Protocolos seguros en voto electrónico

Seminarios

Autómatas, Lenguajes Formales y sus Aplicaciones

Seminarios VRAIN

Antonio M. Larriba Flor

February 22, 2021

Universitat Politècnica de València

Índice

¿Por qué el voto electrónico? I

Toda votación está basada en la confianza en el sistema

Ventajas

- Inmediatez.
- Nuevas propiedades.

Inconvenientes

- Barrera tecnológica.
- Posible manipulación.

¿Por qué el voto electrónico? II

Comunes

- Anonimato.
- Privacidad.
- Democracia.

Nuevas

- Verificabilidad (personal y global).
- Deslocalización.
- Precisión.
- Robustez.

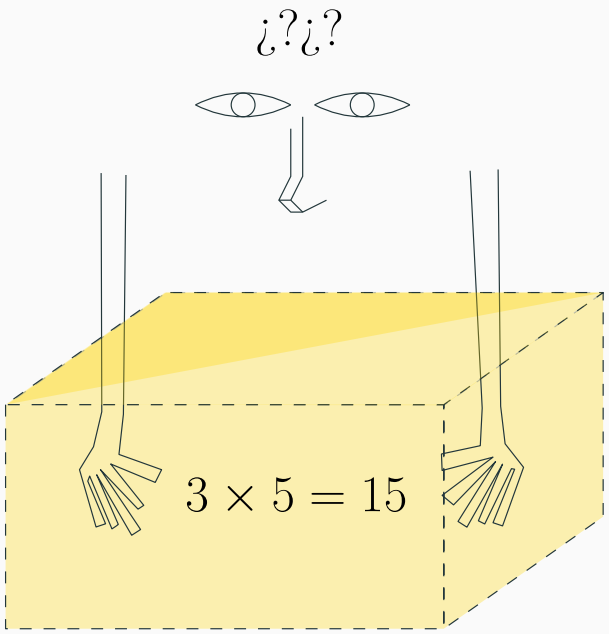
Retos

- Proveer de la verificabildad del voto sin comprometer la privacidad de los votantes.
- Asegurarse de que el ciudadano vota sólo una vez sin comprometer su privacidad.

Estado del arte

Estado del arte | Homomorphic Cryptography

La criptografía homomórfica nos permite trabajar con datos encriptados de manera equivalente a cómo lo haríamos con datos sin encriptar.

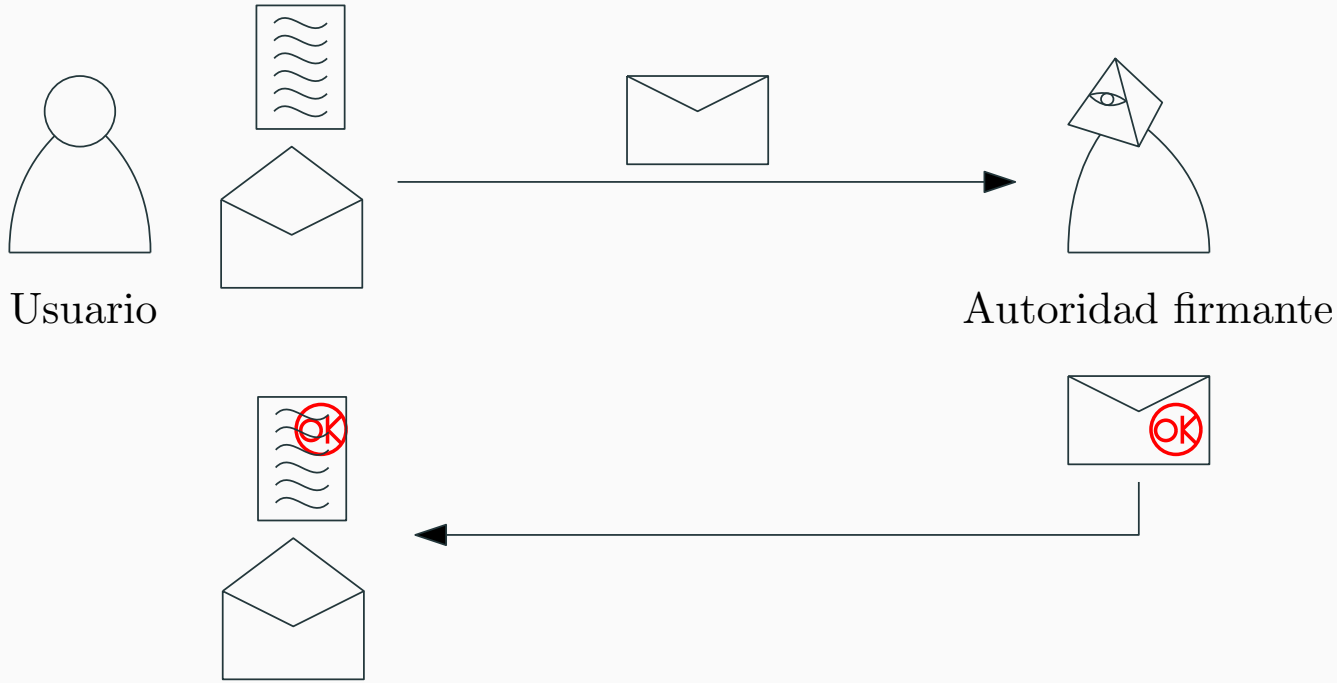


Ejemplo de propiedades homomórficas para la suma y la multipicación.

