



UNIVERSITÀ DEGLI STUDI DI BOLOGNA

TESINA DI SISTEMI DISTRIBUITI

Voting Systems

Dr. Lisa Sajeve

Con il Professore
Dr. Andrea OMICINI

7 settembre 2015

Sommario

In questa tesina, si vuole fare una panoramica dell'evoluzione dei sistemi di voto sino ad arrivare al voto elettronico. Si descriveranno alcune delle architetture software utilizzabili per il voto elettronico ed il modo in cui esso sia immerso nel mondo reale. Inoltre troverete una panoramica di come si sia evoluta la democrazia, non dal punto di vista politico ma economico e matematico.

Abstract

In this essay, I want to do an overview of the evolution of voting systems until arriving at the electronic voting. I will describe some of the software architectures used for electronic voting and the way in which it is immersed in the real world. You will also find an overview of how democracy has evolved, not from a political point of view but look through economic and mathematics.

Indice

INTRODUZIONE	5
1 LA TEORIA DELLA DEMOCRAZIA	6
1.1 Il teorema della democrazia	6
1.2 Il paradosso di Condorcet	7
1.3 Il teorema di Arrow	8
1.4 Una nuova dimensione per la democrazia	9
2 SISTEMI DI VOTO	11
2.1 Voto del consiglio EU	11
2.2 Voto a punteggio	11
2.3 Voto elettronico	12
3 SISTEMI COMPLESSI E SISTEMI DISTRIBUITI	14
3.1 I sistemi complessi	14
3.2 I sistemi distribuiti	15
3.3 Le architetture	16
3.3.1 Stile architetturale	16
3.3.2 Architetture di sistema	17
3.4 Una possibile strutturazione del progetto di voting	18
4 CASI DI STUDIO	19
4.1 Sistema CINECA	19
4.1.1 Sito web riservato	19
4.1.2 Sito web pubblico	19
4.1.3 Architettura del sistema di voto	20
4.2 LiquidFeedback	21
4.2.1 Architettura	22
5 CONCLUSIONI	24

INTRODUZIONE

Quando si parla di *voting systems* (sistemi di voto) si intendono le modalità di elezione in una certa organizzazione. I metodi elettorali adottati fino ad oggi nella nostra società, tra più di due candidati, sono in generale poco equi, nel senso che l'esito della votazione dipende anche dal sistema stesso e non solo dalle preferenze espresse dagli elettori. Il tipo di sistema utilizzato influisce quindi sulla rappresentatività del candidato eletto rispetto alle preferenze degli elettori.

Con il termine *voto elettronico* si indicano le varie fasi del processo elettorale quali: la *fase preliminare* che identifica l'elettore e gestisce la sua legittimità al voto, la *fase centrale* che consiste nell'espressione del voto e la *fase finale* che comprende lo scrutinio, il conteggio e l'elaborazione dei risultati.

Quasi dieci anni di prove hanno dimostrato che il voto elettronico funziona. Ora occorrono tuttalpiù perfezionamenti tecnici in base alla volontà politica per generalizzarlo. I sistemi di voto elettronico sono spesso accusati di mancanza di trasparenza e vulnerabilità ai malware per cui tuttora si cercano soluzioni sempre innovative. D'altro canto, come vedremo, la sicurezza assoluta non esiste nemmeno nei metodi tradizionali di voto.

Un problema nato con questa nuova tipologia di voto è il *digital divide* ovvero la differente alfabetizzazione elettronico-informatica della popolazione. Il *digital divide* nasce dalle diverse condizioni di vita legate alle aree di residenza e differisce anche a seconda delle fasce di età. Tale problema non può essere ignorato da chi voglia sostenere la causa del voto elettronico, ma da alcuni studi emerge che anche una buona maggioranza di anziani è propensa all'avvento del voto elettronico perchè, sebbene possano avere poca dimestichezza con la tecnologia, il disagio di raggiungere il seggio è spesso ritenuto maggiore.

1 LA TEORIA DELLA DEMOCRAZIA

Lo studio dei sistemi di votazione da parte degli economisti e dei matematici ha sempre pervaso la storia della democrazia, ma con scarsa eco, dalla sua introduzione fino ad oggi. In generale, questi studi, sfatano il mito di uguaglianza che i politici hanno sempre attribuito ai sistemi di voto ed inoltre propongono soluzioni in generale più complicate ma che mirano a garantire uguale peso ad ogni voto espresso. Forse è proprio per questa maggiore complessità che fino ad oggi sembra abbia prevalso la retorica politica sulle logiche matematiche.

Con l'avvento dell'informatica e di Internet, la potenza di calcolo disponibile è nettamente aumentata ed i sistemi di voto elettronico sono diventati realizzabili. Si può quindi sperare, in avvenire, di avere votazioni più eque grazie all'applicazione di calcoli matematici come, ad esempio, quello illustrato nel paragrafo 1.4 e senza nemmeno il bisogno di recarsi nei seggi, grazie all'uso di reti informatiche.

Secondo l'*Enciclopedia Treccani*, la democrazia è una forma di governo che si basa sulla sovranità popolare e garantisce a ogni cittadino la partecipazione in piena uguaglianza all'esercizio del potere pubblico. Nel senso comune, il termine democrazia, indica invece un *governo di maggioranza*, la votazione è quindi vista come mezzo attraverso il quale il popolo governa. Tale semplificazione, da governo del popolo a mera maggioranza, è giustificata in termini matematici dal *Teorema della Democrazia* che descriveremo brevemente qui di seguito.

1.1 Il teorema della democrazia

Teorema della Democrazia (Kenneth May, 1952).

