THE VOTING CHALLENGES IN E-COGNOCRACY*

Joan Josep PILES
José Luis SALAZAR
José RUIZ

Grupo Tecnología de las Comunicaciones

José María MORENO-JIMÉNEZ

Grupo Decisión Multicriterio Zaragoza

Universidad de Zaragoza. Spain.

* Partially funded under the research project "***Electronic Government. Internet-based Complex Decision Making: e-democracy and e-cognocracy***" *(Ref. PM2004-052)* and "***Internet-based Complex Decision Making. Decisional Tools for e-cognocracy***" *(Ref. TSI2005-02511).*

THE VOTING CHALLENGES IN E-COGNOCRACY

1. Introduction

2. From e-Democracy to e-Cognocracy

3. e-Voting process for e-Cognocracy

4. Implementation

5. Conclusions

1. Introduction

1. Abstract

2. Background

2. From e-Democracy to e-Cognocracy

3. e-Voting process for e-Cognocracy

4. Implementation

5. Conclusions

ABSTRACT (I)

- **E-cognocracy** is a new democratic system that focuses on the creation and social diffusion of the knowledge.
- Using:
  - Multicriteria decision making techniques as the methodological aid
  - The democratic system as a catalyst for the learning that guides the cognitive process distinctive of living beings.
  - Internet as the communication tool.

e-Cognocracy resolves some of the limitations of traditional democracy.

ABSTRACT (II)

- E-voting is not limited to the choice of a given political party, but to the extraction of the relevant knowledge.
- There are still some situations not covered yet by classical bibliography.
- It becomes necessary to introduce new variations to the main schema.
- In this paper, we will present one of such occurrences.

BACKGROUND (I)

- The degree of implication has been an important issue.
- It has been traditionally agreed that it is desirable to achieve as much involvement as possible.
- This has been usually limited by the access of the citizenry to the relevant information.

BACKGROUND (II)

- With the advent of computers, the information flow between people has been steadily increasing.
- Internet is responsible for a great deal of this new communication.
- The technology has evolved, creating electronic voting, or e-voting.
- There have been no shifts in the paradigm of the decision making process.
- One of the obstacles new methods have is the lack of technologic means to allow their implementation.

PHILOSOPHICAL AND METHODOLOGICAL ASPECTS (I)

- **Philosophical and methodological changes**
  - "From *mechanicistic reductionism* to *evolutionistic holism*"
  - "From the *search for truth* to the *search for knowledge*"
  - "From *data analysis* to *knowledge management*"
- **Cognitive approach for social representation based on**
  - Explicit consideration of the human factor (subjective, intangible and emotional aspects)
  - Plurality of ideas and Diversity of opinions
  - Network selection: From **"One person one vote to one person many ideas"**

PHILOSOPHICAL AND METHODOLOGICAL ASPECTS (II)

- **Governance systems**:
  - The fallacy of traditional democracy
  - *Traditional democracy* no longer meets its initial end, which is, of course, the participation of citizens in their own government.
- **E-cognocracy:**
  - Provides room for greater involvement of the citizenry in their own government
  - Resolves some of the limitations of traditional democracy
  - Focuses on the process by which knowledge, related with the scientific solution of problems, is created and socialised.
- **Thus,** the **"cognitive" connection between citizens allows us to establish a network between ideas, cultures and civilizations, helping progress towards the achievement of a *new world*.**

PHILOSOPHICAL AND METHODOLOGICAL ASPECTS (III)

Limitations of traditional democracy:

- The participation of citizens is largely confined to the election of their representatives.
- Only a few of their members actually dominate the configuration of electoral lists.
- Traditional democracy does not take proper account of those people who do not vote, or who deliver a blank ballot
- There is no further control over the activities of politicians other than the votes that will be cast at the next election.
- There is a *social opportunity cost* associated with the failure to make more ambitious use of the democratic system of political participation.

A NEW DEMOCRATIC SYSTEM (I)

- Communications technologies allow new forms of interaction between citizens and the political parties that represent them.
- ***Electronic governance*** *(e-governance)* may be defined as the set of activities organised by public institutions, and sometimes by private organisations or groups, to offer services supported by the information and communications technologies to the citizen.
- **E-governance,** according our proposal, should also pursue the transcendent goals of the human race and, in general, of the "larger world" of which it forms part. These objectives should be linked to the essence of the **evolution of living species**, which is to say **creation and the diffusion of knowledge in society**.

