Le vote citoyen et la technologie blockchain - État de l'art

BAPTISTE VÉRÉ

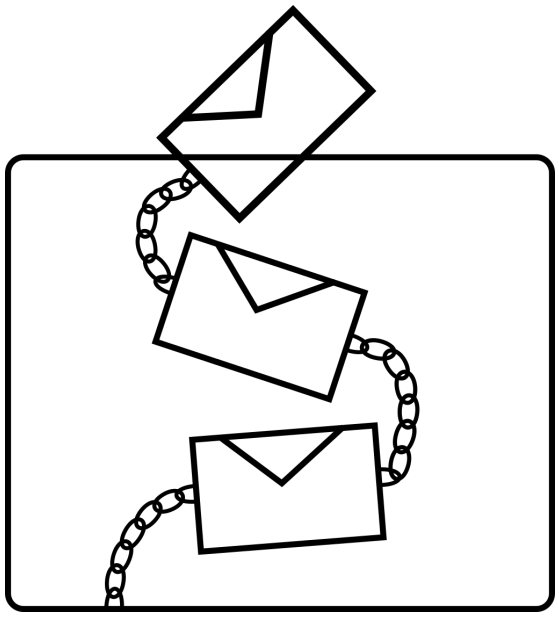

Fig. 1. Le vote par blockchain

Ce document présente un état de l'art concernant les systèmes de vote utilisant la technologie blockchain. Il présente les enjeux et discute des solutions proposées jusqu'à maintenant, de leurs promesses ainsi que de leurs limitations. Les éventuelles possibilités de recherches pour des mises en place futures seront abordées également. Le sujet étant à la fois technique et sociétal, ces deux aspects sont abordés dans ce document.

CCS Concepts: • **Voting / election technologies**;

Additional Key Words and Phrases: information security, blockchain, vote, voting system

Author's address: Baptiste Véré, baptistevere@orange.fr.

Table des matières

1 INTRODUCTION

Le vote est une solution complexe à un problème très simple à exprimer : comment faire participer plusieurs personnes, voire toute une population, à une décision commune ? Il advient que l'acte de vote permet cette décision. Loin de nous satisfaire de cette constatation, il convient de s'intéresser au déroulement d'un tel vote. En effet, la manière utilisée pour voter est très importante, et a un impact réel sur les décisions qui peuvent être prises, ainsi que la perception du vote par les électeurs.

2 TERMES UTILISÉS

Certains termes sont couramment utilisés pour plusieurs usages. Il convient donc de les définir ici clairement. Dans cet article, nous conviendrons des termes suivants :

Définition des termes

système de vote classique	système technique utilisé aujourd'hui pour la plupart des élections, c'est-à-dire l'utilisation de bureaux de vote, d'isoloirs, d'urnes, et les principes d'émargements, de dépouillements, etc.
mode de scrutin	ensemble des règles qui déterminent ce que les électeurs peuvent voter et le choix qui est effectué à l'issue du vote, en fonction de ce qui a été voté par les électeurs

Bien que les deux puissent s'influencer, on distinguera les éléments qui font la procédure électorale des conditions du scrutin.

3 CARACTÉRISTIQUES DES SYSTÈMES DE VOTE

Un vote, pour être utile en pratique, se doit de satisfaire un certain nombre de critères. Nous étudierons ici les critères suivants :

— authentification
— anonymat
— intégrité
— vérifiabilité

Certains de ces critères sont actuellement respectés par les systèmes de vote classique, mais ce n'est pas forcément le cas de tous.

On notera que les utilisations de moyens cryptographiques sont soumises à des critères techniques pour s'assurer de leur fiabilité. Ces points seront traités dans ce document.

3.1 Authentification

Le système doit s'assurer de l'authentification de chaque électeur afin que :

— chaque personne en doit de voter puisse le faire, sans exception
— toute personne ayant déjà voté ne puisse pas voter à nouveau
— personne ne puisse s'accaparer à tort le droit de vote d'un électeur

Implémentations dans le système de vote classique. Combinaison de contrôles d'identités (papiers d'identités) et de l'émargement [11].