La votazione a maggioranza è il solo procedimento di votazione fra due alternative che soddisfa le seguenti condizioni minimali:

- Libertà individuale: *ogni preferenza individuale è accettabile.*
- Dipendenza dal voto: *il risultato della votazione fra due alternative è determinato dai voti su di esse e solo da essi.*
- Monotonicità: *se un'alternativa vince in una votazione, continua a vincere in ogni votazione in cui prenda più voti.*
- Anonimato: *non ci sono votanti privilegiati.*

Dimostrazione.

Si consideri una votazione tra due alternative A e B. Per la dipendenza dal voto, soltanto gli insiemi V_A (votanti che preferiscono A a B) e V_B (votanti che preferiscono B ad A) sono rilevanti per il risultato. Per l'anonimato ogni voto conta nello stesso modo e dunque soltanto i numeri n_A (votanti in V_A) ed n_B (votanti in V_B) sono rilevanti per il risultato.

Supponiamo che A prenda la maggioranza dei voti, cioè $n_A > n_B$, ma che sia B a vincere. Per la libertà individuale, si può immaginare una situazione in cui tutti i votanti scambino i loro voti (cioè chi prima ha votato per A ora voterà per B e viceversa). Si avrebbe allora una situazione simmetrica alla precedente e per lo stesso principio, questa volta, sarebbe A a dover vincere ma per la monotonicità sarebbe B a dover vincere (perchè B vinceva prima quando prendeva meno voti di quanti ne prende ora). Si è giunti così ad una contraddizione che dimostra la tesi. $\square$

1.2 Il paradosso di Condorcet

Ancor prima del *Teorema della Democrazia*, venne scoperto il seguente paradosso del sistema di votazione a maggioranza che porta a concludere che l'unica votazione efficiente di questo tipo sia quella tra due candidati.

Paradosso di Condorcet (1785).

Un insieme di individui con preferenze razionali non ha necessariamente preferenze razionali quando agisce come gruppo.

Ci si aspetta infatti che con un numero $n > 2$ di alternative, si proceda votando a due a due e scegliendo il candidato che abbia riportato la maggioranza contro tutte le rimanenti. Tale alternativa però non può esistere. Anche se le preferenze dei singoli votanti rispetto ai vari candidati fossero ordinate linearmente, la votazione potrebbe comunque produrre un ordine sociale circolare. Ad esempio con $n = 3$, detti A, B e C i candidati, si possono avere i seguenti ordini ciclici di preferenze:

$$1 : A > B > C$$

$$2 : B > C > A$$

$$3 : C > A > B.$$

Ponendo quindi le alternative a due a due si ha che: A vince su B per due voti ad uno ed analogamente B vince su C per due voti ad uno. Si potrebbe quindi pensare che A dovrebbe vincere su C, invece succede il contrario. In particolare, se A viene votata contro la vincitrice tra B e C (B) essa vince

ma lo stesso accade per B se essa viene votata contro la vincitrice tra A e C (C) e per C se viene votata contro la vincitrice tra A e B (A). Il paradosso quindi non lascia scelta: o si votano tutte le alternative una contro l'altra, ed allora non può esserci un vincitore oppure si votano le varie alternative in un certo ordine ed allora il vincitore dipende dall'ordine scelto.

1.3 Il teorema di Arrow

La democrazia, come tutti sappiamo, dominò la storia dalla sua introduzione fino ai giorni nostri, nonostante fosse nota la sua inconsistenza logica. Probabilmente, tale inconsistenza non venne presa in considerazione perchè non esisteva un'alternativa migliore ed il cambiamento era necessario. Gli studiosi come Kenneth Arrow continuarono però a porsi domande a riguardo, cercando soluzioni più eque.

Il paradosso di Condorcet mostra che un particolare sistema di votazione (a maggioranza) non permette di estendere la transitività delle preferenze individuali a quelle sociali. Esiste allora un sistema di votazione che permetta di farlo? Ovvero, è possibile la democrazia? La risposta che Arrow trovò è NO.

Teorema di Arrow.

Sia n il numero dei cittadini votanti e m il numero delle possibili alternative. Se $n \geq 2$ e $m \geq 3$, allora non è possibile costruire una funzione di scelta sociale che soddisfi contemporaneamente tutti i seguenti requisiti:

- Dominio non ristretto: *la funzione di scelta sociale dovrebbe creare un ordinamento delle preferenze sociali deterministico e completo, a partire da qualsiasi insieme iniziale di preferenze individuali.*
- Sovranità del cittadino: *qualsiasi possibile preferenza sociale deve essere raggiungibile a partire da un appropriato insieme di preferenze individuali.*
- Non dittatorialità: *la funzione di scelta sociale non deve semplicemente seguire l'ordinamento delle preferenze di un individuo o un sottoinsieme di individui ignorando le preferenze degli altri.*
- Monotonicità: *se un individuo modifica il proprio ordinamento di preferenze promuovendo una data opzione, la funzione di scelta sociale deve promuovere tale opzione o restare invariata, ma non può assegnare a tale opzione una preferenza minore.*

- Indipendenza dalle alternative irrilevanti: *se si confina l'attenzione ad un sottoinsieme di opzioni, e la funzione di scelta sociale è applicata ad esse soltanto, il risultato deve essere compatibile con il caso in cui la funzione di scelta sociale è applicata all'intero insieme di alternative possibili.*

1.4 Una nuova dimensione per la democrazia

Dunque, come dicevamo, solo l'elezione tra due candidati sembrerebbe compatibile con i principi della democrazia ma nel mondo reale ci troviamo a dover esprimere la nostra preferenza su un range molto più ampio. Inoltre i risultati sono influenzati anche dal metodo scelto per le votazioni. Una possibile soluzione a questo problema viene proposta nel paper [10] che aggiunge alla massimizzazione totale della soddisfazione dei votanti (teoria di Condorcet), un ulteriore principio (*dimensione*) secondo il quale la soddisfazione deve essere distribuita tra i votanti il più equamente possibile. Viene poi dimostrato che la dimensione introdotta è più stabile rispetto alle fluttuazioni della sola massimizzazione della soddisfazione, che da sola, talvolta risulta non ottima.

