# An end-to-end voting-system based on bitcoin

**Stefano Bistarelli, Marco Mantilacci, Paolo Santancini, Francesco Santini. 2017**

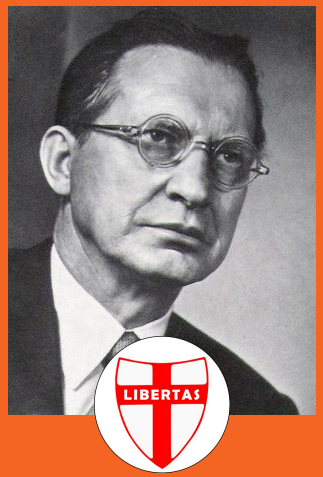
Alessio Zoccoli && Federico Ginosa

# Pre - votazione

# Presentazione lista elettorale

PUBBLICA

PRIVATA




Alcide De Gasperi


Ivan Matteo Lombardo


Palmiro Togliatti

Esempio delle elezioni italiane nel 1948

# Registrazione degli elettori

**Alice** **AS**

ID_Client_Alice: Dammi un **K_session2** valido per comunicare con TDS

{K_session1}K_alice, {AnonymousID, ValidTime, K_session1}K_AS

{AnonymousID, ValidTime, K_session1}K_AS, {AnonymousID, Timestamp}K_session1

{**K_session2**}K_session1, {AnonymousID, ValidTime, K_session2}K_TDS

# Registrazione degli elettori

**Alice**

**TDS**

{AnonymousID, TimeStamp}**K_session2**, {AnonymousID, ValidTime, K_session2}**K_TDS**

{Confirmation}K_session2

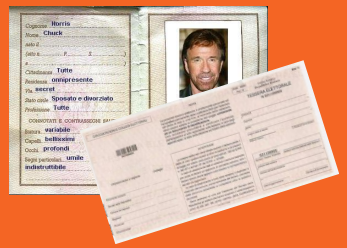
{K_public_bitcoin}K_session2

{token_confirmation, list candidati}k_session2

**TRANSAZIONE BITCOIN**

# Registrazione degli elettori

Alice




Scrutinatore


# Votazione

# Votazione

Alice

Berto

Cecilia

# Post-votazione

# Conteggio

```
const candidati = {
        'De_Gasperi': 0,
        'Lombardo': 0,
        'Togliatti': 0,
};

blocks.forEach(transactions => {
  Object.keys(candidati)
  .forEach(candidato => {
    candidati[candidato] += transactions
   .filter(({ mittente, destinatario }) =>
        destinatario === candidato && isValid(mittente)).length});
});
```