Sistemas de voto basados en encripción homomórfica: Cramer et al. (1997); Yang et al. (2018, 2017).

Estado del arte | Blind Signatures

Las Blind Signatures (firmas ciegas) (Chaum, 1984) permiten al firmante acreditar un documento sin la necesidad de verlo.

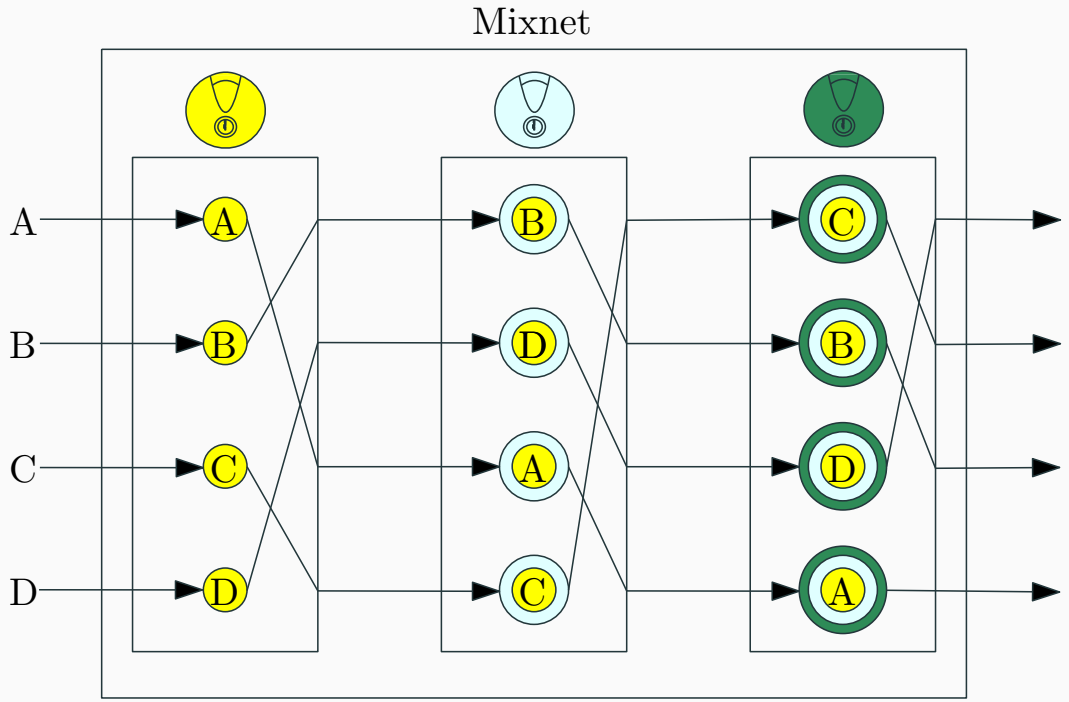


Ejemplo de esquema de blind signature.

Sistemas de voto basados en blind signatures: Li et al. (2009); Thi and Dang (2013).

Estado del arte | Mixnets

Las mixnets (Chaum, 1981) son redes que permiten el envío anónimo de información a través de múltiples capas de encriptación.

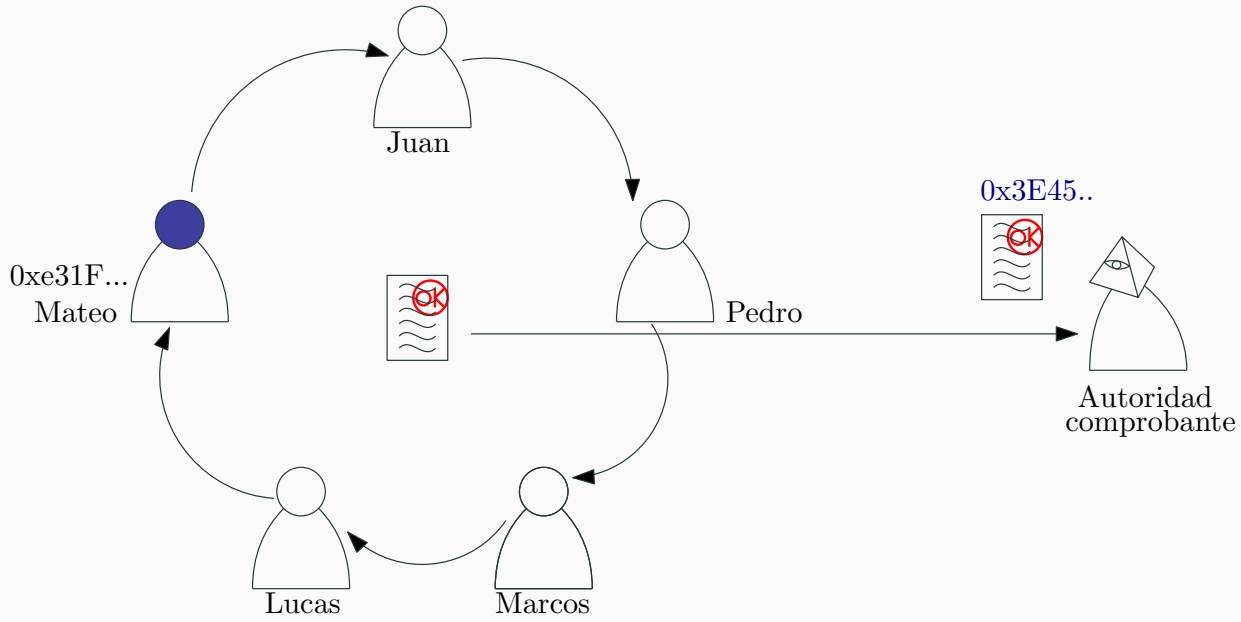


Ejemplo de mixnet de encriptación.

