Blockchain et Vote électronique

La technologie X va résoudre tous les problèmes de Y

Tel que présenté le 19 Octobre 2016
au Café Numérique par David Glaude

Disclaimer

Ceci est mon opinion et n’est en rien lié avec mon employeur.

Mon opinion personnelle peut parfois diverger de celle de PourEVA.

Contexte: Election politique (démocratie parlementaire)

Hors context: Election non politique, choix aléatoire de représentant, liquid democracy, The Voice, Association des Cryptographes Anonymes, ...

Blockchains & Elections: Don’t Believe the Hype

“Using Bitcoin (or a blockchain) as an election system is a bad idea that really doesn’t make sense. While blockchains can be useful in the election process, they are only appropriate for use in one small part of a larger election system.”

“If you were to create a private blockchain distributed across many trusted computers it would be a great way to store cast ballots or election logs. However, secure storage for ballots and logs is only one **tiny** piece of the overall election puzzle. Blockchains are a good solution to this one piece, but not to “running elections” in general as some claim.”

http://freeandfair.us/articles/blockchains-and-elections/

La marteau de Abraham Maslow

« I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail. »

Abraham Maslow (The Psychology of Science, 1966)

J’exprime un problème, définir le problème, je cherche une solution.

vs

J’ai une technologie, je cherche ce que l’on pourrait faire avec.

Autres technologies ‘à la mode’

Chiffrement Homomorphique

- Faire des calculs sur des messages cryptés.
- Déchiffrer que le résultat.

Mix network = Mélanger les messages à travers un réseau de serveur (Tor)

Zero knowledge poof = Preuve à divulgation nulle de connaissance

Secret réparti = Il faut x clefs parmis y pour ouvrir/décoder

End 2 End verifiability = Je peux vérifier que mon bulletin est dans l’urne

“Etudes” de cas

1. ESTONIE: Internet Voting en Estonie *
2. BELGIQUE: Rapport Be-Voting (2008)
3. HELIOS (2009)
4. BELGIQUE: Vote électronique avec “preuve” papier
    - En 2012 et 2014: 50% de la Flandre, Saint-Gilles et Woluwé-Saint-Pierre.
5. Le jour ou la Belgique à buggé (25 mai 2014)
6. AUSTIN (USA): Star-VOTE (futur) *
7. BELGIQUE: Vote électronique avec preuve papier
    - En 2018 et 2019: 50% de la Flandre, 100% de Bruxelles et 100% des Canton Germanophone

* Peut contenir des traces de Blockchain

Secret du vote

DECLARATION ON CRITERIA FOR FREE AND FAIR ELECTIONS

Unanimously adopted by the Inter-Parliamentary Council at its 154th session

(Paris, 26 March 1994)

http://www.ipu.org/cnl-e/154-free.htm

Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE (1990)

http://www.osce.org/odihr/elections/14304

Secret, vraiment secret

- Le secret doit être protégé pour toujours
- Le sentiment que le vote est secret doit être protégé

Contre-exemples:

- UK: Les bulletins de vote sont numérotés et les électeurs enregistrés
- Israël: L'heure d'arrivé de chaque électeur est enregistrée…
- Belgique: Vote multiple et secret du vote
- Belgique: Carte d'identité électronique et vote électronique
  http://www.poureva.be/spip.php?mot31

Règles de la tragédie électoral belge

Règles des trois unités:

- Unité d’action: Le jour de l’élection, rien d’autre se passe.
- Unité de temps: L’élection se déroule en un jour (et une nuit).
- Unité de lieu: Tout se passe dans le bureau de vote (et dépouillement).

Règles de bienséance

- Vraisemblance: Le résultat doit avoir une impression de vérité (crédible).
- Bienséance: Il faut respecter les usages et les conventions.

Le vote à distance n’est pas démocratique

Rapport « Be Voting » (2e partie, page 107) : « ... il subsiste des questions relatives à la coercition, à l’achat de votes, etc., qui sont difficiles à éviter, quel que soit le système de vote à distance mis en œuvre ».

http://www.poureva.be/spip.php?article593

Article 62 de la constitution Belge:

Le vote est obligatoire et secret. Il a lieu à la commune, sauf les exceptions à déterminer par la loi.

