Auteur×ices, relecteur×ices : redoublons de prudence face aux effets de modes technologiques

Enka Blanchard, Fabrizio Li Vigni, Pablo Rauzy

Critique de l'article de Serge Surin "Le renouveau de la promesse du vote électronique. Étude du vote par chaîne de blocs au regard du système électoral français"

Enka Blanchard[a,b,c*] Fabrizio Li Vigni[a,d*] Pablo Rauzy[e,f*]

Abstract

Dans un article paru dans *Amplitude du droit* le 21 juin 2022, le juriste Serge Surin élabore une défense du vote électronique reposant sur la chaîne de blocs (CDB) ou blockchain. Cet article commet de nombreuses erreurs méthodologiques, notamment par sa gestion des sources — utilisation non critique de propagande d'État et de produits publicitaires — ainsi que par une certaine incompréhension des technologies étudiées. Ayant l'habitude de travailler aux interfaces disciplinaires, nous souhaitons sonner l'alarme sur de telles pratiques, facilitées par l'analyse d'un outil technologique sans collaborer avec les personnes ayant l'expertise nécessaire. Nous proposons donc ici une critique et une réfutation détaillée, et interrogeons la rigueur du mécanisme d'évaluation par les pairs censé avoir eu lieu.

1 Synthèse

Dans le premier numéro publié en 2022 de la nouvelle revue *Amplitude du droit*, portée par l'Université de Rennes, le CNRS et la Maison des Sciences de l'Homme, l'un des articles en Varia porte sur la technologie de la blockchain (ou chaîne de blocs, CDB) et sur son application au vote électronique, se basant notamment sur l'exemple du vote de 2018 dans l'État américain de la Virginie Occidentale. Écrit par le juriste Serge Surin (Université Sorbonne Paris Nord) et intitulé "Le renouveau de la promesse du vote électronique. Étude du vote par chaîne de blocs au regard du système électoral français", cet article[1] pose plusieurs problèmes méthodologiques et de fond que nous analysons dans ce texte. Parmi ces problèmes, on compte pêle-mêle une gestion inappropriée des sources — académiques ou pas — une invitation à enfreindre certains droits humains, l'absence d'approche critique vis-à-vis de la CDB, une mauvaise compréhension des caractéristiques, des risques et des limites de cette technologie, ainsi qu'un biais politique libertarien non annoncé et non contrôlé. Bien que certaines conclusions de l'auteur puissent être correctes, le manque de rigueur sur un sujet aussi sensible que le vote dans un article publié dans une revue universitaire pourrait avoir des conséquences dangereuses.

Notre premier but dans ce document est de mettre en garde le lectorat de la revue et le comité de rédaction lui-même contre les discours acritiques et inexacts, voire incantatoires, qui circulent dans plusieurs milieux sociaux autour de la CDB, et qui ont été reproduits tels quels dans l'article.

*Les auteurs et autrice ayant contribué à part équivalente, les noms sont en ordre alphabétique.
[a] CNRS, Centre Internet et Société, UPR 2000
[b] Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines, UMR 8201, UPHF,
[c] Chaire d'Intelligence Spatiale, UPHF
[d] Sciences-Po Saint-Germain-en-Laye
[e] Laboratoire d'Intelligence Artificielle et Sémantique des Données, Université Paris 8
[f] Centre GÉODE (Géopolitique de la Datasphère), Université Paris 8

[1] Une version de l'article archivée quelques jours après sa publication originale est consultable ici : https://web.archive.org/web/20220627130338/https://amplitude-droit.pergola-publications.fr/index.php?id=295.

Ensuite, nous souhaitons soulever les failles du processus d'évaluation par les pairs de la revue. Avant de rentrer dans l'analyse détaillée des paragraphes problématiques de l'article, nous offrons en introduction une synthèse des principaux problèmes que nous avons relevés.

Le premier problème de l'article concerne la gestion des sources, mal choisies, mal comprises et mal restituées. L'utilisation de sources non universitaires n'est pas en soi un problème[2] et est souvent nécessaire dès lors qu'on traite de sujets ayant un impact sur l'actualité. Cependant, l'usage de ces sources doit être approprié, et ne doit pas se faire au détriment de sources scientifiques évaluées par les pairs — quand elles existent. De plus, cet usage doit être critique, notamment sur les biais éventuels présents dans ces sources. L'article que nous critiquons ici ne suit aucune de ces règles. Tout d'abord, un nombre important de sources ne peuvent pas être considérées comme fiables : rapports écrits par des think tanks ayant des conflits d'intérêts, billets de blog anonymes, article publié par Sputnik (média d'État russe régulièrement accusé de propagande)… Ajoutées aux articles de presse généraliste (dont certains sont des éditoriaux politiques rédigés par des lobbyistes), elles forment près de la moitié des sources citées dans l'article. Cela est d'autant plus grave que certaines références standard sont entièrement ignorées, comme l'ouvrage de Werbach [Wer18] ou celui écrit par De Filippi et Wright [WDF18], d'ailleurs proche politiquement des arguments énoncés par Serge Surin[3]. Cela mène à une deuxième faute méthodologique : sur certains sujets, l'auteur se contente de ces sources non critiques. Par exemple, pour deux des élections mentionnées, l'auteur cite des sources gouvernementales, de l'entreprise qui a été chargée de la mise en œuvre du scrutin, ou encore de la presse généraliste favorable, délaissant les articles scientifiques critiques [GG20, SKW20] (alors même que ceux-ci ne sont pas controversées au sein de la communauté scientifique). Les arguments de vente de certains think tanks ou entreprises favorables à la CDB sont aussi acceptés par l'auteur sans être remis en question.

Plusieurs éléments indiquent aussi que l'auteur ne maîtrise pas les principes des technologies qu'il étudie. Tout d'abord, il définit le vote électronique comme totalement dématérialisé alors qu'il n'en est rien, et tend à magnifier l'impact de la CDB sur celui-ci. Cela repose de toute évidence sur une mauvaise compréhension de la technologie CDB, en tant que telle mais aussi par rapport à d'autres technologies de vote électronique. L'auteur souligne aussi à plusieurs reprises que la CDB permet la désintermédiation, mais ne mentionne pas les plateformes intermédiaires qui gèrent les crypto-actifs et fait l'impasse sur les tiers de confiance qui seraient nécessaires pour prévenir la coercition et l'achat des votes dans la solution qu'il préconise lui-même. Même sur la question du secret du vote (technologie ancienne s'il en est), l'auteur fait des contresens sur la sincérité du scrutin. Il utilise aussi une citation de Pierre Martin sortie de son contexte pour attaquer le secret du vote, alors même que la phrase suivant la citation dans le livre original attaquait justement cette interprétation (voir le paragraphe 26, dans la section suivante). L'auteur entretient aussi un flou et ne définit jamais une partie des termes centraux de son article. À aucun moment ne donne-t-il de définition rigoureuse de ce qu'il entend par *vote par chaîne de blocs* — alors que plusieurs interprétations sont possibles, par exemple selon que la CDB ne serve que de support à un vote cryptographique ou que le vote soit transparent et que la CDB serve de registre. Il ne mentionne jamais le *modèle* de sécurité dans lequel il se place — le type d'attaque et d'attaquant potentiel et les buts envisageables — pratique pourtant standard dès que le vote électronique est traité académiquement sous l'angle de la sécurité.

Lorsque l'article montre — à de rares reprises — une précaution vis-à-vis de la CDB, celle-ci est

[2] Sans parler des sources institutionnelles qui ont une valeur spéciale en droit.