Implémentations dans un système de vote par blockchain. Méthodes cryptographiques de signatures. Contrôle des votes inscrits dans la blockchain.

3.2 Anonymat

Afin que les personnes suceptibles d'être mises sous pression par un entourage puisse voter librement, ou encore qu'il ne soit pas possible d'acheter des votes de manière vérifiable, il peut être nécessaire que le choix de chaque électeur reste secret.

Implémentations dans le système de vote classique. Isoloirs et enveloppes non distinguables les unes des autres. Urnes fermées jusqu'au dépouillement [11].

Implémentations dans un système de vote par blockain. Méthodes cryptographiques de chiffrement.

3.3 Intégrité

Le système de vote en lui-même (on ne parle pas ici des votes individuels), doit être protégé contre des attaques le visant directement.

Implémentations dans le système de vote classique. Surveillance du déroulement du vote par des accesseurs. Dépouillement par plusieurs équipes de scrutateurs [11].

Implémentations dans un système de vote par blockain. Sureté intrinsèque du système grâce aux mécanismes cryptographiques. Les mécanismes utilisés doivent l'être avec une grande fiabilité, et les opérations réalisées avec compétence et prudence.

3.4 Vérifiabilité

Dans le cas où un vote aurait des électeurs se sentant concernés par la sureté de leur vote, ou par l'intégrité du scrutin en lui-même, il peut être intéressant que chaque électeur puisse vérifier son vote. Cela n'est par définition pas possible dans le système de vote classique car une fois l'enveloppe dans l'urne, il est impossible de la récupérer et d'en vérifier le contenu.

D'autre part, il pourrait être intéressant que chaque citoyen puisse compter lui-même l'ensemble des votes afin de vérifier que les résultats publiés par les autorités ou les médias reflètent bien la réalité.

Implémentations dans le système de vote classique. Droits accordés à l'électeur pour qu'il puisse surveiller, à son échelle, le déroulement d'un vote (exemple : accesseurs et scrutateurs). Impossibilité de vérifier son vote (en tant qu'individu), ou les résultats complets à grande échelle.

Implémentations dans un système de vote par blockchain. Possibilité pour tout le monde de lire la blockchain à l'issue du vote, et d'en calculer le résultat. Les codes utilisés peuvent également être open source, dans le même objectif de vérifications.

Il est possible d'implémenter, ou non, la vérification des votes individuels. Il convient de décider si elle est souhaitable.

4 PROBLÈMES DU SYSTÈME DE VOTE ACTUEL

Les votes classiques, pratiqués de nos jour de manière courante, sont efficaces [14]. Ils présentent cependant plusieurs problèmes majeurs que l'on pourrait chercher à éviter.

4.1 Erreurs humaines

Le processus de vote n'étant pas automatisé, ce sont donc des élus, fonctionnaires, et citoyens volontaires qui se chargent du bon déroulement du vote.

4.1.1 Émargement. L'émargement est un principe permettant aux organisateurs de savoir qui a voté, et ainsi qui ne pourra pas revoter. Il sert également à des fins de vérifications lors du dépouillement. L'émargement est souvent surveillé par une seule personne dont c'est le rôle dans le bureau. En conséquences, les erreurs dues à un manque d'attention sont courantes et la fraude possible, dans une moindre mesure.

4.1.2 Compte. Lors du dépouillement, les scrutateurs (généralement des électeurs volontaires) procèdent au compte des bulletins. On remarque cependant qu'il est possible de frauder si quelques scrutateurs présents se sont concertés. Ces erreurs et fraudes n'ont généralement qu'un faible impact a une grande échelle. Cependant, lors d'élections à une échelle réduite telle qu'une petite commune, c'est un risque à prendre en compte.

4.2 Coûts

Un des principaux point de critiques du système de vote classique est son coût. En effet, de nombreux coûts entre dans l'organisation d'un vote, et cela à tel point qu'il est difficile d'en établir l'inventaire.

