nVotes

Eduardo Robles

Director Técnico

edulix@nvotes.com

@edulix

Anonimato, cifrado y privacidad

Fundamentos del voto electrónico seguro para decidim.barcelona

*El **voto secreto** se introdujo en las asambleas **romanas** en el **siglo II** como una forma de "disminuir el control de las clases altas sobre el electorado y mejorar la libertad efectiva de elección de los votantes"*

Gerber et al, 2013

“

*La voluntad del pueblo … se expresará en **elecciones** periódicas y genuinas que … se celebrarán por votación **secreta** o por procedimientos equivalentes de voto **libre**.*

Declaración de Derechos Humanos 21.3

La mejor encuesta es una buena votación.

CUAL ES LA RELACIÓN?

Voto secreto → **Voto libre** → **Legitimidad**

- Confidencial
- Dentro del espacio personal
- En la intimidad

- Libre de coacción

- Al expresar la opinión verdadera y **genuina** de los votantes

La seguridad es un estado mental

- Privacidad por **diseño**
  - Para **convencer** al votante
  - Privacidad ante **todos**
  - **Garantías**

Ejemplo de voto

Voto original => **Voto codificado** => **Voto cifrado y secreto**

Option A

1

“alpha:“”42589531826777223714538804092687490513896336998991390971033335609799611441877064526136245284657244122497804586518859294565187778554187485976538525967877077332767449390435547586232307982449004221185788081839146233855834552792403587041865476454151642574286811110595709606305943585368898322670544410819455389389831367809958730183299594989130076538510945687635663683098296210633619365132089120745366382408142036522747296230873086226136520543602814223229543379123164699348284892677673309747460759427014198448582435475370584046553547900607489172617753476769197677750611446020858121000279239450315248197518536252253443532905","beta":"27185711437157390826188462678332007109355128799729923110799814299160657193983088363684193264062089876081017637156241870149226894349790653957339213642936456546081086374214876408722586178972284160068530329077918884142340319827202955478014940261441607806659182188705541155188761329158988352447193849484578841064651028930832649200323884321863998212200685812785602618056731914184968739004824668257801231248906386111937435829903224619050149130528774456591475897031746579331975898008525610664867080700485881529738556514489995892728401965651600190808861489183448335215763800148372583170115673515442416962822562545490072555258”

Resultado electoral y anonimato

- **Nadie** puede conocer **tu voto**
- **Todos** deben poder conocer el **resultado**

Voto **Secreto**, no anónimo

Voto **Anónimo**, no secreto

Agora Voting

Encrypted votes => mixnet => clear text votes and anonymous

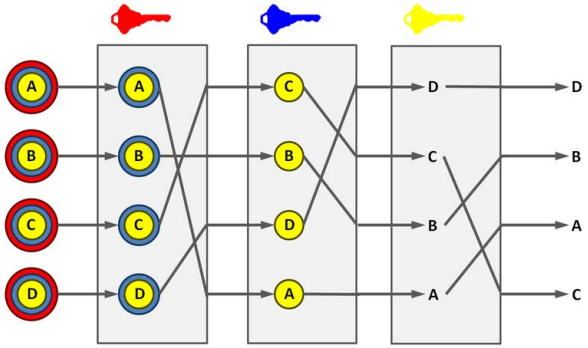
John Vote

"alpha:""42589531826777223714538804092687490513896336998913909710333356097996114418770645261362452846572441224978045865188592945651877785541874859765385259678770773327674493904355475862323079824490042211857880818391462338558345527924035870418654764541516425742868111105957096063059435853688983226705444108194553893898313678099587301832995949891300765385109456876356636830982962106336193651320891207453663824081420365227472962308730

Jane Vote

"alpha:""42589531826777223714538804092687490513896336998913909710333356097996114418770645261362452846572441224978045865188592945651877785541874859765385259678770773327674493904355475862323079824490042211857880818391462338558345527924035870418654764541516425742868111105957096063059435853688983226705444108194553893898313678099587301832995949891300765385109456876356636830982962106336193651320891207453663824081420365227472962308730

.. and more votes ..



Source: wikipedia.org

option A

option B

option A

option C

option A

option A

option C

.. and more votes ..