[3] Cet ouvrage fut l'objet de critiques — similaires à celles que nous formulons ici — à cause de son approche techno-solutionniste et de partis pris libertariens sur les liens entre innovation et régulation [QBGF19].

systématiquement démentie peu après lorsqu'il soutient que les critiques à la CDB risquent d'arrêter le progrès sous-entendu comme un bien en soi. Les quelques mises en garde contre les risques de la CDB que l'auteur prend en compte ne l'empêchent pas d'affirmer que le cas d'étude qu'il a choisi représente un succès — sans preuve à l'appui. Nous relevons à cet égard deux problèmes idéologiques : d'une part, Serge Surin mentionne dans quelques passages l'esprit libertarien qui accompagne le déploiement de la CDB, notamment en matière de crypto-actifs, sans toutefois se positionner explicitement à ce sujet ; d'autre part, l'auteur glisse dans le techno-solutionnisme si bien décrit par Evgeny Morozov dans son livre *Pour tout résoudre, cliquez ici : l'aberration du solutionnisme technologique* [Mor14]. Cette position — souvent adoptée implicitement — consiste à croire que tout problème a une solution technique ; de plus, la fascination pour une nouvelle technologie peut amener ses soutiens à en chercher des applications aberrantes pour la justifier. Elle facilite aussi les comparaisons entre des systèmes "innovants" non testés (et donc idéalisés) et des systèmes existants présentés comme moins performants — alors que les analyses théoriques de ces derniers sont parfois encore meilleures, le problème étant toujours la mise en pratique. L'ensemble de ces positions problématiques portent Serge Surin à des affirmations dangereuses en matière politique et éthique. Certaines chaînes de blocs, avec les *smart contracts*, permettent d'automatiser certains types de contrats ainsi que des sanctions en cas de non-respect de ceux-ci. L'auteur donne comme exemple de rendre un réfrigérateur inaccessible à un locataire mauvais payeur, sans semble-t-il réaliser que cette "solution" va à l'encontre de certains droits humains (ni que, techniquement, une CDB n'est ni nécessaire ni suffisante à la mise en œuvre de tels procédés).

Nous ne souhaitons pas ici attaquer l'auteur sur une question de principe, et partageons d'ailleurs certaines de ses positions. Notamment, un argument central soutenu dans la conclusion est qu'il est important d'analyser voire d'avoir un débat — universitaire ou public — sur ces technologies. Cette position est tout à fait raisonnable. Cependant, vu le danger social et politique que ces technologies peuvent représenter, nous insistons que cette analyse doit se faire dans la plus grande rigueur, potentiellement au sein d'équipes interdisciplinaires à l'expertise mixte couvrant les différents aspects critiques afin de limiter les inévitables biais. Or cette rigueur n'est pas présente dans le cas de l'article critiqué. De plus, même quand ces collaborations sont difficiles, il semblerait logique de faire à minima relire et critiquer son article par des collègues des disciplines concernées — ce que nous avons naturellement fait pour cette réponse.

S'il revient à l'auteur de l'article de vérifier ses sources, de faire une analyse critique de son objet et de respecter la rigueur du travail scientifique, on s'étonne surtout du fait que les évaluateurs de la revue aient laissé passer un texte contenant autant de problèmes analytiques, techniques et éthiques. Étant donné la surcharge de travail de nombreux évaluateurs (dont les efforts ne sont pas rémunérés), quelques références de mauvaise qualité peuvent très facilement se glisser dans un bon article sans être repérées. L'analyse détaillée de la section suivante n'a donc pas pour objectif d'attaquer l'auteur de manière répétée, mais de montrer l'ampleur des incohérences et problèmes méthodologiques, qui n'auraient pas dû passer une évaluation rigoureuse.

Ceci n'est absolument pas une attaque contre le modèle éditorial de la revue — *diamond open access*, que nous soutenons — mais plutôt une interrogation sur les sources de cet échec critique de l'évaluation par les pairs. Ceci montre peut-être à nouveau les limites de l'évaluation anonyme quand cet anonymat des évaluateurs limite leur responsabilisation[4].

[4]Naturellement, cet anonymat est aussi un garde-fou face à certains abus. Cependant, d'autres modèles existent, par exemple celui où l'évaluation en double aveugle est remplacée, en cas d'article accepté, par une vignette affichant le nom des évaluateurs sur l'article publié (potentiellement accompagnée de ses évaluations) — permettant à la fois responsabilisation et mise en valeur de ces derniers, tout en protégeant les évaluateurs critiques.

2 Analyse détaillée

Cette section analyse l'article original paragraphe par paragraphe, en pointant les défauts, en citant quand nécessaire les passages problématiques.

Paragraphe 1 :

> L'objectif de cette analyse n'est pas de revenir sur le sujet, mais de mettre en lumière les avancées technologiques en la matière qui conduisent à interroger le système de vote classique en temps de crise.

La première question est : de quelle crise parle-t-on ? Est-ce une crise de confiance envers les systèmes démocratiques, est-ce la crise de l'abstention, est-ce le Covid et son impact sur les élections ? L'article mentionne à plusieurs reprises cette dernière crise, mais mentionne aussi les problèmes de confiance (note 5). Or il semble étrange de répondre à une crise de confiance envers le système démocratique par l'adoption d'outils qui ne sont pas transparents ou compréhensibles — pour l'immense majorité de la population — et décriés par une grande partie des experts. D'ailleurs, un problème central ne semble pas être la sécurité des élections elles-mêmes[5], mais plutôt la situation politique forçant un choix entre plusieurs alternatives dont aucune ne satisfait une majorité de la population.

Par souci d'exhaustivité, il faut souligner qu'un argument souvent utilisé (mais pas dans cet article) pour souligner la supériorité du vote électronique — et du vote par Internet — est l'économie d'échelle. Or, cet argument ne semble pas viable en pratique. Que ce soit pour l'élection utilisant Voatz en Virginie-Occidentale ou pour le vote de la primaire populaire, les votes par internet coûtent entre 1 et 3€ par inscrit. Par comparaison, les élections nationales en France coûtent autour de 150M€, dont plus de 75% pour la propagande électorale et le remboursement des campagnes[6] (qui subsistent peu importe la technologie utilisée)

Paragraphe 2 :

> En effet, si tous les systèmes de vote électronique partagent des caractéristiques communes, comme un fonctionnement basé sur des « systèmes informatiques », « sans bulletin papier » et donc totalement « dématérialisé »

Une grande partie des systèmes de vote électronique utilisés aujourd'hui ne sont justement pas dématérialisés — et même un système de pure CDB aurait une composante matérielle non négligeable [Mus18]. Les machines avec audit papier ou les machines électroniques qui remplissent et impriment un bulletin sont courantes aux USA [Sel04, OvdB04, CCC+08, Coh05].

L'auteur parle pour la première fois de "vote par chaîne de blocs" sans bien définir le terme, ce qu'il ne fera pas explicitement dans la suite de l'article. On ne peut que deviner ce qu'il voudra dire par cela, en se basant sur les exemples cités (comme le système Voatz).

[5] Le système électoral français est aujourd'hui hautement sécurisé, par un principe simple : l'usage de bulletins papiers empêche un attaquant de faire des économies d'échelle. Pour faire du bourrage d'urne, il faudrait donc corrompre des assesseurs dans de nombreux bureaux, ce qui est moins économiquement viable que d'acheter des voix dans la plupart des cas.

[6] Voir par exemple https://www.senat.fr/rap/r15-123/r15-123_mono.html#toc6 pour les élections de 2012.

Paragraphe 3 :

> Les débats sur le vote électronique ont, pour ainsi dire, été ravivés par l'avènement de la nouvelle technique de vote par la chaîne de blocs (ou blockchain)

Ces débats ont lieu en continu depuis plusieurs dizaines d'années, et la CDB a eu un effet relativement limité sur le vote électronique comparé à d'autres outils. Par exemple, on ne la trouve mentionnée dans aucun titre parmi les 255 articles publiés dans les proceedings de la conférence principale sur le vote électronique (du point de vue informatique) — aujourd'hui l'International Joint Conference on Electronic Voting (E-VOTE-ID), née de la fusion en 2016 de l'International Conference on E-Voting and Identity (VoteID) et de l'International Conference on Electronic Voting (EVOTE). Une recherche sur Google Scholar montre que la plupart des articles proposant du vote électronique par CDB viennent de revues ou actes de conférences ou bien spécialisés sur la CDB et le cloud ou bien généralistes, avec très peu d'articles s'adressant aux spécialistes de sécurité ou de vote électronique.