De plus, de tels coûts sont un frein évident à l'organisation des votes pour des questions pratiques. En effet, des décisions habituellement prises par des assemblées de représentants sont très fréquentes, et il parait impossible d'organiser ces mêmes votes directement par la population, non seulement car cela prendrait du temps à l'échelle individuelle, mais également pour des raisons techniques, car l'organisation de votes aussi fréquents est impossible.

4.2.1 Pour les candidats. En France, chaque candidat/parti doit lui-même imprimer ses bulletins. Cela engendre un coût, qui touche particulièrement les partis sous-représentés. C'est pourquoi certains partis se contentent donc de demander à leurs électeurs d'imprimer leurs bulletins chez eux. En conséquence, cela diminue leur visibilité et n'est pas propice à la création de nouveaux partis.

4.2.2 Pour les collectivités/l'État. Organisation du vote, coordination des volontaires, responsabilité quant à la diffusion des résultats, sont autant de points qui coûtent de l'argent à la communauté, au contribuable.

4.2.3 Pour l'électeur. Une présence physique est requise pour voter, ce qui peut être gênant lorsqu'un citoyen a un empêchement pour cause professionnelle, ou ne souhaite pas avoir à payer le transport nécessaire à son acheminement jusqu'au bureau de vote.

4.2.4 Vérification à grande échelle. Il est possible (détaillé en 3.4) pour chaque électeur de vérifier le bon déroulement d'une élection. Cependant, vérifier l'intégralité de l'élection semble impossible dans le cadre du système actuel, car une présence physique sur tout le territoire serait nécessaire.

5 MOTIVATIONS

Les motivations avancées pour une utilisation d'un système de vote électroniques sont multiples. En voici une liste non exhaustive :

— Facilité de mise en place pour un vote utilisant un mode de scrutin différent (exemple : scrutin de Condorcet) de ceux utilisés majoritairement aujourd'hui

Dans le cas d'un vote par internet :

— Permettre à plus de personnes de voter (personnes habituellement dérangées par le fait de devoir se déplacer ou stopper leur activité)
— Supprimer les contraintes géographiques (vote possible depuis n'importe quelle connexion internet)

Dans le cas d'un vote utilisant la technologie blockchain :
— Transparence des élections accrue
— Fiabilité par rapport à un vote électronique classique

6 EXEMPLES D'IMPLÉMENTATIONS

Les quatre exemples présents dans cette partie ont été réalisés dans un objectif de recherche sur le sujet. Ce sont là de véritables implémentations (ou propositions complètes), et non simplement des études théoriques.

6.1 Secure Electronic Voting System using Blockchain Technology - Kumar, D. Dwijesh, Chandini, D. V., Reddy, B. Dinesh, Bhattacharyya, Debnath, Kim, Tai-hoon

Fiche technique [10]	
nom	Secure Electronic Voting System using Blockchain Technology
auteurs	Dwijesh Kumar, D. V. Chandini, B. Dinesh Reddy, Debnath Bhattacharyya, Tai-hoon Kim
type	Article de recherche
année de publication	2018

Table 1. Fiche d'information

6.1.1 Fonctionnement. Le système qui est proposé permet à des électeurs enregistrés de voter sur un sujet quelconque choisi par la personne qui initie le vote.

Le système utilise deux blockchains :
— Une blockchain d'électeurs
— Une blockchain de votes

La première blockchain sert à stocker les informations des électeurs ainsi que de moyen d'authentification. La seconde est celle sur laquelle les votes sont inscrits, et qui sera lue pour déterminer le résultat de l'élection. Le résultat du vote n'est disponible qu'à l'administrateur, détenteur du seul compte ayant un accès en lecture complet de la blockchain de votes. On peut donc imaginer un scénario où cet accès serait rendu publique à l'issue d'une élection.