Sistemas de voto basados en mixnets: Carroll and Grosu (2009).

Estado del arte | Firmas en anillo

Las firmas en anillo (Rivest et al., 2001) permiten firmar como usuario perteneciente a un grupo sin desvelar al firmante en particular.

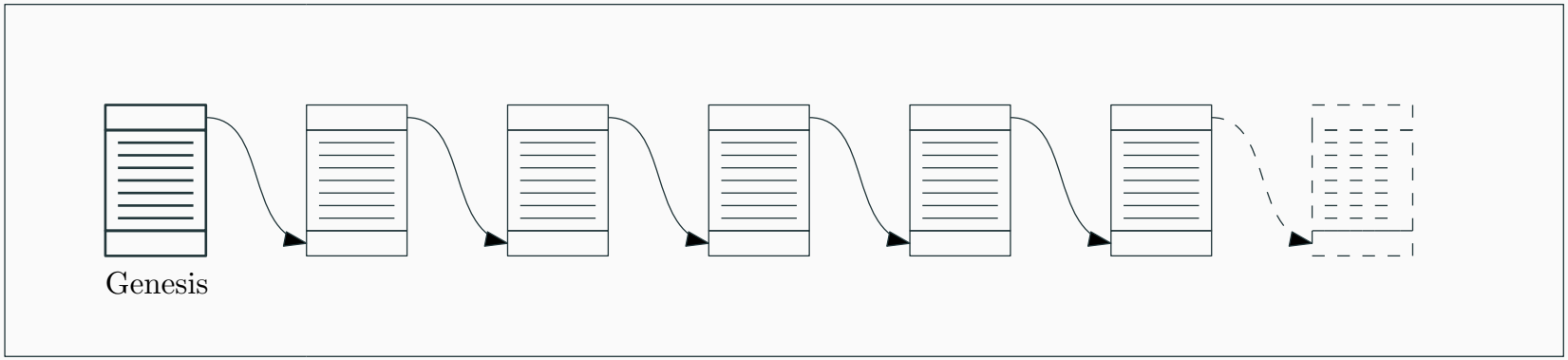


Ejemplo de firma en anillo.

Sistemas de voto basados en firmas en anillo: Salazar et al. (2010); Chen et al. (2008).

Estado del arte | Blockchain

La blockchain (Satoshi, 2008) es una base de datos descentralizada y distribuída que puede ser consultada de manera pública.



Estructura de la blockchain.

Sistemas de voto basados en blockchain: Noizat (2015); Lee et al. (2016); Ayed (2017); Tarasov and Tewari (2017).

Sistemas propuestos

Clave pública

- También llamada clave asimétrica.
  - Clave pública v.
  - Clave privada s.
- Un función para encriptar y otra para desencriptar.

$$Encriptar(Desencriptar(M, s), v) = Desencriptar(Encriptar(M, v), s)$$

TAVS: A Two Authorities electronic Voting Scheme

Características

- Basado en blind signatures.
- Dos autoridades independientes.

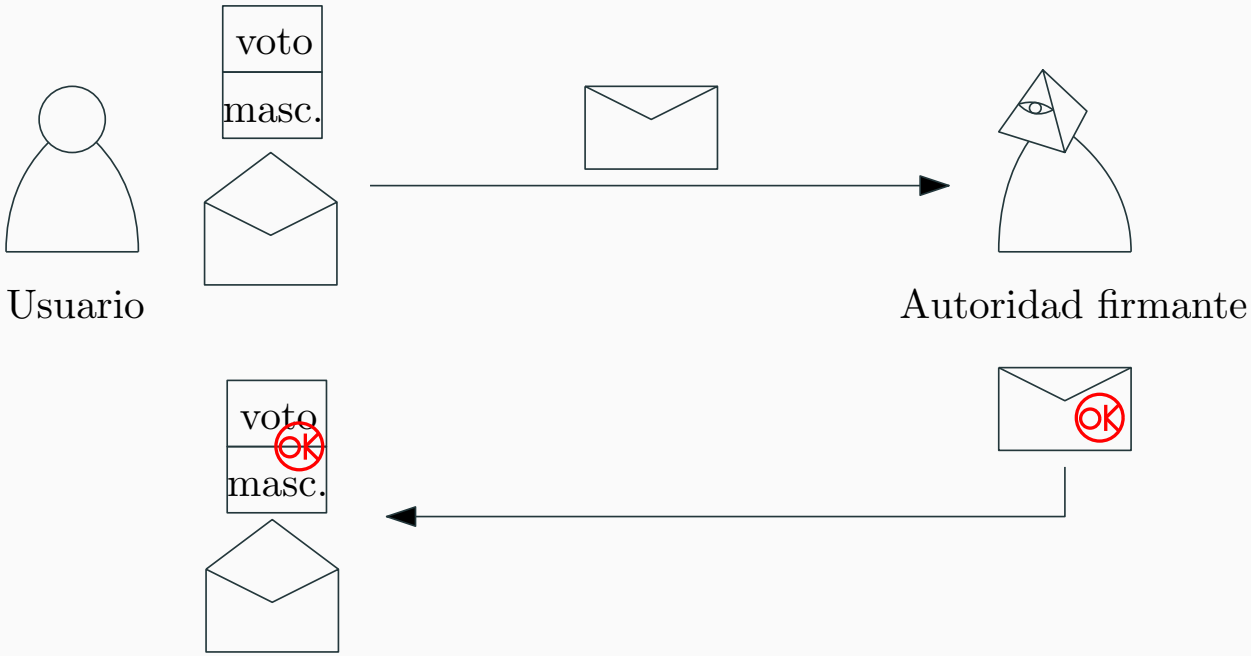
Objetivos

- Simple.
- Reducción autoridades.
- Coste computacional mínimo.