Supponiamo di avere n votanti che esprimano la loro preferenza su m candidati creando una classifica possibilmente con relazioni di ordine totale del tipo $<$ o $\leq$. Chiamiamo r_v il voto dell'elettore v ed assumiamo come distanza tra la posizione in classifica e il voto, quella di *Kemeny*, d_{kem} . Secondo la *teoria di Condorcet* un buon metodo per la selezione del vincitore consiste nel massimizzare la somma totale dei desideri, ovvero trovare le classifiche c^* che minimizzano la somma delle distanze come segue:

$$\mu(c) = \frac{1}{n} \sum_{v=1}^n d_{kem}(r_v, c).$$

Il calcolo di c^* è in generale un problema NP-hard poichè lo spazio di tutte le possibili classifiche, con ordine totale, cresce più velocemente di $m!$. Nella pratica sono stati sviluppati molti algoritmi polinomiali che forniscono soluzioni subottime secondo determinate regole di voto. Sebbene nessuno sia perfettamente equo, si possono in generale considerare sufficientemente ragionevoli. Rimangono però irrisolti alcuni problemi:

- metodi di voto differenti possono avere risultati differenti;
- restituendo un'unica classifica di consensi, molte informazioni sulle preferenze dei votanti vanno perse;

- iii) spesso si ottengono valori di $\mu(c)$ molto vicini all'ottimo e non è chiaro come mai si differenzino.

Anche alla luce di queste osservazioni è stata introdotta la nuova dimensione descritta in precedenza. Supponiamo di considerare come valide tutte le classifiche c abbastanza vicine all'ottimo, ovvero tali che $\mu(c) - \mu(c^*) \simeq 1/\sqrt{n}$. L'idea è far sì che non solo il numero globale di preferenze soddisfatte sia massimizzato ma anche che ogni votante possa avere all'incirca lo stesso numero di preferenze soddisfatte. Chiamiamo quindi $\sigma(c)$ la deviazione standard della variabile di soddisfazione

$$\sigma(c) = \sqrt{\frac{1}{n} \sum_{v=1}^n [d_{Kem}(r_v, c) - \mu(c)]^2}.$$

Se $\sigma(c) = 0$, c soddisfa in modo equo ogni votante, altrimenti al crescere di $\sigma(c)$ aumentano i votanti insoddisfatti.

2 SISTEMI DI VOTO

Attualmente, nel mondo, esistono svariati metodi e tipologie di voto, ognuno con i propri pregi e difetti. Qui di seguito vedremo alcuni dei metodi di votazione attualmente adottati in Europa e nel Mondo.

2.1 Voto del consiglio EU

Per fare un esempio, analizziamo le tipologie prese in considerazione dal *Consiglio dell'Unione Europea* [5]. Il metodo di voto standard del Consiglio è la *maggioranza qualificata*, cioè quella che richiede la presenza del 55% degli stati membri e che essi rappresentino almeno il 65% della popolazione dell'UE.

Esiste poi la *maggioranza semplice*, utilizzata per le votazioni non legislative, che equivale a 15 Stati membri su 28 e l'*unanimità* che richiede il voto favorevole di tutti i membri che hanno però anche la possibilità di astenersi. Sono poi ammessi anche alcuni meccanismi di delega dei quali bisogna tener conto nei relativi calcoli.

2.2 Voto a punteggio

Il voto a punteggio è forse il preferito da matematici ed informatici. Nei sistemi elettorali attualmente più diffusi è possibile che un partito vinca o comunque guadagni molti punti non perchè sia effettivamente il preferito ma perchè i voti degli oppositori sono dispersi su più partiti.

Il *range voting* o voto a punteggio permette di ovviare a questo problema di *voto tattico* garantendo rappresentatività e pluralismo. Invece di scegliere un solo candidato, l'elettore deve dare un voto all'interno di un range (es. da 1 a 10) a ciascun candidato, anche senza esprimere necessariamente un ordine univoco di preferenza. Il vincitore sarà il candidato con il **voto medio** più alto.

Una proprietà importante del voto a punteggio è che è possibile ottenere numerosi altri sistemi elettorali esplorandone i casi limite. Uno degli svantaggi consiste invece nel fatto che non necessariamente vince il candidato di maggioranza ma facilmente porta alla vittoria candidati che non sono i preferiti di nessuno ma che sono decenti per la maggioranza dei votanti. Un sistema elettorale in cui vincono regolarmente le seconde scelte, anche se minimizza l'insoddisfazione di ciascun votante, per molti è comunque insoddisfacente come metodo. Infatti, una misura astratta della soddisfazione dell'elettorato non è una misura che dobbiamo ritenere per forza la più giusta. Inoltre ciascuno usa una scala diversa di valutazione. Alcuni possono

scegliere di dare il voto massimo al candidato preferito e via via voti inferiori agli altri; altri possono dare un voto onesto di soddisfazione personale e quindi voti estremi come 0 o 10 non vengono quasi mai assegnati. Sommare i punteggi a questo punto è un esercizio di confusione, perché il punteggio per ciascun elettore significa qualcosa di diverso. Alla fine si rischia di dare più peso a chi estremizza il voto (dando sempre zero o il massimo), annullando il senso del range voting.