Paragraphe 4 :

> Précisons d'emblée que vote électronique à distance et vote par chaîne de blocs vont de pair, la chaîne de blocs n'est qu'une technologie plus élaborée, ou plus complexe, qu'une simple plateforme de vote en ligne

Tout d'abord, cela n'est pas vrai au sens où l'immense majorité des systèmes de vote électroniques ne dépendent pas de la CDB, la réciproque n'étant pas vraie. De plus, la CDB est une technologie relativement simple reposant sur deux concepts : la présence d'un registre partagé et un mécanisme de mise à jour du registre qui maintient un accord entre les différents acteurs du système distribué. Ses avantages sont souvent mal compris, notamment dans le contexte du vote où un registre public (mis à jour de manière centralisée) est souvent suffisant. Un système de vote en ligne basique (qui se souvient juste d'un email par exemple) est en effet plus simple. Cependant, ces derniers ne sont pas recommandés pour les élections, et les systèmes de vote sécurisés (comme helios ou belenios) sont beaucoup plus complexes qu'une CDB dans le sens conceptuel du terme et nécessitent des compétences plus avancées en cryptographie. Cela n'est d'ailleurs pas un point positif en général : une technologie plus élaborée et plus complexe sera à priori moins compréhensible et transparente, un désavantage pour un outil démocratique.

> La principale particularité du vote par chaîne de blocs ne réside pas tant dans son impossibilité sans l'usage d'Internet, qui permet à la technologie qui l'accompagne de fonctionner, que dans le niveau élevé de sécurité qu'on lui prête.

On lui *prête* un niveau de sécurité élevé. Il dépend donc de l'auteur de vérifier cette assertion, et d'en faire une analyse critique (avec des sources universitaires de qualité). Nous reviendrons sur ce point qui fait défaut au long de l'article. Dans un contexte de sécurité informatique, il faudrait d'ailleurs définir le sens de sécurité — contre quelles attaques ? quels types d'acteurs ? dans le but d'empêcher quelles actions ?

Paragraphe 6 :

> la Commission d'enrichissement de la langue française refuse l'appellation anglo-saxonne blockchain pour aborder la notion de « chaîne de blocs », équivalent, selon le contexte, à « monnaie électronique », « pair à pair », « preuve de travail », « validation de bloc »,

Ce n'est pas le cas et ces notions ne sont pas équivalentes. Dans la source citée par l'article [Com17], les termes correspondant sont *cryptocurrency*, peer-to-peer, *proof-of-work*, *block validation*. Il n'y a donc pas une notion floue de "chaîne de blocs" et c'est clairement explicité dans la source citée.

Paragraphe 7 : Les références citées dans ce paragraphe ne sont ni neutres ni universitaires. Au contraire, la référence principale vient d'une tribune écrite par deux think tanks (le Jade Group et l'Observatoire de l'ubérisation — qui semble sur son site être pro-ubérisation). Les deux autres références sont un livre publié par un groupe commercial pro-CDB et enfin un livre publié à compte d'auteur écrit par Thomas Cambrai. Ce dernier est aussi l'auteur de "Devenir riche en 3 mois sans capital et sans prise de risque" et "Dropshipping : Comment générer 2000 euros par mois de revenus passifs en partant de RIEN !". Enfin, la notion de "copie infalsifiable" défendue dans la première citation ne veut pas dire grand chose. Tout d'abord, il n'est pas nécessaire d'avoir une CDB pour obtenir la propriété que toute modification est visible — cette propriété est standard à la fois dans Git (un des outils centraux dans le développement logiciel) et est une brique de base de nombreux systèmes cryptographiques sous le nom de public bulletin board. De plus, les derniers blocs d'une chaîne sont régulièrement réécrits lors du mécanisme de consensus.

Paragraphe 8 :

> Chaque transaction apparaît sur le registre public, dès lors que l'utilisateur respecte le protocole. Une blockchain publique supprime tout intermédiaire de confiance,

La première partie n'est pas une garantie, car il se peut qu'aucun mineur n'inscrive notre transaction dans un bloc (par exemple si on offre des frais de transactions trop bas). Surtout, la deuxième partie n'est pas exacte si on ne parle pas d'une cryptomonnaie. Le lien entre le monde réel et la CDB dépend du fait que l'ensemble des parties s'engagent à respecter des règles. La seule vérité qui est garantie par l'écriture d'une information sur une CDB, c'est que l'information en question est écrite sur la CDB en question[7]. Ce qui est justement suffisant pour les cryptomonnaies, mais pas pour la plupart des autres utilisations de la CDB.

Paragraphe 11 :

> la chaîne de blocs qui utilise des plateformes « inviolables » où les données sont cryptées supprime tout intermédiaire, y compris, et surtout, l'État.

L'auteur ne précise pas les plateformes en question, ou la notion de sécurité dont il parle. De plus, ces plateformes forment justement des intermédiaires, tout comme le reste de l'infrastructure d'Internet, nécessaire pour le fonctionnement de la chaîne. L'usage est d'ailleurs d'utiliser chiffrer et chiffrement plutôt que crypté/cryptage.

[7] Cette phrase est tirée de https://p4bl0.net/post/2021/06/La-v%C3%A9rit%C3%A9-sur-la-blockchain

> La logique de la chaîne de blocs est l'exécution automatique et systématique des contrats et accords entre personnes sans possibilité de contourner les termes de ces conventions par des habiles et stratégiques interprétations, à condition que lesdits termes soient clairs.

L'auteur mentionne l'esprit libertarien, sans se positionner explicitement à ce sujet. Cependant, il donne plusieurs indicateurs. Tout d'abord par ses tournures : les protections qu'offrent la justice par rapport aux contrats inéquitables (voire frauduleux) deviennent "des habiles et stratégiques interprétations". Ensuite, il part du principe que le contrat peut se suffire, et que l'interprétation n'est pas essentielle [Cov85], alors que le droit n'est pas (encore) automatisable. Le point crucial est que l'aspect automatique va à l'encontre des garde-fous justement établis par le droit. Le côté définitif nuit aussi à la réparation des dommages causés par les nombreuses escroqueries parfois entièrement légales dans le milieu des CDBs, comme celle ayant détruit le DAO en 2016 [MSG+19], mais aussi plus récemment sur le Beanstalk[8] et sur Pancake Bunny[9]. Il ne parle à aucun moment de ces dangers, y compris lorsqu'il mentionne l'expérience de la carte d'identité électronique en Estonie sans parler des problèmes de sécurité liés à l'expérimentation là-bas, justement sur le vote [Vin15].

Paragraphe 12 :

> Actuellement, un locataire de mauvaise foi peut demeurer pendant des mois, voire des années, dans un logement sans payer les loyers. De la même manière, un propriétaire indélicat peut encaisser des loyers pendant des mois, voire des années, sans réaliser les travaux nécessaires qui sont à sa charge. Le contrat intelligent viendrait alors supprimer les contentieux devant les tribunaux d'État, trop tolérants envers les personnes de mauvaise foi, en rendant le logement inutilisable (coupure d'électricité, lumières éteintes, portes condamnées, réfrigérateur inaccessible, etc.) pour le locataire récalcitrant ; et, de même, en rendant impossible le transfert des loyers sur le compte du propriétaire qui n'exécute pas les travaux nécessaires dans le logement.