TAVS | Descripción del sistema I

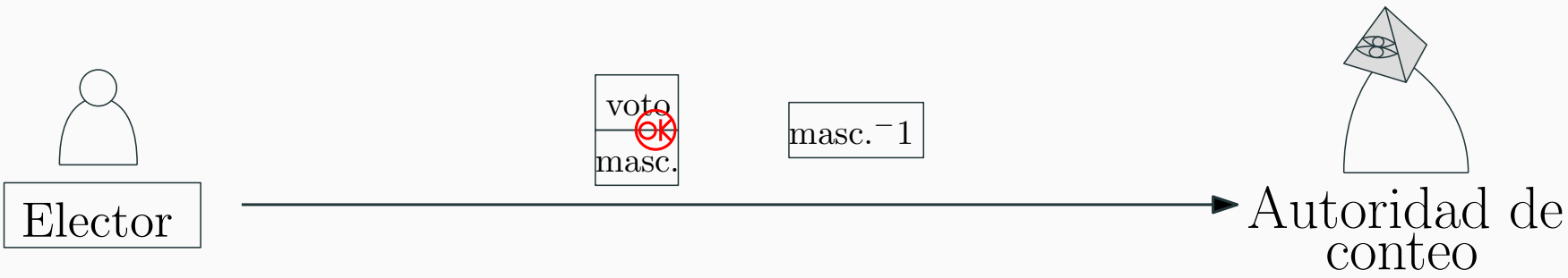
1. El elector decide su voto y prepara la papeleta.
2. Envía la papeleta enmascarada a la autoridad de identificación.
3. La autoridad comprueba la identificación y firma la papeleta.
4. El elector crea el voto definitivo con la papeleta firmada.
5. Envía el voto al sistema de conteo.
6. Se comprueba el voto y se publica en el boletín público.

TAVS | Descripción del sistema II



Creación de la papeleta.

TAVS | Descripción del sistema III



1. Elimina la máscara

2. Desencripta el voto

3. Comprueba la integridad del voto
4. Publica el voto y el hash en el boletín público

Comprobación de la identificación.

- Reducción del coste computacional.
- Reducción del número de autoridades.
- Arquitectura simple.

Distributed Trust, a Blockchain Election Scheme

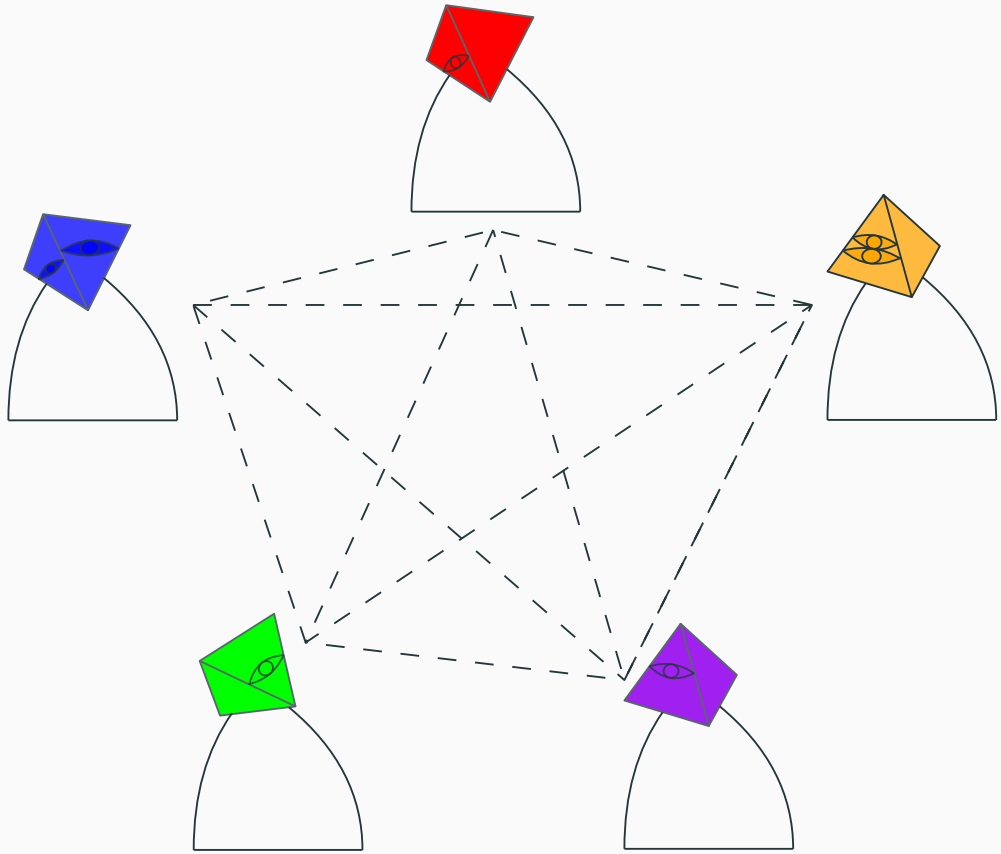
Características

- Basado en blockchain y firmas en anillo.
- Introduce facciones del voto tradicional.