A NEW DEMOCRATIC SYSTEM (II)

➢ **Structure** of the proposed system:

1. Citizens will be able to choose (or systems decide the weights) between participating in the democratic system as they have traditionally done (delegation), or taking part directly in the resolution of problems by contributing their opinions and ideas.
2. Parliamentary would be distributed in two parts (public and private). The share of seats allocated to each part depends on the problem.
3. In order to avoid saturating citizens with participation in these processes, only some particularly relevant problems would be treated in this manner.
4. The direct involvement of citizens in political decision making would be oriented towards the enhancement and diffusion of social knowledge.
5. This knowledge refers to behaviour patterns, preference structures, stylised facts and trends of the decision making process.
6. A multi-criteria framework is used to solve the complex situations associated with public decision making.

A NEW DEMOCRATIC SYSTEM (III)

- **Key characteristics** of the new democratic process:
  - **Direct involvement** of the citizen in decision making processes
  - It **improves control** of the political system and reduces dependence on minority political groups. This would produce wider coalitions between groups, favouring more moderate proposals enjoying democratic support.
  - It would **improve** overall **knowledge** and **understanding** of the system, incorporating a wider range of perceptions of reality, deepening debate and strengthening negotiating processes and the search for consensus.
  - It would **facilitate continuous education** and learning of population
  - It would allow easy expansion and diffusion of knowledge as well as the creation of minimum ethical standards.
  - The **multi-criteria framework** proposed to deal with the specifics of problems integrates the subjective through values and judgements.

Objective treatment of the subjective guarantees the scientific character of the procedure followed (rigour, transparency and accessibility).

TECHNOLOGICAL ASPECTS

➢ Classical security properties needed

- Authenticity
  - *The guarantee that the identity of a sender cannot be supplanted any other user.*
- Integrity
  - *The guarantee that a message will not be changed on its route from the sender to the addressee.*
- Confidentiality
  - *The guarantee that only the addressee (receiver) of a message will be able to read it.*

CHARACTERISTICS (I)

Traditional e-voting systems

- Are limited to the technological aspects associated with the choice of a given party.
- There is very little feedback (if any) from the citizens who will partake in the voting.
- The only really important moment is the voting itself.
- The citizens do not have more information than that provided by the political parties at the beginning of the process.

e-Cognocracy

- Is focused on the extraction of the relevant knowledge
- Analyzes of the individual and social learning derived from the scientific resolution of the problem.

The key element introduced is the linkability of votes.

CHARACTERISTICS (II)

- In order to get the knowledge seeking process, we divide each voting in several rounds.
- Each voter can cast his vote in as many rounds as the voting process determines (but only once each round).
- After each round partial results are published, and more information is provided to the citizens.
- Characteristics of our e-voting system
  - **Precision**
  - **Democracy**
  - **Privacy**
  - **Linkability**

CHARACTERISTICS (III)

- **Precision**
  - It shall not be able for a non authorized person to modify any votes
  - It shall not be possible to:
    - Remove a valid vote from the final counting
    - Include a non-valid vote in the final counting
- Democracy
  - Only voters in the census shall be able to vote
  - Each voter shall be able to vote only once in each round
- **Privacy**
  - A voter shall not be linked to its vote
  - A voter shall not be able to prove its vote
- **Verifiability**
  - Voters shall be able to verify their vote has been correctly accounted
- **Linkability**
  - Two votes from the same voter in different rounds of the voting shall be linked together, but not to the voter who cast them

ACTORS (I)

The Electoral Authority (EA)

- Keeps track of the census
- Validates the users in the voting process
- Signs the votes as a proof of voting
- Keeps enough data about the votes to be able to link them for the Recount server without actually being able to decrypt them

The Certification Authority (CA)

- Shall issue the certificates for each actor involved in the process
- Serves as Trusted Third Party with regard to the validation of certificates

ACTORS (II)

The Recount Authority (RA)

- Is the only entity allowed to decrypt the votes
- The Electoral Authority shall provide information enough to link the votes from the same voter, but not to track them to the actual person who cast them.