Ce passage a de nombreux problèmes. Tout d'abord, au moins une des propositions mentionnées — condamner les portes et rendre le réfrigérateur inaccessible — va à l'encontre des droits humains (selon les interprétations), tout d'abord de l'article 8 du titre 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950, mais surtout de l'article 1 du protocole additionnel de 1952. Ensuite, l'auteur met sur un plan égal deux pertes très différentes : la perte d'un logement et celle d'une rente. La raison pour laquelle les contentieux peuvent être longs est que la justice doit garantir le respect des droits des personnes vulnérables — notamment le respect du chapitre V du Code de l'action sociale et des familles[10] et du droit au logement opposable. Les délais ne sont donc pas dûs à un manque technique mais à la nécessité légale de respecter la dignité humaine. On s'étonne que des juristes, l'auteur autant que ceux ayant participé à l'évaluation par les pairs de l'article et au comité éditorial de la revue, aient laissé passer une telle illustration. Toutes les choses mentionnées sont possibles aujourd'hui mais explicitement interdites par le droit, le

[8] https://www.theverge.com/2022/4/18/23030754/beanstalk-cryptocurrency-hack-182-million-dao-voting

[9] https://www.cryptoninjas.net/2021/05/20/45m-gone-in-a-flash-loan-attack-how-scammers-exploited-vulnerabilities-in-pancake-bunnys-smart-contract-code/

[10] Voir par exemple https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000031130667/.

problème n'étant pas l'inefficacité de l'appareil judiciaire mais la présence d'une protection allant au delà du droit du contrat — et dans une perspective libertarienne, c'est celle-ci qu'on veut éliminer.

De plus, l'auteur ne convainc pas sur le plan technique : non seulement les exemples de sanctions donnés ne nécessitent pas une CDB pour être mises en œuvre — un compteur connecté Linky suffit pour couper l'électricité à distance — mais en plus une CDB n'est pas suffisante à leur mise en œuvre. L'automatisation de la procédure est techniquement envisageable sans CDB ni smart contracts, simplement en liant des notifications de transactions bancaires au système informatique du fournisseurs d'électricité. De plus, une CDB avec smart contracts ne peut avoir d'effet ici que si le fournisseur d'électricité honore la requête effectuée par le smart contract, il reste donc un intermédiaire de fait dont ne permet pas de se passer la technologie dont il est ici question.

> Évidemment, la chaîne des transactions en blocs montrerait plus facilement qui a failli le premier dans la chaîne d'exécution du bail et qui doit être déclaré responsable.

C'est extrêmement peu probable sauf si tout est numérisé (y compris les paroles entre locataire et propriétaire), avec une garantie d'absence de bug. De plus, une CDB ne montrerait que l'ordre dans lequel les actions y ont été inscrites. Dès lors qu'il ne s'agit pas de sa propre cryptomonnaie, pour laquelle l'écriture dans une chaîne de bloc est performative, rien ne garantit que ce qui est écrit dans une CDB correspond à une réalité quelconque (on peut y inscrire que des travaux ont été réalisés même s'ils ne l'ont pas été, on peut ne pas y inscrire le paiement d'un loyer si celui-ci a été fait autrement que par la cryptomonnaie de la CDB en question, on peut aussi inverser l'ordre, etc). Le seul moyen de garantir cela est de recourir à un tiers de confiance servant d'autorité extérieure, mais cela défait complètement l'utilité du recours à une CDB.

Paragraphe 13 :

> on pourrait imaginer que le Conseil constitutionnel n'ait plus à rédiger des centaines de décisions après chaque élection législative grâce à l'impossibilité des fraudes habituelles constatées

Tout comme le paragraphe précédent, ce paragraphe part du principe que tout marcherait parfaitement dans le nouveau système. On oppose alors une version idéalisée de l'alternative à la réalité actuelle. Or les systèmes électroniques ont tout autant d'irrégularités que les systèmes basés sur le papier. D'ailleurs, pour ceux utilisés en France, le taux d'irrégularités est hautement supérieur [EG14]. De plus, un certain nombre de "fraudes" sont entièrement indépendantes du scrutin, comme par exemple l'affaire de l'affichage temporaire de résultats erronés par la chaîne France 2 le soir de l'élection présidentielle française de 2022. L'absence de précision et de référence sur les "fraudes constatées" complique l'analyse. Un autre problème est que l'appareil judiciaire ne se saisit pas toujours des problèmes de vote électronique, potentiellement par manque de compétence technique [BLG+22].

Paragraphe 14 :

> Cette question qui appelle une réponse prophétique est difficilement appréhendable par l'analyse juridique dans la mesure où cette modalité de vote n'est pas juridiquement définie

Cette modalité précise de vote n'est certes pas définie en droit français, mais entre dans la catégorie du vote par Internet qui a un encadrement légal [Com19]. Il y a aussi une confusion entre le vote par CDB et le vote à distance, catégorie plus globale qui en effet a des avantages en période de crise sanitaire.

Paragraphe 15 :

> Bien que les critiques qui bloquent le vote électronique en France depuis les années 1960-70 n'aient pas cessé, cette modalité d'expression démocratique n'a pas non plus cessé d'évoluer et de gagner du terrain à l'étranger

L'auteur n'est pas neutre : les critiques bloquent, elles empêchent le progrès — par opposition à l'expression démocratique. Il faut de plus souligner que le vote électronique pur (inventé par Thomas Edison au départ, mis en oeuvre depuis très longtemps, avec une utilisation généralisée depuis les années 1980 auxÉtats-Unis) a évolué vers des systèmes hybrides permettant un audit papier, notamment aux États-Unis grâce aux travaux de Rebecca Mercuri [Mer00].

Paragraphe 16 : L'auteur suggère que l'expérience de vote en Virginie Occidentale est un succès apparent et donc que la critique n'est pas légitime, mais n'en donne pas de preuve par la suite (ou de source fiable).

Paragraphes 18-19 :

> Malgré la véhémence des détracteurs de ce choix politique majeur et osé, le site du secrétaire d'État de la VO explique dans une vidéo rodée que le vote par CDB, qui est extrêmement encadré, est une réussite.

L'auteur prend clairement parti en faveur du vote par CDB, avec l'expression ci-dessus. On oppose aux critiques une "vidéo rodée" selon laquelle le vote est extrêmement encadré et est une réussite. Les "détracteurs" ont au moins un semblant de neutralité — le groupe "verified voting" étant une association se prétendant non-partisane, principalement universitaire et à but non lucratif visant à garantir la sécurité du vote. Cependant, le secrétaire d'État — au pouvoir depuis 2017 — a un intérêt fort à décrire son propre travail comme étant une réussite, tout comme la société organisatrice, aussi citée comme source au paragraphe 19. On a donc d'un côté une vidéo promotionnelle et un discours politique assurant que tout se passe bien. De l'autre côté, l'auteur ne mentionne qu'un site, sans même expliciter l'article précis dont il parle — plusieurs articles étant consacrés à cette élection.

Le problème principal ici est que l'auteur échoue doublement à adopter une approche critique. Tout d'abord, les arguments de vente sont acceptés sans être remis en question. Ensuite, les critiques sont passées sous silence. L'auteur oublie justement un article établissant de nombreuses vulnérabilités dans le système de vote utilisé [SKW20]. Cet article est important à plusieurs titres : il montre les faiblesses du système, il est cité à de nombreuses reprises (y compris par le groupe "verified voting") et il a mené à l'arrêt de l'utilisation de Voatz par la Virginie Occidentale et d'autres acteurs gouvernementaux. L'auteur oublie aussi de mentionner les autres articles universitaires critiques [PSNR21], ainsi que les appels publics et les articles de presse dénonçant les pratiques controversées des entreprises vendant les logiciels de vote[11].

[11] Voir https://www.aaas.org/programs/epi-center/internet-voting-letter ouhttps://cointelegraph.com/magazine/2020/02/07/safe-harbor-or-thrown-to-the-sharks-by-voatz.