6.1.2 Pour l'utilisateur. L'interface utilisée par l'électeur est une application mobile présentant toutes les fonctionnalités nécessaires à un vote. Un électeur doit donc :
— possèder un téléphone portable compatible
— télécharger l'application sur son téléphone portable
— s'enregistrer via l'interface de l'application
— s'authentifier via l'interface de l'application
— saisir un identifiant de vote
— sélectionner le vote qu'il souhaite effectuer
— valider son vote

Lors de l'authentification, un mot de passe ainsi qu'un code PIN doivent être retenus par l'utilisateur. Par la suite, l'utilisateur peut vérifier son vote, mais pas le modifier. Seul l'administrateur est en mesure de connaitre l'issue du vote. La clé d'accès doit donc être révélée à l'issu du vote si l'on souhaite que les électeurs puissent vérifier les résultats du scrutin.

6.2 A Simple Voting Protocol on Quantum Blockchain - Sun, Xin, Wang, Quanlong, Kulicki, Piotr, Sopek, Mirek

Fiche technique [14]	
nom	A Simple Voting Protocol on Quantum Blockchain
auteurs	Sun, Xin, Wang, Quanlong, Kulicki, Piotr, Sopek, Mirek
type	Article de recherche
année de publication	2018

Table 2. Fiche d'information

En ce qui concerne les protocoles sécurisés à l'aide de moyens cryptographiques, les possibilités offertes par la maitrise de l'informatique quantique entrent en considération. En effet, si ces avancées scientifiques semblent prometteuses, elles posent néanmoins des questions quant à la sécurité de nos protocoles cryptographiques actuels. Cette étude tente d'adresser ce problème.

Le système proposé l'est surtout dans ces principes physiques. La conception du système semble complète, mais n'a pas été réalisée. Les auteurs affirment cependant que tout ce qui est présenté est faisable avec les moyens dont nous disposons aujourd'hui.

6.2.1 Fonctionnement. Le principe serait d'utiliser les propriétés d'un canal de communication quantique (QSC) pour effectuer une mise en gage. Ce type de blockchain a été expliqué dans le même journal la même année [9]. Le principe de mise en gage utilisant les propriétés de la physique quantique a été conçue et expliquée en en 1993 [2]. La mise en gage (engagement) ainsi effectuée est la pièce maitresse de l'étape de vote.

Pour le dépouillement, la méthode de l'accord byzantin est utilisée. Il s'agit d'une méthode permettant la réalisation des calculs de manière distribuée [15]. Ce dépouillement est reproductible, et le fait qu'elle soit distribuée garantie une transparence dans le compte des voix.

6.3 Voter via la blockchain : expérimentations et retours d'expérience - Romain Rouphael, Côme Jean Jarry

Fiche technique [13]	
nom	Voter via la blockchain : expérimentations et retours d'expérience
auteurs	Romain Rouphael, Côme Jean Jarry
type	Article
année de publication	2016

Table 3. Fiche d'information

En avril 2016, le parti politique *Nous citoyens* a décidé d'expérimenter le vote par blockchain lors de ses élections régionales. La société *BELEM* a été chargée de la conception de ce système. Il s'agit donc d'une société privée, contrairement aux autres implémentations traitées dans ce documents, qui émanent toutes, elles, de la recherche fondamentale.

6.3.1 Fonctionnement. Ce système utilisait la blockain Ethereum. En particulier, la fonctionnalité des smarts contracts était utilisée. Chaque vote consiste en une transaction de 0 Ethereum du votant vers un smart contract. Ce smart contract avait pour unique objectif de compter les voix pour chaque option de vote.

Le code compilé du smart contract est disponible publiquement, ce qui permet de s'assurer que les votes sont bien tous pris en compte de la même manière. Une vérification peut être effectuée par la suite en lisant la blockchain Ethereum.

6.3.2 Pour l'utilisateur. Pour procéder à son vote, l'électeur reçoit un email contenant un lien vers un site. Ce lien pointe immédiatement vers une page de sélection de vote. Après le choix de l'utilisateur, la transaction est effectuée et le vote immédiatement comptabilisé.

