene una transazione o un insieme di transazioni. Ogni nuovo blocco si collega a tutti i blocchi precedenti in una catena crittografica in modo da renderne praticamente impossibile la manomissione. Tutte le transazioni all'interno dei blocchi sono convalidate e concordate tramite un meccanismo di consenso, garantendo che ogni

transazione sia effettiva e corretta. La tecnologia blockchain consente il decentramento attraverso la partecipazione dei membri ad una rete distribuita. Non esiste un singolo punto di errore e un singolo utente non può modificare il record delle transazioni. Le reti blockchain possono differire nel ruolo di chi può partecipare e chi ha accesso ai dati. Le reti sono in genere etichettate come pubbliche o private, per evidenziare chi è autorizzato a partecipare, e con autorizzazione o senza autorizzazione, per evidenziare come i partecipanti ottengono l'accesso alla rete.

L'ultimo obiettivo è quello della **disponibilità**, ovvero la capacità delle risorse informatiche di rendere disponibili i dati al momento del bisogno. I dati essendo archiviati all'interno della blockchain posso essere visualizzati in ogni momento e da chiunque tramite lo smart contract. Ribadiamo che questo non significa che la privacy degli elettori sarà violata, in quanto ad essere visibile a tutti sarà solo la chiave pubblica dei soggetti e non il nominativo.

## 4. Analisi dei rischi e di realizzazione

---

### 4.1 Implementazione e-voting da parte di altri stati

Numerosi Paesi hanno provato ad implementare il voto elettronico, ma si sono fermati a causa di difficoltà e preoccupazioni riguardanti questioni di sicurezza e di affidabilità. Inoltre il voto elettronico richiede spese molto elevate, da una parte quelle relative all'aggiornamento di attrezzature e tecnologie necessarie, da effettuarsi coerentemente con l'evolversi delle stesse, e dall'altra parte delle spese annuali, al fine di manutenzione, sicurezza e forniture.

La velocità del sistema può risultare un vantaggio quando ci sono più elezioni da effettuare in ogni singola votazione e contemporaneamente; ma nei sistemi parlamentari, dove ogni livello di governo è eletto in momenti differenti, il conteggio a mano risulta essere più attuabile.

Di seguito vengono riportate le esperienze e difficoltà di alcuni Paesi, che hanno provato ad implementare un sistema di questo genere, evidenziando i limiti ed i rischi che questo potrebbe presentare:

- **Australia**

iVote è un sistema di voto elettronico utilizzato in New South Wales, che permette ai cittadini di votare utilizzando internet. Tuttavia, durante le elezioni statali del 2015, dai dati raccolti è emerso che più di 66000 voti elettronici avrebbero potuto essere stati compromessi. Pur essendo il sito di iVote sicuro, specialisti della sicurezza ritengono che un sito esterno sia stato in grado di attaccare il sistema.

- **Bangladesh**

Nel 2010 venne condotto un esperimento con Electronic voting machines (EVMs) alle Chittagong City Corporation elections in 14 stazioni elettorali ed ebbe successo. A seguito di ciò si provò ad implementare le EVMs nelle Rajshahi City Corporation elections. Fu riscontrato un errore nelle macchine che il produttore non riuscì a risolvere, e conseguentemente circa 1000 macchine furono eliminate. Successivamente furono acquistate EVMs dall'estero, le quali ebbero successo in due stazioni elettorali nel 2016 e perciò fu annunciata l'introduzione delle EVMs in un terzo dei seggi nelle undicesime elezioni parlamentari. Tuttavia vari partiti politici protestarono contro questa decisione, con ancora oggi forti opinioni in opposizione, poiché ritengono che il partito al governo potrebbe così, attraverso le EVMs, essere capace di manipolare facilmente il voto. Inoltre un altro ostacolo è che, la maggior parte dei cittadini del Bangladesh, non ha familiarità con le tecnologie del voto elettronico. Dunque la Commissione di Elezione Elettorale, mandò diversi istruttori in varie parti del Paese, al fine di colmare queste lacune.