Paragraphe 20 :

> D'abord, le vote est sécurisé car il va directement dans la chaîne blocs jusqu'au soir de la journée de la tenue de l'élection, ensuite, l'électeur reçoit une copie de son bulletin rempli par courriel, ce qui lui permet de vérifier la validation de son vote

Il n'est nulle part montré en quoi la première partie garantit la sécurité — ou plutôt l'intégrité du vote. De plus, que veut dire la deuxième partie ? Le courriel reçu indique-t-il le vote ? Si oui, ce système n'empêche nullement la coercition ou l'achat de votes. Sinon, à quoi ce reçu sert-il ? Et de toute façon, sans plus d'information, comment garantir que le courriel correspond d'une manière ou d'une autre au vote envoyé au secrétaire d'État ?

Paragraphe 23 :

> les critiques demeurent intactes dans la mesure où les mineurs chargés de valider les blocs d'opérations de la chaîne peuvent certainement avoir accès au contenu du vote et à l'identité de son émetteur de l'autre côté de l'écran

On ne peut qu'espérer que ceci est une mauvaise interprétation de l'auteur et qu'il n'en est rien. Le principe d'une CDB étant d'être distribuée, si les mineurs ont accès à ces informations, alors elles sont complètement publiques, ce qui détruirait entièrement le secret du vote. C'est d'ailleurs une opposition entre certains systèmes de vote par CDB et les systèmes de vote cryptographiques, où les acteurs intermédiaires n'obtiennent aucune information sur les données (par différents mécanismes de chiffrement). On a encore une fois une confusion entre une CDB où chaque vote serait enregistré en clair, ce qui serait difficilement altérable mais irait directement à l'encontre du secret du vote, et une CDB où les votes sont chiffrés, comme annoncé au 11ème paragraphe.

Dans la note 13, l'auteur parle enfin des critiques contre l'expérience de Voatz en Virginie Occidentale. Il ne cite cependant aucune source universitaire, ayant recours à Vanityfair, Digital Trends, Citylab, et IT Chronicles. De plus, ces sources ne sont pas elles-mêmes critiques mais sont plus souvent des articles écrits en réponse aux critiques. Pour terminer avec un dernier exemple de mauvaise qualité des sources, la seule référence citée est un blog d'aide à la spéculation en cryptomonnaies — alors que des sources de presse grand public existaient, comme Les Échos[12].

Paragraphe 24 :

> Cette critique du vote par CDB s'inscrit donc dans un contexte plus global, celui du traitement algorithmique des décisions publiques.

Ça ne semble absolument pas être le cas, et la citation donnée ensuite ne fait aucun rapprochement entre le problème des décisions politiques prises algorithmiquement et le vote par CDB.

Paragraphe 25 : L'auteur exprime plusieurs assertions sans les justifier, comme l'impact de Black Lives Matter sur l'élection américaine de 2020, ou l'impact du vote à distance sur la participation.

[12] Voir https://www.lesechos.fr/tech-medias/hightech/orange-lance-son-systeme-de-vote-securise-par-la-blockchain-238444.

Paragraphe 26 :

> Si l'on se cantonne au secret du vote, qui demeure un cadre absolu en France, ce traitement informatique, algorithmique ou mathématique ne convient pas aux scrutins politiques.

Cette assertion est vraie, mais pour des raisons différentes de celles qui sont sous-entendues ici. L'état de l'art du vote électronique sait tout à fait garantir le secret du vote par rapport aux tiers que sont les assesseurs ou la plateforme de vote. Ce qui n'est pas soluble, c'est l'isoloir : à partir du moment où le vote peut avoir lieu sur n'importe quelle machine connectée à internet, on ne peut pas contrôler qui est présent ou non aux côtés de l'électeur pendant qu'il vote puis jusqu'à la fin du scrutin (une façon de mitiger le problème de potentielle coercition étant d'autoriser les électeurs à voter plusieurs fois et à ne prendre en compte que le dernier de leur vote).

De plus, l'auteur utilise à nouveau comme source des écrits d'opinion dans de la presse grand public sur les élections législatives de 1993, qui sont moins catégoriques que son propre argument.

> Mais, comme l'a soulevé ce même auteur, pour certains, le secret du vote serait immoral « car il permettrait à certains de céder à des opinions indignes ou trop égoïstes qu'ils n'auraient osé soutenir en public » (2006, p. 19)

L'auteur est ici trompeur sur l'argument de sa source Pierre Martin. Dans l'extrait cité — page 20 et non pas 19 — le mot "certains" désignant à priori des partisans du roi. De plus, P. Martin continue immédiatement en affirmant [Mar06] :

> Mais en fait, derrière l'accusation d'immoralité, il y avait certainement la crainte de ne plus pouvoir vérifier si l'électeur remplissait bien le « contrat électoral » pour lequel il avait été éventuellement soudoyé.

Cet argumentaire rejoint les débats du milieu du 19ème siècle au Royaume-Uni où certains politiciens comme Lord William Russell se battaient contre l'adoption du bulletin secret car contraire à l'esprit anglais et indigne d'un homme [Kin78]. Lord William Russell était d'ailleurs membre du parlement, élu à Tavistock où sa famille possédait la grande majorité des terres depuis plus d'un siècle — et disposait donc d'un contrôle presque complet sur les élections par son influence locale[13]. De l'autre côté de l'Atlantique, l'évolution ayant mené à l'adoption du bulletin secret aux États-Unisétait d'ailleurs causé en bonne partie par deux scandales d'achat massif de votes [Jon03, Kin01].

Paragraphe 27 :

> le vote par CDB serait préférable pour la sincérité du scrutin mais pas pour le secret du vote.

L'auteur commet un contre-sens. La sincérité du scrutin correspond normalement à la capacité de l'électeur à voter comme il le souhaite au sens politique (sans coercition notamment, ou achat de voix). Avec un vote secret, l'électeur peut voter comme il le souhaite, sans révéler son allégeance politique, et le vote n'est que l'expression de sa volonté (et non pas de contraintes ou de récompenses). Sans vote secret, exprimer ses préférences a un coût réel, et il risque donc de ne pas voter (ce qui arrivait à la fin du 19ème siècle) ou de voter pour autre chose (de manière insincère donc,

[13] Voir https://www.historyofparliamentonline.org/volume/1820-1832/constituencies/tavistock

souvent par coercition). Encore une fois, l'auteur malmène les propos de sa source. Si la mise en place du bulletin secret a en effet "pu être utilisée contre la démocratie, afin de restreindre la participation des noirs aux élections dans le sud des États-Unis à partir de 1888", ce n'était qu'une des excuses pour instaurer des tests d'alphabétisme dont les blancs étaient souvent dispensés et n'était en lui-même pas source de cette discrimination [Sha93].

Paragraphe 28 : Si le vote secret pourrait hypothétiquement être dépassé dans le cadre d'une nouvelle sphère démocratique, l'auteur ne mentionne pas que cette possibilité semble difficile à réaliser tant que les réalités économiques ont un impact sur la politique, permettant l'achat d'élections dans de nombreux pays [CÏ13, FRS18].

Paragraphe 29 :

> ce n'est pas tant le risque d'erreur technique lors du vote électronique qui est un problème que l'impossibilité pour le juge d'accéder aux éléments lui permettant d'assurer un contrôle des opérations de vote (2018, p. 384) sans l'intermédiaire de spécialistes dont il ne comprend pas forcément les méthodes de travail.

Encore une fois, on entre en contradiction avec ce qui était affirmé plus haut dans l'article, notamment au paragraphe 13. Cependant, si on admet ce qui est dit ici, on ne peut pas se passer de tiers de confiance, ce qui remet en question l'utilité de la CDB.

Paragraphe 30 : Tout d'abord, la référence citée (G. Koubi, 2015) n'est pas présente dans la bibliographie. Ensuite, l'auteur fait une nouvelle erreur en mélangeant vote par CDB et vote électronique. Le système utilisé en Russie était bien par CDB, mais sur une chaîne privée ne disposant pas des avantages des chaînes publiques.