On peut immédiatement remarquer quelques risques :
— Compromission du site de vote
— Compromission de la boite email de l'électeur
— Compromission de la chaine d'envoi des liens

Pour ce qui est du premier point, on peut imaginer que cela s'applique à tout système de vote en ligne. En revanche, en ce qui concerne les deux autres points, notons qu'aucune authentification n'est requise, si ce n'est qu'il faut possèder la clé présentée dans l'URL envoyée par email.

6.4 Blockchain-Based E-Voting System - Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðars Mohammad Hamdaqa, Gísli Hjálmtýsson

Fiche technique [8]	
nom	Blockchain-Based E-Voting System
auteurs	Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðars Mohammad Hamdaqa, Gísli Hjálmtýsson
type	Article
année de publication	2018

Table 4. Fiche d'information

Un atout de cet article est qu'il compare l'implémentation sur plusieurs blockchains et de plusieurs frameworks. La comparaison est par exemple effectuée pour les frameworks suivants :
— Go Ethereum
— Exonum
— Quorum

Cette comparaison amène une réflexion qui n'a pas été discutée auparavant : La blockchain serait-elle en mesure d'absorber un trafic aussi important que celui d'un jour d'élection ? Les expérimentations actuelles, ou même les implémentations de cryptomonnaies, semblent très favorables à des performances meilleures que dans un système centralisé.

De plus, ces frameworks ont différentes approches à la décentralisation. Quelle serait la meilleure option ? On peut imaginer que, dans le cas d'un vote concernant des élections importantes (comme à l'échelle d'un pays), des moyens seraient mis en place pour qu'une blockchain spécialisée, et donc optimisée pour cet usage, soit mise en place.

Pour ces raisons, on peut imaginer qu'un grand nombre d'électeurs nécessiterait une blockchain spécialisée.

6.5 Autres implémentations

Les quatre précédentes implémentations ne constituent pas l'intégralité des expérimentations qui ont été réalisées dans le cadre de la recherche sur les systèmes de vote utilisant la technologie blockchain. En particulier, ces implémentations sont majoritairement issues du monde de la recherche scientifique. Cependant, comme c'est souvent le cas, en particulier dans le secteur de l'informatique, des entreprises se sont mises, de leur coté, et avec parfois des compétences déjà reconnues, à faire de la recherche sur ce sujet.

Voici une liste non exhaustive d'entreprises ayant effectuées un travail de recherche sur cette technologie, ou proposant dès à présent un service concernant le vote par blockchain :

— Follow my Vote [6]
— BELEM [1]
— NetService [12]
— Votem [16]
— Democracy Earth [4]

7 PROBLÈMES D'ACCEPTATION SOCIALE

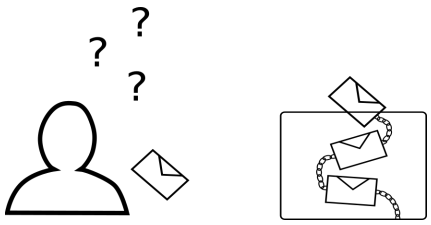

Fig. 2. Questionnement par rapport au vote par blockchain

Comme toute nouveauté scientifique ayant un impact sur la population, un vote électronique, aussi fiable soit-il, devra faire face à de nombreuses critiques et à l'incompréhension normale d'une population n'ayant pas les compétences pour juger du niveau de fiabilité d'un tel dispositif.

7.1 Pédagogie nécessaire

De nombreuses associations, ainsi que des administrations, cherchent à promouvoir le vote comme un élément central de la démocratie. Le vote souffre cependant d'un manque d'intérêt d'une partie de la population, ces personnes estimant qu'elles ont mieux à faire ou que leur seul vote n'est pas suffisamment impactant. Dans ces conditions, et même en estimant que la population comprenne parfaitement les enjeux du vote, il reste des questions concernant la meilleure approche pour enseigner l'intérêt de l'utilisation de la blockchain et le fonctionnement d'un tel système sans entrer dans des détails qui nécessiteraient des compétences spécifiques.