Objetivos

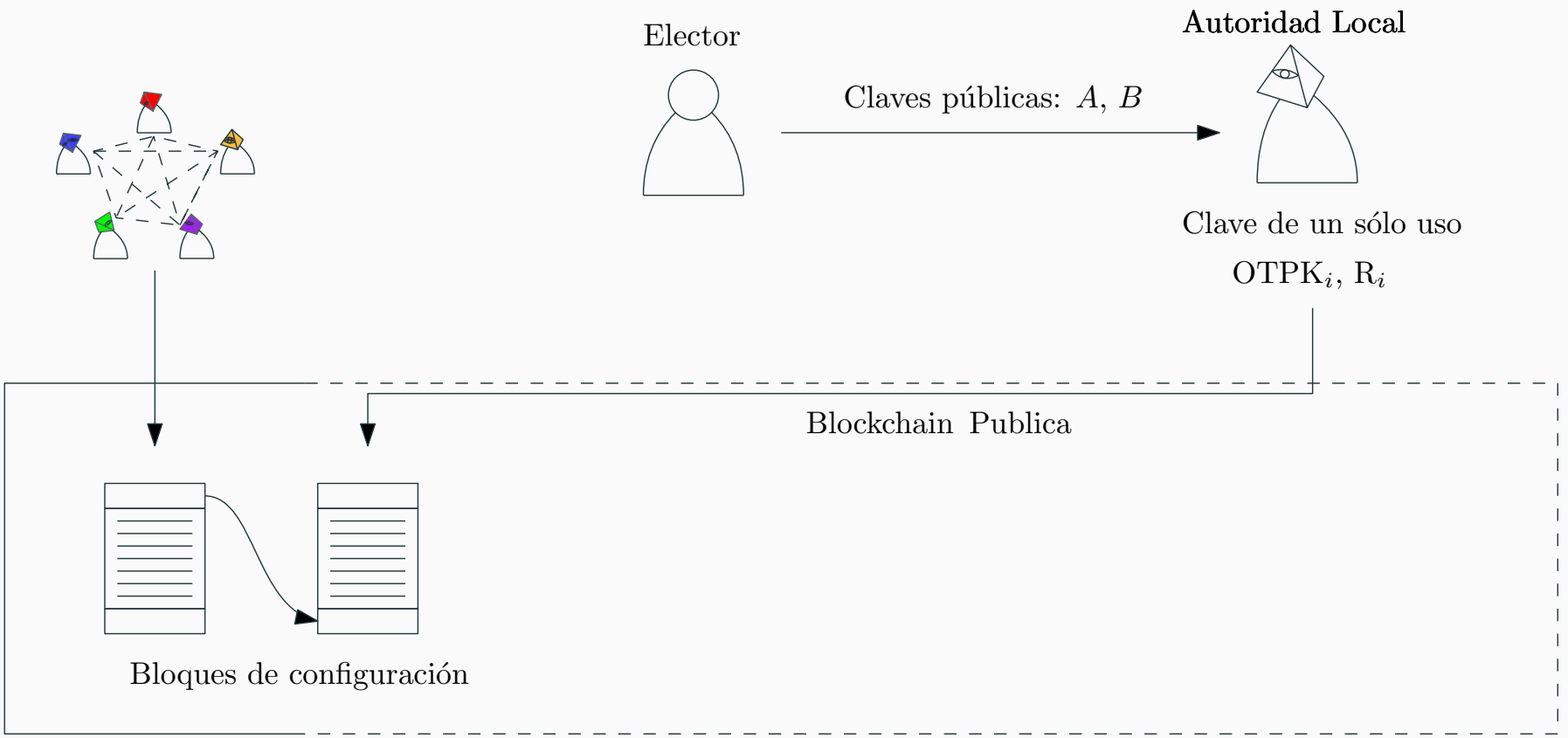
- Aumentar la confianza.
- Máxima transparencia.