Enfin, l'auteur franchit un nouveau cap dans la gestion des sources. La seule référence assurant que les élections russes se sont bien passées venant de Sputnik, l'agence de presse du gouvernement russe régulièrement accusée de n'être qu'un outil de propagande [Glo22, Wat18]. Enfin, il mentionne un succès malgré les failles dénoncées par un français, sans mentionner les travaux de ce dernier, y compris ceux montrant que les failles n'avaient pas été réparées [GG20].

Paragraphe 31 :

> la pratique de plus en plus fréquente des consultations en ligne initiées par l'État (1.2.2), désormais soutenues par les menaçantes crises provoquées par des pandémies comme la Covid-19.

Cette pratique avait été fortement dénoncée, par exemple par la lettre ouverte citée plus haut[14], mais l'auteur n'en parle pas.

Paragraphe 32 : L'auteur parle notamment de Neovote, qui a étendu ses activités aux primaires des présidentielles, mais vu les délais de publication on ne peut lui reprocher de ne pas être au courant des derniers développements [BLG+22]. Cependant, il semblerait logique de citer les rares décisions de justice portant sur ce sujet (notamment [Coua] et [Coub]).

[14] https://www.aaas.org/programs/epi-center/internet-voting-letter

Paragraphe 33 : Le choix du vocabulaire est encore très loin d'être neutre (projet de loi *avorté* [italique dans l'original]), sans donner plus d'information ou de sources sur les raisons de l'abandon du projet de loi.

Paragraphe 36 :

> Si le Conseil d'État appelle les pouvoirs publics à « compenser le point faible de cette technologie [à savoir la CDB], qui est la certification de la relation entre le monde réel et le monde virtuel

Cette remarque pertinente du Conseil d'État n'est pour l'instant par résoluble techniquement sans tiers de confiance, qui par leur existence annulent l'intérêt d'avoir recours à une CDB.

Paragraphe 39 :

> le législateur a défini des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme

Il n'est pas évident qu'un scrutin électronique soit assimilable à une décision administrative individuelle, et il faudrait donc argumenter en ce sens pour étayer l'affirmation de l'auteur. Il n'est d'ailleurs pas évident qu'un scrutin électronique rentre dans la catégorie d'une décision prise sur le fondement exclusif d'un algorithme.

Paragraphe 41 :

> Ces signaux positifs du côté des tribunaux chargés de contrôler le respect des principes fondamentaux des modalités de vote sont complétés, outre le système de soutien aux RIP qui vient d'être évoqué, par les expériences consultatives et participatives en ligne qui ont tendance à s'imposer aux pouvoirs publics.

Il est justement intéressant de voir que ces expériences ont tendance à s'imposer malgré des signaux négatifs du côté des tribunaux, en partie à cause de la complexité technologique associée [BLG+22].

Paragraphe 43 : L'auteur cite un discours politique datant de plusieurs années ayant des annonces, sans revenir sur le fait que plusieurs des promesses citées dans le paragraphes n'auront pas été tenues.

Paragraphe 45 :

> il reconnaît que des voix s'élèvent pour demander « à ne pas brider l'innovation et à tirer les enseignements de l'usage des "blockchains" avant de légiférer »

L'auteur s'engage encore une fois politiquement en défense d'une expérimentation technologique sans garde-fou.

Paragraphe 47 :

> il se pourrait que cette modalité de vote devienne incontournable de la même manière qu'Internet est devenu indispensable dans le quotidien des individus (2.2).

Une différence notable est que l'exercice d'un droit citoyen doit se faire avec le moins possible de contraintes. La numérisation de certaines tâches est donc une possibilité tant qu'il existe une manière de s'y soustraire. Or les systèmes de vote par internet sont rarement compatibles avec un vote papier hybride.

Paragraphe 49 : Ce n'est pas Internet qui est géré par l'ICANN, mais la répartition des noms de domaine, ce qui limite fortement son impact. De plus, citer Laurent Alexandre comme spécialiste en IA est un non-sens : ce dernier est urologue de formation, entrepreneur du numérique (fondateur de doctissimo), militant libertarien pro-solutionnisme technologique, et s'exprime parfois sur l'IA en tant que militant et non pas spécialiste.

Paragraphe 50 :

> en théorie en effet, l'ICANN peut tout simplement effacer, en un clic, l'ensemble des ressources d'un État ou rendre inaccessibles toutes les adresses en ".fr"

Cette assertion est fausse, et l'ICANN a un pouvoir assez limité. Tout d'abord, l'impact principal de l'ICANN serait de couper un pays du reste (son Internet national fonctionnerait bien, mais les échanges dans les deux sens seraient plus complexes). Pas question donc de supprimer l'ensemble des ressources d'un État ou même de les rendre inaccessibles pour les personnes vivant au sein de cet État. De plus, il suffirait d'avoir un DNS privé pour ignorer une partie de ces effets. Enfin, l'ICANN n'est généralement pas prêt à prendre ces mesures, même en temps de guerre[15] [Zal19].

Paragraphe 51 : Dans la note 28, l'auteur utilise encore une fois des sources de qualité discutable, ici une interview sur la chaîne youtube Thinkerview. Cette dernière présente de nombreuses interviews critiques de qualité variable, accusée de confusionnisme[16].

Paragraphe 52 :

> le problème de la gestion du Web demeure intact au regard de la souveraineté des États, ce qui, pour le moment, plombe l'idée d'un vote souverain à tous les niveaux d'un État par le biais de la CDB.

Le lien entre la gouvernance technique d'Internet et la souveraineté d'un vote par CDB est pour le moins ténu, et semble à partir d'ici être, aux yeux de l'auteur, le principal souci qui se pose concernant ce mode de scrutin.

[15] Voir notamment https://news.bloomberglaw.com/tech-and-telecom-law/why-we-cant-disconnect-russia-from-the-internet et https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf.

[16] Voir par exemple https://www.liberation.fr/checknews/2019/09/04/pourquoi-la-chaine-youtube-thinkerview-bloque-t-elle-des-internautes-sur-twitter_1748982/ ou https://www.multitudes.net/extreme-droitisation-confusionnisme-et-emancipation-batman-contre-zemmour-et-poutine/.

Paragraphe 55 :

> Les CDB publiques, dites sans permissions, c'est-à-dire ouvertes à toutes et tous, sont considérées comme pouvant être « l'incarnation de valeurs politiques et sociales, comme la transparence et la redistribution du pouvoir » (Boucher, Nascimento, Kritikos, 2017, p. 6).

Cette affirmation provient d'un rapport parlementaire européen qui prend notamment comme source, au sujet du vote électronique par CDB, un lobby américain libertarien ("Follow My Vote") dont l'objectif est principalement de promouvoir le vote par CDB.

Paragraphe 56 :

> Selon un spécialiste

Le "spécialiste" dont il est ici question est l'auteur (non identifié) d'un article de blog sur le site bitcoin.fr, qui est tenu par des enthousiastes de cette technologie.

Paragraphe 57 :

> Comme la CBD ne fonctionne pas à l'aide d'un organe central de contrôle, à l'instar de traditionnels registres de comptes bancaires ou de cadastres, les experts affirment que

La citation qui suit est issue du même rapport parlementaire européen qu'au paragraphe 55, et est elle même douteuse (l'utilisation du mot "légitimité" y est ambiguë). Le "Comme" de l'auteur laisse penser un lien de cause à effet entre l'affirmation des "experts" et celle de l'auteur — qui est techniquement erronée, une chaîne de bloc dispose d'un centre, mais celui-ci est distribué. Ce lien de causalité n'existe cependant pas.

Paragraphe 58 :

> Tout le problème repose sur le « pour le compte de chaque utilisateur ». Cette information suppose un tiers de confiance sur la légitimité duquel « l'ensemble des utilisateurs s'accordent ». Qui est ce tiers de confiance unanimement légitime ? Comment est institué ce tiers de confiance ? Qu'est-ce qui permet d'avoir un tel niveau de confiance en ce tiers si l'on ne dispose pas de moyens permettant de vérifier individuellement l'origine desdites transactions et opérations ?