2.3 Voto elettronico

Uno dei primi Paesi ad adottare il voto elettronico è stato il Brasile, che si è dotato già dal 1996 di un sistema di votazione elettronica detto Dre (Registrazione Diretta Elettronica). Gli elettori utilizzano un piccolo dispositivo con uno schermo e una tastiera. La macchina visualizza l'elenco dei candidati e le relative immagini, per votare è sufficiente digitare un numero sulla tastiera. Al termine dell'operazione, si riceve una ricevuta che conferma l'avvenuta votazione. Ci sono però altri Paesi che hanno deciso di adottare voting system elettronici. Nel 2009 si sono tenute le prime elezioni completamente digitali per il rinnovo dell'amministrazione di Honolulu, nello stato delle Hawaii. Ogni elettore ha ricevuto un codice con il quale accedere a un sito dove esprimere la propria preferenza. In uno stato dell'Australia si è invece deciso di usare un software open source per garantire la trasparenza del codice e consentire al pubblico di valutarlo. Finora tutto ha funzionato alla perfezione ma il sistema non è stato esteso anche ad altri stati per un problema di costi. L'esempio migliore di voto via internet viene invece dall'Estonia. Il governo ha fornito alla popolazione una carta d'identità digitale che permette l'accesso a un gran numero di servizi online. Attraverso un software di cifratura digitale a 2048 bit, i cittadini hanno la possibilità di votare stando comodamente seduti nel salotto di casa propria. La questione del voto elettronico e online è insomma quanto mai delicata e complessa.

In Italia le prime sperimentazioni di voto elettronico sono state effettuate nel 1997 in quattro Comuni della Valle d'Aosta, dove per l'identificazione si è fatto uso di Carte d'Identità digitali precedentemente distribuite. Nel 2006 sono state effettuate alcune sperimentazioni su amministrazioni locali in Sardegna, Trentino, Liguria, Puglia e Lazio. Nonostante i risultati abbastanza positivi, non è stato dato seguito all'iniziativa e per ora sono inesistenti sia normative in materia sia progetti di sperimentazione su più larga scala. Staremo a vedere cosa ci riserverà il futuro.

Uscendo dal campo puramente politico, l'esempio più articolato ovvero quello che ha interessato fin ora il maggior numero di elettori, è il sistema che il CINECA [8] ha realizzato nel 1999 per conto del Ministero dell'Università e

della Ricerca Scientifica e Tecnologica (MURST), esso è finalizzato all'elezione delle *Commissioni di Valutazione* dei docenti e dei ricercatori universitari. Tale sistema telematico si compone di tre parti: un sito riservato agli Uffici Concorsi degli Atenei per lo scambio tempestivo di informazioni tra le Università e il MURST; un sito Internet ad accesso pubblico per diffondere i bandi e l'esito degli scrutini; ed infine il sistema di voto vero e proprio. In 79 seggi elettorali, e da 203 postazioni di voto (installate su altrettanti computer Javastation) distribuite negli Atenei in tutta Italia, gli elettori votano per via telematica grazie a collegamenti su linea ISDN in un sistema chiuso all'utenza esterna. In circa 2 anni sono state svolte più di 8.000 elezioni ed i voti gestiti sono stati all'incirca 1,5 milioni.

3 SISTEMI COMPLESSI E SISTEMI DISTRIBUITI

Introdurremo qui il concetto di sistemi complessi portando come esempio la nuova dimensione di democrazia introdotta nell'articolo di *Contucci e colleghi* [10] ed in seguito vedremo come questi possano essere trattati con sistemi distribuiti.

3.1 I sistemi complessi

I sistemi complessi sono caratterizzati dall'interazione, non banale, tra componenti autonomi; tali componenti interagiscono localmente ma provocano cambiamenti nel sistema complessivo. La scienza, in genere, può rilevare le modifiche locali ma non può prevedere uno stato futuro del sistema considerato nella sua interezza. Con l'evolversi della conoscenza di Internet e della programmazione in generale, l'interazione tra oggetti di qualsiasi tipo ha assunto via via un ruolo sempre più importante. Non è possibile descrivere un sistema complesso esclusivamente dal comportamento delle sue componenti ma è necessario studiare le *interazioni* tra le componenti che a loro volta sono immerse in uno specifico *ambiente*. Le interazioni sono in genere *mediate* in modo da permettere la comunicazione tra ambienti diversi. Infine per governare l'intero sistema di interazioni è necessaria un'*infrastruttura* che determini leggi collettive e norme per l'interazione.

Sebbene i sistemi complessi si possano ritrovare in tutti i campi delle scienze, vi sono tra loro delle differenze. Ad esempio, mentre i sistemi fisici vengono osservati, capiti e possibilmente modellati, quelli computazionali vengono disegnati e costruiti. Ovvero, nei sistemi computazionali le interazioni e le leggi non vengono ricavate ma devono essere definite dal costruttore del sistema. Tali definizioni, talvolta, possono portare a malfunzionamenti del sistema stesso perchè non esprimevano completamente quello che si pretendeva dal sistema in esame.

I sistemi sociali possono rappresentare un ponte tra statistica matematica ed informatica poichè alcune leggi sociali possono essere descritte matematicamente e quindi poi decodificate in un algoritmo. Un possibile esempio è quello, sopra descritto, dell'elezione in cui un unico vincitore viene eletto per maggioranza (vedi paragrafo 1.4).