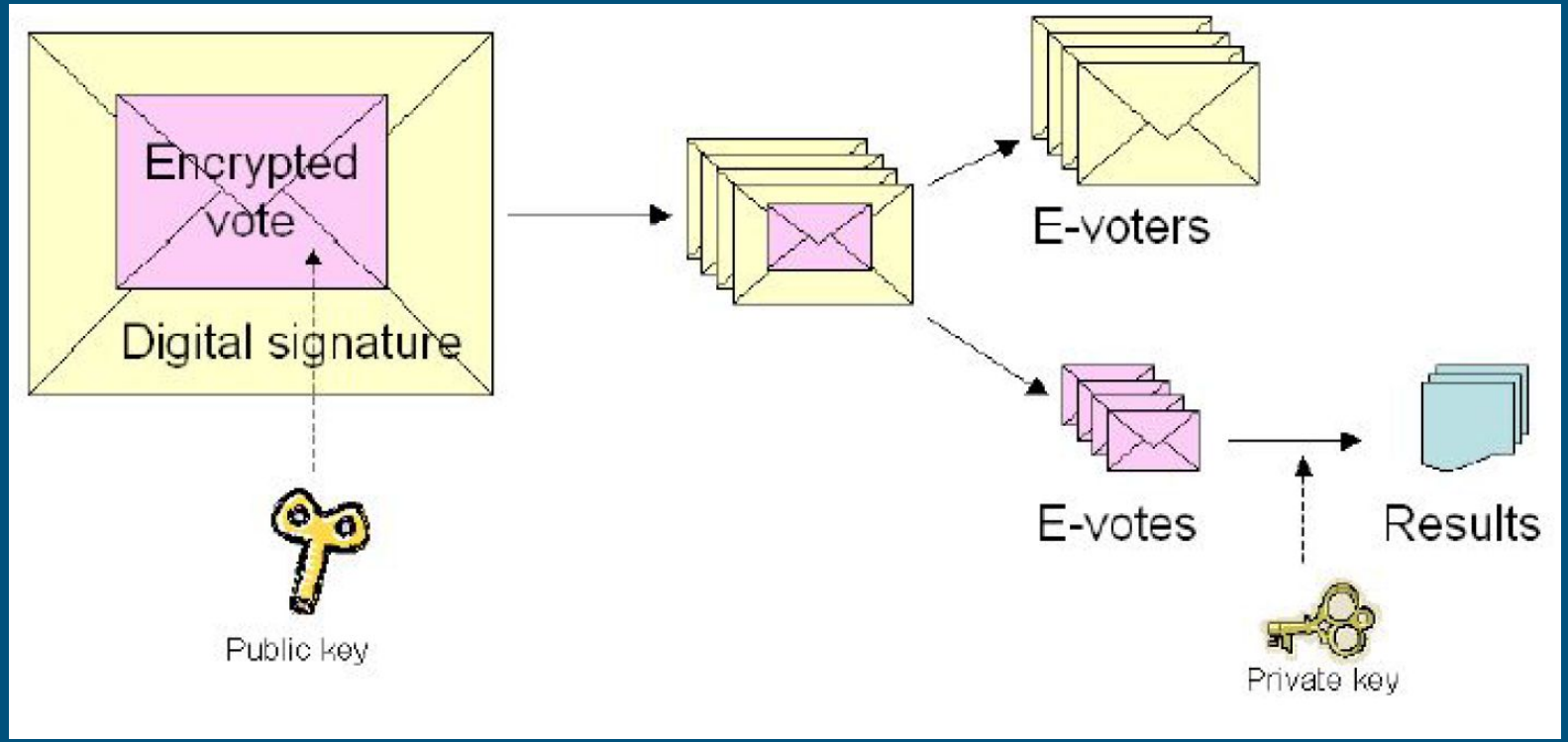
1. Le vote par internet en Estonie

Independent Report on E-voting in Estonia

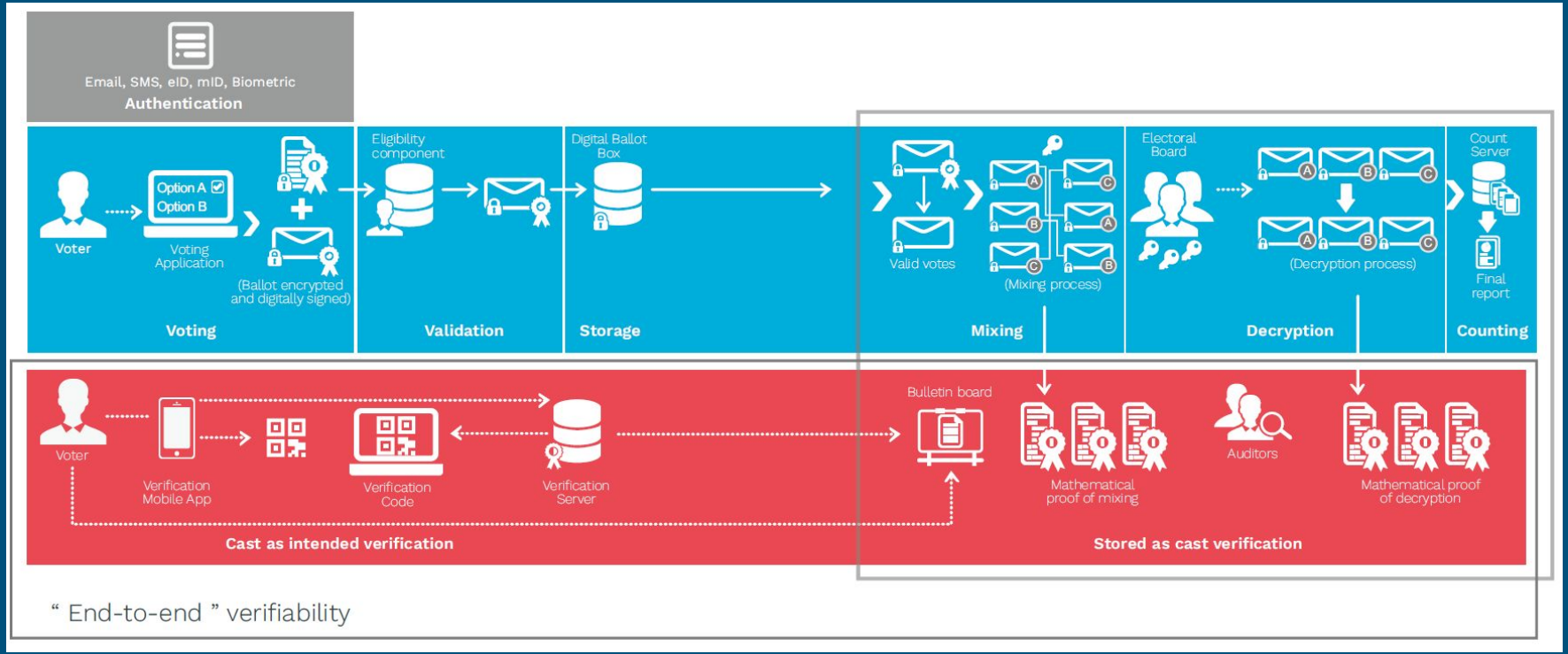
A security analysis of Estonia's Internet voting system by international e-voting experts.

https://estoniaevoting.org/

1.. Estonian internet voting (en 2007)



1… TIVI: Estonian internet voting (en 2016)



1.... TIVI FAQ (Smartmatic + Cybernetica)

The implementation of a **Blockchain** based bulletin board provides additional proof of the integrity of all cast ballots, showing that no ballot preferences have been changed, no valid votes deleted or bogus votes inserted.

http://www.smartmatic.com/fileadmin/user_upload/TIVI_FAQ.pdf

Machine de Vote (DRE)

Hanging Chads (Floride 2000) => Help America Vote Act (2002) => DRE

Association for Computing Machinery: "Voting systems should enable each voter to inspect a physical (e.g. paper) record to verify that his or her vote has been accurately cast, and to serve as an independent check on the result produced and stored by the system,"

http://usacm.acm.org/evoting/category.cfm?cat=14&E-Voting

=> VVAT (Voter Verified Audit Trail) / VVPB (Voter Verified Paper Ballot)