7.2 Coût de la mise en place

Le système de vote classique a un coût non négligeable [7]. Dès lors, on se pose la question du coût d'un vote par blockchain, comparé au système actuel.

7.2.1 Coût économique. Pour aller voter en personne dans un bureau de vote, il est nécessaire d'avoir un accès a des bâtiments, où sont organisés des bureaux. Il est nécessaire d'avoir une main d'oeuvre constituée d'élus, fonctionnaires, et de citoyens. Enfin, l'ensemble des électeurs doivent s'organiser pour se déplacer vers les bureaux

de vote, ou effectuer une procuration auprès d'un service public. Tous ces éléments sont difficiles à évaluer dans leur globalité, mais il advient qu'en comparaison, une infrastructure informatisée et surtout distribuée aurait un coût moins élevé autant à titre individuel pour le citoyen, qu'à titre collectif pour le contribuable (tout cela dans le cas d'un vote organisé par un État) [7]. Il faudra cependant faire attention à ne pas oublier le coût de bureaux de votes avec de l'informatique s'il y en a, ainsi que le coût de toute la communication et la pédagogie nécessaire autour d'un nouveau système.

7.2.2 Coût écologique. Nous pouvons imaginer qu'un vote en ligne aurait un impact environnemental moins élevé qu'un vote où une présence physique des électeurs serait requise. Cependant, peu de recherches existent actuellement sur la question, les principales recherches portant plutôt sur l'impact du numérique en général.

7.3 Gestion des litiges

Les litiges et problèmes électoraux sont par exemple traités dans le code électoral français [11]. Un bulletin de vote, une fois placé dans l'urne, ne peut bénéficier d'aucun suivi particulier (si ce n'est la surveillance de l'urne par les membres du bureaux). Cela présente des avantages, mais réduit fortement les recours envisageables en cas de litige lors d'un vote. Un vote par blockchain, en revanche, peut inclure des mécanismes permettant de vérifier qu'un vote a bien été pris en compte. Il s'agit de garanties mathématiques, difficiles à réfuter.

7.4 Vide juridique

En France, une définition de la blockchain a été donnée en terme financier dans le code monétaire et financier (Article L223-12) :

> Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État.

Cependant, si cette définition (*dispositif d'enregistrement électronique partagé*) est valable le cas de la notion de cryptoactif, elle l'est moins dans le cas d'un dispositif d'enregistrement de votes.

On peut cependant imaginer qu'un tel dispositif de vote impliquerait la création d'un cadre juridique sans précédent exposant précisément les détails non seulement fonctionnels mais également techniques de la ou les blockchains nécessaires au déroulement du vote.

8 PROBLÈMES DE SÉCURITÉ

Comme pour tout changement pouvant affecter la sécurité du vote des citoyens, le vote par blockchain amène de nombreuses réflexions par rapport à la sécurité d'un tel système. Il s'agit donc d'en analyser les risques majeurs, et de voir si chacun de ces risques peut être géré correctement, tout cela dans le but de décider si un tel système serait viable, ainsi qu'en déterminer les risques résiduels.

8.1 Risques de compromission

Dressons un portrait de la chaine nécessaire au vote électronique :

(1) électeur
(2) logiciel de vote
(3) machine(s) de vote
(4) réseau
(5) machine(s) de décompte des votes

À chaque maillon de cette chaine correspond un certain nombre de risques.

élément	**risque(s) de compromission**	**mesures envisageables**
électeur	du choix du vote	encadrement du droit à voter
logiciel de vote	de l'intégrité du programme	vérification par hash de l'intégrité du programme
		possibilité de vérifier son vote sur une autre machine
machine(s) de vote	de la confidentialité du vote	sécurisation de l'environnement de vote
réseau	de la confidentialité du vote	chiffrement
	de la possibilité de voter	mitigation des attaques par déni de service
machine(s) de dépouillement	du résutat du vote	vérification sur d'autres machines, voire de manière ouverte par les citoyens

Ces risques sont traités dans les parties suivantes. Nous pouvons cependant déjà résumer la situation ainsi :

La technologie blockchain apporte des éléments qui réduisent radicalement certains risques. Cependant, d'autres risques comme ceux concernant les électeurs ou encore l'intégrité des logiciels de vote, sont encore présents.