- **Belgio**

Durante le elezioni del 2003, fu riscontrato un problema riguardante il voto elettronico, poiché candidato raccolse 4096 voti extra. L'errore fu rilevato perché la candidata aveva più voti di quelli della propria lista, cosa impossibile nel sistema di voto. La spiegazione ufficiale è stata l'inversione spontanea di un bit alla

posizione 13 della memoria del computer. (*soft error*)

- **Canada**

Sulla base dei dati e delle analisi provenienti da Nova Scotia, New Brunswick, Quebec, Ontario e British Columbia, si sconsiglia il voto provinciale tramite internet. Una commissione federale si è espressa contro il voto nazionale tramite internet. Le elezioni della leadership del Nuovo Partito Democratico del 2012 furono condotte parzialmente online. Tuttavia, il server per il voto online subì un attacco del tipo *denial-of-service* causando un ritardo nel completamento e nella tabulazione dei risultati. Anche le elezioni municipali del 2018 in Ontario furono condotte principalmente online. Il giorno delle elezioni 51 di queste municipalità subirono alcuni guasti tecnici, causati da un limite di banda imposto a causa dell'eccessivo traffico dal Colocation Centre Provider, senza autorizzazione dall'online voting contractor Dominion Voting Systems. A causa di ciò il voto fu esteso per alcune ore, per compensare l'interruzione.

- **Estonia**

L'Estonia è uno dei paesi che più utilizza il voto elettronico e i funzionari della sicurezza affermano che non sono state mai rilevate attività inusuali o manipolazioni dei voti. Tuttavia dei ricercatori hanno trovato delle debolezze nel design di sicurezza del suo sistema di voto online, così come imponenti problemi per quanto riguarda il trasferimento dei risultati elettorali, concludendo che siano sistemi poco sicuri e che pertanto non dovrebbero essere utilizzati a causa dell'importanza della validità delle elezioni.

- **Finlandia**

Nel 2017 fu costituito un gruppo di lavoro per studiare il voto via Internet per la Finlandia, che si è espresso contrario, concludendo che i rischi superano i benefici.

- **Francia**

Nel 2017 la Francia annunciò che il voto via Internet, precedentemente offerto ai cittadini all'estero, non sarebbe stato permesso per le elezioni legislative a causa di preoccupazioni riguardanti la sicurezza informatica.

- **Germania**

Vi sono stati diversi tentativi di introduzione della votazione elettronica, ma si sono manifestati dubbi riguardo la vulnerabilità del sistema e preoccupazioni da parte della popolazione riguardanti la trasparenza e la sicurezza del sistema. Perciò nel 2009 cessò completamente di utilizzarlo, in seguito alla decisione da parte della Corte Costituzionale della Germania Federale di incostituzionalità del voto elettronico, motivata sulla base dell'incapacità di garantire una votazione sicura e corretta.

- **Olanda**

Dal 1990 al 2007 furono utilizzate macchine per il voto elettronico per le elezioni. Nel 2006 il gruppo "Wij vertrouwen stemcomputers niet" dimostrò come le macchine potessero essere rapidamente manipolate, senza alcun segno evidente ai votanti o ai funzionari delle elezioni. Inoltre fu dimostrato, dal General Intelligence and Security Service, che si potesse captare il voto sino a 40 metri di distanza utilizzando il Van Eck phreaking. Questi ed altri svariati problemi por-



tarono alla decisione di bandire le macchine per il voto elettronico nel 2007.

- **Stati Uniti**

Il voto elettronico negli Stati Uniti coinvolge diversi tipi di macchinari: touch screen per gli elettori per contrassegnare le scelte, scanner per la lettura delle schede elettorali, scanner per verificare le firme sulle buste delle schede elettorali assenti e server web per mostrare i conteggi al pubblico. Le macchine elettorali sono computer, spesso datati, poiché i processi di certificazione e acquisto richiedono almeno due anni e gli uffici competenti non dispongono di risorse monetarie sufficienti a sostituirli finché non sono del tutto obsoleti. Come tutti i computer, sono soggetti ad errori, che sono stati ampiamente documentati e problemi di sicurezza che permettono hackeraggi non rilevabili. Inoltre i dati rilevati, mostrano come i computer compiano parecchi errori nella procedura di verifica delle firme sulle buste elettorali postali.

Ci teniamo a ribadire che nessuno di questi paesi ha implementato sistemi decentralizzati su blockchain o smart contract. Questo significa che molte delle problematiche registrate potrebbero essere legate alla centralizzazione del sistema. Nonostante questo, risulta essenziale garantire un sistema che non solo sia sicuro, in tutte le sue sfaccettature e componenti, ma che risulti anche essere accettato dai cittadini. A tal fine si renderanno necessarie delle campagne mirate di sensibilizzazione ed informazione riguardo le tecnologie innovative che verrebbero implementate ed i processi che governerebbero il nuovo sistema elettorale. L'affidabilità e la fiducia nei confronti di un sistema del genere risultano pertanto essere componenti essenziali per il successo dell'iniziativa.

