Universidad de Zaragoza

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY*

José María MORENO-JIMÉNEZ
Juan AGUARÓN
María Teresa ESCOBAR
Alberto TURÓN
Grupo Decisión Multicriterio Zaragoza
Universidad de Zaragoza. Spain.

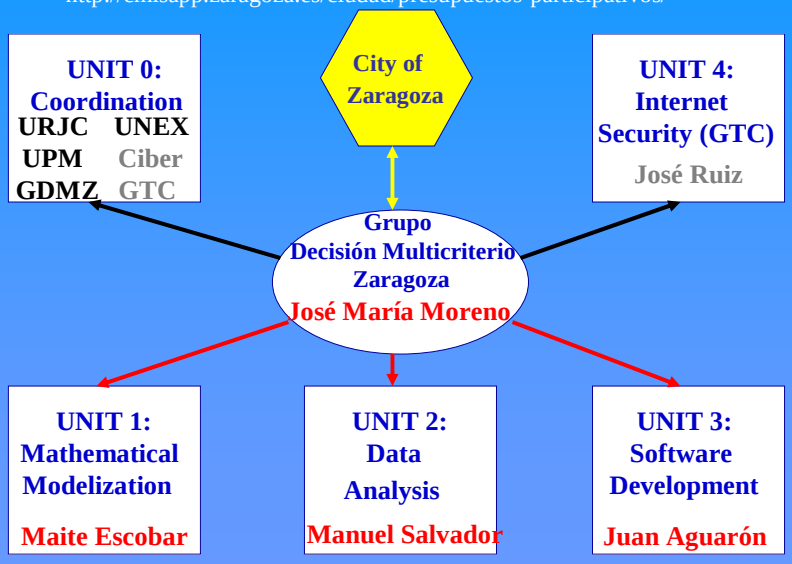
* Partially funded under the research projects *"Electronic Government. Internet-based Complex Decision Making: e-democracy and e-cognocracy" (Ref. PM2004-052)* and *"Internet-based Complex Decision Making. Decisional Tools for e-cognocracy" (Ref. TSI2005-02511).*

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

http://cmisapp.zaragoza.es/ciudad/presupuestos-participativos/



GDMZ

Universidad de Zaragoza

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

1. Introduction
2. Philosophical foundations of e-cognocracy
3. Methodological foundations of e-cognocracy
4. Technological foundations of e-cognocracy
5. Conclusions and future lines

Universidad de Zaragoza

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

1. Introduction
   1. Knowledge Society
   2. E-democracy and e-cognocracy
2. Philosophical foundations of e-cognocracy
3. Methodological foundations of e-cognocracy
4. Technological foundations of e-cognocracy
5. Conclusions and future lines

KNOWLEDGE SOCIETY

- Philosophical changes:

"mechanicistic reductionism to *evolutionistic holism*

- Methodological changes:

*"**search for truth*** to the ***search for knowledge**"*

- Technological changes.

*"**data analysis*** to ***knowledge management**"*

- **Knowledge Society** (Moreno, 2003)
  - New social and political order
  - Connectivity, Dependency, Communication
  - **Human factor** (from data to knowledge)

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

KNOWLEDGE SOCIETY

- In contrast to the **prediction**, **control**, **rigidity** and **hierarchy** of the **Information Society**, the **Knowledge Society** offers the **understanding**, **communication**, **consensus**, **flexibility** and **network** (Moreno, 2003).
- It not only seeks for **provide processed information**, but also to:
  - **promote learning**
  - **develop intelligence**
  - **increase communication** (interconnection and interaction between the human beings)
  - **improve coexistence**
  - **favour evolution** (novelty creation vs. gradual adaptation to the environment)

KNOWLEDGE SOCIETY

- Knowledge Society is understood as a space for the **ingenious** and the **human talent** **(social intelligence and talent)**.
- It tries:
  - **To educate** the individual (intelligence and learning)
  - **To favour** the relation with the others (communication and coexistence)
  - **To improve** the society (quality of live and cohesion)
  - **To construct** the future in an increasing complex world (evolution).

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

KNOWLEDGE SOCIETY

- Change of values:

Classical Values	New Values
Expansion	Conservation
Competition	Cooperation
Quantity	Quality
Domination	Association
Adaptation	Innovation

- New information and communication technology (ICT), understood as a socio-technical system that implies new forms of social-organization.

