

LAMBRUSCO TEAM

National e-voting system

Smart contract based

ITC PROJECT 2022/2023

INDICE

- 1** Introduzione al problema
- 2** L'attuale sistema di votazione
- 3** Riprogettazione del processo tramite BPR
- 4** Analisi dei rischi, realizzazione e preventivo
- 5** Conclusioni

Introduzione

DATI SULLE ULTIME ELEZIONI



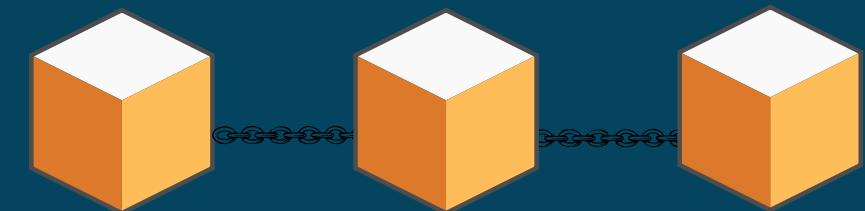
● Chi non vota?



● Perché?



COSA PROPONIAMO ?












L'attuale sistema di votazione

SCHEDA DI SINTESI DELLE ELEZIONI

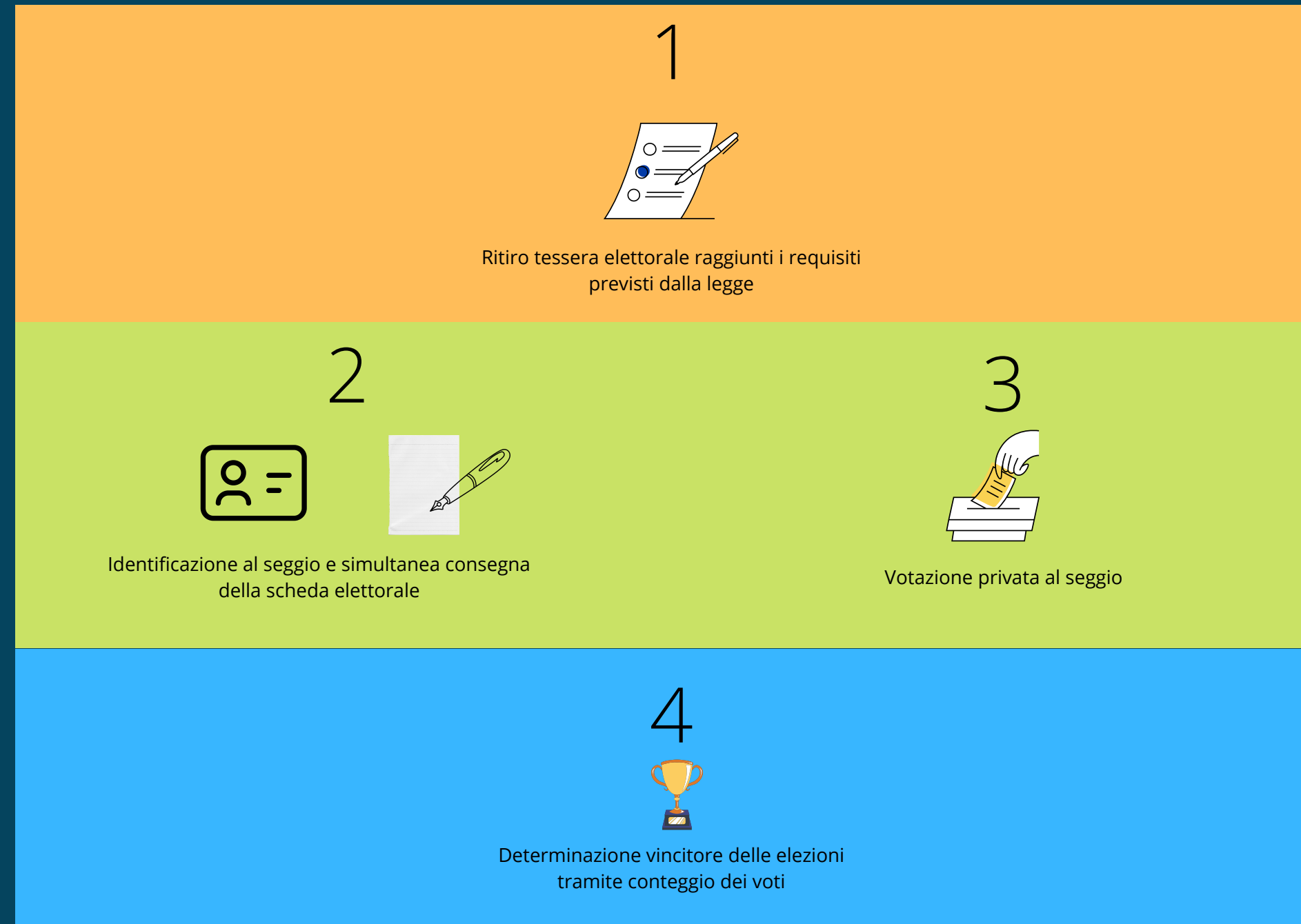
● Parlamento

● Senato

	Camera dei Deputati	Senato della Repubblica
	Circoscrizioni	28
	Collegi uninominali (seggi)	147
	Collegi plurinominali	49
	Numero seggi nei collegi plurinominali	245
	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 plurinomiale
	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 plurinomiale 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