Voter (V)

- Must show its preferences in a multiple choice and rank them
- The census is kept constant throughout all the rounds of the same voting

E-VOTING PROCESS (I)

1. Initialization:

- **EA** initialises the e-voting process
- **CA** shall initialise only once before the start of any voting process.
- **RA's private key initialization.**
- **EA's private key initialization.**
- **Voters' registry.**

E-VOTING PROCESS (II)

2. Voting:

- Voter identifies himself to EA and sends it a hash of his vote for EA to issue a blind signature of it, and a ticket made from a mix of his identity and a random value that will be signed by EA as well.
- EA verifies the voter's identity, checking it against the census and validating the client's certificate, and checks that the voter has not already cast its vote in this round.
- EA issues a blind signature of the vote, and a signature of the ticket, and stores them linked to the voter for future rounds.
- Voter encrypts the vote with R's public key.
- **Voter sends to EA** the vote and the blinding factor for the blind signature ciphered for RA
- **EA sends to R** the ciphered vote and secret with the blind signature of it and the signature of the ticket via a secure channel.

E-VOTING PROCESS (III)

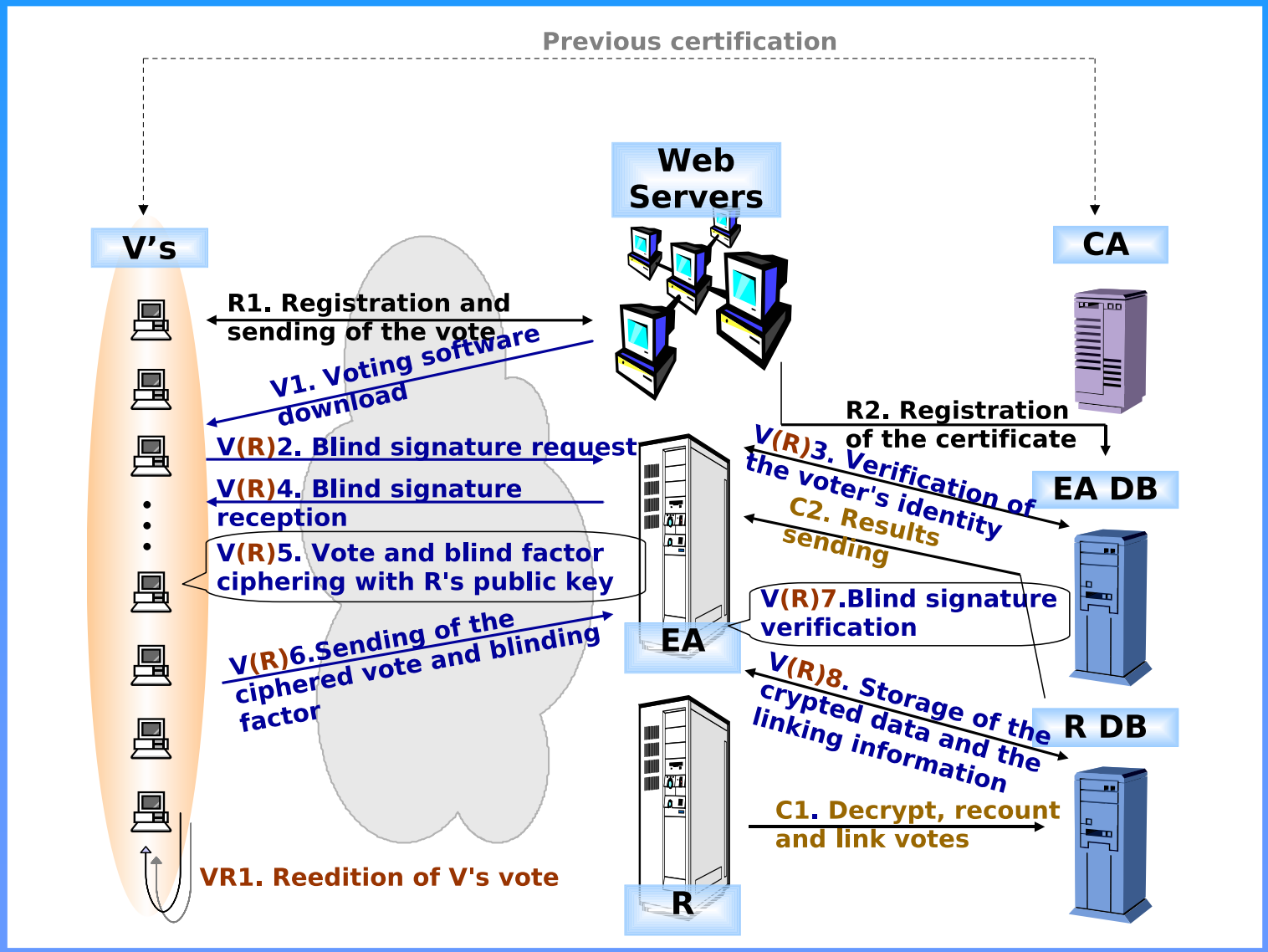
2. Voting (cont'd):