Universidad de Zaragoza

GDMZ

E-DEMOCRACY AND E-COGNOCRACY

- **Democracy:**
  - Origin:
    - ***demos*** **(common people) and**
    - ***kratos*** **(govern)**
  - Definition:
    - "Democracy is understood as that political regime in which the people exercise sovereignty through their intervention government to improve their own conditions of life. In this political system, universal suffrage gives the people the right periodically to elect and control politicians"
  - Limitations:
    - such intervention in government is almost entirely confined to the delegating representation to a political party

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

E-DEMOCRACY AND E-COGNOCRACY

- **Evolution of democracy**
  - Athenians Democracy (VIII-V b.C.)
  - Roman Republic (V-I b.C.)
  - Mean Age (V-XIII)
  - Republic Democracy (XIII-XV)
  - Constitutional Monarchy (XV-XVIII)
  - Liberal Democracy (XVIII-XIX)
  - Marxist Democracy (XIX)
  - Contemporary Democracy (XX)
  - Competitive Elitism Democracy (XX)
  - Plural Democracy (XX)
  - **REPRESENTATIVE Democracy** (XX)
  - **PARTICIPATIVE Democracy** (XX)
  - **COGNITIVE Democracy** (XXI)

E-DEMOCRACY AND E-COGNOCRACY

- The **REPRESENTATIVE or legal democracy** -the "**New Right**" of **Francis Fukuyama**-, where elected "functionaries" assume the representation of the citizens' interests in a legal framework.
- Limitations (Moreno-Jiménez, 2003, 2004; Moreno-Jiménez and Polasek, 2003):
  - **Specific** participation confined to the election
  - **Control of electoral lists** by the political parties
  - Hiding of **critical positions** and **interests**
  - **Clumsy system** with **slow participation** and **control**
  - **Fallacy of Democracy**!

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

E-DEMOCRACY AND E-COGNOCRACY

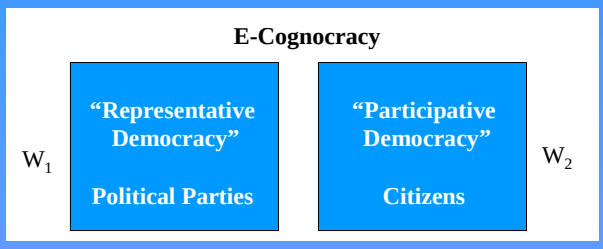
- The **PARTICIPATIVE or direct democracy** - The "**New Left**" (**Alex Callinicos**)-, where the citizens are directly implicated in the decision making process.
- **Limitations** of participative democracy:
  - **Populism**
  - **Lack of a global perspective**
- **Limitations** of both:
  - **Social opportunity cost** (more ambitious goals)
  - **Technological opportunity cost** (not use of ICT)

Universidad de Zaragoza

GDMZ

E-DEMOCRACY AND E-COGNOCRACY

- **E-cognocracy** is a new democratic system that combines the representative or liberal democracy with the participative or direct democracy to address the limitations of both.



- E-cognocracy seeks to convince citizens nor to defeat them (e-democracy).

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

E-DEMOCRACY AND E-COGNOCRACY

- **E-cognocracy** uses:
  - **Internet** as the communication tool.
  - **Multicriteria decision making techniques** as methodological aid
  - The **democratic system** as a catalyst for the learning that guides the cognitive process distinctive of living beings
- **Key characteristics of the E-cognocracy:**
  - **Direct involvement of citizens in decision making processes.**
  - **Improve control of political system.**
  - **Improve overall knowledge and understanding.**
  - **Continuous education.**
  - **Expansion and diffusion of knowledge.**
  - **Quality of live.**

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

E-DEMOCRACY vs. E-COGNOCRACY

- **E-democracy** refers to the **PARTICIPATION,** via the internet, of citizens in public decision making. This participation, in practice, consists of citizens simply offering their comments, opinions and suggestions to the elected representatives (debate and discussion for assistance)
- **E-cognocracy** refers to the **IMPLICATION,** via the internet, of citizens in public decision making. This implication consists of their direct intervention in the decision making process (decision).
- "**One person, one vote**" vs. "**One person, many ideas**" to convince citizens of the appropriateness of a given decision.

Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

E-DEMOCRACY vs. E-COGNOCRACY

E-democracy	E-cognocracy
Participation	Implication
Discussion	Decision
One person, one vote	One person, many ideas
Political Filter (parties)	Individual Filter (network)
Defeat	Convince

Universidad de Zaragoza

GDMZ

1. Introduction

2. Philosophical foundations of e-cognocracy

3. Methodological foundations of e-cognocracy

4. Technological foundations of e-cognocracy

5. Conclusions and future lines

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

PHILOSOPHICAL FOUNDATIONS

EVOLUTION OF LIVING SYSTEMS
(Capra, 1996)

- Patron (Maturana and Varela)
  - **Authopoiesis**
- Structure (Prigiogine)
  - **Dissipative Structures**
- Process
  - **Cognitive process**

MASLOW`S NEEDS HIERARCHY

Only species that **learn** (extract and spread knowledge) and which **adapt** to the context are able to **survive (vital or cognitive process)**.
The **representative process** belongs to the second level of needs (control and order and the third level (**social relations**)
The **cognitive process** deals with the **physiologic needs** (survival)
Knowledge is the distinct element of the new social and political framework

Universidad de Zaragoza

GDMZ

PHILOSOPHICAL FOUNDATIONS

- **e-Cognocracy** is a new democratic system that focuses on the creation and social diffusion of the knowledge related with the scientific resolution of high complexity problems associated with public decision making related with the governance of society.
- This is a **cognitive process** that facilitates**,** in analogous way of evolutionism of living systems, the **survival and evolution of the human race** (genetic diversity and nature selection)**,** based on:
  - the "**plurality of opinions**" (**knowledge diversity**)
  - the "**network discussion**" of ideas (**people selection**)

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

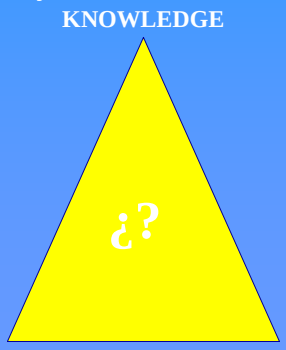
Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

PHILOSOPHICAL FOUNDATIONS

- The key idea: is to **educate** people (intelligence and learning), **promote** relationship with others (communication and coexistence), **improve** society (quality of life and cohesion) and **construct** the future (evolution) in a world of increasing complexity.



PHILOSOPHICAL FOUNDATIONS

➢ Philosophical Characteristics of e-cognocracy:

- Human beings are considered in a holistic and systemic context.
- The search for knowledge is the basic criterion guiding the behaviour of individuals and systems.
- Emphasis is placed on the strengthening in implication and control.
- All ideas, even minorities positions, are included.
- Decisions are taken according the majority rule.
- Individual and social education is encourage through discussion and debate (reducing human ignorance).
- Effort, learning and continuous improvement are favoured.
- Recognition should be given to the skills and abilities of individuals, thereby identifying social leaders.

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Knowledge Society
E-democracy and e-cognocracy
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

PHILOSOPHICAL FOUNDATIONS

➢ **e-democracy** (representative democracy) is the governance of citizens using ICT.

➢ **e-cognocracy** (cognitive democracy) is the governance of knowledge and wisdom using ICT.

➢ To improve society

*"There can be no democracy without **freedom**, and no freedom without **knowledge**"*

E-DEMOCRACY vs. E-COGNOCRACY

E-democracy	E-cognocracy
Participation	Implication
Discussion	Decision
One person, one vote	One person, many ideas
Political Filter (parties)	Individual Filter (network)
Defeat	Convince
Security&Social needs	Physiologic need
Governance of people	Governance of knowledge
Delegation	Freedom

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

Universidad de Zaragoza

GDMZ

METHODOLOGICAL FOUNDATIONS

(Moreno-Jiménez, 2003, 2004, 2006; Moreno and Polasek, 2003)

- From a scientific point of view:
  - The use of the new scientific method.
  - The consideration of human factor (subjective, intangible and emotional aspects).
  - Employment of MCDM techniques as decisional tools.
  - Modelling of problems, incorporation of preferences that reflects all the visions of reality and synthesis of preferences.
  - Exploitation of mathematical model to extract patterns and trends by analysing the behaviour of the system.