L'ELETTORE AL VOTO

- **Requisiti per votare**
- **Obblighi per l'elettore**



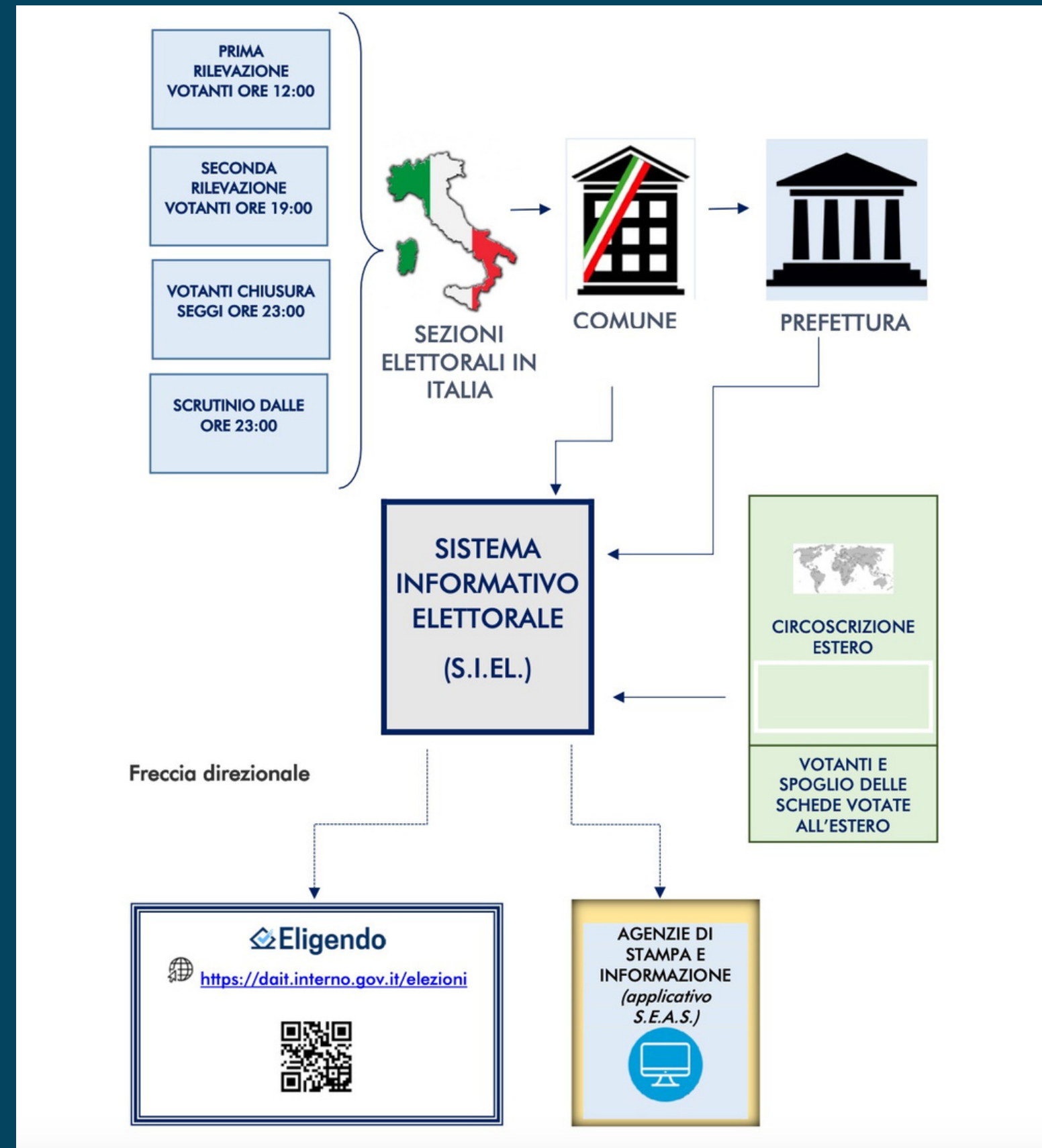
**Prima delle
elezioni**

**Durante le
elezioni**

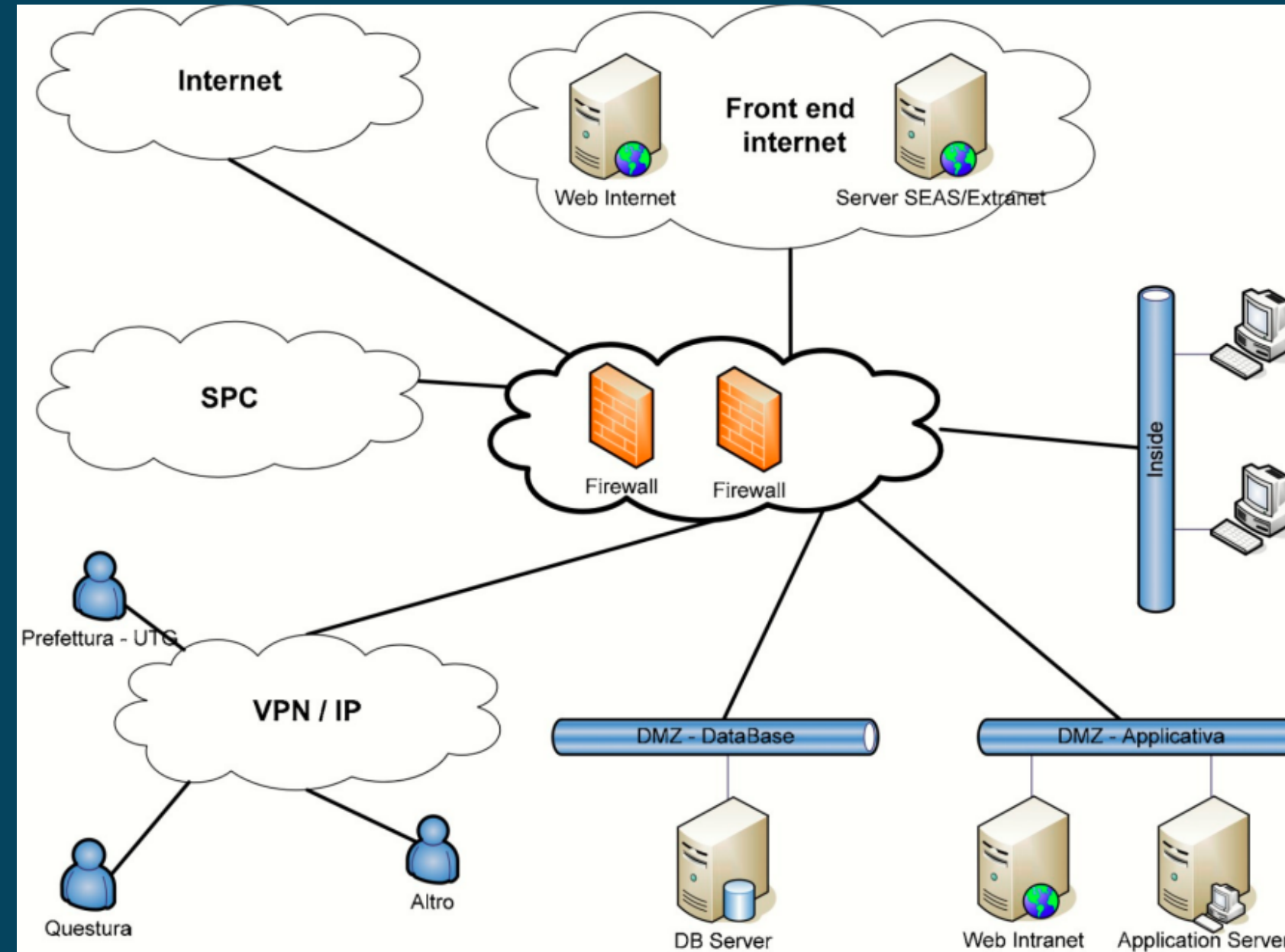
**Dopo le
elezioni**

IL FLUSSO DEI DATI

- Orario rilevazioni parziali
- Il ruolo contrale del S.I.EL.



IL SISTEMA INFORMATICO



Applicazione elettorale



ODE, SEAS E Query

Principali rischi



Ritardo, errore umano

Protocollo SOAP



Comunicazioni

Riprogettazione del processo tramite BPR

LE TECNOLOGIE

**SELF
SOVEREIGN
IDENTITY**



BLOCKCHAIN



**SMART
CONTRACT**



Caratteristiche

Vantaggi

Svantaggi

Riprogettazione del processo tramite BPR

IL NUOVO PROCESSO

FASE 1

- **Definizione dei requisiti per l'accesso al voto elettronico**



- **Creazione identità digitale tramite Dizme**



- **Con l'identità digitale ottenuta accesso verificato all'app per le votazioni Lambrusco**