8.2 Usage des droits à voter

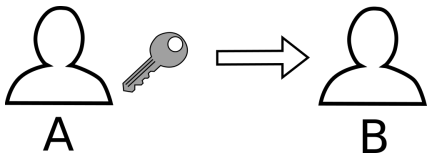

Fig. 3. transfert d'un droit à voter

Dans plusieurs implémentations, le "droit à voter" se présente sous forme d'une clé, élément maitre de l'authentification de l'électeur. Doit-on permettre à un électeur de voter avec la clé d'un autre électeur ?

Un consensus sur de telles questions semble nécessaire. En revanche, nous savons dès à présent (ne serait-ce qu'en étudiant les exemples traités précédemment dans ce document) que le ces conditions sont adaptables dans un système de vote par blockchain. Ces questions ne sont donc pas d'ordre technique mais relèvent plutôt d'une décision politique.

8.3 MITM

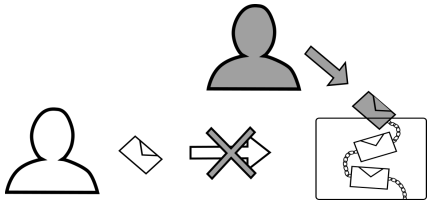

Fig. 4. attaque de type MITM

Les risques concernant les machines et logiciels sur lequel le vote sera effectué sont principalement liés à des attaques de type MITM (Man In The Middle), c'est-à-dire de situations où un attaquant chercherait à intercepter et/ou modifier le vote d'un ou de plusieurs électeur(s).

Il y a donc un choix à faire : Faut-il utiliser des machines spécifiquement conçues et installées pour le vote, par exemple, en accès libre au public, sous surveillance de fonctionnaires ou de citoyens volontaires comme aujourd'hui pour les bureaux de vote ? Ou faut-il plutôt permettre à la population de voter chez elle, puis de vérifier son vote sur une autre machine ? Ou enfin, faut-il laisser cet usage complètement libre, en pariant ainsi sur une sensibilisation générale à la sécurité informatique de la part de la population ? Si certaines de ces décisions semblent résolument plus réalistes que d'autres, elles relèvent de décisions politiques qui devront faire consensus.

8.4 DoS

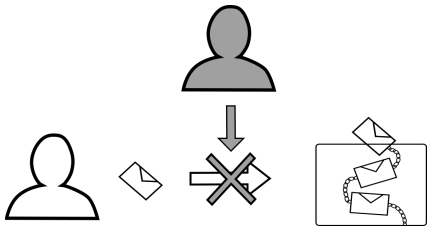

Fig. 5. attaque de type DoS

La blockchain étant par nature décentralisée, il semble particulièrement peu probable qu'une attaque par déni de service soit réalisable. Il faudra cependant veiller à une surveillance importante de la couverture internet afin que personne ne soit affecté par une coupure de service qui aurait lieu pendant toute la durée du vote.

8.5 Attaques spécifiques à la blockchain

De manière générale, dans le cas d'implémentations classiques de blockchains, il est bon de rappeler qu'il convient de ne pas laisser un acteur détenir plus de la moitié de la puissance de calcul nécessaire au fonctionnement du système. Cela pourrait en effet avoir un effet dévastateur : une seule entité serait ainsi capable de contrôler la blockchain contenant les votes [3, 5].

Néanmoins, une telle attaque est résolument détectable, et semble très peu probable dans le cas d'un vote à large échelle.

9 CONCLUSION

A d'heure où le recours au vote électronique est envisagé mais également fortement critiqué, la technologie blockchain vient apporter des éléments de solution à des problèmes de confiance, aussi bien dans la technologie que dans les institutions.

Dans tous les cas, il convient que l'utilisation, ou non, de ces systèmes de votes électroniques ainsi que leurs modalités et mesures de sécurité seront conditionnées à l'importance de chaque élection.

