Gawaboumga

Geste de savoir

Tribune : Vote électronique ou vote papier

30 mai 2022

Table des matières

Introduction

Dans cette tribune, nous allons revenir sur le mode de scrutin par vote électronique et tenter de dresser le portrait des avantages et inconvénients de cette technique par rapport au mode de scrutin classique, dit *papier*. Nous jugeons nécessaire de rappeler qu'une tribune présente des idées, avis, ou critiques laissés à la responsabilité de leurs auteurs; sachant qu'ils ne sont généralement pas experts dans le domaine abordé.

La première question que l'on peut se poser est "Quelles sont les garanties qu'un mode de scrutin doit apporter ?". À priori, nous pensons que tout le monde sera d'accord sur les points suivants:

— Unicité du vote.
— Anonymat du vote.
— Assurance de la prise en compte de son vote.
— Tous les votes exprimés ont été comptabilisés.

À cela, d'autres garanties peuvent être envisagées, mais davantage orientées au concept de démocratie:

— Les individus peuvent s'informer auprès de sources transparentes et pluralistes.
— Ils peuvent participer au débat public et aux élections et peuvent donc décider de manière effective de leur avenir.

Ou celles qui posent davantage débat et liées au mode de scrutin employé:

— Sincérité du vote.
— Confiance dans le fonctionnement du scrutin, transparence et possibilités de fraudes.

Nous reviendrons plus en détail sur ces derniers points.

1. Vote électronique

Lorsque l'on parle de vote électronique, on distingue deux grands modes de fonctionnements différents: les urnes électroniques et le vote par Internet.

Les urnes électroniques reprennent l'infrastructure du vote papier, les gens sont donc plus familiers avec la procédure. Elles présentent trois avantages par rapport au vote par Internet:

— La sincérité du vote par la présence de l'isoloir.
— La réduction de la fracture numérique.
— La possibilité d'offrir un contre-contrôle avec un vote papier.

À l'inverse, le vote par Internet offre plusieurs intérêts:

— Pas de déplacement à effectuer jusqu'au bureau, ni d'attente.
— Accessibilité aux personnes à mobilité très réduite, ou bloquées par une obligation quelconque.
— Pas d'infrastructure à mettre en place, *tout le monde* possède un ordinateur.

Outre ces points, le vote électronique offre l'accessibilité aux malvoyants, ils peuvent brancher un casque pour effectuer leur choix au lieu de donner procuration. On pourrait imaginer des systèmes pour également satisfaire les besoins des manchots, comme des pédales ou des contrôleurs à base du souffle.

Une question que soulève le vote par Internet est la sincérité du vote. En effet, comment vérifier qu'il s'agit bien du vote en pleine âme et conscience de la personne? Subit-elle des pressions familiales lors de celui-ci? L'isoloir offre le cadre de se retrouver seul face à sa décision (qui risque de sortir, un jour, à un repas, mais ce n'est pas spécifique au vote électronique).

Anonymat et unicité

Mais dans le fond, comment peut fonctionner le vote électronique d'un point de vue technique?

Afin de garantir l'anonymat et le secret du vote, David Chaum a développé, dans les années 80[1], le concept de *blind signature*. Pour l'anecdote, il développera même une monnaie digitale 20 ans avant le Bitcoin! La *blind signature* est une forme de signature numérique dans laquelle le contenu du message est "caché" avant d'être signé. Un tiers peut donc vérifier que la signature correspond bien au message "caché" mais seul l'émetteur de la signature peut s'assurer qu'il s'agit bien de son message originel.

Il y a bien sûr des technicités à considérer mais l'idée consiste à :

1. On vote.
2. On met le vote dans une enveloppe en papier carbone de telle sorte que si quelqu'un écrit dessus, l'écriture soit répliquée sur le contenu de l'enveloppe (ici le vote).
3. On envoie cette enveloppe dans une autre enveloppe à la personne en charge des élections.
4. Elle ouvre le courrier, signe la lettre carbonée et la renvoie sans même l'avoir ouverte.
5. Le votant peut alors ouvrir sa lettre carbonée, constater la présence de la signature et renvoyer son enveloppe en papier carbone au dépouillement.

6. Le dépouillement peut s'assurer que le vote est valide par la présence de la signature de la personne en charge des élections.

Ce genre de propriété est souvent associée au concept de *zero-knowledge proof*, le secret (ou un dérivé direct), qui identifierait la personne, n'a pas besoin d'être échangé. Ce qui est échangé est indistinguable de l'aléatoire mais n'aurait pas pu être généré par une autre personne (avec une probabilité très faible, comparable au fait de trouver le mot de passe de la personne au hasard).

Tous les votes exprimés sont comptabilisés et vérification que son vote est bien repris

Mais là où est toute la magie, c'est que le système de comptabilisation des votes est capable de lire le vote pour le prendre en considération, mais il n'est pas attaché à une personne, il est bel et bien anonyme.

Maintenant pour s'assurer que son vote a été pris en considération. On peut regrouper des votants par paquet et appliquer une *multi-signature*[2], l'idée étant que chaque intervenant peut vérifier que sa signature a bien été prise en compte.

Pour les problèmes liés au fait que tous les votes exprimés ont bien été comptabilisés, il existe un champ de la cryptographie qui s'attarde aux problèmes de faire collaborer différentes parties en vue de calculer une fonction sur toutes les entrées, tout en garantissant le fait que ces entrées restent privées. Ce sous-domaine est dénommé : *Secure multi-party computation* suite aux travaux de Yao en 1982[3].