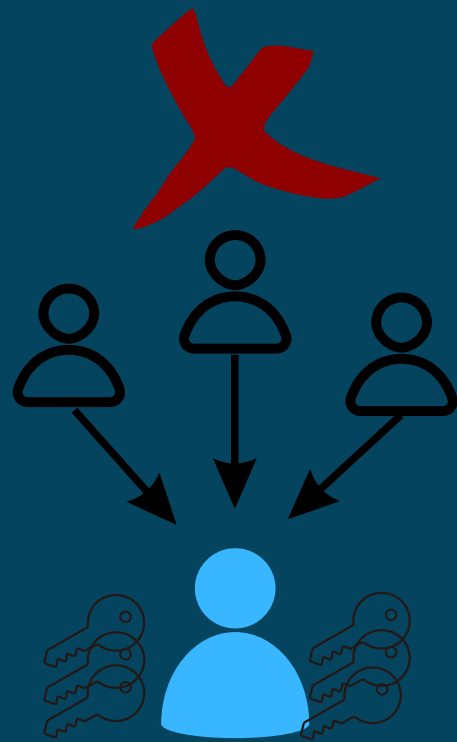
FASE 2

● La gestione delle chiavi

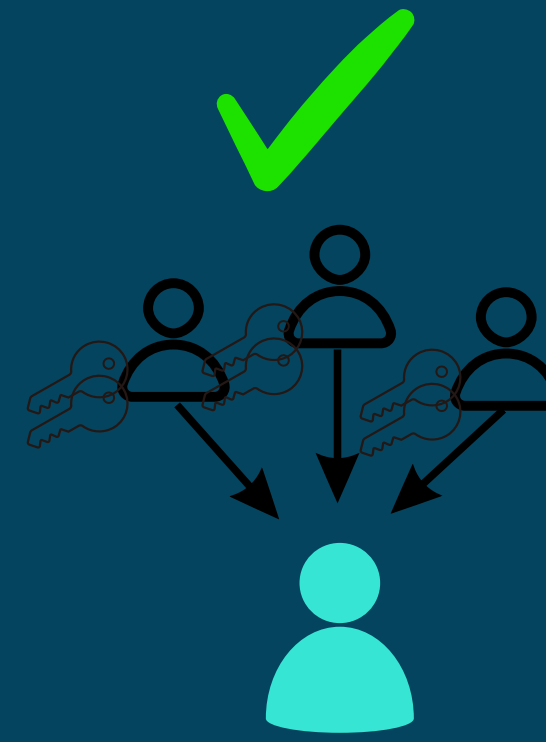
PERCHÈ È IMPORTANTE LA
CHIAVE PRIVATA?



MODELLO CENTRALIZZATO VS
MODELLO DECENTRALIZZATO



Provider



Provider

FASE 2

● La blockchain

PUBBLICA

SICURA

SCALABILE

DECENTRALIZZATA

SMART CONTRACT

TOKEN FUNGIBILI



ETHEREUM

FASE 2

● Lo smart contract



GESTIONE DEL VOTO

IL TOKEN

LE FUNZIONI

FASE 2

● Lo smart contract

```
pragma solidity ^0.8.0;

// Importo lo standard ERC20 dei token fungibili
abstract contract ERC20Interface {

    // funzioni dello smart contract richiamabili individualmente

    function totalSupply() public virtual view returns (uint256);
    function balanceOf(address _owner) public virtual view returns (uint256 balance);
    function transfer(address _to, uint256 _value) internal virtual returns (bool success);
    function transferFrom(address _from, address _to, uint256 _value) internal virtual returns
(bool success);
    event Transfer(address indexed _from, address indexed _to, uint256 _value);
    event Approval(address indexed _owner, address indexed _spender, uint256 _value);
}

contract Token is ERC20Interface{

    string public name = "VOTE";
    string public symbol = "EVT";
    // rendo la total supply pari al numero degli iscritti alla Dapp
    uint public supply = 10000;

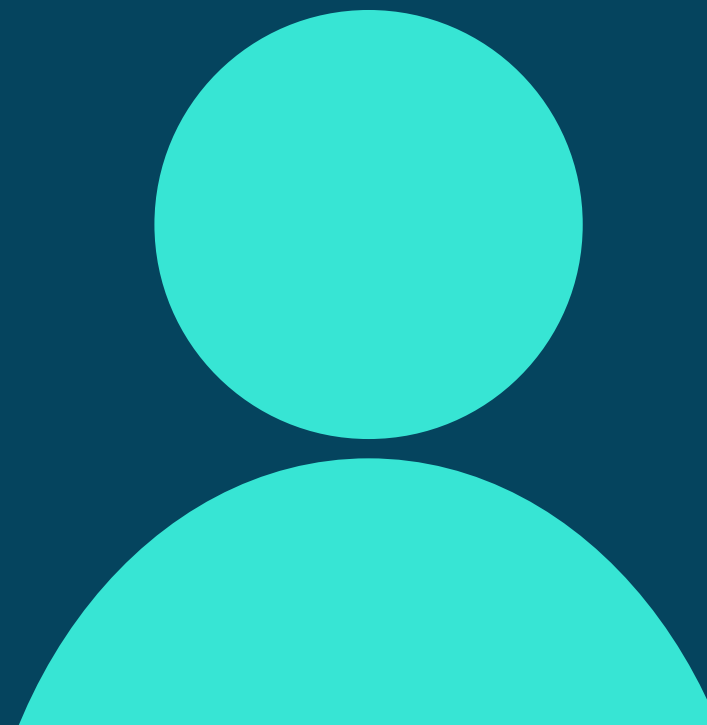
    address payable public founder;
    mapping(address => uint) public balances;
    mapping(address => mapping(address => uint)) allowed;

    event Transfer(address indexed _from, address indexed _to, uint256 _value);
    event Approval(address indexed _owner, address indexed _spender, uint256 _value);
```

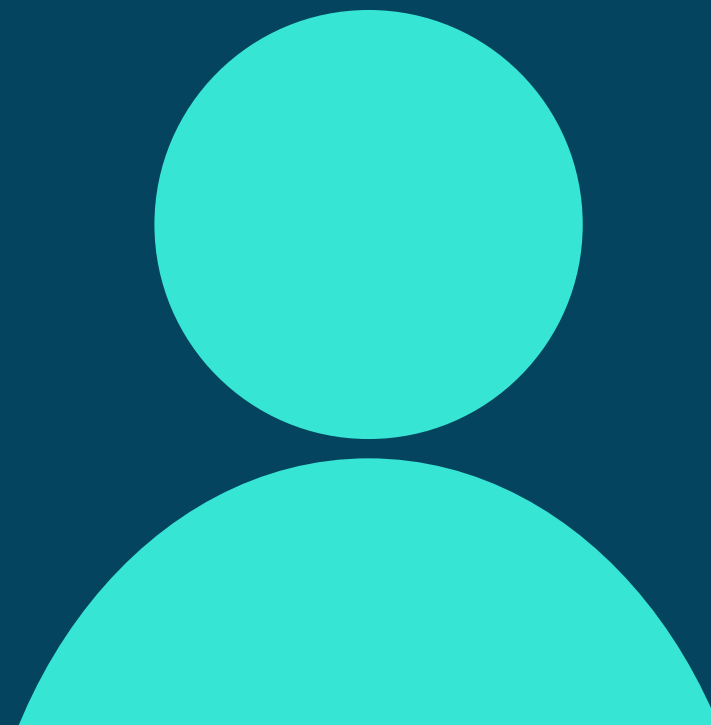
```
    constructor() public {
        supply = 10000;
        founder = msg.sender;
        balances[founder] = supply;
    }

    function initializeAccount() public override view returns (uint256){
        [...]
    }
    function totalSupply() public override view returns (uint256){
        [...]
    }
        function balanceOf(address _owner) public override view returns (uint256
balance){
        [...]
    }
    function transfer(address _to, uint _value) internal override returns (bool success)
{
        [...]
    }
        function transferFrom(address _from, address _to, uint256 _value) returns (bool
success){
        [...]
    }
}
```