2. BeVoting le futur du vote électronique

- Etude commandée par le Fédéral, la Flandre et Bruxelles-Capitale
- Consortium de toutes les universités Belges
- Partie 1: Analyse des systèmes existants
- Partie 2: Proposition d'un nouveau système (4 décembre 2007)
- Vote au Parlement pour continuer l'expérimentation
- Appel d'offre (gagné par Smartmatic + Stéria)
- Test d'un prototype (27 Octobre 2011)

http://www.poureva.be/spip.php?mot27

2.. BeVoting: “Bulletin de vote” hybride

Vote émis à Liège

Vérifiez et pliez ce bulletin

Élection Sénat *Parti préféré*	Élection Chambre *Parti préféré*	Élection Europe *Parti préféré*	Élection Province *Parti préféré*	Élection Région *Parti préféré*	Élection Locale *Parti préféré*
1. Premier Nom	17. Premier Nom	33. Premier Nom	49. Premier Nom	65. Premier Nom	81. Premier Nom
2. Deuxième Nom	18. Deuxième Nom	34. Deuxième Nom	50. Deuxième Nom	66. Deuxième Nom	82. Deuxième Nom
3. Troisième Nom	19. Troisième Nom	35. Troisième Nom	51. Troisième Nom	67. Troisième Nom	83. Troisième Nom
4. Quatrième Nom	20. Quatrième Nom	36. Quatrième Nom	52. Quatrième Nom	68. Quatrième Nom	84. Quatrième Nom
5. Cinquième Nom	21. Cinquième Nom	37. Cinquième Nom	53. Cinquième Nom	69. Cinquième Nom	85. Cinquième Nom
6. Sixième Nom	22. Sixième Nom	38. Sixième Nom	54. Sixième Nom	70. Sixième Nom	86. Sixième Nom
7. Septième Nom	23. Septième Nom	39. Septième Nom	55. Septième Nom	71. Septième Nom	87. Septième Nom
8. Huitième Nom	24. Huitième Nom	40. Huitième Nom	56. Huitième Nom	72. Huitième Nom	88. Huitième Nom
9. Neuvième Nom	25. Neuvième Nom	41. Neuvième Nom	57. Neuvième Nom	73. Neuvième Nom	89. Neuvième Nom
10. Dixième Nom	26. Dixième Nom	42. Dixième Nom	58. Dixième Nom	74. Dixième Nom	90. Dixième Nom
11. Onzième Nom	27. Onzième Nom	43. Onzième Nom	59. Onzième Nom	75. Onzième Nom	91. Onzième Nom
12. Douzième Nom	28. Douzième Nom	44. Douzième Nom	60. Douzième Nom	76. Douzième Nom	92. Douzième Nom
13. Treizième Nom	29. Treizième Nom	45. Treizième Nom	61. Treizième Nom	77. Treizième Nom	93. Treizième Nom
14. Quatorzième Nom	30. Quatorzième Nom	46. Quatorzième Nom	62. Quatorzième Nom	78. Quatorzième Nom	94. Quatorzième Nom
15. Quinzième Nom	31. Quinzième Nom	47. Quinzième Nom	63. Quinzième Nom	79. Quinzième Nom	95. Quinzième Nom
16. Seizième Nom	32. Seizième Nom	48. Seizième Nom	64. Seizième Nom	80. Seizième Nom	96. Seizième Nom