## 4.2 Formazione e sicurezza

Un aspetto fondamentale da considerare è quello relativo alla campagna di promozione del voto elettronico. Difatti, gli scetticismi e le perplessità andrebbero superati, tenendo conto di una base solida a livello di sicurezza e affidabilità del sistema, attraverso una massiccia campagna di sensibilizzazione che abbia come obiettivo quello di ottenere l'approvazione di una larga fetta dei cittadini. I primi a dover essere coinvolti in tutto ciò saranno, per l'appunto, i fuorisede, target per eccellenza di questo progetto.

La campagna dovrà attuarsi attraverso una opportuna strategia di marketing che sappia sfruttare al meglio le nostre conoscenze attuali in merito al funzionamento della società e delle persone che la compongono. Potremmo partire da concetti fondamentali dell'economia comportamentale. Quello di nudge (spinta gentile) e, in particolar modo, della loss aversion (avversione alle perdite).

Presentando i dati relativi alla mancata partecipazione al voto a causa di impossibilità di spostamento per recarsi nel proprio Comune e rinforzando la necessità del voto come strumento per eccellenza di partecipazione alla vita democratica e formazione della scelta collettiva sarà possibile dare rinforzo alla necessità per tutti di permettere l'introduzione del voto elettronico. Mezzi di diffusione delle informazioni saranno i social media e i mass media tradizionali. In qualche modo, sarebbe opportuno creare da una parte una sorta di senso di privilegio per coloro che possono decidere di votare online, ovvero i fuorisede in questa prima macro-fase di introduzione dell'iniziativa, al

fine di far riconoscere il voto elettronico come un vero e proprio beneficio, e dall'altra parte un senso di impellente sdegno nei confronti di qualsivoglia ostacolo all'esercizio del proprio diritto di voto. Lo schema di pensiero che si vuole costituire è uno del tipo: *Non voglio rinunciare al mio diritto di voto. La possibilità di votare a distanza va a mio vantaggio per questioni di comodità ed efficienza.*

Dovrebbe essere resa come l'alternativa migliore rispetto al dover fare molti chilometri di viaggio per votare o rispetto al non votare affatto, abbellendo l'iniziativa di far partecipare tutti al processo democratico.

Per quanto riguarda l'istruire il pubblico sulla questione, le fasce di pubblico più familiari con le nuove tecnologie e i social media avranno opportune istruzioni semplificate che illustrino come funziona il procedimento attraverso pochi ma esplicativi passaggi, al fine di attenuare eventuali sensazioni di sfiducia e sospetto nei confronti dell'iniziativa.

Per un'eventuale estensione del voto elettronico a tutti i cittadini, quanto fatto in questa prima fase sarà determinante. Bisogna creare un desiderio, una necessità di poter essere fra coloro che godono del beneficio di votare elettronicamente. A ciò si accompagnerà una campagna più incisiva di pubblicizzazione, resa giustificata e più sicura nei suoi risultati, da quanto fatto nella prima campagna di sensibilizzazione per i fuorisede. Si potranno sfruttare le sedi URP locali, l'operato dei Comuni, i social media, i mass media tradizionali. Non si esclude la possibilità di volantini da consegnare porta a porta. Persino il passaparola diventerà fondamentale.

Il piano d'azione dovrebbe prevedere, come già evidenziato, **tre fasi**:

Una **prima fase** in cui il target è rappresentato solo dai fuorisede. Riteniamo di soffermarci su questa fase per diverse elezioni, stimiamo un tempo di circa 5 anni. Questo con l'obiettivo di far conoscere bene il sistema e risolvere eventuali problemi che dovessero presentarsi. Si vuole ottenere familiarità e fiducia prima di estenderlo ed esporsi a rischi maggiori;

Nella **seconda fase**, il voto elettronico potrà essere esteso a chi ne faccia richiesta. Non si esclude la possibilità che questa fase duri diversi anni, circa da 5 a 15 anni. In modo tale da dare il tempo necessario alla cementificazione dell'idea e della pratica. In questa fase ci aspettiamo che sia la popolazione stessa ad avvicinarsi alle nuove tecnologie e a riconoscerne le potenzialità;

La **terza e ultima fase**, basata sul successo delle precedenti, potrà prevedere un'estensione a tutti i cittadini, con sostituzione totale del vecchio sistema. Riteniamo che l'attuazione di questa fase possa richiedere dai 15 anni in avanti.

Ovviamente, quanto detto fin'ora è un piano che richiede delle specifiche elaborate da parte di un team di marketing specializzato, ma la strategia fondamentale è immutata nelle sue fondamenta: il voto elettronico va considerato come una necessità di cui non si può far a meno. Bisognerà fare attenzione anche a loghi e slogan da implementare nella strategia.