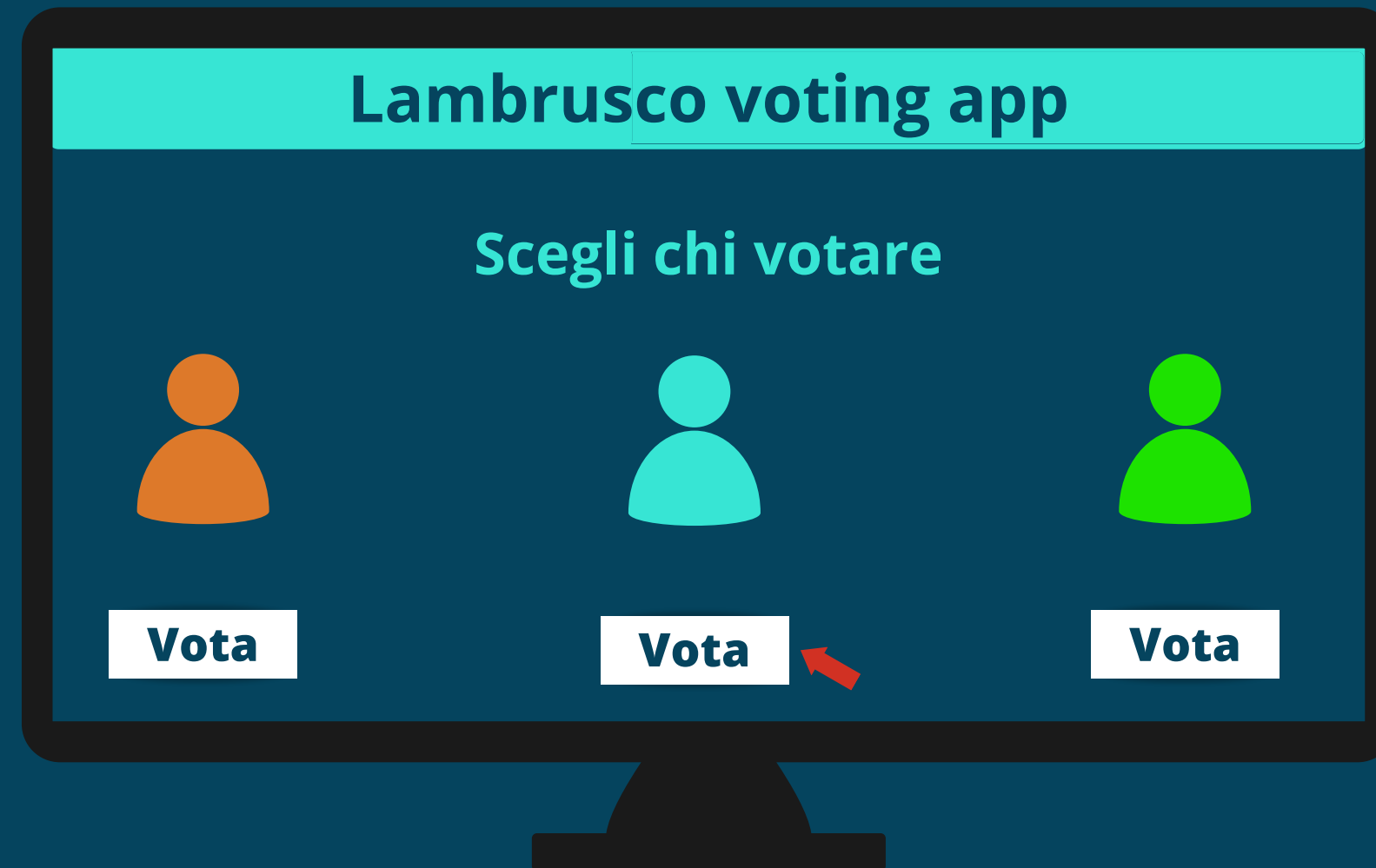
GUIDA AL VOTO TRAMITE SMART CONTRACT



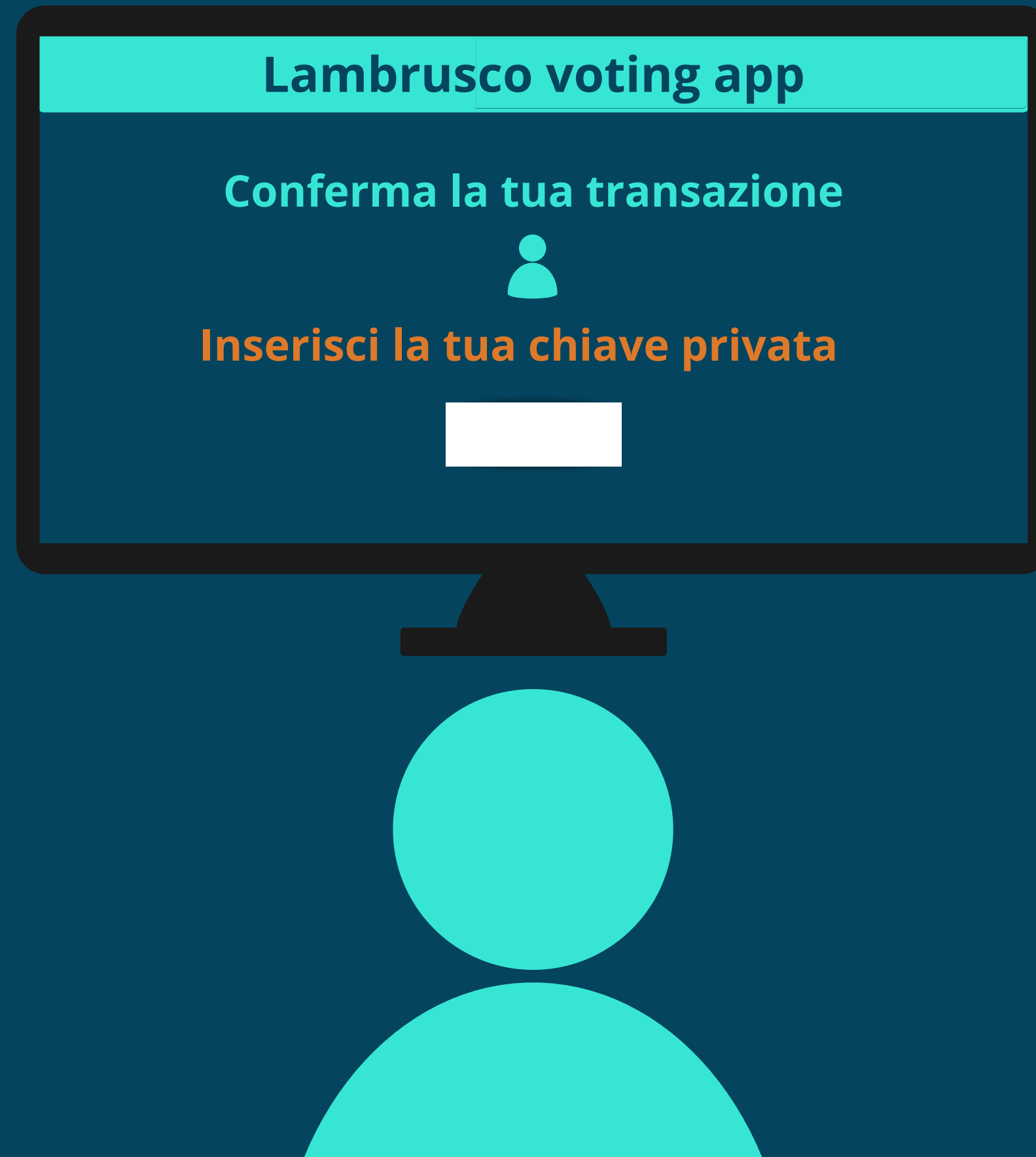
GUIDA AL VOTO TRAMITE SMART CONTRACT



GUIDA AL VOTO TRAMITE SMART CONTRACT



GUIDA AL VOTO TRAMITE SMART CONTRACT



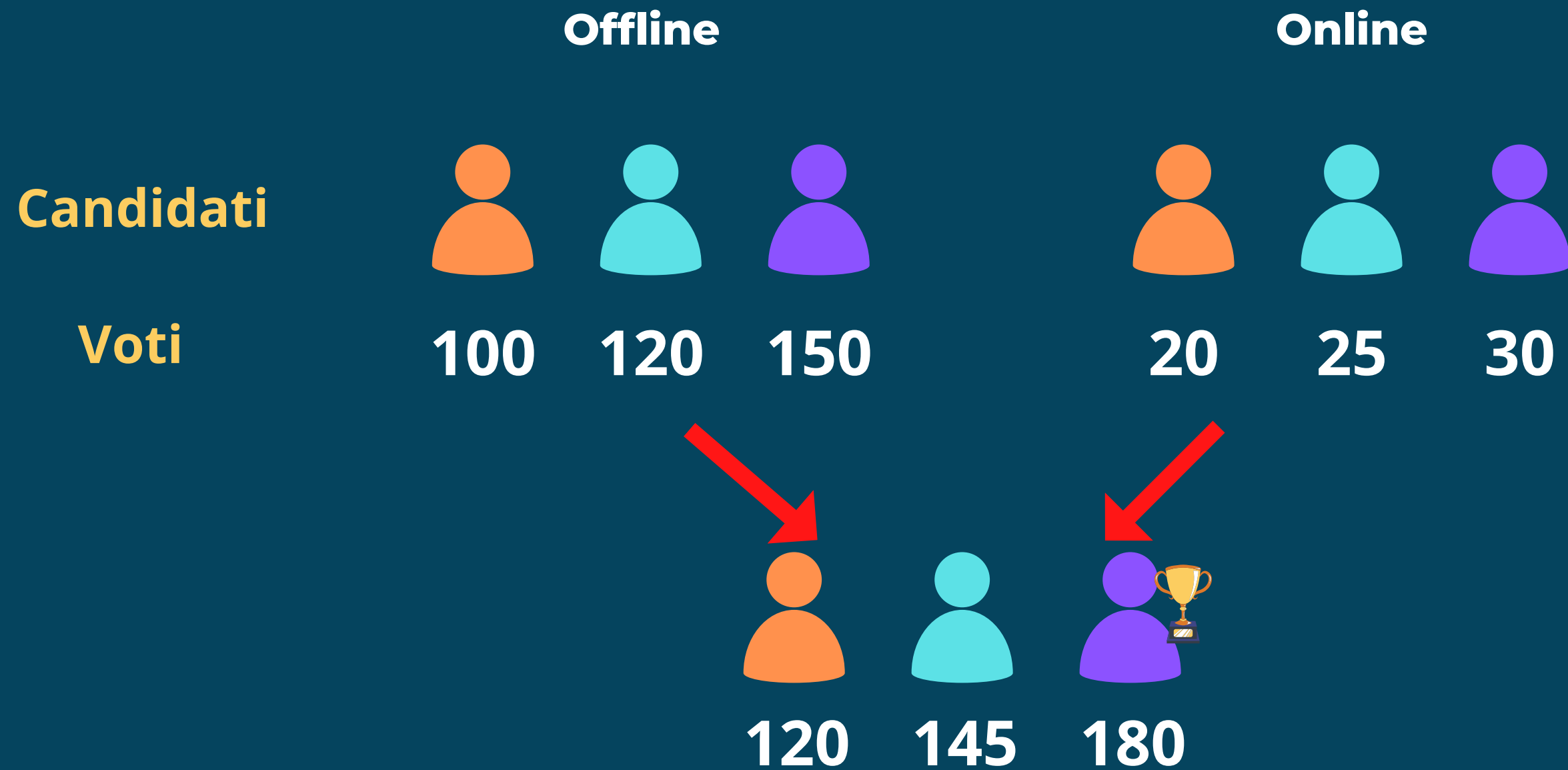