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

GDMZ

METHODOLOGICAL FOUNDATIONS

- From a procedural point of view:
  - Citizens may participate in the system as they have traditionally done (delegation), or by taking part directly in the resolution of problems.
  - Parliament would be distributed in two parts (**public** and **private**). The share of seats allocated to each part is around (2/3 and 1/3).
  - In order to avoid saturating citizens with participation in these processes, only some particularly relevant problems would be treated in this manner.
  - In order to solve the problem, including the aggregation of the solutions provided by political parties on the one hand and citizens on the other, we use MCDM techniques.
  - Using this model, we are able to extract knowledge as this refers to behaviour patterns, preference structures, stylised facts and trends of the decision making process.
  - Internet is used to incorporate the preference structures of citizens into the decision making process.

Universidad de Zaragoza

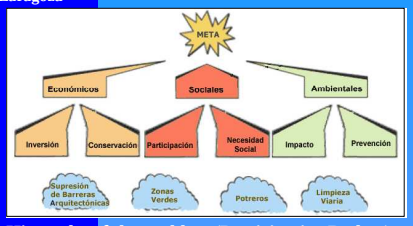
METHODOLOGICAL FOUNDATIONS

- Practical situation:
  1. Who poses the problem?
     - Save for exceptional cases, the political parties
  2. Who supervises the execution of the e-cognocracy procedure?
     - Electronic Electoral Comity
  3. Who manage the procedure?
     - Facilitator
  4. How preferences are incorporated?
     - Internet and MCDM tools
  5. Who decide which is the relevant knowledge and determine the number of rounds?
     - Political parties
  6. What kind of knowledge is extracted and diffused and in what way?
     - Patterns of behaviour that captures opinion groups and the arguments that justify these conclusions.

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza



Hierarchy of the problem (Participative Budget)

Asociations	Weights	Certificates	Votes
Vocales	40	11	5
Picarral	12	20	20
Jota	12	20	5
Arrabal	12	20	2
Zalfonada	6	1	1
Jesús	12	1	1
Ríos_de_Aragón	3	1	1
Teniente_Polanco	3	1	1
Total	100	75	36

Public and Private part (Participative Budget)

Total priorities for the problem (Participative Budget)

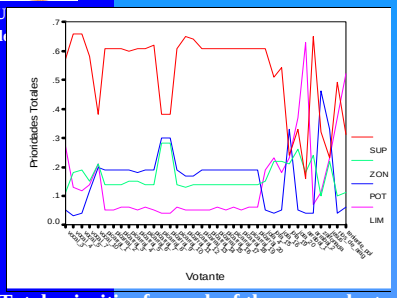
	META				
Asociaciones	SUP	ZON	POT	LIM	peso
Vocales	0.5850	0.1699	0.0727	0.1724	40
Picarral	0.5923	0.1546	0.1995	0.0535	12
Jota	0.4506	0.2240	0.0746	0.2507	12
Arrabal	0.4082	0.2626	0.0506	0.2786	12
Zalfonada	0.3189	0.1024	0.4644	0.1143	6
Jesús	0.2266	0.2169	0.3306	0.2259	12
Ríos_de_Aragón	0.4923	0.1027	0.0371	0.3679	3
Teniente_Polanco	0.3104	0.1102	0.0607	0.5187	3

Total priorities for the public and private parts

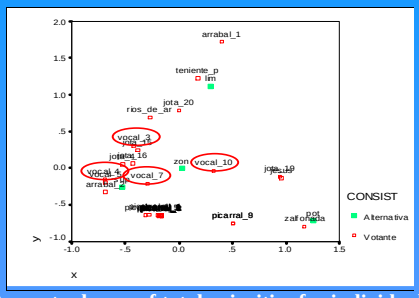
 # 1. e-budget participation

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY



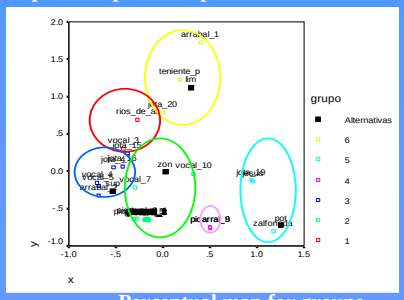
Total priorities for each of the respondents