Seguendo quanto fin'ora delineato, i risultati saranno ottimi con buone probabilità, ferma restando la capacità di interpretare il momento migliore per intervenire riguardo l'iniziativa e il paradigma sociale che si starà vivendo contestualmente. Il voto

elettronico e la sua sponsorizzazione vanno adattati ai cittadini; ma è pur vero che i cittadini dovranno essere abbastanza plastici da accettarlo e farlo proprio.

### 4.3 Realizzazione e preventivo

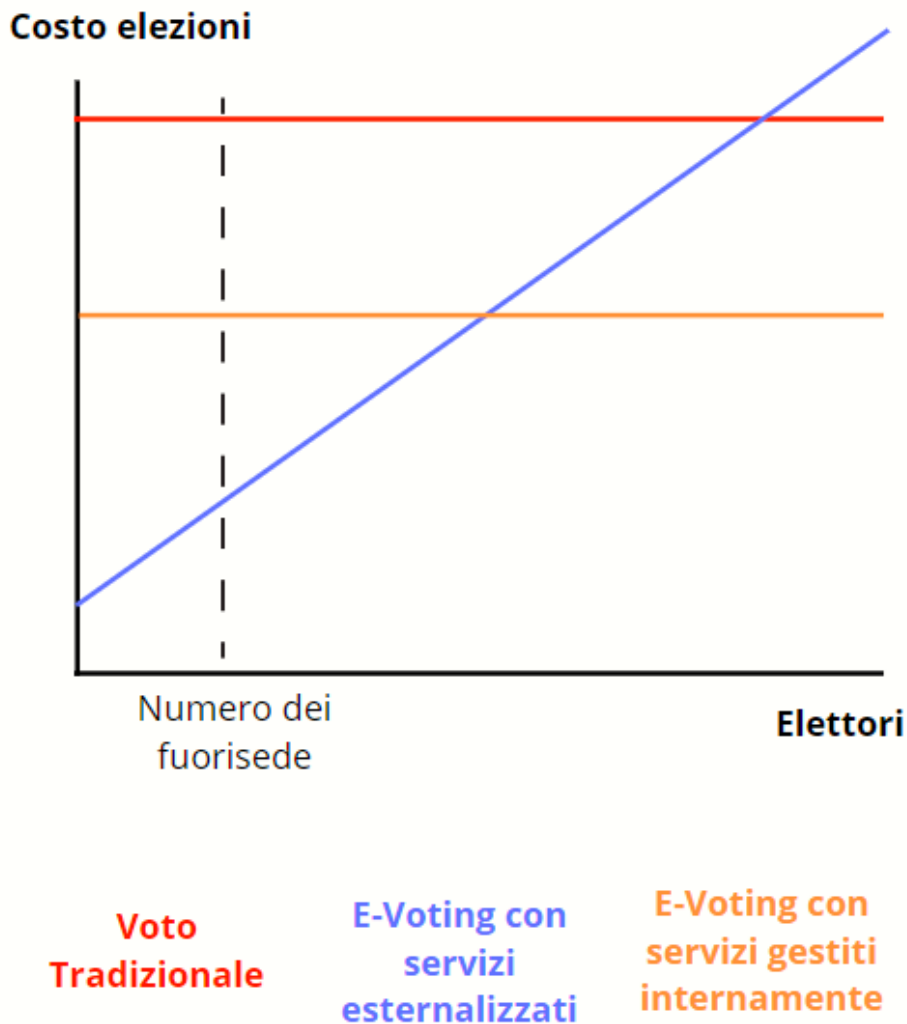
Il costo delle attuali elezioni è decisamente elevato. Non è possibile fornire un dato preciso ma si stima che la spesa si aggiri intorno ai 400 milioni di euro per elezione. Si tratta principalmente di spese fisse non correlate al numero dei votanti. Per il nostro progetto di e-voting abbiamo stimato i costi di realizzazione in suddetta maniera:

ELEMENTO	PREZZO
Smart contract	200.000,00 €
Costo realizzazione piattaforma	70.000,00 €
Formazione e sensibilizzazione	500.000,00 €
Collaborazione dizme	1.000.000,00 €
Costi di transazione su blockchain	20.000,00 €
Assistenza e monitoraggio	250.000,00 €
Fondi spese improvvise	500.000,00 €
Progettazione e implementazione	1.000.000,00 €
	<b>3.540.000,00 €</b>

La caratteristica dei costi di questo progetto è che sono fortemente dipendenti dal numero dei votanti. Più alto sarà il numero degli elettori, più alta sarà la spesa variabile per SII, spese di transazione ecc. Ma essendo il target di riferimento (i fuori sede) estremamente contenuto possiamo garantire la sostenibilità di questi costi.