3.2 I sistemi distribuiti

Secondo la definizione di Coulouris e Dollimore, un sistema distribuito è formato da componenti hardware e software localizzati su computer in rete che *comunicano* e *coordinano* le loro azioni attraverso scambio di messaggi. Ciascun computer può essere indipendente e autonomo ma il progettista del sistema distribuito li concepisce in modo tale che all'utente appaiano come un sistema *unico* e *coerente*. Ricordando quanto detto per definire un sistema complesso si può subito notare quanto i sistemi distribuiti siano adatti a descriverlo, difatti anch'essi trattano con componenti autonome che, comunicando tra loro secondo regole precise permettono di evolvere il sistema generale.

Le caratteristiche peculiari di un sistema distribuito sono: accessibilità delle risorse, trasparenza, apertura e scalabilità.

- **accessibilità delle risorse:** permette a utenti e applicazioni di condividere risorse in maniera efficiente e controllata;
- **trasparenza:** nasconde il fatto che i processi e le risorse sono fisicamente distribuite su molti computer; in generale permette di nascondere proprietà non rilevanti aumentando il livello di astrazione del sistema, ma non è sempre funzionale. Esistono infatti diversi tipi di trasparenza che vanno adottati secondo le esigenze del problema:
 - **Accesso** nasconde le differenze nella rappresentazione dei dati e nelle modalità di accesso alle risorse.
 - **Ubicazione** nasconde la posizione in cui si trova la risorsa.
 - **Migrazione** nasconde che una risorsa si può spostare in un'altra posizione.
 - **Riposizionamento** nasconde che una risorsa si può spostare in un'altra posizione mentre è in uso.
 - **Replica** nasconde la replica di una risorsa.
 - **Concorrenza** nasconde che una risorsa può essere condivisa da più utenti in competizione.
 - **Guasto** nasconde il malfunzionamento e la riparazione di una risorsa.
- **apertura** (*openess*): è una caratteristica tipica della maggior parte dei sistemi complessi e deriva dai requisiti. I sistemi aperti hanno la caratteristica di essere non predicibili; è predicibile a livello di comportamenti (quello che è consentito fare all'utente) ma non è predicibile il momento in cui i comportamenti verranno adottati.

- **scalabilità**: secondo la definizione di Neuman,¹ la scalabilità indica la capacità di un sistema distribuito di migliorare le proprie prestazioni all'aumentare di risorse ed utenti (*scalabilità rispetto alla dimensione*), distanza tra risorse e utenti (*scalabilità geografica*) e del numero di domini amministrativi coinvolti (*scalabilità amministrativa*). La maggior parte dei sistemi distribuiti si occupa soltanto e in modo parziale della scalabilità rispetto alla dimensione. La tecnica più comune e banale è utilizzare macchine più potenti ma esistono altre tecniche per la scalabilità, come ad esempio nascondere le latenze nella comunicazione svolgendo altre operazioni utili all'utente nell'attesa delle risposte, sfruttando le tecniche di comunicazione asincrona oppure suddividendo i dati e le computazioni su molteplici macchine o ancora rendendo disponibili copie dei dati su macchine diverse.

3.3 Le architetture

L'organizzazione dei sistemi distribuiti è relativa ai componenti software che costituiscono il sistema. Al fine di gestire la complessità, i sistemi distribuiti devono essere adeguatamente organizzati. I modi in cui sono organizzati i componenti di un sistema distribuito sono detti in generale *architetture* e l'istanziatura finale di un'architettura software, in generale, si dice *architettura di sistema*. Si dice invece *stile architetturale* l'insieme dei componenti, del modo in cui i componenti sono connessi tra loro e del modo in cui i dati fluiscono attraverso i componenti. La nozione di stile architetturale è quindi un modo per raggruppare e classificare gruppi di sistemi simili, cioè, aventi lo stesso tipo di architettura. Questo significa diminuire le possibilità con cui i componenti (elementi modulari con interfacce ben definite) e i connettori (astrazioni che mediano l'interazione tra i componenti) possono essere uniti. L'*Architettura Software* si utilizza per descrivere la struttura dei sistemi software in termini architetturali, l'*Architettura di Sistema*, invece, descrive in maniera minuziosa anche aspetti quali la distribuzione.

3.3.1 Stile architetturale

Esistono vari tipi di stili architetturali: a strati, ad oggetti, a data center ed a eventi.

¹Alcune dimensioni della scalabilità definite da Neuman sono: (i) il numero degli utenti; un sistema deve crescere quando gli utenti o le risorse crescono, (ii) il luogo degli utenti; un sistema deve crescere quando la distribuzione degli utenti e delle risorse crescono, (iii) un sistema deve crescere quando aumentano i diversi domini amministrativi. Inoltre il sistema deve rimanere facilmente gestibile anche se copre molte strutture indipendenti.

1. **Architetture a strati.** Sono organizzate in strati (*layer*) ed ogni componente che appartiene a uno strato può interagire solo con i componenti degli strati adiacenti. Le richieste scendono lungo la gerarchia mentre le risposte risalgono e insieme ai dati passa anche il controllo.
2. **Architetture ad oggetti.** Tutte le componenti sono oggetti interconnessi mediante il meccanismo RPC (Remote Procedure Call).
3. **Architetture a data center.** Sono costituite da un insieme di processi autonomi che passano attraverso un'unica repository condivisa da cui partono tutte le interazioni.
4. **Architetture a eventi.** I processi comunicano attraverso un event-bus il quale propaga gli eventi portando con sé i dati, in questo modo i processi possono comunicare senza aver bisogno di condividere lo spazio o una referenza per gli altri processi.