Perceptual map of total priorities for individuals

GRUPO	PESOS (%)	SUP	ZON	POT	LIM
1	11	0.5495	0.1077	0.0473	0.2956
2	26.8	0.5451	0.1633	0.1742	0.1124
3	29.2	0.6362	0.1994	0.0388	0.1257
4	1.2	0.38	0.28	0.3	0.04
5	20.4	0.2607	0.1776	0.3723	0.1895
6	11.4	0.2275	0.1753	0.0479	0.5494
Total	100	0.501	0.1948	0.1117	0.1925

Groups in a Cluster Analysis



Perceptual map for groups

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

METHODOLOGICAL REFERENCES

1. ALTUZARRA et al. (2005): Searching for consensus in AHP-group decision making. A Bayesian approach. *CODAWORK'05.*
2. MORENO-JIMÉNEZ, J.M. et al. (2005a): Decisional tools for knowledge improvement in e-cognocracy. In Böhlen et al. (editors): *TED Conference on e-government 2005. Electronic democracy: The challenge ahead*. University Rudolf Trauner-Verlag, *Schriftenreihe Informatik* 13, 70-78.
3. MORENO-JIMÉNEZ, J.M. et al. (2005b): A Spreadsheet Module for Consistent AHP-Consensus Building. *Group Decision and Negotiation*, 14(2), 89-108.
4. MORENO-JIMÉNEZ, J.M. et al (2005c): Group Preference Structures in AHP group decision making. *CODAWORK'05.*

METHODOLOGICAL REFERENCES

5. ESCOBAR and MORENO-JIMÉNEZ, J.M. (2006): Aggregation of Individual Preference Structures. Forthcoming in *Group Decision & Negotiation*.
6. ALTUZARRA, A. et al. (2006): A Bayesian priorization procedure for AHP-group decision making. Forthcoming *European Journal Operational Research.* doi:10.1016/j.ejor.2006.07.025.
7. GARGALLO, P. et al (200?): AHP- Group Decision Making: A Bayesian Approach based on Mixtures. Forthcoming in *Group Decision & Negotiation*.
8. MORENO-JIMÉNEZ, J.M. et al. (200?): The Core of Consistency in AHP-Group Decision Making. Forthcoming in *Group Decision & Negotiation*.

Universidad de Zaragoza

GDMZ

TECHNOLOGICAL FOUNDATIONS

- **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 e-voting system**
  - Ii is focused on the **extraction of the relevant knowledge** and allows for the consideration of different rounds.
  - It analyzes **individual and social learning** derived from the scientific resolution of the problem.

The key element introduced is the linkability of votes

TECHNOLOGICAL FOUNDATIONS

- **Characteristics of the e-Cognocracy e-voting system**
  - Precision
  - Democracy
  - Privacy
  - Verificability
  - Linkability.
- **Actors of the e-Cognocracy e-voting system**
  - The Electoral Authority
  - The Certification Authority
  - The Recount Authority
  - The Voter
- **e-Cognocracy e-voting process**
  - Initialisation
  - Voting
  - Recount
  - Diffusion
- **References:**
  - **Moreno et al.** (**2006**) and **Piles et al.** (**2006**)

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

Universidad de Zaragoza

Introduction
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

CHARACTERISTICS

- **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

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

ACTORS

- **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
- **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
- **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.

Universidad de Zaragoza

Introduction
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

GDMZ

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

E-VOTING PROCESS

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.**
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 RA's public key.

E-VOTING PROCESS

2. Voting:

- **Voter sends to EA** the vote and the blinding factor for the blind signature ciphered for RA
- **EA sends to RA** the ciphered vote and secret with the blind signature of it and the signature of the ticket via a secure channel.
- 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:

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

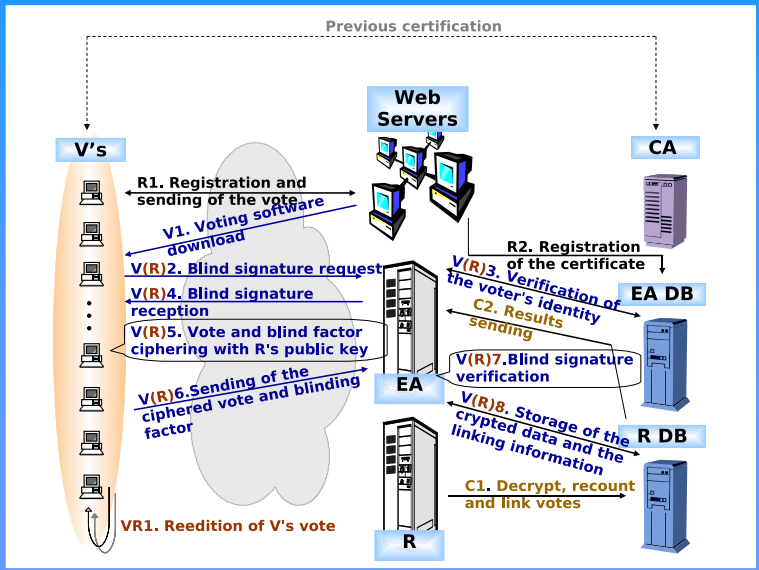
4. Publication: RA publishes the results of the round / voting

Universidad de Zaragoza

Introduction
Philosophical foundations of e-Cognocracy
Methodological foundations of e-Cognocracy
Technological foundations of e-Cognocracy
Future lines and conclusions

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

E-VOTING PROCESS



IMPLEMENTATION DETAILS

- We use JAVA technologies, both in the client side and in the server side. This has several advantages:
  - 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.
- In order to minimize the number of configurations in which the client side had to run, we decided to choose a 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.
- The browser has been completed with some libraries (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.

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

IMPLEMENTATION DETAILS

- 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 votings (both the actual votes and the information about the votings).
- As there are two different servers (Electoral Authority server and Recount server), there could be two web and application servers, working with two different database servers. None the less, when doing the actual deployment it might happen that it is advisable to put both applications in the same application and/or web server.
- Likewise, it could be desirable to use two databases in a single database server. This would not be a problem, but it should be taken into account that should the server machine be compromised, the whole voting and recounting system would be broken.
- 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

- Regarding the choice of software, we used Apache as the webserver and Tomcat 5 as application server, both of them running in LINUX i386 machines. Both databases were stored in a single MYSQL server which was executing in the same machine with Apache and Tomcat.
- There are several options available to link Apache and Tomcat. The simplest way is running two independent servers listening in different ports (in fact, it would even be possible to have them running in different machines, should the need arise). Notwithstanding this, we chose to use a tighter integration between them using the JK Connector. This technology allows to redirect queries that would normally be answered by the Apache server towards the Tomcat application server, in a way that is transparent for the user.
- This choice makes the Tomcat application server unaware of the underlying SSL layer. Even though the voting system cannot obtain the client certificate from the SSL layer, our protocol allows for the certificate to be sent by the client in case the server is not able to directly retrieve it.
- In order to generate the certificates needed, we also set up a Certificate Authority using OpenSSL.

PHILOSOPHICAL, METHODOLOGICAL AND TECHNOLOGICAL FOUNDATIONS OF E-COGNOCRACY

TECHNOLOGICAL REFERENCES

1. MORENO-JIMÉNEZ, J.M. et al. (2006): e-Voting process for e-cognocracy. Proceedings *Euro Working Group on Decision Support Systems* (EWG-DSS). IRIT/RR-06-14-FR, 51-55.
2. PILES, J.J. et al. (2006): The voting challenge of e-cognocracy. Proceedings *2nd International Electronic Voting 2006 Workshop*. Breggen, Austria, GI-LNI, P-86, 225-235.ISBN 1617-5468.
3. PILES, J. et al. (200?): Security Considerations in e-Cognocracy. *Lecture Notes in Computer Science*. Springer-Verlag.

CONCLUSIONS AND FUTURE LINES

➢ Conclusions about e-Cognocracy:

- Overcomes the limitations of representative and participative democracy y effectively combining them with appropriate weights.
- New orientation to democracy which, based on the evolution of living systems, pursues the survival of the species through the extraction and social diffusion of knowledge.
- We have proposed new methodological and technological tools

➢ Future research lines

- Extraction and social diffusion of knowledge