Distributed Trust | Descripción del sistema I



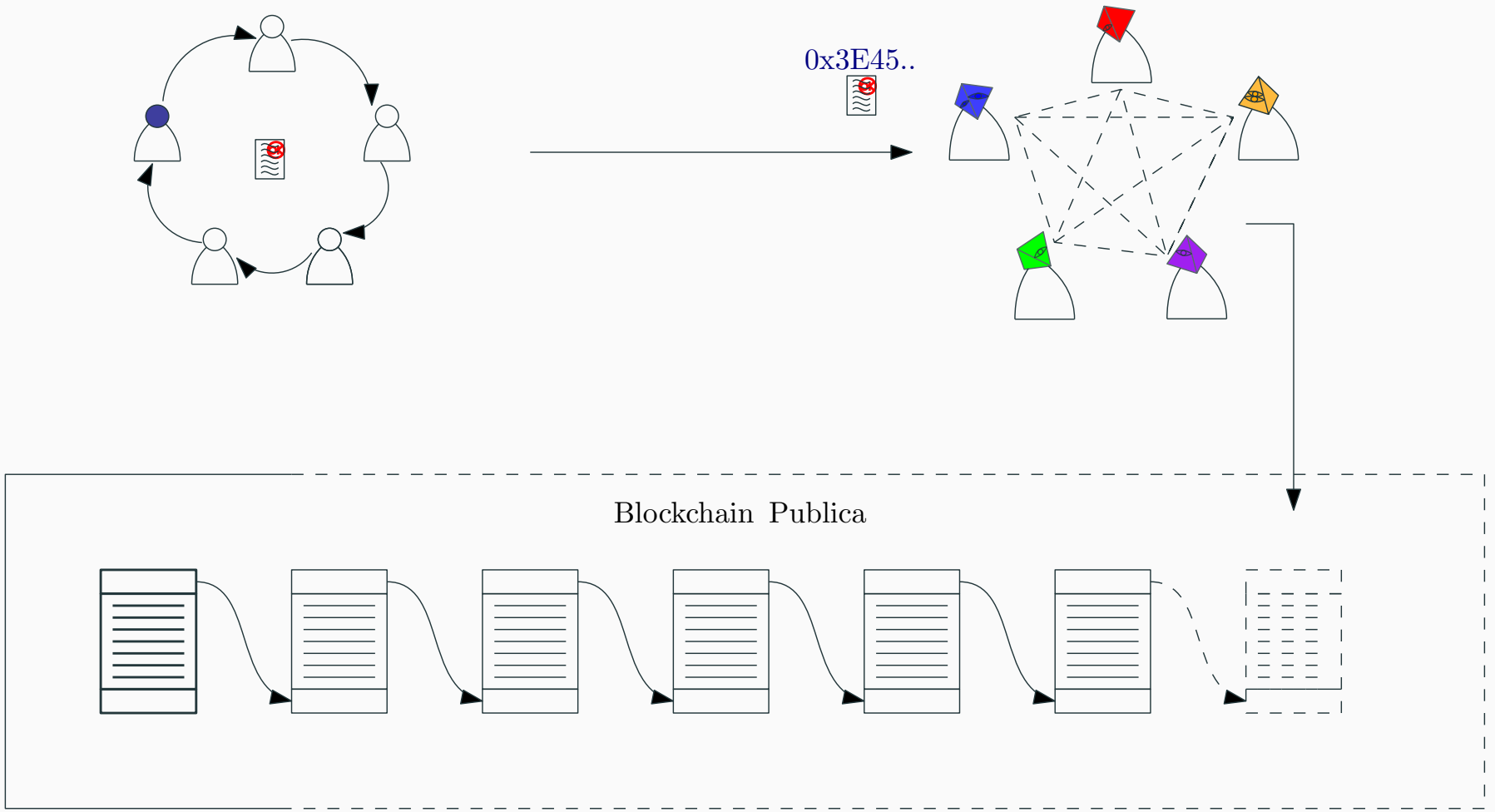
Acuerdo de los partidos.

Distributed Trust | Descripción del sistema II



Registro del elector.

Distributed Trust | Descripción del sistema III



Proceso del voto.

- Introducción de poderes tradicionales.
- Aumento de la confianza en el sistema.
- Máxima transparencia.

Conclusiones

Dudas y preguntas

References

Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3):01–09.

Carroll, T. E. and Grosu, D. (2009). A secure and anonymous voter-controlled election scheme. *J. Netw. Comput. Appl.*, 32(3):599–606.

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88.

Chaum, D. (1984). Blind signature system. In *Advances in Cryptology - EUROCRYPT '84*, pages 153–153. Springer.

Bibliography ii

Chen, G., Wu, C., Han, W., Chen, X., Lee, H., and Kim, K. (2008). A new receipt-free voting scheme based on linkable ring signature for designated verifiers. In *2008 International Conference on Embedded Software and Systems Symposia*, pages 18–23. IEEE.

Cramer, R., Gennaro, R., and Schoenmakers, B. (1997). A secure and optimally efficient multi-authority election scheme. *Eur. Trans. Telecommun.*, 8(5):481–490.

Lee, K., James, J. I., Ejeta, T. G., and Kim, H. J. (2016). Electronic voting service using block-chain. *Journal of Digital Forensics, Security and Law*, 11(2):8.

Li, C., Hwang, M., and Lai, Y. (2009). A verifiable electronic voting scheme over the internet. In Latifi, S., editor, *Sixth International Conference on Information Technology: New Generations, ITNG 2009, Las Vegas, Nevada, USA, 27-29 April 2009*, pages 449–454. IEEE Computer Society.

Bibliography iii

Noizat, P. (2015). Blockchain electronic vote. In *Handbook of digital currency*, pages 453–461. Elsevier.

Rivest, R. L., Shamir, A., and Tauman, Y. (2001). How to leak a secret. In *Proceedings Of The 7th International Conference On The Theory And Application Of Cryptology And Information Security: Advances In Cryptology*, pages 554–567. Springer-Verlag.

Salazar, J. L., Piles, J. J., Ruíz-Mas, J., and Moreno-Jiménez, J. M. (2010). Security approaches in e-cognocracy. *Computer Standards & Interfaces*, 32(5-6):256–265.

Satoshi, N. (2008). Bitcoin: a peer-to-peer electronic cash system. Available at `https://bitcoin.org/bitcoin.pdf`.

Tarasov, P. and Tewari, H. (2017). Internet voting using zcash. Available at `https://dblp.org/rec/bib/journals/iacr/TarasovT17`.