Unendo le caratteristiche delle architetture a data center e di quelle ad eventi, si generano le così dette **Architetture a spazi di dati condivisi** che permettono il disaccoppiamento dei processi anche nel tempo. Un esempio fondamentale di sistemi di questo tipo sono i **sistemi a blackboard** dove i processi mettono i dati su una "lavagna" con varie operazioni. Il disaccoppiamento è dato dal fatto che una volta che il messaggio è stato lasciato e l'evento non c'è più, si può sempre andare a leggerlo direttamente nella repository condivisa. Non vi è quindi bisogno della presenza di chi l'ha scritto.

3.3.2 Architetture di sistema

Oltre a decidere quali software usare, è necessario stabilire come essi interagiscono e dove siano situati, per fare ciò si può scegliere una tra le seguenti macro categorie: architettura centralizzata, decentralizzata o ibrida.

1. **Architettura centralizzata.** I dati e le applicazioni risiedono in un unico nodo elaborativo (server). Il server implementa uno specifico servizio mentre i client lo richiedono e attendono risposta.
2. **Architettura decentralizzata.** I nodi (peer) sono tutti di un tipo, svolgono sia il ruolo di client che di server, non c'è coordinamento centrale delle loro attività.
3. **Architettura ibrida.** A volte è utile sfruttare le caratteristiche di entrambe le architetture precedenti. Si possono distinguere due tipologie principali: sistemi edge-server e sistemi distribuiti collaborativi.

- nei *Sistemi edge-server*, i server sono posizionati ai bordi della rete ("edge" ovvero il confine tra la rete aziendale e internet).
- nei *Sistemi distribuiti collaborativi*, una volta che un nodo si è unito al sistema tramite uno schema client-server tradizionale, può usare per la collaborazione uno schema completamente decentralizzato.

3.4 Una possibile strutturazione del progetto di voting

Quello che ci aspettiamo dal nostro sistema distribuito è che gli utenti possano accedere al sistema in qualsiasi momento, soprattutto durante i periodi, di grande richiesta, in cui sono previste le elezioni. Inoltre vogliamo garantire che ogni votante possa esprimere un solo voto, deve quindi essere identificabile in modo univoco ma deve poter comunque mantenere il voto anonimo. Dall'altro lato vogliamo che il sistema sia in grado di calcolare il vincitore secondo le regole descritte nel paragrafo 1.4, una volta ricevute tutte le informazioni necessarie.

Vediamo quindi quali strumenti e proprietà si possono adattare, in generale, al problema. Per quanto riguarda la scalabilità, non dovrebbero essere necessari particolari accorgimenti riguardo alla dimensione in quanto non ci sono rapide variazioni di popolazione e sono comunque prevedibili con largo anticipo (si vota solo raggiunta una certa età). Si rende però necessaria la scalabilità geografica in quanto bisogna tener conto degli elettori residenti all'estero.

Per il sistema di voting scelto, si può adottare lo stile architetturale ad oggetti di tipo client-server, tale sistema è formato da due tipi di moduli, il client e il server, eseguiti su macchine diverse collegate in rete. Il server svolge le operazioni necessarie per la realizzazione del servizio come la gestione della banca dati e l'aggiornamento dei dati; il client tipicamente gestisce la porzione di interfaccia utente dell'applicazione e verifica i dati inseriti per poi inviare al server le richieste. Tale suddivisione unita a tecniche di crittografia, può garantire anonimato e sicurezza al sistema.

Una possibile scelta per l'architettura di sistema è il sistema distribuito collaborativo, consiste in un'architettura ibrida in cui si impiega uno schema client-server per entrare nel sistema e poi si usa uno schema decentralizzato per la collaborazione. In questo modo ci si può assicurare un funzionamento più agevole.

4 CASI DI STUDIO

Vedremo ora due casi di studio di cui si era già parlato, in forma introduttiva, nel capitolo 2: CINECA e Liquidfeedback.

4.1 Sistema CINECA

Nel paragrafo 2.3 abbiamo visto che il sistema ideato da CINECA per l'elezione delle Commissioni di Valutazione dei docenti e dei ricercatori universitari su base nazionale, si compone di tre parti: il sito web pubblico, il sito web riservato e il sistema per il voto. Il sito web pubblico si avvale di Internet, mentre i restanti due componenti sfruttano una rete privata. In conclusione, tutte le fasi del procedimento di reclutamento, dal bando alla presentazione delle candidature e dall'elezione delle commissioni di valutazione sino alla pubblicazione dei risultati, traggono beneficio dall'uso della rete e quindi sfruttano un sistema distribuito.

4.1.1 Sito web riservato

Il sito riservato è utilizzabile solo dagli uffici preposti dei singoli Atenei e fa uso del protocollo HTTPS consentendo l'accesso solo ai browser che utilizzano il certificato crittografico contenuto in apposite smart card distribuite da CINECA. Poiché CINECA ha il controllo totale su chi accede al sito, ha imposto alcuni browser come ufficialmente supportati in modo da poter sfruttare le funzionalità più avanzate nel creare pagine dinamiche. Questo ha permesso anche di garantire le massime prestazioni del server lasciando ai pochi browser opportunamente selezionati il compito della validazione dei dati. La situazione concorsuale risulta visibile ad ogni ateneo in modo affidabile ed aggiornata in tempo reale. L'intero set di procedure disponibili sul sito sono implementate in PERL utilizzando librerie CGI e DBI che servono rispettivamente per l'implementazione dei dati from HTML e per l'accesso alle tabelle di database Oracle [9].