Précautions

Attention, nous ne sommes nullement experts en cryptographie. Nous montrons uniquement qu'il existe des solutions connues, depuis un certain temps (40 ans), pour résoudre les différents problèmes techniques que l'on peut rencontrer dans le cadre du vote électronique. Ce n'est pas pour autant que chaque concept ait été prouvé et éprouvé, à tous les types d'attaques possibles et inimaginables. Il est même possible que la combinaison de ces différents concepts ne soit pas possible en pratique.

Ce que nous voulons surtout mettre en évidence, c'est que la technique n'est peut-être pas ce qui empêcherait le passage au vote électronique. Il y a d'autres facteurs à prendre en considération.

1. CHAUM, David. Blind signatures for untraceable payments. In: Advances in cryptology. Springer, Boston, MA, 1983. p. 199–203.
2. DIFFIE, Whitfield et HELLMAN, Martin. New directions in cryptography. IEEE transactions on Information Theory, 1976, vol. 22, no 6, p. 644–654.
3. YAO, Andrew C. Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (sfcs 1982). IEEE, 1982. p. 160–164.

2. Une histoire de confiance

Nous avons vu dans la partie précédente comment il serait éventuellement possible d'organiser un vote électronique. Seulement, le problème est beaucoup plus profond. Il faut une expertise du domaine pour comprendre son fonctionnement, être capable de déceler les failles éventuelles et de prouver de manière formelle qu'il n'existe aucune attaque possible.

Même si les algorithmes mis en œuvre étaient corrects, leur implémentation serait potentiellement buguée. Pire que cela, quelles garanties avons-nous au niveau de l'ordinateur en lui-même, au niveau de l'affichage, du contrôleur ou du réseau?

Même parmi les informaticiens, les gens sont généralement perdus par ces problèmes d'audit et de certification qui requièrent des compétences expertes, qui ne peuvent être toutes maîtrisées en même temps. La vérification doit s'effectuer à plusieurs niveaux:

— Les algorithmes de cryptographie sont-ils absents d'attaques?
— Le code écrit est-il valide, est-ce que l'implémentation se comporte comme prévu (vérification formelle/synthèse de code)?
— Les logiciels sont-ils la parfaite représentation du code, ont-ils été bien compilés, le compilateur lui-même est-il certifié?
— A-t-on des certitudes sur la suite des logiciels lancés au démarrage jusqu'au lancement de l'application de vote?
— Existe-t-il des protections matérielles contre la modification du logiciel? Ces procédures sont-elles elle-même vérifiées? Peut-on altérer la machine?
— Peut-on certifier la machine et ses composantes? Comment s'assurer que le vecteur d'attaque n'est pas dans le silicone lui-même?

On peut aussi considérer la situation sous les deux angles. Il est plus facile de crier à la fraude électorale en présence de cette boîte noire, prouver l'inexistence de quelque chose est toujours bien plus difficile que l'existence. À l'inverse, si la boîte est parfaite, pourquoi ne pas l'employer dans des régions où les résultats sont souvent disputés?

C'est vraiment la combinaison des deux facteurs que sont la complexité inhérente et le manque de transparence qui sont un frein à l'adhésion de ce mode de scrutin.

Conclusion

Le vote électronique ne semble pas un problème en soit, puisque techniquement possible et mis en pratique dans de nombreux pays. Le problème réside dans la confiance du vote électronique et non dans le vote électronique en lui-même. Pourrait-on imaginer un monde intermédiaire où l'individu choisit le mode de scrutin qui lui convient le mieux? Cela permettrait d'avoir un groupe témoin par la même occasion et éventuellement détecter les fraudes plus facilement (attention au biais d'échantillonnage, les jeunes seront davantage en faveur du vote électronique).

Nous avons remis sous la forme d'un tableau les principaux arguments associés à chaque mode de scrutin.

Vote électronique Vote papier

Vote électronique	**Vote papier**
Moins de logistique (surtout dans le cadre du vote électronique), dans la production et le transport des votes, du rassemblement des individus pour organiser le scrutin et compter les résultats de l'élection.	Infrastructure plus lourde mais 'classique/habituelle', absence de gestion du parc, coûts de l'impression, affranchissement et mobilisation humaine.
Rapidité du dépouillement.	Processus fastidieux sur plusieurs jours.
Plus écologique (si par Internet), pas de déplacements, d'infrastructure, uniquement de l'électricité potentiellement "verte".	Surimpression et suppression des votes pour chaque candidat (on peut bien sûr prévoir un nombre plus adéquat sur base des sondages ou des résultats aux dernières élections).
Auditabilité particulièrement difficile à effectuer ou fournir des preuves de la fraude ou de son absence.	Système particulièrement simple (même si audité par des comités internationaux).
Incompréhension du fonctionnement par le commun des mortels (même si les gens emploient un micro-onde sans connaître le fonctionnement).	Tout le monde peut comprendre aisément le fonctionnement du scrutin.
Méconnaissance sur l'usage du mode du scrutin.	Familiarité avec le papier.
Problème de la sincérité du vote dans le cas du vote par Internet.	Garantie de l'isoloir (sinon même problème dans le cadre du vote postal).
Potentielle fracture numérique au prix d'une accessibilité accrue aux personnes porteuses d'un handicap (visuel ou moteur).	Système de procuration, pas de risque de fracture numérique.
Pouvons-nous envisager l'usage d'un vote électronique connu comme "sécurisé" dans des pays moins regardant sur la démocratie?	Confiance plus facile à acquérir ainsi qu'à maintenir et assurer

Le vote papier est avant tout "une" solution, simple et efficace, sur laquelle tout le monde peut se baser. Tant que les nouveaux modes de scrutin ne proposent pas un avantage suffisamment intéressant, le statu quo reste la meilleure solution.