Bibliography iv

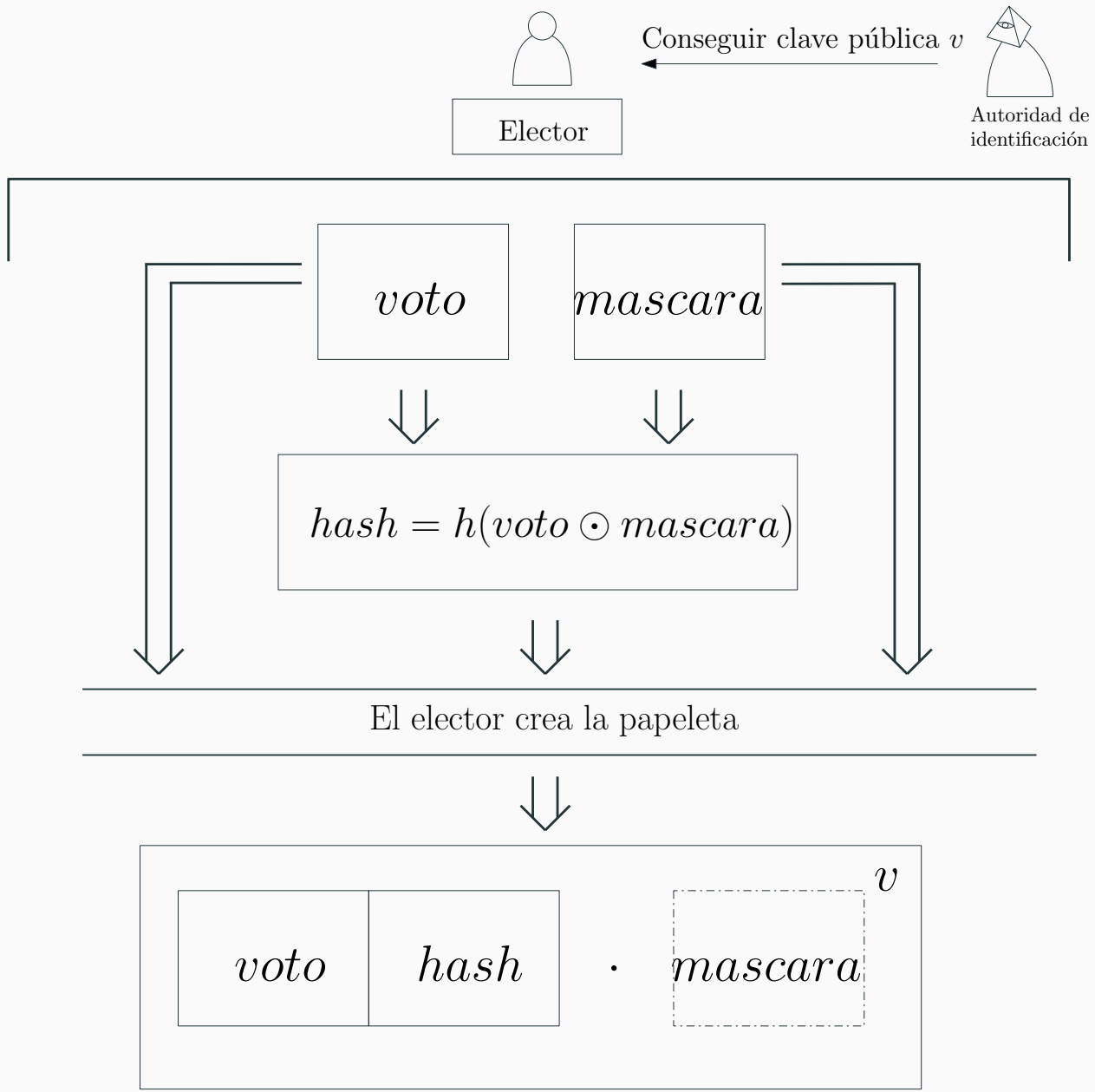
Thi, A. T. N. and Dang, T. K. (2013). Enhanced security in internet voting protocol using blind signature and dynamic ballots. *Electron. Commer. Res.*, 13(3):257–272.

Yang, X., Yi, X., Nepal, S., Kelarev, A., and Han, F. (2018). A secure verifiable ranked choice online voting system based on homomorphic encryption. *IEEE Access*, 6:20506–20519.