Vouw eerst hier – Fold here first – Pliez d’abord ici – Zuerst hier falten

2... BeVoting: Fonctionnement

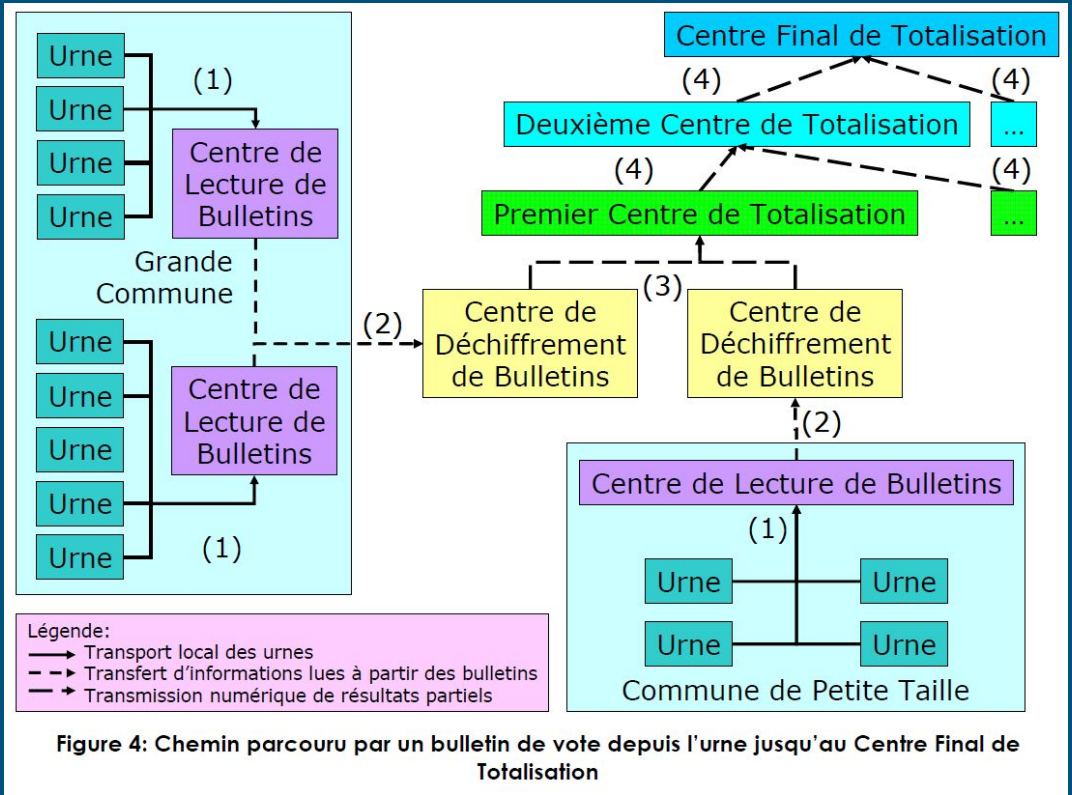


Figure 4: Chemin parcouru par un bulletin de vote depuis l'urne jusqu'au Centre Final de Totalisation

2.... BeVoting: Matériel Off the Shelf

Figure 7: Equipement présent dans l'isoloir (bulletins à code à barres)

2..... BeVoting: Caractéristiques

- Ordinateurs standards (COTS)
- Bulletin hybride RFID ou Datamatrix
- Preuve papier (VVAT)
- Démarrage par média Read-Only (CD-ROM)
- Urne passive
- Centre de décryption
- Pas d’audit (Risk Limiting Audit)