Le fait que ces questions ne soient pas rhétoriques mais sincères pose un problème, car une compréhension effective du fonctionnement de la CDB permet d'y répondre :

- *Qui est ce tiers de confiance* : un pair tiré au sort par un mécanisme de consensus.
- *Comment est institué ce tiers de confiance* : par le tirage au sort du mécanisme de consensus.
- *Qu'est-ce qui permet d'avoir un tel niveau de confiance en ce tiers si l'on ne dispose pas de moyens permettant de vérifier individuellement l'origine desdites transactions et opérations* : il n'y en a pas besoin, étant donné que tous disposent des moyens de vérifier chaque transaction, qui est le principe même de la CDB.

Paragraphe 61 :

> Il est sans cesse répété que la technologie de la CDB « est révolutionnaire car elle instaure d'emblée la confiance dans le réseau, sans dépendre d'une autorité centrale » (Benchoufi, Chiche, 2016).

L'auteur n'utilise toujours pas une approche critique et répète à son tour les propos d'un think tank. De plus, selon l'auteur, la révolution de la CDB est qu'elle permet la confiance, ce qu'il remet en question immédiatement après. Le seul élément manquant à ses yeux c'est le fait de faire croire à la confiance, donc avoir confiance en le fait que le système soit digne de confiance (sans démontrer sa réalité).

Paragraphe 63 :

> Le principal danger du vote électronique concerne la sincérité du scrutin et le secret du vote

Non, ce ne sont que deux des dangers. Au-delà de la désanonymisation du scrutin (rupture du secret du vote) et de la sincérité (problème de coercition/achat de voix), on a surtout le problème de la modification du décompte final. Peu importe la manière dont les individus votent si on a la main-mise sur le résultat. De plus, l'auteur mentionne des "données infalsifiables, car cryptées". Or ces deux aspects sont indépendants, on peut tout à fait falsifier des données chiffrés (et non pas cryptées) [BLG+22]. Cette interprétation est d'ailleurs elle-même contradictoire avec celle présentée au paragraphe 23. Enfin, la note 34 montre une autre faiblesse technique de l'auteur et sa non-vérification de ses propres sources. Selon celles-ci, les bitcoins saisis par la justice américaine ne viennent pas d'un piratage de la CDB, mais de l'usurpation de l'identité de supposés terroristes.

Paragraphe 64 : L'auteur attaque à nouveau le secret du vote. Il remet en question la sincérité en utilisant comme source une rumeur "non démentie", dont l'impact est d'ailleurs complexe car elle correspond plus à une manipulation électorale (se maintenir pour favoriser son adversaire) qu'à une attaque contre la sincérité du vote.

> Partant de là, le secret du vote ne paraît pas nécessaire, bien que le juge constitutionnel y voie un élément de garantie de la sincérité du scrutin

L'auteur utilise donc la faiblesse supposée de la sincérité du scrutin — sans lien logique — que celle-ci implique que le secret du vote n'est pas nécessaire. Il n'offre pas de justification pour ce lien (il)logique. Il ignore encore une fois les rapports de domination existants dans la société et l'impact de ceux-ci sur la politique. D'ailleurs, les exemples abondent dans le milieu même de la CDB, où les mécanismes de vote des systèmes *code is law* sont souvent manipulés[17].

> En ce qui concerne la sincérité du scrutin, si le progrès technique permet de l'évacuer dans le vote par CDB, les humains entre eux trouveront toujours une manière de la fausser, à moins qu'une sanction exemplaire les en dissuade.

Si on admet l'existence d'une autorité pouvant distribuer des sanctions exemplaires et qu'on lui fait confiance pour le faire correctement, on sort du contexte décentralisé de défiance généralisée qui nécessite de recourir à une CDB, et celle-ci devient inutile.

[17] Voir notamment https://www.theverge.com/2022/4/18/23030754/beanstalk-cryptocurrency-hack-182-million-dao-voting.

Paragraphe 65 :

> Autrement dit, le secret du vote est-il si important que cela ? Ce secret n'est-il pas le reflet du manque de transparence dans le fonctionnement des institutions et des services que celles-ci assurent ?

L'auteur fait ici un amalgame grave. La transparence imposée aux acteurs puissants (notamment aux institutions) permet d'empêcher la corruption de ces derniers et les force à agir en faveur de la population. La transparence imposée aux individus augmente le pouvoir qu'ont les autres — notamment les institutions — sur eux. La transparence imposée aux premiers est donc une manière de préserver l'équilibre démocratique et de prévenir les dérives.

Paragraphe 66 :

> C'est ce qu'explique G. Mentré : « Les citoyens rendus participants et assesseurs du système souhaiteront bientôt s'exprimer sur les conditions mêmes du vote.

Le fait de pouvoir être assesseurs n'est pas une propriété unique des chaînes de blocs, voire ne l'est pas tout court, car cette activité est nécessairement automatisée dans le cadre de cette technologie.

L'auteur fait à nouveau une référence à Laurent Alexandre — qui n'est pas une source fiable ou neutre, avec une opposition artificielle entre progressistes ouvert aux changements — donc une science sans limite — et bioconservateurs. Il ne laisse donc aucune place à une éventuelle modération ou à des règles éthiques, qui doivent être sacrifiées en faveur du "progrès".

Enfin, l'auteur utilise une autre référence douteuse, Thinkerview, surtout vu la gravité de l'assertion (de Philippe Pascot) qu'il reproduit sans critique dans son article :

> C'est ceux qui seront derrière l'écran qui dirigent. Et j'ai des preuves aujourd'hui qu'il y a déjà des truandages sur le vote électronique, y compris des élections françaises

Paragraphe 68 :

> le recours aux blockchains rend possible la création d'une urne électronique qui permet d'établir le nombre de votants, sans que l'on sache vers qui se sont portés leurs suffrages », sans ignorer que le procédé de « la connaissance des pseudonymes utilisés par les électeurs permet [...] de retracer l'expression de leurs suffrages »

La CDB n'est pas la seule ni la meilleure manière d'atteindre cet objectif, et les systèmes de vote vérifiables savent faire mieux, qu'ils soient électroniques [Adi08, CGG19] ou non [Rya11, BS20].

Paragraphe 69 : L'auteur cite à nouveau un journaliste non-spécialiste dans un média grand public, au lieu de travaux plus sérieux. L'idée présentée par le journaliste et reprise ici par l'auteur comporte d'ailleurs des soucis évidents : si une autorité tierce attribue une clef à chaque électeur pour organiser un vote de la façon imaginée ici, cette autorité dispose d'une connaissance complète de qui a voté pour qui.

Paragraphe 70 : L'auteur cite à nouveau un éditorial d'opinion par le dirigeant d'une agence de conseils en communication sur les réseaux sociaux. Il ne cite pas non plus de sources pour certaines assertions (comme le fait que les opérations de vote sont confiées à des personnes âgées).

> Cela signifie que ces systèmes ne sont plus en phase avec la société des individus connectés et des nécessités politiques et sociales.

L'auteur fait ici une erreur de logique. Ce n'est pas parce que X est apparu avant Y que Y rend X obsolète.

> La question se pose alors de savoir ce qui pourrait justifier que cette même confiance ne puisse être mise dans les personnes manipulant les algorithmes de la CDB au nom de l'État dans le cadre d'un vote.

La réponse à la question de la justification est la différence de complexité et de compréhensibilité des systèmes de vote en question, qui est d'ailleurs manifeste ici. C'est d'autant plus approprié que l'auteur même de l'article semble avoir confiance en ces technologies sans même les comprendre.

Paragraphe 71 :

> À moins que la quantité d'espace nécessaire au stockage des données dans les CDB, qui se mesure en térabits, ne freine le développement de cette technologie.