4.1.2 Sito web pubblico

Il sito pubblico è il canale informativo ufficiale del Ministero ed oltre alle procedure di valutazione comparativa, contiene gli strumenti di ricerca sugli archivi. A differenza del precedente, si è cercato di renderlo compatibile con il maggior numero di browsers nelle loro varie versioni e il più possibile veloce. L'unica funzione di invio dati di questo sito consiste nella candidatura, qualora l'Ateneo abbia deciso di demandarla ai candidati stessi per sgravare

i propri uffici. Per il resto i form di ricerca generano pagine statiche che non permettono di inserire o aggiornare i dati. Il sito comprende anche una sezione dedicata a chi deve andare a votare, dove trovare le informazioni su seggi e orari, l'elenco dei concorsi per i quali si ha diritto ad esprimere una preferenza e la possibilità di fare una simulazione (realizzata in Java) dell'applicazione che si dovrà usare nei seggi.

I risultati vengono poi pubblicati sia sul sito pubblico che su quello riservato contemporaneamente, con la sola differenza che le pagine riservate contengono più informazioni.

4.1.3 Architettura del sistema di voto

L'architettura è caratterizzata dalla presenza di due server distinti, gestibili da entità amministrative diverse, e centrali: UEC (Ufficio Elettorale Centrale) ed UC (Urna Centrale). In questo modo è possibile tenere separata l'identità degli elettori dai voti che hanno espresso (voto anonimo, la correlazione non è rintracciabile). Per ogni attore del sistema (responsabili e seggi) viene generata una smart card che permette di certificare la chiave pubblica e l'entità che la possiede.

Compito dell'UEC è di gestire la lista degli aventi diritto al voto (elettorato attivo), degli eleggibili (elettorato passivo) nonché emettere le autorizzazioni al voto e tenere traccia del loro utilizzo (preferenza già espressa o ancora da esprimere). L'UEC gestisce quindi tutto tranne il contenuto dei voti espressi che è compito dell'UC. Questo server riconosce i voti validi grazie alle autorizzazioni al voto comunicate dall'UEC che non contengono nessun riferimento all'elettore. I voti vengono quindi cifrati ed immagazzinati, l'UC non dispone delle chiavi di decodifica che sono in possesso solo della postazione di scrutinio.

I seggi sono le interfacce verso i servizi centrali e non conservano localmente nessuna informazione, dipendono quindi totalmente dai server centrali presso i quali si autenticano grazie alle smart card. Ogni seggio è in oltre presidiato da una commissione elettorale che ha il compito di identificare fisicamente gli elettori.

Il protocollo applicativo utilizzato nelle comunicazioni ha lo scopo di garantire i seguenti requisiti:

Legittimità: deve poter votare solo chi ne ha diritto e una volta soltanto.

Integrità: il voto non deve poter essere modificabile una volta che è stato espresso.

Segretezza: il contenuto della preferenza non deve poter essere visibile prima dello scrutinio.

Anonimato: deve essere impossibile associare un voto all'identità dell'elettore che lo ha espresso.

La legittimità viene garantita dall'Ufficio Elettorale Centrale, che autorizza al voto gli elettori una volta soltanto e la firma apposta su ciascun voto dalla Postazione di Voto garantisce l'integrità del voto stesso. Per quanto riguarda la segretezza, l'autorizzazione al voto consiste in una sequenza casuale ed univoca di bit generata automaticamente e difficile da indovinare, viene utilizzata per decidere se un voto è valido e non viene conservata. Come detto prima i voti vengono immagazzinati solo una volta cifrati e con la chiave pubblica. La cifratura consente quindi anche di impedire di conoscere i risultati parziali prima della fine delle operazioni di voto. Come viene garantito l'anonimato è stato descritto in precedenza e deriva dall'uso di due server separati.

Nel caso finora descritto, le variabili del sistema sono tutte direttamente controllabili da CINECA, questo principalmente per essere in grado di garantire la continuità di funzionamento. Una possibile evoluzione dell'infrastruttura a livello geografico, che ottempera ai requisiti di comunicazione fra i seggi remoti ed il CINECA, potrebbe essere la creazione di una Rete Privata Virtuale (VPN), ovvero un insieme di circuiti virtuali criptati che consentono di modellare una rete privata basandosi su un'infrastruttura pubblica preesistente.

In futuro si potrebbe quindi far convergere l'infrastruttura di rete utilizzata per il sistema di voto telematico sull'infrastruttura di rete accademica (GARR), mediante una VPN opportunamente configurata.

4.2 LiquidFeedback

LiquidFeedback (LQFB) è un software gratuito ed open source basato sul concetto di democrazia liquida. Tale concetto nasce in tempi recenti per rispondere alla domanda: "è legittimo aspettarsi che tutti siano in grado di trattare ogni questione in ogni momento?"

La democrazia liquida si basa quindi sull'unione dei principi di democrazia rappresentativa e diretta. I cittadini possono quindi decidere in che forma esercitare il proprio potere politico, in prima persona oppure delegando un rappresentante di fiducia.

In pratica, ciascuno partecipa alle decisioni a cui è interessato, ma per tutti gli altri argomenti, in cui non si sente sufficientemente preparato o interessato, dà la propria delega a qualcuno che agisca nel suo interesse.