3. HELIOS (2009)

Système de vote par internet avec vérification End to End

Utilisé (entre autre) pour l’élection du recteur de l’UCL

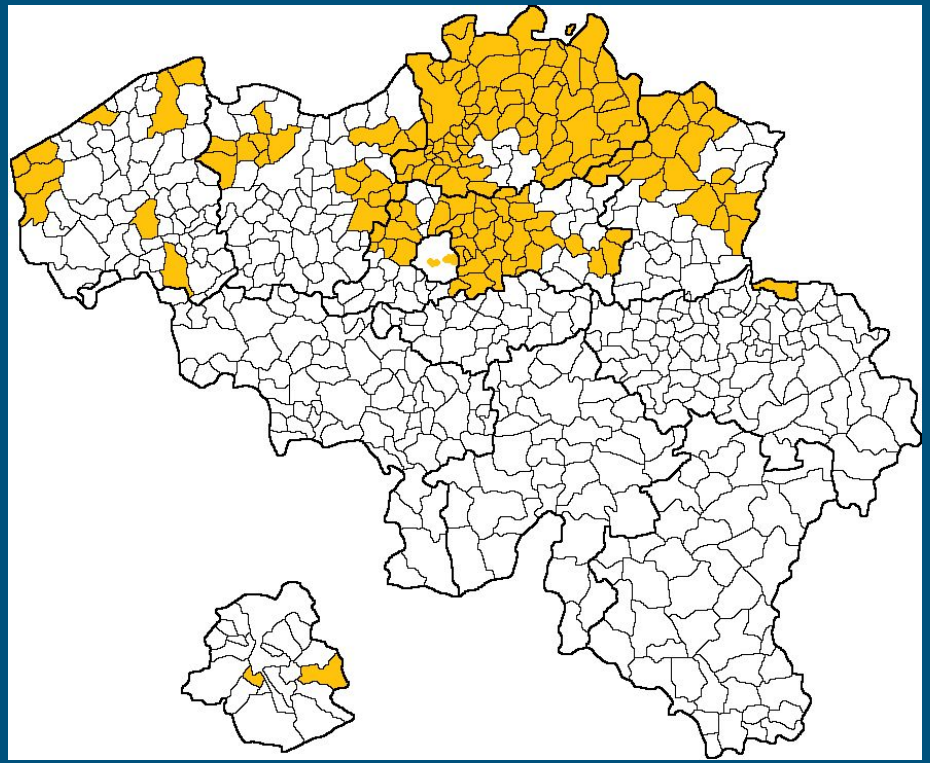
Avec la participation de Olivier Pereira (professeur de cryptographie à l’UCL)