Les expérimentations actuelles laissent penser qu'un système de vote utilisant cette technologie est tout à fait envisageable. Cependant, en facilitant certains aspects, cette technologie pose d'autres questions, qui feront sans aucun doute partie du débat démocratique concernant le vote électronique. Dans le cas du vote *citoyen*, nous avons toutes les cartes en mains pour la construction d'un tel débat.

Liste des tableaux

Table des figures

RÉFÉRENCES

[1] BELEM. 2020. BELEM official website. https://belem.io
[2] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois. 1993. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. IEEE, Palo Alto, CA, USA, 362–371. https://doi.org/10.1109/SFCS.1993.366851
[3] Martin Della Chiesa, François Hiault, and Clément Téqui. 2019. *Blockchain : vers de nouvelles chaînes de valeur.* Eyrolles, Eyrolles. OCLC : 1103211762.
[4] Democracy Earth. 2020. Democracy Earth official website. https://democracy.earth/
[5] Jean-Guillaume Dumas, Sébastien Varrette, and Pascal Lafourcade. 2018. *Les blockchains en 50 questions : Comprendre le fonctionnement et les enjeux de cette technologie innovante.* Dunod, Dunod. http://sbiproxy.uqac.ca/login?url=https://international.scholarvox.com/book/88863925 OCLC : 1104267187.
[6] Follow my Vote. 2020. Follow my Vote official website. https://followmyvote.com
[7] Hervé MARSEILLE, au nom de la commission des finances. 2015. Le coût de l'organisation des élections. http://www.senat.fr/rap/r15-123/r15-123_mono.html
[8] Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa, and Gisli Hjalmtysson. 2018. Blockchain-Based E-Voting System. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, San Francisco, CA, USA, 983–986. https://doi.org/10.1109/CLOUD.2018.00151
[9] E O Kiktenko, N O Pozhar, M N Anufriev, A S Trushechkin, R R Yunusov, Y V Kurochkin, A I Lvovsky, and A K Fedorov. 2018. Quantum-secured blockchain. *Quantum Science and Technology* 3, 3 (July 2018), 035004. https://doi.org/10.1088/2058-9565/aabc6b
[10] D. Dwijesh Kumar, D. V. Chandini, B. Dinesh Reddy, Debnath Bhattacharyya, and Tai-hoon Kim. 2018. Secure Electronic Voting System using Blockchain Technology. *International Journal of Advanced Science and Technology* 118 (Sept. 2018), 13–22. https://doi.org/10.14257/ijast.2018.118.02
[11] legifrance. 2020. Code électoral en vigueur en France. https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070239
[12] NetService. 2020. NetService "crypto-voting". https://www.netservice.eu/en/research-and-development/crypto-voting
[13] Rouphael Romain and Jean Jarry Côme. 2016. Voter via la blockchain : expérimentations et retours d'expérience. https://www.frenchweb.fr/voter-via-la-blockchain-experimentations-et-retours-dexperience
[14] Xin Sun, Quanlong Wang, Piotr Kulicki, and Mirek Sopek. 2019. A Simple Voting Protocol on Quantum Blockchain. *International Journal of Theoretical Physics* 58, 1 (Jan. 2019), 275–281. https://doi.org/10.1007/s10773-018-3929-6
[15] Xin Sun, Quanlong Wang, Piotr Kulicki, and Xishun Zhao. 2018. Quantum-enhanced Logic-based Blockchain I : Quantum Honest-success Byzantine Agreement and Qulogicoin. *arXiv :1805.06768 [quant-ph]* (July 2018). http://arxiv.org/abs/1805.06768 arXiv : 1805.06768.

[16] Votem. 2020. Votem official website. https://www.votem.com

A CADRE DE CETTE ÉTUDE

Cet état de l'art a été réalisé en tant que projet de veille technologique dans le cadre de la première année de cycle ingénieur en cyberdéfense à l'ENSIBS.

B LICENCE

Fig. 6. Licence