- If the voter had previously voted (in other rounds), **EA sends to RA** a copy of the blind signature of the latest vote, which will be then used by RA to link them
- **EA sends to V** the signature of the ticket to prove that his vote has been stored

3. Recount:

- R makes public the signatures of the tickets, and starts a claims period before the publication of the results
- R decrypts the original votes, and uses the secret included with it to get a valid signature from the blind signature
- R checks the vote with the signature obtained and verifies that it is correct
- R links all the votes from the same voter
- R publishes the results of the round / voting

E-VOTING PROCESS (IV)



PROOF OF FITNESS (I)

- Precision
  - As each voter authenticates himself to EA, this implies he must have a knowledge of the private key that is impossible to fake provided we use an adequate key length.
  - As each voter gets a signature of the ticket he sent to EA, and a list of those tickets is published prior to the recount, even if R is compromised, the votes cannot be erased from the ballot, as such an action would be challenged by the voters with their tickets, which would be shown to exist in EA.
- Each vote is stored with a signature from EA. A vote cannot be inserted even if R is compromised because it would be necessary to get a valid signature, and that is not possible without the private key of EA.
- Democracy
  - As the votes are not sent directly to R by the users, it is EA's job to get sure that the voter is properly included in the census.
  - Analogously, EA will store which voters have already voted en each round, to avoid duplicates.

PROOF OF FITNESS (II)

- Privacy
  - All the information provided to R is a ciphered vote, its blind signature, and a signed ticket. None of these includes anything that could lead to track the individual who cast the vote. The only item a voter receives is its signed ticket. That ticket is generated randomly, and has no relation whatsoever with the actual content of the vote.
- Verificability
  - Each time a vote is received, EA sends back to the voter a signed ticket. Later, when the recount starts, the list of the tickets from the votes cast is published. If a voter had a ticket not included in the list, he could use it to challenge EA and see whether it has a copy of it. It EA has a copy, then the vote should be cast again.
- Linkability
  - Together with each vote, EA sends to R the blinded signature of the last vote cast by the same person. At the time of the recount, R looks for each vote the one which blind signature matches the included with the vote, and it reconstructs this way all the links which allow to trace the voting history of a voter, without actually revealing his identity.

IMPLEMENTATION DETAILS (I)

- **JAVA technologies**, both in the client side and in the server side:
  - Better communication between the different components.
  - More code reusability, as we can develop a series of cryptographic libraries which will be used both by the client and by the server software.
- Standard web browser: **Mozilla Firefox**.
  - It has the advantage of being open source, so its source code is readily available, contributing to increase the feeling of transparency in the process.
- Extra libraries needed: **JSS**
  - Needed to be able to access the client certificates which are stored in it from within the JAVA applet that will be the client software.
  - If those libraries were not available, the user should manually add the client certificate and the CA to the JAVA application.

IMPLEMENTATION DETAILS (II)

- The application server to use will depend on the available infrastructure at the moment of the deployment
  - In our tests, we used Tomcat as application server. It is open source and its capacity for this kind of systems is well proven
- It was chosen to use **MySQL** as a backend to store the data related to the voting
  - The actual votes
  - Metainformation about the voting
- Different roles (EA, RA) can be consolidated in the same server
  - Web server
  - Application server
  - Database server
- All the communications between the client and the server will be both authenticated and encrypted
  - To achieve these goals, it will be necessary to set up an infrastructure allowing SSL and client side certificates

IMPLEMENTATION DETAILS (III)

- Choice of software
  - **Apache** as the web server
  - **Tomcat 5** as the application server
  - **MySQL** as the database server
  - **Linux i386** machine
- Link between Apache and Tomcat
  - JK Connector
  - Allows to redirect queries from the Apache server to the Tomcat one in a transparent way
  - It can be made to transfer the SSL layer information
- Certificate Authority using OpenSSL.

CONCLUSIONS

- We have studied the novel challenges that e-cognocracy imposes upon traditional voting. We have built an e-voting system which provides the means to gather the information needed towards a more participative democracy.
- As we have seen, the key to get the linkability of the votes is the separation between the Electoral Authority, who can link the chain of votes to the user but can't know the contents of each vote, and the Recount server, who can link the votes between themselves and decrypt them, but is isolated from the information about each voter.
- This isn't a concern as long as both of them are trusted entities who will not work together to cheat the system.