GUIDA AL VOTO TRAMITE SMART CONTRACT



FASE 3



Riconciliazione dei voti



FASE 4

- **Gestione delle infrastrutture a seguito delle elezioni**



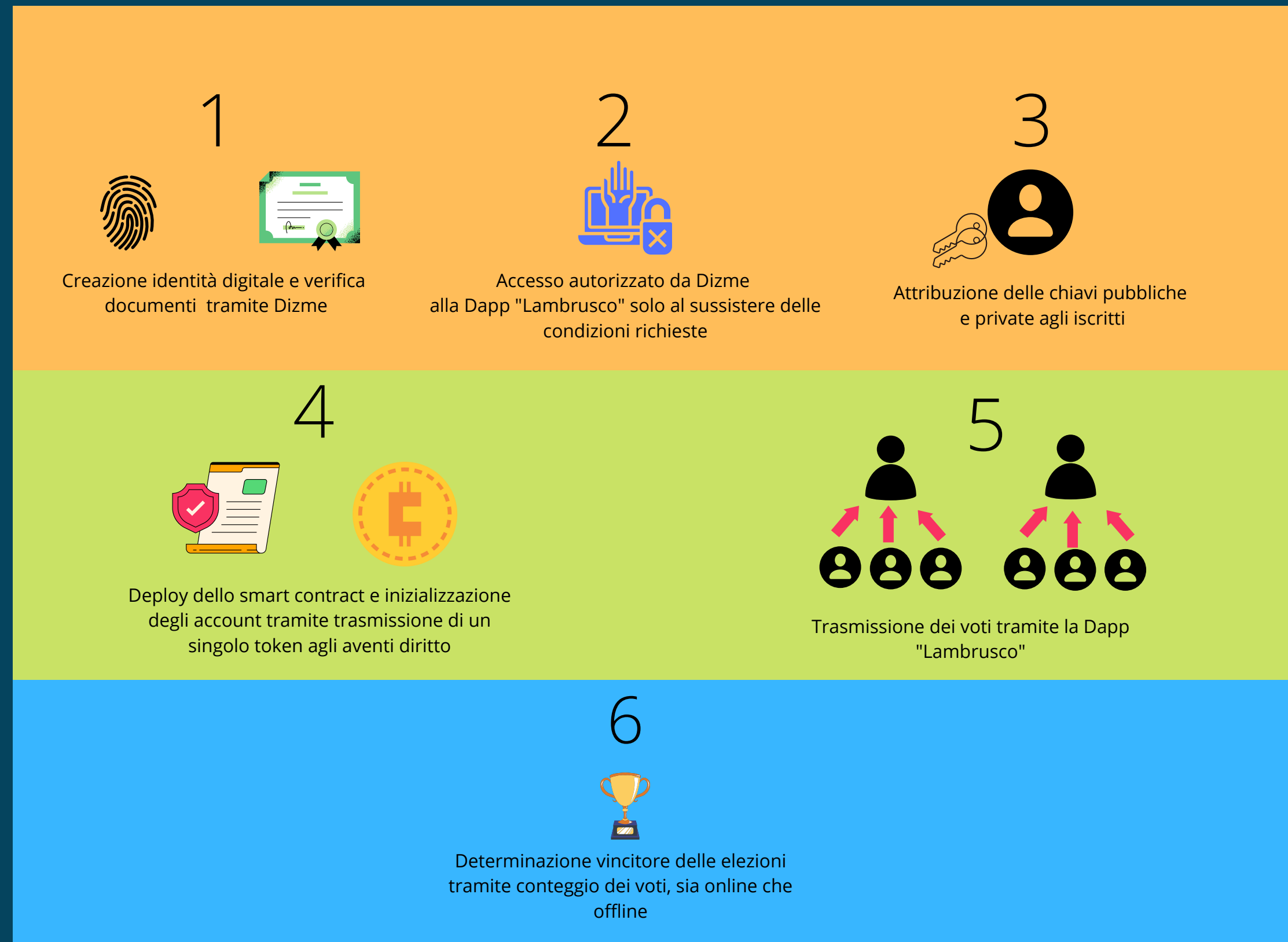
**Riutilizzo delle chiavi
per le elezioni successive**



**Generazione di nuove chiavi
per ogni elezione**

Soluzione?