4. Vote électronique avec “preuve” papier

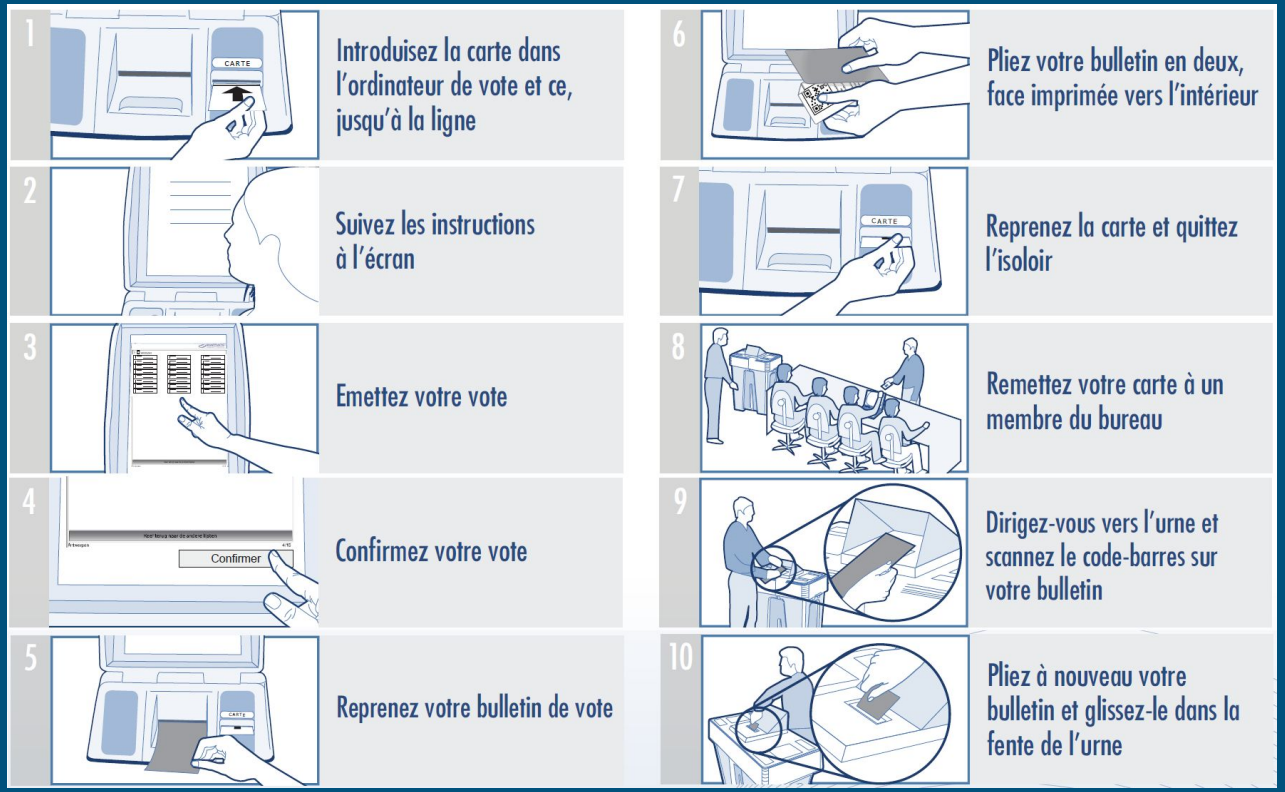
= BeVoting modifié

- 14 octobre 2012: 50% de la Flandre, Saint-Gilles et Woluwé-Saint-Pierre
  - Décret/Ordonnance différentes pour utiliser les machines
  - Problèmes de double click en Flandre
  - Problème choix du parti à Woluwé-Saint-Pierre
- 25 mai 2014: 50% de la Flandre, Saint-Gilles et Woluwé-Saint-Pierre
  - Loi fédérale pour utiliser les machines
- Bruxelles veut étendre: Leasing plutôt que achat.
- Les Germanophones veulent continuer le vote électronique

4.. “preuve” papier: carte 2012/14



4… “preuve” papier: Mode d’emploi



4…. “preuve” papier: Caractéristiques

- Ordinateurs propriétaires (Smartmatic)
- Bulletin hybride QR code
- Preuve papier (VVAT)
- Démarrage par clef USB
- Urne active (scan les bulletins)
- Pas de centre de décryption
- Pas d’audit (Risk Limiting Audit)

5. Le jour où la Belgique a buggé

http://www.medor.coop/bug

6. STAR-Votes: Secure, Transparent, Auditable, & Reliable

Août 2011 EVT/WOTE*: Dana DeBeauvoir (Travis County Clerk) Keynote speech: “We’re going to design a new voting system from scratch and we need your help.”

Avril 2012: Premier meeting au Texas

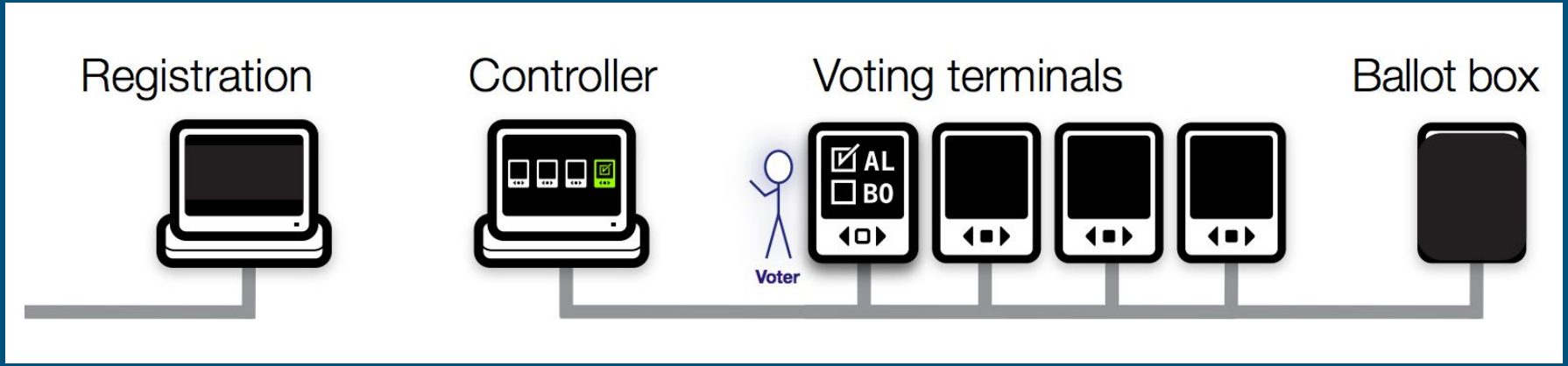
Août 2013: EVT/WOTE*: Présentation de la solution STAR-Vote