VERIFICABLE DE EXTREMO A EXTREMO

A. Codificación del voto

⇒ individual

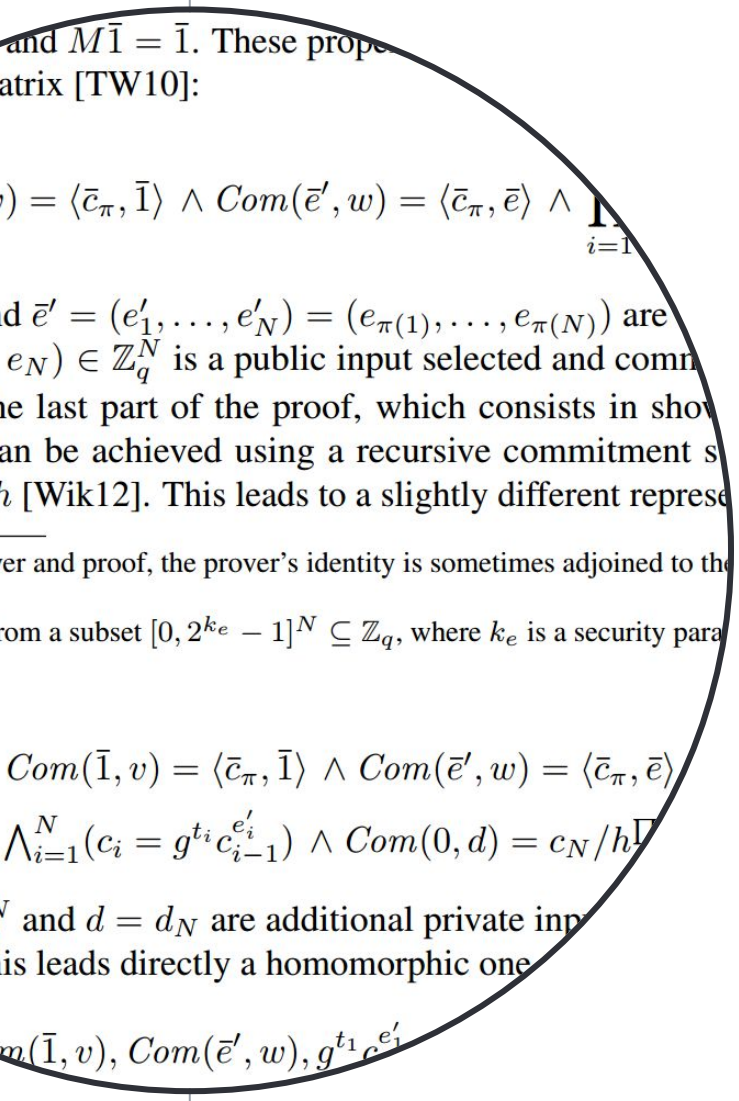
B. Inclusión en el recuento

⇒ universal

C. Escrutinio correcto

⇒ universal

PRIVACIDAD, VERIFICABILIDAD, MATEMÁTICAS



Las propiedades de **privacidad** y **verificabilidad**

de un canal de participación robusto

se fundamentan en última instancia en las **matemáticas**

Procedimiento de anonimización

nVotes

REFERENCES

- Michels, R 1915 Political Parties: A Sociological Study of the Oligarchical Tendencies of Modern Democracy. Free Press, Glencoe, IL
- Weber M 1946. “Economy and Society.” In H.H. Gerth and C. Wright Mills, (eds.)
- Arthur Lupia. 2001. "Delegation of Power: Agency Theory." Published in Neil J. Smelser and Paul B. Baltes (eds.)
- S Gailmard. 2012. Accountability and principal-agent models.
- N Potrafke. 2013. Evidence on the political principal-agent problem from voting on public finance for concert halls.
- Arnstein, Sherry R. 1969. A Ladder of Citizen Participation.
- Gerber, Huber, Doherty. 2012. Is There a Secret Ballot? Ballot Secrecy Perceptions
- and Their Implications for Voting Behaviour
- Universal Declaration of Human Rights
- US Vote Foundation. 2015. The Future Of Voting
- http://web.mit.edu/cis/pdf/Lehoucq.pdf
- http://www.law.gmu.edu/assets/files/publications/working_papers/0942BenthamBallots.pdf
- https://ideas.repec.org/p/ces/ceswps/_4306.html

CREDITS

Special thanks to

- Presentation template by SlidesCarnival

Image credits

- http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/m/
- https://finnaarupnielsen.wordpress.com/2016/05/10/occupations-of-persons-from-panama-papers/
- http://mustsharenews.com/wikileaks-singapore/
- https://kickoffghana.files.wordpress.com/2012/12/ladder-of-participation.jpg
- http://static.obrasweb.mx/media/2013/04/15/puente-durango-mazatlan.jpg