Les chaînes principales sont plus petites que cela (au plus en centaines de gigaoctets pour Bitcoin ou Ethereum). De toute façon, peu d'ordinateurs de bureau sont aujourd'hui vendus avec des disques ne pouvant pas gérer de telles données.

Paragraphe 72 :

> Car, en effet, l'usage quotidien de la carte bancaire permet d'établir auprès de quel commerce un individu fait ses courses, voire quel type de produits il achète ou quel type de vêtements il porte, et ce fait ne paraît pas déranger outre mesure ; alors pourquoi le secret du vote devrait tenir tant à cœur ?

Le secret des transactions est un sujet d'inquiétude récurrent dans la recherche [CLWZ16] — et de nombreux utilisateurs ne sont pas au courant des informations conservées par les entreprises [KDFK15].

Mots de fin

Il est légitime de se demander pourquoi plusieurs auteurs — ainsi que des collègues relecteurs de plusieurs disciplines — passent 18 pages à critiquer 51 des 72 paragraphes de l'article original. Comme nous le disions dans la synthèse, notre but n'était pas de nous acharner sur Serge Surin mais de prouver que l'ampleur des fautes méthodologiques implique une inadéquation du processus d'évaluation de la revue *Amplitude du droit* qui pourrait surprendre vu le sérieux apparent de son comité éditorial. De plus, vu le caractère critique du sujet et son impact potentiel sur nos systèmes démocratiques (chaque publication scientifique aidant à établir la légitimité de ces pratiques), il nous semblait aussi nécessaire d'en expliciter les défauts sans trop tarder.

References

[Adi08] Ben Adida. Helios: Web-based open-audit voting. In *USENIX security symposium*, volume 17, pages 335–348, 2008.

[BLG+22] Enka Blanchard, Emmanuel Leblond, Antoine Gallais, Djohar Sidhoum-Rahal, and Juliette Walter. An analysis of the security and privacy issues of the Neovote online voting system. In *7th International Joint Conference on Electronic Voting – E-Vote-ID 2022*, 2022.

[BS20] Enka Blanchard and Ted Selker. Origami voting: a non-cryptographic approach to transparent ballot verification. In *5th Workshop on Advances in Secure Electronic Voting*, 2020.

[CCC+08] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. *17th USENIX Security Symposium*, 8:1–13, 2008.

[CGG19] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. Belenios: a simple private and verifiable electronic voting system. In *Foundations of Security, Protocols, and Equational Reasoning*, pages 214–238. Springer, 2019.

[Cİ13] Miguel Carreras and Yasemin İrepoğlu. Trust in elections, vote buying, and turnout in Latin America. *Electoral Studies*, 32(4):609–619, 2013.

[CLWZ16] Sherman SM Chow, Russell WF Lai, Xiuhua Wang, and Yongjun Zhao. Privacy preserving credit systems. In *International Conference on Network and System Security*, pages 184–199. Springer, 2016.

[Coh05] Sharon B. Cohen. Auditing technology for electronic voting machines. Master's thesis, MIT, 2005.

[Com17] Commission d'enrichissement de la langue française. Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés). 5 2017.

[Com19] Commission Nationale de l'Informatique et des Libertés. Délibération n°2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via internet. 2019.

[Coua] Cour Administrative d'Appel de Marseille, 5ème chambre. Décision n°19ma03754 du 16/12/2019.

[Coub] Cour de cassation civile, Chambre sociale. Décision n°20-17.073 du 24/11/2021.

[Cov85] Robert M Cover. Violence and the word. *Yale Law Journal*, 95:1601, 1985.

[EG14] Chantal Enguehard and Jean-Didier Graton. Machines à voter et élections politiques en France: étude quantitative de la précision des bureaux de vote. *Cahiers Droit, Sciences & Technologies*, 4(4):159–198, 2014.

[FRS18] Timothy Frye, Ora John Reuter, and David Szakonyi. Hitting them with carrots: Voter intimidation and vote buying in Russia. *British Journal of Political Science*, pages 1–25, 2018.

[GG20] Pierrick Gaudry and Alexander Golovnev. Breaking the encryption scheme of the moscow internet voting system. In *International Conference on Financial Cryptography and Data Security*, pages 32–49. Springer, 2020.

[Glo22] Global Engagement Center Special report. Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem. Technical report, United States Department of State, 2022.

[Jon03] Douglas W. Jones. A brief illustrated history of voting. *University of Iowa Department of Computer Science.*, 2003.

[KDFK15] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. My data just goes everywhere: user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security – SOUPS*, pages 39–52. USENIX Association Berkeley, CA, 2015.

[Kin78] Bruce L Kinzer. The un-englishness of the secret ballot. *Albion*, 10(3):237–256, 1978.

[Kin01] Ronald F. King. Counting the votes: South Carolina's stolen election of 1876. *Journal of Interdisciplinary History*, 32(2):169–191, 2001.

[Mar06] Pierre Martin. *Les systèmes électoraux et les modes de scrutin, 3e édition*. Montchrestien, 2006.

[Mer00] Rebeca Mercuri. *Electronic Vote Tabulation Checks and Balances*. PhD thesis, University of Pennsylvania, 2000.

[Mor14] Evgeny Morozov. *Pour tout résoudre, cliquez ici: l'aberration du solutionnisme technologique*. Fyp, 2014.

[MSG+19] Muhammad Izhar Mehar, Charles Louis Shier, Alana Giambattista, Elgar Gong, Gabrielle Fletcher, Ryan Sanayhie, Henry M Kim, and Marek Laskowski. Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack. *Journal of Cases on Information Technology (JCIT)*, 21(1):19–32, 2019.

[Mus18] Francesca Musiani. L'invisible qui façonne. études d'infrastructure et gouvernance d'internet. *Tracés. Revue de sciences humaines*, (35):161–176, 2018.

[OvdB04] Anne-Marie Oostveen and Peter van den Besselaar. Security as belief user's perceptions on the security of e-voting systems. In *Electronic Voting in Europe - Technology, Law, Politics and Society*, pages 73–82, 01 2004.

[PSNR21] Sunoo Park, Michael Specter, Neha Narula, and Ronald L Rivest. Going from bad to worse: from internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1):tyaa025, 2021.

[QBGF19] Joao Pedro Quintais, Balazas Bodo, Alexandra Giannopoulou, and Valeria Ferrari. Blockchain and the law: A critical evaluation. *Stanford Journal on Blockchain Law and Policy*, 2019.

[Rya11] Peter Y. A. Ryan. Prêt à Voter with confirmation codes. In *Electronic Voting Technology Workshop / Workshop on Trustworthy Elections – EVT/WOTE*, 2011.

[Sel04] Ted Selker. Process can improve electronic voting: a case study of an election. Technical report, Caltech/MIT Voting Technology Project, 2004.

[Sha93] Andrew L Shapiro. Challenging criminal disenfranchisement under the voting rights act: A new strategy. *The Yale Law Journal*, 103(2):537–566, 1993.

[SKW20] Michael A Specter, James Koppel, and Daniel Weitzner. The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in US federal elections. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1535–1553, 2020.

[Vin15] Priit Vinkel. *Remote electronic voting in Estonia: legality, impact and confidence*. TUT Press, 2015.

[Wat18] Kohei Watanabe. Conspiracist propaganda: How Russia promotes anti-establishment sentiment online. In *European Consortium for Political Research General Conference*, 2018.

[WDF18] Aaron Wright and Primavera De Filippi. *Blockchain and the law: the rule of code*. Harvard University Press, 2018.

[Wer18] Kevin Werbach. *The blockchain and the new architecture of trust*. MIT Press, 2018.

[Zal19] Monika Zalnieriute. From human rights aspirations to enforceable obligations by non-state actors in the digital age: The case of internet governance and ICANN. *Yale JL & Tech.*, 21:278, 2019.