RIASSUMENDO: IL NUOVO PROCESSO PER IL CITTADINO

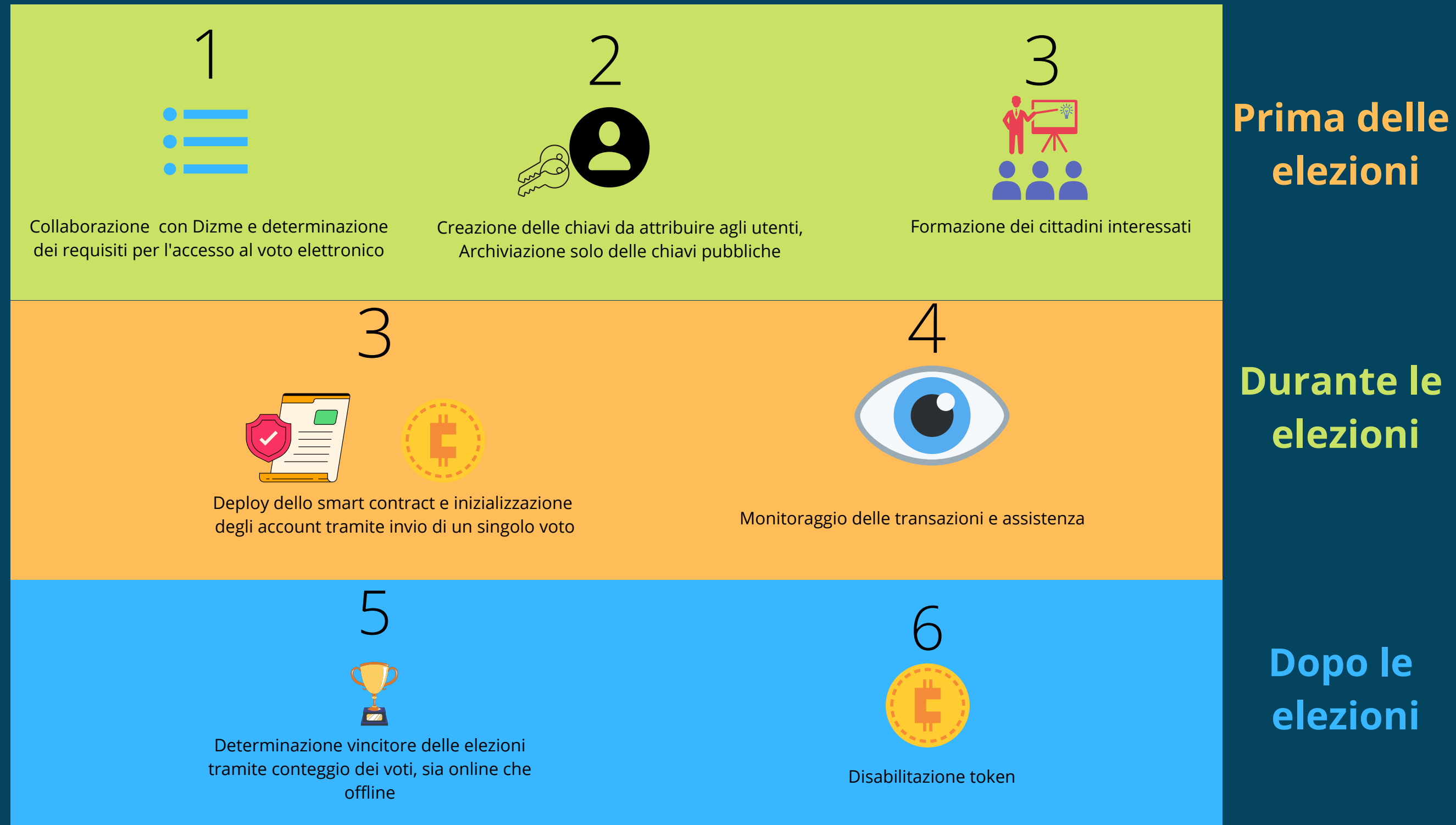


**Prima delle
elezioni**

**Durante le
elezioni**

**Dopo le
elezioni**

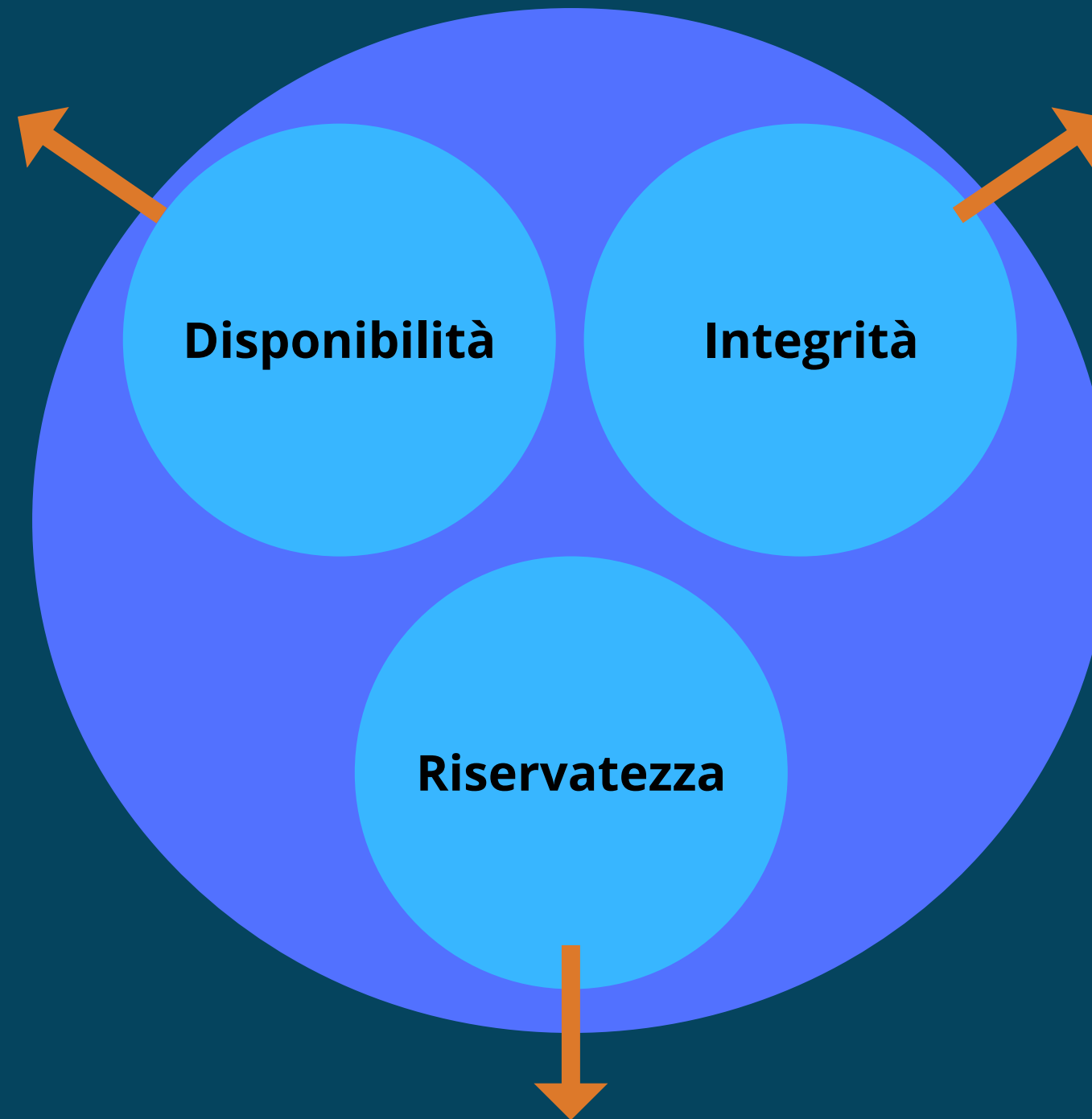
RIASSUMENDO: IL NUOVO PROCESSO PER L'ORGANIZZAZIONE



LA SICUREZZA

SMART CONTRACT

BLOCKCHAIN



SSI

Analisi dei rischi,
realizzazione e preventivo

I RISCHI

Tentativi di attuazione

Australia

Bangladesh

Belgio

Canada

Finlandia

Francia

Germania

Olanda

Estonia