LiquidFeedback è stato sviluppato da alcuni membri dal Partito Pirata tedesco nel settembre 2009 e nell'aprile 2010 è stata rilasciata la prima versione stabile. In Italia è stato utilizzato dall'omonimo partito e da alcune liste civiche quali ad esempio il Movimento 5 Stelle che l'ha utilizzato durante le elezioni regionali siciliane del 2012 per la stesura del programma del candidato Giancarlo Cancelleri, in seguito è stato adottato anche in altre regioni.

LiquidFeedback comprende un sistema deliberativo basato su iniziative o proposte che ricalca quello delle normali democrazie parlamentari cioè si segue un iter per giungere alla fase finale della votazione. I fattori applicabili agli iter sono molto sofisticati e riguardano ad esempio tempistiche e quorum. Essendo stato sviluppato per promuovere iniziative condivise è prevista la possibilità di raccogliere il “sostegno” dei componenti della comunità. Ogni proposta scartata per un qualsiasi motivo rimane comunque disponibile ed accessibile tramite un archivio storico.

Le iniziative sono organizzate all'interno di una grossa “bacheca” suddivisa in varie aree per permettere di ordinare le iniziative a seconda del loro argomento e facilitare così la ricerca. Le “aree” propriamente dette sono, ad esempio: economia, scuola, sviluppo, ecc... . Le aree a loro volta sono suddivise in “sezioni”, dove le iniziative sono raccolte per argomento, o per aree più specifiche. Vi possono essere poi aree comuni per tutti i membri, ed invece aree riservate a gruppi di lavoro. Ci si trova quindi davanti ad una strutturazione ad albero e pertanto simile ad una gerarchia di directory e sotto directory. Un altro aspetto peculiare è la grande attenzione alla trasparenza interna, tutti i membri della comunità possono conoscere le attività degli altri membri. Ciò è possibile dato che tutte le votazioni avvengono con voto palese, (al termine di una votazione, oltre l'esito, è possibile visualizzare chi sono gli elettori e come ognuno ha votato), le deleghe sono pubbliche (in questo modo è possibile prevenire o tenere sotto osservazione concentrazioni di potere). Dal profilo di ogni iscritto è possibile visualizzare tutte le iniziative da lui create o a cui abbia partecipato. Per iscriversi è necessario far parte del partito ed essere invitato da un membro già attivo che garantisca l'identità dell'aspirante mediante il suo documento di identità. É quindi poi possibile usare un nickname se non si vuole usare il proprio nome².

4.2.1 Architettura

L'implementazione di LiquidFeedback è suddivisibile in 2 parti: *LiquidFeedback-Core* (Backend) e *LiquidFeedback Frontend*.

²Come illustrato nell'articolo [4].

Il core consiste in uno schema per il database che include anche gli algoritmi per le deleghe, il feedback e le procedure per le votazioni implementate come views SQL. Il frontend, che cura l'interfaccia con gli utenti, è scritto in Lua, mentre le procedure per il backend sono scritte in PL/pgSQL. Entrambe le parti sono rilasciate sotto licenza MIT.

Allo scopo di creare una piattaforma modulare e aperta a nuove implementazioni, è disponibile una API che consente la creazione di applicazioni esterne per aggiungere ulteriori funzionalità al programma, oppure per collegare apparecchi HW (es. smartphone).

5 CONCLUSIONI

Al giorno d'oggi, la tecnologia è pronta per supportare il voto elettronico. I dispositivi sono nelle tasche e nelle case di tutti ed esistono svariate tecniche per garantire la sicurezza del sistema e che comunque sono sempre in evoluzione. I tempi sono quindi maturi per una svolta politica verso l'adozione di voting systems molto più "democratici", ovvero sulla falsa riga di quello introdotto nel paragrafo 1.4.

Tale tecnica richiede di minimizzare una data somma di distanze, per fare ciò, ci viene incontro un'altra branca della matematica: l'analisi numerica. Questa scienza offre, tra le altre cose, metodi stabili, robusti ed efficienti per algoritmi di ricerca dei minimi vincolati e non (es. minimi quadrati, discesa lungo il gradiente, metodo di Newton, metodo di Uzawa, ecc...).

Per quanto riguarda la struttura del sistema è emerso che l'architettura più soddisfacente è quella decentralizzata che sfrutta due server separati che comunicano tra loro. Uno gestisce le operazioni di autenticazione e l'altro l'archiviazione dei voti opportunamente crittografati con chiave pubblica.

Nel sistema CINECA esiste ancora una componente umana che identifica visivamente i votanti. Questo da un lato potrebbe dare sicurezza a chi ancora non riesce a fidarsi della tecnologia ma è un aspetto destinato a sparire gradualmente finio ad arrivare alla possibilità di esprimere il proprio voto ovunque, senza il bisogno di seggi preposti.

Riferimenti bibliografici

- [1] www.swissinfo.ch
- [2] Piergiorgio Odifreddi, *La democrazia impossibile*, Giugno 1993
- [3] Arrow, K.J., *A Difficulty in the Concept of Social Welfare*, Journal of Political Economy, 58, 328–346, 1950
- [4] www.wired.it
- [5] www.consilium.europa.eu
- [6] www.mtholyoke.edu
- [7] www.electoral-reform.org.uk
- [8] www.cineca.it
- [9] *notizie dal CINECA* n° 38/39, Editoriale Mario Lanzaolini
- [10] Contucci P., Panizzi E., Ricci-Tersenghi, Sirbu A., *A new dimension for democracy: egalitarianism in the rank aggregation problem*, July1, 2014
- [11] Andrea Omicini e Pierluigi Contucci, *Complexity and Interaction: Blurring Borders between Physical, Computational, and Social Systems*.