Octobre 2016: STAR-Vote™ Request for Proposal Released

* EVT/WOTE: Electronic Voting Technology Workshop/Workshop on Trustworthy Elections

6.. STAR-Votes

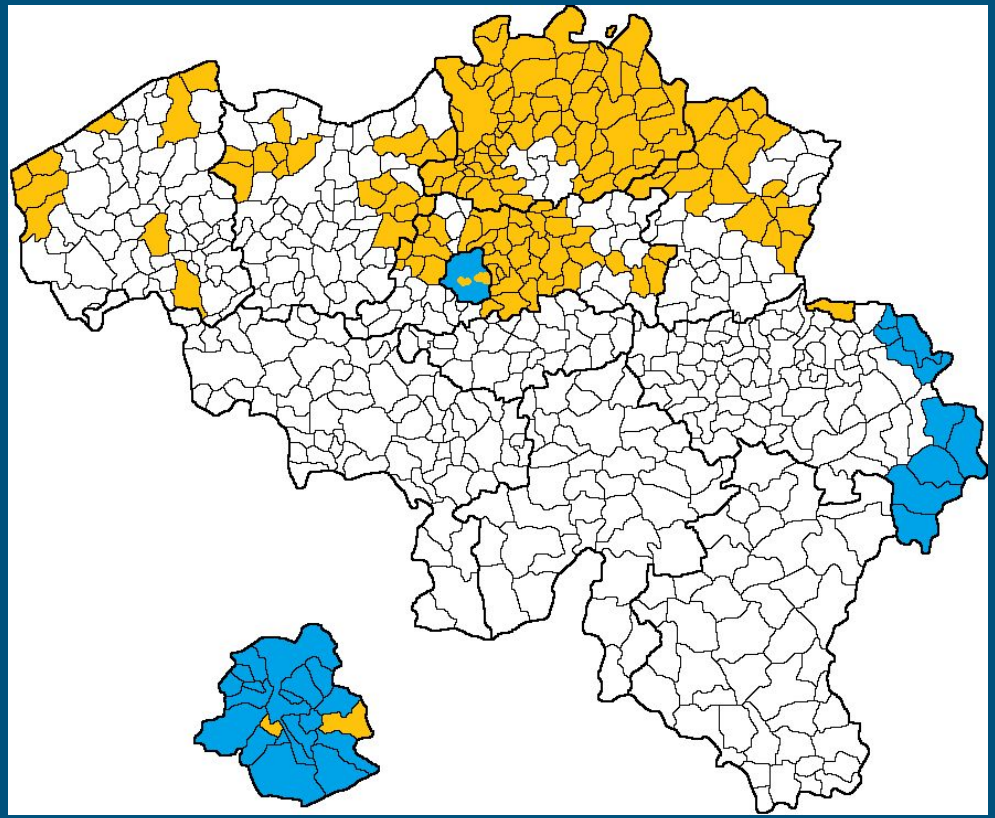
Ballot control station transmits ballot information to the voting device. All secured storage devices in the polling location are continuously updating each other with all voting data, creating multiple redundancies. Prezi link



6... STAR-Votes

- Vote anywhere
- Off-the-shelf hardware
- **Hash chaining, massive data replication**
- E2E cryptography
- Homomorphic verifiable tallies
- Public bulletin board
- Risk-Limiting Audits
- Usability (and accessibility)
- Voter Verified Audit Trail (ballot summary)
- Open Source

7. “preuve” papier: carte 2018/19



Problèmes Belgo-Belges

- Nombre d’élus, complexité du bulletin => taille des bulletins (Bruxelles)
- Trouver des assesseurs^H^H^H^H^H^H^H^H^H^H témoins de parti
- Qui décide des détails du système de vote
- Observateur non partisan
- Déplacement des urnes
- Vote multiple et secret du vote
- Différent niveau de pouvoir responsables
- Publicité des résultats
- Audit des résultats
- Bulletin de vote de Schrödinger

Questions?

Il ne viendrait par exemple à personne l’idée saugrenue de privatiser le dépouillement d’une élection «sur papier».

Vérifiable ne veut pas dire vérifié.