Stati Uniti

Perche il nostro progetto è diverso?



Decentralizzazione

Processo lento e graduale

CAMPAGNA DI PROMOZIONE

● **Nudge**

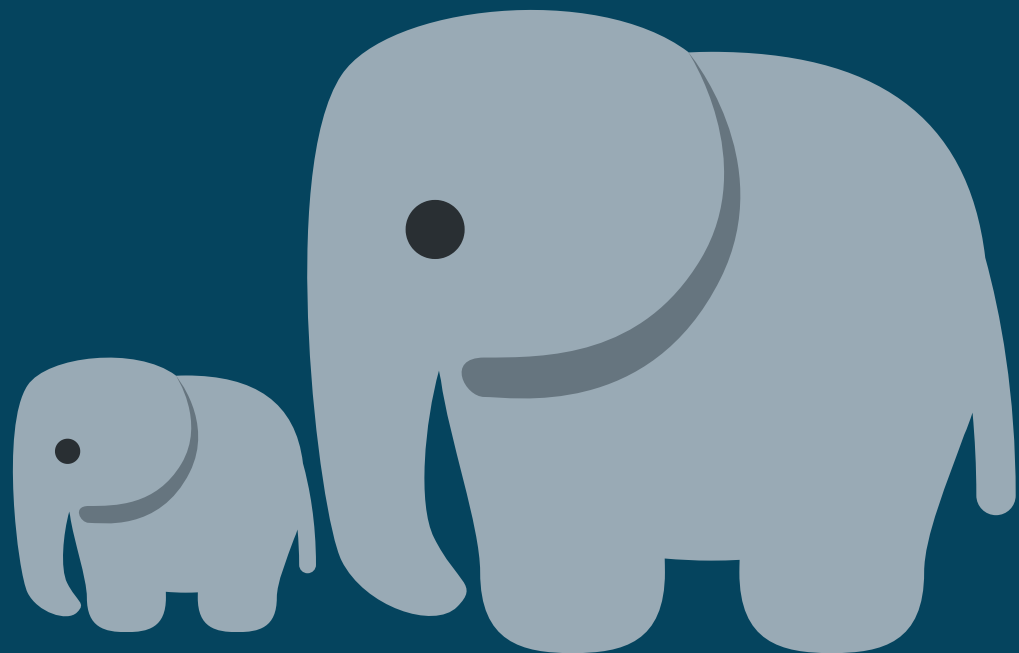


**"impossibilità di votare senza
il voto elettronico"**

● **Loss aversion**



**"il voto è uno strumento fondamentale
per partecipare alla democrazia "**



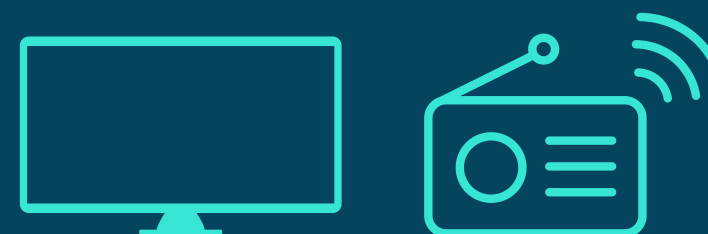
CAMPAGNA DI PROMOZIONE



Social media



Traditional media



"Il voto elettronico è essenziale"