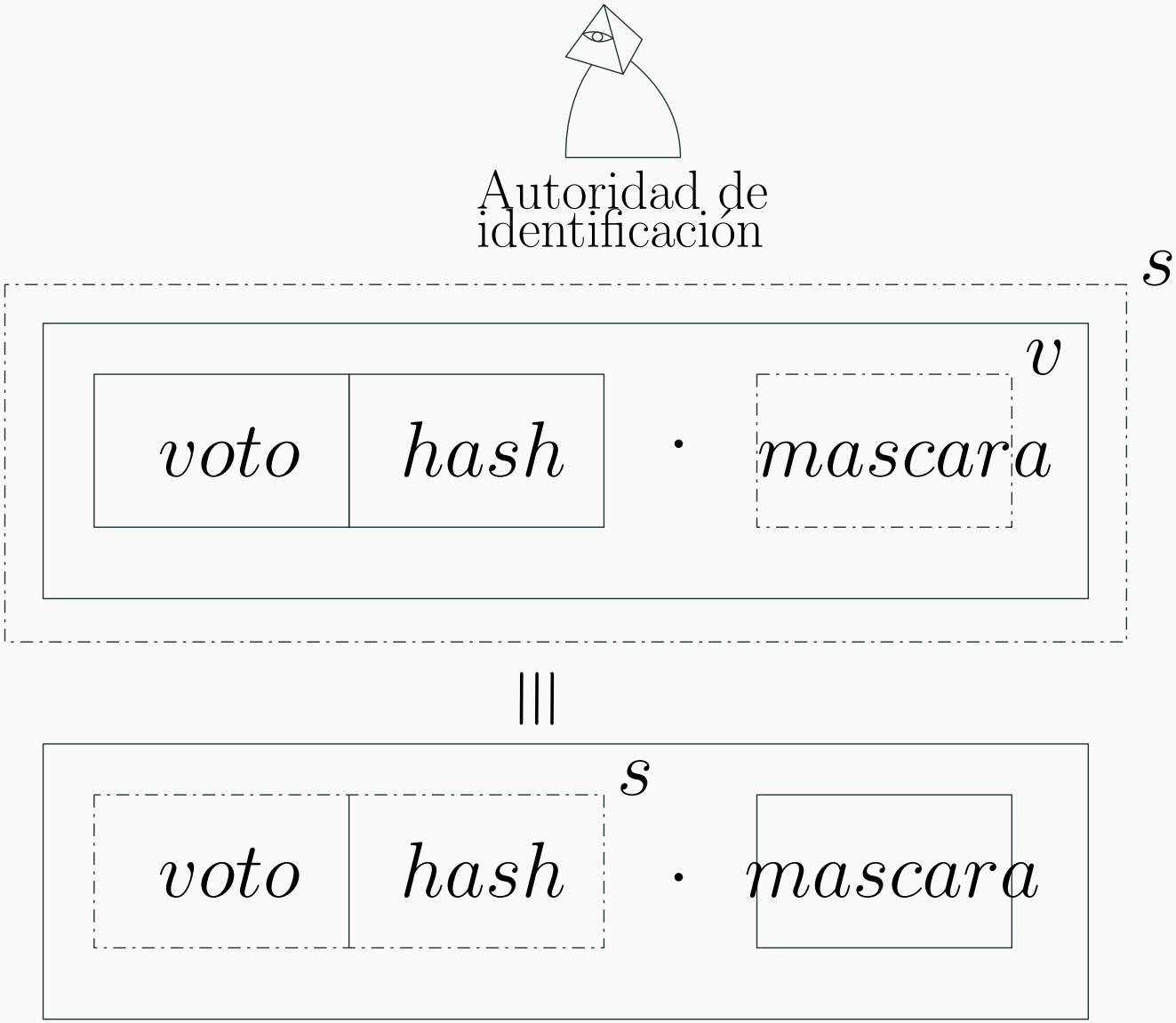
Yang, X., Yi, X., Ryan, C., van Schyndel, R. G., Han, F., Nepal, S., and Song, A. (2017). A verifiable ranked choice internet voting system. In Bouguettaya, A., Gao, Y., Klimenko, A., Chen, L., Zhang, X., Dzerzhinskiy, F., Jia, W., Klimenko, S. V., and Li, Q., editors, *Web Information Systems Engineering - WISE 2017 - 18th International Conference, Puschino, Russia, October 7-11, 2017, Proceedings, Part II*, volume 10570 of *Lecture Notes in Computer Science*, pages 490–501. Springer.

Apéndice

TAVS | Más detalles del sistema I

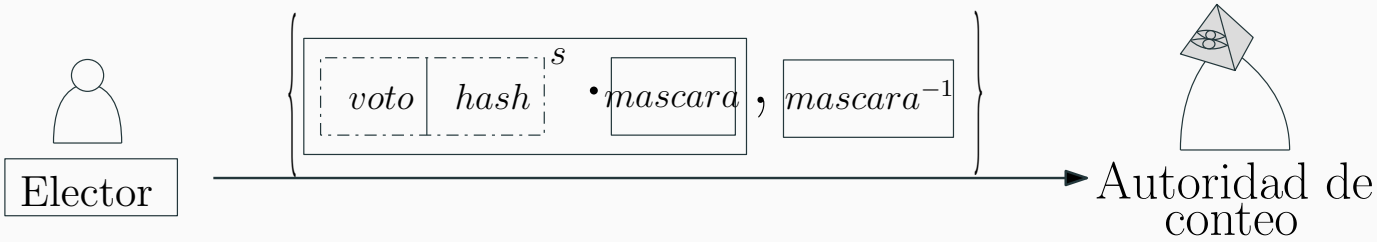


TAVS | Más detalles del sistema II

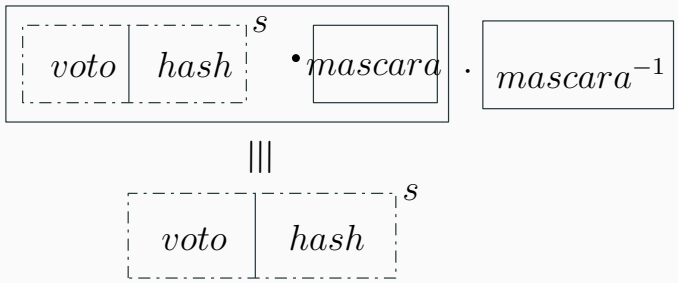


Comprobación de la identificación.

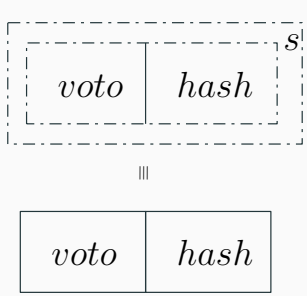
TAVS | Más detalles del sistema III



1. Elimina la máscara



2. Desencripta el voto



3. Comprueba la integridad del voto

4. Publica el voto y el hash en el boletín público

Conteo del voto.