Nel caso in cui invece, il voto elettronico dovesse essere esteso ad una fetta più grande della popolazione sarebbe più vantaggioso gestire alcuni processi internamente: una blockchain ad hoc, un SSI nazionale così da evitare costi eccessivi.

Per capire meglio la convenienza seguiamo il grafico qui riportato:

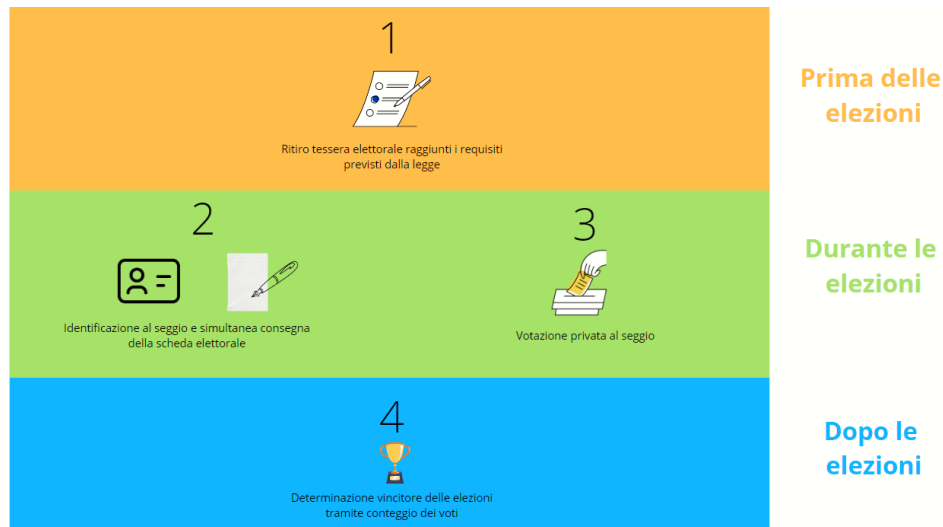


Si tratta ovviamente di una semplificazione ma ci aiuta a capire il motivo per cui, in questa prima fase del voto elettronico, abbiamo optato per un modello di fornitura esterna di servizi. Inoltre questo schema fa riferimento solo al prezzo monetario del sistema di votazione senza considerarne l'efficienza. Quest'ultimo ovviamente andrebbe ad incrementare ulteriormente il beneficio derivante dall'implementazione dell'e-voting system.

## 5. Confronto e conclusioni

Ora che abbiamo analizzato entrambi i processi di elezione, ci occupiamo ora di confrontarli tra loro per capire quali processi vengono sostituiti e quali invece continuano ad esistere.

### VECCHIO PROCESSO PER IL CITTADINO



### NUOVO PROCESSO PER IL CITTADINO



Come possiamo notare, il processo per il cittadino è più semplice con l'attuale sistema. A lui, infatti, non viene attribuita nessuna responsabilità se non quella di

custodire la tessera elettorale per le elezioni successive. Il passaggio ad un sistema di votazione nazionale tramite blockchain potrebbe non essere rapido e ben accettato. Gli studenti fuori sede, invece, potrebbero vedere in questo progetto un modo sicuro ed efficiente per esercitare il proprio diritto di voto in sicurezza, cosa che altrimenti non farebbero, o farebbero a fronte di costi molto elevati. L'introduzione del nuovo processo elettorale per i fuorisede, che si affiancherà all'attuale sistema di votazione, permetterà di riconoscere le potenzialità di questa tecnologia e la sua progressiva introduzione anche per i cittadini italiani stessi nel lungo periodo.

### VECCHIO PROCESSO PER L'ORGANIZZAZIONE



### NUOVO PROCESSO PER L'ORGANIZZAZIONE



Secondo il nostro nuovo processo l'organizzazione cambia radicalmente i processi di erogazione del servizio. Non è più necessario organizzare i seggi, il materiale

e l'identificazione fisica. Questi processi vengono garantiti dalle caratteristiche della blockchain e dallo smart contract, cuore pulsante di questo progetto.

I benefici che si ottengono con il passaggio al nuovo sistema di votazione sono notevoli. Non solo in termini economici (che sono in ogni caso rilevanti) ma soprattutto in termini di efficienza.

---

Scarica la nostra presentazione





# ICT Project



UNIVERSITÀ  
DEGLI STUDI DI BARI  
ALDO MORO

## National Evoting System Smart contract based

Grazie per l'attenzione

L<sup>A</sup>T<sub>E</sub>X