Fuori sede

Estensione e cementificazione

Sostituzione



FASE 1

0-5 Anni

FASE 2

5-15 Anni

FASE 3

+ 15 anni

**Per una società che voglia
definirsi democratica, nessun
cittadino può essere escluso
dal diritto di voto.**

PREVENTIVO

Elementi

Smart contract

Realizzazione piattaforma

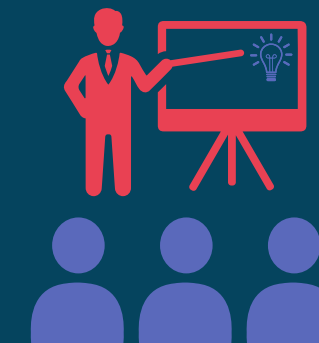
Formazione

Collaborazione dizme

Costi transazione su ethereum

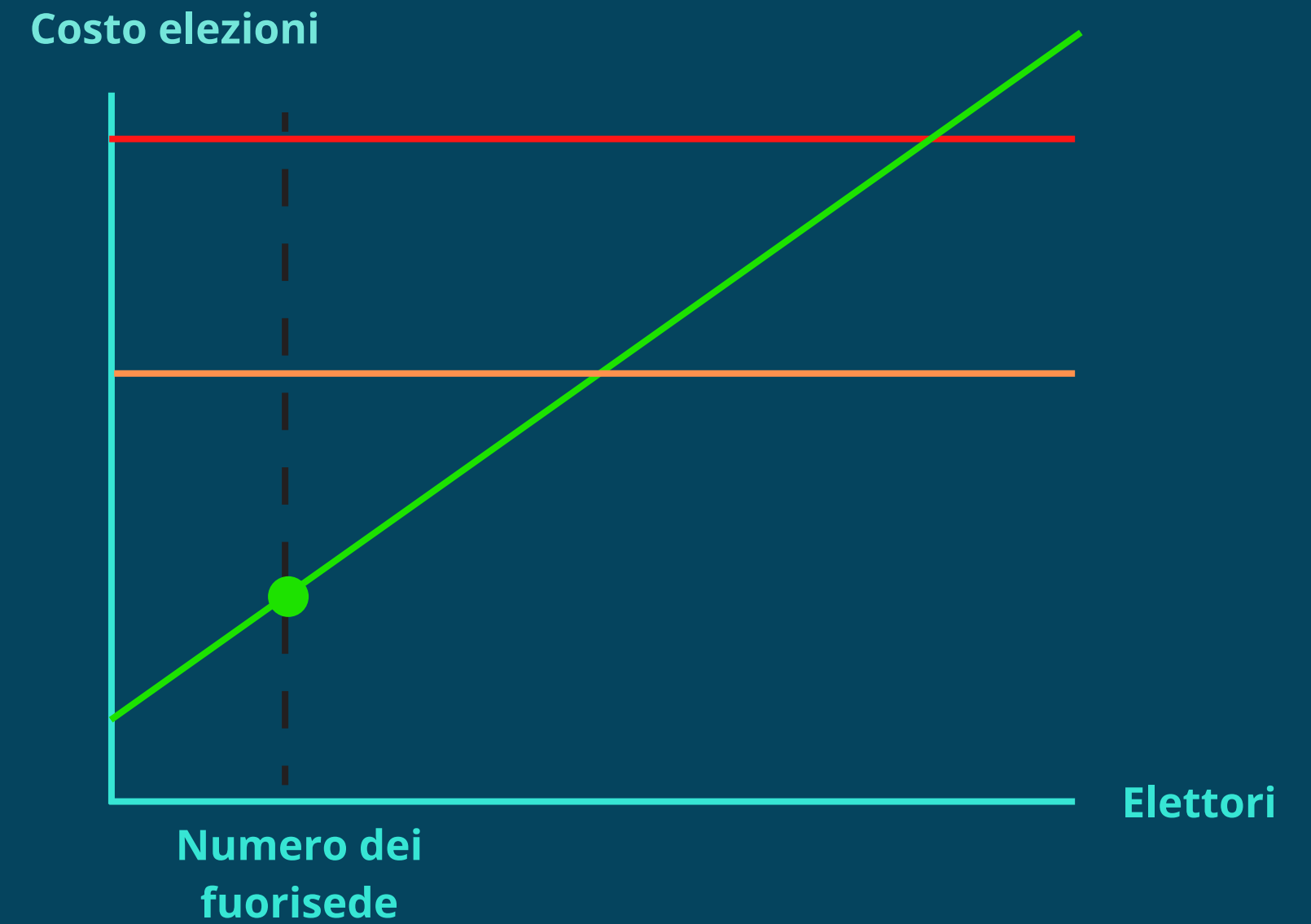
Assistenza e Monitoraggio

Progettazione ed implementazione



PREVENTIVO

Struttura dei costi nei diversi scenari



Voto
Tradizionale

E-Voting con
servizi
esternalizzati

E-Voting con
servizi gestiti
internamente

Conclusioni

L'ATTUALE PROCESSO PER IL CITTADINO

1



Ritiro tessera elettorale raggiunti i requisiti previsti dalla legge

Prima delle elezioni

2



Identificazione al seggio e simultanea consegna della scheda elettorale



3



Votazione privata al seggio

Durante le elezioni

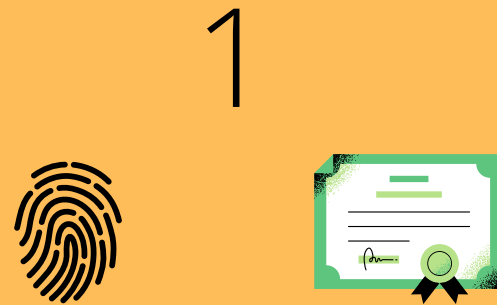
4



Determinazione vincitore delle elezioni tramite conteggio dei voti

Dopo le elezioni

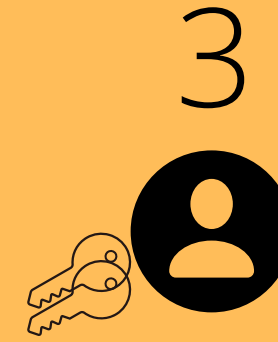
IL NUOVO PROCESSO PER IL CITTADINO



Creazione identità digitale e verifica documenti tramite Dizme



Accesso autorizzato da Dizme alla Dapp "Lambrusco" solo al sussistere delle condizioni richieste

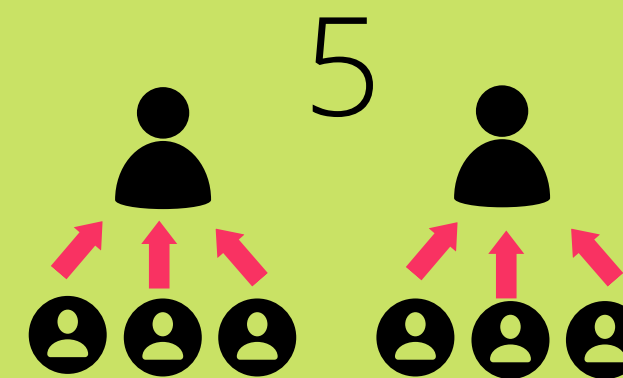


Attribuzione delle chiavi pubbliche e private agli iscritti

Prima delle elezioni



Deploy dello smart contract e inizializzazione degli account tramite trasmissione di un singolo token agli aventi diritto



Trasmissione dei voti tramite la Dapp "Lambrusco"

Durante le elezioni



Determinazione vincitore delle elezioni tramite conteggio dei voti, sia online che offline

Dopo le elezioni

L'ATTUALE PROCESSO PER L'ORGANIZZAZIONE

1



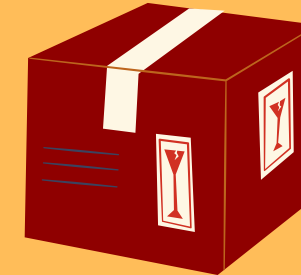
Selezione dall'albo degli scrutatori

2



Organizzazione dei membri dei seggi e degli scrutatori

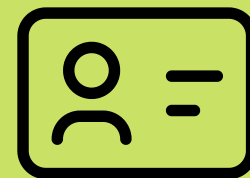
3



Fornitura dei seggi : cabine, schede, matite ecc

**Prima delle
elezioni**

3



Verifica delle identità e consegna delle schede elettorali

4



Gestione della corretto funzionamento delle elezioni

**Durante le
elezioni**

5



Conteggio manuale dei voti dei seggi e aggregazione degli stessi

6

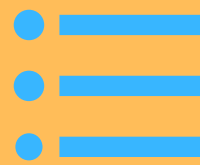


Determinazione vincitore delle elezioni tramite conteggio dei voti

**Dopo le
elezioni**

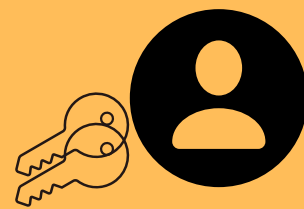
IL NUOVO PROCESSO PER L'ORGANIZZAZIONE

1



Collaborazione con Dizme e determinazione dei requisiti per l'accesso al voto elettronico

2



Creazione delle chiavi da attribuire agli utenti, Archiviazione solo delle chiavi pubbliche

3



Formazione dei cittadini interessati

Prima delle elezioni

3



Deploy dello smart contract e inizializzazione degli account tramite invio di un singolo voto



4



Monitoraggio delle transazioni e assistenza

Durante le elezioni

5



Determinazione vincitore delle elezioni tramite conteggio dei voti, sia online che offline

6



Disabilitazione token

Dopo le elezioni

Grazie per l'attenzione



ROBERTA GNISCI
ANDREA DI CHICCO
FEDERICO CASARANO
NICOLA LOPEZ
MASSIMILIANO AMBRUOSO
DOMENICO CIRIELLO